



Haym Salomon @SalomonCrypto

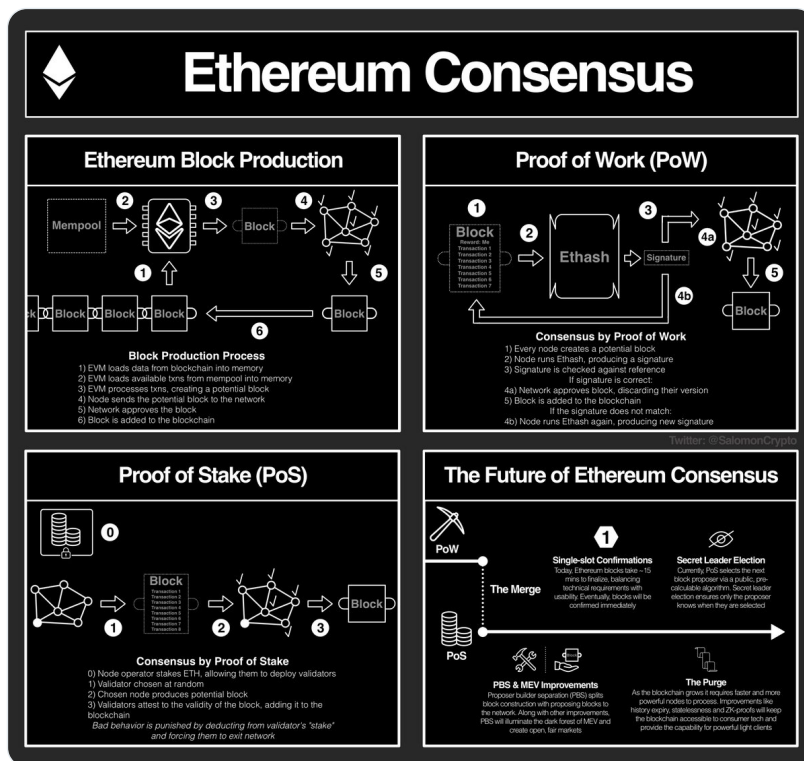
Aug 2 · 24 tweets · [SalomonCrypto/status/1554500348231880704](https://twitter.com/SalomonCrypto/status/1554500348231880704)

Tr

(1/23) Coordination in The World Computer: [@ethereum](https://twitter.com/ethereum) Consensus

The Merge is weeks away... are you caught up on Proof of Work (PoW), Proof of Stake (PoS) and the systems that form the backbone of Ethereum?

Read up anon, time is running short. The world is about to change forever



(2/23) [@ethereum](#) is The World Computer. It's a shared resource upheld by a network of anonymous, untrusted nodes; aligned by consensus and economically secured

The Ethereum Network provides credible neutrality upon which anyone can build... both independently and collaboratively

 **Haym Salomon**
@SalomonCrypto · Follow

(1/18) [@ethereum](#): The World Computer

A guide to the foundational principles and technologies of Ethereum.

If you have ever wondered “what’s the big deal about **\$ETH**?” This is the thread for you!



2:18 AM · Jul 9, 2022

 [Read the full conversation on Twitter](#)

4.8K Reply Copy link

[Read 145 replies](#)

(3/23) While [@ethereum](#) can be thought of as The World Computer, its construction is novel and unlike a typical desktop computer. It is best to think of Ethereum as consisting of 3 parts:

- Ethereum Virtual Machine (EVM)
- Ethereum Blockchain
- Ethereum Network

(4/23) The EVM provides the computing environment, the blockchain provides a permanent, transparent record of The Computer's activity.

The network is the group of real world computers (nodes) that run the software that both executes the EVM and produces the blockchain.

