



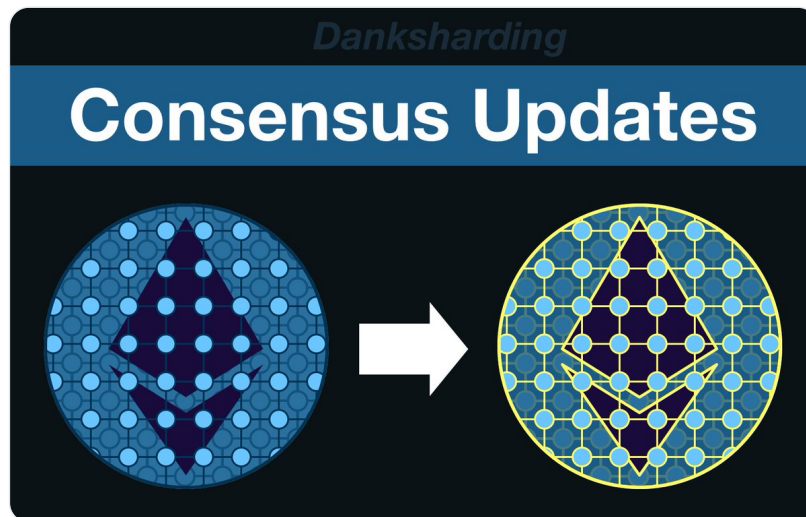
Haym @SalomonCrypto

Oct 26 · 26 tweets · [SalomonCrypto/status/1585298274478542848](https://twitter.com/SalomonCrypto/status/1585298274478542848)

(1/25) [@ethereum](https://twitter.com/ethereum) Roadmap: [Potential Danksharding]
Consensus Updates

Today, Ethereum is not scalable, but there is a clear path from "a big blockchain" to The World Computer, and let me tell you... it is DANK.

Let's talk about the changes we need to make to consensus.



(2/25) [@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](#)

937 Reply Copy link

(3/25) As of mid-September 2022, [@ethereum](#) has switched its consensus mechanism to Proof of Stake (PoS).

Tl;dr node operators stake \$ETH in order to gain the role of validator, earn rewards and secure Ethereum. This stake can be deducted from in cases of malicious behavior.



The image is a screenshot of a tweet from a user named Haym (@SalomonCrypto). The tweet is dated (1/29) and is part of a series titled '@ethereum Fundamentals: Proof of Stake'. The text of the tweet explains that Ethereum is now secured by validators, with 32 \$ETH required at a time. It notes that while PoS is simple at first glance, it becomes more complex under the hood. The tweet includes a link to 'The ultimate guide to the consensus mechanism at the core of the World Computer.' Below the text is a graphic with a blue header 'Ethereum Consensus'. The graphic features a circular grid of blue dots with a dark blue diamond shape in the center, and the text 'Proof of Stake' next to an icon of two hands shaking. The tweet was posted at 10:07 PM on Oct 10, 2022, and has 206 likes. There are options to 'Read the full conversation on Twitter', 'Reply', and 'Copy link'. A 'Read 13 replies' button is also visible.

(4/25) Today, the World Computer is SLOW. The EVM is not a high performance environment, both execution and storage is expensive and we already push up against the limits of [@ethereum](#).

And so, we must look for (credibly neutral) ways to scale.

(5/25) After years of research and development, the [@ethereum](#) community has found the best path forward: rollups.

Rollups are independent, high performance blockchains that settle to Ethereum. Rollups can be fast (and centralized) and STILL benefit from Ethereum security.

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 assets are deposited into a smart contract on-chain. Participants in the channel deposit all data for trading, signing and sending (transactional) data. To close the channel, a participant can sign the highest value (final) request. This state, the state transition, is published on-chain.
- Plasma:** Every Ethereum off-chain transaction and a Merkle tree is deposited. The Merkle tree is published on-chain. Every branch of the Merkle tree is used to generate a proof of the current state of each asset on the plasma chain. Users withdraw assets by sending the Merkle branch of the asset to the mainnet.
- Optimistic Rollups:** Periodically the rollup will post a block to the mainnet, containing the value of state blocks on-rollup and a compressed version of every transaction. The smart contract on the mainnet keeps track of all state state changes (which can be rolled back). To withdraw the user sends a challenge to the rollup, requiring a valid challenge, the withdrawal proceeds.
- Zero-Knowledge Rollups:** Users deposit the funding amount to the smart contract on-chain. Periodically the rollup will group users into a batch and build a zk-rollup (blockchain). The rollup will then bundle on-chain data, the bundle will send a zk-proof to the mainnet. The rollup will then bundle on-chain data, the bundle is written to mainnet. Users can withdraw on-chain. Data are posted on-chain, withdrawal on mainnet. Users can withdraw on mainnet.

