# Ethereum

Slides from Dan Boneh

# Recap of the Last Lecture

- Sybil Attack
  - Adversary impersonates many different nodes to outnumber the honest nodes.
- Sybil Resistance
  - Proof-of-Work: must solve computationally hard puzzle to propose block
- Bitcoin and Nakamoto Consensus
  - Longest chain rule
- Incentives in Bitcoin
  - Block rewards (3.125BTC)
  - Transaction fees
  - Can these *incentives* guarantee *honest* participation?

# State Machine Replication in 1 slide

Let $LOG_t^i$ denote the log learned by a client $i$ at time $t$.

Then, a **secure** SMR protocol satisfies the following guarantees:

**Safety (Consistency):**

- For any two clients $i$ and $j$, and times $t$ and $s$: either $LOG_t^i \preccurlyeq LOG_s^j$ is true or $LOG_s^j \preccurlyeq LOG_t^i$ is true or both (Logs are consistent).

No double spend

**Liveness:**

- If a transaction $tx$ is input to an honest replica at some time $t$, then for all clients $i$, and times $s \geq t + T_{conf}$: $tx \in LOG_s^i$.

No censorship

# Limitations of Bitcoin

Recall: UTXO contains (hash of) ScriptPK

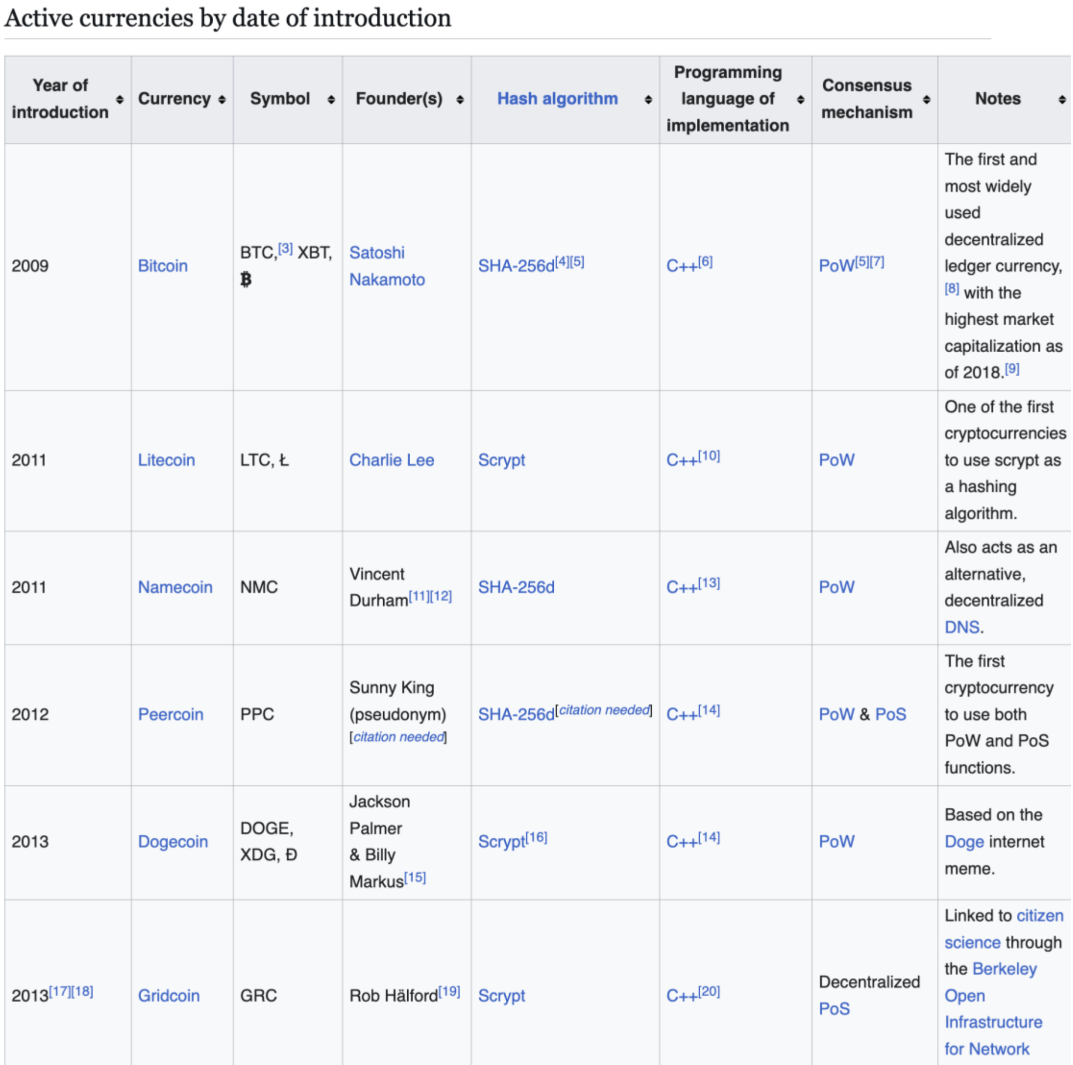
- simple script: indicates conditions when UTXO can be spent

Limitations:

- Difficult to maintain state in multi-stage contracts
- Difficult to enforce global rules on assets

