¿Qué es esa cosa llamada cripto?

¡Aprende fácil sobre criptomonedas!

Daniela Rivera García
Juan Guillermo Rivera Berrío

RED educativa digital descartes

¿Qué es esa cosa llamada cripto?

¡Aprende fácil sobre criptomonedas!

Daniela Rivera García

Juan Guillermo Rivera Berrío

INSTITUCIÓN UNIVERSITARIA
COLEGIO MAYOR
DE ANTIOQUIA

Fondo Editorial RED Descartes

Córdoba (España)
2023

Título de la obra:
¿Qué es esa cosa llamada cripto?
¡Aprende fácil sobre criptomonedas!

Autores:
Daniela Rivera García
Juan Guillermo Rivera Berrío

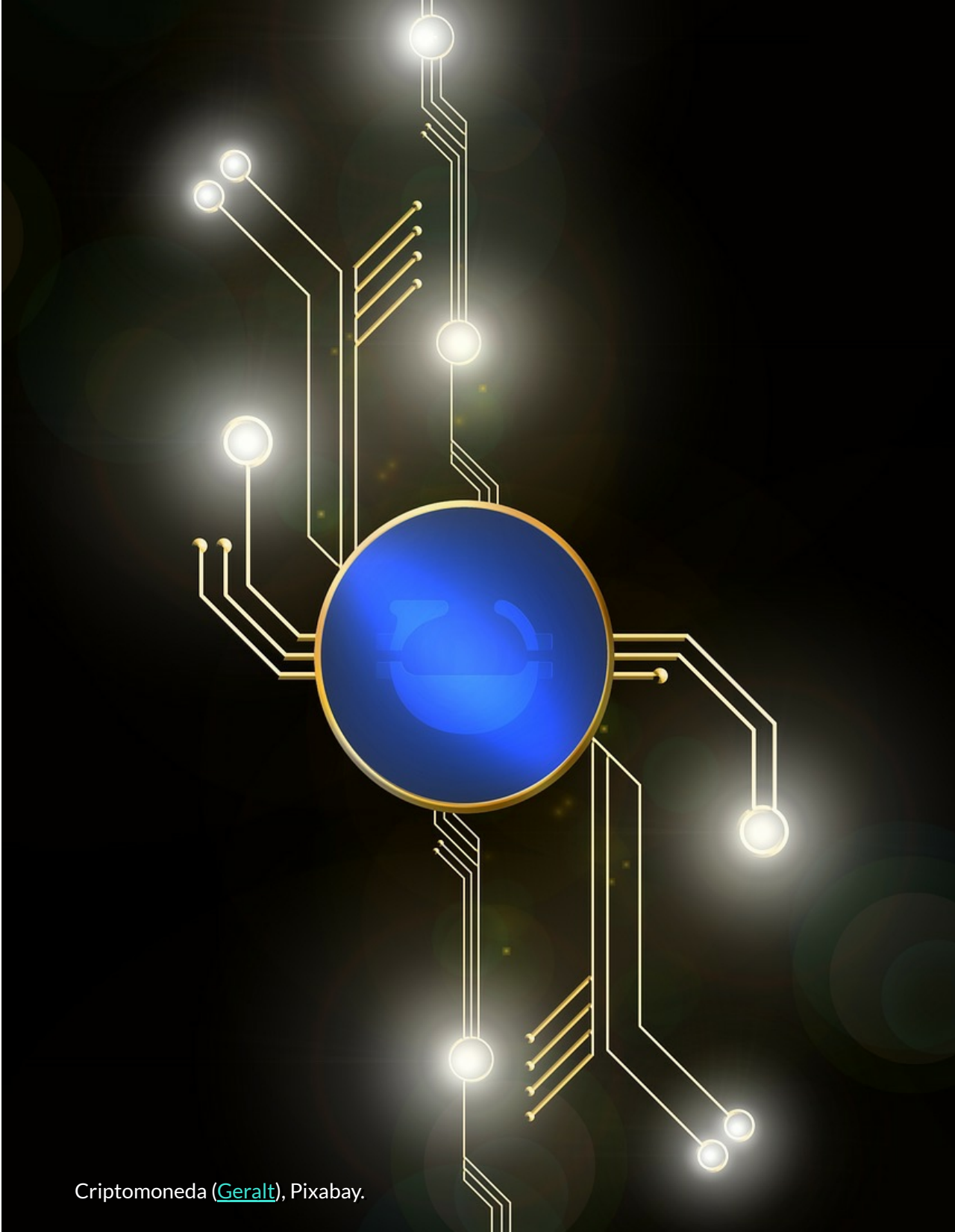
Código JavaScript para el libro: Joel Espinosa Longi, IMATE, UNAM.
Recursos interactivos: DescartesJS
Fuentes: Lato y UbuntuMono
Imagen portada: Criptomoneda, Lingote de oro y Concepto, imagen de WorldSpectrum, en Pixabay.
Núcleo del libro interactivo: septiembre 2023

Red Educativa Digital Descartes
Córdoba (España)
descartes@proyectodescartes.org
https://proyectodescartes.org

Proyecto iCartesiLibri
https://proyectodescartes.org/iCartesiLibri/index.htm
https://prometeo.matem.unam.mx/recursos/VariosNiveles/iCartesiLibri/

ISBN: 978-84-18834-72-1

Tabla de contenido



Criptomoneda (Geralt), Pixabay.

Prefacio

Estamos seguros que has escuchado sobre las criptomonedas, ¿te gustaría aprender sobre ellas?, ¿Sí?, entonces lee este libro e interactúa con las diferentes actividades propuestas. El diseño del libro ha contado con la ayuda de algunas inteligencias artificiales; por ejemplo, ChatGPT nos dice que:

Las criptomonedas son un tipo de moneda digital que utilizan la criptografía para garantizar la seguridad de las transacciones y para controlar la creación de nuevas unidades. Estas monedas son descentralizadas, lo que significa que no están controladas por ningún gobierno ni institución financiera centralizada.

El **Bitcoin** es la criptomoneda más conocida y valiosa. Fue creada en 2009 por una persona o grupo de personas bajo el seudónimo de **Satoshi Nakamoto**. Desde entonces, ha experimentado un crecimiento exponencial en su valor, con altibajos en el camino.

Además del Bitcoin, hay muchas otras criptomonedas en el mercado, algunas de las cuales tienen una capitalización de mercado significativa, como **Ethereum, Binance Coin, Cardano, Dogecoin**, y **Litecoin**. Cada criptomoneda tiene su propia comunidad de seguidores y su propia tecnología subyacente.

El uso de criptomonedas se ha expandido mucho en los últimos años, y ahora se pueden usar para una variedad de propósitos, desde transacciones de compraventa hasta inversiones y

transferencias internacionales de fondos. Algunas empresas incluso han comenzado a aceptar criptomonedas como forma de pago.

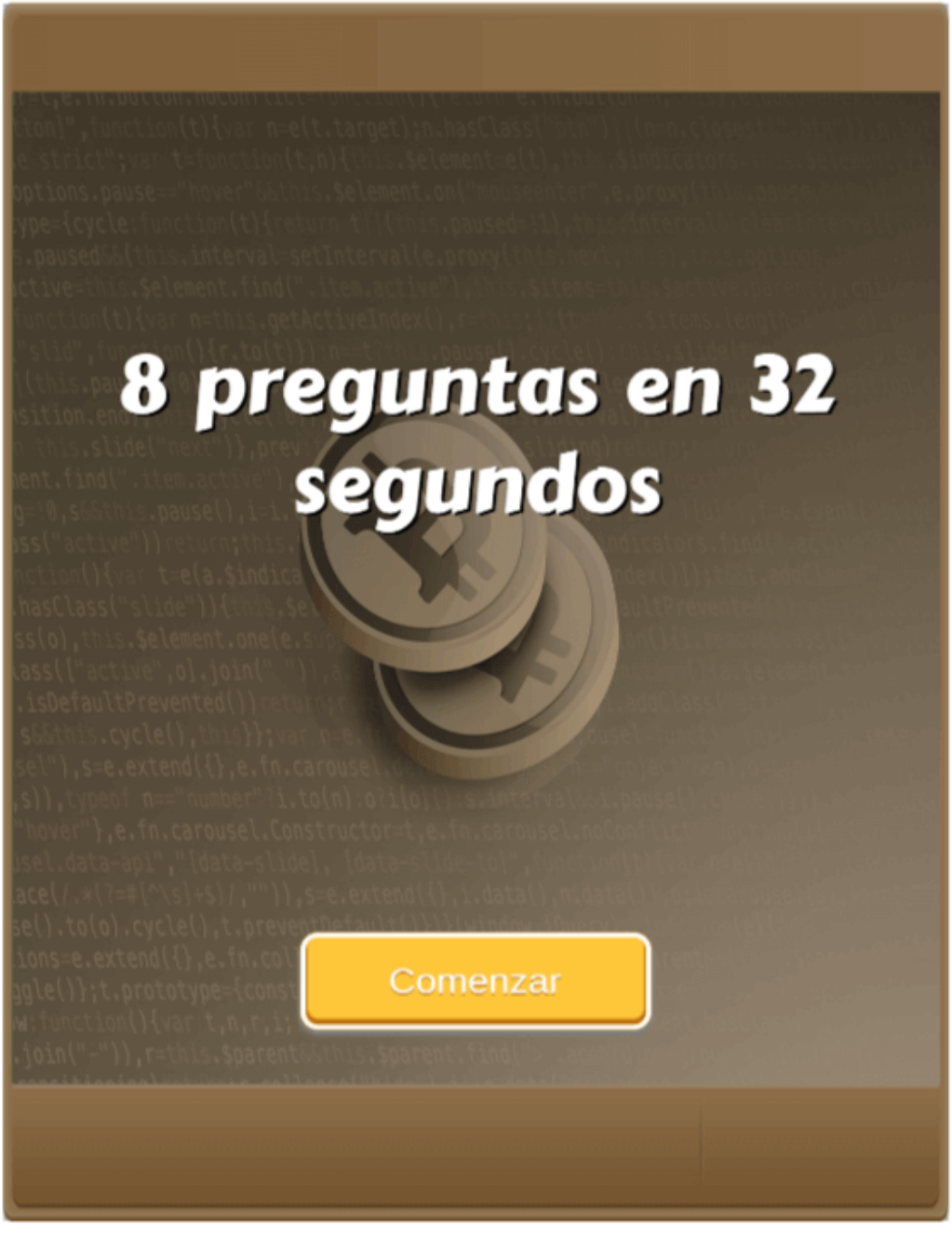
Es importante tener en cuenta que el mercado de criptomonedas es altamente volátil y que el valor de las criptomonedas puede fluctuar significativamente en un corto período de tiempo. También hay riesgos asociados con la seguridad de las billeteras digitales y la posibilidad de fraudes y estafas. Sin embargo, con la creciente aceptación y uso de las criptomonedas, es importante comprender lo que son y cómo funcionan.

Estas son las referencias utilizadas por ChatGPT:

- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de https://bitcoin.org/bitcoin.pdf
- CoinMarketCap. (2021). Cryptocurrency Market Capitalizations. Recuperado de https://coinmarketcap.com/
- Blockchain.com. (2021). What is Bitcoin? Recuperado de https://www.blockchain.com/bitcoin
- Coinbase. (2021). What is cryptocurrency? Recuperado de https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency

¡Advertencia!

Este libro no recomienda invertir en criptomonedas, si lo hace es bajo su propio riesgo. El propósito del libro es informar sobre las criptomonedas.



Actividad evaluativa 1. Criptomonedas.

Contenido multimedia

Para ilustrar mejor la información suministrada en este libro, hemos incluido, entre otros elementos multimedia, los siguientes:

- **Texto**. Además de la gran cantidad de artículos científicos y de divulgación, publicados en la web, los textos de este libro se soportan en información encontrada en sitios como Coin Market Cap, Crypto Miners, The News Crypto, Cointelegraph, coinbase, bit2me Academy, Investopedia, Binance, Ethereum, Marketwatch, We use coins, Wikipedia, HandWiki, y las inteligencias artificiales ChatGPT, Microsoft Bing, YOU.com, Perplexity y Rytr.

  Para el primer capítulo, hemos puesto parte del texto del libro *Historia del dinero* de Manuel Gozalbes, con autorización del autor.

- **Imágenes**. Los iconos de las listas, se han obtenido de Freepik - Flaticon. Por otra parte, la mayoría de imágenes se han obtenido de Pixabay y Pexels.

- **Videos**. Algunos videos, relacionados con las criptomonedas, son tomados de YouTube con licencia creative commons. Otros videos son solo ilustrativos, tales como los obtenidos en Pexels o en Pixabay, como el video que se muestra en la siguiente página, alusivo a la minería criptomonedas.

- **Objetos interactivos**. Todos los objetos interactivos, fueron diseñados con el editor DescartesJS, los cuales incluyen presentadores interactivos, puzle o actividades de evaluación.

Cuando tienes dinero, solo tú recuerdas quién eres. Pero cuando no tienes dinero, todo el mundo olvida quién eres. Así es la vida. (Bill Gates)

Mis cosas favoritas de la vida no cuestan dinero. Está claro que el recurso más preciado que tenemos es el tiempo. (Steve Jobs)

Capítulo 1

Historia del dinero

Monedas romanas de plata de la denominación conocida como denario (*plural denarii*) Wikimedia, CC BY-SA 2.0.

Imagen de esta página: Monedas contemporáneas Lisa Fotios, Pexels.

Historia del dinero

Fuente: "Historia del dinero" de Manuel Gozalbes [1]

1.1 Introducción

Manuel Gozalbes es un destacado investigador de la numismática y ha dedicado gran parte de su carrera a estudiar la historia del dinero. En su libro "La historia del dinero", Gozalbes ofrece una detallada exploración de la evolución de la moneda a lo largo del tiempo, desde los tiempos antiguos hasta el mundo digital actual. El libro se centra principalmente en la moneda como un reflejo de la cultura, la política y la economía en diferentes partes del mundo. Gozalbes proporciona una amplia información histórica y cultural y presenta los tipos de moneda que se han utilizado en diferentes épocas y regiones del mundo.

La asociación del concepto dinero con monedas, billetes o tarjetas de crédito es inmediata. Son las formas más conocidas, sin embargo existen muchos otros materiales y objetos que se han empleado con idéntica función a lo largo de la historia en los cinco continentes y que no resultan tan conocidos. La ordenación de estos formatos a partir de su materia prima permite descubrir tanto paralelos como singularidades entre diferentes culturas a lo largo de la historia. Desde esta perspectiva material, los protagonistas indiscutibles han sido los metales desde su aparición, complementados durante los últimos siglos por los formatos en papel. Ambos han cedido terreno en las últimas décadas a un crecimiento imparable de los pagos

electrónicos, donde el dinero se convierte en algo intangible que cambia de manos con el simple concurso de números y claves, dejando facturas, recibos o comprobantes como única evidencia tangible de las transacciones.

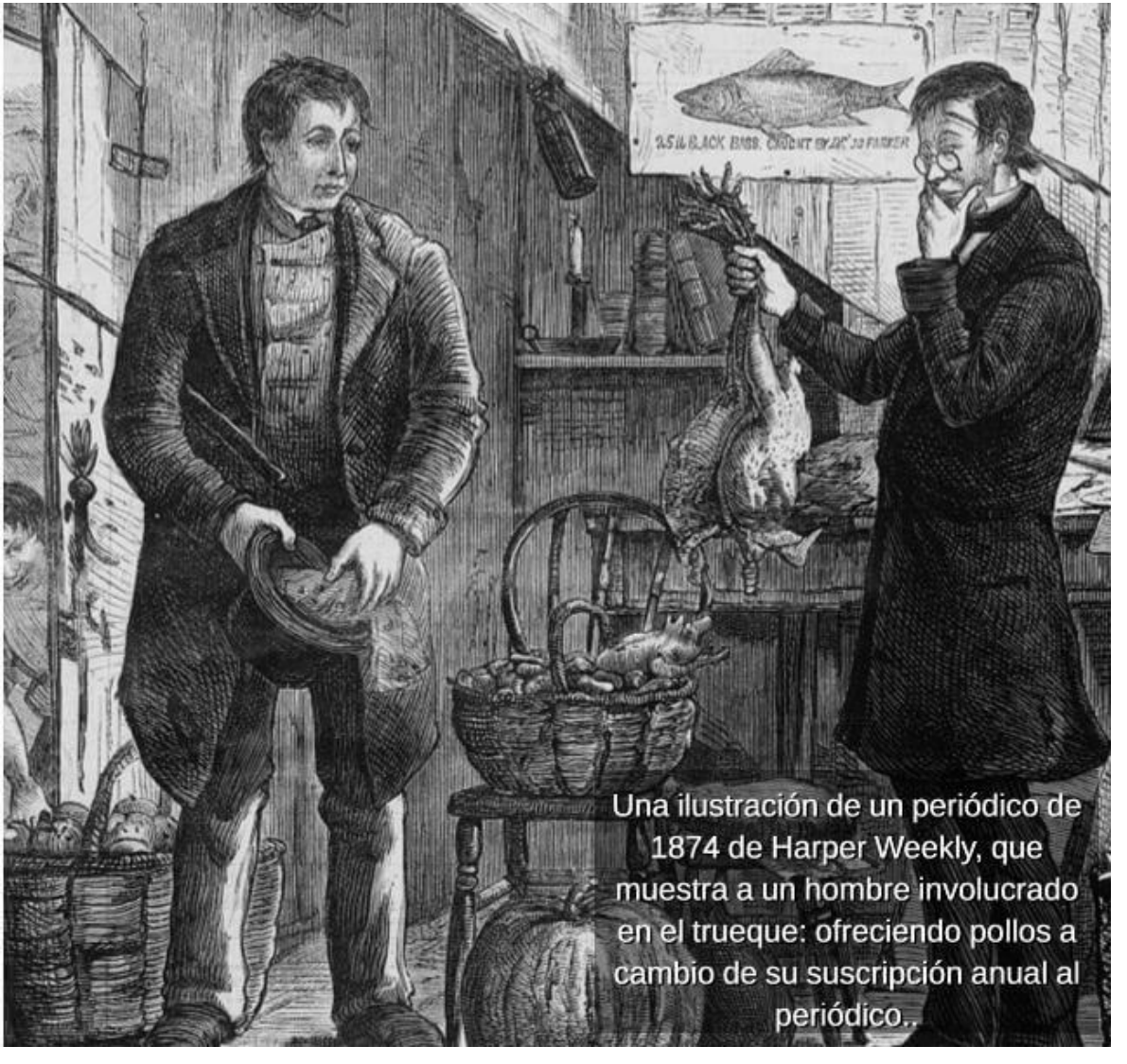
1.2 El dinero

Antes de que apareciera el dinero, algunas mercancías se intercambiaban por medio del trueque, método que continúa empleándose de forma recurrente cuando las circunstancias invitan a ello. Sus posibilidades son evidentes, pero también lo son sus limitaciones. Con la aparición del dinero se solucionaron parte de estos problemas, aunque también se crearon otros nuevos. Tres son las características esenciales del dinero. La más evidente es su utilidad como medio de pago de bienes y servicios, en operaciones mediante las que se transfiere cualquiera de sus formas tangibles. Otras funciones son sus propiedades como medio para acumular riqueza y su gran utilidad como medida de valor. Pero una historia del dinero quedaría incompleta sin referir también algunos de los objetos que tradicionalmente han acompañado a su gestión, como huchas, cajas de seguridad, cajas registradoras, o instituciones como los bancos, protagonistas en su gestión desde finales del siglo xix.

1.2.1 El trueque

Los intercambios de mercancías basados en el consenso de los participantes se denominan trueque. En ellos no existe un precio y no es posible distinguir entre comprador y vendedor, tal y como ya señalaba el Digesto romano. Sus limitaciones son que las partes han de tener interés recíproco en los productos ofrecidos y que deben alcanzar un acuerdo sobre su valor de cambio. Diferentes materiales gozaron de un aprecio general durante la Prehistoria, siendo objeto de intercambios frecuentes. Entre todos ellos, los metales

evolucionaron más tarde hacia formatos estandarizados, convirtiéndose en monedas. Las sociedades que utilizan dinero recurren en ocasiones al trueque cuando aporta una utilidad inmediata bajo circunstancias particulares o extraordinarias.



Interactivo 1.1. Trueque
Haz clic sobre la imagen (Imágenes de Wikimedia commons).

1.2.2 Formas de dinero

Los objetos que sirven para pagar bienes y servicios se denominan dinero. Son útiles como medida de valor, como reserva de riqueza y se encuentran respaldados por la autoridad o por un consenso social. A lo largo de la historia han existido numerosos productos y materiales que han sido utilizados con estos fines en diferentes lugares. Aunque sus características no siempre coinciden, generalmente deben ser objetos cuantificables, transportables, homogéneos, conocidos e intercambiables. A pesar de la gran diversidad de formatos que han existido, monedas, billetes y tarjetas son los medios de pago más comunes en la actualidad.

Interactivo 1.2. Formas dinero (Imágenes de Wikimedia commons).

1.2.3 Los metales

Poseen unas cualidades inmejorables para ser empleados como dinero. Con su producción controlada a partir de un suministro limitado comienzan unas ventajas que incluyen su importante cualidad de ser reciclables. Las virtudes relativas a su uso se resumen en que proporcionan formas de dinero cuantificables, transferibles, manejables y muy duraderas. La clave del éxito de las monedas reside precisamente en su carácter metálico.

1.2.3.1 Plata

Las monedas de plata son propias de las tradiciones occidental e islámica. Minas importantes como Laurion o Potosí, permitieron realizar vastas emisiones en la Atenas clásica o la España de los Austrias. El denario fue una antigua denominación romana de plata acuñada aproximadamente entre 268 a. C. y 360. Su valor inicial equivalía a diez ases, de ahí su nombre y su símbolo X.

Figura 1.1. Trajano, 98-117 d.C. Denario (Grupo Numismático Clásico, Inc., CC BY-SA 2.5).

De la palabra latina *denario*, se deriva la palabra dinero

Figura 1.2. Julio César. Febrero-marzo del 44 a. Denario (Grupo Numismático Clásico, Inc., CC BY-SA 2.5).

1.2.3.2 Oro

La escasez, belleza, maleabilidad y resistencia del oro lo han convertido en el metal más valioso de cuantos existen. A lo largo de la historia su valor oficial ha sido aproximadamente entre 12 y 15 veces superior al de la plata.

Figura 1.3. Dinar de oro del sultán mameluco Lajin acuñado en El Cairo en 1297-1299 (Sociedad Numismática Americana, CC0 1.0).

Un ejemplo es el dinar que tiene su origen en la antigua moneda araboislámica de oro que se empezó a acuñar a finales del siglo VII. La palabra "dinar" (دينار en árabe y en persa) tiene el mismo origen que el vocablo dinero, ya que deriva del denario romano.

1.2.3.3 Cobre y bronce

El cobre y el bronce han desempeñado en los sistemas monetarios un carácter iduciario,condicionado por el crédito y la confianza que mereciesen, siempre con un valor facial muy superior al real. Ocasionalmente, como en Roma durante los siglos iv-iii a.C. o en la Suecia del siglo xviii, circuló en grandes piezas con un valor equivalente a su contenido metálico.

Figura 1.4. Una cruz de Katanga, también llamada handa en los idiomas de la zona, es una cruz de cobre fundido que se usó como moneda en partes de lo que hoy es la República Democrática del Congo durante el siglo XIX y principios del XX, aunque se ha podido atestiguar su uso desde el siglo XIII y especialmente a partir del siglo XVI con la llegada de los exploradores portugueses (Grupo Wikipedia).

La tajadera de cobre era otra forma de moneda que circulaba en el centro de México, partes de América Central y también América del Sur. También conocida como moneda-hacha o moneda-azada azteca.

1.2.4 Los formatos en papel

Ofrecen muchas posibilidades de diseño, son muy manejables y resultan poco costosos de fabricar. Permiten incluir textos a mano o impresos que detallan importes, nombres, fechas y condiciones de uso, admitiendo incluso su individualización mediante números de serie. El empleo de algunos de estos formatos ha decrecido en las últimas décadas por la generali- zación de las transacciones electrónicas. En Europa los primeros billetes de banco aparecieron en Suecia en el siglo XVII.

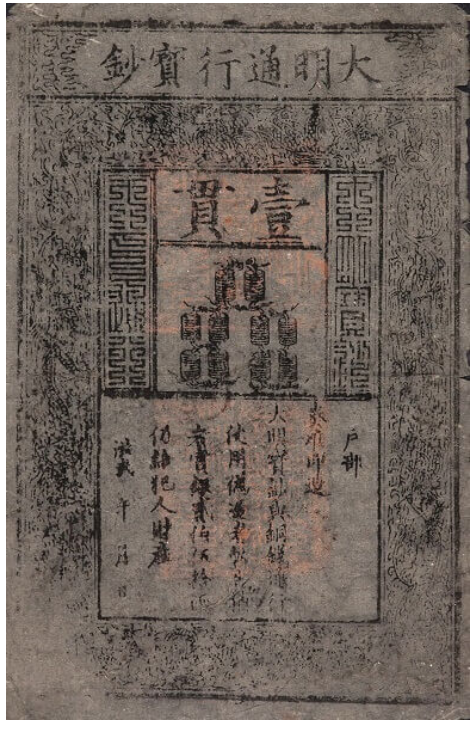


Figura 1.5. Billete denominado en "una cadena de monedas en efectivo" (Guàn) de la dinastía Ming (The Treasury of the Ming Dynast, dominio público).

El billete chino de la dinastía Ming es el más antiguo que se conserva. Se fabricó con papel de morera, equivalía a 1.000 monedas de cobre y sus textos señalan castigos para los falsificadores.

Se denomina papel moneda o billete al trozo de papel impreso que representa un valor fiduciario. Sustituye a la moneda metálica, que, especialmente en grandes cantidades, resulta más incómoda de llevar siempre en la mano o bolsillo. En España, se consideran papel moneda: al billete (de banco), al vale real, a la obligación al portador, al certificado provisional, al certificado de plata y a algunos documentos semejantes.

