Carrera de Contador Público Nacional

Bitcoin:
La Nueva Moneda del Mercado Digital

Trabajo de Investigación

POR

Bruno Javier Cacciavillani Magni
cacciavillanibruno@gmail.com

Federico Daniel Casas Sinner
fdsinner@gmail.com

Emiliano Nicolás Robledo
emilianorobledo00@gmail.com

Isaías Daniel Ruiz
ruizisaias155@gmail.com

DIRECTOR:

Prof. Ricardo Agustín Fornero

M e n d o z a - 2 0 2 1

Índice

Resumen

El presente trabajo de investigación funda su importancia en el análisis de la utilidad y facilidades que permite una nueva moneda digital. Dicha moneda se encuentra en etapa de auge, ya que cada día cuenta con más usuarios o poseedores de la misma; esto conforma una amplia red que va creciendo día a día. La amplitud de dicha red genera que la moneda sea cada día más aceptada y que una alternativa de pago respecto al papel moneda. Cabe mencionar que dicha moneda no sólo posee características que la hacen utilizable desde el punto de vista de las transacciones, sino que toma un segundo plano frente a su utilidad para todo tipo de inversiones la cual aumenta su significatividad constantemente.

Principales conceptos teóricos: Bitcoin es la más reciente tecnología digital que viene a ser presentada como una moneda. Es un invento que viene a aprovechar las posibilidades que existen en la era digital para solucionar distintos inconvenientes de la humanidad, como son el transporte de valor económico en el tiempo y en el espacio.

La moneda, para ser considerada como tal, debe poseer las siguientes funciones:

- MEDIDA DE VALOR. Ya que el valor de las cosas puede ser representado por medio de las unidades que ella representa.
- INSTRUMENTO DE ADQUISICIÓN DIRECTA. Puesto que permite adquirir cualquier bien en función de su valor.
- INSTRUMENTO DE LIBERACIÓN DE DEUDAS. Debido a que tiene una fuerza cancelatoria de las mismas al constituirse en un medio de pago reconocido legalmente.
- MEDIO DE ATESORAMIENTO DE RIQUEZA. Se puede atesorar para necesidades futuras debido a que conserva indefinidamente su valor.

Para ser considerado medio de pago, un instrumento debe poseer las siguientes características:

- El gran valor que representa con relación a su peso y volumen.
- Reconocimiento unánime como medio de pago, que impide juzgar acerca de su calidad.
- Su divisibilidad, que permite fraccionar su valor en forma ilimitada.
- La dificultad en su falsificación, que impide la circulación de un medio de pago que no se encuentra debidamente controlado, ya que en cada país se aprueba sólo una moneda a la vez.

Metodología: Se tuvo en cuenta un enfoque cuantitativo, en donde se plantea un problema de estudio delimitado y concreto. Se revisó la literatura y se constituyó un marco teórico, elaborando la hipótesis y sometiéndola a prueba.

Palabras claves: bitcoin, moneda, moneda digital, criptomoneda, blockchain.

Introducción

El bitcoin es un nuevo instrumento para las inversiones y las transacciones financieras. Es uno de los avances recientes de la tecnología digital, como medio para negociaciones y para el resguardo de valor. La dificultad relacionada con dicha moneda se centra principalmente en su corta vida en comparación con las monedas e inversiones tradicionales, lo cual dificulta poder analizar su impacto en dichos sucesos. La falta de observación y análisis de la misma dio pie a una serie de preguntas planteadas como fundamento para este trabajo. No obstante, hay una amplia gama de bibliografía escrita sobre bitcoin que permite servir de apoyo y sustento a diversas cuestiones que serán planteadas.

Las razones que motivan dar origen al presente trabajo se basan en la utilización que puede tener dicha moneda como medio de pago y como un instrumento de resguardo para que el valor de la moneda se conserve de una forma perdurable en el tiempo y que no se vea afectada por temas económicos, políticos ni geográficos.

Se pretende realizar una investigación que partirá desde el análisis histórico del dinero en general, teniendo en cuenta luego aspectos teóricos de Bitcoin como su funcionamiento y utilidad, para luego poder analizar las funciones de Bitcoin como moneda y como medio de inversión. En el presente estudio también se aportarán elementos adicionales de investigación desde el punto de vista normativo tributario y sus implicancias.

Metodología

La investigación responde a una metodología cuantitativa, ya que existe una realidad objetiva única, la cual no cambia por las observaciones y mediciones realizadas, cuya meta es descubrir, determinar y analizar los fenómenos buscando ser objetivos.

1) Tipo de investigación:
   - Según su profundidad: Es descriptivo, ya que su interés se centra en determinar la importancia en la utilización del Bitcoin, describiendo y enumerando sus principales ventajas y desventajas. También se analizarán sus características como medio de pago e inversión.
   - Según su alcance temporal: Es sincrónica o transversal, ya que se refiere a un período específico en el cual se recolectan datos para determinar y analizar la importancia e incidencia del Bitcoin.
2) Tipo de diseño:

- Es no experimental, ya que se investiga sin manipular las variables y no se influye sobre ellas. Se observan situaciones ya existentes, obteniendo datos a través de revisiones bibliográficas y observaciones del comportamiento del Bitcoin.

Organización del trabajo

En el presente trabajo se tratará el análisis e investigación que pueden realizar los Contadores Públicos respecto del Bitcoin, en donde se recurrirá tanto a bibliografía sobre distintas materias como legislación aplicable para llegar a conclusiones relativas a la materia en cuestión.

Capítulo I

Conceptos básicos

A. Historia del dinero

Para hablar sobre el Bitcoin, el cual es uno de los más recientes avances digitales en el último siglo, tenemos que conocer la evolución del dinero en el tiempo. Empezando desde los tiempos más antiguos hasta el presente, no solamente para entender cómo el mismo fue evolucionando, sino también el motivo de su progreso y relacionarlo con las necesidades del ser humano. El ser humano frente a sus necesidades busca alternativas para solucionar diversos problemas económicos relacionados con el dinero, la adquisición de productos necesarios y su ahorro.

Si nos remontamos a las épocas más antiguas, podemos encontrar aquello que se define como el intercambio directo. Éste consiste en intercambiar un producto por otro, que otra persona necesita.

Es lo que comúnmente se denomina trueque, en donde se puede observar que el instrumento de cambio que se usa son los mismos bienes que se intercambian; es decir, no hay un instrumento externo a dichos bienes que intervenga en la transacción. Dicha solución para realizar transacciones en la antigüedad trae aparejada una gran cantidad de problemas y de cuestiones adversas. Una de ellas podría ser la necesidad de encontrar otra persona que busque el producto que una persona tiene y que a su vez tenga lo que ésta necesita. La situación mencionada anteriormente podría describirse como una congruencia mutua de necesidades, pero no solo en cuanto al tipo de bien, sino en cuanto a la cantidad. Cuando se hace referencia a la cantidad quiere significarse que una persona puede desear cambiar alimentos por un auto, pero para el dueño del auto no sea de utilidad tanta cantidad de alimentos, ya que los mismos podrían ser perecederos.

De la necesidad descrita se plantea la necesidad de una respuesta a las situaciones planteadas, por lo que surge el concepto de dinero como instrumento de cambio.

La definición de dinero puede incluir:

1) “Pieza de oro, plata, cobre u otro metal, regularmente en forma de disco y acuñada con los distintivos elegidos por la autoridad emisora para acreditar su legitimidad y valor, y, por extensión, billete o papel de curso legal”. (Real Academia Española, 2001)

2) "Instrumento aceptado como unidad de cuenta, medida de valor y medio de pago". (Real Academia Española, 2001)

Teniendo en cuenta la definición anterior es posible analizar que en ciertos períodos de tiempo se utilizaron metales preciosos como medio de intercambio. Éstos cuales tenían ciertas ventajas, ya que eran duraderos, divisibles, fácilmente transportables en comparación con los trueques. Además, las monedas de plata y de oro tenían uso extendido entre diversas poblaciones del mundo ya que las mismas servían para realizar intercambios en los distintos lugares del mundo.

Durante muchos años el patrón oro fue el más utilizado y extendido. Pero los avances de la tecnología y de la civilización generaron una nueva concepción del valor del dinero. Tal es así que en determinados países existían grandes riquezas e industrias capaces de producir ingentes cantidades de elementos valiosos y útiles. En consecuencia, se empieza a dejar de lado la importancia que los metales preciosos tenían hasta ese momento para dar paso a lo que hoy conocemos como dinero fiduciario, aquél que se establece como dinero por decreto gubernamental.

> *"El dinero signo o dinero fiduciario es un bien que tiene un valor muy escaso como mercancía, pero que mantiene su valor como medio de cambio porque la gente tiene fe en que el emisor responderá por los pedazos de papel o por las monedas acuñadas y cuidará de que la cantidad emitida sea limitada."* (Mochón Morcillo y Beker, 2008)

Podemos apreciar que la evolución del dinero no termina con el dinero fiduciario tal como lo conocemos hoy, sino que ha habido distintos avances sucesivos en estos últimos años que han marcado un rumbo distinto al que se concebía años atrás. Los medios de pago electrónicos han tomado una gran fuerza. Dichos medios de pago electrónicos son las tarjetas de débito, crédito, transferencias bancarias y transferencias con código QR.

El tramo final de la evolución del dinero está marcado por las criptomonedas, que si bien son medios digitales de intercambio, tienen ciertas características que serán mencionadas en capítulos del trabajo de investigación que proporcionan una amplia gama de ventajas y desventajas frente al dinero fiat. (Ammous, 2018)

B. Definición y caracterización del bitcoin

El bitcoin es una moneda virtual, digital, en el sentido de que es intangible, sin existencia física. Es una criptomoneda, un instrumento basado en criptografía. Se origina en 2009, diseñada por Satoshi Nakamoto, que es un seudónimo que no se ha podido relacionar con una persona o grupo de

personas. La abreviatura utilizada tiene siglas que son BTC o XBT, además puede identificársela con el símbolo ฿.

Bitcoin se caracteriza particularmente por ser descentralizado, y por una red de transacciones P2P (peer to peer - de igual a igual), donde el principal interés de los usuarios es que no es emitido por ningún banco central o gobierno, por lo tanto, no depende de la confianza de las personas en los Bancos. Ello no obstante que ninguna entidad o persona controla su emisión, velocidad de emisión o circulación. Cabe aclarar que dentro del código de desarrollo de dicha moneda ésta no es infinita, sino que su máximo volumen será de 21 millones de unidades. El protocolo usado se destaca por eliminar los intermediarios, como son actualmente los bancos, tomando mayor preponderancia los exchange. Los exchanges son una de las formas de comprar y vender criptomonedas en la red; cabe aclarar que éstas también pueden ser obtenidas mediante el minado de las mismas.

Si indagamos más sobre sus características, tenemos que la cantidad de unidades nunca superará los 21 millones, que es una criptomoneda de libre acceso ya que no es posible restringir el acceso a la misma, permite el anonimato mediante la utilización de seudónimos, por lo que no se revela la verdadera identidad de quien envía y quién recibe bitcoins. Esta criptomoneda es divisible en unidades menores a un bitcoin, por lo que permite que el acceso a la misma sea más sencillo sin que los usuarios se vean obligados a desembolsar grandes cantidades de dinero al momento de realizar una compra. Esta moneda puede ser intercambiada en plataformas digitales, que son uno de los tipos de Exchange que existen, por monedas tradicionales como serían el peso, euro o dólar.

Respecto de los pagos podemos encontrar que es una red que permite una gran seguridad, como veremos en los próximos capítulos, al existir una cadena de bloques que la construyen. Al mismo tiempo permite que las transacciones no puedan ser alteradas, modificadas, ni eliminadas por lo que un error en cuanto al destinatario al que se le desea enviar podría generar un gran perjuicio irreparable. (Ammous, 2018)

C. Descentralización. Concepto

Entender lo que es descentralización en el mundo de las criptomonedas es un factor fundamental para el aprendizaje de las mismas; esta palabra es muy utilizada en la economía, es más, se considera la razón de ser del blockchain.

En el mundo la creación del dinero está centralizada, es decir, que para que exista cierta cantidad de dinero en el flujo de la economía una entidad lo tuvo que haber creado en algún momento con autorización estatal; esto es la típica figura de los Bancos Centrales de los distintos países como el “Banco Central de la República Argentina” o la FED “Reserva Federal de los EE. UU.”. Estos

agentes en la economía, además de crear el dinero también controlan el procesamiento del mismo en la economía, por eso se habla de monedas centralizadas, controladas por una entidad central.

En cambio las criptomonedas, especialmente el Bitcoin, están descentralizadas, es decir, no hay una única entidad que fabrica y pone bitcoin a disposición en el mercado y mejor aún, no está controlado el procesamiento de la misma. (Ammous, 2018)

D. Blockchain

La cadena de bloques es una base de datos compartida que registra todas las transacciones o eventos digitales que han sido ejecutados y distribuidos entre las partes participantes. Cada transacción es verificada por consenso de una mayoría de los partícipes del sistema, quienes poseen una copia exacta de la cadena. Una vez ingresada, la información nunca puede ser borrada. El blockchain contiene un registro exacto y verificable de cada una de las transacciones realizadas.

Bitcoin es el ejemplo más popular que utiliza Tecnología Blockchain. Su sistema ordena las transacciones, colocándolas en grupos denominados bloques y luego uniendo estos bloques a través de una cadena criptográfica. Las transacciones dentro de un bloque se consideran ocurridas al mismo tiempo. Estos bloques están unidos entre sí (como una cadena) en una línea cronológicamente ordenada, en la que cada bloque contiene el hash (número de identificación) del bloque anterior.

Cada bloque es introducido en el blockchain mediante la resolución de un rompecabezas matemático, también conocido como “prueba de trabajo”, en la que un nodo generador de un bloque necesita probar que ha utilizado los suficientes recursos informáticos para resolverlo. Este rompecabezas matemático no es sencillo de resolver y la complejidad del problema produce la demora de, en promedio, 10 minutos para que un nodo en la red de Bitcoin pueda realizar la correcta suposición y generar un bloque. El primer nodo en resolver el problema transmite el bloque al resto de la red. Sin embargo, ocasionalmente, más de un bloque será resuelto al mismo tiempo, llevando a posibles ramificaciones. A pesar de ello, el proceso matemático que requiere ser resuelto es muy complejo, y por ende el blockchain se estabiliza rápidamente. Esto quiere decir que todos los nodos alcanzan un acuerdo en relación al orden de los bloques.

Los nodos que donan sus recursos informáticos para resolver los rompecabezas y generar bloques se denominan mineros, y son recompensados financieramente por sus esfuerzos.

La red sólo acepta la cadena de bloques más larga como válida. Esto hace casi imposible para un agresor introducir una transacción fraudulenta, dado que no sólo debe generar un bloque resolviendo un rompecabezas matemático, sino también realizar una carrera matemática contra los nodos buenos para generar todos los subsecuentes bloques, en búsqueda de lograr que los otros

mineros en la red acepten su transacción como válida. Este trabajo es aún más difícil debido a que los bloques del blockchain están unidos criptográficamente.

La tecnología blockchain ha encontrado un amplio rango de aplicaciones en el mundo financiero y no financiero. Esto se debe a que cada operación online que involucra activos digitales, puede ser verificada en cualquier momento futuro, sin comprometer la privacidad de los activos digitales y partes involucradas.

Las instituciones financieras y bancos ya no ven a la tecnología blockchain como una amenaza a sus modelos tradicionales de negocios. Por el contrario: los bancos más grandes del mundo están buscando oportunidades en esta área, realizando investigaciones sobre aplicaciones innovadoras del blockchain.

Las oportunidades de aplicación en el sector no financiero también son infinitas, entre otros para contratos inteligentes, archivos de registros civiles, bancarios y médicos.

El consenso distribuido y el anonimato son dos características importantes y destacadas de la tecnología blockchain. En particular el anonimato genera un punto claro de controversia dependiendo de los fines para los cuales se busque. Dedicaremos un análisis especial, más adelante, de las desventajas que puede generar el mismo. (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2016) (Ammous, 2018)

E. Funcionamiento

Los Bitcoins pueden adquirirse en sitios web especiales, donde son intercambiados por monedas nacionales. El tipo de cambio del Bitcoin es determinado por el mercado en función de la oferta y la demanda.

Los pagos en Bitcoin pueden llevarse a cabo por cualquier persona con el software requerido en sus computadoras, smartphones o tabletas. Este software se denomina Billetera. El mismo actúa como una cuenta en la que se depositan Bitcoins. Cuando se produce un pago, al emisor del mismo se le debitan los fondos de su cuenta, los cuales se acreditan en la cuenta del beneficiario. Los pagos son realizados a través del intercambio de mensajes encriptados que son verificados dentro de la red del usuario.

La encriptación asimétrica permite que el emisor (persona A) y el receptor (persona B) de los mensajes encriptados puedan ser identificados con certeza. Esta requiere que A y B posean dos llaves de encriptación cada uno. Las llaves de cifrado son únicas y nadie puede tener las mismas que otra persona. Una de las llaves es pública, en otras palabras, es o podría darse a conocer públicamente. La otra es privada o secreta. Cuando A desea enviar un mensaje encriptado a B, utiliza la llave pública

de B para encriptar el mensaje. Posteriormente, el mismo sólo puede ser desencriptado usando la llave privada de B. Por lo tanto, B es la única persona que puede leer el mensaje.

La encriptación asimétrica también puede ser usada para firmar. Si A utiliza su llave privada para encriptar el mensaje, este sólo puede ser desencriptado usando la llave pública de A. La persona que desencripta el mensaje puede por ende estar segura de que fue enviado por A, debido a que nadie más tiene acceso a la llave privada de A. Esto es comparable a que A haya firmado el mensaje.

Para que A realice el pago de Bitcoins a B, ambos deben tener billeteras en sus dispositivos electrónicos, las cuales poseen una llave de cifrado privada y una pública.

La transacción comienza cuando B envía su llave de encriptación pública a A. Luego este último escribe una orden de pago a favor de B firmando con su llave privada, la cual es remitida a la red de usuarios de Bitcoin, quienes tienen que confirmar o verificar la transacción para ser validada.

