SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 10:

Ethereum – Part 2

Module 2 – ETH 2.0 & the Merge (alternative consensus mechanisms)

Ethereum and the Merge

- Ethereum Mainnet now uses proof-of-stake, but this wasn't always the case.

- The upgrade from the original proof-of-work (**PoW**) mechanism to proof-of-stake (**PoS**) is called The Merge.

- The Merge refers to the original Ethereum Mainnet merging with a separate proof-of-stake blockchain called the Beacon Chain. They are now one chain.

- The Merge reduced Ethereum's energy consumption by ~99.95%.

What happened to 'Eth2'?

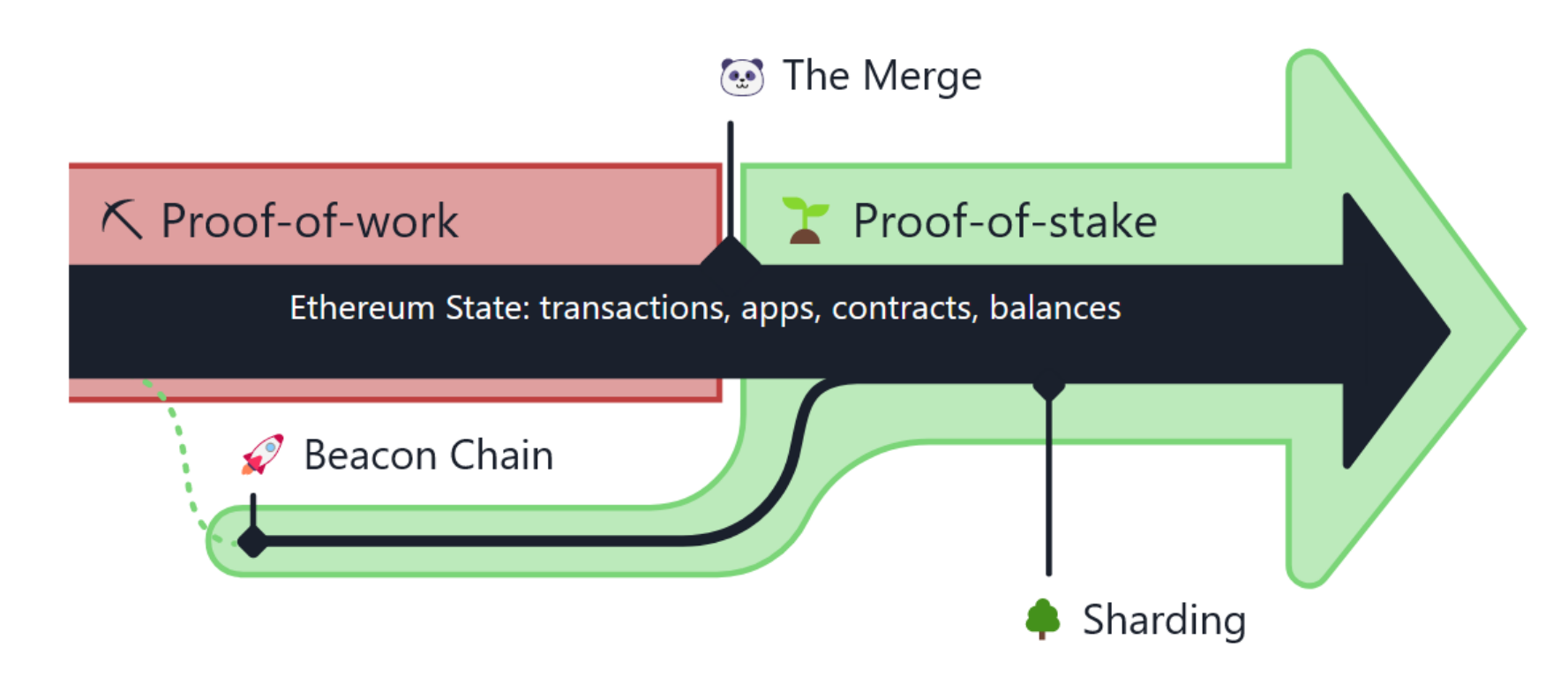
- Previously Eth 2 used to be the name for the new PoS Ethereum with all its new features. But the term **'Eth2'** has been deprecated now.

