***Contador Público Nacional y Perito Partidor***

# *Amanecer de las criptomonedas: un enfoque impositivo ante un nuevo paradigma económico en Mendoza, Argentina 2020*

**Autor:** NAVARTA, Pablo Germán

**Registro:** 26.771

**E-Mail**: pnavarta@navartayasociados.com.ar

**Profesor Titular:** BURKY, Diego

Mendoza, 2020

# Contenido

# Resumen Técnico

Las criptomonedas son un nuevo paradigma económico emergente basado en la criptografía, el cual debe ser analizado desde diferentes disciplinas para adaptarse a los cambios que producirá el mismo.

La presente investigación se propone enfocar su análisis desde el punto de vista tributario, para verificar la adecuación de este nuevo tipo de activo a las leyes impositivas nacionales y provinciales. Este trabajo es una investigación cualitativa exploratoria que se acerca al tema de estudio a través de la revisión y análisis documental.

Se han seleccionado como base para la revisión bibliográfica a libros de los autores más preeminentes del campo de las criptomonedas publicados en los años 2017 y 2018, que exponen en forma clara el funcionamiento de las criptomonedas desde el punto de vista técnico y económico; así como artículos de revistas especializadas en materia tributaria que tratan el tema en cuestión.

Los resultados indican que las criptomonedas están reguladas de manera muy incompleta frente a las distintas leyes impositivas nacionales y provinciales, donde el correcto encuadramiento de las mismas da lugar a múltiples dudas y termina en gran parte dependiendo del criterio de cada profesional.

Palabras clave: criptomonedas, Bitcoin, minería, billeteras, escasez, impuestos, criptografía, regulación.

# Introducción

Las criptomonedas son un fenómeno que han surgido explosivamente en la última década, y reflejan el producto de años de experimentación, así como la aplicación práctica de múltiples teorías económicas y criptográficas. Es un cambio de paradigma revolucionario, que busca completamente transformar el panorama de la economía mundial, y como tal debe ser profundamente analizado por diversas disciplinas para comprender sus efectos a corto y largo plazo.

A lo largo de los últimos 20 años pueden encontrarse numerosos intentos de llevar a cabo un sistema de dinero electrónico que no necesitase del respaldo de un bien físico para su operación, y fuese lo bastante seguro para realizar transacciones. Por diversos motivos (fallas de programación, escasa adopción, manipulación económica) todos fueron intentos fallidos.

No fue hasta el año 2008 que el programador anónimo Satoshi Nakamoto, basándose en prototipos anteriores como Digicash o Hashcash, elaboró un sistema de pagos digitales basado en criptografía, a los que incorporó un sistema de dificultad adaptable que denominó algoritmo Prueba-de-Trabajo. El resultado fue Bitcoin, la primera criptomoneda completamente funcional, que abriría el camino a una nueva forma de realizar transacciones electrónicas.

En nuestro país las criptomonedas no han sido prohibidas completamente por las autoridades gubernamentales, pero su uso tampoco es fomentado de ninguna manera. Tal es así, que no se le ha otorgado la importancia necesaria a la hora de establecer regulaciones para su uso.

La hipótesis de este trabajo plantea que la incipiente regulación tributaria de las criptomonedas ha generado incertidumbre y dudas entre los tenedores. Esta situación podría en su extremo generar que no sean declaradas ante los organismos de recaudación correspondientes, por lo que este prometedor sector económico se encontraría actualmente operando fuera de la ley. Esta investigación buscará por lo tanto, analizar profundamente las características intrínsecas de las criptomonedas para poder definir con mayor claridad el correcto encuadre jurídico-tributario de las mismas.

Este trabajo es una investigación cualitativa exploratoria que se acerca al tema de estudio a través de la revisión y análisis documental. Decimos que es cualitativa ya que es una forma de abordar el fenómeno, es flexible y abierta. Se basa en el análisis no estadístico de datos para luego formular propuestas de interpretación, es un enfoque amplio del estudio de problemáticas.

Es exploratoria ya que los estudios exploratorios, se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde nuevas perspectivas. (Hernández Sampieri, 2014)

Sabemos que la revisión bibliográfica, como momento ineludible de toda investigación científica, supone la aplicación de todo un verdadero método para estructurar la búsqueda, selección, procesamiento e inserción de los fundamentos teóricos del problema, el objeto y el campo de la investigación, en torno a los cuales se estructura el marco teórico de la misma.

En este trabajo el criterio de selección bibliográfico es el criterio de actualidad, que implica que las fuentes consultadas deben ser lo suficientemente actuales como para asegurar que reflejan los últimos avances de la disciplina, los más recientes hallazgos de la ciencia y/o los antecedentes empíricos más pertinentes referidos a sucesos ocurridos en el pasado reciente o en el presente.

Por último, se expone la estructura de organización del trabajo de investigación. La primera sección del trabajo expondrá el funcionamiento técnico de Bitcoin, la primera criptomoneda, como ejemplo del conjunto. Se partirá de ciertos conceptos básicos que deben considerarse respecto de las criptomonedas, para luego proceder a ahondar en los distintos elementos que componen el sistema. La segunda sección corresponde al análisis de Bitcoin desde el punto de vista económico. Se parte nuevamente de ciertos conceptos básicos, para luego analizar las características económicas de Bitcoin, y por último investigar su relación con diversas teorías económicas preexistentes. Por último, considerando todas las características de las criptomonedas ya expuestas, se realiza un análisis tributario de actualidad frente a las diversas leyes impositivas nacionales y provinciales, para determinar en la medida de lo posible su correcto encuadre frente a las mismas.

# Fundamentos Técnicos de Bitcoin

Esta sección del trabajo de investigación expondrá el funcionamiento de la criptomoneda Bitcoin desde el punto de vista técnico. Se basa en los trabajos del autor Andreas Antonopoulos, que es el autor más preeminente del ámbito de las criptomonedas y ha publicado numerosos libros y artículos al respecto.

## Capítulo I: Conceptos Básicos

*En este capítulo se expone de manera general el funcionamiento de Bitcoin y de sus componentes, así como la forma de almacenarlos y transferirlos.*

Bitcoin es un término que puede utilizarse para referirse principalmente a dos conceptos: una unidad de moneda y un protocolo de internet.

Como moneda actúa de manera similar a como podrían utilizarse otras monedas: sirve para comprar bienes o servicios, extender créditos, puede ser transferida o enajenada. Puede ser comprada o intercambiada por otras monedas (tanto criptomonedas como monedas tradicionales) en casas de cambio especializadas.

Como protocolo Bitcoin es un sistema peer-to-peer distribuido. Esto significa que no existe un servidor o punto de control central. La moneda Bitcoin es generada por este protocolo por un proceso denominado “minería”, que consiste en encontrar soluciones a un complejo problema matemático a la hora de procesar las transacciones.

Cualquier operador del sistema puede actuar como minero usando su poder computacional para validar las transacciones de la red. Cada diez minutos en promedio un minero puede validar las transacciones ocurridas en los últimos diez minutos y recibe a cambio nuevos Bitcoin que son generados por el proceso. De esta manera el protocolo descentraliza la emisión de nuevos Bitcoin y elimina en esencia la necesidad de la existencia de un Banco Central.

El protocolo incluye algoritmos que regulan la función de minado. La dificultad de las operaciones matemáticas se ajusta dinámicamente de forma tal que un minero siempre consiga resolverlas en aproximadamente diez minutos, sin importar la cantidad de mineros o de poder computacional estén compitiendo a ese momento.

El protocolo también reduce a la mitad el ratio a partir del cual nuevos Bitcoin son creados cada cuatro años, y limita el total de Bitcoin a emitir a la suma fija de 21 millones. Considerando que las nuevas Bitcoin son creadas aproximadamente cada diez minutos y la forma en que el ratio de emisión se reduce cada cuatro años, se puede crear una curva que prediga el número de Bitcoin en circulación en todo momento, que permite predecir que la cantidad de Bitcoin en circulación llegará al límite de los 21 millones en el año 2140. Como el ratio de emisión va disminuyendo con el tiempo, y como no pueden emitirse más Bitcoin por sobre el ritmo esperado de emisión cada diez minutos, se considera a Bitcoin como una moneda esencialmente deflacionaria.

Los componentes esenciales de Bitcoin son:

- Una red peer-to-peer descentralizada (protocolo Bitcoin)
- Un libro público de transacciones (cadena de bloques)
- Un juego de reglas para la validación de transacciones independientes y emisión monetaria (reglas del consenso)
- Un mecanismo para llegar a un consenso global descentralizado (algoritmo Prueba-de-Trabajo)

Bitcoin fue inventada en el año 2008 con la publicación de un ensayo titulado “Bitcoin: A Peer-to-Peer Electronic Cash System” escrito por Satoshi Nakamoto (un alias de un autor que nunca fue identificado). La clave de este ensayo que lo diferenció de otros sistemas de dinero electrónico antecesores fue la utilización de un sistema de computación distribuida (denominado Algoritmo de Prueba-de-Trabajo) para conducir una “elección” global cada diez minutos que permite a la red alcanzar un consenso acerca del estado de las transacciones sin necesitar de un coordinador central. El sistema fue diseñado para operar sobre principios matemáticos completamente transparentes, de código abierto, de manera tal que ni Nakamoto ni ningún otro individuo pueden ejercer control sobre el sistema.

Para acceder al protocolo Bitcoin es necesario un cliente que interactué con el mismo y provea de una interfaz para el usuario. A esta clase de cliente se lo denomina Billetera Bitcoin.

Existe una gran variedad de Billeteras Bitcoin y mucha competencia entre las mismas. Ofrecen funciones muy variadas y gozan de diversos niveles de confianza. Como es imposible nombrarlas todas las agruparemos según sus principales características.

Según la plataforma podemos hablar de:

- Billeteras de Escritorio: Operan como un programa que se descarga e instala bajo un sistema operativo como Windows o Linux. La primera implementación de un cliente derivada del trabajo de Nakamoto, conocida como Bitcoin Core, es una billetera de estas características. La seguridad de los fondos dependerá en gran medida de la seguridad del sistema operativo base.
- Billeteras Móviles: Billeteras para dispositivos móviles que operan bajo Android o iOS. Suelen priorizar la simplicidad de uso y la practicidad por sobre las funciones más complejas de un cliente. Son el tipo más común de billetera y suelen ser usadas para operaciones diarias.
- Billeteras Web: Se acceden a través de un navegador web y guardan sus datos en el servidor de un tercero, de manera similar a como opera el correo electrónico. Su principal ventaja es la accesibilidad ya que se puede acceder a ella desde cualquier computadora con conexión a internet. Sin embargo, es muy importante que la misma sea de confianza ya que los datos (y por ende los fondos) se encuentran completamente en el servidor del tercero. A su vez son susceptibles de los peligros propios del internet como el hackeo. Por lo tanto son poco recomendables para guardar montos importantes.
- Billeteras Hardware: Dispositivos especializados que contienen una Billetera autónoma en hardware diseñado para tal fin. Se interactúa con el dispositivo a través de un programa o una aplicación de celular, sin embargo todas las transacciones deben ser autorizadas a través del hardware por lo que no pueden ser atacadas remotamente. Se las considera sumamente seguras.
- Billeteras de Papel: Son billeteras *offline* donde los datos de acceso son registrados en un medio físico que generalmente es el papel (aunque pueden ser también de madera o metal) y no se comunican con la red hasta tanto no se reingresen a través de algún otro tipo de billetera. Este modo de almacenamiento offline es el más seguro, y se lo utiliza en general para proteger montos grandes que no van a ser utilizados en el curso habitual.

