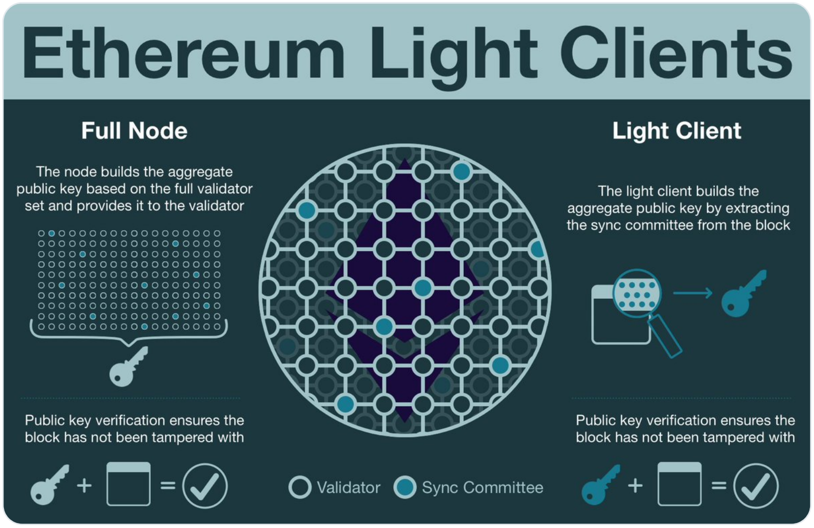
Haym @SalomonCrypto
Oct 10 • 26 tweets • SalomonCrypto/status/1579283196708941824

(1/25) @ethereum Fundamentals: Sync Committees and Light Clients

Just about one year ago, the Altair upgrade gave validators a new duty: sync committee. Learn how this core consensus feature enables the end game:

A truly decentralized World Computer



Ethereum Light Clients

Full Node

The node builds the aggregate public key based on the full validator set and provides it to the validator

Public key verification ensures the block has not been tampered with

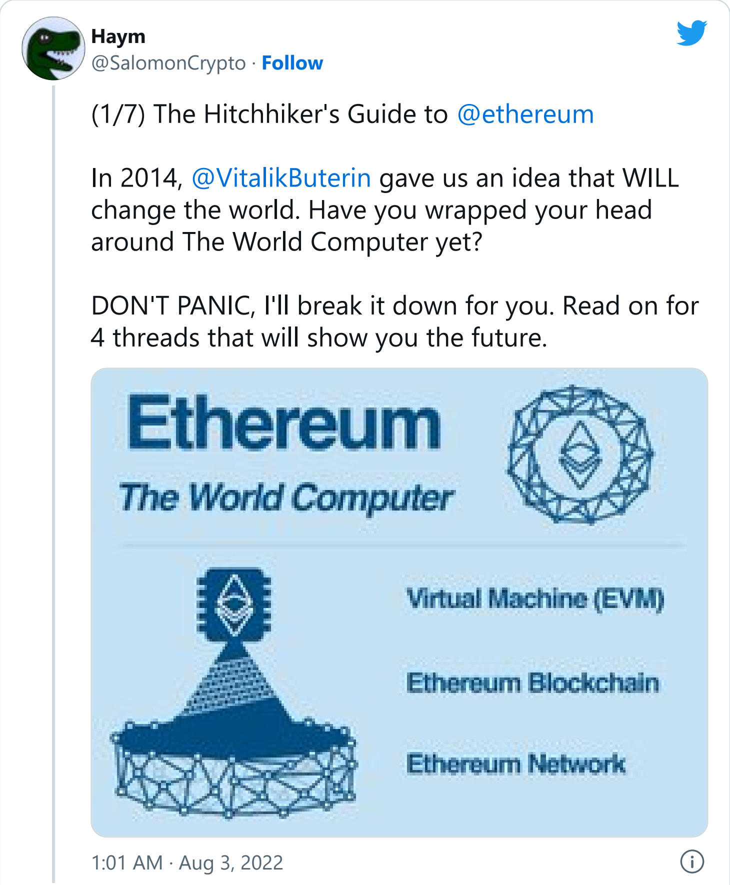
Light Client

The light client builds the aggregate public key by extracting the sync committee from the block

