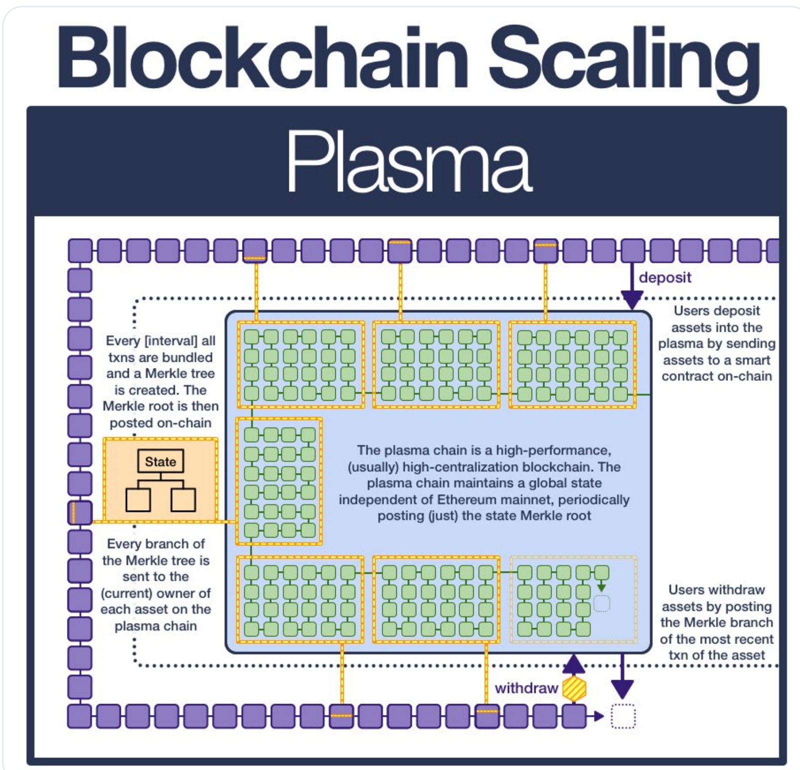
Haym @SalomonCrypto

Sep 11 • 20 tweets • SalomonCrypto/status/1568779570492637185

(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.



(2/19) In 2008, Satoshi Nakamoto gave us @Bitcoin and introduced the dream.

In 2015, @VitalikButerin gave us @ethereum and delivered on that dream: the World Computer was born.

In its early years, the World Computer is painfully slow. Fortunately, we have scaling solutions.

(3/19) The first category: state channels.

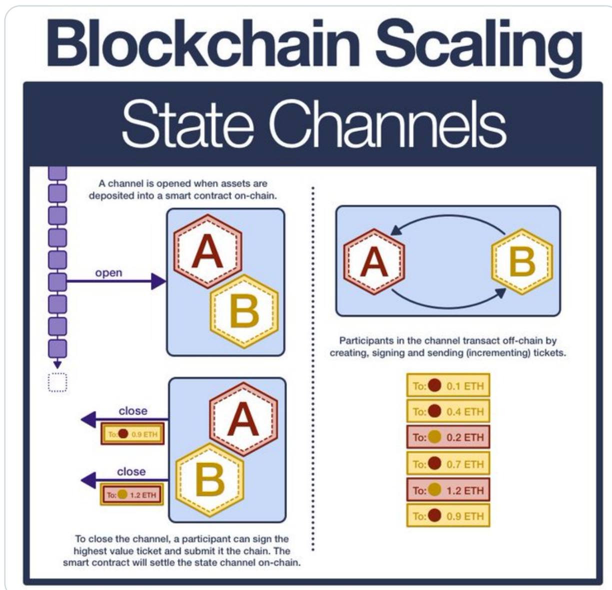
To open a channel, the participating parties fund a smart contract where the funds are held in on-chain-escrow. The participants can transact off-chain as much as they want. When finished, the smart contract settles channel.

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.



