



Haym Salomon @SalomonCrypto

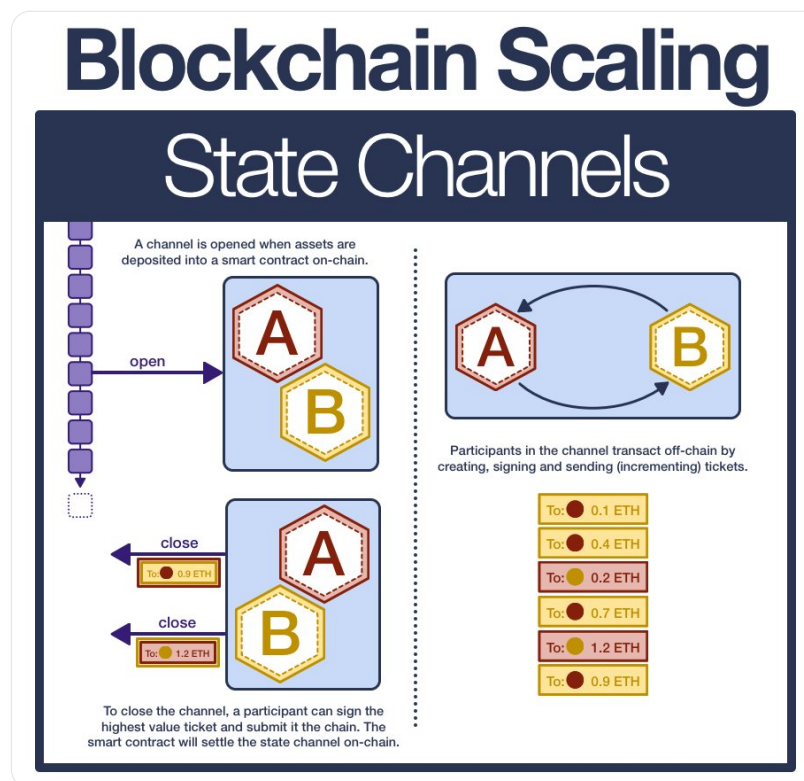
Sep 10 · 15 tweets · [SalomonCrypto/status/1568621672152039426](#)



(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.



(2/14) In 2008, Satoshi Nakamoto created blockchain technology, changing the world forever.

The purpose: to create a shared, untrusted computing platform. A public utility, usable by all... at any time... for any reason.

(3/14) The foundation of Blockchain computers is decentralization: more centralization requires more trust assumptions.

In order to maintain decentralization, we must ensure that a wide spectrum of machines are capable of participating.

(4/14) Therefore a blockchain that cares about decentralization must keep its core protocol requirements relatively light; if it requires a data center the network will centralize VERY quickly.

To put it simply, (good) blockchain computers are trustless... but they are SLOW.

(5/14) And so, the obvious question follows: how can we scale a blockchain computer while maintaining low node requirements (and therefore decentralization)?

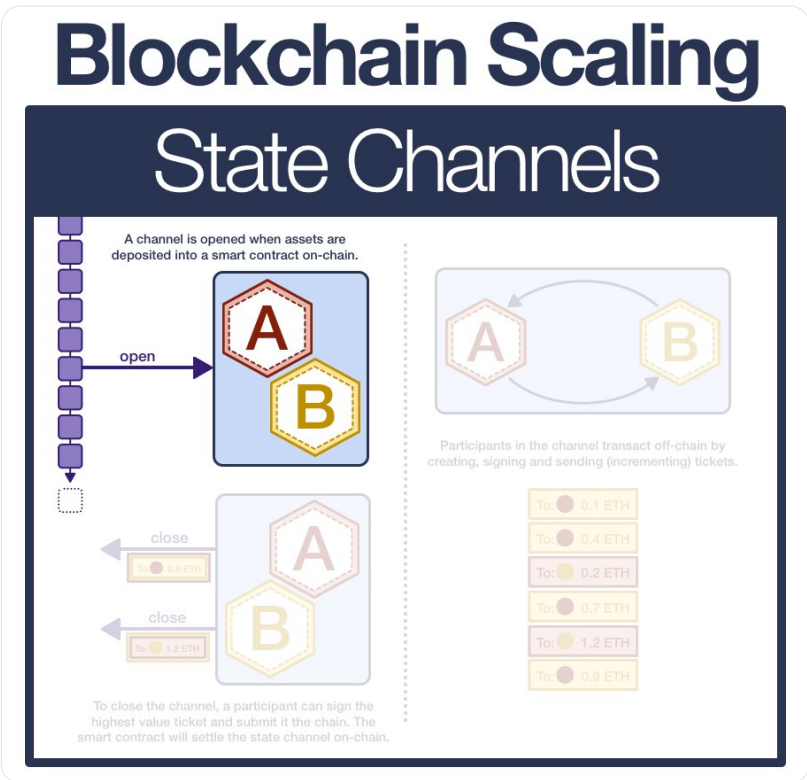
Today, we have many solutions. But let's start with the OG: state channels.

