



Haym @SalomonCrypto

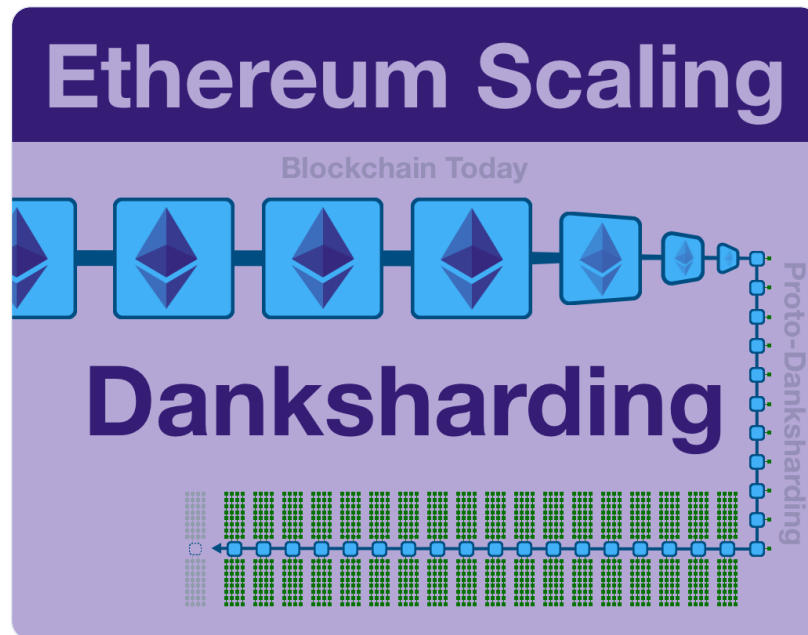
Oct 27 · 31 tweets · [SalomonCrypto/status/1585441288341508096](https://twitter.com/SalomonCrypto/status/1585441288341508096)

(1/30) [@ethereum](https://twitter.com/ethereum) Roadmap: Danksharding

From A to KZG, a comprehensive guide to the post-Merge roadmap of the World Computer:

- Proto-Danksharding (EIP-4844)
- Proposer-Builder Separation (PBS)
- Danksharding

A megathread deep-dive on decentralized scalability.



(2/30) [@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).

These nodes are real computers in the real world, communicating directly from peer to peer.



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](#)

 958  Reply  Copy link

[Read 45 replies](#)

(3/30) As of mid-September, [@ethereum](#) has switched its consensus mechanism from Proof of Work to Proof of Stake (PoS).

Tl;dr node operators stake \$ETH to gain the role of validator, earning \$ETH and securing Ethereum. If the operator acts maliciously, he forfeits his stake.

**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.



The graphic features a blue header with the text 'Ethereum Consensus'. Below this, on a dark blue background, is a circular grid of light blue dots with a dark blue diamond shape in the center. To the right of the grid, the text 'Proof of Stake' is written in white, with 'of' in a smaller font. Below the text is a white icon of two hands shaking.

10:07 PM · Oct 10, 2022 

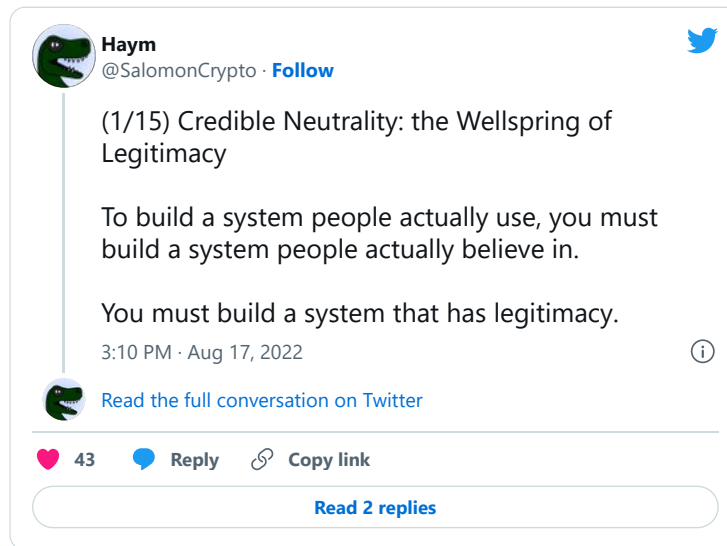
 [Read the full conversation on Twitter](#)

