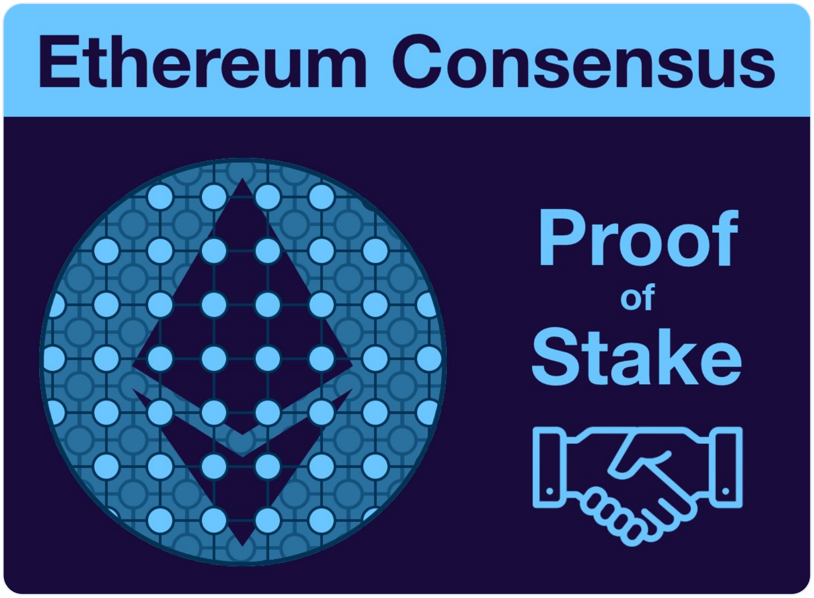
Haym @SalomonCrypto

Oct 10 • 30 tweets • SalomonCrypto/status/1579594609855934465

(1/29) @ethereum Fundamentals: Proof of Stake

We are post-Merge; Ethereum is now secured by validators, 32 $ETH at a time. At first glance, PoS is simple, but under the hood things get complicated.

The ultimate guide to the consensus mechanism at the core of the World Computer.



(2/29) @ethereum is the World Computer, a single, globally shared computing platform that exists in the space between a network of 1,000s of computers (nodes).

Haym
@SalomonCrypto · **Follow**

(1/21) @ethereum: The Big Picture

From 1492 to 2022, the context, technology and vision of the World Computer. The complete, top-to-bottom case for $ETH.

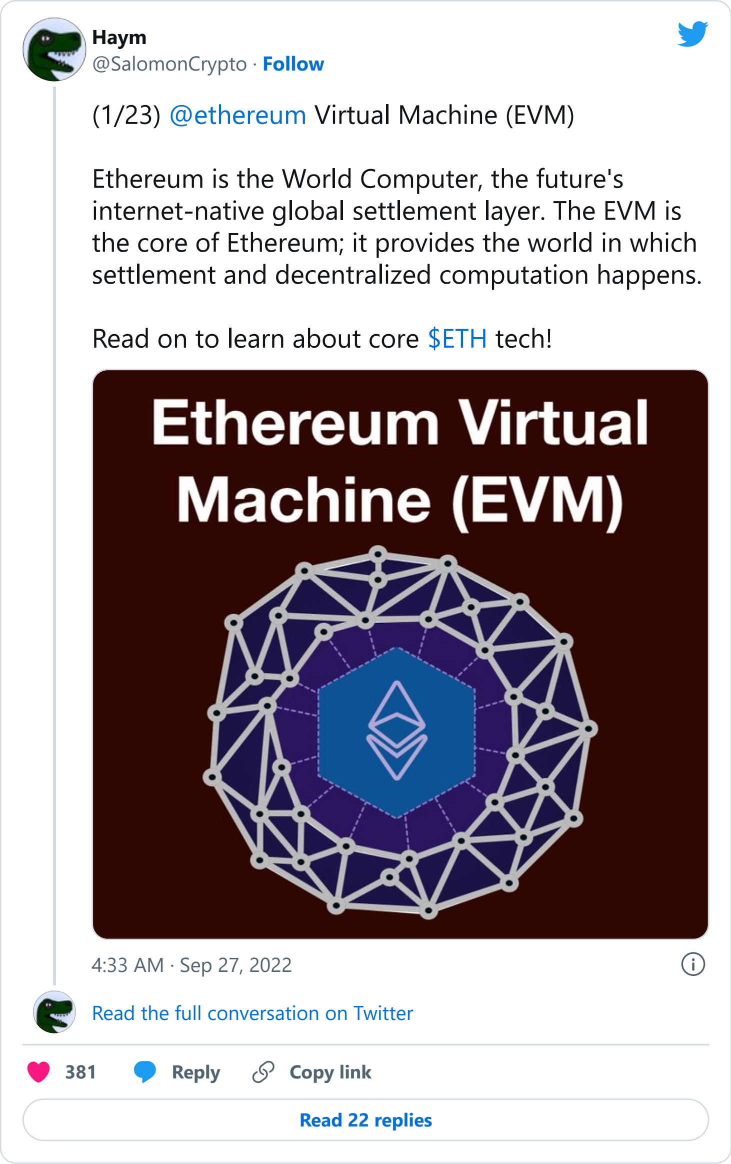
An (unprecedented) mega-thread.

3:00 PM · Sep 3, 2022

Read the full conversation on Twitter

(3/29) Each node runs a local copy of the @ethereum Virtual Machine (EVM), a Turing-complete environment that computes the state of the World Computer

Although each node's copy is independent, every EVM is sync; the state of any local copy IS the state of the globally shared EVM



Haym
@SalomonCrypto · Follow

(1/23) @ethereum Virtual Machine (EVM)

Ethereum is the World Computer, the future's internet-native global settlement layer. The EVM is the core of Ethereum; it provides the world in which settlement and decentralized computation happens.

Read on to learn about core $ETH tech!

Ethereum Virtual Machine (EVM)

4:33 AM · Sep 27, 2022

Read the full conversation on Twitter
381
Reply
Copy link
Read 22 replies

(4/29) Coordination is achieved via a leader-follower dynamic. Once per [cycle], a new leader updates their copy of the EVM.

