

Blockchain for Industrial Engineers: Decentralized Application Development

**บล็อกเชนสำหรับวิศวกรอุตสาหกรรม: การพัฒนาแอปพลิเคชันแบบ
กระจายศูนย์**

Short history - Bitcoin

- October 31, 2008
 - "White paper" by *Satoshi Nakamoto*
 - Describing a system to allow peer to peer payments without a financial intermediary (like a bank)
- January 3, 2009
 - The bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of bitcoin (block number 0), which had a reward of 50 bitcoins

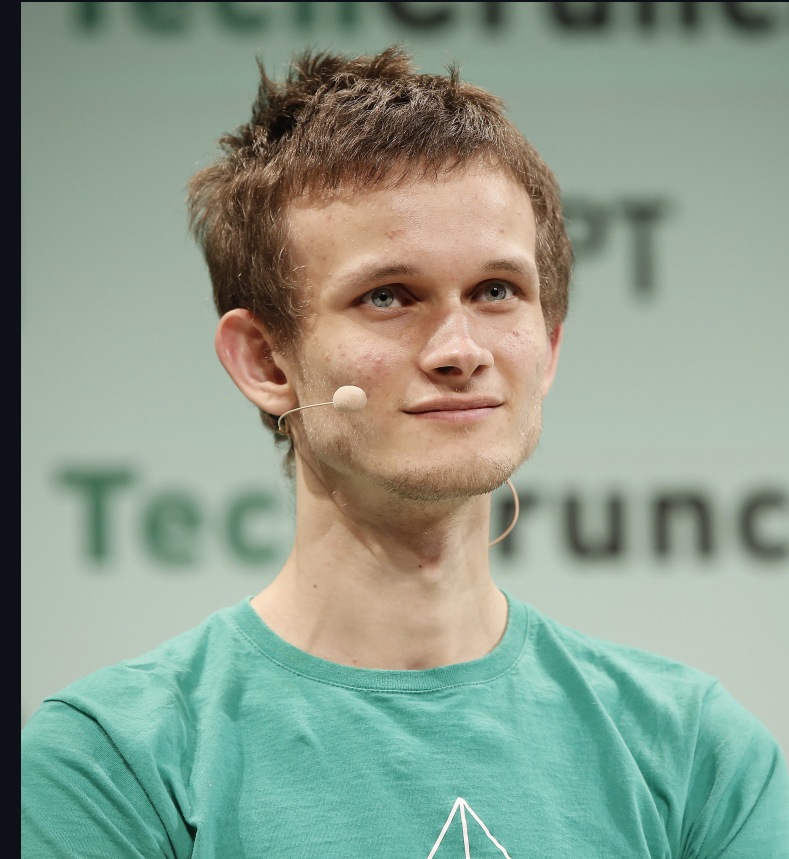
Shortcoming

Bitcoin can only be used for sending money.

| Can we use bitcoin technology to transfer other types of exchanges?

Short history - Ethereum

- December 2013
 - "White paper" by *Vitalik Buterin*
 - Discussing need for more programmatic control over transactions
 - Introducing the idea of *Smart Contracts* as an entity that can send and receive currency, beyond just humans
- July 2015
 - Birth of Ethereum network



Shortcoming

- Scalability
 - Bitcoin (Layer 1): 7 tps
 - Ethereum (1.0): 30 tps
 - Visa 24,000 tps
- Interoperability
 - Moving token between different networks.
- Governance system
 - Bitcoin Foundation and Ethereum Foundation are centralized organization.

Source

3rd-Generation blockchain

Source



OPTIMISM



Polkadot.



