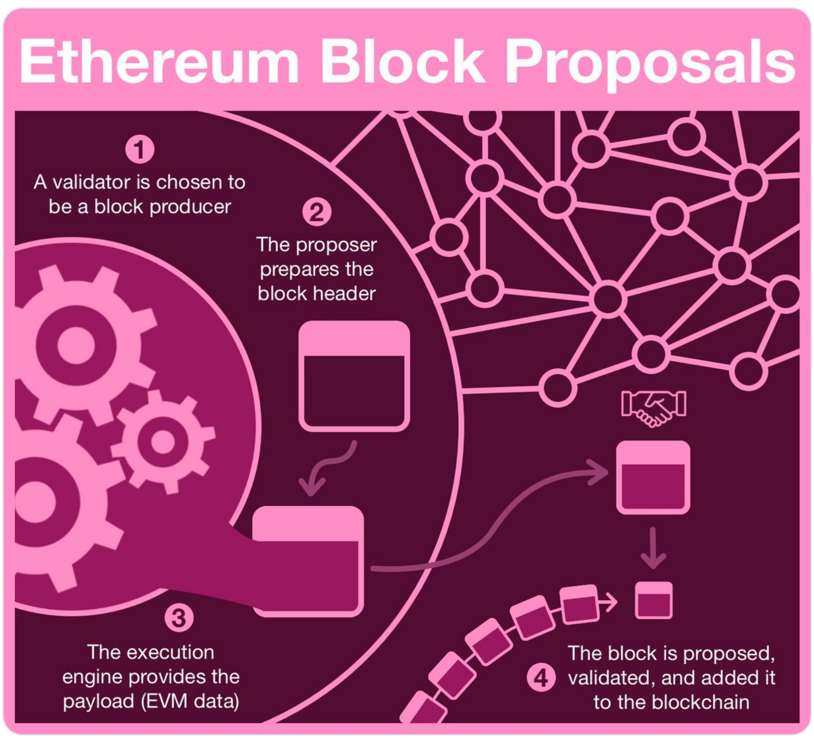
Haym @SalomonCrypto
Oct 8 • 26 tweets • SalomonCrypto/status/1578842388964859904

(1/25) @ethereum Fundamentals: Block Proposals

Once every 12 seconds, a block is born. Have you ever thought about how a block is made? Or how it is accepted by the network and added to the blockchain?

Want to know how everything is going to change... again?



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

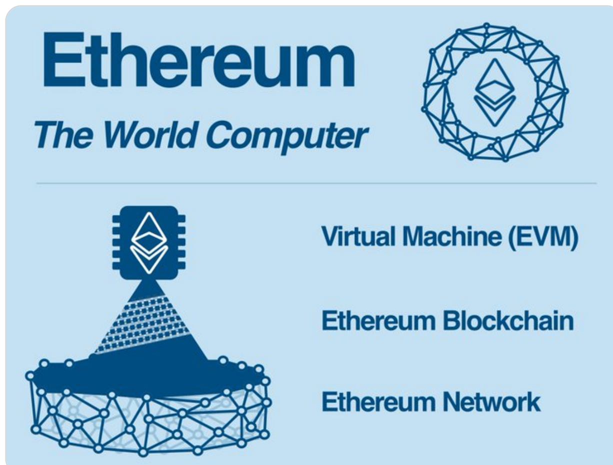
Every local EVM is in sync; the state of any node is the state of the World Computer.

Haym
@SalomonCrypto · **Follow**

(1/7) The Hitchhiker's Guide to @ethereum

In 2014, @VitalikButerin gave us an idea that WILL change the world. Have you wrapped your head around The World Computer yet?

DON'T PANIC, I'll break it down for you. Read on for 4 threads that will show you the future.



1:01 AM · Aug 3, 2022

Read the full conversation on Twitter

432 Reply Copy link

Read 17 replies

(3/25) The EVM is an isolated unit; it cannot reach out to other nodes and interact directly with another EVM.

Instead, the EVM is attached to a consensus mechanism, which is responsible for communicating between nodes, securing @ethereum and updating the EVM.

(4/25) A consensus mechanism will do things:

- select a leader (block proposer)
- allow a proposer to submit a change to the EVM (block) to the network
- allow the network to confirm the block was valid
- provide credibly security guarantees

(5/25) Originally, the World Computer used Proof of Work (PoW) as its consensus mechanism.

Today, @ethereum has replaced PoW with Proof of Stake (PoS).

