IPSE: The Traffic Portal for Next-generation Value Internet

IPSE Technical Paper

IPSE TEAM

Contents

1. Introduction

1.1 Background

The global distributed storage industry has gradually entered the stage of landing. Whether it is the Sia, Storj and other senior projects that have been testing the entire distributed storage in the past, or the Filecoin that is currently in the developing stage, or several those can't wait for the Filecoin mainnet launch then start their counter-type projects, most of which are public chains, such as Lambda, YottaChain and Filestorm. Regardless of their consensus mechanism difference, It is still an excellent step in building an open storage market. However, they have to face a very challenging problem, that is, whether users are willing to pay for the storage space first and let miners store the data for those distributed storage markets?

1.2 Summary

IPSE is a search engine based on IPFS, it implements the hash tagging of the file on IPFS network. The major mission of IPSE is to make the IPFS network transition from a state of few nodes difficult to use, to a state where nodes are widely available and easy to use.

IPSE provides a fast retrieval portal for stored content based on IPFS network, while establishing a reward mechanism for users to share data and storage space.

IPSE will use *PoST (Proof-of-Storage-True)* algorithm to ensure efficient storage and utilization of data. In the future, the IPSE mainnet will adopt the *DPoS* consensus mechanism of 21 SuperNodes to ensure the efficient operation and reliability of the consensus network.

IPSE will be the first distributed storage network to complete the life cycle of data: from the source of data, to the storage of data, to the retrieval of data, to the access of data, they will be processed and completed in the IPSE system. IPSE will be different from regular distributed storage public chain projects such as Filecoin. IPSE will not provide a distributed storage market, but through a distributed storage task distribution system.

With the help of IPFS-based underlying storage network, and graphene-based technology, a mature and efficient consensus network makes IPSE a search portal for value internet. Based on this portal, IPSE will build a DAPP matrix, including content payment, content reward, copyright protection, copyright prosperity, streaming portal, distributed advertising platform, etc.

1.3 Technical Components

IPSE mainly consists of the following technical components:

Consensus Network: The consensus network of IPSE consists of 21 SuperNodes and 100 alternative nodes, based on *DPoS* as the underlying consensus. The IPSE Consensus Network will assume all logic operations on the blockchain, including rewarding token for storage providers (Storage Miners), rewarding token for pledges, penalize pledges, blacklist maintenance, data source provider rewards, token collateral, penalize collateral.

While the underlying virtual machine of the entire consensus network supports Turing-complete and smart contracts deployment.

Storage network: IPSE's storage network is based on IPFS as the underlying infrastructure. Currently, it supports IPFS network. Of course, it does not exclude access to more underlying storage networks. On the IPSE system, the storage network is logically decoupled and completely different from the consensus network. The data retrieved by IPSE is compatible with different storage networks.

Task Distribution System: IPSE has a distributed task distribution system. This distribution platform not only has the distribution of data download tasks, but also the sharing of data download sources. IPSE will also consider the action of sharing as mining and rewards will be delivered. In short, the IPSE task distribution system will ensure that the data has both sources and whereabouts.

Node Client: IPSE will launch its own node client for the data access layer. If the underlying storage is not just the IPFS, but also other networks, the node client needs to integrate all these P2P networks. The client will optimize the lookup of Peer, making all Peers on the IPSE can join the seed list. In short, the user who downloads the IPSE node client can enjoy all the data on the IPSE network.

1.4 Process Brief Description

IPSE builds an index portal in distributed storage networks and aims to be the infrastructure for the next-generation value internet. POST is the native digital token of IPSE. SuperNodes in IPSE will shoulder multiple tasks, 21 SuperNodes and 100 alternative SuperNodes will be the verifier and maintainer for IPSE consensus network. There are two aspects of verification: one is data possession verification, and the other is data source authenticity verification. The security of the entire storage network needs to rely on the maintenance of the SuperNodes verification. The implementation is mainly through the penalty of the token reward in the contract. In addition, the entire data source needs to be docked from the open task distribution system. Whether the data source provider can download data and store, it requires a SuperNode to verify and maintain the network through the rules of penalize pledge & collateral.