Interactivo 1.3. Papel moneda (Imágenes de Wikimedia commons).

- Los billetes son el formato en papel más importante. Su emisión la realizan generalmente los estados y resultan de gran utilidad para el pago de sumas elevadas, aunque necesitan de la precisión complementaria de las monedas (Alemania, 1923).
- Los cheques permiten transferir al instante cualquier cantidad de dinero (Estados Unidos, 1915).
- La particularidad de los pagarés reside en que constituyen un compromiso de pago diferido (España, 1930).
- Las obligaciones o bonos son una promesa de pago con interés fijo como forma de participación en una deuda (Londres, 1852).

- Las acciones son participaciones de valor variable en la propiedad de una empresa (Estados Unidos, 1982).
- Las letras de cambio se crearon en el siglo XIV, permitiendo el envío de dinero a distancia sin correr riesgos. Son órdenes de pago diferidas en la que media un girado entre el emisor y el beneficiario (Tortosa, 1806).
- Los cheques de viaje funcionan como sustituto del dinero en efectivo, tienen un importe fijo y deben firmarse tras la comprobación de la identidad del titular (Londres, 1978).
- Un giro postal permite enviar dinero a distancia disponiendo simplemente de un nombre y una dirección (Gran Bretaña, 1950).

1.2.5 Bancos

En el siglo XIX los bancos asumieron y ampliaron las funciones realizadas desde la Antigüedad por los cambistas. Su instalación en locales permanentes cambió definitivamente el modo en que los particulares podían salvaguardar y gestionar su dinero.

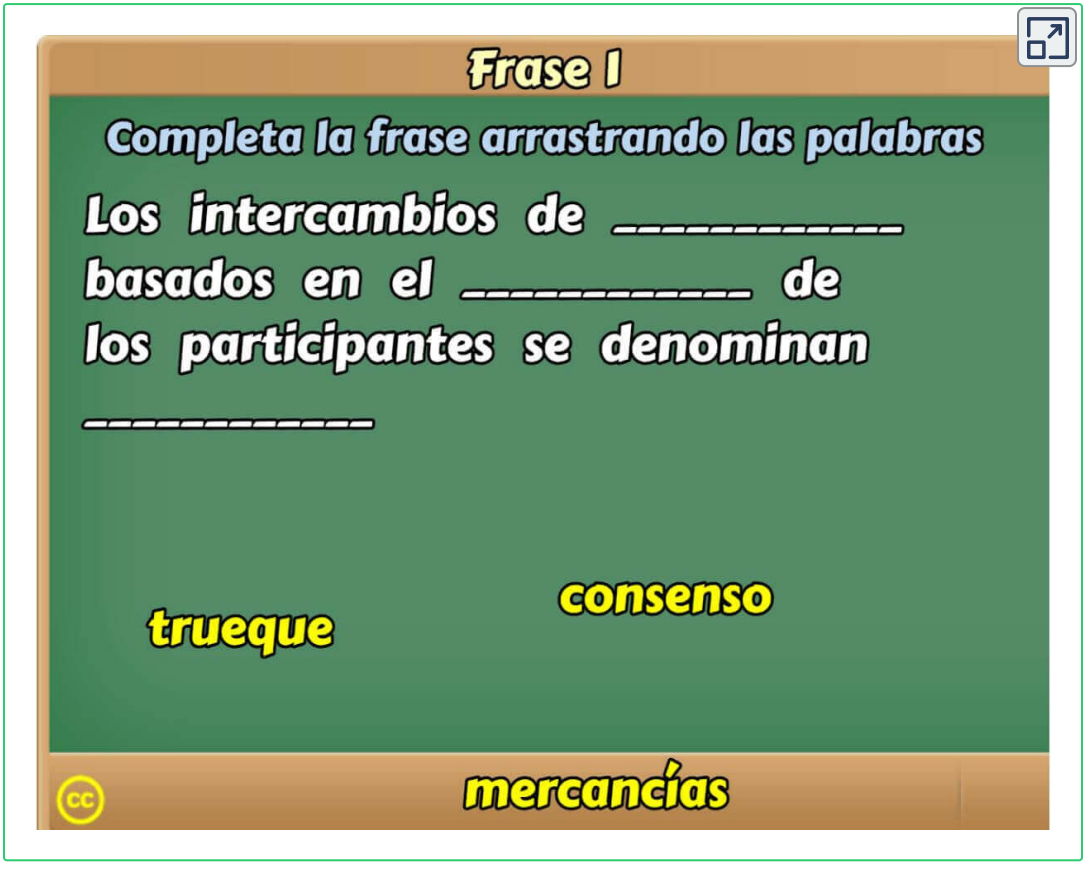
Caja de caudales. Se usan para guardar dinero y documentos importantes. Los modelos con cerradura triple obligaban a que tres personas concurriesen simultáneamente para su apertura, logrando de esta manera un acceso más controlado a su contenido.

Caja registradora. Se ha convertido en un objeto cotidiano, resultando imprescindibles para la gestión de la mayoría de comercios actuales. Su gran utilidad deriva de las amplias posibilidades que ofrecen para el cálculo comercial. Fueron inventadas por James Ritty en Estados Unidos en el año 1879.

¡Haz clic sobre la siguiente imagen para ver otras fotos!

Sede del Banco Mundial en Washington D. C.

En la siguiente escena interactiva, vas a encontrar seis frases presentadas en este apartado. Tu tarea es armarlas sin cometer errores.



Actividad evaluativa 1.1. Completa frases relacionadas con el dinero.

No pienses que el dinero lo hace todo o acabarás haciéndolo todo por el dinero. (Voltaire)

1.3 Orígenes de la moneda

Las monedas son la forma de dinero mas importante de la historia. Griegos y chinos se percataron de forma independiente y prácticamente simultánea, hacia el siglo VII a.C., de que el dinero podía adoptar la forma de unidades estandarizadas de metal con una indicación de autoridad. Los griegos acuñaron monedas en metales preciosos, mientras que los chinos fabricaron exclusivamente monedas fundidas de bronce. Desde ambos lugares se expandieron, dominando por completo los circuitos económicos hasta la incorporación de los billetes y de las tarjetas en época contemporánea. Las ventajas que estas pequeñas piezas metálicas proporcionaban para el desarrollo de transacciones cotidianas no han sido superadas hasta la actualidad por ningún otro formato. Únicamente, la consolidación del papel moneda retiró definitivamente a los metales preciosos de la circulación, dando carta de naturaleza a sistemas exclusivamente fiduciarios en los que la emisión de dinero ya no dependía de una riqueza objetiva en reservas de oro o plata, sino de una decisión política de fabricación.

La historia de las monedas puede analizarse desde múltiples perspectivas, incluyendo aspectos tan diversos como la metrología, los sistemas monetarios, la política, las autoridades, los diseños o el fenómeno de las falsificaciones. Todo ello se relaciona con monedas griegas de arte excepcional, con las emisiones ibéricas que iniciaron la monetización de la Península, con las piezas romanas que consolidaron definitivamente la economía monetaria en el Mediterráneo occidental o con una gran variedad de piezas medievales, modernas y contemporáneas que narran multitud de aspectos esenciales de nuestra historia. Ponderales, libros y documentos, junto a objetos relacionados con la fabricación en diferentes épocas y lugares contribuyen a hacer más comprensible la historia de las monedas.

Con el desarrollo del comercio se fue consolidando una nueva etapa, la del dinero metálico, la cual se puede dividir en tres grandes sub-etapas [2] :

La moneda pesada: apareció en Egipto, dos mil años antes de nuestra era, bajo la forma de lingotes que se pesaban en el momento de cada transacción.

La moneda-cuenta: se creó unos 800 años antes de nuestra era, cuando los lingotes fueron divididos en piezas, innovación que se generaliza en Grecia, Roma, China, la India y el mundo islámico.

La moneda acuñada: son las monedas metálicas en que se fue acuñando una inscripción que indicaba el peso de la pieza; el valor de la pieza en unidades de cuenta se fijó según su peso en metal.

Las monedas, aparecidas en la costa griega de Asia Menor a finales del siglo VII a.C. y en China entre los siglos VII y III a.C., constituyen la forma de dinero más extendida históricamente. Son piezas metálicas, generalmente discoidales, con la imagen, peso y calidad establecidas por la autoridad emisora. Su concepción tuvo lugar de forma independiente en Grecia, China y, posiblemente, la India.

1.3.1 Grecia

Los griegos facilitaron los pagos con metales preciosos al crear monedas de `electro` (aleación de oro y plata) con peso estándar y marcas de autoridad que garantizaban su valor. Se iniciaba así la técnica de acuñación de moneda a martillo que sobreviviría hasta la Edad Moderna.

Crearon la moneda en las costas de la actual Turquía en el siglo VII a.C., desde donde pasó a Grecia continental, la Magna Grecia y Sicilia.

Pronto se consolidó el modelo basado en las acuñaciones de plata de las ciudades-estado, hegemónico hasta que surgieron las emisiones de los monarcas helenísticos a finales del siglo IV a.C. Los diseños fueron básicamente de carácter religioso, hasta que en época helenística se introdujeron los retratos de gobernantes.

Interactivo 1.4. Emisiones de monedas griegas a nombre de ciudades.

Las emisiones de las polis se crearon en torno a la plata, ya que el oro sólo se emitió en ocasiones excepcionales. La dracma, que era el valor central del sistema, se acuñaba siguiendo patrones de peso diferentes en Atenas, Egina o Corinto.

Periodo helenístico. Desde finales del siglo IV a.C. las monedas se originaron en unidades políticas más amplias, incorporando el retrato del basileus. Las emisiones de Alejandro Magno se extendieron desde Macedonia hasta Babilonia, repitiendo en todos los talleres los mismos diseños, diferenciándose tan solo por monogramas o marcas que servían para identificar el lugar de emisión. Los herederos de su imperio las continuaron acuñando y fueron ampliamente imitadas hasta mucho más tarde en territorio celta.

Monedas púnicas. La tradición monetal púnica estuvo fuertemente influenciada por la griega, fruto en parte de su convivencia en Sicilia. El caballo fue el diseño más empleado en sus emisiones[1].

Monedas celtas. La mayoría de diseños celtas son toscos o esquemáticos. Normalmente prescindieron de leyendas que indicasen la autoridad.

La monetización a gran escala se produjo durante la Segunda Guerra Púnica cuando los contendientes promovieron importantes emisiones para financiar el conflicto [3]

[1] La moneda cartaginesa o púnica hace referencia a las monedas de la antigua Cartago, una ciudad-estado fenicia situada cerca de la actual ciudad de Túnez. Entre finales del siglo V a. C. y su destrucción en el año 146 a. C., Cartago produjo una amplia gama de divisas en oro, electro, plata, vellón y bronce. Solo una minoría de las monedas acuñadas se produjo o utilizó en el norte de África (Wikipedia).

Macedonia - rey Kassandros - 316-297 aC - tetradracma de plata - cabeza de Alejandro III

Haz clic en el botón para ver otra imagen →

Un poco mas de información la puedes encontrar en el siguiente video:

Vídeo

Video 1.1. El dinero y su origen ¿Quien lo inventó y cuando? (crédito: video de En Busca De la Verdad 2.0, en YouTube).

1.3.2 Roma

El Imperio romano impuso su sistema monetario de producción centralizada en todo el Mediterráneo. La ceca[2] principal fue Roma hasta mediados del siglo III, cuando las acuñaciones se descentralizaron para facilitar la demanda de las zonas fronterizas. La continuidad de las emisiones de oro y plata estuvo asegurada por el aprovisionamiento de metales preciosos que les reportaron sus numerosas conquistas. Durante los primeros siglos del imperio se

[2] Establecimiento oficial donde se fabricaba y acuñaba moneda.

permitió que algunas ciudades acuñasen su propia moneda. Lograron que las monedas de bronce ocupasen un lugar permanente en la vida cotidiana.

1.3.2.1 Monedas Romanas antiguas de la República

La base del sistema monetario republicano fue el denario de plata, equivalente a 10 ases de bronce. El oro sólo se acuñó en situaciones de emergencia.

El Denario. Moneda de plata oficial de la Antigua Roma, con un peso de 4 gramos y un tamaño de unos 18 milímetros.

Figura 1.6. Denario de plata de Cornelio Ceteo, acuñado en Roma, 115-114 a.C. (Gallica, CC0).

El sestercio. Del latín *sestertius*, *semistertius* es una antigua moneda romana de plata, cuyo valor equivalía a un cuarto de denario, a la centésima parte de un áureo, y a dos ases y medio. Solía ir marcado con las letras LLS (*duae librae et semis*, «dos libras y medio as»), rememorando al as libral. Forma parte del nuevo sistema monetario introducido en el año 212 a. C., que sustituyó al cobre como patrón monetario basado en el As.

El dupondio, fue una antigua moneda romana con un valor de dos ases o de medio sestercio.

As romano. Con el nombre as (del griego, *eis*, uno o del latín *aes*, bronce) se conocen las monedas primitivas de los romanos y las monedas que les siguieron como unidades monetarias de bronce. Parece ser que los romanos copiaron su as de los etruscos pero el as etrusco ofrecía menos relieve y formas más sencillas que el romano. Hacia el año 286 a. C., se redujo el as y con él todo el sistema a la mitad de su peso constituyendo el sistema semilibral y en el 268, coincidiendo con la primera emisión de monedas de plata, llegó el as a reducirse al peso de un sestercio. La disminución fue progresando en tiempo de la República hasta desaparecer este tipo de pieza al comenzar el Imperio.

Figura 1.7. As romano (Classical Numismatic Group, Inc, CC BY-SA 3.0).

Figura 1.8. Áureo del emperador Augusto (Autor desconocido, Dominio público).

El áureo. *Aureus*, en latín, era una moneda en la antigua Roma de oro, equivalente a 25 denarios de plata. Fue emitido regularmente desde el siglo I a. C. hasta el siglo IV d. C., cuando fue sustituido por el sólido bizantino (*solidus*). El áureo tenía aproximadamente las mismas dimensiones del denario, aunque mucho más pesado debido a la mayor densidad del oro.

El sistema monetario establecido por Augusto se mantuvo vigente hasta comienzos del siglo III. Se introdujo la acuñación regular de oro, que ya no se abandonaría hasta el final del imperio, y se crearon los sestercios de oricalco. A partir del siglo III disminuyó la cantidad de plata disponible para acuñar. Los cambios de formato en los bronces fueron frecuentes y en sus diseños predominaron los temas militares.

1.4 Sistemas monetarios

A través de la historia, la moneda ha adoptado diversas formas. Siguiendo un proceso de desmaterialización, las formas monetarias han pasado de la moneda mercancía a la moneda virtual de la época contemporánea...Pero la moneda no es únicamente un instrumento económico, pues tiene una dimensión política y social fuerte [2] .

El valor de las monedas de oro y plata dependía de su peso, magnitud variable que se vigilaba desde la fabricación hasta el momento en que se realizaban pagos. Las cecas desechaban algunos ejemplares que excedían o no alcanzaban el peso deseado y los cambistas, para evitar fraudes con monedas manipuladas, realizaban comprobaciones mediante balanzas de precisión y ponderales, llamados dinerales cuando estaban preparados para verificar valores monetarios concretos. En intercambios cotidianos, sin el concurso de estos instrumentos, eran la experiencia y voluntad de los usuarios las que determinaban la aceptabilidad de las monedas.

Los diferentes valores monetales se distinguen por su metal, tamaño, diseños o la inclusión de cifras. El valor de las monedas de oro y plata tradicionales era ligeramente superior al del metal que contenían debido a los costes y beneficios generados en su fabricación. En la primera mitad del siglo XX se impusieron los sistemas fiduciarios, formados exclusivamente por monedas de metales comunes y billetes sin valor intrínseco.

Figura 1.9. Monedas en diferentes épocas (imágenes de Wikimedia commons).

1.4.1 Política monetaria

Los estados deciden sobre el diseño, cantidad y calidad del dinero que ponen en circulación, determinando su retirada del curso legal mediante desmonetizaciones. Cuando se acuñaban oro y plata las manipulaciones se encaminaban normalmente a reducir el peso o la pureza de las piezas. Desde que se impusieron los sistemas exclusivamente fiduciarios, formados por piezas sin valor intrínseco, resulta fácil fabricar dinero en exceso, política monetaria que produce fenómenos como la **inflación**.

La inflación se puede deber a un incremento de la cantidad de piezas emitidas o a una elevación continuada de sus valores faciales[3].

1.4.2 Autoridades y diseños

Entre las prerrogativas de los estados se encuentra la emisión de dinero. Las monedas y billetes indican el poder del que emanan y que respalda su emisión, generalmente estados, ciudades, emperadores, monarcas o bancos. Los diseños y leyendas adoptados actúan como emblema de su soberanía, avalan la calidad de las piezas y otorgan al dinero una función publicitaria, misión esencial en épocas en las que los repertorios figurados eran escasos en la vida cotidiana.

Los estados monárquicos han sido la forma política preponderante desde el período helenístico hasta el siglo XIX. Las monedas

[3] Valor facial de estampillas, monedas y billetes es el que le asignó la casa de impresión, mientras que el valor nominal se refiere generalmente al valor verdadero de la moneda, estampilla o acción (como con las monedas de circulación). Puede a veces ser en gran parte simbólico, por ejemplo un pliego de centavos de escudos de 1972 (Wikipedia).

reforzaban la visibilidad de los monarcas presentándolos con sus atributos reales junto a leyendas que detallaban sus títulos o dominios territoriales.

Desde el siglo XX predominan los diseños relacionados con la historia, tradiciones, personajes, lugares o hechos memorables de cada país.

Figura 1.10. Moneda colombiana de $500 con ilustración de una Rana de Cristal.

1.4.3 Metales y aleaciones

Los metales acuñados tradicionalmente fueron básicamente oro, plata y cobre o bronce[4]. En el siglo XX se introdujeron excepcionalmente otros en situaciones de emergencia donde eran los únicos disponibles. El mayor cambio de las últimas décadas ha consistido en la incorporación de nuevas aleaciones y del sistema de capas múltiples.

Terminamos este capítulo con el artículo "La evolución histórica de la moneda y de los sistemas monetarios", que te recomendamos leer.

[4] Una opción para los griegos fue el electro (del latín *electrum*) que es una aleación de oro y plata, su color varía del amarillo pálido al brillante, dependiendo de cuáles sean las proporciones de oro y plata.

Diálogos Revista Electrónica de Historia
E-ISSN: 1409-469X
historia@fcs.ucr.ac.cr
Universidad de Costa Rica
Costa Rica

Viales Hurtado, Ronny J.
La evolución histórica de la moneda y de los sistemas monetarios. Bases conceptuales para estudiar la historia monetaria de Costa Rica del siglo XVI a la década de 1930
Diálogos Revista Electrónica de Historia, vol. 9, núm. 2, agosto-febrero, 2008, pp. 267-291
Universidad de Costa Rica
San Pedro de Montes de Oca, Costa Rica

Capítulo 2

Del blockchain al Bitcoin

Portada del capítulo: Busto de Satoshi Nakamoto en Budapest (Fekist, CC-BY-SA 4.0.

Imagen de esta página: Bitcoins Karolina Grabowska, Pexels.

Del blockchain al Bitcoin

2.1 Introducción

Las criptomonedas y el blockchain están estrechamente relacionados. El blockchain es la tecnología que permite el registro seguro y descentralizado de las transacciones con criptomonedas, lo que las hace únicas en comparación con las monedas tradicionales.

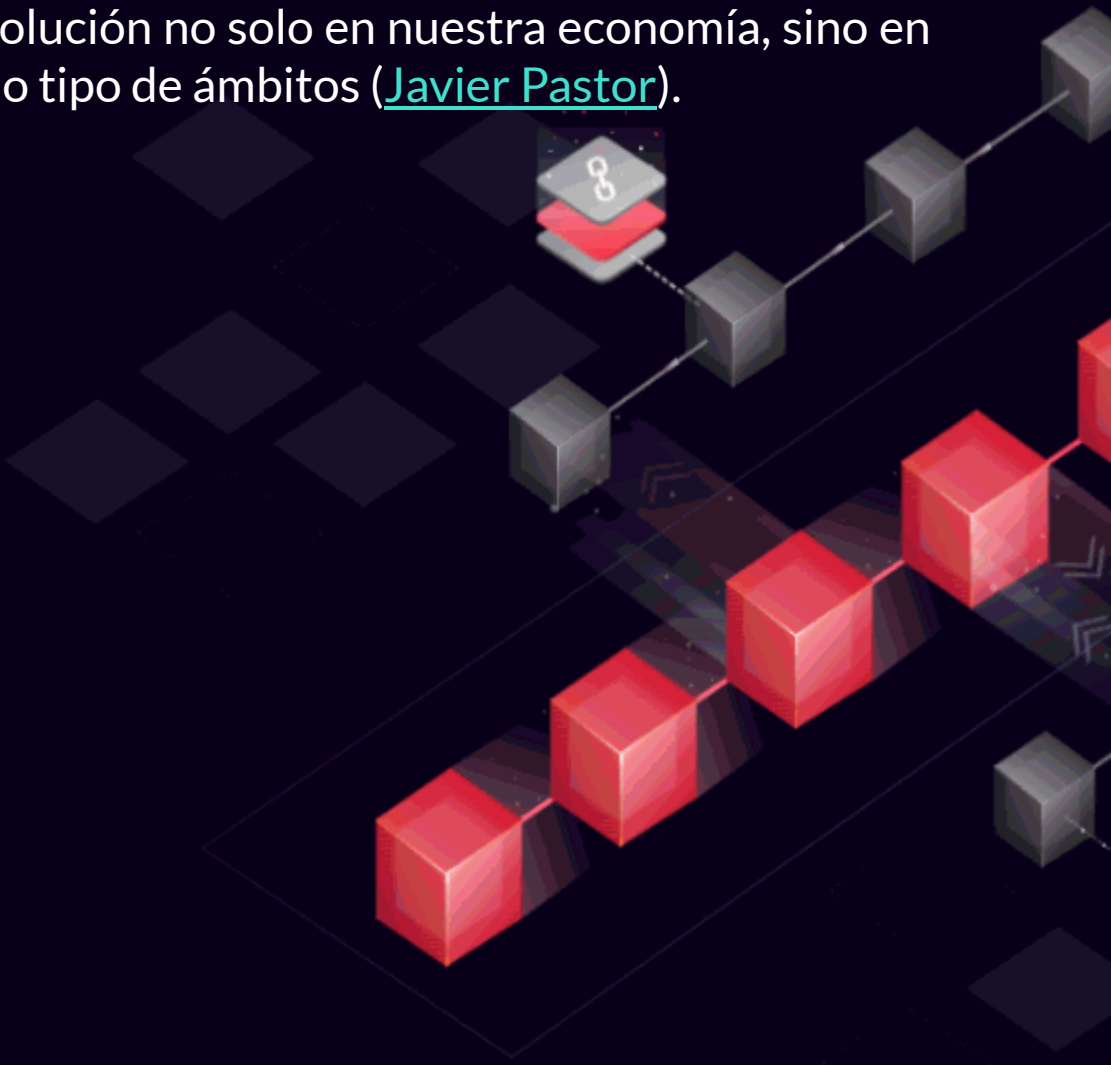
El blockchain es una tecnología de registro distribuido que permite la creación de una base de datos descentralizada y segura. Las criptomonedas son monedas digitales que utilizan esta tecnología para registrar y verificar transacciones.

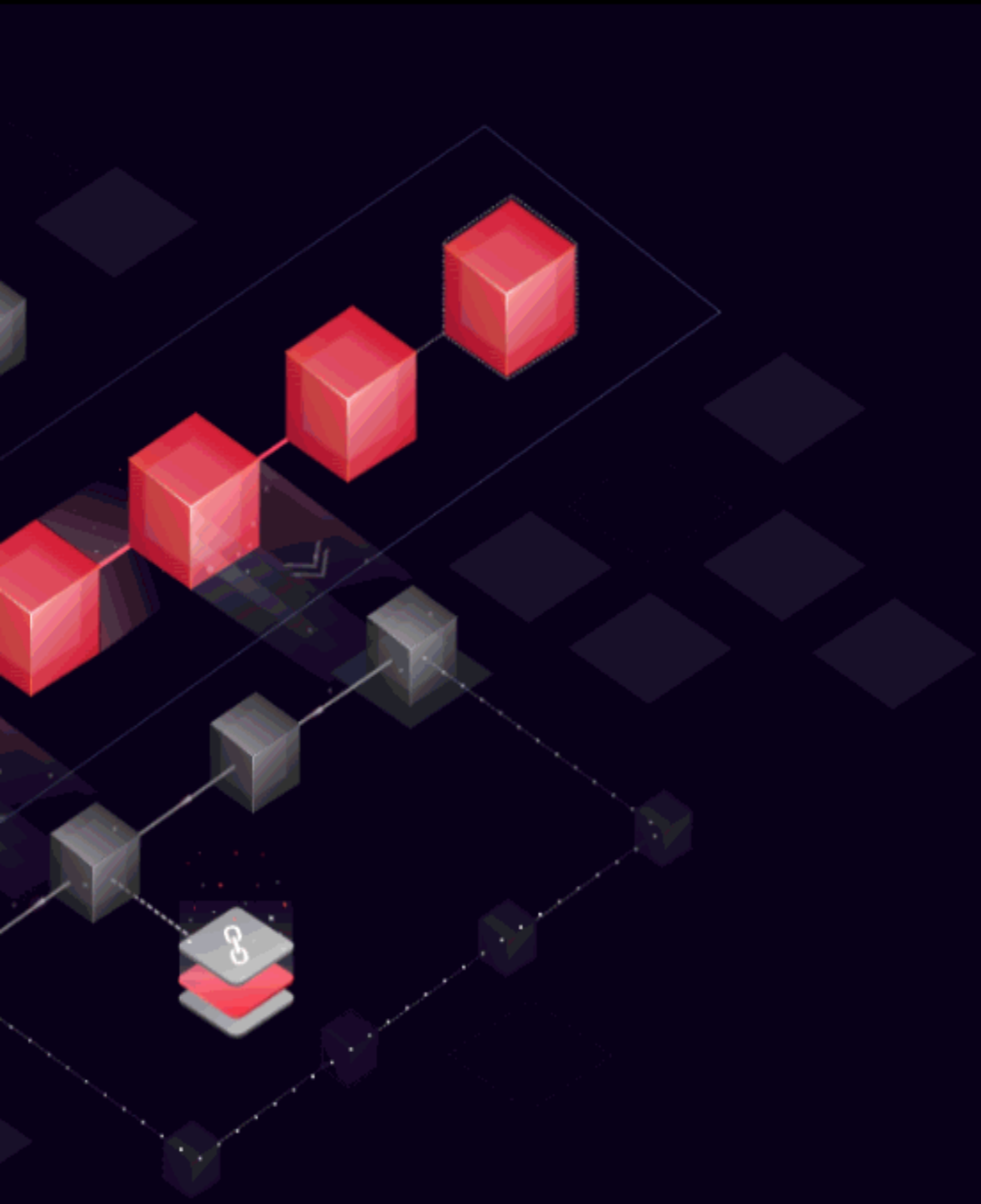
El blockchain es la base de las criptomonedas porque permite la creación de un registro público y transparente de todas las transacciones realizadas con ellas. Esto hace que las criptomonedas sean seguras y difíciles de falsificar.

