Proof-of-Stake Consensus in the Doge Protocol Blockchain

Authors: The Doge Protocol Community

Publication Date: November 2021

Contents

Introduction

Doge Protocol will be a Quantum Resistance blockchain that initially will use Proof-of-Stake (PoS) consensus and later move on to a PoW+PoS hybrid consensus scheme. This whitepaper is a summary of the Proof-of-Stake consensus system. A follow-up whitepaper will cover the various parts of the consensus scheme in detail.

At a high level, the Doge Protocol blockchain is a BFT chain that will closely follow Casper CBC consensus model while adjusting the protocol to improvise the liveness property. The blockchain also takes some inspirations from PolkaDot and Near Protocol consensus schemes.

The uber goal is to build a robust blockchain that's resistant to byzantine failures while at the same time is decentralized and scalable. We shall see the tradeoffs involved as part of this design.

Design Principles

The Doge Protocol consensus system will follow the below design principles.

- Abstract
  The consensus scheme itself will be abstract, leaving out details like cryptography, hardware, programming language etc. to implementation.

- Security
  Secure the network in adversarial conditions while at the same time maintaining a fine balance with liveness.

- Decentralization
  The consensus platform will favor decentralization moderately over scalability. It's a fine balance between decentralization and scalability that Doge Protocol blockchain aims to achieve.

- Scalability
  The consensus model should be adaptable to improving hardware and

network speed over a period of time, as a way to increase transactions per second (TPS) (which also improves the usability).

Out of Scope

The below topics will be covered in follow-up whitepapers.

- Economics
  While validator rewards, slashing are covered in general in this whitepaper, the actual percentages and reward models will be left to implementation detail.

- Cryptography, Randomness & Sortition
  The quantum resistance of Doge Protocol blockchain has been already covered in a different whitepaper. Randomness, Sortition and Forward Secrecy will be covered in a different whitepaper.

- Data Availability
  Data Availability is an important part of any blockchain. This topic will be covered in a whitepaper of its own, detailing incentives as well as how it would fit in the overall blockchain model.

- Sharding
  Sharding is a future improvement and will be covered in a whitepaper of its own. However, we briefly touch upon this topic in this whitepaper.

- Hybrid PoW + PoS
  The proof-of-work + proof-of-stake consensus system is a future improvement to improve decentralization and will be covered in a follow-up whitepaper. We briefly touch on the motivation for this hybrid model in this whitepaper.

- Smart Contract Specifics
  The implementation details of the smart contract such as programming language will be covered in a different whitepaper.

- Hardware Requirements
  While hardware requirements are important, the consensus scheme will not detail specific hardware and TPS requirements but will be abstract.

- Staking Details
  Proof-of-Stake systems need an initial stake to kickstart the blockchain. This wouldn't be covered as part of the consensus whitepaper.

- Satellite Chains
  The mechanism in which satellite chains would plug into the Doge Protocol blockchain will not be covered in the consensus scheme itself, however it does play an affect on the underlying scheme. The consensus adjustments will be detailed in a different whitepaper.

Terminology

Block

A list of transactions combined with other metadata forms a block.

Clients

A client refers to an account that wants to send a transaction for inclusion in the blockchain, such as sending funds to another account.

Proposer

A proposer will propose a block for inclusion in the blockchain.

Validator

A validator notarizes the blocks proposed by the proposer, for inclusion int the blockchain. Validators also become block proposers based on the validator selection algorithm.

Committee

A committee is a set of validators who are selected to form a block.

Inspector

An inspector is an actor who can inspect any block and oppose it, typically to catch fraudulent transactions.

Slot

A slot is a fixed interval in which blocks are created. Its also the block-time of the blockchain.

Epoch

An epoch is a period denoted by N sequential slots.

Staking

A validator can stake coins to run a validator node which becomes part of the underling blockchain network.

Rewards

Rewards are paid to validators, proposers, and inspectors for running and securing the blockchain network.

