



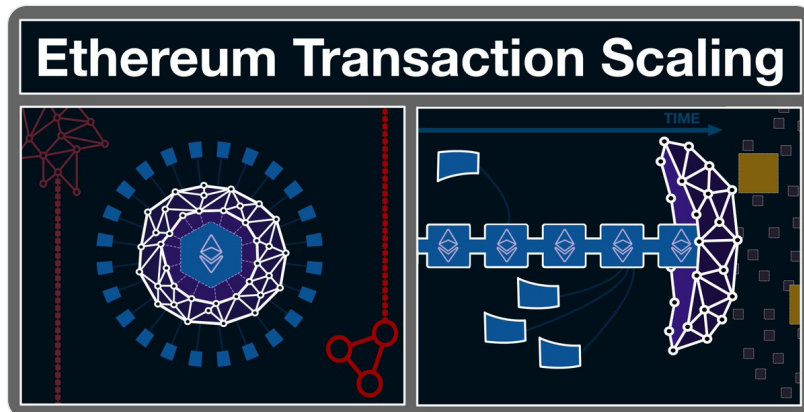
Haym @SalomonCrypto

Nov 13 · 24 tweets · [SalomonCrypto/status/1591614638138875905](https://twitter.com/SalomonCrypto/status/1591614638138875905)

(1/23) [@ethereum](https://twitter.com/ethereum) Roadmap: Scaling Execution

\$ETH is inevitable; I am more confident today than I have ever been. But let's face facts: Ethereum is SLOW and EXPENSIVE. How will the World Computer scale?

Your guide to Rollups, Danksharding, PBS and more!



(2/23) [@ethereum](#) is a distributed computing platform. A network of 1,000s of computers (nodes) coordinating using Proof of Stake (PoS) to keep the Ethereum Virtual Machine (EVM) in sync.

The EVM is the shared computing platform, the blockchain its history and \$ETH its lifeblood.

 **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](#)

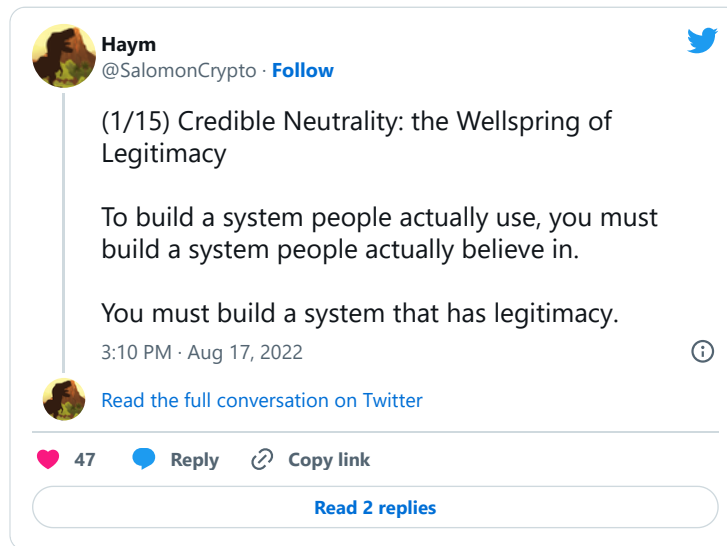
---

 993  Reply  Copy link

[Read 47 replies](#)

(3/23) This "network of nodes" is the foundation upon which [@ethereum](#) ultimately derives its value. The more decentralized, the more value.

From decentralization comes credible neutrality. Without credible neutrality, we might as well be using FB-dollarroos in Farmville-DeFi.



(4/23) Today, the World Computer is slow and expensive to use. Raising the minimum requirements of a node would improve both the execution and associated costs.

But raising requirements is the opposite of decentralization: higher requirements = higher costs = less participants.

(5/23) And here is where the phrase "World Computer" might actually be more confusing than helpful...

Today, [@ethereum](#) is a complete computing platform, but this is not its final state.