Además, el blockchain permite la descentralización de las criptomonedas, lo que significa que no están controladas por un banco central o una autoridad gubernamental. Esto les da a las criptomonedas una mayor libertad y flexibilidad en comparación con las monedas tradicionales.

2.2 Blockchain

¿Blockchain? Es una de las palabras de moda en los últimos tiempos. La cadena de bloques es también un concepto que plantea una enorme revolución no solo en nuestra economía, sino en todo tipo de ámbitos (Javier Pastor).





2.2.1 Definiciones

Existen varias definiciones sobre el blockchain, de las cuales hemos seleccionado cuatro:

Blockchain es un sistema de registros para realizar transacciones de valor, de manera peer-to-peer (P2P), lo que significa que no hay necesidad de un intermediario confiable, como bancos, corredores y otros servicios, debido a que esta tecnología de cadenas de bloques permite mantener la seguridad y privacidad en cada proceso de transacción que se haga [4] .

La cadena de bloques o blockchain, es un registro público donde se comparten todas las transacciones jamás realizadas sobre algo en concreto, impidiendo de esta manera que se produzcan falsificaciones (economipedia).

La cadena de bloques es un registro digital distribuido que se caracteriza por su inmutabilidad. Consiste en una base de datos de transacciones. A diferencia de los sistemas tradicionales de registro de transacciones que están controlados por una autoridad central, como un banco o un proveedor de servicios, la tecnología de cadenas de bloques permite distribuir la responsabilidad entre todas las computadoras participantes (denominadas “ nodos ”). Una vez que los nodos llegan a un consenso sobre la validación, la transacción se consigna en un bloque, que resulta muy difícil de modificar o eliminar [5] .

Es una base de datos cifrada y segura que se usa para tran sacciones y que no vive en un solo lugar, sino en muchas partes de internet. Cuando alguien quiere hacer una transacción, la información de esa operación se cifra y se valida de manera independiente por una serie de usuarios, llamados nodos, que actualizan la base de datos y dejan un registro permanente de la transacción (BID).

Recogiendo de una y otra definición, podemos afirmar que:

El blockchain es una base de datos o sistema de registros digitales segura, que se usa para hacer transacciones peer-to-peer (de igual a igual), sin intermediarios. Cada transacción validada por los usuarios (nodos) es un bloque difícil de modificar, eliminar o falsificar.

En la Figura 2.1, hemos representado una transacción usando la tecnología blockchain.

Figura 2.1. Transacciones en blockchain a prueba de manipulaciones (crédito: Diseño de los autores con iconos de freepik).

Obviamente, las transacciones digitales no son tan simples como lo muestra la imagen, pero tampoco son complejas. Por ejemplo, una

transacción de valores entre monederos Bitcoin requieren una clave privada, que evita alteraciones. De ello nos ocuparemos más adelante.

2.2.2 Orígenes del blockchain

1979 - Árboles de Merkle

En 1979, Ralph Merkle patenta una estructura de datos en árbol, que llamó árbol de Merkle. Cada hoja del árbol está etiquetada y es irrepetible; por ello, también se llama árbol hash, pues cada nodo (hoja) está etiquetado con el hash criptográfico de un bloque de datos, que por ser del área de la criptografía garantizan seguridad, resistentes a ataques maliciosos. El árbol además de tener códigos únicos e irrepetibles, permite detectar cualquier intento de alteración, pues un solo dato alterado afecta al hash raíz y, en consecuencia, a todo el árbol.

1991 - Método de Haber y Stornetta

Stuart Haber y Scott Stornetta presentan un método usando el árbol de Merkle e incorporando marcas de tiempo en los documentos que no se puedan manipular.

1998 - Primera moneda digital

El criptógrafo Nick Szabo fue el primero en hablar de **contratos inteligentes**, que acompañó con una propuesta de moneda digital, que llamó *bit gold*, la cual nunca se implementó.

2008 - El Bitcoin

Lanzado en 2009, Bitcoin fue la primera criptomoneda en utilizar un nuevo tipo de libro mayor distribuido, conocido como **Blockchain**.

De acuerdo con la definición y la historia anterior, el blockchain fue generando, según las exigencias de los usuarios, algunos atributos clave que son altamente interdependientes, en especial la confianza, la seguridad y la no intermediación. En la siguiente infografía, puedes ver ocho atributos del blockchain.

Pasa el puntero del mouse por cada uno de los atributos:

Interactivo 2.1. Los atributos clave del blockchain (textos: Lapointe y Fishbone [7]).

2.2.3 Tipos de tecnologías blockchain

En la siguiente figura se describen los tipos de blockchain:

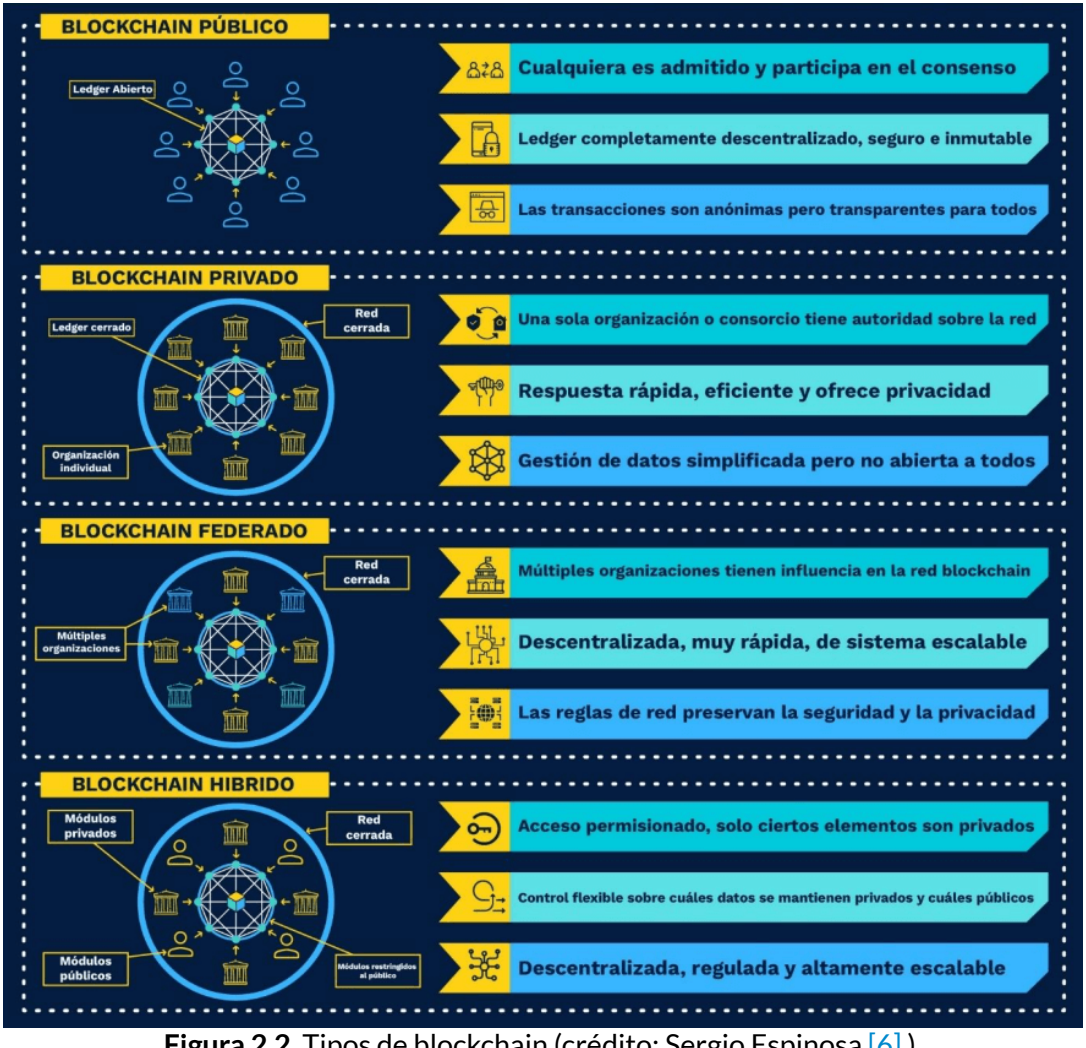
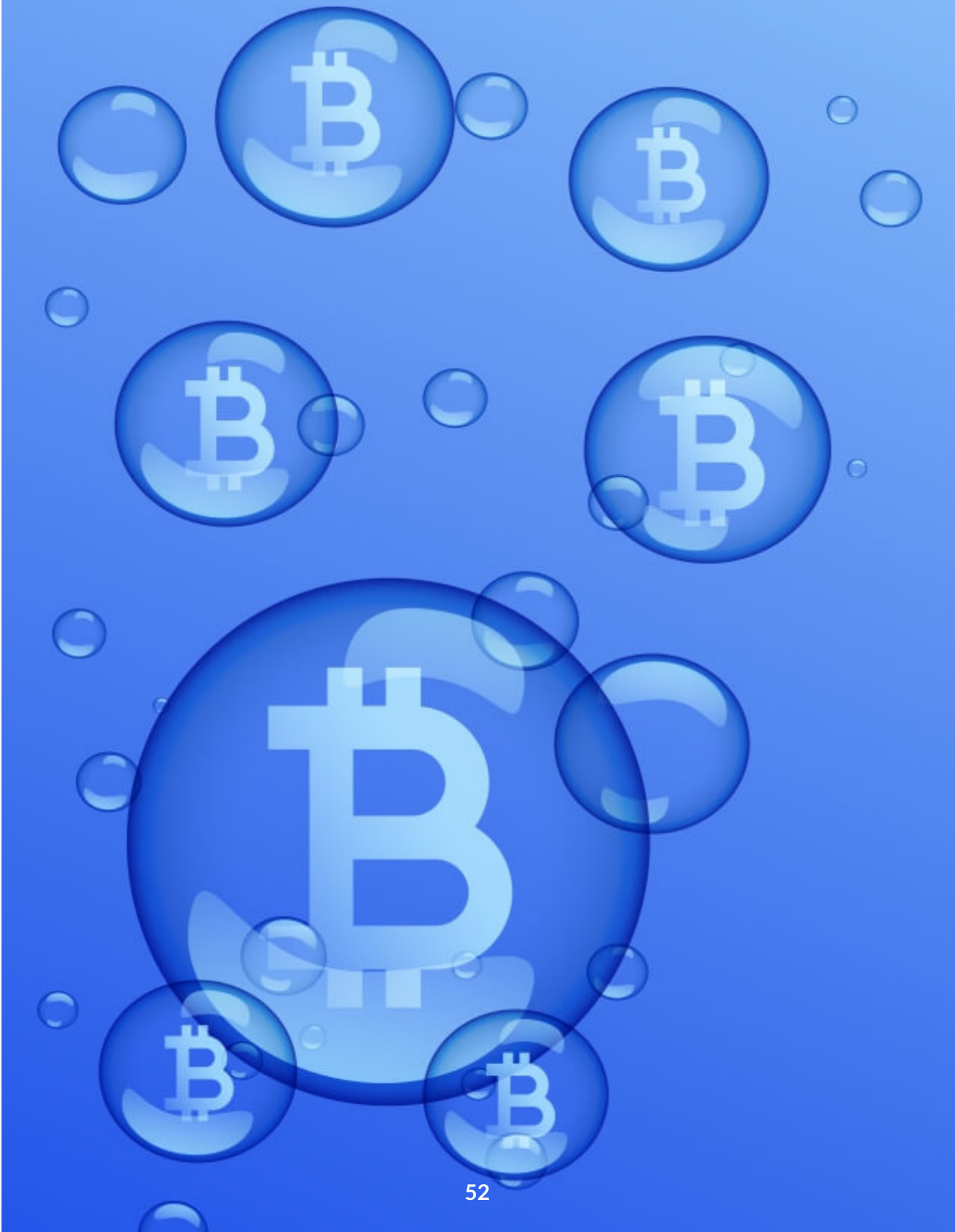


Figura 2.2. Tipos de blockchain (crédito: Sergio Espinosa [6]).

A continuación, presentamos la evolución del blockchain según la propuesta de Melanie Swan [8] , que va del blockchain 1.0 al blockchain 3.0.



Blockchain 1.0 - Criptomonedas

No es extraño que los desconocedores de la tecnología blockchain, la identifiquen como criptomonedas y, tampoco es extraño, que las criptomonedas la identifiquen con bitcoin. Todo lo anterior se justifica por dos momentos históricos del blockchain. El primero, como lo dijimos antes, es que el blockchain nació con el bitcoin en 2009, activo digital y sistema de pago inventado por Satoshi Nakamoto[5]. El segundo, tiene que ver con la antigüedad, pues el bitcoin es la criptomoneda mas antigua, lo que la ha generado más popularidad frente a otras criptomonedas como Ethereum, Cardano, Binance Coin, Ripple, entre otras. Pero, lo anterior no significa que bitcoin sea la mejor opción, pues todo depende de algunos factores que entraremos a discutir más adelante; sin embargo, sólo por información inicial, el Ethereum, lanzada en 2015, se ha convertido en la plataforma descentralizada más grande del mundo, permitiendo la implementación de contratos inteligentes y aplicaciones (blockchain 2.0).

Retornando al bitcoin, se trata de un sistema peer-to-peer (P2P) en el que los usuarios realizan transacciones sin intermediarios, de acuerdo a los pasos descritos en la figura 2.1. El sistema funciona sin un repositorio central o administrador único; es decir, es una moneda digital descentralizada.

En los siguientes apartados profundizamos sobre este tema, en los que se explicarán cómo funcionan las billeteras (*wallet*), las claves privadas (*private key*), el trading, el holding y, en general, las transacciones con diferentes criptodivisas.

[5] Satoshi Nakamoto es el pseudónimo usado por la persona o grupo de personas que crearon el protocolo Bitcoin y su software de referencia, pero a la fecha se desconoce la persona o grupo de personas que responden a ese nombre (Wikipedia)

Blockchain 2.0 - Contratos inteligentes

Ahora, comprenderás porqué el blockchain es más que criptomonedas:

> Mientras que Blockchain 1.0 es para la descentralización del dinero y los pagos, Blockchain 2.0 es para la descentralización de los mercados en general y contempla la transferencia de muchos otros tipos de activos más allá de la moneda utilizando la cadena de bloques, desde la creación de una unidad de valor desde la creación de una unidad de valor hasta cada vez que se transfiere o se divide [8] .

En este estado evolutivo del blockchain, como lo dice Swan, las transacciones no se limitan al dinero, se incluye el mercado en general; por ejemplo, las transacciones con propiedades o también llamadas *smart property*. Para comprender cómo funciona un "contrato inteligente" en blockchain, Swan nos pone el siguiente ejemplo: cuando seleccionas una bebida en una máquina expendedora e ingresas el dinero, se ejecuta "sí o sí" el código con las instrucciones de entregar el producto (siempre que la máquina esté en buenas condiciones), en forma análoga "los contratos inteligentes son simplemente programas almacenados en una cadena de bloques que se ejecutan cuando se cumplen condiciones predeterminadas" (IBM).

A diferencia de la máquina expendedora, la máquina blockchain difícilmente se va a averiar, la expendedora genera pérdida de confianza, en el blockchain es uno de sus atributos:

> La confianza mínima a menudo hace que las cosas sean más convenientes al eliminar el juicio humano de la ecuación, lo que permite una automatización completa [8] .

Nuevamente, Swan nos presenta un buen ejemplo de contrato inteligente: se trata de una transacción para que un nieto obtenga

una herencia cuando sea mayor de 18 años y sus abuelos hayan fallecido, el programa verifica la edad del nieto en forma permanente y, además, escanea la base de datos de defunciones, una vez se cumplan las condiciones envía "sí o sí" los fondos. Para terminar esta muy resumida información, te recuerdo que es Ethereum una buena opción para la implementación de contratos inteligentes.

Blockchain 3.0 - Más allá de la moneda, la economía y los mercados

La tecnología blockchain ofrece una gran cantidad de posibilidades, que van mucho más allá de su propósito inicial. Estas son algunas de ellas:

Blockchain y Big Data. La operación de grandes clases de tareas podría aliviar a los humanos porque las tareas serían manejadas por un sistema informático universal, descentralizado y distribuido globalmente.

Blockchain y gestión documental. Este es otro interesante uso del blockchain. Existen varios proyectos orientados a la gestión documental; por ejemplo, el proyecto Arcángel verifica si un documento es modificado legalmente por un archivo, pues los hashes del contenido también quedan registrados en la cadena de bloques creando una pista de auditoría, que permite saber cómo, cuándo y quién lo ha modificado. Alexandria es otro proyecto basado en blockchain, cuyo objetivo es crear un registro histórico inalterable mediante la codificación de los feeds de Twitter en una cadena de bloques, capturando tuits que podrían ser censurados más tarde mediante solicitudes de eliminación.

Blockchain y el arte digital. "Comprar un cuadro o una escultura en una subasta con su sello de autenticidad es garantía de que nos

estamos llevando a casa una pieza única y original. Usando **NFT** (Non-Fungible Token, o token no fungible), se certifica que lo que estamos adquiriendo es completamente original" (Izan González).

Blockchain y gobernanza. Otra gran utilidad del blockchain es la implementación de modelos de gobernanza digital, que

> inicia en la negociación democrática y horizontal sobre el contrato de fundación que blinda el modelo innovador, descentralizado, distribuido y sin intermediarios. Permite la creación de un sistema de votación transparente y democrático no sólo para las decisiones constituyentes de la organización, sino también para los procesos que la requirieran. Como modelo político y de gobernanza resulta disruptivo, porque su sistema es transparente y fomenta la creación de la confianza social, elimina la corrupción y prescinde de intermediarios –por tanto, también de costos– en un prototipo que es potencialmente replicable [9] .

Blockchain y la salud pública. Otra aplicación de blockchain es en la salud pública mundial, para la entrega eficiente, inmediata y específica de suministros en el caso de crisis como el ébola y la COVID-19.

Blockchain y la Internet de las Cosas. La tecnología Blockchain puede proporcionar soluciones a los problemas de seguridad y privacidad que se presentan en las redes IoT descentralizadas, ofreciendo, además, gestión de datos y soporte para microtransacciones entre dispositivos IoT basadas en el intercambio de datos y servicios [10] .

Blockchain en la Nube. Según Kleinerman [11] , "las aplicaciones de blockchain en la computación en la Nube están vinculadas a la Nube de las Cosas (CoT), una combinación de Computación en la Nube e Internet de las Cosas (IoT)", pudiéndose usar para la gestión segura de la red, a través de un *Blockchain as a Service* (BaaS) en un entorno de Nube.

Como lo dijimos antes, las aplicaciones de la tecnología blockchain, tanto actuales como futuras, son inmensas, cubriendo sectores como el financiero, gubernamental, educativo, comercial, salud, y un largo etcétera.

Terminamos este apartado con la siguiente evaluación formativa:

Actividad evaluativa 2.1. Evaluación formativa del blockchain, tipo falso y verdadero.

2.3 El Bitcoin... un desarrollo revolucionario

El Bitcoin es una criptomoneda o moneda virtual descentralizada, es decir, que no está controlada por ningún banco central o gobierno, y que se utiliza como medio de intercambio electrónico para adquirir productos y servicios como cualquier otra moneda. Fue creada en 2009 y es la criptomoneda más conocida y utilizada en todo el mundo.

Complementando la definición de You, en el siguiente video, puedes saber un poco más del bitcoin:

Vídeo

Video 2.1. ¿Qué es Bitcoin? (crédito: video de El Canal de Shackra, en YouTube).

Bitcoin es una red de consenso que posibilita un nuevo sistema de pago y un dinero completamente digital (https://www.weusecoins.com/).

Sin embargo, no todo es color de rosa, pues todas las criptomonedas se caracterizan por ser volátiles; por ejemplo, un tuit de Elon Musk hizo caer el precio del Bitcoin hasta 15% en una jornada (https://www.bbc.com/) o el histórico de diciembre de 2017, cuando cae de US$19.600 a US$3.000. Los hechos anteriores, no significan que no debemos invertir en criptomonedas, pues al 16 de abril de 2023 un Bitcoin tiene un precio de US$30,347.78 (https://coinmarketcap.com/). Este último dato, tampoco significa que debemos que invertir en Bitcoin, sólo nos advierte que debemos conocer más sobre esta y otras criptomonedas, así que...

¡A prestar atención!

al siguiente audio (traducido al español) de Andreas M. Antonopoulos, uno de los expertos en Bitcoin y cadenas abiertas, conocido por dar charlas que combinan la economía, la psicología, la tecnología y la teoría de los juegos con los acontecimientos actuales, trasladando los complejos temas de la tecnología de las cadenas de bloques desde lo abstracto al mundo real.

Audio 2.1. Introducción a Bitcoin - El Consenso (audio tomado de El Internet del Dinero, en YouTube).

Un sistema con reglas sin reguladores, una gobernanza sin gobernantes, un sistema que no puede ser sometido por reguladores, resistente a la censura.

2.3.1 El origen del Bitcoin

Como lo dijimos en el apartado 2.2.3, el activo digital **Bitcoin** fue inventado por alguien (o grupo de personas) que se hizo llamar `Satoshi Nakamoto`, quien en 2008 envía el siguiente correo:

Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, sábado 01 de noviembre 2008, 16:16:33 -0700

He estado trabajando en un nuevo sistema electrónico de efectivo que es totalmente de peer-to-peer, sin terceros confiables.
El documento está disponible en: http://www.bitcoin.org/bitcoin.pdf
Las principales propiedades:

- *El doble gasto se previene con una red peer-to-peer.*
- *Sin Banco Central u otras partes de confianza.*
- *Los participantes pueden ser anónimos.*
- *Las nuevas monedas se crean de la prueba de trabajo estilo Hashcash*
- *La prueba de trabajo para la nueva generación de monedas también impulsa a la red para evitar el doble gasto.*

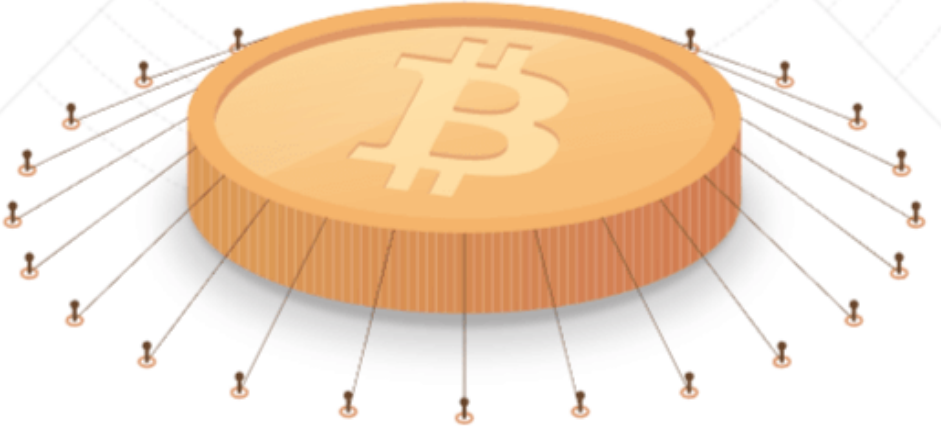
El artículo, en español, lo puedes leer en la página 43 de **El libro de Satoshi**, que hemos puesto en la siguiente página.

Del bestseller en inglés

The Book of Satoshi

PHIL CHAMPAGNE

El Libro de Satoshi



El 11 de febrero de 2009, Satoshi Nakamoto publicó, en el portal *P2P foundation*, el mensaje: "*Bitcoin open source implementation of P2P currency*". Satoshi da a conocer el portal oficial de Bitcoin, sus características fundamentales, el artículo donde se describía el diseño y el cliente inicial con el que comenzar a participar en la red [12] . En la página 96 del libro de Satoshi [13] , que presentamos en la página anterior, puedes leer el mensaje completo.

Supuestamente, «Satoshi Nakamoto», por los datos publicados en su perfil del portal P2P foundation, es un hombre de nacionalidad japonesa de 38 años de edad, pero esta información no ha sido verificada. En abril de 2011 se tiene el registro del último correo de Satoshi, enviado a Gavin Andresen, cuya primera parte es la siguiente (véase la página 312 del libro de Satoshi [13]):

> *Martes 26 de abril 2011, Satoshi Nakamoto*
> *<satoshin@gmx.com>*
> *Desearía que no siguieras hablando de mí como una figura misteriosa en la sombra, la prensa simplemente lo trata como una especie de moneda pirata. En cambio, podrías incidir más en la idea de que es un proyecto de código abierto y dar más énfasis a las contribuciones de tus colaboradores; lo que ayudaría a motivarlos.*

SATOSHI NAKAMOTO reunió muchos conceptos matemáticos y de software existentes para crear Bitcoin. Desde entonces, Bitcoin ha sido un experimento continuo, sigue evolucionando y se actualiza regularmente. Hasta el momento, ha demostrado su utilidad y ha revolucionado la industria financiera y monetaria, en particular el sistema de pago electrónico, y está siendo aceptado en todo el mundo. Bitcoin, en sí mismo, puede o no sobrevivir hasta el año 2140, cuando todos los bitcoins hayan sido minados, pero la idea de la distribución de igual a igual de una divisa con oferta limitada y descentralizada está aquí para quedarse [13] .

