FileStar Project Litepaper

A Web3.0 Decentralized Storage，Verifiable Computation，Mensurable Bandwidth Physical Infrastructure

By dev@filestar.net

2020.10.20

Abstract

The blockchain industry has plateaued and needs substantial technical innovations to propel it to the next level.

In 2009, Satoshi Nakamoto published the Bitcoin Whitepaper, ushering the world into an era of cryptocurrencies. But limited by its network scalability issues, Bitcoin has digressed from its original goal as a digital currency and was instead nudged by the market to be the digital gold. Ethereum added a smart contract virtual machine to the Bitcoin concept, enabling programmability and more flexibility. The Ethereum smart contract is Turing complete and hence more powerful than the BItcoin script. Ethereum has achieved enormous success. But still, Ethereum has its constraints.

Regardless of their differences, Bitcoin or Ethereum is essentially providing computation and data consistency in a peer to peer network. Due to the scarcity of on-chain resources, Bitcoin can only process its own transactions, and Ethereum can process limited transactions and logic for Ether and ERC20 tokens. The existing public blockchains are siloed networks. And both Bitcoin and Ethereum rely on their full nodes' hardware, which has apparent limitations and bottlenecks the networks' processing power. Ethereum is like a micro cloud service, providing global consistency but minimal processing capabilities.

Filecoin is the first project that bridges the physical world and the blockchain world. By using Proof of Spacetime, it connects large volumes of powerful processors and other hardware to the blockchain world, bringing an end to the mere internal loop of the blockchain world.

FileStar is a further step forward based on Filecoin. Unlike the storage-centric Filecoin, FileStar incentivizes the community to build the infrastructure for decentralized storage and verifiable computation, and measurable bandwidth. FileStar aspires to serve all future blockchain projects. For example, in the future, Ethereum Rollups will be able to verify on FileStar. FileStar is an improvement based on Filecoin. It will keep iterating and build the physical infrastructure for Web3.0.

The blockchain essentially provides a set of distributed clearing and settlement protocols. If the blockchain can only clear and settle tokens issued by weak-credit communities, it does not fully utilize blockchain's value. Current oracles can bring simple real-world information such as prices on-chain. FileStar will further bridge the physical world with the blockchain world. FileStar aspires to bridge real computation, storage, and bandwidth of the Internet to the blockchain, form unified measurement and representation of such resources, and migrate those resources on-chain, building the physical infrastructure for a distributed Internet.

Background

On October 15th, 2020, the Filecoin mainnet went live at the block height 148888. Filecoin has been one of the most expected distributed networks. It proposed a new proof mechanism, the Proof of Replication (PoRep), and the Proof of Spacetime (PoST). The proof mechanism is the first success representation and measurement of real-world storage resources on-chain. On top of that, Filecoin has also attracted many miners with powerful processors to join the network. The Filecoin network has integrated a large volume of computation, storage, and bandwidth resources. Filecoin and its design principles are excellent references for the future of the blockchain+ Internet's infrastructure. It has been a significant milestone for the whole blockchain industry.

Although Filecoin is a great innovation, its design is not perfect and might hinder its growth.

- Unlike Filecoin's "decentralized" storage concept, Filecoin's project development and management tend to be "centralized." The Filecoin team was still revising its consensus mechanism, key features, and economic model right before the mainnet launch, which has affected the stability of the network to a certain extent;
- The Filecoin token(FIL) distribution and release plan are relatively unfriendly to miners. At the early stage after the mainnet launch, the miners can only buy FIL tokens through the market to pay Pledge Collateral and sustain mining. That's why a large percentage of miners stopped on-ramping storage as soon as the mainnet launched. The economic design does not have a good incentive for infrastructure providers (i.e., miners). Also, other community participants are not sufficiently motivated, and their willingness to maintain the network is not strong;

- The threshold for participating in Filecoin mining is relatively high. Miners need to have many FIL tokens to deposit as Pledge Collateral before they start mining and purchase mining machines with high-end processors. Both requirements have hindered retail miners or miners with Intel processors to participate.
- The Filecoin network architecture and technical design result in a relatively limited amount of on-chain processing capability (TPS). When the network is congested, it is impossible to prove valid storage on-chain or process regular transactions. This will be a critical constraint for the network to scale.
- The availability of data stored in the Filecoin network is relatively limited, and it can only store some “cold data” that is not frequently used; for “hot data” that needs to be accessed at any time, the Filecoin network is not suitable;
- Besides, the mining software officially launched by Filecoin still has a large room for optimization in sealing efficiency. In a sense, it is a waste of real-world storage, computing, and bandwidth resources.