11:04 PM · Sep 12, 2022

[Read the full conversation on Twitter](#)

791 [See the latest COVID-19 information on Twitter](#)

[Read 17 replies](#)

(6/25) But rollups are only part of the solution; while they provide an incredible performance environment, they do not scale the storage capabilities of [@ethereum](#).

In fact, because they are so fast (generating so much data) rollups make the problem worse.

(7/25) As of today, we have a plan: Danksharding. But we are still so far away from implementation and a lot of details need to be filled in.

So, let's begin with the big picture idea. We'll begin with blobs.

(8/25) Imagine the blockchain like a database that contains all the transactions that have ever happened on the World Computer. It is critical that this information is always directly available to any node; this is the internal state of [@ethereum](#).

(9/25) Rollups, on the other hand, are completely outside of [@ethereum](#). Yes, they settle (post a reconstructable copy of all transactions) on the World Computer, but that's just a copy.

It's NOT important that nodes can directly access this data.

(10/25) What IS important is that we can guarantee that this data was posted to [@ethereum](#), is completely public and request-able by anyone and is 100% available for download.

So this is our design space: data blobs that exist outside of the EVM.

(11/25) Today, tomorrow and forever it will be 100% necessary for every node to download every block. But our new scheme will not force every node (or even any single node) to download all the data, just to ensure that the data is available in aggregate across the entire network.

(12/25) We can achieve this effect with some clever peer-to-peer (P2P) networking design.

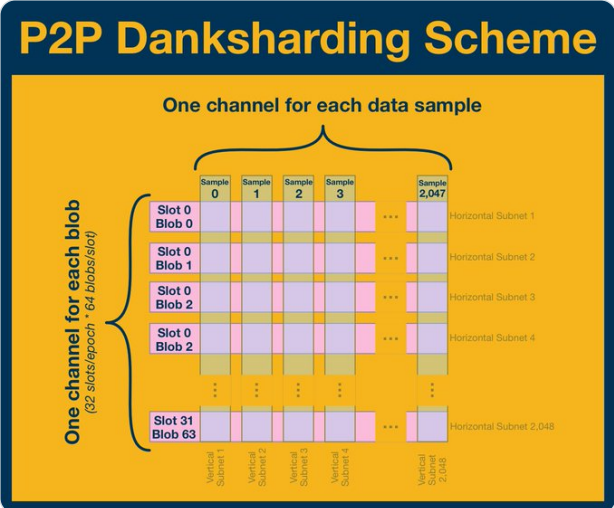
Tl;dr in P2P networks nodes communicate directly with each other (instead of a centralized node). We can organize a network to store huge amounts of data without crushing any single node.

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.



The diagram, titled "P2P Danksharding Scheme", illustrates a data distribution model. It features a grid where columns represent "Sample" (0, 1, 2, 3, ..., 2,047) and rows represent "Slot" and "Blob" (e.g., Slot 0 Blob 0, Slot 0 Blob 1, ..., Slot 31 Blob 63). A bracket on the left indicates "One channel for each blob (32 slots/epoch * 64 blobs/slot)", showing that each blob is replicated across 32 slots. A bracket at the top indicates "One channel for each data sample", showing that each sample is replicated across all slots. The grid is divided into "Vertical Subnets" (1-4, ..., 2,048) and "Horizontal Subnets" (1-4, ..., 2,048).

10:57 PM · Oct 25, 2022

[Read the full conversation on Twitter](#)

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

[Read 18 replies](#)

(13/25) Good news and bad news:

Bad news: this is going to require some big changes to [@ethereum](#)... especially in the consensus mechanism.

Good news: a huge amount of the work is coming early in EIP-4844 (Proto-Danksharding).



(14/25) EIP-4844 will deliver the following changes to [@ethereum](#) consensus:

- data blobs with an independent gas market
- changes needed at the intersection between execution and consensus
- separation between block verification and blob data availability verification

(15/25) EIP-4844 is a huge step forward, creating the blob market and making all the changes needed to the execution layer of [@ethereum](#).

But there is still a lot of work that needs to be done, and a lot of designs that need to be finalized.

(16/25) The biggest obstacle we still need to overcome is the actual implementation of the erasure coding and the data availability sampling that is foundational to our P2P network design.

It doesn't matter how complete the architecture without the actual process of sampling.

(17/25) < NOTE >

We also still need to formalize the implementation of the KZG commitment scheme (theory/math is well understood).

We haven't discussed how KZG commitments will be used in Danksharding (yet), but just including now for completeness.

< /NOTE >

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
- 2) Request
- 3) Proof Evaluation

Verifier

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

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

Calculated by verifier Proof Commit Evaluation

6:25 AM · Oct 22, 2022

[Read the full conversation on Twitter](#)

184 Reply Copy link

[Read 5 replies](#)

(18/25) Full Danksharding is dependent on another, independent [@ethereum](#) upgrade: enshrined-PBS.