 209  Reply  Copy link

[Read 13 replies](#)

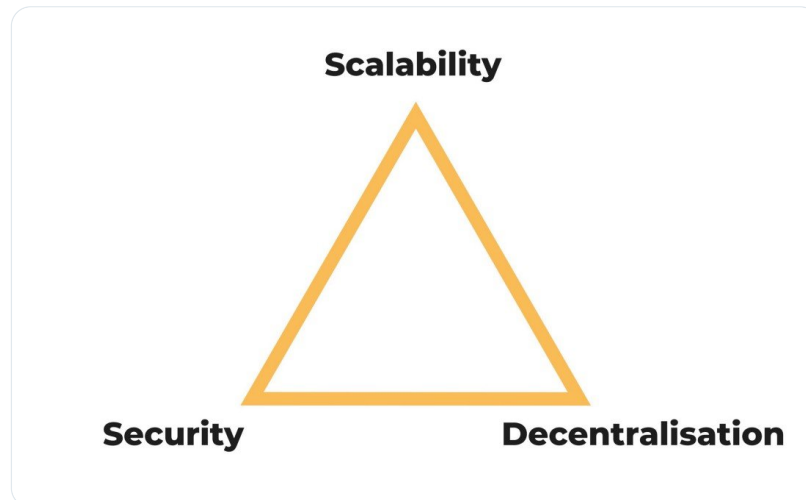
(4/30) At the end of the day, real computers need to run the [@ethereum](#) software. And so, the World Computer is limited by the min requirements it sets for nodes.

Our primary goal: credible neutrality through decentralization. If we lose \$ETH decentralization, we lose everything.



(5/30) Enter the Scalability Trilemma. The classic framing goes "A blockchain can only have two of these three properties: scalability, security and decentralization."

But [@VitalikButerin](#), [@dankrad](#) and the gigabrain of [@ethereum](#) just reject the framing.




(6/30) [@ethereum](#) PoS delivers incredible security, both through direct economic implications and through the defensive mechanisms built into PoS.

And Ethereum is decentralization maxi; full nodes can run in your girlfriend's closet, taking ~1 hr/month (based on experience).

(7/30) Scalability is where things get interesting. After years of research, [@ethereum](#) has solved the execution problem: move it off-chain!

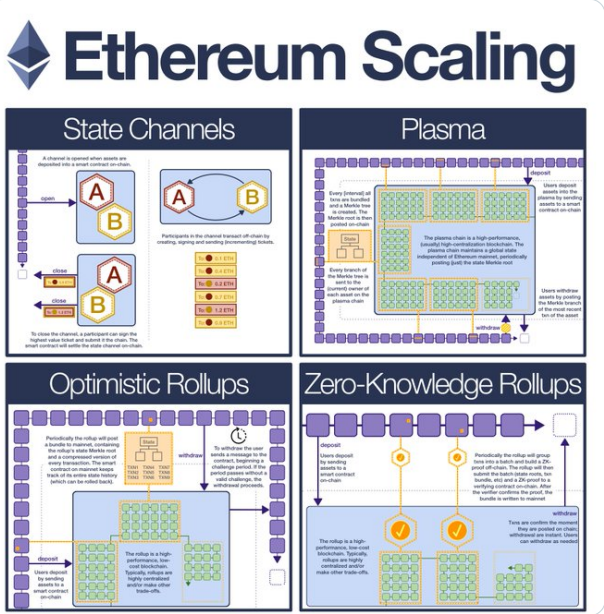
Tl;dr Rollups are independent, high performance blockchains that settle to Ethereum.

 **Haym**
@SalomonCrypto · Follow

(1/15) [@ethereum](#) Scaling Technology

State Channels → Plasma → Optimistic Rollups → ZK-Rollups

Your guide to the technologies that will scale Ethereum from 12 to 100,000 txns/sec... at a lower cost than you pay today!