- **Storage Mining:** The Storage Miner receives the task from the task distribution network, completes the download and stores the data on the IPFS network, submits the completed task to blockchain, and waits for the SuperNode to initiate the PDP challenge. After receiving a random challenge initiated by a SuperNode, the Storage Miner needs to response and compete the PDP. Once the SuperNode verified the PDP, the Storage Miner can get the reward.

- **Distributing Sharing Mining:** The task distribution node needs a large number of storage tasks to be distributed. Anyone who has this kind of storage task can share it with the task distribution node to get rewards. The data should be downloaded normally. But the data of the storage task can't infringe copyright, and illegal data is not allowed.

- **Retrieving and Accessing Data:** Retrieving data on IPSE is free. Accessing data is free. If you need to use the copyrighted content, you need to pay it with token before you can use it.

1.5 Terminology

- **SuperNode:** On the entire consensus network of IPSE, the SuperNodes are responsible for the creations of new blocks, and undertakes the work of two other core verifications. One is the *PDP(Proof-of-Data-Possesion)* verification, and the other is data source authenticity verification. The SuperNodes guarantee the efficient and stable operation of the entire IPSE consensus network, and the SuperNodes can't be fraudulent, because there are still 100 alternative nodes to participate in the candidate, the SuperNodes need to get enough voting support from the community to be elected.

- **StorageMiner:** A Storage Miner that provides storage space and receives storage tasks for the task distribution system, completes data download and storage process, and provides stable data access service as a node. Storage Miners are mainly rewarded by the amount and type of data stored. The tasks distributed by the task distribution system are random, the time of mining reward period is random, but it will be stable in the long term. Storage Miners are the most basic part of the IPSE ecosystem, and they are the infrastructure builders of the next decentralized value internet.

- **DataSourceMiner:** Data source miners are the nodes that can provide data resources that need to be responsible for. For example, data sources can't consist of privacy data and copyright content. Data source miners involved in mining also need to deposit collateral proportional to it. Once a Data source miner is reported and the action is confirmed, there will be no mining reward and collateral will be penalized. Data source miners are decent porters, they play a great role of the entire IPSE ecosystem. In the next decade of decentralized network development, they are responsible for the relocation of centralized internet data to decentralized networks.

- **PDPPD:** Partially authorized and provable possession mechanism is called *PDPPD(Provable-Data-Possession-Based-on-Partial Delegation)*.The task distribution node authorizes the agent to verify the data stored by the miner. This scheme is based on bilinear pairing and partial authorization technology. It supports the data owner to directly appoint the agent to perform data owner verification by key form, and the data owner can cancel or replace the agent at any time to prove the security of the solution. The main advantage of this solution is that it reduces the amount of calculation and traffic, and the application scenario is more extensive.

- **SuperNode-PDP:** IPSE uses a unique data integrity proof design based on the *PDP* of trusted SuperNodes and *PDPPD* scheme, IPSE will be distinguished from the regular distributed storage public chains, and will not be extremely convenient in terms of data integrity. This is designed with efficiency in mind, because the storage node should be used for data storage and distribution, rather than using most CPUs for data integrity. In order to ensure the basic security of the data, it is necessary to prove the data integrity which is based on the *PDP* and *POR* certification. The IPSE will use the parameters on the blockchain as random numbers, so that the SuperNodes assume the challenger role of the storage proof verification. The Storage Miners need to execute a predefined proof function to generate a *ProofSet* for multiple proofs, then submit it to the network, and then SuperNodes randomly pick and verify it.

- **Sector:** The sector is some disk space that a Storage Miner provides to the network. The Storage Miners' storage is divided in sectors, and then proves the data integrity in units of sectors. When the SuperNodes require a challenge to a certain sector, the Storage Miner needs to use this sector and send the data integrity proof, and the SuperNodes also need to verify it, and then these proofs and verifications are recorded on the blockchain.

- **DistributionNode:** The task distribution node is a unique concept of IPSE, and all data sources are randomly distributed through the task distribution node. All Storage Miners need to be registered to the task distribution node so that they have a corresponding probability of being distributed to the task. Any node can be registered as a task distribution node as long as it follows the IPSE task distribution criteria. Of course, task distribution has rewards and requires collateral.