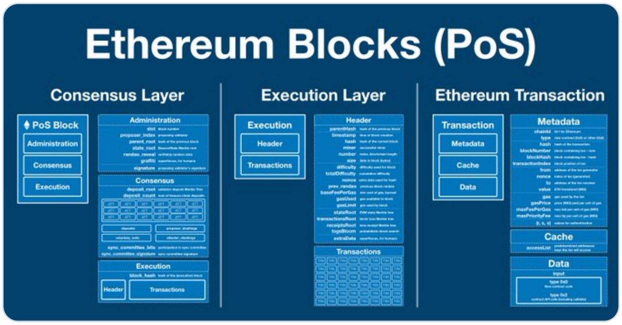
The leader (block producer) then packages all these changes into a block; the rest of the network uses the block to sync their EVM with the proposer's.

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

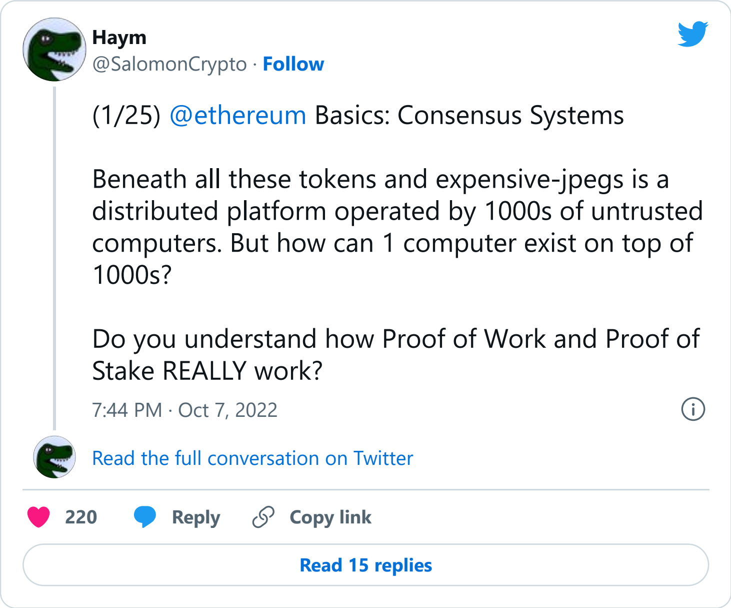
Read the full conversation on Twitter

489 Reply Copy link

Read 38 replies

(5/29) Coordinating blocks between thousands of computers is not trivial; we need a consensus mechanism.

Until Sept 2022, the World Computer relied on Proof of Work (PoW) to achieve consensus. But just last month The Merge finally came; Ethereum is 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

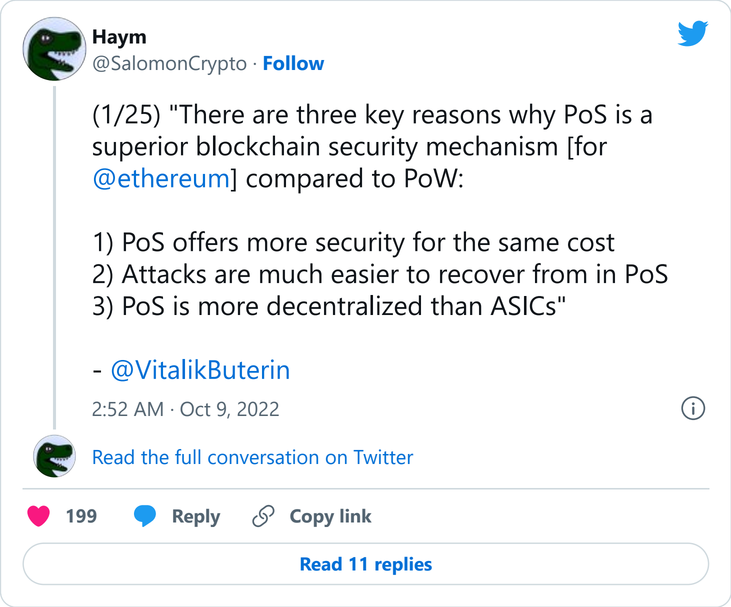
♥ 220 Reply Copy link

Read 15 replies

(6/29) Before we dive in, let me just address the unasked question: "Was the switch to PoS a good thing for @ethereum?"

The answer is an unhesitating, emphatic YES!

But don't take my word for it, better men than I have already explained why:



Haym
@SalomonCrypto · **Follow**

(1/25) "There are three key reasons why PoS is a superior blockchain security mechanism [for @ethereum] compared to PoW:

1) PoS offers more security for the same cost
2) Attacks are much easier to recover from in PoS
3) PoS is more decentralized than ASICs"

- @VitalikButerin

2:52 AM · Oct 9, 2022

Read the full conversation on Twitter

♥ 199 Reply Copy link

Read 11 replies

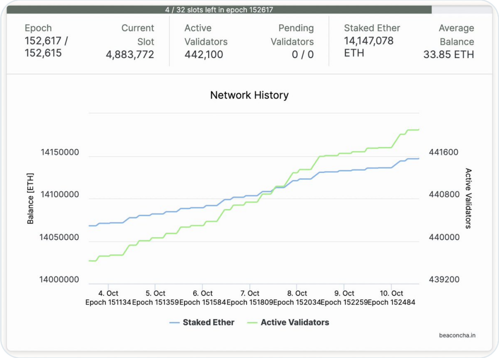
(7/29) Those who participate in PoS are making an explicit agreement: "I will be an honest, good faith participant. To ensure good behavior I will put capital at stake."

Those who make this promise are called validators. A validator must deposit exactly 32 $ETH.

(8/29) Quick vocabulary note: A node is a real-world computer; a validator stakes 32 $ETH and has responsibilities to operate and secure the network.

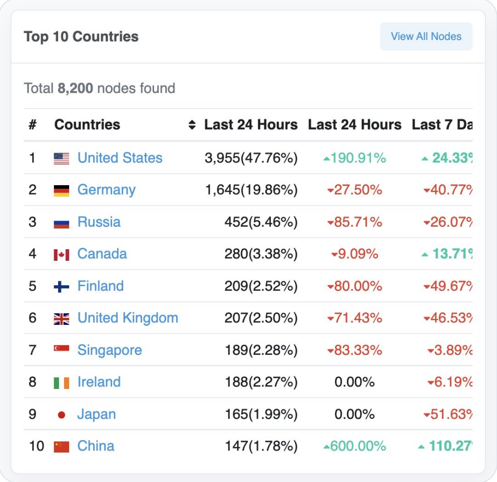
A node runs validator software and a single node can run many validators.