Haym
@SalomonCrypto · Follow

(1/25) @ethereum Basics: Consensus Systems

Beneath all these tokens and expensive-jpegs is a distributed platform operated by 1000s of untrusted computers. But how can 1 computer exist on top of 1000s?

Do you understand how Proof of Work and Proof of Stake REALLY work?

7:44 PM · Oct 7, 2022

Read the full conversation on Twitter

203 Reply Copy link

Read 12 replies

(6/25) Just due to how PoW operates, block proposer selection is very straightforward; all nodes are potential block proposers but only the first person to solve the puzzle wins the privilege.

Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(5/25) PoW was invented for @Bitcoin by Satoshi Nakamoto in 2008. PoW is based around incredibly difficult mathematical puzzles; every node creates a new block and races to finish one of these puzzles.

The first to solve the puzzle proposes their block (with the solution).

7:44 PM · Oct 7, 2022

5 Reply Copy link

Read 1 reply

(7/25) Perhaps the biggest change from PoW to PoS is that PoS removes these puzzles entirely; In PoS, the block proposer is randomly selected.

Before we dive in, let's review a few key concepts:

(8/25) Time in @ethereum

Slot: 12 seconds, during which the block proposer (should) broadcast their block

Epoch: 32 slots = 6.4 minutes

Haym
@SalomonCrypto · **Follow**

(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.

3:30 AM · Oct 6, 2022

Read the full conversation on Twitter

528 Reply Copy link

Read 20 replies

(9/25) Randomness in [@ethereum]

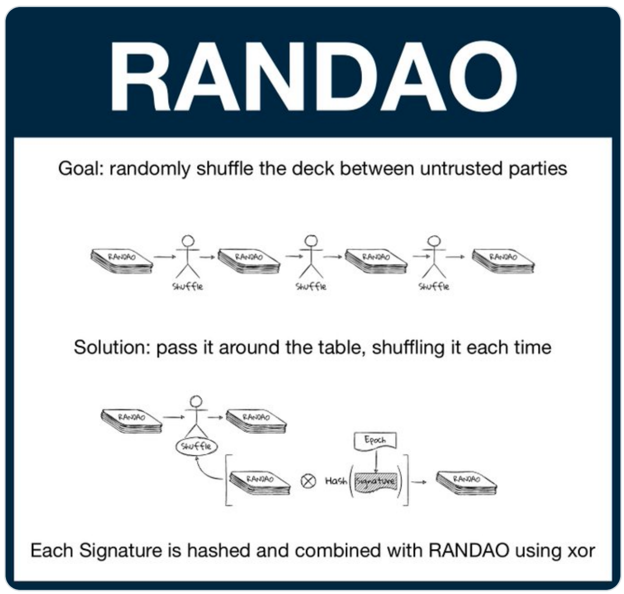
Credible randomness is critical to PoS's security design, particularly in regards to validator assignments (including block proposer). Ethereum uses a process called RANDAO to generate "good-enough" randomness.

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.



