Haym Salomon @SalomonCrypto

Aug 16 · 26 tweets · SalomonCrypto/status/1559402384526258176

(1/25) @ethereum Scalability: The Roadmap to 100k Transactions per Second

Over the next 3-5 years, Ethereum will evolve from a primitive blockchain into the backbone of the internet.

Your guide to:

- The Merge
- EIP-4844 (proto-danksharding)
- Enshrined PBS
- Danksharding

(2/25) @ethereum is The World Computer!

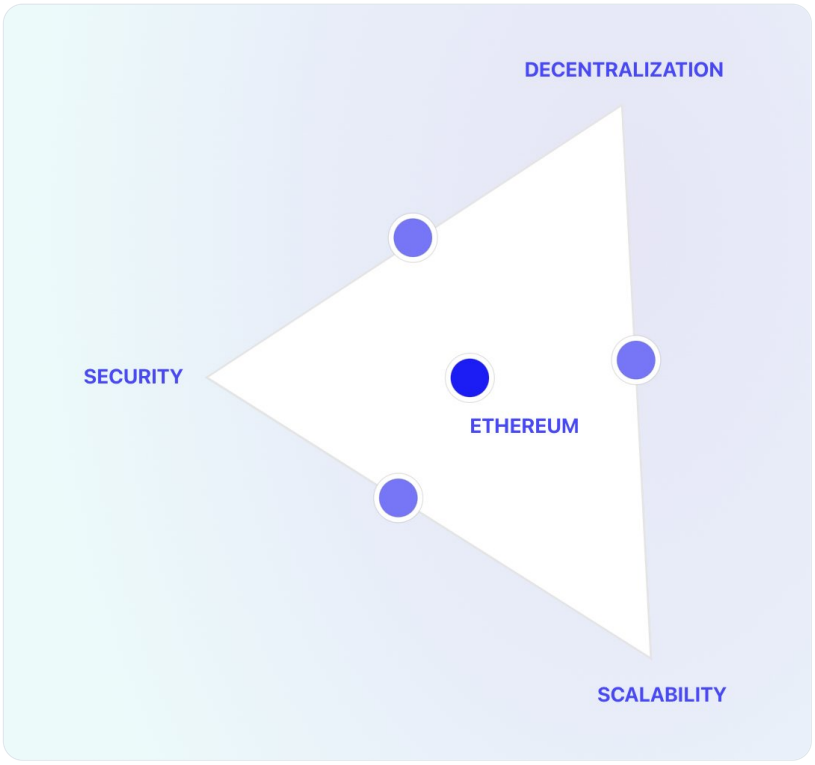
Today the computer is... primitive. Execution is slow, gas costs are outrageous and user experience is terrible.

What's worse: the more people use it the worse it gets.

Fear not... upgrades are coming!

(3/25) Before we discuss @ethereum's roadmap, we need to understand the challenges of blockchain scaling.

Summarized by the Scalability Paradox, it is (seemingly) impossible to remain decentralized, secure and scalable; optimizing for one compromises the other two.

