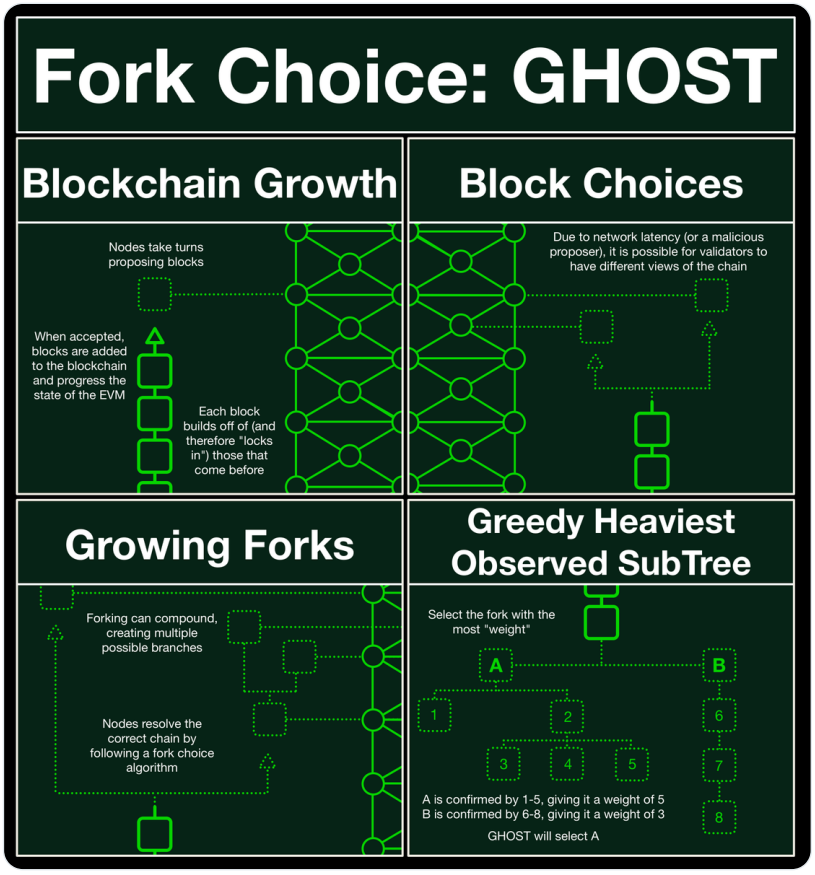
Haym @SalomonCrypto

Oct 1 • 17 tweets • SalomonCrypto/status/1576016595452731394

(1/16) @ethereum Consensus: LMD-GHOST

The World Computer coordinates via Proof of Stake. Most of the time, consensus is orderly and the blockchain grows 1 by 1.

But sometimes, a choice appears... and that's why we have our fork-choice rule.



(2/16) @ethereum exists between a network of 1,000s of computers, each running a local version of the Ethereum Virtual Machine (EVM).

All copies of the EVM are kept perfectly in sync. Any individual EVM is a window into the shared state of the World Computer.

(3/16) Keeping 1,000s of copies of the EVM in sync is trivial... if we are willing to have them all sync to a centralized server.

Unfortunately the easy solution breaks the core principle of @ethereum: credible neutrality through decentralization.

(4/16) Fortunately, we have a solution: decentralized consensus!

A consensus mechanism is the system a blockchain uses to keep all its nodes in sync.

Until recently, Ethereum used Proof of Work (PoW); ~2 weeks ago we experienced The Merge and switched to Proof of Stake (PoS).

(5/16) Both PoW and PoS are systems that designate a "leader" node and allow them to progress their copy of the EVM forward (using transactions submitted from users like you and me).

