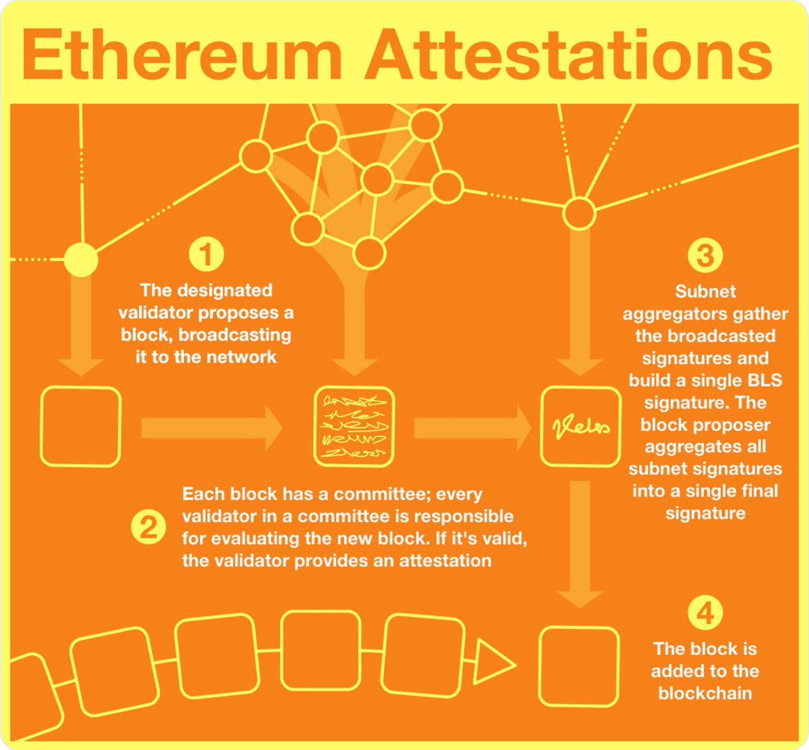
Haym @SalomonCrypto

Oct 8 • 21 tweets • SalomonCrypto/status/1578540111930699778

(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.



Ethereum Attestations

1 The designated validator proposes a block, broadcasting it to the network

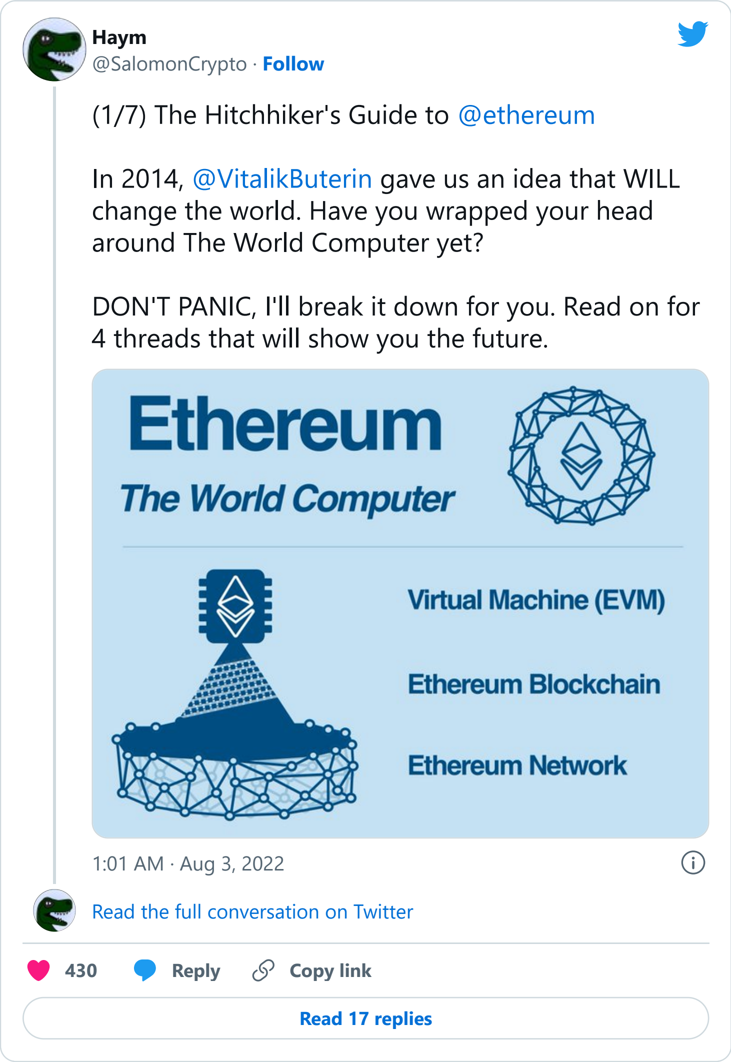
2 Each block has a committee; every validator in a committee is responsible for evaluating the new block. If it's valid, the validator provides an attestation