La verificación del proceso se produce del siguiente modo: cada diez minutos, un minero de la red Bitcoin reúne las transacciones propuestas en el último periodo de diez minutos. Esto ocurre automáticamente, y la ronda de transacciones reunidas se denomina bloque. Los mineros tienen la tarea de verificar la transacción añadiendo el nuevo bloque al blockchain, es decir la lista oficial o registro de transacciones de Bitcoin verificadas, resolviendo un problema matemático cuya solución es difícil de calcular, pero sencilla de verificar una vez resuelta.

Los mineros compiten entre sí para definir quién encontrará la solución más rápido. Cuando un minero ha encontrado una solución, la misma es enviada a la red, en la cual otros mineros pueden simplemente verificar si la solución es correcta. La aceptación de la solución es tomada por decisión mayoritaria, en la cual el poder de votación de un minero depende de la extensión de la capacidad de cálculo o poder informático que él brinda a la red.

Como consecuencia de que la cadena de bloques contiene información del monto de los envíos y recepciones por parte de las billeteras, ésta puede ser usada para verificar el saldo de Bitcoins que posee una billetera específica. Esto implica que una billetera puede ser vista como una cuenta, cuyo número es definido por la llave pública.

Una transacción de Bitcoin no es completamente anónima, debido que al ser añadida al blockchain es registrada y automáticamente se encuentra disponible online. Por esto es bastante simple identificar las billeteras entre las que una transacción ha sido realizada. Sin embargo, es más difícil relacionar las billeteras a usuarios individuales. (Segendorf, 2014)

F. Funciones de una moneda

Para poder realizar un análisis de qué funciones características de una moneda cumple Bitcoin, primero hay que definir cuáles son las mismas. Ellas son:

- MEDIO DE PAGO O DE CAMBIO. Esta función hace referencia a que la misma es susceptible de ser aceptada como un instrumento válido para poder cancelar deudas y comprar bienes o servicios de la economía. Se requiere una aceptación generalizada de la misma dentro del sistema económico. La utilidad de que la moneda sea un medio de pago o cambio se basa en que la misma elimina la necesidad de una doble coincidencia de deseo, como hemos visto en el caso del trueque. Es decir, superamos la instancia del trueque para una forma más evolucionada de intercambio de valor. Ésta es una de las más importantes del dinero, ya que sin la misma carece de utilidad práctica el mismo.
- UNIDAD DE CUENTA O DE CAMBIO. Con esta función se logra otro avance muy importante, ya que la misma es la que permite llevar cuenta y medida del valor de los distintos bienes a los que se puede acceder. Permite así determinar el valor de los bienes entre sí de forma uniforme, y facilita la comparación entre diversas opciones de compra.
- DEPÓSITO DE VALOR. La realización misma de las transacciones, sean o no cotidianas, de productos esenciales o no, destinados al ocio o esparcimiento y de productos de capital deriva en una situación temporal. Esta situación temporal consiste en que existe una diferencia de tiempo entre el momento en que se produce la venta de un producto y la compra de otro producto, ya sea por razones de diferencia de valor que generan la necesidad de ahorrar para obtener dicho producto o por la falta de una necesidad inmediata de adquirirlos, sea por preferencias individuales o por razones de conveniencia individual. Por lo tanto, otra de las funciones del dinero va más allá del intercambio meramente inmediato, sino que busca ser un medio o instrumento que permita mantener el valor obtenido es decir ser un activo financiero para poder transportar ese valor a un período de tiempo futuro. Es posible afirmar que el dinero es la forma más liquida de depósito de valor, ya que existen otras opciones como títulos de deuda, acciones, etc.

El objetivo de que el dinero sea un depósito de valor radica en que éste sea suficientemente resistente a variaciones del nivel general de precios y no se vea alterado por dicha variación.

Patrón de pagos diferidos: Sin el dinero sería complejo plantear una situación de financiamiento para la gran mayoría de empresas e individuos, ya que es necesario fijar una medida de común acuerdo para la restitución de distintos prestamos en un período futuro. Sin embargo, en muchos países debido a las grandes tasas de inflación es necesario tener en cuenta ese componente en la determinación de la tasa de interés en la respectiva operación. Por lo que podemos observar que la función de reserva de valor se ve plenamente afectada.

Respecto del Bitcoin podemos realizar el análisis sobre el cumplimiento de las funciones del dinero.

Si realizamos el análisis respecto de ser un medio de pago o cambio, se puede ver en la vida cotidiana que Bitcoin carece de aceptación generalizada, aunque la misma se encuentre actualmente en gran ascenso. Sin más que realizar un análisis superficial, es posible tomar noción de que la moneda mencionada no puede ser utilizada en compras tanto en los negocios minoristas como en las grandes cadenas de supermercados, o shoppings.

Analizando la función de unidad de cuenta, ésta puede ser plenamente cumplida por la moneda, ya que su consistencia permite que los bienes o servicios se expresen en dicha moneda. Sin embargo, su principal característica o ventaja se encuentra por el lado de reserva de valor. Como veremos más adelante, Bitcoin desde su creación ha tenido numerosos avances respecto de su valor, es decir que no solo sirvió como reserva de valor sino como un instrumento por el cual mantuvo el poder adquisitivo y se acrecentó de manera simultáneamente. En comparación con el papel moneda tradicional surge que la moneda tradicional no mantiene su valor, sino que disminuye a lo largo del tiempo debido a la inflación. (Mochón Morcillo y Beker, 2008)

G. Requisitos de los medios de pago

Para poder decir que el Bitcoin u otra moneda es un medio de pago válidamente utilizable, necesita poseer ciertas características, entre las que podemos encontrar las siguientes:

- Poseer un valor intrínseco, ya sea por elementos tangibles o intangibles del mismo.
- Reconocimiento amplio en la economía como medio de pago. Se especifica la palabra amplio y no unánime, ya que no siempre la moneda local es aceptada de forma unánime en las transacciones de diversos activos de gran valor.
- Que sea susceptible de división, es decir poder dividirlo en tantas partes como sea necesario para realizar una transacción.
- Sistema que otorga una protección frente a falsificaciones y alteraciones del medio de cambio en cuestión.
- Posibilidad de determinar fácilmente la autenticidad de la moneda utilizada.
- Inmediatez en las transacciones.
- Seguridad en el intercambio.
- Bajos costos en su implementación.

Realizando un análisis de las características que debería tener Bitcoin para poder ser considerado un medio de pago válidamente utilizable, se puede observar que Bitcoin posee un valor intrínseco muy grande que descansa en los diversos protocolos y sistemas de emisión que hacen difícil la tarea de la emisión de nuevos Bitcoins al basarse en cálculos matemáticos cada vez más

complejos. Además, la cantidad de moneda a emitir está previamente determinada, por lo que no es infinita, como las monedas tradicionales. Por otro lado, podemos decir que tiene un amplio reconocimiento como activo valioso, pero aún no en todo el universo de las transacciones, lo cual cada día va evolucionando más, tendiendo así a una economía digitalizada. Como hemos mencionado anteriormente, una unidad de Bitcoin es divisible en fracciones menores por lo que se adapta de forma correcta para las distintas transacciones que pueden ser requeridas.

La cadena de datos llamada "blockchain" permite la interconexión entre las diversas bases de datos por lo que la falsificación del Bitcoin es muy dificultosa. A su vez esta misma razón es la que da facilidad al momento de comprobar la autenticidad de las monedas en cuestión.

Por último, cabe destacar que Bitcoin ofrece numerosas ventajas desde el punto de vista de la seguridad de las transacciones, de costos reducidos y de inmediatez en su transacción, por lo que estamos frente a una moneda realmente revolucionaria en los mercados globales.

Capítulo II

Análisis del nivel de sostenibilidad y desarrollo a largo plazo de la tecnología de cadena de bloques

A. Antecedentes y seguridad

Blockchain o cadena de bloques es una tecnología originada a principios de los años 1990 y que se hace notoria a partir de la aparición de bitcoin. Esta tecnología hace posible diseñar un sistema de seguridad altamente confiable para sustentar las transacciones realizadas por los usuarios. Dicha tecnología tiene como base las redes existentes P2P más conocidas como semilla a semilla mediante la criptografía avanzada. Blockchain permite alcanzar los fines que se plantean para bitcoin: seguridad, privacidad (en cuanto a emisores y receptores de las transacciones) y transparencia en el funcionamiento. El contexto social y económico en el que se da su nacimiento es un panorama en el cual las transacciones se encontraban altamente controladas por entidades bancarias e instituciones que poseían información plena en sus servidores y gestionaban los datos particulares de las personas involucradas en cada una de sus transacciones.

Como consecuencia de la situación mencionada anteriormente es como el nacimiento de esta moneda digital devuelve el equilibrio y anonimato de la información.

La red de cadena de bloques es la respuesta a la necesidad de un modelo de internet donde la información se encuentre descentralizada, segura y transparente.

Si hacemos un análisis integral de la principal tecnología de la cadena de bloques como son las conexiones semilla a semilla, tenemos que remontarnos a su fecha de creación que viene de fines de la década de los noventa. Este tipo de conexión sirvió como principal herramienta para compartir archivos entre distintos ordenadores sin la necesidad de un servidor que gestione estos datos almacenados en la nube, es decir la propiedad guarda y la disposición está a cargo plenamente de los usuarios involucrados.

Por lo tanto, en Bitcoin tenemos una red de usuarios que manejan la propiedad guarda y pone a disposición de sus criptomonedas sin necesidad de una institución que sirva de intermediario para la guarda y custodia. La cadena de bloques tiene similitud con un gran libro de contabilidad en el cual se registran cada una de las transacciones, sin olvidar que esta información es pública y plenamente

conocida por todos los usuarios que participan en la red. Cabe aclarar que podemos conocer qué transacciones se hicieron y los montos, pero no la identidad de quién las realiza. La base de datos de blockchain se asemeja a gran libro de contabilidad, además no hay que olvidar que es pública. En consecuencia, con lo anteriormente descripto resulta que todos los computadores poseen la información histórica de las transacciones, lo cual hace mucho más sencillo evitar las alteraciones y modificaciones de las transacciones de la red ya que los archivos se mantienen inalterables.

Al momento de realizar cada transacción se necesita validar las transacciones dentro de ese gran libro de contabilidad, y ésta es aprobada cuando ha sido revisada o validada por la mayoría de los participantes.

Cada nueva transacción está enlazada con la anterior, es por eso que recibe el nombre de cadena de bloques ya que todos están plenamente unidos como una cadena. (Antonopoulos, A., 2014)

B. Uso proyectado

La tecnología de cadena de bloques está en un punto de la historia en el que tiene un auge a nivel mundial, ya que múltiples monedas digitales utilizan la misma tecnología.

Esto permite que en el corto y largo plazo se sigan extendiendo en el universo de las transacciones producidas en los sistemas informáticos.

Bitcoin plantea una situación a futuro que promete transparencia, inmutabilidad, costos bajos, transacciones rápidas y confiables, además de privacidad en el manejo de la información. En este escenario, seguirá generando una adaptación de los demás sistemas de intercambio para acompañar el ritmo de la tecnología, factor que al día de hoy Bitcoin posee y seguirá incrementando.

C. Otras aplicaciones de la tecnología blockchain

Con lo expresado se pone de manifiesto los muchos usos que pueden hacerse de la tecnología blockchain. No sólo se puede usar en criptomonedas, para dar seguridad extrema originada en la estructura de bloques, sino también en otras actividades. La realidad actual es que se requiere un flujo de información para las transacciones y las decisiones que sea confiable y de rápido acceso. Sin embargo, un inconveniente que se aprecia es el gran volumen de información que circula es falsa o está distorsionada. Ya se ha mencionado el uso de blockchain como base de Bitcoin. El uso se está expandiendo a otras actividades que hasta ahora se desarrollan con tecnologías que son menos seguras y fiables en el resguardo y la comunicación.

Otro aspecto para tener en cuenta es que la tecnología en cuestión producirá un gran cambio informático frente a la burocratización de la información, por ejemplo, los Registros Públicos de

Propiedad podrán tener un gran avance frente a la seguridad de almacenamiento y la privacidad al momento de visualizar la información, permitiendo así tomar decisiones por parte del solicitante de manera mucho más segura y confiable.

Por lo tanto, la tecnología blockchain viene a dar justo en el punto y es la respuesta a la burocratización de la economía y la principal benevolencia es nuestro punto de vista es la fiabilidad que da al usuario de la información de saber que lo que está en el bloque blockchain es totalmente verdadero y no que esté dañado o modificado.

En un primer momento, serán los mismos notarios o escribanos quienes adoptarán estas nuevas herramientas. Pueden servir para digitalizar y hacer más eficiente su trabajo.

Actualmente, existen compañías que combinan tecnología de firma electrónica con certificación de blockchain para ofrecer soluciones de certeza digital, garantizando la autoría y la fecha cierta tanto de documentos como de procesos. Asimismo, la firma digital no es novedosa, pero al agregarle la tecnología blockchain la hace aún una herramienta más poderosa.

- Primero, ofrece una certeza total del momento en que fue firmado un documento.
- Segundo, garantiza que ese documento que fue firmado electrónicamente no pueda ser alterado ni en una coma.

La combinación entre la certeza de la fecha y la garantía de inalterabilidad del documento, sumado a la garantía de autoría que da la firma digital, hace que el servicio de estas compañías sea como el de un escribano. Si bien no tiene las mismas consecuencias legales ni las mismas obligaciones, es una solución digital casi perfecta de custodia de evidencia digital.

Usos más comunes de firma digital y blockchain:

1. La firma de contratos. Estas compañías ofrecen un servicio que asegura que el contrato se firmó en determinado momento y que no fue modificado. Esto se complementa con un servicio de validación de identidad que se realiza con datos biométricos y de organismos públicos.
2. Para dar garantía de custodia de fecha o información digital en casos en que lo requiere el marco regulatorio. Algunas empresas europeas utilizan la certificación de fecha en blockchain para cumplir con requisitos de compliance.
3. Algunas universidades utilizan este servicio para la emisión de diplomas digitales. En el blockchain, queda registrado quién recibió el diploma, en qué fecha y con qué calificaciones. Es una forma de evitar falsificaciones de títulos. (Antonopoulos, A., 2014)

D. Blockchain contra el cambio climático

El secretariado para las Naciones Unidas, es la entidad responsable de manejar el proceso político internacional para combatir el cambio climático a medida que la comunidad mundial trabaja para implementar el acuerdo de París es necesario utilizar nuevas tecnologías.

Con la tecnología de blockchain, la ONU cree que se puede utilizar para contribuir en una participación más grande de partes interesadas, en la transparencia y ayudar a aportar confianza y soluciones innovadoras en la lucha contra el cambio climático

El blockchain a diferencia de las redes centralizadas fue diseñada para evitar el monopolio del sistema, así la tecnología registra transacciones de manera abierta y permanente como ya hemos dicho, fomentado así la transparencia y seguridad. Las transacciones eliminan los intermediarios y esto tiene distintas aplicaciones vinculadas contra el cambio climático.

En primer lugar, muchos consumidores eligen comprar únicamente productos que sean producidos de manera sostenible y amigables con el medio ambiente, pero ¿Cómo asegurarse que el producto que está en el supermercado esté en esas condiciones? Ahí donde la tecnología blockchain entra en el juego ya que garantiza la trazabilidad de productos en sus cadenas de suministros que actualmente son complejas y opacas permitiendo al consumidor elegir productos sostenibles en líneas con los objetivos de la ONU contra el cambio climático.

En segundo lugar, el blockchain en combinación con sensores tiene el potencial de automatizar y fortalecer el monitoreo, el reporte y verificación del impacto ambiental de proyectos permitiendo un aumento en la confianza de los actores involucrados en estos proyectos.

Algunos de los temas que se trabajaron fue el desarrollo de aplicaciones de blockchain para combatir el cambio climático en áreas como el monitoreo de bosques, las transacciones de energías renovables y de bonos de carbono.

Si bien han sido mencionados aspectos determinantes por los cuales la tecnología blockchain puede ser beneficiosa para el cambio climático, pero nos encontramos con una disyuntiva importante. Al mismo tiempo que podría generar todos los beneficios enunciados anteriormente, la tecnología blockchain necesita de un consumo eléctrico muy grande seguido de una gran cantidad de hardware que genera efectos contaminantes en el medio ambiente. Por lo tanto, se puede concluir que no existe una opinión unánime sobre si es beneficiosa o no ya que genera al mismo tiempo efectos contrapuestos. Dicha situación es destacada desde el punto de vista de la forma en que se produce la energía que nutre estos sistemas de blockchain, la misma puede ser formas no contaminantes como sería la energía eólica o formas fuertemente contaminantes y dañinas para el planeta como el carbón, la energía nuclear. Por su parte, el hardware utilizado de manera masiva para procesar las transacciones se produce con materiales contaminantes como el plomo, cadmio y mercurio.

E. Contra el fraude en las elecciones

El uso del blockchain también se puede utilizar para implementar en el sistema de votación democráticas tanto de una región como de una empresa mejorando la calidad de las instituciones o las áreas de las empresas.

El uso de esta tecnología está orientada a resolver ciertos puntos donde todavía hay un alto nivel de centralidad o burocratización en el proceso electoral, por ejemplo, en una elección las autoridades que cuentan los votos son un grupo pequeños que generalmente son el gobierno, donde la posibilidad de auditar una elección está sujeta a ese tipo de autoridad.

En cambio, utilizando el blockchain cualquier votante o participante de esa elección puede auditar la elección sin requerir ningún permiso especial. Es decir, los votos están registrados en el blockchain y uno, sin requerir ningún tipo de autorización, puede verificar que su voto sea contado de forma correcta, al igual que los votos de los participantes que participaron en la elección. Por eso los distintos conflictos en el proceso electoral tradicional centralizado como el control de base de datos, el permiso de entidades registradas para participar en el conteo, etc., todo este punto de centralidad al operar en el blockchain de repente se democratiza y se reduce la posibilidad de coerción.

Hay otros aspectos que tienen que ver con garantizar la integridad del voto, desde el momento que el votante que emite su voto hasta que es registrado, donde la tecnología blockchain garantiza mucho más, ya que el votante al emitir su voto el mismo se registra en la entidad que contabiliza el voto (el blockchain) reduciendo la distancia, los intermediarios, evita la confusión donde se pueda alterar la integridad del voto en un proceso electoral.

