

# **Introduction to Blockchain**

**Prepared by Kirill Sizov**

**Why we are here?**



# Syllabus

- Hamster Kombat tokenomics
- Launching shitcoins on Solana
- Trade signals v TG
- NFT



# Syllabus

- Hamster Kombat tokenomics
- Launching shitcoins on Solana
- Trade signals v TG
- NFT



# True syllabus

- Basic cryptography
- Bitcoin
- Consensus algorithms
- Ethereum Virtual Machine (EVM)
- Smart contracts
- DeFi patterns
- DEX protocols
- Lending protocols
- Staking protocols
- Bridges
- Layer 2 solutions
- ZK
- MEV

# Evaluation

$$O_{total} = [0.7 \cdot O_{nakop} + 0.3 \cdot O_{exam}]$$

$$O_{nakop} = 0.6 \cdot O_{CTF} + 0.3 \cdot O_{projects} + 0.1 \cdot O_{quiz}$$

$$[O_{nakop}] \geq 8 \Rightarrow O_{total} = [O_{nakop}]$$

# CTF

- CTF (Capture The Flag) challenges with blockchain interaction.
- Start after ~4th lecture.
- Soft and hard deadlines on tasks.

# Projects

- The goal: develop the ability to explore a topic in greater depth.
- Can be research or software project.
- A list of topics will be provided, but students can propose their own.

# Quiz

- The goal: lectures marketing.
- After each lecture, a short quiz of 5 questions will be given on the covered material.

# **Exam**

- The exam will be conducted in an oral format.
- The list of questions will be provided in advance.

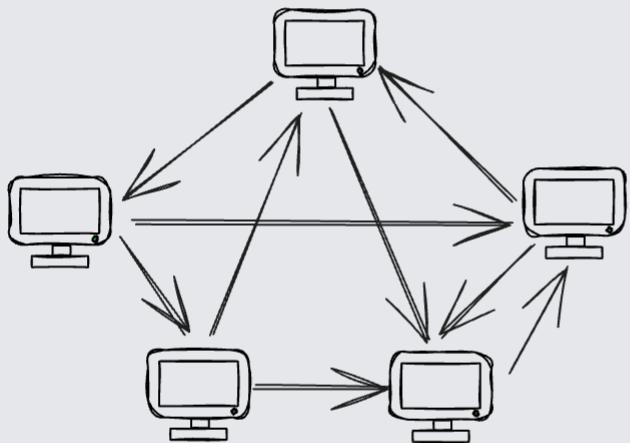
# **Questions?**

# Agenda today

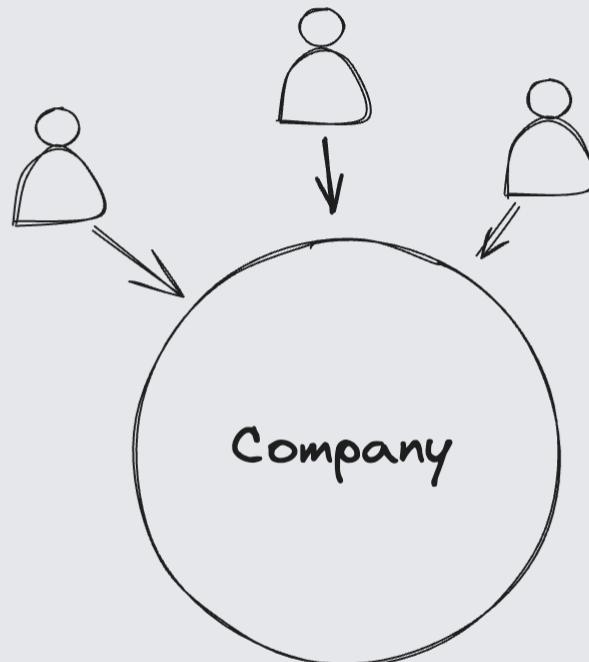
- History
- What is a blockchain?
- Cryptography background
- Crypto wallets