3:25 PM · Sep 10, 2022

Read the full conversation on Twitter

118 Reply Copy link

Read 7 replies

(4/19) While state channels are powerful; they have limits:

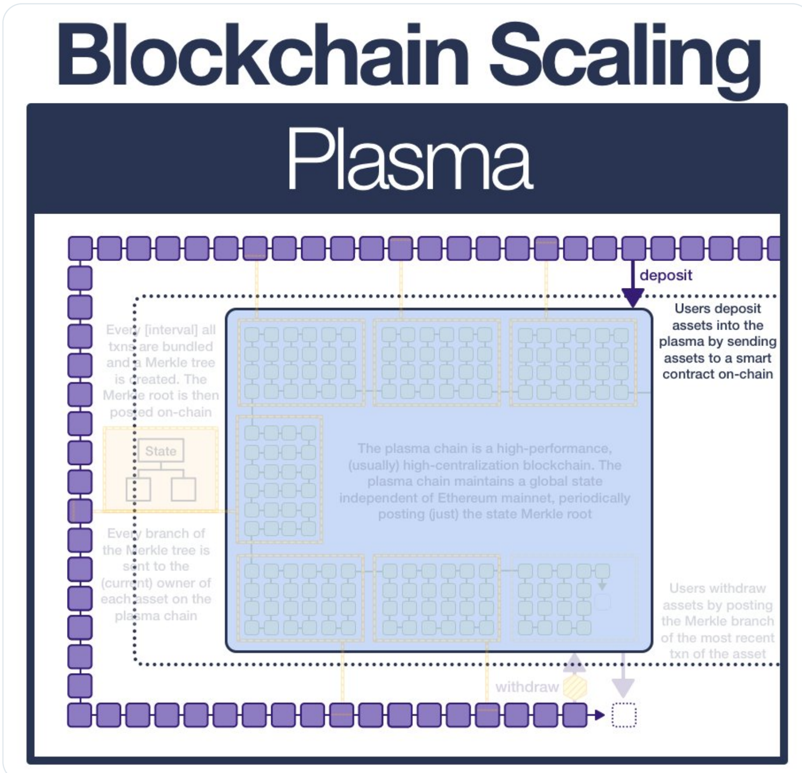
- All participants must opt-in; channels cannot send funds to non-participants
- Channels cannot represent objects without a clear owner (eg @Uniswap)
- Channels require large amounts of capital to be locked up

(5/19) The next development in blockchain scaling is a technology called Plasma.

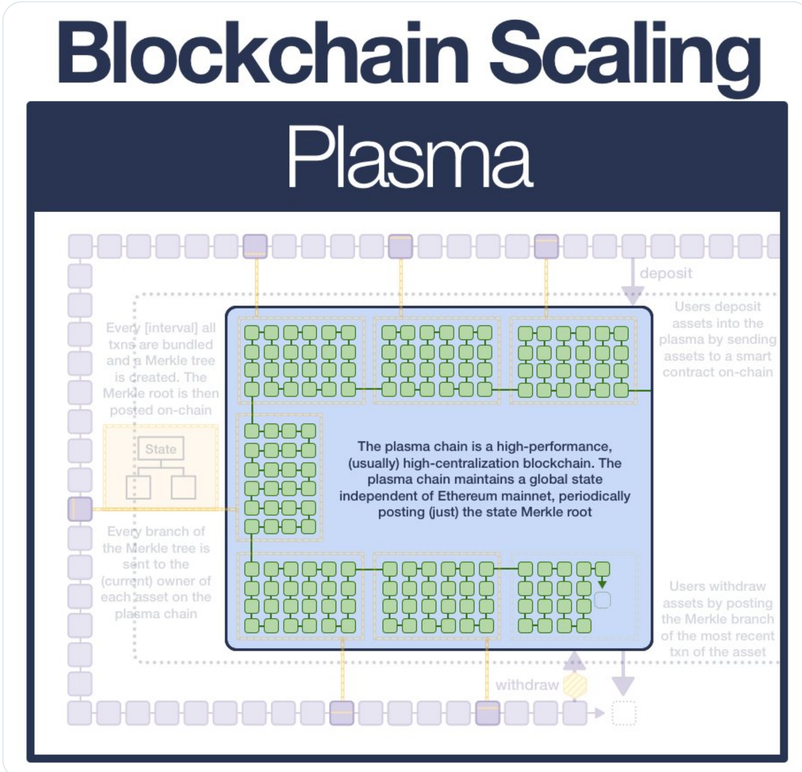
A plasma chain is a separate blockchain anchored to @ethereum but that executes transactions off-chain (with its own consensus system).