Public key verification ensures the block has not been tampered with

(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

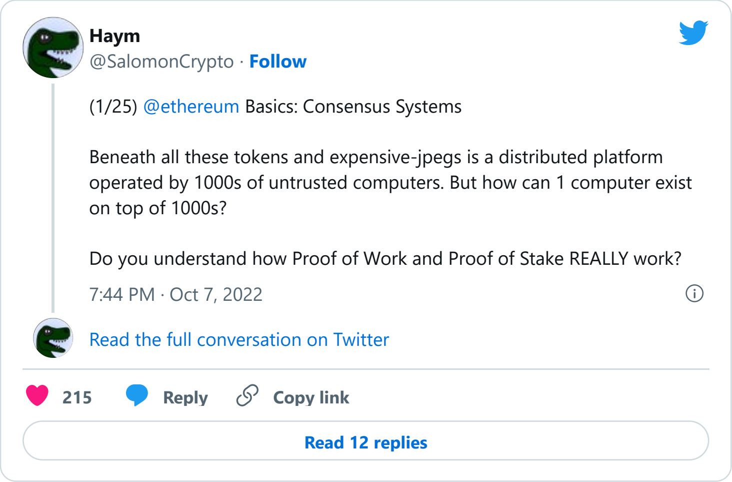
In 2014, @VitalikButerin gave us an idea that WILL change the world. Have you wrapped your head around The World Computer yet?

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

(3/25) The network's EVMs stay in sync through a consensus mechanism: the protocols/algorithms/incentives that allow the network of nodes to agree on the state of the EVM.

At birth, @ethereum used Proof of Work; as of last month it has switched to 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?

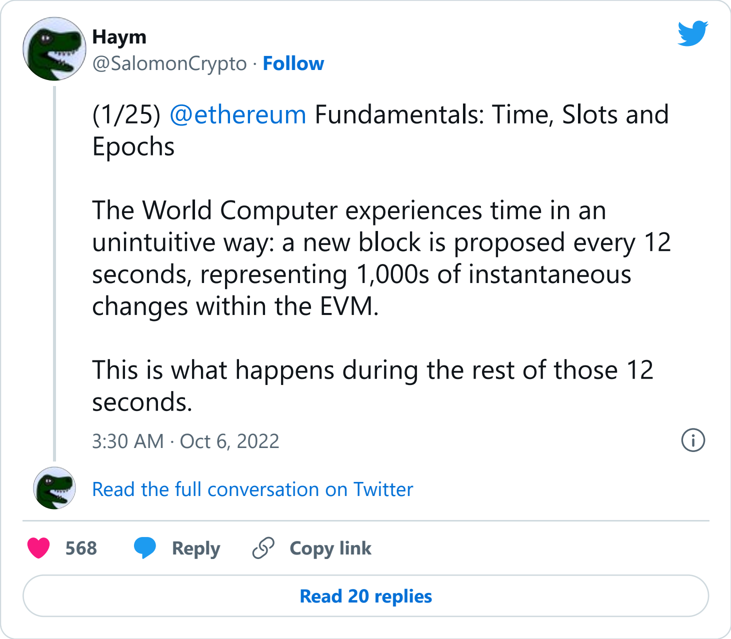
7:44 PM · Oct 7, 2022

Read the full conversation on Twitter

(4/25) @ethereum's PoS implementation is... complicated. We'll try to summarize it in just a few tweets so we can get to the good part.

First, we need to learn about time on the World Computer.

- A block goes in a slot
- 1 slot = 12 seconds
- 32 slots = 1 epoch = 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

(5/25) Every epoch, @ethereum shuffles the validator set into 32 committees (one per slot) and each committee into 64 subnets.