2.3.2 Pruebas de trabajo

Las pruebas de trabajo (*proofs of work*, en inglés) son el principal componente de Bitcoin responsable de garantizar que la red mantiene un comportamiento legítimo.
Brevemente, esta idea hace que validar/calcular nuevos bloques de transacciones conlleve un coste computacional muy elevado, de forma que, para hacerse con el control de la red (y por tanto de qué se valida y qué no), un atacante necesitaría una potencia de cómputo extremadamente difícil de conseguir. El principal precursor de esta idea es el método Hashcash.

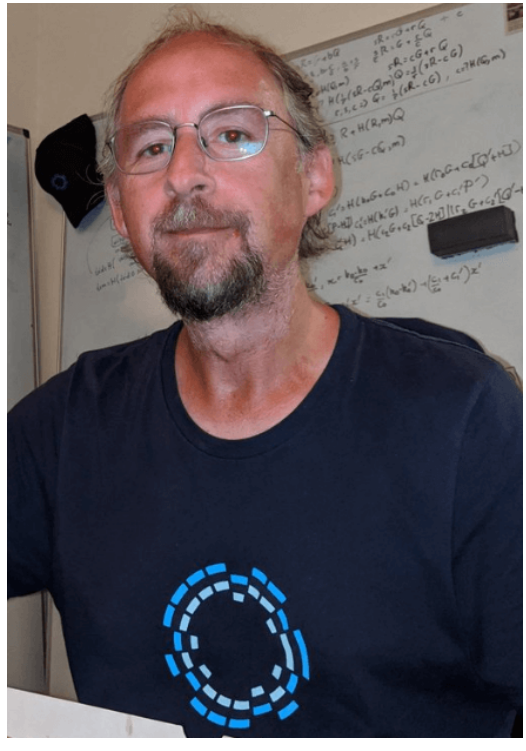


Figura 2.3. Adam Back es reconocido por ser el inventor del sistema de prueba de trabajo en hashcash, que más tarde se utilizó en el algoritmo minero de Bitcoin (imagen en Twitter).

En concreto, en Bitcoin este control de complejidad en los cálculos para los nuevos bloques se realiza obligando a que el hash de cada nuevo bloque deba comenzar con un número determinado de ceros. Dado que las funciones hash criptográficas no son invertibles, para encontrar un bloque válido la única alternativa será ir obteniendo diferentes nonce[6] hasta encontrar uno que cumpla el requisito preestablecido [12] .

[6] En criptografía, un nonce es un número generado aleatoriamente que se usa solo una vez en el proceso de cifrado para agregar una capa adicional de seguridad. El uso de un nonce evita que los atacantes reproduzcan mensajes antiguos para obtener acceso no autorizado al sistema. En criptomoneda, un nonce es un número que se agrega a un bloque cifrado o con hash en una red de cadena de bloques para que el hash del bloque cumpla con ciertos criterios y garantizar que se pueda agregar a la cadena de bloques (Wikipedia).

2.3.3 ¿Cómo funciona Bitcoin?

El funcionamiento es igual al descrito en el apartado 2.2.1, pues Bitcoin va de la mano del Blockchain que, como dijimos antes, es un sistema de registros digitales segura, que se usa para hacer transacciones peer-to-peer (de igual a igual), sin intermediarios. Así las cosas, el Bitcoin funciona así:

- **Inicia con una transacción**. Esta se registra en la red mediante un sistema de nodos llamado cadena de bloques. Los nodos tienen una copia de la cadena de bloques, lo que garantiza la transparencia y la seguridad del sistema. Para realizar la transacción Bitcoin, se necesita tener una cartera digital de Bitcoin (*wallet*), que puede ser una aplicación móvil, una cartera en línea o una cartera de hardware.
- **La transacción debe ser verificada**. Cuando se hace una transacción, esta se debe verificar para evitar el doble gasto de las criptomonedas. Los nodos de la red deben aprobar la transacción antes de que esta sea validada y agregada a la cadena de bloques. Cada transacción se registra en un libro de contabilidad público llamado "blockchain".
- **Validación de la transacción**. Una vez que se ha validado la transacción, el destinatario recibe los bitcoins. El destinatario también puede verificar la transacción en la blockchain de Bitcoin. Una vez que todas las operaciones de un bloque se han validado a éste se le asigna un código único e identificativo llamado **hash**.

El proceso de confirmación y validación de las transacciones se llama **minería de Bitcoin**. Los mineros utilizan su poder de procesamiento para resolver los complejos problemas matemáticos que verifican las transacciones y las agregan a la blockchain.

En resumen, los pasos para realizar una transacción peer-to-peer en un sistema como Bitcoin incluyen la obtención de una cartera de Bitcoin, la obtención de la dirección de Bitcoin del destinatario, el ingreso de la información de la transacción, la verificación de la información de la transacción, el envío de los bitcoins, la validación de la transacción por parte de la red de Bitcoin y la confirmación de la transacción por el destinatario.

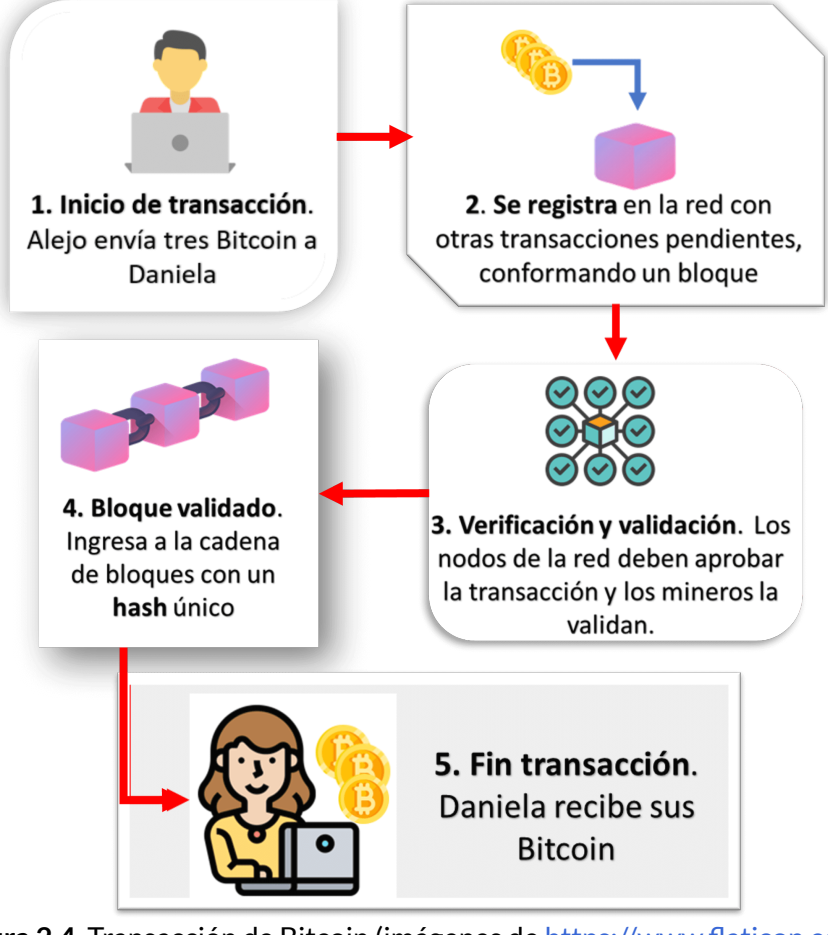


Figura 2.4. Transacción de Bitcoin (imágenes de https://www.flaticon.es/).

2.3.4 Volatilidad y discrepancias

Ya hemos advertido sobre la volatilidad de las criptomonedas, entre ellas el Bitcoin, las cuales presentan súbitas caídas cuando ocurre un hecho que afecta la confianza de los usuarios, tal como ocurrió con el colapso de FTX en noviembre de 2022, que llevó el Bitcoin (BTC) a un valor por debajo de los US$16.000 (ver Figura 2.5).

Figura 2.5. Caída del Bitcoin por el colapso de FTX.

No obstante, llama la atención la rápida recuperación de la criptomoneda, pues en abril de 2023 el BTC estaba por encima de los US$30.000. También llama la atención que estas súbitas caídas se convierten en oportunidades para que los enemigos de las criptomonedas, en especial políticos y banqueros, publiquen sus discrepancias, largamente reprimidas por el éxito prolongado del emergente sistema monetario. Algunos ejemplos son: el reporte sobre criptomonedas presentado al congreso de los Estados Unidos, en febrero de 2023 [14] y el libro blanco "*The Death of Cryptocurrency*" de Weaver [15] , publicado en diciembre de 2022.

Arrastra las frases al contenedor correspondiente

FRASES

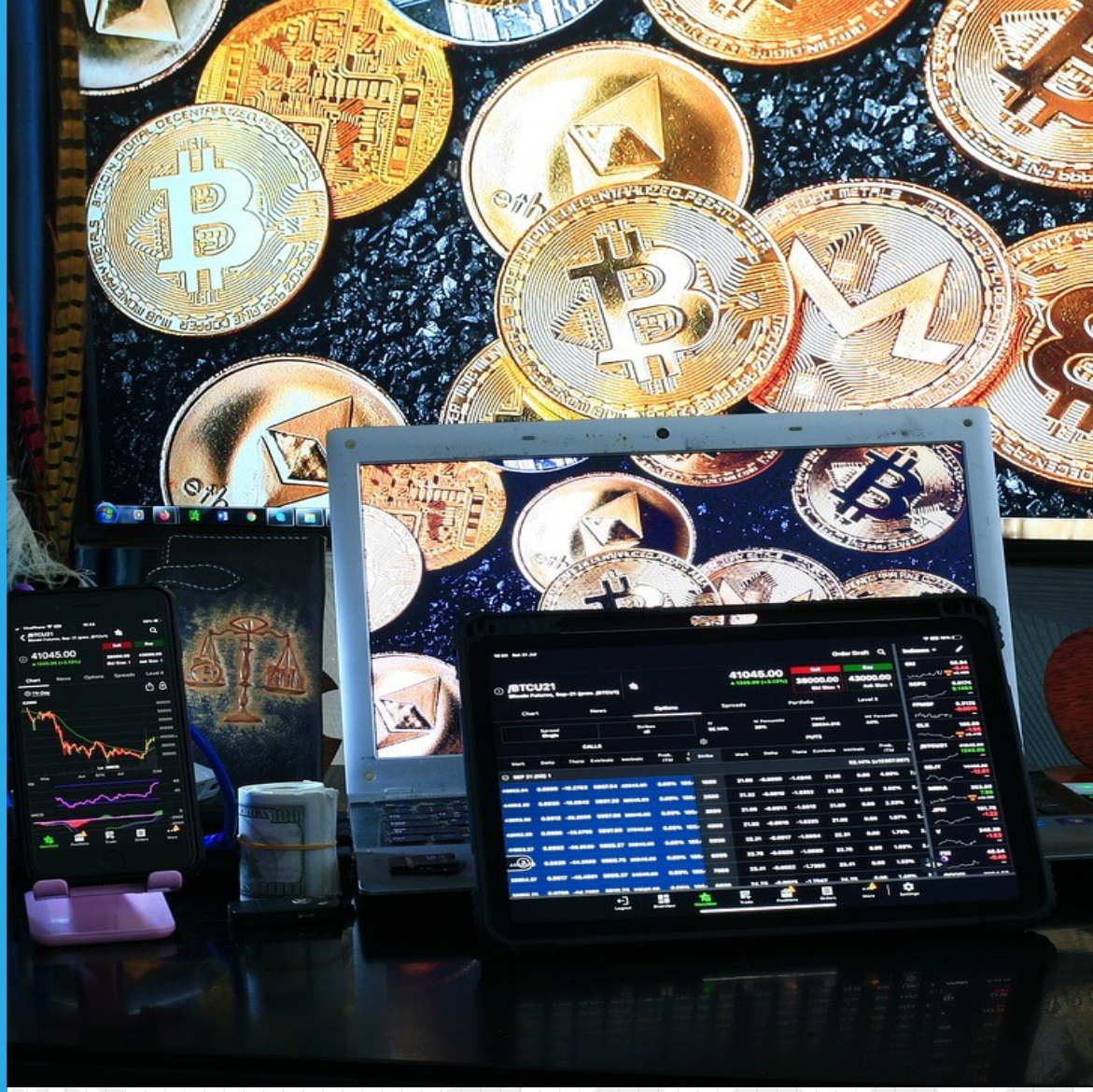
SÍ	NO

El Bitcoin es una criptomoneda o moneda virtual descentralizada.

Bitcoin es una red de consenso que posibilita un nuevo sistema de pago.

Las pruebas de trabajo son responsables de garantizar que la red mantiene un comportamiento legítimo.

Bitcoin es transferido de persona a persona, sin intermediarios.



Capítulo 3

Diversidad de criptomonedas

Portada del capítulo: Criptomonedas (Sergei Tokmakov), en Pexels.

Imagen de esta página: Criptomonedas (Jievani Weerasinghe), en Pixabay.

Diversidad de criptomonedas

3.1 Introducción

Aunque el Bitcoin es la criptomoneda más popular y reconocida, hay cientos de otras criptomonedas con diferentes características y propósitos. Algunas criptomonedas son diseñadas para ser utilizadas como medio de intercambio para comprar bienes y servicios, mientras que otras están diseñadas para funcionar como activos financieros o como tokens de utilidad para acceder a ciertas aplicaciones o plataformas.

Cada criptomoneda tiene su propia tecnología y conjunto de reglas únicas, lo que significa que las transacciones, la seguridad y la privacidad pueden variar entre ellas. Algunas criptomonedas utilizan sistemas de consenso diferentes, como la prueba de trabajo, la prueba de participación o la prueba de autoridad, lo que puede afectar la velocidad y eficiencia de las transacciones.

La diversidad de criptomonedas puede ofrecer a los usuarios una mayor variedad de opciones para satisfacer sus necesidades y preferencias. Sin embargo, también puede hacer que sea difícil para los nuevos usuarios comprender las diferencias entre ellas y elegir la criptomoneda adecuada para sus necesidades. Es importante investigar y comprender las características y el propósito de cada criptomoneda antes de invertir en ellas.

Referencias:

The Top 10 Most Popular Cryptocurrencies
Proof of Work vs. Proof of Stake: Which Is Better?
A Beginner's Guide to Cryptocurrencies" de Forbes
What Are Utility Tokens?

3.2 Las criptomonedas

Algunas de las criptomonedas más populares son Bitcoin (BTC), Ethereum (ETH), Binance Coin (BNB), Cardano (ADA), Dogecoin (DOGE), Ripple (XRP), Tether (USDT), USD Coin (USDC), Solana (SOL) y Polkadot (DOT). No obstante, el mercado de las criptomonedas es muy volátil y las criptomonedas más populares pueden cambiar con el tiempo.

Haremos una descripción de algunas de estas criptomonedas, incluyendo a Litecoin (LTC). Es necesario precisar que el número de criptomonedas existentes es superior a los 11,000; sin embargo, la gran mayoría de estas criptomonedas tienen una capitalización de mercado relativamente baja y son desconocidas para la mayoría de las personas.

También, es importante entender que hay criptomonedas propiamente dicho, y otros activos digitales llamados tokens, que se crean y operan en una plataforma blockchain existente, como Ethereum. Los tokens no tienen su propia red descentralizada y dependen de la plataforma blockchain existente en la que se crean. Más adelante veremos algunos ejemplos.

Desde 2009, cuando se lanza el Bitcoin, han surgido miles de criptomonedas y diferentes clases de otros activos digitales. En el siguiente objeto interactivo, mostramos la línea de tiempo de las principales criptomonedas.

Interactivo 3.1. Línea de tiempo de las criptomonedas.

Las dos criptomonedas más predominantes son Bitcoin y Ethereum, que combinadas representan alrededor del 61 % de todo el mercado de criptomonedas[7] [14] . A continuación, describimos algunas de estas criptomonedas.

[7] Al 15 de abril de 2023, es del 65 %.

3.2.1 Ether (ETH)

Ether es la criptomoneda nativa de la cadena de bloques `Ethereum`, que afirma "construirse sobre Bitcoin, con algunas grandes diferencias". En una evaluación de Bitcoin, Vitalik Buterin, el fundador de Ethereum, describió a Bitcoin como una "versión débil de un concepto de contratos 'inteligentes'".

El ether es la criptomoneda del blockchain Ethereum

Los contratos inteligentes son programas o software que pueden ejecutarse automáticamente cuando varios participantes cumplen con un conjunto predeterminado de criterios. Por lo tanto, Ethereum se propuso crear un "protocolo alternativo para crear aplicaciones descentralizadas... que permita a cualquier persona escribir contratos inteligentes y aplicaciones descentralizadas en las que pueda crear sus propias reglas arbitrarias para la propiedad, los formatos de transacción y las funciones de transición de estado". En criptomonedas y finanzas descentralizadas (consulte "Finanzas descentralizadas (DeFi)" a continuación), los contratos inteligentes se utilizan a menudo para facilitar los intercambios entre usuarios sin un intermediario. Ethereum comparte algunas similitudes con Bitcoin, incluido el seudónimo, la inmutabilidad, la descentralización y, en términos generales, sus funciones básicas como unidad de cuenta y medio de intercambio, entre otras. Sin embargo, hay algunas diferencias importantes [14] .

En el siguiente vídeo, Arnau Ramio de *Cryptomaster Academy* nos cuenta que es la criptomoneda de ethereum y cuáles son sus utilidades, además de como generar ingresos con blockchain.

Vídeo

Video 3.1. ¿Para qué sirve Ethereum? (crédito: video de Tutoriales CRIPTO en Español, en YouTube).

En este momento, miles de desarrolladores de todo el mundo están creando aplicaciones en Ethereum e inventando nuevos tipos de aplicaciones, muchas de las cuales puede usar hoy en día:

- Carteras de criptomonedas que le permiten realizar pagos baratos e instantáneos con ETH u otros activos (tókenes).
- Aplicaciones financieras que le permiten pedir prestado, prestar o invertir sus activos digitales.

- Mercados descentralizados, que permiten intercambiar activos digitales, o incluso intercambiar "predicciones" sobre eventos en el mundo real.
- Juegos donde tienes activos en el juego e incluso puedes ganar dinero real.
- Tókenes no fungibles (NFT).

El desarrollador de software Vitalik Buterin, propuso integrar un lenguaje Turing completo en el sistema de scripting de Bitcoin como mejora del protocolo, aunque el concepto es una idea original de Sergio Demian Lerner que desarrolla en su tesis. El desarrollo del mismo se logró gracias a una plataforma de financiamiento colectiva, desde julio a agosto de 2014. El sistema salió definitivamente el 30 de julio de 2015.

Después de una bifurcación de la blockchain en julio de 2016, hay dos cadenas de bloques de Ethereum activas: Ethereum y Ethereum Clásico.

Al igual que otras criptomonedas, Ethereum ha sido criticado por su huella de carbono muy alta. Si Bitcoin y Ethereum fueran un país separado, Bitcoin y Ethereum combinados tendrían el 12° mayor consumo de energía de cualquier país, solo detrás del Reino Unido y Francia. Ethereum requiere más energía de procesamiento que los Países Bajos, más de 100 TWh por año, tanto para minar la moneda.

como para confirmar transacciones en la cadena de bloques.5 Con emisiones de 50 a 60 millones de toneladas de CO2 al año, Ethereum es casi el doble de dañino para el clima que la central eléctrica de carbón más grande de Europa.

El ether se cotiza en las bolsas con el código de moneda ETH. El carácter griego Xi en mayúscula (Ξ) se utiliza a veces para su símbolo de moneda.

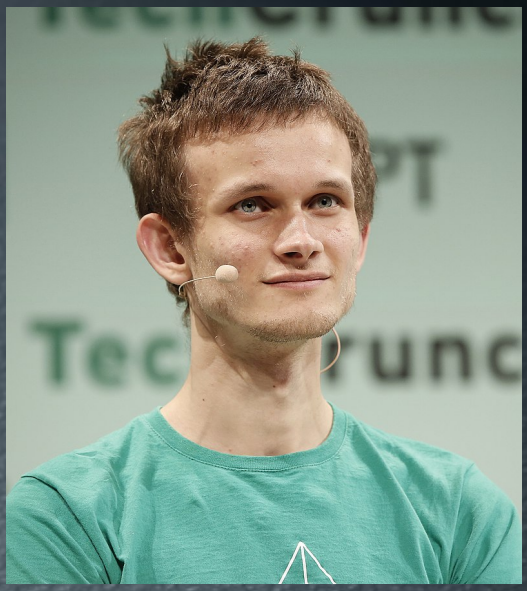


Figura 3.1. El fundador de Ethereum, Vitalik Buterin, durante el *TechCrunch Disrupt London* 2015, Inglaterra (foto de John Phillips).

A diferencia de Bitcoin, Ethereum promete ser la cuna de cualquier software descentralizado o criptográfico que se desee y pueda programar utilizando lenguajes específicos para la creación de sus contratos inteligentes y también la tecnología Blockchain.

3.2.2 Tether (USDT)

Tether es una *stablecoin* (moneda estable[8]) que salió al mercado en el año 2014 y ahora es la criptomoneda con mayor volumen de comercialización (https://www.criptonoticias.com/).

Tether USDT es una encarnación del dólar estadounidense, por ello su denominación es USDT, que es la unión entre la abreviatura oficial del dólar (USD) y la inicial del proyecto (T).

Tether: una moneda muy distinta a Bitcoin

La centralización de Tether es una de sus características más polémicas, puesto que todo activo que esté en manos de una entidad se puede revertir o censurar transacciones sin consultar. Esto va a en contra del principio de inmutabilidad de Bitcoin, que es considerado una de sus características más novedosas y confiables. No obstante, también permite que las autoridades puedan retornar a los usuarios fondos robados o perdidos; una opción que no tienen los usuarios de criptomonedas descentralizadas (Ibid).

Según la página oficial de Tether, sus tokens se basan en varias cadenas de bloques, lo que ofrece una fácil integración y adopción. Las cadenas de bloques admitidas son Bitcoin (protocolo Omni y Liquid), Ethereum, TRON, EOS, Algorand, Solana y Bitcoin Cash (SLP)

[8] Se considera moneda estable, aquella cuyo valor se respalda en una moneda fiduciaria, que para Tether es un dólar americano.

y, agrega otro beneficio com: "desde intercambios y aplicaciones de billetera digital hasta protocolos de finanzas descentralizadas (DeFi) y servicios de pago, los tokens Tether ofrecen una alternativa inteligente a las puertas de enlace fiduciarias".

El auge de Tether se ha visto opacado por algunas polémicas, entre ellas la presunta manipulación de precios. Por otra parte, según Funcas, el rápido crecimiento de Tether, creada por la plataforma Bitfinex, está generando preocupación entre reguladores, supervisores y economistas por los riesgos que puede conllevar para la estabilidad financiera, pues se teme que el emisor de Tether carezca de suficientes reservas en dólares para justificar su paridad con el dólar. "El porcentaje en efectivo se antoja del todo insuficiente". Bloomberg, por su parte, informa que Tether, que tiene $ 67 mil millones en monedas estables vinculadas al dólar en circulación, fue multado por las autoridades estadounidenses en 2021 por mentir sobre sus reservas.

Figura 3.2. Brock Pierce, cofundador de Tether, es un empresario estadounidense y exactor. Como actor, participó en películas de Disney como The Mighty Ducks (1992) y First Kid (1996) (foto de DavidCLee).

Pese a las polémicas, a la fecha (19 de abril de 2023), Tether es el tercer criptoactivo más grande, después de Bitcoin y Ethereum, y la stablecoin de mayor capitalización.

3.2.3 Binance Coin (BNB)

Binance es un *exchange* o empresa de intercambio de criptomonedas[9] que proporciona una plataforma para comerciar más de 100 activos digitales. Desde 2020, es considerada la plataforma de intercambio con el mayor volumen comercial del mundo (Wikipedia).

¡Binance Coin fue, inicialmente, un contrato inteligente del blockchain Ethereum"

Actualmente, tiene su propio blockchain, llamado *Binance Smart Change*, que permite, también, hacer contratos inteligentes. Este sistema, finalmente, se convierte en BNB Chain, cuya **visión** es que será: Abierto, multicadena, para creadores e inventores, sin permisos, siempre descentralizado y más grande que Binance (https://www.binance.com/).

¿Cómo nace Binance?

En 2014, Changpeng Zhao, fundador de Binance, vendió su apartamento para comprar Bitcoin, que adquirió a unos 600 dólares solo para ver cómo caía a 200 dólares durante dos años.

[9] El nombre de exchange de criptomonedas o intercambio de criptomonedas, hace mención a un espacio generalmente virtual, en el que se realizan acciones de compra-venta de criptomonedas (bvit2me Academy).

Tres años después, Zhao creó Binance mediante una oferta inicial de monedas de 15 millones de dólares en julio de 2017.

La plataforma de criptomonedas creció a un ritmo vertiginoso y se volvió rentable después de solo tres meses, relata. En seis meses o alrededor de 180 días, la Binance Coin (BNB) alcanzó una capitalización de mercado de 1.000 millones de dólares (iproup.com).

Figura 3.3. Changpeng Zhao es el fundador y CEO de Binance. En 2013, Zhao fue miembro del equipo que desarrolló Blockchain.com. Bloomberg lo posiciona en el trigésimo quinto puesto de su lista de personas más ricas del mundo (foto de Aevozer).

Zhao reveló que casi el 100% de sus bienes está en criptomonedas y dijo que lo que más le gustó de esta moneda es que no tiene fronteras y que se puede transferir de un país a cualquier otro sin estar limitado por personas o intermediarios (Ibid).

