



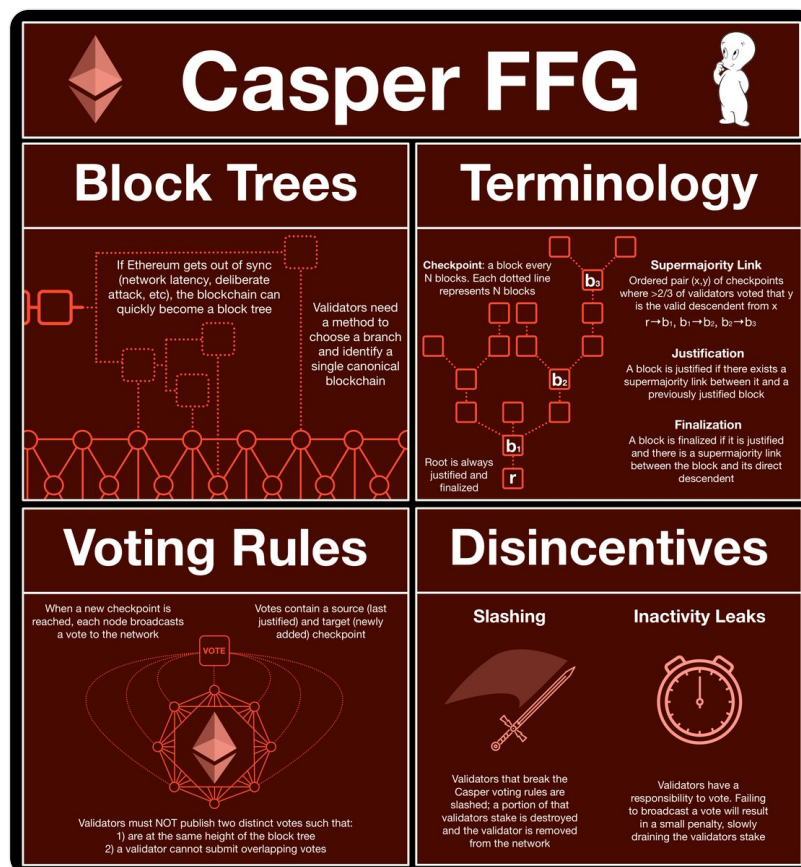
Haym @SalomonCrypto

Oct 2 · 23 tweets · [SalomonCrypto/status/1576721911265996800](https://twitter.com/SalomonCrypto/status/1576721911265996800)

(1/22) [@ethereum](#) Consensus: Casper FFG

The World Computer coordinates via Proof of Stake; validators place \$ETH at stake in order to participate in the system. But what actually IS this system and how does it achieve consensus?

A guide to Ethereum finality.



(2/22) [@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.



(3/22) The EVM stays in sync through a process called 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).

(4/22) Both PoW and PoS are systems that designate a "leader" node (validator) 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 many transactions as they can, they create a block.

(5/22) 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.

**Haym**
@SalomonCrypto · [Follow](#)



(1/21) [@ethereum](#) Fundamentals: PoS Blocks

In less than 1 week, the Ethereum blockchain will Merge with the Beacon Chain and the World Computer will transition from PoW to PoS. The blockchain will never be the same.

A field-by-field guide to on-chain future.



The diagram, titled "Ethereum Blocks (PoS)", is divided into three main sections: Consensus Layer, Execution Layer, and Ethereum Transaction. The Consensus Layer includes a PoS Block (with sub-sections for Administration, Consensus, and Execution), a Consensus table, and an Execution table. The Execution Layer includes an Execution table, a Header table, and a Transactions table. The Ethereum Transaction section includes a Transaction table, a Metadata table, a Cache table, and a Data table. Each table contains various fields and data points related to the Ethereum PoS system.

