



BITCOIN: LA EVOLUCIÓN DEL DINERO

AUTORES

JULIANA TOBÓN TOBÓN

ÁLVARO GRAJALES PATIÑO

DIRIGIDA POR

DR. IUR. SANTIAGO DUSSAN, LL.M. (COLOGNE)

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE HUMANIDADES Y CIENCIAS SOCIALES

CARRERA DE DERECHO

SANTIAGO DE CALI

2021

ÍNDICE

1. Introducción
2. Objetivos de investigación
 - 2.1. Objetivo general
 - 2.2. Objetivos específicos
3. Desarrollo de los objetivos
 - 3.1. Criptomonedas
 - 3.1.1. La tecnología detrás de las criptomonedas: la cadena de bloques (*Blockchain*)
 - 3.1.2. Bitcoin: la primera criptomoneda
 - 3.1.2.1. Surgimiento del Bitcoin
 - 3.1.2.2. Aspectos relevantes del Bitcoin y su funcionamiento
 - 3.1.2.2.1. Los sistemas que soportan las transacciones en Bitcoin son descentralizados
 - 3.1.2.2.2. La principal característica funcional de Bitcoin es la verificación
 - 3.1.2.2.3. La oferta de Bitcoin es limitada y no se puede alterar
 - 3.1.2.2.4. Bitcoin es divisible
 - 3.1.2.2.5. Bitcoin es fácilmente portable
 - 3.1.2.2.6. Bitcoin depende de incentivos económicos
 - 3.1.2.2.7. Bitcoin puede operar con una relativa seguridad
 - 3.1.2.3. ¿Qué es Bitcoin?
 - 3.2. Teoría del dinero: El origen evolutivo del dinero
 - 3.2.1. Truque spot
 - 3.2.2. Trueque diferido

3.2.3. La alternativa

3.2.4. Funciones del dinero

3.2.5. ¿Qué es el Bitcoin?

3.2.6. Competencia de las diferentes criptomonedas

3.3. Marco regulatorio del dinero en Colombia

3.3.1. Intervención

3.3.2. Monopolio

3.3.3. Marco regulatorio general del dinero de curso legal en Colombia

3.4. Marco regulatorio de las criptomonedas en Colombia

3.4.1. Banco de la República de Colombia

3.4.2. Superintendencia Financiera de Colombia

3.4.3. Superintendencia de Sociedades de Colombia

3.4.4. Dirección de Impuestos y Aduanas (DIAN)

4. Conclusión

5. Referencias bibliográficas

1. Introducción

Con el pasar de los años, los individuos han perdido la capacidad de ver la realidad por sí mismos. Se ha vuelto costumbre en la humanidad, necesitar de una institución, por perversa que sea, para que diga que es verdad o mentira, que existe y que no. La institución que más relevancia ha tomado para expresarse sobre lo anterior es el Estado. A través de él se ha negado la verdad por años¹.

¹ Un ejemplo de ello, fue la negación de derechos naturales que hizo el régimen socialista alemán a través del ordenamiento jurídico del Estado. El Partido Nacionalsocialista Alemán (NAZI), a través del derecho positivo,

Ahora, el presente trabajo busca establecer si el Estado, a través del ordenamiento jurídico, intenta desconocer otra realidad. A lo largo de este texto, estudiaremos, en primer lugar, la cadena de bloques o *Blockchain*, aquel invento innovador y tecnológico que es utilizado para realizar las transacciones en criptomonedas toda vez que permite que su funcionamiento sea descentralizado, seguro y casi imposible de falsificar. En segundo lugar, estudiaremos el Bitcoin, un revolucionario desarrollo tecnológico que se convirtió en un medio de intercambio y que se constituye en una alternativa de libre elección a las monedas de curso legal. Estudiaremos su origen, qué es y cómo funciona. La problemática radica en que, a pesar de que esta criptomoneda se utiliza como dinero, no cuenta con el reconocimiento de la mayoría de los Estados², consecuencia de ello, no se le da tratamiento de dinero.

En tercer lugar, exploraremos la teoría evolutiva del dinero. Esta teoría es de vital importancia, pues nos permite entender cómo determinado bien que tiene ciertas cualidades se convierte en un medio universal de intercambio y, con ello, en dinero. En este punto, también revisaremos las funciones del dinero que se derivan de su principal función: ser un medio de intercambio. Esto, con la intención de establecer si el Bitcoin, a la luz de la teoría evolutiva del dinero, puede o no ser considerado como tal así el Estado se niegue a reconocerlo.

desconoció el derecho a la vida y libertad de millones de personas. Este régimen socialista, utilizando las normas del ordenamiento jurídico, se habilitó y exterminó a través de genocidio, asesinato de rehenes, trabajo forzado, inanición, experimentos médicos, campos de concentración, entre otros; a una cantidad que oscila entre los 15.000.000 y 31.600.000 de personas; dentro de las víctimas se encuentran judíos, polacos, ucranianos y homosexuales (Rummel, 2017).

² Hasta la fecha, el único gobierno que ha reconocido, a través de su ordenamiento jurídico, al Bitcoin como dinero es El Salvador.

También se hace necesario estudiar el marco regulatorio del dinero en Colombia, para entender qué se considera como dinero en el territorio nacional. En este punto, se estudiarán conceptos claves como intervención y monopolio.

Por último, pasaremos a revisar el marco regulatorio de las criptomonedas como el Bitcoin en Colombia. Para ello, habrá que estudiar qué han dicho las instituciones colombianas encargadas de la política monetaria, bancaria, de valores, entre otras, tales como el Banco de la República, la Superintendencia Financiera, la Dirección de Impuestos y Aduanas Nacionales (DIAN) y la Superintendencia de Sociedades.

Abarcado el estudio de los temas mencionados anteriormente, procederemos a dar nuestras conclusiones sobre el tema y establecer si, en esa situación, nos encontramos ante una realidad que el Estado busca desconocer por alguna causa.

2. Objetivos de investigación

2.1. Objetivo general

2.1.1. Analizar cuál es la naturaleza jurídica otorgada a las criptomonedas en Colombia para determinar si aquello es consecuente con el origen, características y definición de las mismas.

2.2. Objetivos específicos

2.2.1. Analizar el concepto de las criptomonedas, su funcionamiento y características.

2.2.2. Investigar si, de acuerdo a la teoría evolutiva del dinero, las criptomonedas son o no son dinero.

2.2.3. Analizar la naturaleza jurídica de las criptomonedas a la luz del ordenamiento jurídico colombiano.

3. Desarrollo de los objetivos

3.1. Criptomonedas

3.1.1. La tecnología detrás de las criptomonedas: la cadena de bloques (*Blockchain*)

Para entender cómo surgió la cadena de bloques (*Blockchain*), resulta interesante comprender qué sucedía en el mundo antes de su creación. En 2008 se dio la crisis financiera y económica más fuerte de la historia³ desde la Gran Depresión de 1929, dicha crisis generó que el mercado hipotecario de Estados Unidos colapsara y, a su vez, provocó que las grandes instituciones financieras, como los bancos de inversión, se declararan en bancarrota (Zurita, Martínez y Rodríguez, 2009). Lo anterior, junto con las demás crisis financieras ocurridas a lo largo de los años, generó en las personas una gran desconfianza hacia el Estado como intermediario en el proceso de intercambio de bienes y servicios en el mercado (Castellanos, 2018).

Durante décadas se intentó crear un sistema que permitiera realizar transacciones de forma digital sin intermediarios en el proceso, es decir, sin la intervención de una entidad

³ La crisis financiera más fuerte de la historia estalló cuando en el año 2008 el banco de inversión de Lehman Brothers se declaró en bancarrota. Esta crisis financiera tuvo su origen en la intervención estatal (Zurita et al., 2009). Todo comenzó cuando el entonces presidente de EE.UU, George W. Bush, decidió poner en práctica la ley estatal The Community Reinvestment Act (CRA), promulgada por el socialista de Jimmy Carter, con la cual se fomentaba, entre otras cosas, el crédito a personas sin historial crediticio y sin capacidad de pago, esto conllevó a que la Reserva Federal redujera rápidamente y en gran proporción las tasas de interés inundando el mercado de liquidez lo que a su vez generó que los bancos y agentes hipotecarios iniciaran una agresiva expansión del crédito hipotecario a personas con poca capacidad de pago, estas hipotecas fueron denominadas como “hipotecas *subprime*”, la crisis se perpetuó cuando empezaron a caer los precios de los bienes raíces y los deudores empezaron a incumplir con los pagos de sus hipotecas (Zurita et al., 2009).

centralizada como el Estado que validara las operaciones en el mercado. Estos intentos no tuvieron éxito durante muchos años debido a la dificultad de encontrar una solución al denominado “problema del doble gasto” toda vez que la comunicación digital no permitía que un archivo que había sido enviado a otro computador desapareciera del computador del remitente para instalarse en el computador del destinatario, lo que ocurría era que se generaba una copia de este, permitiendo que una misma unidad de archivo fuera usada varias veces (Castellanos, 2018)⁴.

Lo anterior es un problema porque el dinero es un medio y, al ser un medio, es escaso. Esta condición implica que el dinero es exclusivo para lograr un fin o un número de fines limitados, como consecuencia, se genera la exclusión, es decir, en el momento en que se elige a qué curso de acción se va a asignar el dinero, se excluyen otros a los que también se pudo haber asignado. En otras palabras, el dinero como medio de intercambio debe abandonar la cuenta de la que sale y reflejarse en la de la persona que lo recibe, dado que no puede existir en dos o más lugares a la vez porque al ser un medio no puede asignarse a dos o más cursos de acción al mismo tiempo, además, se daría el riesgo de gastar una unidad de moneda digital en dos lugares de tal forma que uno de ellos rebotaría como lo haría un cheque sin fondos (Tapscott y Tapscott, 2016).

⁴ Esta situación se puede explicar con el siguiente ejemplo: Juan enviaba una unidad de un archivo a María como contraprestación por un servicio prestado, el problema es que cuando Juan enviaba ese archivo a María, este no salía de su cuenta como lo haría si pagara con billetes, por el contrario, se creaba una copia de esa unidad de archivo, entonces Juan seguía teniendo en su poder esa misma unidad de archivo al igual que María, lo que significaba que Juan podía seguir usando la misma unidad de archivo para gastarla en más cosas.

Es así, como en el año 2008, se hizo público un documento titulado *Bitcoin: a Peer-to-Peer Electronic Cash System* de autoría de Satoshi Nakamoto, en el cual se anunciaba la creación de un registro cronológico respaldado por algoritmos criptográficos⁵ (lo que más adelante llamaremos *hash*) y por una cadena de bloques de todas las transacciones, que permite que las partes puedan realizar un pago en línea de forma directa (totalmente *peer-to-peer* o par a par) sin la necesidad de acudir a una institución financiera centralizada que valide las mismas y realice el registro de abonos y deducciones en las cuentas de cada persona (Gómez et al., 2017). En otras palabras, brindó una solución al problema del doble gasto que generaba consigo el riesgo de fraude en el mercado y que surgía al no haber un intermediario financiero centralizado que validara las transacciones (Rincón, 2018).

Este nuevo sistema fue denominado como Cadena de Bloques (*Blockchain*) mediante el cual, en breves palabras, se ordenan las transacciones en grupos que son llamados *bloques*⁶ los cuales se van uniendo secuencialmente a otros *bloques* conforme se van agregando nuevas transacciones, creando consigo una cadena de bloques que se encuentra disponible en línea y

⁵ La criptografía es definida por la RAE como el arte de escribir con clave secreta o de un modo enigmático. La criptografía se utiliza en la actualidad para dar garantías de seguridad a la información. Es la responsable de proteger nuestros datos en las comunicaciones para que solamente la persona receptora de ese mensaje pueda leerlo y ninguna otra pueda acceder a esa información si no es la destinataria legítima (Llorente, 2019).

⁶ Las transacciones que se encuentren en el mismo bloque se entenderán que fueron llevadas a cabo al mismo tiempo y, las transacciones que no se encuentren en ningún bloque se entenderá que están pendientes (Gem Coin Bank, 2015).

puede ser validada por cualquier participante del sistema mediante las billeteras electrónicas⁷ a las que se puede acceder desde cualquier dispositivo con acceso a internet (Rincón, 2018).

En este sistema, el control de los procesos no recae en manos de un Estado o de una autoridad centralizada, es decir, es un sistema completamente descentralizado dado que, la validación y el registro de las transacciones que van conformando la cadena de bloques, recae en todos los ordenadores que se encuentran conectados a la red, estos últimos son conocidos como *nodos* quienes compiten por resolver algoritmos o pruebas matemáticas de alta complejidad a fin de realizar lo anteriormente mencionado (validación, verificación y registro de transacciones) a cambio de incentivos (Coindesk, 2018).

Estos incentivos serán nuevas unidades de criptomonedas y las comisiones que pagan los participantes del sistema para que su transacción sea agregada al bloque (Arango et. al., 2018). Aquellos participantes que logran resolver estos algoritmos de alta complejidad invirtiendo su tiempo, conocimiento, recursos eléctricos y computacionales son conocidos como *mineros*, este proceso computacional que realizan es conocido como “prueba de trabajo” (en inglés *Proof of Work*). Este proceso lo podemos comparar con la minería de oro, dado que los mineros invierten recursos, esfuerzo, conocimiento y tiempo para encontrar este bien en cualquier lugar del planeta y así poder ponerlo en circulación a cambio de un incentivo (Nakamoto, 2008).

Gracias a este sistema de la cadena de bloques, la información de las operaciones y transacciones realizadas “no está guardada en un archivo central, está representada por

⁷ Las billeteras electrónicas, también llamadas e-wallets, son uno de los nuevos medios de pago de los últimos años. Este medio de pago se maneja desde una aplicación que descarga el usuario en su dispositivo, ya sea celular, tablet o computador, que le permite administrar su dinero de forma virtual y realizar pagos de forma sencilla en cualquier momento (MyChoise2pay, s.f.).

transacciones registradas en una hoja de cálculo global o libro mayor, que aprovecha los recursos de una gran red *peer-to-peer* para verificar y aprobar transacciones” (Corredor, 2018, p. 67). Es decir que este llamado libro mayor⁸ está controlado por miles de *nodos*, lo que hace que la tarea de validar y agregar datos al sistema se descentralice y lo que impide que alguna entidad centralizada pueda tomar el control del mismo; generando consigo una reducción significativa de costos, errores humanos, corrupción y manipulación de los datos (Ittrends, 2017).

Por otro lado, en la cadena de bloques las transacciones son ordenadas cronológicamente y les es asignado un código alfanumérico o algoritmo criptográfico conocido como *hash*⁹ que corresponde al bloque que los precede, “gracias a ese *hash* todos están referenciados por el bloque que los creó, por lo que solo los bloques que contienen un código válido son introducidos en la cadena y replicados a todos los nodos” (Navarro, 2017, p. 7). Para ello, es necesario que todos los nodos que se encuentran en la red estén sincronizados, es decir, contengan almacenada

⁸ Este denominado “libro mayor” se asemeja al libro de registros de contabilidad de una empresa en donde se registran todas las entradas y salidas de dinero, solo que en este caso hace referencia a un libro de acontecimientos digitales que no requiere de un intermediario centralizado que identifique y certifique la información (Gómez et al., 2017).

