



**Haym** @SalomonCrypto

Oct 7 · 26 tweets · [SalomonCrypto/status/1578471242331365376](https://twitter.com/SalomonCrypto/status/1578471242331365376)

---

(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?

(2/25) [@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.



The image is a screenshot of a tweet from a user named Haym (@SalomonCrypto). The tweet is the first in a thread of seven parts, discussing Ethereum as 'The World Computer'. It references Vitalik Buterin's 2014 idea and offers to break it down in four threads. The tweet includes a graphic with the Ethereum logo and the text 'Ethereum The World Computer'. The graphic also features a diagram of a computer chip connected to a network of nodes, with labels for 'Virtual Machine (EVM)', 'Ethereum Blockchain', and 'Ethereum Network'. The tweet has 428 likes and 17 replies.

**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.

**Ethereum**  
*The World Computer*

Virtual Machine (EVM)  
Ethereum Blockchain  
Ethereum Network

1:01 AM · Aug 3, 2022

Read the full conversation on Twitter

428 Reply Copy link

Read 17 replies

(3/25) The World Computer progresses in units known as blocks (containing transactions, or actions, within the EVM). A block producer will create a block and send it to the network

As nodes receive new blocks they feed them into their copy of the EVM, syncing it to the leader

**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.

### Ethereum Blocks (PoS)

Consensus Layer	Execution Layer	Ethereum Transaction
<b>PoS Block</b> Administration Consensus Execution	<b>Administration</b> Consensus Execution	<b>Transaction</b> Metadata Cache Data

10:28 PM · Sep 9, 2022

[Read the full conversation on Twitter](#)

484 Likes   Reply   Copy link

[Read 36 replies](#)

(4/25) The system by which proposers are chosen and blocks are decided on is called consensus.

For the first 7 years of its life, @ethereum used Proof of Work (PoW) as a consensus mechanism. But as of mid Sept 2022, the World Computer has transitioned to Proof of Stake (PoS).

(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).

(6/25) The rest of the nodes verify the block and puzzle. If both are valid, they discard their block and add the new one to their local EVM. Then they begin working on a new block

Each new block confirms the ones before it acceptance is an implicit vote on the canonical chain

(7/25) These "incredibly difficult mathematical puzzles" are the cornerstone of PoW. The only way to solve them is by running many powerful machines (and spending huge amounts of electricity).

This work provides the gravity that makes each implicit vote have so much weight.

(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

(9/25) This system alone is not secure; it replaces PoW's foundation of real world work/electricity with trust.


Trust each proposer will propose valid blocks, trust the network will honestly verify, trust in optimal network conditions... so much trust.

(10/25) Thus, we introduce stake: a capital contribution by each validator that acts of a bond for engaged, honest participation.

In order to become an [@ethereum](#) validator, an operator must first lock 32 \$ETH in the deposit contract, making it eligible for slashing.


(11/25) Slashing is a two part process:

- 1) Impose economic penalties for bad behavior by draining the validators stake (up to the entire 32 \$ETH in the worst cases)
- 2) Forcibly ejecting the offender from the network/validator set



AN ETHEREUM STAKER'S GUIDE

## Slashing & Other Penalties



**A Staker's Guide to Ethereum Slashing & Other Penalties**  
Educate yourself and avoid being slashed as an Ethereum validator. ✓ Read Blocknative's guide to ensure that all of your bases are covered.  
<https://www.blocknative.com/blog/an-ethereum-stakers-guide-to-slashing-other-penalties>

(12/25) Slashing is a very rare occurrence and only happens when malicious nodes attack the network (or EXTREME operator error).

Nevertheless, slashing is the primary enforcement mechanism and source of security of PoS.

(13/25) Slashing alone is not enough to secure our simple PoS system.

A core dynamic of PoW and the incredible difficulty of its puzzles was the implicit vote on the canonical chain. Creating one new block is very hard; creating two (let alone many more) is new impossible.

(14/25) Attacking the chain requires overcoming a real-world constraint.

The vote is implicit because it doesn't actually exist, it's just a metaphor we use to describe blockchain from the perspective of the network.

(15/25) In PoS we must replace the implicit votes with explicit ones. Just like PoW, every block will receive a copy of each block, but in PoS a subset will also explicit vote on the validity of each block.

Each of these validators is personally voting that a block is valid.

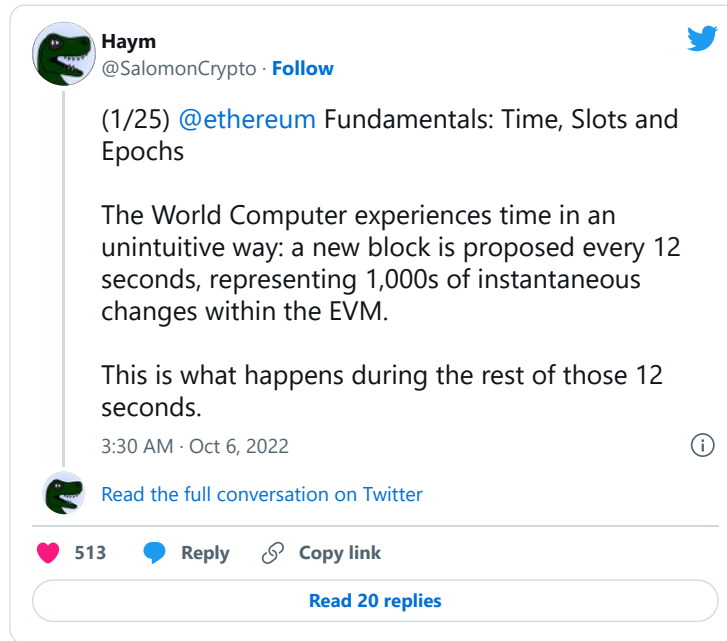
(16/25) A vote is called an attestation. By signing an attestation, the validator is putting their stake at risk: if the block ends up being invalid, they too will be slashed.

