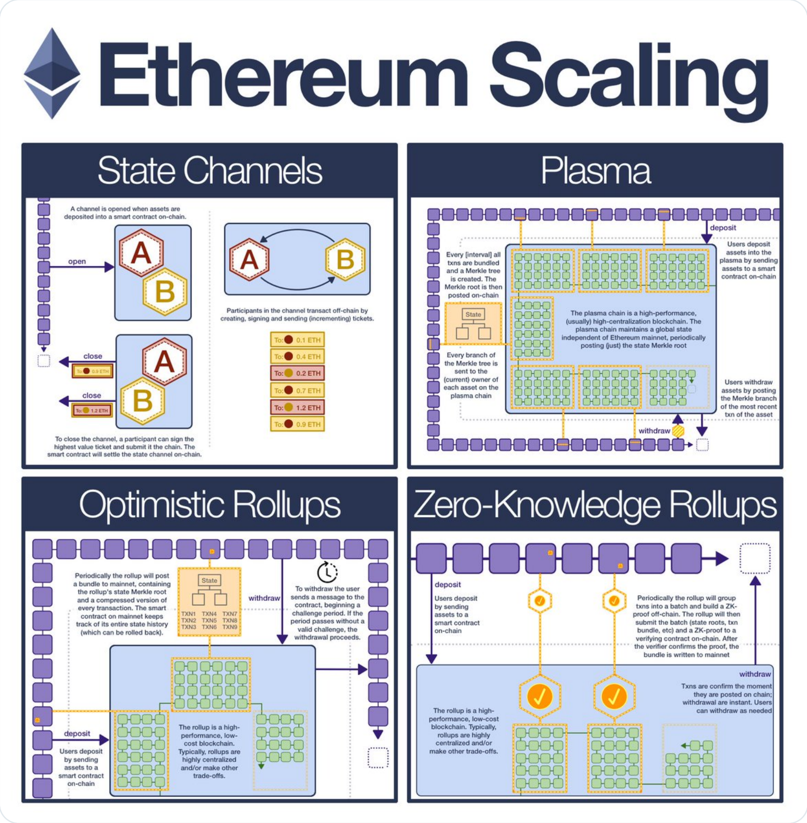
Haym @SalomonCrypto

Sep 12 • 16 tweets • SalomonCrypto/status/1569461980821606403

(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 transact off-chain by creating, signing and sending (incrementing) tickets.

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

Plasma

Every [interval] all txns are bundled and a Merkle tree is created. The Merkle root is then posted on-chain

Every branch of the Merkle tree is sent to the (current) owner of each asset on the plasma chain

The plasma chain is a high-performance, (usually) high-centralization blockchain. The plasma chain maintains a global state independent of Ethereum mainnet, periodically posting (just) the state Merkle root

Users deposit assets into the plasma by sending assets to a smart contract on-chain

Users withdraw assets by posting the Merkle branch of the most recent txn of the asset

Optimistic Rollups

Periodically the rollup will post a bundle to mainnet, containing the rollup's state Merkle root and a compressed version of every transaction. The smart contract on mainnet keeps track of its entire state history (which can be rolled back).

To withdraw the user sends a message to the contract, beginning a challenge period. If the period passes without a valid challenge, the withdrawal proceeds.

Users deposit by sending assets to a smart contract on-chain

The rollup is a high-performance, low-cost blockchain. Typically, rollups are highly centralized and/or make other trade-offs.