⁹ El nombre de *hash* se usa para identificar una función criptográfica muy importante en el mundo informático. Estas funciones tienen como objetivo primordial codificar datos para formar una cadena de caracteres o identificadores únicos e irrepetibles a partir de una información dada. Todo ello sin importar la cantidad de datos introducidos inicialmente en la función. Estas funciones sirven para asegurar la autenticidad de datos, almacenar de forma segura contraseñas y la firma de documentos electrónicos. Las funciones *hash* son ampliamente utilizadas en la tecnología *blockchain* con el fin de agregar seguridad a las mismas. El Bitcoin, es un claro ejemplo de cómo estos códigos alfanuméricos pueden usarse para hacer posible la tecnología de las criptomonedas (Bit2meacademy, 2021)

la cadena de bloques que está actualizada y contengan el mismo historial de registro (Castellanos, 2018).

Lo anterior permite que la cadena de bloques sea bastante segura, porque, por un lado, el llevar un registro cronológico de todas las operaciones o transacciones permite saber cuándo y en qué secuencia han tenido lugar las mismas y; por otro lado, todas las transacciones y movimientos estarán identificadas con un código único e irrepetible (un *hash*). Esto da lugar a que se pueda lidiar con el problema del doble gasto mencionado anteriormente puesto que se impide que un participante del sistema vuelva a disponer de recursos que ya ha gastado en el pasado (Gómez et al., 2017).

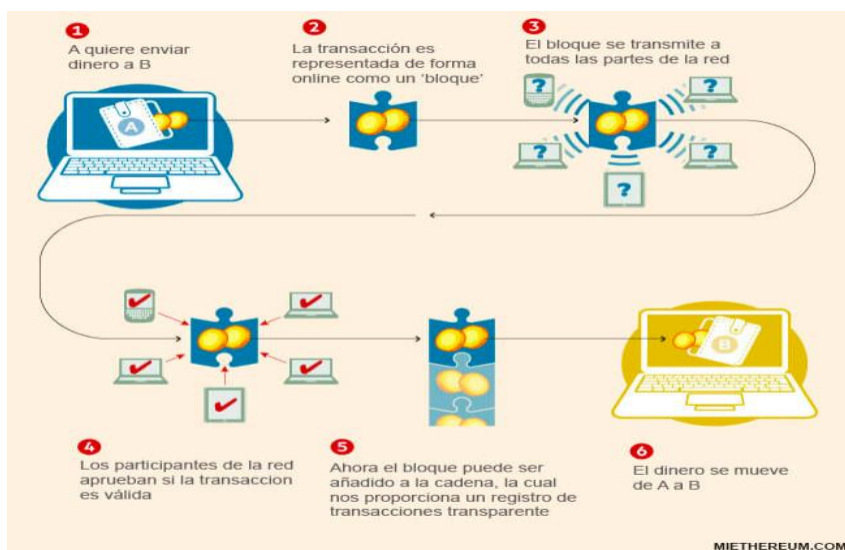
La cadena de bloques es también una tecnología distribuida y de consenso. Es distribuida porque la información es pública para todos los nodos o participantes del sistema dado que los mismos se encuentran conectados entre sí de manera directa (*peer-to-peer*) por ende, la validación de la cadena de bloques no recae en una autoridad central sino en todos los participantes de la red (Arango et al., 2018). Para lo anterior, cada uno de los participantes del sistema debe contar con una copia idéntica de la cadena de bloques, lo que elimina a su vez el riesgo de falsificación que puede devenir de un sistema centralizado (Amores, 2020). Por otro lado, es de consenso porque “permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos” (Preukschat, 2017, p. 7). En otras palabras, se requiere que todos los participantes del sistema aprueben y validen unánimemente las transacciones u operaciones que se encuentran distribuidas en el sistema para poder que estas sean agregadas a la cadena de bloques sin la necesidad de una entidad centralizada que se encargue de supervisar o validar los procesos que se llevan a cabo (Gómez et al., 2017).

A pesar de ello, podría suceder que uno de los participantes del sistema logre obtener el 51% del control de la cadena de bloques y obtenga la posibilidad de modificar o editar la información, sin embargo, es muy poco probable que esto suceda ya que existe un gran obstáculo económico, se requeriría la inversión de una gran cantidad de recursos que incluso podría superar los beneficios que recibiría quien pretenda corromperlos (Castellanos, 2018).

Ahora bien, un ejemplo práctico del proceso ya descrito es el siguiente: Andrés desea enviar a Andrea cierta cantidad de unidades de valor (Bitcoins, pesos, dólares, etc.), para esto, mediante la billetera electrónica que use lo que hace es crear y firmar digitalmente una transacción a nombre de la identidad digital de Andrea, esta información es enviada a todos los nodos de la red en donde queda guardada y en la lista de pendientes, posterior a ello, los llamados *mineros*, mediante su poder de cómputo (Prueba de Trabajo), resuelven los algoritmos o problemas matemáticos con los que se encargan de procesar y validar las transacciones de terceros y crear el nuevo bloque, aquel ganador agrega el bloque a la cadena de bloques más larga y los demás nodos usan el *hash* de este último como punto de partida del siguiente bloque, una vez sucede esto, las unidades de valor que envió Andrés pasan a la cuenta de Andrea y salen de la suya. A continuación, se adjunta una imagen explicativa del proceso mencionado:

Figura 1

Cómo funciona Blockchain (cadena de bloques) para realizar pagos



Fuente: (Mietherium, s.f.). Página web: <https://www.mietherium.com/blockchain/>

De esta forma la cadena de bloques es definida como:

Una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. Otro elemento muy importante a tener en cuenta en ella es que, por definición, se trata de un sistema que permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos. (Preukschat, 2017, p. 7)

Así mismo, se puede afirmar que la cadena de bloques es una estructura que sirve para almacenar datos de manera que sea casi imposible de falsificar (lo que podría suceder si existiera un ente centralizado que vigilara tal proceso) porque la información que este sistema recoge no puede modificarse, editarse o eliminarse gracias a la criptografía que la respalda (Ittrends, 2017).

Aquello permite que se pueda llevar “la historia transaccional completa del archivo digital entre cuentas de distintos participantes sin la necesidad de que sea intermediada por una contraparte centralizada” (Arango et. al., 2018, p. 5).

Por lo anterior, este sistema de la cadena de bloques es utilizado para realizar las transacciones en criptomonedas¹⁰ por las especiales características que este tiene, esto es, i) es completamente descentralizada, ii) es una tecnología distribuida y de consenso, iii) es un sistema bastante seguro y confiable y iv) elimina el riesgo del doble pago. Satoshi Nakamoto, el creador de la primera criptomoneda llamada Bitcoin, “combinó herramientas de cifrado establecidas como métodos de computación que permitieran que una red pública de participantes que no necesariamente confían entre sí acuerden, una y otra vez, que un libro contable compartido refleja la verdad” (Ittrends, 2017, p. 3).

3.1.2. Bitcoin: la primera criptomoneda

3.1.2.1. Surgimiento del Bitcoin

El 1 de noviembre de 2008, cuando Satoshi Nakamoto “envió un correo electrónico a una lista de correo de criptografía para anunciar que había estado trabajando en un nuevo sistema de dinero electrónico que utiliza por completo una red *peer-to-peer*, sin un tercero de confianza” (Ammous, 2018, p. 15), se inicia una gran revolución del dinero (entendido como medio de

¹⁰ A pesar de que las características varíen dependiendo de la criptomoneda de la que se hable, todas coinciden en que su emisión e intercambio se produce a través del sistema de *Blockchain* (cadena de bloques) (Tapscott y Tapscott, 2016).

intercambio)¹¹. Actualmente existen muchas y diferentes criptomonedas tales como el Bitcoin, Ether, Litecoin, Tether, Cardano, Binance Coin, Dogecoin, etc. Sin embargo, a lo largo de este trabajo nos vamos a referir al Bitcoin, la criptomoneda más popular hoy en día pues fue la primera en entrar al mercado y es actualmente la más usada como medio de intercambio por inversionistas, comerciantes e instituciones financieras, además, su crecimiento ha sido bastante acelerado en aproximadamente 12 años que han transcurrido desde su creación (Palacios et al., 2015).

Durante los primeros meses de la creación del Bitcoin, el mismo era usado, por decirlo de alguna forma, como un simple juego digital. Los pocos participantes que se unieron a la red en un principio, que se puede decir eran expertos en criptografía, se dedicaban a resolver los algoritmos matemáticos para crear nuevos Bitcoins, pues no había muchos en circulación sino en la medida en que los iban minando. Estos participantes solo usaban los Bitcoins, que iban obteniendo fruto de su esfuerzo, como un tipo de medalla o premio, fue así, como los mismos empezaron a adquirir el estatus de artículos de colección, pero en formato digital, más no se les daba todavía el estatus de dinero o de medio universal de intercambio pues los mismos no eran usados para hacer intercambios de forma indirecta en el mercado (Ammous, 2018).

Sin embargo, en octubre de 2009, se registró la primera compra de un Bitcoin con dinero, “una casa de cambio en internet vendió 5.050 Bitcoins por 5,02 dólares (a un precio de 1 dólar por cada 1.006 Bitcoins)” (Ammous, 2018, p. 16), el precio, en aquel momento, fue determinado

¹¹ En la actualidad, la emisión de dinero (moneda fiat) es un monopolio estatal en cabeza de los bancos centrales (Rallo, 2017). En el caso colombiano, el Banco de la República es el encargado, entre otras funciones, de la emisión del peso colombiano y la manipulación de la tasa de interés (Binance academy, 2020).

por el costo de la electricidad que se requería para producir un Bitcoin. Este hecho fue considerado como el más trascendental y significativo en la trayectoria del Bitcoin pues pasó de ser solo un artículo coleccionable a ser un bien comercializable y con un precio, esto es, la red había operado con tanto éxito que alguien estuvo dispuesto a renunciar a dinero de curso legal para adquirir varios Bitcoins (Ammous, 2018).

Posterior a ello, el 22 de mayo de 2010, ocurrió otro suceso trascendental en la historia del Bitcoin cuando una persona compró, con 10.000 Bitcoins, dos pizzas que costaban 25 dólares, aquello constituyó la primera vez que se usaban los Bitcoins como medio de intercambio en el mercado. En poco menos de 10 meses el Bitcoin dejó de ser solo un bien de consumo para empezar a convertirse en un medio universal de intercambio, lo cual es importante porque alguien estuvo dispuesto a entregar Bitcoins a cambio de pizzas y, así mismo, alguien estuvo dispuesto a aceptar aquellos como una forma de pago por las pizzas entregadas, es decir, se realizó el primer intercambio indirecto con esta criptomoneda (Ammous, 2018).

Gracias a esta serie de acontecimientos, ha ido aumentando el número de participantes en la red y con ello las transacciones en Bitcoin lo que ha permitido que su precio y su valor aumenten significativamente, tanto así que hoy, un solo Bitcoin, cuesta más de 30.000 USD.

3.1.2.2. Aspectos relevantes del Bitcoin y su funcionamiento

3.1.2.2.1. Los sistemas que soportan las transacciones en Bitcoin son descentralizados. Como ya se mencionó, el control no recae en una autoridad central que se responsabiliza de la emisión de la criptomoneda y del registro de sus movimientos. El mantenimiento y registro de todas las operaciones se hace de forma abierta y se distribuye entre

los participantes del sistema¹², es decir, son los mismos nodos, que no necesariamente se conocen o confían unos en otros, quienes se encargan de validar las transacciones y, los mineros, quienes, por medio de la solución de algoritmos matemáticos complejos, crean nuevos Bitcoins que aumentan la oferta (Boar, 2018)¹³.

3.1.2.2.2. La principal característica funcional de Bitcoin es la verificación.

Gracias a que Bitcoin puede funcionar “sin la necesidad de sistemas centralizados de emisión, registro, compensación y liquidación” (Arango et al., 2018, p. 1) en donde solo queda confiar en el tercero que lo controla, las transferencias de información de esta criptomoneda se realizan mediante un registro público, el cual es compartido y sincronizado con los demás participantes del esquema a fin de que todos puedan verificar que la información es correcta y certera. Tal como lo menciona Ammous (2018):

¹² Estos sistemas pueden ser abiertos o cerrados en el sentido que la criptomoneda puede ser convertible o no por dinero de curso legal, sin embargo, la mayoría de las plataformas actualmente son abiertas y descentralizadas (Arango et al., 2018).

¹³ También existen sistemas centralizados, aunque son más pocos, que respaldan transacciones en criptomonedas, en donde el control recae en una autoridad que emite la criptomoneda y tiene la libertad de definir los protocolos de registro, validación de saldos en cuenta y transacciones, por ejemplo, la criptomoneda Ripple (XRP) fue creada por la empresa Ripple Labs como una solución dirigida a permitir que bancos y entidades financieras de todo tipo pudieran usar la tecnología de la cadena de bloques para mejorar sus procesos de pago transfronterizos, en este caso, Ripple Labs es quien elige los protocolos que deben seguir los validadores (*nodos*) que en su mayoría son propiedad de los mismos bancos que hacen uso del sistema y de la empresa de Ripple Labs, puede además, congelar activos y manipular la emisión de la misma a su entera discreción, es decir, no se puede *minar* como sucedería con Bitcoin y se puede decir que es una criptomoneda con la misma capacidad de manipulación que el dinero fiat (Bit2meacademy, 2021).

Nakamoto eliminó la necesidad de confiar en un tercero al crear Bitcoin sobre la base de una prueba de verificación muy rigurosa e invulnerable. Se puede decir que la principal característica funcional de Bitcoin es la verificación, y sólo por eso puede eliminar por completo la necesidad de un tercero de confianza. (p. 230)

Lo anterior es posible gracias a la tecnología de la cadena de bloques que, como lo hemos mencionado, es la que permite que se lleve una historia transaccional pública de todas las operaciones en criptomonedas, transacciones que son validadas por medio del consenso de todos los nodos y no de una entidad centralizada como lo es el Estado (Barroilhet, 2019).

3.1.2.2.3. La oferta de Bitcoin es limitada y no se puede alterar. La producción de los Bitcoins está creada bajo una política de emisión controlada. Sólo pueden existir 21 millones de unidades¹⁴. Así pues, la producción de Bitcoins está atada a la «prueba de trabajo» que realizan los mineros y que mantiene la misma red de pagos (Barroilhet, 2019). Esta última está gobernada, como ya se ha mencionado, por desafíos matemáticos de validación de alta complejidad que están abiertos a los participantes que deseen resolverlos quienes compiten por algún incentivo del sistema. Lo anterior significa que, entre más algoritmos sean resueltos por los mineros habrá más Bitcoins en circulación y, por ende, la oferta aumentará. Por el contrario, mientras los mineros no logren resolver estos algoritmos matemáticos no habrá más ni menos Bitcoins hasta que dichos algoritmos sean resueltos (Coindesk, 2018).