- **DistributionSystem:** The task distribution system is composed of task distribution nodes. Each node distributes tasks according to the IPSE task distribution rules, and the entire system will be designed with new contracts. The IPSE Foundation will build a task distribution reward pool to encourage communities to build powerful task distribution nodes, allowing the entire the ecology of IPSE is more diverse. The task distribution system will be a system of rewards and penalties, and the upload task requires POST collateral. When the download task is completed by the storage node, the task uploader will receive a partial reward. If there is no dispute during the data source clarification period, the task uploader will receive all rewards and collateral. If the upload task can't be completed, or if there is a dispute during the clarification period, all the rewards and collateral will be loosed, once the case is loosed and confirmed by the *Data Source Valid Arbitrator*.

- **DataSourceClearPeriod:** During the data source clarification period, the task distribution node receives the uploaded data sources, and it takes some time to clarify the legality of its data sources. This legality includes data ownership, whether it will infringe on the copyright of others, whether it involves child pornography, terrorist violence, and so on. IPSE reasonably sets a data source with a clarification period of 1 year.

- **DataSourceValidArbitrator:** The Data source Valid arbitrators will assume the role of final ruling in the data source clarification period if there is a dispute (such as copyright complaints). As the arbitrator is powerful, it needs the deep involvement of IPSE stakeholders. The SuperNodes are the biggest stakeholders, and it is a good choice for each SuperNode to elect an arbiter.

- **ProofSet:** The *ProofSet*, the Storage Miner stores the proof in units of sectors, and then the *ProofSet* of all sectors will be posted on the blockchain, and then broadcast to all consensus nodes. and the SuperNodes complete the challenge verification by random selection. Storage Miner can win a block reward by successfully submitting the *PDP*.

- **PledgeRatio:** Storage Miners do not get all the token (POST) in the first time when they store the data, because there is a Token with a *PledgeRatio* scheme in the contract, the pledged tokens will be released to the Storage Miners in the next 5 years. This *PledgeRatio* will change dynamically, which is related to the credit rating of IPSE miners.

- **CreditDegree:** *CreditDegree* is very lowa in the early stage of mining. As time goes by, the miners can store data to mine accurately ane make the *CreditDegree* higher. In the task distribution system,higher miner's *CreditDegree* means more reward.

- **ChallengeJump:** The SuperNodes will ask the first challenge after the Storage Miner completes the storage.

However, in order to ensure the load balance of the entire system, it will not be challenged frequently. The challenge request correlate to the Storage Miner's *CreditDegree* and will be processed in different time periods based on hop time. The higher the Storage Miner's *CreditDegree* is, the longer the hop time is, the lower the challenge frequency is, otherwise the challenge request will be processed frequently.

- **SystemContracts:** The IPSE SystemContracts is a built-in contract, basically follows the EOS system will always be updated. Therefore, with the excellent public chain development of EOS, IPSE will also have an excellent consensus layer and draw on EOS's strongest community governance model and experience.

- **Wallet:** The IPSE Wallet is a wallet for digital currencies and assets. It is developed alongside the EOS wallet ecosystem. The EOS ecosystem will gradually become one of the most mainstream blockchain ecosystems, and the IPSE Wallet will also benefit from the diversification of this ecosystem. IPSE Wallet will be adaptable on many platforms, including mobile, desktop and server. IPSE is the traffic portal for the next generation of value internet, and the real value-bearing gate will be the IPSE Wallet which will be the ultimate in ease of use and compatibility.

2. The IPSE Starting Point

2.1 0 to 1

A valuable project must contain two parts. The first part is production, it means that the product is from 0 to 1. It requires the market reputation to make the competitive product. The second part is distribution, which means the competitive product needs a lower cost advantage in service of a sustained development. In-depth analysis of all these distributed storage projects, the economic model and technical characteristics determine its 1 to N distribution replication design will be a huge advantage. As long as it can be achieved from 0 to 1, there is no reason to suspect that they can't be the main storage option. But these projects have a fatal flaw, which is a question of *which came first: the chicken or the egg?*

There is storage cost to store the exponential growth of data. The distributed storage public chain project can easily build a storage market with transparent, fluctuating and reasonable prices. But is the data willing to be stored in the network? According to current market feedback, there may not be many people who are willing to pay to store. Why is this seemingly unreasonable situation? The logic is actually relatively clear. From the perspective of the project developers, they build a distributed storage market with low cost advantage, and they think users should and have to pay for data storage no matter what; from the perspective of data storage providers, they need to think more about the stability and profit. They will refuse to pay to store the data to the network that has not been absolutely tested. For them, the data storage costs are lower than the data distribution costs. Centralized storage is efficient but unsafe. The decentralized storage network, Filecoin, is a good choice. However, the clients have to spend fees(tokens) for retrieving data, which not only can't reduce costs but increase costs for large-scale use.

