Blockchain

A blockchain is a distributed database that is shared among the nodes of a computer network. This page covers how the Filecoin blockchain is designed, and the various functions it has.

Tipsets

The Filecoin blockchain is a chain of tipsets rather than a chain of blocks. A tipset is a set of blocks with the same height and parent tipset. Therefore, multiple storage providers can produce blocks for each epoch to increase network throughput.

Each tipset is assigned a weight, so the consensus protocol directs nodes to build on the heaviest chain. This provides a certain level of security to the Filecoin network by preventing a node from intentionally intervening with other nodes to produce valid blocks.

Actors

An Actor in the Filecoin Blockchain is the equivalent of the smart contract in the Ethereum Virtual Machine. It is essentially an ‘object’ in the Filecoin network with a state and a set of methods that can be used to interact with it.

Built-in actors

There are several built-in system actors that power the Filecoin network as the decentralized storage network.

- System Actor - general system actor.
- Init actor - initializes new actors and records the network name.
- Cron Actor - a scheduler actor that runs critical functions at every epoch.
- Account Actor - responsible for user accounts (non-singleton).
- Reward Actor - managing block reward and token vesting (singleton).
- Storage Miner Actor - storage mining operation and validate storage proofs.
- Storage Power Actor - keeping track of the storage power allocated at each storage provider
- Storage Market Actor - managing storage deals.
- Multisig Actor - responsible for operations involving the Filecoin multi-signature wallet.
- Payment Channel Actor - set up and settle payment channel funds.
- Datacap Actor - responsible for datacap token management.
- Verified Registry Actor - responsible for managing verified clients.
- Ethereum address Manager (EAM) Actor- responsible for assigning all Ethereum compatible addresses on Filecoin Network, including EVM smart contract addresses and Ethereum account addresses.
- EVM Account Actor - a non-singleton built-in actor representing an external Ethereum identity backed by a secp256k1 key.
-

User-programmable actors

Along with the maturity of FVM, developers can write actors and deploy them to the Filecoin network in the same way as other blockchains. Other blockchains refer to these programs assmart contracts . User-programmable actors can also interact with built-in actors using the exported API from built-in actors.

You can check out this talk on How Filecoin Actors Work to learn more:

Distributed randomness

Filecoin uses distributed and publicly verifiable random beacon protocol Ðrand as the randomness beacon for the leader election during theexpected consensus to produce blocks. This randomness guarantees that the leader election is secret, fair, and verifiable.

Nodes

Nodes in the Filecoin network are primarily identified in terms of the services they provide to serve the Filecoin storage network, including chain verifier nodes, client nodes, storage provider nodes, and retrieval provider nodes. Any node participating in the Filecoin network should provide the chain verification service as a minimum.

Filecoin is targeting multiple protocol implementations to guarantee the security and resilience of the Filecoin network. Currently, the actively maintained implementations are:

- Lotus
- Venus
- Forest
-

Addresses

In the Filecoin network, addresses are used to identify actors in the Filecoin state. The address encodes information about the corresponding actor, providing a robust address format that is easy to use and resistant to errors. There are five types of addresses in Filecoin. Mainnet addresses begin with the letterf , and Testnet addresses begin with the lettert .

- f0/t0
- : an ID address for an actor in a more “human friendly” way. For instance, f0123261 is the ID for a storage provider.
- f1/t1
- : a secp256k1 wallet address with encrypted key pair. Essentially, this is a wallet address generated from the secp256k1 public key.
- f2/t2
- : an address represents an actor (smart contract) and is assigned in a way that makes it safe to use during network forks.
- f3/t3
- : a BLS wallet address generated from a BLS public encryption key.
- f4/t4
- : the addresses which were created and assigned to user-defined actors by user-definable “address management” actors. This address can receive funds before an actor has been deployed to the address.
- f410/t410
- : the address space managed by Ethereum Address Manager (EAM) built-in actor. The original Ethereum addresses can be cast as f410/t410 addresses and vice versa to enable existing Ethereum tools to interact seamlessly with the Filecoin network.
-

Consensus

Let’s quickly cover how consensus works in the Filecoin network.

Expected consensus

Expected consensus (EC) is the underlying consensus algorithm used by Filecoin. EC is a probabilistic Byzantine fault-tolerant consensus protocol that runs a leader election among a set of storage providers to submit a block every epoch. Like proof-of-stake, Filecoin uses proof-of-storage for the leader election, meaning the likelihood of being elected depends on how much provable storage power a miner contributes to the network. The storage power of the network is stored in the storage power table and managed by the Storage Power Actor.

At a high level, the consensus process relies onDrand to provide distributed and verifiable randomness to keep leader election secret, fair and verifiable. All the election participants and their power are drawn from the Power Table, which is calculated and maintained over time by the Storage Power Consensus subsystem. Eventually, EC takes all valid blocks produced in this epoch and uses a weighting function to select the chain with the highest weight to add blocks.

Block production process

The process of producing a block for each epoch can be briefly described as follows:

- Elect leaders from eligible miners.
- Miners need to check if they are elected.
- An elected miner gets the randomness value to generate WinningPoSt.
- If all above is successful, miners build and propagate a block.
- Verify whether a miner won the block and verify the leader election.
- Eventually, select the heaviest chain to add blocks.
-

Finality

EC enforces a version of soft finality whereby all miners at roundN will reject all blocks that fork off before roundN - F .F is set to900 . This is important to enforce finality at no cost to chain availability and functionality.

Proofs

As a decentralized storage network, Filecoin is built on the proof-of-storage in which miners contribute their vacant storage space to the network to store data and then provide proofs for the client to verify if their data has been stored throughout a period.

Proof of replication

Using proof-of-replication (PoRep), storage providers prove that they have created a unique copy of the client’s data and stored it on behalf of the network.

Proof of spacetime

Storage providers also need to continuously prove that they store clients' data for the whole lifetime of the storage deal. There are two types of challenges as part of the proof-of-spacetime (PoSt) process:

- Winning PoSt guarantees that the storage provider maintains a copy of data at a specific time.
- Window PoSt is used as proof that a copy of the data has been continuously maintained over time.
-

Slashing

If storage providers fail to provide reliable uptime or act maliciously against the network, they will be penalized by slashing. Filecoin implements two kinds of slashing:

- Storage fault slashing to penalize storage providers for not being able to maintain healthy and reliable storage sectors for the network.
- Consensus fault slashing to penalize storage providers to sabotage the liveness and security of the consensus process.
-

Previous Crypto-economics Next Storage model

Last updated5 months ago