3:04 PM · Oct 3, 2022

Read the full conversation on Twitter

214 Reply Copy link

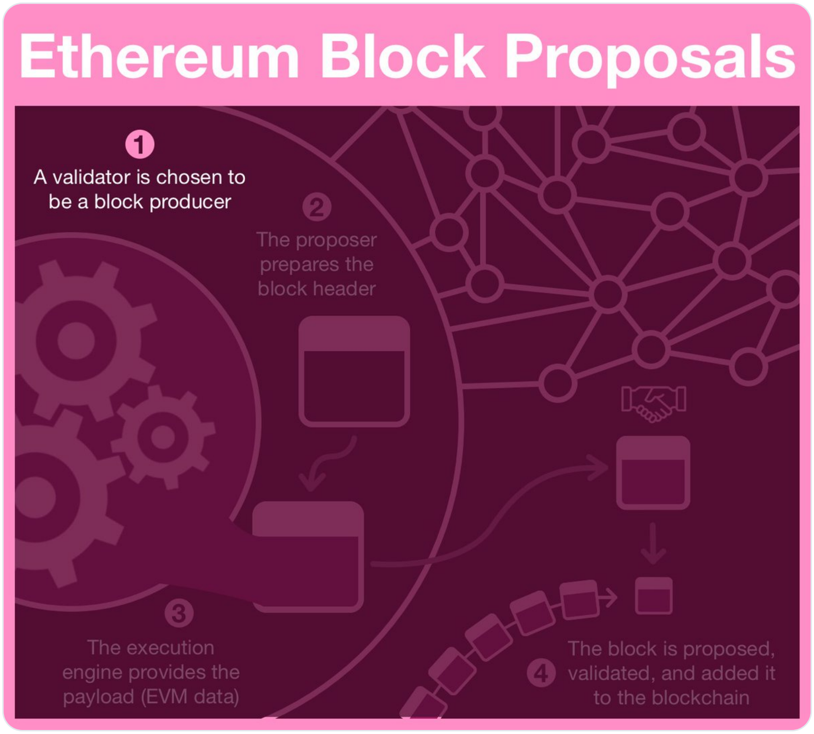
Read 8 replies

(10/25) At the beginning of every epoch, [@ethereum] executes a beacon chain shuffle, providing validator assignments (including block proposals) for the next epoch.

Beacon chain shuffling is a lookahead function; it provides assignments 1 epoch ahead to allow preparation.

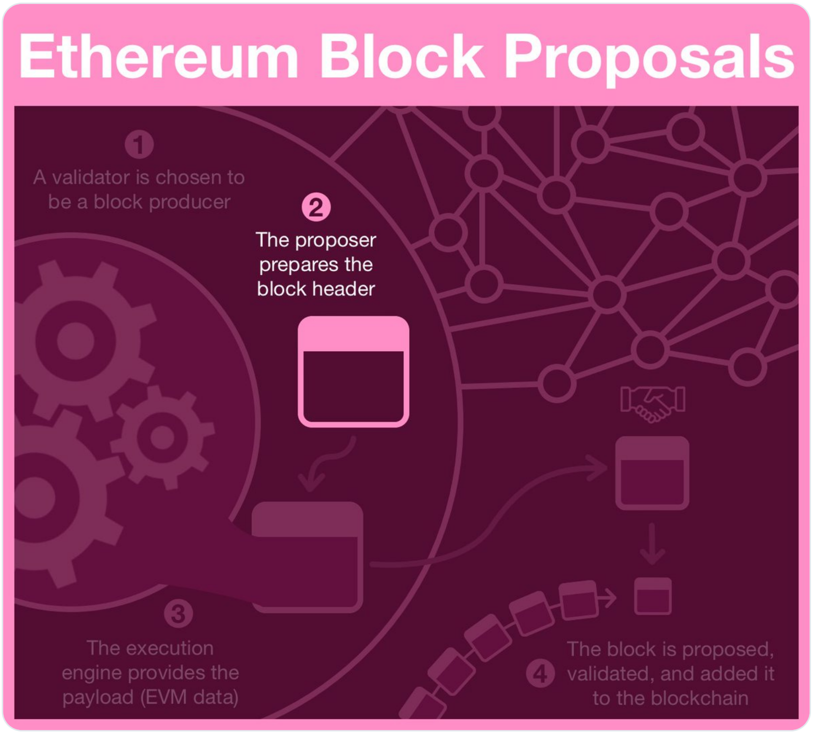
(11/25) Though the block producer was actually set at the beginning of the last epoch, it's useful to think of assignment of happening at the beginning of each slot.

And so, at the beginning of each slot, a validator is randomly chosen.



(12/25) The proposer begins building the block by filling out all of the block headers.

The block header contains all the information related to the beacon chain and PoS consensus. It does not contain any data about the EVM; in fact, the EVM cannot query this data (directly).