There are currently 8k nodes and ~440k validators.



4 / 32 slots left in epoch 152617

Epoch	Current Slot	Active Validators	Pending Validators	Staked Ether	Average Balance
152,617 / 152,615	4,883,772	442,100	0 / 0	14,147,078 ETH	33.85 ETH

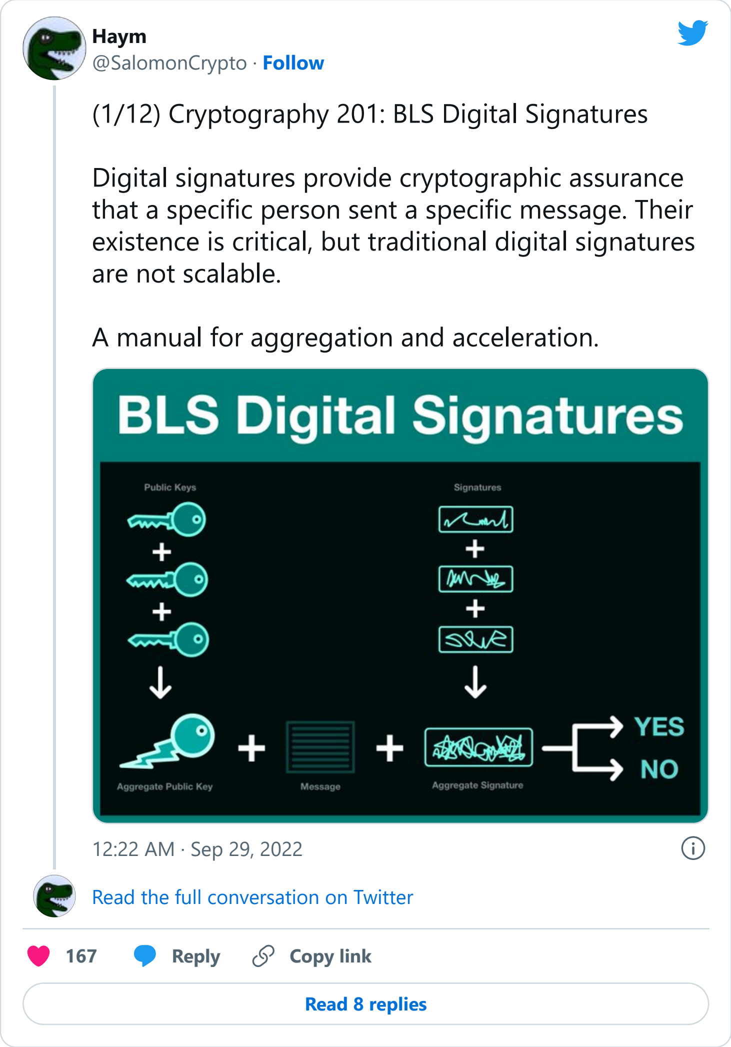


Total **8,200** nodes found

#	Countries	Last 24 Hours	Last 24 Hours	Last 7 Da
1	United States	3,955(47.76%)	▲190.91%	▲ 24.33
2	Germany	1,645(19.86%)	▼27.50%	▼40.77
3	Russia	452(5.46%)	▼85.71%	▼26.07
4	Canada	280(3.38%)	▼9.09%	▲ 13.71
5	Finland	209(2.52%)	▼80.00%	▼49.67
6	United Kingdom	207(2.50%)	▼71.43%	▼46.53
7	Singapore	189(2.28%)	▼83.33%	▼3.89%
8	Ireland	188(2.27%)	0.00%	▼6.19%
9	Japan	165(1.99%)	0.00%	▼51.63
10	China	147(1.78%)	▲600.00%	▲ 110.27

(9/29) At the most basic level, the process is based around digital signatures. A digital signature proves a SPECIFIC validators signed a SPECIFIC message (in our case, a block).

A BLS signature is a special kind of signature that can be aggregated for batched verification.



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

(10/29) Digital signatures allow us to hold individual validators accountable. If they act maliciously, they can be identified and the $ETH they staked can be slashed.

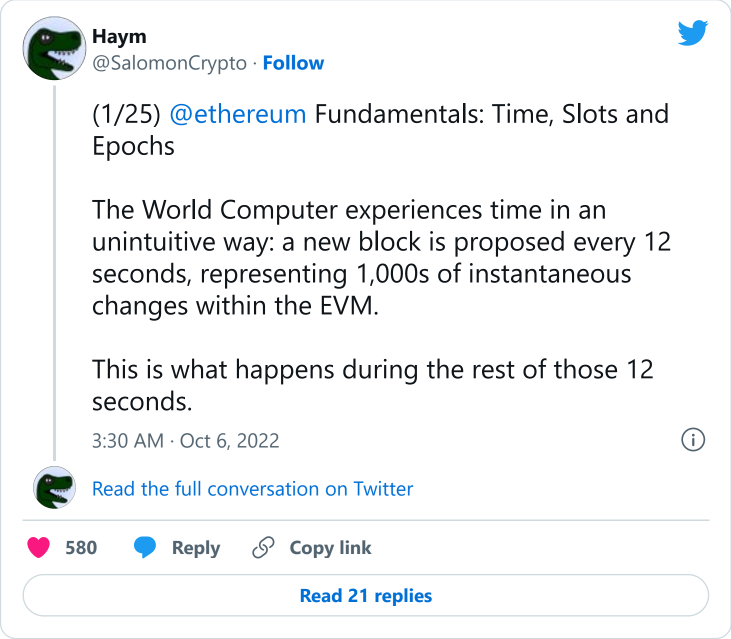
Slashing is the processes of destroying a validators stake and ejecting them from the validator set.

(11/29) Slashing is the mechanism that gives PoS its security. Because validators do not want to lose their investment in resources and infrastructure, slashing ensures that validators stay honest and act in a fashion that does not harm the network.

