Proofs

In Filecoin cryptographic proving systems, often simply referred to as proofs, are used to validate that a storage provider (SP) is properly storing data.

Different blockchains use different cryptographic proving systems (proofs) based on the network's specific purpose, goals, and functionality. Regardless of which method is used, proofs have the following in common:

- All blockchain networks seek to achieveconsensus
- and rely on proofs as part of this process.
- Proofs incentivize network participants to behave in certain ways and allow the network to penalize participants who do not abide by network standards.
- Proofs allow decentralized systems to agree on a network state without a central authority.
-

Proof-of-Work and Proof-of-Stake are both fairly common proof methods:

- Proof-of-Work
- : nodes in the network solve complex mathematical problems to validate transactions and create new blocks,
- Proof-of-Stake
- : nodes in the network are chosen to validate transactions and create new blocks based on the amount of cryptocurrency they hold and "stake" in the network.
-

The Filecoin network aims to provide useful, reliable storage to its participants. With a traditional centralized entity like a cloud storage provider, explicit trust is placed in the entity itself that the data will be stored in a way that meets some minimum set of standards such as security, scalability, retrievability, or replication. Because the Filecoin network is a decentralized network of storage providers (SPs) distributed across the globe, network participants need an automated, trustless, and decentralized way to validate that an SP is doing a good job of handling the data.

In particular, the Filecoin proof process must verify the data was properly stored at the time of the initial request and is continuing to be stored based on the terms of the agreement between the client and the SP. In order for the proof processes to be robust, the process must:

- Target a random part of the data.
- Occur at a time interval such that it is not possible, profitable, or rational for an SP to discard and re-fetch the copy of data.
-

In Filecoin, this process is known asProof-of-Storage , and consists of two distinct types of proofs:

- Proof of Replication (PoRep)
- : a procedure used at the time of initial data storage to validate that an SP hascreated and stored
- a unique copy of some piece of data.
- Proof of Spacetime (PoST)
- : a procedure to validate that an SP iscontinuing to store
- a unique copy of some piece of data.
-

Proof-of-Replication (PoRep)

In the Filecoin storage lifecycle process,Proof-of-Replication (PoRep) is used when an SP agrees to store data on behalf of a client and receives a piece of client data. In this process:

1. The data is placed into asector
2. .
3. The sector is sealed by the SP.
4. A unique encoding, which serves as proof that the SP has replicated a copy of the data they agreed to store, is generated (described inSealing as proof
5.).
6. The proof is compressed.
7. The result of the compression is submitted to the network as certification of storage.
8.

Sealing as proof

The unique encoding created during the sealing process is generated using the following pieces of information:

- The data is sealed.

- The storage provider who seals the data.
- The time at which the data was sealed.
-

Because of the principles of cryptographic hashing, a new encoding will be generated if the data changes, the storage provider sealing the data changes, or the time of sealing changes. This encoding is unique and can be used to verify that a specific storage provider did, in fact, store a particular piece of client data at a specific time.

Proof-of-Spacetime (PoSt)

After a storage provider has proved that they have replicated a copy of the data that they agreed to store, the SP must continue to prove to the network that:

- They are still storing the requested data.
- The data is available.
- The data is still sealed.
-

Because this method is concerned with proving that data is being stored in a particularspace for a particular period or at a particulartime , it is calledProof-of-Spacetime (PoSt) . In Filecoin, the PoSt process is handled using two different sub-methods, each of which serves a different purpose:

- WinningPoSt
- is used to prove that an SP selected using an election process has a replica of the data at the specific time that they were asked and is used in the block consensus process.
- WindowPoSt
- is used to prove that, for any and all SPs in the network, a copy of the data that was agreed to be stored is being continuously maintained over time and is used to audit SPs continuously.
-

WinningPoSt

WinningPoSt is used to prove that an SP selected via election has a replica of the data at the specific time that they were asked and is specifically used in Filecoin to determine which SPs may add blocks to the Filecoin blockchain.

At the beginning of eachepoch , a small number of SPs are elected to mine new blocks using theExpected Consensus algorithm , which guarantees that validators will be chosen based on a probability proportional to theirpower . Each of the SPs selected must submit a WinningPoSt, proof that they have a sealed copy of the data that they have included in their proposed block. The deadline to submit this proof is the end of the current epoch and was intentionally designed to be short, making it impossible for the SP to fabricate the proof. Successful submission grants the SP:

- Theblock reward
- .
- The opportunity to charge other nodes fees in order to include their messages in the block.
-

If an SP misses the submission deadline, no penalty is incurred, but the SP misses the opportunity to mine a block and receive the block reward.

WindowPoSt

WindowPoSt is used to prove that, for any and all SPs in the network, a copy of the data that was agreed to be stored is being continuously maintained over time and is used to audit SPs continuously. In WindowPoSt, all SPs must demonstrate the availability of all sectors claimed everyproving period . Sector availability is not proved individually; rather, SPs must prove a wholepartition at once, and that sector must be proved by the deadline assigned (a 30-minute interval in the proving period).

The more sectors an SP has pledged to store, the more the partitions of sectors that the SP will need to prove per deadline. As this requires that the SP has access to sealed copies of each of the requested sectors, it makes it irrational for the SP to seal data every time they need to provide a WindowPoSt proof, thus ensuring that SPs on the network are continuously maintaining the data agreed to. Additionally, failure to submit WindowPoSt for a sector will result in the SPs’ pledge collateral being forfeited and their storage power being reduced.

Previous Drand Next Assets

Last updated6 months ago