Capítulo III

Análisis del Bitcoin como moneda

A. Comparación frente a monedas tradicionales

Si deseamos realizar un análisis justo entre las monedas tradicionales emitidas por instituciones oficiales de los distintos países, ya sea euro, dólar o peso argentino y las criptomonedas, en este caso particularmente estaremos desarrollando dicha cuestión para el Bitcoin tenemos que tener en cuenta distintos aspectos que son importantes destacar ya que ellos otorgan diferencias irreconciliables entre los dos modos de entender lo que significa una moneda y sus funciones.

Desde el punto de vista del intercambio, en las transacciones tradicionales intercambiamos papel moneda, es decir dinero, para conseguir un objeto de valor o un servicio de utilidad. En el caso del Bitcoin también puede llegar a ser utilizado para adquirir otro objeto de valor, pero posee ciertas particularidades. Esta cuestión puede explicarse ya que su valor no sólo tiene que ver con su aceptación, sino con las expectativas de crecimiento a futuro y el aumento repentino y brusco de aumento de valor que ha tenido en varias oportunidades. Por lo que en el mercado es visto no sólo como una posibilidad de mantener valor e intercambiarlo sino también como una forma de aumentar la riqueza.

Si visualizamos su proceso de creación esta moneda no necesita de papel o algodón, sistemas de impresión y tinta, sino que su obtención o minado como es generalmente mencionado, necesita de componentes informáticos de alta tecnología una gran cantidad de energía eléctrica para su obtención. Es así que bitcoin posee costos mucho más altos de fabricación que las monedas fiduciarias.

Otro aspecto para destacar es que las monedas tradicionales son hasta el momento físicas con posibilidad de ser resguardadas y transferirlas por medio del sistema bancario. Es decir, en su aspecto físico poseen limitaciones en cuanto a su traslado y resguardo. Dichas limitaciones se producen ya que el dinero en efectivo genera complicaciones para trasladarlo en grandes cantidades y trae aparejado un riesgo significativo en su seguridad debido a los posibles robos de éste.

El sistema bancario es una de las respuestas frente a las mencionadas limitaciones, permitiendo realizar transferencias fácilmente y facilitando el resguardo de éste. Sin embargo, al depositar el dinero fiduciario en una cuenta bancaria, el usuario pierde legalmente la propiedad de

éste. Es así como se suscribe un contrato de depósito en dinero, por lo que el banco tiene la obligación de restituirlo en la moneda de la misma especie a simple requerimiento del depositante. Por lo descripto anteriormente, podemos observar que nos encontramos con una promesa por parte de la entidad bancaria plasmada en un contrato avalado por el derecho y con los depósitos garantizados por el Banco Central de la República Argentina de que nuestro dinero será devuelto a simple requerimiento. Bitcoin tiene la ventaja de permitirnos almacenar gran cantidad de valor en un dispositivo físico o una billetera de papel, por lo que nunca perdemos la propiedad de éste. Es de suma importancia destacar que las claves privadas que se encuentran ya sea en el dispositivo físico o billetera papel deben ser resguardadas cuidadosamente ya que si éstas son extraviadas no hay forma de recuperar el acceso a los Bitcoin. Por el contrario, el sistema bancario permite al usuario recuperar sus claves de acceso de una forma más sencilla.

Otra característica limitativa de las monedas tradicionales es que no son aceptadas en todo el mundo, es decir uno para poder adquirir bienes y servicios en otro país debe previamente recurrir al mercado de cambios vigentes para poder realizar la conversión de la misma y adquirir moneda de curso legal. Bitcoin, por otra parte, al no ser emitida por ningún gobierno tiene ese aspecto potencial de globalidad que no poseen las monedas tradicionales. Esto quiere decir que, si bien hoy mismo no es posible utilizarla para comprar bienes en los distintos países, tiene mayor probabilidad de ser aceptada de forma generalizada en el futuro.

Desde el punto de vista de la inversión, podemos decir que las monedas tradicionales necesitan de un instrumento de inversión como lo son los plazos fijos, los fondos comunes de inversión y los bonos. Por su parte, las criptomonedas también son susceptibles de utilizarse para obtener una renta mediante depósitos a plazo, pero también es posible el acrecentamiento de valor con el sólo almacenamiento de la misma ya que suele incrementar su valor con el tiempo.

Si queremos basarnos en el aspecto inflacionario vemos que las monedas tradicionales sufren pérdida de valor debido a la constante inflación y el Bitcoin, por su parte no se ve afectado ya que no es un organismo estatal quien determina su cantidad de la misma. Por el contrario, desde su creación se previó la cantidad de monedas máximas que pueden ser creadas. Su principal variación de precio o cotización depende exclusivamente por la oferta y la demanda de la misma.

Si analizamos la forma de emisión, las monedas tradicionales son emitidas por los gobiernos, mientras que las criptomonedas son emitidas mediante el minado. Las transacciones tanto de Bitcoin y de monedas tradicionales poseen costos asociados y derivados de las mismas, por lo que el usuario debería abonar un precio por la realización de éstas. En el caso de las transferencias bancarias, dicho costo generalmente no se traduce en un precio que deba pagar el usuario ya que las transferencias bancarias nacionales entre personas humanas no poseen costo alguno para quien las realice. En el caso de transferencias bancarias internacionales, éstas si requieren el pago de un precio para la

realización. Por el contrario, para poder realizar transferencias de Bitcoin, es necesario que el usuario realice el pago de la misma.

Sin duda, ambos tipos de monedas tanto tradicionales como las criptomonedas más actuales poseen sus características propias. Pero es muy importante destacar que el sistema bancario actual se ve en una situación en la que debe adaptarse a los cambios y avances tecnológicos que plantean día a día las criptomonedas para no quedarse relegadas del mercado actual, si bien no son competidores directos, pero impulsan al crecimiento de la tecnología cada día.

B. Ventajas y desventajas de su utilización

Con el pasar de tiempo, las personas se han organizado en distintas agrupaciones de personas que precisan medios de pago y formas para ser capaces de intercambiar bienes o prestar servicios. Actualmente, es reconocida la importancia de descentralizar el modo en que éstos se adquieren, eliminando a los intermediarios. Las criptomonedas representan la respuesta de estas comunidades o agrupaciones de personas frente a los antiguos medios centralizados de pago, controlados por bancos, políticos y grupos de interés.

Las ventajas del Bitcoin se definen del siguiente modo:

- PROTECCIÓN DE DATOS PERSONALES. Existe un bajo riesgo para los distintos usuarios de Bitcoins, frente a casos en los que sus proveedores o socios se vean expuestos a un ciberataque y pierdan información personal o financiera, tanto de sus clientes como propia. Los usuarios de Bitcoins se encuentran en riesgo únicamente si los hackers obtienen acceso a sus llaves privadas, las cuales deberían estar resguardadas frente a los terceros.
- BAJOS COSTOS DE TRANSACCIÓN. Son más bajos que los que actualmente ofrecen las distintas tarjetas de crédito, por lo que las tarifas impuestas por este tipo de transacción se ven reducidas en los negocios que aceptan pagos en Bitcoins.
- LA VELOCIDAD DE LA TRANSFERENCIA PROTEGE A LOS COMERCIANTES DE LOS CARGOS DE DEVOLUCIÓN POR FRAUDES. Un pago de Bitcoin es confirmado en un lapso de 10 a 30 minutos, mientras que un banco podría necesitar varios días para concluirlo. Es necesario aclarar que nos referimos a los pagos realizados con tarjetas de crédito ya que éstos son acreditados en la cuenta del vendedor una vez cumplido el plazo pactado. Dicho plazo es elegido por el vendedor de acuerdo a las opciones que ofrezca el emisor de la tarjeta. Es decir, a menor plazo la comisión que le cobrará al vendedor será mayor. Esto da lugar a que el proveedor de tarjetas de crédito pueda demandar al vendedor el reembolso de las pérdidas producidas frente a transacciones fraudulentas. Además, las

transacciones con criptomonedas son irreversibles, excepto en el caso en que el vendedor acuerde lo contrario con sus clientes, por lo que el riesgo de fraude es insignificante.

- BITCOIN ES INMUNE A LA INFLACIÓN. La tasa de inflación monetaria del Bitcoin se reducirá a una tasa fija a medida que el número de Bitcoins en circulación continúe incrementándose a tasa constante hasta alcanzar su límite máximo de 21 millones.
- SU ACEPTACIÓN HA CRECIDO VERTIGINOSAMENTE EN DIFERENTES COMERCIOS DE DISTINTOS PAÍSES. Esta moneda ha tenido un gran incremento en su aceptación con el transcurso del tiempo. Tal es así que es posible utilizarla para diversas compras vía web y también en algunos locales físicos como sería Burger King.
- ES SEGURA. Es imposible la falsificación o duplicación de las criptomonedas gracias a una sofisticada combinación de técnicas criptográficas. En este sentido, cada persona cuenta con claves criptográficas que son necesarias para realizar cualquier tipo de operación digital.
- ES TRANSPARENTE. Todas las transacciones realizadas a través de blockchain son públicas. El archivo de la cadena de bloques se guarda en múltiples ordenadores de una red, y no en un solo lugar. Así, este tipo de almacenamiento permite que sea legible para todos los usuarios, haciéndolo transparente y difícil de alterar.

Por otra parte, la criptomoneda posee las siguientes desventajas:

- CARENCIA DE UN SÓLIDO Y COMPLETO ANONIMATO. Si bien Bitcoin es una moneda que posee un mayor grado de anonimato frente a las transacciones bancarias. Cabe aclarar que si las transacciones son realizadas en efectivo, éstas no sufren del problema antes mencionado ya que las mismas otorgan la posibilidad de anonimato total. Por otro lado, con la utilización de bitcoin el anonimato no es total, dicha situación de vulnerabilidad del anonimato se produce cuando los usuarios tienen billeteras digitales de criptomonedas en plataformas en línea que se dedican al almacenamiento, y a la compra y venta. Por dicha razón es que el almacenamiento y el intercambio del Bitcoin por intermedio de dichas plataformas como intermediarias generan una carencia de un sólido y completo anonimato. Por otro lado, si las transacciones se realizan por intermedio del software original o mediante billeteras físicas de usuario a usuario no se genera la mencionada situación.
- MAYOR ANONIMATO DE TRANSACCIONES DE BITCOIN FRENTE A TRANSACCIONES BANCARIAS. Tomando como punto de partida lo descripto en el punto anterior, es posible afirmar que la existencia de un mayor anonimato de los datos personales de quienes intercambian criptomonedas puede ser un factor de riesgo para la sociedad. Este factor de riesgo se ve representado como una facilidad para realizar el pago de actividades

ilícitas. Por lo tanto, el sentido del anonimato puede generar diferentes opiniones según el punto de vista que se tome.

- PROPENSA A ESTAFAS. La llave privada otorga al propietario acceso a su billetera de Bitcoin. Si esa llave es perdida o robada, el propietario no puede acceder más a su dinero. Para robar la llave, el perpetrador necesita acceso directo a la carpeta que la contiene.
- DESCONFIANZA. Adoptar criptomonedas y confiarles los ahorros y ganancias propias puede ser una elección difícil para las personas. especialmente para las generaciones mayores que sólo están habituadas a utilizar las monedas clásicas. Dado que el fenómeno de las criptomonedas es relativamente nuevo, puede comprenderse el rechazo de personas y negocios a lanzarse hacia lo desconocido. Para el público en general, los complejos algoritmos y la idea de una billetera virtual pueden generar temor. (Dumitrescu, 2017)

C. Impacto inflacionario del Bitcoin

Uno de los aspectos más destacados e importantes para los usuarios de las distintas monedas siempre ha sido la inflación. Dicho fenómeno monetario posee gran preponderancia especialmente a nivel nacional, ya que es punto de partida para distintos análisis a nivel micro y macro económico.

Como bien sabemos el dinero fiduciario, es decir el dinero emitido por los Banco Centrales de los distintos países, se caracteriza con respecto al usuario en carecer éste de potestad para decidir sobre la emisión del mismo. Tal situación implica que pueda ser emitido en forma exponencial sin el consentimiento de quienes poseen dicha moneda. En Bitcoin la situación es diferente, éste no se emite por un ente centralizado por lo que no existe una parte con facultades para decidir sobre la cantidad y la tasa de velocidad para su emisión. Dichos atributos fueron determinados al momento de su emisión, tal es así que se definió la máxima cantidad de monedas a emitir. La mencionada situación implica que existe un límite cuantitativo a su emisión. Además, la tasa de emisión es decreciente debido a su diseño, ya que a medida que se minan más bloques de Bitcoin, la tarea de minado se hace más compleja. Por lo tanto, la tasa de inflación de Bitcoin a futuro no solamente es decreciente, sino que la misma es posible de conocer ya que sabemos el máximo de monedas que podrán emitirse.

El análisis realizado anteriormente fue realizado desde el punto de vista de la oferta del mismo, pero es importante tener en cuenta que implicancias genera la demanda del Bitcoin.

La creciente demanda de la moneda, junto con la utilización o compra por grandes referentes del mundo de los negocios como será visto en capítulos posteriores genera una gran fuerza compradora que produce un incremento del precio debido a que la oferta no tiene la capacidad para satisfacer esa oferta de forma inmediata. Es decir, cada vez más cantidad de personas destinan sus

pesos o dólares a comprar Bitcoin y genera una constante puja del precio. Por ejemplo, si existen en un mercado 100 personas con 1 dólar cada una, es decir en total hay 100 dólares para comprar 100 Bitcoins. Cada persona comprará 1 Bitcoin. Pero si la demanda se duplicara, es decir hubiera 200 personas que quisieran comprar Bitcoin, la oferta no podría satisfacer dicha demanda ya que no maneja la cantidad de Bitcoins que pueden emitirse ni su velocidad de emisión. La situación descripta anteriormente generaría un nuevo punto de equilibrio en el mercado que tendría una cantidad constante y un precio mayor por lo menos en el corto plazo.

Respecto de la inflación propiamente dicha, se puede decir que la gran mayoría de precios de bienes actualmente no se encuentran expresados en Bitcoin. Dichos precios se encuentran expresados en las distintas monedas locales. Un ejemplo claro de referencia comúnmente utilizado es el dólar o el peso. Dichas monedas poseen una pérdida de poder adquisitivo, en algunos casos mayor y en otros menores. Pero el resultado, en definitiva, es una situación en donde el dinero fiduciario que actualmente compra un bien, en el corto o mediano plazo puede no comprar el mismo bien. Por el contrario, Bitcoin, manejándose a través de los tipos de cambio y por el aumento de su cotización, siempre y cuando no nos encontremos en un punto de bajada excesivo de cotización, puede comprar el mismo bien.

En conclusión, la inflación que es conocida como el aumento generalizado y sostenido en el precio de los bienes no es más que una pérdida de valor de la moneda a la que Bitcoin no se encuentra sujeto. Es importante recordar que los incrementos o disminuciones estacionales o de productos en específicos no constituyen inflación ya que ésta debe ser generalizada y sostenida en el total o la gran mayoría de los productos. (Mochón Morcillo y Beker, 2008) (Fornero, 2014)

Capítulo IV

Análisis del Bitcoin como medio de pago e inversión

A. Análisis de sus características

El bitcoin es un medio de pago directo que no requiere la necesidad de intermediarios o la utilización de medios adicionales siendo ésta una gran ventaja respecto a otros medios de pago tradicionales como pueden ser las transferencias bancarias, tarjetas de débito, crédito, etc. El pago es como si fuera pagar en efectivo, sin la intervención de gobiernos, bancos, por lo que de cierta manera sería anónimo ya que dicho pago solo lo conocen las partes intervinientes de la operación (comprador y vendedor). Si bien el anonimato es una gran ventaja cabe recalcar que hay otras también importantes como es la ausencia de costos asociados al pago, como mencionamos anteriormente el pago es directo sin que intervenga un tercero en la operación, como podría ser un banco que cobre una comisión, por lo que el costo de la operación es cero aun cuando el vendedor y el comprador se encuentren en países diferentes.

Por otro lado, para invertir en bitcoin hay que tener en cuenta que es un tipo de inversión variable que puede tener un cambio fuerte en su capitalización de un día a otro por la volatilidad de la misma. En general se deberían seguir los siguientes pasos para poder invertir en este tipo de moneda:

a) ADQUIRIR UN MONEDERO VIRTUAL. Es un sistema para operar y almacenar bitcoin que contiene pares de llaves criptográficas (una clave privada y otra pública).
b) DESCARGAR LA APLICACIÓN. Los monederos son utilizados desde dispositivos móviles o computadoras a través de la aplicación que posee bitcoin para poder llevar a cabo las transacciones.
c) REALIZAR OPERACIONES. Siempre entre personas que tengan monederos electrónicos.

B. Minería, trading y holding

1. Minería

La minería es una tarea que consiste en comprobar que las monedas no se usan dos veces y que no se puedan introducir bitcoins falsos en el mercado debido a que las criptomonedas son un sistema descentralizado. De esta manera, se examinan las operaciones realizadas y se juntan las últimas creadas en un grupo llamado bloque, así el conjunto de bloques permite corroborar las transacciones y el saldo de las personas.

El proceso comienza con un problema matemático que los mineros reciben cada diez minutos y el primero en resolverlo es el que obtiene las nuevas monedas que se ponen en circulación y las comisiones de las operaciones, siendo éstos los beneficios del trabajo, una vez que el resto de los miembros de la red confirme que la respuesta es correcta.

Anteriormente dijimos que los mineros reciben como recompensa del trabajo realizado las nuevas monedas que se ponen en circulación, pero esto tiene una limitación ya que la cantidad de bitcoins que reciben se reduce a la mitad cada 210.000 bloques, esto se lo conoce como holding. Dicho esto, para que la minería sea rentable debería aumentar el valor del bitcoin, pero también se debe tener en cuenta los beneficios que pueden traer las comisiones de las transacciones.

Un factor para tomar en consideración es la potencia de computación que se tenga ya que al tener mejores máquinas para realizar la tarea se tienen mejores oportunidades para resolver el problema y debido a esto nacieron las mining pools que son grupos de mineros que cooperan entre sí con el objetivo de minar bloques de una blockchain cuya finalidad es la de facilitar el minado y dividir equitativamente los beneficios entre sus miembros según la potencia aportada por todos sus participantes.

