Glossary

Definitions and usage for Filecoin terminology

Address

In the Filecoin network, an address is a unique cryptographic value that serves to publicly identify a user. This value, a public key, is paired with a corresponding private key. The mathematical relationship between the two keys is such that access to the private key allows the creation of a signature that can be verified with the public key. Filecoin specifically employs the Boneh–Lynn–Shacham (BLS) signature scheme for this purpose.

Block

In a blockchain, a block is the fundamental unit of record. Each block is cryptographically linked to one or more previous blocks. Blocks typically contain messages relating changes to some state (for example, financial records) tracked by the blockchain.

Blockchain

Fundamentally, a blockchain is a system of record in which new records, or blocks are cryptographically linked to preceding records. This construction is a foundational component of secure, verifiable, and distributed transaction ledgers.

Block height

The height of a block corresponds to the number of epochs elapsed before the block was added to the blockchain. The height of the Filecoin blockchain is defined to be the maximum height of any block in the blockchain.

Capacity commitment

If a storage provider doesn't find any available deal proposals appealing, they can alternatively make a capacity commitment , filling a sector with arbitrary data, rather than with client data. Maintaining this sector allows the storage provider to provably demonstrate that they are reserving space on behalf of the network.

CommP

The commitment phase of the Proof-of-Replication (PoRep) process. PoRep is a mechanism used to verify that a storage provider is storing data on behalf of a client by requiring the provider to prove that they have replicated the client's data to their storage space.

Content IDentifier (CID)

A self-describing format for referencing data in distributed information systems by it's contents , rather than its location using cryptographic hashing and self-describing formats. It is a core component of IPFS and IPLD, which are in turn components of Filecoin.

Collateral

In order to enter into a storage deal , a storage provider is required to provide FIL as collateral , to be paid out as compensation to a client in the event that the provider fails to uphold their storage commitment.

Deal

Two participants in the Filecoin network can enter into a deal in which one party contracts the services of the other. The Filecoin specification currently details storage deals (in which one party agrees to store data for the other for a specified length of time) and retrieval deals (in which one party agrees to transmit specified data to the other).

Election

Every epoch , a small subset of Filecoin storage providers are elected to mine a new block for the Filecoin blockchain. A provider's probability of being elected is roughly proportional to the share of the Filecoin network's total storage capacity that they contribute.

Epoch

Time in the Filecoin blockchain is discretized into epochs that are currently thirty seconds in length. Every epoch, a subset of storage providers are elected to each add a new block to the Filecoin blockchain via Winning Proof-of-Spacetime .

FIL

FIL is the name of the Filecoin unit of currency; it is alternatively denoted by the Unicode symbol for an integral with a double stroke (ⅉ).

Faucet

A faucet is a service that provides free FIL . Typically, faucets are run for the benefit of new users in a network, providing them with the necessary seed capital to begin making transactions.

Fault

When a storage provider fails to complete Window Proof-of-Spacetime for a given sector, the Filecoin network registers a fault for that sector, and the provider is slashed . If a storage provider does not resolve the fault quickly, the network assumes they have abandoned their commitment.

Filecoin

The term Filecoin is used generically to refer to the Filecoin project, protocol, and network.

Finality

Finality refers to the immutability of messages and state recorded to the Filecoin blockchain. As new blocks are added to the blockchain, it becomes more and more difficult for older blocks to be altered, until they become effectively impossible to modify. The finality period is the amount of time that must elapse before a block is considered completely immutable. In the current mainnet , this is configured as 900 epochs .

Gas

Gas is a property of a message , corresponding to the resources involved in including that message in a given block . For each message included in a block, the block's creator extracts a fee from the message's sender; this fee is proportional to the message's gas.

Mainnet

A portmanteau of "main" and "network," mainnet is a term used to refer to the predominant public-facing network of the Filecoin project and community. The mainnet embodies an expectation of widespread adoption and permanence; changes to its protocol are subject to the adoption of the network participants.