- **Ethereum.org:** “After merging 'Eth1' and 'Eth2' into a single chain, there is no longer any need to distinguish between two Ethereum networks.”

- To limit confusion, the community has updated these terms:
  - 'Eth1' is now the 'execution layer', which handles transactions and execution.
  - 'Eth2' is now the 'consensus layer', which handles proof-of-stake consensus.

(Ethereum.org)

Beacon Chain & the Merge

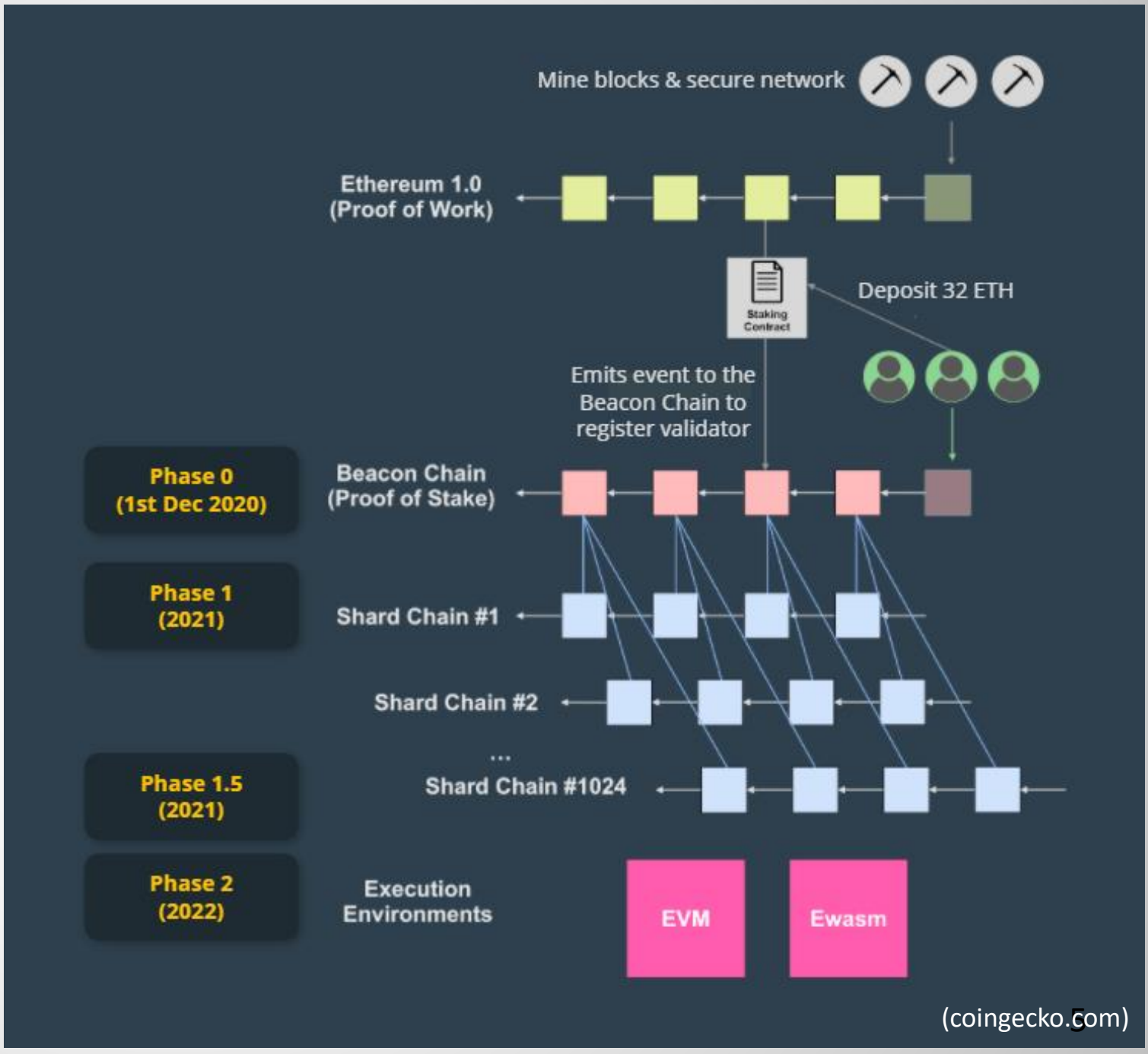


The New ETH

- **Beacon Chain** is the core of the future network. It reaches consensus based on PoS. It is also the place shards synchronize themselves with. To become a miner in the new PoS system, you should deposit 32 ETH. One is elected to mine in each round, and a group of others are chosen to check the mined block.