Ethereum Scaling

State Channels

A channel is opened when users are depicted into a smart contract on-chain.

Participants in the channel transact off-chain by creating, signing and submitting transactions.

To close the channel, a participant can sign the highest value state and submit it to the chain. The smart contract will settle the state channel accordingly.

Plasma

Every transaction on the main chain is hashed and stored in a Merkle tree. The Merkle tree is a data structure that stores data in a hierarchical manner. The Merkle tree is used to verify the integrity of the data.

The plasma chain is a high-performance, low-cost blockchain. It is a decentralized system that allows users to transact off-chain and settle on-chain.

Optimistic Rollups

Periodically the rollup will send a bundle to the main chain, containing the rollup state, the rollup state root, and a commitment to the rollup state.


To withdraw the user sends a message to the rollup, requesting a withdrawal. The rollup will then submit the withdrawal to the main chain.

Zero-Knowledge Rollups

The rollup is a high-performance, low-cost blockchain. It is a decentralized system that allows users to transact off-chain and settle on-chain.

There are no state roots. The rollup will submit the state root to the main chain. The rollup will then submit the state root to the main chain.

11:04 PM · Sep 12, 2022

 [Read the full conversation on Twitter](#)

❤️ 801 ⚡ See the latest COVID-19 information on Twitter

[Read 17 replies](#)

(8/30) Settlement is a loaded word that gets thrown around a lot, so let's make this simple.

Settlement refers to the ultimate source of ownership. When things go wrong, the place you go to get your stuff.

Rollups compute off-chain and then post a record on to [@ethereum](#).

(9/30) Today, we're still in the infancy of rollup technology and even still we're seeing execution time and cost drop orders of magnitude.

But rollups only address the execution problem. In fact, as they scale they will create enormous amounts of data.



(10/30) If we were to stop here, the World Computer would still be the most secure, fastest smart contract platform on the planet... but the cost of posting data might be too expensive for anything but the highest value financial txns.

Fortunately, we are not going to stop here.

(11/30) < NOTE >

The subjects beyond this tweet are the active development-part of the [@ethereum](#) roadmap. Implementations WILL change. Details WILL change. I am confident that some of this is already out of data.

We do, however, know A LOT about what's coming...

< /NOTE >

(12/30) Rollup development will continue and even accelerate, but this activity will be increasingly taken up by private companies.

The [@ethereum](#) core devs will focus on data scalability through a 3 part plan:

- 1) Proto-Danksharding (EIP-4844)
- 2) Enshrined PBS
- 3) Danksharding



(13/30) The first step - Proto-Danksharding - does a lot of the preparation for Danksharding. Interestingly, Proto-Danksharding is named after people ([@protolambda](#) & [@dankrad](#)), but it works descriptively.

The most important thing to understand about Proto-Danksharding is blobs.

(14/30) Today, we post data to the blockchain by passing it into a smart contract through the "calldata" field. This is a field that is intended for code and other data to be passed into the EVM. Therefore, Rollups post their receipts INTO the EVM.

But... do they need to?

(15/30) Let's consider a (hypothetical) ZK-rollup. The rollup bundles txns, creates a ZK-proof (ensuring the batch is valid and final) and posts it on-chain.

Once on-chain, the EVM never needs to access this data. The important thing is just that it is publicly available.

Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(19/23) Once every [interval], the rollup operator will bundle the previous transactions and build a ZK-proof (off-chain). It will then submit the batch and the proof to a verifying contract on-chain. If the contract accepts the proof, the batch is finalized instantly.

Blockchain Scaling

Zero-Knowledge Rollups

The diagram illustrates the Zero-Knowledge Rollups process. At the top, a sequence of purple blocks represents transactions on the mainnet. A dashed line separates the mainnet from the rollup. Below the mainnet, a blue box represents the rollup. Inside the rollup, green blocks represent transactions. A yellow box with a checkmark indicates a batch of transactions being processed. A yellow arrow points from the batch to the mainnet, representing the submission of the batch and the ZK-proof. A yellow arrow points from the mainnet to the rollup, representing the withdrawal process. Text labels include: 'deposit' (Users deposit by sending assets to a smart contract on-chain), 'Periodically the rollup will group txns into a batch and build a ZK-proof off-chain. The rollup will then submit the batch (state roots, txn bundle, etc) and a ZK-proof to a verifying contract on-chain. After the verifier confirms the proof, the bundle is written to mainnet', 'The rollup is a high-performance, low-cost blockchain. Typically, rollups are highly centralized and/or make other trade-offs.', and 'withdraw' (Txns are confirmed the moment they are posted on-chain, withdrawal are instant. Users can withdraw as needed).

