

Conceptos Básicos de Criptomonedas

Qué es Bitcoin?

Bitcoin: A Peer-to-Peer Electronic Cash System

Es decir, un “**Sistema de Efectivo Electrónico de Par a Par**”. Así lo definió Satoshi Nakamoto en el Whitepaper (un manifiesto técnico) publicado en 2008.

Hasta hoy (August 2022), puedes ver el Whitepaper aquí:

- <https://bitcoin.org/bitcoin.pdf>
- <https://www.bitcoin.com/bitcoin.pdf>
- <https://bch.info/bitcoin.pdf>

¿Qué significa “De Par a Par”?

Significa eliminar a los intermediarios en las transacciones de monedas:

- Separar Moneda del Estado.
- Separar Moneda de los Bancos.
- Separar Moneda de las Corporaciones.
- Separar Moneda de cualquier otro intermediario.

Qué significa “Efectivo Electrónico”?

En mi opinión significa que fusiona las buenas características monetarias del efectivo con el soporte electrónico que permite potenciarlas:

- Privacidad del efectivo.
- Fungibilidad del efectivo.
- Abierto (sin fronteras) ya que es electrónico.
- Transportabilidad ya que es electrónico.

Bitcoin inaugura el concepto de CRIPTOMONEDA.

¿Por qué "cripto"?

Porque utiliza la criptografía (sistema para encriptar y desencriptar información) para asegurar las transacciones.

Lo cual permite en Bitcoin que cada usuario (dueño de una “private key”) tenga soberanía monetaria sobre sus monedas.

También permite a los usuarios transaccionar libremente sin la necesidad de intermediarios.

También elimina el problema del doble-gasto. El sistema de reserva fraccional, por ejemplo, no existe en Bitcoin.

Mutabilidad

Dado que Bitcoin es también una aplicación informática (la implementación de este sistema de efectivo electrónico p2p), el grupo de desarrolladores que lo mantiene y actualiza, introduce cambios en esta app.

Por lo tanto, Bitcoin y otras criptomonedas son DINERO QUE MUTA EN EL TIEMPO.

Algunas mutaciones podrían potenciar las características que lo hacen efectivo electrónico de par a par

Pero algunas otras mutaciones podrían ser tan bruscas como para socavar los fundamentos del sistema

Y eso es lo que hoy está pasando en la mayoría de las más famosas y mal llamadas “criptomonedas”.

Hay una guerra de propaganda

Y el escenario hoy luce así:

- Marketing
- Estafas
- Desinformation
- Distracciones
- Censura
- Ignorancia
- Historia borrada
- Cambios en el significado de los conceptos

Entonces, repasemos y veamos unos ejemplos:

Estás usando Bitcoin

- Si estás en una blockchain que puede usarse como efectivo electrónico p2p.
- Si nadie puede pedirte KYC para permitirte usar tus monedas.
- Si nadie puede congelar o confiscar tus monedas.
- Si nadie puede prohibir o cancelar tus transacciones.
- Si nadie controla la mayoría de los nodos de la blockchain.

No estás usando Bitcoin

- Si estás en una blockchain que no puede usarse como efectivo electrónico p2p.
- Si un intermediario te pide KYC para permitirte usar tus monedas.
- Si un intermediario puede congelar o confiscar tus monedas.
- Si un intermediario puede prohibir o cancelar tus transacciones.
- Si un organismo controla la mayoría de los nodos de la blockchain.

Cómo usar Bitcoin?

1. Crear una billetera donde tengas control de la private key (eso te hace dueño de las monedas de esa billetera).
2. Usarla de par a par.

Listo.

Si quieren investigar más por su cuenta, aquí hay algunos conceptos importantes y alguna información interesante:

Conceptos

- Blockchain.
- Decentralization.
- Nodes.
- Mining.
- Proof of Work.
- Private Key.
- Public Key.
- Not Your Keys Not Your Coins.
- Bitcoin monetary policy.
- Fees.
- Block size.

Información

- Los Whitepapers de las criptomonedas en las cuales estén interesados.
- Andreas Antonopoulos work:
 - Web: <https://aantonop.com/>
 - The Internet of Money (book)
 - Mastering Bitcoin (book)
 - Mastering Ethereum (book)
- Documentary of BCH origin:
<https://odysee.com/@laeternavigilancia:4/who-killed-bitcoin-full-doc:4>