Hoy en día, Binance es el principal ecosistema de blockchains del mundo y cuenta con una oferta de productos que incluye el mayor exchange de activos digitales. Nuestra misión consiste en convertirnos en el proveedor de infraestructuras para las criptomonedas del mundo del mañana (Binance)".

3.2.4 USD Coin (USDC)

USD Coin (USDC) es una moneda estable digital vinculada al dólar estadounidense. USD Coin es administrado por un consorcio llamado Centre, que fue fundado por Circle e incluye miembros del intercambio de criptomonedas Coinbase y la compañía minera Bitcoin Bitmain, un inversionista en Circle. USDC es emitido por una entidad privada y no debe confundirse con una moneda digital del banco central (CBDC).

Figura 3.4. Jeremy Allaire, co-fundador y CEO de Circle (foto de Twitter).

USDC fue anunciado por primera vez el 15 de mayo de 2018 por Circle, y fue lanzado en septiembre de 2018. El 29 de marzo de 2021, Visa anunció que permitiría el uso de USDC para liquidar transacciones en su red de pago. A partir de julio de 2022, Circle afirma que hay 55 mil millones de USDC en circulación.

Según Forbes (5 de abril de 2022), "USD Coin" es una de las monedas estables de más rápido crecimiento en el mundo, con una capitalización de mercado superior a los $ 50 mil millones, acercándose al liderazgo de Tether en las *stablecoin*; no obstante, al 18 de abril de 2023, la capitalización de mercado de Tether recupera el dominio del 65% de las monedas estables y está por alcanzar casi mil millones de dólares (ámbito).

Se han revelado varios casos de uso para la moneda USD. Además de proporcionar un refugio seguro para los comerciantes de criptomonedas en tiempos de volatilidad, los que están detrás de la moneda estable dicen que también puede permitir que las empresas acepten pagos en activos digitales y sacudir una variedad de sectores, incluidas las finanzas descentralizadas y los juegos.

En general, el objetivo es crear un ecosistema en el que el USDC sea aceptado por la mayor cantidad posible de billeteras, intercambios, proveedores de servicios y dApps (https://coinmarketcap.com/).

El CEO de Circle, Jeremy Allaire, el 13 de julio de 2022, decía con satisfacción que USDC había crecido significativamente. Se ha más que duplicado en circulación año tras año a $ 55 mil millones (al 6 de julio) y ha facilitado casi $ 5 billones en transacciones en cadena totales desde que se lanzó en 2018 (https://www.circle.com/). Pero, en marzo de 2023,

cuando el *Silicon Valley Bank* quebró, Circle reveló que tenía 3.300 millones de dólares en depósitos en el banco cerrado. Los criptooperadores entraron en pánico al conocer la noticia y liquidaron miles de millones de USDC, lo que provocó que la stablecoin «rompiera el dólar» al cotizar por debajo de su par de 1 dólar durante unos tres días, hasta un mínimo de 88 céntimos (Forbes).

Al 31 de abril de 2023 la capitalización de USDC es cercana a los $ 31 mil millones. Surge la pregunta:

¿Qué tan estables son la monedas estables?

3.2.5 XRP

Figura 3.5. Chris Larsen es un ejecutivo de negocios e inversor ángel, fundador de la empresa Ripple Labs, Inc., con la que desarrolló Ripple (foto de Forbes).

XRP es un proyecto de software libre y un protocolo de pagos que persigue el desarrollo de un sistema de crédito basado en el paradigma peer-to-peer. Cada nodo de la red funciona como un sistema de cambio local, de manera que la totalidad del sistema forma un banco mutualista descentralizado. Algunos consideran que implementada hasta sus últimas consecuencias esta red constituiría un servicio de red social descentralizado basado en el honor y en la confianza entre sus participantes a nivel global (de esta manera, su capital financiero se sustenta en el capital social). Una versión reducida de la red consistiría en una extensión del sistema bancario tradicional en el que existirían rutas de pago alternativas que no dependerían de los bancos centrales (Wikipedia).

Ripple es una tecnología que actúa como criptomoneda y como red de pago digital para transacciones financieras (Cointelegraph).

3.2.6 Litecoin (LTC)

Figura 3.6. Charlie Lee es un científico informático , mejor conocido como el creador de Litecoin. Se desempeña como director gerente de la Fundación Litecoin (foto de Charlie Lee).

Criptomoneda diseñada para proporcionar pagos rápidos, seguros y de bajo costo. Se creó con base en el protocolo de Bitcoin, pero difiere en términos de cómo es utilizado el algoritmo de hash, la capitalización máxima, los tiempos de transacción de bloque y algunos otros factores. Litecoin tiene un tiempo de bloques de tan solo 2,5 minutos, y comisiones por transacción extremadamente bajas, lo que la hace apta para microtransacciones y pagos en puntos de venta.

Litecoin fue lanzado a través del código abierto de un cliente en GitHub el 7 de octubre de 2011, y la red de Litecoin se puso en marcha el 13 de octubre de 2011. Desde entonces, ha crecido tanto su uso como la aceptación entre los comerciantes, por lo que ha sido incluida entre las diez criptomonedas principales por capitalización de mercado. La criptomoneda fue creada por Charlie Lee, un ex empleado de Google, que pretendía que Litecoin fuera una "versión lite de Bitcoin", ya que cuenta con muchas de las mismas propiedades que Bitcoin, pero con un peso más ligero (Coinmarketcap).

3.2.7 Cardano (Ada)

CARDANO

Figura 3.7. Charles Hoskinson es fundador de la plataforma de cadenas de bloques Cardano, y fue cofundador de Ethereum (foto de 24/7 Crypto).

Ada es la criptomoneda creada y utilizada por la plataforma de cadena de bloques Cardano. Es la empleada para recompensar a los nodos y la utilizada en los contratos inteligentes creados por esta plataforma. Ada comenzó su emisión en 2015 cuando Charles Hoskinson ultimó la programación de la primera de las cuatro fases en las que plantea desarrollar su plataforma Cardano. El desarrollo del proyecto está supervisado por la Fundación Cardano, con sede en Zug (Suiza). Es una de las criptomonedas que utiliza una blockchain de **prueba de participación**[10], que se considera una alternativa más ecológica a los protocolos de prueba de trabajo (Wikipedia).

Cardano es una de las mayores cadenas de bloques en utilizar con éxito un mecanismo de consenso de pruebas de participación, el cual consume menos recursos que el algoritmo de pruebas de trabajo en el que confía Bitcoin.

[10] En las cadenas de bloques que usan prueba de participación, los nodos de la red se involucran en la validación de bloques, en lugar de asignar sus recursos informáticos para "minarlos".

3.2.8 Dogecoin (DOGE)

Figura 3.8. Billy Markus, uno de los fundadores de Dogecoin (foto de https://cdn.coingape.com).

Dogecoin (DOGE) se basa en el popular meme de Internet "doge" y tiene un Shiba Inu en su logotipo. La moneda digital de código abierto fue creada por Billy Markus de Portland, Oregon y Jackson Palmer de Sydney, Australia, y se bifurcó de Litecoin en diciembre de 2013. Los creadores de Dogecoin la vieron como una criptomoneda divertida y alegre que tendría un mayor atractivo más allá de la audiencia principal de Bitcoin, ya que se basó en un meme de perro. El CEO de Tesla, Elon Musk, publicó varios tuits en las redes sociales en los que decía que Dogecoin era su moneda favorita (Coinmarketcap).

Dogecoin se ha utilizado principalmente como un sistema de propinas en Reddit y Twitter para recompensar la creación o la compartición de contenido de calidad.

3.3 ¿En cuál criptomoneda invertir?

Como lo hemos advertido antes, este libro sólo pretende ilustrar al lector sobre el emergente mundo de las criptomonedas y no sobre cómo invertir en ellas. No obstante, es importante comprender que

¡Toda inversión es un riesgo!

Un riesgo de inversión puede definirse como la probabilidad de que un rendimiento sea menor a lo esperado, en palabras sencillas sería que la inversión realizada no brinde la rentabilidad esperada o que la pérdida supere la inversión inicial (BMF Inversiones). En el mundo cripto el riesgo es mayor; por ejemplo, mientras redactamos este capítulo (abril de 2023), el valor del Bitcoin ha caído de U$ 30,821 a U$ 28,748 entre el 14 y 20 de abril.

Figura 3.9. El precio del Bitcoin en los primeros 20 días de abril de 2023.

Seríamos excelentes inversores si hubiéramos comprado Bitcoin el 4 de abril de 2023 o, por contraste, pésimos inversores si lo hubiéramos hecho el 14. Por ahora, nuestro mejor consejo es que sigas leyendo este libro y te enteres de algunas estrategias para evitar un colapso financiero, una de ellas son los portafolios de inversión, que te sugieren tener un monedero con varias criptodivisas; es decir, no sólo Bitcoins o Ether o, invertir sólo en **monos** como en el siguiente video:

Vídeo

Video 3.2. Así es como manipulan el precio de las criptomonedas (crédito: video de Nexsson Trading, en YouTube).

Ten presente que en la inversión con criptodivisas, por su volatilidad, "podemos perder", lo importante es reaccionar a tiempo para evitar grandes pérdidas. Hasta los grandes inversores pierden; por ejemplo, Facebook le apostó a *stablecoin* llamada **Diem** (después nombrada Libra), lanzada en enero de 2021 y apoyada por PayPal, Ebay, Vodafone y Mastercard, entre otras, pero el 31 de enero de 2022...

Facebook dice adiós a su criptomoneda con la venta de Diem por 200 millones de dólares (El Economista).

Es tal la volatilidad de las criptomonedas que expertos mundiales en comercio e inversiones, también te pueden dar una predicción errónea; por ejemplo, *IG Group*, publicó el 13 de abril de 2023 **las 6 mejores criptomonedas para invertir en Abril 2023** (IG): Bitcoin (BTC), Ethereum (Ether), Dogecoin (DOGE), Chainlink (LINK), Litecoin (LTC) y Crypto 10 Index; sin embargo, las cuatro primeras monedas entre el 13 y el 20 de abril fue negativo(ver Figura 3.10)

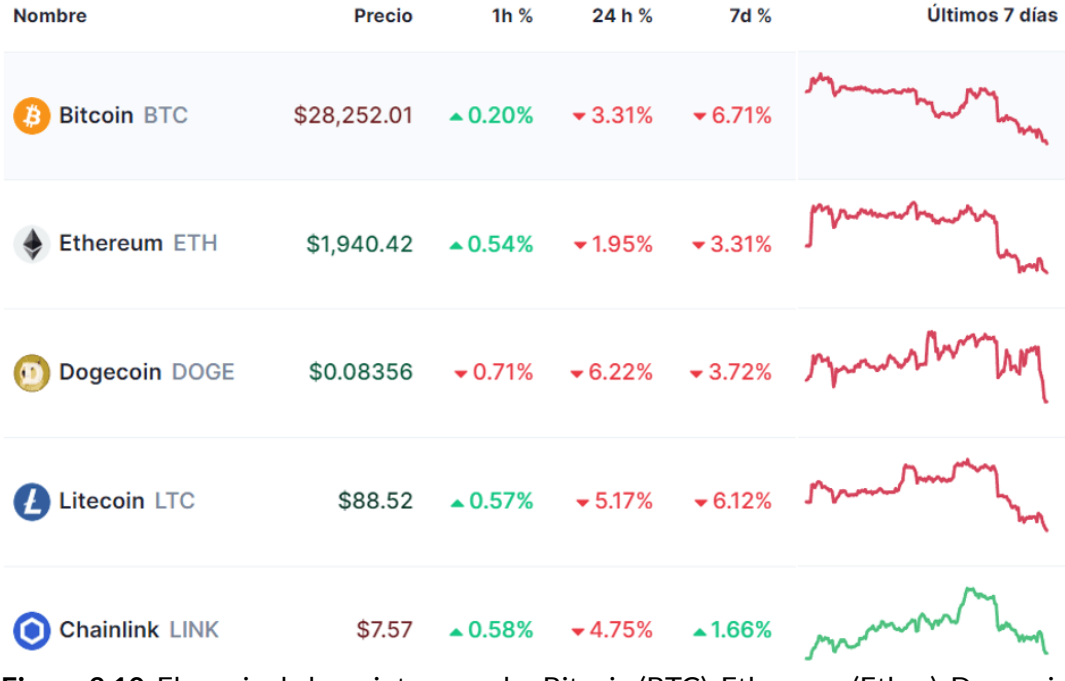


Figura 3.10. El precio de las criptomonedas Bitcoin (BTC), Ethereum (Ether), Dogecoin (DOGE), Litecoin (LTC) y Chainlink (LINK), entre el 13 y 20 de abril de 2023.

No obstante, tampoco podríamos afirmar que la tendencia negativa permanezca, he ahí la importancia de seguir profundizando en este libro; pero antes, no te dejes ahorcar a continuación.

EL AHORCADO

Criptomonedas

_ _ o _ _ _ _ _ _ i _ _

LETRAS ELEGIDAS = 7

FALLOS = 5

Q	W	E	R	T	Y	U	I	O	P
A	S	D	F	G	H	J	K	L	Ñ
Z	X	C	V	B	N	M			

Capítulo 4

Billeteras de criptomonedas

Portada del capítulo: Billetera cripto (Shutter_Speed), en Pixabay.

Imagen de esta página: mercado de criptomonedas (Alesia Kozik), en Pixabay.

Billeteras de criptomonedas

4.1 Introducción

Microsoft Bing

Las billeteras de criptomonedas o wallets son sistemas que almacenan claves públicas y privadas que permiten a los usuarios enviar y recibir monedas digitales y controlar el saldo que tiene en su wallet. Hay varios tipos de billeteras de criptomonedas (Bitso).

Las **billeteras de hardware** son parecidas a los pendrives (memorias USB). Dado que la validación de las transferencias es realizada por la propia wallet de hardware de forma externa, su uso es seguro incluso en dispositivos infectados (ripio).

Las **billeteras de papel** son tan simples que solo consisten en un papel con la clave privada y la dirección pública impresas o escritas. No hace falta dejar online datos que puedan verse expuestos a ataques; y eso ayuda a evitar el robo o hackeo del acceso a los fondos (Ibid).

Las **billeteras de software** pueden ser para computadora (*desktop wallets*), para teléfonos celulares (*mobile wallets*) o en línea (*web wallets*). Las billeteras para computadora utilizan una copia externa de la blockchain para que la computadora acceda a la red. Las billeteras para teléfonos celulares nos permiten operar en cualquier lugar y a toda hora. Las billeteras online dependen de una empresa que se hace responsable de la seguridad de las criptomonedas (Ibid).

En *stricto sensu* la expresión correcta que deberíamos usar es **monedero** (wallet[11]) y no billetera, pues su contenido son monedas y no billetes.

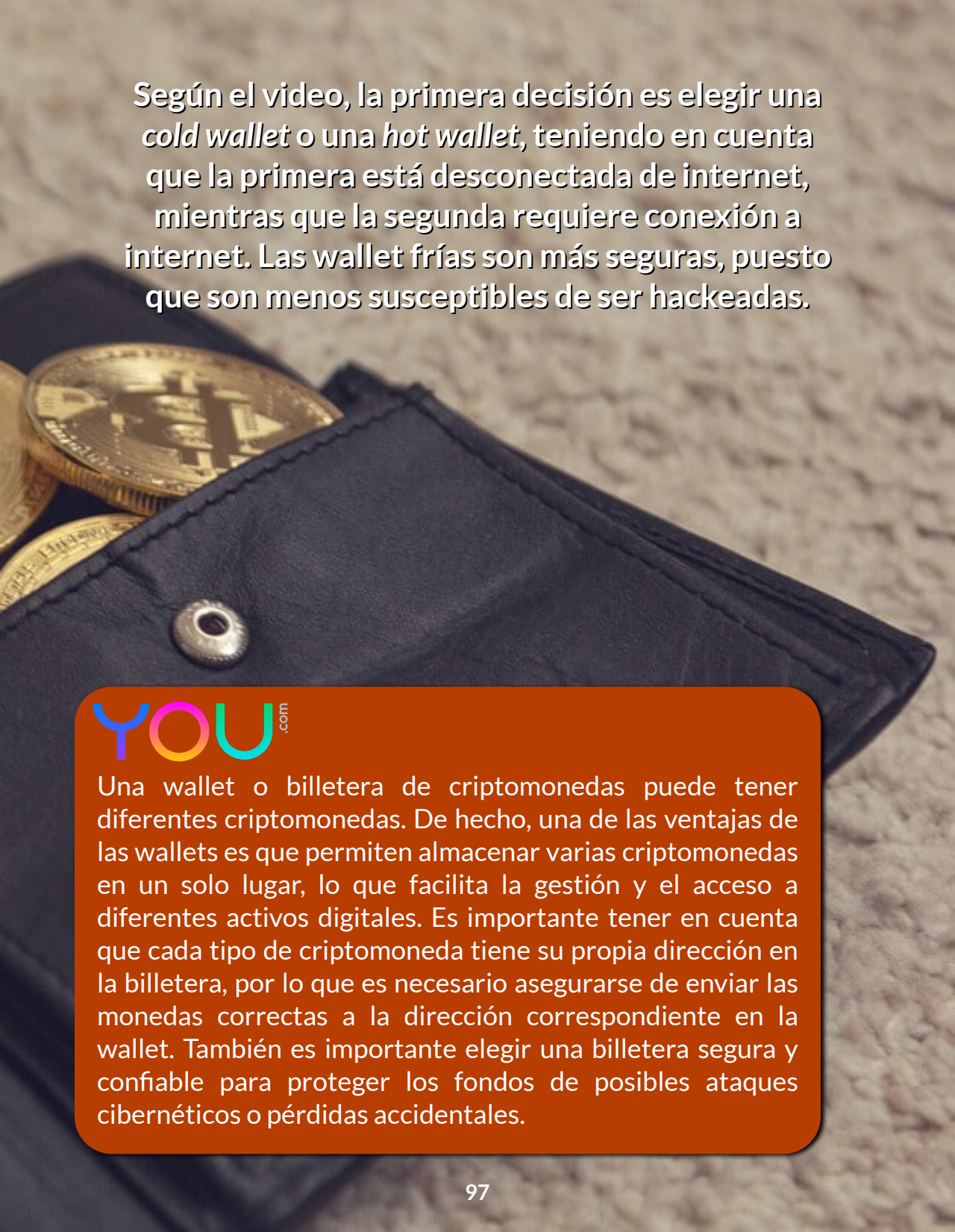
4.2 Monederos de criptomonedas o wallets

Iniciamos este apartado con el siguiente video:

Vídeo

Video 4.1. Monederos de criptomonedas o wallets (crédito: video de Artech Digital C.A, en YouTube).

[11] El término wallet hace referencia a una cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos (bit2me Academy).



Según el video, la primera decisión es elegir una *cold wallet* o una *hot wallet*, teniendo en cuenta que la primera está desconectada de internet, mientras que la segunda requiere conexión a internet. Las wallet frías son más seguras, puesto que son menos susceptibles de ser hackeadas.

YOU.com

Una wallet o billetera de criptomonedas puede tener diferentes criptomonedas. De hecho, una de las ventajas de las wallets es que permiten almacenar varias criptomonedas en un solo lugar, lo que facilita la gestión y el acceso a diferentes activos digitales. Es importante tener en cuenta que cada tipo de criptomoneda tiene su propia dirección en la billetera, por lo que es necesario asegurarse de enviar las monedas correctas a la dirección correspondiente en la wallet. También es importante elegir una billetera segura y confiable para proteger los fondos de posibles ataques cibernéticos o pérdidas accidentales.

Seguramente, por tu temor a los ciberdelincuentes, tu decisión va por las wallets frías; no obstante, ello depende de tus objetivos en el mundo cripto; por ejemplo, si vas a realizar transacciones rápidas y frecuentes una opción conveniente serían las wallets calientes. Pero, si deseas una mayor seguridad, puedes recurrir a un tipo especial de *cold wallets*, que son las *paper wallets* o billeteras de papel.

4.2.1 Wallets de papel

Son una forma de almacenar criptomonedas de manera segura y fuera de línea. Se trata de una hoja de papel que contiene la información de la clave pública y privada necesaria para acceder a una dirección de criptomoneda específica. La clave privada se imprime en el papel en forma de código QR o en texto claro, mientras que la clave pública se utiliza para recibir fondos en la dirección correspondiente. Las wallets de papel son una forma segura y conveniente de almacenar criptomonedas que no se utilizan con frecuencia, y son especialmente útiles para aquellos que desean mantener sus monedas desconectadas de Internet y su almacenamiento en línea.

4.2.2 Hardware Wallets

Son, también, *cold wallets*; su denominación de hardware o dispositivo físico se debe a que tienen forma de disco duro portátil o, algunas, en forma de USB. No requieren de conexión a Internet y por tanto, son inmunes a virus y malware que sí pueden atacar a los ordenadores, permiten añadir un PIN o contraseña adicional con el fin de que si se extravían, no puedan ser usados por terceros. Entre los más conocidos podemos mencionar a Trezor y Ledger (bit2me Academy).

¡Haz clic sobre la siguiente imagen para ver otras wallets!

Con LEDGER gana en tranquilidad protegiendo y gestionando más de 35 monedas, entre ellas, Bitcoin y Ethereum, además de todos tus tokens y NFTs.

Figura 4.1. Billetera de papel con la clave pública (*share*) y privada (*secret*) (Crypto oof).

4.2.3 Wallets calientes

Las *hot wallets* son wallets que están conectadas a Internet y son más convenientes para el uso diario y las transacciones frecuentes. Algunos ejemplos de hot wallets incluyen wallets basadas en la nube, wallets móviles y wallets de software.

> Puede ser la gran desventaja y riesgo el que las carteras calientes permitan ingresar desde cualquier dispositivo con Internet, respecto a las carteras frías que no están conectadas a Internet y nadie puede acceder a ella. A partir de estar conectadas en línea, las carteras calientes / *hot wallets* son un atractivo para los hackers que buscan como los antiguos piratas que buscaban las monedas de oro, en este caso los piratas informáticos o hackers buscan las criptomonedas (Rankia).

Veamos los tipos de *hot wallets*

Billeteras calientes de escritorio (*desktop*). Puedes bajar el software e instalarlo en el ordenador. Permite recibir y gestionar criptomonedas con un alto nivel de seguridad respecto a otras hot wallets. Lo que no quita que el ordenador pueda ser hackeado pueden perder sus criptomonedas (Ibid.). En este tipo de billeteras, el acceso a la clave privada permanece en posesión del usuario. Entre las wallets de escritorio más comunes se tienen: Electrum, Exodus y Bitcoin Core

Billeteras móviles (*smartphone*). Son aplicaciones instaladas en los teléfonos inteligentes. Aunque disponen de un espacio mucho más limitado que las de ordenador. Estas nos permiten una mayor facilidad de uso debido a que pueden ser empleadas desde cualquier lugar, por lo que son ideales para realizar operaciones del día a día (bit2me Academy). Las principales wallets para Android e iOS: Mycelium, Electrum, BreadWallet (BRD), Edge, Jaxx, Coinomi, Coin.Space y Trust Wallet

Billeteras en línea (*online*). Estas wallets son servicios que ofrecen las webs sin necesidad de descargar ni instalar ninguna aplicación. Funcionan directamente en línea como su nombre lo indica. Su mayor ventaja es que facilita realizar una operación desde cualquier parte del mundo que cuente con internet. Sin embargo para operarlas en su mayoría, es necesario ceder las claves privadas a un tercero, lo que implica confiar los fondos a otra persona. En temas de seguridad no es recomendable (Ibid.). Las más utilizadas son: BitGo, Blockchain.com y Bit2Me Wallet.

Imagen central, tomada de PNG EGG

4.2.4 Billeteras basadas en Exchange

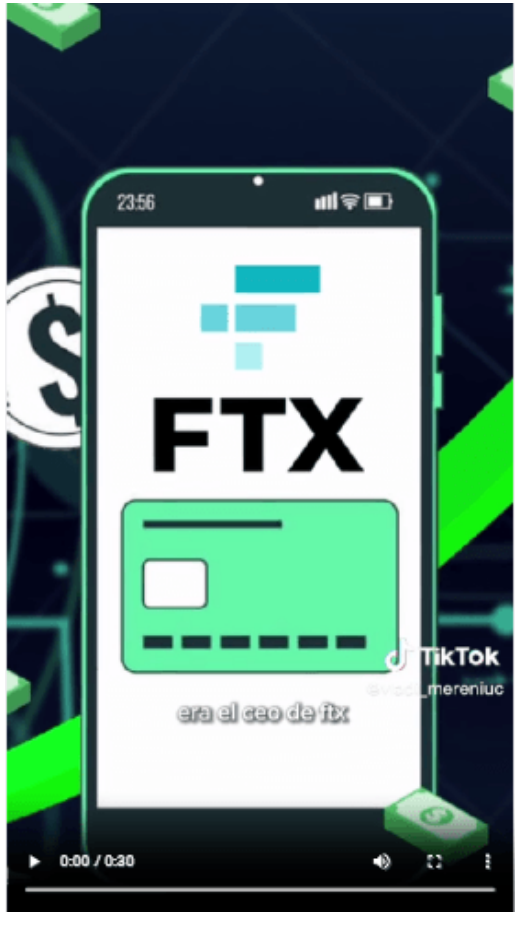
Son básicamente billeteras web, en este tipo de billeteras, las criptomonedas se almacenan en billeteras que son mantenidas por los intercambios de criptomonedas (*exchange*). Sin embargo, las claves privadas permanecen en posesión del *exchange* y no del usuario; esta es la razón por la que los ataques al intercambio resultan en una pérdida importante de criptomonedas.

Entre los *exchange* se destaca *Binance Holdings Ltd.*, con la marca Binance, que es una empresa global que opera el intercambio de criptomonedas más grande del mundo en términos de volumen diario de transacciones de criptomonedas. Fue fundado en 2017 (Wikipedia), le siguen (en función del tráfico, la liquidez y los volúmenes de comercio): Coinbase exchange, Kraken, KuCoin, Bybit y Bitfinex (CoinMarketCap, datos a abril de 2023). Haz clic sobre el video del banner lateral, para mayor información del Binance (video de abccriptoo, en TikTok).