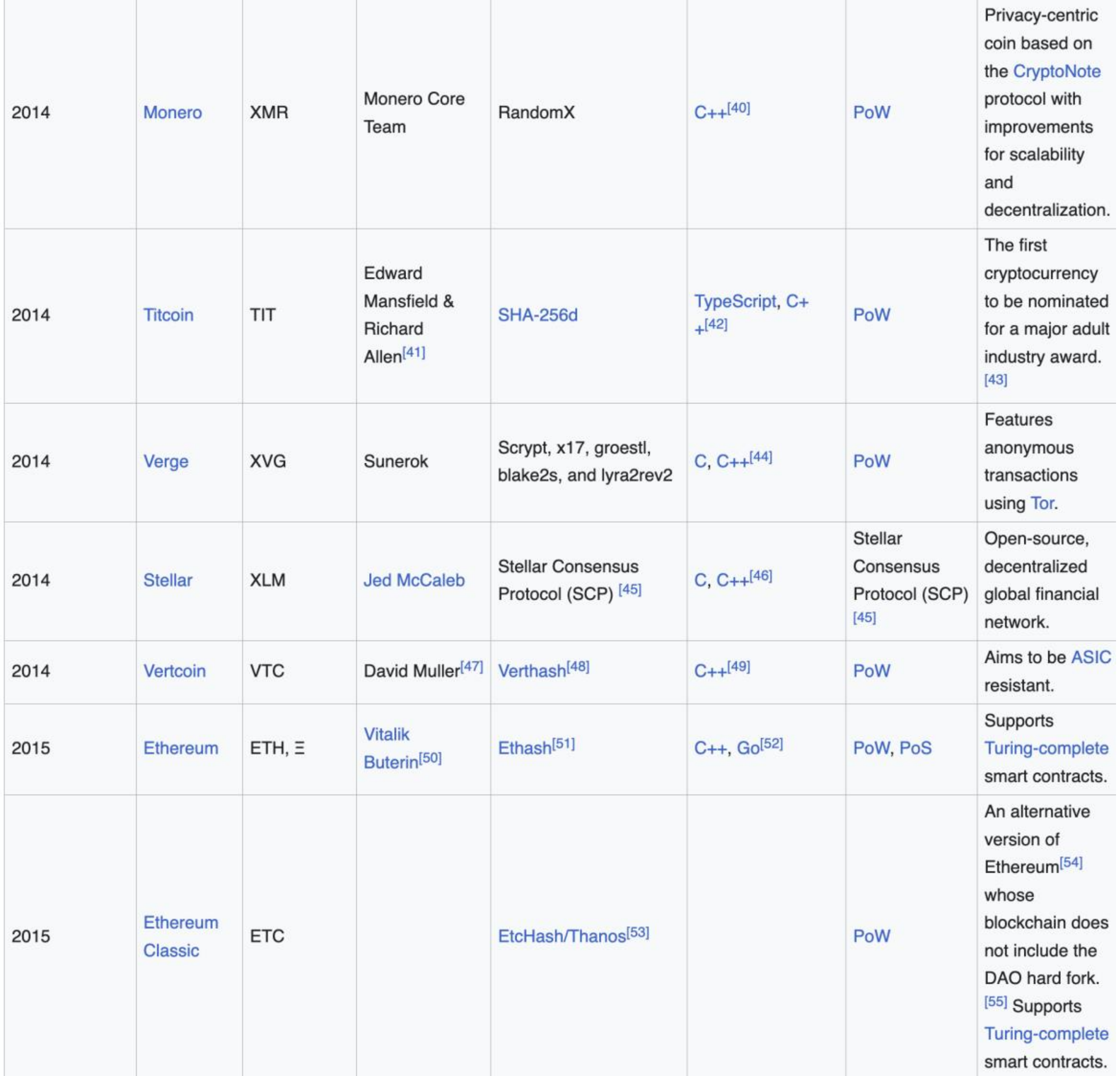
A simple example: rate limiting. My wallet manages 100 UTXOs.

- Desired policy: can only transfer 2BTC per day out of my wallet



## Active currencies by date of introduction

| Year of introduction | Currency | Symbol | Founder(s) | Hash algorithm | Programming language of implementation | Consensus mechanism | Notes |
|---|---|---|---|---|---|---|---|
| 2009 | Bitcoin | BTC,[3] XBT, ₿ | Satoshi Nakamoto | SHA-256d[4][5] | C++[6] | PoW[5][7] | The first and most widely used decentralized ledger currency,[8] with the highest market capitalization as of 2018.[9] |
| 2011 | Litecoin | LTC, Ł | Charlie Lee | Scrypt | C++[10] | PoW | One of the first cryptocurrencies to use scrypt as a hashing algorithm. |
| 2011 | Namecoin | NMC | Vincent Durham[11][12] | SHA-256d | C++[13] | PoW | Also acts as an alternative, decentralized DNS. |
| 2012 | Peercoin | PPC | Sunny King (pseudonym)[*citation needed*] | SHA-256d[*citation needed*] | C++[14] | PoW & PoS | The first cryptocurrency to use both PoW and PoS functions. |
| 2013 | Dogecoin | DOGE, XDG, Đ | Jackson Palmer & Billy Markus[15] | Scrypt[16] | C++[14] | PoW | Based on the Doge internet meme. |
| 2013[17][18] | Gridcoin | GRC | Rob Hälford[19] | Scrypt | C++[20] | Decentralized PoS | Linked to citizen science through the Berkeley Open Infrastructure for Network |



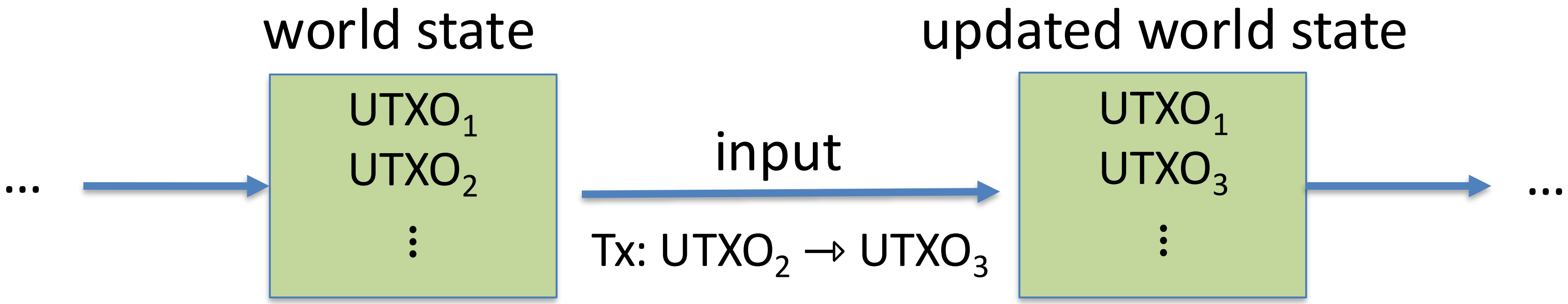
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2014 | Monero | XMR | Monero Core Team | RandomX | C++[40] | PoW | Privacy-centric coin based on the CryptoNote protocol with improvements for scalability and decentralization. |
| 2014 | Titcoin | TIT | Edward Mansfield & Richard Allen[41] | SHA-256d | TypeScript, C++[42] | PoW | The first cryptocurrency to be nominated for a major adult industry award.[43] |
| 2014 | Verge | XVG | Sunerok | Scrypt, x17, groestl, blake2s, and lyra2rev2 | C, C++[44] | PoW | Features anonymous transactions using Tor. |
| 2014 | Stellar | XLM | Jed McCaleb | Stellar Consensus Protocol (SCP) [45] | C, C++[46] | Stellar Consensus Protocol (SCP) [45] | Open-source, decentralized global financial network. |
| 2014 | Vertcoin | VTC | David Muller[47] | Verthash[48] | C++[49] | PoW | Aims to be ASIC resistant. |
| 2015 | Ethereum | ETH, Ξ | Vitalik Buterin[50] | Ethash[51] | C++, Go[52] | PoW, PoS | Supports Turing-complete smart contracts. |
| 2015 | Ethereum Classic | ETC | | EtcHash/Thanos[53] | | PoW | An alternative version of Ethereum[54] whose blockchain does not include the DAO hard fork.[55] Supports Turing-complete smart contracts. |

# Ethereum: on-chain Turing machine

- **New coins:** ERC-20 standard interface
- **DeFi**: exchanges, lending, stablecoins, derivatives, etc.
- **Insurance**
- **DAOs**: decentralized organizations
- **NFTs/RWAs**: Managing asset ownership (ERC-721 interface)