A su vez, según la forma en que interactúan con la red, podemos clasificarlas en:

- Cliente Completo: También llamados nodos, los clientes completos almacenan todas las transacciones de Bitcoin que hayan sido realizadas. Un cliente completo maneja todos los aspectos del protocolo, interactúa directamente con la cadena de bloques y puede validar cualquier transacción que se haya llevado a cabo de forma autónoma e independiente, pero al costo de un uso significativamente mayor de recursos informáticos.

- Cliente Liviano: Un cliente liviano interactúa con un nodo para acceder al historial de transacciones de la cadena de bloques, pero puede crear, validar y transmitir transacciones de manera independiente. No valida todas las transacciones de la red sino solamente las que pertenecen al usuario.
- Cliente API: Un cliente API no interactúa directamente con la cadena de bloques sino que lo hace a través del sistema de un tercero por medio de una Interfaz Programada de Aplicación (API).

Entre otras funciones, una billetera genera una Dirección Bitcoin a través de un juego de llaves públicas y privadas (explicada en la sección). Hasta que la dirección no recibe fondos la misma no es más que un valor teórico de una dirección posible, pero una vez recibidos los fondos pasa a ser conocida e identificada por la red Bitcoin. En general las direcciones son generadas localmente por la Billetera sin que se haga referencia o registración en ningún lado, y no deberían ser asociadas con ninguna información externa como por ejemplo la identidad del usuario.

Las transacciones de Bitcoin son irreversibles una vez han sido aceptadas por la red. Esto es siempre así para todas las circunstancias, ni siquiera pueden ser revertidas por casos delictivos como robo o estafa. Es esencial por ende que quien envíe Bitcoin comprenda plenamente el sistema y sea cuidadoso con el manejo de sus fondos. Para protegerse de este riesgo por parte del emisor es común que las instituciones y casas de cambio que operan con Bitcoin implementen procedimientos de verificación de identidad y conoce-a-tu-cliente (KYC).

Bitcoin, como muchas otras monedas, posee una tasa de cambio flotante. Esto significa que su precio variará respecto de la oferta y demanda que exista, y en general de manera muy frecuente. Es importante informarse acerca de la tasa de cambio vigente al momento de realizar una operación con Bitcoin.

El sistema de Bitcoin se compone de usuarios con Billeteras conteniendo llaves públicas y privadas, transacciones que se propagan por la red y mineros que producen (a través de competencia computacional) la cadena de bloques del consenso, que es el registro de todas las transacciones.

Una transacción le dice a la red que el dueño de cierto valor en Bitcoin ha autorizado la transferencia de dicho valor a otro dueño. El nuevo dueño puede entonces utilizar ese valor en una nueva transacción que autoriza la transferencia de valor a otro dueño, y así sucesivamente en una cadena de propiedad.

Cada transacción se compone de dos componentes: las entradas (*inputs*), que son como débitos a la cuenta de Bitcoin, y las salidas (*outputs*), que son como créditos a la cuenta de Bitcoin. Las salidas son

levemente menores que las entradas, y la diferencia entre ambas es la tarifa de transacción, que es un pequeño pago que obtiene el minero por incluir la transferencia en el registro de la cadena de bloques.

La transacción también incluye una prueba de posesión para cada *input* en la forma de una firma digital por parte del dueño, firma que puede ser validada independientemente por cualquiera. Por lo tanto, "gastar" Bitcoin equivale a firmar digitalmente una transacción que transfiere valor de una transacción anterior a un nuevo dueño, identificado por una Dirección Bitcoin.

Un ejemplo de este mecanismo sería: A genera una transacción tomando como entrada el valor que obtuvo en la salida de una transacción anterior. Genera una transacción transfiriendo ese valor a B y firma su entrada para autorizar la transferencia de valor, creando una salida para la dirección de B (menos la tarifa del minero). La dirección de B recibe esta salida y a partir de entonces es dueño del valor transferido por A, pudiendo utilizar esta salida como la entrada de una nueva transacción mediante el uso de su firma digital. Esto genera una cadena de propiedad donde se puede rastrear el cambio de posesión del valor de Bitcoin a lo largo de todas las direcciones que han tenido posesión.

La firma digital en Bitcoin sirve a tres propósitos:

- Prueba que el dueño de la llave privada (o sea, el dueño de los fondos) ha autorizado el gasto de esos fondos.
- La prueba de autorización que hace no se puede negar (no repudio).
- Prueba que la transacción (o alguna de sus partes) no ha sido y no podrá ser modificada por nadie luego de haber sido firmada.

Muchas transacciones contienen dos salidas, siendo una a la dirección del nuevo dueño y otra a una dirección del dueño actual. Esta dirección se conoce como la dirección de cambio. Esto es así porque las entradas de una transacción, como un billete, no pueden dividirse sino que deben ser gastadas por completo. Si A desea comprar algo por $ 5 pero tiene una entrada de transacción por $ 20 deberá utilizar completamente los $ 20 en generar dos salidas: una por los $ 5 de lo que desea comprar y otra de $ 15 que vuelve a su dirección como cambio. La dirección de cambio no debe ser necesariamente aquella de donde se originó la transacción, y muchas billeteras generan una nueva dirección para recibir el cambio de la transacción por cuestiones de privacidad.

En resumen, las transacciones mueven valor de una entrada de transacción a las salidas. Una entrada hace referencia a una salida de una transacción anterior, mostrando de donde se origina el valor transferido. Una salida de transacción dirige un valor específico a la dirección Bitcoin de un nuevo dueño,

y puede incluir una salida de cambio hacia la Dirección del dueño actual. Las salidas de una transacción pueden ser utilizadas como entradas de una nueva transacción, generando una cadena de valor de dueño a dueño.

Los nodos o clientes completos poseen el historial completo de todas las transacciones realizadas, y pueden al momento de generar una transacción validar la correcta posesión de la entrada de la transacción rastreando dicho valor a lo largo de la cadena de bloques hasta su origen. De esta forma se puede asegurar que no se pueda gastar un valor de Bitcoin del cual uno no es dueño legítimamente. Los clientes livianos no pueden realizar esta validación, sino que debe conectarse a un nodo al momento de generar la transacción y solicitar los datos necesarios para validar la posesión.

La transacción contiene en sí misma todos los elementos necesarios para ser procesada independientemente de cómo o dónde se realice la transmisión a la red Bitcoin. La red Bitcoin es una red peer-to-peer, donde cada cliente participante se conecta a múltiples otros clientes. El objetivo de esta red es propagar transacciones y bloques a todos los participantes. Cualquier nodo que detecte una transacción que no ha visto anteriormente la reenviará a todos los otros nodos a los que esté conectado, que la propagarán a su vez hasta que la transacción se encuentre en pocos segundos en un gran porcentaje de los nodos de la red. Sin embargo aunque haya sido propagada a los nodos, la transacción no forma parte todavía de la cadena de bloques, y para ello debe ser validada e incluida en un bloque a través del proceso denominado minería.

El sistema de confianza de Bitcoin se basa en la computación. Las transacciones se compilan en bloques, que requieren una cantidad enorme de computación para ser validados, pero solo una cantidad muy pequeña de computación para ser verificados como validados.

El proceso de minería sirve dos propósitos en Bitcoin:

- Los nodos mineros validan las transacciones haciendo referencia a las reglas del consenso de Bitcoin. Proveen entonces seguridad a la red rechazando transacciones inválidas o mal conformadas.
- La minería genera nuevos Bitcoin en cada bloque, como un Banco Central emitiendo moneda. La cantidad de Bitcoin creadas por bloque son limitadas y disminuyen con el tiempo, según un calendario fijo de emisión.

La minería busca un balance delicado entre costo y recompensa. Utiliza electricidad para solucionar un problema matemático y obtiene por ello una recompensa en la forma de nuevas Bitcoin emitidas y las

tarifas de transacción. Sin embargo, el minero solo puede cobrar su recompensa si ha validado correctamente todas las transacciones en cumplimiento de las reglas del consenso. Este balance delicado provee seguridad a la red de Bitcoin sin la existencia de una autoridad central.

La solución del bloque, denominada Prueba-de-Trabajo, requiere hacer repetidamente un *hash* del encabezado del bloque anterior y de un número aleatorio con el algoritmo criptográfico SHA256, hasta que una combinación con un patrón específico emerge. El primer minero en encontrar esta solución gana la ronda de competencia y publica su bloque en la cadena. Arribar a esta solución implica cuatrillones de operaciones de *hash* por segundo a lo largo de toda la red.

Nuevas transacciones fluyen constantemente hacia la red desde las billeteras y otras aplicaciones. A medida que son detectadas por los nodos se van añadiendo a un conjunto temporal de transacciones no verificadas que mantiene cada nodo. Cuando los mineros construyen un nuevo bloque añaden transacciones al bloque de este conjunto no verificado e intentar verificar su validez a través del algoritmo de minado.

Las transacciones se añaden a los nuevos bloques por prioridad según varios criterios, entre ellos la mayor o menor tarifa de transacción pagada. Cada minero comienza el proceso de minado ni bien recibe el bloque anterior de la red, utilizando este encabezado y llenándolo de transacciones, y comenzando a calcular la Prueba-de-Trabajo de este nuevo bloque. A las transacciones que incluye añade una propia, que le paga a su propia dirección la recompensa del bloque y la suma de todas las tarifas de las transacciones incluidas en el bloque. Si encuentra una solución válida para el bloque, el mismo se añade a la cadena de bloques y la transacción de la recompensa se vuelve válida y utilizable, efectivamente ganando la recompensa.

Algunos mineros pueden agruparse en asociaciones denominadas *mining pool*, donde todos aportan su poder computacional en un esfuerzo unificado para resolver el bloque, y si lo consiguen reciben una proporción de la recompensa en base al poder computacional aportado.

Cada vez que un nuevo bloque se va añadiendo a la cadena, se vuelve exponencialmente más difícil revertir una transacción ya incluida en la cadena, requiriendo cada vez más poder computacional. Un bloque posterior al de la transacción se lo llama una confirmación de la transacción, porque se ha encontrado un nuevo bloque válido partiendo de aquel que incluyó la transacción. Una transacción que ha obtenido seis confirmaciones (o sea, que se han minado seis nuevos bloques desde el que incluyó la

transacción) se la suele considerar irreversible ya que el poder computacional que sería necesario para invalidar estos seis bloques y revertirla es tan grande que no es práctico hacerlo

La seguridad de la cadena de bloques Bitcoin, distribuida y sellada cronológicamente, la hace atractiva para otros usos, como servicios notariales digitales o contratos inteligentes. Ciertas transacciones pueden ser creadas donde, en lugar de una dirección Bitcoin se envía información a la cadena de bloques. Los fondos enviados en esta transacción quedan perdidos para siempre, pero a cambio la información remitida queda también por siempre grabada en la cadena de bloques, pudiendo ser verificada públicamente por cualquiera como toda transacción.