(6/19) Users interact with a plasma chain by depositing assets into a smart contract on @ethereum mainnet. The plasma operator then mints an equivalent amount of assets on the plasma chain and gives it to the depositor.

The on-chain assets remain in escrow.



(7/19) Because the plasma chain ultimately relies on [@ethereum](https://twitter.com/ethereum) for decentralized property rights, the plasma operator can be much more centralized (often a single entity) resulting in cheap and fast execution.



(8/19) The plasma chain is its own blockchain with its own virtual machine and state.

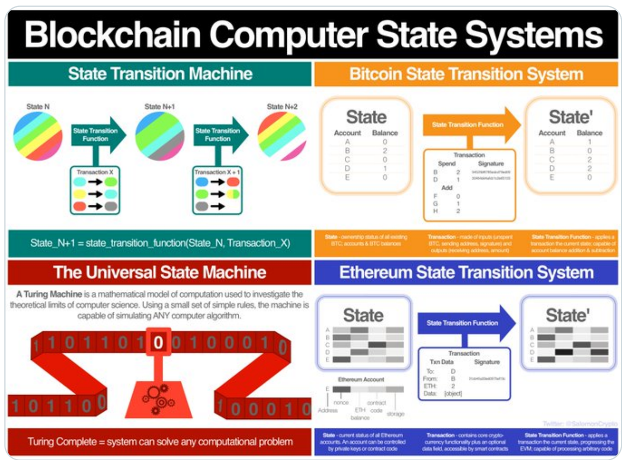
A virtual machine state describes everything within the virtual machine (and therefore blockchain/plasma computer) - every account, every smart contract, and every balance.

Haym
@SalomonCrypto · **Follow**

(1/19) Computer Science Fundamentals: Blockchain Computers, **@Bitcoin** and **@ethereum**

What is a blockchain computer and what makes it special? How did **@VitalikButerin** build on top of Bitcoin to create Ethereum? Why is Ethereum The World Computer?

This thread has answers!



10:38 PM · Aug 5, 2022

Read the full conversation on Twitter

230 Reply Copy link

Read 16 replies

(9/19) Blockchain computers, including plasma chains, store the state in a (modified) Merkle tree. A Merkle tree can be reduced to a single hash.

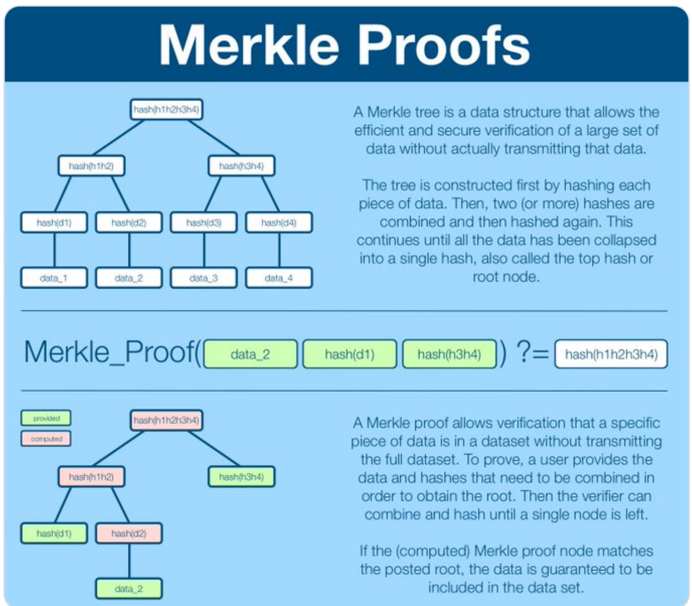
A Merkle tree allows the efficient confirmation a piece of data exists without transferring the whole dataset.