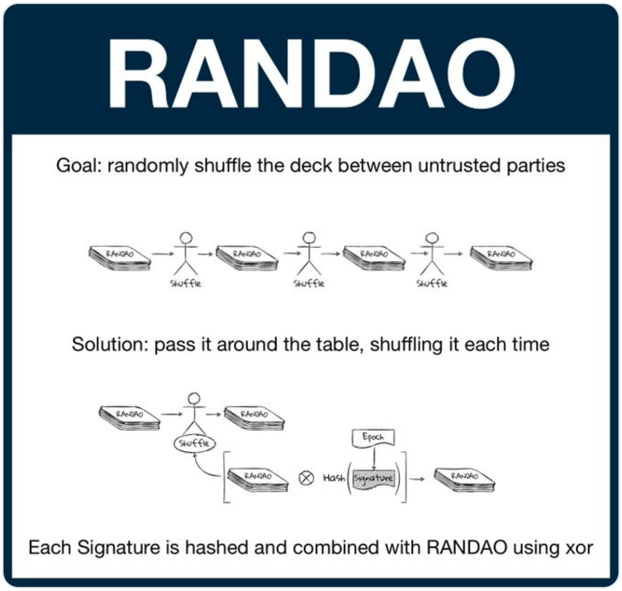
The process known as RANDAO provides credible randomness for this shuffling, critical to the protocol's security.

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

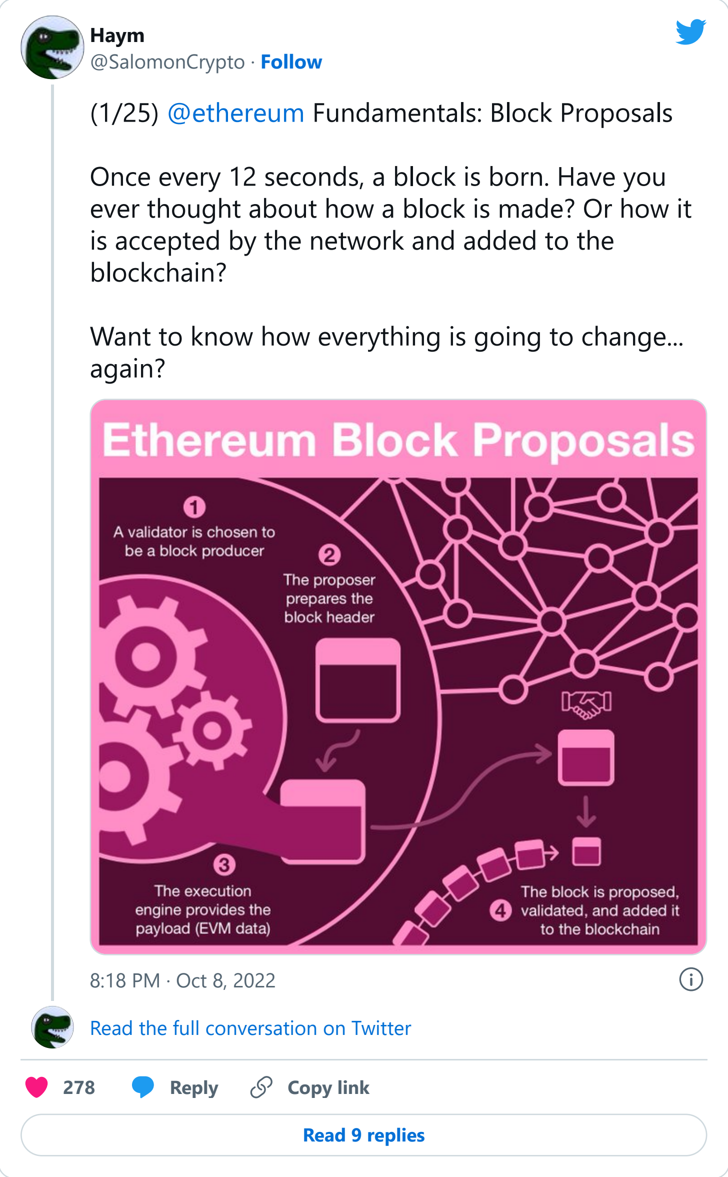
Read the full conversation on Twitter

215 Reply Copy link

Read 8 replies

(6/25) The first member of each committee is designated the block proposer. The proposer is responsible for building (or otherwise sourcing) a block and broadcasting it to the network.

