



Capítulo 3 - Bitcoin

Narcisa Medranda Morales
Miguel Arcos Argudo

SciELO Books / SciELO Livros / SciELO Libros

MEDRANDA MORALES, N., and ARCOS AGUDO, M. Bitcoin. In: *Blockchain, criptoactivos y metaverso*. Una aproximación teórica [online]. Quito: Editorial Abya-Yala, 2023, pp. 63-84. ISBN: 978-997-810-802-4. Available from: https://books.scielo.org/id/pb8tf. https://doi.org/10.17163/abyaups.6



All the contents of this work, except where otherwise noted, is licensed under a Creative Commons Attribution 4.0 International license.

Todo o conteúdo deste trabalho, exceto quando houver ressalva, é publicado sob a licença Creative Commons Atribição 4.0.

Todo el contenido de esta obra, excepto donde se indique lo contrario, está bajo licencia de la licencia Creative Commons Reconocimento 4.0.

Capítulo 3

Bitcoin

Funcionamiento y características

Su creación se ubica en 2008, cuando bajo el seudónimo de Satoshi Nakamoto se hace público su propuesta y diseño. El 3 de enero de 2009 se creó el *bloque génesis* (primer bloque de *bitcoin*). El *bitcoin* es la primera criptomoneda que por su naturaleza virtual y su base en la tecnología *blockchain* cuenta entre sus características que pueden pasar por alto las restricciones locales para realizar transferencias internacionales por transmitirse directamente a la red *peer-to-pe*er sin la participación de intermediarios (bancos o instituciones centralizadas), menores costos de transacción y con un sistema de validación de pagos descentralizado (Nakamoto, 2008; Fernández *et al.*, 2021; Binance Academy, 2020d; López Gómez-Cadiñanos, 2021).

Figura 13
Logotipo de Bitcoin



Nota: Tomado de http://bit.ly/3mpLNAn

Recordando que en ese momento se presentó la crisis financiera de los grandes bancos en Estados Unidos, se propuso como respuesta a las necesidades de seguridad y garantía de las transacciones virtuales, en virtud del alto riesgo que tienen las partes debido a las probabilidades de fraude en el cual su institución de confianza (sistema financiero internacional) no asumiría la totalidad de la pérdida. Además, en el documento oficial de creación del *bitcoin* se asegura que más que una institución de confianza se requieren servidores con sellos que generen pruebas computacionales de las transacciones que protejan al vendedor y comprador (Nakamoto, 2008).

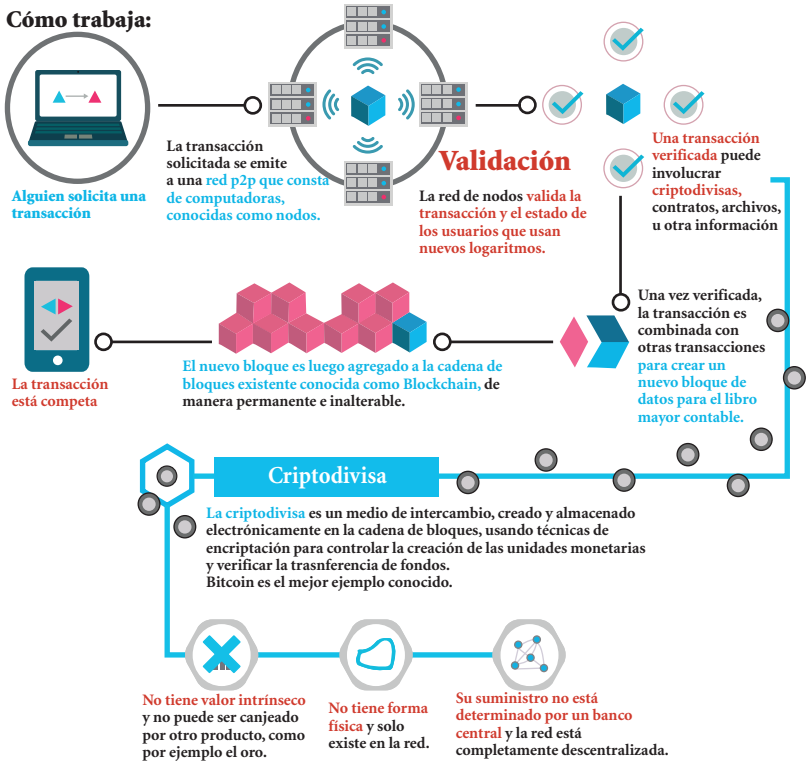
El *bitcoin* es considerado como el primer criptoactivo y conserva la característica de no ser confiscable, así como de no ser censurable.

El *bitcoin* tiene una oferta finita de 21 millones de unidades, las cuales se crean a través de la minería asociada a la verificación y validación de las operaciones, su inclusión en el bloque, hasta su incorporación a la *blockchain,* proceso que está programado para que tenga una duración de aproximadamente 10 minutos. Tal validación se realiza a través de algoritmos de consenso PoW. Al culminar exitosamente, se genera la llamada recompensa de bloque (*block reward*) que constituye la forma de generar *Bitcoins* y las comisiones de las transacciones realizadas (figura 14) (Nakamoto, 2008; Fernández *et al.*, 2021; Binance Academy, 2020d; López Gómez-Cadiñanos, 2021).

