**Haym** @SalomonCrypto

Sep 18 • 26 tweets • SalomonCrypto/status/1571524423639007232

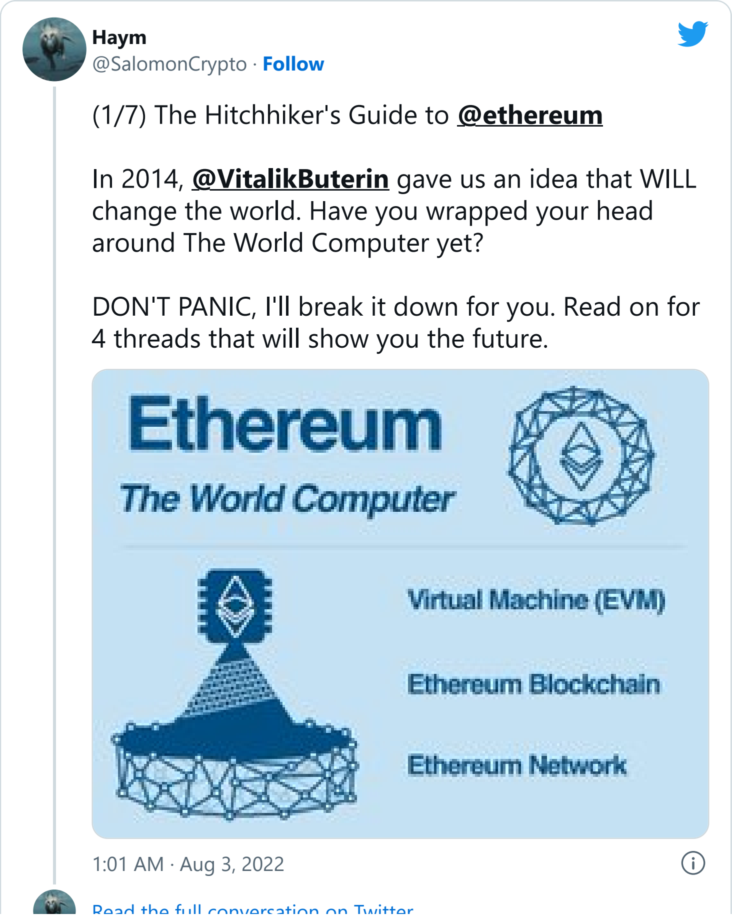
(1/25) @ethereum Roadmap: Data Availability

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.

(2/25) @ethereum is the World Computer, a globally shared utility that exists between a network of 1,000s of computers (nodes), each running a local version of the EVM.

Today, the World Computer is SLOW.



**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

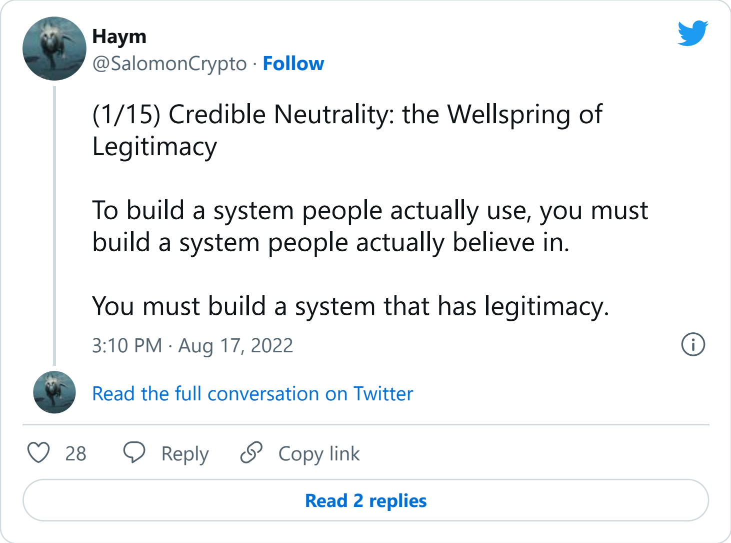
(3/25) However, this slowness is a feature, not a bug. In order to keep the World Computer as decentralized as possible, we want to allow as many machines/connections to be able to be nodes as possible.

Staking isn't just for AWS and supercomputers; everyone can participate.

(4/25) The core value @ethereum is decentralization. Everyone person, whether MEGACORP CEO or Aunt Phillis, can become a node operator and keep the network honest.

From decentralization flows credible neutrality.

