**Filecoin**

The Filecoin network is a decentralized data storage marketplace. Users can store and retrieve their data on the network. The storage space is provided by storage provided on the network.

### **What is the Filecoin network?**

[The Filecoin network](https://filecoin.io/) is a decentralized data storage network. It has been developed by [Protocol Labs](https://protocol.ai/), an open source R&D lab. Filecoin allows its users to sell their excess storage space on an open platform. It acts as an incentive and security layer for IPFS. Filecoin enables the IPFS storage system to act as an algorithmic market. Using this market users can interact with storage providers. Users pay using Filecoin’s native token, FIL, in exchange for storing and distributing data on the network. In short, IPFS is the backbone and Filecoin network is the surface market layer.

## **For users**

Filecoin enables users to store their files at hypercompetitive prices and verify that their files are being stored correctly.

## **For storage providers**

Filecoin enables storage providers to sell their storage on an open market.Storage providers are people and organizations that run storage providers, earning Filecoin tokens for doing so.

### **The Filecoin token, FIL**

### FIL is the native crypto token of the Filecoin network. In order to participate in the storage and retrieval mining process users require FIL token. In exchange for their proof-of-work, they can earn rewards in terms of FIL. Users can also use FIL token to participate and transact on the Filecoin network. Users can pay miners in FIL to store their data or to retrieve it. Storage provides also use FIL as collateral in case of invalid or missing proofs.

The total token supply of FIL tokens is 147,799,573, and the current circulating supply is set at 147,799,573.00 FIL.

# **How Filecoin Works?**

## **The Network**

The Filecoin network is a distributed, peer-to-peer network formed by Filecoin peers who participate in different ways. Peers communicate over secure channels that they use to distribute information to the network (gossiping), to transfer data among themselves, and to discover other peers, maintaining a well-connected swarm in which information like blocks and messages flows swiftly even when many thousands of peers participate.

## **Filecoin nodes**

*Filecoin Nodes* or *Filecoin clients* are peers that sync the Filecoin blockchain and validate the messages in every block, which, once applied, provide a global state.

Filecoin Nodes can also publish different types of *messages* to the network by broadcasting them. Nodes can propose [storage and retrieval deals](https://docs.filecoin.io/about-filecoin/how-filecoin-works/#deals) to Filecoin storage providers and pay for them as they are executed.Running a Filecoin Node is a low-level task that usually implies keeping a program running 24/7.

**Filecoin storage providers**

The storage providers provide services to the network by executing different types of [deals](https://docs.filecoin.io/about-filecoin/how-filecoin-works/#deals) and appending new blocks to the chain (every 30 seconds), for which they collect FIL rewards. Running a Filecoin storage provider is a highly-technical task with strong [hardware requirements](https://docs.filecoin.io/storage-provider/hardware-requirements/), as needed to complete the necessary [proofs](https://docs.filecoin.io/about-filecoin/how-filecoin-works/#proofs).

## **Deals**

There are two main types of deals in Filecoin: ***storage deals* and *retrieval deals*.**

Storage deals are agreements between clients and *storage providers* to store some data in the network. Once a deal is initiated, and the storage provider has received the data to store, it will repeatedly [prove](https://docs.filecoin.io/about-filecoin/how-filecoin-works/#proofs) to the chain that it is still storing the data per the agreement so that it can collect [rewards](https://docs.filecoin.io/storage-provider/rewards/). If not, the storage provider will be [slashed](https://docs.filecoin.io/storage-provider/slashing/) and lose FIL.

Retrieval deals are agreements between clients and *retrieval providers* (which may or not be also storage providers) to extract data that is stored in the network (hopefully in a fast and reliable manner). Unlike storage deals, these deals are fulfilled off-chain, using *payment channels* to incrementally pay for the data received.