Haym
@SalomonCrypto · **Follow**

Replying to @SalomonCrypto

(9/13) A Merkle proof is established by providing the specific data and the intermediate hashes which allow a verifier to recreate the Merkle tree.

If the newly computed root node matches root node of the dataset, the verifier can be certain the data is in the dataset.

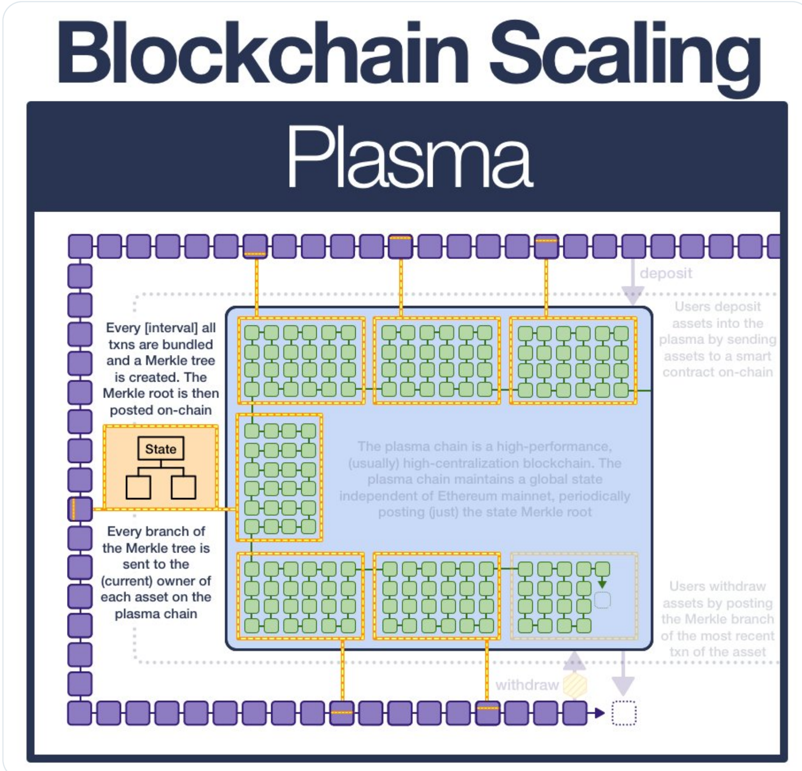


10:17 PM · Sep 7, 2022

10 Reply Copy link

Read 1 reply

(10/19) Once every interval (15 sec, 1 hour), the plasma operator batches all the txns they have received and generate a Merkle tree for the state of the plasma chain.