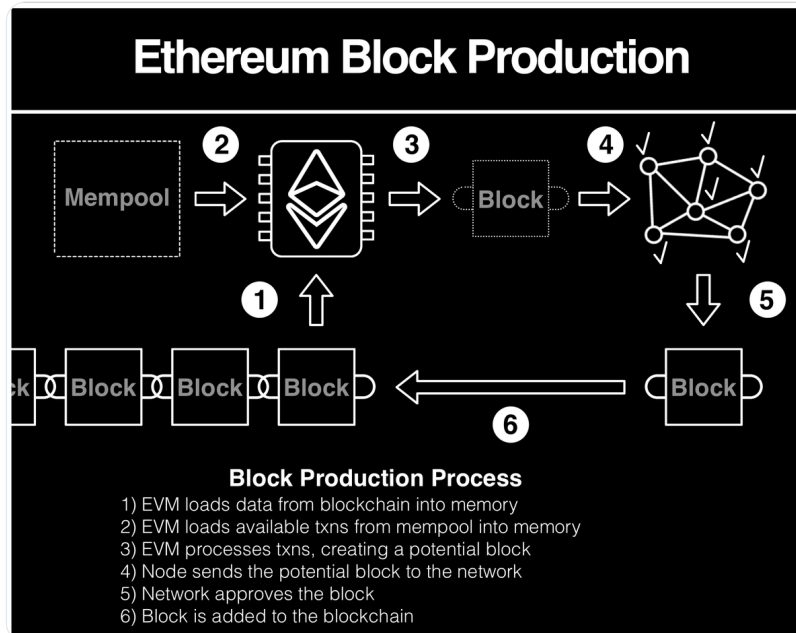
(5/23) As The World Computer executes transactions, it records the changes in the EVM and reports it as a block.

Each node is executing this process locally, coordinating with the network and progressing in lockstep.

Let's examine how.

(6/23) We begin with the blockchain, from which the EVM can load everything into memory. From there it can begin transacting.

Potential transactions are chosen from the mempool and bundled together. The EVM then executes all bundled transactions, producing a potential block.



(7/23) The potential block is then sent to the network. The other nodes inspect and approve the potential block, adding it to their copy the blockchain

The network must maintain uniform execution across tens of thousands of nodes. All must progress together, one block at a time

(8/23) Consensus is the process by which all the nodes coordinate, stay in sync and create economic security.

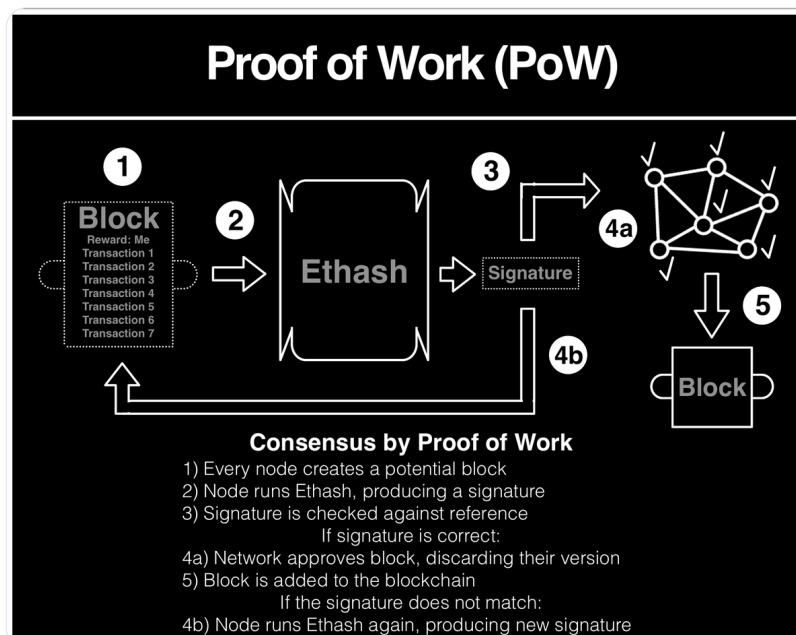
Currently, the [@ethereum](#) network uses Proof of Work (PoW) to coordinate. However, soon™ Ethereum will transition to Proof of Stake (PoS).



(9/23) Today, nodes (miners) compete to solve puzzles generated by the current state of the blockchain.