## **Proofs**

Storage providers must prove that they are storing the data per the terms of a deal. That means that:

* They must store all the data submitted by the client
* They must store it during the whole lifetime of the deal

Using ***Proof Of Replication (PoRep)*,** storage providers demonstrate that they have received all the data and that they have encoded it in a way unique to that storage provider using their physical storage in a way that no other storage provider can replicate (so two deals for the same data cannot end up re-using the same disk). This proof is provided when the deal starts, and the *sealing* operation completes.

Once a deal is active and during its full lifetime, the storage provider will use ***Proof of Spacetime (PoSt)*** to prove that it is *still* storing the data associated with a deal. For PoSt, random storage providers need to prove that random parts of the data they store are still there.

## **Gas fees**

*Gas* is a measure of resources consumed by messages. The gas consumed by a message directly affects the cost that the sender has to pay for it to be included in a new block by a storage provider.

In Filecoin, an amount of the fees is burned (sent to an irrecoverable address) to compensate for the network expenditure of resources, since all nodes need to validate the messages. The idea is based on Ethereum’s [EIP1559](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md).

The amount of fees burned in the Filecoin network is determined by a dynamic \**BaseFee*, which gets automatically adjusted according to the network congestion parameters (block sizes).

The total cost of a message for a sender will be:

* *GasUsage \* BaseFee* FIL (burned) +

*GasLimit \* GasPremium* FIL (storage provider’s reward) +

*OverEstimationBurn \* BaseFee* FIL

***GasUsage***: the amount of gas that a message’s execution actually consumes.

***BaseFee***: the amount of FIL that gets burned *per unit of gas consumed* for the execution of every message. It is measured in units of attoFIL/Gas.

***GasLimit***: the limit on the amount of gas that a message’s execution can consume, estimated and specified by a message sender.It is measured in units of Gas.

***GasFeeCap***: the maximum token amount that a sender is willing to pay per GasUnit for including a message in a block. It is measured in units of attoFIL/Gas.

***GasPremium***: a priority fee that is paid to the block-producing storage provider. This is capped by *GasFeeCap*.It is measured in units of attoFIL/Gas

***Overestimation******burn***: an additional amount of gas to burn that grows larger when the difference between *GasLimit* and *GasUsage* is large.

## **Actors**

Actors are a [software design pattern](https://en.wikipedia.org/wiki/Actor_model) for managing state. Accounts, Multisigs, Storage Providers, and anything with a state, such as an account balance, are implemented as an *actor*.

Actors are the Filecoin equivalent of smart contracts in the Ethereum Virtual Machine. As such, Actors are very central components of the system. Any change to the current state of the Filecoin blockchain has to be triggered through an Actor.

## **Addresses**

In Filecoin, addresses are used to identify actors. There are 4 address types:

* 0 - ID Address
* 1 - SECP256K1 Public Key Address
* 2 - Actor Address
* 3 - BLS Public Key Address

### **ID addresses - f0**

All actors have an ID such as 99, a short integer assigned to it by the InitActor when the actor is created. An *ID address* is an actor’s ID prefixed with the network (f for mainnet) and address type 0 for ID.

### **Public key addresses - f1 and f3**

Actors managed directly by users, like accounts, are derived from a public-private key pair. If you have access to a private key, you can sign messages sent from that actor. The public key is used to derive an address for the actor.

Public key addresses allow devices like the Ledger to derive a valid Filecoin address for your account from just the public key. It doesn’t need to ask a remote node what your ID address is.Filecoin supports both secp256k1 addresses that begin with f1 and BLS addresses that begin with f3.

### **Actor addresses f2**

Actor addresses provide a way to create robust addresses for actors not associated with a public key. They are the essentially random sha256 hash of the output of the account creation.

### **BLS Curve f3**

Filecoin uses curve bls12-381 for BLS signatures. Bls12-381 is a pair of two related curves: G1 and G2. Implementations of bls12-381 can vary based on if public keys are on G1 and signatures on G2 or vice-versa.