Although PBS was originally conceived in the context of MEV, it will become incredibly important for Danksharding.

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](#)

514 Likes · Reply · Copy link

[Read 11 replies](#)

(19/25) It turns out that a lot of the work that will go into constructing a blob is pretty computationally intense and will (probably) be unrealistic for a minimal [@ethereum](#) node.

PBS will allow blob builders to centralize and specialize without compromising on security.

(20/25) A future with both PBS and Danksharding might look like this:

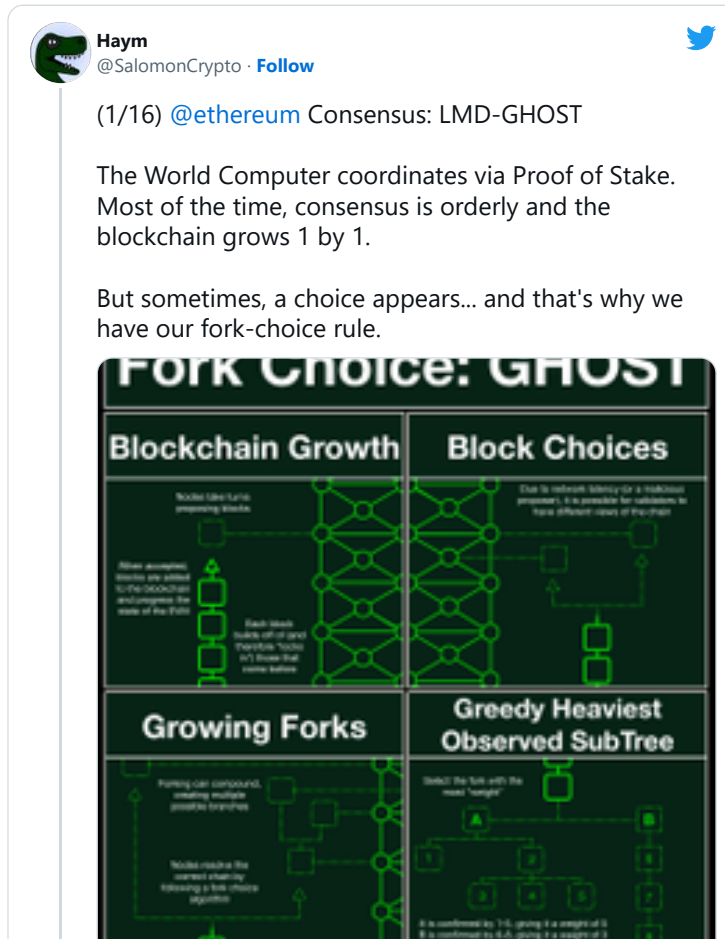
- 1) validator selected as a block proposer
- 2) proposer selects highest value block from block market
- 3) proposer selects highest value blobs from the blob market
- 4) proposer proposes the block/blobs combo

(21/25) This workflow assumes a robust block and blob market, with at least 2 honest competitors bidding for proposer selections.

But, in the worst case, the validator can just build their own. It's just both the blocks will be suboptimal and the blobs will not be filled.

(22/25) Another important aspect of [@ethereum](#) PoS that needs to change is the fork-choice rule.

Today, LMD-GHOST only looks at blocks. Under Danksharding, the protocol will also need to consider blobs (although some/all of this logic may be released with EIP-4844).



(23/25) The new rule introduces the concept of "tight coupling" which states that a block is only eligible if all blobs in that block have passed a data availability check.

With tight coupling, if the chain contains even a single invalid blob, the entire chain is invalid.

(24/25) The rest of the changes needed are less interesting and more about implementation. Things like "which fields need to be added to blocks" and "how to distribute validators when validator count is unreasonably low."

But if you've made it this far, you get the big picture.


(25/25) [@ethereum](#) is the World Computer, and today the World Computer is SLOW and EXPENSIVE...

...today.

Just keep looking forward anon, you don't want to miss what's coming

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](#) 

(1/25) [@ethereum](#) Roadmap: [Potential Danksharding] Consensus Updates

Today, Ethereum is not scalable, but there is a clear path from "a big blockchain" to The World Computer, and let me tell you... it is DANK.


Let's talk about the changes we need to make to consensus.



The diagram is titled "Danksharding Consensus Updates". It features two circular diagrams representing consensus mechanisms. The left diagram shows a single large diamond shape composed of many small blue circles, representing a traditional Proof of Work consensus. The right diagram shows a more complex structure with a central diamond shape and multiple smaller diamonds branching out, representing a sharded consensus mechanism. A white arrow points from the left diagram to the right diagram, indicating a transition or update.

3:52 PM · Oct 26, 2022 

 [Read the full conversation on Twitter](#)

 5  Reply  Copy link

[Read 1 reply](#)

...