What we are really building is like a huge, completely unalterable public notice board.

(6/23) The core at the center of [@ethereum](#) is the EVM, specifically that the EVM has native property rights.

Ethereum will be the global settlement layer. Applications (centralized or not) will compute elsewhere and simply post proof back to Ethereum.




(7/23) Let's say Alice enters into a computationally difficult transaction. Both parties want to settle to [@ethereum](#), so that ultimate ownership exists and is transferred on Ethereum mainnet.

But the computation itself? Well that can be done by basically anyone.

(8/23) This is the core idea behind [@execution](#) transaction scaling: move execution off-chain, retain settlement on-chain.

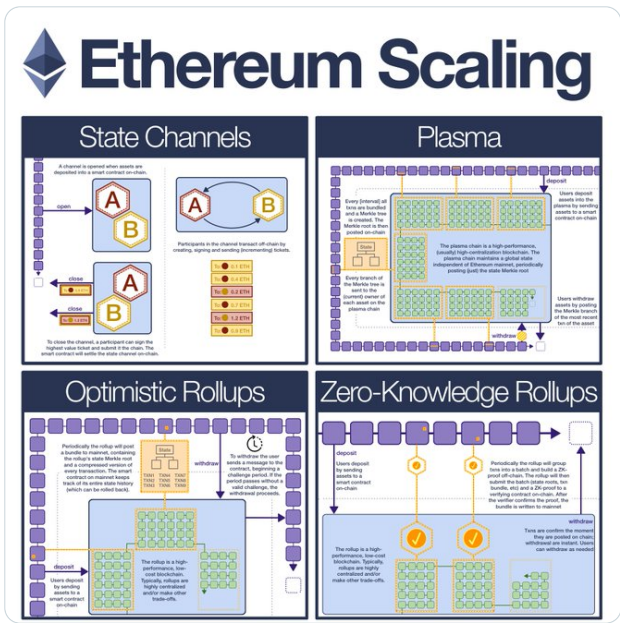
Moving execution off-chain is easy, we can use performance-tuned blockchain (or even [@aws](#)). The trick is settlement.

 **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 execute all trades by signing, signing and sending transactional data.  
To close the channel, a participant can sign the highest value deposit request. This state, the state transition, is posted back on-chain.


**Plasma**  
Every Ethereum off-chain transaction and a Merkle tree commitment, the commitment, are posted on-chain.  
The plasma chain is a high-performance, fault-tolerant, high-availability blockchain. The plasma chain is a general state independent of Ethereum network, periodically posting back the state Merkle root.  
Users withdraw assets by sending the Merkle branch of the state Merkle root of the state transition.

**Optimistic Rollups**  
Periodically the rollup will post a block to Ethereum, containing the value of state Merkle root and a compressed record of every transaction. The smart contract on Ethereum keeps track of all state state transition (which can be rolled back).  
To withdraw the user sends a challenge to the rollup, requesting a state challenge, if the smart contract returns a valid challenge, the rollup is rolled back.  
The rollup is a high-performance, fault-tolerant, high-availability blockchain. The rollup is a general state independent of Ethereum network, periodically posting back the state Merkle root.  
Users withdraw assets by sending the Merkle branch of the state Merkle root of the state transition.

**Zero-Knowledge Rollups**  
Users deposit the funding amount to the smart contract.  
Periodically the rollup will group users into a batch and build a zk-rollup (zk-rollup). The rollup will send the batch, and send a zk-proof to the Ethereum network. The rollup is a high-performance, fault-tolerant, high-availability blockchain. The rollup is a general state independent of Ethereum network, periodically posting back the state Merkle root.  
Users withdraw assets by sending the Merkle branch of the state Merkle root of the state transition.

11:04 PM · Sep 12, 2022

 [Read the full conversation on Twitter](#)

808  See the latest COVID-19 information on Twitter

[Read 18 replies](#)

(9/23) After a few attempts, we've aligned on the best path forward: rollups.