So... how does it work?

(12/29) Every 12 seconds, @ethereum opens a new slot, expecting a new block. Within a block there are thousands txns, but they execute atomically: either all together or none at all.

An epoch is made up of 32 slots.



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

(13/29) Every epoch, @ethereum shuffles the validator set into 32 committees (one per slot) and each committee into 64 subnets.

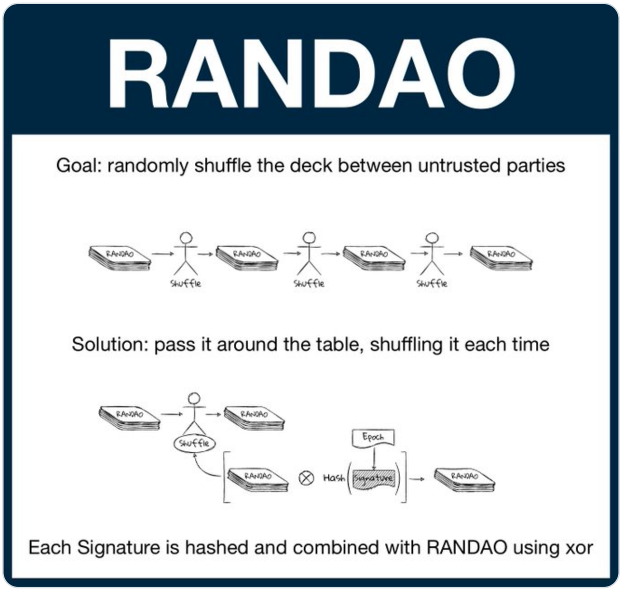
The security of the World Computer requires credible randomness during this shuffling, which is delivered by a process known as RANDAO.

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

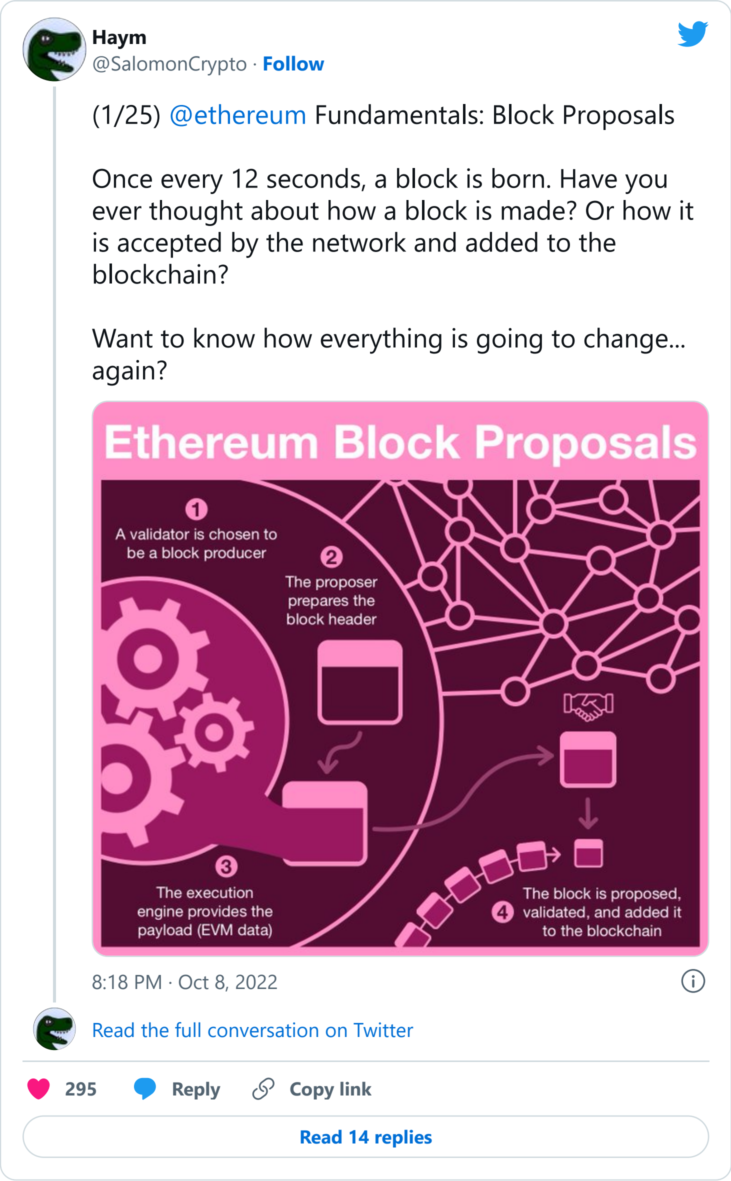
Read the full conversation on Twitter

216 Reply Copy link

Read 8 replies

(14/29) The first member of each committee is designated the block proposer and earns the right to progress the EVM. The proposer must build (or otherwise source) the block and then broadcast it to the network.

The proposer's stake is at risk if s/he proposes an invalid block.