(6/14) State channels allow participants to securely transact off-chain while keeping interaction with the main (slow and expensive) chain to a minimum.

The system allows peers to conduct an arbitrary number of (off-chain) txns while only submitting two on-chain txns.

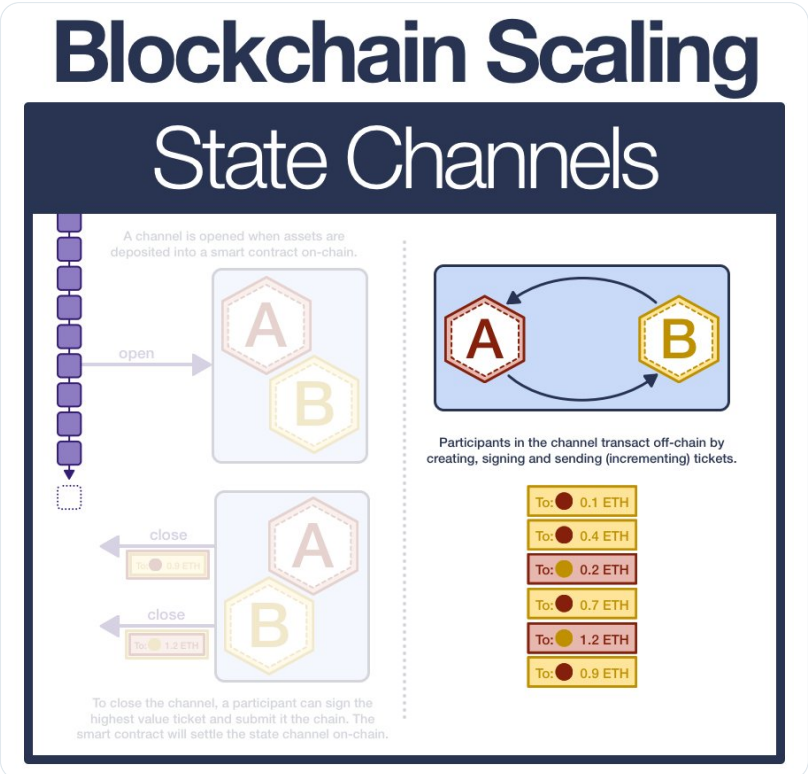
(7/14) Users open a state channel by depositing funds into a smart contract on the main blockchain, escrowing the capital.

This capital cannot be touched until the state channel is closed.