¹⁴ Actualmente se han minado más de 18 millones de Bitcoins que se encuentran en circulación, esto significa que falta por minar aproximadamente un poco más de 2 millones para que la totalidad se encuentre en circulación (Blockchain, 2021).

Para que fuese posible que el sistema de la oferta de Bitcoin fuera prácticamente inmodificable, Nakamoto programó para que se produjera un nuevo bloque cada 10 minutos aproximadamente y para que cada bloque generara una recompensa de 50 Bitcoins en los primeros 4 años de su operación, para posteriormente, reducirlo a 25 Bitcoins y a la mitad cada 4 años (Ammous, 2018).

Así, cada que más personas adquieren Bitcoins, el valor de este aumenta lo que genera que el proceso de minar se vuelva más rentable y, a su vez, conlleva a que más nodos entren a competir por la solución de la prueba de trabajo para obtener la recompensa. Esto último implica el uso de muchos más recursos computacionales y capacidad de procesamiento que se podría ver traducido en llegar a las soluciones de los algoritmos matemáticos mucho más rápido, aumentando la tasa de emisión de nuevas unidades. Sin embargo, gracias al ajuste de dificultad con el cual se programó el sistema, cada que aumenta la capacidad de procesamiento, se incrementa la dificultad de los algoritmos matemáticos que se deben resolver para generar la recompensa lo que hace más costoso todo el proceso, por lo tanto, esta tecnología garantiza que la creación de los bloques continúe demorándose cerca de 10 minutos aproximadamente y por ende, se puede afirmar que la cantidad de Bitcoins “no puede alterarse por mucho esfuerzo y energía que se emplee en la prueba de trabajo” (Ammous, 2018, p. 231)¹⁵.

Precisamente aquello es lo que hace que el Bitcoin sea tan innovador. No es tanto el hecho de que sea más portable, divisible, imperecedero y prácticamente infalsificable, sino el

¹⁵ “De acuerdo con esta programación, la oferta continuará aumentando a un ritmo menor, acercándose de forma asintótica a los 21 millones de monedas hacia el año 2140, momento en el que no se emitirán más Bitcoins” (Ammous, 2018, p. 239).

hecho de que pueda funcionar con una escasez predecible en un ambiente como el virtual donde la escasez no es algo natural (Barroleilhet, 2019).

Es por ello, que la actividad de los mineros, la denominada “prueba de trabajo”, determina de forma predecible el crecimiento de la oferta de Bitcoin. No existen otras formas de crear nuevos Bitcoins ya que no hay un banco emisor, su oferta no está supeditada a la voluntad caprichosa de un gobernante y tampoco se pueden incorporar más a la masa comprándose los a otras personas, la única forma es mediante la obtención de incentivos otorgados a los mineros que con su esfuerzo logran resolver aquellos algoritmos para crear el respectivo bloque (Coindesk, 2018). Por ende, se puede decir que Bitcoin “es el primer ejemplo de un bien digital que es escaso y no puede reproducirse de forma indefinida” (Ammous, 2018, p. 237).

3.1.2.2.4. Bitcoin es divisible. Cada unidad de Bitcoin es divisible en 100 millones de satoshis, que es la fracción más pequeña en la que se puede dividir un Bitcoin. En este sentido, 1 Bitcoin es igual a 100 millones de satoshis y 1 satoshi es igual a 0,00000001 Bitcoins. Lo anterior hace que el Bitcoin tenga una gran flexibilidad de pago y sea altamente vendible a cualquier escala y en cualquier lugar del mundo, tal como lo afirma Ammous (2018):

Su naturaleza digital, que facilita el envío seguro por todo el mundo, lo hace vendible en el espacio de una forma jamás vista respecto a otras formas de dinero, mientras que su divisibilidad en 100 millones de satoshis hace que sea vendible en escala. (p. 242)

Además, Bitcoin, a diferencia del dinero fiat¹⁶, ha ido ganando con el tiempo poder adquisitivo pese a su aumento moderado de la oferta, que como ya se mencionó, es limitada y no

¹⁶ El dinero fiat, en pocas palabras, es dinero de curso legal cuyo valor no deriva del hecho de ser un bien físico o mercancía, sino del hecho de ser emitido y respaldado por un gobierno (Binance academy, 2020).

se puede manipular por nadie para beneficio propio, ni siquiera por una autoridad gubernamental. Mientras que, la emisión del dinero fiat o de curso legal puede ser manipulada en cualquier momento por el Estado, dado que es quien detenta el monopolio del mismo. Por lo anterior, puede el Estado, de forma arbitraria y como un mecanismo de expropiación, aumentar la oferta del dinero sobre el cual detenta el poder para su beneficio propio haciendo que, el poder adquisitivo de ese dinero disminuya¹⁷.

3.1.2.2.5. Bitcoin es fácilmente portable. En este punto se hace necesario mencionar que, para que una persona pueda enviar, recibir, almacenar y monitorear sus Bitcoins debe contar con una billetera electrónica. Existen billeteras electrónicas que cuentan con diferentes características dependiendo el propósito que se tiene, por ejemplo, si la persona desea almacenar una gran cantidad de Bitcoins de forma segura se recomienda usar un tipo de billetera totalmente diferente a la que usaría si deseara almacenar una pequeña cantidad de Bitcoins para hacer transacciones en montos pequeños. Ahora bien, las billeteras electrónicas pueden ser en almacenamiento en frío y en almacenamiento en caliente (Criptoeconomía, 2020).

Las billeteras electrónicas en almacenamiento en frío no requieren acceso a internet, por ello, son casi imposibles de hackear y son más seguras, pues la clave privada¹⁸ está almacenada

¹⁷ Al respecto, Rothbard (1990) afirmó que “La inflación es un método por el cual el gobierno, su sistema bancario controlado y los grupos políticos favorecidos pueden expropiar parcialmente la riqueza de otros sectores de la sociedad. Quienes están facultados para controlar la oferta monetaria emiten nuevo dinero para su propio beneficio, a expensas del resto de la población. Si se otorga al gobierno el monopolio de la emisión y de la oferta monetaria, inflará la oferta para su propio beneficio, en detrimento de quienes carecen de poder político”. (p. 13)

¹⁸ “Una clave privada es simplemente una cadena muy larga de números y letras que actúa como la contraseña de tu monedero Bitcoin. Es a partir de este número que tu monedero obtiene su poder para enviar tus

en monederos de hardware que son dispositivos físicos, similares a una USB, por lo que, si se desea interactuar con los Bitcoins se deberá conectar a algún ordenador que tenga un software que permita el control sobre el monedero hardware. En este caso, el monedero hardware es fácil de portar, pues no es un dispositivo grande y siempre mantiene su tamaño a pesar de la cantidad de Bitcoins que la persona posea, así mismo, el ordenador al cual se conecta puede ser un celular, un portátil, etc. que no necesariamente debe ser el personal, pues se puede conectar a cualquier ordenador que cuente con las características adecuadas para conectar el monedero hardware (Criptoeconomía, 2020).

Por otro lado, si se cuenta con alguna billetera electrónica caliente (en inglés *hot wallet*) se requiere tener una conexión a internet, estas billeteras pueden ser descargadas en cualquier dispositivo como celulares, portátiles, tabletas, etc. por esta razón son más susceptibles de ser hackeadas (Criptoeconomía, 2020). Este tipo de billeteras electrónicas se pueden portar con una facilidad casi que inigualable por el dinero fiat o dinero en efectivo toda vez que existen en cualquier parte del mundo y cualquier persona con un dispositivo móvil con acceso a internet y conocimiento suficiente puede acceder al registro digital de Bitcoin y hacer sus transacciones (siempre que cuente con su clave privada) (Ammous, 2018).

3.1.2.2.6. Bitcoin depende de incentivos económicos. Esto significa que el costo de realizar una transacción en Bitcoins depende de la comisión –o *fee*- de minería que se pague, el

Bitcoins a otras personas” (Criptoeconomía, 2020, párr. 9). Sin esta clave privada la persona no podrá acceder a los Bitcoins que se tienen. Por ejemplo, si una persona apunta la clave privada en algún lugar y pierde el dispositivo móvil donde tenía la billetera electrónica podrá luego desde otro dispositivo recuperar el control de los Bitcoins, pero si esta clave se pierde será imposible volverla a la recuperar, por ende, se perderá el control de los Bitcoins (Criptoeconomía, 2020).

cual es un pago que incentiva a los mineros para que realicen su trabajo y con el que se garantiza la eficiencia y seguridad de la red, ahora, “la comisión no es algo fijo, ni impuesto explícitamente, es el usuario quien determina cuánto está dispuesto a pagar en función de su necesidad” (Bit2meacademy, 2021, p. 1)¹⁹.

Es decir, si la necesidad de una persona en realizar una transacción es muy alta y urgente lo que puede hacer esta persona es pagar una comisión más alta para que la misma tenga mayor prioridad, dado que esto incentiva a los mineros para que tomen la transacción y la confirmen más rápido que las demás, mientras que, si se paga una comisión baja, lo que pasará es que la transacción no se tendrá como prioritaria y el tiempo de confirmación estará supeditada a la demanda de transacciones que se realicen, cuando esta demanda es alta, la red tiende a sobrecargarse lo que hace que la confirmación de las transacciones se retrase (Bit2meacademy, 2021). Además de este incentivo, actualmente los mineros que incluyen un bloque válido de transacciones al sistema son recompensados con nuevos Bitcoins que, como ya lo mencionamos, son añadidos a la oferta monetaria (Ammous, 2018)²⁰.

Para Nakamoto, estos incentivos son importantes, pues sin ellos se impediría el funcionamiento de una red pública de cadena de bloques descentralizada, porque ninguno de los *nodos* estaría dispuesto a invertir grandes recursos para mantener actualizado el registro de las

¹⁹ La lógica *peer-to-peer* permite la realización de transacciones inmediatas entre el vendedor y el comprador sin la necesidad de un intermediario que pueda cobrar una comisión obligatoria (Christidis y Devetsikiotis, 2016).

²⁰ Se dice que una vez se encuentren todos los Bitcoins en circulación, este incentivo desaparecerá, por lo tanto, los mineros encargados de registrar las transacciones en el libro mayor tendrán como único incentivo el costo de transacción pagado por aquellos participantes de la red que desean realizar una transacción (Ammous, 2018).

transacciones y para agregar nuevos bloques a la cadena de bloques de forma gratis y sin retribución alguna (Castellanos, 2018).

Sin embargo, aunque lo anterior se constituya como un incentivo para el minero, se puede convertir en un desincentivo para aquella persona que desee usar sus Bitcoins como medio de intercambio en el mercado, toda vez que, para que su transacción sea aprobada rápidamente tendrá que pagar una comisión que puede superar el beneficio esperado. Utilizar Bitcoin para realizar pagos de bienes de consumo masivos puede acarrear altos costos transaccionales lo que se convertiría en un desincentivo para la persona usar esta criptomoneda como medio de intercambio (Ammous, 2018).

3.1.3.2.7. Bitcoin puede operar con relativa seguridad. La criptografía, como ya lo hemos mencionado, es la que permite que haya transparencia en todo el proceso, por ejemplo, con Bitcoin es muy poco probable que una persona se pueda hacer pasar por otra como sucede con las tarjetas de crédito, es posible realizar un pago bajo el anonimato y cuenta con registros contables que son actualizados constantemente por miles de computadores encargados de verificar que no existan usos duplicados (Bitcoin, s.f.). El hecho de que Bitcoin sea relativamente seguro reside en “la asimetría existente entre el coste de resolver la prueba de trabajo necesaria para realizar la transacción al registro y el coste de comprobar su validez” (Ammous, 2018, p. 233), es decir, cada vez es más costoso, en términos de recursos eléctricos y computacionales, registrar transacciones y resolver la prueba de trabajo; por el contrario, el costo de validar aquellas operaciones se aproxima a cero, por lo tanto, intentar realizar transacciones fraudulentas en el libro mayor de Bitcoin requeriría usar demasiados recursos en resolver la prueba de trabajo para que al final los nodos rechacen la misma en el proceso de validación a un costo demasiado bajo.

A pesar de lo anterior, los expertos en criptografía e informática han logrado descubrir diversas formas con las que se puede desafiar el sistema. Una de estas formas es el denominado “ataque del 51 por ciento”, este se da cuando uno o varios participantes del sistema compran suficientes equipos de minería para así controlar más del 50% de la tasa de hash²¹ de una cadena de bloques. Así, uno o varios participantes que controlen la mayoría de la tasa de hash podrían generar transacciones fraudulentas gastando dos veces la misma moneda, cancelando una de las dos transacciones y defraudando al receptor (Coindesk, 2021).

Otra forma de defraudar el sistema es mediante el uso de softwares maliciosos o *malware*. Con estos, los hackers podrán invadir, dañar o deshabilitar ordenadores, dispositivos móviles, celulares, etc. logrando tener el control parcial del dispositivo y de todas las operaciones realizadas a través de él (Malwarebytes, 2021). Igualmente, podrán hacerlo mediante la instalación de alguna tecnología espía en los ordenadores de cualquier participante del sistema, logrando así obtener las claves privadas de cada usuario y con ello el control de sus Bitcoins (Ammous, 2018).

Mediante la técnica “*phishing*” también se puede defraudar el sistema. Con esta se engaña a las personas para que compartan información confidencial como contraseñas y usuarios. Los hackers, haciéndose pasar por la plataforma de confianza en donde se almacenan las criptomonedas, envían mensajes de texto o correos electrónicos a sus víctimas con el fin de infundirles miedo, el mensaje puede exigir que la víctima acuda a un sitio web y actúe de

²¹ La tasa de hash o “*hash rate*” es “el poder computacional total combinado que se utiliza para minar transacciones en una blockchain que funcione con un sistema de prueba de trabajo. Cuantas más máquinas dediquen los mineros honestos a descubrir el siguiente bloque, mayor será el hash rate y más difícil será para los agentes maliciosos perturbar la red” (Coindesk, 2021, p. 3).

inmediato porque de lo contrario tendrá que afrontar alguna consecuencia negativa. A menudo estos sitios web son una imitación de la página legítima de la plataforma en donde le solicitan información como usuario y clave privada, las personas al llenar aquella información le permiten al hacker acceder a ella y utilizarla para fines fraudulentos (Malwarebytes, 2021).