- **Sharding** is the process where the entire state of the network is split into a number of partitions called shards that contain their own independent piece of state and transaction history. This addresses the issues of scalability and transaction speed and stops one app from slowing down the network.

- **eWASM** (Ethereum Web-Assembly) allows code to execute faster by expanding the coding options and capabilities for the Ethereum Virtual Machine.



(coingecko.com)

Sharding

- Sharding is a component of the Ethereum upgrade, designed to improve the scalability and transaction processing capacity of the network.

- It involves partitioning the network into smaller units/chains called shards, each capable of processing its own transactions and smart contracts.

Shard Creation and Shard Chains

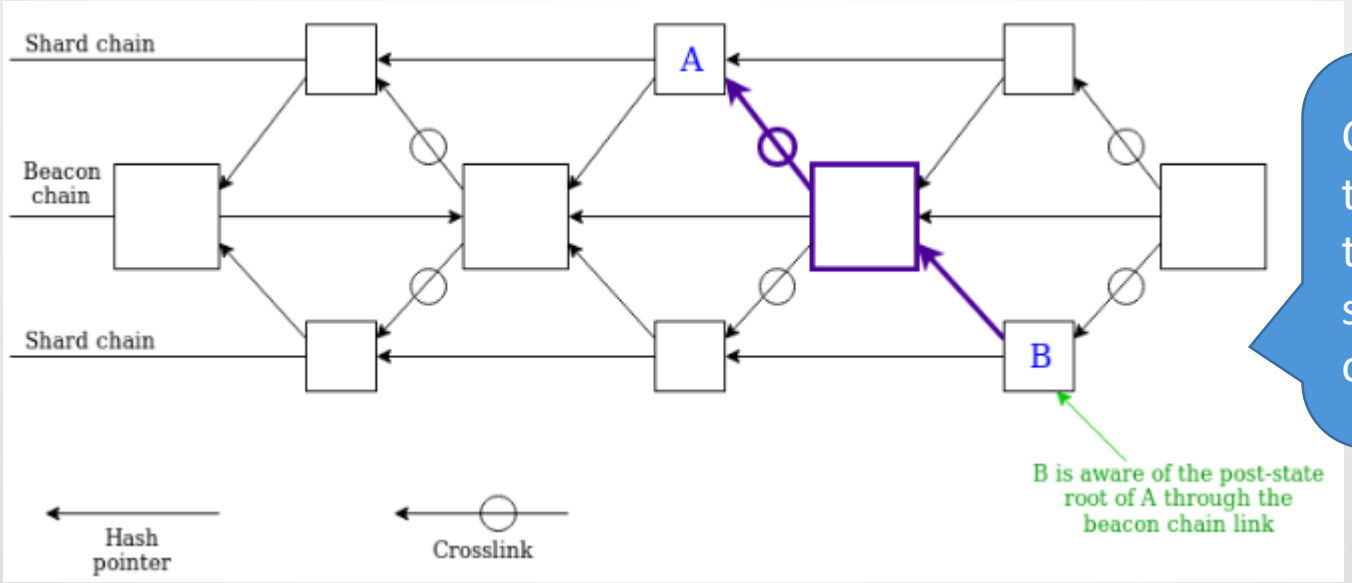
Shard Creation: The new Ethereum network will consist of multiple shards, each with its own set of validators. Validators are responsible for proposing and validating blocks within their assigned shard.