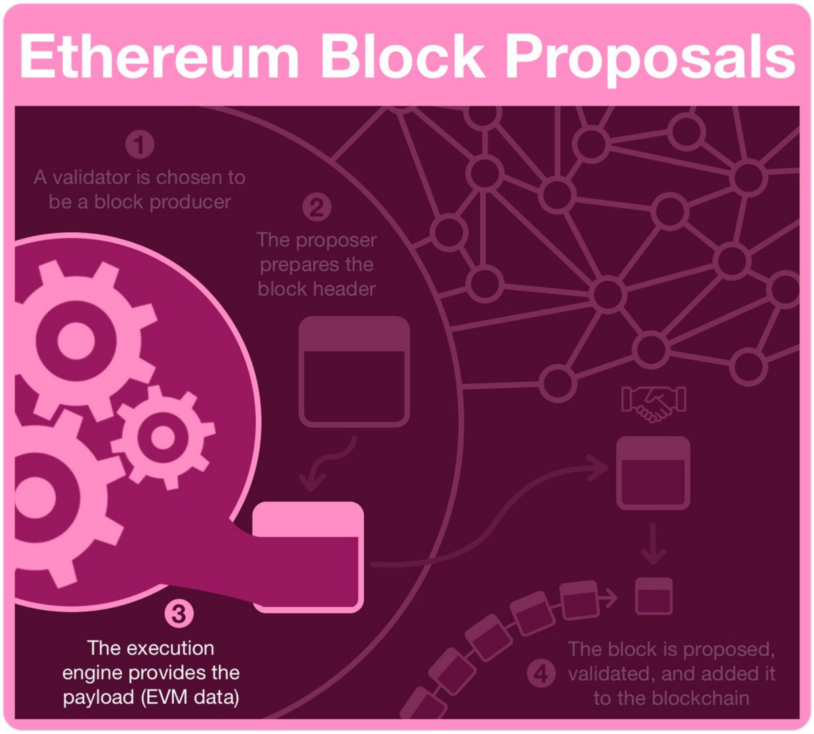


(13/25) Most of the header data is straightforward and/or can be identified using the block thread below (tweet 15).

Proposer and attester slashings are interesting; the validator receives a small "whistleblower" reward for including valid incidents.

(14/25) Next, the validator will turn to the execution engine, which is the process that holds the EVM.

In fact, the execution engine/layer is nearly identical to what was happening when [@ethereum](https://twitter.com/ethereum) was using PoW.



(15/25) The easiest way to understand block construction is to just look at a block.

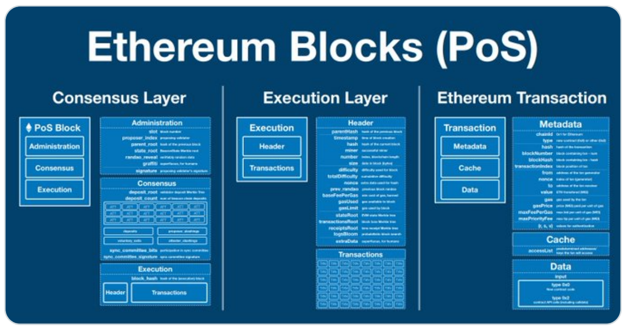
The consensus layer contains the entire execution layer (which previously was the entire PoW block).

Haym
@SalomonCrypto · **Follow**

(1/21) @ethereum Fundamentals: PoS Blocks

In less than 1 week, the Ethereum blockchain will Merge with the Beacon Chain and the World Computer will transition from PoW to PoS. The blockchain will never be the same.

A field-by-field guide to on-chain future.



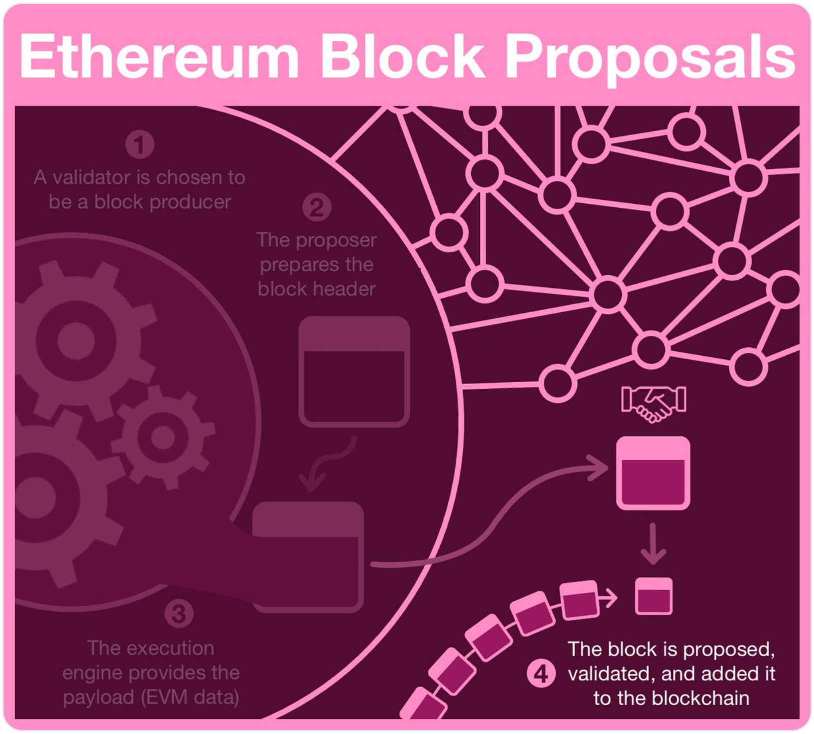
10:28 PM · Sep 9, 2022

Read the full conversation on Twitter

486 Reply Copy link

Read 36 replies

(16/25) Finally, the proposer finishes preparing the block and broadcasts it to the network. The vast majority of the time, the block will be perfectly valid and be readily accepted the rest of the @ethereum network.