La validación a través del sistema de prueba de trabajo (PoW), requiere que los mineros realicen actividades de verificación y añadan bloques de información, para lo que es necesaria la resolución de logaritmos matemáticos de alta complejidad, haciendo falta solo el conocimiento sino de capacidad financiera para contar con los equipos adecuados, cubrir el alto gasto energético y mantener la seguridad del sistema las 24 horas del día. Este modelo de PoW contribuye a la seguridad y validez del sistema; sin embargo, produce una alta ineficiencia en el uso de los recursos y un entorno hostil tomando en cuenta que la recompensa solamente la obtiene el minero que logre efectivamente

incluir el bloque en la cadena (Parra *et al.*, 2019; Fernández *et al.*, 2021; Binance Academy, 2020d).

Figura 14
Proceso de minado de bitcoin



Nota: Tomado de Tecno Global Solution (2020).

De manera resumida, una prueba de trabajo funciona de la siguiente manera: cuando un nodo de la red desea ejecutar una transacción con *bitcoins*, lo debe comunicar a todos los demás ordenadores conectados a la red. Cada uno de los computadores que recibe la ins-

trucción debe verificar la validez de la transacción, para lo cual debe cumplir con todas las reglas acordadas por todos los participantes. El resultado también debe ser comunicado a todos los nodos de la red. Este proceso se repite de manera indefinida con el objetivo de que la totalidad de la información sobre las transacciones sea difundida a todos los integrantes de la red.

Vale la pena mencionar que dentro de la red de bitcoin se pueden distinguir dos tipos de nodos:

- Nodos completos: contienen toda la información histórica de todas las transacciones ejecutadas en la red.
- Nodos mineros: son nodos completos pero que además tienen la capacidad de introducir bloques nuevos en la red de *bitcoin*.

Según diversos autores (Fernández *et al.*, 2021: Bolaños *et al.*, 2019; Romo Conde, 2021; Binance Academy, 2018a, 2020d), entre algunas de las características de la prueba de trabajo destacan:

- Funcionalidad: requiere de hardware dotado de alta capacidad de computacional para la resolución de los algoritmos y resguardo de la *blockchain*.
- Criptoactivo propio: *BTC*.
- Mecanismo de generación de bloques: se basa en una red P2P, distribuida, con algoritmo PoW.
- Cantidad máxima: cuenta con una cantidad máxima fija de 21 millones, con generación decreciente a la mitad cada 210 000 bloques.
- Velocidad de las transacciones: los bloques se procesan cada 10 minutos.

Valor del *bitcoin*

Según Ciaian *et al.* (2018), los factores que ha influido en el precio del *bitcoin* son la oferta y demanda del mercado, el interés de los inversionistas, la influencia en el desarrollo de los mercados macrofinancieros en

el mundo y los vínculos que ha ganado con la economía de bienes físicos en la medida que los minoristas empezaron a aceptarla como una forma de pago, aunque no todos usan el mismo método (Pieters y Vivanco, 2017).

El precio del *bitcoin* es un producto de la especulación, junto con las fuerzas de oferta y demanda del mercado; los cuales generan un indicador atractivo para los inversionistas, donde la interacción con el mercado global aumenta la incertidumbre en virtud de la ausencia de respaldo de valor que efectivamente su confianza y disminuya los riesgos de la inversión (Ciaian *et al.,* 2016).

Así, el valor del *bitcoin* está asociado al precio de mercado, marcado por la subjetividad y la especulación, lo que explica su volatilidad. Binance Academy (2021d) señala algunos factores en los cuales se basa este valor:

- Utilidad: se refiere a los beneficios que se derivan de su capacidad para transferir de forma rápida grandes cantidades de valor en todo el mundo, sin requerir de intermediarios. Las comisiones pudieran considerarse grandes cuando se trata de operaciones por montos pequeños.
- Descentralización: debido a la tecnología *blockchain* y su código abierto.
- Distribución: la participación de muchas personas mejora la seguridad de la red, en la medida que se conecten más nodos a la red, más valor tendrá.
- Confianza: la tecnología de *bitcoin* ha demostrado ser muy confiable y segura. Además, su código fuente es abierto y su algoritmo de consenso *Proof of Work* es un mecanismo transparente, verificable y comprobable por sí mismo.
- Escasez: existe un suministro limitado de 21 millones de BTC.
- Seguridad: los ataques maliciosos a la red *bitcoin* requieren contar con la participación de más del 51 % de la potencia minera actual, lo que hace de coordinación a escala mundial sea casi imposible de lograr. De allí que la probabilidad de un ataque exitoso es extremadamente baja y, en caso de ocurrir, duraría muy poco tiempo.