Shard Chain: Each shard operates independently with its own shard chain. A shard chain is a blockchain within a specific shard, storing and processing transactions and smart contracts relevant to that shard.

Shard CrossLink

Crosslinks: Periodically, each shard creates a crosslink—a summary of the shard chain's state—and includes it in the Beacon Chain.

The Beacon Chain acts as the central coordinator and is responsible for securing the network and maintaining consensus.



Cross-links are references to the latest shard chain state in the Beacon Chain, allowing shards to interact with each other when needed.

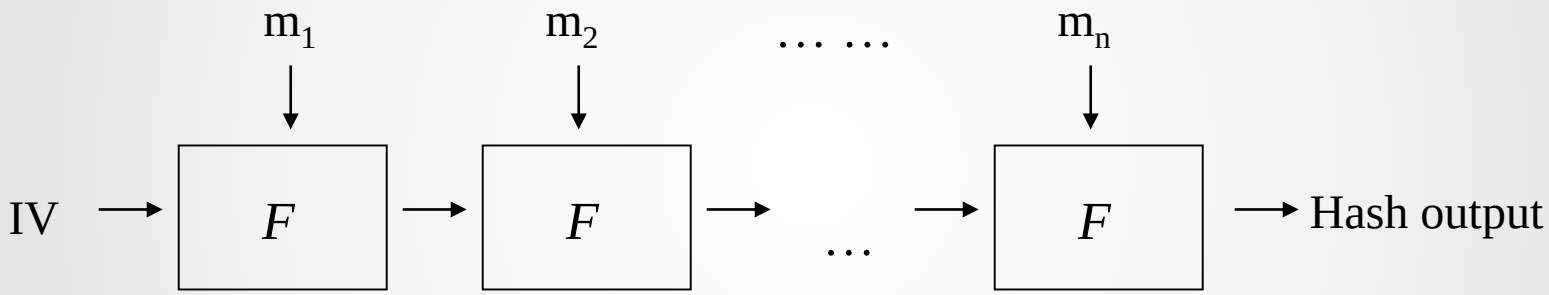
(ethereum.org)

Ethereum Previous PoW Puzzle

- Before the merge (happened on **September 15, 2022),** Ethereum consensus was based on PoW, similar to Bitcoin.
  - block generation was every 13~15 secs.
  - The puzzle was based on a hash function, similar to Bitcoin.
  - The hash function used was Keccak.