From credibly neutrality comes global dominance



Haym
@SalomonCrypto · Follow

(1/15) Credible Neutrality: the Wellspring of Legitimacy

To build a system people actually use, you must build a system people actually believe in.

You must build a system that has legitimacy.

3:10 PM · Aug 17, 2022

Read the full conversation on Twitter

(5/25) The result: while nearly anyone can operate an @ethereum node, the network can only process ~15 txns/second.

There are ~9B people on this planet. The WOLRD computer is going require A LOT more power to service the entire globe.

(6/25) Fortunately, we have solutions: rollups!

Rollups are independent blockchains that anchor to the World Computer. Rollups are (/can be) much more centralized, but because they settle @ethereum, they derive the same security and decentralization properties as mainnet.

Haym
@SalomonCrypto · Follow

(1/21) Scaling **@ethereum**: Execution

The World Computer will be the decentralized settlement layer of the internet and of the world. Although Ethereum has successfully Merged, it is still a far from ready for the global stage... for now.

It's time to scale.

(7/25) Conceptually, rollups work by splitting an @ethereum txn into two parts: execution and settlement.

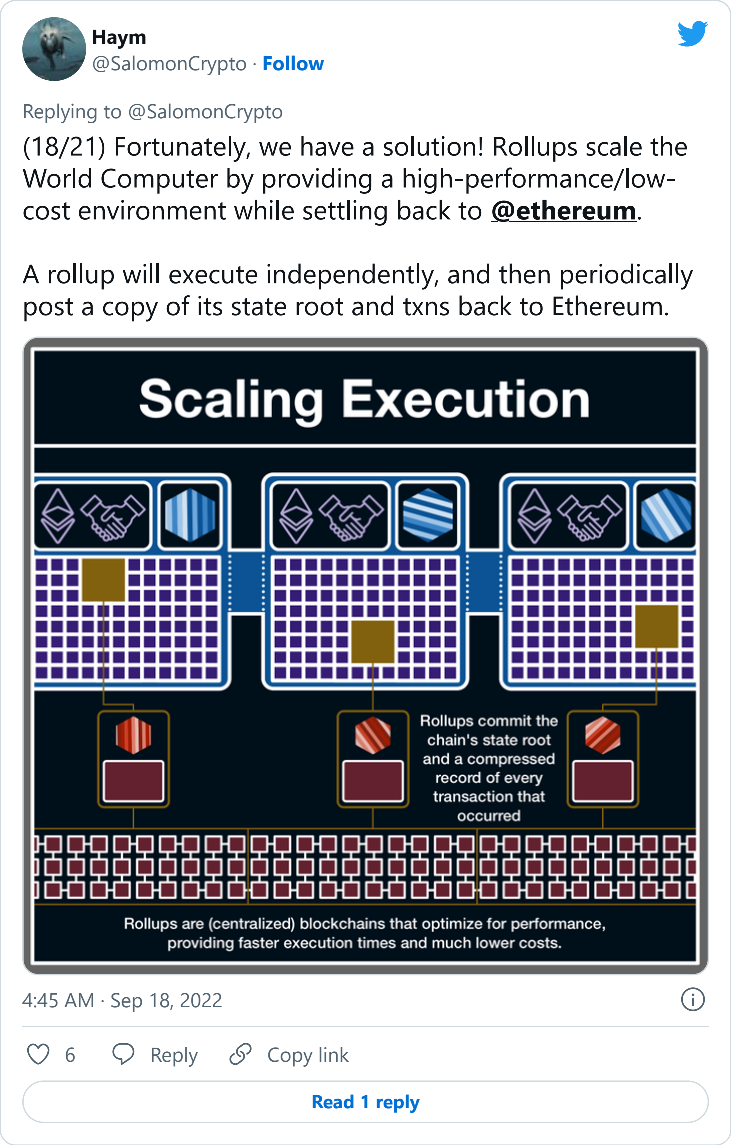
Execution: the computational work needed to complete the txn

Settlement: the transfer of ownership, including the exchange of assets and record keeping

(8/25) It will always remain vital to retain settlement on @ethereum; settlement is the purpose of the World Computer and the reason we care so much about decentralization.

Execution is a different animal. We care much less about decentralization, we just need the job done.

(9/25) Rollups execute all of their transactions on a separate (high performance) blockchain. Once every [interval], the bundle up all the transactions they've executed and post a record back on to mainnet.



Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(18/21) Fortunately, we have a solution! Rollups scale the World Computer by providing a high-performance/low-cost environment while settling back to **@ethereum**.