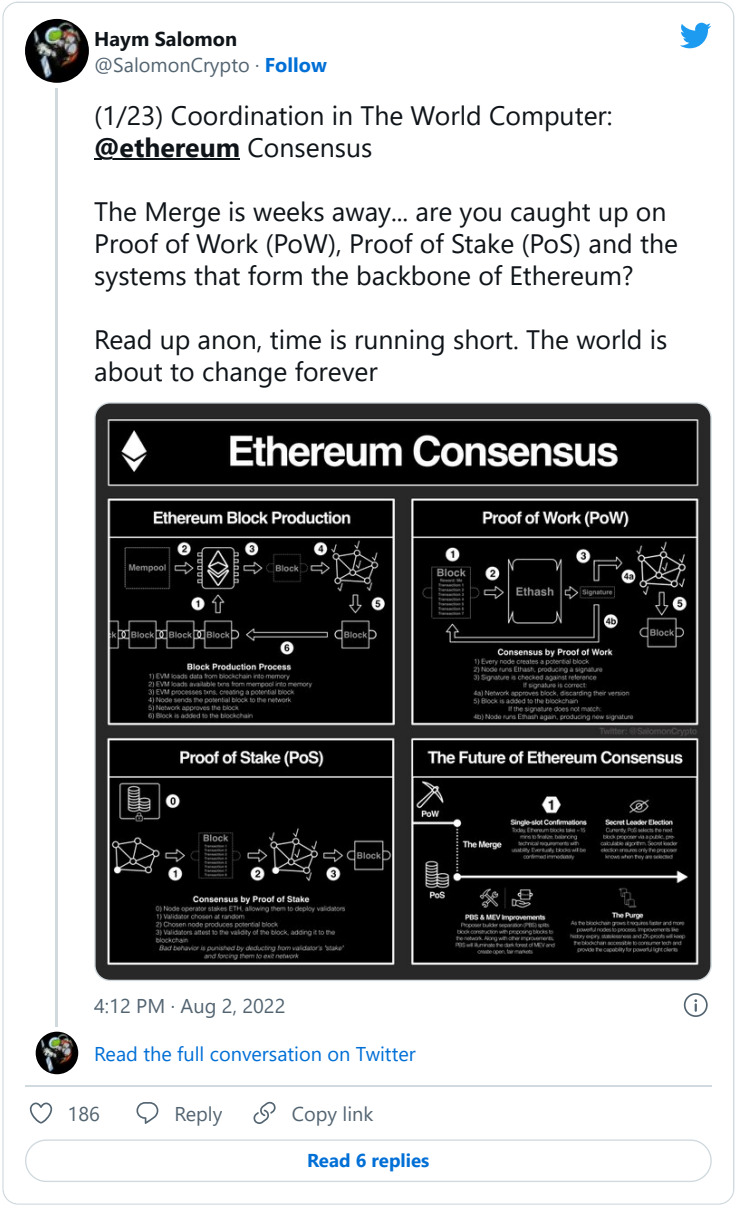


(4/25) But thanks to the world class researchers and devs at the Ethereum Foundation, we have a solution; the Scalability Paradox has been reduced to the Scalability Trilemma!

Here's how it'll be done:

(5/25) The first major upgrade is imminent: @ethereum will be switching its consensus system from PoW to PoS.

Instead of being secured by the computing power of the computers supporting it, (after The Merge) The World Computer will be secured by the economic value of $ETH.



(6/25) Today the system requires top-of-the-line computers; soon anyone with a home computer will be able to participate in the @ethereum network

The Merge will be a leap forward for decentralization, allowing large scale participation and removing the economies of scale factor

(7/25) This provides a network with credible neutrality, where everyone plays by the same rules.

No centralized player can change the rules to pick winners and losers. No personal conflict can spill over into the rules of the network.

One computer, supported by >10k nodes.

(8/25) The problem: as @ethereum/the EVM becomes more simple, its capabilities/speed stop improving.

The solution: move the execution environment off-chain.

The Ethereum blockchain will always be the settlement layer of The World Computer, but execution will migrate to layer 2.

(9/25) Deep-dive later, layer 2s/rollups are blockchains that commit to settling all transactions on @ethereum (thus inheriting its decentralization and security guarantees), but are free to use more efficient (centralized) execution environments and compression techniques.

(10/25) Rollups will focus on execution, users will interact with rollups.

Proof-of-stake will make @ethereum the most secure and decentralized consensus layer for rollups while all the difficult stuff moves off-chain, to the powerful computers.

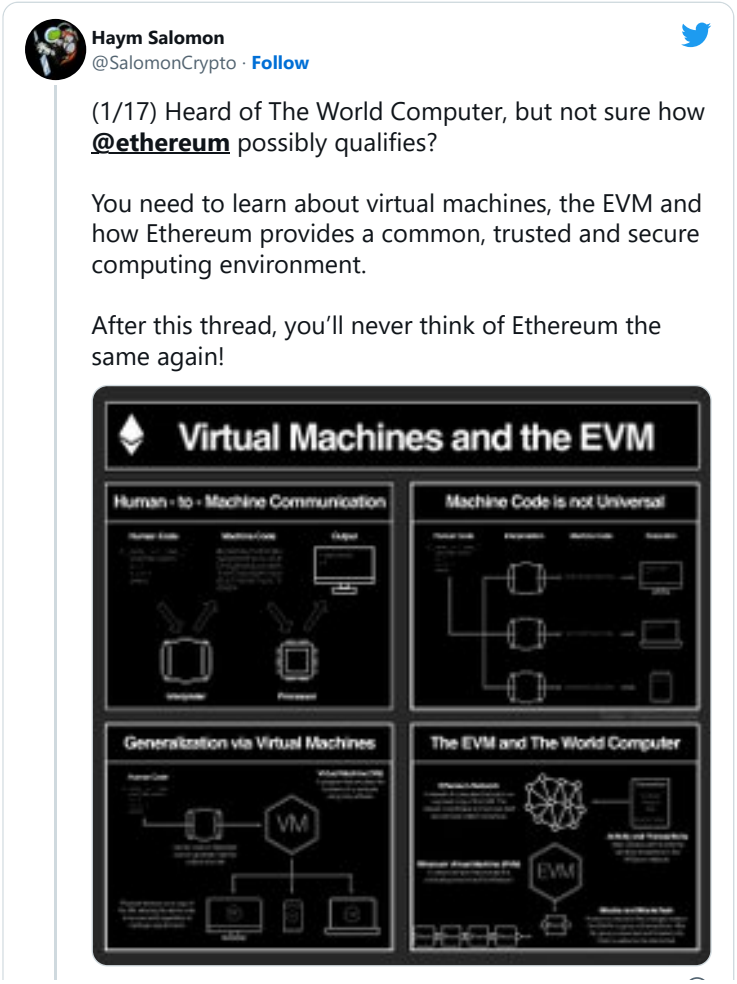
https://polynya.medium.com/understanding-ethereums-rollup-centric-roadmap-1c60d30c060f

