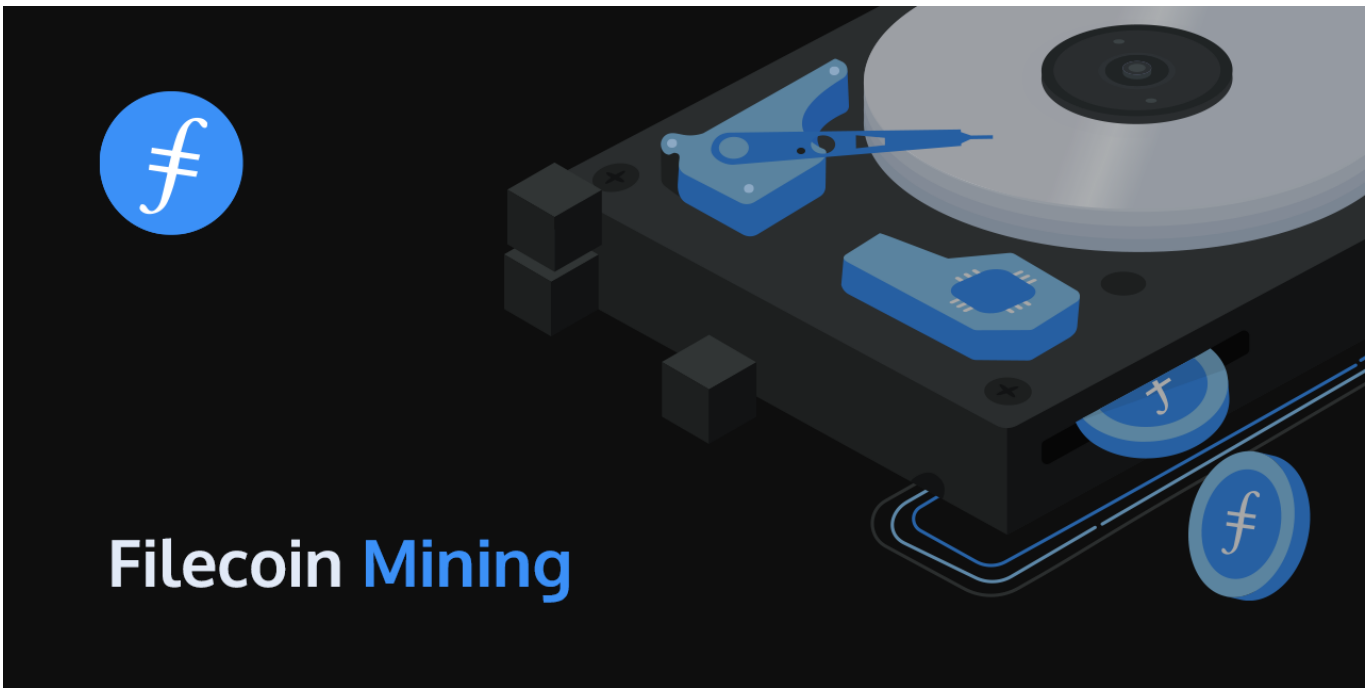
←Back to the index

July 7, 2020

A Guide to Filecoin Storage Mining



A lot has changed since our last set of guidelines for Filecoin testnet storage miners was published! At the time, we had just launched the first iteration of the testnet, and our advice then reflected the uncertainty and experimental nature of the nascent network. We're extremely grateful to all who participated (and continue to participate) in the testnet – thanks to your support, we've been able to rapidly mature our protocols and implementations. We're now in the second testnet phase, and are steadily progressing towards mainnet launch.

In this post, we offer an updated guide to Filecoin storage mining, and discuss some of the recently announced incentives and opportunities for members of the growing Filecoin community.

Please note that Filecoin is still being refined. New insights from the experimentation afforded by the testnet are actively being incorporated into the ultimate specification. Consequently, vital network parameters are still subject to change before the mainnet launch. We strongly encourage miners to buy hardware at small scale for testing, experimentation, and benchmarking before investing significant capital.

Participating in the Filecoin network

At the present time, there are two primary roles a node can play in the Filecoin network: storage and retrieval. We anticipate that miners will seek to specialize in particular roles.

Storage market

In the Filecoin network, nodes have the ability to contract with clients, offering to store their data for an agreed-upon period of time in exchange for filecoin.

Nodes that supply storage to the Filecoin network are termed *storage miners*. These nodes are periodically granted the ability to extend the Filecoin blockchain with blocks of their own creation. When they create a new block, storage miners are rewarded with newly minted filecoin, and by the transaction fees they can levy on other nodes seeking to include messages in the block.

