

# CRYPTO 101 GUIDEBOOK



Welcome to the world of Crypto!

# Table of Content

## WHAT IS MONEY

Medium of exchange

Store of value

Unit of account

## EVOLUTION OF MONEY

Fiat currency

Central banks

Federal Reserve

Gold standard

# BLOCKCHAIN FUNDAMENTALS

Open  
Permissionless  
Decentralization  
Immutability  
Censorship resistance  
Predictable monetary policies  
Deflationary

## THE BLOCKCHAIN TRILEMA

Blockchain use cases  
Actors  
Developers, Miners/Validators  
Market  
Wallet (hot/cold)  
Exchange (centralized/decentralized)  
Block explorer  
Public-Private key encryption

# CONSENSUS ALGORITHMS

Proof of Work  
Proof of Stake

## SEMANTICS

Blockchain  
Cryptocurrency  
FOMO  
HODL  
FUD  
DeFi  
Sources

# Terms to Know

## Medium of Exchange

A medium of exchange is an intermediary instrument used to facilitate the sale, purchase, or trade of goods between parties. In this guidebook, we will distinguish between fiat currency and cryptocurrency. In addition, a good medium of exchange is relatively stable, allowing parties to value their monetary units accurately and plan budgets.

## Store of Value

Store of value refers to the function of an asset that maintains or increases its worth over time. Ideally, the asset will have purchasing power in the future. The long-term stability of the asset also influences how strong or good the store of value is. Some popular stores of value are fiat currency, cryptocurrency, precious metals, property, and fine art.

## Unit of Account

Sometimes referred to as "common measure of value," unit of account is the standard monetary measurement used for transactional and recordkeeping purposes.

The unit of account helps customers and merchants understand how much a good or service is worth. Historically, when people exchanged commodities as a form of payment, an underlying value had to be assigned to each item to determine a proper, fair trade.

## Evolution of Money

As society evolves, so does our medium of exchange. From barter to precious metals coins to plastic cards, today, we now have internet money in the shape of cryptocurrencies.

## Fiat Currency

Fiat currency is a government-issued currency that is not backed by a physical commodity but by the stability of the issuing government.

## Central Banks

A country's central bank can influence and manipulate the money supply. It can print more money, buy government securities or decrease/increase interest rates, which also affects the value or purchasing power of the fiat currency.

## Federal Reserve

The Federal Reserve was created in 1913. However, it's not part of the federal government of the USA. It's a private bank but acts in the interest of the stability of the US economy to maintain the strength of the US dollar.

## Gold standard

The gold standard established an exchange rate from gold to banknotes. Central banks had to hold enough gold in their reserves to back the value of their circulating currency. In 1971, the U.S. dollar was taken off the gold standard—the dollar was no longer redeemable in gold, and the price of gold was no longer fixed to any dollar amount. This meant that it was now possible to create more paper money than there was gold to back it; the health of the U.S. economy backed the dollar's value.

# Blockchain fundamentals

## Open

"Blockchain" is often described as a distributed ledger. This means that no single entity or person is in charge of recording transactions or changes. Instead, the ledger exists across multiple servers. Imagine a blockchain like a Google doc. Everyone can access it and modify it simultaneously, and everyone can always see the changes being made. But unlike a Google doc, no one can permanently delete any changes on the blockchain. Every modification is permanent and verified using cryptography.

An open blockchain is a public network where anyone can take part in and own, sell, exchange, stake, and mine cryptocurrencies.

## Permissionless

Permissionless means that no bank, government, company, or gatekeeper approval of any kind is required to join and modify a blockchain. Anyone may download and create a Bitcoin wallet for themselves and immediately start transacting with the cryptocurrency.

## Decentralization

Decentralization is the distribution of the network and activities of a group or organization. In cryptocurrency, the blockchain is a decentralized network maintained over nodes that are located all around the world. As a result, a public blockchain can not go down.

## Immutability

Decentralization is the distribution of the network and activities of a group or organization. In cryptocurrency, the blockchain is a decentralized network maintained over nodes that are located all around the world. As a result, a public blockchain can not go down.

## Censorship resistance

Cryptocurrency is inherently resistant to censorship because it has no regulating body. You are free to trade, whenever you want, with whomever you wish. No one institutional actor can block an individual from trading or exchanging cryptocurrencies as payment.

## Predictable monetary policies

Cryptocurrencies usually have a fixed monetary policy baked into the protocol. In Bitcoin (BTC), there will only ever be 21 million bitcoins, which means it has a predictable supply. In contrast, fiat currency can be printed by Central Banks at their discretion.

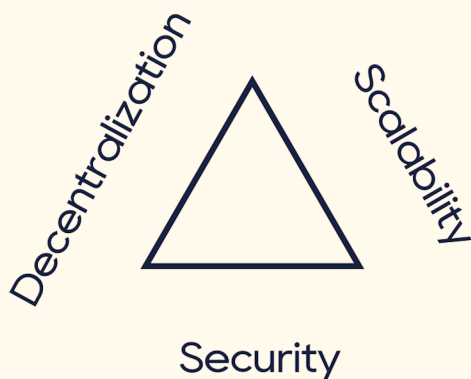
## Deflationary

When a cryptocurrency is described as deflationary, it means that the supply of the token or coin is limited. It can be limited by production or by removal from the market in the form of hoarding, burning, or making it inaccessible (ex: putting it in an inaccessible wallet).

For example, there is a maximum supply of Bitcoin set at 21 million coins.