3 Subnet aggregators gather the broadcasted signatures and build a single BLS signature. The block proposer aggregates all subnet signatures into a single final signature

4 The block is added to the blockchain

(2/20) @ethereum is the World Computer, a globally shared platform that exists between a network of 1,000s of computers, 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?

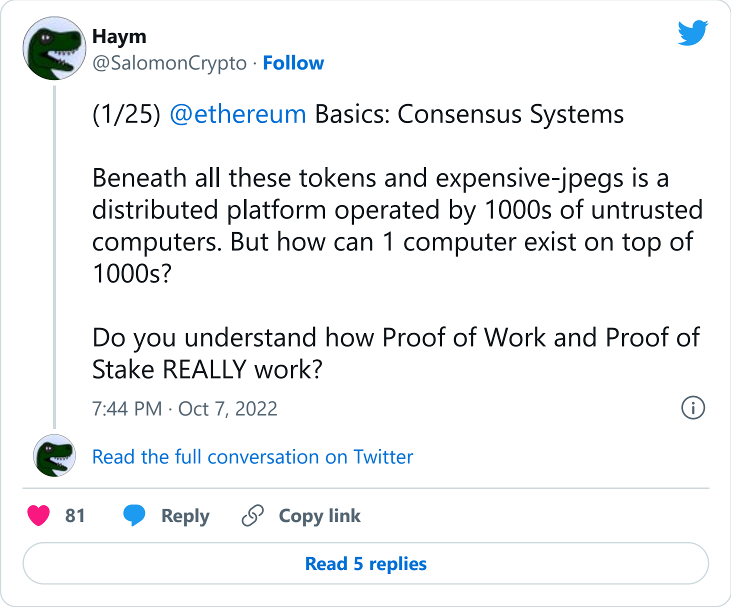
DON'T PANIC, I'll break it down for you. Read on for 4 threads that will show you the future.

1:01 AM · Aug 3, 2022

Read the full conversation on Twitter

(3/20) This distributed network of EVMs is held in sync via a consensus mechanism.

A consensus mechanism is a system by which a leader (block proposer) updates the state of their EVM and the rest of the network trustlessly follows.



Haym
@SalomonCrypto

(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?

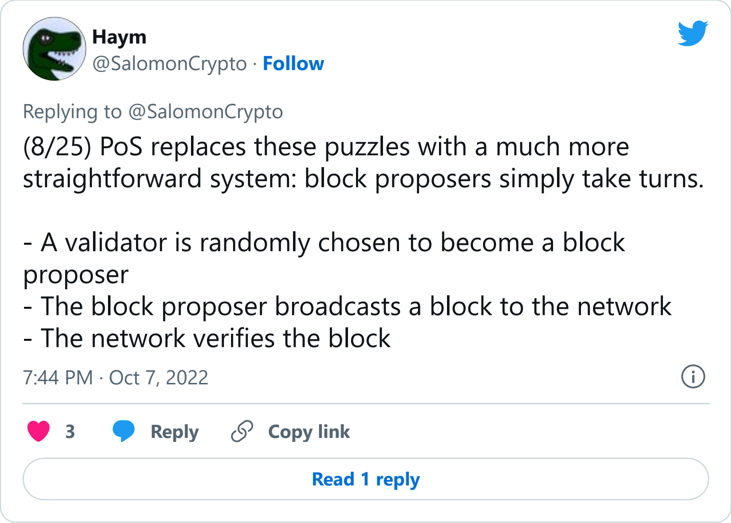
7:44 PM · Oct 7, 2022

Read the full conversation on Twitter

(4/20) Today, @ethereum uses Proof of Stake (PoS).