Each block progresses the state of the EVM and adds to the blockchain.



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?

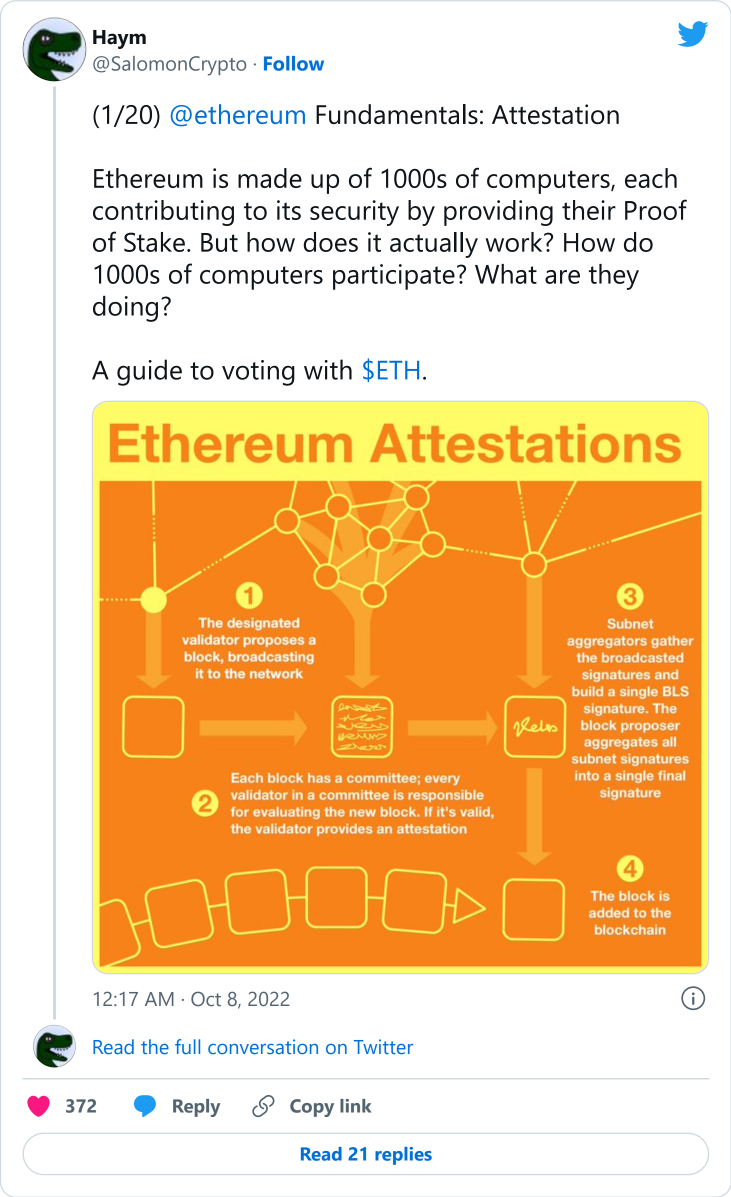
Ethereum Block Proposals
1 A validator is chosen to be a block producer
2 The proposer prepares the block header
3 The execution engine provides the payload (EVM data)
4 The block is proposed, validated, and added it to the blockchain

8:18 PM · Oct 8, 2022

Read the full conversation on Twitter
278
Reply
Copy link
Read 9 replies

(7/25) Each validator in the committee is responsible for verifying the block. Assuming the block is valid, each committee member creates and publishes a cryptographic signature.

These signatures are aggregated and added to the (next) block header, completing the process.



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

(8/25) Every epoch, the validator set is split into 32 committees, each responsible for attesting to one block.

Thus, every epoch every validator submits a signature that represents their personal guarantee the block is valid and part of the blockchain.