The first miner to solve the puzzle broadcasts the block they produced to the network, who add it to their copy of the blockchain.

Then everyone begins the next puzzle.



(10/23) Read about Ethash to learn more about these puzzles.

Just know that they are difficult to solve but easy to verify. Even with endless processors dedicated to each puzzle, it takes ~15 seconds to solve!

(in computer years that's HUGE)



(11/23) Importantly, the way this system works is winner take all. Only the first miner with the correct solution is rewarded. Every other node discards their work and starts on the next one.

Not only is everyone else's effort trashed, it's responsible for all that energy waste.

PROOF-OF-WORK ENERGY-USAGE

A major criticism of proof-of-work is the amount of energy output required to keep the network safe. To maintain security and decentralization, Ethereum on proof-of-work consumes 73.2 TWh annually, the energy equivalent of a medium-sized country like Austria.

(12/23) There are pros and cons to PoW. It served its purpose well for the early years of [@ethereum](#).

Anyone can plug in their computer and start mining \$ETH, distributing it broadly. Over time, the competition has grown so fierce that only massive pools can win.

PROS AND CONS	
Pros	Cons
Proof-of-work is neutral. You don't need ETH to get started and block rewards allow you to go from 0ETH to a positive balance. With proof-of-stake you need ETH to start with.	Proof-of-work uses up so much energy that it's bad for the environment.
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 could potentially dominate the mining game, leading to centralization and security risks.

(13/23) As we approach The Merge, signifying [@ethereum](#)'s switch from PoW to PoS, we must remind ourselves that this has been the vision from the beginning

[@VitalikButerin](#) was posting about Ethereum's "PoS war chest" back in 2014, before Ethereum launched



(14/23) PoS begins with a commitment by every node (validator): "I will play by the rules."

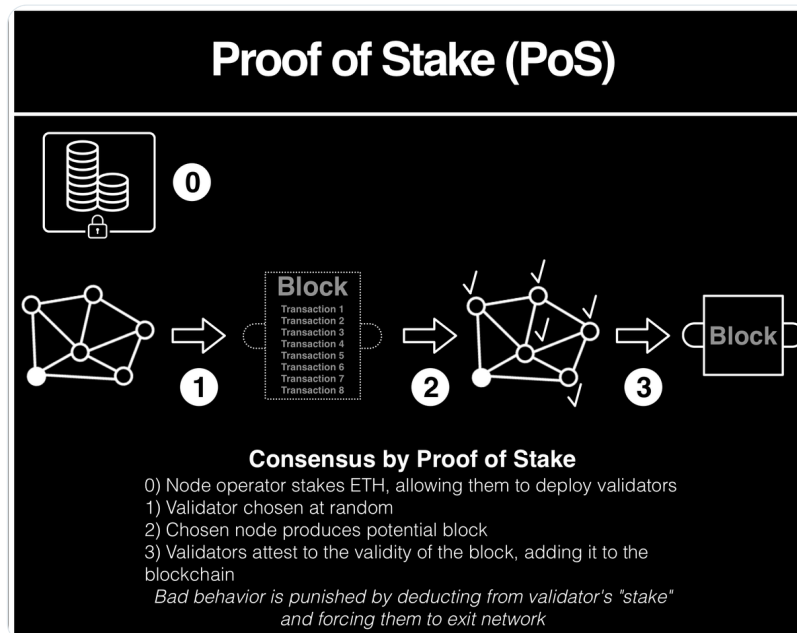
But this is the internet, we don't rely on promises from anonymous IP addresses. [@ethereum](#)
PoS requires a pledge of collateral.

Something at stake.

(15/23) In PoS, a validator is chosen at random, becoming the block producer

The block producer chooses transactions from the mempool (or elsewhere), constructs a block and sends it to the network

Validators attest to the validity of the new block, adding it to the blockchain



(16/23) Proposals are rewarded with a lot of \$ETH, attestations with a little

The network is made of nodes, each of which can support multiple validators. A validator has exactly 32 \$ETH at stake

Deploying more validators means a better chance to be selected as block proposer

(17/23) PoS is more complex and less battle-tested than PoW, and has taken many years (and attempts) to get right.