Es así como a lo largo de los años, varios participantes del sistema han sido víctimas de ataques o hackeos a sus cuentas. Por ejemplo, en el año 2019, unos hackers lograron robar cerca de siete mil Bitcoins de la plataforma Binance – la mayor plataforma de criptomonedas del mundo en volumen diario – usando técnicas como la de *phishing* y *malware* (“Un nuevo robo millonario golpea al bitcoin”, 2019). Así mismo, recientemente, los hackers realizaron lo que hasta ahora se considera el mayor robo de criptomonedas de la historia a la plataforma Poly Network, logrando robar cerca de 600 millones de dólares en criptomonedas probablemente por un problema criptográfico poco usual según anunció la misma plataforma (Gómez, 2021).

Así como los casos anteriores, se han registrado varios hackeos, en donde muchos participantes del sistema han resultado perjudicados, por ello se puede decir que, aunque Bitcoin opera con una tecnología bastante segura, la misma no está exenta de ser blanco de algún fraude o hackeo a la red. Como tampoco están exentas las entidades financieras que manejan monedas de curso legal. La cuestión es que, la posibilidad de hackeo o fraude no le quita o le otorga a un bien la capacidad de ser un medio universal de intercambio tal como se expondrá más adelante.

3.1.2.3. ¿Qué es Bitcoin?

Nakamoto (2008) define al Bitcoin como un sistema de efectivo electrónico que está basado en pruebas criptográficas y que permite a las partes transar directamente entre sí sin la necesidad de un tercero quien es reemplazado por una red *peer to peer* lo cual lo hace un sistema

descentralizado, que guarda registro cronológico de las transacciones y evita el problema del doble gasto²².

Por su parte, Ralph Merkle (2016) se refiere a dicha criptomoneda en los siguientes términos:

Bitcoin es el primer ejemplo de una nueva forma de vida. Vive y respira en internet. Vive porque puede pagarle a la gente para mantenerlo vivo. Vive porque realiza un servicio por el que le pagará la gente. Vive porque cualquiera, en cualquier lugar, puede ejecutar una copia de su código. Vive porque todas las copias en ejecución están constantemente hablando entre sí. Vive porque si una copia está corrompida se descarta, de forma rápida y sin ningún tipo de problema. Vive porque es radicalmente transparente: cualquiera puede ver su código y ver con precisión lo que hace.

No puede ser cambiado. No se puede discutir. No se puede falsificar. No se puede corromper. No se puede detener. Ni siquiera se puede interrumpir.

Si una guerra nuclear destruyera la mitad de nuestro planeta, continuaría viviendo incorrupto. Continuaría ofreciendo sus servicios. Seguiría pagando a las personas por mantenerlo con vida.

²² Respecto a las criptomonedas en general nos podemos encontrar con diversas definiciones. Arango et al., (2018) las define como unidades digitales susceptibles de ser usadas como medios de pago en el intercambio de bienes y servicios, como depósitos de valor y como unidades de cuenta. Sarmiento y Garcés (2016) afirman que las criptomonedas “son un medio de intercambio digital que, por su diseño y funcionamiento cumplen con las funciones del dinero tradicional permitiendo el intercambio de bienes y servicios”. (p. 153)

La única manera de apagarlo es destruir todos los servidores que lo hospedan. Lo cual es difícil, porque muchos servidores lo alojan en muchos países y mucha gente quiere usarlo.

Siendo realistas, la única forma de aniquilarlo es hacer que el servicio que ofrece sea tan inútil y obsoleto que nadie quiera utilizarlo. Tan obsoleto que nadie quiera pagar por él, que nadie quiera albergarlo. Entonces no tendrá dinero para pagarle a nadie. Entonces morirá de hambre.

Pero, mientras haya personas que quieran usarlo, será muy difícil matarlo, corromperlo, detenerlo o interrumpirlo. (p. 14)

3.2. Teoría del dinero: El origen evolutivo del dinero

Ahora bien, teniendo en cuenta las características del Bitcoin y sus aspectos más relevantes, resulta pertinente dar respuesta al segundo objetivo de este trabajo de investigación, esto es, determinar si el Bitcoin es o no es dinero a la luz de la teoría evolutiva del mismo para luego establecer si el Estado colombiano pretende desconocer dicha realidad. Para lo anterior, será necesario estudiar el origen evolutivo del dinero y las condiciones que debe tener un bien para que sea considerado como tal.

Para entender cómo surgió el dinero resulta interesante, primero, entender cómo se dan los intercambios entre los individuos de la sociedad, porque son esos intercambios los que darán lugar a la necesidad de hallar un bien que sirva como un medio de intercambio universal.

La acción humana es intercambio y elección, con ella se pretende remover un estado de cosas que la persona considera poco satisfactorio por otro que considera más satisfactorio. Se abandona lo que satisface menos, a fin de lograr algo que se apetece más. Una sociedad libre

implica acción concertada entre los individuos que la conforman; es decir, es una sociedad donde se práctica la división del trabajo y se realizan intercambios bilaterales (Rothbard, 2008).

La división del trabajo implica que, las tareas necesarias para la producción de bienes y servicios se distribuye en las personas teniendo en cuenta su capacidad y conocimiento, ya que no todas las personas cuentan con las mismas capacidades, en este sentido, en la sociedad unos se encargan de producir zapatos, otros se encargan de producir comida, otros se encargan de producir ropa y así sucesivamente, para después intercambiarlos. Tal y como lo afirma Rothbard (2008) “El intercambio es la sangre, no solo de nuestra economía, sino de la civilización misma” (p. 8).

Ahora, si ninguna persona pudiese realizar intercambios con otros, simplemente moriría porque no tendría todas las capacidades suficientes para ser autosuficiente toda la vida. Es ahí donde surge el trueque, como forma de satisfacer las necesidades.

3.2.1. Trueque spot

Rallo (2015) define al trueque spot “como un intercambio directo y al contado de dos mercancías” (p. 140). Esto significa que, si Juan tiene excedentes de la mercancía X y necesita la mercancía Y, y a su vez, Pedro tiene excedentes de la mercancía Y, pero necesita la mercancía X, ambos podrán trocar las mercancías y satisfacer sus necesidades.

Podemos observar que este trueque les permite a los individuos que participan del mismo satisfacer de manera inmediata sus necesidades, convirtiendo esta característica en su principal ventaja. Sin embargo, para poder realizar este tipo de intercambio, se deben cumplir ciertos requisitos entre los intervinientes para que el trueque salga avante.

El primer requisito es que Juan debe necesitar lo que Pedro tiene y, a su vez, Pedro debe necesitar lo que Juan tiene. El segundo es que Juan no solo debe tener lo que Pedro

necesite, sino cuando él lo necesite; a su vez, Pedro no solo debe tener lo que necesite Juan, sino que debe tenerlo cuando él lo necesite. El tercer requisito es que Juan debe tener la cantidad exacta que Juan necesita del bien a intercambiar con Pedro, a su vez, Pedro también debe poseer la cantidad exacta del bien a intercambiar con Juan.

Al primer requisito se le conoce como coincidencia espacial entre oferta y demanda, al segundo como coincidencia temporal entre oferta y demanda y, al tercero, como coincidencia cuantitativa entre oferta y demanda. Si no se cumplen estos requisitos el trueque no podrá perfeccionarse (Rallo, 2015).

3.2.2. Trueque diferido

Ahora bien, el trueque diferido surge como una alternativa que permite subsanar el incumplimiento de los requisitos necesarios para que se perfeccione el trueque spot. En este tipo de trueque, los sujetos que intervienen en la operación realizan el intercambio de forma directa (igual que en el spot). La cuestión es que las mercancías que son objeto del intercambio no están disponibles (o al menos una) al momento de trocar; sino que una parte cumplirá con la prestación que tiene a cargo, mientras la otra mercancía objeto del intercambio se entregará en un plazo determinado. De esta manera, uno de los intervinientes asumiría la calidad de deudor y el otro de acreedor (Rallo, 2015).

Un ejemplo de esto es que Pedro tiene la mercancía M y necesita la mercancía H; por su parte, Juan necesita la mercancía M y llegará a tener disponible la mercancía H. Tanto para Pedro, como para Juan, puede significar ventajoso realizar el trueque siempre y cuando a Pedro le nazca el derecho a reclamarle a Juan el cumplimiento de la prestación. Respecto a esta modalidad de trueque, Rallo (2015) manifiesta que es “un intercambio incompleto: solo uno de los sujetos (deudor) adquiere originalmente la propiedad de la mercancía que desea, mientras que

el otro sujeto (el acreedor) no la adquirirá hasta el futuro (de ahí que sea un intercambio *diferido*)” (p. 141).

Si bien este trueque suplía las diferencias del trueque spot, estaba lejos de ser perfecto. El trueque diferido también tenía dos grandes problemas. El primero, era la existencia de información asimétrica; es decir, al momento de realizar el trueque no se contaba con toda la información necesaria para establecer si la otra parte iba a cumplir con la obligación que tenía a su cargo. El segundo, era la inexistencia de un patrón en el que se pudiera expresar el valor líquido de las deudas antes de la creación de estas (Rallo, 2015).

Por su parte, Rothbard (2008) resume que “la indivisibilidad y la falta de coincidencia o disparidad de deseos de cada uno, de lo que cada uno quiere” (p. 8) son los problemas del trueque en general. Cualquier economía del mundo que se denomine “civilizada” sería inviable si solo se practican los intercambios a través del trueque (Rothbard, 2008).

3.2.3. La alternativa

Como una alternativa al trueque, que no resultaba tan efectivo, el hombre descubrió el intercambio indirecto, el cual ha hecho que sea posible el desarrollo de la civilización. Nos referimos a intercambio indirecto cuando dos individuos que tienen disparidad de deseos utilizan un bien no solo para su propio consumo sino para intercambiarlo por un bien que, si desean consumir, a su vez, este primer bien será utilizado por otras personas como medio de intercambio²³ (Rothbard, 2008).

²³ Felipe es dueño de una librería y quiere comprar un celular que vende María. Sin embargo, ella no quiere libros, ella lo que desea es, v. gr. arroz. Entonces, Felipe intercambia sus libros por el arroz que vende Santiago, para después intercambiarlo con María y así poder obtener el celular. Dicho de otra forma, compra arroz, no porque lo quiera para su consumo, sino porque le permite obtener el celular. A su vez, Marcela, propietaria de un cultivo de

Ahora, Rothbard (2008) indica que, cuando “un bien es más “comercializable” que otro - si todos confían en que será más fácilmente vendible- entonces aumentará su demanda porque será utilizado como un “medio de intercambio”.” (p. 9). Así pues, para que un bien sea más comercializable que otro debe cumplir con ciertas características. La primera, es que debe ser mucho más divisible que otros bienes. La segunda, es que debe ser más duradero por largos períodos de tiempo que otros bienes. La tercera es que debe ser más apto para ser fácilmente transportado a cualquier parte del mundo (Rothbard, 2008).

Si un mismo bien cumple con todas estas características en mejor medida que otros, será este el bien escogido, de forma gradual, hasta ser generalmente aceptado por todos como medio de intercambio (Rothbard, 2008). Por lo tanto, la demanda de aquel bien o bienes que vayan siendo más utilizados con ese propósito, aumentará como consecuencia de ese uso y esto, a su vez, aumentará su comerciabilidad (Rothbard, 2008). En efecto, Rothbard (2008) afirmaba:

El resultado es una espiral que se refuerza a si misma: la mayor comerciabilidad causa un uso más intenso como instrumento de cambio lo que a su vez produce una mayor comerciabilidad, etc. ... Eventualmente, uno o dos tipos de bienes se acaban utilizando de forma generalizada como instrumento de intercambio –en la mayoría de intercambios– y a esos instrumentos se les llama dinero. (p. 10)

El dinero es una mercancía (*un bien intercambiable*) que surge de forma libre en el mercado pero que se diferencia de las demás mercancías, en el hecho de que es principalmente

flores, las venderá por un bien que podrá dividir y vender más fácilmente, supongamos que, por arroz, y cambiará entonces parte de ese arroz por ropa, comida, enseres, etc. Finalmente, el arroz se convierte en un medio de intercambio.

usado como medio para realizar intercambios y no solo para satisfacer las necesidades propias del individuo (Rothbard, 2008). Al respecto Rothbard (2008) expresó lo siguiente:

El dinero no es una unidad abstracta de cuenta, que se pueda separar de un bien concreto; no es una ficha sin valor sólo útil como medio de cambio; no es un “crédito o derecho contra la sociedad”; no es una garantía de un precio fijo. Es tan solo una mercancía. Difiere de las demás mercancías o bienes en que es principalmente demandado para ser empleado como medio para realizar intercambios (p. 11).

Por ende, para que un bien sea considerado como dinero primero tuvo que haber sido demandado y valorado como bien de consumo para, posteriormente, convertirse en un medio de intercambio²⁴(Rothbard, 2008). Ahora, como el dinero es una mercancía existe una cierta cantidad, como en todas las mercancías, por ende, se producen diversas variaciones o fluctuaciones en la demanda, esto es, el precio del dinero, así como de cualquier otra mercancía, viene determinado por la interacción entre la oferta total de ese bien o su disponibilidad y la demanda total de las personas que desean tenerlo (Rothbard, 2008).

De esta forma, podemos afirmar que el dinero surge de forma espontánea en la sociedad, sin que ningún Estado lo tenga que producir o lo tenga que categorizar como moneda de curso legal, dado que los individuos en el mercado son quienes eligen de forma descentralizada y competitivamente aquellos bienes que tienen las mejores características para usarlos como medios de intercambio, hasta que uno o unos pocos de toda la oferta de bienes, se vuelven los más preferidos por los individuos que interactúan en el mercado convirtiéndose así en dinero

²⁴ Por ejemplo, el oro primero fue usado como un adorno, pero, con el pasar de los años, se empezó a usar también como medio de intercambio y el que haya sido usado posteriormente como dinero se deriva de que primero fue usado o demandado como adorno.

(Rothbard, 2008). El dinero no surge de ninguna otra forma, ni siquiera porque un Estado decida denominar dinero a un pedazo de papel u otro material (Rothbard, 2008). A lo largo de la historia, varios objetos han fungido como dinero sin que hayan sido producidos por un banco central o hayan sido categorizados como moneda de curso legal por algún Estado²⁵.

3.2.4. La función del dinero

Generalmente, al dinero se le asignan tres funciones. La primera es que sirve como un medio de intercambio; la segunda, es que sirve como depósito de valor; la tercera, es que funciona como unidad de cuenta. Sin embargo, es importante mencionar que todas estas funciones se derivan de su función principal que es la de ser un medio universal de intercambio. Rothbard (2008) ejemplifica esto de la siguiente manera:

Como el oro es un medio de cambio generalmente aceptado, es más comercializable, puede guardarse para servir en futuros intercambios, igual que puede intercambiarse ahora, y todos los precios se expresan por referencia a él²⁶. Como el oro es una

²⁵ Por ejemplo, las piedras rai (Ammous, 2018), las conchas marinas (Szabo, 2002), el ganado y la sal (Fekete, 1996). Estos fueron algunos de los bienes que a lo largo de la historia surgieron espontáneamente en la sociedad como medios de intercambio. Por sus especiales características eran elegidos por las personas como medios de intercambio, pero, a medida que encontraban un bien con mejores características que el anterior, este dejaba de ser usado como medio de intercambio para empezar a usarse otro.