General Structure - Merkle-Damgard

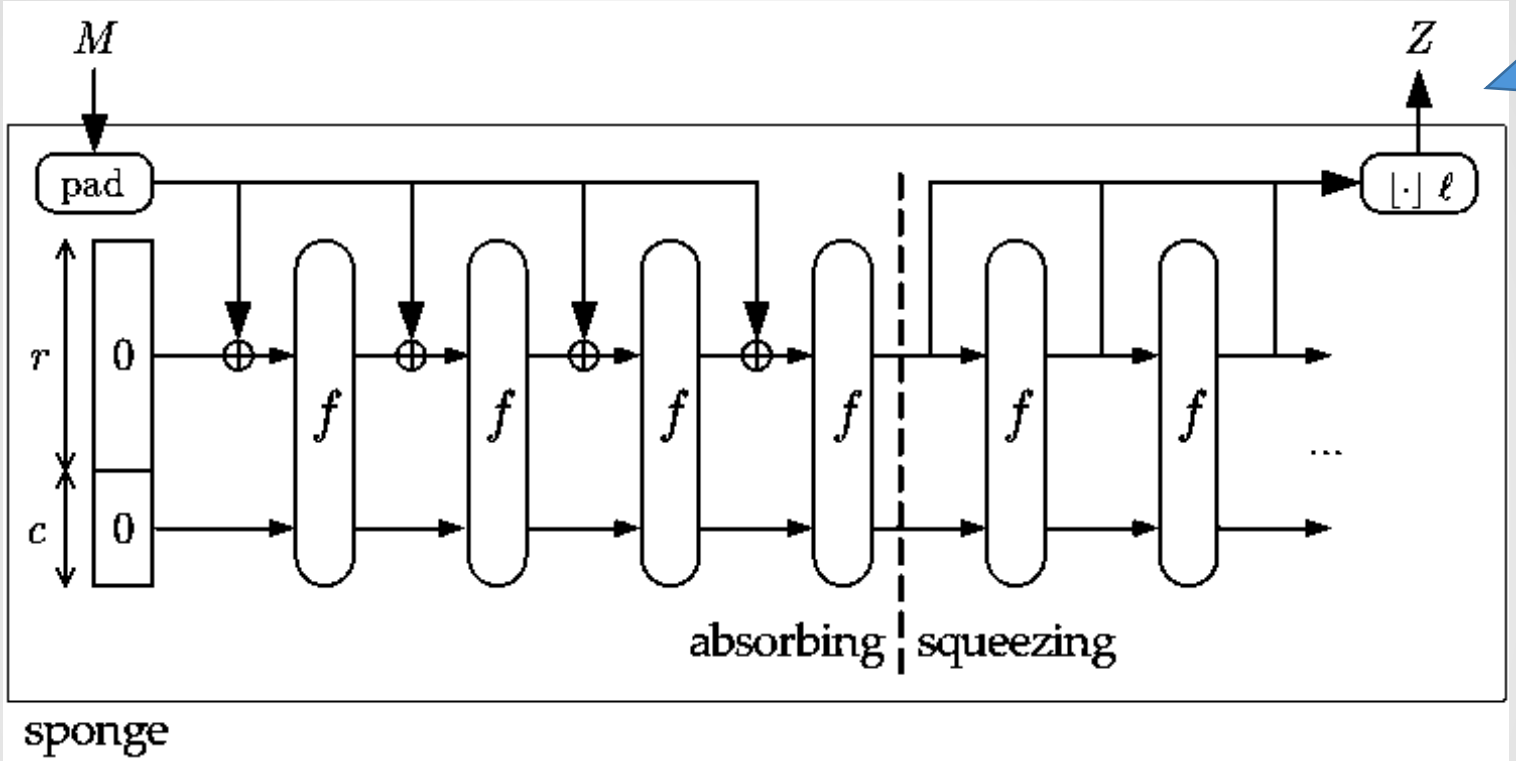
Classic hash functions were used be constructed based on Merkle-Damgard architecture. Message m padded to M, a multiple of a fixed-length block
M is divided into segments m_1,m_2, … m_n



Merkle-Damgard (1989)
F is called the compression function
- Takes inputs m_i and output of previous iteration
- Typically a series of rounds
- Output called a "chaining variable"
- Typically, a function operates on chaining variables then adds to m_i