However, it has considerable advantages, especially in regards to decentralization.

PROS AND CONS	
Pros	Cons
Staking makes it easier for individuals to participate in securing the network, promoting decentralization. validator node can be run on a normal laptop. 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
Proof-of-stake offers greater crypto-economic security than proof-of-work	Users need to run three pieces of software to participate in Ethereum's proof-of-stake.
Less issuance of new ether is required to incentivize network participants	

(18/23) My favorite analogy is a running race.

PoW is a brutal competition between every athlete, from little Jimmy to [@usainbolt](#). 1st gets the prize, 2nd-last get nothing.

PoS is an agreement to take turns and to share the winnings, enforced by a claim on your bank account.

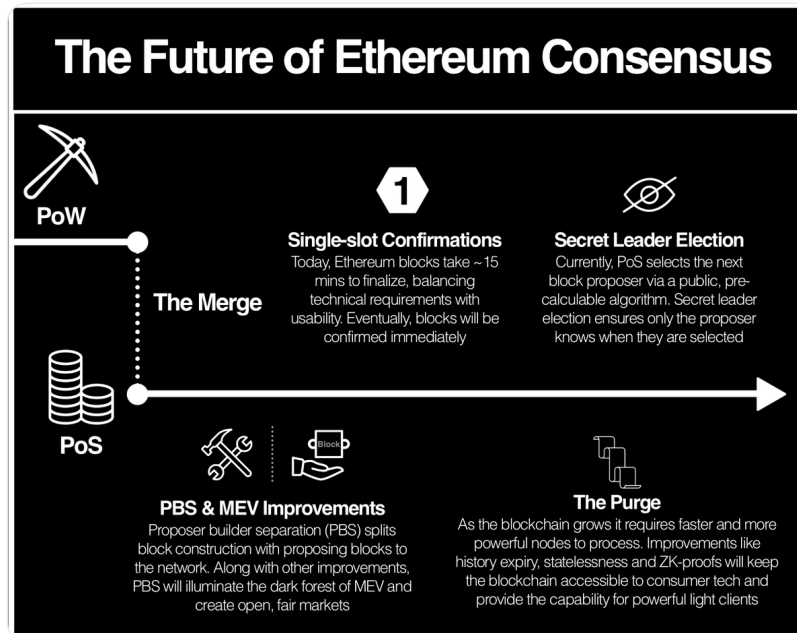
(19/23) In summary, while [@ethereum](#) is about to finish a transition of consensus mechanisms, both provide the same role: network coordination and economic security

PoW was for bootstrapping, PoS is for institution building

But The Merge isn't the end of the development...

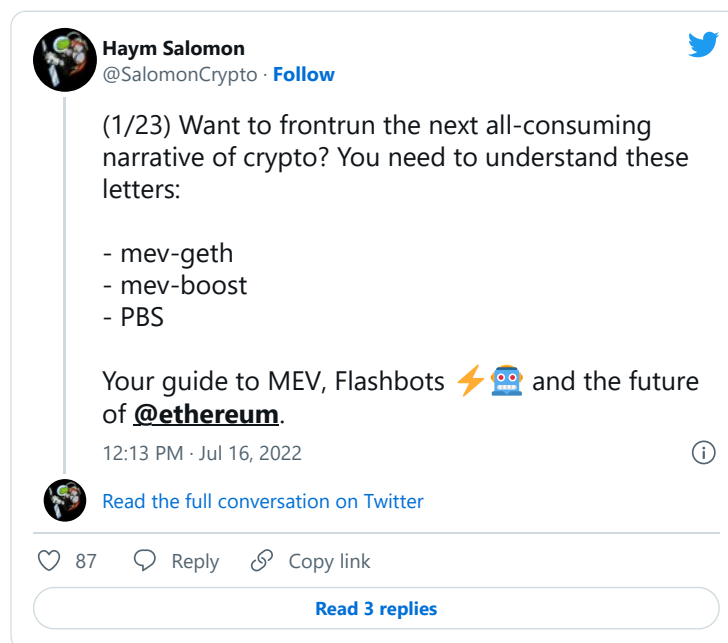
(20/23) @ethereum consensus still has many incredibly important improvements in the pipeline. In general, we can organize them into 2 categories:

