Talking about storage and retrieval transactions in Filecoin

FileCoin (https://learnblockchain.cn/tags/FileCoin) IPFS (https://learnblockchain.cn/tags/IPFS)
Distributed storage
(https://learnblockchain.cn/tags/%E5%88%86%E5%B8%83%E5%BC%8F%E5%AD%98%E5%82%A8)

The Filecoin network is composed of hundreds of storage providers distributed around the world. The content addressing and encrypted storage proof verify that the data is stored correctly and securely on the miner's hardware for a long time, thus creating a powerful and reliable service.

The Filecoin (https://ipfs.cn/100011/type-100044.html) network is composed of hundreds of storage providers distributed around the world. The content addressing and encrypted storage proof verify that the data is stored correctly and securely on the miner's hardware for a long time, thus creating a powerful and reliable service.

This article elaborates on the two types of transactions in Filecoin, storage transactions and retrieval transaction operation stages, and explains their life cycle in detail. It also explains how the cryptographic proof is used to verify whether the participants in the system perform their duties as promised.

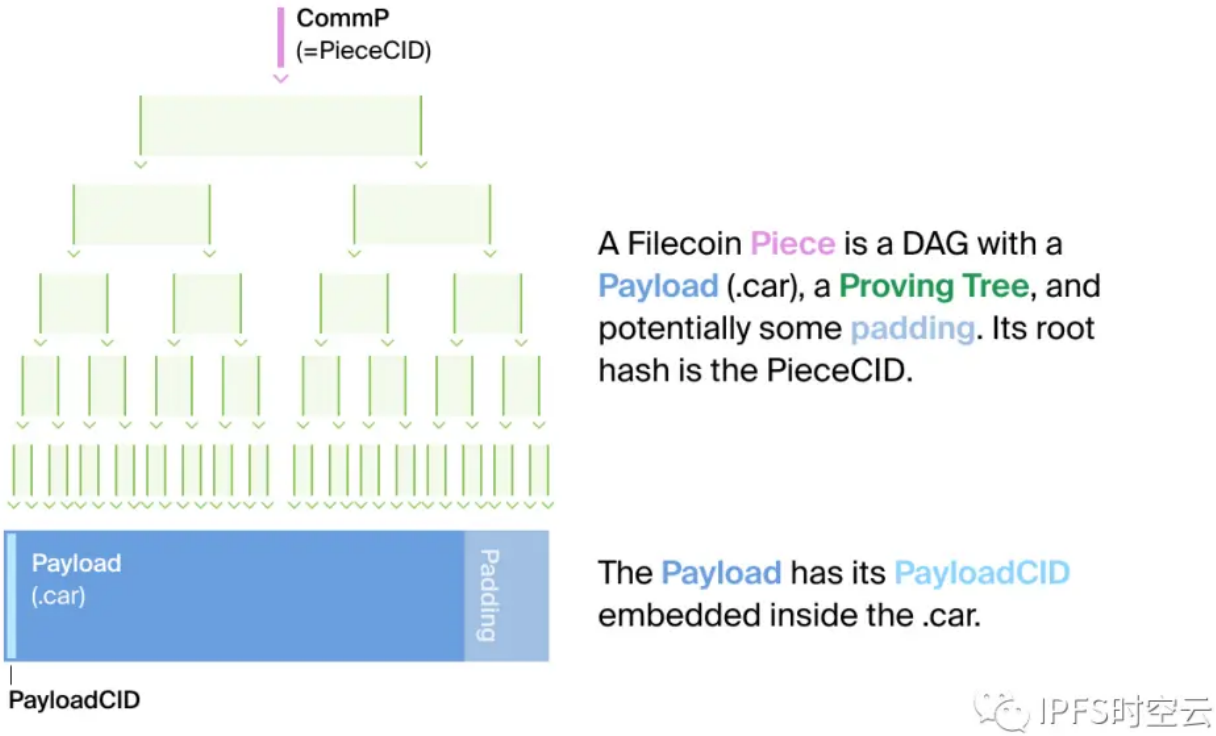
Data on Filecoin

To store files on Filecoin, users must first import the files in their local Filecoin node. This step will generate a data CID-the content identifier, a unique ID describing the content. After that, the data was passed to the miners.