If used as a proper noun, capitalize the term: "I am providing on Mainnet."

Message

The term message is used to refer to data stored as part of a block . A block can contain several messages.

Merkle Directed Acyclic Graph

Abbreviated as Merkle DAG . A graph data structure where nodes:

- Have a unique identifier that is the hash of the nodes contents
- Are directionally related to other nodes
- Never form a closed loop
-

Merkle DAGs are a fundamental component for the representation of relationships between content-addressed data in IPLD, which is in turn used by Filecoin.

Miner

The Filecoin project uses the term provider to refer to participants in the network who provide a service of value to a client. Other blockchains, like Ethereum and Bitcoin, use the term miner . At present, the Filecoin specification recognizes two provider types: storage providers and retrieval providers .

Pledged storage

Storage capacity that a provider has promised to reserve for the Filecoin network via Proof-of-Replication is termed pledged storage .

Proof-of-Storage

Many blockchain networks are underpinned by the notion that participants supply something of value to the blockchain - a contribution that is hard to fake, but which, if actually made, can be trivially verified. Blockchains based in this approach are often said to require "Proof-of-X", where X is the valued contribution. The Filecoin blockchain values contributions of storage

capacity; it is predicated upon a novelProof-of-Storage construction, distinguishing it from other blockchains that, as is most often the case, require a contribution of computing power.

As a term, Proof-of-Storage refers to the design elements of the Filecoin protocol that allow one to guarantee (to some very high tolerance) that participants that claim to be contributing a given amount of storage are indeed fulfilling that pledge. In fact, Filecoin's Proof-of-Storage construction provides for a much stronger claim, allowing one to efficiently verify that a participant is storing aparticular piece of data , without requiring that one have a copy of the file itself.

Note : "proof" here is used in an informal sense - typically, these proofs take the form of a probabilistic argument, rather than a concrete proof; that is, it mighttechnically be possible to convince other participants that one is making a contribution one is not, but the possibility is so vanishingly slight as to border on impossibility.

Proof-of-Replication (PoRep)

Proof-of-Replication is a procedure by which astorage provider can prove to the Filecoin network that they have created a unique copy of some piece of data on the network's behalf.

Proof-of-Spacetime (PoSt)

Proof-of-Spacetime is a procedure by which astorage-provider can prove to the Filecoin network they continue to store a unique copy of some data on behalf of the network. Proof-of-Spacetime manifests in two distinct varieties in the present Filecoin specification:Window Proof-of-Spacetime andWinning Proof-of-Spacetime .

Quality-adjusted storage power

The storage power astorage provider earns from a storage deal offered by averified client will be augmented by a multiplier. Power totals that take into account this multiplier are termedquality adjusted .

Retrieval provider

Aretrieval provider is a Filecoin participant that enters retrievaldeals with clients, agreeing to supply a client with a particular file in exchange forFIL . Note that unlikestorage providers , retrieval providers are not additionally rewarded with the ability to add blocks to the Filecoin blockchain; their only reward is the fee they extract from the client.

Seal

Sealing is one of the fundamental building blocks of the Filecoin protocol. It is a computation-intensive process performed over asector that results in a unique representation of the sector. The properties of this new representation are essential to theProof-of-Replication and theProof-of-Spacetime procedures.

Sector

Storage providers store data on behalf of the Filecoin network in fixed-size blocks of data calledsectors .

Slash

When afault is registered for asector , the Filecoin network willslash thestorage provider that is supposed to be storing the sector; that is, it will assess penalties to the provider (to be paid out of thecollateral fronted by the provider) for their failure to uphold their pledge of storage. When slashing takes place, the power a provider earns for the associated sector is subtracted from the provider's total power for the purposes ofelection .

Storage provider

Astorage provider is a Filecoin participant that stores data on behalf of the network. Storage providers are rewarded for this service through payments by clients that contract their services, as well as by periodic authorization to extend the Filecoinblockchain withblocks of their own creation. When they create a block, storage providers are rewarded with newly mintedFIL , as well as the transaction fees they can levy on other participants seeking to includemessages in the block.