# History

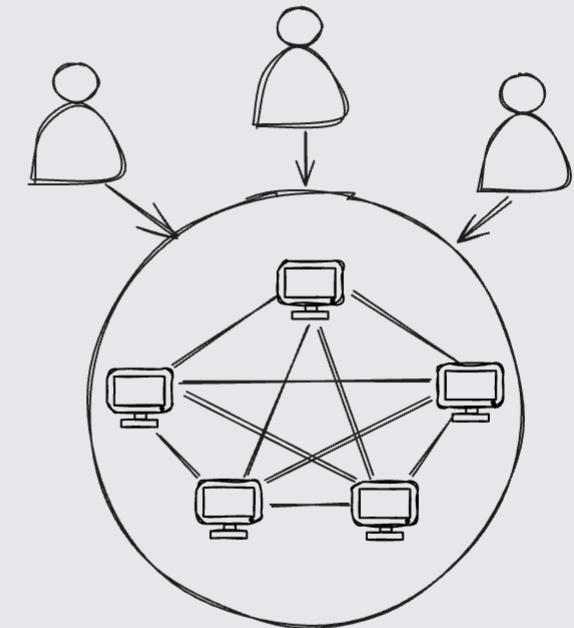
# Three eras of networks



Protocol Networks

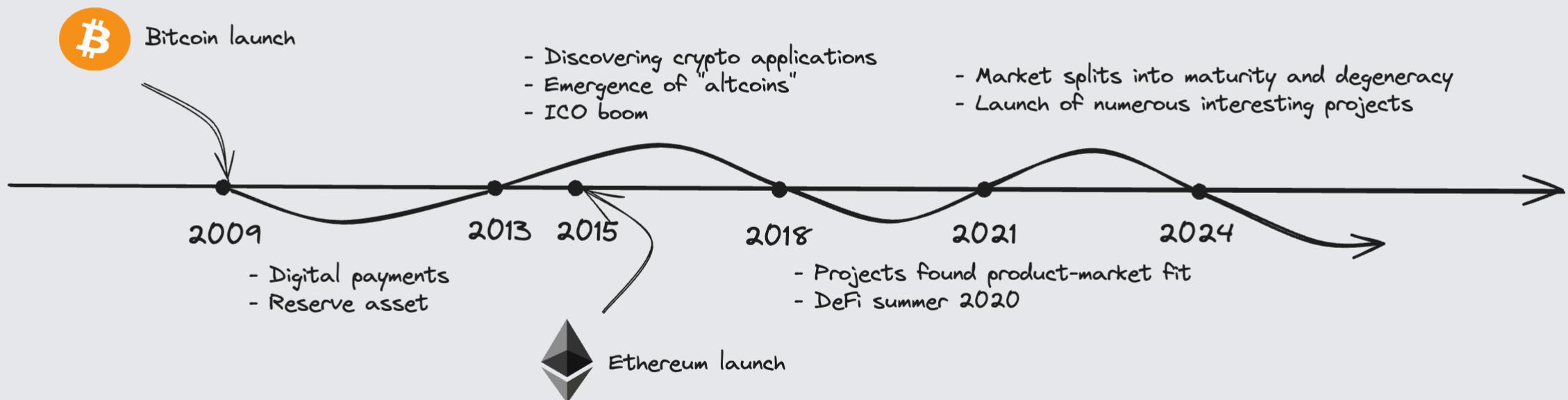