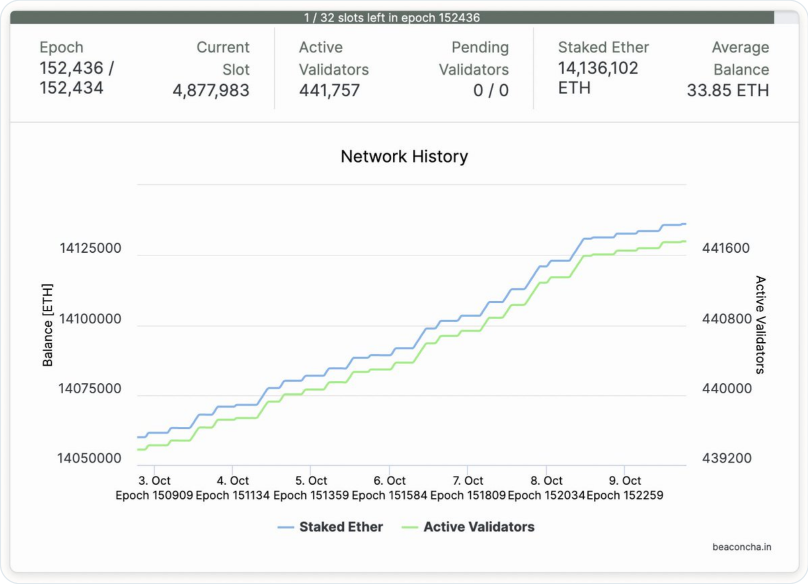
(9/25) PoS is predicated on these cryptographic signatures; economic security is derived from the fact that each attesting validator can be slashed.

Without the signatures (and the ability to verify them), the whole system just becomes "trust the data in the block."

(10/25) Alright, we've gotten through the idea; now let's look at the reality.

Right now there are ~442k validators, each submitting an attestation (digital signature) once every 6.4 minutes.

~442k signatures is a lot of signatures.

