BITCOIN, CRIPTOMONEDAS Y TOKENS

BREVE GUÍA TEÓRICO-PRÁCTICA PARA PRINCIPIANTES

MÓNICA CASTRO

Monica Castro

Bitcoin, criptomonedas y tokens

Аннотация

Guía breve con aspectos teóricos y prácticos acerca de bitcoin, las criptomonedas y la tecnología vinculada a su desarrollo y funcionamiento. Libro orientado a lectores principiantes.

Содержание

Table of Contents	4
Bitcoin, criptomonedas y tokens, Breve guía teórico-práctica para principiantes por Mónica Castro Plaza	7
Introducción	9
I. Contexto y fundamentos teóricos	11
¿Qué es Bitcoin?	12
¿Por qué se llama “cripto” moneda?	13
Contexto de nacimiento de Bitcoin	14
¿Quién creó Bitcoin?	16
Bitcoin y tecnologías involucradas	18
Qué es blockchain (o cadena de bloques)	19
¿Por qué la tecnología blockchain es diferente a otras bases de datos?	20
Конец ознакомительного фрагмента.	22

Table of Contents

Información editorial
Introducción
I. Contexto y fundamentos teóricos
¿Qué es Bitcoin?
¿Por qué se llama “cripto” moneda?
Contexto de nacimiento de Bitcoin
¿Quién creó Bitcoin?
Bitcoin y tecnologías involucradas
¿Qué es blockchain?
¿Por qué la tecnología blockchain es diferente a otras bases de datos?
Clasificación de blockchain
Los participantes de la red Bitcoin
II. Los mitos sobre bitcoin
1. Bitcoin es una estafa
2. Bitcoin es una burbuja financiera
3. Bitcoin es anónimo y por eso lo utilizan delincuentes
4. Bitcoin es un sistema inseguro donde se puede perder dinero
5. Bitcoin contamina el ambiente
III. Lo que vino después de Bitcoin
La red Ethereum
Los contratos inteligentes o smart contract

Criptomonedas y tokens
IV. Aspectos prácticos en el uso de criptomonedas y token
Dónde se almacenan las criptomonedas o token
Aspectos de seguridad en wallets
Dónde se compran las criptomonedas y token
Aspectos de seguridad en plataformas
V. Oportunidades de ahorro e inversión
Holdear
Inversión en criptomonedas y tokens
ICO (Oferta Inicial de Criptomoneda)
Algunas herramientas de análisis de criptomonedas, token, ICO
Trading de criptomonedas
VI. Las finanzas descentralizadas (DEFI)
¿Qué es DEFI?
Requerimiento de participación en DEFI
Yield farming o agricultura de rendimiento
Préstamos
Aspectos de seguridad en DEFI
VII. El mercado del trabajo creativo en blockchain
Los NFT o Tokens No Fungibles
VIII. Recursos y herramientas para seguir aprendiendo
Lista de recursos y herramientas de consulta
Agradecimientos
Achicrip
Criptonoticias

Cryptea
Acerca de la autora

Bitcoin, criptomonedas y tokens, Breve guía teórico-práctica para principiantes por *Mónica Castro Plaza*

Registro de propiedad intelectual
2021-A-8332
Registro ISBN
978-956-9822-08-7
Registro en red Bitcoin 1
Tx
5c8704b1d85dfb3bdf2aaea1175cf0c96cb6722f49c5ef3dd8c7d
Imagen de portada
Libros Móviles
Corrección de textos
Cristian Vázquez
Libros Móviles Editores
Santiago de Chile, julio 2021

1 El registro de propiedad intelectual en la red Bitcoin consistió en la carga de un documento que contiene los datos principales de este libro (título del libro, autora, nacionalidad, etc) subidos a la blockchain a través de Proof of existence (prueba de existencia) que asignó al documento un código de transacción y una marca de tiempo.

El trámite tardó 10 minutos en hacerse efectivo.