Corporate Networks



Blockchain Networks

# Timeline



# TVL (Total Value Locked)



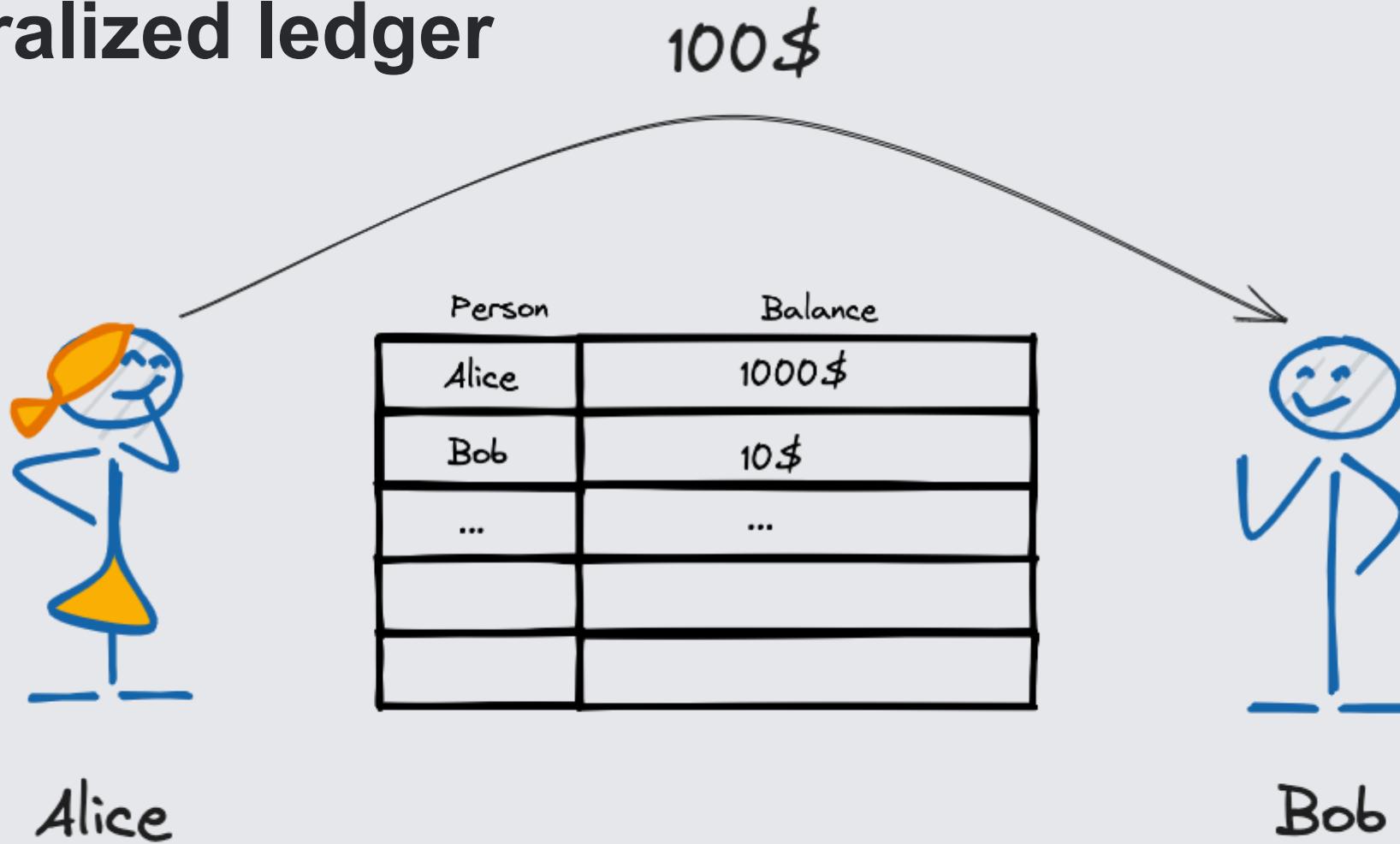
# What is a blockchain?