2:40 PM · Sep 12, 2022

7 ❤️ Reply Copy link

Read 1 reply

(16/30) This is the idea behind blobs: huge amounts of data (think 10x the size of blocks), inaccessible to the EVM, that are MUCH cheaper than the old way (calldata).

Blobs will get their own independent gas market; the supply/demand of execution gas will not affect data gas.

(17/30) Proto-Danksharding introduces blobs (including the independent gas market) to [@ethereum](#) via a new transaction type. Post EIP-4844, proposers will be able to attach a single blob to the blockchain.

A single blob that every node will have to download.

(18/30) The transition from Proto-Danksharding to Danksharding involves two important changes:

- available blobs per block will increase from 1 to 64 (as of now)
- blob data will be distributed across the network, so that no single node needs to download them all

(19/30) This increase from 1 to 64 blocks is massive, both in terms of network data capacity but also in terms of the computational power needed to build them. A [@ethereum](#) node with minimum specs couldn't realistically keep up with a professional operation.

(20/30) Fortunately, we already have a solution for these types of problems: protocol enshrined Proposer-Builder Separation (PBS).

The concept was born out MEV research but maps perfectly to our problem. We simply separate the action of building and proposing a block.

 **Haym**
@SalomonCrypto · Follow

(1/26) [@ethereum](#) Roadmap: Proposer-Builder Separation

The Merge was successful, [\\$ETH](#) is Proof of Stake! As the era of miners closes, we find ourselves entering a new meta: the age of MEV

Your guide to existential threat facing Ethereum... and the plan to vanquish it



11:38 PM · Sep 15, 2022

 [Read the full conversation on Twitter](#)

517 Reply Copy link


[Read 11 replies](#)

(21/30) With PBS, node min spec remains low, we get the benefits of centralized performance and we maintain decentralization. Builders will create blocks/blobs, bidding for inclusion.

And, of course, nodes will always be able to be built solo (they just won't earn optimal fees).


(22/30) PBS gives us the ability to propose our blobs, but we still need to address our biggest problem: how can we achieve 100% data availability without forcing any nodes to download 100% of the data.

Well, we'll just distribute it across the P2P network!



Haym

@SalomonCrypto · Follow

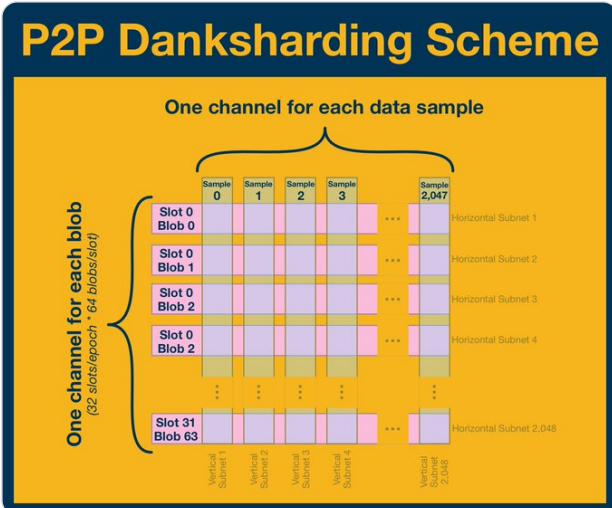


(1/24) @Ethereum Roadmap: Peer-to-Peer Networking


In order to achieve the vision of the World Computer, Ethereum needs more data bandwidth. But more bandwidth = higher node requirements = centralization. So what's the path forward?


Let's look into the future of the P2P network.