CØSMOS



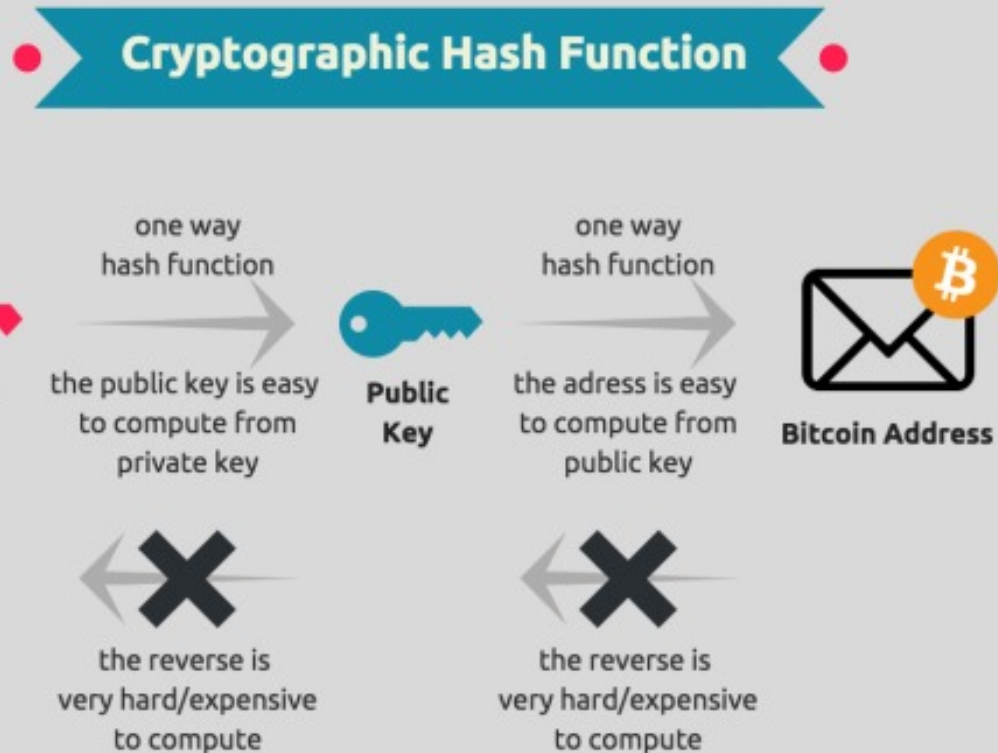
Getting to know blockchain

- Blockchain demo
- Public and private keys
- Block explorer

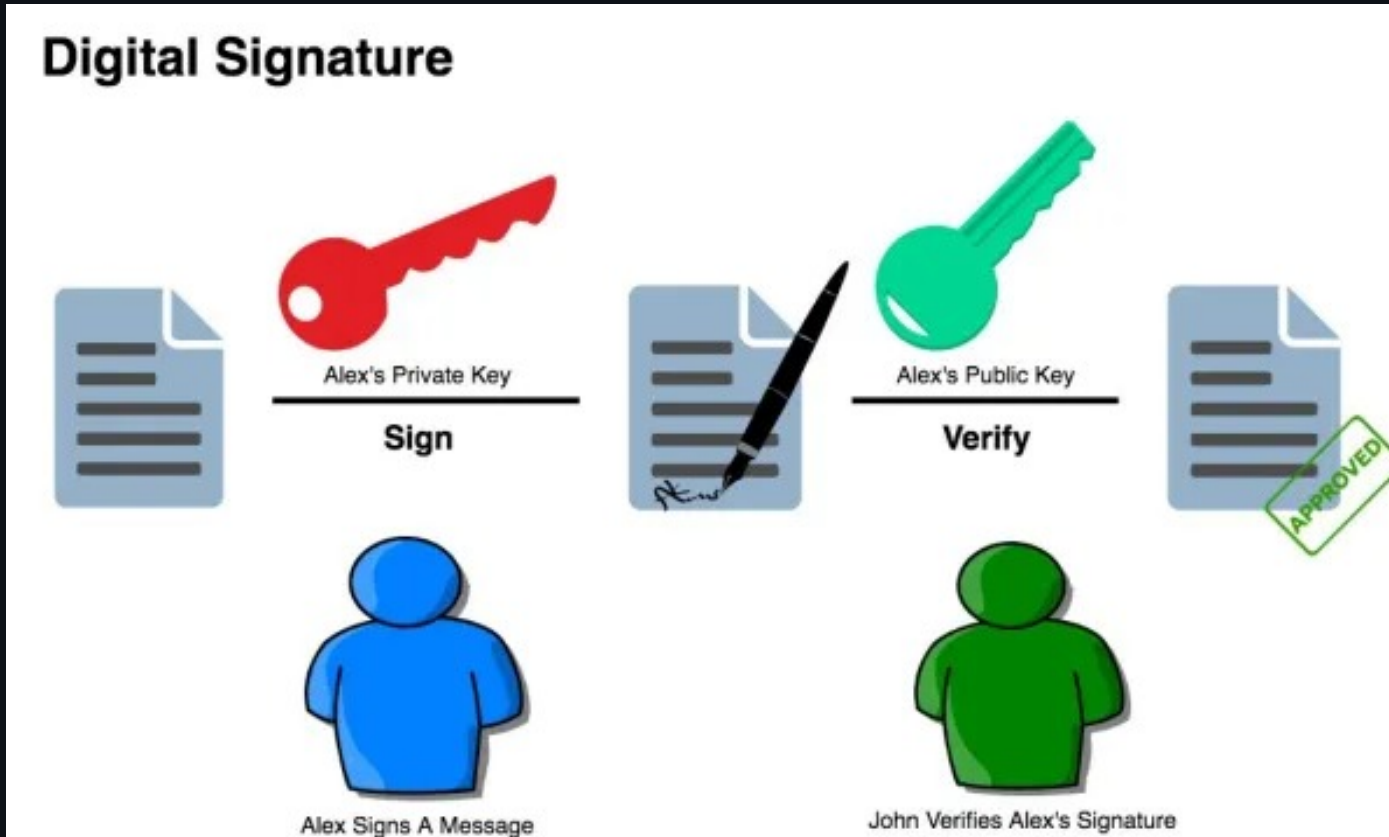
Other cool demos

- Blockchain demo
- Coin demo

Keys

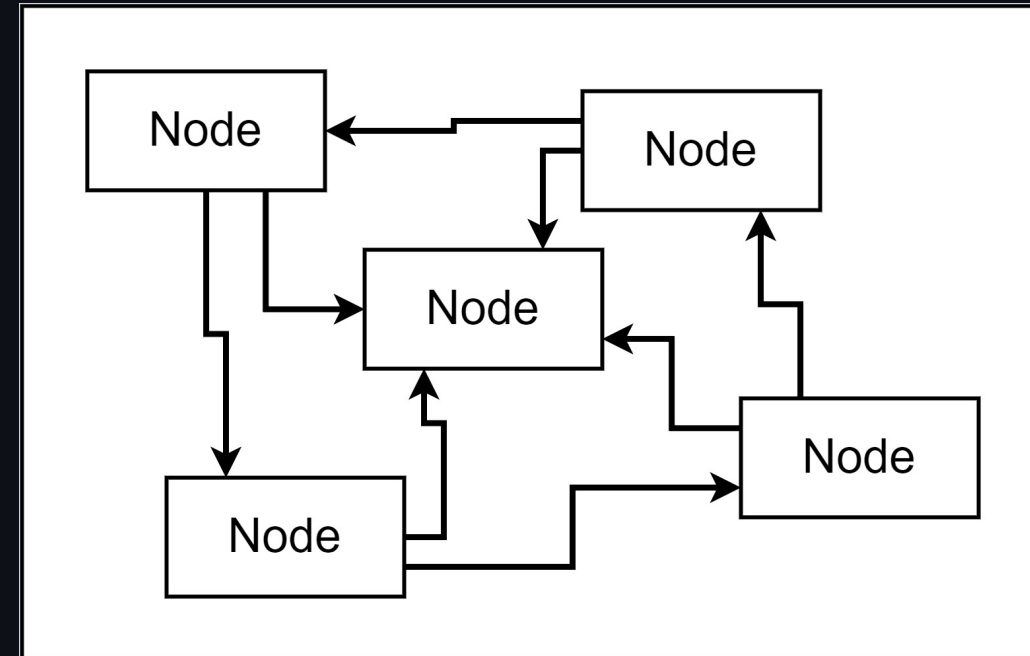


Signature



Getting to know ethereum