# Why is a blockchain?

- A system for coordinating between many parties when no single trusted party exists.
- If trusted party exists ⇒ No need for blockchain
- Often used in financial systems

# Decentralized ledger



# Decentralized ledger



Alice

Person	Balance
Alice	900\$
Bob	110\$
...	...

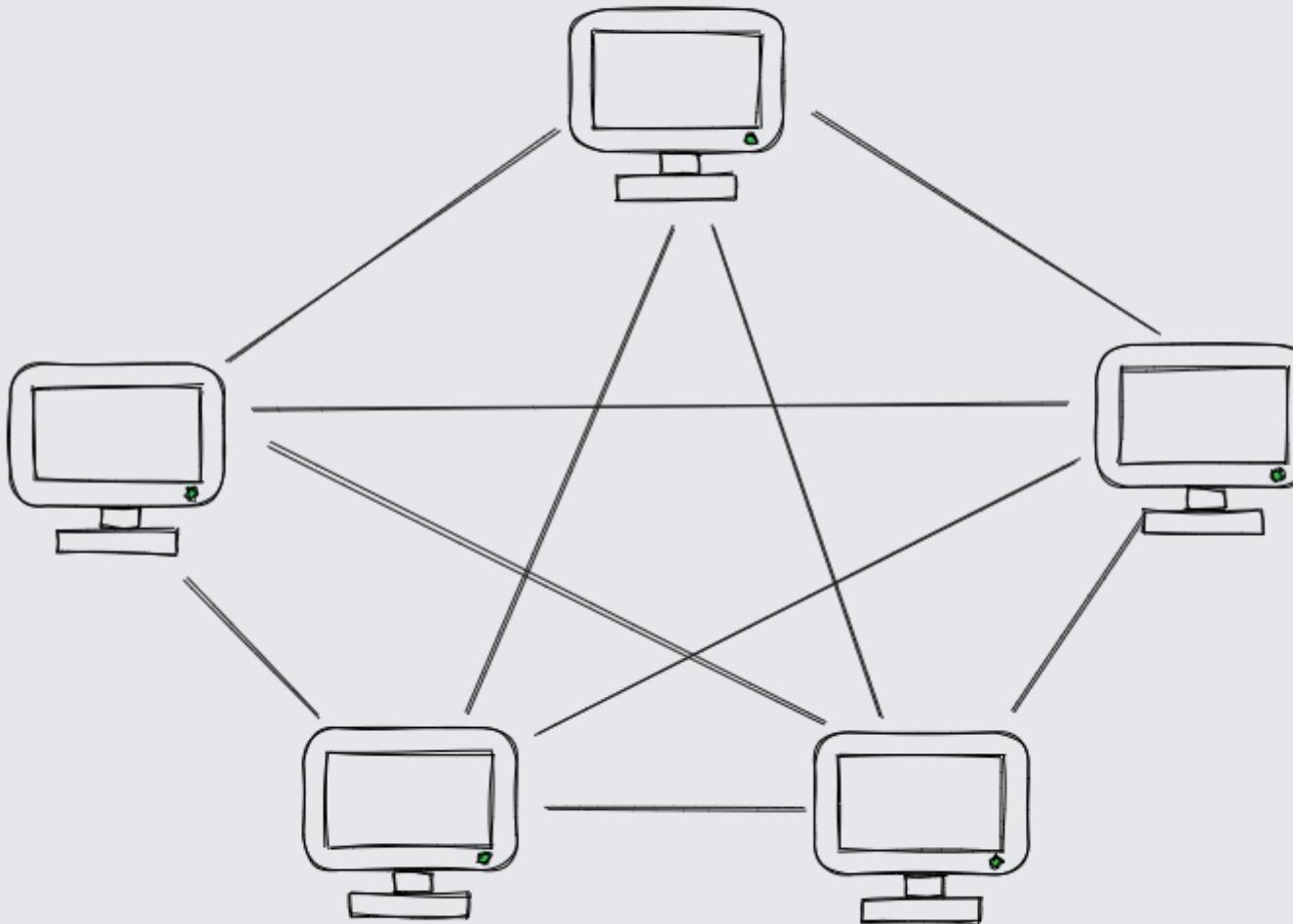


Bob

# Requirements for the system

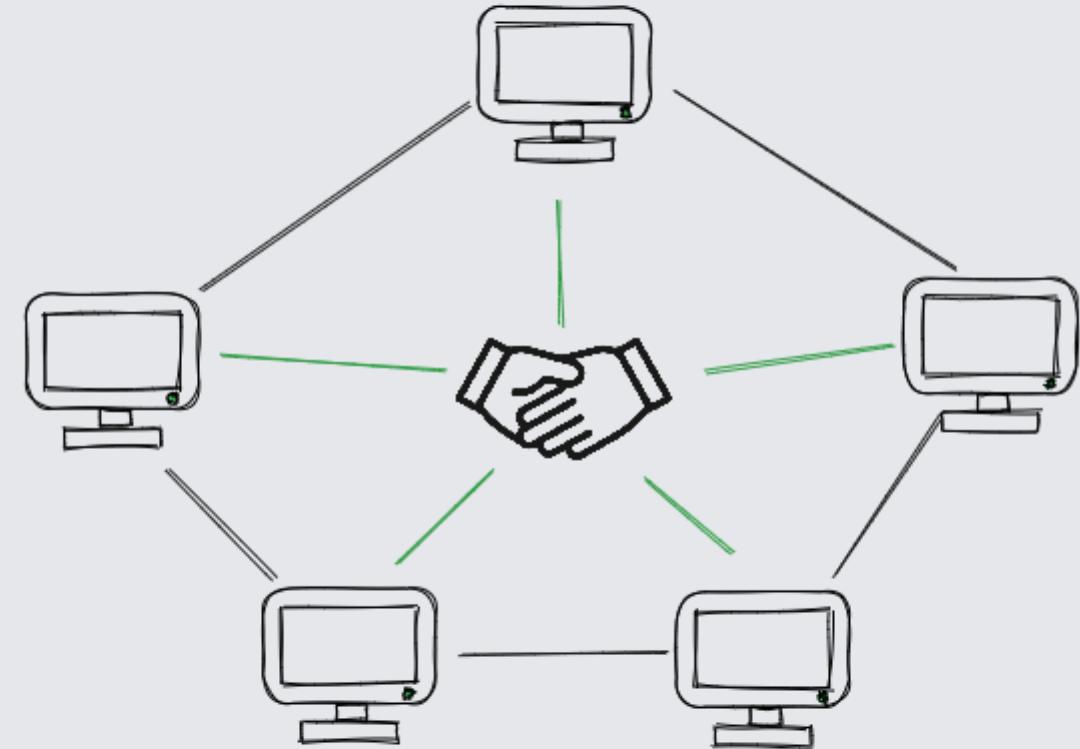
- Broadcast signed messages (transactions).
- Performs state transitions.
- Doesn't allow overspending.
- Decentralized.

# Peer-to-Peer (P2P) network



# Consensus mechanism

- The term refers to the mechanics, that allow a network of nodes to agree on the state of a blockchain.