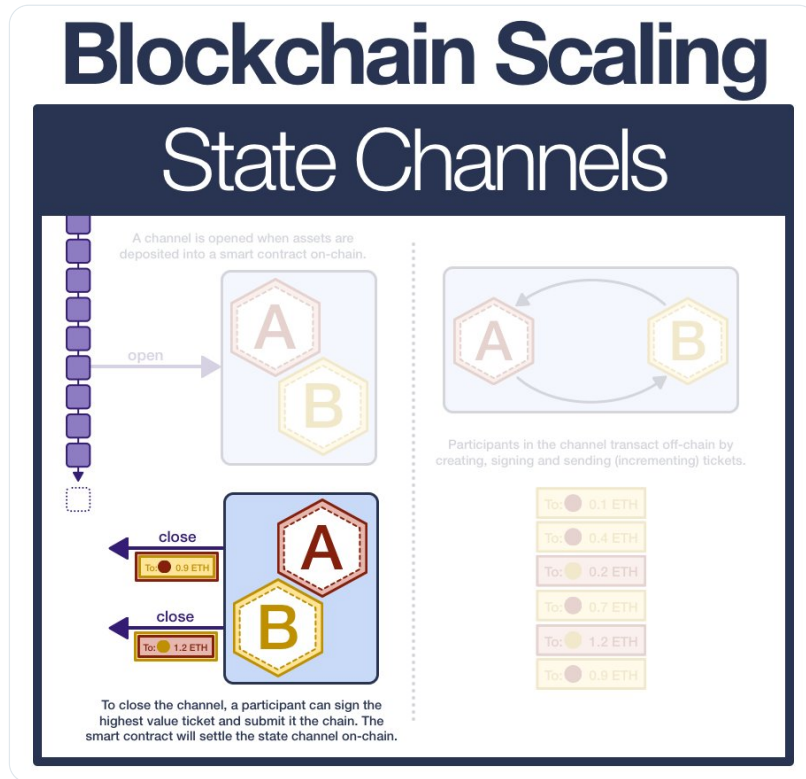
(8/14) Within the state channel, participants can send each other funds for little to no cost.

To make a payment, a user signs a ticket (off-chain message) and delivers it to the recipient. This can continue for as many payments as needed.



(9/14) When the participants are done transacting, they can sign and publish the highest-value ticket back to the main blockchain.

The smart contract will verify the signatures and settle the state channel (paying the receiver and sending the rest to the original owner)



(10/14) If one party is unwilling to close the channel (malice, tech failure, etc), the other participant(s) can initiate a withdrawal period.

If the unwilling party does not provide a ticket within the withdrawal time, the withdrawing participant gets all his/her money back.

(11/14) Example: Alice is offering fuel for \$1.3/L, Bob needs fuel.

Bob sends \$20 to a smart contract and begins pumping fuel. After every liter, Bob signs a new ticket, incrementing by \$1.30. When he reaches 10 liters, he's done.

(12/14) Now, Alice takes the highest value ticket (\$13), signs it and posts it to the smart contract in order to close the state channel.

The smart contract validates the ticket, and then settles the channel. \$13 are sent to Alice and the remaining \$7 are sent to Bob.

(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

(14/14) Researchers have been working to address these issues, however we have found better solutions... first plasma chains and then rollups.

Today, state channels are only used for niche apps and chains that cannot support modern scaling solutions.

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 Salomon**
@SalomonCrypto · Follow 

(1/14) Blockchain Scaling: State Channels

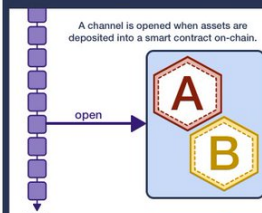
@Bitcoin, **@ethereum** and all (good) blockchain computers share one important quality: they are SLOW. State channels are the first attempt at changing this and bringing blockchain to scale.

Your guide to the original scaling tech.

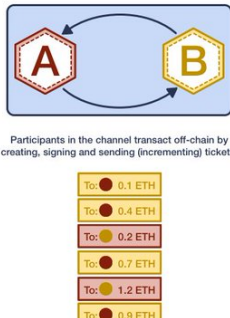
Blockchain Scaling

State Channels

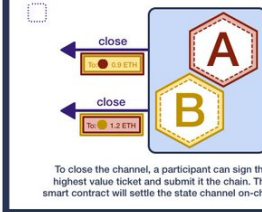
A channel is opened when assets are deposited into a smart contract on-chain.





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.



3:25 PM · Sep 10, 2022 

 [Read the full conversation on Twitter](#)

 8  Reply  Copy link

[Read 2 replies](#)

...