- Reserva de valor: está ganando reputación como alternativa moderna de reserva de valor.

Un aspecto resaltado por Ciaian *et al.* (2016) es la importancia del valor de la información en la formación de precios del *bitcoin*, en virtud de que se trata de un determinante de las decisiones de compra o venta de los participantes y de la volatilidad de su precio. Al momento de su creación, el precio del *bitcoin* era de $0,03/1BTC aproximadamente y a lo largo del año 2010 su precio más alto registrado fue de $0,39. Más reciente, alcanzó su máxima cotización el 07 de noviembre de 2021 al llegar a los $67 549,14 por unidad y su mínima de $ 29 795,55 el 10 de julio de 2021, registrando para el 12 de febrero de 2022 un valor de $ 42 353,74 (figura 15).

Figura 15
Valor del bitcoin (periodo: 2013-2023) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/bitcoin/

Tipos de *bitcoins*

Luego del lanzamiento de la criptomoneda en 2009, se han generado nuevas versiones de *bitcoin* como respuesta de la comunidad a las limitaciones en cuanto a la demanda y el incremento masivo de las transacciones que han sobrepasado el rendimiento de la red, produciendo demoras en el procesamiento de las transacciones y el aumento de las comisiones. Como consecuencia se han producido bifurcaciones, dando lugar al *bitcoin cash* en primera instancia y *bitcoin gold* unos meses después (Domínguez y García, 2018).

- *Bitcoin* (*BTC*): criptomoneda original que da origen a todas las divisas virtuales posteriores.
- *Bitcoin cash* (*BCH*): criptomoneda creada en 2017 a partir del bitcoin con la finalidad de acelerar la velocidad de las transacciones. Desde su salida a los mercados, ha venido cotizando al alza.
- *Bitcoin Gold* (*BTG*): nace en 2017 a partir de otra división más en los bloques de la *blockchain* de *bitcoin*, con el objetivo de mejorar los rendimientos económicos del sistema de recompensas y liberar la red de las grandes compañías que están influyendo de forma negativa en el curso de la moneda.

También se desarrolló la *Lighthing Network* como solución a la escalabilidad, siendo una solución de "capa dos" alejando las transacciones de la *blockchain*, en lugar de registrar todas las transacciones en la *capa base*, se realizan a través de otro protocolo incorporado encima que les permite a los usuarios enviar fondos casi al instante y de forma gratuita, sin restricciones en el rendimiento (Binance Academy, 2020a).

Opciones para la obtención del *bitcoin*

Cuando un usuario desea adquirir criptomonedas, la manera de obtenerlas a través de internet y deben almacenarse en un monedero virtual, aunque ya existe en algunos países la opción de materializarlos en cajeros

automáticos (López Gómez-Cadiñanos, 2021; Binance Academy, 2020d). En general, se cuenta con tres posibilidades para obtenerlas, a saber:

- Minería: los *bitcoins* se obtienen como recompensa, una vez que se logra validar e incorporar un bloque a la cadena, tal como se ha detallado anteriormente.
- Compra: la forma más utilizada es a través de las plataformas *exchange*, las cuales a su vez sirven de monedero digital. No requiere otros intermediarios para concretar las operaciones, por lo que sus costos son mínimos. En tales plataformas es posible comprar, vender o intercambiar criptomonedas. Se pueden comprar con monedas de circulación legal y pagar con tarjeta de crédito o débito, o con otras monedas virtuales.
- Salario en divisas electrónicas: existen empresas en algunos países que pagan el salario de sus empleados en criptomonedas, utilizando el *bitcoin* como referencia.