- Technical improvements, focusing on performance, usability and security
- Emergent properties of Ethereum and blockchain technology



(21/23) The most important group of emergent @ethereum properties is Maximum Extractable Value (MEV); MEV is value that can be extracted from a system by a participant with privileged knowledge or access

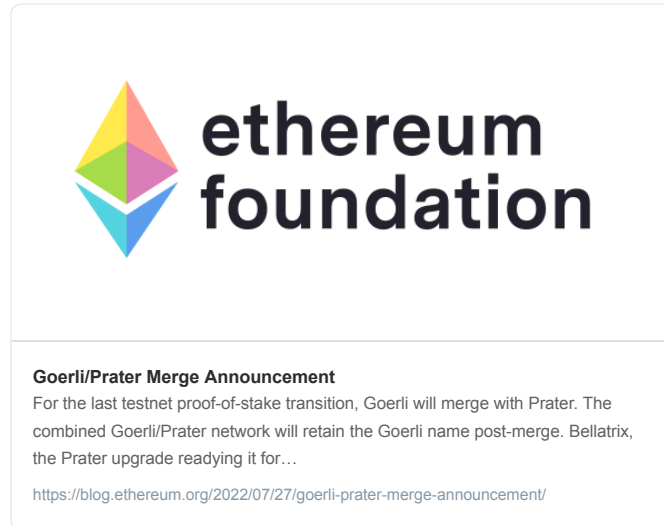
MEV is older than crypto, but Ethereum has illuminated and supercharged it



(22/23) The Merge is just around the corner.

Ropsten has merged. Sepolia has merged. Only Goerli left... One more testnet to go!

If all goes well, we could have PoS [@ethereum](#) by National Horchata Day!



(23/23) [@ethereum](#) is The World Computer, native to the internet.

The EVM and the blockchain speak to The World Computer. Consensus systems speak to internet native, coordinating trustlessly and progressing in unison.

The future is in the applications you build on top of it!

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.



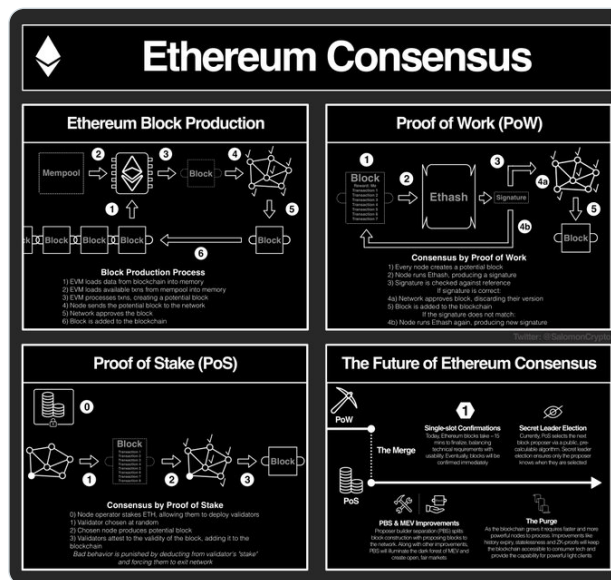
Haym Salomon
@SalomonCrypto · Follow



(1/23) Coordination in The World Computer: @ethereum Consensus

The Merge is weeks away... are you caught up on Proof of Work (PoW), Proof of Stake (PoS) and the systems that form the backbone of Ethereum?

Read up anon, time is running short. The world is about to change forever



4:12 PM · Aug 2, 2022



[Read the full conversation on Twitter](#)

74 Reply Copy link

[Read 3 replies](#)

...