El 19 de marzo 2022, Forbes presentaba los mejores **exchanges** de criptos del mundo, siendo los primeros seis: Coinbase, Kraken, Robinhood, Crypto.com, FTX y Binance.

Se destaca FTX, fundada en 2019 por el estadounidense Sam Bankman-Fried. Meses después de la información de Forbes, tenía más de un millón de usuarios y ya era el tercer mercado de criptomodenas más grande del mundo; sin embargo, en noviembre de de 2022 se declaró en bancarrota.

El origen de la debacle eran los préstamos que Bankman-Fried había realizado a su empresa comercial, Alameda, miles de millones de dólares en fondos de clientes FTX. El colapso de FTX provocó una caída estrepitosa del Bitcoin, que tocó su valor más bajo desde fines de 2020.



Video 4.2. El multimillonario en bancarrota (Video de Vladi Mereniuc, en TikTok).

La quiebra de FTX constituye el "tercer eslabón de una caída secuencial" que comenzó con el desplome del precio del Bitcoin, a la que siguió la estrepitosa caída de Luna, el token de Terra (Xataka).

Sam Bankman-Fried es el fundador y ex director ejecutivo de FTX, sus delitos constituyen "uno de los mayores fraudes financieros de la historia de Estados Unidos".

4.3 Claves públicas y privadas

Las claves públicas y privadas son componentes esenciales de una wallet de criptomonedas. Una clave pública es una cadena de caracteres que se utiliza para recibir criptomonedas en una dirección de wallet determinada. Es segura para compartir con otros usuarios, ya que no permite el acceso a los fondos en la wallet y se utiliza para recibir transacciones solamente.

Por otro lado, una clave privada es una cadena de caracteres secreta que se utiliza para firmar digitalmente transacciones salientes y autorizar transferencias de criptomonedas desde la wallet. La clave privada es fundamental para mantener la seguridad de los fondos de criptomonedas en la wallet. Se debe guardar en un lugar seguro y nunca se debe compartir con nadie más. Si alguien tiene acceso a la clave privada, podrá acceder a los fondos de la wallet sin necesidad de autorización.

La clave pública, entonces, es una dirección, la cual es un conjunto de números y letras generados aleatoriamente. Esta clave es similar al número de una cuenta bancaria[12]. La primera dirección de Bitcoin de la historia fue:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

[12] Hay una diferencias con las cuentas bancarias, pues en las redes de Bitcoin o Ethereum, los saldos y transacciones pueden ser vistas por cualquiera que conozca la dirección pública, pero sólo para ver saldos no para acceder a ellos.

La clave privada es la que tiene la información sobre el usuario, garantizando su identidad y su anonimato, permitiéndole acceder a sus activos. Esta clave no debe ser compartida con otras personas y, si se pierde, los activos asociados también. En general, un mensaje cifrado con la clave privada de un usuario, sólo podrá descifrarse con la clave pública de ese mismo usuario, asegurando que fue esa persona, propietaria de esas claves, quien envió ese mensaje. Por otro lado, si un mensaje se cifra con la clave pública de un usuario, sólo ese usuario podrá descifrar el mensaje con su clave privada. Cualquier transacción funciona de forma parecida (Figura 4.2). Los bloques que se almacenan digitalmente en blockchain, mezclan la información de las direcciones de las partes involucradas en la transacción, la cantidad de unidades de valor o tokens en movimiento y una marca temporal. Luego, las procesa a través de una función llamada hash. Esta función hash es un complejo algoritmo criptográfico que condensa en una secuencia alfanumérica única de longitud fija, información de cualquier extensión. Esta información es la huella dactilar (*fingerprint*) o hash del bloque y es imposible encontrar dos entradas en el blockchain con el mismo valor [17].

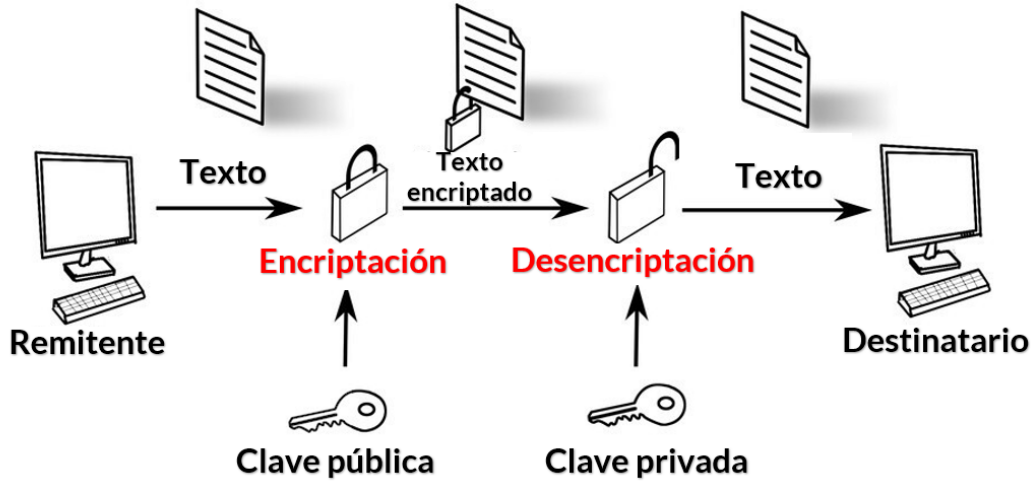


Figura 4.2. Transacciones usando las claves pública y privada (Adaptación de la imagen mostrada en el exchange ByBit).

Imagen página derecha: Shubham Dhage, en Unsplash.

Artículos de *Bitcoin Magazine en 2012*

Independientemente del tipo de sistema de pago electrónico que esté utilizando, si desea gastar dinero digital, debe tener una billetera digital. Bitcoin se diferencia de cualquier otro sistema de pago en línea. Bitcoin no tiene un proveedor central y cualquiera puede construir una billetera Bitcoin. En consecuencia, hay varias docenas de billeteras de Bitcoin para elegir y todas varían en términos de facilidad de uso, seguridad y características avanzadas, lo que hace que sea importante considerar cuidadosamente estas revisiones de billeteras de bitcoin (Vitalik Buterín, 5 de marzo de 2012).

Sobre Exchange. En una billetera en línea administrada, todo está controlado por el proveedor de la billetera. Tiene una cuenta con el proveedor con un nombre de usuario y contraseña, como una cuenta de correo electrónico o una cuenta de foro de Internet, y puede iniciar sesión en su cuenta y enviar y recibir bitcoins desde cualquier computadora que tenga acceso a Internet. En general, estos servicios no mantienen billeteras separadas para usuarios separados detrás de escena; se parecen más a los bancos en la forma en que todo el dinero se agrupa y solo realizan un seguimiento de cuánto pertenece a quién. Las más destacadas de estas billeteras son en realidad cuentas de intercambio de bitcoins como las de MtGox y CryptoXchange (Vitalik Buterín, 28 de febrero de 2012).

Tienes que confiar en que el proveedor no perderá tu billetera debido a una falla o pirateo, o que resultará ser malicioso.

BITCOIN
MAGAZINE
Frauds
POWER ISSUE
BITCOIN

Artículos de *Bitcoin Magazine en 2023*

Una de las billeteras *Lightning* más rápidas y fáciles de usar es *Wallet of Satoshi*. He visto a mucha gente usándolo en sus teléfonos, por ejemplo en Sudáfrica, Ghana o Zambia. Siempre se presenta como la solución más conveniente y fácil para principiantes (Anita Posh, 21 de febrero de 2023).

A la luz de los eventos recientes dentro de la industria de las criptomonedas, es hora de preguntarse qué está haciendo para proteger sus activos digitales. El panorama actual de las criptomonedas ofrece varias opciones que puede usar para proteger su bitcoin, pero una de las formas más sencillas de hacerlo es utilizando una billetera sin custodia (Brandon Mintz, 15 de febrero de 2023).

A la luz de lo que sucedió con Celsius, Voyager, Three Arrows Capital y FTX en 2022, cuando perdieron todos los bitcoins de sus clientes debido a malas prácticas comerciales, lo que los llevó a la bancarrota, el caso de la autocustodia no podría ser más sólido. Si bien estas quiebras fueron una píldora difícil de tragar para la industria de las criptomonedas, no fueron el primer rodeo de Bitcoiners con intercambios en bancarrota, ya que el hackeo de Mt. Gox en 2014 condujo al movimiento inicial de "no sus llaves, no sus monedas", que ha continuado hasta el día de hoy (¿Qué es una billetera de Bitcoin?, 24 de marzo de 2023).

Los bitcoiners a menudo se refieren a sí mismos como individuos soberanos. Para ser un individuo soberano, debe asumir la autocustodia de su BTC. Para hacer esto, debes aprender sobre billeteras.

Otro beneficio de una billetera sin custodia es que, en caso de pérdida de acceso a la billetera debido a la pérdida o el compromiso de una clave privada, un usuario puede utilizar la frase de contraseña asociada con la clave privada de la billetera para recuperar las existencias de la billetera, ya sea volviendo a acceder a la misma billetera o creando una nueva billetera. Esencialmente, perder su clave privada no significa que haya perdido el acceso permanente a su bitcoin (ibid).

YOU.com

Una billetera sin custodia, también conocida como billetera no custodial o billetera descentralizada, es un tipo de billetera de criptomonedas en la que el usuario tiene control total sobre sus claves privadas y activos digitales, sin necesidad de confiar en un tercero para su almacenamiento y gestión. En otras palabras, una billetera sin custodia permite que los usuarios sean dueños y controlen sus activos de criptomoneda y les da la responsabilidad total de asegurar que se almacenen y se utilicen de manera segura. Este tipo de billetera es considerado más seguro que las billeteras de criptomonedas con custodia, en las que un tercero como un exchange o una empresa de billetera tiene control sobre las claves privadas y puede controlar los activos digitales guardados en ella.

Si tienes temor a que tus criptodivisas se esfumen debido a una debacle como la de FTX, usa una billetera (fría) sin custodia.

No obstante las afirmaciones anteriores, podrás encontrar información que defiende el uso de billeteras con custodia; por ejemplo, *Binance Academy*, no dice que:

La principal desventaja de las billeteras con custodia es que tienes que confiar tus fondos y claves privadas a un tercero. En la mayoría de casos, estos proveedores de servicios también requerirán que completes una verificación de identidad (KYC). La ventaja, sin embargo, es la tranquilidad y comodidad. No tendrás que preocuparte por perder tu clave privada y podrás contactar al servicio de atención al cliente si tienes algún problema.

Una desventaja de utilizar billeteras sin custodia está vinculada a la accesibilidad y facilidad de uso. Por lo general, son menos intuitivas y tienden a ser un problema para holders de criptomonedas novatos. A medida que los proveedores de servicios sin custodia evolucionen, esto debería resolverse en un futuro. Además, eres el único responsable de tus claves y tienes que tomar tus propias precauciones al gestionarlas. Esto significa que, en lugar de confiar en otra persona para que proteja tus fondos, tendrás que confiar en ti mismo.

¿Billeteras con custodia o billeteras sin custodia? La mayoría de los usuarios de criptomonedas utiliza ambas, pero todo depende de tus necesidades. Si te gusta tener control total sobre tus activos o simplemente quieres utilizar la tecnología blockchain para interactuar con aplicaciones DeFi, deberías considerar una billetera sin custodia. Sin embargo, si lo que quieres es un proveedor de servicios que pueda encargarse de tus necesidades de almacenamiento de criptos mientras haces trading o inviertes, puedes buscar proveedores de servicios de billetera con custodia que sean de confianza.

Foto de regularguy.eth en Unsplash.

Actividad lúdica 4.1. Revistas Cripto.

Actividad evaluativa 4.1. Billeteras digitales.

Capítulo 5

Criptomonedas en el Metaverso

Portada del capítulo: Ilustración realizada con la IA (lexica.art).

Imagen de esta página: ilustración realizada con la IA (lexica.art).

Criptomonedas en el Metaverso

5.1 Introducción

Las criptomonedas son una forma de moneda digital descentralizada que se puede usar para una variedad de propósitos. En los metaversos, las criptomonedas se utilizan a menudo como una forma de cambio para comprar y vender bienes virtuales. Los metaversos son mundos virtuales en línea en los que los usuarios pueden interactuar con otros usuarios, crear sus propios avatares y personalizar el mundo en el que viven.

Un ejemplo de metaverso que utiliza criptomonedas es Decentraland, que es un mundo virtual en línea basado en blockchain. En este mundo, los usuarios pueden comprar y vender bienes virtuales utilizando la criptomoneda nativa del mundo, Mana. Otro ejemplo es Somnium Space, que es un metaverso que también utiliza una criptomoneda nativa para las transacciones. En este mundo, los usuarios pueden comprar propiedades virtuales y otros bienes utilizando la criptomoneda Somnium Cubes.

Además, en Landian, una plataforma descentralizada basada en blockchain, se utiliza una criptomoneda nativa llamada LNDA para realizar transacciones en el mercado del mundo virtual. Los usuarios pueden comprar y vender bienes virtuales, incluidos terrenos y edificios, utilizando esta criptomoneda.

5.2 El Metaverso

> El Metaverso es un universo post-realidad, un entorno multiusuario perpetuo y persistente que fusiona la realidad física con la realidad virtual. Se encuentra basado en la convergencia de tecnologías que permiten interacciones multisensoriales en entornos virtuales, objetos digitales y personas, como la realidad virtual (VR) y la realidad aumentada (AR). Por tanto, El Metaverso es una red interconectada de entornos inmersivos en red sociales y plataformas multiusuario persistentes [18].

En la novela *Snow Crash* publicada por Neal Stephenson en 1992 surge el término **metaverso**, en el contexto de un entorno virtual. En la página de la derecha, puedes conocer la historia del metaverso, a través de una infografía que incluye algunas imágenes relacionadas con el hito histórico que se destaca.

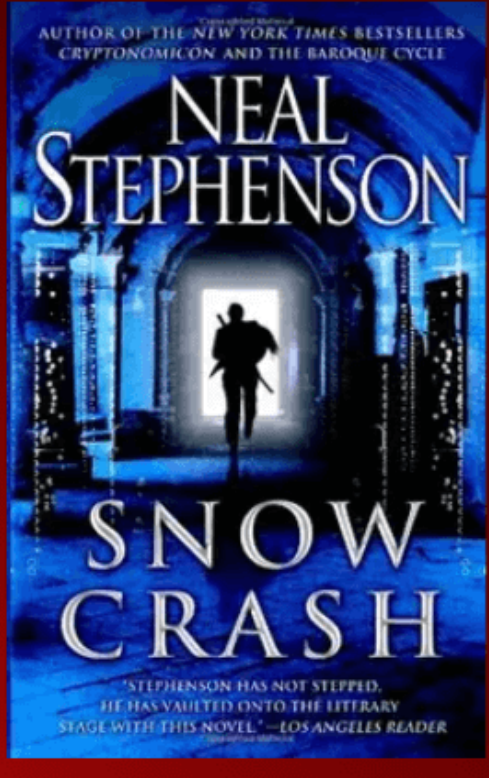
Si revisamos la palabra "Metaverso", observamos que está compuesta del término "Meta" que en griego significa post, después o más allá y "verso" que es universo. En conclusión, Metaverso es un universo post-realidad, "un entorno multiusuario perpetuo y persistente que fusiona la realidad física con la realidad virtual" [19].

Este tipo de fusión fue recreado por Ernest Cline en su novela de ciencia ficción "*Ready Player One* de 2011, en la que el protagonista Wade Watts, en su búsqueda de un huevo de Pascua, entra en un video juego de realidad virtual mundial, llamado OASIS... todo un metaverso. En 2018, la novela es llevada al cine por Steven Spielberg y es nominada al Óscar a Los Mejores Efectos Visuales.

Línea de tiempo del Metaverso

1992

Neal Stephenson, publica su novela Snow Crash en donde se menciona y describe el concepto de Metaverso.



Desplaza el punto naranja a lo largo de la línea de tiempo o haz clic en alguno de los puntos.

1993 1998 2003 2004 2005 2015

1992 1995 1998 2004 2005 2013 2021

A continuación, presentamos el tráiler de la película, que nos da una idea del universo de realidad virtual del juego OASIS, ambientado en el año 2045, cuando el mundo está al borde del caos y del colapso.

Vídeo

Video 5.1. Tráiler de la película Ready Player One. (crédito: video de Warner Bros., en YouTube).

Dionisio et. al. [19] dicen que el Metaverso se basa en el progreso en cuatro áreas: realismo inmersivo, ubicuidad de acceso e identidad, interoperabilidad y escalabilidad.

Por su parte, Mystakidis describe cuatro dimensiones principales del Metaverso, que incluye las tecnologías inmersivas de Realidad Virtual y Realidad Aumentada [18].

Ambas propuestas reiteran la inmersión y la identidad, para la primera se recurre al avatar como nuestra representación en el mundo virtual.

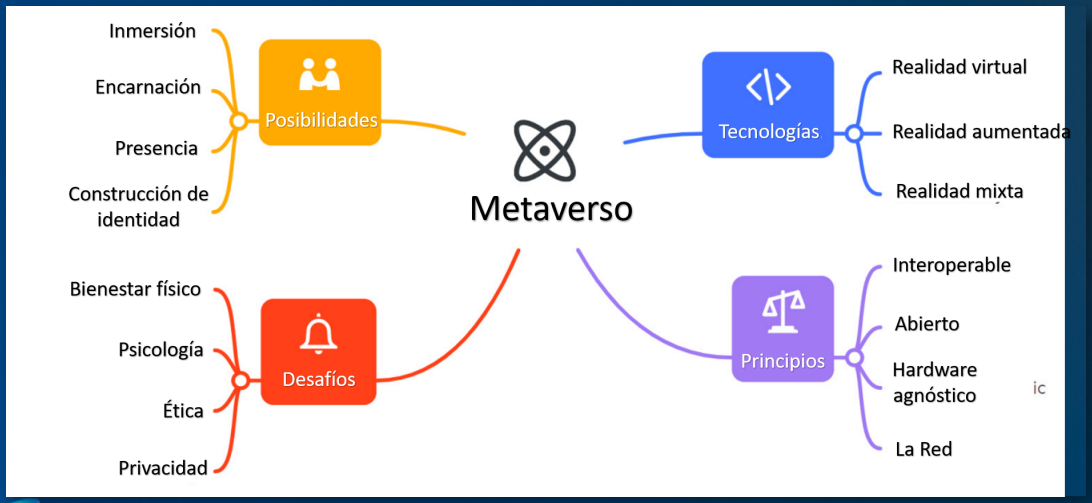


Figura 5.1. Tecnologías, principios, posibilidades y desafíos del metaverso.

El haber visto películas de ficción como *Matrix* o *Ready Player One*, nos permite comprender conceptos de inmersión, identidad, avatar, presencia e interactividad en los mundos virtuales. A 2023, son muchos los metaversos que se ofrecen y están en continuas mejoras; entre ellos:

- **Sandbox**. Metaverso de juegos NFT descentralizado basado en Ethereum, que permite crear, vender, comprar y monetizar NFT de realidad virtual.
- **Axie Infinity**. Un nuevo tipo de juego, parcialmente propiedad de sus jugadores y operado por ellos, incluye robots voladores, mutantes con martillos y bestias voladoras.
- **Landian**. Proyecto descentralizado que utiliza la tecnología blockchain y los contratos inteligentes para permitir a los usuarios construir, diseñar, vender y comercializar sus ideas y productos.

- **Bloktopia**. Incluye bloques de bienes raíces virtuales. Según su página, Bloktopia es un Rascacielos compuesto por 21 niveles para pagar reconocimiento a 21 millones de Bitcoin. Los titulares de fichas se conocerán como Bloktopians.
- **Star Atlas**. Metaverso de juegos que surge de la confluencia de blockchain, gráficos en tiempo real, videojuegos multijugador y tecnologías financieras descentralizadas.
- **Decentraland**. Plataforma de realidad virtual descentralizada 3D que consiste en 90.601 parcelas de tierra. La propiedad virtual en Decentraland son los NFT que se pueden comprar por medio de la criptomoneda MANA, que está basada en la Blockchain de Ethereum (Wikipedia).

5.3 Tokens

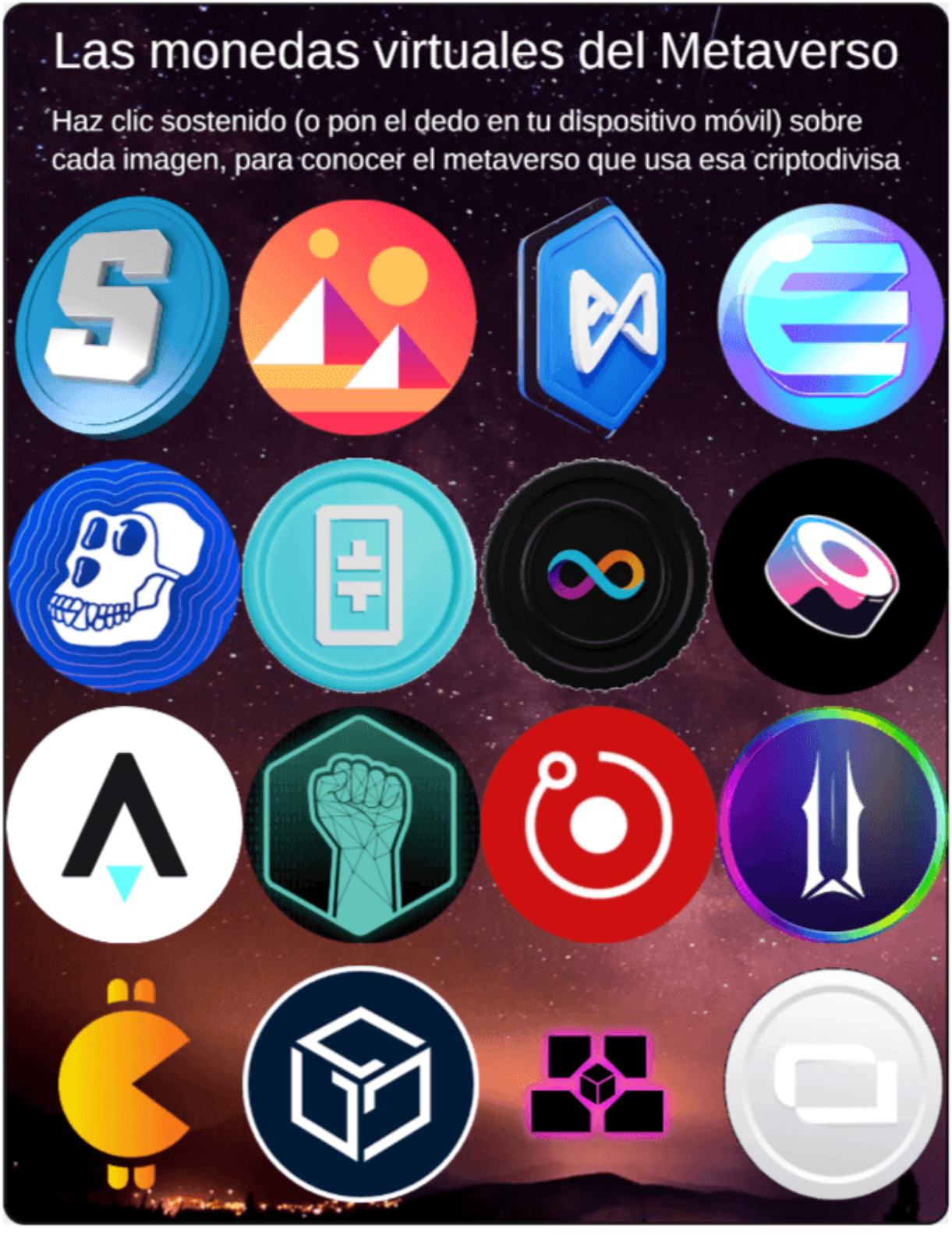
El metaverso cuenta con una economía virtual propia, donde los usuarios intercambian activos de valor mediante el uso de moneda de metaverso[13], tokens no fungibles (NFT) y metaverse tokens (Prensa Libre). A diferencia de las monedas, un token se emite sobre una red existente y no tiene su propia cadena de bloques única. Un token de metaverso también difiere porque se crea a través de la acuñación en lugar de la minería. Además de esto, las monedas casi siempre se usan como pagos dentro de los sistemas de criptomonedas.

En el siguiente objeto interactivo, presentamos algunas de estas monedas virtuales (haz clic sobre cada una de ellas, para saber más).

[13] Una moneda de metaverso está vinculada a un libro de contabilidad digital persistente llamado blockchain. Esto proporciona una amplia variedad de beneficios tecnológicos. Y también significa que los desarrolladores pueden vincular la lógica programable con la moneda del metaverso. Por ejemplo, Ether (ETC) de Ethereum se usa comúnmente como una plataforma de contratos inteligentes para programas de computadora (https://metamandrill.com/).

Las monedas virtuales del Metaverso

Haz clic sostenido (o pon el dedo en tu dispositivo móvil) sobre cada imagen, para conocer el metaverso que usa esa criptodivisa



5.3.1 Tokens ERC-20, ERC-721 y ERC-1155

> Ethereum introdujo el concepto de aplicaciones y protocolos descentralizados basados en cadenas de bloques. Y aunque Ethereum también tiene su propia "moneda", que se llama ETH, su principal caso de uso es servir de **gas** para alimentar las transacciones y las operaciones en las aplicaciones y los protocolos creados a partir de la red. Además, los desarrolladores de estas aplicaciones pueden crear en ellas monedas que no tengan una cadena de bloques específica y, en su lugar, se almacenen en Ethereum. Ethereum también permite a los usuarios crear otras formas de activos digitales independientes que se pueden almacenar de manera inmutable en el propio Ethereum. Estos activos digitales o monedas en la aplicación, creados y guardados en Ethereum, son lo que llamamos **tokens** [20] .