# Consensus types

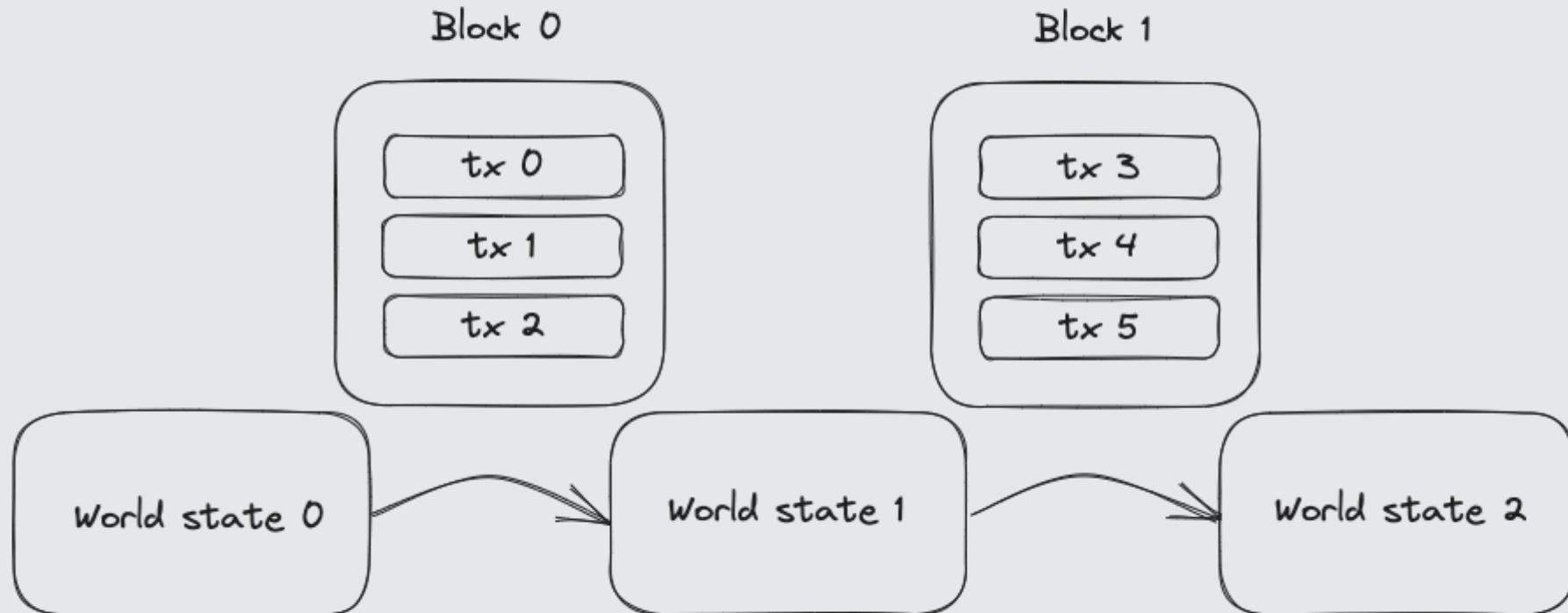
## Proof of Work (PoW)

- Block creators are called miners.
- Miners run software that solves complex mathematical problems to validate and add new transactions.
- Mining consumes significant electrical power.

## Proof of Stake (PoS)

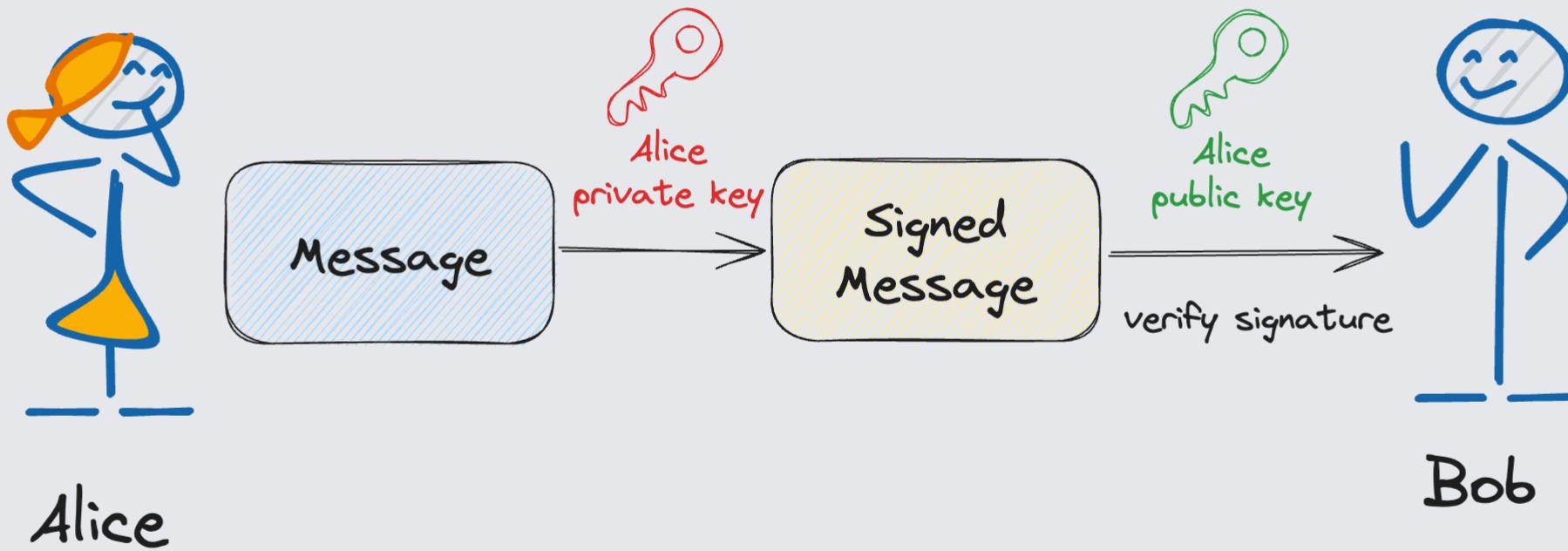
- Block creators are called validators.
- Validators lock up a certain amount of cryptocurrency as collateral to validate and produce new blocks.
- Malicious validators will be losing their staked assets if they attempt to validate fraudulent transactions.

