



Haym @SalomonCrypto

Oct 6 · 26 tweets · [SalomonCrypto/status/1577863907976220672](#)

(1/25) [@ethereum](#) Fundamentals: Time, Slots and Epochs

The World Computer experiences time in an unintuitive way: a new block is proposed every 12 seconds, representing 1,000s of instantaneous changes within the EVM.

This is what happens during the rest of those 12 seconds.

(2/25) [@ethereum](#) is the World Computer, a globally shared computing platform that exists between a network of 1,000s of computers, each running a local version of the Ethereum Virtual Machine (EVM).

The network is able to stay in sync using a consensus system.



(3/25) For its first 7 years, [@ethereum](#) used Proof of Work (PoW) to reach consensus and stay in sync; today it uses Proof of Stake (PoS).

Both methods are predicated on identifying a node who gets the privilege of adding a new block to the blockchain.

(4/25) Under PoW, nodes (miners) compete to earn the right to be the next block proposer. The proposer is a powerful position; not only can they pick, choose and order the txns as they desire, they also earn:

- Block rewards, paid by the network
- Tips, paid by the txn generator

(5/25) The competition: an incredibly difficult puzzle which can only be solved by trial and error. Miners guess and guess until they solve the puzzle, proving they've done work in the real world (using electricity to power the machines solving these puzzles).

(6/25) Under PoW, the block proposer was the miner who was able to solve a cryptographic puzzle the fastest. When finished, it broadcasts its block to every other node in the network.

Each node then checks to make sure the txns are valid and the puzzle is complete.

(7/25) PoS is fundamentally different - there is no competition at all.

Instead of choosing the next block proposer by wasting as much electricity as possible, what if we just... took turns?

This is the core of PoS; the 32 \$ETH stake is just a bond to guarantee good behavior.

(8/25) One effect of changing from PoW to PoS is that we've switched the fundamental cadence of [@ethereum](#) to be based on a unit of time derived from a an unpredictable race to turn-based system.


By its very nature, we can't control the timing of PoW, but we can with PoS.

(9/25) Today, time on the World Computer is divided into 12 second units called "slots."

Every slot, a different validator is assigned to propose a new block. If it does its duties, it will propose a valid block (within 4 seconds), otherwise the slot will pass along empty.

(10/25) The block proposer will send the block to every node in the network who is then responsible for processing it and updating the state of their EVM.

This keeps all nodes in sync with the proposer, and turns the environment of the EVM into the collective World Computer.

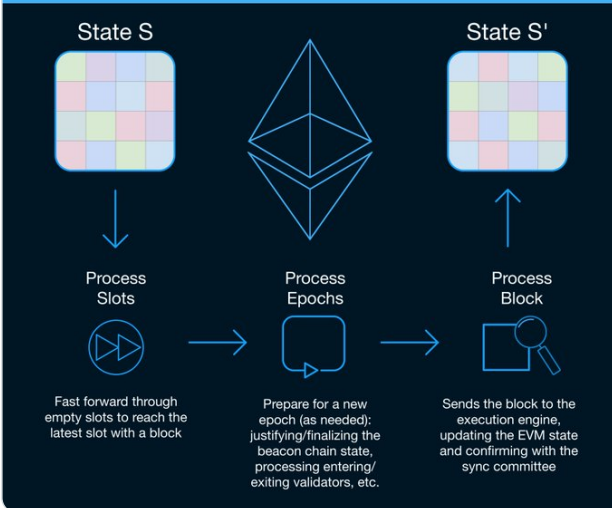
 **Haym**
@SalomonCrypto · Follow

(1/17) @ethereum Fundamentals: The (Post-Merge) State Transition Function

The World Computer is a decentralized state machine, let's walk through the state transition function

Sound like nonsense? This thread will explain what happens every time a validator receives a new block

State Transition Function




The diagram illustrates the State Transition Function process. It starts with 'State S' (a 4x4 grid of colored squares) and ends with 'State S'' (another 4x4 grid). The process is divided into three main steps, each with an icon and a description:

- Process Slots:** Represented by a play button icon. Description: 'Fast forward through empty slots to reach the latest slot with a block'.
- Process Epochs:** Represented by a circular arrow icon. Description: 'Prepare for a new epoch (as needed): justifying/finalizing the beacon chain state, processing entering/exiting validators, etc.'.
- Process Block:** Represented by a magnifying glass icon. Description: 'Sends the block to the execution engine, updating the EVM state and confirming with the sync committee'.

Arrows indicate the flow from State S to Process Slots, then to Process Epochs, then to Process Block, and finally to State S'. A central Ethereum logo is also present.

8:03 PM · Oct 5, 2022

 [Read the full conversation on Twitter](#)

128 Reply Copy link

[Read 6 replies](#)

(11/25) Each slot also has a committee assigned to it. A committee is a group of validators who are assigned to verify and attest to the validity of the block broadcasted by the block proposer.

After verification, committee members broadcast a cryptographic attestation.