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

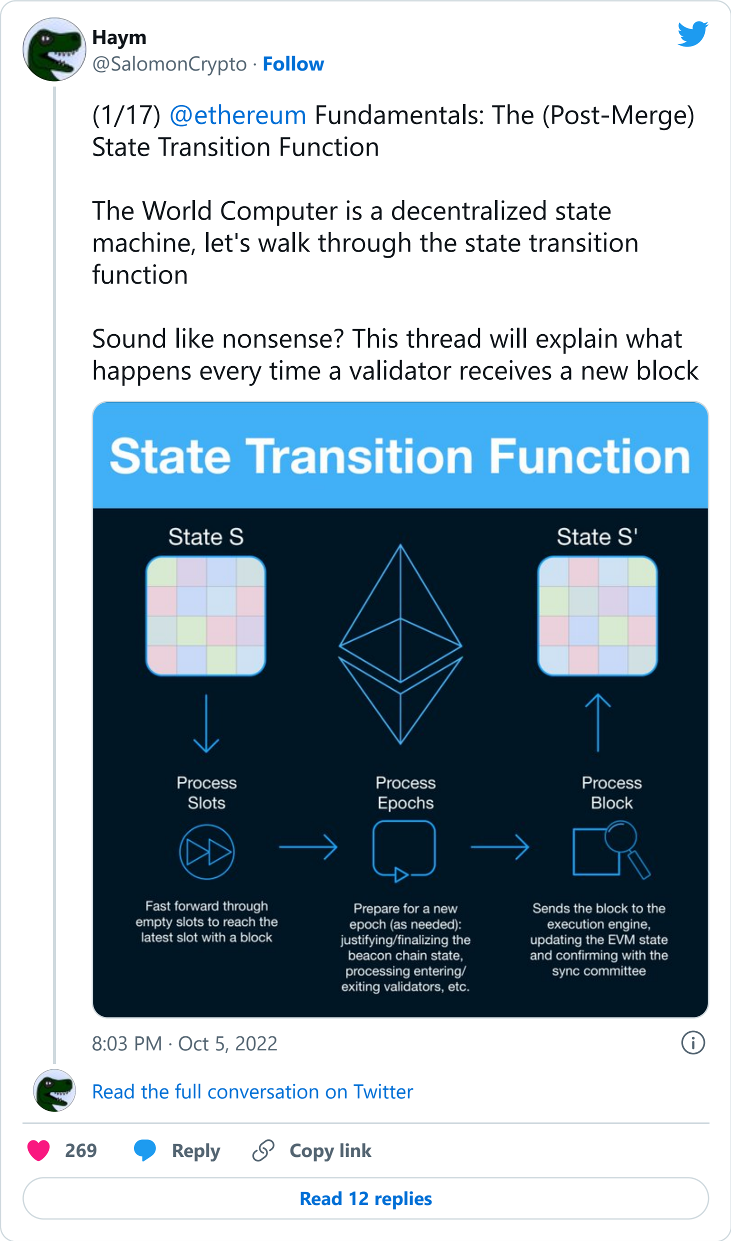
Read the full conversation on Twitter

295 Reply Copy link

Read 14 replies

(15/29) Every validator on the network is listening for a copy of every block. When it receives a new block, it executes the state transition function.

The state transition function is the actual process of updating the EVM (and processing epochs, when appropriate).



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

State S

State S'

Process Slots

Fast forward through empty slots to reach the latest slot with a block

Process Epochs

Prepare for a new epoch (as needed): justifying/finalizing the beacon chain state, processing entering/exiting validators, etc.

Process Block

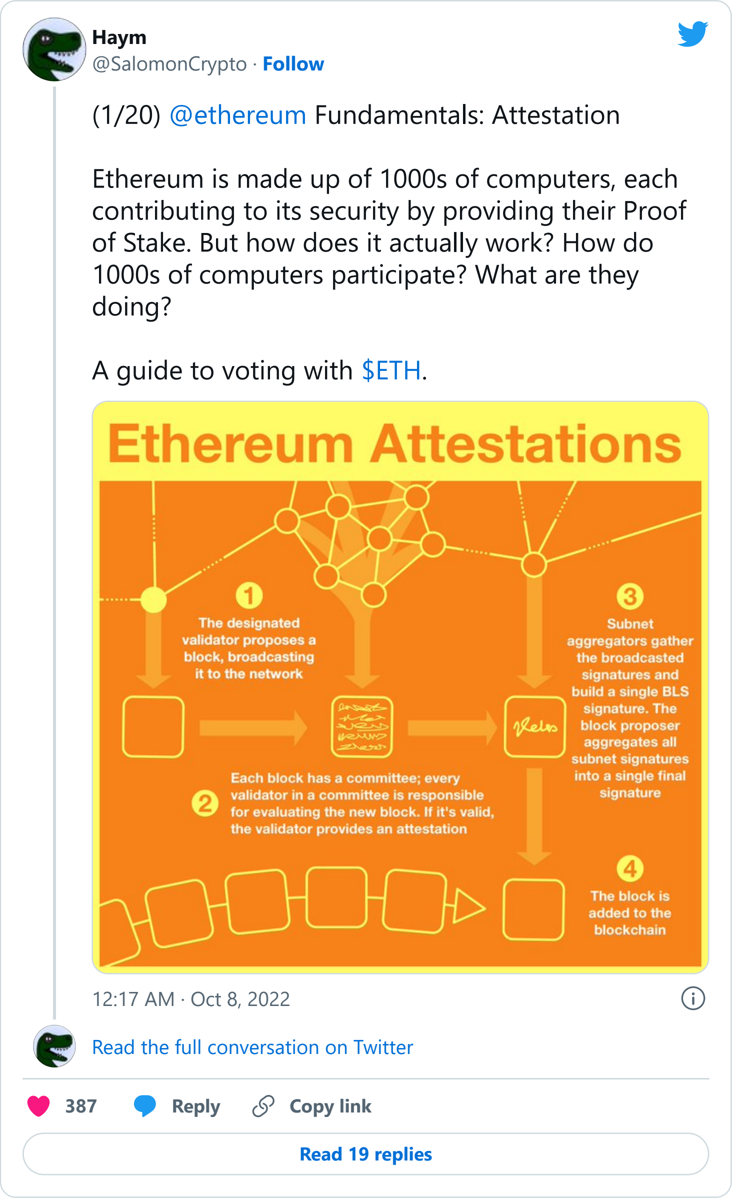
Sends the block to the execution engine, updating the EVM state and confirming with the sync committee

8:03 PM · Oct 5, 2022

Read the full conversation on Twitter

(16/29) The validators in the committee corresponding with each slot have an additional duty: they must verify the block.

Assuming each block is valid, each committee member creates and publishes a cryptographic signature (attestation), putting their stake at risk.



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.