# Chain of states



# Cryptography background

# Digital signature

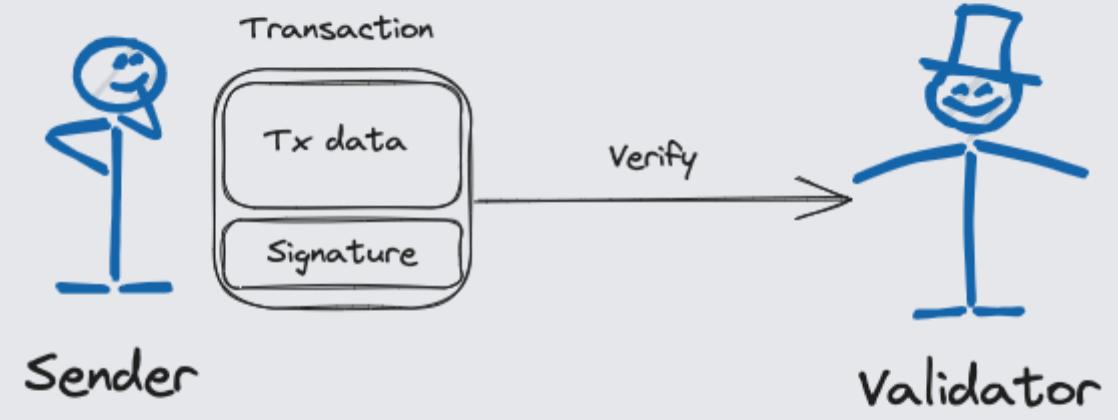


# Digital signature: algorithms

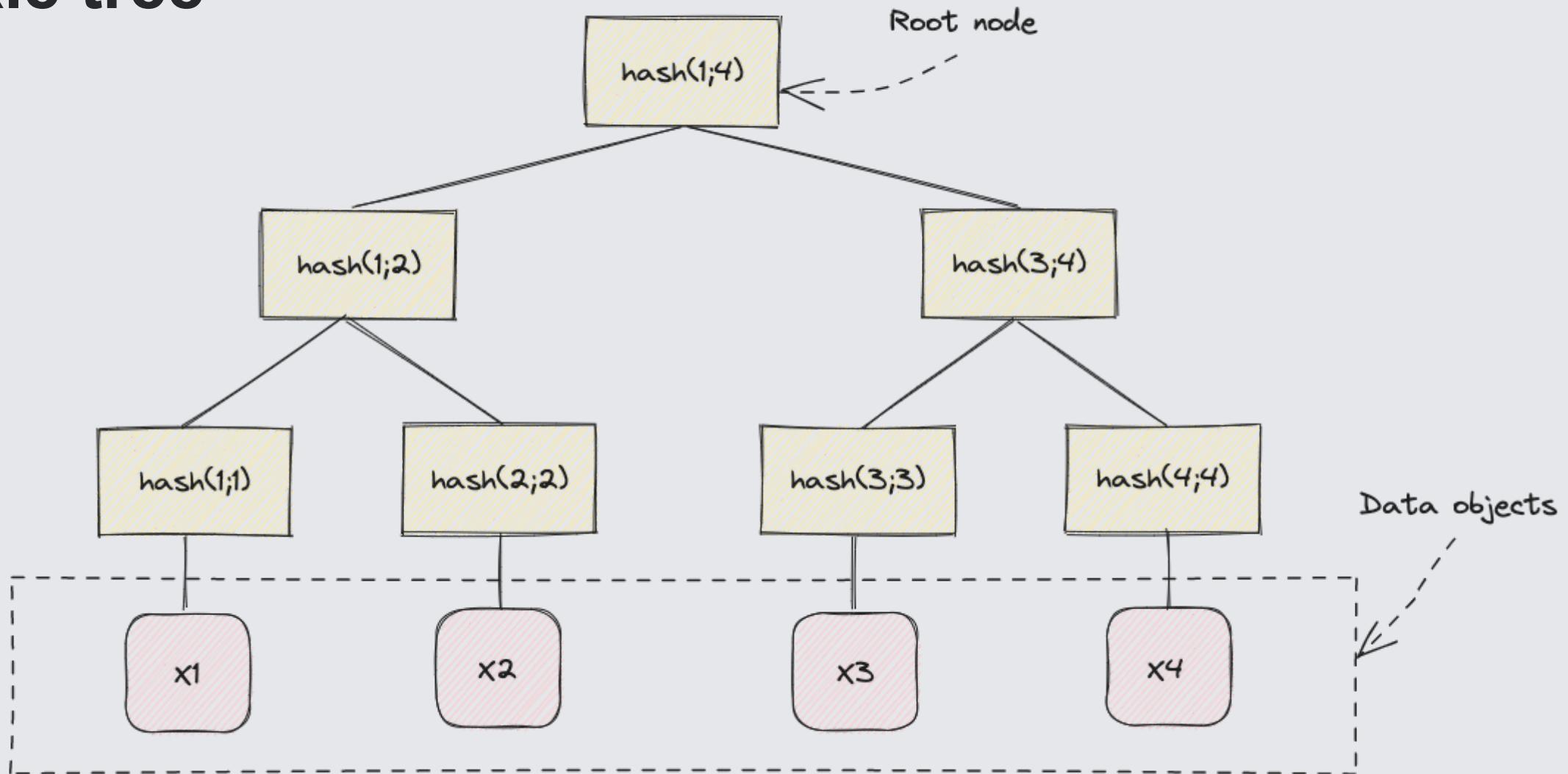
- `gen()` – generate a key pair `(public_key, private_key)`.
- `sign(data, private_key)` – signs data.
- `verify(signature, public_key)` – verifies signature or extract the data.