PoS randomly selects a block proposer, who gets to construct the next block. The rest of the network validates these blocks, voting them into the blockchain.

In order to participate, you must put $ETH at stake.



Haym
@SalomonCrypto

Replying to @SalomonCrypto

(8/25) PoS replaces these puzzles with a much more straightforward system: block proposers simply take turns.

- A validator is randomly chosen to become a block proposer
- The block proposer broadcasts a block to the network
- The network verifies the block

7:44 PM · Oct 7, 2022

(5/20) By putting $ETH at stake, network participants (validators) are placing their capital at risk for slashing - the punishment the network applies to malfunctioning (intentional or not) validators.

This is the mechanism by which the $ETH stake projects economic security.

(6/20) Most obviously, this dynamic applies to the block proposer; if they submit an invalid block, the network will consider them a malicious actor and remove them from the network.

But this also applies to the next step - the validation of the block by the rest of the network.

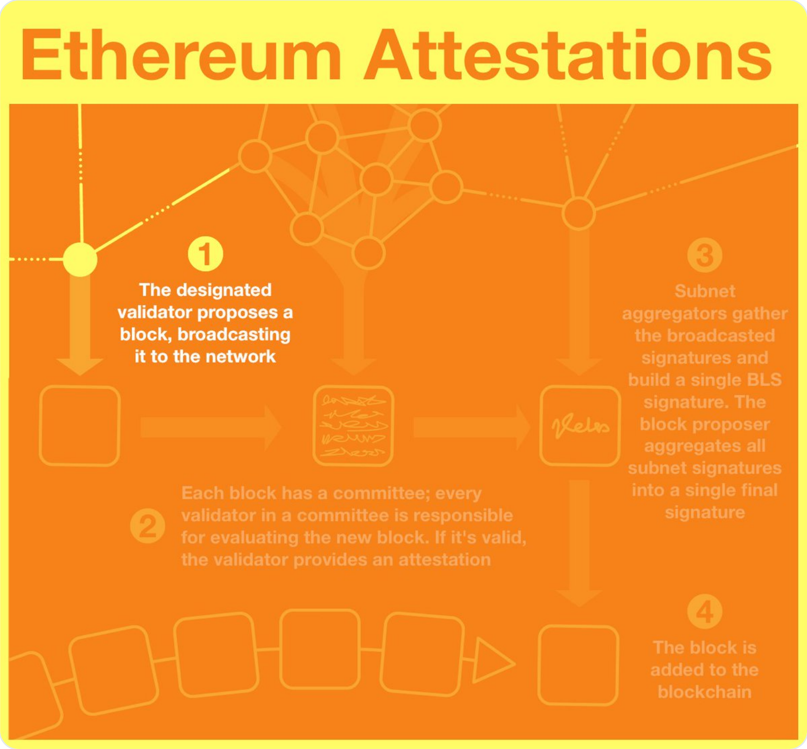
(7/20) The block producer sends out a block; validators evaluate it and if it is valid, they broadcast an attestation.

If a validator attests to an invalid block, the network considers them just as hostile as an invalid block proposer.

Attestations are core to $ETH security.

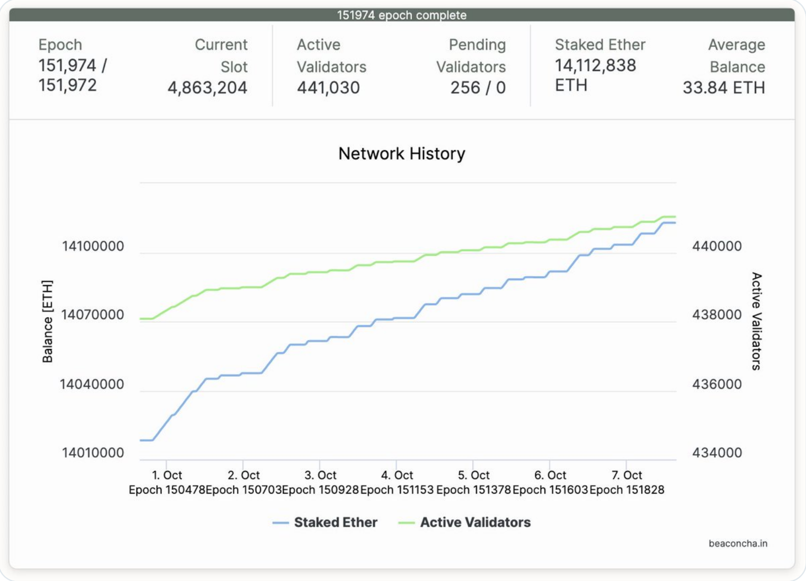
(8/20) Alright, we've finally made it. Now that we understand how attestations fit in to the World Computer, we can finally dig in: what is an attestation?