A rollup will execute independently, and then periodically post a copy of its state root and txns back to Ethereum.

Scaling Execution
Rollups commit the chain's state root and a compressed record of every transaction that occurred
Rollups are (centralized) blockchains that optimize for performance, providing faster execution times and much lower costs.

4:45 AM · Sep 18, 2022

6
Reply
Copy link
Read 1 reply

(10/25) In reality, these checkpoints are complicated data structures, but we can think of them as having two parts: the rollup's state root and a compressed record of every transaction that happened during the previous interval.

(11/25) The state root is the Merkle root for @ethereum's state... but let's unpack that into something a little more useful.

A machine's state is its configuration. Think about your computer, the state is the contents of your hard drive, memory, what's on the screen, etc.

(12/25) For the World Computer, the state is a snapshot of all the accounts, balances and smart contracts at a given point in time. The state is what we need to keep in sync between all nodes in a blockchain network.

Unfortunately, @ethereum's state is MASSIVE (GBs).

(13/25) Instead of passing around the World Computer's full state, we can organize it into a data structure called a Merkle Tree.

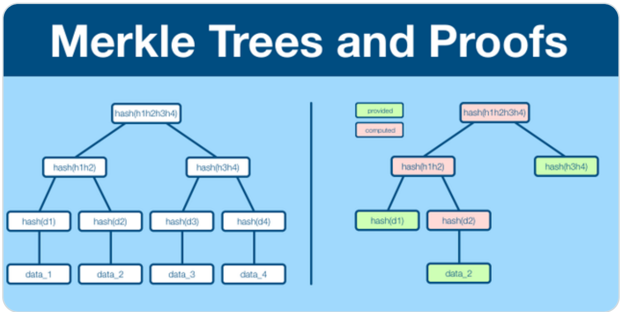
Merkle trees allow us to condense an arbitrarily large amount of data into a single unique line (Merkle root).

**Haym**
@SalomonCrypto · **Follow**

(1/13) Computer Science 201: Merkle Trees and Merkle Proofs

If you want to understand **@Bitcoin**, **@ethereum** and blockchain technology, you need to learn:

- How a Merkle trees expresses a large dataset
- How a Merkle proof works
- Why a Markle tree is so efficient



10:17 PM · Sep 7, 2022

Read the full conversation on Twitter

421 Reply Copy link

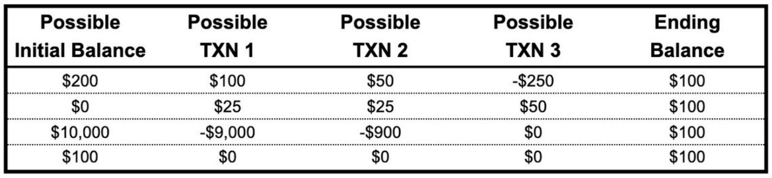
**Read 15 replies**

(14/25) @ethereum (and rollups) communicate the state of the EVM by socializing the state root and a list of all the txns executed since the last block.

Each node can locally execute every txn on that list and compare their local state root to the one published by the network.

(15/25) A Merkle root cannot extract the txns that were applied to create the current state.

Imagine a list of balances at a bank. You can confirm all the txns were included by checking balances, but you can't see the individual txns.



| Possible Initial Balance | Possible TXN 1 | Possible TXN 2 | Possible TXN 3 | Ending Balance |
|---|---|---|---|---|
| $200 | $100 | $50 | -$250 | $100 |
| $0 | $25 | $25 | $50 | $100 |
| $10,000 | -$9,000 | -$900 | $0 | $100 |
| $100 | $0 | $0 | $0 | $100 |

(16/25) Thus, coordination requires both the state root and the list of transactions. With both these pieces of information, every node of the @ethereum network can update their copy of the EVM and progress the World Computer.

Rollups post both pieces of information on-chain.

(17/25) This is the method by which rollups settle to @ethereum. By posting the canonical version of the state root and txns, rollups are ensuring that ultimate ownership will always be resolved on mainnet.

In fact, this can literally be true...

(18/25) Some rollups optimistically accept all updates  and then open a fraud challenge period for each update.

If a challenger submits a fraud proof, the rollup runs the disputed txn on mainnet and evaluates the result.

Ownership is resolved on-chain, by smart contracts.