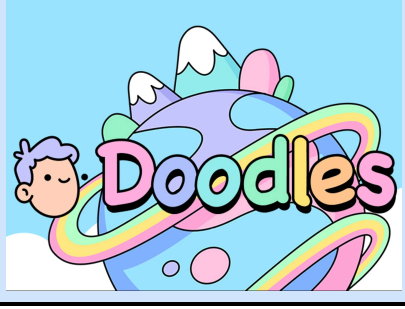
Un token ERC-20 es un *smart contract* (contrato inteligente) que cuenta con una estructura de datos ya preestablecida. Esta estructura está pensada en facilitar la implementación de diversas funcionalidades sobre la blockchain de Ethereum, facilitando el trabajo de creación a los desarrolladores (bit2me Academy).

> La blockchain de Ethereum, a diferencia de Bitcoin, ha sido creada para ser todo un ecosistema integrado. Por ello, sus desarrolladores crearon nuevos mecanismos para facilitar ciertas tareas. Un ejemplo de esto era mejorar la capacidad de crear nuevas monedas “sobre” una blockchain existente. Para lograr esto, los desarrolladores de Ethereum crearon los tokens ERC-20. Las siglas ERC significan *Ethereum Requests for Comments* o Solicitud de Comentarios para Ethereum, mientras el número 20 proviene del EIP donde se describe (Ibid.).

A medida que se ampliaban los casos de uso del blockchain, crecía la necesidad de tokenizar y representar datos únicos en la cadena de bloques. Fue entonces que se introdujo el estándar de tokens ERC-721, que permite crear tokens no fungibles, es decir, que tienen un valor único y que actúan como objetos digitales verificables únicos que no pueden cambiarse entre sí, como los tokens ERC20 [20] .

El problema de los estándares ERC20 y ERC721 es que no permiten que un contrato inteligente admita más de un tipo de token fungible o no fungible. Por ello se estableció el estándar de tokens ERC-1155, que permite a los desarrolladores de Ethereum crear tokens fungibles, semifungibles y no fungibles con el mismo estándar (Ibid.).

Algunos Metaversos que usan tokens ERC

AXIE INFINITY	Axie Infinity usa el token AXS o Axie Infinity Shard, que es un token del tipo ERC-20 que funciona sobre Ethereum. El objetivo de este token es sencillo: permitir la creación de un sistema de recompensas e incentivos para los jugadores.
	Doodles es una colección de 10,000 tokens no fungibles (NFT). Los Doodle NFT se componen de más de cien rasgos de rostros, cabello, sombreros, cuerpo y fondos. Cada Doodle es un token no fungible (NFT) único en la cadena de bloques de Ethereum.
ENJIN	Enjin ha creado avances como la creación del estándar ERC-1155, un tipo de token que reúne lo mejor de los tokens ERC-20 y ERC-721, dentro de un mismo *smart contract*. Como resultado, Enjin creó un tipo de token altamente flexible sobre el que se basa la construcción de las plataformas de desarrollo blockchain en el ámbito de los videojuegos.

5.3.2 NFT (Non Fungible Token)

Los tokens no fungibles (NFT, por sus siglas en inglés) son derechos transferibles de activos digitales, como arte, elementos del juego, coleccionables o música. El fenómeno y sus mercados han crecido significativamente desde principios de 2021 [21] .

> Ejemplos destacados de tokens no fungibles (NFT), como el artista Beeple que vende una obra de arte digital por $ 69 millones o el CEO de Twitter, Jack Dorsey, que subasta su primer tweet por $ 2,9 millones, muestran que los NFT han recibido la atención general y representan una aplicación popular en FinTech y el ecosistema de criptomonedas (Ibid).

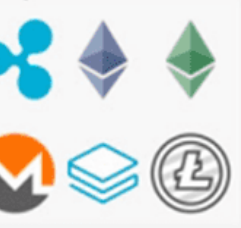
La idea práctica de los NFT se propuso por primera vez en 2017 y se implementó debido al estándar ERC−721 en el blockchain Ethereum. Los NFT son tokens/códigos inmutables basados en blockchain que certifican la unicidad. Se conocen con las siguientes propiedades principales [22] :

1. Singularidad: Se refiere a artículos únicos que pueden ser digitales o no.

2. Inmutabilidad: esta característica depende principalmente de la seguridad de la cadena de bloques para que ninguna persona pueda borrar, destruir o manipular los datos registrados.

3. No intercambiabilidad: Se entiende por las siglas de los NFT, locs cuales no son reemplazables por otros, incluso si se encuentra una gran similitud entre ellos.

Blockchain



edas y tokens

Metaverso

NFTs

Aplicaciones NFT

evas aplicaciones de NFT
en el Metaverso

tidad
atar
tidad
ficado
presía

Activo digital
Objeto digital
Tierra
Certificado virtual
transferencia de propiedad

o físico
ba de
iedad
cado
o digital

Atributo
Reputación
Grado académico
Posición
Valor

Arte
Pintura
Álbum musical
Clip de video

Evento
Boleto
Moda
Votación

Entretenimiento
Juego
Cartas coleccionables
Viaje

Ciencia y Tecnología
Cadena de suministro
Web, bienes raíces, Patente, Activo físico

El atractivo de los NFT ha hecho que se apliquen rápidamente en varios campos, en primer lugar para el arte digital y las tarjetas coleccionables (la primera aplicación). Recientemente, los NFT también se utilizan para terrenos digitales en el metaverso.

La prestación de servicios relacionados con NFT (por ejemplo, creación, infraestructura comercial, compra, venta, intercambio, etc.) es un trabajo recién surgido en el área de blockchain. Por lo tanto, estos servicios son proporcionados por varias compañías famosas como OpenSea, Rarible, ZORA, Teia y Marketplace [22] .

Arnau Ramió nos da la siguiente explicación sobre los NFT:

Vídeo

Video 5.2. ¿Qué es un NFT? (crédito: video de Tutoriales CRIPTO en Español, en YouTube).

Pero, ¿qué es la tal DeFi, que mencionan en el video?

5.3.3 DeFi

Las **Finanzas descentralizadas** (DeFi) son una forma experimental de finanzas que no dependen de intermediarios financieros centrales como corretajes, plataformas de intercambio o bancos para ofrecer instrumentos financieros tradicionales y, en cambio, usan contratos inteligentes en cadenas de bloques (blockchains), siendo Ethereum la más conocida. Las plataformas DeFi permiten a las personas prestar o tomar prestado fondos de terceros, comerciar con criptomonedas, asegurarse contra riesgos, y ganar interés en cuentas de ahorro. Algunos aplicaciones DeFi ofrecen altos índices de interés, pero están sujetas a un alto riesgo (Wikipedia).

Nuevamente, Arnau Ramió nos da una explicación adicional:

Vídeo

Video 5.3. ¿Qué son las Finanzas Descentralizadas o DeFi? (crédito: video de Tutoriales CRIPTO en Español, en YouTube).

En octubre de 2020, alrededor de 11 mil millones de dólares se depositaron en varios protocolos de finanzas descentralizadas, que experimentaron una subida de más de 10 veces su valor durante el transcurso del año 2020. En enero de 2021, aproximadamente 20.5 mil millones de dólares se invirtieron en DeFi (Wikipedia).

En lugar de depender de intermediarios centralizados, las aplicaciones DeFi utilizan contratos inteligentes (*smart contracts*) y protocolos descentralizados para permitir que los usuarios realicen transacciones financieras de igual a igual (peer-to-peer) de manera segura y transparente.

Algunos ejemplos de aplicaciones DeFi incluyen préstamos, mercados de predicción, exchange descentralizados (DEX), fondos de inversión descentralizados (DAFI), y seguros descentralizados. Estas aplicaciones suelen estar construidas en la red Ethereum, aunque también existen aplicaciones DeFi construidas en otras redes blockchain.

Las aplicaciones DeFi han ganado popularidad en los últimos años debido a que ofrecen una mayor transparencia, seguridad y accesibilidad en comparación con los sistemas financieros tradicionales. Además, las aplicaciones DeFi también ofrecen una mayor inclusión financiera, ya que cualquier persona con acceso a Internet puede utilizarlas, independientemente de su ubicación geográfica o situación económica.

https://cointelegraph.com/
https://www.investopedia.com/

Arrastra las frases al contenedor correspondiente

FRASES

SÍ	NO

Las plataformas DeFi permiten a las personas prestar o tomar prestado fondos de terceros.

Las DeFi son una forma de finanzas que dependen de intermediarios financieros.

En la novela Snow Crash publicada por Neal Stephenson en 1992 surge el término metaverso.

Los NFT son derechos transferibles de activos digitales como una obra de arte.

Capítulo 6

Del Bitcoin al Ethereum

Portada del capítulo: Foto de Jonathan Borba, en Pexels.

Imagen de esta página: Foto de Jonathan Borba, en Unplash.

Del Bitcoin al Ethereum

6.1 Introducción

Ethereum y Bitcoin son dos criptomonedas populares que utilizan tecnología blockchain para permitir transacciones seguras y descentralizadas. Bitcoin fue la primera criptomoneda que se creó en 2009 y su objetivo principal es ser un medio de intercambio electrónico descentralizado. Ethereum, por otro lado, fue creado en 2015 por el programador Vitalik Buterin con el objetivo de crear una plataforma descentralizada para desarrollar aplicaciones descentralizadas (DApps) y contratos inteligentes (*smart contracts*).

Ethereum también utiliza la tecnología blockchain, pero su enfoque es más amplio que el de Bitcoin. Ethereum permite a los desarrolladores crear y ejecutar aplicaciones descentralizadas en su plataforma, lo que significa que es una plataforma de computación distribuida.

Además, mientras que Bitcoin se centra principalmente en el intercambio de valor, Ethereum permite a los usuarios crear y ejecutar programas complejos de computación en la cadena de bloques. Los contratos inteligentes de Ethereum permiten crear aplicaciones que se ejecutan automáticamente cuando se cumplen ciertas condiciones, lo que significa que las aplicaciones pueden funcionar sin la necesidad de intermediarios.

6.2 El *white paper* (libro blanco) en el mundo cripto

Un white paper en el contexto de las criptomonedas es un documento técnico en el que se describe a detalle el proyecto y el protocolo en el que se basa una criptomoneda. Por lo general, los white papers son escritos por los desarrolladores del proyecto y contienen información sobre el funcionamiento del proyecto, su estructura, su tecnología, su visión y su plan de negocio. Los white papers también pueden incluir diagramas técnicos, pseudocódigo y detalles de implementación. En resumen, el white paper es un documento clave que proporciona un nivel de transparencia y credibilidad a un proyecto y ayuda a los inversores y usuarios a entender mejor el proyecto y su potencial.

Algunos ejemplos de criptomonedas o proyectos basados en blockchain que han publicado un libro blanco son:

Bitcoin: El primer y más conocido proyecto de criptomoneda, desarrollado por Satoshi Nakamoto y presentado en un white paper en 2008.

Ethereum: Una plataforma blockchain que permite a los desarrolladores construir aplicaciones descen- tralizadas utilizando contratos inteligentes. Su white paper fue publicado en 2013 por Vitalik Buterin.

Ripple: Una criptomoneda y red de pago que funciona como una plataforma de transferencia de dinero en tiempo real. Su white paper fue publicado en 2012 por Ryan Fugger.

6.2.1 El libro blanco de Bitcoin

El white paper original de Bitcoin, escrito por Satoshi Nakamoto en 2008, describe el plan y protocolo original para la criptomoneda. En este documento, Nakamoto propone un sistema de efectivo electrónico *peer-to-peer* que elimina la necesidad de intermediarios financieros y permite a los usuarios realizar transacciones directamente entre ellos a través de una red descentralizada basada en blockchain. El white paper también detalla el proceso de creación de nuevos bitcoins a través de la minería y cómo se resuelven los problemas de doble gasto y la confianza en la red. En resumen, el white paper de Bitcoin sentó las bases para el desarrollo de una nueva forma de intercambio de valor en línea a través de la innovadora tecnología de la cadena de bloques.

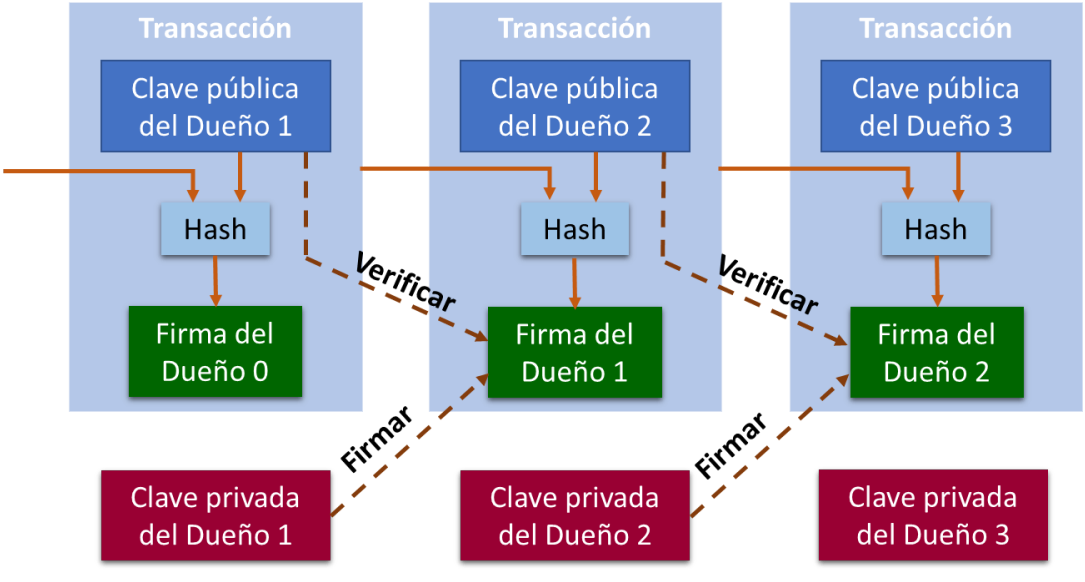
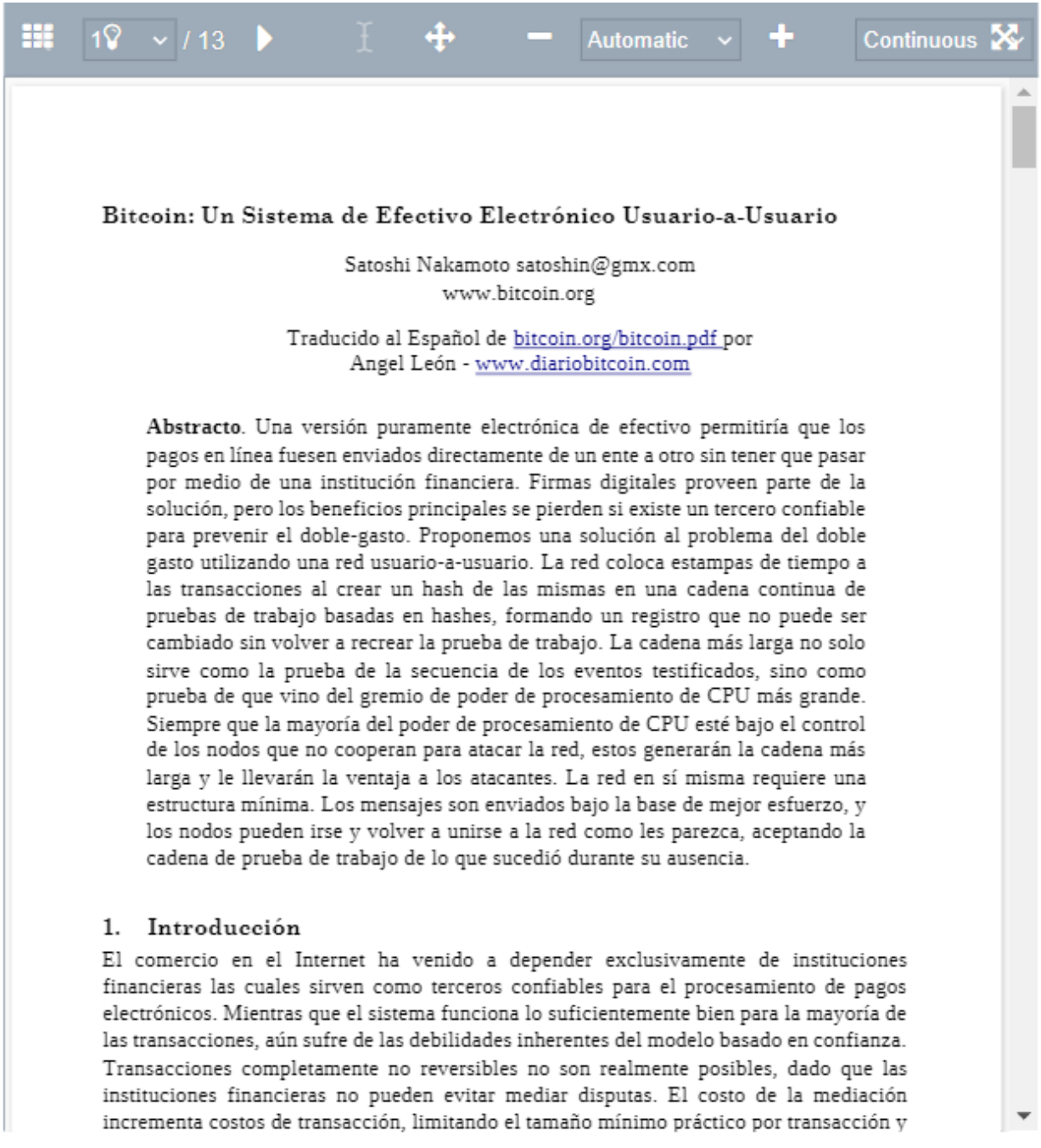


Figura 6.1. Transacciones, según el *white paper* de Nakamoto. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash de la transacción previa y la clave publica del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad.

Se destaca el uso de un sistema de **prueba-de-trabajo** similar al Hashcash de Adam Back [23] . He aquí el *white paper*:



1 / 13 Automatic Continuous

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

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

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

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

1. Introducción

El comercio en el Internet ha venido a depender exclusivamente de instituciones financieras las cuales sirven como terceros confiables para el procesamiento de pagos electrónicos. Mientras que el sistema funciona lo suficientemente bien para la mayoría de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente no reversibles no son realmente posibles, dado que las instituciones financieras no pueden evitar mediar disputas. El costo de la mediación incrementa costos de transacción, limitando el tamaño mínimo práctico por transacción y

6.2.2 El libro blanco de Ethereum

En 2014, Vitalik Buterin publica el white paper: "*Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*" (Una plataforma de aplicación descentralizada y un contrato inteligente de próxima generación), del cual extraemos dos apartados:

6.2.2.1 Historia

Figura 6.2. Harold Thomas Finney II (foto de Wikipedia).

El concepto de moneda digital descentralizada, así como aplicaciones alternativas como los registros de propiedad, ha existido durante décadas. Los protocolos anónimos de efectivo electrónico de las décadas de 1980 y 1990, que en su mayoría dependían de una primitiva criptográfica conocida como *Chaumian blinding*, proporcionaban una moneda con un alto grado de privacidad, pero los protocolos en gran medida no lograron ganar terreno debido a su dependencia de un intermediario centralizado. En 1998, el *b money* (dinero b) de Wei Dai se convirtió en la primera propuesta para introducir la idea de crear dinero a través de la resolución de acertijos computacionales, así como el consenso descentralizado, pero la propuesta era escasa en detalles sobre cómo se podría implementar realmente el consenso descentralizado. En 2005, Hal Finney introdujo un concepto de "*reusable proofs of work*" (pruebas de trabajo reutilizables), un sistema que utiliza ideas de *b-money* junto con los rompecabezas Hashcash

Figura 6.3. Adam Back (foto de Wikipedia).

computacionalmente difíciles de Adam Back para crear un concepto para una criptomoneda, pero una vez más no alcanzó el ideal al confiar en la informática confiable como backend. En 2009, una moneda descentralizada fue implementada por primera vez en la práctica por Satoshi Nakamoto, combinando primitivas establecidas para administrar la propiedad a través de criptografía de clave pública con un algoritmo de consenso para realizar un seguimiento de quién posee monedas, conocido como "prueba de trabajo".

El mecanismo detrás de la prueba de trabajo fue un gran avance en el espacio porque resolvió simultáneamente dos problemas. Primero, proporcionó un algoritmo de consenso simple y moderadamente efectivo, que permitió a los nodos de la red acordar colectivamente un conjunto de actualizaciones canónicas del estado del libro mayor de Bitcoin. En segundo lugar, proporcionó un mecanismo para permitir la libre entrada en el proceso de consenso, resolviendo el problema político de decidir quién puede influir en el consenso y, al mismo tiempo, prevenir los ataques de sibila. Lo hace sustituyendo una barrera formal a la participación, como el requisito de estar registrado como una entidad única en una lista particular, con una barrera económica: el peso de un solo nodo en el proceso de votación por consenso es directamente proporcional al poder de cómputo. que trae el nodo. Desde entonces, se ha propuesto un enfoque alternativo llamado prueba de participación (*proof-of-stake*), calculando el peso de un nodo como proporcional a sus tenencias de moneda y no a los recursos computacionales; la discusión de los méritos relativos de los dos enfoques está más allá del alcance de

este documento, pero se debe tener en cuenta que ambos enfoques se pueden usar para servir como la columna vertebral de una criptomoneda.

6.2.2.2 Ethereum

La intención de Ethereum es crear un protocolo alternativo para crear aplicaciones descentralizadas, proporcionando un conjunto diferente de compensaciones que creemos que serán muy útiles para una gran clase de aplicaciones descentralizadas, con especial énfasis en situaciones en las que el tiempo de desarrollo es rápido, la seguridad para las pequeñas y medianas empresas. Son importantes las aplicaciones que se utilizan con poca frecuencia y la capacidad de las diferentes aplicaciones para interactuar de manera muy eficiente. Ethereum hace esto mediante la construcción de lo que es esencialmente la última capa fundamental abstracta: una cadena de bloques con un lenguaje de programación completo de Turing incorporado, que permite a cualquier persona escribir contratos inteligentes y aplicaciones descentralizadas donde puede crear sus propias reglas arbitrarias de propiedad, formatos de transacción y Funciones de transición de estado. Se puede escribir una versión básica de Namecoin en dos líneas de código, y otros protocolos como monedas y sistemas de reputación se pueden construir en menos de veinte. Los contratos inteligentes, "cajas" criptográficas que contienen valor y solo lo desbloquean si se cumplen ciertas condiciones, también se pueden construir sobre la plataforma, con mucho más poder que el que ofrece la secuencia de comandos de Bitcoin debido a los poderes adicionales de la integridad de Turing, conciencia de valor, conciencia de blockchain y estado.

A continuación, presentamos el libro blanco de Ethereum en inglés (una versión en español, se encuentra en https://ethereum.org/es/). Luego, en la otra página, encontrarás 10 *white papers* adicionales, para consultar.

Ethereum Whitepaper

This introductory paper was originally published in 2013 by Vitalik Buterin, the founder of Ethereum, before the project's launch in 2015. It's worth noting that Ethereum, like many community-driven, open-source software projects, has evolved since its initial inception.

While several years old, we maintain this paper because it continues to serve as a useful reference and an accurate representation of Ethereum and its vision. To learn about the latest developments of Ethereum, and how changes to the protocol are made, we recommend this guide.

A Next-Generation Smart Contract and Decentralized Application Platform

Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or intrinsic value and no centralized issuer or controller. However, another - arguably more important - part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments (colored coins), the ownership of an underlying physical device (smart property), non-fungible assets such as domain names (Namecoin), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules (smart contracts) or even blockchain-based decentralized autonomous organizations (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

Libros blancos

Cardano | Binance | Landian | Decentraland | Theter

Lite Coin | Polygon | Solana | USD Coin | Ripple

Selecciona un libro blanco

6.3 Diferencias entre Bitcoin y Ethereum

> Ethereum y Bitcoin pueden ser de alguna manera similares cuando se trata del aspecto criptmoneda, pero la realidad es que son dos proyectos completamente diferentes con objetivos completamente diferentes. Mientras que Bitcoin se ha establecido como una criptomoneda relativamente estable y la más exitosa hasta la fecha, Ethereum es una plataforma multipropósito con su moneda digital Ether siendo sólo un componente de sus aplicaciones inteligentes para contratos (https://es.cointelegraph.com/learn/).

Arnau Ramió resume las diferencias diciendo que "Bitcoin es una moneda y Ethereum es una plataforma" ¡escuchemos!

Audio 6.1. Diferencias entre Bitcoin y Ethereum (audio tomado de Tutoriales CRIPTO en Español, en YouTube).

Ethereum, entonces, es una plataforma de código abierto, que sirve para ejecutar contratos inteligentes. Es programable, lo que significa que los desarrolladores pueden usarlo en la creación de aplicaciones descentralizadas.

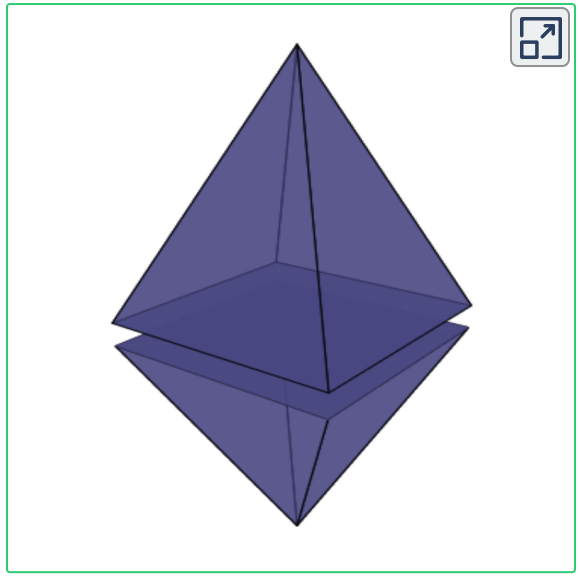
Estas aplicaciones descentralizadas (abreviado en inglés como **dapps**) se valen de la capacidad de transaccionar de las criptomonedas, la programabilidad de un contrato inteligente y la tecnología de cadena de bloques. Son confiables y predecibles, lo que significa que una vez que se cargan (minan) en Ethereum, siempre se ejecutarán según lo programado.