⋮

# Bitcoin as a state transition system



world state

$UTXO_1$
$UTXO_2$
⋮

input

Tx: $UTXO_2 \rightarrow UTXO_3$

updated world state

$UTXO_1$
$UTXO_3$
⋮

…

…

Bitcoin rules: $\boxed{F_{bitcoin} : S \times I \rightarrow S}$

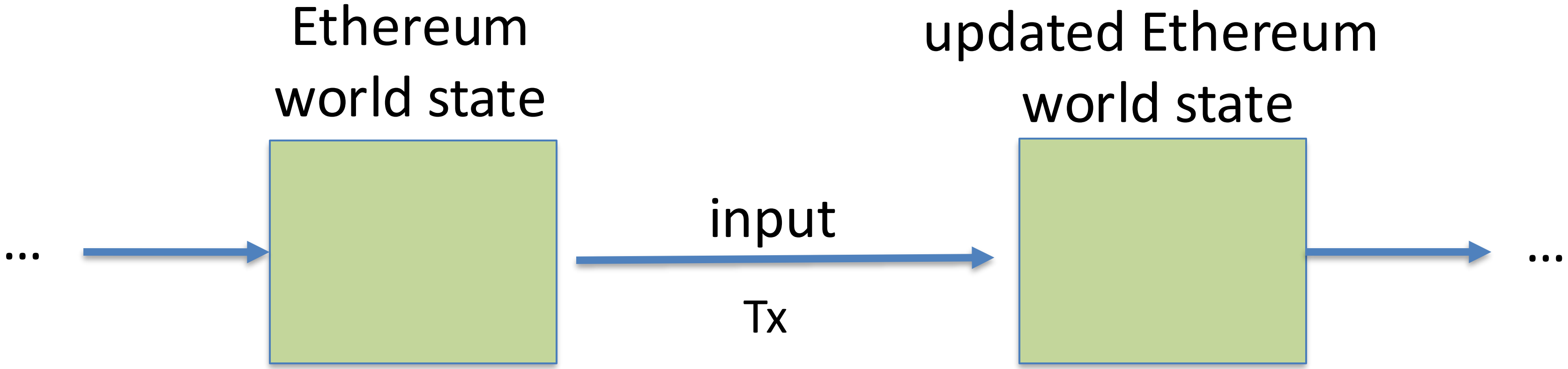
S: set of all possible world states, $s_0 \in S$ genesis state

I: set of all possible inputs

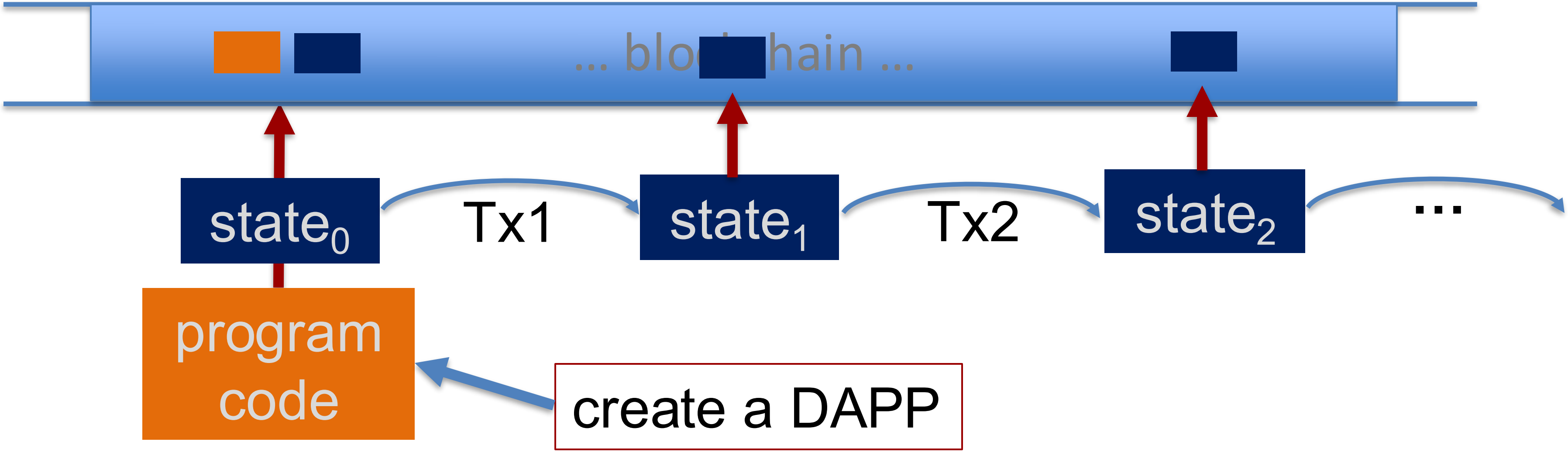
# Ethereum as a state transition system

Much richer state transition functions

⇒ one transition executes an entire program



# Running a program on a blockchain (DAPP)



create a DAPP

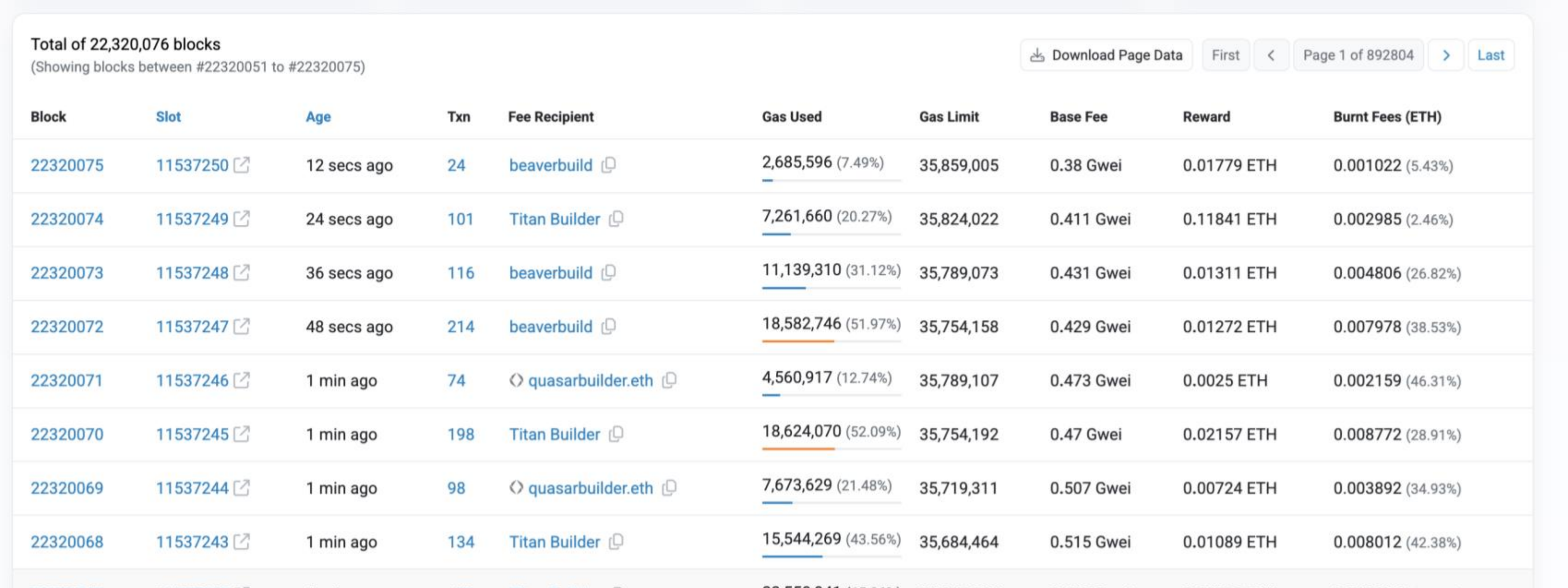
compute layer (execution chain): The EVM

