Filecoin Summary

Truebit

What is Filecoin?

Filecoin is a blockchain built on top of IPFS to further act as an incentivization layer for storage and retrieval of data. Filecoin features two Proofs of Storage(PoS), namely Proof of Spacetime and Proof of Replication. We will further discuss these PoSs in detail further one, but here's a short explanation for now:

Proof Of Spacetime

It's used to prove that the storage miner is indeed storing the data for the agreed-upon duration.

Proof Of Replication

It's used to prove that the storage miner is indeed storing the data in the agreed-upon number of physically distinct locations.

Miners

Miners collectively and individually assume three separate roles in the Filecoin ecosystem:

- **Storage Miners**: The group of miners that pledge to store data.
- **Retrieval Miners**: The group of miners that pledge to retrieve data from the storage miners.
- **The Network**: The aggregate of all users that are running full nodes. The network handles the repair of data and validation of the proofs.

There are also the so called `clients` that use the retrieval and storage services without directly dealing with the blockchain itself.

Definitions and Concepts

Next we will take a look at some definitions and concepts for Filecoin:

Storage Miners

Storage miners pledge a certain amount of storage and put up the same amount in collateral proportional to their pledged storage amount.
Storage miners will post periodic proofs of space time that prove they are storing the data for the pledged amount of time onto the blockchain which is in turn verified by the `network`.
In case the proofs are invalid or missing, the storage miner will be penalized and loose part of their collateral.
Storage miners are eligible for mining new blocks in which case they will be given the reward for mining a new block and a percentage of the transaction fees inside the block.

Retrieval Miners

Retrieval miners provide data retrieval to the network.
Retrieval miners are not required to provide proofs of storage.
Clients pay them for every piece they retrieve, when they retrieve it.
Retrieval miners can also act as storage miners.
Retrieval miners can obtain pieces directly from clients(?) and the Retrieval market.

The Network

The aggregate of all the Filecoin full nodes.
The network, at every new block, handles managing the available storage, validates pledges, audits the storage proofs and tries to repair possible faults.

The Ledger

Is a sequence of transactions(TXs).
At any given time, the users have access to the ledger at the given time.
The ledger is append-only.
Filecoin's ledger is built using **useful work**.

Markets

Filecoin features two separate decentralized exchange markets, namely the Storage Market and the Retrieval Market.
Clients and miners(storage and retrieval) set the prices for their services in the respective markets.
The exchanges provide a way for the clients and miners to see matching offers and initiate deals.
The network guarantees that the services are provided and that the miners get paid for the provided services.

Data Structures

Filecoin features a number of prominent data structures. Knowing the contents and the role they play will help us have an overall better understanding of how Filecoin works so we will go through them one by one:

Pieces

A `piece` is some part of data that a client is storing on the network. Data can be deliberately broken into many pieces and stored by different storage miners.

Sectors

A `sector` is some disk space that a storage miner pledges to the network.

Data Structures

AllocationTable

The **AllocTable** is a data structure that keeps track of `pieces` and which `sector` they are being stored in.
The **AllocTable** is updated at every block in the ledger and its Merkle root is stored on the blockchain.
The table is used to keep the state of the DSN(**D**istributed **S**torage **N**etwork) allowing for quick look-ups during proof verification.

Data Structures

Orders

An `order` is a statement of intent to request or offer services.

Bid Orders

Clients submit `bid` orders to the networks depending on which service(storage or retrieval) they seek.

Ask Orders

Miners submit `ask` orders to offer their services. After a pledge order appears in the blockchain and the miner has paid the collateral, they can offer storage via ask.

Deal Orders

After an ask and bid order are matched and after the miner receives the data to be stored, the client and miner sign a `deal` order.

Data Structures

Orderbook

Orderbooks(one for each market) are sets of orders. For the Storage Market, the orderbook will contain `ask` orders from storage miners, `bid` orders from the clients who want to store data on the DSN and the matched orders(`deal` orders). The orderbook for the retrieval market features the same set of orders, but the `ask` orders come from retrieval miners instead.

Pledge

A `pledge` is a commitment to offer a `sector` to the network accompanied with a collateral respective to the actual size of the `sector`.

Blockchain contents

- Merkle root of **AllocTable**.
- Periodic proofs of storage which the network will verify.
- A `deal` order for the retrieval scenario
- `orderbook`

Consensus

- Useful work consensus protocol
- The probability that the network elects a miner to create the next block is proportional to their **storage currently in use**(not pledged) in relation to the rest of the network.
- The storage currently in use can be traced in **AllocTable**.

Consensus

Expected Consensus(EC)

The mathematical expectation of number of leaders for each epoch is 1 but some epochs might have 0 or more than one leaders. In case there are zero leaders, an empty block is created.
Leaders extend the chain by propagating a block to the network.
At each epoch, the chain is extended by one or more blocks.
The data structure is a directed acyclic graph.
EC is a probabilistic consensus. Each epoch introduces more certainty over the previous epochs' blocks until the likelihood of a different history is `sufficiently small`.
A block is committed if the majority of the participants add their weight on the chain where the block belongs to, by extending the chain or by signing the blocks.

System Parameters

A minimum amount of epoch of storage

Δ_{proof}

The interval between proofs of storage.

Smart Contracts

- Will feature a contract system based on Ethereum.
- Will provide a bridge system to bring Filecoin storage to other blockchains and to bring other blockchains' functionalities to Filecoin.

Questions

- How does proof of spacetime prove that the replicas actually are physically stored separately?
- Who keeps the collateral storage miners pay via pledge?
- In case a piece is `faulty`, the network will introduce a new order. Is there a cap on how many times the network will retry?
- Is there an oracle for the storage miners to use to set their price?
- Deal orders are submitted after receiving and sending files. What if the receiver in the retrieval scenario and the receiver in the storage scenario are dishonest?