Zero-Knowledge Rollups

Users deposit by sending assets to a smart contract on-chain

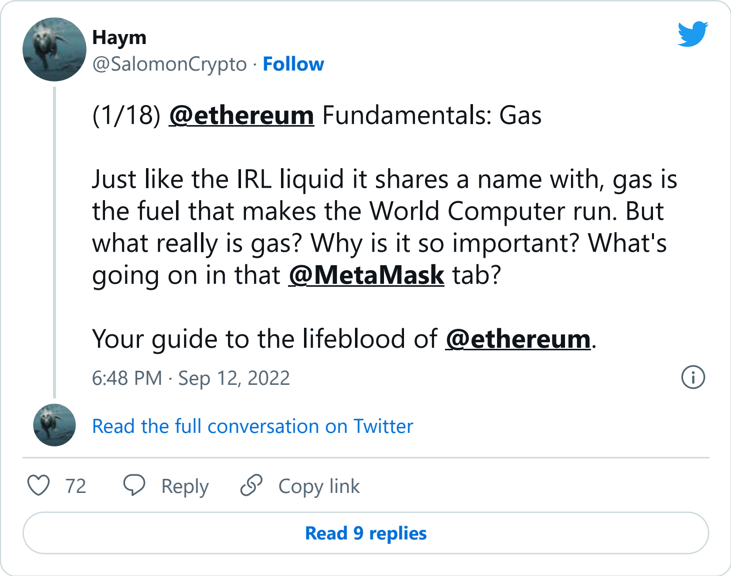
Periodically the rollup will group txns into a batch and build a ZK-proof off-chain. The rollup will then submit the batch (state roots, txn bundle, etc) and a ZK-proof to a verifying contract on-chain. After the verifier confirms the proof, the bundle is written to mainnet

Txns are confirm the moment they are posted on chain; withdrawal are instant. Users can withdraw as needed

The rollup is a high-performance, low-cost blockchain. Typically, rollups are highly centralized and/or make other trade-offs.

(2/15) @Bitcoin is the suggestion that trustless computing was possible; @ethereum, the World Computer, is the delivery.

The World Computer is slow, intentionally. That slowness manifests in two ways: sluggish execution and high gas costs.



Haym
@SalomonCrypto

(1/18) @ethereum Fundamentals: Gas

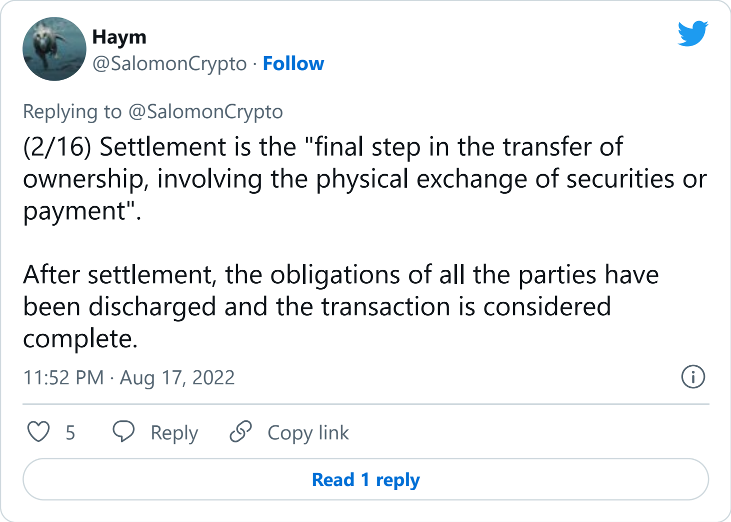
Just like the IRL liquid it shares a name with, gas is the fuel that makes the World Computer run. But what really is gas? Why is it so important? What's going on in that @MetaMask tab?

Your guide to the lifeblood of @ethereum.

6:48 PM · Sep 12, 2022

(3/15) Which brings us to the framework that defines @ethereum scaling: keep as much execution off-chain as possible while still ultimately settling to Ethereum.

If the transaction settles on Ethereum, then it gains all the properties of Ethereum.



Haym
@SalomonCrypto

Replying to @SalomonCrypto

(2/16) Settlement is the "final step in the transfer of ownership, involving the physical exchange of securities or payment".

After settlement, the obligations of all the parties have been discharged and the transaction is considered complete.

11:52 PM · Aug 17, 2022

(4/15) State channels are the first attempt at moving execution off-chain.