Therefore, Filecoin still has a long way to go before it becomes a usable decentralized storage infrastructure. Storage has already been only a part of the Internet infrastructure. In the future, the distributed Internet will require a complete set of incentive mechanisms to encourage miners to contribute to the storage, computing, and bandwidth resources.

FileStar Vision

FileStar aspires to become the Web3.0 Internet infrastructure, build a distributed storage, computation, and bandwidth network based on IPFS, integrate the global Internet infrastructure resources, and realize optimal use of resources. Our vision is fundamentally different from the storage-centric Filecoin.

The Main Difference from Filecoin

FileStar has a more reasonable incentive mechanism for distributed storage. It will gradually evolve from that to be an incentive layer for the distributed Internet, enabling incentive at a more refined granular level and facilitating an optimized utilization of computation, storage, and bandwidth resources.

The main advantages of FileStar are:

- Lower mining requirement: no Pledge Collateral in the early stage of the network; no SHA256 algorithm and therefore no longer dependent on AMD processor exclusively, hence more miners can join the network;
- Higher scalability: FileStar modifies the WindowPoST's spot check logic and introduces recursive storage proof to improve the on-chain processing capability and TPS;
- High-efficiency mining software: FileStar improves the performance of existing Filecoin mining software and improves the overall sealing efficiency of the network;
- High data availability: FileStar can store “hot data” and “warm data,” and users can quickly access the stored data.
- Decentralized governance: FileStar adopts community governance. Developers, miners, and other participants in the community will jointly determine the direction of the network;
- Reasonable token distribution: FileStar will do a fair launch, with no pre-mining, no fundraising. Most of the tokens will be distributed through mining and as long-term incentives to all participants;
- FileStar will map rewards for the valid storage on Filecoin. FileStar will incentivize Filecoin miners to maintain the FileStar Network jointly.

FireStar Technical Improvements and Innovations

As the first step of a distributed Internet incentive network based on the IPFS protocol, FileStar has several technical improvements and innovations.

No Pledge Collateral

In Filecoin, Pledge Collateral means that the miners must lock FIL for each sector till the end of the sector's life cycle. It is a security mechanism to encourage miners to store data for a long time and ensure data availability.
However, the design of the Pledge Collateral in the current Filecoin network is not reasonable. First, the Pledge Collateral per sector is not a small amount. When the Filecoin network grows, miners are not likely to have a positive cash flow for a long time because of the Pledge Collateral and unable to sustain. Second, most of the sealed sectors are "junk sectors," meaning order sectors that do not have valid data. It does not make any sense to lock Pledge Collateral to ensure the availability of the junk data. Pledge Collateral is the main reason that miners went on a strike.
In addition to Pledge Collateral, the Filecoin network also locks the mining reward. All mining rewards will be vested gradually through 180 days under the premise that the data is continuously stored. Locked mining rewards alone can ensure data security and availability.
Therefore, FileStar will remove Filecoin's Pledge Collateral and keep the mining reward vesting mechanism. FileStar will also make the following improvements to the collateral rules to further ensure safety.

- First, FileStar will allow "junk sectors" to have a shorter life cycle. The junk sector's primary purpose is to prove a corresponding valid storage space available in the network. The life cycle of any sector in the Filecoin network is at least one year. But in fact, storing junk data for an extended time is a waste of resources. In the FileStar network, the junk sector that does not store any valid data will have a shorter life cycle to avoid waste of resources;
- Secondly, FileStar's order sectors will require collaterals. The order sector stores valid data from the users. Using the users' storage fees as collateral encourages the miners to prioritize order sectors and ensure data availability.

