Filecash English Whitepaper V2

1. Introduction

IPFS is an emerging Internet content acquisition protocol committed to providing an alternative to the HTTP protocol and to create a content-based underlying Internet protocol.

As of present, a robust ecosystem has been built based on the IPFS protocol, and Filecoin has become one of the most influential blockchain projects built on top of it.

The Filecoin project was founded in 2017 and has undergone many iterations along its development path leading to multiple delays of its mainnet. The main net will be launched soon, and market enthusiasm for Filecoin has reignited. However, just before the mainnet launch, Filecoin's centralization problem has grown increasingly severe, as it has gradually diverged from the decentralized nature of blockchain.

Filecoin is becoming more and more like a corporate product under their developer Protocol Labs, rather than a blockchain community project.

Filecoin has repeatedly ignored miners' feedback and proposals for adjusting the consensus algorithm, resulting in a large number of miners' equipment failure. Before the mainnet launch, Filecoin has repeatedly made adjustments to their economic model, which have challenged the miners' bottom line, and left them feeling left behind.

Members from the IPFS community inherited the original intention of IPFS, and aim to rebuild a community-driven decentralized storage system, thus initiating Filecash. The goal is to create a win-win ecosystem that is miner-friendly, community-friendly, user-friendly, and investor-friendly.

As Filecoin's first pre-fork project, most of the features of Filecash are similar to those of Filecoin, so this whitepaper will focus on the characteristics and optimization points of Filecash that differ with Filecoin.

In addition, the economic model will not be elaborated in the V1 version. The details will be disclosed in the updated V2 version.

Table of Contents

2. Values

Filecoin's original vision was to use the idle hard drive space from individuals' computers globally to serve the storage ecosystem. However, during its development path, Filecoin has deviated from its original vision and ordinary household hard drives cannot meet the main net requirements for storage, and the cost of procuring designated mining equipment is becoming more expensive.

Filecoin miners face extremely high penalties for failures to retrieve effective data and this harsh penalty becomes a barrier to entry for miners. Filecoin's mining ecosystem is transitioning towards that of a centralized cloud service provider. In the Filecoin environment, the miners and the participants are forced to use more expensive and commercial-grade hardware in IDC level environments, resulting in overly centralized network performance and low usability.

Filecash is committed to restoring Filecoin's original vision. Using the world's idle hard drive space to serve the storage market, Filecash will construct a storage infrastructure for Web 3.0 that is community-driven and autonomous.

3. Consensus

Filecash is designed with the goal of *"creating a Web 3.0 basic storage engine that everyone can participate in"* as its core. Web 3.0 is an open and free ecosystem. As the basic storage engine of Web 3.0, Filecash needs to create an open ecosystem environment with lowering the barrier to participation as one of its core missions.

➢ **Compatible with Idle Capacity**

The original vision of Filecoin was to use the world's idle hard drives to realize storage. Filecash returns to its origins and reduces the threshold for user participation by optimizing the algorithm to ensure existing idling hard drives can be compatible with Filecash's main

network.

➢ Improving the Base Algorithm

Filecash will upgrade the current AMD-centric algorithm to support Intel processors with the same performance, which accounts for more than 90% of the market share. This upgrade will widely expand the potential market size of IPFS ecosystem.

➢ Remove Regional Restrictions

Filecoin officially divides the world into 5 major regions and token distribution is carried out in the form of a planned economy among the regions. We think this is unreasonable and far too simple. Filecash's token distribution model removes area restrictions, uses code to detect geographic regions, and allows the storage market to automate the distribution and control of tokens.

➢ Reduce the penalty of Proof-of-Space-Time

Proof-of-Space-Time is designed to improve the security of the system, encourage miners to continue storage, and validate their storage capabilities. This sounds very logical and reasonable, however, the Space-Time proof itself cannot enter the production environment. Only when the Proof-of-Space-Time storage upgrades to a block of valid data can it enter the production environment. Therefore, excessive punishment in the Proof-of-Space-Time algorithm will only reduce miners' enthusiasm, discourage participation, and raise the barrier to participation.

➢ Improve System Fault Tolerance

It is not feasible to rely solely on the penalty mechanism to ensure the security of the system. The internal system may be secure, but can be vulnerable to external attacks. Even a harsh penalty mechanism cannot ensure the system's regular operation in the case of a single point failure. Therefore, the security of the production process needs to be improved.