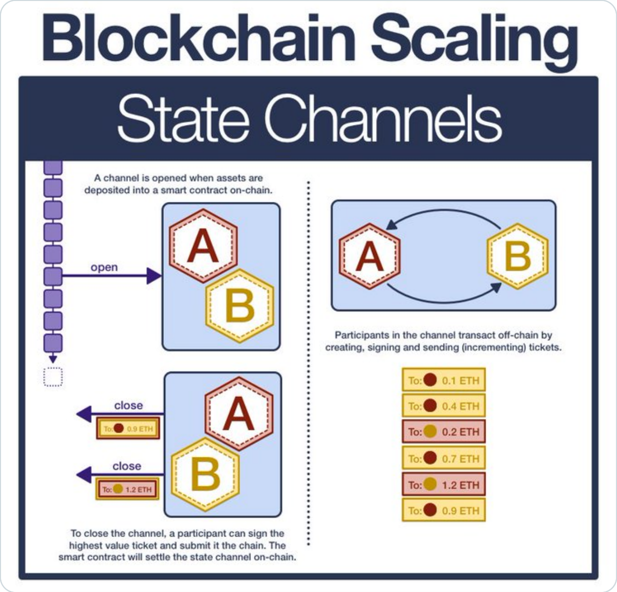
Channels are one-time relationships between two or more parties. The parties lock up capital on-chain, allowing them to exchange IOUs for no cost.

Haym
@SalomonCrypto · **Follow**

(1/14) Blockchain Scaling: State Channels

@Bitcoin, **@ethereum** and all (good) blockchain computers share one important quality: they are SLOW. State channels are the first attempt at changing this and bringing blockchain to scale.

Your guide to the original scaling tech.


Blockchain Scaling
State Channels
A channel is opened when assets are deposited into a smart contract on-chain.
open
A
B
Participants in the channel transact off-chain by creating, signing and sending (incrementing) tickets.
To: ● 0.1 ETH
To: ● 0.4 ETH
To: ● 0.2 ETH
To: ● 0.7 ETH
To: ● 1.2 ETH
To: ● 0.9 ETH
close
To: ● 0.9 ETH
close
To: ● 1.2 ETH
To close the channel, a participant can sign the highest value ticket and submit it the chain. The smart contract will settle the state channel on-chain.

3:25 PM · Sep 10, 2022

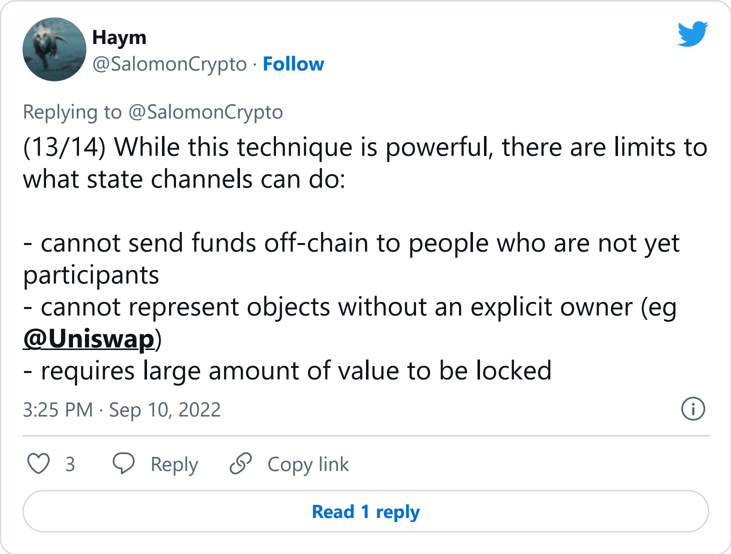
Read the full conversation on Twitter

♡ 166 Reply Copy link

Read 10 replies

(5/15) From @ethereum's perspective, a state channel is 2 txns (per participant): open and close. These txns represent much more computation that happened off-chain, but are ultimately settled to mainnet.

State channels provide scaling, but are limited in application.