Puedes descargar desde aquí el documento y subirlo al sitio Proof of existence para vincularlo a la transacción.

Introducción

La primera vez que oí hablar de bitcoin fue a través del documental Deep web. Relataba la existencia de un mercado llamado Silk Road. Ahí se ofertaban de manera libre toda clase de estupefacientes para uso personal. La moneda de cambio era bitcoin. Se trató de una experiencia de naturaleza "libertaria", es decir, apegada a una visión política que promueve, por sobre cualquier idea, la facultad de decidir sobre la propia vida. Cualquiera sea la opción escogida. La iniciativa terminó con uno de sus creadores, Ross Ulbricht, encarcelado hasta el día de hoy.

La segunda vez, fue con una de las alzas históricas del precio, ocurrida a fines de 2017, cuando bitcoin alcanzó cerca de los 20 mil dólares. El entusiasmo general duró hasta que inició un largo recorrido en sentido contrario, pero hizo que varios nos quedásemos a tratar de comprender de qué se trataba todo este asunto de una moneda digital. No emitida por bancos. Ni controlada por el gobierno de turno.

Y quedarse, o entrar en la "madriguera de bitcoin", como dicen algunos, no significó solo seguir por un largo camino para entender cómo funcionaba su compleja tecnología. También fue sentir por primera vez curiosidad sobre cómo funcionaba la economía, el mercado, el sistema financiero. Quitarle al dinero su aura de pecado capital -escuela en la que muchos hemos sido educados- y comprender su poderoso rol a través de toda la

historia de nuestra civilización.

Bitcoin constituye para mí el símbolo del dinero tal como lo concebimos en los inicios de la historia: una herramienta de intercambio, que surgía de manera espontánea, para resolver las limitaciones del trueque. Un instrumento para ponernos de acuerdo al momento de interactuar con el fin de promover y asegurar nuestra sobrevivencia. Una forma de poder individual y colectivo, que nos permite desenvolvernos en las aguas, a veces turbulentas, del ciclo de la vida.

Con el tiempo, este dinero digital, ha sido naturalmente aceptado por personas de todas partes del mundo, que no se vieron jamás. Porque quienes entran en bitcoin, saben que la confianza ha sido rota demasiadas veces por custodios y "benefactores" y ya no quieren ser la contraparte obligada de esos contratos sociales que nunca firmaron. Y este universo alterno llamado Bitcoin, se hace cada vez más grande, más diverso y más eficiente.

Este manual es una invitación a conocer, participar y seguir aprendiendo de este ecosistema, que crece cada día más y donde se comparten los valores de la autonomía, la libertad y la responsabilidad personal. Y espero sinceramente, que su contenido sea una puerta de entrada para todo aquel que elija dejarse caer por esta encantadora madriguera.

La autora

I. Contexto y fundamentos teóricos

¿Qué es Bitcoin?

Bitcoin es una red de pagos que emite su propio dinero, también llamado bitcoin[1] (BTC). Esta red de pagos funciona a través de procesos informáticos, basados en matemáticas.

Estos procesos permiten, por una parte, la transferencia de bitcoin (envío y recepción) y por otra, que la red permanezca segura ante cualquier ataque.

[1] Escribiremos “Bitcoin” con mayúscula inicial cuando hablemos de la red de pagos. Y “bitcoin” con minúscula inicial, cuando hablemos de la criptomoneda.

¿Por qué se llama “cripto” moneda?

Se llama criptomoneda porque la red Bitcoin **utiliza técnicas criptográficas** o de cifrado de información, con el fin de ejecutar las tareas y funciones necesarias para que la red opere con altos estándares de seguridad.

Ente otras funciones, el uso de técnicas criptográficas permite a la Red crear llaves (o claves) que equivalen a firmas que se vinculan a un propietario.

Una **llave o clave pública** es un código alfanumérico que se comparte con otros usuarios para **recibir btc**.