Retrieval market

A node can additionally participate in retrieval contracts, supplying clients with a specified file in exchange for filecoin. This incentivizes well-placed nodes with high-throughput, high-bandwidth connections to participate in the network, promoting the widespread and rapid distribution of files – especially those that command high demand.

Other roles

A number of other roles (for example "repair" nodes that facilitate network self-healing) are presently in development, but are not yet finalized or supported in any implementation. However, the network is fully functioning without these proposed improvements.

Storage mining explained

The role of storage miners is to keep files on behalf of the Filecoin network. Storage miners must cryptographically prove that they are honoring their pledge to store these files – this is achieved via the mechanisms of *Proof-of-Replication* (PoRep) and *Proof-of-Spacetime* (PoSt). Pledging storage to the Filecoin network itself requires filecoin; these are used as collateral to ensure that storage miners uphold their contractual obligations.

Storing data

In the Filecoin network, data is stored in fixed-size *sectors*. Generally, storage miners fill these sectors with data stored on behalf of clients, who contract storage miner services for a particular length of time via *deals*. However, storage miners are not forced into making deals; if a storage miner doesn't find any of the available deal proposals appealing, they can alternatively make *capacity commitments*, filling sectors with arbitrary data. This allows them to provably demonstrate that they are reserving space on behalf of the network. If desired, sectors created to serve as capacity commitments can later be "upgraded" to provide the contracted storage for future deals.

Proof-of-Replication

Once a sector has been filled, PoRep sees storage miners *seal* the sector – sealing is a computation-intensive process that results in a unique representation of the data (the original representation can subsequently be reconstructed by *unsealing*). Once data is sealed, storage miners: generate a proof; run a SNARK on the proof to compress it; and finally, submit the result of the compression to the blockchain as a certification of the storage commitment. Storage reserved for the network through this process is termed *pledged storage*.

Proof-of-Spacetime

After PoRep has been completed, storage miners must continuously prove that they are still storing the data they pledged to store. This is accomplished via PoSt, a procedure in which storage miners are issued a cryptographic challenge that can only be correctly answered by consulting a sealed sector directly. The storage miner must respond to this challenge within strict time limits; the computational difficulty of sealing ensures that storage miners must maintain ready access to and integrity of the sealed sector.

In Filecoin, PoSt manifests in two distinct challenges: *WindowPoSt* and *WinningPoSt*.

WindowPoSt

WindowPoSt is the mechanism by which the commitments made by storage miners are audited. It sees each 24-hour period broken down into a series of windows. Correspondingly, each storage miner's set of pledged sectors is partitioned into subsets, one subset for each window. Within a given window, each storage miner must submit a PoSt for each sector in their respective subset. This requires ready access to each of the challenged sectors, and will result in a SNARK-compressed proof published to the 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 miner's continued commitment is kept.

The Filecoin network expects constant availability of stored files. Failing to submit WindowPoSt for a sector will result in a *fault*, and the storage miner supplying the sector will be *slashed* – that is, a portion of their collateral will be forfeited, and their storage power (see Storage Power, below) will see a reduction. Storage miners will have a limited period of time to recover from faults before they are considered to have abandoned their storage commitment altogether. Should the need arise, storage miners will also have the ability to preemptively issue a *declared fault*, which will result in reduced penalties, but which still must be addressed within a reasonable timeframe.

WinningPoSt

WinningPoSt is the mechanism by which storage miners are rewarded for their contributions. In the Filecoin network, time is discretized into a series of epochs – the blockchain's height corresponds to the number of elapsed epochs. At the beginning of each epoch, a small number of storage miners are *elected* to mine new blocks (Filecoin utilizes tipsets, which permit multiple blocks to be mined at the same height). Each elected miner who successfully creates a block is granted filecoin, as well as the opportunity to charge other nodes fees to include messages in the block.

A storage miner's probability of being elected corresponds to their storage power. In a process similar to that underlying WindowPoSt, storage miners are tasked with submitting a compressed proof of storage for a specified sector before the epoch concludes. Storage miners who fail to complete WinningPoSt in the necessary window will forfeit the opportunity to mine a block, but will not otherwise incur penalties for their failure to do so.

Storage power

A Filecoin storage miner's *power*, which corresponds to the likelihood that a storage miner will be elected to mine a block, is roughly proportional to the amount of storage they have sealed on behalf of the network. To further incentivize the storage of "useful" data over simple capacity commitments, storage miners 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 miner earns for these deals is augmented by a multiplier. The total amount of power a given storage miner has, after accounting for this multiplier, is known as *quality-adjusted* power.

Filecoin implementations

The *Filecoin Distributed Storage Network* is an open specification with numerous implementations.

At the time of writing, the most mature implementation, and the one that should be used to access the current testnet, is the Go-based Lotus. The Lotus client is capable of running on Linux and macOS; detailed instructions for installing and using Lotus are available via its documentation.