By removing the Pledge Collateral, FileStar encourages the miners to join the network at any time and gives miners a long-term incentive to maintain the network.

New Hash Algorithm

Filecoin uses the SHA256 hash algorithm, which relies heavily on the optimization of the instruction set of the AMD processor and excludes a large volume of Intel processors that do not support instruction optimization. The limited hardware compatibility excludes a large amount of Intel miners and restricts the Filecoin network's growth.

FileStar aspires to become the incentive layer of the future Internet infrastructures, and encourages more diverse hardware into the network. Therefore, while ensuring security, FileStar must make sure that X86 based miners have the same performance. FileStar is testing different hash algorithms, including SHA512, Poseidon, Pederson, and Blake2s. FileStar will evaluate these hash algorithms' security and feasibility on various platforms and choose the most suitable one to support Intel mining machines or other high-performance mining machines.

Recursive ZK-SNARK

Proof of Copy (PoRep) is an essential part of the Filecoin storage proof system. Combined with zero-knowledge proof, PoRep can quantify storage resources and generate corresponding proofs on-chain. In Filecoin's PoRep proof mechanism, when the miner seals one sector, they need to submit two proofs to the network, and the corresponding messages are PreCommitSector and ProveCommitSector. In the existing Filecoin network, most of the on-chain messages are the submission of these two proofs. However, the on-chain message processing capability (TPS) of the Filecoin network is minimal. When the network becomes congested, the proof messages will occupy most on-chain resources, and ordinary messages will not be packaged. This also leads to the "self-mining" behavior of many miners, meaning miners only process its own messages, and the proof messages of small miners cannot be put on-chain.

FileStar proposes a Recursive ZK-SNARK technology to solve the above-mentioned TPS bottleneck problem.

The basic concept of Recursive ZK-SNARK is that the proof of multiple sectors produced within a certain period will be verified off-chain, forming a Merkle tree and generating an aggregate proof. At the end of that period, only one proof needs to be submitted to the network, containing proof of multiple sectors. It significantly reduces the amount of the proof message that each miner needs to submit. The Recursive ZK-SNARK improves TPS and achieves network scaling. By adjusting the number of aggregated proofs, it will adapt the network's processing capability to meet the needs of different development stages of the FileStar network in the future.

WindowPoST + VRF

After completing the PoRep, the miners need to provide the Proof of SpaceTime(PoST) to prove that the data has been continuously stored. The miner will get penalized when he fails to submit Proofs-of-Spacetime to the chain. Large miners need to submit a massive number of PoST. As the network grows, the number of WindoePoST submissions will also increase, which will lead to network congestion and affects normal message processing.

FileStar introduces a random checkup for WindowPoST, lowering the WindowPoST submission frequency. If the miner can predict the time of checkup, they can potentially cheat and hamper network security. Therefore, FileStar uses the Verifiable Random Function to avoid such acts.

High-performance Mining Software

FileStar will also optimize the existing open-source mining software, fully improve the mining efficiency. The optimization mainly focuses on the task scheduling module and the zero-knowledge proof module.

- Task scheduling optimization: all things being equal, different task scheduling strategies will directly affect the mining machine's sealing efficiency. The mining software of Filecoin has many flaws in task scheduling, which has affected the network storage growth. FileStar will release mining software with optimized task scheduling to increase the mining efficiency of the miner.

- Zero-knowledge proof optimization: both the PoRep and PoST in Filecoin uses zero-knowledge proof. There is a large room for optimization in the creation process of zero-knowledge proof. FileStar will optimize the zero-knowledge proof and offer it for all miners.

In general, FileStar will have a much high mining efficiency than Filecoin, meaning that with the same hardware input, FileStar will likely be a larger distributed storage network.

Filecoin Storage Mapping

The Filecoin network has nearly 600 PiB of valid storage, and it is still growing. Filecoin miners are the pioneers in building the decentralized storage infrastructure. They will also be a cornerstone of the Web3.0 infrastructure. After launch, FileStar will map rewards for storage on the Filecoin network. If Filecoin miners join FileStar mining, they will have the chance to receive FileStar rewards proportionate to their storage power on Filecoin. The specific mapping rules will be announced when the FileStar mainnet is launched.