consensus layer (Beacon chain)

# The Ethereum system

One block every 12 seconds (~150 Tx per block)

Block proposer receives Tx fees for block (+tips)



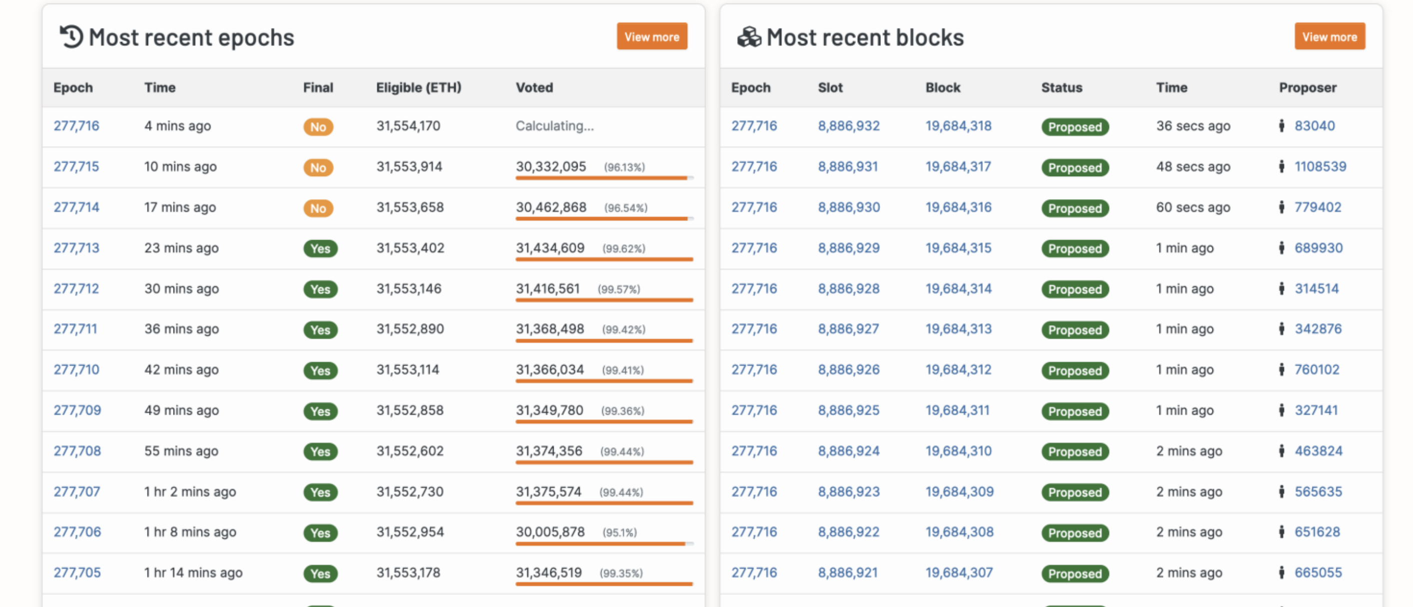
Total of 22,320,076 blocks
(Showing blocks between #22320051 to #22320075)

| Block | Slot | Age | Txn | Fee Recipient | Gas Used | Gas Limit | Base Fee | Reward | Burnt Fees (ETH) |
|---|---|---|---|---|---|---|---|---|---|
| 22320075 | 11537250 | 12 secs ago | 24 | beaverbuild | 2,685,596 (7.49%) | 35,859,005 | 0.38 Gwei | 0.01779 ETH | 0.001022 (5.43%) |
| 22320074 | 11537249 | 24 secs ago | 101 | Titan Builder | 7,261,660 (20.27%) | 35,824,022 | 0.411 Gwei | 0.11841 ETH | 0.002985 (2.46%) |
| 22320073 | 11537248 | 36 secs ago | 116 | beaverbuild | 11,139,310 (31.12%) | 35,789,073 | 0.431 Gwei | 0.01311 ETH | 0.004806 (26.82%) |
| 22320072 | 11537247 | 48 secs ago | 214 | beaverbuild | 18,582,746 (51.97%) | 35,754,158 | 0.429 Gwei | 0.01272 ETH | 0.007978 (38.53%) |
| 22320071 | 11537246 | 1 min ago | 74 | quasarbuilder.eth | 4,560,917 (12.74%) | 35,789,107 | 0.473 Gwei | 0.0025 ETH | 0.002159 (46.31%) |
| 22320070 | 11537245 | 1 min ago | 198 | Titan Builder | 18,624,070 (52.09%) | 35,754,192 | 0.47 Gwei | 0.02157 ETH | 0.008772 (28.91%) |
| 22320069 | 11537244 | 1 min ago | 98 | quasarbuilder.eth | 7,673,629 (21.48%) | 35,719,311 | 0.507 Gwei | 0.00724 ETH | 0.003892 (34.93%) |
| 22320068 | 11537243 | 1 min ago | 134 | Titan Builder | 15,544,269 (43.56%) | 35,684,464 | 0.515 Gwei | 0.01089 ETH | 0.008012 (42.38%) |

# The Ethereum system

One block every 12 seconds (~150 Tx per block)

Block proposer receives Tx fees for block (+tips)