4. Feasibility

➢ **Modify the sha256 Algorithm**

For the fairness of AMD, Intel, and general-purpose processors, different processor's performance needs to be algorithmically compatible and averaged. Filecash will consider modifying the Sha256 algorithm to reduce the AMD processor's advantage with the ShaIn expansion set. The goal is to reduce the advantage that AMD processors have during performing P1 and P2 computations.

➢ **Modify the P1 Layer**

In the current official Filecoin code, P1 implements 11 layers of encrypted calculations. Excessive P1 calculations do not substantially improve security. Instead, an extensive amount of computational burden is imposed on the miners, wasting resources. These meaningless calculations yield zero substantial gain to the storage itself.

➢ **Modify the P2 Layer**

P2 shares the similar problem of repetitive calculations as P1, taking up many computing resources without adding value.

➢ **Modify the Order System**

The Filecoin original code contains an order matching market, but this single order matching system is shared for globally, which lacks efficiency, and usability. Filecash plans to develop an order matching system similar to Uber. The order is divided into regions where various performance data of miners, including latency, capacity, and absolute bandwidth, are displayed simultaneously, so as to facilitate users' order selection.

➢ **Revise the Proof-of-Space-Time validation**

Proof-of-Space-Time validation needs to happen regularly. When the miners have stored

enough space-time proofs, the system will not only prove the additional storage space but also consume considerable overhead to prove the existing storage space. The validation of consensus in the system is too redundant and reduces overall efficiency. Filecash will modify the Proof-of-Space-Time validation algorithm, simplify the redundant validation process, and minimize the overhead to maximize storage performance.

5. Technical Roadmap

➢ **Optimize Smart Contract Support**

The Filecoin native system is immature in supporting smart contracts. Filecash will consider directly inheriting the smart contract code of Ethereum to establish the foundation for the application layer of the Filecash ecosystem. At the same time, the directly inherited smart contract code facilitates the transplantation and development of the existing blockchain ecosystem. This makes it easier for developers to migrate to Filecash's ecosystem.

➢ **Optimize Data Distribution Logic**

Filecash will optimize the underlying storage structure, optimize the P2P network data distribution logic, and divide the storage nodes into 3 levels. The first layer is the IDC-level raw data layer; the second layer is the data storage layer for miners; and the third layer is a P2P layer that accelerates ordinary bandwidth. By optimizing the peer-to-peer data distribution logic, usability and economy performance can both be achieved in balance.

➢ **Optimize the Node Mechanism**

Filecash believes that it is more reasonable to build a blockchain structure with a dual-layer network in the IPFS ecosystem. The bottom layer is responsible for building the basic economic model and maintaining the security of the economic model layer, while the second layer builds the application system. The bottom layer uses IPFS mining machines to provide basic security. At the user experience level, when users use Filecash's blockchain, they will be unaware of the existence of the second-layer network yet enjoy the fast and efficient user

experience. The dual-layer system will significantly enhance user experience, attracting more applications and non-blockchain users to the ecosystem.

In the structure of the dual-layer network, random number generator and node elections will be used for block verification. The total number of nodes will be limited so that faster block confirmation speed and a higher TPS can be achieved, similar to the experience of a consortium chain. This will lead to a more friendly user experience for applications such as DEX, DeFi, and Dapp.

➢ **Increase PoS Flexibility**

PoS is an excellent alternative to PoW that often brings a better user experience. Filecash has designed a more flexible operating mechanism for PoS nodes. Through the random number + election system, nodes will have better fault tolerance, give faster transaction confirmation, and a higher TPS.

➢ **Add Cross-chain Support**

As part of the Web 3.0 blockchain infrastructure, Filecash's cross-chain compatibility is crucial. Filecash has developed a set of efficient and highly compatible cross-chain middleware based on Filecash's tokenomics. The middleware enables Filecash to interact with the external systems through a cross-chain bridge. Meanwhile, the native cross-chain components will significantly reduce the cost of using Filecash and acquiring information.

➢ **Add Oracle Support**

Oracles are the most indispensable middleware in the Web 3.0 ecosystem, but third-party oracles have low performance and high cost. With Filecash PoS node's previously mentioned advantages, a native oracle can be built to achieve an integrated solution of storage, retrieval, and oracle feed within the node, which will reduce the waiting time for Dapps to obtain data and maximize node server processing performance. Since off-chain data access and data processing are reduced, this can increase the speed and performance of the blockchain and

greatly reduce the cost of oracle data acquisition. This will reduce the cost of user cross chain interactions and is conducive to a prosperous blockchain ecosystem.

➢ **Optimize Virtual Machine Performance**

Although the Ethereum virtual machine is optimized to near perfection, Filecash is not as simple as a public chain, and a lot of work and modifications has been carried out to optimize the Filecash virtual machine's performance for storage.