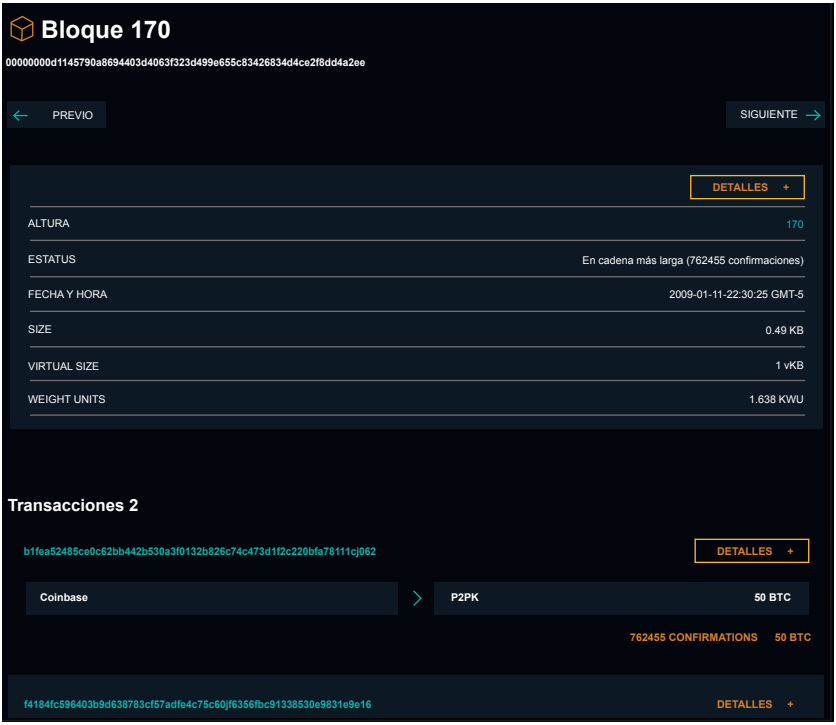
Funcionamiento del *bitcoin*

Como se ha mencionado ya en varias ocasiones, *bitcoin* consiste en una cadena de bloques que se almacena en una base de datos descentralizada; esto requiere que todos los ordenadores que conforman la red trabajen de manera colaborativa y sincronizada, de tal manera que la información almacenada en cada uno de ellos sea una réplica exacta de la información que tienen almacenada los demás ordenadores. Esto se logra mediante un software de código abierto que cada nodo de la red debe ejecutar; este programa realiza la tarea de validar que cada uno de los bloques cumplan con las reglas acordadas por los mineros. En principio, cualquier usuario de un computador puede descargar dicho software e instalarlo para formar parte de la red. De esta manera, todos los miembros de la red validan todos los bloques que transitan por ella, con ello se establece que una transacción es válida o no, si algún nodo de la red no está conforme con el resultado no se da por legítima la validación, caso contrario, cuando todos los nodos validan satisfactoriamente

un bloque se determina a la transacción como legítima; este proceso se conoce como "consenso". Debido a este funcionamiento se dice que este sistema es incorruptible.

Cada transacción puede entenderse como una transferencia electrónica de bitcoins de un usuario A hacia un usuario B. El primer movimiento de esta criptomoneda la realizó Satashi Nakamoto el 11 de enero de 2009, quien transfirió diez *bitcoins* a Hal Finney, lo cual se puede verificar mediante la página https://blockstream.info/ en la figura 16.

Figura 16
Resultado de la transacción realizada utilizando el bloque 170 de la blockchain de bitcoin



Nota: Tomado de https://blockstream.info/

Pero el *bitcoin* no tenía un valor económico dentro del mercado, a pesar de ello, el 22 de mayo de 2010 un profesional informático llamado Laszlo Hanyecs fue el primero en intercambiar *bitcoins* por un producto real, compró dos pizzas a cambio de 10 mil BTC. Si se realizara esta misma compra con el precio actual del *bitcoin* se podría decir que Hanyecs compró las pizzas más caras de la historia.

Sin embargo, no fue sino hasta el 5 de octubre de 2010 que se realizara la primera transacción de compra-venta dándole al *bitcoin* un valor económico de aproximadamente $0.000764 dólares americanos. En aquella ocasión se vendieron 1309 BTC por un dólar estadounidense. El valor máximo histórico que *bitcoin* ha alcanzado fue de aproximadamente $65 000 dólares americanos en noviembre de 2021 (ver figura 17).

Figura 17
Valores históricos del bitcoin en el mercado



Nota. Tomado de https://coinmarketcap.com/currencies/bitcoin/

Existen entonces razones suficientes para considerar que el *bitcoin* fue el primer activo de carácter digital, pues a diferencia de otro tipo

de archivos digitales, las cadenas de bloques de *bitcoin* no pueden ser replicadas digitalmente, siempre tendrán un único dueño y el sistema es prácticamente incorruptible. Para ello la tecnología *bitcoin* utiliza un sistema de criptografía asimétrica (o criptografía de clave pública), el cual consiste en la utilización de dos claves diferentes, una para encriptar el contenido y la otra para desencriptarlo. Una persona, para demostrar que es el auténtico dueño de cierta cantidad de *bitcoins* y transferirla a otra persona, encripta el contenido de su mensaje con su clave privada (es importante que ningún otro usuario tenga acceso a esta clave aparte del dueño) y comparte su clave púbica con todos los demás miembros de la red; de esta manera, cualquier usuario puede confirmar la autenticidad de la clave privada del dueño, pero no podrá modificar el mensaje debido a que para ello necesitaría la clave privada. Las claves públicas también son utilizadas para crear direcciones a las cuales una persona puede recibir *bitcoins*, pero hay que tener presente que el proceso no es reversible, es decir, es imposible determinar una clave pública a partir de una dirección creada con dicha clave.

Ventajas y desventajas del *bitcoin*

Entre sus ventajas, Fernández *et al.* (2021) destacan el hecho de que esta es una criptomoneda y solo se ocupa de transacciones, su buena reputación y su amplia aceptación como medio de pago. Entre las desventajas se encuentran la volatilidad de su precio, los elevados costos de la actividad de minería en cuanto a requerimientos de inversión en *hardware*, la cartelización de mineros dado que la extracción en solitario se hace imposible y solo unas pocas agrupaciones de bits controlan la cadena de bloques, el tiempo de las transacciones (10 min.), la competencia hostil entre los participantes y su innegable ineficiencia debido el elevado consumo de energía con su consecuente impacto medioambiental. Adicionalmente, existen otros riesgos debido a la posibilidad de perder la clave privada de acceso, ya que no existe manera de recuperarla y, en consecuencia, no se puede recuperar los montos correspondientes.