It starts with a block, broadcast to the network.


Ethereum Attestations
1
The designated validator proposes a block, broadcasting it to the network
2
Each block has a committee; every validator in a committee is responsible for evaluating the new block. If it's valid, the validator provides an attestation
3
Subnet aggregators gather the broadcasted signatures and build a single BLS signature. The block proposer aggregates all subnet signatures into a single final signature
4
The block is added to the blockchain

(9/20) Sending the block to a few (or even 1,000) validators is no problem, but once you start getting passed 10K, the chatter requirements become so huge that no credibly decentralized network could handle it.

Currently there are about 440k @ethereum validators.



151974 epoch complete

Epoch	Current Slot	Active Validators	Pending Validators	Staked Ether	Average Balance
151,974 / 151,972	4,863,204	441,030	256 / 0	14,112,838 ETH	33.84 ETH

(10/20) An @ethereum where every validator validates every block is not realistic. Instead, we have a different goal: every validator will validate every epoch.

One epoch = 32 blocks = 6.4 minutes.

Once every 6.4 minutes every validator will vote on the canonical blockchain.

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

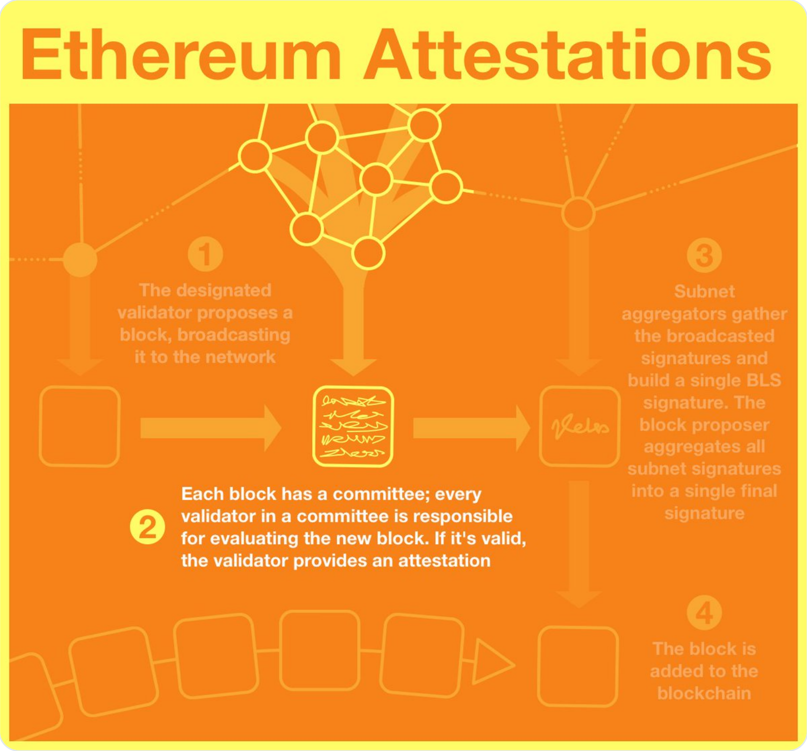
Read the full conversation on Twitter

♥ 517 Reply Copy link

Read 20 replies

(11/20) At the beginning of every epoch (once every 32 blocks), the entire validator set is randomly shuffled into 32 groups called committees.

The block proposer sends every validator a copy of the block, but only its committee members need to attest.