If we explore its nature to look at this problem, we can argue that data storage has strong service attributes. The clients do not care about the underlying storage hardware life, disaster recovery, data migration, hardware failure and other issues. They paid to store data and they only care about: The data must be secured and the cost should be reasonable and controllable. Data storage is a service industry, and efficiency is the first. But for the centralized storage network, they have to worry about data security issues as well as uncontrollable cost.

2.2 Fatal Inefficiency

Speaking of the distributed storage public chains, Filecoin is the most outstanding project with solid technology and the clearest development roadmap. But from a fundamental design perspective, Filecoin currently faces several challenges:

1.Does it cost a lot of CPU to achieve *PoRep* calculations, does the cost advantage over centralized storage still exist?

2.Whether a large number of matching orders and deals can be completed efficiently in the *DSN (Distributed Storage Network)* market?

3.Can data retrieval be efficient and free?

4.Can the storage nodes (Storage Miners) provide effective storage space without static public *IP*?

In terms of efficiency, the current distributed storage networks need to solve some technical difficulties more or less by observing further.

If each storage node uses a very high-performance CPU that still can't meet the *PoRep* calculations, it means that a more expensive GPU is needed to solve this problem. Although this can be achieved, the cost far exceeds the controllable degree. In contrast, centralizing storage node is relatively simple and easy. If a large number of orders and deals can't be completed in the decentralized matching market, then the market will be difficult to succeed due to cost problems, and at the same time, it is difficult to develop and build the Dapp based on the distributed system. Because the high efficiency advantage no longer exists. If the retrieval of data is not as efficient and near free as a centralized storage service, then the distributed storage market is difficult to have advantages. If the distributed storage node also needs a static public ip, it is neither the network be distributed nor low cost compared to centralized storage.

2.3 PoST(Proof of Storage True)

IPSE's token is *POST* (the name itself is an abbreviation for the IPSE consensus). The IPSE consensus is *Proof-of-Storage-True (PoST)*. It corresponds to the meaning of "Discard the false and retain the true". Which means real Storage Miners, real storage activity, real and valuable data.

Which came first: the chicken or the egg? When most projects are still going after the chicken and egg debate while exploring for chicken first (distributed storage network with low cost advantages) or egg first (data that can be efficiently stored on the network). It is difficult to find a way out when they are on the way of 0 to 1.

IPSE has made another exploration, first of all, it allows nodes storing massive amounts of data in a distributed storage network, instead of letting a large amount of space empty. If there is no data to store, it is silly to spend almost all CPUs to do the proof calculations that just to prove that the storage space is still empty and then everyone to participate in the speculation in the coins, and no one cares whether those distributed storage space is really efficient use. IPSE is different. The truthfulness of the IPSE consensus is that all nodes actually let the data be stored, and it needs to prove that the storage is real and effective.

3. IPSE Consensus

3.1 Reward Formulas

IPSE allows the data actually stored in a distributed network. The storage providers can get rewards within the rules. There are three dimensions to consider: data size, data category and the number of data copies.

We define the data size as s, the data category is $c \in C$, and the number of data copies is n, then the calculation power w is calculated as:

$$w = s * c * 1/n$$

The amount of miners' token rewards is defined as t, which is also related to the last day's total network power TW, as well as the full amount of token release of each day TT.