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

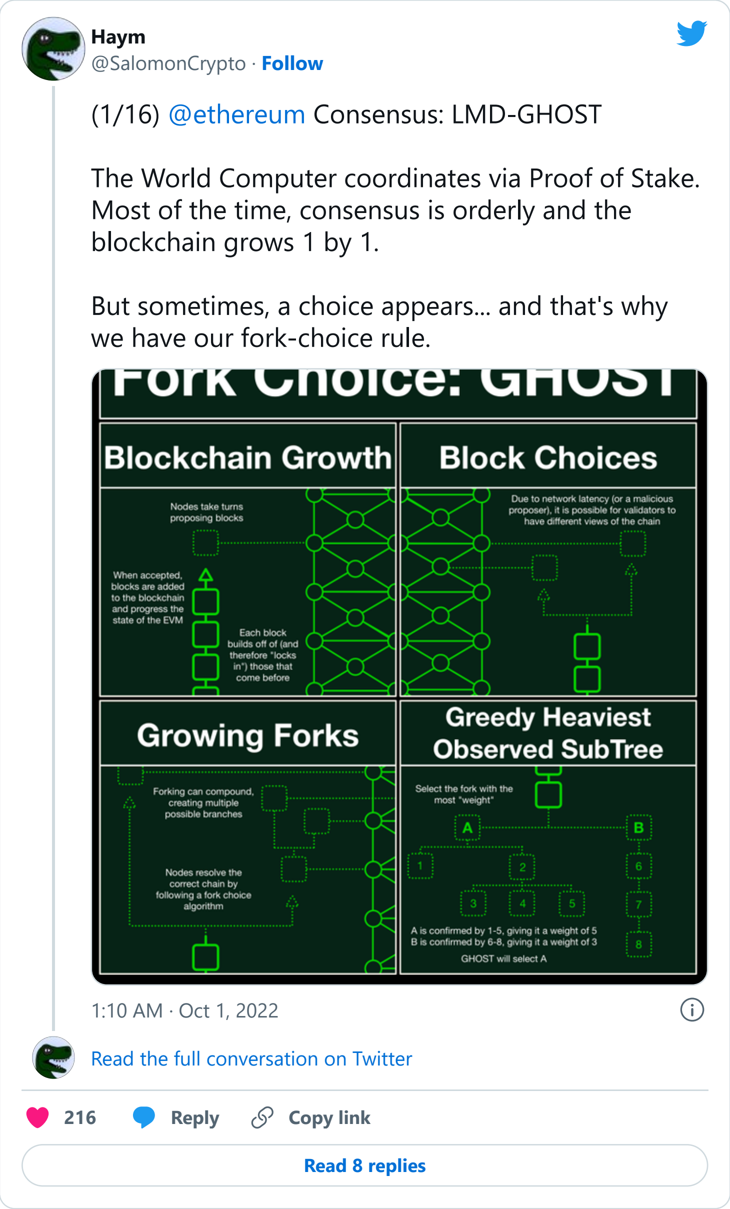
(17/29) In a perfect world, this is pretty straightforward; in the real world, things get tricky very quickly.

In sub-ideal network conditions (the vast majority), it's possible that every validator might not receive every block.

(18/29) Imagine the impending block proposer didn't receive a copy of the last block; he creates a new block based on the previous state and sends it out to the network.

Now our blockchain has turned into a block-fork.

LMD-GHOST is the rule we use to resolve these situations.



Haym
@SalomonCrypto · **Follow**

(1/16) @ethereum Consensus: LMD-GHOST

The World Computer coordinates via Proof of Stake. Most of the time, consensus is orderly and the blockchain grows 1 by 1.

But sometimes, a choice appears... and that's why we have our fork-choice rule.

Fork Choice: GHOST
Blockchain Growth
Nodes take turns proposing blocks
When accepted, blocks are added to the blockchain and progress the state of the EVM
Each block builds off of (and therefore "locks in") those that come before
Block Choices
Due to network latency (or a malicious proposer), it is possible for validators to have different views of the chain
Growing Forks
Forking can compound, creating multiple possible branches
Nodes resolve the correct chain by following a fork choice algorithm
Greedy Heaviest Observed SubTree
Select the fork with the most "weight"
A
B
1
2
3
4
5
6
7
8
A is confirmed by 1-5, giving it a weight of 5
B is confirmed by 6-8, giving it a weight of 3
GHOST will select A

1:10 AM · Oct 1, 2022

Read the full conversation on Twitter

216
Reply
Copy link
Read 8 replies

(19/29) Every slot a new committee becomes active and is expected to provide attestations.

440k validators / 32 committees = ~14k validators/committee.

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

(21/29) Fortunately, we've already split committees into 64 subnets.

Each subnet consists of ~250 validators, of which 16 are designated as aggregators. As validators review blocks, they broadcast their attestations to their subnet.

(21/29) All 16 aggregators are attempting to build the same aggregate signatures, but network conditions often make perfection possible.

The best aggregate in each subnet is chosen and aggregated one final time, created a single BLS signature representing the entire committee.

(22/29) Technically speaking, the aggregation process (obviously) happens after the block is proposed (and therefore created); the final aggregate attestation cannot be added on to it. Instead, it is included in the next block.

Conceptually, it's part of the same slot cycle.

(23/29) At the end of every epoch, all 32 committees (and therefore every validator) has either proposed or attested; therefore the entire network has voted and made their stake eligible for slashing.

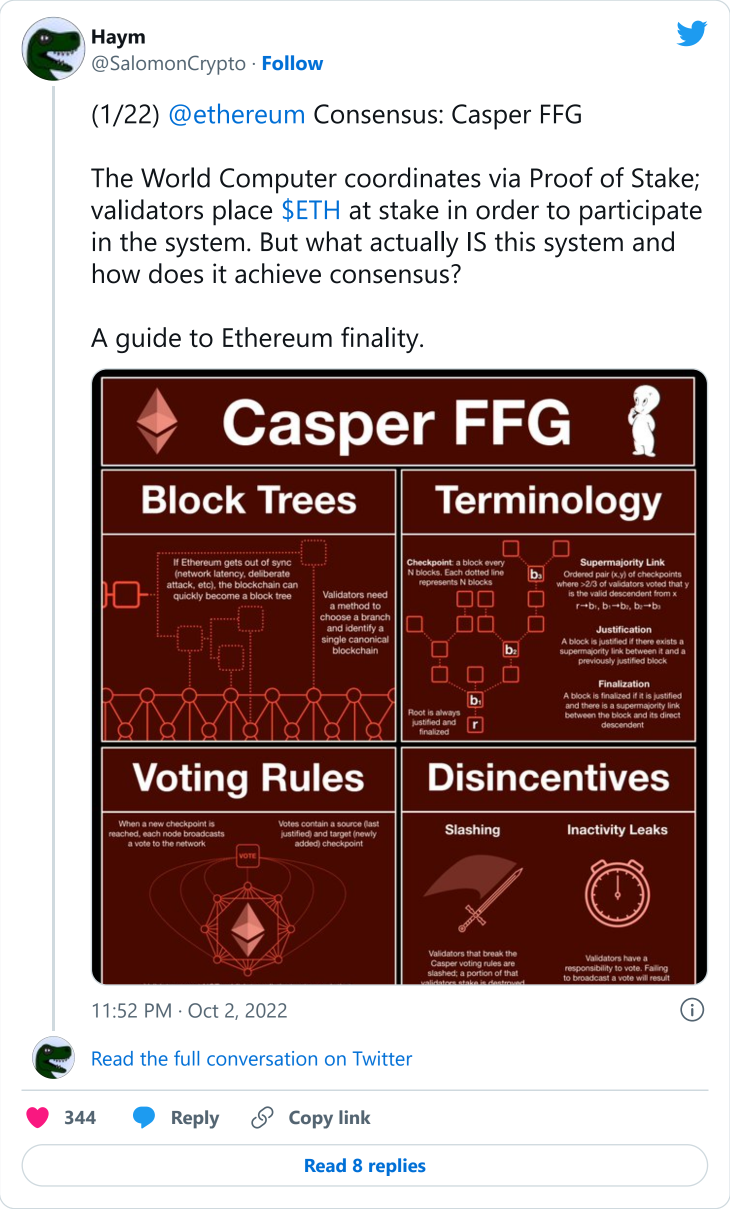
Thus, the epoch is the unit of time we judge finalization on.