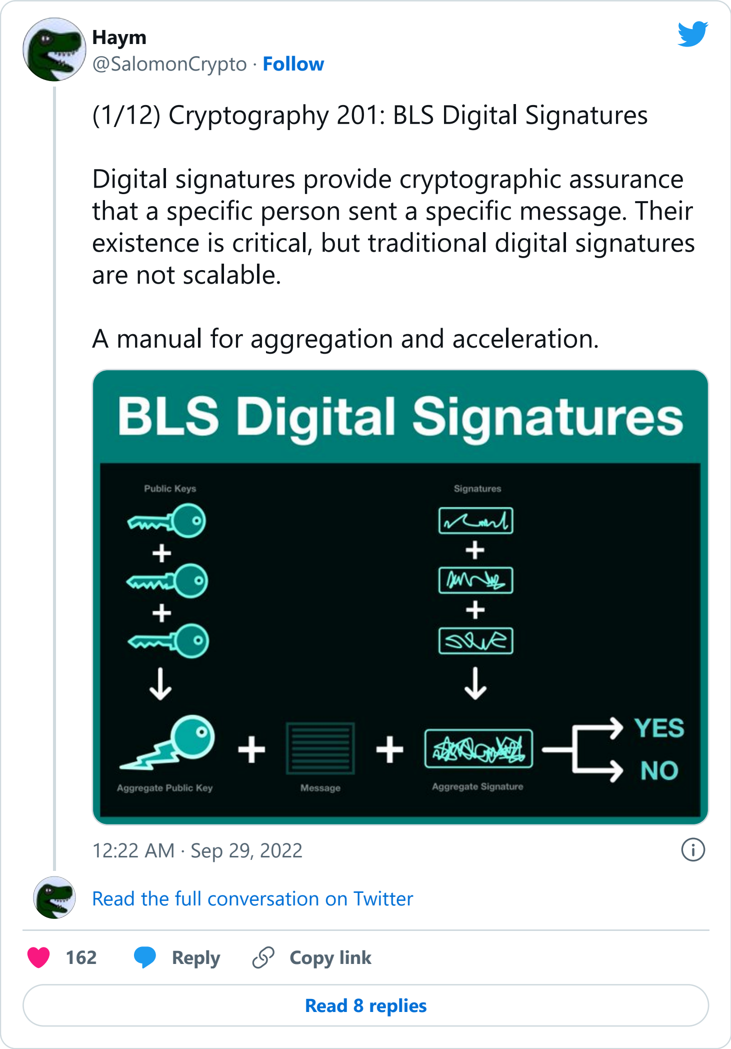


1 / 32 slots left in epoch 152436

Epoch	Current Slot	Active Validators	Pending Validators	Staked Ether	Average Balance
152,436 / 152,434	4,877,983	441,757	0 / 0	14,136,102 ETH	33.85 ETH

(11/25) The most apparent problems in dealing with half a million signatures is the time needed to process that many and/or the space required to store that many

Fortunately, both of these problems are gracefully solved by BLS signatures, which allow signatures to 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

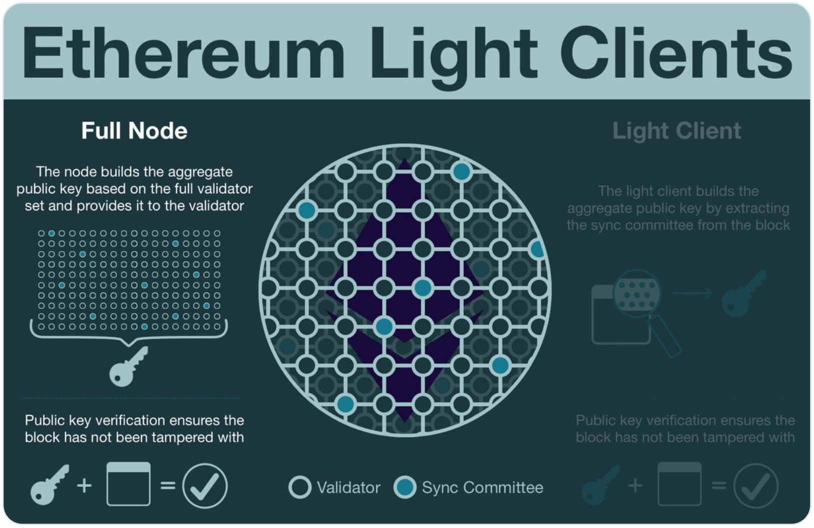
(12/25) Tl;dr BLS signatures allow you to verify a huge amount of signatures with the same operation as a single signature.

But in order to create the (public) key needed to verify the message, you need access to the underlying individual public keys.

(13/25) When a block proposer is preparing the block, they add the aggregate signature to the block header, but they do not add the aggregate key.

The whole point is to build the aggregate key independently. Else, what's the point of verification?

(14/25) For an @ethereum node, this is no problem. Part of the responsibilities of running a node (and therefore running validators) is to hold the validator set in accessible memory and quickly compute aggregate signatures.



Ethereum Light Clients

Full Node

The node builds the aggregate public key based on the full validator set and provides it to the validator

Public key verification ensures the block has not been tampered with

Light Client

The light client builds the aggregate public key by extracting the sync committee from the block

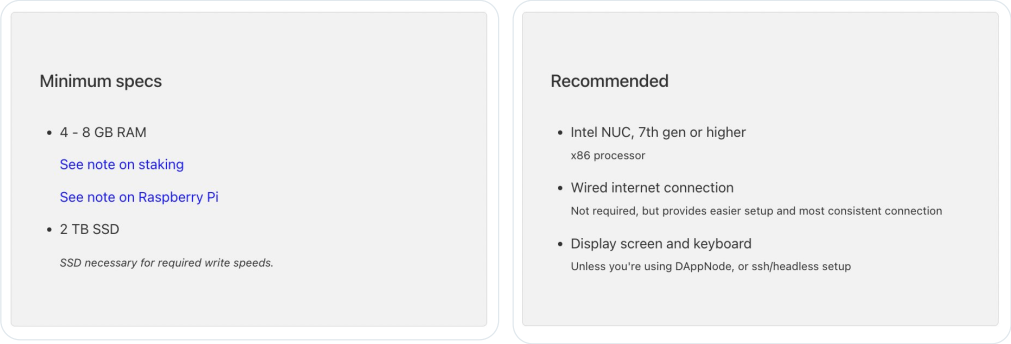
Public key verification ensures the block has not been tampered with

(15/25) One of the core design philosophies is that a full @ethereum node has (relatively) low requirements. This is the cornerstone of the World Computer's decentralization and credible neutrality.