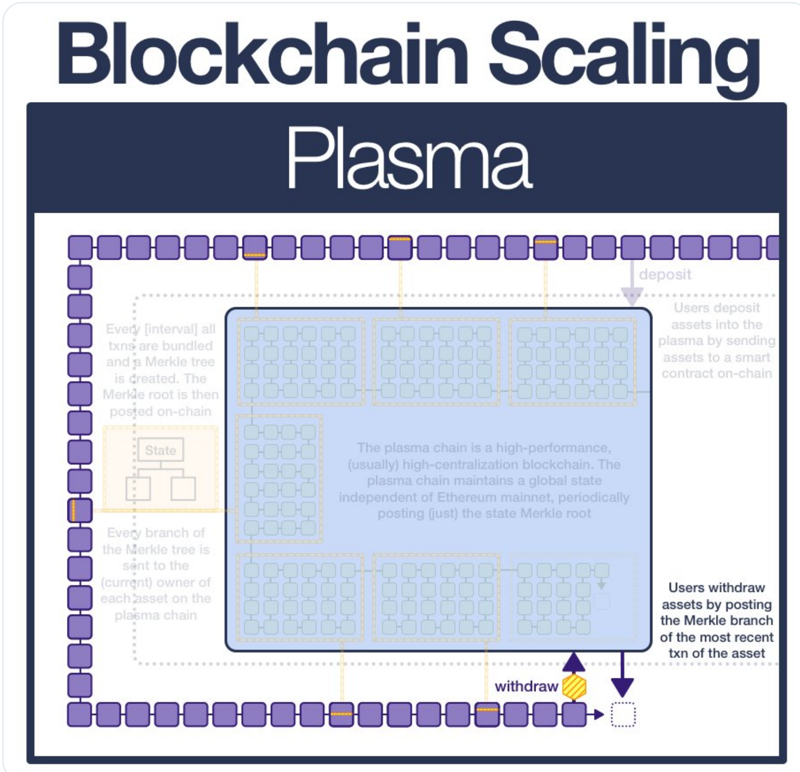


(11/19) First, the operator posts the Merkle root (the single hash representing the full state of the plasma chain) to mainnet.

Next, the operator sends the Merkle branch to the current owner of each asset.

(12/19) To withdraw an asset, the user sends the Merkle branch (proving they own the asset) to the smart contract.

This begins a withdrawal period.



(13/19) During the withdrawal period, anyone can invalidate the withdrawal by submitting a Merkle branch that proves the withdrawer doesn't own the asset.

If the period passes without any successful challenges, the assets can be withdrawn.

(14/19) The biggest difference between state channels and plasma is that plasma supports a persistent state.

A new state channel means a new state; when that channel is closed, that state is destroyed.

Plasma state exists in its own context, even if users enter and exit.

(15/19) Plasma provides much stronger security properties than state channels; a record of your transactions exist on-chain while in operation.

It also allows users to send assets to participants who are not yet part of the system (state channels require opt-in).

(16/19) However, Plasma has trade-offs:

- requires regular (costly) transactions on mainnet
- doesn’t support instant withdrawal (must wait for operator to post to mainnet)

(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

(18/19) This is a reasonable trade-off for some applications, but fundamentally cannot support more EVM-native applications that don't have an explicit owner.

Plasma even struggles with applications that can change a balance without a users explicit consent (eg paying interest)

(19/19) These factors the main reasons that it is just not possible to build a full EVM environment in a plasma. Therefore, the @ethereum community has taken the learnings from plasma and built something better.

Something we call a rollup!

Like what you read? Help me spread the word by retweeting the thread (linked below).

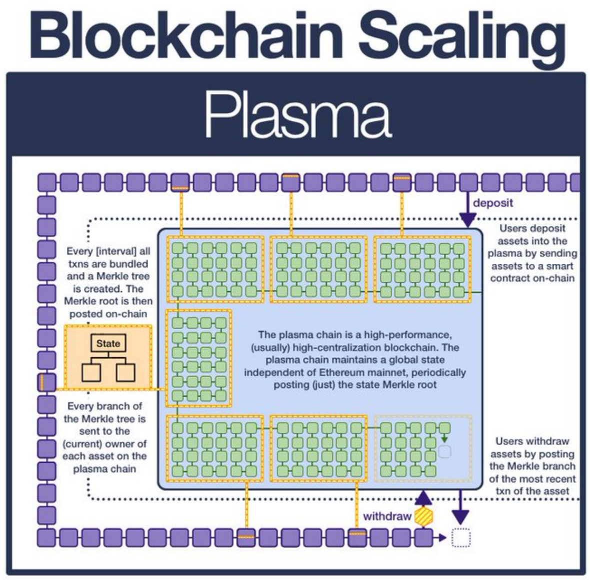
Follow me for more explainers and as much alpha as I can possibly serve.

Haym
@SalomonCrypto · **Follow**

(1/19) 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.



1:52 AM · Sep 11, 2022

Read the full conversation on Twitter

59 See the latest COVID-19 information on Twitter

Read 10 replies

• • •