Otro tema no menor es la relación costo beneficio a la hora de llevar a cabo esta tarea ya que como dijimos la potencia de computación es muy importante y eso representa una inversión, pero el consumo de energía que esto genera es también importante, tanto para alimentar el minero como para refrigerar el calor que generan, por ello el costo de la electricidad es otro factor a tener presente. (Antonopoulos, A., 2014)

2. Trading

Se trata de una práctica que se basa en un mercado especulativo donde se compra a precios bajos para luego vender a precios altos. De esta manera, se puede seguir una tendencia o realizar operaciones cortas durante el día. Para poder llevarlo a cabo se realizan distintas estrategias que se basan en 4 tipos de análisis a mencionar, como lo son el análisis técnico (mediante el análisis de

gráficos se trata de predecir precios futuros y curvas de tendencias), análisis fundamental (se busca a través de la información contable de una empresa evaluar la tendencia de su precio), análisis macroeconómico (teniendo en cuenta las variaciones de la economía) y por último el análisis cuantitativo (haciendo uso de la estadística para predecir los movimientos en los precios). Es así como las traders buscan aprovecharse de la volatilidad de la moneda para generar ganancias en el corto plazo realizando distintas operaciones.

3. Holding

A diferencia del trading, el holding se caracteriza por ser una estrategia más tranquila a la hora de invertir en bitcoins ya que consiste en comprar y mantener esa inversión por un largo periodo de tiempo pese a las subidas y bajadas que pueda sufrir la moneda, todo esto con el fin de que a medida que aumenten su valor, la inversión inicial comience a revalorizarse. Cabe recalcar que las personas que llevan adelante esta práctica, los llamados holders, deben realizar un estudio de mercado sobre el activo en cuestión para poder estimar su rentabilidad en el tiempo, caso contrario más que una inversión se estaría haciendo una apuesta. (Antonopoulos, A., 2014)

C. Factores que generan variaciones de la cotización

Como es de público conocimiento Bitcoin es una moneda que a lo largo de su corta vida ha tenido grandes cambios con respecto a su cotización. Debido a esta situación es descripta como una de las más volátiles del mundo, tanto es así que su cotización puede variar un alto porcentaje en tan solo horas. Desde su inicio se pudo notar su alta volatilidad que es consecuencia directa de múltiples factores. Entre ellos tendremos los siguientes:

- IMPACTO FOLDERS Y A NIVEL DE NOTICIAS. Debido a que bitcoin posee una escasa vida, el conocimiento sobre la criptomoneda no está tan extendido por lo que diversas noticias que anuncias grandes aumentos de cotización en períodos de tiempo cortos generan una sensación, a simple vista, de admiración o intriga sobre nuevos usuarios. No únicamente se basa en eventos o noticias que indiquen signos de variación excesiva de su cotización, sino que también nos podemos encontrar con declaraciones oficiales o anuncios de gobiernos tanto para regular o por falta de capacidad para regular la misma. Es así que noticias como la pandemia también tuvieron un impacto grande siendo una de las caídas más grande de valor a lo largo de su vida.
- GRANDES VENTAS O COMPRAS. En vocabulario bitcoin quienes realizan grandes compras o ventas en espacios de tiempo cortos con capacidad de influir a corto plazo en el precio se los

considera ballenas. Las transacciones que realizan estos usuarios pueden impactar rápidamente y con una fuerza muy grande sobre la tendencia de la moneda.

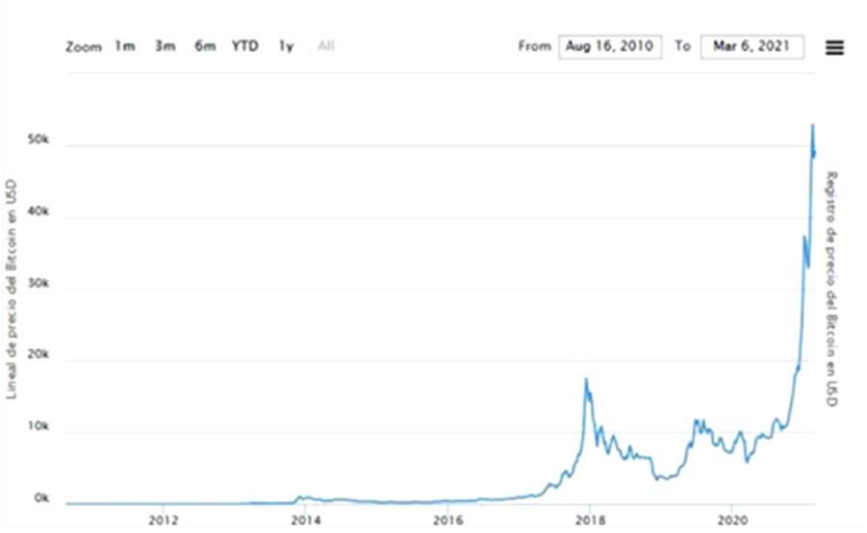
- VALOR DE LOS ACTIVOS FINANCIEROS SUBYACENTES. Esta causa tiene que ver sobre la situación en la que se encuentran los activos por los que se intercambia Bitcoin, por ejemplo, la caída de una moneda regional como sería el peso, o de una moneda fuerte como el dólar tendrá impacto en la cotización del Bitcoin ya que se necesitará mayor cantidad de moneda fiduciaria para poder realizar la compra de la misma.
- COSTOS DE ELECTRICIDAD Y DE HARDWARE INFORMÁTICO. El aumento o la disminución de costos de energía eléctrica y hardware tendrán impacto sobre el costo de extraer o minar un Bitcoin, esto se debe a que constituyen de alguna forma la materia prima para conseguirlos. Pero hay que tener en cuenta que puede no generar en todos los casos variación del precio de Bitcoin ya que éste generalmente está manejado por las expectativas del mercado. En caso de que los costos aumentaran, por ejemplo, aumentara el precio de la electricidad o del hardware informático que deban utilizar los mineros, esto podría tener repercusión en el precio o en el caso de que el precio del Bitcoin estuviera constante o a la baja, en la cantidad de personas dispuestas a minar y a contribuir con la red de transacciones. Si esta situación ocurriera sería muy desventajosa para Bitcoin ya que podrían verse afectadas las transacciones que se realicen en la red. Por el contrario, el aumento del costo podría generar un avance tecnológico muy grande destinado a poder ser más eficiente en la manera o forma de minar los Bitcoin. Es así, que este punto en específico podría generar diversos resultados dependiendo del impacto que tenga en los mercados y las decisiones de los mineros.
- DIFICULTAD DE MINADO DEL BLOQUE. A medida que aumenta la cantidad de Bitcoins conseguidos a nivel global, el mismo algoritmo dificulta la obtención de nuevos Bitcoin, por lo que se necesitan cada vez más recursos para poder extraer la misma cantidad de Bitcoins.
- CAPACIDAD COMPRADORA O VENDEDORA DEL MERCADO. El valor del Bitcoin no se basa únicamente de costos sino también de la oferta y demanda del mismo. Es decir, si hay mayor cantidad de compradores, el precio necesariamente deberá subir para poder atender esa demanda. Y de modo contrario, si la cantidad de compradores es menor, los precios deberán bajar a un punto en el cuál la oferta se equilibre con la demanda. (Mochón Morcillo, y Beker, 2008)

Gráficos de cotización

A la hora de analizar los gráficos, es necesario tener en cuenta que los gráficos de Etc./Peso Argentino muestran variaciones que se ven afectadas por la cotización del Dólar contra el Peso Argentino. Es decir, para una cierta fecha la cotización del Btc/Usd podría verse constante sin

alteraciones, pero podría haber un cambio de gran aumento o disminución por la situación que se dé entre el Peso Argentino y el Dólar Estadounidense.

Gráfico 1
Gráfico de historial del precio de Bitcoin.
Bitcoin/USD

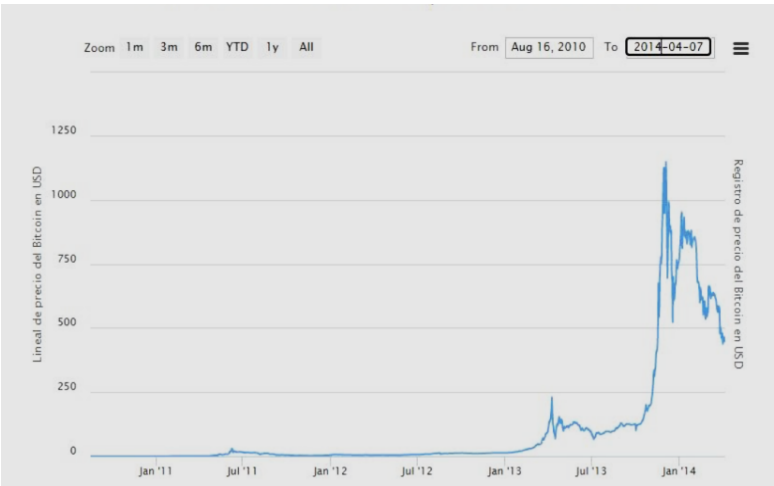


Fuente: Comprar Bitcoin en todo el mundo, s.f.

Si observamos este primer gráfico cuyo período abarca desde el 16 de agosto de 2010 hasta el día de la fecha, podemos observar como la cotización de Bitcoin frente al dólar se mantuvo varios años constante sin grandes variaciones al comienzo de su vida. Podemos observar que a la fecha mencionada de comienzo del gráfico la cotización del Bitcoin se encontraba en 0,06 centavos de dólar. Cabe aclarar que es un precio ínfimo en comparación con el valor que actualmente posee.

Recién a fines del año 2013 y comienzos del 2014 encuentra un primer punto de inflexión. Luego tendremos otras variaciones considerables en los años 2018, en fines de 2020 y comienzos de 2021.

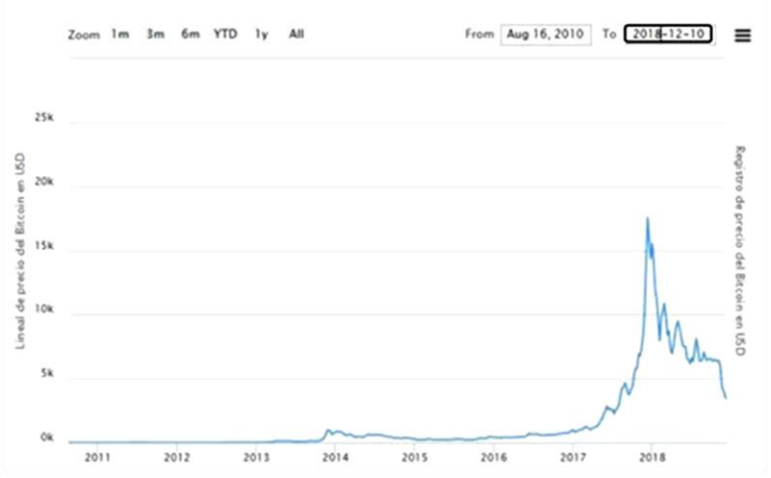
Gráfico 2
Gráfico de historial del precio de Bitcoin.
Bitcoin/USD



Fuente: Comprar Bitcoin en todo el muindo, s.f.

Tal como fue mencionado en la descripción del primer gráfico, se puede observar como el precio de Bitcoin se dispara rápidamente pasando de valer tan sólo unos centavos de dólar a tener un precio considerablemente mayor, llegando así a los 1120 dólares por unidad de Bitcoin. En consecuencia, con lo anteriormente mencionado también se observa un primer patrón, el cual se basa en una rápida subida, con mucha fuerza compradora en un período de tiempo muy corto. Por otro lado, el patrón mencionado se basa en una brusca bajada de precio seguida de inestabilidad en el cual el precio tiene a realizar oscilaciones estando en rango para realizar bajas abruptas.

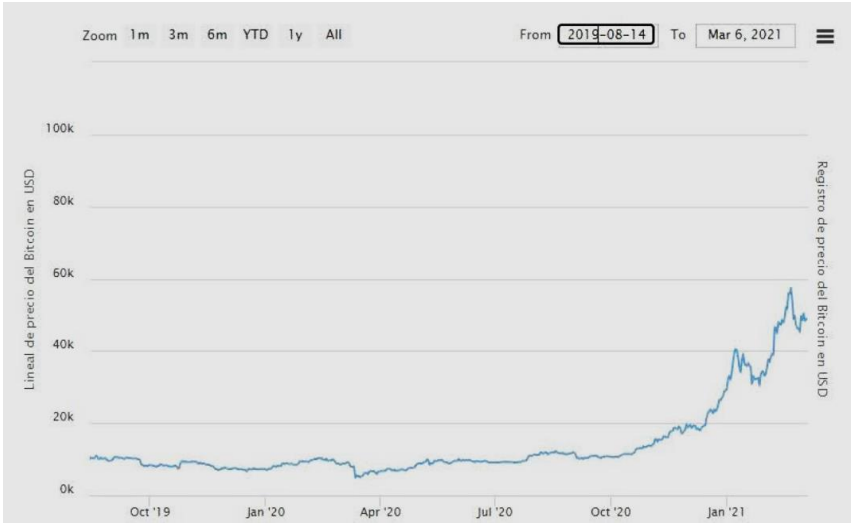
Gráfico 3
Gráfico de historial del precio de Bitcoin.
Bitcoin/USD



Fuente: Comprar Bitcoin en todo el muindo, s.f.

Años más tarde, es posible observar que se repite el mismo patrón identificado en el análisis del gráfico anterior. Es decir, a fines del año 2017 se produce un incremento repentino y rápido de su valor de cotización, el cuál alcanza un punto máximo el 11 de diciembre de 2017, llegando a cotizar en 17.549,67 dólares. Posteriormente se repite la bajada de precio que se observaba en el análisis anterior y cae hasta los 3.854,68 dólares el 17 de diciembre de 2018. Es decir, se produjo una gran subida, pero una bajada estrepitosa.

Gráfico 4
Gráfico de historial del precio de Bitcoin.
Bitcoin/USD



Fuente: Comprar Bitcoin en todo el muindo, s.f.

Por último, podemos ver que el precio del Bitcoin tuvo oscilaciones en donde se produjeron subidas y bajadas de igual magnitud sin repetir el patrón observado. Pero con el avance de la pandemia, la incertidumbre en los mercados y el temor se produce una gran baja de la cotización. La cotización se hunde hasta los 6.702,19 dólares el 30 de marzo de 2020. Luego Bitcoin recupera un poco de terreno hasta llegar a la situación marzo, pero dicha situación plantea nuevamente el patrón mencionado en los dos análisis anteriores. A fines del año 2020 se produce un incremento vertiginoso del precio alcanzando un máximo de 52.869,11 dólares el 15 de febrero de 2021.

Temporalidad 5 años:

Gráfico 5
Bitcoin/USD

Fuente: Investing.com, s.f.

Se aporta otro gráfico de temporalidad de 5 años para poder observar las situaciones planteadas en análisis anteriores.

Gráfico 6
Cotización Btc/ Peso Argentino

Fuente: Ripio, s.f.

Por último, analizaremos la situación del Bitcoin contra el peso. Como mencionamos al principio cualquier temporalidad que observemos se verá distorsionada por la depreciación del Peso Argentino, es decir el Peso pierde valor frente a todas las divisas. La comparación más relevante y comúnmente realizada es con el dólar. Tal es así, que puede que en algunos períodos el precio del Bitcoin contra el Dólar se encuentre a la baja, pero si observamos el gráfico de Bitcoin contra el Peso, éste podría estar subiendo con motivo de una mayor depreciación del peso. Por lo tanto, se invita al lector a profundizar en caso de ser de su interés la observación del comportamiento del Bitcoin/Peso Argentino ya que las grandes variaciones reales y netas de los efectos inflacionarios locales se dan a nivel Bitcoin/Dólar.

D. Valuación del Bitcoin

Tras auge inicial y el gran aumento de precio del 2017, cada vez más cantidad de personas se han ido volcando hacia las inversiones en criptomonedas. Algunos, con la intención de hacer una diferencia con las fluctuaciones de corto plazo. Otros, con una visión más estratégica de largo plazo.

Los traders suelen realizar análisis técnicos para predecir movimientos en el precio de los activos. Estudian puntos de “soporte” y “resistencia” para definir los momentos óptimos de entrada y salida del mercado.

Los inversores, por el contrario, realizan un análisis fundamental de los activos para construir posiciones de largo plazo. Así como en el mundo de la bolsa tradicional se analizan variables como la evolución de la industria, valores de acciones, administración de empresas, la posición estratégica de una empresa para predecir la evolución del valor de una acción, etc. pero el mundo cripto tiene sus propias variables clave.

La valuación de tanto, es todavía un terreno muy nuevo que recién estamos empezando a comprender. A continuación, presentamos algunas pautas que debe considerar todo inversor para entender el potencial de un tanto, en el largo plazo.

Dentro de las herramientas más utilizadas para valuar tanto, tenemos el denominado “White paper” o Libro blanco. Es decir, este White paper contendrá un conjunto de información técnica destacada y recopilada para poder darle al usuario o lector interesado un conocimiento profundo y específico con un alto grado de detalle y fundamento que tiene como finalidad que el lector pueda tener conocimiento y tomar decisiones sobre su comportamiento en el mercado. El White paper de bitcoin el cual podrán encontrar en el Anexo en caso de que el lector quiera profundizar su análisis, permite tener conocimiento de cómo se realizan las transacciones, en qué consiste la prueba de trabajo, cómo funciona la red y los sistemas de incentivo, cuál es la privacidad y los cálculos pertinentes. Por lo tanto, opera como una especie de información que puede en muchos casos no solo

ser una herramienta técnica sino de marketing para poder introducir a posibles nuevos usuarios, dándoles a conocer las ventajas y aspectos relevantes del sistema propuesto.

Respecto de esta herramienta se puede decir que como los criptoactivos se basan en proyectos que tienen un código abierto, los equipos de desarrollo en la mayoría de los casos poseen un documento en el cual se explique el problema a resolver y la forma o mecanismo por el cual el criptoactivos permitirá resolver el mismo. Por esta misma razón es de suma importancia ver si ese documento tiene cierto grado de coherencia. Además, se buscará determinar si realmente constituye un problema real con una solución existente que permita efectivamente resolverlo.