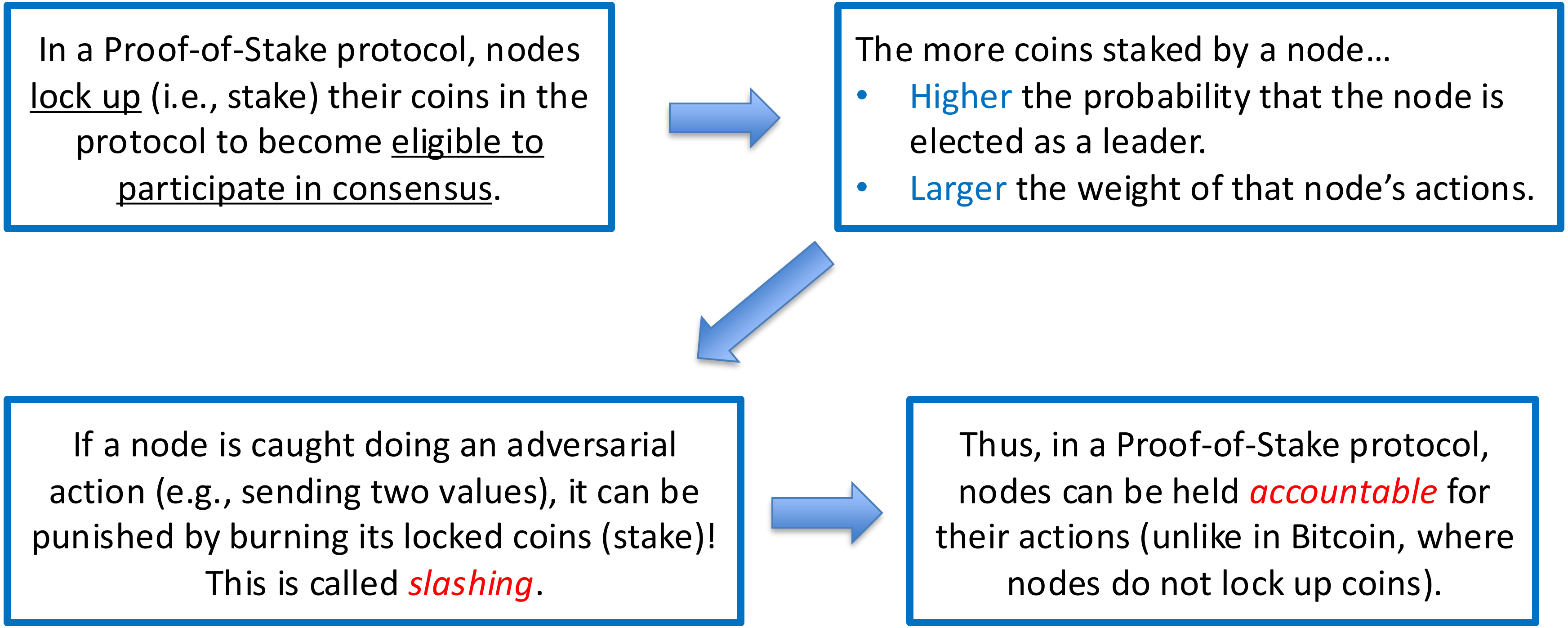
Most recent epochs

| Epoch | Time | Final | Eligible (ETH) | Voted |
|---|---|---|---|---|
| 277,716 | 4 mins ago | No | 31,554,170 | Calculating... |
| 277,715 | 10 mins ago | No | 31,553,914 | 30,332,095 (96.13%) |
| 277,714 | 17 mins ago | No | 31,553,658 | 30,462,868 (96.54%) |
| 277,713 | 23 mins ago | Yes | 31,553,402 | 31,434,609 (99.62%) |
| 277,712 | 30 mins ago | Yes | 31,553,146 | 31,416,561 (99.57%) |
| 277,711 | 36 mins ago | Yes | 31,552,890 | 31,368,498 (99.42%) |
| 277,710 | 42 mins ago | Yes | 31,553,114 | 31,366,034 (99.41%) |
| 277,709 | 49 mins ago | Yes | 31,552,858 | 31,349,780 (99.36%) |
| 277,708 | 55 mins ago | Yes | 31,552,602 | 31,374,356 (99.44%) |
| 277,707 | 1 hr 2 mins ago | Yes | 31,552,730 | 31,375,574 (99.44%) |
| 277,706 | 1 hr 8 mins ago | Yes | 31,552,954 | 30,005,878 (95.1%) |
| 277,705 | 1 hr 14 mins ago | Yes | 31,553,178 | 31,346,519 (99.35%) |

Most recent blocks

| Epoch | Slot | Block | Status | Time | Proposer |
|---|---|---|---|---|---|
| 277,716 | 8,886,932 | 19,684,318 | Proposed | 36 secs ago | 83040 |
| 277,716 | 8,886,931 | 19,684,317 | Proposed | 48 secs ago | 1108539 |
| 277,716 | 8,886,930 | 19,684,316 | Proposed | 60 secs ago | 779402 |
| 277,716 | 8,886,929 | 19,684,315 | Proposed | 1 min ago | 689930 |
| 277,716 | 8,886,928 | 19,684,314 | Proposed | 1 min ago | 314514 |
| 277,716 | 8,886,927 | 19,684,313 | Proposed | 1 min ago | 342876 |
| 277,716 | 8,886,926 | 19,684,312 | Proposed | 1 min ago | 760102 |
| 277,716 | 8,886,925 | 19,684,311 | Proposed | 1 min ago | 327141 |
| 277,716 | 8,886,924 | 19,684,310 | Proposed | 2 mins ago | 463824 |
| 277,716 | 8,886,923 | 19,684,309 | Proposed | 2 mins ago | 565635 |
| 277,716 | 8,886,922 | 19,684,308 | Proposed | 2 mins ago | 651628 |
| 277,716 | 8,886,921 | 19,684,307 | Proposed | 2 mins ago | 665055 |

# Ethereum is Proof-of-Stake (POS)



In a Proof-of-Stake protocol, nodes lock up (i.e., stake) their coins in the protocol to become eligible to participate in consensus.

The more coins staked by a node…

- Higher the probability that the node is elected as a leader.
- Larger the weight of that node's actions.

If a node is caught doing an adversarial action (e.g., sending two values), it can be punished by burning its locked coins (stake)! This is called *slashing*.

Thus, in a Proof-of-Stake protocol, nodes can be held *accountable* for their actions (unlike in Bitcoin, where nodes do not lock up coins).