# Signatures on blockchain

- Signing user transactions.
- Signing blocks (for validators).
- Other applications,  
such as voting mechanics.



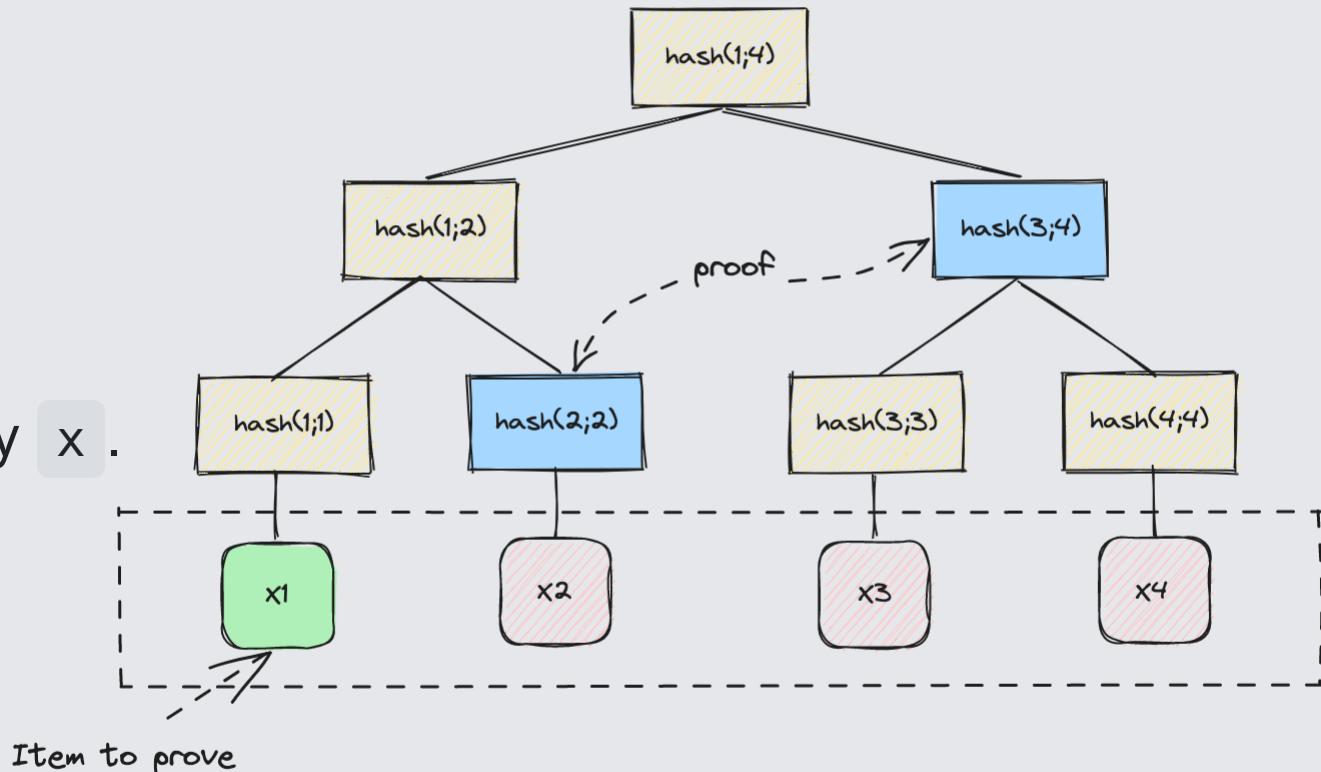
# Merkle tree



# Merkle tree

## Goal

- get a short representation to the array  $x$ .
- later prove that element  $i$  is  $x[i]$ .



# **Merkle tree on blockchain**

- Each block contains only merkle root of transactions.
- Later we can prove that a transaction is on the blockchain.