Respecto a esta manera de valuar un Bitcoin tenemos que hacernos la siguiente pregunta ¿realmente necesitamos un criptoactivo descentralizado? Ya que en numerosos casos intentó introducirse la tecnología de cadena de bloques a proyectos que era mucho más eficiente desarrollarlos de manera centralizada.

En el caso de criptomonedas como el bitcoin, la descentralización tiene sentido. Es importante que la emisión de bitcoin no esté controlada por un agente centralizado que pudiera manipular el sistema monetario. El mundo de las criptomonedas no quiere de la existencia agentes centralizados que controlen el poder de cómputo de la red y decidan qué flujo de moneda virtual debe estar en circulación.

Es así como nos hacemos una segunda pregunta clave para evaluar un criptoactivo ¿cuál es el motivo para que deba ser prestado de manera distribuida y segura? Si no hay un motivo convincente para que el activo deba estructurarse de manera descentralizada, entonces es probable que no sea demandado y que no suba de valor en el futuro.

Por otro lado, uno de los puntos para tener en cuenta es la competencia. En este ítem solo debemos preguntarnos ¿cómo se relaciona el criptoactivo con otros de su clase? Al igual que en el mundo de las compañías y empresas, la competencia también se encuentra presente y existente entre proyectos de mínimo. Distintos criptoactivos compiten entre sí por ver quién cumple de mejor manera cierta función.

El bitcoin permite realizar pagos de bajo costo, sin intermediarios y con protección de la privacidad. Todos los criptoactivos que cumplan con esta misma función van a afectar la demanda de bitcoin y, por lo tanto, la evolución de su valor en el largo plazo.

En diciembre de 2017, la congestión de la red de Bitcoin impulsa fuertemente el costo de las transacciones. Un pago que antes costaba unos pocos centavos pasó a 20 o 30 dólares. Por este aumento de precios, una parte importante de los usuarios empezaron a volcarse a monedas competidoras, como Litecoin o Dash.

Es así como encontramos en la red de internet una gran cantidad de monedas digitales que compiten en cierto punto con Bitcoin. Algunas de estas alternativas mencionadas permiten realizar transacciones con un mayor grado de privacidad que con bitcoins. Por lo que podemos determinar

que si lo valorado es estrictamente la privacidad podrían volcarse hacia otra de las alternativas existentes en el mercado. Por otra parte, no solo se analizará privacidad sino velocidad y costo frente a otras opciones disponibles.

Otro concepto que destaca es la concentración de la criptomoneda. Esto quiere decir que se va a analizar si el universo de monedas emitidas pertenece a una cantidad reducida de miembros como podrían ser los equipos de desarrollo o los primeros mineros de dichas monedas. Esta situación descripta anteriormente puede derivar en que éstos posean un poder de influencia muy grande que permita determinar el precio.

Por último, se evalúa el grado de adopción de la criptomoneda, el cual es un indicador clave. Será de gran importancia determinar la cantidad de usuarios, cantidad de transacciones diarias, valor de las transacciones.

Capítulo V

Situación legal tributaria argentina

A. Marco legal en la Argentina

El marco legal es fundamental a la hora de comercial, realizar inversiones y de evaluar alternativas. Es por eso por lo que como parte de este trabajo de investigación no solo analizamos funcionamiento, características de la moneda y de los medios de pago, sino que buscamos un conocimiento un poco más detallado de la situación en la que se encuentra la moneda digital en cuestión en nuestro país. Al día de hoy podemos observar que existen dos proyectos de ley que buscan darle transparencia a la situación de Bitcoin y regular los aspectos de su compraventa en distintas casas de intercambio.

Es por eso por lo que los proyectos de ley buscan brindar definiciones sobre moneda digital, casas de intercambio, y de brindarle atribuciones a la Comisión Nacional de Valores para elaborar políticas tendientes a la regulación, protección, vigilancia, inspección y control de las operaciones realizadas con criptoactivos. El presente proyecto de regulación presentado al congreso, que se encuentra en el Anexo II del presente trabajo, pretende regular a quienes emitan monedas, o bien quienes ofrezcan ámbitos de intercambio de las mismas, así también pretende darle legalidad y transparencia a la información que se distribuye al público. Además, se busca otorgarle la posibilidad de elaborar y mantener un registro nacional de operaciones, y de disponer la realización de auditorías, inspecciones y pericias vinculadas a la actividad normada en dicho proyecto de ley. Se busca regular a los intercambistas habituales de dicha moneda y de establecer una política clara de información hacia los usuarios respecto de los beneficios y riesgos que generan dichas operaciones. El consentimiento informado toma un papel preponderante en dicho proyecto de ley, en el cual el usuario debe estar informado y las entidades deberán informar todas las características de los criptoactivos a sus compradores. Se destaca la mención de que no son monedas de curso legal y que no cuentan con el respaldo del banco central de la República Argentina. Se menciona que las operaciones no son reversibles por lo cual los usuarios deben ser conscientes de la importancia de las mismas y que existen riesgos tecnológicos, cibernéticos y de fraude inherentes a las operaciones con criptoactivos.

Por otra parte, el proyecto de ley busca informar que no hay días hábiles ni tampoco inhábiles cuando hablamos de criptomonedas.

Se busca establecer la obligatoriedad de inscribirse en un registro para todos los vendedores de criptomonedas en el país. (Schwint, 2020)

Luego de analizar el proyecto de ley, el cual se encuentra en el Anexo II del presente trabajo, podemos destacar que dicha ley se basa primordialmente en el conocimiento para todos los ciudadanos de los riesgos y situaciones que hay que tener en cuenta a la hora de operar con esta moneda digital. Por otra parte, busca dar un primer paso a la regulación de manera más estricta sobre los habitualitas en la intermediación de compra venta. Será de análisis en el futuro la aplicabilidad de dicha norma sobre las transacciones, ya que la gran mayoría de las mismas se realizan de forma anónima sin distinguir países de origen ni de destino. (Lacha & Núñez, 2020) (Zocaro, 2020) (Arnáez, 2020) (Aballay, 2020)

B. Marco tributario en la Argentina

Las criptomonedas no solamente plantean nuevos escenarios a nivel económico, legal y cultural, sino que las mismas implican una ardua tarea por parte del fisco y de los legisladores para poder determinar la gravabilidad de las mismas. En consecuencia, con lo anteriormente descripto se plantean varias situaciones no previstas en las normas y que exceden lo legislado hasta el momento lo cual genera nuevos desafíos tributarios y legales en cuanto a determinar los hechos y situaciones que serán eje fundamental de generación de los hechos imponibles de los diferentes tributos. (Tapscott, A. y Tapscott, D., 2016)

Como punto de partida para desarrollar un esquema tributario se debe definir qué se entiende por criptomoneda o moneda digital. Si buscamos recurrir a las normas legales emitidas podemos notar que no existe al día de la fecha una definición establecida, ni siquiera en resoluciones interpretativas por parte del fisco acerca de la materia en cuestión. Es así como en el primer acercamiento nos encontramos con una situación de falta de normativa, jurisprudencia y doctrina interpretativa sobre el tema. Al no haber determinado una definición, la cuál es un punto de partida muy importante para poder definir un hecho imponible, esto dificulta el nacimiento de la obligación tributaria. (Smith, 2018)

De la misma manera podríamos realizar un análisis un poco más allá de la definición legal que nos permitiría definir qué es una moneda digital y centrarnos que dicen las diferentes leyes tributarias sobre la materia bajo análisis.

Si analizamos pormenorizadamente la ley de impuesto a las ganancias vigente (Ley 27.430/17), podemos ver que se encuentran gravados según el artículo 2 inciso 4) los rendimientos,

rentas, beneficios o enriquecimientos que obtenga cualquier sujeto ya sea persona física o jurídica sobre las monedas digitales. Como mencionamos anteriormente, ni la ley de impuesto a las ganancias ni su decreto reglamentario planteaban un concepto sobre moneda digital. Sin embargo, se puede decir que dichos rendimientos o enriquecimientos se encuentran gravados cumplan o no con el criterio de la fuente que menciona dicho artículo. Es decir, la cuestión no versaría sobre la existencia o no de permanencia, habilitación y habitualidad de dicha fuente generadora de ganancias. Una vez determinada la gravabilidad en impuesto a las ganancias de los rendimientos y rentas de las monedas digitales existe una cuestión muy importante a determinar, la cuál es determinar el tipo de fuente de esta. La ley menciona que existen fuentes de origen extranjeras y argentinas, la diferencia entre ambas, en especial a lo que nos interesa en el trabajo en cuestión recae en el tratamiento que respecta a las mismas. Ya que si las mismas son renta de fuente argentina, su tratamiento correspondiente será la aplicación del impuesto cedular definido en el artículo 98 de dicha ley. Por otro lado, si su tratamiento fuese de fuente extranjera, correspondería el artículo 94 de la ley de impuesto a las ganancias. Es por esa misma razón que debemos recurrir al artículo 7 de la misma ley donde nos indica que se considerarán de fuente argentina, cuando el emisor se encuentre domiciliado, establecido o radicado en la República Argentina. Del análisis del texto del artículo mencionado previamente se puede destacar que la norma pone énfasis en dónde se encuentra domiciliado o radicado el emisor. De la misma manera podemos observar que Bitcoin posee una característica muy importante la cuál es que no es emitida por una entidad oficial bancaria de ningún país, por lo que se puede decir que es una moneda descentralizada que no posee un emisor en concreto determinable. De esta manera vemos que Bitcoin al ser una moneda descentralizada, la cual no es emitida por un sujeto determinable en un área geográfica específica dificulta o imposibilita la aplicación del artículo en cuestión.

Por otra parte, si analizamos la situación tributaria del Bitcoin respecto del impuesto al valor agregado, con un análisis de la ley se puede apreciar que no se hace una referencia a la moneda mencionada. Además de una lectura el artículo primero de la ley surge que la venta de Bitcoin no se encuentra contemplada al no ser una venta de una cosa mueble, ni obra, ni tampoco una locación ni una prestación de servicio. Por otro lado, las cesiones de derechos tampoco se encuentran incluidas en la misma, ya que podría considerarse al Bitcoin como un derecho incluido dentro del libro de contabilidad que lleva el registro de las transacciones mundiales, es decir dentro de la cadena de bloques.

Por su parte, la situación de bienes personales no es muy diferente, la misma carece de detalle pormenorizado del tratamiento que debe otorgársele. El análisis debe basarse en como considerar dicha criptomoneda, puede dársele el carácter de un bien inmaterial por sus características propias, en el cual se encontraría exenta por el artículo 21 inciso d) de la Ley de Bienes Personales (1997). En contrario a lo anteriormente descripto podrían considerárselas también como un activo financiero en

cuyo caso se encontrarían gravadas, ya que la ley de bienes personales al no tener un tratamiento en particular para este caso buscaría sustento en la ley de impuesto a las ganancias, en la cual se encuentra gravada. Más allá de tomar una u otra postura frente a cómo debe considerárselas, habría que analizar la alícuota a aplicar. La misma dependerá dónde se encuentran ubicadas, es por lo que aquí nace otro interrogante ya que no es posible determinar si las mismas se encuentran en el país o en el extranjero ya que las mismas se encuentran en la cadena de datos global que se encuentra en línea. Tal es así que cuando se accede a un agente de intercambios en el país o se tiene una billetera física, lo único que se tiene son las claves tanto públicas y privadas para poder acceder a esas criptomonedas que se encuentran en la cadena de bloques global. Adicionalmente a la incógnita que se genera respecto de la alícuota a considerar, también surge otra gran incógnita respecto de la cotización a emplear. La ley mencionada, establece que la cotización debe ser la vigente al 31 de diciembre de cada año en el mercado oficial, pero Bitcoin no posee un mercado oficial regulado sobre el cuál poder tomar una cotización válida. Por otro lado, la ley menciona que para aquellas operaciones que no coticen en bolsa debería valuares al costo, es decir por ser un activo financiero que no cotiza.

Luego si analizamos el impuesto sobre los ingresos brutos podemos ver que dicha ley establece que debe haber una actividad a título oneroso, lucrativa o no, en la cual exista habitualidad y se dé una relación con el elemento espacial para poder determinar en qué provincia corresponde tributar. Como hemos visto anteriormente, Bitcoin no permite identificar claramente el elemento espacial del hecho imponible por lo que nos vemos en una situación de imposibilidad para determinar el elemento espacial. Pero esta no es la única dificultad que se plantea con respecto al tributo mencionado ya que la habitualidad es muy difícil de determinar debido a que existe un universo de transacciones demasiado grande y anónimo.

Es así que se puede concluir que Bitcoin posee un marco tributario todavía muy poco desarrollado el cuál carece de elementos básicos como una definición clara de que son las monedas digitales y el hecho imponible. Por esa misma razón, debe revisarse constantemente las nuevas normativas y resoluciones sobre el fisco respecto del tema mencionado. (Boar, 2018)(Mougayar, 2018)

C. Aspectos prácticos

Luego de haber realizado el análisis detallado de cada uno de los aspectos de Bitcoin, partiendo de su definición y características que lo hacen único y lo diferencian de cualquier otra moneda tradicional, llegamos a un punto donde se plantea la explícita necesidad de abordar temas

prácticos que permitan al lector poder tomar contacto de manera directa con cada uno de los aspectos tratados en el presente trabajo. (Champagne, 2018)

De tal manera podemos decir que hay varias formas de acceder a la criptomoneda, puede ser a través del minado, el cuál fue desarrollado en puntos anteriores, que es una actividad muy demandante de recursos a nivel de hardware informático o puede adquirírselas en agentes de intercambio denominados Exchange. Esto agentes nos permitirán pasar de una moneda fiduciaria como sería el peso o el dólar a Bitcoin. Nos brindarán el servicio de intercambio ya sea de compra y venta de Bitcoins. El primer paso radica en crear una cuenta en alguno de los Exchange más reconocidos a nivel nacional como serían Ripio, XapooCoinbase quienes a través de una cuenta nos permiten tener acceso a las claves públicas y privadas. Cabe aclarar que el usuario no tiene esos Bitcoin depositados en cuentas ya que éstos son un mero registro en el gran libro de contabilidad mundial de la moneda mencionada. Otro de los aspectos relevantes a considerar es la cantidad de información que piden algunos de estos Exchange, ya que por normativa argentina se encuentran obligados a conocer a sus clientes. Por lo tanto, deberemos reunir ciertos requisitos para poder acceder a ese mercado que ofrecen estos Exchange. Una vez creada la cuenta, deberemos esperar la aprobación y el alta de la misma, ya que se encuentra sujeta a verificación por parte del ente otorgante. Con la aprobación recibida deberemos siniestrarle fondos para poder realizar la operación. La mencionada operación tendrá que ser realizada mediante transferencia de cuenta bancaria, cabe aclarar que estos entes operan las 24 horas, por lo tanto, puede ser realizada en cualquier horario del día sin restricciones.

Si revisamos los apartados disponibles para el usuario podremos observar que veremos el saldo en moneda fiduciaria que poseamos, y además contaremos con opciones para realizar la compra y venta de las criptomonedas. Es importante recordar que no solo se puede adquirir Bitcoin, sino que también podrá ser adquirida cualquier otra criptomoneda. Dentro de la misma cuenta podemos tener diferentes billeteras virtuales, que contengan distintos saldos.

Por su parte, crear una cuenta en un Exchange no es la única forma de almacenar las claves públicas y privadas, ya que también es posible almacenarlas en dispositivos físicos que son de las opciones más seguras que existen. Esto es así gracias a que nos permiten administrar nosotros mismos las claves para acceder a los mismos y se suple la dependencia de los mismos respecto de un intermediario. Además, desde el mismo dispositivo podemos enviar órdenes a la cadena de bloques.

Por su parte también es posible utilizar un monedero físico de papel, en el cuál tengamos escritas las claves para el acceso a la red.

Dentro degráfico las alternativas mencionadas podemos ver que existen aquellas en las que se crea una cuenta en un Exchange, las cuales son riesgosas ya que los depósitos no se encuentran garantizados por el Banco Central de la República Argentina. En contrario a lo anteriormente mencionado, las billeteras físicas si bien permiten mayor control de los fondos, pero tienen un coste

elevado que implica un gran desembolso inicial. Además, el usuario se encuentra sujeto al riesgo de robo del dispositivo empleado.

Será de análisis de cada usuario determinar cuál opción se ajusta más a sus necesidades, a su riesgo aceptado y a su tolerancia al riesgo. (Antonopoulos, 2017)

Conclusiones

Partiendo de la base de que Bitcoin posee una corta vida y una escasa observación desde el punto académico y científico, en el desarrollo de la investigación se pudo analizar y obtener respuesta a los distintos interrogantes que han dado origen al presente trabajo. Respecto de las funciones de moneda, que cumple de manera óptima, podemos encontrar su utilidad como medio de pago e intercambio, depósito de valor y patrón de pago diferido. Por su parte, vemos que todavía le queda mucho camino por recorrer para lograr cumplir la función de unidad de cuenta, ya que la gran mayoría de los bienes expresa su valor en moneda fiat.

Por otra parte, pudieron demostrarse cuáles fueron los factures que generan la volatilidad del Bitcoin en sus cotizaciones, entre ellos se encuentran el impacto de las noticias, las grandes ventas o compras realizadas por usuarios, dificultad de minado y la capacidad o interés comprador o vendedor del mercado.

También pudieron analizarse las oportunidades que presenta Bitcoin como medio de inversión, como sería el trading y el holding, las cuales pueden ser desarrolladas por los usuarios para generar más valor a partir del dinero inicial. Cabe destacar que es posible constituir depósitos a plazo en criptomonedas.

Luego se destacó el impacto negativo en cuanto a contaminación que genera dicha criptomoneda, la cual construirá otro elemento más para futuros análisis sobre los beneficios y costos que genera su utilización.

Por último, el presente trabajo analizó tal como era uno de los objetivos planteados, las variaciones de cotización determinando patrones o relaciones. Y se hizo una comparación profunda entre las monedas tradicionales fiat y el Bitcoin.