10:28 PM · Sep 9, 2022



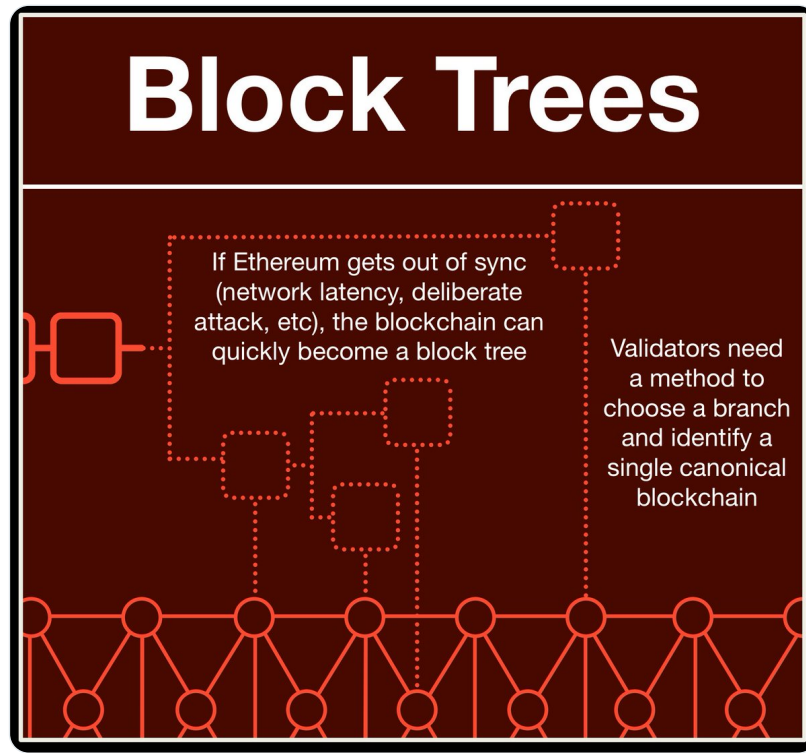
 [Read the full conversation on Twitter](#)

 481  Reply  Copy link

[Read 37 replies](#)

(6/22) During normal operation, every ~12 seconds a leader is chosen, who then builds and proposes a block.

However, the network can fall out of sync and more than one node might broadcast a validly produced block.



(7/22) One of these choices is called a fork, and forks can grow.

Even small forks are existential threats to a distributed system. Without one true blockchain, the independent EVMs on each node must decide which txns to execute.

(8/22) This creates an issue for both the nodes of the network and the users of the network:

The nodes can't be certain which is the one true path through the block tree.

The users can't be certain if their txns are on the "true" path; if they aren't they won't count.

(9/22) Casper the Friendly Finality Gadget (FFG) was introduced by [@VitalikButerin](#) and Virgil Griffith in 2019 to provide block certainty.

BTW, all of you should know who Virgil Griffith is; he is paying for his belief in [@ethereum](#).


<https://arxiv.org/pdf/1710.09437.pdf>

(10/22) Casper FFG is a process that exists atop a block proposal mechanism; it is responsible for finalizing these blocks, canonizing the true [@ethereum](#) blockchain.


Casper consists of two main parts: the finalization algorithm and the penalization scheme.

(11/22) The finalization algorithm draws from the field of research derived from the Byzantine Generals Problem.

The field looks for answers to the question "how can members of a network agree on a specific reality when no one can verify the identities of other members?"



Haym
@SalomonCrypto · [Follow](#)

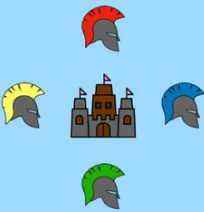


(1/21) Byzantine Fault Tolerance (BFT) and the Practical Solution (pBFT)

What is the Byzantine Generals Problem? Why is it important for distributed systems? Does this problem have a solution?

A guide to the core principles underlying decentralized consensus.

Byzantine Generals Problem

























A city is surrounded by several divisions of the Byzantine army, each commanded by its own general. The generals can only communicate by messenger.

If all generals attack, the city will fall. If all generals retreat, the army will live to fight another day. If some generals attack and some retreat, the entire army will be lost.

Some generals are loyal, some are traitors.


How can the Byzantine generals reach consensus?


Victory through Consensus


					
					
					
					
Result	Win	Win	Lose	Lose	Lose


6:55 PM · Oct 1, 2022



[Read the full conversation on Twitter](#)

 500


 Reply

 Copy link

Read 12 replies

(12/22) Casper is derived from a particular solution to the Byzantine Generals Problem called practical Byzantine Fault Tolerance (pBFT).

pBFT is a two vote process. After both votes, consensus can always be reached (as long as $>2/3$ of the validators are honest).