Ethereum Attestations
1
The designated validator proposes a block, broadcasting it to the network
2
Each block has a committee; every validator in a committee is responsible for evaluating the new block. If it's valid, the validator provides an attestation
3
Subnet aggregators gather the broadcasted signatures and build a single BLS signature. The block proposer aggregates all subnet signatures into a single final signature
4
The block is added to the blockchain

(12/20) Zooming in, an attestation is really a BLS signature wrapped in some identifying metadata

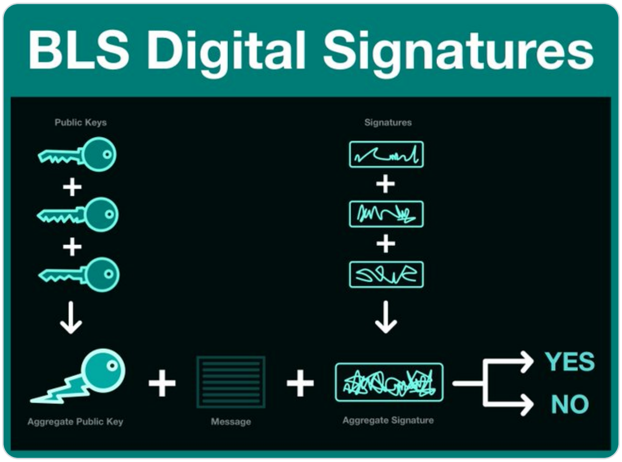
A BLS signature is a type of digital signature that maintains all the properties of a normal digital signature but with a special property: multiple keys/messages can be aggregated

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

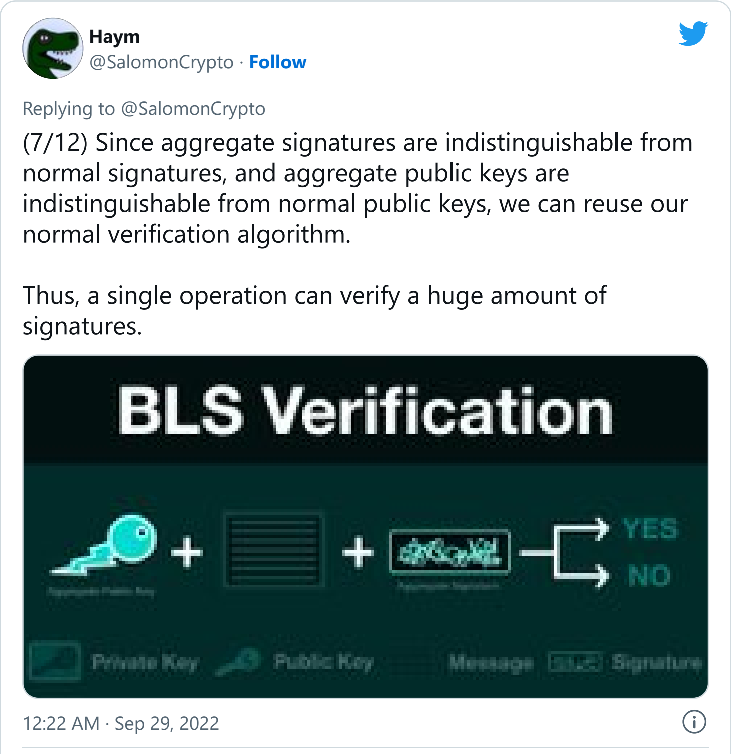
Read the full conversation on Twitter

158 Reply Copy link

Read 8 replies

(13/20) The magic of BLS signatures is that at the data level, an aggregate signature is the exact same thing as a single signature.

Thus, a BLS signature can store (and verify) a HUGE amount of signatures in a very efficient manner.



Haym
@SalomonCrypto · **Follow**

Replying to @SalomonCrypto

(7/12) Since aggregate signatures are indistinguishable from normal signatures, and aggregate public keys are indistinguishable from normal public keys, we can reuse our normal verification algorithm.

Thus, a single operation can verify a huge amount of signatures.