(12/25) At this moment, there are 440k validators. If every validator was on every committee, the network would freeze under a deluge of attestations.


So we make a decentralization trade-off. Every validator will not attest to every slot, but they will attest to every epoch.

(13/25) Epochs are made of 32 slots. 1 slot = 12 secs, so 1 epoch = 6 mins 24 secs

At the beginning of each slot, the entire validator group is randomly split into 32 committees corresponding to the 32 slots of the upcoming epoch

This randomness is non-trivial; we need RANDAO

**Haym**
@SalomonCrypto · Follow



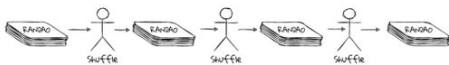
(1/20) @ethereum Fundamentals: Randomness and RANDAO

Randomness is critical property for crypto and the World Computer. Unfortunately, computers are terrible at generating randomness without external input... and the EVM has no external input.

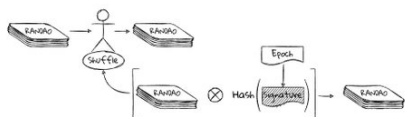
A guide to untrusted randomness.

RANDAO

Goal: randomly shuffle the deck between untrusted parties







Solution: pass it around the table, shuffling it each time



Each Signature is hashed and combined with RANDAO using xor

3:04 PM · Oct 3, 2022

 [Read the full conversation on Twitter](#)

 203  Reply  Copy link

[Read 8 replies](#)

(14/25) Each slot brings a new committee forward. The first member is the block proposer; the rest are attesters.

The block proposer has 4 seconds to send a block to the committee. Each member verifies the block and creates a BLS signature (no block, they attest to last block).

(15/25) A BLS signature is a digital signature that provides all the normal guarantees (proof a specific message was signed by a specific person) but has a useful bonus property: it can be aggregated.

Once aggregated, thousands of signatures can be verified in one operation.

 **Haym**
@SalomonCrypto · Follow

(1/12) Cryptography 201: BLS Digital Signatures

Digital signatures provide cryptographic assurance that a specific person sent a specific message. Their existence is critical, but traditional digital signatures are not scalable.

A manual for aggregation and acceleration.



12:22 AM · Sep 29, 2022

 [Read the full conversation on Twitter](#)

153 Reply Copy link

[Read 8 replies](#)

(16/25) For those of you not following along at home, 440k validators / 32 committees = 13.7k validators / committees. This is too big a number to aggregate all at once.

And so, committees are broken up into 128 subnets.

~100 validators / subnet

(17/25) In each subnet, 16 validators are designated as aggregators. All subnet-members publish their BLS signatures, but only aggregators listen and do the aggregation.

All 16 are trying to build the same ideal aggregate signature, but conditions are often not ideal.

(18/25) Next, the block proposer will pick the best BLS aggregate signature, one from each of the 128 subnets

The BLS aggregation algorithm is applied one final time, and the 128 subnet signatures are merged into one final committee BLS signature, representing ~13.7k validators

(19/25) As an aside, this whole process is the reason 32 \$ETH is the minimum amount of \$ETH required to become a validator. This aggregation process is slow and complex; reducing the minimum stake increases the number of validators, exponentially increasing the problem.

(20/25) After 32 slots, an epoch ends.

At the end of every epoch, every validator runs `process_epoch`. The tweet below will give you more detailed information, but we'll summarize it in 2 sections:

- 1) Finalization
- 2) Consensus and Housekeeping

**Haym**
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(8/17) Consensus Spec: `process_epoch`

Below is the consensus spec, as you can see it's very dense. The next tweet will provide a summary of each step.

```
def process_epoch(state: BeaconState) -> None:
    process_justification_and_finalization(state) # [Modified in Altair]
    process_inactivity_updates(state) # [New in Altair]
    process_rewards_and_penalties(state) # [Modified in Altair]
    process_registry_updates(state)
    process_slashings(state) # [Modified in Altair]
    process_eth1_data_reset(state)
    process_effective_balance_updates(state)
    process_slashings_reset(state)
    process_randao_mixes_reset(state)
    process_historical_roots_update(state)
    process_participation_flag_updates(state) # [New in Altair]
    process_sync_committee_updates(state) # [New in Altair]
```

8:03 PM · Oct 5, 2022

  Reply  Copy link

Read 1 reply

(21/25) Finalization is the application of the Casper FFG protocol.