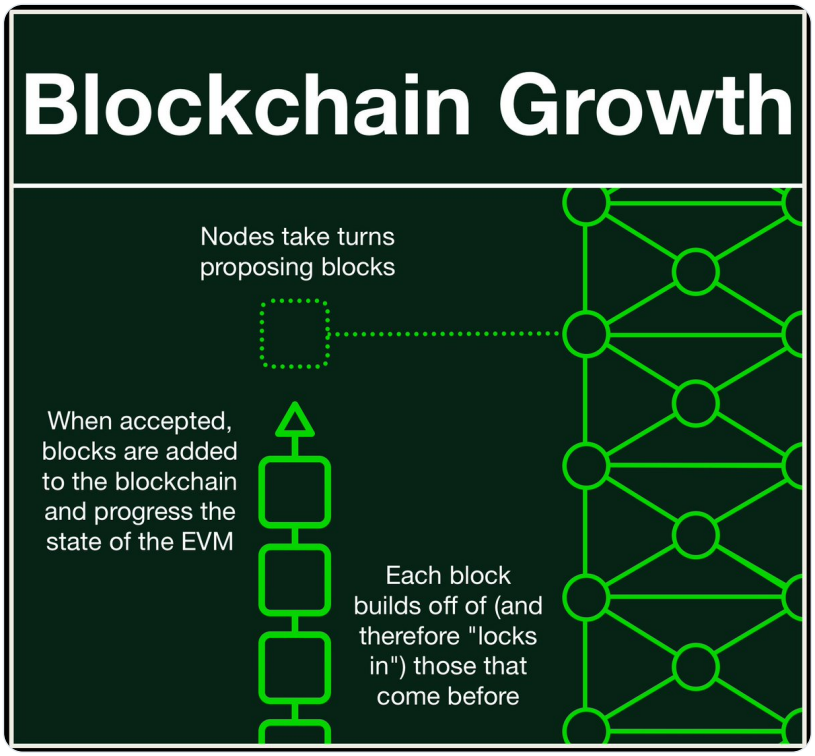
Once they have done as much transactions as they can, they create a block.

(6/16) A block is a complete record of all the transactions that occurred within the EVM during each node's turn at being leader.

Any other node can read the block, process the transactions and progress their copy of the EVM to match the leader.

(7/16) Every ~12 seconds (called a slot), a new leader is chosen. The leader selects txns, runs them through their local EVM, builds a block and publishes it to the network.

When other nodes receive blocks, they run the enclosed txns locally thereby syncing their local EVM.



(8/16) Progressing the state of the EVM is predicated on the state of the EVM at the beginning of the transaction.

By accepting the next transaction, each node (and therefore the network/World Computer) is confirming every transaction that came before it.

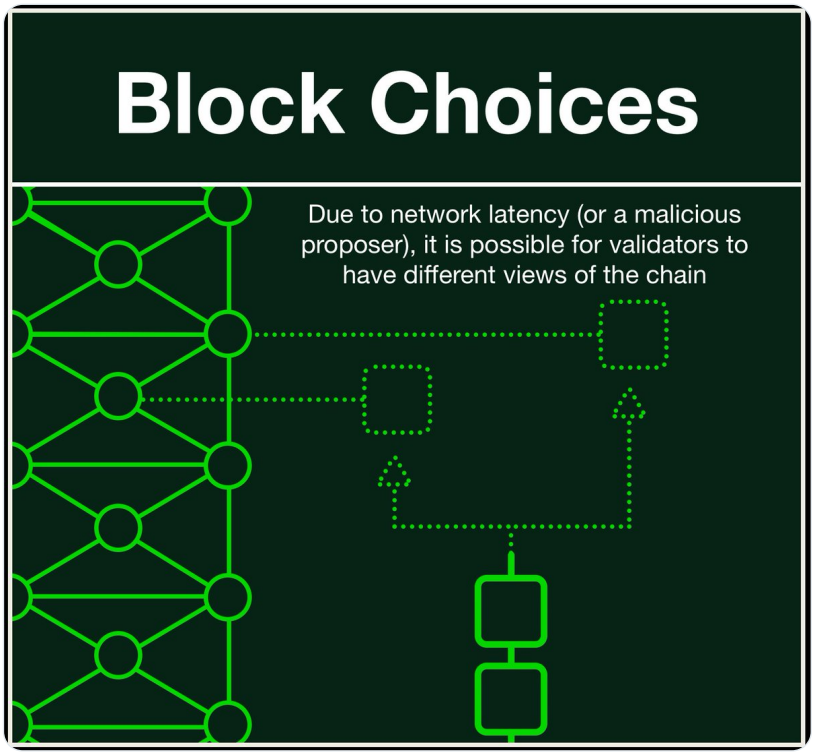
(9/16) Here's a quick example to illustrate the principle:

Transaction #5 is not possible unless transaction #4 happens first (Bob will not have the 11 he intends to send). By executing #5, we are confirming that #4 MUST have happened (and those before it as well).