Filecoin uses G1 for public keys and G2 for signatures as G1 allows for a smaller representation of public keys.

In Brief:

1. On the Filecoin network, peers interact across secure channels to broadcast information through the network, transmit files amongst themselves, and discover additional peers, resulting in a well-connected [swarm](https://coinmarketcap.com/alexandria/glossary/swarm) in which information such as blocks and messages moves quickly even when vast numbers of peers are involved.
2. Filecoin Nodes, also known as Filecoin clients, are peers who sync the Filecoin blockchain and validate the messages in each block, resulting in a global state once applied.
3. Filecoin Nodes can also disseminate various types of messages to the rest of the network. A client, for instance, can publish a message to send FIL from one address to another. Nodes can offer Filecoin miners storage and retrieval services, and miners can charge for them as they are completed.
4. Miners contribute to the network by completing various types of transactions and adding new blocks to the chain, for which they receive FIL rewards.
5. Retrieval and storage deals happen on the [Filecoin](https://coinmarketcap.com/currencies/filecoin/) network.
   1. Clients and storage miners make arrangements to store data in the network through storage deals. Once a deal is made and the miner receives the data to store, it must repeatedly show to the chain that it is still storing the data in accordance with the agreement in order to get rewards. Otherwise, the miner would be sliced, and [FIL](https://coinmarketcap.com/currencies/filecoin/) will be lost.
   2. Clients and retrieval miners make agreements to retrieve data that is stored on the network in a fast and reliable manner.
6. Storage miners must demonstrate that they are storing data in accordance with the conditions of a contract. That implies they must save all of the information provided by the client and keep it for the entire duration of the transaction/deal. Miners show that they have acquired all of the data and have encrypted it in a way that is unique to that miner using their physical storage in a way that no other miner can replicate using Proof of Replication (PoRep).
7. A dynamic BaseFee determines the number of fees burned in the Filecoin network, which is constantly changed based on network congestion parameters.
8. A number of gas-related factors are also connected to each message, and these parameters impact the number of rewards that miners receive.
9. Actors are a state management software design paradigm. Any modification to the Filecoin blockchain's current state must be initiated by an Actor.

# **Why Filecoin??**

### **Verifiable storage**

Filecoin has built-in processes to check the history of files and verify that they have been stored correctly over time. Every storage provider proves that they are maintaining their files in every 24-hour window. Clients can efficiently scan this history to confirm that their files have been stored correctly, even if the client was offline at the time. Any observer can check any storage provider’s track record and will notice if the provider has been faulty or offline in the past.

### **Open market**

In Filecoin, file storage and retrieval deals are negotiated in open markets. Anybody can join the Filecoin network without needing permission. Running a storage provider only requires an internet connection and spare disk space. By lowering the barriers to entry, Filecoin enables a thriving ecosystem of many independent storage providers.

### **Competitive prices**

Prices for storage and retrieval are determined by supply and demand, not corporate pricing departments. Filecoin makes reliable storage available at hyper-competitive prices. Miners compete based on their storage, reliability, and speed rather than through marketing or locking users in.

### **Reliable storage**

Because storage is paid for, Filecoin provides a viable economic reason for files to stay available over time. Files are stored on computers that are reliable and well-connected to the internet.

### **Reputation, not marketing**

In Filecoin, storage providers prove their reliability through their track record published on the blockchain, not through marketing claims published by the providers themselves. Users don’t need to rely on status pages or self-reported statistics from storage providers.

### **Choice of tradeoffs**

Users get to choose their own tradeoffs between cost, redundancy, and speed. Users are not limited to a set group of data centers offered by their provider but can choose to store their files on any storage provider participating in Filecoin.

### **Censorship resistance**

Filecoin resists censorship because no central provider can be coerced into deleting files or withholding service. The network is made up of many different computers run by many different people and organizations. Faulty or malicious actors are noticed by the network and removed automatically.