Decentralized Governance

The FileStar development team is responsible for maintaining the FileStar project. The community will determine future development and governance.
In the FileStar community, anyone can submit a pool request with a complete test code. All submissions will be merged into the test network after a thorough test and launched on the mainnet after stable running for some time.
The FileStar project fully respects the opinions of all community participants. The development and launch of each new feature require community members to vote on. FileStar developers, miners, and average token holders can participate in the vote and jointly determine the network's direction.

Token Economic Model

The FileStar protocol native token is STAR, used to pay for gas and storage. Miners get STAR mining rewards and gas rewards. To attract miners to contribute to the storage, computing, and bandwidth and encourages the participation of more dynamic participants, FileStar has designed a more refined token incentive model.

The total supply of STAR tokens is 2,000,000,000 STAR, with no fundraising and no pre-mining. The token distribution is as follows, which may subject to fine-tuning at the mainnet launch:

- 70% to FileStar miners, the output decreases daily and halves every six years
    - 30% to storage miners
    - 15% to computation miners
    - 15% to bandwidth miners
    - 10% to other valuable miners, such as zero-knowledge proof services, AI, big data, which will be decided by the community
- 30% to long-term community participants
    - 15% to the FileStar Foundation, 5-year vesting from one year after mainnet launch;
    - 7% to community developers
    - 5% to projects and apps in the FileStar ecosystem;
    - 1% to media & community
    - 1% to exchanges and wallets that support FileStar
    - 1% to legal and compliance

Project Roadmap

- October 20th, 2020 Release the first draft of the whitepaper;
- October 30th, 2020 Release the first version of FileStar code, with filecoin-based improvements such as removal of Initial Pledge Collateral and several Filecoin bug fixes;
- February 28th, 2021 Implement most of the designs in the whitepaper, including the new sealing Hash algorithm, Recursive ZK-SNARK to improve the full TPS, and introduction of random checkup of Window PoST+VRF, etc.;
- August 30th, 2021 Launch the verifiable computing network, encourage some of FileStar’s miners to switch to mine the verifiable computing network
- December 30th, 2021 Launch the measurable bandwidth network, encourage some of FileStar's miners to mine the measurable bandwidth network;

Future Works

In FileStar’s vision, the successful launch of an incentive layer for decentralized storage is step one. The incentive layer will attract large volumes of hardware, providing abundant storage, bandwidth, and computation resources. After the network is stable in the first stage, FileStar will execute a more diversified incentive mechanism to encourage the building of Web3.0 infrastructure. Directions include:

- Propose a proof mechanism for computing and bandwidth resources to further attract different resource providers to build a decentralized computing network and distributed bandwidth network;
- Incentivize computation resources on FileStar to provide zero-knowledge proof services for other nodes;
- Provide verifiable computing services for other nodes in the network.

Summary

Based on Filecoin, FileStar implements a better incentive layer for distributed storage network, with improvements such as the removal of Initial Pledge Collateral and the use of new hash

functions, which have collectively lowered the threshold for mining. FileStar also adds Recursive ZK-SNARK, PoST+VRF, and other technological innovations to solve the TPS and on-chain message congestion, with much-improved scalability and mining efficiency.
FileStar will have a fair token launch and adopt community governance. It will be equal and long-termly sustainable.
FileStar aspires to build a network of distributed storage, computing, and bandwidth based on the IPFS protocol, becoming a significant cornerstone of the Web3.0 infrastructure. Unlike storage-centric Filecoin, FileStar will incentivize participants to provide verifiable computation and measurable bandwidth resources in addition to distributed storage. With the blockchain industry's collective endeavor and the dedication of the FileStar team, we will soon see the distributed Internet unfold.

Contact us

Official website: https://filestar.net
Developer: dev@filestar.net
Media: media@filestar.net

Community

Github: https://github.com/filestar-project

Slack: https://join.slack.com/t/filestarworkspace/shared_invite/zt-infr76dh-S3m3SwbjMTMAXIUUU54efw

Twitter: https://twitter.com/FileStarProject
Telegram: https://t.me/filestarofficial
WeChat: filestarofficial