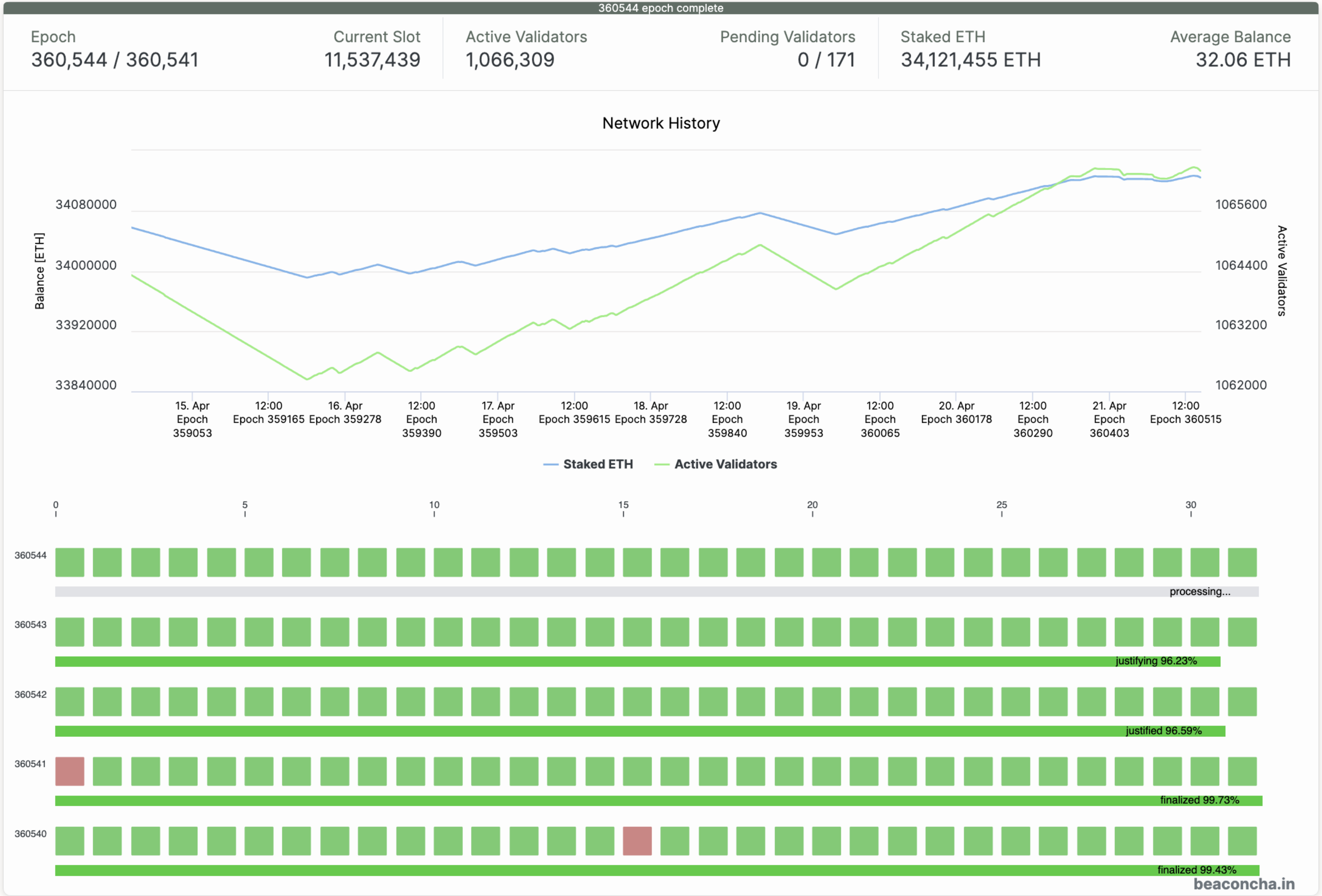
# A bit about the Beacon chain (Eth2 consensus layer)

To become a validator: stake (lock up) at least 32 ETH

Validators:

- sign blocks to express correctness (finalized once enough sigs)
- occasionally act as ***block proposer*** (chosen at random)
- correct behavior ⇒ get **new ETH** every epoch (32 blocks)
  small reward for attesting, large reward for proposing
- incorrect behavior ⇒ get **slashed** (lose ETH)

  cannot distinguish incorrect from malicious so must punish



360544 epoch complete

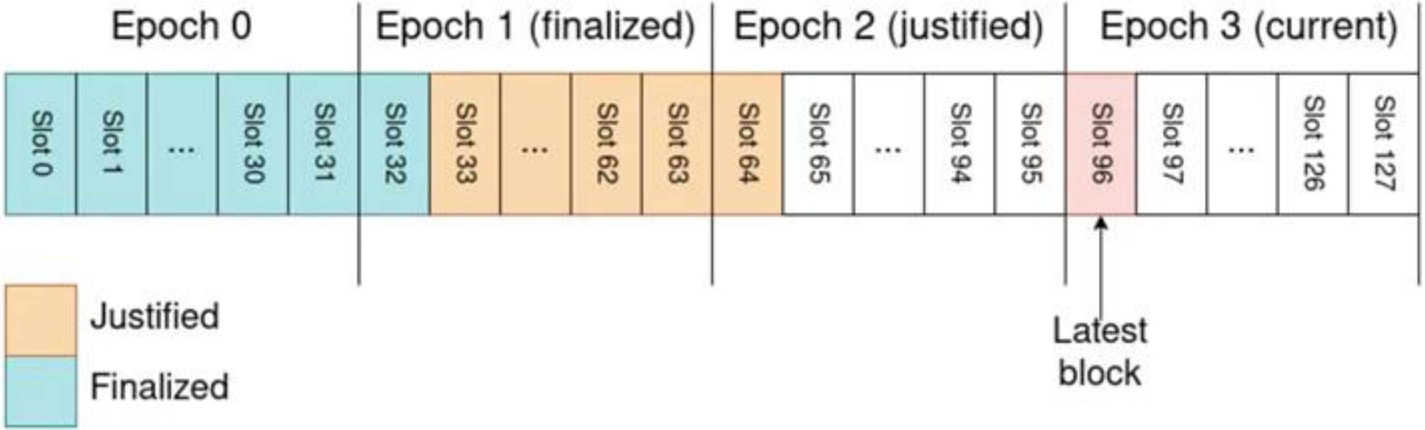
| Epoch | Current Slot | Active Validators | Pending Validators | Staked ETH | Average Balance |
|---|---|---|---|---|---|
| 360,544 / 360,541 | 11,537,439 | 1,066,309 | 0 / 171 | 34,121,455 ETH | 32.06 ETH |

Network History

| | 0 | | | | | 5 | | | | | 10 | | | | | 15 | | | | | 20 | | | | | 25 | | | | | 30 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 360544 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | processing... |
| 360543 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | justifying 96.23% |
| 360542 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | justified 96.59% |
| 360541 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | finalized 99.73% |
| 360540 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | finalized 99.43% |

beaconcha.in

# Blocks are proposed for slots



Epoch 0 | Epoch 1 (finalized) | Epoch 2 (justified) | Epoch 3 (current)