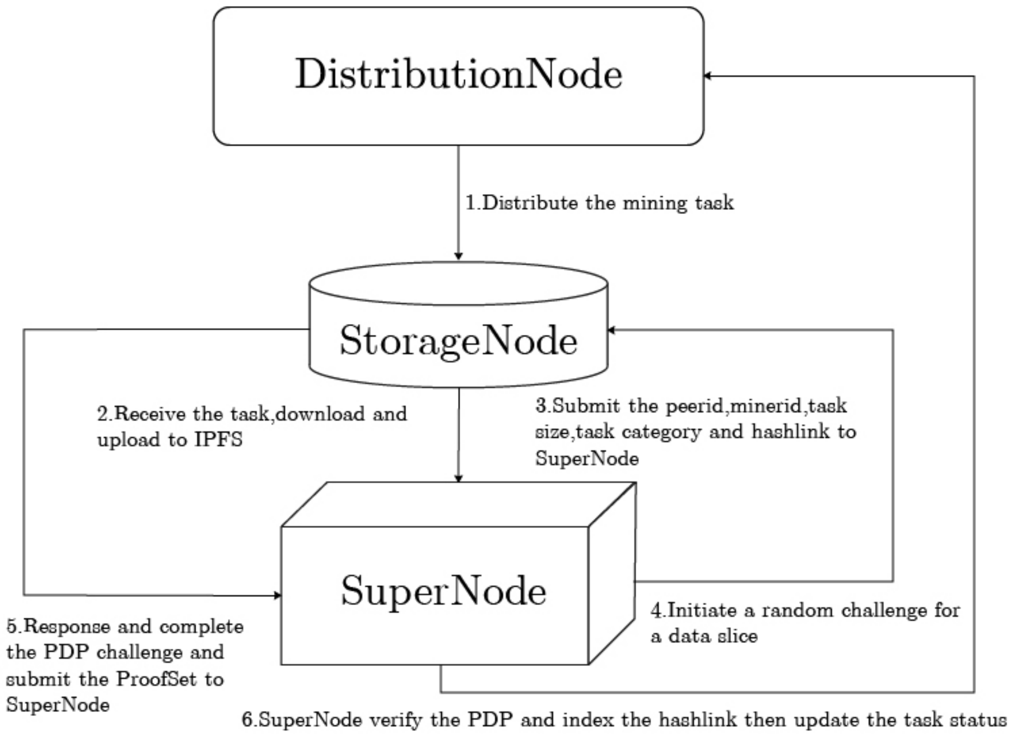
The calculation formula of the miners' mining output (the amount of token) is as follows:

$$t = w / TW * TT$$

Swing Attacks

Assume that a lot of miners joined forces and passively mined on the first day, resulting in a very large reduction in the total network power. The next day, they start to mine actively, which led to a very high token output on the second day. This phenomenon is called Swing Attacks. IPSE uses two mechanisms to deal with Swing Attacks: The first one is to set a threshold value to the decrease of the total network power. (The miners can make the network's computing power drop a lot, but the computing power is not infinitely reduced due to the limit, when it drops to a certain level, it can no longer decrease.) The second is to set the total output stability mechanism of the day (when the total power of the day exceeds yesterday', it will lead to a rapid decline in the total token output of the current day). These two mechanisms will prevent miners from Swinging Attacks, basically ensuring that the total amount of tokens per day remains stable.

3.2 Consensus Process



The basic steps of the IPSE Consensus algorithm are as follows:

1) The task distribution node randomly extracts tasks from the task database and randomly issues them to the registered Storage Miner. The *taskid* is the ID of the task.

2) After the Storage Miner receives the task, then upload the downloaded data to the IPFS network through the local IPFS node,and transmit it to the IPSE *hashlink*.

3) After completing the download and upload tasks, you need to report the mining results to the SuperNodes, including *hashlink, minerid, taskid, size, category* and other parameters.

4) After the SuperNode receive the successful mining result, the result will be posted on the blockchain.and another SuperNode randomly selects a data slice to initiate the *PDP* challenge. Additional SuperNodes also begin random verification. When one of the SuperNodes initiates a challenge, the other SuperNodes will no longer initiate the same challenge. which can effectively prevent the SuperNodes and miners from colluding and cheating.