Transaction	To	From	Amount	Balance	
				Alice	Bob
1	Alice	Bob	2	12	8
2	Alice	Bob	6	18	2
3	Bob	Alice	5	13	7
4	Bob	Alice	4	9	11
5	Alice	Bob	11	20	0

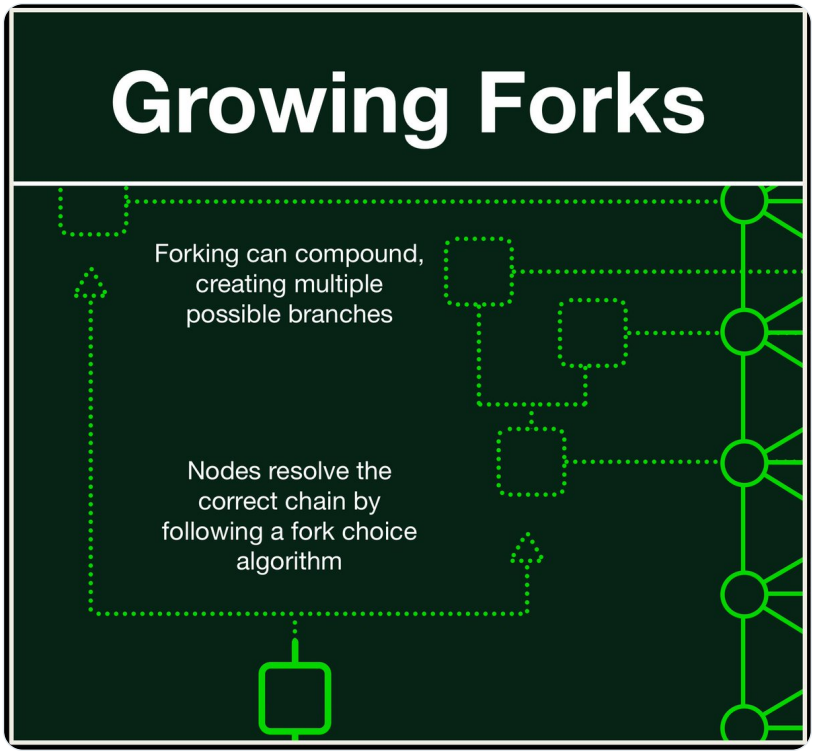
(10/16) In normal circumstances, the blockchain grows 1 by 1; each leader orderly proposes a new block which is accepted by the network and added to the blockchain.

However, the network can fall out of sync and nodes can be presented with more than one validly constructed block.



(11/16) A choice is called a fork, and a fork can grow.

If the network falls out of sync, it might fall out of sync for more than one slot. As the issue persists, the forks will branch wider and deeper, presenting more and more choices.



(12/16) Choices are an existential danger to systems trying to stay in sync. If a node operator has discretion, he might make a choice different from another node operator.

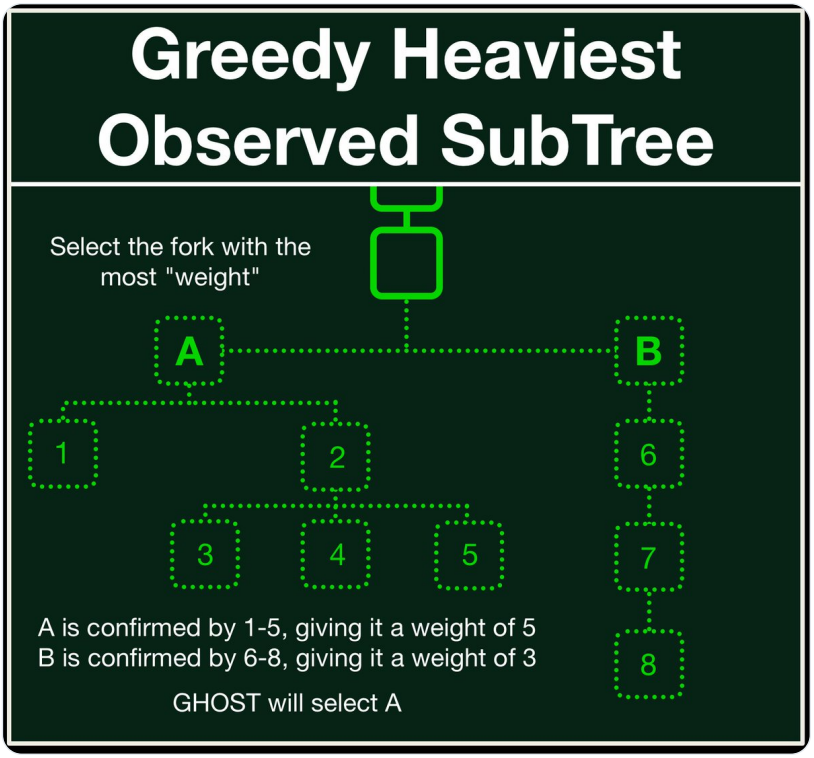
Instead of a choice, the node operator gets a fork-choice algorithm.