(24/29) Finalization is a mathematical guarantee that @ethereum has fully applied PoS to an epoch; it cannot be reverted without the destruction (via slashing) of at least 1/3 of the $ETH at stake (~$6B right now).

(25/29) If more than 2/3s of the network votes on an epoch, that epoch becomes justified.

If more than 2/3s of the network votes for an epoch that is dependent on a justified epoch, the justified epoch becomes finalized.

These rules are defined by Casper FFG.



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.

Casper FFG

Block Trees

If Ethereum gets out of sync (network latency, deliberate attack, etc), the blockchain can quickly become a block tree

Validators need a method to choose a branch and identify a single canonical blockchain

Terminology

Checkpoint: a block every N blocks. Each dotted line represents N blocks

Supermajority Link
Ordered pair (x,y) of checkpoints where >2/3 of validators voted that y is the valid descendent from x
r→b1, b1→b2, b2→b3

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 descendent

Root is always justified and finalized

Voting Rules

When a new checkpoint is reached, each node broadcasts a vote to the network

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 validators stake is destroyed

Inactivity Leaks

Validators have a responsibility to vote. Failing to broadcast a vote will result

11:52 PM · Oct 2, 2022

Read the full conversation on Twitter

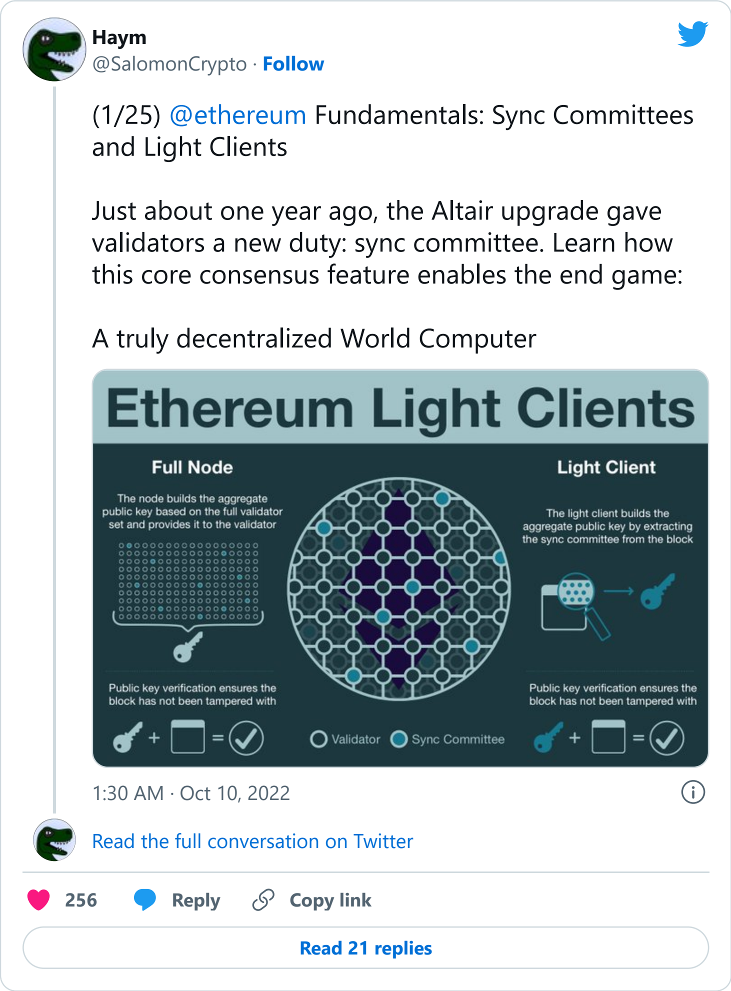
(26/29) At this point we've nearly finished out @ethereum PoS specifications; as you can see it is complicated.

In fact, it is so complicated that many computers with limited resources and/or bandwidth cannot possibly execute it.

Many computers that would be incredibly useful.

(27/29) And so, before @ethereum was ever actually PoS, the future of the World Computer was baked directly into the consensus specs.

In fall 2021, in preparation for a light client-based future, the Altair upgrade introduced the third validator responsibility: sync committee.