Importing data to the local Filecoin node can be done through the lotus client import command. Remember the generated data CID (which can also be obtained on the local node later), because it will be used when retrieving data from the miner later.

After importing the data to the local node, the user needs to initiate a transaction. This step is done through the lotus client deal command. This command takes a data CID as input, generates a Filecoin Piece, and interactively guides the user to complete the storage transaction process.

Filecoin Piece is the main negotiation unit for users to store data on the Filecoin network. Filecoin Piece does not have a specific size, but uses the sector size as the upper limit, which is controlled by network parameters. If a Filecoin Piece is larger than the sector size supported by the miner, it must be divided into more pieces so that each piece fits into a sector.



Filecoin Piece

Each Filecoin Piece is a CAR file, including an IPLD DAG, with corresponding data CID and piece CID.

CAR is a content addressable file. Each CAR file is a serialized representation of an IPLD DAG, that is, its data blocks are stringed together, plus the header information describing the DAG graph (and the root CID).

When users want to store files in the Filecoin network, they must first use UnixFS to make the IPLD DAG of the file (this is the function of the lotus client import command). The hash representing the root node of the DAG is an IPFS-style CID, called the data CID.

UnixFS is a protobuf-based format used to describe files, directories and soft links in IPFS. In Filecoin, UnixFS is the file format standard, and files are submitted to the Filecoin network in this format.

The generated CAR file is filled with additional zero bits so that the file is written as a binary merkle tree.

Store transaction process

Users access data through transactions in the Filecoin network. Participants of the network, including miners (supply side) and users (demand side), interact with each other by storing transactions and retrieving transactions.

The life cycle of storage transactions is as follows:

1. Find

The user first determines the miner and its pricing, that is, the price per GiB per epoch (30 seconds) that the miner hopes to receive in order to accept the transaction, in attoFIL. Currently, the minimum period of a transaction in Filecoin is 180 days.

You can query the synchronized nodes through the JSON RPC API to list all currently active miners, using the Filecoin.StateListMiners method. You can choose according to the miner's reputation and ability in the network. The reputation indicator of miners has not yet entered the Filecoin protocol.

After you have selected the miner, you can use methods such as Filecoin.StateMinerInfo to obtain the miner’s PeerID, which is used to establish a secure connection with the other party in the libp2p protocol.

Next, you can use the Filecoin.ClientQueryAsk method to obtain a signed StorageAsk.

The result includes the transaction details that the miner is willing to accept, such as the size range of the accepted Filecoin Piece and the price per GiB per epoch. It should be noted that proposing a storage transaction that matches the storage requirements of the miner is only a prerequisite, but it is not sufficient to ensure that the transaction is accepted-the storage provider may run its own decision logic later.

2. Price negotiation and data transmission

At this stage, the two parties reach an agreement on the terms of the transaction, such as transaction costs, transaction period, and transaction start time.

Then, the data is sent from the user to the miner.

3. release

Publish the transaction on the chain through the PublishStorageDeals message, making the storage provider responsible for the disclosure of the transaction.

4. carry out

Once the transaction is released on the chain, it will be handed over to the mining subsystem, packaged into sectors, then packaged, and then continuously proven to be usable.

Storage mining subsystem

The storage mining subsystem ensures that the data of the Filecoin network is effectively saved by the miners, and:

Participate in the Filecoin storage market, take over user data, and participate in storage transactions.
Participate in the Filecoin storage computing power consensus, verify and generate blocks, let the Filecoin blockchain grow, and get block rewards.

The system monitors the following processes:

Commitment to new storage and registration of new sectors

In order to register a sector in Filecoin, miners must encapsulate the sector. The _encapsulation_ process requires a lot of calculations to produce a unique representation of the data in the form of proof, that is, proof of replication or PoRep. Once the proof is generated, the miners compress it and submit the result to the blockchain. This proves that the miners did make copies of the data they agreed to store.