Se puede establecer un bloqueo temporal sobre una salida de transacción, de modo tal que no se pueda utilizar esa salida en una transacción hasta que no haya transcurrido cierta cantidad de tiempo. También se pueden implementar bloqueos condicionales en la transacción, que impiden que se muevan los fondos hasta tanto no se haya cumplido una condición definida en un *script*.

# Capítulo II: Llaves y Direcciones Bitcoin

*En este capítulo se analiza el concepto criptográfico de llaves digitales públicas y privadas, y la forma en que se relacionan con las direcciones de Bitcoin, así como su encriptamiento y seguridad.*

Bitcoin está basada en criptografía, que es una rama de las matemáticas usada extensamente en la seguridad informática. Además de la transmisión de mensajes secretos (encriptación), la criptografía puede emplearse para demostrar que se conoce un secreto sin revelar dicho secreto (firma digital) o para probar la autenticidad de información (huella digital). Estas son las aplicaciones que son críticas para la implementación de Bitcoin y de sus aplicaciones.

La propiedad de Bitcoin se establece a través de la interacción de llaves digitales, direcciones Bitcoin y firmas digitales. Las llaves digitales no son almacenadas en la red, sino que son creadas y guardadas por los usuarios en un archivo denominado Billetera. Las llaves digitales de la billetera del usuario son independientes de la red, y pueden ser creadas inclusive sin acceder al internet.

Las transacciones Bitcoin requieren de una firma digital válida para ser incluidas en la cadena de bloques, que solamente puede ser generada con una llave secreta, por ende quien tenga una copia de esta llave tiene el control del Bitcoin. La firma digital testifica acerca de la verdadera posesión de los fondos que están siendo transmitidos.

Las llaves digitales vienen de a pares: una llave privada (secreta) y una llave pública, que son mayormente gestionadas por el software de la billetera. En la porción de pago de una transacción, la llave pública del receptor se representa por su huella digital, denominada Dirección Bitcoin. Las direcciones Bitcoin abstraen los receptores de los fondos haciendo el destino de las transacciones flexible, ya que se utilizan indistintamente para pagar a una persona, compañía, a efectivo, etc.

La llave pública se deriva de la llave privada, y sirve para recibir fondos. La llave privada sirve para firmar las transacciones para usar los fondos. Hay una relación matemática entre la llave privada y la pública que permite a la llave privada generar firmas en mensajes, que luego pueden ser validados contra la llave pública sin revelar la privada. Cuando se transmiten Bitcoin, el dueño actual presenta su llave pública y una firma digital (diferente cada vez, pero generada desde la misma llave privada). Con estos elementos, todos en la red Bitcoin pueden verificar y aceptar la transacción como válida, confirmando que la

persona que los transfiere era el propietario a la hora de la transmisión, pero asegurando que solo el dueño de la llave privada puede firmar la transacción.

Bitcoin emplea como su base criptográfica la Multiplicación de Curva Elíptica. Esta es una función matemática de las denominadas "irreversibles", ya que es muy sencilla de calcular en una dirección y casi imposible de calcular en la dirección opuesta.

Una billetera Bitcoin contiene dos llaves, una pública y una privada. La llave privada es un número, generalmente aleatorio, entre 1 y 2256, número astronómicamente grande. Obtenida la llave privada se emplea la Multiplicación de Curva Elíptica para obtener la llave pública. Luego, tomando como base la llave pública, se emplea una función de hash criptográfica de una sola dirección para generar una dirección Bitcoin. Esta es una función criptográfica que a partir de un valor emite una huella digital o hash de un tamaño determinado que la identifica. Luego es encriptada nuevamente en Base58Check que reduce a 58 sus caracteres con un checksum para ayudar a la lectura humana, evitar valores ambiguos y proteger contra errores en la transcripción de la dirección.

Una dirección Bitcoin es una serie de dígitos y caracteres que son compartidos con cualquiera que desee enviar dinero a ella. Si la transacción Bitcoin fuese un cheque, la dirección Bitcoin sería el beneficiario. Como el cheque, que emplea una abstracción para referirse a una persona o entidad sin especificar el número de cuenta bancaria, en una transacción Bitcoin una dirección Bitcoin puede representar a cualquier persona o entidad sin necesidad de especificar, o incluso a un script de computación automático. Esto la vuelve un instrumento de pago muy flexible.

Se pueden generar distintos tipos de direcciones Bitcoin. Una de ellas es el pago a un script de computación (Pay-to-Script-Hash o P2SH) que al recibir cierta cantidad de fondos en determinada dirección Bitcoin realiza una función automática determinada. El clásico ejemplo es al comprar algún artículo online con Bitcoin que se genera una dirección Bitcoin donde el comprador debe enviar los fondos en los subsiguientes 15 minutos para concretar el pago. Si el script detecta en este intervalo de tiempo el ingreso de los fondos valida la transacción y la mercadería es remitida. De lo contrario la transacción se da por anulada.

Otra dirección que puede usarse es la dirección multifirmas o multisig, donde se requiere la firma digital de más de una llave privada para poder utilizar los fondos. Funciona de manera similar a lo que sería una cuenta bancaria conjunta. Direcciones multifirma de 3 o más firmas son empleadas también por las empresas en las direcciones que reciben fondos de los clientes, requiriendo por ejemplo la firma digital

del tesorero y del gerente para mover los fondos. Cuando se aplica correctamente es una forma de proteger los fondos de la compañía contra el fraude interno o el robo.

Se puede aumentar la seguridad de la llave privada encriptándola a su vez con Base58Check basada en un password suministrado por el usuario. De esta manera, incluso si alguien obtiene acceso a la llave privada, la misma es inutilizable salvo que se conozca el password. Este método es muy recomendable para billeteras Hardware o billeteras de Papel, que están destinadas a guardar offline grandes montos de Bitcoin.

# Capítulo III: La red Bitcoin

*En este capítulo se analiza el funcionamiento de Bitcoin como una red de nodos interrelacionados, y su interacción entre los distintos participantes.*

La red Bitcoin está estructurada como una red peer-to-peer a través de Internet. Esto significa que los participantes son iguales entre sí, no hay nodos privilegiados o especiales, y todos comparten la carga de proveer los servicios de la red. No hay servidores, servicios centralizados o jerarquías en la red. Los nodos proveen y a la vez consumen los servicios de la red, siendo la reciprocidad el incentivo para la participación

Además del protocolo de la red Bitcoin, existen otros protocolos que interactúan con la red a través de servicios de enrutamiento, usados por pools de minería o ciertas billeteras. Se llama red Bitcoin extendida al conjunto de la red que incluye el protocolo Bitcoin y todos estos otros protocolos que interactúan con él.

Si bien los nodos son iguales entre sí, los roles que asumen no son necesariamente los mismos. Un nodo puede implementar cualquier combinación de los siguientes roles:

- Enrutamiento: Esta función la poseen todos los nodos sin excepción. Consiste en validar y propagar transacciones y bloques, y en descubrir y mantener conexiones a otros nodos.
- Cadena Completa: Algunos nodos, llamados nodos completos, mantienen una copia completa y actualizada de la cadena de bloques. Los nodos completos pueden autónomamente verificar cualquier transacción sin referencias externas.
- Minería: Los nodos mineros compiten para crear nuevos bloques corriendo hardware especializado para resolver el algoritmo Prueba-de-Trabajo.
- Billetera: Una billetera del usuario puede estar incluida como parte del nodo.

Además de lo anteriormente mencionado, existe una red secundaria, denominada red de relé Bitcoin, que actúa como relé para reducir la latencia de la red Bitcoin en la transmisión de bloques entre los nodos. Es especialmente útil para los nodos mineros, quienes deben reducir al máximo el período de espera entre la transmisión de un bloque ganador y el comienzo del minado del bloque que le sigue. Para ellos la reducción de la latencia está directamente relacionada con su ganancia.

Cuando un nuevo nodo se incorpora a la red, debe descubrir otros nodos para poder participar. Para ello debe poseer la dirección IP de al menos un nodo (sin importar cual, la geografía de los nodos no influye)

y establecer una conexión. Envía al nodo un *handshake*, esto es, un mensaje con información básica como la versión del nodo para determinar la compatibilidad. Una vez hecha la conexión, puede pedir la dirección de servidores DNS que contienen un listado de nodos permanentes de Bitcoin para interconectarse con todos ellos. Luego enviará un mensaje a estos nodos con su propia dirección IP, que estos a su vez propagarán con sus nodos vecinos, haciendo que el nuevo nodo sea más conocido e incorporado a la red. Como en la mayoría de los casos lo nodos no son permanentes sino que van y vienen, un nodo debe buscar constantemente nuevos nodos para mantener su conexión a la red.

Un nuevo nodo completo que se incorpora a la red solo posee un bloque, el bloque génesis. Cuando este se conecta a otro nodo intercambian información acerca de cuál es el último bloque que cada nodo posee en la cadena. El nodo que posee la cadena más larga identifica que el nuevo nodo está desactualizado y comienza el proceso para ponerlo al día. Envía un listado con el encabezado de 500 bloques, que el nuevo nodo empieza a solicitar y descargar uno a uno de todos los nodos de la red. Una vez haya obtenido estos 500 bloques, le remiten el listado de los 500 bloques siguientes, y el proceso se repite hasta que el nuevo nodo se pone al día con el resto de la red.

Un nodo liviano, en cambio, no solicita la descarga de todos los bloques sino solamente los encabezados, ocupando 1000 veces menos espacio en disco que los nodos completos. Por ende, no puede verificar él mismo la validez de todas las transacciones. Lo que hace es verificar la existencia de la transacción que le importa, y luego esperar que transcurra cierta cantidad de bloques luego de la inclusión de esa transacción en un bloque. El nodo liviano confía en que, si el resto de la red validó ese bloque y luego siguió sumando bloques nuevos a partir de este, entonces la transacción incluida en el bloque es válida.

Para mejorar la privacidad y seguridad de las conexiones, se puede configurar el nodo para establecer sus conexiones a través de la red TOR. TOR es una red que ofrece encriptación y encapsulación de la información a través de conexiones de red aleatorias que ofrecen anonimidad, intrazabilidad y privacidad.

## Capítulo IV: La Cadena de Bloques

*En este capítulo se analiza el funcionamiento de la denominada "cadena de bloques" y sus principales características.*

La estructura de la cadena de bloques es una lista ordenada de bloques de transacciones, donde cada bloque refiere al bloque anterior de la cadena. Cada bloque se identifica con un *hash* (creado por el algoritmo criptográfico SHA256) en su encabezado, que adentro contiene al *hash* del encabezado del bloque anterior. De esta forma se crea una cadena que va hacia atrás hasta el primer bloque de la cadena, denominado bloque génesis. Si un bloque es modificado, cambiará el *hash* de su encabezado, lo que a su vez causará un cambio en el encabezado del bloque siguiente, y este en el subsiguiente. Así, no puede modificarse un bloque sin la necesidad de recalcular todos los bloques que le sigan, lo que requiere una cantidad enorme de poder computacional, cantidad requerida que aumenta cada vez más a medida que más larga se hace la cadena. Por eso es que, cuando ya han transcurrido cierta cantidad de bloques siguientes, la cadena se vuelve inmutable.