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 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

256 Reply Copy link

Read 21 replies

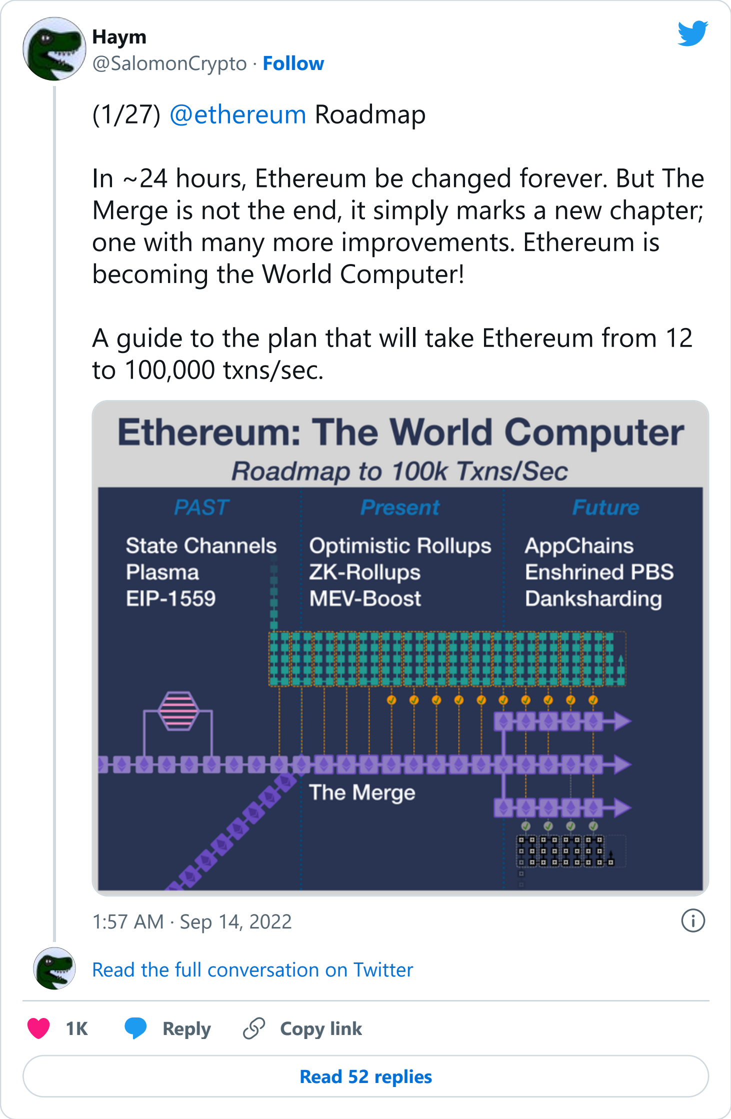
(28/29) Tl;dr a sync committee is a subset of 512 validators, chosen once every 256 epochs (~27 hours). Members of the sync committee must listen for EVERY block and provide a digital signature.

This provides the blockchain-level scaffolding needed to support light clients.

(29/29) And that, my friends, is @ethereum Proof of Stake!

Well... that's the PoS we have today; the first version of the consensus engine at the core of the World Computer. But it's definitely not the end.

We are STILL so early!



Haym
@SalomonCrypto · Follow

(1/27) @ethereum Roadmap

In ~24 hours, Ethereum be changed forever. But The Merge is not the end, it simply marks a new chapter; one with many more improvements. Ethereum is becoming the World Computer!

A guide to the plan that will take Ethereum from 12 to 100,000 txns/sec.

Ethereum: The World Computer
Roadmap to 100k Txns/Sec

PAST	Present	Future
State Channels Plasma EIP-1559	Optimistic Rollups ZK-Rollups MEV-Boost	AppChains Enshrined PBS Danksharding

1:57 AM · Sep 14, 2022

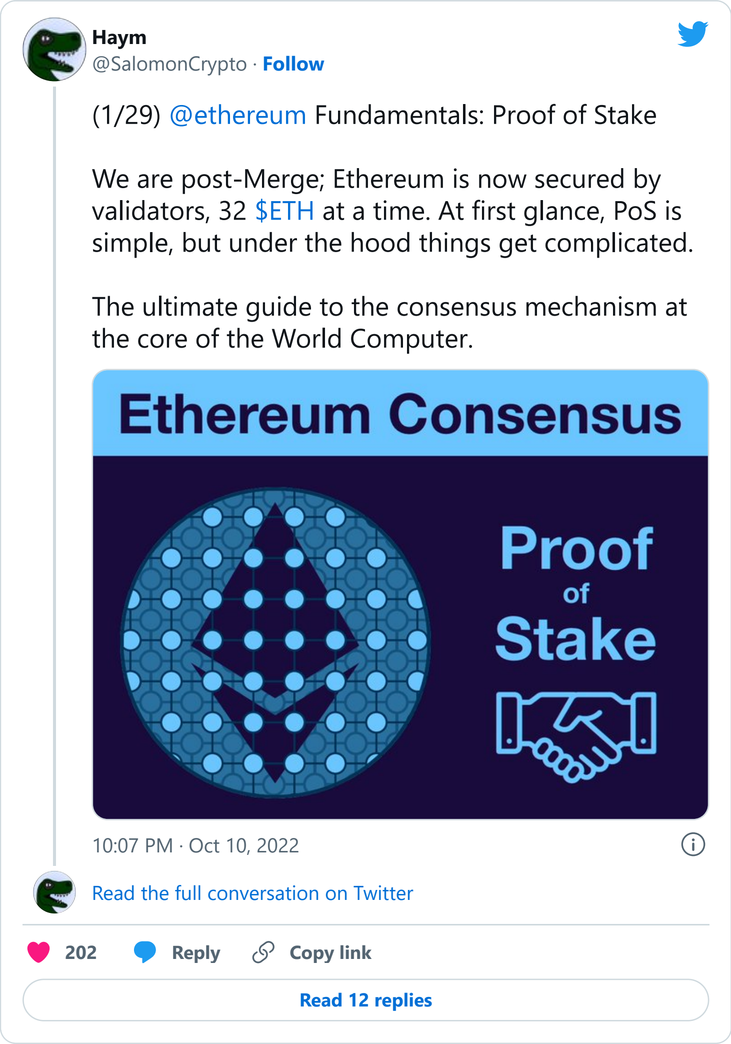
Read the full conversation on Twitter

1K Reply Copy link

Read 52 replies

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

(1/29) @ethereum Fundamentals: Proof of Stake

We are post-Merge; Ethereum is now secured by validators, 32 $ETH at a time. At first glance, PoS is simple, but under the hood things get complicated.

The ultimate guide to the consensus mechanism at the core of the World Computer.

10:07 PM · Oct 10, 2022

Read the full conversation on Twitter

• • •