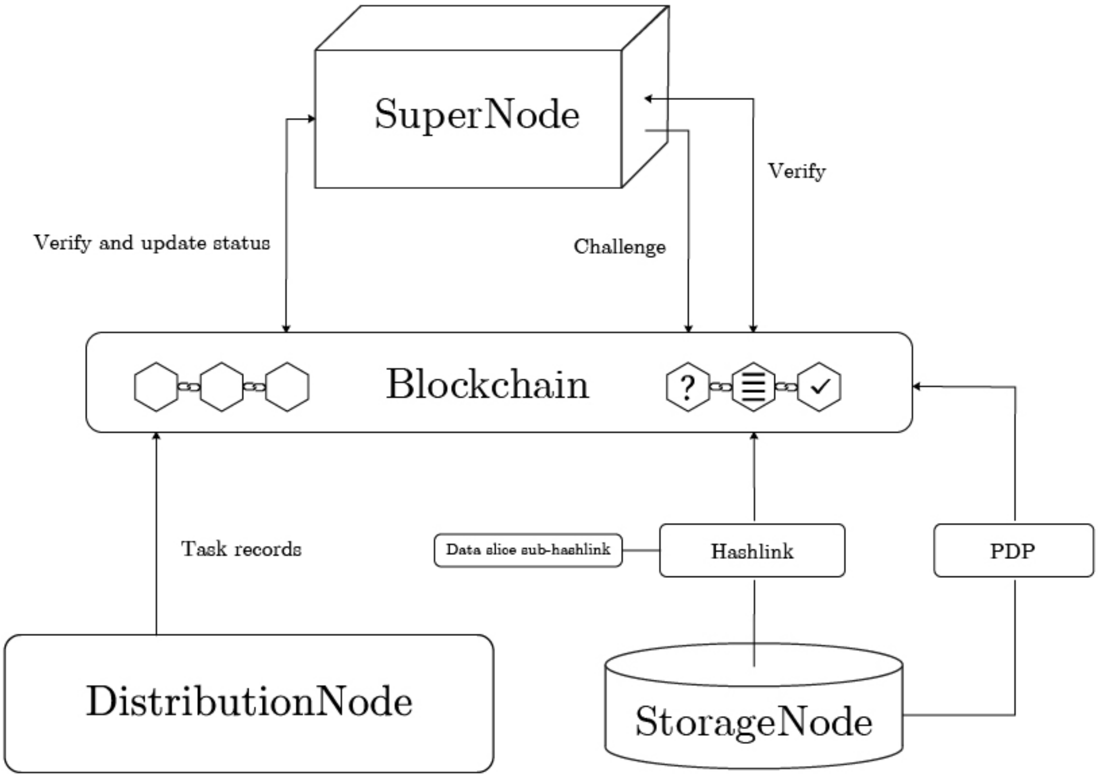
5) The Storage Miner needs to provide the *PDP* for the sectors involved in these data slices and submit the *ProofSet* to the SuperNode.

6) The SuperNode verifies the *PDP*. If they pass the verification, the Storage Miner will be rewarded and the final reward result will be synchronized to the consensus network. Then index the *hashlink* and update the status of the delivered task.

Note:① If the Storage Miner can't download the task and submit a result to the SuperNode, the

SuperNode will verify the validity of the delivery task, what will happen? This will be detailed in the next chapter. ② If the Storage Miner is unable to complete the *PDP* challenge, or if the SuperNode verifies that its *PDP* can't pass, what kind of punishment the Storage Miner will face? This will be detailed in the next chapter as well.

3.3 PDP(Provable Data Possession)



Depending on the role of the inspection in the agreement, the *PDP* is divided into two basic types: one is private (private verifiability), only the data owner can check the data on the server; the other is public (multiple of public verifiability), any competent authority can perform inspection procedures. IPSE data ownership is described in detail in the chapter of task distribution system. The task distribution node has ownership of the data. It is reasonable for the task distribution node to check the data possession, but the task distribution node in the IPSE system can entrust the SuperNodes to check the data possession.

1)The task distribution node will inject a tag for each task, and each task will have its own *taskid*, which is the unique identifier of the task. And the task distribution node will also add its own signature, so that no other task distribution nodes can pretend to distribute the tasks with Sybil Attacks.

2) The SuperNode will send a challenge about a data slice of *sub-hashlink* of the *hashlink* to the Storage Miner, which may involve one *sub-hashlink* sector or multiple sectors, this challenge contains the random number obtained by the SuperNode from the previous block.

3) The Storage Miner calculates and generates a new proof based on the block challenged, tag information,

challenge information, and a random number generated by itself.

4) The SuperNode uses the predefined verification function to check whether the Storage Miner actually stores the data based on the parameters: challenge, proof and user public key.