Un bloque se compone principalmente de su encabezado y las transacciones que contiene. Su encabezado, a su vez, se compone de:

- El *hash* del bloque anterior.
- Una estructura de datos que actúa de resumen de todas las transacciones contenidas, denominada Raíz Merkel
- Un sello temporal que indica el momento de creación del bloque (momento a partir del cual el trabajo de los mineros se vuelve inútil y deben pasar a intentar calcular el bloque siguiente)
- La dificultad del algoritmo Prueba-de-Trabajo que tuvo calcular el bloque.
- Un número verificador, denominado *nonce*

Un bloque puede ser identificado por dos formas: por su *hash* que actúa como una huella digital única, o por lo que se denomina su "altura". La altura de un bloque es el número de bloque que se le asigna, donde el bloque génesis es el bloque 0, el siguiente es el bloque 1, etc.

El bloque génesis es el origen de la cadena. Todos los nodos sin excepción comienzan con el bloque génesis programado estáticamente, por lo que no puede ser alterado, y a partir de él se puede reconstruir toda la cadena para llegar a la actualidad. El bloque génesis posee un mensaje oculto: "The Times 03/01/2009 Canciller a punto de segundo rescate a los bancos". Este mensaje sirve para ofrecer prueba de la fecha exacta de creación de este bloque, haciendo referencia al diario *The Times* de esa

fecha. Sirve también como un mensaje dirigido a recordar la importancia de Bitcoin como un sistema monetario independiente, que surge en el contexto de una crisis monetaria global. Este mensaje fue grabado por Satoshi Nakamoto, el creador de Bitcoin.

# Capítulo V: Minería y Consenso

*En este capítulo se analiza el proceso de minería de Bitcoin, y su importancia para el correcto y seguro funcionamiento de la red Bitcoin.*

La minería es el proceso por el cual las transacciones son validadas y autorizadas. Es la razón de ser de Bitcoin, un mecanismo de seguridad descentralizado que es la base para el dinero digital. El propósito principal de la minería no es la creación de nuevas Bitcoin, esto es meramente un incentivo económico a los mineros para que realicen la función de seguridad dela red.

Los mineros validan nuevas transacciones y las registran en un registro público que es la cadena de bloques. Un nuevo bloque es minado cada 10 minutos en promedio, añadiendo más transacciones a la cadena. Las transacciones que forman parte de un bloque que se añadió a la cadena se consideran "confirmadas", y permiten a los nuevos dueños de los fondos a gastar los Bitcoin que recibieron en esas transacciones.

Los mineros reciben dos recompensas por la seguridad que proveen a la red: nuevas Bitcoin que son creadas en cada bloque, y las comisiones de las transacciones incluidas en el bloque. Para obtener estas recompensas los mineros deben competir para resolver un problema matemático basado en un *hash* criptográfico, que se denomina algoritmo Prueba-de-Trabajo. Se lo denomina así porque su resolución sirve de prueba de haber gastado una gran cantidad de poder computacional y electricidad (muchos consideran que esta es la base del valor económico de Bitcoin, un reflejo del gasto económico en electricidad y poder de procesamiento en el que incurren los mineros para mantener la red).

El proceso se denomina minería porque, como la minería de metales preciosos, otorga resultados que disminuyen con el tiempo. La cantidad de nuevos Bitcoin que los mineros pueden emitir en cada bloque se reduce a la mitad cada cuatro años (más precisamente cada 210.000 bloques) en un evento que se denomina *halving*. De esta forma, las recompensas del minado van disminuyendo exponencialmente hasta aproximadamente el año 2140, fecha en la cual se habrán emitido todos los Bitcoin (la cantidad total de Bitcoin no puede superar nunca los 21 millones, es su límite de emisión).

Por todo lo anterior (emisión fija de bloques cada 10 minutos reduciéndose exponencialmente con el paso del tiempo) podemos decir que Bitcoin es una moneda deflacionaria. Fue diseñada así intentando que el efecto deflacionario se produzca por una oferta restringida y no produzca un colapso de la demanda donde la gente almacene Bitcoin desmedidamente y se niegue a gastarlos. El éxito o fracaso de

este planteo económico se revelará con el paso del tiempo a medida que Bitcoin evolucione como sistema.

La red funciona a través de la cadena de bloques, que es un registro público de todas las transacciones que todos en la red aceptan como la verdad. ¿Pero como llegan todos a la misma conclusión sin tener que confiar en otros participantes de la red? Normalmente los sistemas de pago poseen una autoridad central que verifica las transacciones y otorga seguridad a los pagos realizados; Bitcoin, sin embargo, no posee esta autoridad central, la cadena de bloques se va construyendo individualmente por los nodos de la red, pero a pesar de ello todos son capaces de llegar a la misma conclusión.

La principal invención de Satoshi Nakamoto es el mecanismo descentralizado de *consenso emergente*. Emergente porque no surge específicamente por una elección o momento fijo, sino que va emergiendo de la interacción asincronizada de miles de nodos independientes, todos siguiendo reglas simples. Toda la creación en todos los aspectos de lo que es Bitcoin deriva de esta invención.

El consenso descentralizado de Bitcoin emerge de la interacción de cuatro procesos que ocurren independientemente en los nodos de la red:

- Verificación independiente de cada transacción por cada nodo completo, basada en una lista de criterios.
- Agregación independiente de esas transacciones en bloques realizada por los nodos mineros, junto con demostración de la computación realizada a través del algoritmo Prueba-de-Trabajo.
- Verificación independiente de los nuevos bloques por cada nodo y su incorporación a la cadena.
- Selección independiente, hecha por cada nodo, de la cadena que posea cumulativamente la mayor cantidad de computaciones hechas a través del algoritmo Prueba-de-Trabajo.

Las transacciones, como se explicó anteriormente, son propagadas por los nodos a través de la red. Sin embargo, antes de ello los nodos verifican que la transacción cumpla con ciertos criterios y requisitos. Al verificar las transacciones, cada nodo va armando un conjunto de transacciones válidas pero que todavía no han sido incluidas en un bloque. Los nodos que son mineros, además, toman de este conjunto de transacciones no conformadas y las usan para armar un bloque candidato, que luego intentarán incorporar a la cadena resolviendo el algoritmo Prueba-de-Trabajo. Cuando intenta generar el nuevo bloque, el minero debe incorporar el *hash* del encabezado del bloque que reconoce como el anterior. Al hacerlo el minero está tácitamente votando como que esa cadena que lo incluye es la cadena más larga de bloques, y por ende la cadena válida.

Puede ocurrir que dos nodos consigan validar un nuevo bloque en un similar período de tiempo, y propaguen su resultado a la red. Este evento se conoce como *fork*, donde dos cadenas diferentes se desprenden del mismo bloque. Aquí es donde el poder de votación de los mineros se explicita: los nodos mineros comenzarán a intentar crear un nuevo bloque a partir de uno de los dos bloques del *fork*, aquel que hayan recibido primero. La cadena que primero incorpore otro bloque será la ganadora (es muy poco probable que nuevamente se vuelva a encontrar un bloque para cada cadena en un período similar de tiempo) y la otra cadena pasa a ser una cadena secundaria. Estos conflictos suelen resolverse en el transcurso de un sólo bloque. El bloque de la cadena perdedora pasa a ser inválido, y las transacciones que contenía vuelven al conjunto de transacciones a incluir en un bloque futuro.

Este fenómeno es el origen de un posible vector de ataque hacia la red Bitcoin, denominado Ataque del 51%. En este escenario, un grupo malicioso de mineros controlando la mayoría del poder computacional de la red (51% garantizaría el éxito del ataque pero se puede iniciar con un menor porcentaje; cuanto mayor cantidad de poder computacional se posea más chances de éxito tendrá el ataque y más bloques pueden atacar), causan deliberadamente un *fork* algunos bloques atrás y reminan los siguientes bloques hasta que su nueva cadena se vuelve la más larga, y por ende la principal. Esto invalidaría las transacciones en los bloques de la cadena atacada, lo que permitiría a los antiguos dueños de los fondos volver a gastarlos en la cadena nueva (*double-spend)* y obtener gratis la contrapartida de la operación que habían realizado anteriormente, ya sea otra moneda o algún producto o servicio. Mientras más bloques quiera invalidar y reminar el grupo atacante mayor será el costo en poder computacional y electricidad, por lo que en la mayoría de los casos este ataque no es redituable (esto es así por la gran dificultad de minado de Bitcoin que hace que el rédito que se obtiene por las transacciones revertidas casi nunca compense el costo; sin embargo en el caso de otras criptomonedas con menor dificultad de minado es un ataque que se ha llevado a cabo y provoca un desplome de su valor). Por este motivo es una buena práctica de seguridad esperar al menos seis confirmaciones (seis nuevos bloques minados) antes de entregar el producto o servicio por el que se está recibiendo Bitcoin.

Las reglas del consenso determinan la validez de las transacciones y bloques. En el corto plazo son invariables, pero en el largo plazo pueden sufrir cambios. Implementar un cambio de las reglas en toda la red requiere mucha coordinación ya que todos los nodos deben cambiar a las nuevas reglas. Esto provoca una división en la cadena, denominada *hard fork*. Se diferencia en qué, mientras que el *fork* común es un acontecimiento que se depura con el tiempo ignorando la cadena secundaria, en el *hard fork* ambas cadenas permanecen ya que sus reglas son diferentes. Los nodos pueden optar por cambiar

sus reglas y seguir a la cadena principal, o no hacerlo y continuar minando la cadena vieja (pero ya no serían la cadena principal, pasarían a ser una criptomoneda diferente que se desprende). La implementación de un *hard fork* exitoso requiere de que se actualicen los software de las billeteras, nodos y mineros, y que todos a la vez acepten e implementen las nuevas reglas, por lo que se requiere bastante coordinación.

Puede realizarse también otro tipo de cambio de las reglas del consenso, denominado *soft fork*. Este no es un *fork* en realidad ya que no causa una división de la cadena, sino que implementa una nueva restricción a las reglas de ahora en adelante.

# Fundamentos Económicos de Bitcoin

*En esta sección del trabajo se analiza a Bitcoin desde un punto de vista económico, donde se tiene en cuenta sus características como unidad de valor o de transacción y su utilidad frente a las operaciones diarias que componen la economía mundial. Se utilizará para el análisis a la obra del autor Saifdean Ammous, economista especializado en criptomonedas.*

## Capítulo VI: Bitcoin como dinero digital

*En este capítulo se analizan las características generales del dinero en sí mismo, y de Bitcoin en particular como una nueva forma de realizar transacciones de valor*

Antes de la invención de Bitcoin se podía dividir a los medios de pago en dos categorías:

- Contado: Llevado a cabo entre dos partes presentes. Es inmediato y final, no requiere de confianza entre las partes, no hay demora en la ejecución y no puede intervenir un tercero para detener la transacción. El principal problema es la necesidad de que ambas partes estén presentes en el mismo lugar al mismo tiempo, en especial en la era actual de las telecomunicaciones.
- Pago por Intermediario: Un tercero de confianza actúa como intermediario entre ambas partes. La ventaja es que permite realizar operaciones sin que ambas partes tengan que estar en el mismo lugar al mismo tiempo, o tener que llevar el dinero encima para hacer el pago. La desventaja es que es necesaria confianza para la ejecución de las transacciones, que hay un riesgo de que el tercero se vea comprometido, y el costo y tiempo hasta que el tercero autoriza el pago y permite al receptor gastar los fondos.