Haym
@SalomonCrypto · **Follow**

Replying to @SalomonCrypto

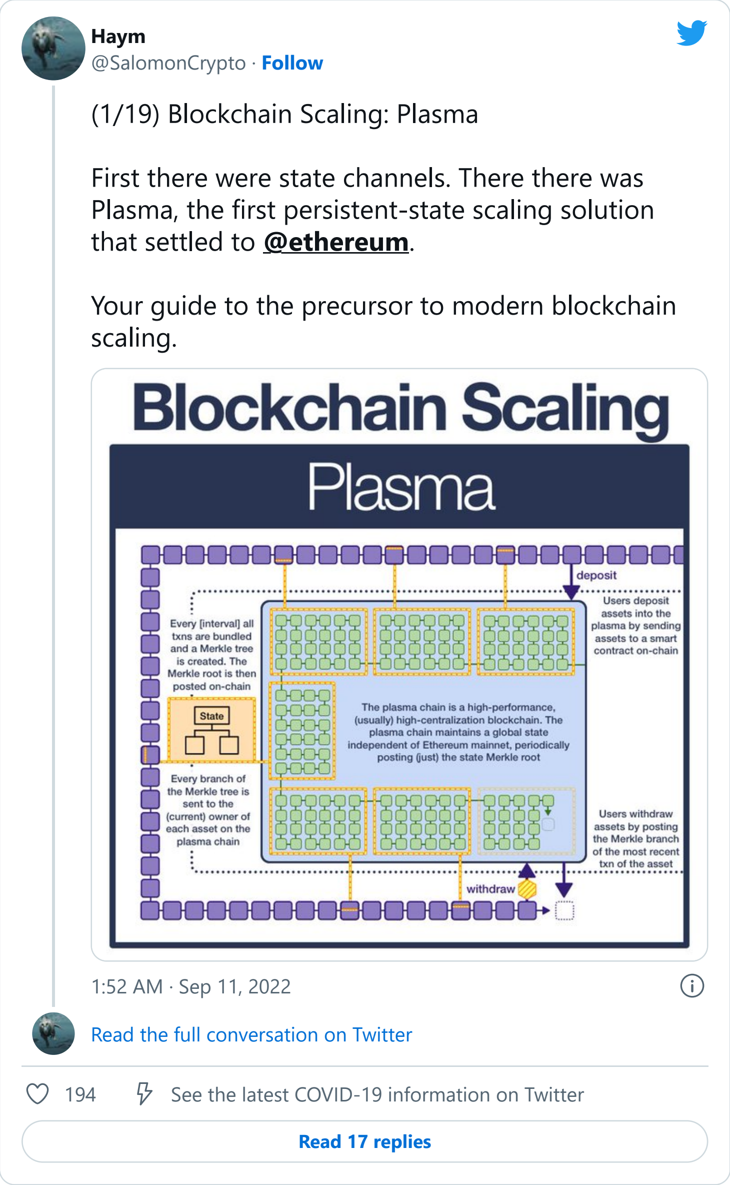
(13/14) While this technique is powerful, there are limits to what state channels can do:

- cannot send funds off-chain to people who are not yet participants
- cannot represent objects without an explicit owner (eg **@Uniswap**)
- requires large amount of value to be locked

3:25 PM · Sep 10, 2022

(6/15) Plasma (chains) were developed to address (some of) these issues.

Plasma are independent blockchains that are much higher performance (and much more centralized) than @ethereum. However, they are anchored to the World Computer by posting data back to mainnet.



Haym
@SalomonCrypto · **Follow**

(1/19) Blockchain Scaling: Plasma

First there were state channels. There there was Plasma, the first persistent-state scaling solution that settled to **@ethereum**.

Your guide to the precursor to modern blockchain scaling.

Blockchain Scaling

Plasma

deposit

Users deposit assets into the plasma by sending assets to a smart contract on-chain

Every [interval] all txns are bundled and a Merkle tree is created. The Merkle root is then posted on-chain

The plasma chain is a high-performance, (usually) high-centralization blockchain. The plasma chain maintains a global state independent of Ethereum mainnet, periodically posting (just) the state Merkle root

Every branch of the Merkle tree is sent to the (current) owner of each asset on the plasma chain

Users withdraw assets by posting the Merkle branch of the most recent txn of the asset