## Blockchain Trilemma

Decentralized:  
blockchain that  
does not rely on a  
central point of  
control



Scalable: ability for  
the blockchain to  
handle an  
increasingly  
growing number of  
transactions

Secure:  
the ability of the blockchain to operate  
as expected, defend itself from attacks,  
bugs

# Blockchain use cases

Medium of Exchange

Store of Value

Liquidity Mining

Crowdfunding

Exchange

Attention Economy

Prediction Market

Decentralised Storage

Identity

Supply Chain

Governance

API Data

Oracle Data

Domain Names

Collectibles

Banking

Derivatives

# Actors

## Developers

In this industry, there are many developers. They may be coding the blockchain, developing apps, or working on UI/UX of exchanges. They are key players in the governance of certain blockchain protocols.

## Miners/Validators

In a proof-of-work system (POW), miners solve consensus algorithms to process transactions, which requires enormous quantities of energy. Whoever solves the algorithm first receives a small amount of crypto as a reward, and their solution creates a block on the blockchain.

Validators confirm transactions in a proof-of-stake (POS) system. Whereas a miner can be anyone, a validator must hold a minimum amount of the cryptocurrency to participate in the POS ecosystem. They may also receive a small amount of crypto as a reward.

## Market

The market is comprised of several actors who exchange goods and services. In the case of cryptocurrencies, the market may include:

Retail investors: individuals who participate in the market on behalf of themselves

Hedge funds: entities that can purchase large quantities of crypto at a time on behalf of their investors

Whales: individuals or groups who own (and hold) influential quantities of a particular cryptocurrency

## Wallet (hot/cold)

A wallet stores cryptocurrencies. Each wallet address holds a single cryptocurrency type, but a wallet app or device may hold multiple wallet addresses for different currencies.

A hot wallet is connected to the internet and easily accessible. It may be stored on a mobile device or computer. While there should be security protocols in place, there is always a chance that the wallet can be hacked and funds stolen.

In contrast, a cold wallet is not connected to the internet, but it is more cumbersome to access the funds stored in it. It will be a separate hardware device that connects to a computer or ATM to access or transfer funds.

## Exchange (centralized/decentralized)

A wallet stores cryptocurrencies. Each wallet address holds a single cryptocurrency type, but a wallet app or device may hold multiple wallet addresses for different currencies.

A hot wallet is connected to the internet and easily accessible. It may be stored on a mobile device or computer. While there should be security protocols in place, there is always a chance that the wallet can be hacked and funds stolen.

In contrast, a cold wallet is not connected to the internet, but it is more cumbersome to access the funds stored in it. It will be a separate hardware device that connects to a computer or ATM to access or transfer funds.

## Block explorer

The block explorer allows individuals to see the transactions on a blockchain. Because the blockchain is decentralized and public, anyone can see the transaction history. However, the block explorer does not reveal personally identifiable information (PII) of anyone involved in the transactions.

# Consensus algorithms

A consensus algorithm confirms the integrity of a single piece of data value. The process maintains the validity of that data across multiple systems or servers.

## Proof of Work

Proof of work (POW) is a system used to decide who can add new blocks to a blockchain. POW helps ensure the integrity of the blockchain as a whole and prevents double-spending and hostile attacks. Every 10 minutes, when a miner successfully solves a consensus algorithm first, they win the right to create the next block with its record of transactions.

Because multiple miners compete to win, POW requires copious amounts of energy to generate the computational power to solve the algorithms.

## Proof of Stake

An alternative to POW, proof of stake (POS), is another system used to add blocks to a blockchain. In a POS system, validators (instead of miners) may add new blocks to the blockchain based on their commitment to the chain's native cryptocurrency as a "bond" (their "stake"). A node will be selected, and it will then solve the algorithm to add the new block. This helps ensure their correct functionality and the overall integrity of the ledger of transactions. POS is less energy-intensive because validators solve algorithms based on their stake percentage of the cryptocurrency.

# Semantics

## Blockchain

Blockchain refers to the record of transactions that occurs with any given cryptocurrency. But in a broader sense, a blockchain is a distributed ledger. Once an action is recorded on it, the record cannot be modified. The record of the action exists in multiple places, which adds to the difficulty of modifying it.

## Cryptocurrencies

Cryptocurrencies are digital mediums of exchange. They use cryptographic security to protect transactions and mathematical algorithms to regulate new units (tokens) of currency. They operate independently of banks, and a variety of factors may determine the value. Unlike fiat currencies, ownership information about units of cryptocurrency is stored in digital public ledgers.

## FOMO

FOMO is an acronym that stands for "Fear Of Missing Out."

## HODL

HODL is an acronym that stands for "Hold On for Dear Life." To HODL is to hoard or hold on to a cryptocurrency, either for long-term investment or out of fear of missing out on future profits.

Its spelling is attributed to a typo when trying to spell "HOLD," which has since become a popular turn of phrase in the crypto community.

## FUD

FUD is an acronym that stands for "Fear Uncertainty Doubt."

## DeFi

DeFi is a shortened term that stands for "Decentralised Finance."

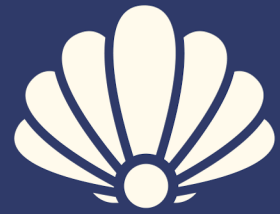
## Sources:

Medium of exchange, Investopedia

<https://www.investopedia.com/terms/m/mediumofexchange.asp>

# ELÉONORE BLANC

## Founder, CryptoCanal



 @blockblanc

 Eleonore Blanc

 @blockblanc

<https://cryptocanal.org/>

The cryptocurrency industry is made of visionaries, and ruthless moneymakers, the perfect mix for a monetary revolution, and Eleonore is all in. Thrilled to be part of an ongoing social and financial experiment, she's passionate about peer-to-peer cash, voluntarism and economic freedom.

Active since 2017 with the crypto community in Amsterdam, she began working in the wallet, mining industry at BTC.com. She later founded CryptoCanal in 2019 to offer educational, marketing and business development services.