12:22 AM · Sep 29, 2022

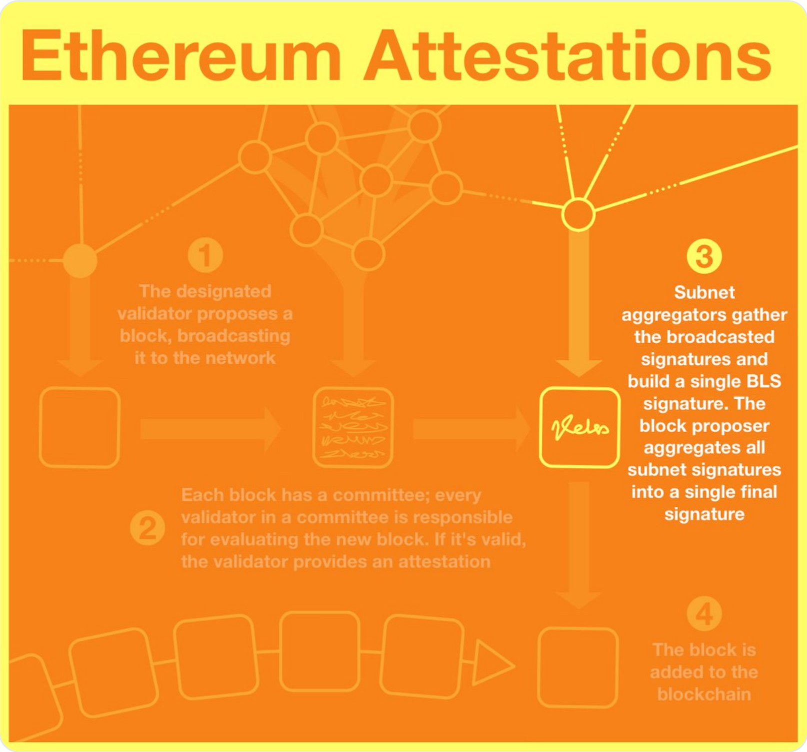
(14/20) If there are 440k validators and 32 committees, there must be ~14k validators/committee.

14k validators still poses a problem; it's both too much network chatter and too many signatures to aggregate all at once.

And so, we split one more time. 1 committee = 64 subnets.

(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.



Ethereum Attestations

1 The designated validator proposes a block, broadcasting it to the network

2 Each block has a committee; every validator in a committee is responsible for evaluating the new block. If it's valid, the validator provides an attestation

3 Subnet aggregators gather the broadcasted signatures and build a single BLS signature. The block proposer aggregates all subnet signatures into a single final signature

4 The block is added to the blockchain

(16/20) All 16 are attempting to build the same aggregate signature containing all the subnet's validators, but network conditions can cause some aggregators to miss a few attestations. There's only so much you can do. 🤷‍♂️

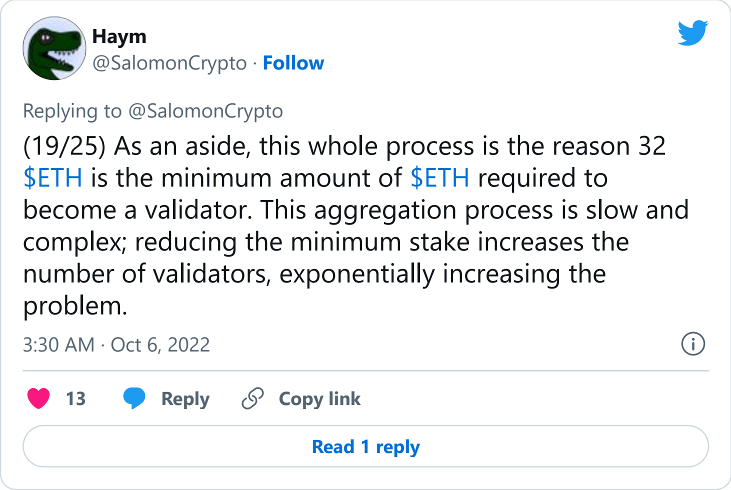
Each validator does their best and publishes the result.

(17/20) At this point, the ball moves back to the block producer's court. The validator who proposed the node begins to go subnet by subnet and selects the best aggregate signature.

Once the 64 best signatures are gathered, the block proposer aggregates them one last time.

(18/20) This final aggregation is then added on to the block, signifying that all 14k validators in that committee saw that block and agreed with it - on threat of slashing.

Incidentally this process limits the number of validators the network can support.