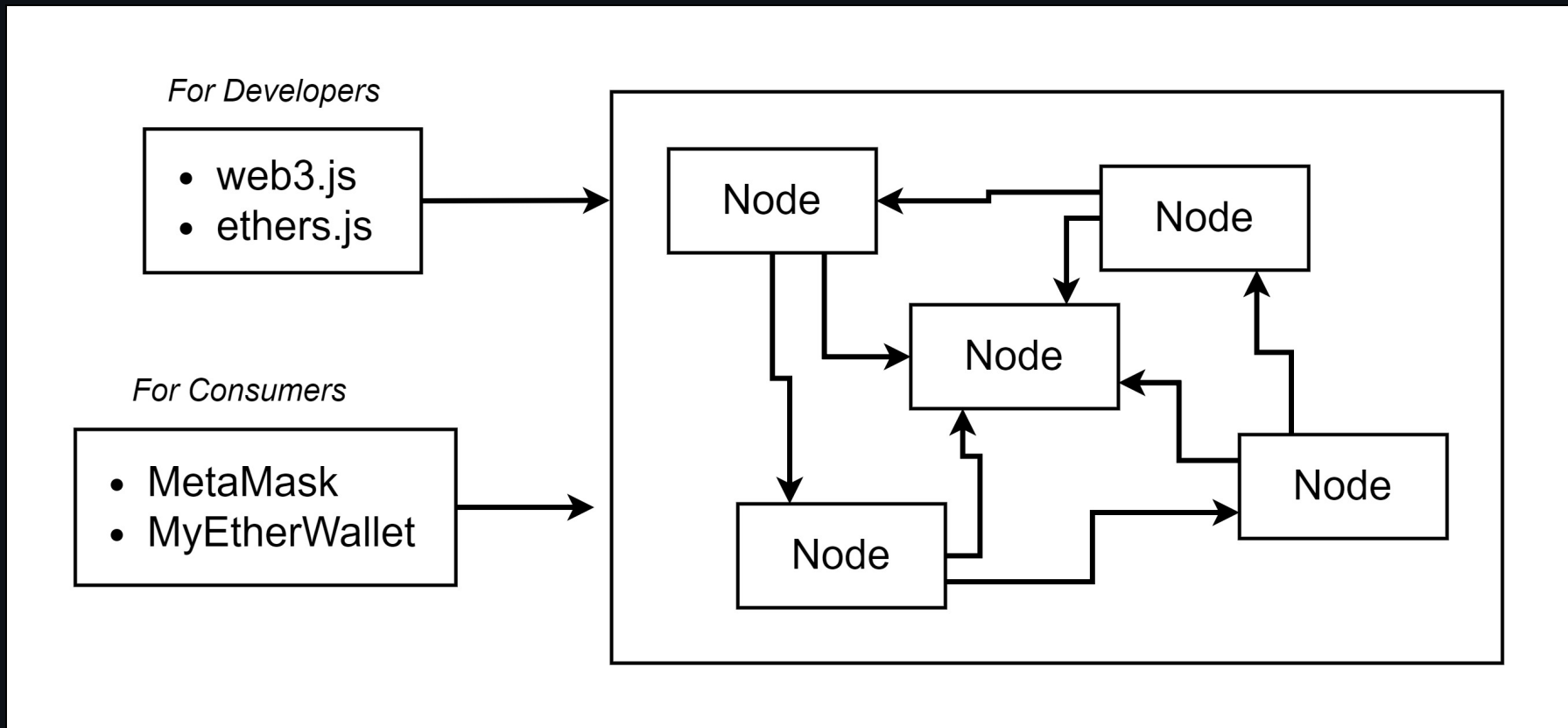
- Ethereum networks are used to transfer money and store data
- There are many different **Ethereum networks**.
- Networks are formed by one or more nodes.



Getting to know ethereum

- Each node is a machine running an **ethereum client**.
 - Anyone can run a node.
- Each node can contain a full copy of the blockchain.