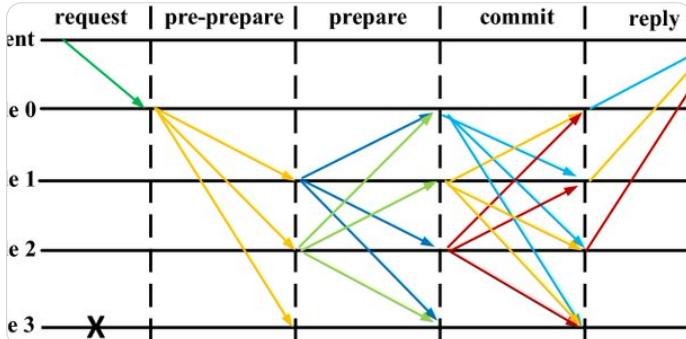
 **Haym**
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(18/21) This is the typical diagram you will see; IMO it's pretty inaccessible.

Node 0 is the leader, who broadcasts the action to the rest of the group (pre-prepare).

Then each member of the group broadcasts its received message to all other members (prepare).



6:55 PM · Oct 1, 2022

6 ❤️ 6 💬 Reply 🔗 Copy link

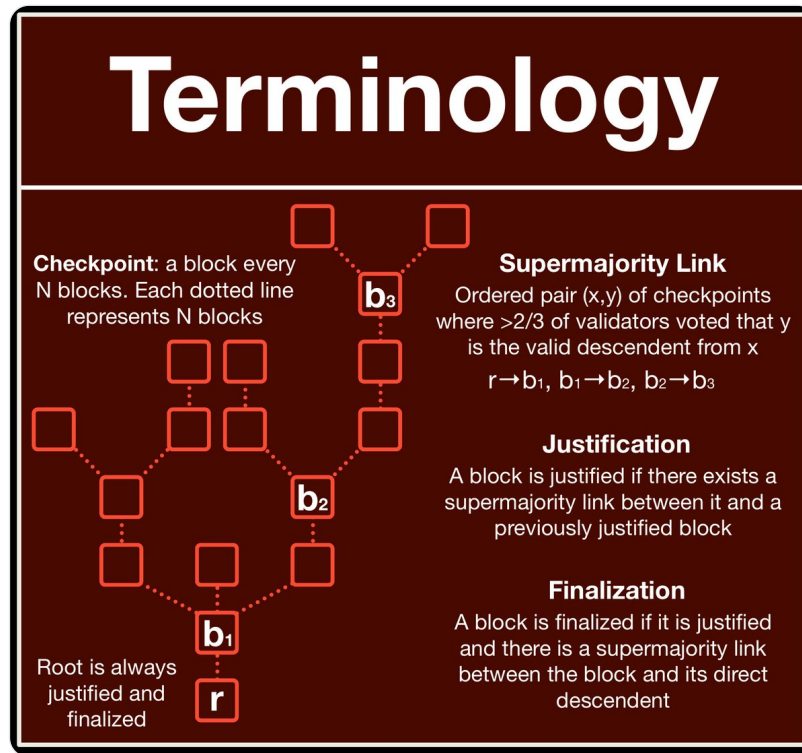
Read 1 reply

(13/22) At its core, pBFT uses a voting scheme to provide mathematical certainty that a decentralized network has made a collective, final decision.

This is the principle that Casper applies: finalization certainty for [@ethereum](#).

(14/22) Rather than finalizing blocks, Casper finalizes "checkpoints," a single block once every N blocks (N = 32 blocks for PoS).

The Casper equivalent of pBFT's voting is called a "supermajority link," meaning $>2/3$ s of validators confirmed the validity of the checkpoint.