(13/16) A fork-choice algorithm (also called a fork-choice rule) is a function that takes in all the possible branches and outputs the one single "canonical chain."

All node operators share the fork-choice rule. Therefore all nodes act in unison when faced with a choice.

(14/16) Greedy Heaviest Observed SubTree (GHOST) is a fork-choice rule that selects the fork with the greatest accumulated weight (number of confirmations).

In this example, GHOST would confirm block A even though B has a longer chain.



(15/16) @ethereum has implemented a modified version of GHOST called Latest Message-Driven GHOST (LMD-GHOST).

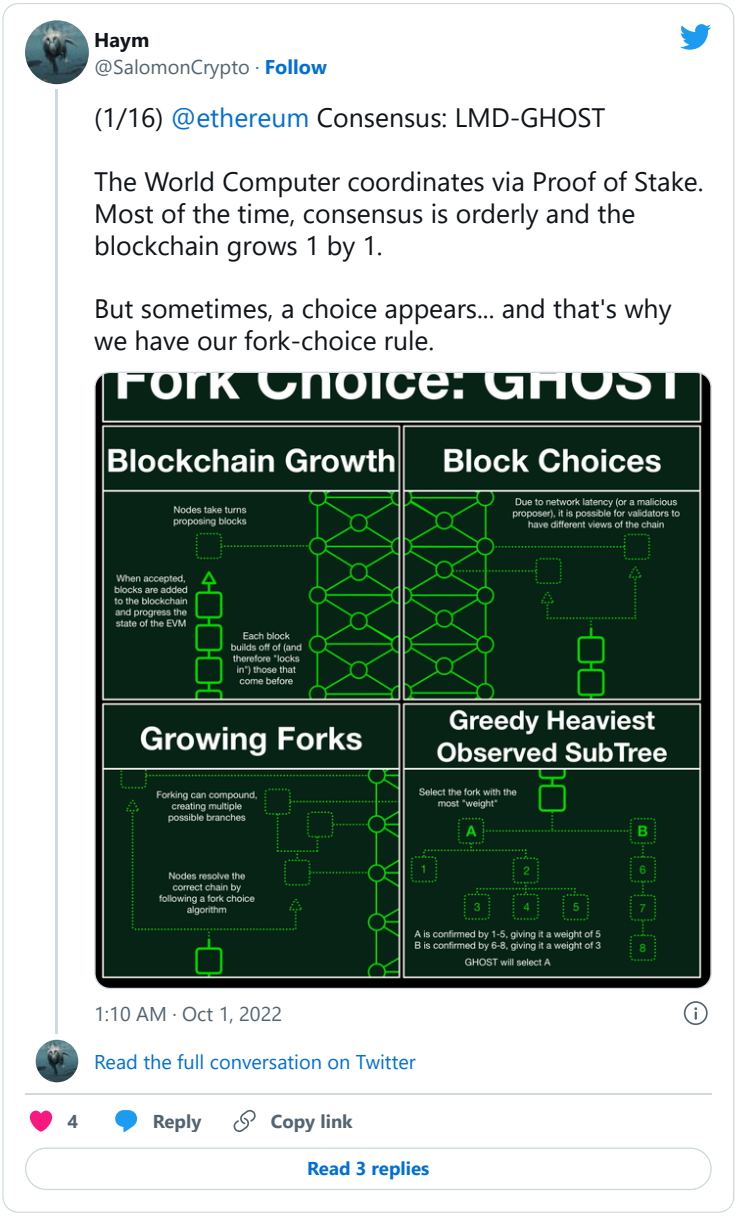
This describes the decisions made if multiple messages are received from a node. LMD-GHOST will only consider the latest one, discarding the rest.

(16/16) LMD-GHOST is a critical part of keeping @ethereum in sync. Without a fork-choice algorithm, normal network congestion could push the network into a chaotic spiral, accelerating further and further out of sync.

LMD-GHOST provides clarity when a node gets confused.

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.



• • •