And, generally speaking, Ethereum has knocked it out of the park!

(16/25) Today, a relatively modest current (dedicated) computer will do the job. As time passes, the cost for a minimum-spec @ethereum node will drop further and further.

And yet, there are certain types of computers that will never be suitable... very useful types of computers.



Minimum specs

- 4 - 8 GB RAM

  See note on staking

  See note on Raspberry Pi
- 2 TB SSD

  SSD necessary for required write speeds.

Recommended

- Intel NUC, 7th gen or higher

  x86 processor
- Wired internet connection

  Not required, but provides easier setup and most consistent connection
- Display screen and keyboard

  Unless you're using DAppNode, or ssh/headless setup

(17/25) What about a computer with ridiculously low specs, maybe in a developing economy?

What about a smartphone, with more than enough processing power but unreliable connectivity?

What about within an application, like an in-browser wallet (imagine if MM didn't need Infura)?

(18/25) @ethereum is the World Computer; all (well, most) blockchains are decentralized computers...

What about running a node within a smart contract on another blockchain?

(19/25) While running a full node might never be realistic in the examples above, running a light client very well might be.

And so, in October 2021 the beacon chain received its first upgrade in preparation for light client support: Altair.

The Ethereum Altair Upgrade Is Next Week. Here's What's in It - Decrypt

Altair may be the only update for the beacon chain before it merges with the current Ethereum proof-of-work blockchain.

https://decrypt.co/84176/ethereum-altair-upgrade-next-week-heres-whats-in-it

(20/25) Among other things, the Altair upgrade added Sync Committees to the @ethereum PoS specification.

A sync committee is a group of 512 validators, chosen every 256 epochs (~27 hours), who continually signs block headers for every slot in the beacon chain.

(21/25) Every time a block is produced, each member of the sync committee will verify and, if valid, sign it. These signatures are broadcast back out to the network.

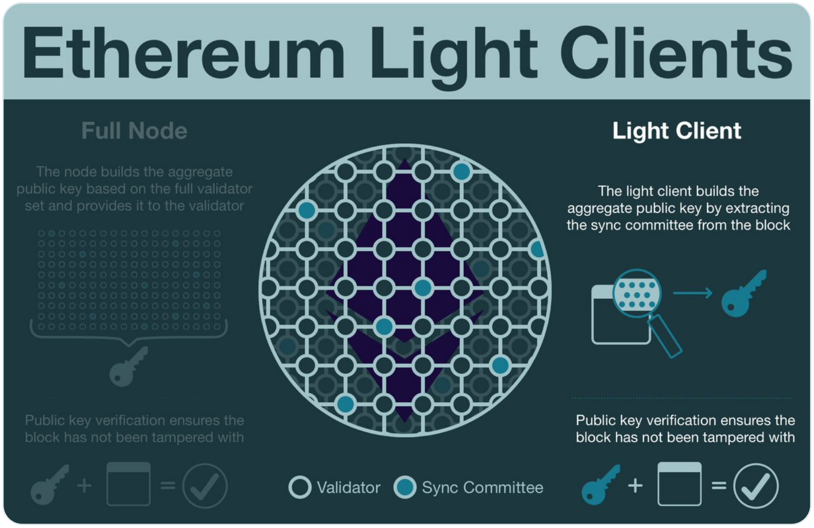
Then, the next slot begins and a new proposer is selected. This new proposer listens for these signatures.

(22/25) The block producer collects all the signatures that match their view of their chain and aggregates them into a final sync committee signature.

Then the producer adds the signature AND the sync committee's public keys (quickly verifiable) directly into the block header.