Respecto de la opinión personal formada por los autores a través del presente trabajo de investigación, se puede concluir que Bitcoin no viene a ser un reemplazo de los medios tradicionales, sino un complemento para las operatorias actualmente utilizadas. Tal es así, que el uso del Bitcoin genera un impacto beneficioso en los sistemas modernos de pagos y de utilización del dinero tradicional, ya que los impulsa a avanzar tecnológicamente y a buscar opciones que permitan mayor facilidad a los usuarios.

Bibliografía

Aballay, V. (Noviembre de 2020). Criptomonedas: apuntes para el conocimiento de las monedas digitales y su impreciso tratamiento fiscal. *Práctica y Actualidad Tributaria (PAT), Tomo XXVII*.

Ammous, S. (2018). *El patrón Bitcoin: La alternativa descentralizada a los bancos centrales.* España: Deusto.

Antonopoulos, A. (2014). *Mastering Bitcoin.* USA: O'Reilly Media.

Antonopoulos, A. (2017). *Internet del dinero.* EEUU.: Merkle Bloom LLC.

Argentina. (15 de Abril de 1997). Ley de Bienes Personales. Obtenido de http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42700/texact.htm

Argentina. (26 de Marzo de 1997). Ley de impuesto al valor agregado. Obtenido de http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42701/texact.htm

Argentina. (29 de Diciembre de 2017). Ley 27.430. Impuesto a las ganancias. Obtenido de http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/44911/texact.htm

Arnáez, E. (Diciembre de 2020). Bitcoin dejó de ser "el futuro": cómo entenderlo desde una perspectiva actual argentina. *Información de Interés Profesional*.

Boar, A. (2018). *Descubriendo el Bitcoin: Cómo funciona, como comprar, invertir, desinvertir.* EEUU.: Profit.

Champagne, P. (2018). *El libro de Satoshi.* Madrid: Blockchain España.

Comprar Bitcoin en todo el mundo. (s.f.). Obtenido de https://www.buybitcoinworldwide.com/

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2 de Junio de 2016). *Bitcoin, BlockChain Technology: Beyond Bitcoin*. Obtenido de https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf.

Dumitrescu, G. (2017). *Bitcoin – a brief analysis of the advantages and disadvantages*. Obtenido de http://www.globeco.ro/wp-content/uploads/vol/GEO_Vol_5_No_2.pdf#page=63

Fornero, R. (2014). *Análisis Financiero en Condiciones de Inflación*. Obtenido de https://www.academia.edu/42101663/Analisis_financiero_en_condiciones_de_inflacion20200229_58010_1umztve

Infotechnology.com. (s.f.). *Opinión de un magnate sobre el Bitcoin*. Obtenido de infotechnology.com.

Investing.com. (s.f.). Obtenido de https://www.investing.com/

Lacha, P., & Núñez, M. (Octubre de 2020). Economía pospandemia. Aspectos tributarios para considerar en relación con los criptoactivos. *Práctica Integral Santa Fe*.

Mendoza. (2021). Código Fiscal de Mendoza. Obtenido de https://www.atm.mendoza.gov.ar/portalatm/zoneBottom/normativas/codigoFiscal/pdf/codigo_fiscal_2021.pdf

Mochón Morcillo, F. y Beker, V. (2008). *Economía, principios y aplicaciones.* México: McGraw-Hill.

Mougayar, W. (2018). *La tecnología blockchain en los negocios.* Madrid: Anaya.

Nakamoto, S. (25 de Agosto de 2017). *Bitcoin: Un sistema de efectivo electrónico usuario-a-usuario*. Obtenido de https://www.diariobitcoin.com/que-es-bitcoin/bitcoin-un-sistema-de-efectivo-electronico-usuario-a-usuario/

Real Academia Española. (2001). *Definición de Moneda*. Obtenido de https://www.rae.es/drae2001/moneda

Ripio. (s.f.). Obtenido de https://www.ripio.com/ar/.

Schwint, M. (2020). *Proyecto de ley de regulación de criptoactivos*. Obtenido de https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6055-D-2020.pdf.

Segendorf, B. (2014). *What is Bitcoin?* Obtenido de http://archive.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_1400918_eng.pdf#page=73

Smith, J. (2018). *Criptomonedas para principiantes (Blockchain y Bitcoin).* México: Tektime.

Tapscott, A. y Tapscott, D. (2016). *La revolución Blockchain.* España: Deusto.

Zocaro, M. (Diciembre de 2020). El confuso marco tributario de las criptomonedas. *Información de Interés Profesional*.

Anexo I

Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

(Nakamoto, 2017)

Traducido al Español de bitcoin.org/bitcoin.pdf
por Angel León - www.diariobitcoin.com

Abstrac. Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario-a-usuario. La red coloca estampas de tiempo a las transacciones al crear un hash de las mismas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y le llevarán la ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia.

1. Introducción

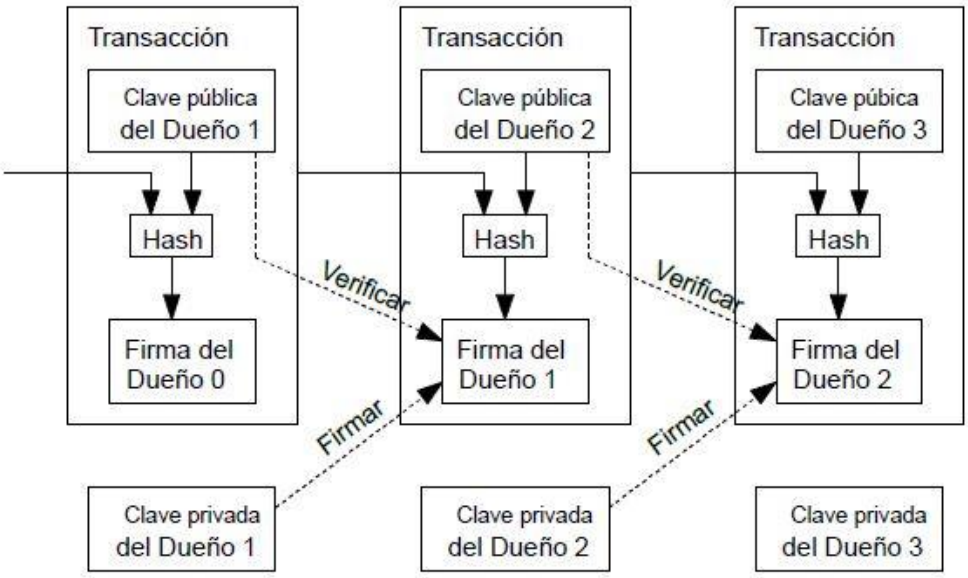
El comercio en el Internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos. Mientras que el sistema funciona lo suficientemente bien para la mayoría de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente norevertibles no son realmente posibles, dado que las instituciones financieras no pueden evitar mediar disputas. El costo de la mediación incrementa costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de pequeñas transacciones casuales, y hay un costo más amplio en la pérdida de la habilidad de hacer pagos no-reversibles por servicios no-reversibles. Con la posibilidad de revertir, la necesidad de confianza se expande. Los comerciantes deben tener cuidado de sus clientes, molestándolos pidiendo más información de la que se necesitaría de otro modo. Un cierto porcentaje de fraude es aceptable como inevitable. Estos costos e incertidumbres de pagos pueden ser evitadas en persona utilizando dinero físico, pero no existe un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable.

Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero confiable. Las transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, y mecanismos de depósitos de fideicomisos de rutina podrían ser fácilmente implementados para proteger a los compradores. En este trabajo, proponemos una solución al problema del doble-gasto utilizando un servidor de marcas de tiempo usuario-a-usuario distribuido para generar una prueba computacional del orden cronológico de las

transacciones. El sistema es seguro mientras que nodos honestos controlen colectivamente más poder de procesamiento (CPU) que cualquier grupo de nodos atacantes en cooperación.

2. Transacciones

Definimos una moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad.

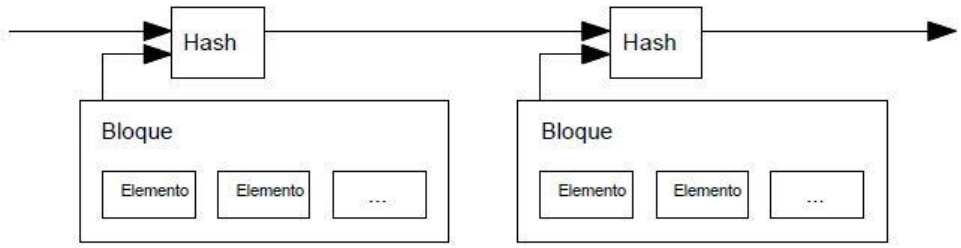


El problema claro es que el beneficiario no puede verificar si uno de los dueños no se hizo un doble-gasto de la moneda. Una solución común es introducir una autoridad central confiable, o casa de moneda, que revisa cada si cada transacción tiene doble-gasto. Después de cada transacción, la moneda debe ser regresada a la casa de moneda para generar una nueva moneda, y solo las monedas generadas directamente de la casa de moneda son las que se confían de no tener doble-gasto. El problema con esta solución es que el destino del sistema monetario entero depende de la compañía que gestiona la casa de moneda, con cada transacción teniendo que pasar por ellos, tal como un banco.

Necesitamos una forma para que el beneficiario pueda saber que los dueños previos no firmaron ningunas transacciones más tempranas. Para nuestros propósitos, la transacción más temprana es la que cuenta, así que no nos importan otros intentos de doble-gasto más tarde. La única forma de confirmar la ausencia de una transacción es estando al tanto de todas las transacciones. En el modelo de la casa de moneda, la casa de moneda estaba al tanto de todas las transacciones y esta decidiría cuales llegaban primero. Para lograr esto sin un tercero confiable, las transacciones deben ser anunciadas públicamente [1], y necesitamos un sistema de participantes que estén de acuerdo con una historia única del orden en que estas fueron recibidas. El beneficiario necesita prueba de que a la hora de cada transacción, la mayoría de los nodos estuvieron de acuerdo que esta fue la primera que se recibió.

3. Servidor de marcas de tiempo.

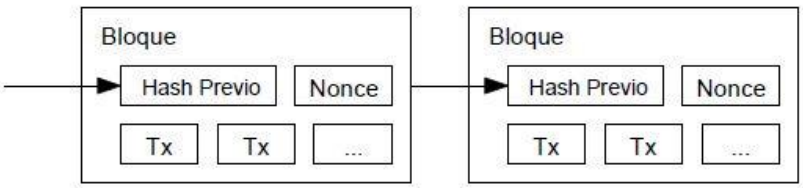
La solución que proponemos comienza con un servidor de marcas de tiempo. Un servidor de marcas de tiempo funciona al tomar un hash de un bloque de elementos a ser fechados y publicando ampliamente el hash, tal como en un periódico, o una publicación Usenet [2-5]. La marca de tiempo prueba que la data debe haber existido en el tiempo, obviamente, para meterse dentro del hash. Cada marca de tiempo incluye la marca de tiempo previa en su hash, formando una cadena, con cada marca de tiempo adicional reforzando las anteriores a esa.



4. Prueba-de-trabajo

Para implementar un servidor de marcas de tiempo en una base usuario-a-usuario, necesitaremos utilizar un sistema de prueba-de-trabajo similar al Hashcash de Adam Back [6], en vez de un periódico o una publicación en Usenet. La prueba-de-trabajo envuelve la exploración de un valor que al calcular un hash, tal como SHA-256, el hash empiece con un número de bits en cero. El trabajo promedio requerido es exponencial en el número de bits puestos en cero requeridos y puede ser verificado ejecutando un solo hash.

Para nuestra red de marcas de tiempo, implementamos la prueba-de-trabajo incrementando un nonce en el bloque hasta que un valor es encontrado que de el número requerido de bits en cero para el hash del bloque. Una vez que el esfuerzo de CPU se ha gastado para satisfacer la pruebade- trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo. A medida que más bloques son encadenados después de este, el trabajo para cambiar el bloque incluiría rehacer todos los bloques después de este.



La prueba-de-trabajo también resuelve el problema de determinar la representación en cuanto a decisión por mayoría. Si la mayoría fuese basada en un voto por dirección IP, podría ser subvertida por alguien capaz de asignar muchos IPs. Prueba-de-trabajo es esencialmente un- CPU-un-voto. La decisión de la mayoría es representada por la cadena más larga, la cual tiene la prueba-de-trabajo de mayor esfuerzo invertido en ella. Si la mayoría del poder de CPU es controlada por nodos honestos, la cadena honesta crecerá más rápido y pasará cualquier cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba-de-trabajo del bloque y de todos los bloques después y luego alcanzar y pasar el trabajo de los nodos honestos. Luego demostraremos

que la probabilidad de un atacante más lento de alcanzar disminuye exponencialmente a medida que bloques subsecuentes son añadidos.

Para compensar por el incremento de velocidad de hardware y en el interés variante de corre nodos en el tiempo, la dificultad de la prueba-de-trabajo es determinada por una media móvil dirigida a un número promedio de bloques por hora. Si estos se generan muy rápido, la dificultad incrementa.

5. La Red

Los pasos para gestionar la red son como sigue:

1) Transacciones nuevas son emitidas a todos los nodos.

2) Cada nodo recolecta nuevas transacciones en un bloque.

3) Cada nodo trabaja en encontrar una prueba-de-trabajo difícil para su bloque.

4) Cuando un nodo encuentra una prueba-de-trabajo, emite el bloque a todos los nodos.

5) Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no se han gastado ya.

6) Los nodos expresan su aceptación del bloque al trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo.

Los nodos siempre consideran la cadena más larga como la correcta y empiezan a trabajar en extenderla. Si dos nodos emiten versiones diferentes del próximo bloque simultáneamente, algunos nodos puede que reciban uno o el otro primero. En ese caso, trabajan en el primero que reciban pero guardan la otra rama en caso de que esta se vuelva más larga. El empate se rompe cuando la próxima prueba-de-trabajo es encontrada y una rama se vuelve más larga; los nodos que estaban trabajando en la otra rama luego se cambian a la más larga.

Las emisiones de nuevas transacciones no necesariamente necesitan llegar a todos los nodos. Tanto estas lleguen a muchos nodos, entrarán a un bloque antes de que pase mucho tiempo. Las emisiones de bloques también son tolerantes a mensajes perdidos. Si un nodo no recibe un bloque, lo va a pedir cuando reciba el próximo bloque y se de cuenta que se perdió uno.

6. Incentivo

Por convención, la primera transacción en el bloque es una transacción especial que comienza una moneda nueva cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial de distribuir monedas en circulación, dado que no hay una autoridad para crearlas. Esta adición estable de una cantidad constante de monedas nuevas es análoga a mineros de oro gastando recursos para agregar oro a la circulación. En nuestro caso, es el tiempo del CPU y la electricidad que se gasta.

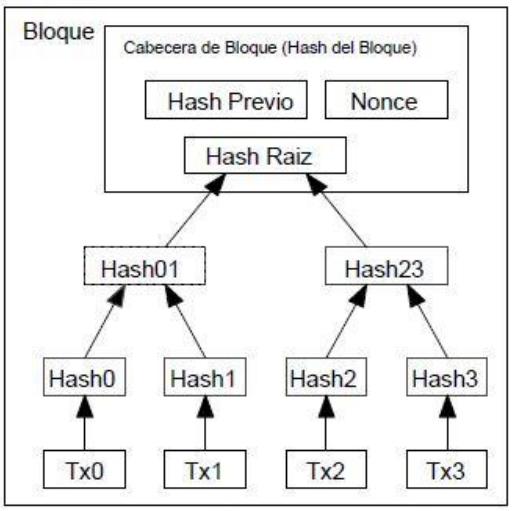
El incentivo también puede ser fundado con costos de transacción. Si el valor de salida de una transacción es menor que la entrada, la diferencia es una tarifa de transacción que se le añade al valor de incentivo del bloque que contiene la transacción. Una vez que un número predeterminado de monedas han entrado en circulación, el incentivo puede transicionar enteramente a tarifas de transacción y ser completamente libre de inflación.

El incentivo puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más potencia de CPU que todos los nodos honestos, este tendría que elegir entre

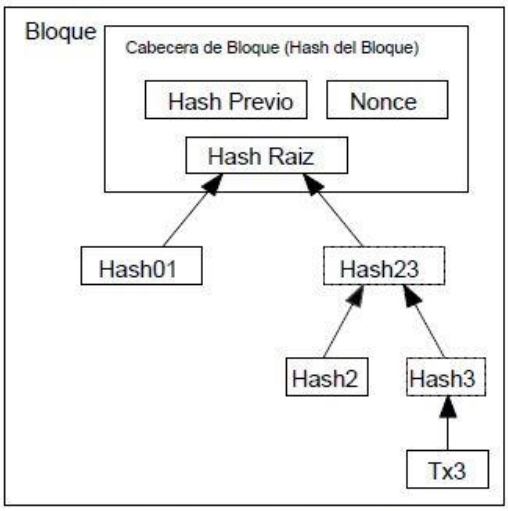
utilizarla para defraudar a la gente robando sus pagos de vuelta, o en utilizarla para generar monedas nuevas. Debería encontrar más rentable jugar por las reglas, tales reglas lo favorecen a él con más monedas que a todos los demás combinados, que socavar el sistema y la validez de su propia riqueza.

7. Reclamando Espacio en Disco

Una vez que la última transacción en una moneda es enterrada bajo suficientes bloques, las transacciones gastadas antes de estas pueden ser descartadas para ahorrar espacio en disco. Para facilitar esto sin romper el hash del bloque, las transacciones se les comprueba en un árbol Merkle [7] [2] [5], con la única raíz incluida en el hash el bloque. Los bloques viejos pueden ser compactados al sacar ramas del árbol. Los hashes interiores no necesitan ser guardados.