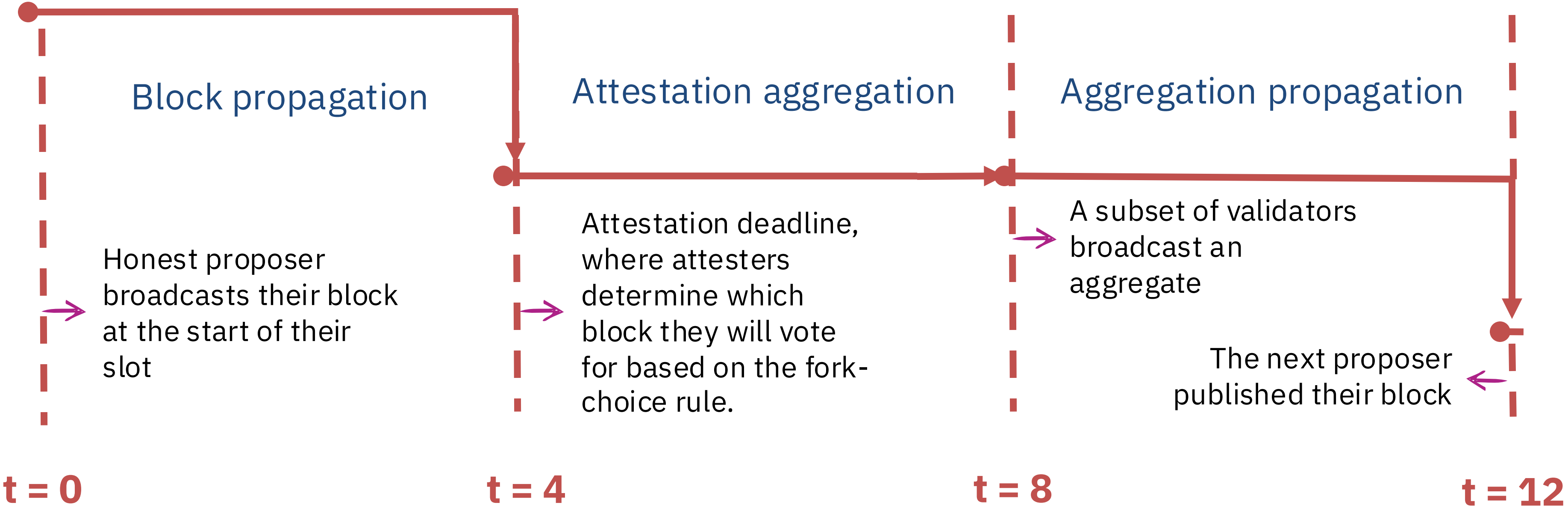
Slot 0 | Slot 1 | ... | Slot 30 | Slot 31 | Slot 32 | Slot 33 | ... | Slot 62 | Slot 63 | Slot 64 | Slot 65 | ... | Slot 94 | Slot 95 | Slot 96 | Slot 97 | ... | Slot 126 | Slot 127

Latest block

🟧 Justified

🟦 Finalized

# What happens within a slot?



Block propagation

Attestation aggregation

Aggregation propagation

Honest proposer broadcasts their block at the start of their slot

Attestation deadline, where attesters determine which block they will vote for based on the fork-choice rule.

A subset of validators broadcast an aggregate

The next proposer published their block

t = 0

t = 4

t = 8

t = 12

# Incentivized to behave correctly

Validator locks up 32 ETH.

Annual validator income (an example):

| | | |
|---|---|---|
| Issuance: | 1.0 ETH | |
| Tx fees: | 0.4 ETH | |
| MEV: | 0.4 ETH | |
| Total: | 1.8 ETH | (5.6% return on 32 ETH staked) |

Can be adjusted
(BASE_REWARD_FACTOR)

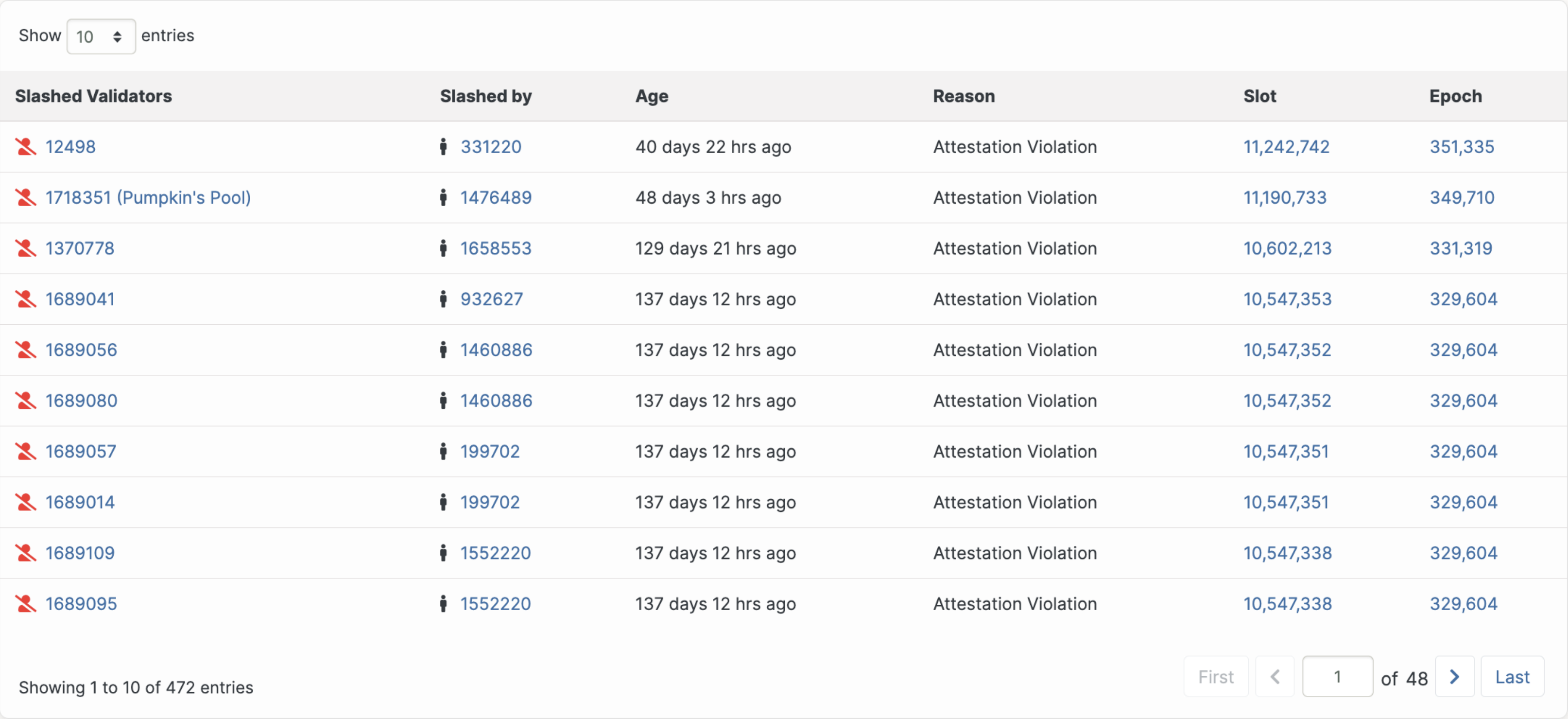
A function of congestion

In practice: staking provider (e.g., Ankr or LIOD) takes a cut

# How does slashing work?

- Slashed for breaking protocol rules
  - Double sign
  - Surround vote
- Penalty:
  - Exited from the beacon chain + lose % of staked ETH
  - When many validators are slashed: you lose more
- Incentive for slashing:
  - Receive rewards for reporting evidence of slashable offences.