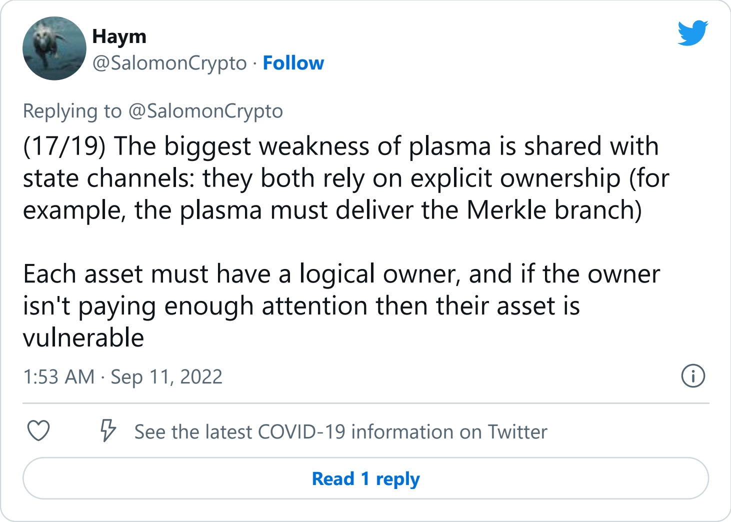
1:52 AM · Sep 11, 2022

Read the full conversation on Twitter

(7/15) Plasma offers huge improvements over state channels:

- can send assets to users who haven't opted-in yet
- supports a persistent state (exists even when users exit the system)
- data is posted on-chain periodically

But, plasma is only half the solution.



Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(17/19) The biggest weakness of plasma is shared with state channels: they both rely on explicit ownership (for example, the plasma must deliver the Merkle branch)

Each asset must have a logical owner, and if the owner isn't paying enough attention then their asset is vulnerable

1:53 AM · Sep 11, 2022

(8/15) The full solution: rollups!

Where plasma only posted the state root (a single line used to verify if a txn happened), rollups post everything you would need to fully reconstruct the chain.

Imagine an entire blockchain that's squeezed into the main @ethereum blockchain.

(9/15) The first category of rollups are optimistic rollups.

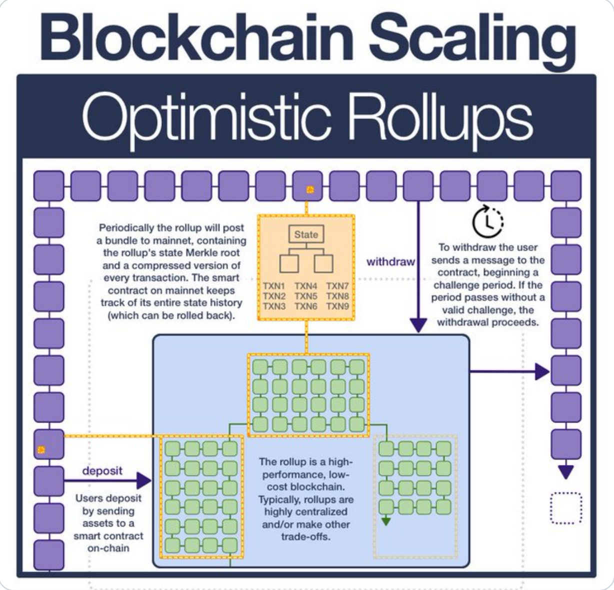
Optimistic rollups make the assumption that all txns that are posted to mainnet are valid and so it records them on-chain. But, just in case, they also leave open a challenge window.

Haym
@SalomonCrypto · **Follow**

(1/24) Blockchain Scaling: Optimistic Rollups

Wondering why folks are comfortable bridging assets to **@arbitrum**? Curious what's going on under **@optimismFND**'s hood? Need to understand how **@MetisDAO** secures your **$ETH**?

Your guide to the today's premier blockchain scaling solutions.



Blockchain Scaling

Optimistic Rollups

Periodically the rollup will post a bundle to mainnet, containing the rollup's state Merkle root and a compressed version of every transaction. The smart contract on mainnet keeps track of its entire state history (which can be rolled back).

To withdraw the user sends a message to the contract, beginning a challenge period. If the period passes without a valid challenge, the withdrawal proceeds.

Users deposit by sending assets to a smart contract on-chain

The rollup is a high-performance, low-cost blockchain. Typically, rollups are highly centralized and/or make other trade-offs.