Pueden controlar los activos digitales para crear nuevos tipos de aplicaciones financieras. Se pueden descentralizar, lo que significa que ninguna entidad o persona los controla (Wikipedia).

Ethereum fue concebido en 2013 por Vitalik Buterin. En 2014, el trabajo de desarrollo comenzó y fue financiado por crowdfunding , y la red se puso en marcha el 30 de julio de 2015. Ethereum permite que cualquier persona implemente aplicaciones descentralizadas permanentes e inmutables en él, con las que los usuarios pueden interactuar. Las aplicaciones de finanzas descentralizadas (DeFi) brindan una amplia gama de servicios financieros sin la necesidad de intermediarios financieros típicos como corretaje, bolsas o bancos, como permitir que los usuarios de criptomonedas tomen prestado contra sus tenencias o los presten a cambio de intereses. También permite a los usuarios intercambiar NFT, que son tokens únicos que representan la propiedad de un activo o privilegio asociado, reconocido por cualquier número de instituciones. Muchas otras criptomonedas utilizan el estándar de token ERC-20 además de la cadena de bloques Ethereum y han utilizado la plataforma para las ofertas iniciales de monedas. El 15 de septiembre de 2022, Ethereum hizo la transición de su mecanismo de consenso de prueba de trabajo (PoW) a prueba de participación (PoS) en un proceso de actualización conocido como "la fusión". Esto ha reducido el uso de energía de Ethereum en un 99% (HandWiki).

Imagen central: logo de Ethereum (Wikideas1, CC0).

En la introducción de este capítulo, la IA YOU se refería a Ethereum como una criptomoneda, pero ya está claro que es una plataforma. No obstante, Ethereum también tiene su criptomoneda llamada Ether (la segunda criptomoneda en capitalización), la cual se suma a cientos de criptomonedas alternativas (**Altcoin**).



Interactivo 6.1. Logo de Ethereum en 3D, diseñado por los autores.

Con respecto a las altcoin, Daniel Krawisz defiende a Bitcoin, al expresar que:

Algunas altcoins incorporan nuevas ideas interesantes, pero hay una característica esencial de Bitcoin de la que todas carecen. No se trata de su tecnología, sino de historia y comunidad. Sencillamente, un medio de intercambio que goza de mayor aceptación en el mercado es más útil que uno que no lo es. Esto se conoce como el efecto de red. Un desequilibrio inicial entre dos medios de intercambio casi iguales beneficiará al que tenga mayor aceptación hasta que uno solo abrume al resto. No hay límite para este efecto: en última instancia, uno siempre esperaría que una moneda única superara a todos sus competidores.

Debido a que se inició antes y ha tenido una mayor oportunidad de crecer y atraer usuarios, Bitcoin tiene un mercado más grande por un amplio margen que todos los mercados de todas las altcoins juntas, y esto lo hace mucho más útil como moneda. Para derrotar a Bitcoin, una altcoin requeriría no solo una tecnología superior, sino una

tecnología tan superior como para ser un avance sobre Bitcoin comparable al avance que Bitcoin representa sobre la moneda fiduciaria. He aquí el artículo completo:

El problema con las monedas alternativas

daniel krawisz

22 de agosto de 2013

Por qué ninguna altcoin puede tener éxito

La historia de Ethereum

2013

White Paper

Documento introductorio, publicado en el 2013 por Vitalik Buterin, fundador de Ethereum, antes del lanzamiento del proyecto en 2015.

2014 2016 2019 2021

2013 2015 2017 2020

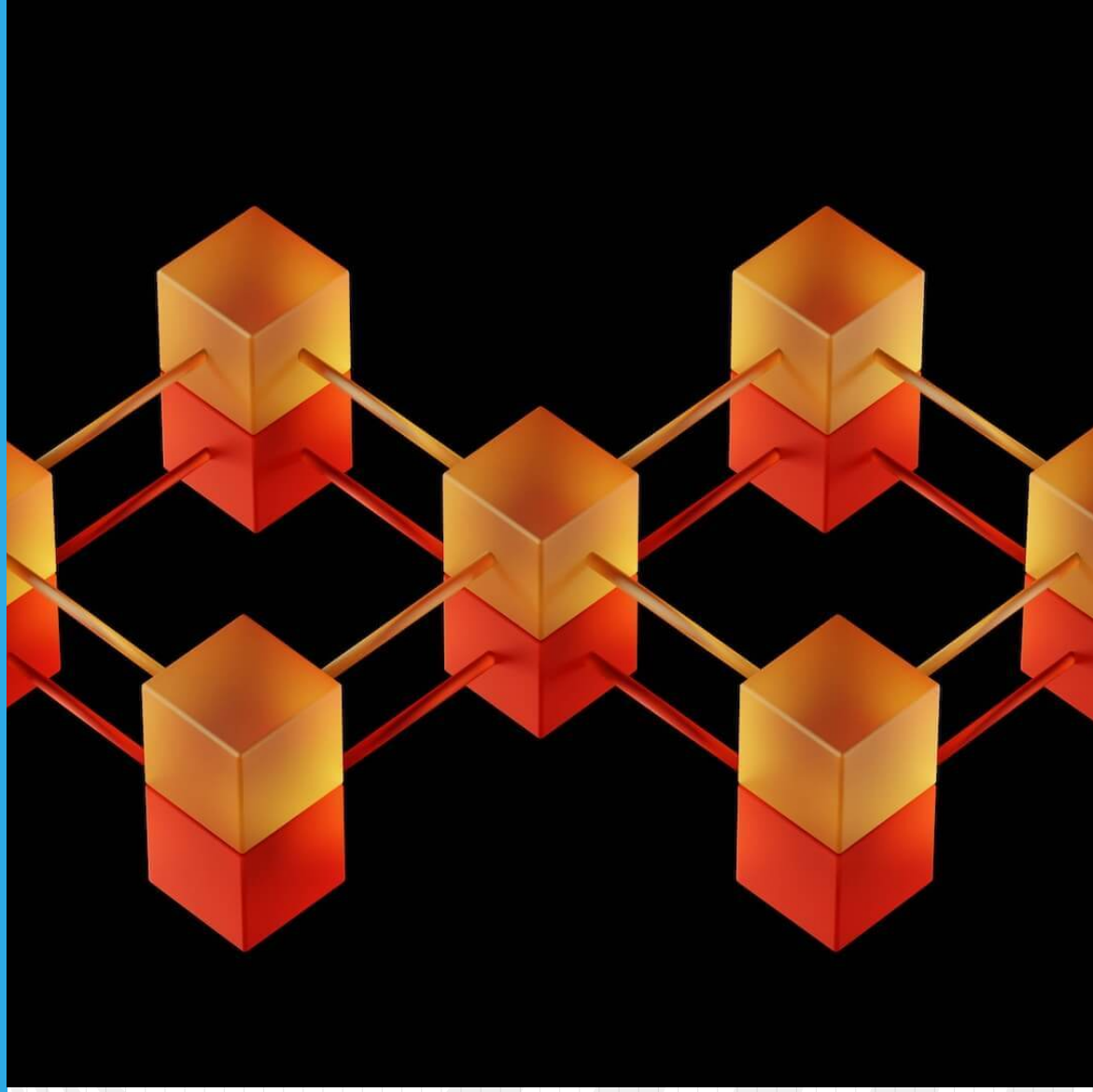
Mueve el punto naranja a lo largo de la línea de tiempo o haz clic en alguno de los puntos

Haz clic sobre la respuesta, SI/NO, en cada caso

Bitcoin fue la primera criptomoneda que se creó en 2009.	Sí	No
Los contratos inteligentes de Bitcoin permiten crear aplicaciones.	Sí	No
Hal Finney introdujo el concepto de "reusable proofs of work" (pruebas de trabajo reutilizables).	Sí	No
Nakamoto propuso un sistema de efectivo electrónico peer-to-peer que elimina la necesidad de intermediarios.	Sí	No

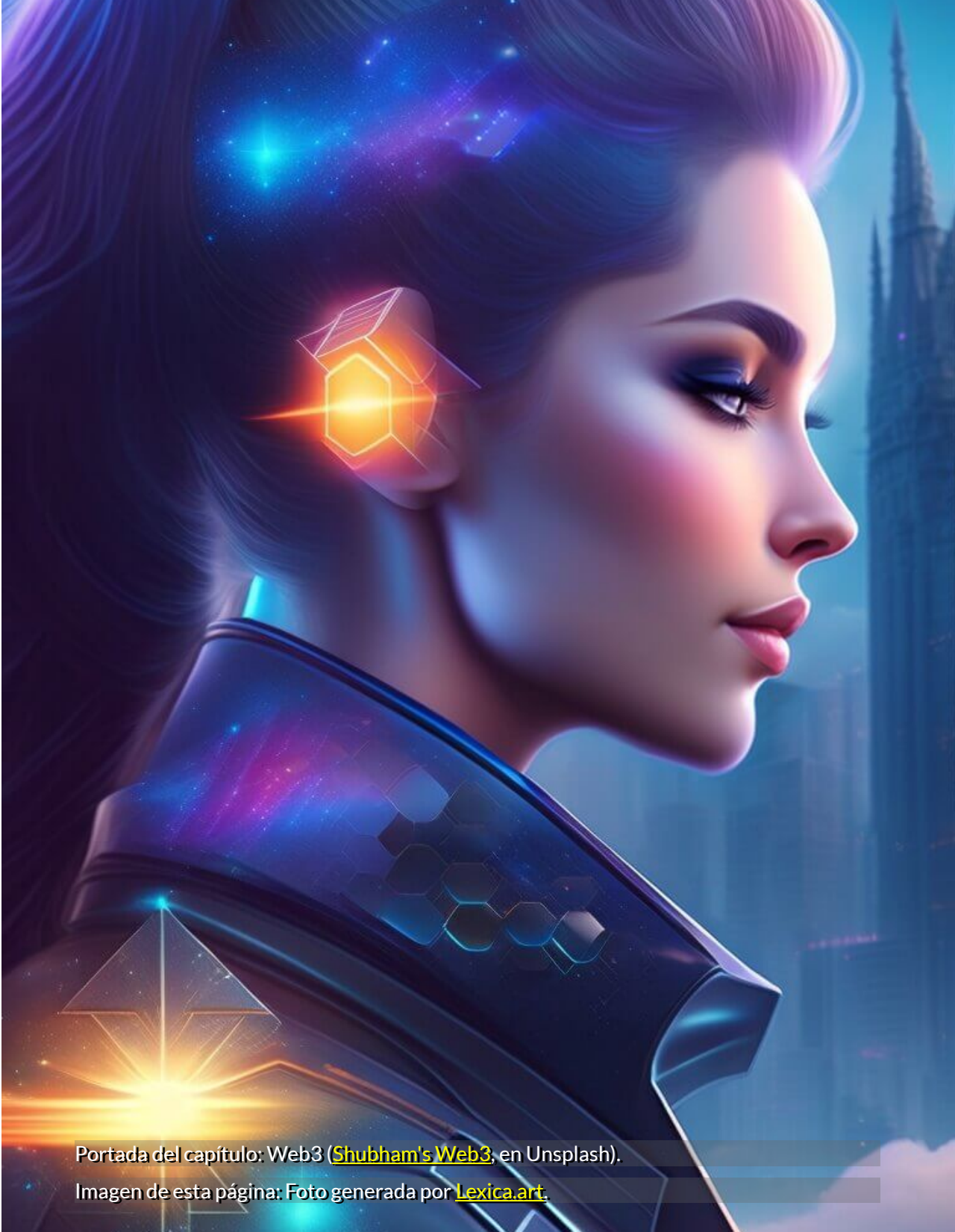
Estas afirmaciones son acerca de la plataforma Ethereum y de las criptomonedas tratadas en este capítulo.

Verificar



Capítulo 7

De la Web 3.0 a la Web3



Portada del capítulo: Web3 (Shubham's Web3, en Unsplash).

Imagen de esta página: Foto generada por Lexica.art.

De la Web 3.0 a la Web3

7.1 Introducción

La Web 3.0 y Web3 son términos que a menudo se utilizan indistintamente, pero en realidad se refieren a cosas diferentes.

La Web 3.0, también conocida como "Web semántica", es una evolución de la Web actual que busca proporcionar una experiencia más inteligente y personalizada para los usuarios. En la Web 3.0, los datos se organizan de manera más eficiente y se utilizan para crear conexiones más significativas entre los usuarios y la información.

Por otro lado, Web3 se refiere a una red descentralizada basada en blockchain que permite a los usuarios interactuar con aplicaciones descentralizadas (DApps) y contratos inteligentes. En otras palabras, Web3 es una infraestructura técnica que permite la creación de aplicaciones descentralizadas y el uso de criptomonedas y tokens digitales.

En resumen, la Web 3.0 se centra en proporcionar una experiencia de usuario más avanzada e inteligente en la Web, mientras que Web3 se centra en la creación de una infraestructura técnica que permite la creación y el uso de aplicaciones descentralizadas basadas en blockchain.

7.2 Aplicaciones descentralizadas (DApps)

Las aplicaciones descentralizadas han proliferado gracias a la creciente pujanza de tecnologías DLT (*Distributed Ledger Technologies*) como blockchain o Ethereum, donde las "DApps" sirven habitualmente para implementar contratos inteligentes (Wikipedia).

El siguiente video es un comparativo de servicios de la Web 2.0 y la Web3 (TikTok).

Imagen de esta página: Foto de Shubham's Web3.


Web 2.0
Web 3.0
App
Dapp
TikTok
@nest_protocol
nest
The First Constraint
nest
0:00 / 0:12

Según el libro blanco *The General Theory of Decentralized* Applications, una aplicación puede considerarse una "DApp" cuando cumple: i) la aplicación debe ser de código abierto y operar de forma autónoma; ii)los datos de la aplicación deben almacenarse en una cadena de bloques (blockchain) pública; iii) la aplicación utiliza algún token criptográfico, necesario para obtener acceso a la DApp; iv) la aplicación debe generar tokens, mediante algún algoritmo criptográfico.

A continuación, presentamos algunas DApps que hacen de la Web3 una realidad en el presente y el futuro más cercano de la Web 3.0.

7.2.1 Alojamiento de videos: Odysee

Odysee es una plataforma de alojamiento de videos creada en septiembre de 2020 por la compañía estadounidense LBRY.inc cuyo CEO y cofundador es Jeremy Kauffman. Se basa en el protocolo LBRY, de código abierto, el cual está basado en una red descentralizada de compartición de ficheros peer-to-peer, donde se alojan los contenidos, y una cadena de bloques que proporciona:

- Un índice de contenidos publicados disponibles en la red que permite como descubrir contenido.
- Un sistema de pago y registro por el visionado o descarga de contenido de pago.
- Un proveedor de identidad criptográfica de publicadores de contenido (Wikipedia).

El siguiente video se encuentra en TikTok[14], también se ha alojado en Odysee.

[14] TikTok y TouTube son plataformas centralizadas (Web 2.0) que permiten el control centralizado por parte de empresas privadas que buscan el beneficio económico o, posiblemente, acciones de espionaje como se ha denunciado contra TikTok.


WEB 2.0
YouTube
WEB 3.0
Odysee
nest
The First Constraint
The Second Constraint
TikTok
@nestfans
0:06 / 0:13

Sobre las redes sociales actuales, Evan Malmgren [24] expresa que

estas plataformas no intentan fomentar la conexión humana, sino empujar a los usuarios "a comportarse de forma que sean lo más legibles posible para los sistemas automatizados que los rastrean y analizan"

7.2.2 El navegador Brave

Como lo hemos dicho, las DApps residen en redes descentralizadas, mientras que aplicaciones como las redes sociales tradicionales existen en redes centralizadas.

Las DApps desempeñan un papel fundamental en el proceso de transición entre la experiencia actual que brinda la Web 2.0 y el universo funcional de oportunidades y libertades de la Web3. Por ejemplo, el navegador **Brave** brinda una experiencia similar a la de Google Chrome o Firefox, pero ofrece valor añadido, como un criptomonedero integrado que permite interactuar con las DApps. Además, el navegador Brave admite funciones de **privacidad** que se ajustan al dogma de la descentralización (brave.com).

Brave es un navegador web de código abierto basado en Chromium, creado por la compañía Brave Software en el año 2016, fundada por el cofundador del Proyecto Mozilla y creador de JavaScript, Brendan Eich.

El siguiente video es tomado de TikTok.


WEB 2.0 APPS
WEB 3.0 DAPPS
Chrome
Brave
TikTok
@nest_protocol
0:00 / 0:13

7.2.3 El servicio de música Audius

Audius es un servicio de transmisión de música descentralizado basado en blockchain con capacidades de redes sociales . Está impulsado por una comunidad de código abierto de artistas, fanáticos y desarrolladores y tiene su propio token criptográfico nativo , AUDIO. En julio de 2021, Audius tenía más de cinco millones de usuarios activos mensuales.

Audius es un protocolo de transmisión y uso compartido de música basado en criptografía diseñado para brindar a los artistas más control sobre la monetización de su música que los servicios de transmisión tradicionales, al mismo tiempo que les permite colaborar de manera directa y sin problemas para ponerse en contacto con sus fanáticos. Detrás de Audius está la empresa Audius Inc. de San Francisco (Wikipedia).

7.2.4 Almacenamiento en la nube con Storj

Storj es una plataforma de código abierto de almacenamiento en la nube, su principal novedad es que funciona de una forma descentralizada (sin intermediarios) a través de más de 13.000 nodos repartidos por todo el mundo. Cualquier usuario con un PC puede crear un nodo y recibir ganancias por ello. El token o criptomoneda Storj se puede comprar en las principales plataformas como Binance o Coinbase entre otras (Academia Finanzas).

Storj es una alternativa a las plataformas de almacenamiento en la nube como las que ofrecen Amazon o Google.


WEB 2.0
WEB 3.0
Spotify
Audius
nest
TikTok
@nest_protocol
0:00 / 0:15

7.3 La web en 3D

Otro posible destino para la Web 3.0 es la dirección hacia la visión 3D, liderada por el *Web3D Consortium*[15]. Esto implicaría la transformación de la Web en una serie de espacios 3D, llevando más lejos el concepto propuesto por Second Life. Esto podría abrir nuevas formas de conectar y colaborar, utilizando espacios tridimensionales (Wikipedia).

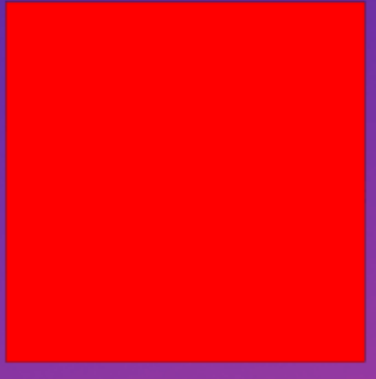
La web en 3D es un fenómeno con el cual las páginas web se están convirtiendo en entornos en tercera dimensión.

Metaversos, Realidad Aumentada, Realidad Virtual e Inteligencia Artificial, son conceptos que se relacionan más de lo que pensamos en esta nueva etapa de la era digital, donde las tecnologías comparten la idea de utilizar los datos de nuestro mundo para parecerse y comprender mejor nuestra realidad. Con la llegada de tecnologías como OpenGL, WebGL y Three.js (lenguajes de visualización de 3D) se implementó el plano de profundidad, permitiéndonos un desplazamiento más libre con la sensación de acercarnos, alejarnos, subir, bajar y movernos lateralmente. La llegada de esta tecnología también incorporó la posibilidad de añadir objetos con profundidad, dando origen a los espacios y elementos 3D que actualmente componen gran parte del metaverso y experiencias XR como la Realidad Aumentada o la Realidad Virtual. (Leonel Pérez, en Linkedin).

[15] Web3D es una organización sin fines de lucro que desarrolla y mantiene los estándares internacionales X3D, VRML y HAnim. Estos son formatos de archivo de gráficos 3D y especificaciones de tiempo de ejecución para la entrega e integración de datos 3D interactivos a través de redes. Los miembros del Consorcio Web3D trabajan juntos para producir capacidades abiertas, libres de regalías y con certificación ISO para la Web.

Una página HTML usando la librería JavaScript X3DOM

Con clic sostenido,
mueve los objetos



Algunas Web3D

	**SBS City**. Una ciudad 3D interactiva basada en un sitio inmersivo que permite descubrir la información relacionada con la empresa de una manera lúdica (open-sbs.brig.ht).
	**Admire Amaze**. Este viaje a través del sitio web de comercio electrónico de De Bijenkorf comienza con una abeja. Las chispas parpadean mientras flota y se lanza a través de un denso bosque, llegando a los tesoros ocultos que son sus productos (https://admireamaze).
	**Enric Moreu**. Un cielo azul con nubes angulosas y una figura solitaria de pie sobre un terreno flotante abre este currículum digital de Eric Moreu . Al desplazarte hacia abajo, gira esta isla flotante y te lleva a la siguiente escena colorida suspendida en el aire (resume).
	**LE JARDIN Extraordinaire**. Descubre el jardín provenzal de PHA5E. En este jardín descubrirás una selección floral gracias a la cual podrás crear tu jardín en realidad aumentada (lejardin).

En la página siguiente, puedes ver video clips de estos cuatro ejemplo (haz clic en los botones superiores, para ver el video que desees).


SBS City
Admire Amaze
Enric Moreu
Le Jardin
Revolutionary
Financing
SBS
Innovation
Kickoff
0:00 / 0:05

Arrastra las imágenes al contenedor correspondiente

CLASIFICA

Web 2.0	Web3
YouTube Spotify	

PayPal

Audio Glosario

El audio sobre NFT fue tomado de Tutoriales CRIPTO en Español y el audio sobre Web3 de interesante, ambos bajo Licencia Atribución de Creative Commons. Los demás audios son de los autores del libro.

Bibliografía

[1] Gozalbes, M. (2011), *Historia del dinero: guía de sala*. Museu de Prehistòria de València, Valencia (España), 75 p.

[2] Viales, R. J., (2008). La evolución histórica de la moneda y de los sistemas monetarios. Bases conceptuales para estudiar la historia monetaria de Costa Rica del siglo XVI a la década de 1930. *Diálogos Revista Electrónica de Historia*, 9(2): 267-291.

[3] Gozalbes, M.; Torregrosa, J.M. (2014). De Iberia a Hispania. Plata, dracmas y denarios entre los siglos VI y I a.C. *Archivo de Prehistoria Levantina*, Valencia, Vol. XXX: 275-316.

[4] Mela, José; Cedeño, Edwin (2020). Tecnologías Blockchain y sus aplicaciones. *Visión Antataura*, Vol. 3, núm. 2, pp. 110-126.

[5] Dumitriu, Petru (2020). *Aplicaciones de las cadenas de bloques en el sistema de las Naciones Unidas: hacia un estado de disponibilidad operacional*. Naciones Unidas, Ginebra.

[6] Espinosa, Sergio (2020). *Guía de Referencia para la adopción e implementación de proyectos con tecnología blockchain para el Estado colombiano*. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Colombia.

[7] Lapointe, Cara; Fishbane, Lara (2019). The Blockchain Ethical Design Framework. *Innovations Technology Governance Globalization*, Vol. 12, núm. 4, pp. 50-71.

[8] Swan, Melanie (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc, United States of America.

[9] Benítez-Eyzaguirre, Lucía (2021). Blockchain para la transparencia, gestión pública y colaboración. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, Vol. 18, núm. 1, pp. 23-32.

[10] Sedrati, Anass; Abdelraheem, Mohamed; Raza, Shahid (2021). *Blockchain and IoT: Mind the Gap*. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 113–122.

[11] Kleinerman, Kenny (2022). Aplicaciones De La Computación En La Nube Basada En Blockchain. *RIDGE*.

[12] Díaz, J.; Sánchez, A. (2014), *BITCOIN: Una moneda criptográfica*. Instituto Nacional de Tecnologías de la Comunicación, España, 46 p, disponible en https://www.incibe-cert.es/ .

[13] Champagne, P. (2014), *El Libro de Satoshi*. Edición BlockchainEspana.com, 353 p, disponible en https://libroblockchain.com/satoshi/.

[14] Tierno, P. (2023), *Cryptocurrency: Selected Policy Issues*. Congressional Research Service. Reporte, disponible en https://crsreports.congress.gov/.

[15] Weaver, N. (20222), *The Death of Cryptocurrency: The Case for Regulation*. Digital future whitepaper series. Yale Low School, disponible en https://law.yale.edu/.

[16] Swan, Melanie (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc, United States of America, 149 p.

[17] Millán, R.J. (2019). La cadena de bloques segura, inalterable, transparente… y disruptiva!. *bit* , núm. 212, pp. 56-60, disponible en https://www.coit.es/ .

[18] Mystakidis, S. (2022). Metaverse. *Encyclopedia*, núm. 2, pp. 486-497, https://doi.org/10.3390/encyclopedia2010031.

[19] Dionisio, John; Burns III, William; Gilbert, Richard (2013). 3D Virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*. Vol. 45, núm. 3, pp. 1-38, https://doi.org/10.1145/2480741.2480751.

[20] Caumartin, A. (2022). ¿Qué son los tokens ERC y por qué los utilizamos? *Ledger Academy*. En línea, disponible en https://www.ledger.com/.

[21] Ante, L. (2022). The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum. *FinTech*. Vol. 1, núm. 3, pp. 216-224, https://doi.org/10.3390/fintech1030017.

[22] Saeed, F.; Seyed, H.; Qiang, Q.; et al. (2022). The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum. *Procedia Computer Science*. Num. 214, pp. 755–762, https://doi.org/10.3390/fintech1030017.

[23] Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. *hashcash.org*. Documento en línea, disponible en http://www.hashcash.org/papers/.

[24] Malmgren, E. (2022). Así debería ser internet": cómo una plataforma pionera está desintoxicando las redes sociales. *Business Insider*. Documento en línea, disponible en https://www.businessinsider.es/.


DESCARTES
matemáticas interactivas