Billeteras o monederos digitales

Una billetera o un monedero (o *wallet* en inglés) "es una herramienta que puedes usar para interactuar con una red *blockchain*" (Binance Academy, 2019b), la cual consiste fundamentalmente en un programa informático que permite el acceso a diferentes cadenas de bloques, de tal forma que se pueda visualizar el balance de la cuenta, así como enviar y recibir dinero. Cada billetera contiene solo las claves públicas y privadas de cada usuario, que le permiten tener acceso a las cadenas de bloques donde las criptomonedas se encuentran "almacenadas" (Leal, 2022).

Funcionamiento de las billeteras digitales

Las billeteras "pueden generar la información necesaria para enviar y recibir criptomonedas a través de transacciones en *blockchain*" (Binance Academy, 2019b), que contiene de uno o más pares de claves públicas y privadas. Además, incluye una dirección, la cual es un identificador alfanumérico generado a partir de las claves pública y privada. Esta dirección es una "ubicación" específica en la cadena de bloques donde se pueden enviar las monedas. Por lo tanto, puedes compartir la dirección con las otras personas con la finalidad de recibir fondos y, en ningún caso, la clave privada. La clave privada otorga acceso a las criptomonedas, sin importar la billetera utilizada.

Tipos de billeteras digitales

Es posible clasificar las billeteras digitales de acuerdo con diferentes criterios, entre los que se pueden mencionar: cantidad de criptomonedas que puede manejar (una o varias), con custodia o sin custodia, tipo de dispositivo utilizado (apps móviles, desktop/software descargable, online, hardware, tarjetas/papel, otros) o conexión a internet, entre otros (Parra *et al.,* 2019; Binance Academy, 2019b, 2020d, 2021d, 2021e). En este punto se presentan los tipos de billeteras digitales según su conexión a internet, a saber:

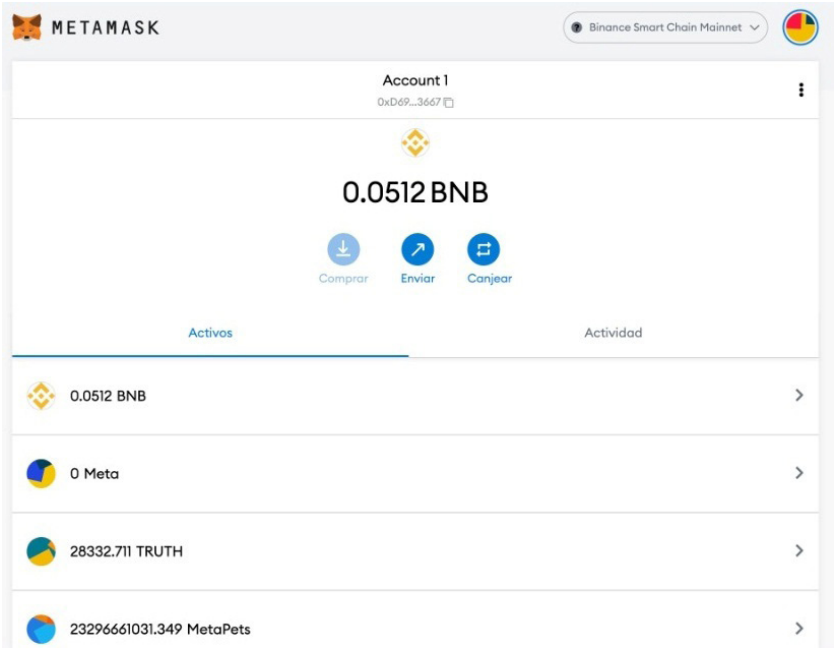
- Billeteras o monederos calientes (*hot wallets*): constituye un *software*, el cual se conecta a internet. Por lo general, es una app móvil o de ordenador de escritorio, a través del cual es posible enviar y recibir monedas. Suelen ser convenientes para realizar pagos, aunque tienen mayor vulnerabilidad ante ataques maliciosos. Como ejemplo de estos monederos se encuentra Trust Wallet y Binance.
- Billeteras o monederos fríos (*cold wallets*): este tipo de monedero no se encuentra expuesta a internet; por lo tanto, son menos susceptibles de ser objeto de ataques maliciosos. Utilizan un medio físico con el fin de almacenar las claves, manteniéndolas fuera del entorno digital, con lo cual son menos vulnerables. Sin embargo, esta misma característica, hace que su utilización sea un poco más engorrosa, pero más recomendable para quienes desean conservar inversiones de largo plazo. Entre estas se cuentan las billeteras de hardware o las de papel.