There are at least three other implementations currently undergoing active development. These include go-filecoin (another Go-based implementation), forest (a Rust implementation developed by ChainSafe), and fuhon (a C++ implementation by Soramitsu).

Hardware considerations

Participants in the Filecoin network will need to ensure that their systems are sufficiently equipped for the role they are intended to fill.

Running the Lotus client without mining

If you don't wish to mine, but would still like to run the Lotus client for the purposes of keeping a wallet or interfacing with the network, a system with 2-4 CPU cores, 8GiB of RAM, and enough storage for the Filecoin blockchain should be sufficient (the current testnet chain grows at about 12GiB per week; improvements to reduce this storage requirement are ongoing).

Storage mining

It bears noting that in its current state, Filecoin storage mining necessitates fairly powerful hardware to meet the storage and proof requirements. These requirements are driven largely by the design constraints imposed by the PoRep and PoSt mechanisms, and the balance that needs to be struck between accessibility, computational feasibility, and cryptographic security.

Filecoin storage mining is *not* proof-of-work mining – sealing storage is the only way to gain power on the network – but fast and efficient hardware is required to compute the necessary proofs in an acceptable timeframe. Protocol Labs is currently working on ways to relax these requirements (for example, by introducing efficiencies into the proof mechanisms themselves, or by outsourcing SNARK computation to obviate the need for expensive GPUs). In the meantime, however, before making a large investment in hardware, prospective storage miners should carefully consider and experiment with the composition of their systems to ensure that they are capable of the performance required.

Example mining machines and benchmarks

The optimal system composition will depend largely on a storage miner's operating model, include capital expenditure and operating cost; as such, Protocol Labs is unable to give any concrete recommendations. We have, however, published some of our own designs, including outlines for machines that are presently suitable for testing and small-scale mining.

We expect storage miners to tailor their configurations to their own needs; it is possible to mine on the testnet with alternative configurations, and we expect that many of these configurations will surpass the efficiency of our own builds. We encourage experimentation, and would ask interested community members to share their own benchmark scores on GitHub.

General hardware concerns

While we cannot give concrete recommendations, we can offer some general guidelines.

CPUs. As a rule of thumb, multi-core CPUs with high clock rates will accelerate the sealing process, allowing storage miners to onboard storage to the network more quickly. Protocol Labs' own testing has shown modern AMD processors with SHA extensions to offer sizable advantages over other processors.

GPU. Powerful GPUs are necessary to complete SNARK computations within the required time limits. Lotus is currently designed to support NVIDIA-manufactured chips; we anticipate supporting cards from other manufacturers in the future. Our benchmarks offer insight into chips that we have had success with.

RAM. The current Filecoin network only supports the sealing of 32GiB and 64GiB sectors. Performing the necessary computations on these larger sectors requires commensurately more RAM; it is advised that mining systems be equipped with at least 128GiB.

Storage. There are numerous considerations involved in selecting an appropriate storage solution, perhaps the most important being the specific revenue model assumed by the mining operation. Storage miners currently need to pledge 1TiB of raw storage (or its quality-adjusted equivalent; this will be increased to 100TiB for the mainnet) in order to mine blocks, but there are many more factors beyond this requirement that they might find it useful to consider.

- First and foremost, storage miners should be mindful of the slashing penalties for losing data; even one flipped bit could result in steep penalties. As a consequence, storage miners may wish to factor in overhead to implement data redundancy.
- It may also be prudent for storage miners seeking to participate in the retrieval market to consider incorporating additional storage in preparation for serving "hot" copies of sealed data. Although it is of course possible to unseal a sector to recover the original data, a Filecoin implementation that supports this use-case would eliminate this computational burden (this is a feature presently in-development for Lotus).
- Another consideration to take into account is the Filecoin network's expectation of high availability. While in theory storage miners should be able to participate with most commodity HDDs, SSDs, or other suitable, non-cold storage solutions, not all storage solutions can be relied upon to perform optimally when operating $^{24}/_{7}$.
- Storage miners currently require enough space to store the blockchain itself as well; shrinking the footprint of the blockchain on-disk is a feature in active development for Lotus. Filecoin implementations may also require additional on-disk storage, equivalent to a small percentage of pledged storage, for bookkeeping.
- Finally, Protocol Labs has found in testing that employing NVMe storage as swap space can serve as a supplement in systems with lower amounts (128GiB) of RAM; storage miners may otherwise experience out-of-memory issues during certain operations (sealing, in particular, requires a large amount of working memory).

Network. If using distributed Lotus seal workers (see Advanced mining considerations, below) high-performance networking is suggested (10GbE+ network cards and switches are recommended). High-performance networking is also suggested when using network-attached storage.