²⁶ Si el valor que se le asigna en la producción al bien de intercambio es demasiado incierto, llevaría a que mientras se valora; exista la tendencia a producir por encima de la demanda y eso haría que se desplome el valor del dinero y deje de servir como bien de intercambio. Como una de las características del dinero es que debe ser escaso para que su valor no fluctúe, variaciones importantes en su producción desestabilizarían su valor y, un bien cuya valoración fluctúe a causa de producciones inestables no es útil como dinero o bien de intercambio.

mercancía apta para todo tipo de transacciones, puede servir de unidad de cuenta tanto para precios actuales como para precios futuros. Es importante tomar conciencia de que el dinero no puede ser una abstracta unidad de cuenta o de crédito, excepto en la medida en que sirva como medio de cambio. (p. 13)

Ahora bien, la primera función permite que, a través del dinero, podamos “adquirir bienes, servicios y activos financieros sin recurrir al trueque” (FMI, 2001, p. 53). La segunda lo convierte en un “medio de tenencia de patrimonio o riqueza” (FMI, 2001, p. 53). La tercera significa que el dinero es un “patrón para denominar los precios de los bienes y servicios y los valores de los activos financieros y no financieros, proporcionando de esa manera un medio para comprar valores y preparar las cuentas financieras” (FMI, 2001, p. 53). Sin embargo, como ya se mencionó, un bien no podría tener ninguna de estas funciones si no fuera un medio general de intercambio.

3.2.5. ¿Es el Bitcoin dinero?

Teniendo claridad sobre las respuestas a las preguntas de ¿cómo surge el dinero? Y ¿qué es dinero? Podemos entonces analizar si el Bitcoin, a la luz de la teoría evolutiva del dinero, es o no es dinero. En primer lugar, recordemos que el dinero surge de forma espontánea en la sociedad sin que ningún Estado lo decreta o determine como tal. Para el caso de Bitcoin, como ya se ha mencionado, quizá el momento más trascendental fue aquel día en que alguien estuvo dispuesto a abandonar dinero para poseer varias de las monedas que se encontraban en circulación en la red, esto es, en 2009 cuando una casa de cambio de internet vendió Bitcoins al precio de 0,000994 dólares. Y el segundo hecho, en 2010, cuando por primera vez alguien pagó 10.000 Bitcoins por 2 pizzas de 25 dólares, estableciendo el precio del Bitcoin en 0,0025 dólares

(Ammous, 2008). Estos hechos fueron considerados como trascendentales ya que, para que cualquier medio evolucione como dinero, tuvo que haber tenido previamente demanda como medio de consumo y, así sucedió con Bitcoin, toda vez que pasó de ser solo un artículo coleccionable a ser un medio de intercambio en el mercado y para que lo anterior sucediera, ningún Estado lo tuvo que decretar previamente, ningún Estado tuvo que decir que se podía transar con Bitcoin (Ammous, 2018).

En segundo lugar, para que un bien sea utilizado como medio universal de intercambio, debe ser altamente comercializable, más que otros bienes. Para determinar que un bien es más comercializable que otro Rothbard (2008) menciona ciertas características que debe tener ese bien las cuales son: i) ser más divisible que otros bienes, ii) ser duradero por largos períodos de tiempo y iii) ser fácilmente transportado a cualquier parte del mundo.

En este sentido, como ya se mencionó, cada unidad de Bitcoin es divisible en 100 millones de satoshis, por ende, 1 Bitcoin es igual a 100 millones de satoshis y 1 satoshi es igual a 0,00000001 Bitcoins. Además, con el tiempo, el poder adquisitivo de Bitcoin ha ido aumentando a pesar de su aumento moderado de la oferta, que como ya se sabe, es limitada y no se puede alterar (Ammous, 2019). Así pues, podemos decir que Bitcoin cumple con la primera característica para que un bien sea más comercializable que otros bienes y es que es divisible y su poder adquisitivo aumenta pese al crecimiento moderado de su oferta.

Por otro lado, Bitcoin es un bien digital que usa el internet para mantenerse en funcionamiento. Bitcoin, individualmente considerado, no está compuesto por algún material que se pueda dañar, romper, quemar, deteriorar, destruir, alterar, mojar, etc. Sin embargo, al estar almacenado en billeteras electrónicas, que contienen las claves privadas y públicas de los

participantes del sistema, y donde nadie puede acceder a las criptomonedas de otro sin permiso, cabe la probabilidad de que el usuario pierda su clave privada, sin que sea factible recuperarla, lo cual implicará que pierda el acceso a los activos y no puedan ser usados como medio de intercambio (Emet, 2019).

A pesar de lo anterior, mientras la persona tenga acceso a su clave privada podrá, desde cualquier dispositivo con acceso a internet, realizar transacciones con sus Bitcoins pues la única manera de que Bitcoin deje de funcionar es destruyendo todos los ordenadores que lo albergan, sin embargo, aquello sería muy difícil porque lo albergan millones de ordenadores en todo el mundo (Merkle, 2016). En este sentido, Bitcoin cumple con la segunda característica para que un bien sea más comercializable que otros bienes y es que es duradero por largos períodos de tiempo.

Así mismo, Bitcoin también cumple con la tercera característica para que un bien sea más comercializable que el resto dado que se puede portar con una facilidad casi que inigualable por el dinero fiat o el dinero tradicional, siempre que la persona tenga a mano su clave privada, puede acceder a su billetera electrónica desde cualquier parte del mundo, en cualquier dispositivo móvil con acceso a internet y siempre que cuente con el conocimiento suficiente podrá acceder al registro digital de Bitcoin y hacer sus transacciones (Ammous, 2018).

Gracias a que Bitcoin cuenta con estas 3 características que lo hacen altamente comercializable, más que otros bienes, las personas lo han empezado a utilizar, ya no solo como un bien o artículo coleccionable, sino también como un medio de intercambio. Al igual que las piedras rai, las conchas marinas y los metales preciosos, el Bitcoin paso de ser solo un bien de consumo para emplearse como un instrumento de cambio. Igualmente, gracias a que se ha

empezado a usar como medio de intercambio, su demanda ha aumentado, y esto, según Rothbard (2008) hace que a su vez aumente la comerciabilidad de ese bien.

En conclusión, podemos decir entonces que el Bitcoin es dinero a la luz de la teoría evolutiva del mismo dado que surgió de forma espontánea en la sociedad, las personas lo han empezado a adoptar paulatinamente; por sus especiales características de divisibilidad, portabilidad y durabilidad; como medio de intercambio, lo que ha conllevado a que su demanda aumente cada vez más y su valor también²⁷. Además, debido a que cumple con la función principal del dinero también cumple con las demás funciones del mismo, es decir, permite intercambiarse por bienes y servicios (medio de intercambio), sirve para tener patrimonio²⁸ y sirve para expresar los precios.

3.2.6. Competencia de las diferentes criptomonedas

²⁷ Respecto a este punto vale la pena mencionar que hay una relación entre la demanda del dólar y el Bitcoin. Dicha relación consiste en que, cuando hay menos dólares circulando en la economía, la demanda del Bitcoin disminuye porque las personas no sienten la necesidad de acudir a otros medios de intercambio toda vez que sus dólares no pierden poder adquisitivo. Por el contrario, cuando hay muchos dólares circulando en la economía, el valor de los mismos disminuye y, así mismo, pierden poder adquisitivo, la demanda del Bitcoin aumenta porque las personas tienen incentivos de acudir a otros medios de intercambio en donde la oferta responde a la demanda, tal como sucede con esta criptomoneda (Forbes, 2021).

²⁸ Incluso, se convierte en un medio para evitar la expropiación vía impuestos, pues el Estado no tiene forma de rastrear las transacciones que realizan los individuos. Esto lo imposibilita para usar la coacción para obligar a que una persona se desprenda de su propiedad a través del latrocinio llamado impuestos.

Sumado a lo anterior, es necesario mencionar que la competencia de las criptomonedas²⁹ es bastante amplia, lo cual es positivo pues solo las criptomonedas con las características más adecuadas³⁰ serán elegidas por las personas como el medio de intercambio universal (Barroilhet, 2019). Gracias a estas especiales características, las criptomonedas aspiran a ser consideradas como dinero electrónico y, a su vez, dinero corriente (Halaburda y Sarvary, 2016). Tal como lo mencionan Sarmiento y Garcés (2016) las criptomonedas son “una alternativa al sistema monetario actual” (p. 152) toda vez que con ellas se evita la presencia de un ente centralizado que funja como un intermediario de todo el proceso (emisión, validación, registro, compensación y liquidación), ya que este ente centralizado es susceptible de perversión por la avaricia de los individuos, las necesidades financieras de los gobiernos y la intervención sistemática de las autoridades (Huerta de Soto, 2016). Las criptomonedas, por otro lado, son completamente descentralizadas y el sistema se mantiene por la participación de todos los nodos (Arango et. al, 2018).

3.3. Marco regulatorio del dinero en Colombia

3.3.1. Intervención

²⁹ Es importante distinguir la diferencia entre las criptomonedas y el denominado dinero electrónico o (*e-money*). Este último es una representación digital de la moneda de curso legal de una jurisdicción (He et al., 2016).

³⁰ Es decir, los individuos de forma libre van escogiendo la criptomoneda que consideren más adecuada para ser usada como un medio de intercambio, y de forma paulatina, será siendo elegida por otros individuos hasta convertirse en un medio universal de intercambio. Por ejemplo, una persona puede considerar que determinada criptomoneda es más adecuada que otra porque tiene mayor divisibilidad lo cual le permite a la persona transar en montos más pequeños para así satisfacer alguna necesidad.

En una sociedad libre, los individuos no se ven forzados a realizar intercambios con nadie. Ellos buscarán maximizar su utilidad realizando intercambios para satisfacer sus necesidades según su escala valorativa. Sin embargo, con la existencia del Estado, se legitima a través de todo el ordenamiento jurídico el uso de la violencia contra los individuos que conforman la sociedad. Esa violencia desencadena en tres tipos de intervención, que, en últimas, terminan por disminuir la utilidad de los intercambios que se realizan.

Rothbard (2009) distingue entre 3 tipos de intervención estatal. El primer modelo de intervención lo denomina *autista* el cual consiste en que el Estado (*agresor*) obliga a los individuos a hacer o no hacer alguna acción que involucra exclusivamente a la propiedad de la persona y la afectación es exclusiva. El segundo tipo de intervención la denomina *binaria*, consiste en obligar al individuo a realizar un intercambio con el invasor (*Estado*); un ejemplo de esta obligación son los impuestos o el gasto público.

El último tipo de intervención que plantea, lo llama intervención *triangular*, este consiste en que el Estado prohíbe u obliga a dos individuos el hacer un intercambio o, lo permite, pero con la observancia de ciertas condiciones v. gr. el control de precios o regulaciones sobre productos. Ahora, las normas que imponen un bien como moneda o dinero de curso legal son un ejemplo de este tipo de intervención, pues a través de ella, el Estado, se reserva para sí mismo el monopolio del dinero (acuñación de moneda), es decir, permite que los individuos hagan intercambios, pero con la condición de que estos usen como medio de intercambio aquel bien al que ellos han denominado de curso legal. Lo anterior, genera que los consumidores se vean forzados a transar con el bien que el monopolista destine para ello³¹ (Rothbard, 2009).

³¹ Recordemos que, según la teoría evolutiva del dinero, el mismo surge de forma espontánea en la sociedad libre. El dinero no es dinero solo porque un Estado diga que lo es (Rothbard, 2008).

3.3.2. Monopolio

El concepto de monopolio reviste gran importancia cuando se habla de criptomonedas, pues el surgimiento de esta a través de la tecnología de la cadena de bloques pone en riesgo el monopolio que tienen los Estados sobre la producción de dinero. Empecemos por definir que es un monopolio. El jurista inglés, Lord Coke (cómo se citó en Ely et al., 1917) expresa que “un monopolio es una institución o permiso del rey, de su consecución, comisión u otra” (p. 191). Ahora, Blackstone (cómo se citó en Ely et al., 1917) lo define “como una licencia o privilegio permitido por el rey” (p. 191).

Por otro lado, Rothbard (2009) logra condensar dichas definiciones cuando manifiesta que “un monopolio es un privilegio especial concedido por el Estado, reservando cierta área de la producción a un individuo en particular o a un grupo” (p. 669). En otras palabras, la emisión de dinero es un monopolio porque el ordenamiento jurídico de un Estado se reserva la facultad de decidir qué bien será considerado como dinero de curso legal, emitir ese dinero y manejar la tasa de interés.

Ahora bien, la ley de curso legal no es una prohibición en sí misma porque el Estado no prohíbe la producción o venta de cierto bien para que sea usado como medio de intercambio, lo que sucede es que el Estado se otorga a sí mismo el privilegio de decir que bien será usado como medio de intercambio y así mismo será el de curso legal, haciendo entender que, cualquier otro bien que sea usado como tal no será de curso legal lo cual hará que sea más difícil transar con otro bien (Rothbard, 2009).

Por otro lado, la ley de curso legal no es un control de precios toda vez que este opera cuando el Estado “puede establecer o bien un precio mínimo del que no se puede vender un producto o bien un precio máximo por encima del cual no puede venderse. Puede asimismo

obligar a realizar una venta a un precio fijo” (Rothbard, 1970, p. 79). Es decir, en este caso el Estado no está imponiendo un valor máximo o un valor mínimo por el cual se puede vender un producto, sino que lo que hace el gobierno es conceder un privilegio especial a una sola institución para que sea esta la única autorizada para producir y emitir el bien de curso legal que será usado como medio de intercambio y todo aquello que no sea producido y emitido por aquella institución simplemente no será considerado como dinero.

3.3.3. Marco regulatorio general del dinero de curso legal en Colombia

Los constituyentes de 1991 le otorgaron al Congreso de la República la función de “determinar la moneda legal, la convertibilidad y el alcance de su poder liberatorio³², y arreglar el sistema de pesas y medidas” (Const. P., art. 150, 1991). Por otro lado, se estableció que, “El Estado, por intermedio del Banco de la República, velará por el mantenimiento de la capacidad adquisitiva de la moneda” (Const. P., art. 373, 1991). En este sentido, el constituyente en la misma constitución le asignó las siguientes funciones al Banco de la República:

Regular la moneda, los cambios internacionales y el crédito; emitir la moneda legal; administrar las reservas internacionales; ser prestamista de última instancia y banquero de los establecimientos de crédito; y servir como agente fiscal del gobierno. Todas ellas se ejercerán en coordinación con la política económica general (Const. P., art. 371, 1991).