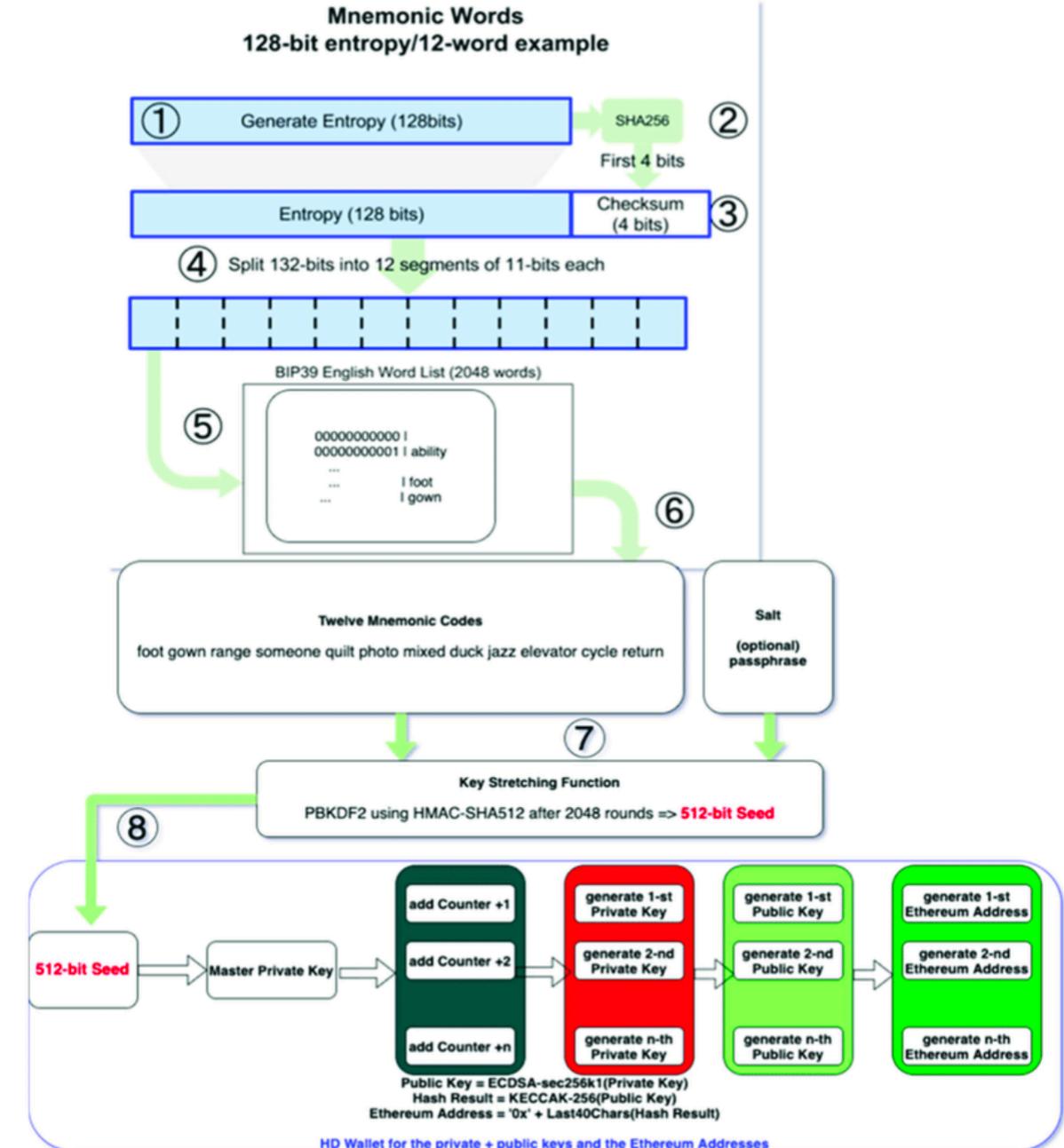
# Crypto wallets

# What wallets do

- Generate private and public key.
- Store private key.
- Sign and send transactions.
- Show balances.

# Mnemonic phrase

A mnemonic phrase is superior for human compared to the handling of raw seed.



# Types of wallets

- Cloud
  - Cloud holds private keys.
- Soft
  - Browser extension.
  - Mobile application.
  - Desktop app.
- Hardware
  - Ledger, Trezor, etc.
- Paper
  - Write secret key on paper.
- Brain
  - Memorize your secret key.

# Hardware wallets

- Physical devices designed to securely store cryptocurrency private keys offline.
- Connect to a computer via USB and require physical confirmation for transactions.



# Brain wallet

- Storing private key using a memorized phrase, that was self-generated.
- Have low entropy, vulnerable to brute-force.



# Paper wallet

- Write private key on paper (or other physical item).
- Secure from digital attacks, but vulnerable to physical risks like damage, theft, or loss.



# Let's create a hot wallet

- **Metamask** is the most popular one.