Haym
@SalomonCrypto · Follow

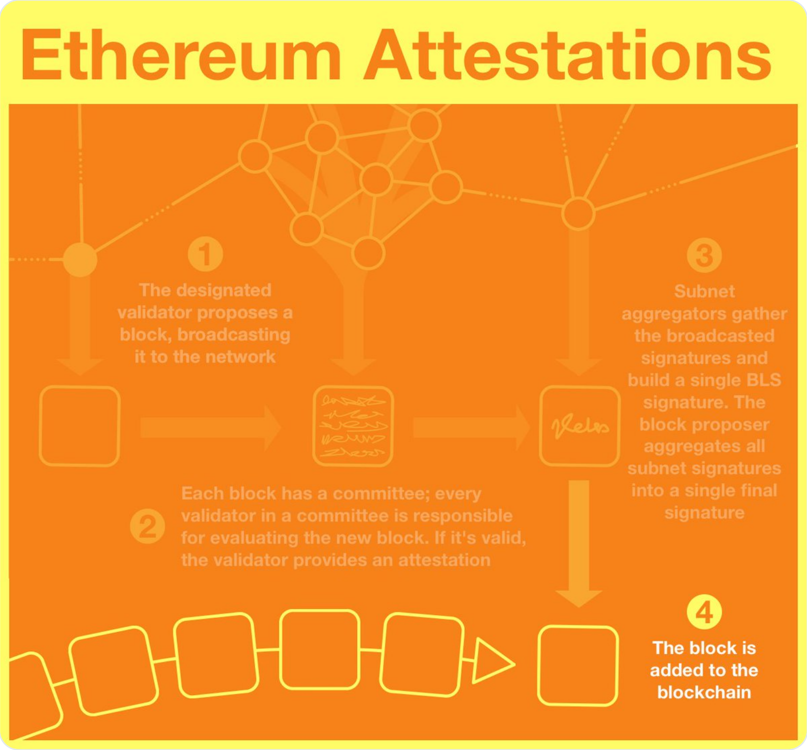
Replying to @SalomonCrypto

(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.

3:30 AM · Oct 6, 2022

(19/20) At this point we have a valid block, attested to by its entire committee and carefully prepared to allow quick verification. And so, it's time to add it to the blockchain...

In fact, by virtue of this process, it WAS added to the blockchain.



Ethereum Attestations

1 The designated validator proposes a block, broadcasting it to the network

2 Each block has a committee; every validator in a committee is responsible for evaluating the new block. If it's valid, the validator provides an attestation

3 Subnet aggregators gather the broadcasted signatures and build a single BLS signature. The block proposer aggregates all subnet signatures into a single final signature

4 The block is added to the blockchain

(20/20) Every time a block is proposed, 1/32 of the network places their stake on the line and votes.

Every 32 blocks, the entire network participates.

And so, once every epoch, @ethereum becomes secured by the entire value of all staked $ETH.

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

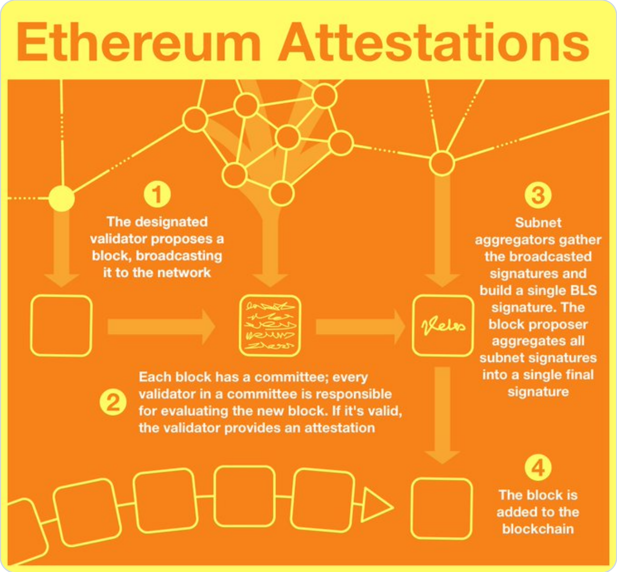
Follow me for more explainers and as much alpha as I can possibly serve.

Haym
@SalomonCrypto · **Follow**

(1/20) @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.



Ethereum Attestations

1 The designated validator proposes a block, broadcasting it to the network

2 Each block has a committee; every validator in a committee is responsible for evaluating the new block. If it's valid, the validator provides an attestation

3 Subnet aggregators gather the broadcasted signatures and build a single BLS signature. The block proposer aggregates all subnet signatures into a single final signature

4 The block is added to the blockchain

12:17 AM · Oct 8, 2022

Read the full conversation on Twitter

6 Reply Copy link

Read 1 reply

• • •