³² El poder liberatorio de una moneda es “la facultad que la ley asigna a ciertas especies monetarias en virtud de la cual, el deudor puede imponer a su acreedor, aún por la fuerza compulsiva de las leyes, su aceptación a título de pago” (Garcés, 1963, p. 7). En el caso de Colombia este poder liberatorio es absoluto, pleno e ilimitado, es decir, el acreedor de una obligación está obligado a recibir el total de su crédito en una determinada especie monetaria, es decir, está obligado a recibir el total de su crédito en pesos colombianos (Garcés, 1963).

Ahora bien, en la ley 31 de 1992, por la cual se dictan las normas a las que deberá sujetarse el Banco de la República para el ejercicio de sus funciones, se indica que “la unidad monetaria y unidad de cuenta del país es el peso emitido por el Banco de la República” (L. 31, art. 6, 1992), adicional a ello, en la misma ley se establece que “el Banco de la República ejerce en forma exclusiva e indelegable el atributo estatal de emitir la moneda legal constituida por billetes y moneda metálica” (L. 31, art. 7, 1992) y, en su artículo 8 establece que “la moneda legal expresará su valor en pesos de acuerdo con las denominaciones que determine la Junta Directiva del Banco de la República y será el único medio de pago de curso legal con poder liberatorio ilimitado” (L. 31, art. 8, 1991).

Lo anterior significa, que el Congreso de la República es quien determina la moneda de curso legal mediante la cual los individuos en el territorio colombiano pueden realizar transacciones o intercambios en el mercado. Y el Banco de la República, en particular su Junta Directiva, es la única autoridad monetaria, cambiaria y crediticia según el artículo 372 de la Constitución Política de Colombia. Es la autoridad monetaria porque el Banco de la República es “la entidad encargada de emitir el dinero que se utiliza en nuestro país, que como sabemos es el peso colombiano” (Cárdenas, 2007, p. 240) y, es la entidad encargada de controlar el precio de la moneda y el poder adquisitivo de la misma por medio de diversas operaciones de mercado abierto³³ que ayudan a controlar la masa monetaria (Cuéllar de Martínez, 1997). Es autoridad

³³ Las Operaciones de Mercado Abierto (OMA) “son el principal instrumento que tiene el Banco de la República para aumentar o disminuir la cantidad de dinero en la economía. Cuando es necesario aumentar la liquidez, el Banco de la República compra títulos o papeles financieros en el mercado, inyectando dinero a la economía; por el contrario, cuando el Banco quiere disminuir la liquidez, vende títulos y, por lo tanto, recoge dinero del mercado” (Banco de la República, s.f., párr. 1).

cambiaría porque se encarga de regular la entrada y salida de las divisas extranjeras, de controlar la tasa de cambio y de regular el mercado de derivados³⁴, y, finalmente, es autoridad crediticia porque participa en la fijación de las diversas tasas de interés como la tasa de interés de mercado y, porque realiza su operación de banquero y prestamista de los bancos comerciales de última instancia (Cuéllar de Martínez, 1997).

3.4. Marco regulatorio de las criptomonedas en Colombia.

En este punto, se expondrá lo afirmado por algunas instituciones en Colombia, tales como: el Banco de la República, la Superintendencia financiera de Colombia, la Superintendencia de Sociedades y la Dirección de Impuestos y Aduanas Nacionales, sobre el tratamiento que se les da actualmente a las criptomonedas dentro del territorio nacional colombiano.

3.4.1. Banco de la República de Colombia

Respecto al Bitcoin, el Banco de la República (2014) en el comunicado de prensa del 1 de abril de 2014 expresó, en resumidas cuentas, que:

1. La única unidad monetaria y de cuenta en Colombia es el peso (billetes y monedas) emitido por el Banco de la República.

³⁴ Un producto derivado es aquel que su precio varía dependiendo del precio de otro bien subyacente o de referencia, tales como acciones o materias primas y energía. Así, el mercado de derivados es un instrumento financiero “que asegura el precio a futuro de la compra o venta del bien subyacente o de referencia, esto con el objetivo de prevenir las posibles variaciones al alza o a la baja del precio que se genere sobre éste producto” (Forbes, 2019, párr.5).

2. El Bitcoin no es una moneda en Colombia y, por lo tanto, no constituye un medio de pago de curso legal con poder liberatorio ilimitado. No existe entonces obligatoriedad de recibirlo como medio de cumplimiento de las obligaciones.

3. El Bitcoin tampoco es un activo que pueda ser considerado una divisa debido a que no cuenta con el respaldo de los bancos centrales de otros países. En consecuencia, no puede utilizarse para el pago de las operaciones de qué trata el Régimen Cambiario expedido por la Junta Directiva del Banco de la República³⁵.

Adicional a lo anterior, el Banco de la República se ha pronunciado sobre este tema en diversas respuestas a derechos de petición. En efecto, en el concepto JDS-25631 del 30 de noviembre de 2016 se advirtió que:

Ninguna moneda virtual -MV-, incluyendo el *Bitcoin* ha sido reconocida como moneda por el legislador ni por la autoridad monetaria. En la medida que no constituye un activo equivalente a la moneda de curso legal, carece de poder liberatorio ilimitado para la extinción de obligaciones³⁶ (Banco de la República, 2016, p. 1).

³⁵ Según la Resolución Externa No 01 de 2018 emitida por la Junta Directiva del Banco de la República, estas operaciones son aquellas en que la negociación o transferencia de divisas debe hacerse a través de los Intermediarios del Mercado Cambiario (IMC) o de cuentas de compensación, y no por el mercado libre o no regulado. Entre estas operaciones están la importación y exportación de bienes, las operaciones de endeudamiento externo celebradas por residentes, así como los costos financieros inherentes a las mismas, las inversiones de capital del exterior en el país, así como los rendimientos asociados a las mismas, las operaciones de derivados, las inversiones de capital colombiano en el exterior, así como los rendimientos asociados a las mismas, entre otras.

³⁶ Esto mismo ha sido reiterado en diversos conceptos del Banco de la República tales como el JDS-14890 del 18 de junio de 2017, JDS-CA-13581 del 21 de junio de 2019, C20-162943 del 28 de diciembre de 2020 y el Q20-1115 de enero de 2020.

También, a través del concepto JDS-27301 del 22 de diciembre de 2017 se indicó lo siguiente:

Adicionalmente, estos instrumentos [las criptomonedas] no se caracterizan por su alta liquidez en el mercado, lo que significa que no son fácilmente intercambiables sin restricciones en la forma o montos negociados, circunstancias que no las hacen congruentes con las condiciones señaladas para su consideración como divisa de libre uso por el Fondo Monetario Internacional y el Banco de Pagos Internacionales (Banco de la República, 2017, p. 2).

Igualmente, el Banco de la República ha reiterado en diversas ocasiones que las entidades que actúan como Intermediarios del Mercado Cambiario (IMC) no han sido autorizadas para emitir o vender criptomonedas como el Bitcoin conforme a lo establecido en el artículo 59 de la Resolución Externa No. 08 de 2000 y en la Circular Reglamentaria DCIN 83 del Banco, además, ha recordado con ello, que estas entidades son las únicas autorizadas para realizar giros o remesas de divisas desde o hacia el exterior y “realizar gestiones de cobro o servicios bancarios similares, manejar y administrar sistemas de tarjeta de crédito y de débito internacionales y distribuir y vender tarjetas prepago emitidas por entidades financieras del exterior” (Banco de la República, 2017, p.1).

Finalmente, esta entidad estatal emitió un documento técnico relacionado con el tema en cuestión en donde concluyó que, si bien estos esquemas de criptomonedas presentan grandes ventajas en términos de menores costos de tenencia y transferencia de riqueza, la volatilidad de

su precio, su limitada adopción y aceptación³⁷, los altos riesgos que estas traen y el ser operadas por agentes privados y de manera anónima y no por una entidad centralizada hace que las mismas sean de poca relevancia y muy poco usadas como medio de intercambio en el mercado y como depósito de valor (Arango et al., 2018).

Además, en este mismo documento se indica, que el permitir el desarrollo de estos esquemas en Colombia genera diversos riesgos, entre ellos, posibles pérdidas económicas las cuales, teniendo en cuenta la regulación vigente en Colombia, recaerían exclusivamente en quien utilice las criptomonedas de forma voluntaria para hacer intercambios en el mercado. Otros de los riesgos más significativos del uso de estos esquemas son los siguientes:

1) la integridad financiera y fiscal, debido a que estos esquemas pueden convertirse fácilmente en canales para actividades asociadas al lavado de activos, la financiación del terrorismo (LA/FT) y la evasión tributaria, y 2) la protección del consumidor frente a los riesgos asociados con estos esquemas y con los operadores especializados que ofrecen servicios de negociación, custodia y transferencia de fondos en estos Criptoactivos (Arango et al., 2018, p.40).

3.4.2. Superintendencia Financiera de Colombia

De igual forma, la Superintendencia Financiera de Colombia se ha pronunciado en diversas cartas circulares sobre los riesgos a los que se someten los usuarios cuando realizan un intercambio en el mercado por medio de estas criptomonedas. En efecto, en la Carta Circular No. 29 de 2014 se expresó que:

³⁷ Recordemos que, según la teoría evolutiva del dinero, la volatilidad del precio de un bien y su limitada adopción no son condiciones obligatorias para que un bien llegue a ser dinero o medio de intercambio. Más bien es un argumento que busca evitar reconocerlo.

- i) “(...) el Bitcoin no es un activo que tenga equivalencia a la moneda legal de curso legal en Colombia al no haber sido reconocido como moneda en el país”
(Superintendencia Financiera, 2014, p. 1).
- ii) En segundo lugar, el Bitcoin no es un activo que pueda ser considerado como divisa, “dado que tampoco cuenta con el respaldo de los bancos centrales de otros países y por lo tanto no tiene poder ilimitado para la extinción de obligaciones”
(Superintendencia Financiera, 2014, p. 1).
- i) El Bitcoin ni demás criptomonedas “se encuentran respaldadas por activos físicos, por un banco central (...) por lo que el valor de intercambio de las mismas podría reducirse drásticamente e incluso llegar a cero” (Superintendencia Financiera, 2014, p. 1). Indican que por lo anterior las personas se exponen a la volatilidad del precio de las mismas dada la amplia especulación que se realiza.
- ii) Ninguna de las plataformas transaccionales, ni comercializadores de las criptomonedas se encuentran reguladas por el ordenamiento jurídico colombiano, es decir, no se encuentran sujetas al control, vigilancia o inspección de la Superintendencia Financiera. “Por lo anterior, tales plataformas pueden no contar con estándares o procesos seguros y de mitigación de riesgos, por lo que con regularidad presentan fallas que llevan a que los usuarios de las mismas incurran en pérdidas” (Superintendencia Financiera, 2014, p. 1).
- iii) Las plataformas por donde se realizan este tipo de transacciones no están sometidas al control, vigilancia o inspección de la Superintendencia Financiera, como consecuencia de ello, podría suceder que dichas plataformas no cuenten con

los estándares idóneos para la mitigación de riesgo y la garantía de la seguridad lo que generaría fallas en el sistema y con ello, grandes pérdidas económicas.

- iv) Estas plataformas pueden estar domiciliadas en múltiples jurisdicciones, por lo tanto, su regulación y control se salen del rango que abarca la ley colombiana.
- v) Las transacciones en las plataformas pueden ser anónimas, por ende, el uso de estas criptomonedas podría ser usada para el desarrollo y ejecución de actividades ilícitas o fraudulentas.

También, la Superintendencia Financiera mediante las Cartas Circulares No. 29 de 2014, 78 de 2016 y No. 52 de 2017, ha dejado claro que “las entidades vigiladas no se encuentran autorizadas para custodiar, invertir, ni intermediar con estos instrumentos, así como tampoco permitir el uso de sus plataformas para que se realicen operaciones con monedas virtuales” y “corresponde a las personas conocer y asumir los riesgos inherentes a las operaciones que realicen con monedas virtuales”, dado que “no se encuentran amparadas por ningún tipo de garantía privada o estatal, ni sus operaciones son susceptibles de cobertura por parte del seguro de depósito”.

Por otro lado, según la Carta Circular No. 52 de 2017, las criptomonedas como el Bitcoin no constituyen un valor en los términos de la ley 964 de 2005³⁸, toda vez que, según el artículo 2 de la mencionada ley, “será valor todo derecho de naturaleza negociable que haga parte de una emisión, cuando tenga por objeto o efecto la captación de recursos del público” además, enuncia expresamente cuáles son los conceptos denominados como tal. Por ende, las mismas no hacen

³⁸ Ley por la cual se dictan normas generales y se señalan en ellas los objetivos y criterios a los cuales debe sujetarse el Gobierno Nacional para regular las actividades de manejo, aprovechamiento e inversión de recursos captados del público que se efectúen mediante valores y se dictan otras disposiciones.

parte de “la infraestructura del mercado de valores colombiano, no constituyen una inversión válida para las entidades vigiladas, y tampoco sus operadores se encuentran autorizadas para asesorar y/o gestionar operaciones sobre las mismas” (Superintendencia Financiera, 2017, p. 2).

Finalmente, en esta circular se indica que, las entidades vigiladas deben aplicar las medidas adecuadas tendientes a prevenir que las criptomonedas sean usadas como instrumento “para el lavado de activos³⁹ y/o canalización de recursos hacia la realización de actividades terroristas o para el ocultamiento de activos provenientes de las mismas por la materialización de los riesgos potenciales en el uso de monedas Electrónicas-Criptomonedas (...)” (Superintendencia Financiera, 2017, p. 2).

3.4.3. Superintendencia de Sociedades de Colombia

Teniendo en cuenta lo anterior podemos afirmar que a la luz del ordenamiento jurídico colombiano las criptomonedas como el Bitcoin no son consideradas como dinero de curso legal, ni divisas, ni activos financieros. Sin perjuicio de ello, las mismas tampoco están prohibidas en Colombia. La Superintendencia de Sociedades de Colombia (2020) indicó en el Oficio 100-237890 del 14 de diciembre de 2020 que, según su Grupo de Regulación e Investigación Contable, existe la posibilidad de que las criptomonedas sean objeto de aporte en especie a las sociedades.

Así pues, el *International Accounting Standards Board*-IASB (como se citó en el Oficio 100-237890 de la Superintendencia de Sociedades, 2020) mediante la Decisión de Agenda emitida en junio del 2019 consideró que la naturaleza de las criptomonedas es el de un activo intangible, en efecto:

El párrafo 8 de la NIC 38 Activos Intangibles define un activo intangible como “un

³⁹ Artículo 323 del Código Penal Colombiano.

activo identificable, de carácter no monetario y sin apariencia física”.

El párrafo 12 de la NIC 38 señala que un activo es identificable si es separable o surge de derechos legales o contractuales. Un activo es separable si "es susceptible de ser separado o escindido de la entidad y vendido, transferido, dado en explotación, arrendado o intercambiado, ya sea individualmente o junto con el contrato, activo identificable o pasivo con los que guarde relación".