 - Stores the record of every transaction that has ever taken place.

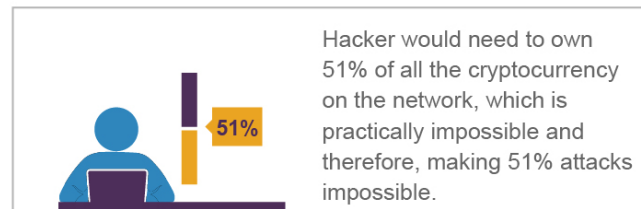
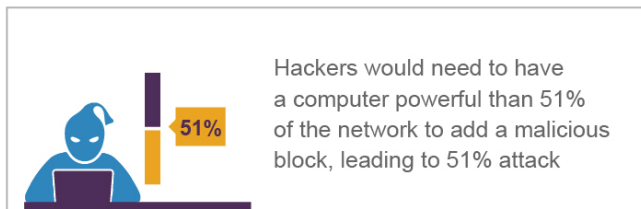
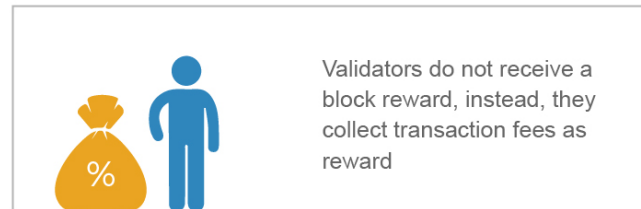
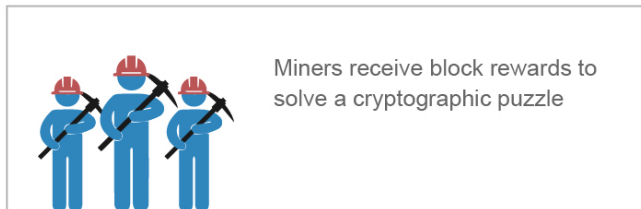
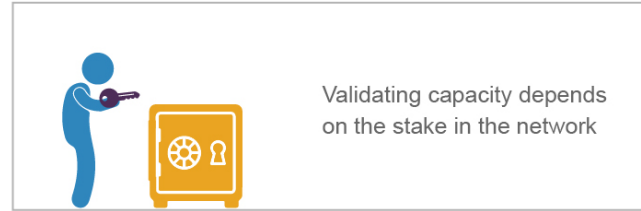
Interacting with Ethereum network