Los pagos por medios digitales habían sido solamente a través de intermediarios porque los recursos digitales no son escasos. La información puede ser duplicada infinitamente y un usuario malicioso puede intentar gastar múltiples veces fondos que no tiene. La única forma de asegurar la honestidad de las partes intervinientes era a través de un tercero que gestionara la operación digital.

Bitcoin sin embargo finalmente surge como un medio de pago digital que no requiere de un tercero de confianza. Elimina los riesgos añadidos de robo o falla técnica que agrega el tercero en la operación, además de la vigilancia y control de las transacciones por parte de la autoridad política de turno.

La evolución de las transacciones a lo largo de grandes distancias ha hecho que las transacciones de contado se vuelvan imprácticas. Pero a medida que los usuarios han tornado más hacia los pagos digitales, más se ha reducido la soberanía de la gente sobre su dinero. Están sujetos a las arbitrarias decisiones del tercero que muchas veces es el depositario de los fondos, por lo que no tienen más opción que confiar en él. Además, el cambio de la moneda del oro (que nadie puede imprimir) hacia monedas estatales controladas por bancos centrales reducen aún más la soberanía de los usuarios sobre sus riquezas y los dejan indefensos frente a la erosión de su valor a medida que los bancos centrales inflan la base monetaria para financiar la operación del gobierno. Es cada vez más difícil acumular capital y riquezas sin el permiso del gobierno que emite ese dinero.

Satoshi Nakamoto buscó crear una moneda digital que no requiriese confianza en ningún tercero y que su oferta no pudiese ser alterada por ninguna otra parte. Traería las características deseables del pago contado (falta de intermediarios, finalidad de las transacciones) al dinero digital, combinado con una política monetaria de acero que no puede ser manipulada para producir inflación a expensas de los tenedores. Nakamoto alcanza esto a través de una red descentralizada sin puntos singulares de falla, hashing, firmas digitales y el algoritmo Prueba-de-Trabajo.

El aspecto más singular de Bitcoin es el ajuste dinámico de la dificultad de Prueba-de-Trabajo. A medida que más gente elige Bitcoin más sube su valor de mercado, lo que hace más rentable minar nuevas monedas, lo que lleva a más mineros a gastar más recursos en resolver problemas de Prueba-de-Trabajo. Más mineros significan más poder de procesamiento, lo que resultaría en las soluciones de Prueba-de-Trabajo obtenidas más rápido, aumentando la emisión. Pero a medida que el poder de procesamiento sube, la dificultad de Prueba-de-Trabajo aumenta para asegurar que la emisión de nuevos bloques se mantenga constante alrededor de 10 minutos.

El aumento en el valor de cualquier moneda lleva a más recursos dedicados a su producción, lo que termina en un aumento de la oferta ya que hay un incentivo en producir más, siendo las monedas más fuertes aquellas que más obstáculos poseen en su producción (como el oro). En cambio en Bitcoin un aumento de los recursos productivos no resulta en la producción de más Bitcoin, sino que lleva a un aumento en el poder de procesamiento necesarios para remitir transacciones válidas a la red, volviéndola más segura y difícil de comprometer.

El crecimiento meteórico del precio de Bitcoin se puede explicar por esta imposibilidad de aumentar la oferta más allá de lo programado: cuando la demanda de Bitcoin aumenta los mineros no pueden ofrecer más Bitcoin que las que obtienen según lo programado, y tampoco hay una autoridad central

que inunde el mercado emitiendo más Bitcoin. Por ende, la única forma que tiene el mercado para resolver la demanda creciente es aumentar el precio para convencer a los tenedores a vender sus Bitcoin a nuevos usuarios. Esto también es la causa de la gran volatilidad de Bitcoin ya que ante cambios de la demanda los mineros no pueden aumentar o reducir su producción para mover la oferta, sino que todos los cambios se verán reflejados directamente en el precio. A medida que Bitcoin evolucione como sistema, habrá menor cantidad de nuevos usuarios ingresado y por ende habrá menos fluctuaciones de la demanda, por lo que a largo plazo su volatilidad se reducirá.

La seguridad de Bitcoin subyace en la asimetría de costos entre registrar una transacción y verificar su validez. Registrar una transacción en un bloque implica enormes cantidades de electricidad y poder de procesamiento para resolver el algoritmo Prueba-de-Trabajo, mientras que verificar la validez de dicha transacción es prácticamente cero, y así seguirá siéndolo sin importar cuanto crezca la red. De esa forma, intentar hacer una transacción fraudulenta es gastar enormes recursos resolviendo Prueba-de-Trabajo, solo para que los demás nodos rechacen la transacción como inválida casi sin esfuerzo.

Bitcoin puede ser dividida en unidades de medida 100.000.000 más pequeñas (denominadas satoshis), lo que permite hacer operaciones por fracciones de Bitcoin de manera muy simple, y además está disponible para cualquiera que posea una conexión a internet.

Bitcoin descansa en incentivos económicos, que hacen que el costo del fraude sea mucho mayor que sus beneficios. Un nodo deshonesto se vería descubierto casi de inmediato, haciendo que obtenga nada a cambio de un gran esfuerzo en electricidad y procesamiento. Si en cambio, múltiples nodos deshonestos se asociaran, destruirían los valores sobre los que se sostiene la red de Bitcoin y su valor se desplomaría a nada, volviendo una vez más todo su esfuerzo inútil.

# Capítulo VII: Usos de Bitcoin

*En este capítulo se analizan en detalle las características de Bitcoin como dinero digital, y su posible uso en las operaciones cotidianas de la economía mundial*

## Reserva de Valor

El dilema que los humanos enfrentan con el tiempo consiste en como resguardar el valor de lo que producen empleando su tiempo hacia el futuro. Cualquier objeto que los seres humanos hayan elegido como reserva de valor subirá en valor, y como puede producirse más de este objeto, otros producirán más para intentar apropiarse del valor resguardado en él. Cualquier metal excepto el oro que fue usado como moneda fue sobre producido hasta que su precio colapsó. Los estadounidenses comenzaron a utilizar sus casas como medio de ahorro, pero entonces la oferta inmobiliaria aumentó tanto que el precio de ellas se desplomó. A medida que la inflación monetaria avanza, las distintas burbujas financieras pueden explicarse como apuestas especulativas para encontrar una buena reserva de valor. Solo el oro ha estado cerca de solucionar este problema por lo dificultoso que es incrementar su oferta, pero el control sobre él que han ejercido los gobiernos reemplazándolo por billetes que pueden emitir a voluntad ha arruinado su efecto.

Esto sirve para reflejar el gran suceso tecnológico que es Bitcoin. Por primera vez en la historia de la humanidad existe un activo cuya oferta está estrictamente limitada. Sin importar cuanta gente use la red, o cuanto suba su valor, o que tan avanzada sea la tecnología para producirlas, solo pueden haber 21 millones en existencia. Si la gente demanda más Bitcoin no puede incrementarse más la oferta para hacer frente a la demanda, solo puede apreciarse más la oferta ya existente. Como cada Bitcoin puede dividirse en 100 millones de satoshis, hay mucho espacio para que el valor aumente empleando menores unidades de valor. Por ello es que este es un activo bien diseñado para jugar el rol de reserva de valor.

Una implicancia importante de la emisión reducida de Bitcoin a un ritmo decreciente es que la oferta de Bitcoin existentes es mucho mayor que las nuevas monedas emitidas. Esto favorece que se empleen cada vez menos tiempo y recursos en generar nuevas monedas que en otras actividades económicas que puedan ser intercambiadas por Bitcoin. A medida que la recompensa por nuevos bloques disminuya, los mineros serán más recompensados por el procesamiento de las transacciones y la protección de la red que por la emisión de nuevas monedas.

## Soberanía Individual

Como el primer dinero digital, Bitcoin ofrece acceso a cualquier individuo a dinero soberano. Cualquier persona que posee Bitcoin tiene un nivel de libertad económica que no era posible antes de su invención. Los usuarios de Bitcoin pueden enviar inmensas cantidades de valor a lo largo del planeta sin necesidad de pedir permiso a nadie. El valor de Bitcoin no subyace en un medio físico, por lo que nunca puede ser completamente impedido, destruido o confiscado por cualquier fuerza física del mundo político o criminal.

Actualmente las naciones modernas, con sus leyes restrictivas, elevados impuestos y actuaciones arbitrarias han llegado a un nivel de represión de las libertades individuales similar a las impuestas por la Iglesia en la Edad Media. De la misma forma que entonces, se está preparando un cambio hacia una nueva forma de organización política y económica para reemplazarlo. Nuevas formas de organización emergerán de la tecnología informática, destruyendo la capacidad del estado de obligar a sus ciudadanos a pagar más por sus servicios de lo que desean. La revolución digital destruirá el poder del estado nacional sobre sus ciudadanos, reduciendo la significatividad del estado como unidad de organización y dando a los individuos un mayor poder y soberanía sobre sus vidas.

Un buen ejemplo de este proceso son las telecomunicaciones. En la Edad Media la imprenta fue revolucionaria porque permitió a los individuos comunes acceso al conocimiento que estaba prohibido o monopolizado por la Iglesia. Sin embargo, existía la limitación en la necesidad de producir libros físicos que podían ser confiscados, prohibidos o quemados. Esta limitación casi no existe en el mundo digital, donde todo el conocimiento humano existe disponible para los individuos sin que los gobiernos puedan eficientemente controlarlo o censurarlo.

La emergencia de las telecomunicaciones también ha reducido la importancia geográfica en el trabajo. Los trabajadores pueden estar domiciliados donde deseen mientras que los frutos de su labor, cada vez más informatizados e inmateriales, pueden ser transferidos instantáneamente a cualquier lugar del mundo. Las regulaciones gubernamentales e impuestos irán perdiendo su poder a medida que los individuos puedan vivir donde les plazca y entregar sus trabajos por telecomunicación.

A medida que el valor de la producción económica asume la forma de bienes inmateriales, el valor relativo de la tierra y los medios de producción físicos declina, reduciendo las ventajas de apropiarse violentamente de estos factores. El capital productivo se vuelve más encarnado en el individuo, haciendo que la amenaza de apropiación violenta sea cada vez más vacía, ya que la productividad de cada individuo está inextricablemente unida a su consentimiento. Los seres humanos ahora pueden

trasladarse a otra jurisdicción donde no se vean amenazados, o ser productivos en una computadora sin que el gobierno pueda ver o siquiera saber que están produciendo.

Había una pieza que faltaba en la revolución digital que era la transferencia de dinero y valor. Incluso si la tecnología de la información podía subvertir las restricciones geográficas y gubernamentales, los pagos seguían estando muy controlados por los gobiernos y el monopolio bancario que imponen. Como todos los monopolios impuestos por el gobierno, los bancos han resistido por años a aplicar innovaciones y cambios que beneficien a sus consumidores y limiten su capacidad de cobrar comisiones y rentas.