Slashing

Slashing is used to penalize bad actors in the blockchain network (including validators, proposers, and inspectors).

Slots and Epoch

A blockchain is comprised of blocks which represent a set of transactions that were committed into the block, along with metadata such as notarizations of validators, block-number and so on.

In Doge Protocol, a block is created in roughly fixed intervals (T seconds) denoted by a Slot. Each slot has one block. A set of N sequential slots form an epoch.

A committee is assigned to create each block. A committee is a set of V validators that includes one Proposer. For example, if there are 1000 validators, a subset of these validators (say 128) will be selected for each S slot and will form the committee. Among these validators, one of them will be selected as a Proposer. The committee selection algorithm will be detailed in a different whitepaper (including proposer selection).

The committee itself will be rotated every S slots, so that more validators get a chance to take part in the block creation. This also improves the decentralization factor of the blockchain network.

Happy Case

In this section, we will see how a block is created in an ideal environment where there are no bad actors and network conditions are also ideal.

1) A committee (validator and one proposer) is selected for a set of S slots in each epoch (say E1). Let's say, there are S slots in this epoch.
2) Various clients send their transactions to the blockchain network.
3) Validators and the proposer for a slot also receive these transactions (in the ideal case).
4) The proposer proposes a block with the list of transactions to include in the block, the block height, other metadata and signs this payload with the proposer's key.

5) The proposer sends this proposed block to other validators in the committee and is also passed on to the other actors in the network.
6) Each validator in the committee will check the block to see if it contains the transactions as expected. They will also verify that the proposer is indeed part of the committee and verify the signature.
7) After verifying, each validator will notarize the block by signing it with their validator key and send this notarization to other validators, actors in the network.
8) Other validators will validate the notarization by verifying that the validators are indeed part of the committee for that slot and will verify the signature of the validators. Note that the validator votes are weighted by number of coins staked, hence not all validator votes are equal.
9) Inspectors will look at the block and the notarization from validators. If they find them valid, inspectors will perform no other action in that slot.
10) Validators, proposers, and other actors on receiving at-least 2/3rd valid notarizations of the proposed block will commit the transactions in their local state. Note that 2/3rd is an example, and the actual constant will be detailed in an over-arching whitepaper.
11) Subsequently the next slot follows the same routine until it's the first slot of the next epoch.
12) In the first slot of the next epoch (and each epoch), transactional hashes of the state of the chain and additional metadata are also stored and signed by validators and proposers.

Rewards

Proposers and Validators earn coins as rewards for running and securing the network. When validators accept a block proposed by the Proposer, the Proposer earns block rewards in the form of coins. Likewise, when Validators notarize a block that's accepted by the other committee members, validators also earn rewards. Inspectors also earn rewards for detecting and reporting fraudulent transactions.

Slashing

Slashing is a way of penalizing bad actors in the system by removing a certain percentage of their staked coins and using it for other purposes including rewarding other honest actors. The economic model to be detailed in a follow-up whitepaper will ensure that the percentage slashed is a reasonable sum to keep the network secure as a hedge against the bad actors.

Byzantine Fault Tolerance

This section details the how various failure conditions in the Doge Protocol blockchain are handled.

Bad Proposer

A bad proposer can propose a block with one or more fraudulent transactions. A bad proposer may also send different transactions to different validators for the same block. Under ideal network conditions, Validators will detect the invalid block and will reject the transactions. The proposer selection algorithm will also kick-in again to select a different proposer who will propose a new block and so on.

Under bad network conditions (network partitioning), it's possible that some validators received correct transactions while a few received invalid transactions

in the block. However, validators will commit the transactions in the block only if more than 2/3rd of the validators in the committee notarized the block.

Its also possible that there is extended network partitioning and less than 2/3rd of the validators were able to receive notarized transactions from others in the committee, thus stalling the block creation. We will see how the system behaves in this scenario in the liveness section.