A rollup is a blockchain that posts a full record of itself onto [@ethereum](#) mainnet. With this record, users can permissionlessly withdraw (even if the rollup is offline or acting maliciously).

(10/23) Rollups ARE the path forward to >100k transactions per second, but they are not the entire solution.

Let's break [@ethereum](#) transaction costs into two buckets: execution and data storage.

Rollups solve execution, but they only make data storage worse.

(11/23) Tl;dr in order to ACTUALLY settle to [@ethereum](#), rollups need to post a record of every transaction. We can greatly compress them (getting good data storage gains), but we still need a record.

As rollups make execution cheaper, data storage becomes a bigger problem.



**Haym**  
@SalomonCrypto · Follow

(1/25) [@ethereum](#) Roadmap: Data Availability

The World Computer has a long road before it is ready to be the globe's premier settlement layer. Rollups will scale execution, quickly revealing a new bottleneck.

Before we talk solutions, let's define the data availability problem.

3:39 PM · Sep 18, 2022

[Read the full conversation on Twitter](#)

94   Reply   Copy link

[Read 3 replies](#)

(12/23) Fortunately, we have a solution: Danksharding (named after [@dankrad](#)).

Danksharding creates a new [@ethereum](#) data structure tailor-made for rollups: a blob. A blob is simply a huge, cheap storage container that cannot be accessed by the EVM.



The image is a screenshot of a Twitter post. At the top left is the user's profile picture and name 'Haym' with the handle '@SalomonCrypto' and a 'Follow' button. The tweet text reads: '(1/30) @ethereum Roadmap: Danksharding' followed by 'From A to KZG, a comprehensive guide to the post-Merge roadmap of the World Computer:' and a bulleted list: '- Proto-Danksharding (EIP-4844)', '- Proposer-Builder Separation (PBS)', and '- Danksharding'. Below the text is a link to a megathread. The main content is a graphic titled 'Ethereum Scaling' with a subtitle 'Blockchain Today'. The graphic shows a sequence of blue blocks representing transactions, with the last one being a 'Proto-Danksharding' block that branches into a vertical chain of smaller blocks. Below this, the word 'Danksharding' is written in large letters, with a diagram showing a horizontal chain of blocks connected to a vertical chain of blocks, representing the integration of rollups into the main chain.

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.

**Ethereum Scaling**  
Blockchain Today

**Danksharding**

1:20 AM · Oct 27, 2022

Read the full conversation on Twitter

489 Reply Copy link

Read 18 replies


(13/23) Here's an analogy: imagine [@ethereum](#) is a train company and rollup data is cargo.

Before Danksharding, the cargo needed to go in the passenger cabin, paying passenger pricing.

After, the cargo can go in its own separate car, but the train company can't monitor it.

(14/23) Danksharding is a huge upgrade and needs to be approached in phases.

Phases 1 is Proto-Danksharding (named for [@protolambda](#) and Danksharding), which will make the changes needed to support a single blob (per block) and create an independent gas market just for blobs.



A screenshot of a Twitter post from user Haym (@SalomonCrypto). The tweet is the first in a thread of 25 parts. The text discusses Ethereum's scalability roadmap, mentioning the Merge, EIP-4844 (proto-danksharding), Enshrined PBS, and Danksharding. The tweet has 595 likes and 29 replies. The interface includes a profile picture, a follow button, a retweet icon, and a link to read the full conversation.

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

(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

4:51 AM · Aug 16, 2022

[Read the full conversation on Twitter](#)

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

[Read 29 replies](#)



(15/23) Phase 2 is enshrined PBS, an upgrade that was first developed from MEV research.

Full Danksharding requires so much computation that it would compromise the decentralization of @ethereum. Fortunately, we can limit this to block building and maintain decentralization.

**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](#)

531 Likes   Reply   Copy link

[Read 11 replies](#)

(16/23) Phase 3: Danksharding.

To achieve full Danksharding, first we need to implement a data sampling scheme that will distribute blobs across the network. The purpose is to ensure that no node has to download every single blob while still guaranteeing all data is available.