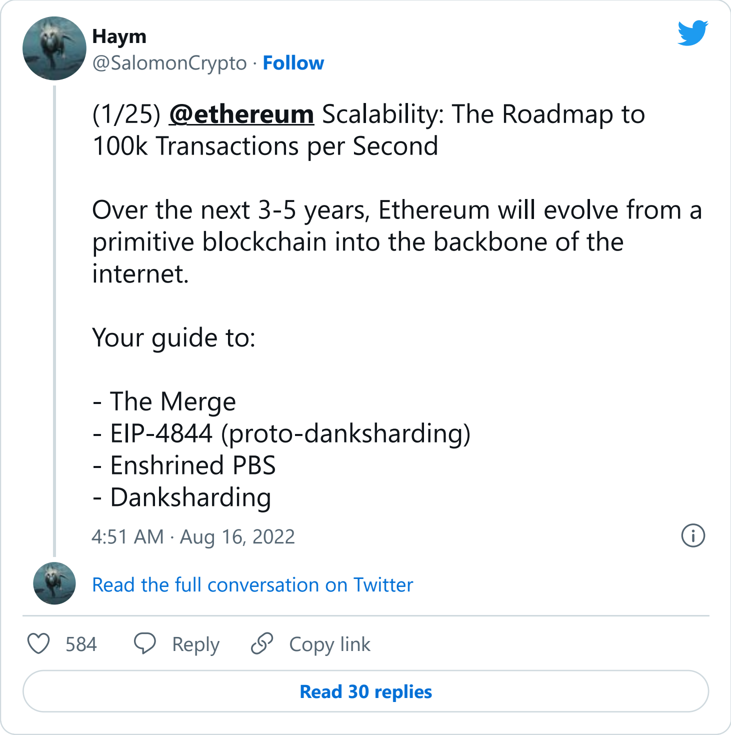
(19/25) In summary, rollups scale the World Computer by providing a very high performance computing environment while still respecting the rules of @ethereum. It does this by posting a canonical copy of the rollups machine state and all the transactions executed off-chain.

(20/25) However, this model has scaling limits: regardless of how much computation you can offload, you still need to post the txn data back to mainnet.

Rollups make progress by compressing txn data into the smallest possible form factor. Even still, these costs add up quick.

(21/25) There are already plans to further optimize the World Computer for a rollup-focused future.

In particular, EIP-4844 will create an independent gas market for storage costs (decoupling form executing and reducing price) and danksharding will increase capacity.



(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

(22/25) All of this work is critically important to the development of the World Computer; we should all celebrate it and ask how we can contribute!

But some folks are thinking about this problem a little differently.

(23/25) It starts off with a simple question: When does settlement actually occur on the World Computer?

Does it happen when a copy of the txn is stamped into the blockchain...

...or does it happen right before that, when the txn is run through the EVM and its state is updated?

(24/25) If you answered the former, you belong with the EIP-4844/danksharding/capacity crowd (good crowd). If you answered the later, welcome to the data availability club.

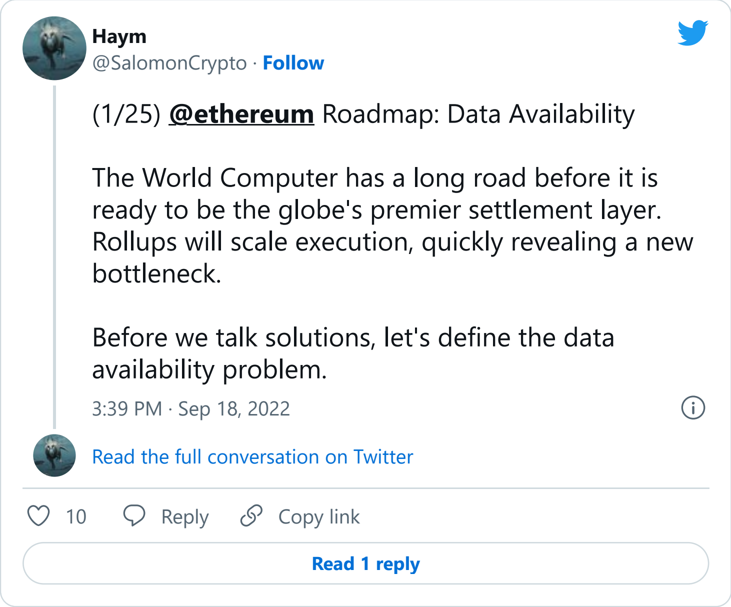
We believe that what's important is what happens in the EVM. A copy of your txn will be made available...

(25/25) ...but we aren't (necessarily) going to promise that a copy of your txn is available on chain.

You thought rollups were cool? You haven't even see half their full potential.

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: 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

• • •