Bitcoin (y la criptografía en general) es una forma de tecnología defensiva, que hace que el costo de defender la información y propiedad sea mucho menor que el costo de atacarla. Hace que el robo sea costoso e incierto, y favorece por ello a los que desean vivir en paz sin agredir a otros. Reduce la dependencia del individuo en el estado para su supervivencia y bienestar. La desventaja que tenía la anterior mejor reserva de valor, el oro, era que no podía ser trasladado de un lugar a otro con facilidad, por lo que los pagos debían estar centralizados en bancos y bancos centrales y la confiscación era muy fácil. En cambio en Bitcoin verificar pagos es trivial y virtualmente gratuito, ya que cualquiera con una conexión a Internet puede acceder al registro de transacciones. Si Bitcoin continúa con su crecimiento y captura una gran parte de la economía mundial, puede obligar a los gobiernos a transformarse en una forma de organización voluntaria, que solo podrá obtener ingresos ofreciendo a los individuos servicios por los que estén dispuestos a pagar. Podría decirse que Bitcoin es una forma pacífica de anarquismo, que provee la infraestructura monetaria para un mundo construido únicamente por la cooperación voluntaria, y si resulta exitoso será por sus propios méritos tecnológicos y no por haber sido impuesto a otros.

En el futuro cercano, si Bitcoin fuera adoptado masivamente, es esperable que el costo de las transacciones aumente significativamente, por lo que no sea razonable para los individuos ejecutar para todos sus actos transacciones incensurables en la cadena de bloques evadiendo las regulaciones. Por ende, es esperable que alguna forma de control gubernamental o moneda estatal permanezca. Sin embargo de todas formas el efecto de la adopción masiva de Bitcoin en las libertades individuales será beneficioso, ya que reducirá la capacidad de los estados para financiar su funcionamiento a través de la inflación.

## Liquidación Internacional en Línea

Tradicionalmente, el oro era el medio de liquidación de los pagos y reserva internacional de valor. La dificultad de cualquier parte para incrementar de manera significativa su oferta lo hacía así. Sin embargo,

a medida que el oro fue retirado de las manos de los individuos hacia las bóvedas de los bancos, y luego bancos centrales, ya no fue posible liquidar los pagos internacionales entre individuos en oro. En cambio debieron ser realizados con las monedas nacionales emitidas por los gobiernos que fluctúan en su valor, creando problemas significativos para el comercio internacional.

La invención de Bitcoin ha creado una nueva alternativa independiente para la liquidación de pagos internacionales, que no necesita de ningún intermediario y puede operar completamente separada de la estructura financiera existente.

La posibilidad de cualquier individuo de correr un nodo Bitcoin y enviar su dinero sin permiso de nadie, y sin necesidad de exponer su identidad, es una diferencia notable entre Bitcoin y el oro. No es necesario que las Bitcoin sean guardadas en una computadora, ya que la llave privada que da acceso a las riquezas es una serie de caracteres que puede ser guardada en cualquier medio, o expresada en palabras mnemónicas que el individuo puede memorizar. Es mucho más sencillo moverse con una llave privada de Bitcoin que con una gran cantidad de oro, y puede ser enviado a través del mundo con mucho menor riesgo de ser robado o confiscado.

A medida que Bitcoin evoluciona en tener un mayor valor de mercado con mayores comisiones de transacción, tiene más y más apariencia de una moneda de reserva que de una moneda para las transacciones diarias. Incluso en el escaso nivel de adopción actual, la mayoría de las operaciones se producen en Bolsas o plataformas online como casinos virtuales. Estas plataformas debitan o acreditan Bitcoin en sus registros internos, y solo realizan transacciones en la red Bitcoin cuando los clientes depositan o retiran fondos. Es de esperar entonces que las transacciones cotidianas se realicen a través de aplicaciones de segundo nivel como estas, que emitan valores respaldados en Bitcoin, pero en los que todos los individuos puedan auditar en tiempo real las tenencias del intermediario y asegurarse de que no se esté produciendo inflación.

Es posible que la mayor ventaja comparativa de Bitcoin no consista en reemplazar a los pagos en contado, sino en permitir pagos en contado a través de grandes distancias. Bitcoin es actualmente el medio más rápido de liquidación de pagos internacionales en el mundo digital, que se vuelve más evidente al ser comparado con los métodos actuales. En la actualidad hay muy pocas monedas (principalmente el dólar, el euro y el oro) que son aceptadas para realizar pagos internacionalmente, y la mayoría de las transacciones deben ser realizadas en alguna de ellas. Realizar un pago internacional suele ser muy costoso ya que se deben abonar altas comisiones, a veces impuestos; suelen demorar varios días en ser liquidados y están sujetos a investigaciones invasivas de las instituciones financieras. El

alto costo de las transacciones suele darse principalmente por la volatilidad de las distintas monedas, y por la dificultad de la liquidación entre instituciones pertenecientes a distintos países, que necesita el uso de varios intermediarios.

Bitcoin es dinero libre del riesgo de la contraparte, y su red puede ofrecer liquidación final de pagos de gran volumen en cuestión de minutos. Es muy favorable en comparación con la liquidación de pagos entre bancos e instituciones financieras, no solo por su velocidad y bajo costo, sino por su verificabilidad de transacciones, seguridad criptográfica e invulnerabilidad respecto de fallas de seguridad de terceros. Es un dinero neutral que no le da a ningún país el privilegio extraordinario de emitir la moneda de reserva global, y que al estar separado de las economías nacionales no depende del desempeño económico de los países. Por ende su valor no se verá afectado por el volumen de las operaciones que se denominen en ella, evitando de esta forma los problemas de tasa de cambio que han plagado a todas las operaciones internacionales.

### Unidad Global de Medida

Desde el final de la era del estándar oro, el comercio global se ha visto dificultado por las diferencias de valor entre las monedas de los países. Esto ha destruido la capacidad de los individuos para conducir intercambios en un único medio y en vez ha causado que el comprar a lo largo de otros países deba ser precedido por comprar la moneda en la que opera el productor, en una forma semejante a lo que era el trueque. Esto ha dañado la capacidad de calcular económicamente las operaciones entre fronteras; y ha generado y agigantado una industria dedicada al intercambio entre monedas nacionales que, más que aportar mayor valor a las operaciones, se limita a amortiguar las malas consecuencias monetarias del nacionalismo.

El estándar oro proveía solución a este problema, donde una única forma de dinero. Independiente de cualquier gobierno o autoridad era el estándar mundial. Todos los precios podían ser medidos contra el oro y expresados en él, facilitando el cálculo entre fronteras. La dificultad de su traslado físico, sin embargo, llevo eventualmente a su centralización en bancos centrales que se hicieron cargo de la liquidación de los pagos internacionales entre ellos. Una vez centralizado el oro, los gobiernos no pudieron resistirse a su valor y tomaron el control del mismo, remplazándolo por dinero que ellos emiten y del cual controlan la oferta.

Todavía es temprano para decidir si Bitcoin podrá ocupar ese rol de unidad de medida única para el comercio y la actividad económica mundial. Para que esto se concrete Bitcoin deberá ser adoptado por una inmensa cantidad de gente, probablemente de manera indirecta como una moneda de reserva de

los bancos centrales. Se verá entonces si la estabilidad de la oferta de Bitcoin lleva a una estabilidad de su valor.

Actualmente Bitcoin constituye menos del 1% de la oferta global monetaria, por lo que transacciones individuales grandes o pequeñas variaciones en la demanda pueden causar grandes variaciones en su precio. Si Bitcoin tiene éxito en capturar una gran parte de la oferta global monetaria y de las operaciones de comercio internacional, la demanda debería hacerse mucho más predecible y estable, llevando a una estabilización de su precio. En ese punto, la demanda de Bitcoin será tan solo la demanda de dinero líquido, y el componente especulativo que está tan marcado en la actualidad desaparecerá. Esto es similar a la época del estándar oro, donde en los siglos que se utilizó el oro como unidad de medida su valor no aumentó ni disminuyó de manera muy significativa, volviéndolo la unidad perfecta de medida a través del espacio y el tiempo.

# Capítulo VIII: La Teoría de Juegos y Bitcoin

*En este capítulo se analiza uno de los fundamentos económicos más grandes de Bitcoin, la denominada Teoría de Juegos; y la forma en que Bitcoin manifiesta sus características frente a los diversos escenarios*

La Teoría de Juegos es una rama de la Economía que estudia el proceso estratégico de formación de decisiones, considerando las acciones que tomarán los competidores.

Según la teoría de juegos hay dos clases de escenarios: de Suma Cero, donde la ganancia de un individuo surge de la pérdida de otro individuo; y de No Suma Cero, donde la ganancia de un individuo no surge de la pérdida de otro individuo. También hay tres clases de elementos: los *jugadores* (que efectúan las decisiones), las *estrategias* que adoptan y los *resultados* que obtienen por ello.

## El Equilibrio de Nash

Se llama equilibrio de Nash (en honor al economista John F. Nash) a la solución donde cada jugador elige la estrategia óptima en función a las estrategias adoptadas por los demás, y no tiene más nada que ganar cambiando su estrategia.

El ejemplo más claro de un equilibrio de Nash es el llamado Dilema del Prisionero. Consiste en dos criminales capturados que no pueden comunicarse entre sí, y a los que se les ofrece el siguiente dilema:

- Si uno confiesa el crimen y el otro no confiesa, el que confesó queda libre y el que no tiene 7 años de prisión.
- Si ninguno confesa ambos obtienen 2 años de prisión.
- Si ambos confiesan ambos obtienen 4 años de prisión.

A simple vista parecería que el mejor resultado general es el escenario donde ninguno de los dos confiesa. Sin embargo este escenario es poco probable porque ambos saben que tienen una mejor oferta sobre la mesa si confiesan y el otro no confiesa. Al no poder comunicarse para ponerse de acuerdo, cada uno decidirá la mejor opción para ellos en base a sus circunstancias, que es confesar (ya que si el otro no confiesa quedan libres, y si también confiesa recibe solo 4 años, que es menos que lo que obtendrían si no confiesan y el otro sí). Por ende este dilema gravitará naturalmente hacia el escenario en donde ambos confiesan, que es el equilibrio de Nash.

Este simple escenario se complejiza si consideramos que una de las opciones por las que pueden optar es perjudicial para la sociedad. Por ejemplo, si en vez de decidir entre confesar y no confesar los

criminales deben decidir entre volver a robar o no volver a robar. Puede ser que la opción que más utilidad ofrezca a los individuos sea la que perjudica a la sociedad. Para evitar caer en una situación social de supervivencia del más fuerte, se debe incorporar al análisis un factor de castigo. El factor de castigo debe actuar de forma tal que, por cada punto de utilidad que pierda la sociedad en su conjunto, el individuo pierde mucha más utilidad. De esta forma se altera el equilibrio de Nash para que converja en un resultado que le sirva también a la sociedad además de a los individuos que toman la decisión.

## El Punto Schelling o Punto Focal

El economista Thomas Schelling llevó a cabo un experimento donde le preguntó a un grupo de personas: "Mañana debes reunirte con un extraño en Nueva York. ¿Dónde y cuándo te reúnes?". La respuesta más común fue ""Al Mediodía, en la terminal Grand Central". Esto fue así porque para los neoyorquinos, la terminal Grand Central es un punto focal natural.

Se define entonces al punto Schelling como lo siguiente: es la solución que los individuos tienden a usar en ausencia de comunicación, porque la consideran relevante, especial o natural.

Un ejemplo de esto sería: si dos personas aisladas, de la siguiente serie de números: 15876231, 1285496, 32654085, 1000000; deben elegir el número que piensan que la otra persona elegirá, lo más probable es que ambas elijan 1000000. Esto es porque este número es distinto a los demás, por lo que es percibido como más relevante.