Bad Validator

A bad validator can send different blocks at the same height and broadcast it. A bad validator might also collude with other validators in the committee or the proposer and might also attempt to bribe other validators. Sometime validators might also appear as bad actors due to software bugs, especially during network problems when message deliveries might be delayed or reach out of order.

As long as more than 2/3rd of the validators are good validators, the network will continue to create a new block. Under some circumstances, it's possible that the validator managed to collude or control the committee. An inspector can step up in this case and broadcast to the network that the block is invalid.

Other honest actors who are not part of the committee but are candidates to become validators (in other words those who have staked coins) can detect the fraudulent transactions from the bad validator(s) and slash the bad actor's coins. As long as more than 2/3rd of actors are honest, the fraudulent transactions can be avoided.

Bad Inspector

A bad inspector might likewise point out that certain valid transactions are fraudulent. In this case, like validator slashing, the staked coins of the inspector is also slashed, as long as more than 2/3rd of the honest actors agree.

Nothing at Stake

Another form of a bad actor is the lazy actor who doesn't do any work and either shutdowns the node or just notarizes blocks blindly without storing state.

In one case, the validator node might be shutdown and not participating in the network anymore. In this case, there will be periodic slashing though at a lower scale, since its possible the validator node has run into software bugs or transient hardware/network issues.

In the second case, the validator might just blindly notarize transactions but doesn't invest in storing the state of the blockchain. We shall see how the slashing is performed in this case, in the Data Availability whitepaper.

Liveness

The liveness property of the blockchain is equally important to security and safety guarantees. The liveness property indicates the ability of the blockchain to keep producing new blocks under poor network conditions and adversarial conditions.

Let's look at some conditions that test the liveness property.

1) Poor network, no bad actors
   In this case there could be network partitioning and poor network conditions causing out of order message delivery, delayed message delivery. As long as more than 2/3rd of the validators are available, the network will continue to function the normal sequence of steps. We shall see the extreme case next.

2) Dead validators, no bad actors
   In this case, either due to network partitioning or actual dead hardware, more than 1/3rd of the nodes might be dead or unavailable. For example, there could have been a major internet problem worldwide or in a large country having many validators. The nodes themselves could have shut-down and not return-back.

   In these cases, after a fixed period of time Y (fencing window), the slot is

abandoned by the remaining validators. They send a slot abandonment message to the other validators and again wait for another fixed period of time Y. Post this, a new committee is formed by the selection algorithm that will include a new set of validators. The rest of the sequence resumes.

Its also possible that some of the validators came back after a brief outage in the network. Validators who haven't been able to sync with more than 2/3rd of the validators over a period of time Y (the fencing window), will treat their slot as abandoned and will sit out of the committee for that slot.

3) Poor network, bad actors
   This is an extremely adversarial condition. Sometimes the poor network conditions might have been caused due to denial of service by adversaries. The inspector approach wherein any good actor can earn reward by pointing to fraudulent transactions will prevent the fraudulent transactions. As long as more than 2/3rd of the overall actors are honest (not just validators), the blocks will continue to be produced.

Finality and Reconciliation

A block is finalized over two epochs, if the previous two blocks have been finalized and no inspector has pointed out to fraudulent transactions. If fraudulent transactions have been detected, for example due to validators notarizing different blocks at the same height, there will be reconciliation based on LMD Ghost fork choice approach (see appendix).

Summary

The Doge Protocol consensus whitepaper outlines typical problems that can happen on a Proof-of-Stake consensus blockchain and how the system works around it. A lot of the items are kept abstract and high level, leaving specifics to implementation details, on purpose. Some essential properties of the blockchain like "Data Availability" will be detailed in follow-up whitepapers.

Appendix

- LMD Casper https://arxiv.org/abs/2003.03052
- Casper CBC https://vitalik.ca/general/2018/12/05/cbc_casper.html
- Near Protocol Whitepaper https://near.org/papers/the-official-near-white-paper/
- Polkadot GRANDPA consensus https://wiki.polkadot.network/docs/learn-consensus