The formal definition of *PDP* is as follows:

SuperNode	**StorageMiner**
1. Receive the mining record, get the tags Σ, verify DistributionNode's and StorageMiner's signature,and quit if fail;	2. Receive the DistributionNode's task and download the data, then chunk data and upload it to IPFS. Block(sk , pk , sub-hashlinks) -> (Σ) sk is the private key of StorageMiner and pk is the public key of StorageMiner submit mining record to SuperNode
3. generate a random challenge chal = { (i , sub-hashlink) } i ∈ **I** submit chal to blockchain and signature for it	4. get StorageMiner's chal and generate the proof GenProof (sub-hashlink , chal , Σ) -> **P** submit the proofSet to blockchain and signature for it
5. SuperNode verify the signature and check the proof CheckProof (sk , chal , **P**) -> ("success" , "failure") sk is the public key of SuperNode	

4. Consensus Security

4.1 Safety and Efficiency Trade-offs

IPSE's storage consensus mechanism is *PoST (Proof-of-Storage-True)*. The most notable and distinctive feature is: efficiency first. Most of the data is stored on disk for data access, especially for hot data. IPSE indexes data that can be quickly retrieved and accessed by users. It is no doubt that IPSE can save the hottest data on IPFS, and relying on a powerful search engine. IPSE will also be able to grasp the hotspots of data on IPFS.

Efficiency for IPSE is that data can be accessed quickly, and security for IPSE is that data is accessed under specific mechanisms. Because IPSE is not a distributed storage public chain, there is no guarantee that data will be eternally securely stored on distributed storage nodes for contractual terms. So how does IPSE keep the data secured?

- 1.Data is stored with multiple copies and distributed in multiple nodes. IPSE's task distribution mechanism determines that data is not stored in a single node. IPSE's storage cost is sufficient to support multiple copies of data and will be distributed across different nodes.

- 2.The data retention period will be synchronized with the hardware life of the machine. IPSE assumes that the hardware life is about 5 years, and the data life cycle will be about 5 years. Five years later, when the data is gradually lost as the machine is eliminated, IPSE will be able to redistribute these old tasks.

- 3.IPSE requires Storage Miners to provide the *PDP* for the challenged data slices. Although it is also a priority principle of efficiency, only randomly selected will be challenged. Nevertheless, the best strategy for Storage Miner is to completely store the data and not delete the data.

4.2 Rewards and Penalties

4.2.1 Real Storage Rewards

The mining reward of IPSE is divided into two parts. The core part is the reward of real storage data. This part of the reward is different from the distributed storage public chain. It does not require the miner to pre-collateralize (deposit collateral before store data) , but only the part of the output token pledged into the contract and then gradually released to the user in the next 5 years. This involves the issue of the pledge ratio. Since IPSE is a decentralized system, there is no authority can guarantee the credibility of miners. IPSE defines a new concept of credibility called *CreditDegree (Cd)*, which is calculated as follows:

$$cd = stable\ access\ days\ /\ 1825$$

The number of stable access days: From the first day of accessing the IPSE, if there is no data loss on the day and the *PDP* is verified, then the stable access days will be increased by 1.

The calculation formula of the *PledgeRatio* is as follows:

$$pr = \begin{cases} P_0 - cd \\ 0\ (pr < 0) \end{cases}$$

The Token pledged in the contract will be released linearly to the Storage Miners in the next five years, releasing 20% of the total tokens pledge each year. As the Storage Miners stabilize mining, ensuring that the machine runs stably without shutdown, the *CreditDegree* will accumulate and the proportion of pledged token will be gradually reduced, and the token reward will be more.

4.2.2 Distribute Task Rewards

Another part of the IPSE reward is the reward for the task distribution node, which also rewards the upload data source. IPSE will give different weights to different data source node. The calculation method is the same as power calculation. Any task distribution node will declare the task information before distributing it, including the category and size of the data source. When the Storage Miner completes the task, as long as the category and the actual size are not much different from the declared size and the data source passes through the clarification period and there is no dispute, then the data source is legal. When the task distribution node declares a task, it needs to pledge the token first. This is to prevent a large number of spamming tasks.