Examples: MD5, SHA1, SHA2

Keccak – Sponge Construction

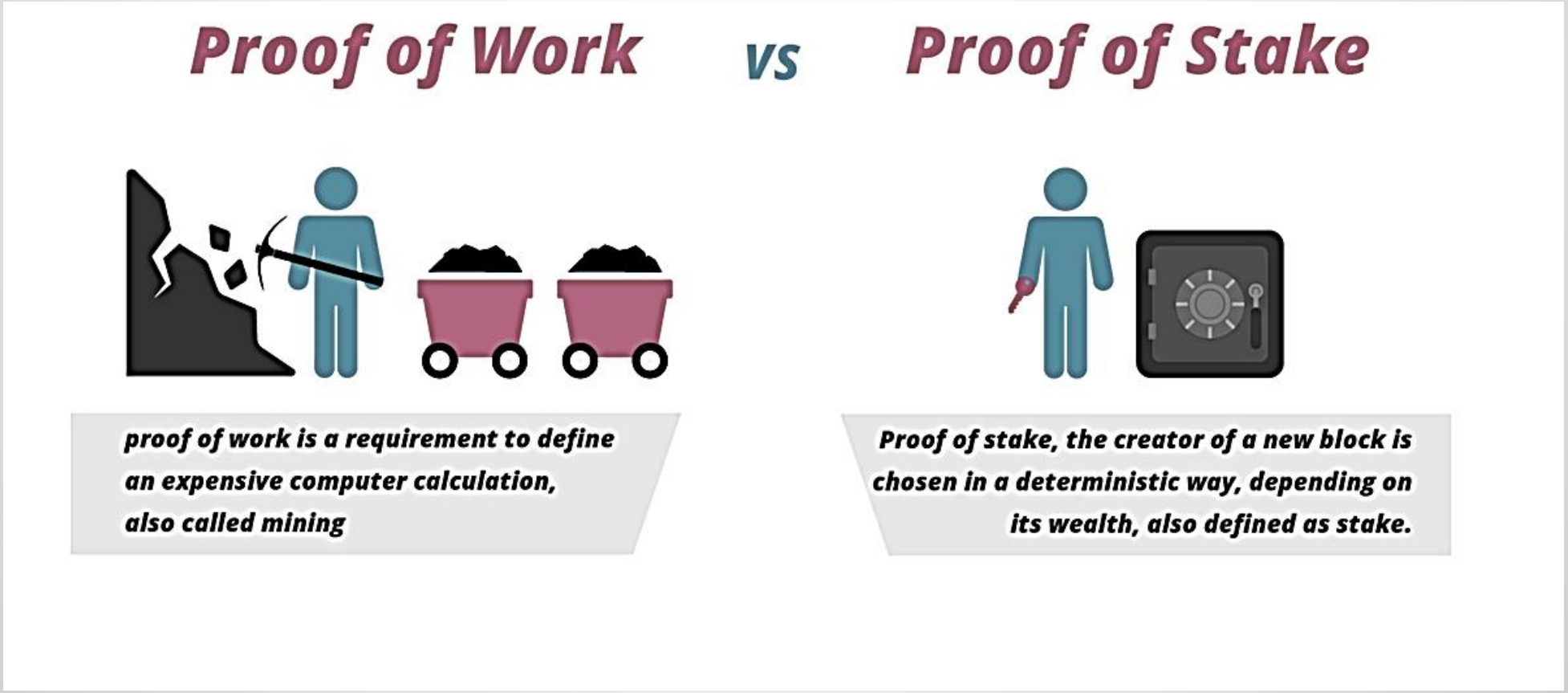


Ethereum used Keccak-256 before the merge.

- Each round, the next r bits of message is XOR'ed into the first r bits of the state, and a function f is applied to the state.
- After message is consumed, output r bits of each round as the hash output; continue applying f to get new states
- SHA-3 uses 1600 bits for state size.

Proof of Work vs Proof of Stake vs …

- PoW: It requires too much work, sometimes done in parallel, to find a block. Why should everybody do the mining?



Some Proofs

- **PoW** (e.g. Bitcoin, Ethereum classic)
  - Solving a **hard** mathematical puzzle, which can be **easily** verified by the others.
  - The solver gets some reward, and the reward is deemed acceptable by everybody.
  - **Problem:** Energy/Resource Waste.

- **PoS** (e.g. Ethereum in Beacon Chain & after Sep. 2022)
  - Miners are selected pseudo-randomly, yet deterministically, based on what they have at stake.
  - If a miner cheats, everybody can find out.
    - If he/she does wrong, he/she loses the deposit. The loss should be more than the reward for block construction.
  - **Problem:** The rich get richer.

Casper Protocol

- Ethereum version of PoS is called Casper.

- In the Casper protocol, validators (who have deposited 32ETH already) will set aside a portion of their ether as stake. When they discover blocks which they believe should be validated (or added to the Ethereum blockchain), they then place a bet on that block in ether.
  - If and when the block becomes appended to the chain, validators are rewarded based on their bets.