Storage power

Astorage provider's storage power is a value roughly proportional to the amount of storage capacity they make available on behalf of the network viacapacity commitments orstorage deals . Storage power is used to select storage providers for rewards in proportion to their contributions to the total network storage capacity.

Zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK)

Anargument of knowledge is a construction by which one party, called theprover , can convince another, theverifier , that the prover has access to some piece of information. There are several possible constraints on such constructions:

- Anon-interactive
- argument of knowledge has the requirement that just a single message, sent from the prover to the verifier, should

serve as a sufficient argument.

- A zero-knowledge
- argument of knowledge has the requirement that the verifier should not need access to the knowledge the prover has access to in order to verify the prover's claim.
- A succinct
- argument of knowledge is one that can be "quickly" verified, and which is "small", for appropriate definitions of both of those terms.
-

A zero-knowledge, succinct non-interactive argument of knowledge (zk-SNARK) embodies all of these properties. Filecoin utilizes these constructions to enable its distributed network to efficiently verify that storage providers are storing files they pledged to store, without requiring the verifiers to maintain copies of these files themselves.

Testnet

A portmanteau of "test" and "network," testnet is a term used to refer to one of the primary Filecoin testing networks .

Note: if used as a proper noun, capitalize the term. For example, "I am providing on Testnet."

Tipset

A tipset is a set of blocks that each have the same height and parent tipset; the Filecoin blockchain is a chain of tipsets, rather than a chain of blocks.

Each tipset is assigned a weight corresponding to the amount of storage the network is provided per the commitments encoded in the tipset's blocks. The consensus protocol of the network directs nodes to build on top of the heaviest chain.

By basing its blockchain on tipsets, Filecoin can allow multiple storage providers to create blocks in the same epoch , increasing network throughput. By construction, this also provides network security: a node that attempts to intentionally prevent the valid blocks of a second node from making it onto the canonical chain runs up against the consensus preference for heavier chains.

Verified client

To further incentivize the storage of "useful" data over simple capacity commitments , storage providers have the additional opportunity to compete for special deals offered by verified clients . Such clients are certified with respect to their intent to offer deals involving the storage of meaningful data, and the power a storage provider earns for these deals is augmented by a multiplier.

Window Proof-of-Spacetime (WindowPoSt)

Window Proof-of-Spacetime (WindowPoSt) is the mechanism by which the commitments made by storage providers are audited. It sees each 24 hour period broken down into a series of windows. Correspondingly, each storage provider's set of pledged sectors is partitioned into subsets, one subset for each window. Within a given window, each storage provider must submit a Proof-of-Spacetime for each sector in their respective subset. This requires ready access to each of the challenged sectors, and will result in a proof compressed via zk-SNARK being published to the Filecoin blockchain as a message in a block . In this way, every sector of pledged storage is audited at least once in any 24 hour period, and a permanent, verifiable, and public record attesting to each storage provider's continued commitment is kept.

The Filecoin network expects constant availability of stored data. Failing to submit WindowPoSt for a sector will result in a fault , and the storage provider supplying the sector will be slashed .

Winning Proof-of-Spacetime (WinningPoSt)

Winning Proof-of-Spacetime (WinningPoSt) is the mechanism by which storage providers are rewarded for their contributions to the Filecoin network. At the beginning of each epoch , a small number of storage providers are elected to each mine a new block . As a requirement for doing so, each provider is tasked with submitting a compressed Proof-of-Storage for a specified sector . Each elected provider who successfully creates a block is granted FIL , as well as the opportunity to charge other Filecoin participants fees to include messages in the block.

Storage providers who fail to do this in the necessary window will forfeit their opportunity to mine a block, but will not otherwise incur penalties for their failure to do so.

Last updated 7 months ago