Advanced mining considerations

As previously discussed, Filecoin storage mining is dominated by concerns related to the PoRep and PoSt mechanisms. PoRep itself is comprised of several stages, and the Lotus implementation of Filecoin facilitates the delegation of these stages to different machines for maximum efficiency using *seal workers*. Protocol Labs has developed an example architecture designed to leverage these capabilities for large-scale mining. Here, we break down the different bottlenecks to consider when designing similar systems.

Sealing preCommit phase 1. In this phase, PoRep SDR encoding takes place. This stage is CPU-bound, and single-threaded (by design, it is not amenable to parallelization). This stage is expected to take on the order of several hours, with the precise amount of time depending on the size of the sector being sealed and, of course, the specifications of the machine doing the sealing. As previously noted, Protocol Labs (and others) have found that AMD processors with SHA extensions accelerate this process to a considerable degree. Using CPUs with higher clock rates will also improve performance.

Sealing preCommit phase 2. In this phase, Merkle tree generation is performed using the Poseidon hashing algorithm. This process is primarily GPU-bound – a CPU can be utilized as an alternative, but should be expected to be considerably slower. When employing a GPU, this phase is expected to take on the order of 45 minutes to an hour.

Sealing commit phase 1. This is an intermediate phase that performs preparation necessary to generate a proof. It is CPU-bound, and typically completes in tens of seconds.

Sealing commit phase 2. Finally, this sealing phase involves the creation of a SNARK, which is used to compress the requisite proof before it is broadcast to the blockchain. This is a GPU-intensive process that is expected to take on the order of 20-30 minutes to complete.

Protocol Labs has found it efficient to co-locate preCommit phase 2, commit phase 1, and commit phase 2 on the same machine, leveraging high-density compute machines for preCommit phase 1. However, there is a large file transfer between preCommit phase 1 and preCommit phase 2; on machines that have slower network access or that use hard disks instead of solid state drives, this may outweigh performance gains made in other areas. In this case, having all phases occur on the same machine may be more efficient.

PoSt is primarily GPU-bound, but can take advantage of a CPU with many cores to accelerate the process. WindowPoSt, for example, must currently take place within a 30-minute window; the difference between an 24-core CPU and an 8-core CPU could be the difference between clearing that window by a comfortable margin and just narrowly passing in time. WinningPoSt is a less intensive computation that must be completed in the much smaller window of a Filecoin epoch (currently 25 seconds).

Joining Testnet Phase 2

Our *testnet* is the preliminary stage to the official launch of the Filecoin network – we're currently in Testnet Phase 2, which is expected to run until the *mainnet* launch in Q3 2020.

During the testnet phase, storage miners can retrieve filecoin from our faucet to serve as the collateral necessary for pledging storage.

Please note that testnet filecoin do not have any value – official filecoin will only be available after the launch of the mainnet.

Accelerating the Filecoin ecosystem

As the launch of the mainnet approaches, a growing number of opportunities are becoming available for community members to get involved with Filecoin.

SpaceRace

In preparation for the mainnet, Protocol Labs has recently announced an incentives program, SpaceRace, to stress-test the testnet. Participants will have the opportunity to compete for mainnet filecoin by onboarding as much storage as possible.

HackFS

HackFS is a 30-day virtual hackathon aimed at building the foundation of the decentralized web. Developers will build dapps, games, dev tools, DeFi integrations, and other hacks that utilize decentralized storage. HackFS will be hosted by ETHGlobal and Protocol Labs, and will have all the hackathon staples: workshops, mentorship, inspiring talks, AMAs, and prizes!

Filecoin Discover

Filecoin Discover is a recently announced initiative to seed Filecoin with some of humanity's most valuable cultural and scientific data. Individuals that buy in to the Discover program will receive one-year quality-adjusted storage deals, with Discover acting as the verified client.

Filecoin dev grants

We continue to promote the growth of the Filecoin ecosystem by sponsoring contributors via Filecoin dev grants. The Wave 4 grant proposal deadline was July 1st for priority consideration, but we will continue to evaluate proposals submitted after the deadline as capacity allows. Wave 5 proposals will be due October 1st.

Summary

Blockchains are complicated pieces of software with a lot of moving pieces, and building a successful blockchain from scratch is a tremendous undertaking. Filecoin would not be where it is today without the support it has received from community members all over the world, and we cannot emphasize enough how grateful we are to everyone who has helped Filecoin get to this point! Once again, thank you for your continued support, involvement, and patience as we enter the final days before the mainnet comes online. We are extremely excited to be welcoming new community members into the fold – miners, developers, and users alike – and hope that this guide can serve as a jumping-off point for anyone looking to join us as we embark on the next steps of this awesome journey!

← Back to the index