## Equilibrio del Activador Siniestro

La mejor forma de entender el equilibrio del activador siniestro es a través de un escenario concreto. Supongamos un país donde gobierna un rey, y la gente cree que es inmortal porque es un ser divino, y por ello tiene derecho a mandar. Este rey es injusto, por lo que se organiza un grupo para asesinarlo, y lo consiguen. Al morir el rey, la gente comprende que no era inmortal ni hay un derecho divino de mando, sino que cualquiera puede enarbolar el poder de mando. Esto lleva a sucesivas e interminables guerras, revoluciones, opresiones; que ocasionan una masacre en el país y lo llevan a la ruina. La mejor solución entonces, consiste en no matar al rey.

## Problema de Coordinación

Un problema de coordinación típico consiste en un grupo de personas que se encuentran en un punto A y se las debe llevar a un punto B. Esto es muy sencillo de lograr cara a cara o por teléfono cuando el grupo es pequeño, pero a medida que el grupo aumenta más y más de tamaño la solución se complejiza. Además surge un factor adicional: ¿por qué el grupo debe cambiar al punto B?

Por lo tanto, un problema de coordinación se compone de dos factores: la comunicación exitosa entre los individuos y el incentivo para llevar a cabo el cambio. El problema de coordinación será un fracaso si tan solo la minoría realiza el cambio, y viceversa.

### Racionalidad Limitada

Un individuo todos los días va a la tienda a comprar comida. Cada día el dueño de la tienda va al baño por 5 minutos, y no hay cámaras de seguridad. El individuo podría fácilmente robar de la tienda sin ser atrapado, sin embargo jamás lo hace.

Este escenario es un ejemplo de lo que se denomina racionalidad limitada. Consiste en que un individuo tiene una decisión que hacer, suele elegir el camino más simple y al que está acostumbrado, aunque no sea el más beneficioso para él.

### Aplicaciones en Bitcoin

El sistema de Bitcoin está fuertemente respaldado en sus mineros. Ellos son los que verifican las transacciones y mantienen la seguridad de la red, además de emitir nuevas monedas. Por ende, el poder que manejan los mineros es inmenso, y si actuaran de manera deshonesta podrían causar un desastre en la red. ¿Cómo se puede asegurar entonces la honestidad de los mineros?

Consideremos primero todos los escenarios en los cuales un minero deshonesto podría atacar a la red para obtener beneficio personal, a saber:

- Inclusión en un bloque de una transacción inválida, que les de Bitcoin adicionales.
- Añadir bloques aleatoriamente sin preocuparse por validarlos con Prueba-de-Trabajo.
- Minar basándose en un bloque inválido para obtener más Bitcoin.
- Minar basándose en un bloque viejo, y crear una nueva cadena que le permita realizar un doble gasto.

La genialidad de la cadena de bloques es que está diseñada de manera tal que sea un equilibrio de Nash auto aplicado. La razón para esto es que la minería trae intrínseco un sistema recursivo de castigos:

- Cualquier bloque minado a partir de un bloque inválido es inválido también. Por lo tanto, los mineros evitarán minar a partir de un bloque inválido y malgastar recursos, y simplemente lo ignorarán.
- La misma lógica se aplica a la altura del bloque. Si todos los mineros están minando a partir del último bloque 100, ningún minero querrá arriesgarse a minar a partir del bloque 99 y desdoblar

la cadena, porque lo más probable es que todos los demás mineros sigan minando a partir de la otra cadena y su bloque se vuelva inválido.

Los dos escenarios anteriores se ven resueltos porque los mineros, como mayoría, optarán por el escenario más estable, el status quo, y este se vuelve el equilibrio de Nash. Para cambiar este status quo aparece un problema de coordinación imposible de resolver, porque la cantidad de mineros es tan grande que coordinarlos a todos resulta poco realista. Se puede aplicar entonces una conclusión derivada de la teoría del Problema de Coordinación: si la mayoría rechaza cambiar su estado, la minoría no tendrá ningún incentivo para permanecer en su estado cambiado.

Viendo el escenario desde la perspectiva de los usuarios, ¿por qué los usuarios preferirían la cadena principal en lugar de una nueva? La respuesta es que para ellos la cadena principal es un punto Schelling. La cadena principal se percibe como la opción más natural y relevante, y por ello le asignan valor. También puede explicarse como un caso de racionalidad limitada: permanecer en la cadena principal es lo más fácil.

Por último, supongamos un escenario donde se logre resolver el problema de coordinación, y un gran grupo de mineros que representan más del 51% del poder de minado de la red se ponen de acuerdo para atacar la cadena, minando una nueva cadena a partir de un bloque más viejo para volver a gastar fondos ya utilizados. Aquí se aplica el argumento del Activador Siniestro: ¿quién impediría entonces que la nueva cadena vuelva a ser atacada de la misma manera? Se entraría en un ciclo interminable de creación de nuevas cadenas, que destruiría completamente la confianza de los usuarios en la red, y provocaría que el valor de Bitcoin se vuelva cero. Por lo tanto, la única forma de que las Bitcoin de los mineros conserven su valor es no atacando la red en primer lugar.

Este último argumento no se sostiene si la criptomoneda en cuestión puede ser minada con CPU o GPU que pueden ser empleadas para minar otras criptomonedas luego del ataque. Los mineros maliciosos podrían realizar el ataque del 51% y vender los fondos obtenidos como fruto, destruyendo completamente el valor de la criptomoneda en el proceso, pero esto no les importaría ya que ellos pueden seguir trabajando en la otra criptomoneda.

En el caso de Bitcoin, sin embargo, el argumento vale ya que para minar Bitcoin actualmente con cierto grado de éxito es necesario adquirir chips especializados que solamente sirven para minar Bitcoin (denominados ASIC). Estos mineros especializados son considerablemente caros, y si no se emplean para minar Bitcoin son absolutamente inútiles. Los mineros, entonces, querrán proteger su inversión y no

realizarán un ataque que destruiría completamente su infraestructura y los dejaría fuera del mercado, ya que no pueden pasarse a otra criptomoneda con sus ASIC.

# Análisis Tributario

*Esta sección del trabajo analiza en detalle el encuadramiento tributario de Bitcoin impuesto por impuesto, teniendo en cuenta sus características únicas detalladas en las secciones anteriores. Se tiene en cuenta para el análisis opiniones de doctrinarios como Mihura Estrada que han tratado el tema, así como naturalmente el texto ordenado de cada una de las leyes tributarias nacionales y provinciales.*

## Impuesto a las Ganancias

### Criterio de la Fuente

El artículo 7 de la Ley de Ganancias (LIG en adelante) establece que se considerarán ganancias de fuente argentina a las ganancias provenientes de la tenencia y enajenación de monedas digitales *cuando el emisor se encuentre domiciliado, establecido o radicado en la República Argentina.*

Si bien esto puede ser un criterio de utilidad para ciertas criptomonedas que sí poseen un emisor centralizado, no lo es en el caso de Bitcoin. No puede decirse que Bitcoin tenga un emisor específico, sino que son emitidos por la interacción entre los mineros y la red. Los mineros en la práctica emiten la moneda, pero realmente lo que están haciendo es resolver cálculos matemáticos a cambio de una recompensa que les otorga la red, en ese sentido son más bien locadores de servicios que emisores. El minero no asume ninguna obligación por los Bitcoin que mina o vende, por lo que no puede decirse que haya un emisor (como en las acciones) que esté obligado a reconocer derechos u obligaciones que emanen de las Bitcoin.

Es necesario, por lo tanto, ir al criterio general del artículo 5 de la LIG, que establece que son ganancias de fuente argentina:

- Las provenientes de bienes situados, colocados o utilizados económicamente en la República.
- Las provenientes de la realización en el territorio de la Nación de cualquier acto o actividad susceptible de producir beneficios
- Las provenientes de hechos ocurridos dentro del límite de la misma, sin tener en cuenta nacionalidad, domicilio o residencia del titular o de las partes que intervengan en las operaciones, ni el lugar de celebración de los contratos.

Respecto del primer punto, no es posible decir que las Bitcoin se encuentren situados en la República Argentina ni en ningún otro país. Los Bitcoin se encuentran situados en la cadena de bloques, que se

encuentra simultáneamente en todos los diversos nodos a lo largo de todo el mundo. Hablar de nacionalidad en el caso de Bitcoin es tan inconsecuente como hablar de nacionalidad de la Internet.

Con respecto a los demás puntos, respecto de la tenencia y compraventa de Bitcoin tampoco es posible su aplicación. Esto es así porque en la compraventa no hay un lugar físico determinable de la misma, sino que se trata de la transmisión de un derecho de propiedad dentro de la cadena de bloques entre partes que pueden realizar la operación desde cualquier lugar. Se podría determinar la operación en base a la localización en que se realice el acuerdo o la nacionalidad de las partes, pero la Ley expresamente indica que no se tendrá en cuenta la nacionalidad, domicilio o residencia de las partes intervinientes, ni el lugar de celebración de los contratos.

Puede argumentarse la fuente argentina si el intercambio se realiza por intermediación de una página web argentina que pertenezca a un operador residente en el país (los comúnmente denominados *broker),* o si se los deposita a una empresa domiciliada en el país para obtener ganancias de capital. La intervención de un tercero con radicación en argentina es necesaria en este caso para asegurar la fuente argentina de las ganancias, cosa que se dificulta en un intercambio entre particulares.

Quien sí se encuentra claramente en el criterio del segundo punto son los mineros. Su operación requiere de una gran infraestructura que le genera sus beneficios, y si esa infraestructura se encuentra dentro del territorio nacional claramente el acto que produce esos beneficios debe considerarse también dentro del territorio nacional.

Respecto de la fuente extranjera, de manera simétrica el artículo 124 de la LIG establece como ganancias de fuente extranjera:

- Las que provengan de bienes situados, colocados o utilizados económicamente en el exterior.
- Las que provengan de la realización en el extranjero de cualquier acto o actividad susceptible de producir un beneficio.
- Las que provengan de hechos ocurridos fuera del territorio nacional, excepto los tipificados expresamente como de fuente argentina

Los inconvenientes que tiene entonces para encuadrarse las ganancias de Bitcoin como de fuente extranjera son similares. Podría determinarse la misma si la granja minera se encontrase establecida en el exterior, o si interviniese un *broker* domiciliado en el exterior.

Un caso de complicación especial consiste en las bolsas de intercambio de criptomonedas, comúnmente denominadas e*xchange.* Estos sitios web muchas veces son directamente imposibles de ubicar, pero los más reconocidos tienen domicilio físico verificable en el extranjero. Al operar con estos *exchanges* de forma habitual para obtener ganancias de capital, se estaría operando en una página extranjera y se tendrían por lo tanto los Bitcoin depositados en el exterior, sin embargo toda la infraestructura informática para realizar las operaciones y generar las ganancias se encontraría en el país. A diferencia de las acciones comunes donde el lugar de residencia del emisor soluciona el inconveniente, se produce aquí un conflicto entre el lugar en donde se encuentra ubicado el capital y el lugar donde se lo explota.

## Impuesto Cedular

La ley de Ganancias, en su artículo 98 inciso b) se refiere a "… monedas digitales, así como cualquier otra clase de título o bono y demás valores, **en todos los casos en moneda nacional con cláusula de ajuste o en moneda extranjera**: quince por ciento (15%)".