El párrafo 16 de la NIC 21 Efectos de las Variaciones en las Tasas de Cambio de la Moneda Extranjera señala que "la característica esencial de una partida no monetaria es la ausencia de un derecho a recibir (o una obligación de entregar) una cantidad fija o determinable de unidades monetarias.

El Comité observó que la tenencia de criptomonedas cumple la definición de un activo intangible de la NIC 38 sobre la base de que (a) puede ser separado del tenedor y vendido o transferido de forma individual; y (b) no otorga al tenedor un derecho a recibir un número fijo o determinable de unidades monetarias (p. 9).

Por lo anterior, las criptomonedas son consideradas en Colombia como un activo intangible, por consiguiente, la Superintendencia de Sociedades (2020) precisó que, conforme al ordenamiento jurídico colombiano, las personas pueden, a fin de capitalizar su empresa, realizar aportes en especie (que pueden ser bienes tangibles o intangibles), dado que conforme a los artículos 126 y subsiguientes del Código de Comercio, los aportes pueden hacerse en bienes diferentes al dinero, sin embargo, indica que para que ello sea válido los mismos deberán cumplir a cabalidad las normas legales que regulan el aporte en especies (artículos 122 y subsiguientes del Código de Comercio y demás normas aplicables). Pese a lo anterior la

Superintendencia de Sociedades (2020) en el Oficio ya mencionado advierte lo siguiente:

En cuanto a la responsabilidad que se asume al invertir en Criptoactivos⁴⁰ por parte de sociedades comerciales, es preciso señalar que sus administradores han sido suficientemente advertidos por esta Entidad sobre lo riesgoso de estas inversiones, dada la volatilidad de su valor, la ausencia de regulación local y la inseguridad que genera el total anonimato en la cadena de partícipes, entre otros aspectos (p. 5).

3.4.4. Dirección de Impuestos y Aduanas Nacionales (DIAN).

La DIAN (2017) por medio del Concepto 20436 del 2 de agosto de 2017, se acogió a lo indicado por el Grupo de Acción Financiera mediante el documento de junio de 2014 titulado “Monedas Virtuales Definiciones Claves y Riesgos potenciales de LA/FT” en el cual se afirma lo siguiente:

Moneda virtual es una representación digital⁴¹ de valor que puede ser comerciada digitalmente y funciona como (1) un medio de cambio; y/o (2) una unidad de cuenta; y lo (3) un depósito de valor; pero no tiene curso legal (es decir, cuando se ofrece a un acreedor, es una oferta válida y legal de pago) en ninguna jurisdicción (p.2).

Esto quiere decir que la DIAN acepta que las criptomonedas son un medio de intercambio, una unidad de cuenta y un depósito de valor, es decir, cumplen con las funciones del dinero propiamente dicho, empero, el único inconveniente para que puedan ser usadas como

⁴⁰ Es importante mencionar en este punto que los criptoactivos son, por así decirlo, la categoría y las criptomonedas son una de las especies. Los tokens y los commodities también son otras especies de criptoactivos (EGA Futura, 2021).

⁴¹ Se debe entender como representación de algo en forma de dato digital, es decir, datos informáticos representados con el uso de valores que conforman la información.

dinero en Colombia es que no son de curso legal, esto es, ninguna entidad estatal las ha reconocido formalmente como tal. Por otro lado, en relación con la minería la DIAN (2017) indicó lo siguiente:

Considerando que el resultado de la minería virtual es: bien sea, la obtención de nuevas monedas como resultado del servicio de confirmación de transacciones y aseguramiento de la red y/o el reconocimiento de comisiones por quienes las ofrecen para que se verifiquen sus transacciones, en uno y otro caso suponen el registro de la operación realizada a través de las billeteras como en la contabilidad común, registro que no es más que el apunte de ese algo que se posee que se evidencia como dato digital. En tanto los participantes en esa red están de acuerdo que la solución de algoritmos, como esencia de la confirmación de transacciones, permite obtener nuevas monedas acorde con las reglas, así como algunas a título de comisión, implican un nuevo concepto al reconocer valor a los datos digitales, esto implica, para efectos tributarios, determinar en primer lugar la naturaleza jurídica de los bienes producto del minado (p.5).

En este sentido, la DIAN determinó que la naturaleza jurídica de las criptomonedas es que son un bien que no tiene existencia física, es decir, son un bien de carácter incorporeal o inmaterial susceptible de ser valorado. Así, aquellos participantes que se dedican a minar para obtener nuevas criptomonedas obtienen un bien a título de retribución o recompensa por los servicios de confirmación y aseguramiento, por tanto, estas nuevas criptomonedas son consideradas como un ingreso en especie. Por lo anterior, dichos ingresos están gravados en Colombia dado que “desde el punto de vista patrimonial en tanto esas monedas corresponden a

bienes inmateriales, susceptibles de ser valoradas, forman parte del patrimonio y pueden conducir a la obtención de una renta (presuntiva)”⁴² (DIAN, 2017, p.6).

4. Conclusión

Al hablar de dinero, nos referimos a un bien altamente comercializable que puede ser fácilmente transportable, duradero y divisible. Adicional, es un bien que en sus inicios fue una mercancía normalmente usada para satisfacer una necesidad y que, con el paso del tiempo, se empezó a usar como medio de intercambio.

Ahora, el Bitcoin al ser 100% digital, es fácilmente transportable. Por un lado, si la persona cuenta con una billetera electrónica de almacenamiento frío puede transportar fácilmente el monedero hardware a cualquier lugar dado que se asimila a una USB y, así mismo, podrá conectarla a cualquier dispositivo que sea compatible con la misma. Por otro lado, si una persona tiene una billetera electrónica caliente podrá desde cualquier dispositivo con acceso a internet (siempre que tenga acceso a su clave privada) acceder a su billetera electrónica e interactuar con sus Bitcoins.

⁴² “La renta presuntiva es un método alternativo para determinar el impuesto de renta (...). El objeto de la renta presuntiva es presumir la percepción de ingresos, utilidades o beneficios en cabeza de una persona que da lugar al cumplimiento por parte de esta y del ciudadano, del deber de “contribuir al financiamiento de los gastos e inversiones del Estado dentro del concepto de justicia y equidad”. (...) El hecho gravado en la renta presuntiva es la percepción de utilidades o beneficios que se presume se han obtenido por el contribuyente por tener dentro del balance del patrimonio unos activos que resultan ser superiores a los pasivos (...). De esa forma, es claro que la renta comprende toda ganancia obtenida por el sujeto, independientemente de cuál sea su fuente.” (C.C., C-564/96, p. 11, 1996)

Adicionalmente, es muy duradero, pues no se destruye con la facilidad que se destruye, por ejemplo, un billete de \$10.000 pesos colombianos, sin embargo, como ya se ha mencionado, para que una persona pueda interactuar con sus Bitcoins debe tener una billetera electrónica y una clave privada, si esta clave privada se pierde, es casi imposible volver a recuperarla y, así mismo, recuperar el control de los Bitcoins que se poseían, debido a que no existe la opción de “olvide mi contraseña”, pero, mientras los usuarios tengan su clave privada, podrán acceder a su billetera electrónica y así mismo interactuar con sus Bitcoins.

Y finalmente, es divisible, lo que permite que se puedan realizar transacciones pequeñas empleándolo como medio de intercambio en el mercado.

Esto no es todo, el Bitcoin en sus inicios, fue un bien que la gente adquiriría para coleccionar y que, con el paso del tiempo, ha ido adquiriendo popularidad como medio general de intercambio.

Esto nos permite evidenciar que el Bitcoin cumple con todas las características que, según la teoría evolutiva del dinero, debe cumplir un bien que aspira a convertirse en dinero. Sin embargo, el Bitcoin es criticado por su volatilidad en el precio, la cuestión es que, tal como lo afirma Rothbard (2008), el dinero, al ser un bien de intercambio, está sujeto a la interacción entre oferta y demanda para establecer su precio. De hecho, si la crítica de la volatilidad en el valor fuera requisito indispensable para establecer la calidad de dinero, entonces tendríamos que afirmar que el bolívar y el peso argentino (por citar dos ejemplos), tampoco lo serían, pues a

pesar de ser “moneda de curso legal”, su volatilidad es muy alta y afecta a millones de personas⁴³.

A la luz de la teoría evolutiva del dinero, podemos afirmar que el Bitcoin es dinero, pero eso no significa que no tenga cosas por mejorar. Creemos que uno de los aspectos más importantes, aunque no es un aspecto que ponga en tela de juicio su identificación como medio universal de intercambio, es que las operaciones con Bitcoin⁴⁴ tienden a ser complejas de entender, lo que genera reticencia de algunas personas a comprar y utilizar el Bitcoin como dinero. De facilitar el proceso de adquisición de conocimiento para operar Bitcoin, se crearía un incentivo para que las personas acudan a él y lo puedan usar también con ese propósito, lo que hará que la demanda del mismo aumente y, su vez, su comerciabilidad.

Es esa ignorancia en el uso del Bitcoin, lo que podría estar ocasionando que el Estado colombiano no prohíba el uso de criptomonedas. Pues no siente amenazado su monopolio de acuñación de moneda. Empero, en el momento en que esa dificultad se vaya solucionando, y más colombianos acudan al Bitcoin para escapar de la devaluación y la inflación, y, por ende, el Estado pierda su poder de interferir en la política monetaria, se crearía el incentivo para que el Estado prohíba las criptomonedas⁴⁵ y con ello se logre eliminar el peligro de perder su poder de intervenir en la economía.

⁴³ En junio del 2021, el peso argentino se devaluó el 53,3%; el real, moneda oficial de Brasil, presentó una devaluación del 11,4%, el peso mexicano se devaluó el 3,1%, el sol peruano tuvo una devaluación del 15,3%, Uruguay vio devaluar su moneda en un 11% y Colombia sufrió una devaluación del 7,4% (Di Stéfano, 2021).

⁴⁴ O con cualquier criptomoneda en general.

⁴⁵ Por ejemplo, en el primer semestre del 2021, el presidente turco, Recep Tayyip Erdogan, decidió destituir al gobernador del banco central, Naci Agbal, quien fuera un ministro de Finanzas muy bien valorado por

Por otro lado, teniendo en cuenta lo indicado por el ordenamiento jurídico colombiano a través de entidades como el Banco de la República, la Superintendencia Financiera, la Superintendencia de Sociedades y la Dirección de Impuestos y Aduanas, si bien las criptomonedas como el Bitcoin cumplen con las funciones propias del dinero, en Colombia no son dinero dado que no tienen curso legal, *contrario sensu*, las mismas son reconocidas como un activo intangible o un bien incorporal dado que indican que el Bitcoin es un bien que puede ser separado del tenedor, puede ser vendido o transferido de forma individual y no otorga al tenedor un derecho a recibir un número fijo o determinable de unidades monetarias. El Estado Colombiano no reconoce al Bitcoin como lo que realmente es porque quiere seguir teniendo el monopolio del dinero, lo cual no podrá hacer si reconoce al Bitcoin como dinero de curso legal.

Si en Colombia se reconociera al Bitcoin como dinero, el monopolio del mismo, que recae sobre el Estado, y sus mecanismos de expropiación como lo son la inflación se verían en graves riesgos. Como ya lo hemos mencionado, el control de la oferta del Bitcoin no recae en una entidad centralizada que la pueda manipular para beneficio propio, por el contrario, el aumento o estabilidad de la oferta de esta criptomoneda está supeditada a la prueba de trabajo que realicen los mineros que no necesariamente se conocen o confían entre sí.

los mercados (El País, 2021). Esta situación generó un alto grado de incertidumbre, lo que terminó en que la lira turca tuviera una devaluación superior al 16%. Esta situación hizo que la gente demandara Bitcoin como mecanismo para protegerse de la inflación y la devaluación de la moneda (El Confidencial, 2021). Poco después, las autoridades de Turquía decretaron la prohibición de utilizar el bitcoin como método de pago, ya fuera de bienes o servicios. Este veto se extendía a todas las criptomonedas y criptoactivos existentes (La República, 2021).

Referencias bibliográficas

- Ammous, S. (2018). *El patrón Bitcoin, la alternativa descentralizada a los bancos centrales*. Barcelona, España: Editorial Planeta.
- Amores, M. A. (2020). *Blockchain, algoritmos de consenso*. <http://openaccess.uoc.edu/webapps/o2/handle/10609/127926>
- Arango, C. A., Barrero, M. M., Bernal, J. F. y Boada, A. (2018). *Criptoactivos*. Bogotá D.C: Banco de la República. <https://www.banrep.gov.co/es/publicaciones/documento-tecnico-criptoactivos>.
- Banco de la República de Colombia. (2000, 05 de mayo). Resolución Externa No. 8 de 2000. *Por la cual se compendia y modifica el régimen de cambios internacionales*. <https://www2.deloitte.com/content/dam/Deloitte/co/Documents/legal/comercioexterior/Diciembre%202016/1.%20Resoluci%C3%B3n%20externa%208%20de%202000.%20Banco%20de%20la%20Rep%C3%BAblica%20.pdf>
- Banco de la República de Colombia. (2014, 1 de abril). *Comunicado Bitcoin* [Comunicado de prensa]. <https://www.banrep.gov.co/es/comunicado-01-04-2014>
- Banco de la República de Colombia. (2016, 30 de noviembre). Concepto JDS-25631. <https://www.banrep.gov.co/es/contenidos/concepto-jdbr/jds-25631>
- Banco de la República de Colombia. (2017, 18 de junio). Concepto JDS-14890. <https://www.banrep.gov.co/es/contenidos/concepto-jdbr/jds-14890>
- Banco de la República de Colombia. (2017, 22 de diciembre). Concepto JDS-27301. <https://www.banrep.gov.co/es/contenidos/concepto-jdbr/jds-27301>
- Banco de la República de Colombia. (2018, 25 de mayo). Resolución Externa No. 1 de 2018. *Por la cual se compendia y modifica el régimen de cambios internacionales*.

<https://incp.org.co/Site/publicaciones/info/archivos/Resolucion-Externa-No.-1-de-2018-28052018.pdf>

Banco de la República de Colombia. (2019, 21 de junio). Concepto JDS-CA-13581.

<https://www.banrep.gov.co/es/jds-ca-13581>

Banco de la República de Colombia. (2020, 23 de enero). Concepto C20-1115.

<https://www.banrep.gov.co/es/q20-1115>

Banco de la República de Colombia. (2020, 28 de diciembre). Concepto C20-162943.

<https://www.banrep.gov.co/es/c20-162943>

Banco de la República de Colombia. (s.f.). ¿Qué son las OMA?

<https://www.banrep.gov.co/es/contenidos/page/qu-son-las-oma>

Barroilhet, D. A. (2019). Criptomonedas, economía y derecho. *Revista chilena de derecho y tecnología*, 8(1), 29-67.

https://scielo.conicyt.cl/scielo.php?pid=S0719-25842019000100029&script=sci_arttext&tlng=en

Binance academy. (2020). ¿Qué es el Dinero Fíat? <https://academy.binance.com/es/articles/what-is-fiat-currency>

<https://academy.binance.com/es/articles/what-is-fiat-currency>

Bit2me academy. (2021). ¿Cómo saber la comisión de una transacción Bitcoin?

