

Cryptocurrencies Basic Concepts

# What is Bitcoin?

# Bitcoin: A Peer-to-Peer Electronic Cash System

This is the way Satoshi Nakamoto defined it on the Whitepaper (technical manifesto) published in 2008.

Until today (August 2022), you could read the Whitepaper here:

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

---

# What does “peer-to-peer” mean?

It means removing third parties from money transactions:

- Separate money from government.
- Separate money from banks.
- Separate money from corporations.
- Separate money from any other third party.

---

# What does “Electronic Cash” mean?

IMHO it mixes the good currency features of cash with the electronic support that potentiates them:

- Privacy of cash.
- Fungibility of cash.
- Openness (without borders) as it is electronic.
- Transportability as it is electronic.

# Bitcoin inaugurates the concept of CRYPTOCURRENCY.

Why "crypto"?

Because it uses cryptography (system of encrypting and decrypting information) to secure the transactions.

It allows that in Bitcoin each user (owner of a private key) has monetary sovereignty of their own coins.

It also allows users to freely transact between one another without the need for an intermediary.

And it also avoids the double-spend issue. Fractional-reserve system, for example, does not exist on Bitcoin.

# Mutability

Since Bitcoin is also a software application (the implementation of the p2p e-cash system), the group of developers that maintains and updates it introduces changes that modify this application.

Therefore, Bitcoin and the other cryptocurrencies are  
MONEY THAT MUTATES  
OVER TIME.

Some mutations could  
potentiate its characteristics  
as a p2p e-cash

These mutations can be so  
forceful as to undermine the  
foundations of the system.

And that is what is happening  
in the majority of famous and  
wrong-called  
cryptocurrencies today.

# There is a propaganda war

And the scenario today looks like:

- Marketing
- Scams
- Misinformation
- Distraction
- Censorship
- Ignorance
- Erasing history
- Changing the meaning of concepts

# So lets recap and give some examples:

## You are using Bitcoin

---

- If you are in a blockchain that can work as peer-to-peer electronic cash.
- If no third party can ask you for KYC to allow you to use bitcoin.
- If no third party can freeze your funds.
- If no third party can prohibit or cancel your transactions.
- If no third party controls the majority of the nodes of the blockchain.

## You are not using Bitcoin

---

- If you are in a blockchain that does not work as peer-to-peer electronic cash.
- If a third party asks you for KYC to allow you to use bitcoin.
- If a third party can freeze your funds.
- If a third party can prohibit or cancel your transactions.
- If a third party controls the majority of the nodes of the blockchain.



# How to use Bitcoin?

1. Create a wallet where you have control of the private key (that makes you the owner of the funds of that wallet).
2. Use it as peer to peer.

That is it.

If you wanna investigate more on your own, here are some important concepts and interesting info:

## Concepts

---

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

## Info

---

- Whitepapers of the currencies you are interested into.
- 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>