➢ **Enhance Blockchain Interoperability**

A complete oracle and cross-chain middleware set the hardware foundation for blockchain interoperability. Filecash will redefine blockchain interoperability by unifying API and building the middleware system with developers from Filecash's ecosystem, achieving efficient and concise interoperable functions with a mature middleware system.

6. Economic Model

➢ **Basic Release Improvement**

The security of the ecosystem lies in its equilibrium. The equilibrium of miners, participants, and external opportunity cost all need to be carefully factored into the establishment of the economic models. A sound equilibrium game model guarantees the stability of the ecosystem, especially in the later stages of development. With a strong user base, data security relies on the survival of the main chain. A reasonable equilibrium model and a fault-tolerant mechanism based on the equilibrium game model are rational security guarantees and bring higher security than miners' short-term belief and loyalty to the project.

Filecash will prioritize changes in the existing economic model that can benefit the miners.

On top of the staking model designed by Filecoin, Filecash added the concept of base release amount. Treating the miner network as an economic system, miners release the tokens in the

network through mining to increase the supply. In the original Filecoin tokenomics design, a certain amount of tokens must be staked upfront before miners can participate in the main net mining. To improve this mechanism, Filecash will introduce a 10% benchmark release. Miners can participate in the Filecash ecosystem to carry out mining activities without any staking, and promote economic activities on the network.

Filecoin raised the baseline concept, an excellent design to prevent the rapid centralization of the network in the early stage and avoid the appearance of giant whales in mid to later stages. Filecash will inherit this proposal and slightly adjust the baseline parameters. Under the premise of keeping the lower limit of computing power and growth rate unchanged, the baseline release is reduced to 20%, superimposed on the base release of 10%, for a total of 30%, which is consistent with Filecoin.

A portion of 70% above the baseline will be retained and used for future data retrieval and as important economic base tokens for the PoS ecosystem operations.

➢ **Equilibrium Game Relationship Improvement**

The PoS implementation method proposed by Filecoin is Expected Consensus (EC), which selects the miners responsible for producing blocks through a method similar to throwing a dart. This is an innovative and excellent consensus mechanism that can ensure the fairness and stability of the entire system to a certain extent. But, the greater the proportion of a miner's storage of the total network storage, the greater the probability of being selected to be responsible for mining and producing blocks. When the network TPS is insufficient, big miners selfishly pack and produce blocks in the network, which will eventually lead to a shrinking network.

Filecash realized this problem and designed the BFT + PoS node and introduced two participants (nodes and currency holders) into the equilibrium game, forming at least a three-party equilibrium game and decentralizing the power of miners.

● **Miners:** obtain computing power by providing storage services, and select nodes

through computing power voting (weights are the same for large and small miners).

- **Nodes:** voted by miners, responsible for packaging messages and generating blocks, and obtaining a certain percentage of commissions.

- **Holders:** decide whether the block producer will receive block rewards.

In this equilibrium game, miners are no longer responsible for packing and producing blocks. Instead, nodes voted by miners are responsible for message packing and block production. The token holders will decide, according to the working conditions of the nodes, whether the node can get rewards. The equilibrium game of "miners voting to generate nodes and token holders deciding on whether to issue rewards" avoids the situation where big miners pack and produce blocks privately. Because the three parties are all stakeholders of the network, maintaining a stable operation and healthy development of the network is a shared interest of all three parties. Compared with the expected consensus of Filecoin, the power of miners has been weakened and the rights of token holders has increased. The introduction of nodes can better achieve fairness and community governance of the network.

➢ **Token Distribution**

Filecash's token is FIC, with a total supply of 2 billion, divided into 5 parts:

Filecash Foundation 2.5%: 6 years of linear release, 694,444 tokens in circulation every month, 16,666,667 tokens in circulation in the first year;
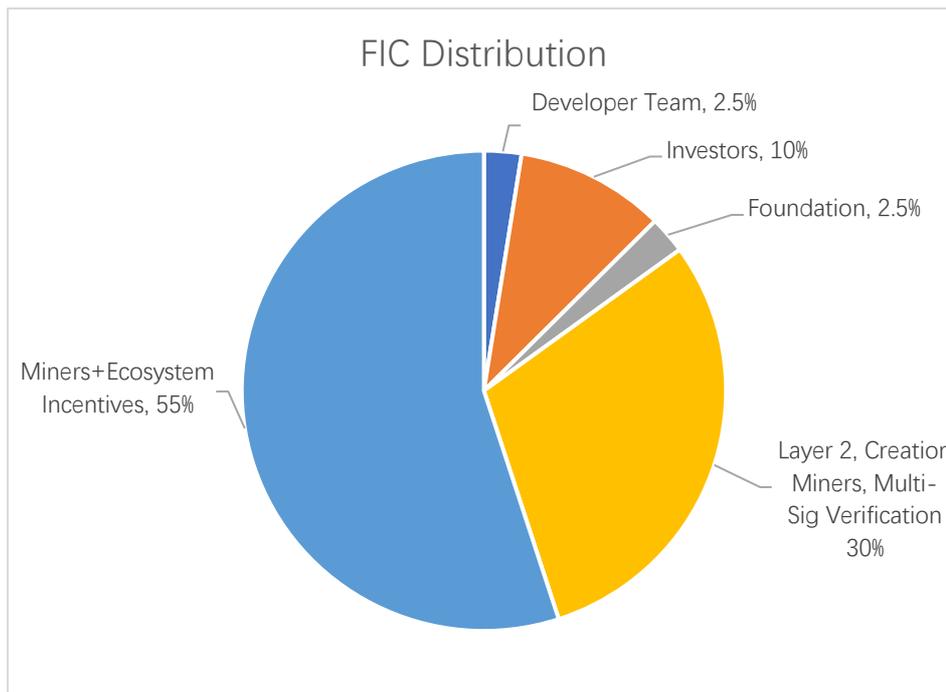
Development team 2.5%: The original Filecoin development team reserves 15% of the total supply. Since Filecash inherits most of the Filecoin's original code and reduces development work, the development team's reserved portion is reduced to 2.5%. This part will be released linearly in three years, with 1,388,889 tokens in circulation every month, and 8,333,333 tokens in circulation in the first year;

Investor 10%: The Filecash ecosystem needs to be jointly built by professional investment

institutions. The mining ecosystem needs incentives to support network startup in the early stage. SAFT sales of 10% and are consistent with the original Filecoin plans, and funds raised are used for project development. Linear release in two years, with a monthly circulation of 1,388,889, and 8,333,333 in the first year;

Layer 2, Genesis miners, and multi-signature verification accounted for 30%: Layer 2 reserves 595,999,900 tokens and the one-time release of 2.5 million tokens for the initial pledge during the staking-free period, where all excess will be destroyed. 1.5 million tokens are released to genesis miners to help them clear negative numbers after the network restarts, and the excess will be destroyed. 1 million tokens are released to manage private key multi-signature fees for multi-signature verification purposes;

Mining + Ecosystem Incentive 55%: Mining and the ecosystem are the main body of Filecash. This portion of tokens is directly structured on the blockchain and will be released to the entire network through mining and ecosystem incentives in a decentralized manner. Each Filecash participating entity has the opportunity to obtain some tokens. Linearly halved over six years. Based on the calculation that the entire network is below the baseline (2500P) of the computing power in the first quarter, 30% of the total released will be used as a reward for miners' output. The initial output is about 10W per day, and the actual daily output gradually decreases with the linear halving.

FIC Distribution

Developer Team, 2.5%

Investors, 10%

Foundation, 2.5%

Miners+Ecosystem
Incentives, 55%

Layer 2, Creation
Miners, Multi-
Sig Verification
30%

7. Ecosystem

➢ **Provide bottom-up ecosystem support**

The Filecash blockchain includes five core components: IPFS storage framework, PoS node mechanism, Layer2, cross-chain middleware, and oracle.

➢ **Leader of the Web 3.0 era**

Filecash believes that the Web 3.0 era and the internet ecosystems of the past still have a lot in common. In the current field of decentralized storage, Arweave is characterized by consistent data across the entire network. As long as there is still one node in the whole system, the data remains intact. On the other hand, Filecoin is characterized by unique data in the entire network, that is, once the storage node is lost, the data is lost.

Filecash meets the two designs in the middle and revises the scoring mechanism. The high-quality storage nodes hosted in IDC environments will get a high score and function as master nodes. The rest of the unused hash power of the entire network operate as backups for the master nodes. The current traditional IDC service architecture is the same - professional IDC

computer rooms provide high-quality core services while peer-to-peer hybrid networks provide supplementary network acceleration and backup. Filecash's architecture is similar to the infrastructure of current internet telecommunication facilities.

Through the optimizations and upgrades mentioned in this paper, Filecash will inherit the original ideals of IPFS and build a Web 3.0 storage ecosystem that everyone can participate in.