6:02 PM · Sep 11, 2022

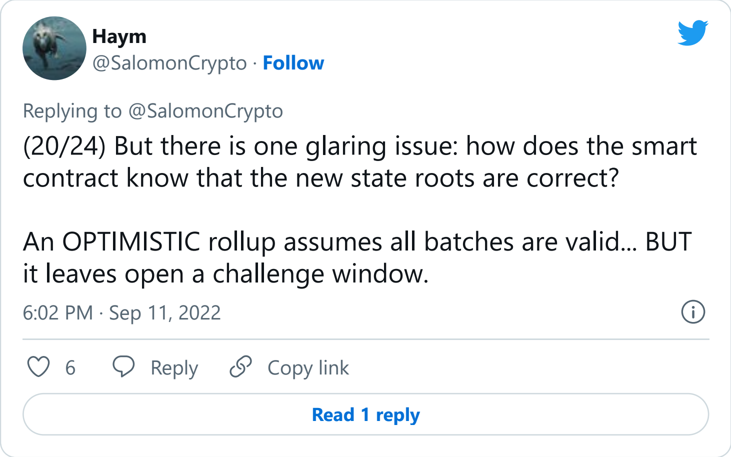
Read the full conversation on Twitter

460 Reply Copy link

Read 13 replies

(10/15) The rollup creates its own blockchain, which anyone can watch for fraud. When detected, they can publish a fraud proof, proving the batch is invalid and should be reverted.

The result: no txn is finalized until the challenge period (up to 7 days) has passed.



Haym
@SalomonCrypto · **Follow**

Replying to @SalomonCrypto

(20/24) But there is one glaring issue: how does the smart contract know that the new state roots are correct?

An OPTIMISTIC rollup assumes all batches are valid… BUT it leaves open a challenge window.

6:02 PM · Sep 11, 2022

(11/15) Which brings us to the real solution to blockchain scaling and the future of @ethereum: ZK-Rollups.

Like their optimistic brothers, ZK-rollups post ALL data to mainnet, but they also provide a a zero-knowledge proof.

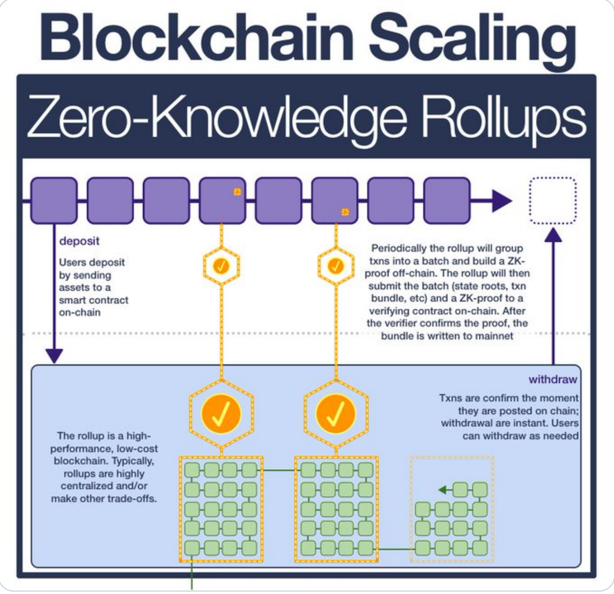
Haym
@SalomonCrypto · **Follow**

(1/23) Blockchain Scaling: Zero-Knowledge Rollups

State Channels → Plasma → Optimistic Rollups → ZK-Rollups

This is how **@ethereum** scales to 100k txn/sec. This is how Ethereum becomes the World Computer.

Your guide to the future of blockchain scaling technology.


Blockchain Scaling
Zero-Knowledge Rollups
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
withdraw
Txns are confirm the moment they are posted on chain; withdrawal are instant. Users can withdraw as needed
The rollup is a high-performance, low-cost blockchain. Typically, rollups are highly centralized and/or make other trade-offs.