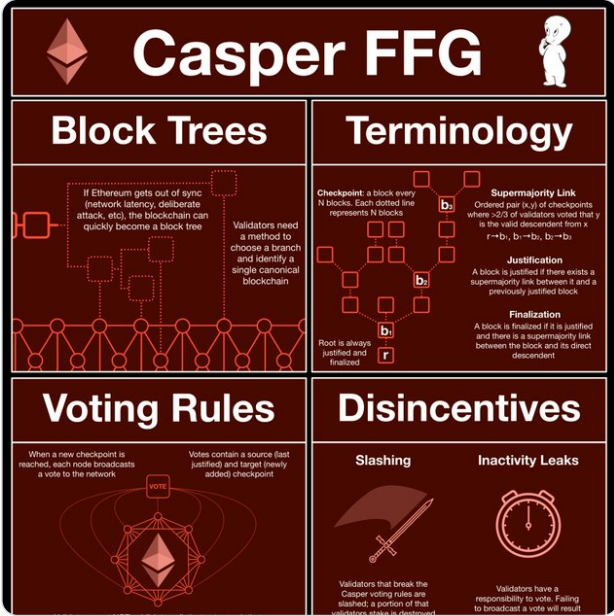
Tl;dr Finalization is a promise by the protocol that an epoch (and therefore the blocks/txns within) are irreversible.

 **Haym**
@SalomonCrypto · Follow

(1/22) @ethereum Consensus: Casper FFG

The World Computer coordinates via Proof of Stake; validators place \$ETH at stake in order to participate in the system. But what actually IS this system and how does it achieve consensus?

A guide to Ethereum finality.



The infographic is titled "Casper FFG" and is divided into four main sections: Block Trees, Terminology, Voting Rules, and Disincentives.
- **Block Trees**: Explains that if Ethereum gets out of sync, the blockchain can become a block tree. It shows a diagram of a block tree and states that validators need a method to choose a branch and identify a single canonical blockchain.
- **Terminology**: Defines key concepts:
 - **Checkpoint**: A block every N blocks. Each dotted line represents N blocks.
 - **Supermajority Link**: An ordered pair (x, y) of checkpoints where >2/3 of validators voted that y is the valid descendant from x.
 - **Justification**: A block is justified if there exists a supermajority link between it and a previously justified block.
 - **Finalization**: A block is finalized if it is justified and there is a supermajority link between the block and its direct descendant.
- **Voting Rules**: States that when a new checkpoint is reached, each node broadcasts a vote to the network. It also notes that votes contain a source (last justified) and target (newly added) checkpoint.
- **Disincentives**:
 - **Slashing**: Validators that break the Casper voting rules are slashed; a portion of that validator's stake is destroyed.
 - **Inactivity Leaks**: Validators have a responsibility to vote. Failing to broadcast a vote will result in a loss of stake.
The infographic includes various diagrams: a block tree, a checkpoint diagram, a supermajority link diagram, a voting diagram, a slashing diagram, and an inactivity leak diagram.

11:52 PM · Oct 2, 2022

 [Read the full conversation on Twitter](#)

338 Reply Copy link

[Read 8 replies](#)

(22/25) Finalization is the mathematical and economic guarantee that a specific action on the World Computer is part of the canonical blockchain.

Undoing a single finalized transaction would necessitate destroying 1/3 of staked \$ETH - more than \$20B, today.

(23/25) Epochs mark the boundaries for finalization.

If more than 2/3s of the network attest during an epoch, it becomes justified.

If a second epoch with a 2/3 majority follows the first, it will finalize that epoch, granting it the security guarantees of @ethereum.

(24/25) The other section of process_epoch is consensus and housekeeping.

Basically this is everything needed to uphold the rules of consensus (processing slashing, rewards, etc) and resetting the stage for the next epoch.

Again, if you want more detail check the other thread.

(25/25) In summary:

Slot: every 12 secs, the World Computer expects a new block (EVM changes)

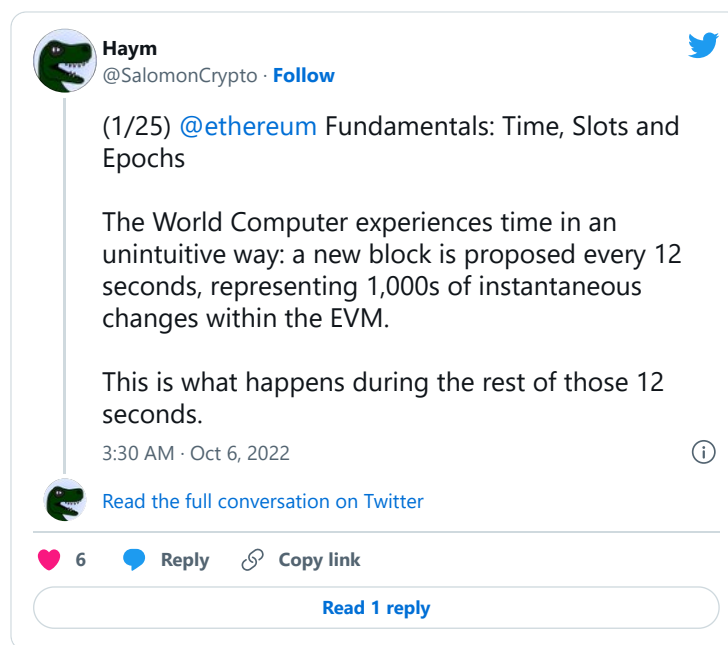
Epoch: every 32 slots, the entire network votes

Finalization: following justification, a second supermajority of validators vote to confirm an epoch

Finalization = \$ETH security

Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.



...