To prove that the storage is continuously available, all storage miners need to continue to submit on-chain proofs to verify that the sectors are completely stored.

Announcing storage failures and recovering from failures. If the above proof required by the sector is not successfully submitted, it will cause a failure and the miners will be punished.

For storage miners and users, as mentioned above, storage transactions are activated and encapsulated only after they are released on the chain. This is important because publishing a transaction will lock the user's funds in the chain for custody. Only in this way, after the data is sealed into the sector, the profit of the miner can be guaranteed.

You can think of publishing transactions on the chain as signing a contract, and encapsulating and activating transactions as starting to make promises.

From the user's point of view, if you want to use Filecoin to store data, the transaction roughly goes through the following stages:

For transaction deposits , the user locks the funds in the escrow,
submits a transaction proposal to the miner,
checks the intent to accept the transaction, and
transmits the data to the miner for the transaction, which is done through the GraphSync protocol. GraphSync is a protocol for synchronizing IPLD graphs between nodes. This protocol allows the local node to send a request to the remote node to obtain the result of the search by the selector on the IPLD graph of the remote node. Lotus uses the implementation of GraphSync protocol ipfs/go-graphsync.
Check acceptance-make sure that the miner has accepted the transaction and posted it on the chain.
Encapsulation-The transaction is already on the chain, and the miner is encapsulating the sector containing the transaction.
Active-The transaction has been sealed and is active. From here on, storage providers/miners should regularly prove that they continue to store data.

From the miner's point of view, by storing user data to provide services, the transaction roughly goes through the following stages:

Verify transaction-receive a transaction proposal and check its parameters (size, price, etc.).
Check if there are locked funds-make sure that the user has locked funds and can pay for the transaction.
Waiting for data-receive transaction data provided by the customer.
Provide collateral for transactions for on-chain transactions.
Post transactions on the chain.
Encapsulation sector activation transactions, storage providers (miners) regularly submit WindowPoSt to prove that they are continuously storing data.

Retrieve transaction flow

The retrieval transaction is different from the storage transaction. The payment channel is used, which is mainly done off-chain. Data transmission is priced by volume, and users gradually pay the miners during the process of data transmission. In the entire process, only the creation of payment channels and redemption of vouchers are involved in interaction with the Filecoin blockchain.

The overall process is as follows:

Discovery-The user finds the miner who has the data he needs, and asks him to retrieve the quotation details-price per byte, unblocking price, payment interval.
Set up a payment channel-the user needs to set up a payment channel with the miner (if it does not already exist).
Data transmission and payment-miners send data to users until payment is required. When a certain threshold is reached, payment processing will be required, and then data transmission will continue. Depending on whether miners have data in their block storage, they may need to unpack the data first-this is an unconventional and non-transient operation, which is the reverse operation of encapsulation described in the section on storage transactions.
At this time, the user has not yet obtained complete data.

Time and Space Proof

The above section quickly enumerates many details that make Filecoin unique and provides a guarantee for user data in terms of probability. This section introduces the two proofs used by Filecoin and explains how they become part of the protocol and the problems they solve.

Proof of Time and Space (PoSt) is a proof submitted by a miner to the Filecoin network to prove that it is continuing to store the only copy of data for the network.

Currently, time-space proofs exist in two types in Filecoin:

WindowPoSt
WinningPoSt

WinningPoSt

WinningPoSt is a mechanism that rewards storage miners for their contributions to the Filecoin network. At the beginning of each epoch, a small number of storage miners are selected, and each miner digs a new block. The specific requirement is that these miners submit proof of compressed storage for the designated sector. Each elected miner who successfully creates a block will receive a FIL (block reward) and the opportunity to collect fees from other Filecoin participants who want to include information in the block.

