Blockchain Storage – Summary

Blockchain storage is one of many applications of blockchain technologies following the development of Bitcoin. As with most such applications, the main advantage is decentralization. Some users would rather have their data spread across the world, so that there is not a single point of failure. One representative of such a system is IPFS – Interplanetary file system. IPFS can also host websites in a distributed manner, and it uses a content-based addressing, where the stored files are addressed by the content. It is important to note that IPFS needs an incentive system to work and ensure security of the files, so it uses its own incentive layer: Filecoin. However, the two work independently.

Structure

All data is split in chunks or blocks, and every block is identifiable by a content identifier (CID). Merkle directed graphs are used, which are very similar to Merkle trees in Bitcoin. Since IPSFS is content based, there are no duplicates. Even files that are not the same, but share a certain part, will share the same CID for that part.

There are 3 different types of orders: bid, ask and deal. Bid is done by the client to store or retrieve data. Ask is a node announcing the conditions to do that. Finally, the deal connects the two. Every order will be stored in orderbook, which is stored on-chain as well.

The execution of deals is ensured via PoRep (proof-of-replication) and PoST (proof of space time).

Use cases

- Coordinate botnets
- Often combined with blockchains when storing data is wanted, the blockchain can then provide integrity/authenticity or just point to the data.
- Can be used for archiving websites or storing data in general without blockchain