Billeteras digitales más utilizadas

A continuación se presentan algunas de las billeteras digitales más utilizadas:

- *MetaMask:* fue desarrollada en 2016 por *ConsenSys*. Se trata de una extensión de navegador y una criptobilletera de tipo aplicación móvil compatible con diversas *blockchain* como *Ethereum*, *Polygon*, *Binance Smart Chain (BSC)* y *Binance Chain* (figura 18) (Bit2me Academy, s.f.).
  La extensión de navegador de *MetaMask* permite realizar transacciones e interactuar con contratos inteligentes y aplicaciones descentralizadas (*DApps*) (Binance Academy, 2021f). Esta última brinda a los usuarios acceso seguro a distintos servicios y se pueden utilizar en computadores personales, teléfonos inteligentes o vía *web* (Bit2me Academy, s.f.). También permite la conexión a diferentes *blockchain*, firmar transacciones, gestionar claves públicas y privadas, y cuenta con un servicio de intercambios (*swaps*) que brinda los mejores precios de múltiples *exchanges* descentralizados.

Figura 18
MetaMask



Nota: Tomado de *MetaMask*, https://metamask.io/

- *Trust Wallet:* es una billetera móvil de código abierto disponible para iOS y Android. Es la billetera descentralizada oficial de Binance, y compatible con los ecosistemas *blockchain* de *Ethereum*, *BSC*, *Binance Chain*, entre otros. En ella, el usuario cuenta con acceso completo a sus claves privadas mediante una "frase semilla". La aplicación presenta algunas funcionalidades extra incorporadas, como la compra de criptomonedas a través de tarjeta de crédito o débito, y una billetera para *tokens* no fungibles (NFTs). Además, la versión Android dispone de un navegador para *DApps* (Binance Academy, 2021f). *Trust Wallet* tiene un *token* de tipo "*utility*" y de

gobernanza, llamado *TWT*, el cual permite participar en la toma de decisiones como añadir soporte para nuevas *blockchains* e integrar nuevos *tokens*, y también obtener descuentos en el *DEX* y en la compra de criptomonedas (Binance Academy, 2021e).

- *MathWallet:* es una billetera de criptomonedas de tipo extensión de navegador, y una *app* móvil para dispositivos iOS y Android, compatible con casi 40 *blockchains* diferentes. Fundada por MATH Global Foundation en 2017, ofrece la flexibilidad suficiente para utilizar la misma billetera en distintos dispositivos. Según las necesidades de los usuarios, resulta fácil moverse entre el dispositivo móvil, la extensión del navegador y la billetera de base web (Binance Academy, 2021f).
- *Binance Chain Wallet:* es la billetera de tipo extensión de navegador oficial de Binance, compatible con *Binance Chain, BSC* y *Ethereum* (figura 19). Cuenta con una función *Wallet Direct,* la cual es utilidad para usuarios que tienen criptomonedas en el *exchange* de *Binance*, pero ocasionalmente usan *DApps* (Binance Academy, 2021e).
- *SafePal*: se trata de un proveedor de billetera hardware que también ofrece una billetera móvil descentralizada de tipo app. Con una funcionalidad similar a la de *Trust Wallet*, ofrece adicionalmente una sección de finanzas descentralizadas que tiene enlaces a otras plataformas y *DApps* similares, así como un navegador. También cuenta con un *token* de tipo "*utility*", denominado *SFP*, para descuentos y bonificaciones (Binance Academy, 2021f).

Transacciones con criptomonedas

De acuerdo con Parra *et al.* (2019), el proceso de compra de criptoactivos para un usuario común requiere que previamente configure una billetera o monedero digital y abra una cuenta en una plataforma de intercambio. En caso de ser un nuevo usuario en el sistema de criptoactivos, debe adquirirlos a otro usuario vez en la plataforma seleccionada mediante una transferencia electrónica o tarjeta de crédito. Los precios de compra y venta de *bitcoin* incluirán el margen establecido por la pla-

taforma de intercambio, la cual también puede cobrar comisiones por los pagos recibidos y enviados. A través de la tecnología *Blockchain* se verifica y registra la transacción de forma distribuida, en la billetera digita de cada usuario tendrá la información de sus *bitcoins*.

Según Armstrong (2018, citado por Parra *et al.,* 2019), la conexión de las plataformas de intercambio con el sistema financiero hace que estas tiendan a centralizar la estructura del sistema de criptoactivos mientras la adopción de las criptomonedas se masifica. En opinión de Böhme *et al.* (2015), las billeteras digitales propician la centralización de la información de los usuarios como consecuencia de las facilidades que ofrecen para el mantenimiento y utilización de los criptoactivos.