If storage miners fail to comply with the requirements within the necessary time window, they will lose the opportunity to produce blocks, but they will not be punished for not producing blocks.

WindowPoSt

WindowPoSt is a mechanism for the Filecoin blockchain to review the commitments made by storage miners.

Every storage miner should maintain their commitment sector. These sectors contain transactions with users, or they may be empty. The latter is called committed capacity, which means that miners can make capacity commitments to fill a sector with arbitrary data instead of user data. Maintaining these sectors allows storage miners to prove that they reserve space on the generation network.

Each day is divided into several time windows, currently 48 time windows, each duration is 30 minutes (60 epoch, because 1 epoch is equal to 30 seconds).

Each miner's commitment sector is divided into several groups, and each group corresponds to a time window.

Within a time window (30 minutes), each storage miner must submit a time-space certificate for each sector in the time window. This requires access to every sector in the turn of the time window at any time, and generate a zk-SNARK proof to join the block and publish it to the Filecoin blockchain. In this way, every sector promised to

store will be reviewed at least once every 24 hours, and a permanent, verifiable, and public record will be kept to prove that each storage miner is conservative in its promise.

In the example above, you can see that a miner should submit time-space proofs in deadline 0 (> 16TB), deadline 1 (< 8TB) and deadline 2 (< 8TB), most of which are in deadline 0. The deadline of each miner is random. For this particular miner, it starts from epoch 1635, epoch 1695 and epoch 1755 respectively. You can check these deadlines and more details about miners on the SpaceGap tool.

The Filecoin network expects the stored data to be continuously available. Failure to submit WindowPoSt for a sector will result in a failure, and the storage miner who supplies the sector will be punished. This encourages the healthy operation of storage miners.

malfunction

The failure occurs when the proof is not included in the Filecoin blockchain within the time limit due to loss of network connection, storage failure, or malicious behavior.

When a sector is registered as a fault, the Filecoin network will punish the storage miner who should have stored the sector; that is, the miner’s failure to continue storage will be assessed for punishment (paid from the collateral prepaid by the miner)).

There are three types of sector failure fees:

Sector failure fee: It needs to be paid every day by each sector in a failure state. The size of the fee is slightly higher than the estimated block reward for the sector every day. If a sector is in a failed state for more than 2 consecutive weeks, the sector will pay a termination fee and be removed from the blockchain state.

Sector failure detection fee: This is a one-time payment, if the failure is detected by the on-chain mechanism instead of the miner reporting honestly. Taking into account the probabilistic nature of the space-time proof check, the fee is set as the block reward for the corresponding sector in several days.

Sector termination fee: A sector may be terminated before the expiration date due to failure or the miner's initiative. In principle, the collected termination fee is equivalent to the current income generated by a sector, and does not exceed a limit, so as not to hinder the long-term sector.

in conclusion

This article describes some concepts about storing and retrieving data on Filecoin, the protocols used by users and miners to access data, and the various proofs and guarantees involved in these processes.

From the perspective of users and miners, the process of storing transactions and retrieving transactions is introduced in detail; and when a party has malicious behavior, the Filecoin protocol will penalize it.

In summary, this article outlines how the Filecoin protocol manages the Filecoin network, making it a reliable and trustless decentralized storage network.

Investors who want to know more about IPFS and Filecoin, please contact the IPFS China Community Operations Officer (WeChat ID: chuanzhang129) or the IPFS China Community official website: http://ipfs.cn (http://ipfs.cn)

Published on 2021-03-23 13:58 Reading (130) Credits (0)
Category: FileCoin (https://learnblockchain.cn/categories/FileCoin)

Articles you may be interested in

Why is NFT different? How does Filecoin's distributed storage solution empower NFT? (https://learnblockchain.cn/article/2495) 21 views

A detailed look at Filecoin: what it is, how it works, why you choose it, and frequently asked questions (https://learnblockchain.cn/article/2471) 61 views

Development Guide: Deploy decentralized web pages/DApps on Crust (https://learnblockchain.cn/article/2434) 134 views