2:39 PM · Sep 12, 2022

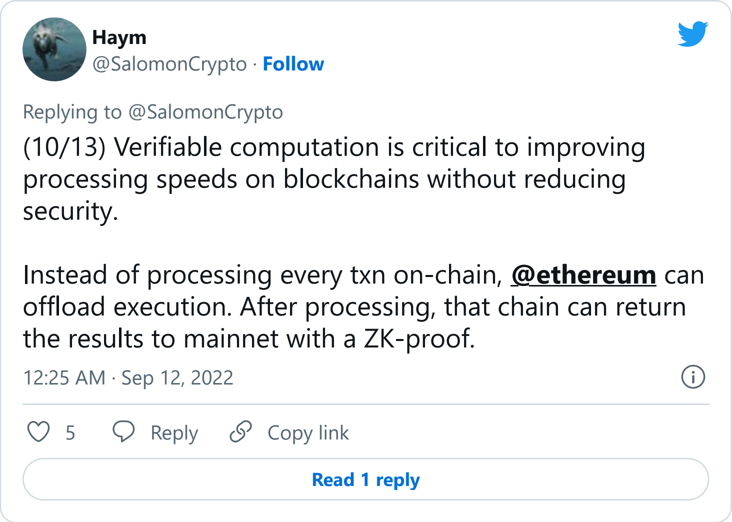
Read the full conversation on Twitter

♡ 173 See the latest COVID-19 information on Twitter

Read 7 replies

(12/15) The ZK-proof represents mathematically certainty that whatever is posted on-chain was both valid and actually happened on the rollup. If the proof verifies, the transaction is final both on the rollup and on @ethereum.

All the benefits of rollups with instant settlement.



Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(10/13) Verifiable computation is critical to improving processing speeds on blockchains without reducing security.

Instead of processing every txn on-chain, **@ethereum** can offload execution. After processing, that chain can return the results to mainnet with a ZK-proof.

12:25 AM · Sep 12, 2022

♡ 5 Reply Copy link

Read 1 reply

(13/15) ZK-Rollups are still the bleeding edge of blockchain technology; (I believe) there isn't a single general purpose/EVM-compatible ZK-Rollup ready for production... today.

But we are not far away, if you look carefully you'll find a testnet or two.

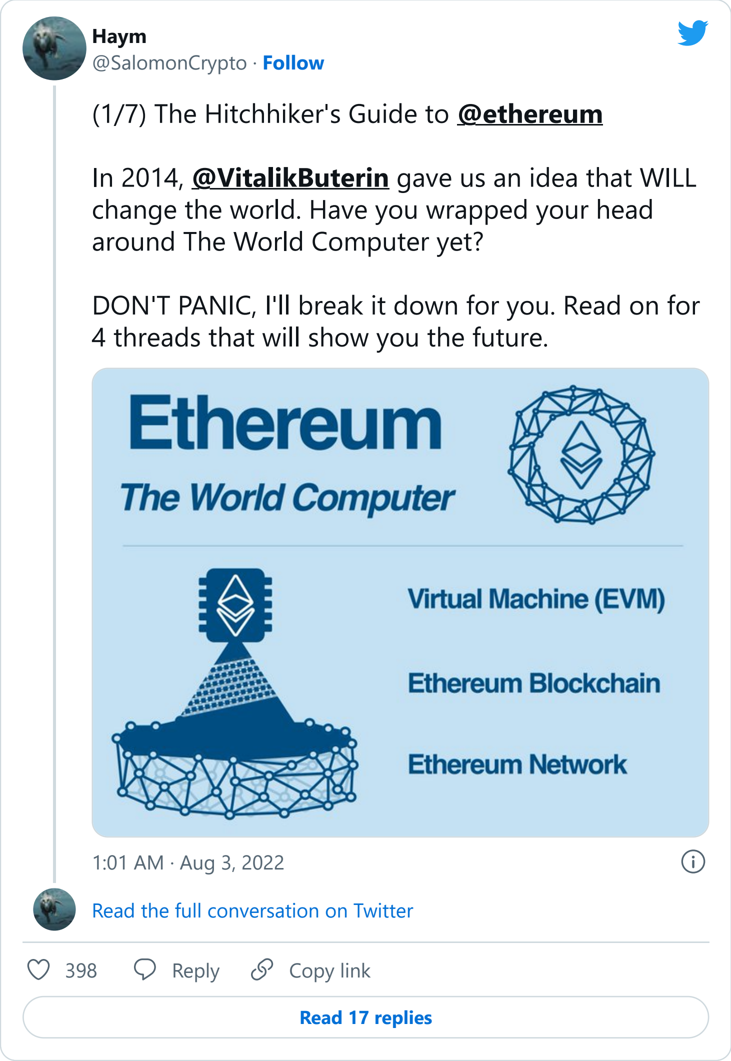
(14/15) Back in November 2021, @ukolodny and @EliBenSasson were on @BanklessHQ. Uri mentioned that @StarkWareLtd was already fast and cheap enough to support physics simulations.

