Consensus Introduction

Decentralized consensus algorithms require Sybil resistance, using a resource that is both cryptographically verifiable and scarce (not infinite). In previous blockchain systems, two different scarce resources have been used: computing power (Proof of Work) and staked money (Proof of Stake).

Proof of Space and Time consensus uses storage capacity as the scarce resource. This comes much closer than previous systems to Satoshi's original ideal of "one CPU, one vote," where a *vote* refers to a chance to win and validate a block, not an actual vote on-chain. For example, someone storing 500 GiB has 5 "votes," and someone storing 100 GiB has 1 "vote."

One other cryptographic puzzle piece is used to secure BPX: a verifiable delay function (VDF), which is a cryptographic proof that real time has passed.

A fair system can be created by combining proofs of space and time. In such a system, users store random-looking data on their hard drives. Their chance to win BPX is proportional to their allocated space. Furthermore, such a system scales to billions of participants in a similar way to the Proof of Work lottery. No funds, special hardware, registration, or permission is required to join, only a hard drive and an internet connection. The system is completely transparent and deterministic - anyone can efficiently and objectively verify which chain is the canonical one, without relying on any trusted parties.

Some notes to keep in mind as you continue reading:

- Whenever the word *signature* is used, it refers specifically to a deterministic BLS signature, following the IETF specification with the Augmented scheme.
- The private keys performing these digital signatures are controlled and stored by the farmers.
- A unique private key is used for each plot.
- The hash function used is SHA256, except for the proofs of space which also use CHACHA8 and BLAKE3.

Revision #2
Created 5 June 2023 11:22:36 by Admin
Updated 6 June 2023 06:12:46 by Admin