Una **llave o clave privada** es un código alfanumérico que permite **enviar/gastar btc.**

Si lo comparamos con una cuenta bancaria, la llave pública vendría a ser el número de cuenta y la llave privada, la clave de acceso a dicha cuenta.

Por otra parte, el uso de criptografía impide que las transacciones puedan ser corrompidas, asignándoles a cada una su propia “huella digital”.

Contexto de nacimiento de Bitcoin

El origen de Bitcoin lo podemos encontrar en el grupo autodenominado "cypherpunk". Se trata de una agrupación de desarrolladores e informáticos (principalmente), pero también de personas de otras áreas del saber (abogados, periodistas, profesores, etc.).

Comenzaron a reunirse en el año 1992 y se comunicaban a través de un foro en internet. Enfocaban su discusión en la necesidad de privacidad en el ambiente digital, en un contexto en que el uso de internet empezaba su proceso de masificación.

A la par, algunos de ellos desarrollaban herramientas basadas en la criptografía o cifrado de datos, mediante lenguajes creados para comunicarse a través de claves o códigos secretos. Estas herramientas se fundan en uno de los preceptos más importantes del cypherpunk: "Privacidad es el poder de mostrarse selectivamente al mundo", es decir, las personas debiéramos ser dueñas de nuestra información y tener la facultad de compartirla solo con quienes nosotros decidamos.

Este contexto es relevante, puesto que es aquí donde **nace la preocupación por crear un dinero privado** que pudiera separar nuestras transacciones de valor de nuestros datos personales.

Contrapuesto así al dinero fíat -o dinero de curso legal- donde muchos de los movimientos que hacemos con él, quedan

informados tanto a los bancos como a los organismos del Estado. Especialmente en el caso de que estos movimientos se realicen mediante la versión digital del dinero fíat, es decir, el que utilizamos para hacer pagos en entornos digitales (internet).

Cabe mencionar también que muchos cypherpunk **se consideraban libertarios e incluso anarcocapitalistas.** Estos movimientos comparten la idea de que a través de la historia no ha existido peor administrador de los recursos que las instituciones del Estado, sumado al hecho de que, siendo su mecanismo de financiamiento la tributación coercitiva (el que no paga impuestos recibe una multa o va a la cárcel), dichas instituciones no se ven obligadas a dar cuenta de la ineficiencia o corrupción sobre los recursos tributados.

Los Estados, junto con los Bancos Centrales, serían los primeros responsables en monopolizar la tenencia de dinero, riqueza y, por ende, el poder. Este vínculo sería también el principal generador de crisis económicas con su consecuente empobrecimiento de la población.

El dinero privado sería entonces una forma de "descentralizar" este poder, permitiendo a los ciudadanos y ciudadanas volver a ser los dueños del fruto de su trabajo (dinero y riqueza). Por consiguiente, cada persona se convertiría en la administradora y custodia principal de su patrimonio monetario, limitando tanto el control como la dependencia de instituciones estatales y/o financieras.

¿Quién creó Bitcoin?

Se conoce como el creador de la red Bitcoin a **Satoshi Nakamoto**.

Su identidad permanece en el anonimato al día de hoy, pero se sabe que formaba parte de los cypherpunks, quienes se comunicaban principalmente, mediante una lista de correos.

El 31 de octubre de 2008, Nakamoto envió a dicha lista el siguiente mensaje:

He estado trabajando en un nuevo sistema de efectivo electrónico que es totalmente de usuario a usuario (peer-to-peer) sin un tercero de confianza.

Seguidamente compartía un link a un documento llamado "whitepaper" o libro blanco, donde explicaba en detalle cómo funcionaría la Red. Se sabe que el proyecto fue recibido al principio con cierta desconfianza, sin embargo, algunos desarrolladores se sumaron desde sus inicios, al trabajo de construcción y prueba de la Red.

Unos meses después, el 12 de enero de 2009, se realizó la primera transacción en bitcoin. Satoshi Nakamoto transfirió la suma de 10 BTC a Hal Finney, un desarrollador que fue también el primero en ejecutar el software de Bitcoin.