Transacciones *Hasheadas* en un árbol Merkle

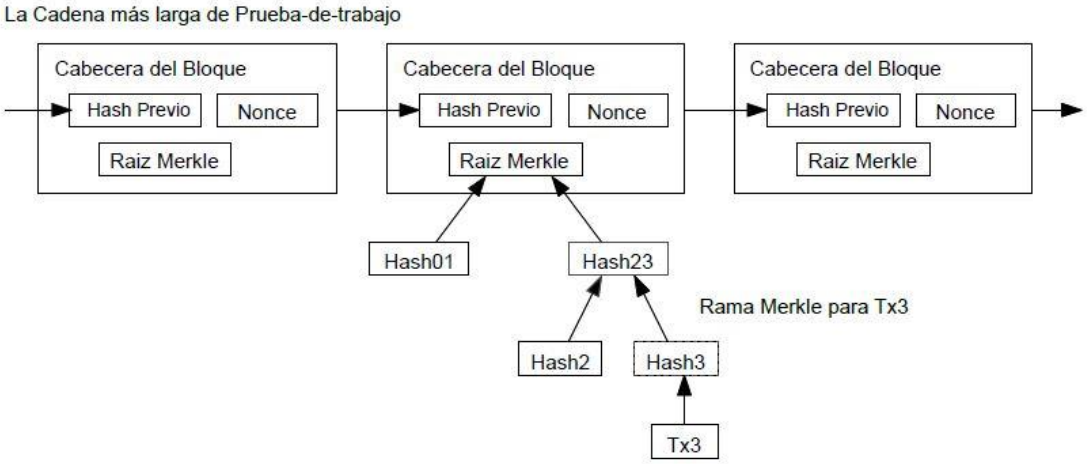


Después de podar Tx0-2 del Bloque

La cabecera de un bloque sin transacciones sería de unos 80 bytes. Si suponemos que cada bloque es generado cada 10 minutos, 80 bytes * 6 * 24 * 365 = 4.2MB por año. Con computadoras generalmente vendiéndose con 2GB de RAM para el 2008, y la ley de Moore prediciendo el crecimiento actual de 1.2GB por año, el almacenamiento no debe ser un problema aun si las cabeceras de los bloques deben permanecer en memoria.

8. Verificación de Pagos Simplificada

Es posible verificar pagos sin correr un nodo de red completo. Un usuario solo necesita mantener una copia de las cabeceras de los bloques de la cadena más larga de prueba-de-trabajo, la cual puede obtener haciendo una búsqueda en los nodos de red hasta que esté convencido que tenga la cadena más larga, y obtenga la rama Merkle que enlaza la transacción al bloque en que ha sido fechado. No puede verificar la transacción por sí mismo, pero al enlazarla a un lugar en la cadena, ahora puede ver que un nodo de la red la ha aceptado y los bloques añadidos después confirman aún más que la red lo ha aceptado.



Como tal, la verificación es confiable a medida que nodos honestos controlen la red, pero es más vulnerable si la red es dominada por un atacante. Mientras que los nodos de la red puedan verificar transacciones por sí mismos, el método simplificado puede ser engañado por las transacciones fabricadas de un atacante hasta que el atacante pueda continuar dominando la red. Una estrategia para protegerse de esto es aceptar alertas de los nodos de la red cuando detecten un bloque inválido, pidiéndole al usuario que se baje el bloque completo y las transacciones alertadas para confirmar la inconsistencia. Los negocios que reciban pagos frecuentes van a querer correr sus propios nodos para seguridad más independiente y verificación más rápida.

9. Combinando y Dividiendo Valor

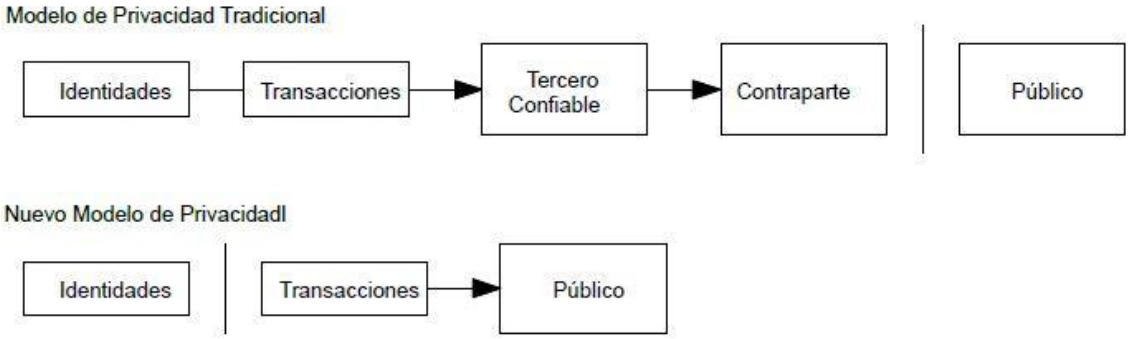
Aunque sería posible manipular monedas individualmente, sería difícil de manejar el hacer una transacción por cada centavo en una transferencia. Para permitir que el valor se divida y se combine, las transacciones contienen múltiples entradas y salidas. Normalmente habrá o una sola entrada de una transacción previa más grande o múltiples entradas combinando cantidades más pequeñas, y al menos dos salidas: una para el pago, y una para devolver el cambio, si es que hay algún cambio, de vuelta al emisor.

Debe ser notado que donde una transacción depende de varias transacciones, y esas transacciones dependen en muchas más, no hay ningún problema. Nunca existe la necesidad de extraer una copia completa de la transacción por si sola de la historia de transacciones.

10. Privacidad

El modelo bancario tradicional logra un nivel de privacidad al limitar el acceso a la información de las partes envueltas y del tercero confiado. La necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún puede ser mantenida al romper el flujo

de la información en otro lugar: al mantener las claves públicas anónimas. El público puede ver que alguien está enviando una cantidad a otra persona, pero sin información que relacione la transacción a ninguna persona. Esto es similar al nivel de información mostrado por las bolsas de valores, donde el tiempo y el tamaño de las transacciones individuales, la "cinta", es público, pero sin decir quiénes son las partes.



Como un cortafuegos adicional, un par nuevo de claves debe ser utilizado para cada transacción de modo que puedan ser asociadas a un dueño en común. Algún tipo de asociación es inevitable con transacciones de múltiples entradas, las cuales pueden revelar que sus entradas fueron apropiadas por el mismo dueño. El riesgo está en que, si el dueño de una clave es revelado, el enlazado podría revelar otras transacciones que pertenecieron al mismo dueño.

11. Cálculos

Consideramos el escenario en el que un atacante intenta generar una cadena alterna más rápido que la cadena honesta. Aún si esto es logrado, esto no abre el sistema a cambios arbitrarios, tal como crear valor del aire o tomar dinero que nunca le perteneció al atacante. Los nodos no aceptarían una transacción inválida como pago, y los nodos honestos nunca aceptará un bloque que las contenga. Un atacante puede únicamente intentar cambiar solo una de sus propias transacciones para retomar dinero que ha gastado recientemente.

La carrera entre una cadena honesta y la cadena de un atacante puede ser caracterizada como una Caminata Aleatoria Binomial. El evento de éxito es la cadena honesta siendo extendida por un bloque, incrementar esta ventaja por +1, y el evento de fracaso es la cadena del atacante siendo extendida por un bloque reduciendo la distancia por -1.

La probabilidad de que un atacante pueda alcanzar desde un déficit dado es análogo al problema de la Ruina del Apostador. Supóngase que un apostador con crédito ilimitado empieza en un déficit y juega potencialmente un número infinito de intentos para intentar llegar a un punto de equilibrio. Podemos calcular la probabilidad de que llegase al punto de equilibrio, o que un atacante llegue a alcanzar a la cadena honesta, como sigue [8]:

p = probabilidad de que un nodo honesto encuentre el próximo bloque

q = probabilidad de que el atacante encuentre el próximo bloque

qz = probabilidad de que el atacante llegue a alcanzar desde z bloques atrás.

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Dada nuestra hipótesis de que p > q, la probabilidad cae exponencialmente mientras que el número de bloques el cual el atacante debe alcanzar incrementa. Con las probabilidades en contra, si no hace una estocada afortunada desde el principio, sus chances se vuelven extremadamente pequeños a medida que se queda más atrás.

Ahora consideramos cuánto necesita esperar el recipiente de una nueva transacción antes de tener la certeza suficiente de que el emisor no puede cambiar la transacción. Asumimos que el emisor es un atacante el cual quiere hacerle creer al recipiente que le pagó durante un rato, luego cambiar la transacción para pagarse de vuelta a sí mismo una vez que ha pasado un tiempo. El receptor será alertado cuando esto suceda, pero el emisor espera que sea demasiado tarde.

El receptor genera un nuevo par de claves y entrega la clave pública al emisor poco después de hacer la firma. Esto previene que el emisor prepare una cadena de bloques antes de tiempo al trabajar continuamente hasta que tenga la suerte de adelantarse lo suficiente, y luego ejecutar la transacción en ese momento. Una vez que la transacción es enviada, el emisor deshonesto empieza a trabajar en secreto en una cadena paralela que contiene una versión alterna de su transacción.

El recipiente espera a que la transacción sea añadida al bloque y z bloques han sido enlazados después de la transacción. El no necesita saber la cantidad exacta de progreso que al atacante ha logrado, pero asumiendo que los bloques honestos se tardaron el promedio esperado por bloque, el progreso potencial del atacante será una distribución de Poisson con un valor esperado:

$$\lambda = z\frac{q}{p}$$

Para obtener la probabilidad de que el atacante aún pueda alcanzar ahora, multiplicamos la densidad de Poisson por cada cantidad de progreso que pudo haber hecho por la probabilidad de que pudo alcanzar desde ese punto:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Re-organizamos para evitar la suma de la cola infinita de la distribución...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Convertimos a código en C...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
```

```
double p = 1.0 - q;
double lambda = z * (q / p);
double sum = 1.0;
int i, k;
for (k = 0; k <= z; k++)
{
          double poisson = exp(-lambda);
          for (i = 1; i <= k; i++)
              poisson *= lambda / i;
          sum -= poisson * (1 - pow(q / p, z - k));
}
return sum;
   }
```

Ejecutamos algunos resultados, podemos ver que la probabilidad cae exponencialmente con z.

```
q=0.1
z=0 P=1.0000000
z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173
z=9 P=0.0000046
z=10 P=0.0000012

q=0.3
z=0 P=1.0000000
z=5 P=0.1773523
z=10 P=0.0416605
z=15 P=0.0101008
z=20 P=0.0024804
z=25 P=0.0006132
z=30 P=0.0001522
z=35 P=0.0000379
z=40 P=0.0000095
z=45 P=0.0000024
z=50 P=0.0000006
```

Resolvemos para P menor que 0.1%...