# Does anybody get slashed?

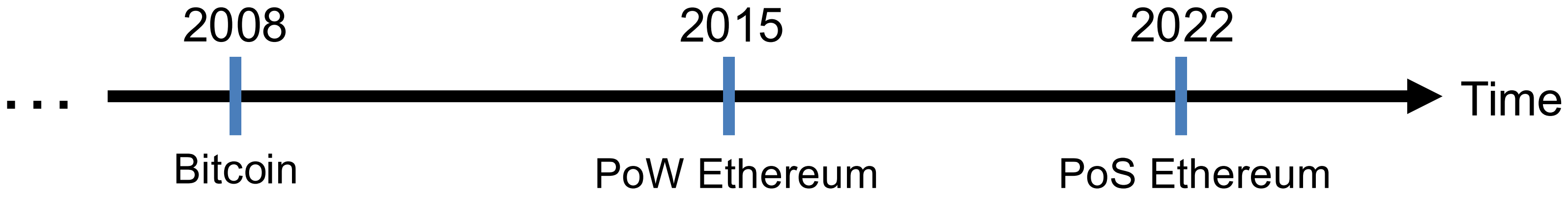


Show 10 entries

| Slashed Validators | Slashed by | Age | Reason | Slot | Epoch |
|---|---|---|---|---|---|
| 12498 | 331220 | 40 days 22 hrs ago | Attestation Violation | 11,242,742 | 351,335 |
| 1718351 (Pumpkin's Pool) | 1476489 | 48 days 3 hrs ago | Attestation Violation | 11,190,733 | 349,710 |
| 1370778 | 1658553 | 129 days 21 hrs ago | Attestation Violation | 10,602,213 | 331,319 |
| 1689041 | 932627 | 137 days 12 hrs ago | Attestation Violation | 10,547,353 | 329,604 |
| 1689056 | 1460886 | 137 days 12 hrs ago | Attestation Violation | 10,547,352 | 329,604 |
| 1689080 | 1460886 | 137 days 12 hrs ago | Attestation Violation | 10,547,352 | 329,604 |
| 1689057 | 199702 | 137 days 12 hrs ago | Attestation Violation | 10,547,351 | 329,604 |
| 1689014 | 199702 | 137 days 12 hrs ago | Attestation Violation | 10,547,351 | 329,604 |
| 1689109 | 1552220 | 137 days 12 hrs ago | Attestation Violation | 10,547,338 | 329,604 |
| 1689095 | 1552220 | 137 days 12 hrs ago | Attestation Violation | 10,547,338 | 329,604 |

Showing 1 to 10 of 472 entries

# What security do get from this?



Consensus in the Internet Setting

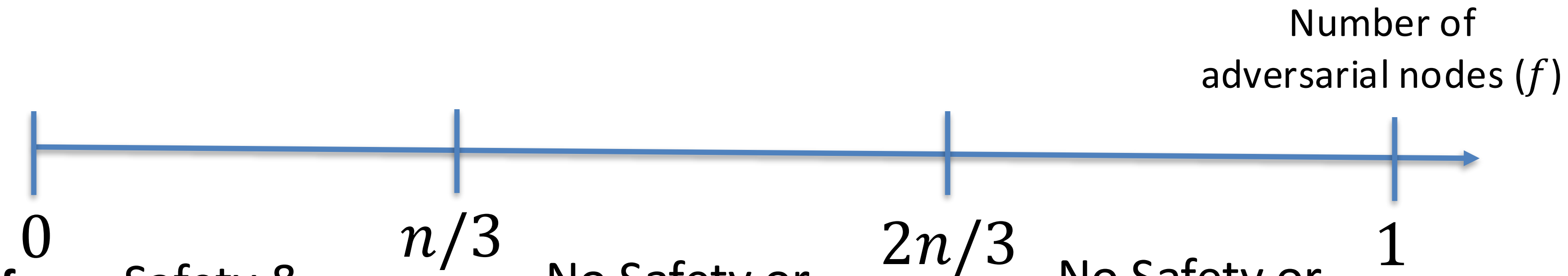
- Sybil resistance
- Dynamic availability
    - (Liveness under changing part.)

Block rewards (carrot)

- ➢ to incentivize participation!

- ➢ Consensus in the Internet Setting
    - ➢ Sybil resistance
    - ➢ Dynamic availability
- ➢ Block rewards (carrot)
- ➢ Finality and accountable safety
- ➢ Slashing (stick)
    - ➢ to punish protocol violation!

# Accountable Safety

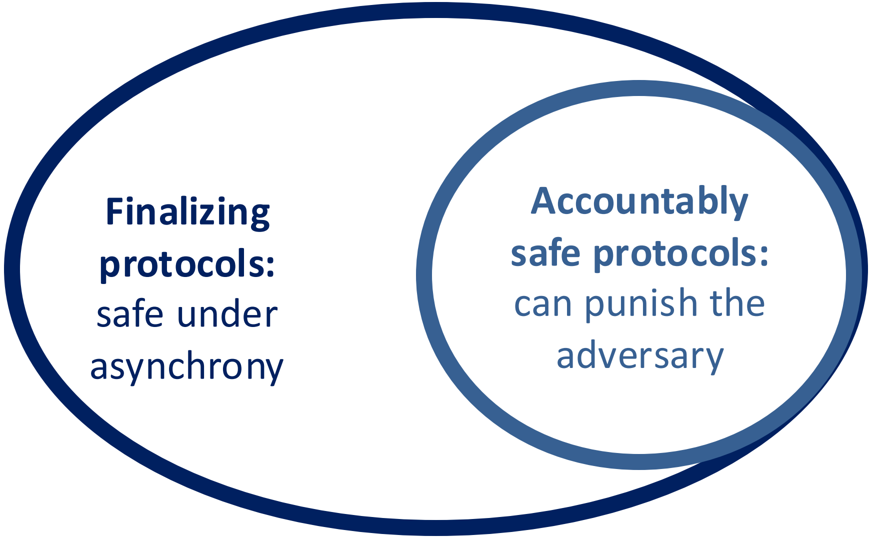


| | | | |
|---|---|---|---|
| **Resilience of n/3** | Safety & Liveness ☺ | No Safety or Liveness ☹ | No Safety or Liveness ☹ |
| **Accountable safety resilience of n/3** | Safety & Liveness ☺ | • No liveness ☹<br>• If safety is violated, catch and punish adversarial nodes ☺ | |

# Accountability implies Finality

**Accountability implies Finality:**

**Accountable safety** (with resilience $\frac{n}{3}$) implies **finality** (with resilience $\frac{n}{3}$).



**(Accountable safety:)** if the protocol can punish at least $\frac{n}{3}$ adv. nodes after a safety violation (and is safe when there are less than $\frac{n}{3}$ adv. nodes),

Then **(Finality:)** it must be safe when there are less than $\frac{n}{3}$ adv. nodes even under asynchrony.