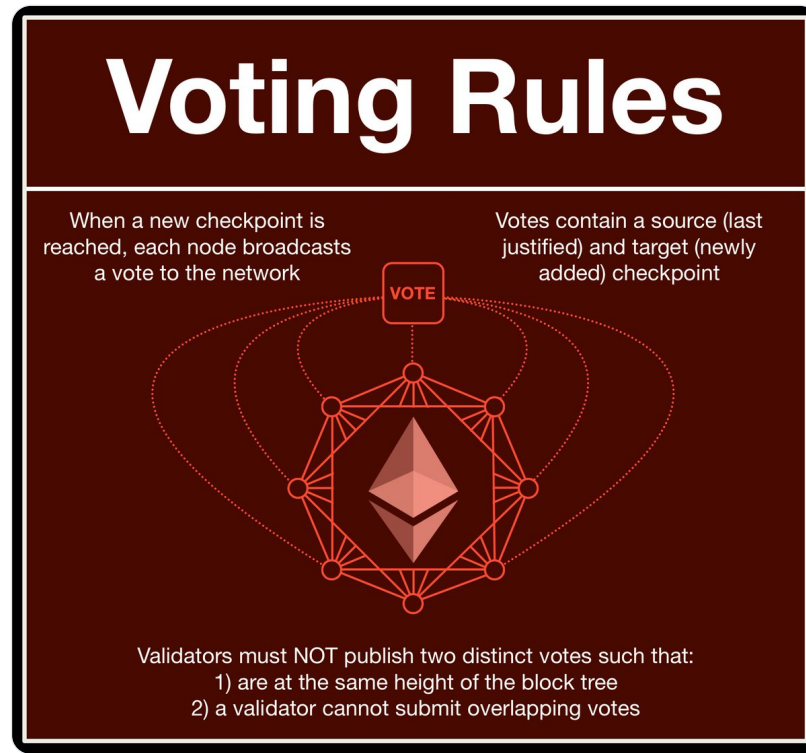


(15/22) The two rounds of voting in pBFT are called prepare and commit; at the end of commit the action is final.

In Casper, these ideas have different names: if a checkpoint has been confirmed once it is "justified." If it has been confirmed twice it is "finalized."

(16/22) Every time a checkpoint is reached, each validator is responsible for evaluating the block and creating a vote.

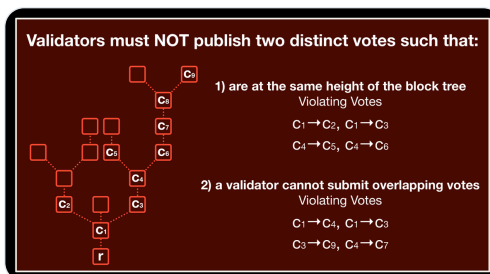
A vote simply marks the source checkpoint, the target block, proof of validity and the validator's signature.



(17/22) These votes are both a privilege and a responsibility of being a validator.

Successfully voting earns \$ETH rewards, but missing votes will incur an \$ETH penalty.

Voting maliciously will incur a much bigger penalty and get the validator removed from the network.



(18/22) Building on the pBFT and the other research around the Byzantine Generals Problem, we can mathematically prove that these properties round out a robust BFT system.

This thread is long enough, but the proofs are in the original Casper paper (tweet 9).

(19/22) BFT systems have two properties: safety (any txn run by one node will be run by all) and liveness (consensus cannot stall).

Casper FFG is not a full BFT algorithm (hence "gadget"). It will guarantee safety, but liveness depends on the proposal mechanism.

(20/22) However, Casper does provide new properties:

- Accountability, violations of Casper can be detected and the violator can be identified
- Defenses, against long range revision attacks and situations where $>1/3$ of nodes are offline
- Dynamic, nodes can be added or removed

(21/22) Casper FFG is a Proof of Stake system derived from decades of research - however it is not entirely complete.

For one, there is no block proposal method. For another, Casper does not direct validators which checkpoint to pick if it needs to make a choice.

(22/22) Fortunately, research did not stop in 2019; in fact, it still continues to this day, building on the work of pBFT and Casper.

And before long, Casper will become mature enough to take center stage, Merge with LMD-GHOST and provide consensus to [@ethereum](#).

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](#)



(1/22) [@ethereum](#) Consensus: Casper FFG

The World Computer coordinates via Proof of Stake; validators place [\\$ETH](#) at stake in order to participate in the system. But what actually IS this system and how does it achieve consensus?

A guide to Ethereum finality.



The infographic is a 2x2 grid with a dark red background and white text. The top-left quadrant is titled 'Block Trees' and shows a diagram of a block tree with a fork. The top-right quadrant is titled 'Terminology' and defines 'Block', 'Supermajority/Quorum', 'Proposer', and 'Finalization'. The bottom-left quadrant is titled 'Voting Rules' and shows a diagram of a block with a vote. The bottom-right quadrant is titled 'Disincentives' and shows icons for 'Slashing' (a sword) and 'Inactivity Leases' (a clock).

...