(11/25) Today, we already have rollups. Between chains like @arbitrum, @optimismFND and @MetisDAO, billions of dollars of TVL have been moved to layer 2.

But this is just the beginning! @ethereum is currently general purpose, now its time to build to the rollup-roadmap.

(12/25) The EVM is the virtual computing environment in which all of @ethereum exists and all transactions happen.

After compressing a bundle of transactions, a rollup loads it into the EVM and commits it to the Ethereum blockchain.



(13/25) From a function standpoint, we only care that the compressed bundle is committed to the blockchain (settlement).

We can build tools to decompress the bundle into a readable format and/or move the data off-chain, but we don't need the EVM to be able to access it.

(14/25) Today, the EVM treats a bundle exactly the same as core programatic variables... and the gas fee market reflects that.

A rollup must pay a relatively large amount of $ETH to commit a bundle, even though the bundle's contents are irrelevant to the operation of the EVM.

(15/25) Which brings us to EIP-4844: Proto-Danksharding. The technicals are out of scope of this thread, but we are going to talk big picture.

EIP-4844 brings important changes to @ethereum's base layer that fundamentally reorients the system towards the rollup-centric future.

(16/25) Instead of using "calldata," storage which persists on-chain forever, rollups will be able to post bundles under a new transaction type.

This transaction will carry a blob, a large amount of data - inaccessible by the EVM - which is much cheaper than calldata.

(17/25) Blobs are 10x larger than blocks, but they are pruned out of the blockchain after ~a month. A new data-availability layer will arise, and the scalability of the system increases by an order of magnitude.

EIP-4844 also creates a separate fee market for these transactions.

(18/25) The result will be a tailored data layer – regular transactions and blobs will get distinct fee markets with independent gas prices.

So even if some NFT project is blowing up gas fees, your rollup data costs won't go up (though settlement costs would).

(19/25) As the name suggests, proto-danksharding is a step on the road to Danksharding which will unlock huge amounts of @ethereum's scalability.

EIP-4844 creates a channel for data, danksharding uses data sampling tech to reduce the resources system uses to validate it.

(20/25) From here, development gets complicated. In order to implement danksharding, we need to make another change to the @ethereum core-protocol.

Essentially, we need to separate out a core function of an Ethereum node: block building.

(21/25) Danksharding requires incredibly sophisticated and complex computation to prepare data samples for blocks that are ready for validation.

Implementing danksharding into today's nodes would require advanced, expensive machines... not great for centralization.

(22/25) The solution, originally proposed for MEV research, is to separate block building from the action of proposing the block to the @ethereum network.

Block builders can specialize in sophisticated block making (as danksharding requires) with Ethereum remains decentralized.

(23/25) As proto-danksharding gets rolled out with EIP-4844, Protocol-Builder Separation (PBS) is being prototyped via Flashbot's mev-boost.

This product is the first block builder-proposer marketplace; eventually, PBS will be enshrined at the protocol level.

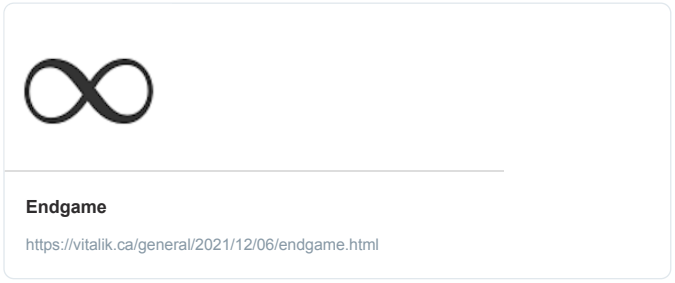
(24/25) After enshrined PBS, danksharding can be deployed in full. When initially activated, it will instantly scale proto-danksharding by 10+. From there, @ethereum's data availability can scale indefinitely

Now we are in 2025+... Ethereum has gone from 15 txns/sec to 100k plus

(25/25) This is the @ethereum endgame:

Execution and user interaction has been pushed out to layer 2s and beyond. Mainnet provides incredible economic security and unimpeachable neutrality.

...and $ETH is the glue that binds it all together.



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.

• • •