4.2.3 Storage Miner punishment

Storage Miners face penalties if they failed to complete the *PDP* challenge. There are various situations in which a Storage Miner can't complete a *PDP* challenge, such as deleting data, shutdown, network disconnection, disk corruption, etc. The strength of the penalty is directly related to the collateral. The formula for calculating the penalized token ratio is as follows:

$$slashratio = \rho * n * (1 - cd)$$

- ρ is the initial parameter of the system.
- n is the number of times about PDP fails.
- cd is the $CreditDgree$ for Storage Miners.

The punishment is not only limited to deducting the collateral token of the Storage Miner, but also reduces the $CreditDgree$ of the Storage Miner. The number of $CreditDgree$ and PDP fails has the following relationship:

$$cd' = cd - \alpha * n$$

- α is the initial parameter of the system.

4.2.4 Task Distribution Node Penalty

The task delivered by the task distribution node affects the operation of the entire IPSE system, and whether the task is legal or not is not intermediate. In the case of the that data source can't be downloaded or if there is a dispute during the clarification period and the case is lost, all rewards and collateral will be directly penalized. If the task distribution node issues a spamming task, it will not get rewards and face other losses.

4.3 Perfect Combination

Like a saying says, borrow talent from abroad to develop the nation effectively. IPSE is perfectly compatible with distributed storage public chains such as Filecoin. The distributed storage public chain is to build a decentralized storage market, and then let the decentralized storage node ensure data storage securely. IPSE is to distribute storage as much as possible. The data can be retrieved. The two networks can work together. If the data on a distributed storage public chain is authorized by the data owner and is willing to index the data into the IPSE ecosystem, and the replication proof itself is completed in a similar way to Filecoin($PoRp$), then IPSE can learn from the talent and contribute to it. After the indexing of the data, a partial token reward can be given.

IPSE data sources can be diversified, either as task distribution nodes to porters, and to transfer data from traditional centralized networks to decentralized & distributed networks (the value internet). At the same time, data that exists from the beginning of distributed networks can also be indexed into IPSE and ensure the token reward.

5. Road Map

5.1 The 1st Phase: Deploy Smart Contracts and Start Mining

High-efficiency mining of central nodes: Build and deploy the smart contract on the EOS blockchain and start mining. Deploy the entire storage contribution reward mechanism, collateral mechanism and penalty mechanism to the EOS through the contract. The central node verifies the authenticity of the storage and verifies the legitimacy of Storage Miners. To prevent attacks, the central node authorizes Storage Miners to mine.

This phase has been achieved from 2018.07 to 2019.05.

5.2 The 2nd Phase: Distribution Task Mining

Deploy new contract on the EOS blockchain, allowing the central node achieve rewards with task distribution. Deploy the entire reward mechanism, collateral mechanism and penalty mechanism to the EOS through the contract, and the trusted central node verifies task legality.

Research and development have begun from 2019.06 to 2019.09

5.3 The 3rd Phase: Sidechain Launch

Launch the Sidechain based on the EOS and the underlying code needs to be rewritten to implement the SuperNode to randomly initiate and verify the *PDP* challenge. At this phase, the Storage Miner needs to provide the real *PDP* that will be on blockchain. The SuperNode acts as a TPA (Third Party Auditor). Once the SuperNode verified the *PDP* from the miner, then can ask the smart contract to send rewards to miner. The mining node access will be open, and the Storage Miner *CreditDegree* mechanism will begin to work.

This phase will be developed and tested from 2019.10 to 2020.03. But this phase will not affect the operation of IPSE on the EOS mainnet. Once the side chain is successfully launched, the original token (collateral included) on EOS mainnet will be mapped to the Sidechain one by one.

5.4 The 4th Phase: Distributed Task Distribution

Distributed task distribution: Centralized task distribution turns to distributed task distribution. IPSE will build a complete task delivery standard. The primary consideration is that the task distribution node and the Storage Miner collude and deliver the task to specific one. The task distribution reward, collateral, penalty mechanism and contracts need to be migrated to the Sidechain. The distributed task distribution structure is completed, and the source of the data will be completely solved. Relying on community governance, data sources are motivated, data storage and distribution are motivated, data access is free, data copyright is protected, and data copyright prosperity plan motivated as well.

This phase will be achieved between 2020.04 and 2020.08.