### **Useful blockchain**

In Filecoin, storage providers are rewarded for providing storage, not for performing wasteful computations. Filecoin secures its blockchain using proof of file replication and proof of storage over time. It doesn’t rely on energy-intensive proof-of-work schemes like other blockchains. Miners are incentivized to amass hard drives and put them to use by storing files. Filecoin doesn’t incentivize hoarding of graphics cards or application-specific integrated circuits for the sole purpose of mining.

### **Provides storage to other blockchains**

Filecoin’s blockchain is designed to store large files, whereas other blockchains can typically only store tiny amounts of data, very expensively. Filecoin can provide storage to other blockchains, allowing them to store large files. In the future, mechanisms will be added to Filecoin, enabling Filecoin’s blockchain to interoperate with transactions on other blockchains.

### **Content addressing**

Files are referred to by the data they contain, not by fragile identifiers such as URLs. Files remain available no matter where they are hosted or who they are hosted by. When a file becomes popular, it can be quickly distributed by swarms of computers instead of relying on a central computer, which can become overloaded by network traffic.

### **Content distribution network**

Retrieval providers are computers that have good network connections to lots of users who want to download files. By prefetching popular files and distributing them to nearby users, retrieval providers are rewarded for making network traffic flow smoothly, and files download quickly.

### **Single protocol**

Applications implementing Filecoin can store their data on any storage provider using the same protocol. There isn’t a different API to implement for each provider. Applications wishing to support several different providers aren’t limited to the lowest-common-denominator set of features supported by all their providers.

### **No lock-in**

Migrating to a different storage provider is made easier because they all offer the same services and APIs. Users aren’t locked into providers because they rely on a particular feature of the provider. Also, files are content-addressed, enabling them to be transferred directly between providers without the user having to download and re-upload the files.

### 

### 

### **Open source code**

The code that runs both clients and storage providers is open-source. Storage providers don’t have to develop their own software for managing their infrastructure. Everyone benefits from improvements made to Filecoin’s code.

### **Active community**

Filecoin has an active community of contributors to answer questions and help newcomers get started. There is an open dialog between users, developers, and storage providers.

In brief

### Made for Users and Storage Providers

### A Great Platform for Miners

### A Storage Platform for NFTs

### Dependable Storage

### Storage That Can Be Verified

### A Solitary Protocol

### Resilience to Censorship

### Open Source Code

### Addressing the Content

# **IPFS and Filecoin**

Filecoin and IPFS are complementary protocols for storing and sharing data in the distributed web. Both systems are free, open-source, and share many building blocks, including data representation formats (IPLD) and network communication protocols (libp2p). While interacting with IPFS does not require using Filecoin, all Filecoin nodes *are* IPFS nodes under the hood, and (with some manual configuration) can connect to and fetch IPLD-formatted data from other IPFS nodes using libp2p.

**Filecoin Mining**

Filecoin platform mining works differently from the classic mining that characterizes Bitcoin and other cryptocurrencies.

First of all, the Filecoin network has two consensus mechanisms: Proof-of-Replication (PoRep) and Proof-of-Spacetime (PoSt).

In Filecoin, miners instead of contributing computational power, contribute storage capacity to meet the needs of users/customers who want to store data. In other words, in the Filecoin ecosystem, miners work as “databases”.

In Filecoin they exist:

5 types of users that can trade FIL tokens which are: developers, customers, miners, token holders and ecosystem partners.

3 types of markets: file storage, file retrieval and token exchange.

3 types of miners:

– **Storage miners**: earn FIL token rewards by storing data for clients and computing cryptographic proofs to verify storage over time. Unlike Bitcoin miners, the probability of earning the per-block reward and transaction fees depends on the amount of storage these miners contribute to the Filecoin network, not hashing power.

– **Retrieval miners**: earn FIL tokens and mining fees for a particular file, depending on the market value and size of that file. Their bandwidth and initial bid/ask time for deals determine the total number of deals they can make.