We are building a legit supercomputer!

https://www.youtube.com/embed/7Kq3YWsysc0

(15/15) When you look at @ethereum today, it might be hard to see the World Computer. Even if you wrap your head around the metaphor, it's hard to see how 12 txns/sec is going to support the whole world.

But I'm not looking at today, I'm looking at a zero-knowledge future.



Haym
@SalomonCrypto · **Follow**

(1/7) The Hitchhiker's Guide to **@ethereum**

In 2014, **@VitalikButerin** gave us an idea that WILL change the world. Have you wrapped your head around The World Computer yet?

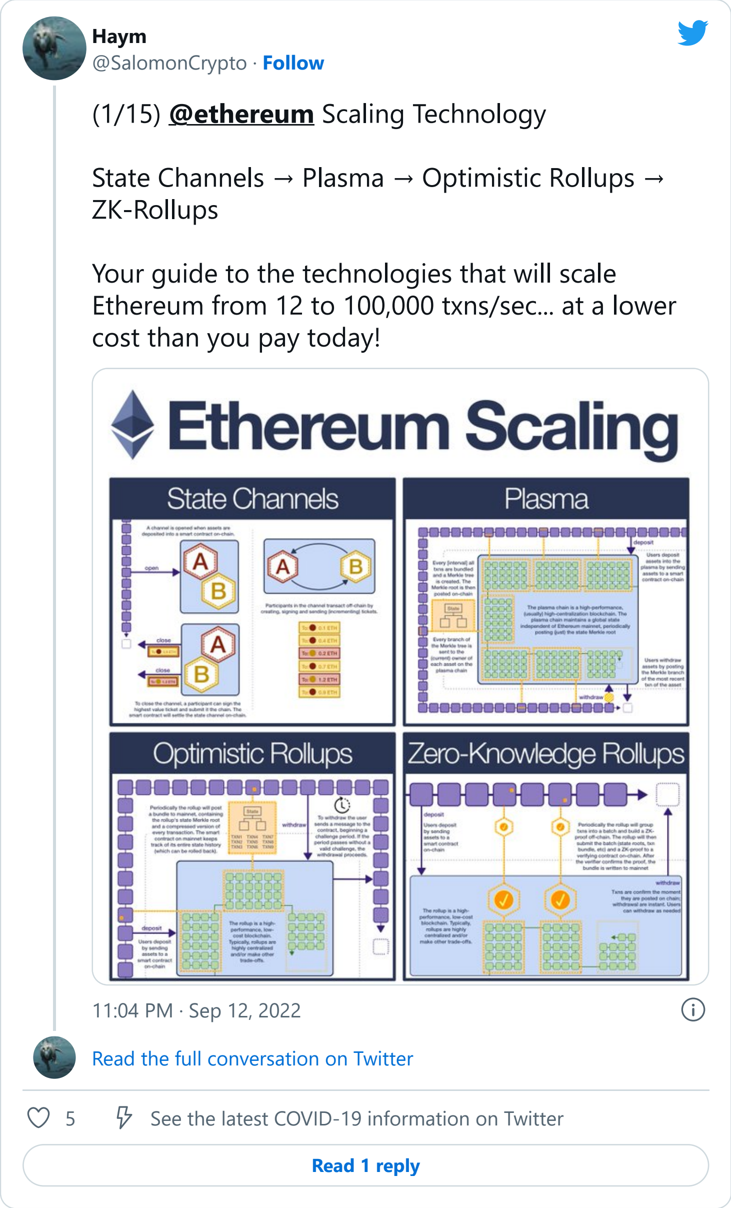
DON'T PANIC, I'll break it down for you. Read on for 4 threads that will show you the future.

1:01 AM · Aug 3, 2022

Read the full conversation on Twitter

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

(1/15) @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!

11:04 PM · Sep 12, 2022

Read the full conversation on Twitter

5

See the latest COVID-19 information on Twitter

Read 1 reply

• • •