Esta expresión fue hecha revelando un claro desconocimiento de la situación especial que implica Bitcoin, ya que se infiere que el legislador pretende decir emitidas en todos los casos en moneda nacional con cláusula de ajuste o en moneda extranjera. Como bien indica Ricardo Mihura Estrada:

"El *Bitcoin* es un valor en sí mismo, no es emitido en moneda alguna, no tiene respaldo ni garantía de nadie, no contiene promesa ni obligación de que alguien lo habrá de cambiar o redimir por moneda nacional o alguna divisa. El valor del *Bitcoin* es intrínseco, es como el oro. Solo vale por la aceptación voluntaria que de él hacen sus adquirientes y depende de la combinación del interés especulativo del mercado, de la utilidad práctica actual o potencial que tiene el *Bitcoin* para algunos actores y del ritmo de la nueva emisión originaria. Por ello, hablar de moneda de emisión carece de sentido en estos casos". (Estrada, 2018)

Por lo tanto, teniendo en cuenta este hecho, que Bitcoin no está emitido en ninguna moneda nacional ni extranjera, se puede concluir que se encuentra fuera del encuadre del impuesto cedular.

La consecuencia de esto es que entonces necesariamente debe considerarse a Bitcoin dentro del impuesto integrado. Aquí es donde surge con plenitud el problema de determinación de la fuente indicado anteriormente, que dificulta el encuadre de Bitcoin como resultado de segunda categoría o como resultado de fuente extranjera. La enumeración taxativa que hacen de las fuentes argentina y extranjera los artículos 5 y 124 se aplican difícilmente a la cadena de bloques, que se encuentra alojada

en la Argentina y el resto del mundo en simultáneo. Queda por lo tanto Bitcoin en un limbo, donde hasta podría argumentarse que no se encuentra alcanzado por la Ley de Ganancias.

Otra consecuencia, posiblemente no prevista y no deseada por el legislador, es que si se determina que las ganancias por operar con Bitcoin pertenecen a la segunda categoría, entonces se podrán netear sus resultados contra las demás categorías, computar sus quebrantos y aplicarle las deducciones personales y específicas; así como inclusive ajustar por inflación su costo de adquisición (para aquellos casos que hayan sido adquiridas con posterioridad al 01/01/18).

Por último, siendo que Bitcoin no es una moneda ni nacional ni extranjera reconocida por la Ley, bien podría argumentarse que se trata de un bien en especie. Por ende, aquellos locadores de servicio que hayan recibido Bitcoin como su remuneración y los vendan en el transcurso de dos años atraerían la ganancia de la operación a la cuarta categoría, en virtud de lo dispuesto por el artículo 82 de la Ley y el artículo 177 del Reglamento.

## Impuesto a los Bienes Personales

Las criptomonedas no se encuentran mencionadas específicamente en la Ley del Impuesto sobre los Bienes Personales. Podría argumentarse su inclusión dentro de "dinero" pero es un concepto abierto a interpretación. El concepto de "dinero" suele emplearse para identificar a la moneda de curso legal o a otras monedas nacionales, y no a bienes cuyo valor es intrínseco como el oro o Bitcoin. Parecería ser que las criptomonedas han quedado también fuera del alcance de esta ley.

Otra posición frecuentemente adoptada es la de considerar a Bitcoin como un bien inmaterial por sus características intrínsecas, lo que llevaría a su exención del impuesto en virtud de lo dispuesto por el artículo 21 inciso d) de la Ley.

Por último, se puede considerar por un criterio residual a Bitcoin como incluídos dentro de la categoría de "Otros Bienes" que define la Ley. Esta categoría engloba a todos los bienes no definidos específicamente por la Ley, por lo que sería apropiado decir que Bitcoin puede considerarse dentro de ella.

Es importante aclarar que nuevamente surge para este impuesto el conflicto del lugar de residencia de las Bitcoin. Si se las fuese a considerar como bienes localizados dentro del país, entonces necesariamente deberán ser tenidas en cuenta para el cálculo de los Bienes del Hogar. Por el contrario, si se las considerase como bienes localizados fuera de la República Argentina, entonces el titular (siempre que

sea un residente argentino) deberá tributar sobre ellas por la alícuota diferencial que establece la Ley para los bienes en el exterior no repatriados.

## Impuesto al Valor Agregado

El caso de Bitcoin difícilmente encuadra como venta o prestación de servicios en el sentido habitual. Como indica Miguel Chamatrópulo:

"Las operaciones con *bitcoins* requieren formalizar digitalmente una "billetera" o "monedero virtual", en las cuales constarán las claves necesarias para permitir únicamente al propietario acceder a su tenencia de *bitcoins* y gestionar con ella en las diversas redes de *bitcoins* existentes. Al no tratarse de bienes físicos, el propietario, más que poseer bienes, dispone de firmas digitales que le permiten operar. Vemos entonces que, al transferir *bitcoins*, no existe entrega de bien ni prestación de servicios. Solo se realiza una declaración pública de que tales *bitcoins* deberán asociarse a la cuenta del receptor" (Chamatrópulo, 2014)

En el caso de los mineros, podría intentar encuadrarse su actividad en el inciso m) del apartado 21 del inciso e) del artículo 3 de la Ley (Servicios Digitales). Sin embargo, el artículo 1 en su inciso b) establece: "Las obras, locaciones y prestaciones de servicios incluidas en el artículo 3º, **realizadas en el territorio de la Nación**". Similarmente, el inciso e) indica: "Los servicios digitales comprendidos en el inciso m) del apartado 21 del inciso e) del artículo 3º, prestados por un sujeto residente o domiciliado en el exterior **cuya utilización o explotación efectiva se lleve a cabo en el país**...". Nuevamente entonces, la dificultad de fijar la territorialidad de Bitcoin provoca un conflicto en el encuadre de sus actividades bajo estos artículos.

## Impuesto a los Ingresos Brutos

El artículo 1 del Código Fiscal de la Provincia de Mendoza adopta una postura generalista bastante acertada, que permite encuadrar a Bitcoin dentro de ella, siendo el único limitante la habitualidad. De allí se desprende que aquellos que hagan comercio frecuente con Bitcoin, como los comerciantes habitualistas (*traders)* y los mineros que tengan residencia en Mendoza se encuentren alcanzados por este impuesto.

A su vez, podría considerarse como gravadas a las operaciones de intercambio y/o enajenación de Bitcoin que se lleven a cabo presencialmente (ya que a través de medios electrónicos se dificulta determinar la ubicación de la operación) dentro del territorio de la Provincia.

# Conclusión

A lo largo del trabajo se ha realizado un completo análisis de las características técnicas y económicas de Bitcoin, así como todos los posibles encuadramientos legales. Se expondrá por último a continuación la posición tributaria que considero que es la más apropiada para Bitcoin teniendo en cuenta todo lo ya expuesto.

Lo novedoso de esta forma comercial y el escaso conocimiento por parte de los legisladores de las características intrínsecas de Bitcoin han causado una especie de vacío legal alrededor del mismo, donde podría interpretarse hasta el absurdo tributario de que Bitcoin no esté gravado por ningún impuesto.

Es esencial, por lo tanto, que se haga una reforma a todas las leyes tributarias existentes considerando el caso específico de Bitcoin y todas sus posibles implicancias, de manera tal que se defina claramente su situación tributaria y puedan los contribuyentes cumplir con su obligación.

Considero que, respecto del Impuesto a las Ganancias, se debería incluir a Bitcoin en el impuesto cedular gravando su enajenación al 15%. Esto obedecería a la intención original del legislador, que únicamente ha dejado a Bitcoin fuera del impuesto por error y desconocimiento, y no porque esta haya sido su intención. Además sería aconsejable agrupar a Bitcoin junto con los resultados de enajenación de acciones, bonos y títulos valores a los cuales por sus características se asemeja. Los sujetos que deberían ser gravados por este impuesto son principalmente los residentes argentinos que realicen operaciones con criptomonedas, y secundariamente puede gravarse la renta que obtengan residentes del exterior sobre criptomonedas que puedan ser localizadas específicamente dentro del territorio de la República Argentina.

Respecto de Bienes Personales no estoy de acuerdo con la postura que considera a las criptomonedas como un bien inmaterial exento. Considero que, al redactar esta exención, la intención del legislador al excluir del impuesto a las marcas, patentes, invenciones, etc.; fue la de incentivar estas actividades y la producción y generación de las mismas. Bitcoin en cambio, se lo puede considerar como medio de ahorro (semejante al dólar, que está gravado) o como instrumento de especulación (como las acciones en el exterior, también gravadas). Por ende, considero que se debería gravar a Bitcoin por el valor de la tenencia cotizada al 31/12 del año fiscal. Los sujetos gravados, nuevamente serían principalmente los residentes argentinos que posean tenencia de criptomonedas, ya sea en el territorio nacional o en el

exterior; y secundariamente aquellos residentes del exterior que posean criptomonedas que por alguna característica de las mismas puedan ser localizadas como dentro del territorio nacional.

En el caso de Ingresos Brutos, el criterio fiscal se entiende claramente, y no es necesario entrar en discusiones. Se debe gravar por ende a los habitualistas y mineros radicados en Mendoza, y no afectar al mero tenedor de fondos.

Por último, en el caso del Impuesto al Valor Agregado considero que está bien que no se encuentre alcanzado por el mismo, ya que tanto la minería como el comercio son servicios que se llevan a cabo no necesariamente en la Argentina, y es sumamente discutible si el fruto de estas actividades puede considerarse como generado en el país

De todas maneras, los criterios enumerados anteriormente son considerando el marco fiscal vigente que no se adapta de manera satisfactoria a las características particulares de las criptomonedas. Sería necesario por lo tanto, que se realice una legislación específica sobre el tema que ahonde en el funcionamiento de las mismas y permita encuadrarlas en los respectivos impuestos sin dar lugar a conflictos como los ya mencionados.

# Bibliografía:

CHAMATRÓPULO, M. A. (2014). *Impuestos Varios. "Bitcoin". Tratamiento fiscal*. Doctrina Tributaria Errepar, 1. Recuperado de http://www.errepar.com.ar

ESTRADA, R. M. (2018). *Las "Monedas Digitales" y el Bitcoin en el nuevo Impuesto a las Rentas Financieras*. Doctrina Tributaria Errepar, 233. Recuperado de http://www.errepar.com.ar

ESTRADA, R.M. (2019). *Tenencias y ganancias (y pérdidas) de criptoactivos en las declaraciones juradas personales*. Doctrina Tributaria Errepar, 831. Recuperado de http://www.errepar.com.ar

ANTONOPOULOS,A. (2017) - *Mastering Bitcoin: Programming the Open Blockchain*, EEUU : O'Reilly

AMMOUS, S (2018) – *The Bitcoin Standard: The Decentralized Alternative to Central Banking* , EEUU :Wiley.

HERNÁNDEZ SAMPIERI, R. ,FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2014). *Metodología de la investigación*, (6a. ed. --.). México D.F.: McGraw-Hill.

## DECLARACIÓN JURADA RESOLUCIÓN 212/99 CD

El autor de este trabajo declara que fue elaborado sin utilizar ningún otro material que no haya dado a conocer en las referencias que nunca fue presentado para su evaluación en carreras universitarias y que no transgrede o afecta los derechos de terceros.

Mendoza, 27 de Febrero de 2020

Pablo Navarta
Firma y aclaración

26.771
Número de registro

35.925.162
DNI