MetaMask uses [Infura](#) node.

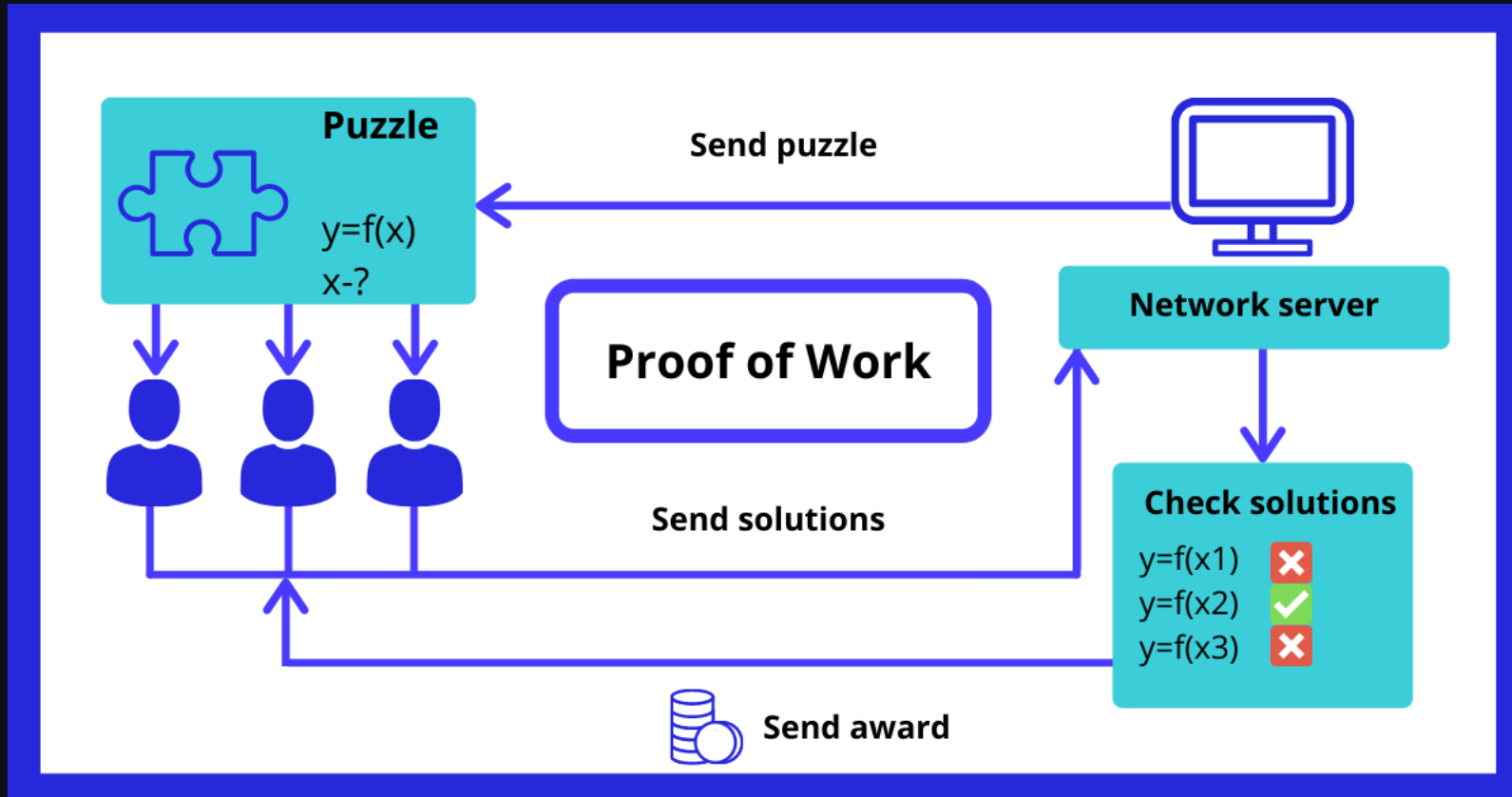
Proof of work vs proof of stake

Proof of Work VS Proof of Stake



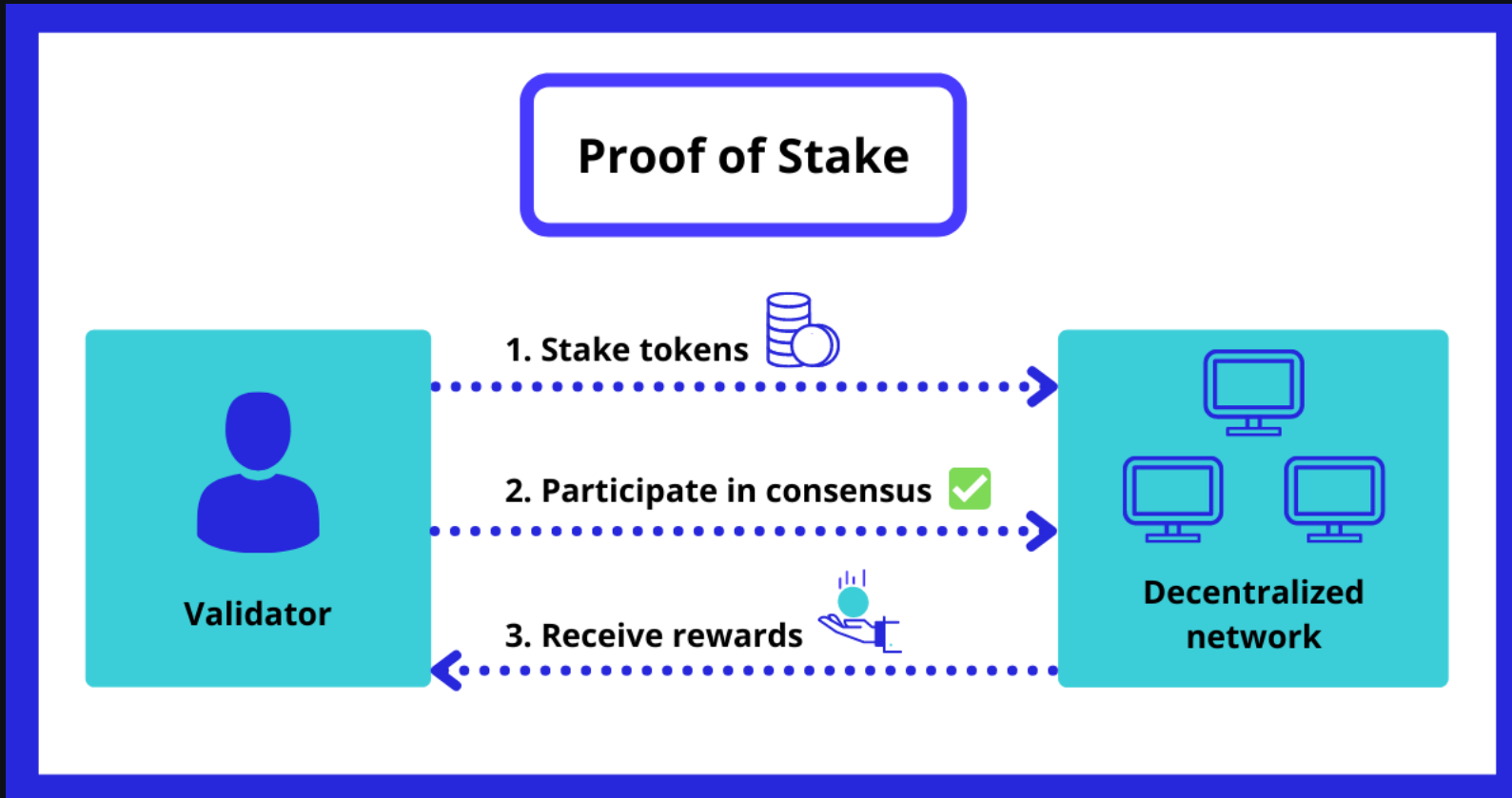
Source

Proof of work



Source

Proof of stake

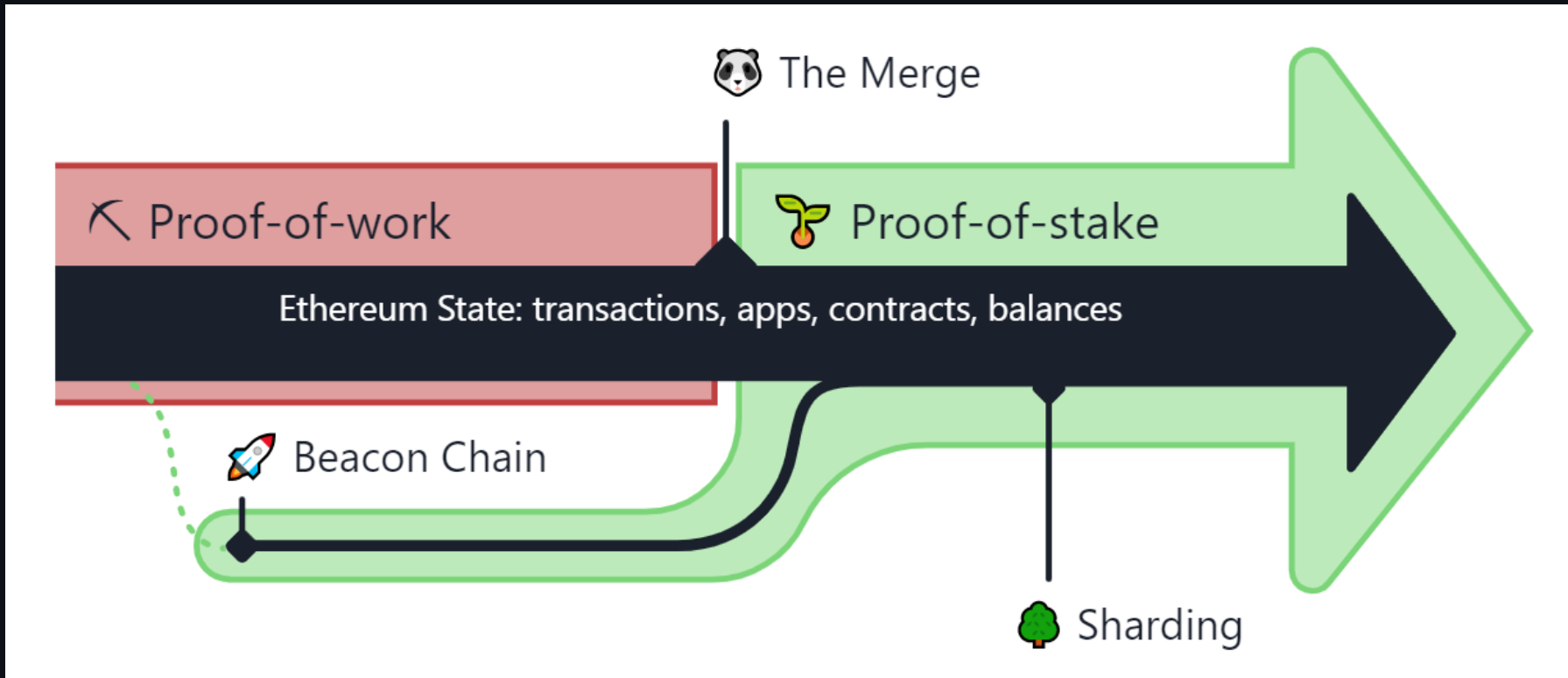


Source

Proof of Work	Proof of Stake
Participating nodes are called miners	Participating nodes are called validators or forgers
Mining capacity depends on computational power	Validating capacity depends on the stake in the network
Mining produces new coins	No new coins are formed
Miners receive block rewards	Validators receive transaction fees
Massive energy consumption	Low to moderate energy consumption
Significantly prone to 51% attacks	51% attacks are virtually impossible

Ethereum merge

- The upgrade from the original proof-of-work mechanism to proof-of-stake was called The Merge.
- The Merge refers to the original Ethereum Mainnet merging with a separate proof-of-stake blockchain called the Beacon Chain, now existing as one chain.
- The Merge reduced Ethereum's energy consumption by ~99.95%.