And so, [@ethereum](#) becomes secured not only against the proposer's stake but also each attester's.

(17/25) [@ethereum](#) sees time differently than we do.

Units of time are broken into slots, each of which (should) contain a block. 32 slots equals an epoch, which is 6.4 mins.

Under PoS, every Ethereum validator will vote (attest or propose) once per epoch.



(18/25) Thus, once every 6.4 mins, the entire validator set will vote on the canonical blockchain and place its entire stake on the line for slashing.

Once every epoch, [@ethereum](#) is secured with the total value of all staked \$ETH.

Today that's ~\$19B.

151940 epoch complete	
Epoch 151,940 / 151,938	Current Slot 4,862,111
Active Validators 441,030	Pending Validators 0 / 0
Staked Ether 14,112,838 ETH	Average Balance 33.84 ETH

(19/25) There's one final, much more nuanced, modification we need to make to our PoS system before it can replace PoW.

PoW is never at risk of locking up. As long as a node exists, it will be able to solve puzzles and progress the chain (although solve times will be very long).

(20/25) PoS comes from a tradition of mathematics stemming from the Byzantine Generals Problem.

Tl;dr consensus requires agreement of at least  $2/3$  between the nodes of the network.

What happens if  $>1/3$  are offline?

**Haym**  
@SalomonCrypto · Follow

(1/21) Byzantine Fault Tolerance (BFT) and the Practical Solution (pBFT)

What is the Byzantine Generals Problem? Why is it important for distributed systems? Does this problem have a solution?

A guide to the core principles underlying decentralized consensus.

### Byzantine Generals Problem

A city is surrounded by several divisions of the Byzantine army, each commanded by its own general. The generals can only communicate by messenger.

If all generals attack, the city will fall. If all generals retreat, the army will live to fight another day. If some generals attack and some retreat, the entire army will be lost.

Some generals are loyal, some are traitors.

How can the Byzantine generals reach consensus?

### Victory through Consensus

<b>Result</b>	<b>Win</b>	<b>Win</b>	<b>Lose</b>	<b>Lose</b>	<b>Lose</b>

6:55 PM · Oct 1, 2022

[Read the full conversation on Twitter](#)

533 ❤️ Reply Copy link

[Read 14 replies](#)

(21/25) @ethereum has a two-line defense approach.

First, validators who fail their duty (eg missing/late/incorrect attestation) receive a mild penalty. This is an encouragement to remain online, but it's felt by everyone during routine maintenance or network volatility.

(22/25) If >2/3 of the network is not participating, [@ethereum](#) cannot finalize. When this situation becomes dire enough, the network activates its 2nd line of defense: inactivity leak.

The inactivity leak is a kind of emergency state that follows rules until 2/3 can be reached:

- Attesters receive no attestation rewards while attestation penalties are unchanged.
- Any validators deemed inactive have their inactivity scores raised, leading to an additional inactivity penalty that potentially grows quadratically with time. This is the inactivity leak, sometimes known as the quadratic leak.
- Proposer and sync committee rewards are unchanged.

(23/25) Both of these defenses are significantly less severe than slashing. Not only are the economic punishments much less, validators are not ejected from the network.

In general, these penalties can be earned back with roughly the same amount of time it took to accrue them.

(24/25) Taken all together, we now have a secure PoS system!

I'll leave this for an overview of the pros and cons (lifted from the [@ethereum](#) website).

Proof of Work (PoW)	
Pros	Cons
Proof-of-work is neutral. You don't need ETH to get started, block rewards allow you to go from 0 ETH to a positive balance.	Proof-of-work uses up so much energy, which is both bad for the environment and poses serious regulatory risks
Proof-of-work is a tried and tested consensus mechanism that has kept Bitcoin and Ethereum secure and decentralized for many years.	If you want to mine, you need such specialized equipment that it's a big investment to start.
Compared to proof-of-stake it's relatively easy to implement.	Due to increasing computation needed, mining pools dominate the mining game, leading to centralization and security risks.

Proof of Stake (PoS)	
Pros	Cons
Staking makes it easier for individuals to participate in securing the network, promoting decentralization. Staking pools allow users to stake without having 32 ETH.	Proof-of-stake is younger and less battle-tested compared to proof-of-work
Staking is more decentralized. Economies of scale do not apply in the same way that they do for PoW mining.	Proof-of-stake is more complex to implement than proof-of-work
Staking is more decentralized. Economies of scale do not apply in the same way that they do for PoW mining.	Users need to run three pieces of software to participate in Ethereum's proof-of-stake.
Less issuance of new ETH is required to incentivize network participants	

(25/25) Less than 1 month ago, [@ethereum](#) mainnet Merged with the beacon chain and the World Computer transitioned to PoS.

Though it takes some thinking through, PoS is the cleaner option; it is the fulfillment of the core vision of \$ETH...

The settlement layer of the internet!



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.



A screenshot of a Twitter post from user Haym (@SalomonCrypto). The post is the first in a thread of 25 tweets. The text discusses the distributed nature of Ethereum and asks for an understanding of Proof of Work and Proof of Stake. The post has 5 likes and one reply. The interface includes a profile picture, name, handle, follow button, tweet text, timestamp, and interaction buttons (like, reply, copy link).

**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](#)

5 [Reply](#) [Copy link](#)

[Read 1 reply](#)

...