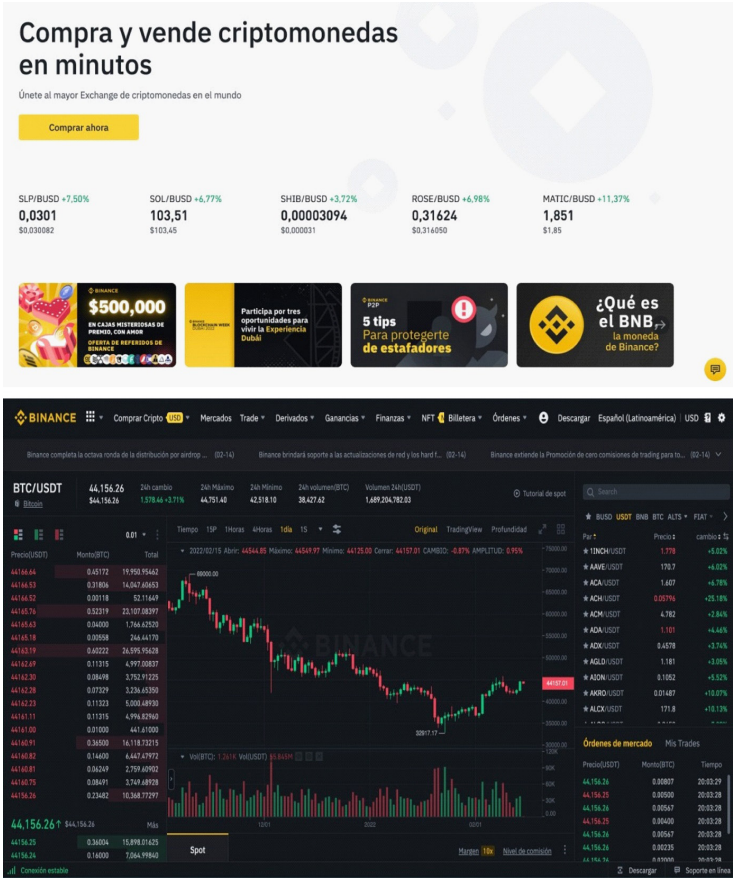
También es posible comprarlas en efectivo entregando físicamente el dinero a otro usuario, quien intercambiará las criptomonedas a través de su monedero digital o adquiriéndolas a través de un cajero electrónico disponible en algunos países. Cuando los usuarios cuentan con criptoactivos, tienen la posibilidad de realizar transacciones para cambiarlos por otras criptomonedas o *tokens*, utilizarlas como medio de pago, a través de una billetera digital.

Las criptomonedas han avanzado como forma de pago cuya aceptación ha avanzado paulatinamente. Sin embargo, existen múltiples temas pendientes cuya tendencia pudiera afectar los principios mismos en los que se sustentan. Aspectos como la red distribuida y el seudonimato pueden verse afectadas en la medida que se requieren mayores inversiones en equipos costosos con la suficiente potencia computacional para poder almacenar las bases de datos y procesar rápidamente las transacciones que le permitan a los nodos lograr rendimientos suficientes para recuperar lo invertido, llevando a una merma del número de usuarios en función de su capacidad financiera. Esto hace pensar en la concentración de los nodos en menos manos, aumentando la posibilidad de ataques del 51 %.

La extrema volatilidad de sus precios, susceptibles a situaciones como la opinión de algunas personalidades, instituciones o gobiernos acerca de ellas, es un tema sobre el cual se han hecho algunos esfuerzos aún

insuficientes. La ausencia de terceros para la ejecución de las transacciones es otro tema que está entrando en contradicción. Las billeteras digitales están asumiendo un rol similar a los bancos tradicionales, de custodia e intermediación financiera, el cual es una de las razones principales que dio origen a las criptomonedas.

Figura 19
Binance Chain Wallet



Nota: Tomado de *Binance*. https://binance.com/es

Entendiendo que aún falta mucho por desarrollarse, existen temas importantes sobre los cuales alertar: la ineficiencia excesiva en cuanto a la utilización de los recursos, fraude, lavado de dinero y financiamiento de actividades terroristas, solo por nombrar algunos.

Regulación sobre la tecnología blockchain *en algunos países*

Las aplicaciones de la tecnología *blockchain*, en particular, el *bitcoin*, no tiene una regulación universal que pueda ser aplicada en todos los países, sin embargo, algunos de ellos han aplicado ciertas políticas sobre este nuevo tipo de moneda. A continuación, se citan algunos ejemplos que han sido extraídos de un documento publicado por la Pontificia Universidad Javeriana (s.f.) en el que se aprecia algunos hitos y datos de diferentes países que han tomado la batuta en este tipo de normas y también sobre aquellos que han prohibido el uso de criptoactivos.

Suiza

Su organismo FINMA (Autoridad Supervisora del Mercado Financiero) en 2018 se convirtió en una de las pioneras entidades del mundo en emitir una norma que regula de manera específica al uso de los criptoactivos, reconociendo tres tipos de tokens: *payment tokens* (tokens de pago), *utility tokens* (tokens de utilidad) y *asset token* (títulos valores en blockchain).

Estados Unidos

No ha emitido una política oficial sobre el uso de criptoactivos, pero algunas instancias del gobierno han adoptado los lineamientos de entidades internacionales; no obstante, esto también ha implicado una desorganización provocada por la diversidad de criterios de dichas entidades, por ejemplo: la CFTC (Comisión de Negociación de Futuros de Commodities) considera a los criptoactivos como material tangible que se pueden negociar, la SEC (Comisión de Valores) los define como títulos de valores, la FinCEN (Agencia de Cumplimiento de Delitos Financieros)

los define como dinero, mientras que el Estado de Wyoming considera que los criptoactivos son una propiedad privada.