(17/23) Once the data has been distributed across the network, we can increase the amount of data @ethereum can accept. We will increase the amount of blobs from 1 to 64 blobs per block.

At 64 blobs we are done; Danksharding will be fully deployed.

(18/23) Before we head out, let's do some SUPER rough calculations. If I am being honest, I have serious questions about anything more precise than this.

Today, @ethereum does ~25 transactions per second.

[ethstats.info](https://ethstats.info)

(19/23) First, let's consider what a high performance rollup might look like.

Lot's of good projections to pull from, but I think we should just look at real world examples.

[@solana](#) claims 50k txs/sec, but that seems high. Let's just drop it down to 5k txs/sec.

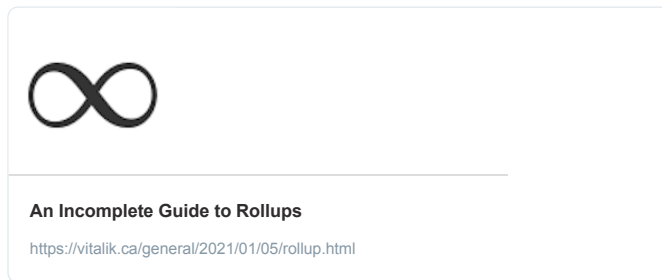
(20/23) Now let's look at data storage.

Today, an [@ethereum](#) block is limited to 1MB. This space must be shared between EVM and rollup transactions.

Full Danksharding is spec'ed at 16MB per block JUST for rollups.

(21/23) Final piece: how much storage space does a rollup transaction take?

Fortunately, [@VitalikButerin](#) answered that for us in this blog post:



Let's use the biggest number, 296 bytes.

Here's a chart for some other example use cases:

Application	Bytes in rollup	Gas cost on layer 1	Max scalability gain
ETH transfer	12	21,000	105x
ERC20 transfer	16 (4 more bytes to specify which token)	~50,000	187x
Uniswap trade	~14 (4 bytes sender + 4 bytes recipient + 3 bytes value + 1 byte max price + 1 byte misc)	~100,000	428x
Privacy-preserving withdrawal (Optimistic rollup)	296 (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient + 256 bytes ZK-SNARK proof)	~380,000	77x
Privacy-preserving withdrawal (ZK rollup)	40 (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient)	~380,000	570x

Max scalability gain is calculated as (L1 gas cost) / (bytes in rollup \* 16) \* 12 million / 12.5 million.

(22/23) Putting this together:

16 MB per block / 296 bytes per txn = 54k txn per block

[@ethereum](#) could support 54k txns without even moving the (new blob) gas market.

That's basically the equivalent of 10 [@solana](#), all paying pennies on the dollar for the full security of \$ETH.

(23/23) So, yes, the [@ethereum](#) we have today is slow and expensive.

But the Merge was barely 2 months ago, this is just the beginning of the second act.

Everything gets faster, cheaper and better from here!

[@ethereum](#) More of a long-form reader? Try this:



**Haym**  
@SalomonCrypto



## Ethereum Transaction Scaling

**Ethereum Transaction Scaling | Haym**  
(1/23) @ethereum Roadmap: Scaling Execution \$ETH is inevitable; I am more confident today than I have ever been. But let's face facts: Ethereum is SLOW and EXPENSIVE. How will the World Computer sca...  
<https://typefully.com/SalomonCrypto/K2PMBOw>

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](#)



(1/23) [@ethereum](#) Roadmap: Scaling Execution

**\$ETH** is inevitable; I am more confident today than I have ever been. But let's face facts: Ethereum is SLOW and EXPENSIVE. How will the World Computer scale?

Your guide to Rollups, Danksharding, PBS and more!



2:11 AM · Nov 13, 2022

 [Read the full conversation on Twitter](#)

572  Reply  Copy link

[Read 20 replies](#)