```
P < 0.001
q=0.10 z=5
q=0.15 z=8
q=0.20 z=11
q=0.25 z=15
q=0.30 z=24
q=0.35 z=41
q=0.40 z=89
 q=0.45 z=340
```

12. Conclusión

Hemos propuesto un sistema para transacciones electrónicas sin depender en confianza. Comenzamos con el marco habitual de monedas hechas de firmas digitales, el cual provee un control fuerte de propiedad, pero es incompleto sino existe una forma de prevenir doble-gasto. Para solucionar esto, hemos propuesto una red usuario-a-usuario que utiliza prueba-de-trabajo para registrar una historia pública de transacciones la cual rápidamente se convierte impráctica

computacionalmente para que un atacante pueda cambiar si nodos honestos controlan la mayoría del poder de CPU. La red es robusta en su simplicidad no estructurada. Los nodos pueden trabajar todos al mismo tiempo con poca coordinación. No necesitan ser identificados, dado que los mensajes no son enrutados a ningún lugar en particular y solo necesitan ser entregados bajo la base de un mejor esfuerzo. Los nodos pueden irse y volver a la red a voluntad, aceptando la cadena de prueba-de-trabajo como prueba de lo que sucedió mientras estuvieron ausentes. Votan con su poder de CPU, expresando su aceptación de los bloques válidos al trabajar extendiéndose y rechazando bloques inválidos al refutar trabajar en ellos. Cualquier reglas necesarias e incentivos se pueden hacer cumplir con este mecanismo de consenso.

Anexo II

Proyecto de ley criptomonedas presentado al Congreso

(Schwint, 2020)

PROYECTO DE LEY REGULACIÓN DE CRIPTOACTIVOS

Artículo 1°- Objeto y Ámbito de Aplicación. La presente Ley tiene por objeto crear un marco regulatorio integral aplicable a las transacciones y operaciones civiles y comerciales de criptoactivos, como medio de pago, ahorro o inversión, incluyendo a todo el ecosistema fintech, llevadas a cabo entre personas humanas, jurídicas privadas o públicas, sean residentes en el país o en el exterior, así como las disposiciones referidas a la protección, vigilancia, inspección y control de dichas transacciones y operaciones como también a todos los que participan en procesos de tecnología blockchain, y los sujetos considerados por la presente Ley como entes operadores, dentro del territorio nacional.

Artículo 2°- Principios. Las transacciones y operaciones de criptoactivos estarán basadas en los principios de confiabilidad, inviolabilidad y reserva de la información, inclusión e innovación tecnológica y financiera, conforme a los usos y costumbres propios de la actividad, la promoción de la competencia privada y la cooperación internacional, la protección al consumidor, al medioambiente, la prevención del lavado de activos y el financiamiento del terrorismo, el derecho a la información, y otras actividades ilícitas.

Artículo 3°- Definiciones. A los efectos de la presente ley, se entenderán como definiciones que permitan la interpretación de la misma, los siguientes:

3.1 Criptoactivos: Representación digital de valor en tanto activo financiero encriptado, definido por un protocolo computacional que puede ser objeto de comercio digital y cuyas funciones son las de constituir un medio de intercambio y/ o pago, y/o una unidad de cuenta, y/o una reserva de valor, y/o herramienta de inversión financiera, y/o medio de financiación, que no posee curso legal y es de carácter descentralizado, estando su valor sujeto a la variación de precios dependiendo de la oferta y demanda en los mercados.

3.2 Banco de prueba de software o Sandbox: Entorno de prueba. Espacios de desarrollo que permiten el ensayo de nuevas tecnologías en un marco de acción limitado donde convergen actores públicos y privados. 3.3 White Paper: Instrumento de carácter público elaborado por el emisor de tokens, que detalla los aspectos técnicos y comerciales del proyecto a financiar.

3.4 Fork o Bifurcación: Es una actualización de código. Se introducen cambios en el software original, pudiendo ser necesaria la actualización de la plataforma. De él pueden surgir un softfork o un hardfork.

3.5 Softfork: El cambio que se requiere producir en el código, no supone incompatibilidad con las versiones anteriores.

3.6 Hardfork: El cambio que se quiere producir en el código, supone la incompatibilidad con las versiones anteriores generando un nuevo criptoactivo donde cada wallet del nuevo criptoactivo tendrá un valor equivalente al del criptoactivo que dio origen a la bifurcación o fork.

3.7 Granja de Criptoactivos: Persona jurídica y personas físicas que realizan la actividad de validación criptográfica de datos en un espacio físico en territorio nacional.

3.8 Token: Bien intangible representado en forma numérica y que atribuye derechos o expectativas de participación potencial en la revalorización o rentabilidad del proyecto de inversión expresado en el White paper. Pueden emitirse, inscribirse, conservarse o transferirse mediante un dispositivo de registro electrónico compartido, que permite identificar, directa o indirectamente, al propietario de dicho bien.

3.9 ICO: Oferta inicial de criptoactivos, que funciona como método de financiación de proyectos. Se debe detallar en un documento técnico denominado White paper cómo funcionará el criptoactivo. Se hará un llamado a la inversión sobre el mismo a través de tokens.

3.10 Trading con criptoactivos. Para efectos de la presente Ley, trading son todas aquellas acciones de compra y venta de monedas virtuales en diferentes plataformas de venta denominadas Exchange, realizadas por traders expertos con conocimiento y experiencia en las transacciones de este tipo.

3.11 De los traders. Se denominan traders las personas naturales o jurídicas que realizan en nombre propio, o por mandato, o administración, trading con criptoactivos, con fines de incrementar los capitales que se reflejan en los valores de cada criptoactivos usada en las plataformas correspondientes, a través operaciones de compra y venta; poniendo a disposición sus conocimientos previos adquiridos, así como los estudios técnicos de mercado que se tengan a su disposición. Todo trader que tenga en poder fondos de terceros deberá contar con una autorización expedida por autoridad de control, que lo habilita para realizar asesorías o transacciones mediante contrato de mandato o de administración. Las personas jurídicas, deberán contar con personal autorizado para la realización de trading con criptoactivos. En todo caso, los traders deberán cumplir con lo establecido en el artículo 6°, de la presente Ley, respecto del consentimiento informado.

3.12 Actos jurídico con criptoactivos. Son aquellas mediante las cuales las partes manifiestan su voluntad libre e informada de realizar las transacciones con criptoactivos, que permitan la creación de actos jurídicos que los vinculen entre sí, siempre que éstos se conceptúen únicamente sobre actividades lícitas y legales.

3.13 Exchange. Es una plataforma que permite operar entre distintos criptoactivos, bajo el libre juego de oferta y demanda dándole un valor económico al mismo.

Artículo 4°- Autoridad de aplicación. La supervisión del cumplimiento de lo dispuesto en esta ley corresponderá a la Comisión Nacional de Valores (CNV) con actividades supletorias de la UIF teniendo en cuenta la Ley n° 25.246.

Artículo 5°- Competencias. Será competencia de la autoridad de aplicación el estudio y la consecuente elaboración de informes sobre la factibilidad de la creación de un criptoactivo nacional.

Artículo 6°- Atribuciones. Serán atribuciones de la Comisión Nacional de Valores:

1) Elaborar políticas tendientes a la regulación, protección, vigilancia, inspección y control de las operaciones con criptoactivos conforme a la legislación vigente;

2) Elaborar y mantener un registro nacional de las operaciones realizadas con criptoactivos;

3) Disponer la realización de auditorías, inspecciones y pericias vinculadas a la actividad normada por la presente ley;

4) Solicitar informes y opiniones a entidades públicas o privadas especializadas en criptoactivos;

5) Llevar a cabo políticas de fomento tendientes a propiciar la utilización de criptoactivos, dando a conocer sus beneficios y riesgos en pos de informar a aquellos adquirentes que deseen realizar transacciones con criptoactivos;

6) Todo trader que administre fondos de terceros, deberá contar con autorización expedida por autoridad competente que lo habilite a realizar asesorías o transacciones mediante contrato de mandato. Las personas jurídicas deberán contar con personal autorizado para la realización de trading con criptoactivos. Los traders deberán cumplir con lo establecido en el artículo 6o de la presente ley, respecto del consentimiento informado

Artículo 7°- Consentimiento informado. Es el deber que tienen las entidades de operaciones con criptoactivos, para con el adquirente, de informar las especificaciones de la comercialización con monedas virtuales, las formas en que pueden adquirir las criptoactivos y toda información que sea necesaria para el cabal entendimiento del uso de las monedas digitales. Así mismo, se deberá informar lo siguiente: a. Las criptoactivos no son monedas de curso legal, y por tal razón no tienen respaldo del Gobierno Nacional, ni del Banco Central de la República Argentina b. Las operaciones realizadas no son reversibles después de ejecutadas. c. Las monedas digitales y el mercado donde éstas operan, son volátiles, y su control está sometido a las reglas propias de ese mercado. d. Existen riesgos tecnológicos, cibernéticos y de fraude inherentes a las operaciones con criptoactivos. e. No existen días inhábiles ni horarios de cierre para hacer operaciones. Este consentimiento informado deberá estar siendo actualizado, según aparezcan nuevos riesgos para las transacciones con criptoactivos.

Artículo 8°- Facultades y obligaciones de los operadores o Exchange con criptoactivos. Se regirán por los términos que surjan de la Reglamentación de la presente ley, teniendo en cuenta como referencia la ley 26.831 de mercado de capitales

Artículo 9°- Condiciones de cumplimiento. Las partes están en libertad de establecer las condiciones de cumplimiento de los actos jurídicos con criptoactivos, sin más límite que los establecidos en esta ley y en aquellas que regulen este tipo de actos. No podrán utilizarse los criptoactivos como medio de pago en especies para extinguir obligaciones de naturaleza laboral y cargas familiares como la cuota alimentaria, entre otras.

Artículo 10°- Representación en moneda legal de los criptoactivos. El valor de los criptoactivos puede ser tasado en moneda de curso legal, para lo cual, las partes podrán establecer dichos valores mediante la plataforma utilizada, ya sea al momento de adquirir la obligación o al de la ejecución de la misma. Si no se establece, se entenderá la tasada al momento del cumplimiento del acto jurídico.

Artículo 11°- Inspección, vigilancia y control. La inspección, vigilancia y control sobre entidades de operaciones con criptoactivos estará a cargo de la autoridad de aplicación.

Artículo 12°- Sujetos obligados. Las casas de cambio o Exchange serán consideradas como sujetos obligados a informar a la Unidad de Información Financiera de acuerdo a los artículos 20, 20 bis, 21, 21 bis y 22 de la ley 25.246.

Artículo 13°- La inspección, vigilancia y control sobre entidades de operaciones con criptoactivos, respecto de la relación entre ésta y el proyecto , lo hará la autoridad de aplicación, con intervención, cuando corresponda, de las autoridades y normativa de las leyes 24240 de Defensa del Consumidor y 27742 de Defensa de la Competencia en especial a lo relacionado con comercio electrónico, oferta, publicidad engañosa y lo demás regulado en dichas leyes y normas complementarias, en lo que sean aplicables.

Artículo 14°- La autoridad de aplicación tendrá la facultad de establecer entornos de prueba de software para incentivar la innovación financiera en Fintech, promoviendo un espacio de desarrollo que conjugue la seguridad, competencia y eficiencia con la innovación. Estos espacios de prueba

estarán abiertos a Exchange, desarrolladores de software o cualquier entidad que realice actividades comerciales con criptoactivos u otra aplicación de blockchain. Los participantes de sandbox deberán seguir las regulaciones hechas a la medida, establecidas dentro de este marco con una cantidad de tiempo y usuarios limitada, compartiendo toda la información necesaria y ofreciendo un trato justo a clientes basado en el consentimiento informado.

Artículo 15°- Toda vez que una persona humana o jurídica esté inscrita debidamente en el registro de la autoridad de aplicación, que actúe como entidad de operaciones con criptoactivos y realice transacciones sin cumplir con los requerimientos previstos en la presente ley, será sancionada con cancelación de la matrícula de comercio, con la suspensión o revocación de la autorización para actuar correspondiente, o con penas de multas, conforme lo determine la reglamentación de la presente ley. A su vez, el prestador de servicio de intercambio de criptoactivos, omitiera o falte al deber de información el usuario tendrá derecho a demandar la nulidad del contrato o de una o más de sus cláusulas.

Artículo 16°- Contrato de Financiamiento Colectivo. Habrá contrato de financiamiento colectivo cuando un emisor de tokens se obligue a transferir la propiedad sobre los tokens que emita, con el fin de financiar el proyecto de emisión expresado en el White Paper correspondiente a la emisión, y la otra parte, denominada inversor, a pagar un precio en moneda de curso legal, moneda extranjera o criptoactivos de otra especie. Junto con la primera transferencia del token el emisor deberá entregar copia en soporte digital o papel del White Paper.

Artículo 17°- Derechos derivados de los tokens. Los tokens pueden otorgar a su titular a su actividad: a) un derecho a expectativa de participación potencial en la revalorización, rentabilidad o la obtención de un beneficio del proyecto de inversión, el cual se denomina token de utilidad; b) un derecho representativo de una cuota parte del capital empleado para el desarrollo del proyecto, el cual se denomina token de seguridad. En ambos casos, su titular tendrá la posibilidad de negociación en mercados equivalentes o similares a los mercados de valores regulados.

Artículo 18°- White paper. Previo a la oferta inicial de token, el emisor deberá elaborar un instrumento que de carácter público denominado White Paper, el cual deberá contener los siguientes requisitos: a) la razón social o denominación del emisor, el domicilio del órgano ejecutivo y la dirección de sitio web; b) el nombre, razón social a denominación de la autoridad central que ejecute el registro electrónico compartido, su domicilio y la dirección de su sitio web, si la tuviese; c) información detallada sobre el proyecto cuya ejecución se pretende desarrollar. Particularmente se deberá contar con el objetivo del proyecto, la forma y los plazos de ejecución e información precisa acerca del capital necesario para el desarrollo y los rubros en los cuales se lo pretende emplear; d) los riesgos provenientes de la inversión que pudieren suscitarse. El emisor en ningún caso podrá garantizar la concreción del proyecto. El incumplimiento de este precepto traerá aparejado la responsabilidad por daños y perjuicios al emisor; e) el precio por token y la forma en que se determina esa cifra; f), la forma de distribución de token de acuerdo aplauso diferentes etapas de emisión, la cantidad de descuentos concedidos, si los hubiere; g), el número de tokens emitidos y aquellos reservados para futuras transferencias en las siguientes etapas del proyecto. Este documento de información y las comunicaciones de carácter promocionales relativas a la oferta inicial de tokens deberán presentar un contenido claro, preciso y no deberá inducir al error del inversor. Previo a la oferta inicial, deberá remitirse copia de este documento a la UIF, la cual constatará el cumplimiento de los presupuestos legales establecidos en esta ley y por las normas que ésta dicte, y en su caso emitirá la autorización para la ejecución de la oferta inicial. La resolución deberá ser emitida dentro de los quince días hábiles de recepcionada la copia. La resolución denegatoria es apelable al solo efecto devolutivo, en el plazo de diez días desde su notificación.

Artículo 19°- Revocación. Si tras haber emitido su autorización la Comisión Nacional de Valores constata que la oferta inicial al público ya no se ajusta al contenido del White Paper, podrá ordenar que se ponga fin a cualquier nueva suscripción o emisión así como cualquier comunicación de

carácter promocional en relación con la oferta y retirar su autorización en las condiciones especificadas en su reglamento general

Artículo 20°- Operaciones Excluidas. A los fines de esta ley no habrá contrato de financiamiento colectivo, cuando la oferta inicial de token: a) Esté dirigido exclusivamente a inversores cualificados definidos por la autoridad de aplicación. b) Esté dirigida a un número de personas que sea inferior al establecido por la autoridad de aplicación, sin incluir inversores cualificados. c) Esté dirigida a inversores que adquieran tokens por un importe superior al establecido por la autoridad de aplicación. d) El valor nominal del valor unitario del token sea, como mínimo, el monto fijado por la autoridad de aplicación.

Artículo 21°- Monitoreo financiero de la actividad. Se instruye dependencia en el Banco Central de la República Argentina con el objeto de monitorear la información sobre las transacciones con criptoactivos en el mercado local y por residentes nacionales en mercados extranjeros; elaborar informes de impacto y evolución en la economía nacional y economías extranjeras; establecer la repercusión en las políticas monetarias, recopilar información actualizada sobre la materia por organismos e instituciones internacionales de relevancia.

Artículo 22°- Partidas presupuestarias. El Poder Ejecutivo dispondrá de las partidas presupuestarias específicas necesarias para solventar los gastos de la presente ley.

Artículo 23°- Sanciones. Las operaciones con criptoactivos que se celebren en contravención de lo establecido por esta ley o en las disposiciones que de ella emanen, darán lugar a la imposición de sanciones administrativas y penales que correspondan. Ante estos supuestos se remite al Código Penal de la Nación y a la ley nacional de procedimiento administrativo.

Artículo 24°- Programa de capacitación. Créase el programa de capacitación para funcionarios del Estado sobre tratamiento de criptoactivos a cargo de la Comisión Nacional de Valores.”

Artículo 25°- Obligatoriedad. La participación en el programa mencionado en el artículo precedente será obligatoria para todo funcionario, ministro y empleado público que, en ejercicio de sus funciones, tenga a su cargo asuntos con criptoactivos, en particular quienes se desempeñen bajo la órbita de la autoridad de aplicación de esta ley.

Artículo 26°- Reglamentación. La presente ley será reglamentada por el Poder Ejecutivo en el término de ciento ochenta (180) días desde su publicación.

Artículo 27°- La presente ley es de orden público y de aplicación en todo el territorio de la Nación Argentina y en los lugares sometidos a su jurisdicción.

Artículo 28°- De Forma.

FUNDAMENTOS

Sr. Presidente:

El espíritu de esta Ley es la Sanción de un Marco Regulatorio integral que se aplique a todas las transacciones y operaciones civiles y comerciales que comprendan criptoactivos, ya sea como medio de pago, ahorro o inversión, incluyendo a todo el ecosistema fintech, ya sean personas humanas, jurídicas, privadas o públicas, residentes en el país o el exterior, garantizando la seguridad jurídica de los inversores, y respetando las recomendaciones OCDE que fueron formuladas en el G20 del 28 de junio de 2019 en Tokio. Generando un entorno amigable a los desarrolladores nacionales que

lideran la formulación de proyectos fintech a nivel global. Para esto será vital también la creación de mecanismos de promoción que beneficien a los actores que desarrollan este tipo de tecnología financiera y tecnologías asociadas como la blockchain o cadena de bloque. El Presente proyecto de Ley surge como iniciativa de una actividad académica-legislativa, denominada Cambio de Roles, realizada por el Instituto de Estudios Estratégicos y Relaciones Internacionales (I.E.E.R.I.) del Circulo de Legisladores de la Nación Argentina, el 6 y 7 de junio del 2019, en donde confluyeron estudiantes de nueve universidades nacionales de todo el país pertenecientes a las carreras de Ciencias Políticas, Relaciones Internacionales y Economía, entre otras, tomando el rol de legisladores llegando al consenso a través de un dictamen de mayoría en la Comisión de Finanzas, sobre los 9 proyectos formulados por las Universidades de Buenos Aires, Universidad Torcuato Di Tella, Universidad de San Andrés, Universidad Nacional de Tucumán, Universidad Nacional de Rosario, Universidad Nacional de La Matanza, Universidad Nacional del Comahue, Universidad Nacional de Cuyo y Universidad Católica de La Plata, que tuvieron tratamiento en las distintas comisiones por las que paso, votándose en Recinto un Anteproyecto que es la base del presente proyecto de Ley.

El panorama internacional actual presenta un ritmo de crecimiento vertiginoso de los mercados de criptoactivos. Países a lo largo y a lo ancho del globo han modificado su escenario legal y político en sintonía con esta situación. No todos los países ven el advenimiento de los criptoactivos solo como una amenaza. Muchas de las jurisdicciones, si bien no las adoptan como moneda de curso legal, ven un gran potencial en su uso, y trabajan en torno a desarrollar un marco regulatorio amigable a los fines de propiciar la realización de inversiones en sectores tecnológicos claves para el desarrollo económico en el largo plazo. La resultante disponibilidad de un set cada vez más amplio de información hace posible identificar patrones de comportamiento y funcionamiento de dichos mercados.

A raíz de este contexto surge la necesidad de legislar aspectos relacionados a la seguridad de los actores que intervienen en los procesos, sin dejar de lado cuestiones ligadas a la prevención de actos ilícitos. Dicho imperativo se deriva de las inversiones en infraestructura de pagos en monedas virtuales, basadas en protocolos de software. El anonimato que estas permiten frente a los métodos tradicionales de pago sin efectivo, así como sus riesgos inherentes, tales como el lavado de activos y el financiamiento terrorista, hacen de la regulación una respuesta necesaria. Dicho anonimato que de manera natural trae consigo estas herramientas tecnológicas es que aparece el primer inconveniente de importancia y que el Estado deberá resolver. Este es el poder determinar la procedencia y el destino de los fondos con los que se operará en este mercado global de criptoactivos.

Asimismo, y debido a la ausencia del control necesario, podrían darse casos de evasión impositiva cuando no pudiese detectarse la registración de las operaciones; o bien elusión impositiva si las partes acordaran un valor ficto a las transacciones. Si esto se produjera habría dos clases de contribuyentes, aquellos que lo hacen de acuerdo a las normas y reglamentos que gravan a la actividad formal y cumplen a conciencia con los mismos, y los que se verían beneficiados por estas maniobras de elusión o evasión.

Hoy en día, el mercado bursátil se encuadra dentro del marco legal de la Comisión Nacional de Valores. Con respecto a los criptoactivos, estos tienen un funcionamiento y características similares a los activos financieros en el mercado bursátil, por lo tanto, pueden ser encuadradas dentro de ese mecanismo, siendo la Comisión Nacional de Valores la autoridad de aplicación correspondiente. Esta organización permitiría un control y registro de las inversiones realizadas. Siendo así, y conforme a las atribuciones del Honorable Congreso de la Nación reguladas en el artículo 75 de nuestra Constitución Nacional, sería de su competencia intervenir en su regulación, en tanto es su atribución hacer sellar moneda, fijar su valor, y el de las extranjeras, así como también fijar un sistema uniforme de pesos y medidas para toda la Nación. Aun cuando no se considere a los criptoactivos como monedas de curso legal, se adopta en este proyecto la idea de que la circulación de estos activos transnacionales impactan directamente en el sistema financiero y en la economía nacional.

Teniendo en cuenta entonces que la Constitución Nacional faculta exclusivamente al Congreso para legislar esta actividad, la falta de una legislación específica que regule a los criptoactivos traduciría dichas atribuciones conferidas al Congreso en letra muerta. Frente a este panorama se perciben dos posiciones iniciales de política legislativa: en primer lugar, una postura de pasividad estatal que no ofrece una solución o bien prohíbe de entrada una posible reglamentación; o por el contrario, un posicionamiento que opta por una efectiva regulación, buscando proteger al consumidor a la vez que se fomenta la competencia privada, sin descuidar los peligros propios de los sistemas de criptoactivos, como el lavado de activos y la financiación del terrorismo.

Dentro del amplio margen regulatorio, no es óptimo ofrecer una normativa laxa pero tampoco así un régimen sancionatorio que termine por desnaturalizar a esta innovadora herramienta financiera. Tomando nota de lo expuesto previamente, el presente proyecto de ley se encuentra asentado sobre cuatro principios fundamentales:

i) La protección al consumidor, siendo necesario darle una protección especial al sujeto último implicado en las actividades comerciales, especialmente frente a los riesgos generados por el uso de criptoactivos que podrían vulnerarlos.

ii) La prevención del fraude y otras actividades delictivas, dado que por la naturaleza de los criptoactivos, estos mismos representan un riesgo de operaciones.

iii) La promoción de la competencia privada basada en una reglamentación clara yaccesible a los emprendedores.

iv) La innovación tecnológica, con el fin de fomentar la investigación y el desarrollo para obtener beneficios tanto privados como sociales.

Por todo lo antes dicho, solicito a las señoras diputadas y a los señoresdiputados, que me acompañen en la aprobación del presente proyecto de ley.-

Diputada Nacional María Liliana Schwint-

Anexo III

Opinión de un magnate sobre el Bitcoin

(Infotechnology.com, s.f.)

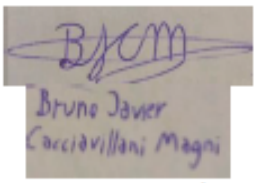
Marcos Galperin, empresario argentino y fundador de Mercado Libre, logró multiplicar el capital invertido en la criptodivisa en el año 2013, gracias al elevado incremento de su cotización. Sin embargo, en una entrevista concedida a infotechnology.com, destacó que aunque el Bitcoin puede ser utilizado como reserva de valor competitiva, enfrenta a su vez la limitación producida por el requerimiento de mucha energía para procesar sus transferencias, lo cual impide el desarrollo de la escalabilidad necesaria para funcionar como medio de pago transaccional en todos los ámbitos de la economía global.

A pesar de esto, augura un escenario futuro favorable en el que estos obstáculos podrán ser resueltos debido a los avances generados en el ámbito de la computación cuántica.

DECLARACIÓN JURADA RESOLUCIÓN 212/99 CD

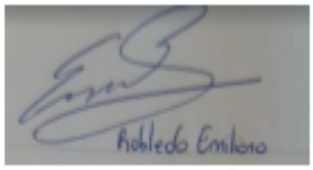
El autor de este trabajo declara que fue elaborado sin utilizar ningún otro material que no haya dado a conocer en las referencias que nunca fue presentado para su evaluación en carreras universitarias y que no transgrede o afecta los derechos de terceros.

Mendoza, 31/03/2021



Firma y aclaración
29.695
Número de registro
39.952.578
DNI

Ruiz, Isaías.
Firma y aclaración
28.901
Número de registro
38.580.261
DNI



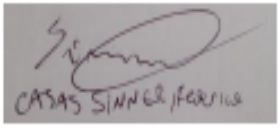
Firma y aclaración

29.334

Número de registro

39.081.634

DNI



Firma y aclaración

29.446

Número de registro

40.241.673

DNI