(17/25) The network validates potential blocks and confirms them into the blockchain with a process called attestation.

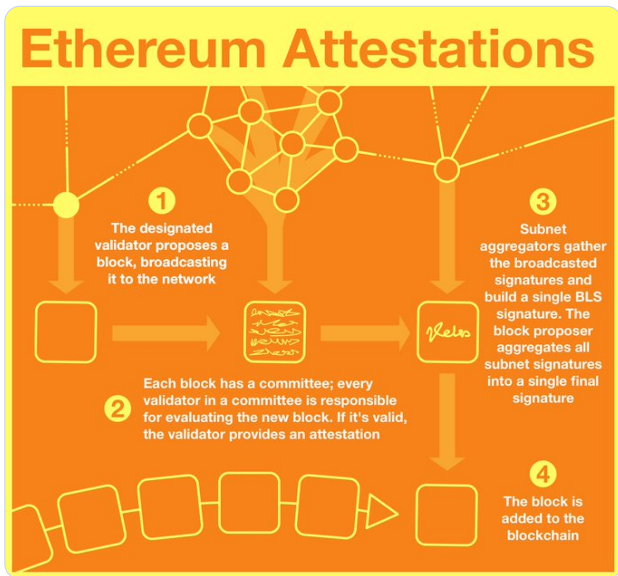
Tl;dr attestation is a formalized process of voting for blocks. Valid attestations are rewarded, invalid attestations are punished (via slashing).

Haym
@SalomonCrypto · Follow

(1/20) @ethereum Fundamentals: Attestation

Ethereum is made up of 1000s of computers, each contributing to its security by providing their Proof of Stake. But how does it actually work? How do 1000s of computers participate? What are they doing?

A guide to voting with $ETH.



12:17 AM · Oct 8, 2022

Read the full conversation on Twitter

315 Reply Copy link

Read 18 replies

(18/25) One of the key steps of attestation is aggregation, a process that combines thousands of digital signatures into a single, condensed piece of data.

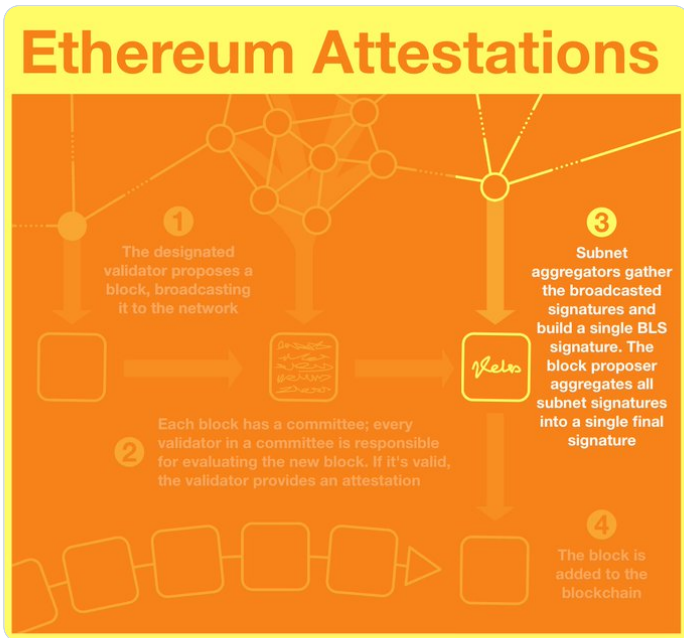
Attestation is tricky; it involves socializing and processing thousands of packets across a busy network.

Haym
@SalomonCrypto · **Follow**

Replying to @SalomonCrypto

(15/20) Validators broadcast their attestations to their assigned subnet, which consist of ~250 validators.

16 validators on each committee are designated as aggregators. They listen for attestations and begin bundling them into a BLS signature.