P2P Danksharding Scheme




10:57 PM · Oct 25, 2022

[Read the full conversation on Twitter](#)

 328

 Reply

 Copy link


[Read 23 replies](#)

(23/30) More detail above, but here's what's important: each node will download just a small data sample from each blob. Upon request, the network will be able to quickly/efficiently reconstruct a blob.

We've just got one final question: how can we securely sample the data?

(24/30) If you've made it this far, you've found the nugget of gold at the center, the true magic: KZG Polynomial Commitments.

TL;DR KZG Commitments use elliptic curve cryptography to commit to the data in VERY useful way.

 **Haym**
@SalomonCrypto · [Follow](#)

(1/24) KZG Polynomial Commitments: The Complete Guide


Our goal: 1) prove we are committed to a specific set of data and 2) allow others to verify specific points within that dataset.



Want to see some mathematical magic? This megathread is for you!

KZG Commitment Scheme


First, the prover commits to data by creating a point on the elliptic curve. If the data changes, the prover cannot create valid proofs.

Prover

1)  Commit

3)   Proof Evaluation

Verifier

2)  Request


Next, the verifier gives a data point. The prover builds a new elliptic curve point and a polynomial evaluation around that point.




KZG Proof Verification

$$e([S - z], [h(S)]) \stackrel{?}{=} e([f(S)] - f(z), [1])$$
$$\downarrow$$
$$e([S - z], [\text{Z}]) \stackrel{?}{=} e([\text{Anchor}] - f(z), [1])$$

Calculated by verifier Proof Commit Evaluation

6:25 AM · Oct 22, 2022

 [Read the full conversation on Twitter](#)

 193  Reply  Copy link

[Read 6 replies](#)

(25/30) Underneath some intimidating (but doable, try the thread above) math, KZG commitments are simple:

- 1) commitment is made to specific data
- 2) a node can "open" the commitment at any point
- 3) the prover sends the data and a proof of validity
- 4) the node verifies the proof

(26/30) It's creating the KZG commitments and proofs for 64 blobs in a single slot timeframe (12 sec) that is particularly intense and will require a centralized actor.

But, again, a node can do all of this itself. It just (probably) won't be able to fill all the blob spaces.

(27/30) Now look, at the end of the day we are putting a HUGE amount of data onto [@ethereum](#). The P2P design is cute, but eventually this will catch up to us.

The solution is blob expiry. After ~a month, nodes will be allowed to delete the samples they have collected.

(28/30) The nature of [@ethereum](#) will change; instead of a permanent database, think public notice board. ~1 month for archive nodes, [@etherscan](#) and others to grab everything for perpetuity.

But don't worry... the KZG commitment will always be available on-chain to verify data.

(29/30) Finally, Danksharding will require upgrades to [@ethereum](#) consensus and the network.

Again, Proto-Danksharding does a lot of this work. The actual Danksharding upgrade is much more about the implementation of KZG commitments, P2P storage and other non-consensus changes.



(30/30) The road from today to Danksharding is long, winding and largely unknown. In fact, it will definitely change, but we know the landmarks to search for:

- Proto-Danksharding (EIP-4844)
- PBS
- Danksharding

Just keep paying attention, things are happening quickly!

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](#)



(1/30) [@ethereum](#) Roadmap: Danksharding

From A to KZG, a comprehensive guide to the post-Merge roadmap of the World Computer:

- Proto-Danksharding (EIP-4844)
- Proposer-Builder Separation (PBS)
- Danksharding

A megathread deep-dive on decentralized scalability.



The diagram illustrates the Ethereum scaling roadmap. At the top, a purple banner reads 'Ethereum Scaling'. Below it, a horizontal sequence of blue blocks represents the 'Blockchain Today' state. This sequence transitions into a vertical stack of green blocks labeled 'Proto-Danksharding' on the right side. The main title 'Danksharding' is prominently displayed in the center. At the bottom, a horizontal line of blue blocks represents the 'Danksharding' state, which is connected to the vertical stack of Proto-Danksharding blocks.

1:20 AM · Oct 27, 2022 

 [Read the full conversation on Twitter](#)

 470  Reply  Copy link

[Read 16 replies](#)

...