- Validators acting in a malicious way will be punished by having their stakes removed.

Some Other Proofs used in Consensus

- **PoB**
  - Those who want to be elected as the miner, burn some money/coins!
  - Burning is sending money to a null address. The more they burn the higher chance they will have to be elected and make money in the future.
  - People should be forward-looking.
  - **Problem:** Not a real solution for Energy/Resource Waste, still they have to burn the coins found by hard work.

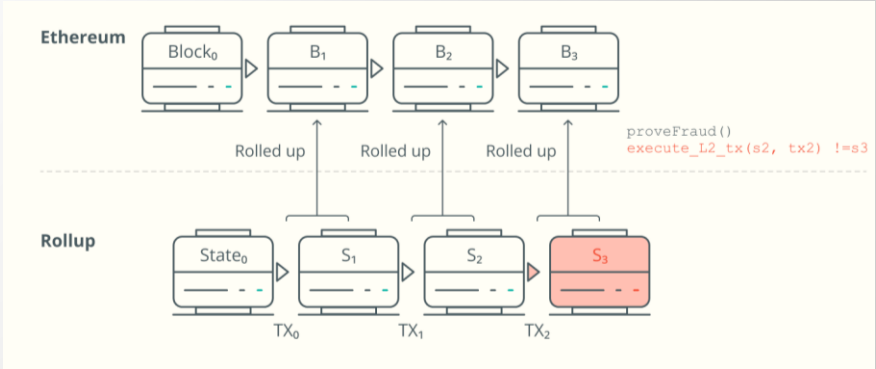
- **PoC/PoS (Proof of Capacity/Space)**
- **PoET (Proof of Elapsed Time)**
- **PoR (Proof of Reputation)** **e.g.** $\mathbf{\Delta R_A = (R_B * V_{BA})}$
- **PoA (Proof of Authority)**
- **…**

Final Note ：Off-Chain Ethereum Scaling Solutions

Plasma is an extra layer that sits on top of the network to handle massive amounts of transactions. It is basically Ethereum's version of **Bitcoin's Lightning Network**.

Raiden, like Plasma, is categorized as an off-chain scaling solution, and therefore can also be compared to the Lightning Network. Rather than processing the transactions on the main blockchain, Raiden uses the so called state channel technology to move transactions off-chain and open a separate payment channel.

Rollup, is not completely off-chain. The transactions happen off-chain but their abstract data is stored and synchronized on the main chain. This is supported by the addition of a new cheaper form of data attached to Ethereum blocks that is specially designed to make rollups cheap for users.



There are a few other scaling solution such as Validium, Sidechains, etc.

(cointelegraph.com, makeuseof.com)

https://ethtps.info

Search

Networks

No.	Name	TPS	Max recorded TPS	Type
1	Loopring	0.14	576	ZK rollup
2	Arbitrum One	2.22	120	Optimistic rollup
3	ZKSync	0.32	110	ZK rollup
4	Ethereum	24.02	56.88	Mainnet
5	Boba Network	0.01	43	Optimistic rollup
6	Immutable X	0.35	39.05	Validium
7	Metis	0.03	23	Optimistic rollup
8	Optimism	1.6	6	Optimistic rollup
9	ZKSwap	0	5.58	ZK rollup
10	Sorare	0.54	3.46	Validium
11	Arbitrum Nova	0.04	2	ZK rollup
12	ZKSpace	0.04	1.49	ZK rollup
13	Habitat	0	0.5	Optimistic rollup
14	DeversiFi	0	0.42	Validium
15	Nahmii 2.0	0	0.14	State pools
16	Aztec	0	0.11	ZK rollup
17	Starknet	0.03	0.08	ZK rollup
18	zkTube	0	0.06	ZK rollup
19	OMG Network	0	0	Plasma

What Comes Next …

- We learned how the new Ethereum works after the merge.
- We got familiar with other consensus mechanisms (other than PoW and PoS).
- We finish the Ethereum discussion here and move to other DLTs in the next session.

See you in the next session …