12:17 AM · Oct 8, 2022

8 Reply Copy link

Read 1 reply

(19/25) @ethereum alleviates this pressure in two ways:

- attestation is run redundantly; many different parties will be working on gathering as many signatures as possible.
- the network will accept aggregation up to a single epoch late (at reduced rewards)

(20/25) @ethereum is more secure with more signatures and it therefore incentivizes gathering as many signatures as possible. The protocol will pay out more $ETH for more signatures.

And so, the block proposer gathers as many signatures as possible and adds them to the block.

(21/25) Now you might be asking "if the block has been proposed, how does the producer add the attestations?"

Actually, they are included one block later. So if a block is proposed in slot N, the attestation for that blo will be attached to the block in slot N+1.

(22/25) In reality the attestation process happens when the proposer is creating the block header - it's just happening for the block that came before.

Regardless, if we zoom out just a little bit, we can consider the point moot. An attested block is part of the blockchain.

(23/25) Before we end, we'll briefly discuss one of the big changes in the @ethereum roadmap.

The problem: some validators are WAYYY better at building blocks than others.

Under PoS, some validators will earn more stake than the others, eventually capturing the network.

(24/25) The solution: Enshrined Proposer-Builder Separation (PBS)

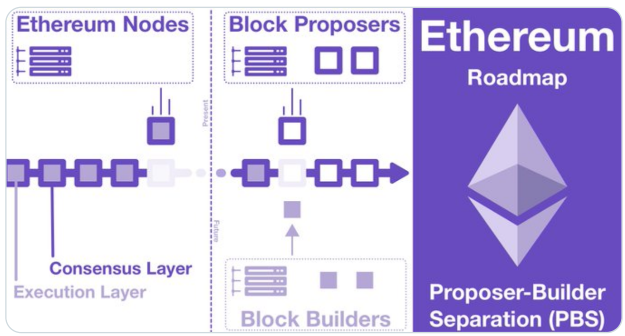
A future upgrade to the World Computer will reconfigure this process to separate building and proposing. Builders can be specialized, centralized entities that sell their blocks to the next block proposer.

Haym
@SalomonCrypto · **Follow**

(1/26) @ethereum Roadmap: Proposer-Builder Separation

The Merge was successful, $ETH is Proof of Stake! As the era of miners closes, we find ourselves entering a new meta: the age of MEV

Your guide to existential threat facing Ethereum... and the plan to vanquish it



11:38 PM · Sep 15, 2022

Read the full conversation on Twitter

516 Reply Copy link

Read 11 replies

(25/25) Today, we've crossed the fabled line: mainnet and the beacon chain have Merged and @ethereum is Proof of Stake; many parts of the World Computer are in their final state.

But not block proposing. The helm of this ship not only got a huge upgrade, but more is coming!

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

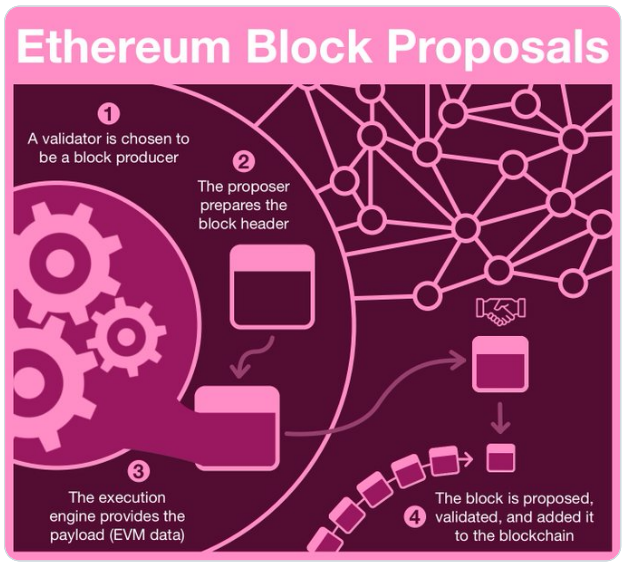
Follow me for more explainers and as much alpha as I can possibly serve.

Haym
@SalomonCrypto · **Follow**

(1/25) @ethereum Fundamentals: Block Proposals

Once every 12 seconds, a block is born. Have you ever thought about how a block is made? Or how it is accepted by the network and added to the blockchain?

Want to know how everything is going to change... again?



8:18 PM · Oct 8, 2022

Read the full conversation on Twitter

5 Reply Copy link

Read 2 replies

• • •