<https://academy.bit2me.com/como-saber-la-comision-de-una-transaccion-bitcoin/>

Bit2me academy. (2021). ¿Qué es la criptomoneda Ripple (XRP)?

<https://academy.bit2me.com/que-es-criptomoneda-xrp/>

Bit2me academy. (2021). ¿Qué es un hash? <https://academy.bit2me.com/que-es-hash/#:~:text=Un%20hash%20es%20el%20resultado,y%20tiene%20una%20amplia%20utilidad.>

<https://academy.bit2me.com/que-es-hash/#:~:text=Un%20hash%20es%20el%20resultado,y%20tiene%20una%20amplia%20utilidad.>

Bitcoin. (s.f.). Bitcoin para personas. <https://Bitcoin.org/es/Bitcoin-para-personas>

Blockchain. (2021). Total de Bitcoins que circulan. Recuperado de <https://www.blockchain.com/es/charts/total-bitcoins>

Boar, A. (2018). Descubriendo el Bitcoin: Cómo funciona, cómo comprar, invertir, desinvertir. Profit editorial.

https://books.google.es/books?hl=es&lr=&id=TtJSDwAAQBAJ&oi=fnd&pg=PT11&dq=bitcoin+que+es+y+como+funciona&ots=ebj9w9_Rcy&sig=qHHBa2JD61A7HOyGJ6Tr3oYmsrU#v=onepage&q=bitcoin%20que%20es%20y%20como%20funciona&f=false

Cárdenas, M. (2007). Introducción a la Economía colombiana. Bogotá: Alfaomega.

Castellanos, E. (2018). Blockchain y el tren de la innovación. *Revista Foro del Jurista*, 32, pp. 1-22. <https://www.camaramedellin.com.co/biblioteca/revista-foro-del-jurista-n176-33-econom237a-digital>

Coindesk. (2018). What is Bitcoin? <https://www.coindesk.com/information/what-is-Bitcoin>

Coindesk. (2021). ¿Qué es el hashrate y por qué importa? <https://www.coindesk.com/que-es-el-hashrate-y-por-que-importa>

Constitución Política de la República de Colombia [Const. P.]. (1991). Diario Oficial 51698 del 07 de junio de 2021. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Corredor, H. J. (2018). Blockchain y mercados financieros: aplicaciones en los mercados e impacto regulatorio para su implementación. *Revista Foro del Jurista*, 32, pp. 1-22. <https://www.camaramedellin.com.co/biblioteca/revista-foro-del-jurista-n176-33-econom237a-digital>

Criptoeconomía. (2020). Las billeteras Bitcoin (guía 2020 para principiantes).

<https://www.criptoeconomia.com/billeteras-bitcoin/>

Cuellar de Martínez, M. (1997). Competencias cambiarias, monetarias y crediticias del Banco de la República. En Velilla, M. (Ed.), Constitución económica Colombiana (pp. 293-298). Bogotá D.C.: El Navegante Editores.

Christidis, K. y Devetsikiotis, M. (2016). Blockchain and Smart Contracts for the Internet of Things. *IEEE*, 4, pp. 2292-2303.

<http://people.cs.pitt.edu/~mosse/courses/cs3720/blockchain-iot.pdf>

Di Stéfano, S. (2021). Cuánto se devaluaron las monedas de América Latina en pandemia. *Ámbito*.

<https://www.ambito.com/opiniones/deuda/cuanto-se-devaluaron-las-monedas-america-latina-pandemia-n5207629>

Dirección de Impuestos y Aduanas (DIAN). (2017, 2 de agosto). Concepto 20436. Impuesto sobre la renta.

https://www2.deloitte.com/content/dam/Deloitte/co/Documents/tax/DocumentosBoletinasesor/impuestoscorporativos/septiembre2017/cuartasemana/Concepto%20DIAN20436_17.pdf

EGA Futura. (2021). Criptoactivos. <https://www.egafutura.com/glosario/criptoactivos>

EL Bitcoin emerge como posible alternativa de la moneda "oficial" en Argentina. (2021, julio 9).

La República. <https://www.larepublica.co/globoeconomia/criptomoneda-bitcoin-emerge-como-posible-alternativa-de-moneda-oficial-en-argentina-3198619>

- Ely, R., Adams, T., Lorenz, M. & Young, A. (1917). *Outlines of economics* [esquemas de economía] (3.^a ed). The Macmillan Company.
<https://archive.org/details/outlinesofeconom00elyr/page/n7/mode/2up>
- Emet. (2019). *Explicando billeteras digitales frías y calientes*.
<https://emetenjoy.com/es/blog/billeteras-digitales-frias-calientes-explicacion?fbclid=IwAR0snnBoiJtcM0ZarWAoCucrd8QAK6n0kzEnsfLuHT64F13FXMJkAwdYdiM>
- Fekete, A. (1996). Whither gold? [a donde oro?].
<https://professorfekete.com/articles/AEFWhitherGold.pdf>
- Fondo Monetario Internacional. (2000). Manual de estadísticas monetarias y financiera.
<https://www.imf.org/external/pubs/ft/mfs/manual/esl/pdf/mfsmch6s.pdf>
- Forbes Advertorial. (2019). El mercado de derivados ¿Qué es y cómo funciona? *Forbes México*.
<https://www.forbes.com.mx/mercado-de-derivados-que-es-y-como-funciona/>
- Forbes Staff. (2021). La extraña tendencia entre Bitcoin y en dólar: ¿Qué está pasando? *Forbes Colombia*. <https://forbes.co/2021/04/28/economia-y-finanzas/la-extrana-tendencia-entre-bitcoin-y-el-dolar-que-esta-pasando/>
- Garcés, B. A. (1963). Dinero, moneda, otros medios comerciales de pago, diferencias jurídicas y económicas. *Revista Facultad de Derecho y Ciencias Políticas*, (37), p. 19-30.
<https://dialnet.unirioja.es/servlet/articulo?codigo=5212482>
- Gem Coin Bank. (2015). Conoce el valor del blockchain tecnología de futuro.
<https://www.youtube.com/watch?v=iVKX2bbg31o>

- Gómez, S. C., Castro, S., presidente, G., Malagón, J., Técnico, V., Montoya, G., & Sánchez, A. (2017). Blockchain: mirando más allá del Bitcoin. *Semana Económica*, 1084(6).
<https://miethereum.com/wp-content/uploads/2017/11/Blockchain-mirando-mas-alla-de-Bitcoin.pdf>
- Gómez, T. R. (2021). Atacantes roban USD 600 millones tras vulnerar protocolo DeFi Poly Network. *Criptonoticias*. <https://www.criptonoticias.com/seguridad-bitcoin/atacantes-roban-usd600-millones-vulnerar-protocolo-defi-poly-network/>
- Halaburda, Hanna y Miklos Sarvary (2016). *Beyond bitcoin: e economics of digital currencies*. Basinstoke: Palgrave Macmillan. <https://b-ok.lat/book/2806426/18929a?id=2806426&secret=18929a>
- He, D., K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakis-Saad, H. Oura, T. Saadi, N. Stetsenko, y C. Verdugo-Yepes (2016). *Virtual currencies and beyond: initial considerations*. Fondo Monetario Internacional discussion note SDN/16/03.
- Huerta de Soto. J. (2016). Dinero, crédito bancario y ciclos económicos. *Unión Editorial*.
<https://www.jesushuertadesoto.com/libros/libros-en-espanol/dinero-credito-bancario-y-ciclos-economicos/>
- Ittrends. (2017). *Blockchain, la tecnología con mayor potencial para redefinir el entorno digital*.
<https://www.ittrends.es/whitepapers/content-download/66882269-de85-4c84-bf83-139452a31539/especial-blockchain-ittrends.pdf>
- La lira turca llega a caer un 17% frente al dólar tras destituir Erdogan al jefe del banco central de Turquía. (2021, marzo 22). El País.<https://elpais.com/economia/2021-03-22/la-lira-turca>

cae-un-17-frente-al-dolar-tras-la-destitucion-del-jefe-del-banco-central-de-turquia-por-erdogan.html

Ley 31 de 1992. (1992, 29 de diciembre). Congreso de la República. Diario oficial No. 51698. http://www.secretariasenado.gov.co/senado/basedoc/ley_0031_1992.html

Ley 964 de 2005. (2005, 8 de julio). Congreso de la República. Diario oficial No. 51698. http://www.secretariasenado.gov.co/senado/basedoc/ley_0031_1992.html

Llorente, A. (2019, diciembre 26). Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen. *BBC News*. <https://www.bbc.com/mundo/noticias-50862657>

Malwarebytes. (2021). *Malware*. <https://es.malwarebytes.com/malware/>

Malwarebytes. (2021). *Suplantación de identidad (phishing)*. <https://es.malwarebytes.com/phishing/>

Merkle, R. (2016). *DAOs, Democracy and Governance*. Magazine, July- August, Vol 37:4, pp 28-40; Alcor, www.alcor.org. <https://alcor.org/cryonics/Cryonics2016-4.pdf#page=28>

Mi ethereum. (s.f.). La Blockchain. <https://www.miethereum.com/blockchain/>

MyChoice2Pay. (s.f.). ¿Qué es una e-wallet o una billetera electrónica? <https://www.mychoice2pay.com/es/blog/que-es-ewallet>

Nakamoto, S. (2008). «Bitcoin: A peer-to-peer electronic cash system Bitcoin: A Peer-to-Peer Electronic Cash System». Bitcoin.org. https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Navarro, B. Y. (2017). Blockchain y sus aplicaciones. <http://jeuazarru.com/wp-content/uploads/2017/11/Blockchain.pdf>

Palacios, Z. J., Vela, M. A. y Tarazona, G. M. (2015). Bitcoin como alternativa transversal de intercambio monetario en la economía digital. *Redes de ingeniería*, 6(1), 106-128. <https://revistas.udistrital.edu.co/index.php/REDES/article/view/8617/10531>

- Preuckschat, A. (2017). Los fundamentos de la tecnología blockchain. *BLOCKCHAIN: la revolución industrial de internet* (pp.7-26). Centro Libros PAPP, S. L. U. https://www.planetadelibros.cl/libros_contenido_extra/36/35615_Blockchain.pdf
- Rallo, J. R. (2015). *Contra la modern monetary theory*. Madrid, España: Unión Editorial S.A.
- Rallo, J. R. (2017). *Contra la Teoría Monetaria Moderna*. Bogotá, Colombia: Editorial Planeta Colombiana S.A.
- Rincon, C. E. (2018). Aspectos jurídicos de las criptomonedas. *Revista Foro del Jurista*, 32, pp. 1-22. <https://www.camaramedellin.com.co/biblioteca/revista-foro-del-jurista-n176-33-econom237a-digital>
- Rothbard, M. (1970). *Poder y mercado*. Leviatán. <https://juandemariana.org/investigacion/biblioteca-ijm/poder-y-mercado-el-gobierno-y-la-economia/>
- Rothbard, M. (1990). La Teoría Austriaca del Dinero. *Revista Libertas*, 13, 1-19. Recuperado de https://www.eseade.edu.ar/files/Libertas/32_2_Rothbard.pdf
- Rothbard, M. (2008). *¿Qué ha hecho el gobierno de nuestro dinero?* Ludwig Von Mises Institute. <https://mises.media.s3.amazonaws.com/Qu%C3%A9%20ha%20hecho%20el%20gobierno%20de%20nuestro%20dinero.pdf>
- Rothbard, M. (2009). *Man, Economy, and State with Power and Market* [El Hombre, La Economía y El Estado con Poder Y Mercado] (2.ª ed). Ludwig von Mises Institute.
- Rummel, R. (2017). *Death by government* [muerte por el gobierno]. Routledge.
- Sarmiento, J., Garcés. J. (2016). Criptodivisas en el entorno global y su incidencia en Colombia. *Revista Lebre*, 8, pp. 151 – 171.

Sentencia C-564/96. (1996, 24 de octubre). Corte Constitucional (Hernando Herrera, M,P).

<https://www.corteconstitucional.gov.co/relatoria/1996/C-564-96.htm#:~:text=La%20renta%20presuntiva%20constituye%20un,durante%20el%20respetivo%20per%C3%ADodo%20gravable.>

Superintendencia de Industria y Comercio. (s.f.). Sistema Internacional de Unidades.

<https://www.sic.gov.co/sistema-internacional-de-unidades#:~:text=En%20Colombia%2C%20el%20Sistema%20Internacional,la%20Ley%201512%20de%202012>

Superintendencia de Sociedades. (2020, 14 de diciembre). Oficio 100-237890. Criptoactivos – su utilización en actos de comercio – aporte en especie al capital de una sociedad.

https://www.supersociedades.gov.co/nuestra_entidad/normatividad/normatividad_conceptos_juridicos/OFICIO_100-237890_DE_2020.pdf

Superintendencia Financiera de Colombia. (2014). *Carta Circular 29 del 26 de marzo de 2014*.

[Riesgos de las operaciones realizadas con “Monedas Virtuales”]. Bogotá, D.C., Colombia.

Superintendencia Financiera de Colombia. (2016). *Carta Circular 78 del 16 de noviembre de 2016*.

[Operaciones realizadas con “Monedas Virtuales”]. Bogotá, D.C., Colombia.

Superintendencia Financiera de Colombia. (2017). *Carta Circular 52 del 22 de junio de 2017*.

[Riesgos potenciales asociados a las operaciones realizadas con “Monedas Electrónicas Criptomonedas o Monedas Virtuales”]. Bogotá, D.C., Colombia.

Szabo, N. (2002). *Shelling Out: The Origins of Money* [desembolso: los orígenes del dinero].

<https://nakamotoinstitute.org/shelling-out/>

Tapscott, D. y Tapscott, A. (2016). *Blockchain Revolution: How the Technology behind Bitcoin is changing Money, Business, and the World* [Revolución Blockchain: cómo la tecnología detrás de Bitcoin está cambiando el dinero, los negocios y el mundo]. New York: Pinguin Random House LLC.

Turquía prohíbe los pagos con criptomonedas debido a sus riesgos (2021, abril 16). El Confidencial. https://www.elconfidencial.com/economia/2021-04-16/turquia-prohibe-los-pagos-con-criptomonedas-debido-a-sus-riesgos_3037560/

Un nuevo robo millonario golpea al bitcoin. (2019, mayo 8). LA VANGUARDIA. <https://www.lavanguardia.com/economia/20190508/462125249330/bitcoin-robo-binance-criptomonedas.html>

Zurita, G. J., Martínez, P. J. y Rodríguez, M. F. (2009). La crisis financiera y económica del 2008. Origen y consecuencias en los Estados Unidos y México. *El Cotidiano*, (157), 17-27. ISSN: 0186-1840. <https://www.redalyc.org/pdf/325/32512739003.pdf>