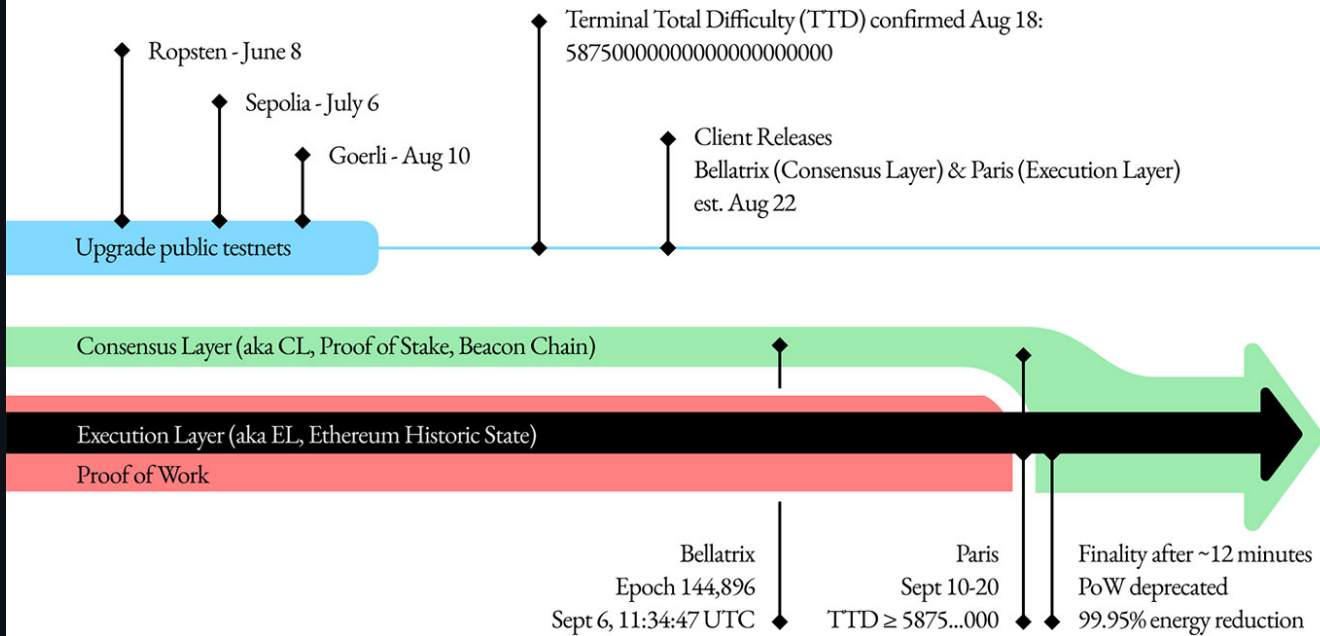


Source

Approaching the Merge

 Offchain Onchain

Aug 22 2022 - @trent_vanepps
pixels between events may not scale to reality



Source

Account

- **Externally-owned account (EOA)** – controlled by anyone with the private keys
- **Contract account** – a smart contract deployed to the network, controlled by code.

Transaction

- An Ethereum transaction refers to an action initiated by an externally-owned account
 - In other words an account managed by a human, not a contract.
- For example, if Bob sends Alice 1 ETH, Bob's account must be debited and Alice's must be credited. This state-changing action takes place within a transaction.

Let's look at a contract

- Send somebody some ETH.
 - If you want, you can send it to me 😊.
0x6269f27234747F4ac12A6d5E88c75e021da290CF
- Transaction example

How long do we have to wait?

- Block time
- Details

Gas

Gas fees help keep the Ethereum network secure. By requiring a fee for every computation executed on the network, we prevent bad actors from spamming the network.

Gas

- Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network.
- Gas fees are paid in ether `ETH`.
- Unit of gas is `gwei`.
 - 1 `gwei` = 0.0000000001 `ETH` (10^{-9} `ETH`).
- Gas limit
 - Maximum amount of gas you are willing to consume on a transaction.
 - A standard ETH transfer requires a gas limit of 21,000 `gwei`.

Gas information

- <https://etherscan.io/gastracker>
- <https://ethgasstation.info/>