Desde su primera transacción, Bitcoin ha sido blanco de algunos eventos de ataque, tales como intentos de robo o de vulneración de la Red. Sin embargo, todos fueron detectados o

resueltos de manera temprana, considerándose, a la fecha, **como una de las redes más seguras jamás creadas.**

Bitcoin y tecnologías involucradas

El protocolo que permite el funcionamiento de Bitcoin es un compendio de varias tecnologías que incluyen la criptografía, mecanismos de consenso (o acuerdo entre los participantes de la Red), prueba de trabajo (o poder de cómputo que se destina a la red para evitar ataques), blockchain o cadena de bloques, entre otras.

No es el objetivo de la presente guía para principiantes, explicar en detalle todos los protocolos involucrados, pero si quieres profundizar en el funcionamiento de la Red, desde el punto de vista técnico, te recomiendo visitar este video, que lo explica paso a paso.

No obstante, abordaremos más en detalle la tecnología blockchain. Esto, debido a que, siendo Bitcoin su primer caso de uso, se convirtió en la columna vertebral de muchas otras criptomonedas y proyectos tecnológicos que vinieron después.

Qué es blockchain (o cadena de bloques)

En primer lugar, es una base de datos virtual. Es decir, un espacio donde se puede registrar y almacenar cualquier tipo de información.

Esta información se guarda en bloques, que se van encadenando de manera sucesiva, formando una “cadena de bloques”.

Se suele comparar a la blockchain con los cuadernos de contabilidad de una empresa. Cada nuevo cuaderno, con nueva información, vendría a ser un “bloque”.

En el caso de la red Bitcoin, la información que almacena su blockchain son todas las transacciones de pago que ocurren con BTC.

Como se trata de un dinero privado, no almacena datos personales como nombre, domicilio o documento de identidad de quien emite o recibe un pago.

¿Por qué la tecnología blockchain es diferente a otras bases de datos?

Antes de la aparición de la red Bitcoin, las bases de datos se manejaban a nivel institucional o privado. En este contexto, toda la información vinculada a una institución financiera, bancaria, empresarial o gubernamental, se encuentra bajo la custodia de unos pocos actores autorizados, que pueden manejar -o corromper- a discreción los datos que guardan de clientes, ciudadanos u otros actores.

Con la irrupción de Bitcoin y una de sus tecnologías principales, blockchain, se vuelve posible contar con una base de datos cuya información se puede distribuir entre diversos actores, sin tener un dueño principal. Cada uno de estos actores, puede descargarse una copia de dicha información y, gracias a ello, actuar como un agente que valida la veracidad de los datos.

En este sentido, la incorruptibilidad de los datos en una blockchain es proporcional a la cantidad de usuarios que posean una copia de esta. Mientras más usuarios participen de la red, más descentralizada se encontrará la información y más difícil se hará corromper o manipular datos.

Para comprender la diferencia, podemos retomar la idea del cuaderno de contabilidad: si en una institución, solo dos o tres personas tienen una copia de este cuaderno, resulta más o

menos sencillo ponerse de acuerdo y cambiar información del cuaderno, asociada, por ejemplo, a un fraude monetario (robo o uso indebido de recursos).

Si en esa misma institución, más de la mitad de sus integrantes tiene una copia de dicho cuaderno, se vuelve mucho más complejo realizar cualquier cambio o modificación para ocultar o modificar información sensible. Es más sencillo ponerse de acuerdo para corromper información, entre dos o tres personas, que entre cincuenta o cien.

Lo mismo ocurre con una blockchain, que no es más que un cuaderno de contabilidad digital, pero que tiene el potencial de integrar cientos, miles o millones de participantes en todo el mundo, que posean y resguarden una copia de la información.

Mientras más actores se hagan parte de una red blockchain, más descentralizada se considera dicha red, siendo Bitcoin la que mejor cumple, a la fecha, con el concepto de descentralización.

Конец ознакомительного фрагмента.