(23/25) Sync committees only contain 512 validators; a tiny amount both in terms of data storage and aggregate key generation.

This allows a light client to build (from scratch) the aggregate public key it needs to trustlessly verify the signature and therefore whole blockchain.


Ethereum Light Clients
Full Node
The node builds the aggregate public key based on the full validator set and provides it to the validator
Public key verification ensures the block has not been tampered with
+
=
Light Client
The light client builds the aggregate public key by extracting the sync committee from the block
Public key verification ensures the block has not been tampered with
+
=
○ Validator
● Sync Committee

(24/25) Today, we don't have fully functioning light clients. Altair upgraded @ethereum at the protocol level and created the necessary surface area needed to support light clients, but we still need to fill in the rest of the pieces

Most important: Merkle proof production.

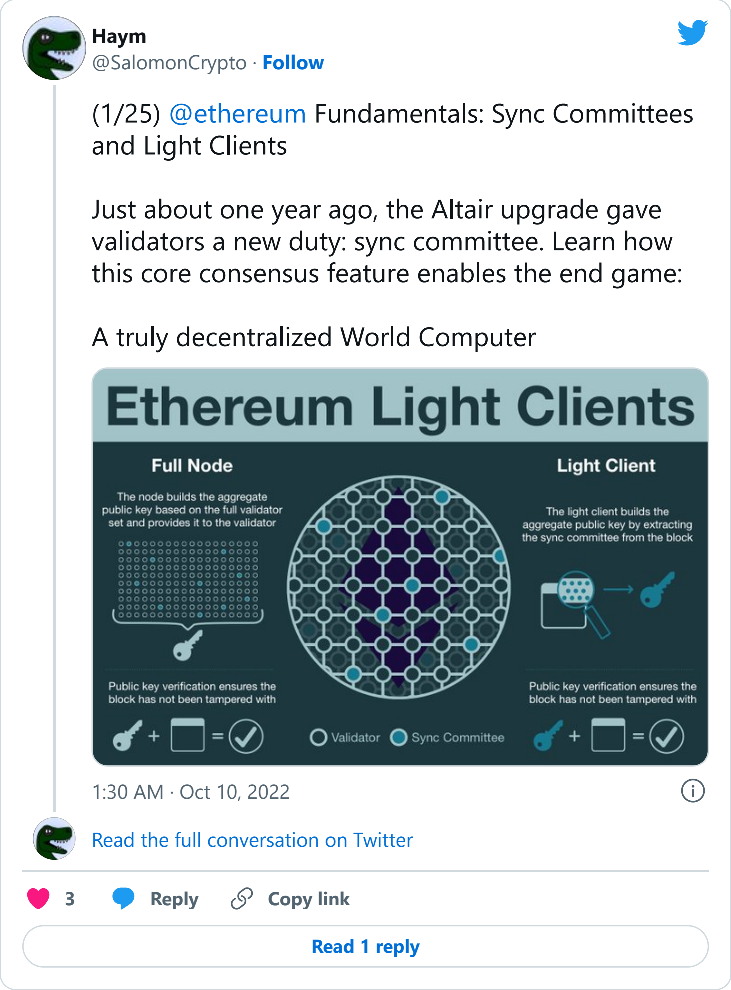
(25/25) What we DO have today is an @ethereum ready to support light clients; we just need to build the tech.

When that day comes, we'll have an Ethereum that welcomes all computers as potential nodes - even other blockchain computers.

A truly decentralized World Computer.

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: Sync Committees and Light Clients

Just about one year ago, the Altair upgrade gave validators a new duty: sync committee. Learn how this core consensus feature enables the end game:

A truly decentralized World Computer

Ethereum Light Clients

Full Node

The node builds the aggregate public key based on the full validator set and provides it to the validator

Public key verification ensures the block has not been tampered with

Light Client

The light client builds the aggregate public key by extracting the sync committee from the block

Public key verification ensures the block has not been tampered with

○ Validator ● Sync Committee

1:30 AM · Oct 10, 2022

Read the full conversation on Twitter

• • •