Malta

Este país es conocido como la "isla blockchain", sobrenombre ganado por la clara regulación que ha adoptado para la regulación de criptoactivos, a través de su Ley de Autoridad de Innovación Digital, Ley de Servicios y Arreglos Tecnológicos Innovadores y su Ley de Activos Financieros Virtuales.

Alemania

Cuenta con una norma que regula el servicio de custodia de criptoactivos, vigente desde el 1 de enero de 2020. Como consecuencia, cualquier entidad financiera o no financiera que ofrezca este servicio lo podrá hacer previa autorización de la BaFin (Autoridad Federal de Supervisión Financiera).

Unión Europea

Hasta marzo de 2020 estuvo recibiendo aportes sobre un documento que especifica algunos aspectos relativos a los criptoactivos, tales como: emisión, intercambio, acceso y transferencia, así como delitos inherentes a esta temática: fraude, ciberataques y manipulación malintencionada.

Catar

Con el fin de precautelar delitos relacionados al lavado de activos y financiamiento de actividades terroristas, este país desde el 2020 prohibió toda actividad relacionada a las criptomonedas; sin embargo, dicha prohibición no considera a los *security tokens*, razón por la cual su uso sería legal.

China

Su gobierno ha estado buscando y probando aplicaciones de la tecnología *Blockchain*, sin embargo, no tienen una regulación específica para ello.

Nueva Zelanda

En 2019, Nueva Zelanda legalizó el pago de los salarios en criptomonedas, algo inédito a nivel mundial. La norma establece que el pago se debe realizar en una criptomoneda que sea fácilmente intercambiable por dinero *fiat* (dinero en efectivo).

España

Su organismo CNMV (Comisión Nacional del Mercado de Valores) ha determinado que la regulación establecida por la Ley de Mercado de Valores debe ser aplicada a los criptoactivos, sean estos *security tokens* o tokens de utilidad. Este criterio se encuentra en constante revisión dada la naturaleza de los criptoactivos.

Colombia

Se encuentra trabajando una ley desde el año 2019 cuyo objetivo principal es "definir los aspectos generales de la operación y funcionamiento de los prestadores de servicios de intercambios de criptoactivos".

Argentina

No dispone de regulación específica, pero su Comisión Nacional de Valores ha manifestado que algunos tokens pueden ser considerados como títulos de valores y aplicaría la regulación existente.

Chile

En 2019 presentó un proyecto de ley que regularía temas relacionados a criptomonedas. Según el Ministro de Hacienda de aquel entonces "la regulación aplicará requerimientos de manera proporcional, regulando según el tipo de servicio prestado y los riesgos que este implica para los usuarios y para el mercado financiero".

Bolivia

Prohibió de forma expresa el uso de criptomoneda mediante un decreto vigente desde el 6 de mayo de 2014.

Brasil

No hay acuerdos ni pronunciamientos oficiales por parte del gobierno sobre esta temática. Han existido posiciones contrarias entre las entidades gubernamentales y la dirigencia del Banco Central de Brasil.

Ecuador

El uso de criptomonedas para realizar actividades de comercio está prohibido desde enero de 2018 mediante un escrito emitido por el Banco Central del Ecuador en el que textualmente dice "el uso de criptomonedas o medios digitales que se utilizan para invertir y realizar transacciones a través de internet no está autorizado en el país". No obstante, las aplicaciones tipo *wallet* funcionan sin inconvenientes.

México

Es de los pocos países latinoamericanos que han decidido regular de alguna manera el uso y comercialización utilizando criptoactivos y tecnología *Blockchain*. Dentro de su Ley Fintech consta una sección dedicada a las criptmonedas reconociéndolas como activos digitales. Según la publicación de la Pontificia Universidad Javeriana dentro de esta temática están involucradas las siguientes entidades mexicanas: Banco de México, la Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores.

Perú

Cuenta con procesos regulatorios sobre el dinero electrónico, pero estos no hablan de manera puntal sobre las criptomonedas, por lo tanto, no son reconocidas como divisas legales. A pesar de ello, su uso no está

expresamente prohibido. Algunas instancias gubernamentales han experimentado con procesos basados en tecnología *Blockchain.*

Venezuela

En 2017 inició un proceso de registro y certificación obligatoria de los usuarios que se dedicaban a la minería de criptomonedas. Con este antecedente, en 2018 el gobierno de turno creó dos entidades importantes: por un lado, la Superintendencia Nacional de Criptoactivos y Actividades Conexas que estaría encargada de regular todos los temas conexos relacionados a los criptoactivos, y por otro lado la Tesorería de Criptoactivos de Venezuela que regularía la emisión, custodia, recaudo y distribución de criptoactivos.