– **Repair miners:** will be implemented in the future.

Each Filecoin miner has an associated power value on the network that is proportional to the amount of space contributed and determines the chances of earning the right to mine a block each epoch.

**Filecoin Rewards Mechanism**

In the Filecoin network miners get different types of rewards for contributing to the network.

The two main types of rewards are:

**Storage fees**

Storage fees are the fees regularly paid by customers after an agreement is reached, in exchange for data storage and for miners sending regular storage proofs to the chain. These fees are automatically deposited into a miner’s associated wallet as they perform their duties and are briefly blocked upon receipt.

PoSt (Proof-of-Spacetime) window checks are performed at 24-hour intervals across the network to ensure that miners continue to host their required sectors as normal. Each day that a miner is not idle, they will receive a fee for the failure committed.

**Block rewards**

By mining blocks, miners earn rewards and charge fees proportional to the amount of storage space contributed to the network.

The mechanism for obtaining the right to mine a new block is called WinningPoSt.

Unlike storage fees, these rewards do not come from an associated customer and it is the network that “prints” new FIL tokens as an inflationary measure and as an incentive for miners moving up the chain.

In addition to the block reward, each miner can collect the fees associated with each message included in the block.

**Verified customers**

To incentivize data storage, storage miners also have the opportunity to compete for special offers provided by verified customers who need the miner to guarantee significant data storage.

**Recovery fees**

Recovery fees are paid incrementally through the payment channels as recovery agreements are fulfilled.

**Penalties/Cuts**

These are penalties that miners must pay if they do not provide reliability to the sector or decide to voluntarily leave the network. These include:

**Fault slashing fees**: paid for each day that a miner’s sector is offline and does not send space-time evidence to the chain.

**Sector penalties:** is a penalty incurred by a miner for a failed sector that was not declared failed before a WindowPoSt check occurs.

**Termination fees** are a penalty incurred by a miner when a sector is voluntarily or involuntarily cancelled and removed from the network.

**Consensus failure reduction**: is a penalty incurred by miners when they commit consensus failures and when they have acted maliciously against the consensus of the network.

**Mining Requirements**

To mine Filecoin there are no minimum requirements although, following the guidelines on its official website, it is currently recommended that your computer has the following features:

CPU: The Filecoin team suggests an AMD with more than 8 cores and possibly supporting the Intel SHA extension.

GPU: A powerful GPU is recommended so that it can significantly accelerate SNARK computations. A list of supported GPUs is available on Github.

RAM: at least 128Gb is recommended.

Disco: According to the recommendations on the official Filecoin website, a minimum amount of NVMe-based disk space of 1TiB is recommended for caching that should be used to store data during the sealing process, to cache Filecoin parameters and serve as a general temporary storage location. Additional hard drives will also be needed for final storage of “sealed sectors”, Lotus chain, etc.

Once you have a computer with these features, you will need to install the Filecoin network client, called Lotus, and you are ready to start storing data from other users and earn your FIL tokens.

**Wallet to store FIL**

Lotus: If you want to use the Lotus wallet you will only need to have a Lotus node installed and running on your computer.

Ledger Nano: Another good option is to store your FIL in a hardware wallet such as Ledger Nano. This will give you the security that an online wallet cannot give you when storing your cryptocurrencies.

**REFERENCES**

<https://zebpay.com/blog/how-filecoin-works/#:~:text=Filecoin%20allows%20its%20users%20to,can%20interact%20with%20storage%20providers>.

<https://docs.filecoin.io/about-filecoin/how-filecoin-works/>

<https://coinmarketcap.com/alexandria/article/what-is-filecoin-fil-features-tokenomics-and-price-prediction>

<https://docs.filecoin.io/about-filecoin/what-is-filecoin/>

<https://kriptomat.io/cryptocurrencies/filecoin/what-is-filecoin/>

<https://blog.bitnovo.com/en/how-to-mine-filecoin-fil/>