



SFIS White Paper



Summary

SFIS is an organic combination of existing mature technologies, upgraded based on IPFS technology, which provides a distributed and efficient record of the ledger and provides comprehensive scripts to support different business logic. In a typical blockchain system, data is generated and stored in blocks, and is linked into a chain data structure in chronological order. All nodes participate in data validation, storage, and maintenance of the blockchain system. The creation of new blocks usually requires the confirmation of the majority of the whole network (the number depends on different consensus mechanisms), and broadcasts to each node to achieve network-wide synchronization, which cannot be changed or deleted afterwards. The parties here only refer to the accounting participants. The SFIS encryption system participants should be composed of multiple entities with inconsistent interests, and the accounting will be initiated by different participants in different billing cycles. Depending on the different consensus mechanisms, other participants will jointly verify the accounting information initiated by the leader.

Contents

Chapter One Industry Status	04
一、 Market background	04
二、 Industry analysis	07
Chapter Two SFIS advantage	09
一、 Functional advantage	10
二、 Performance advantage	13
Chapter Third Technology Architecture....	19
一、 Underlying platform.....	19
二、 User Management.....	24
三、 Smart contract.....	28
Chapter Four Algorithm and network design.....	29
Chapter Five Credit endorsement.....	51
Chapter SixToken introduction.....	54
Chapter VII team introduction.....	57
Chapter Eight Risk warning and disclaimer.....	60

Chapter 1 Industry Status

— . Market background

2018 is the first year of blockchain technology explosion, most people in the industry focus on the cryptocurrency, but the blockchain technology itself is also worthy of attention. The blockchain builds a democratic trust and verification protocol that has overturned the traditional banking model and is having an impact on areas such as healthcare, wealth management, and social applications. However, from a technical perspective, the blockchain is not without pain points. The current PoW (Proof of work) consensus mechanism makes transaction processing so slow that it becomes almost useless in certain situations. For example, the smashing cat that was all the rage was once paralyzed by the entire Ethereum network.

From the current state of the blockchain, storing large amounts of data on the chain is not a good choice. The current background blockchain can only process a small number of characters and texts, and record the payment situation. How can we store large files or pictures directly on the chain? Blockchain can only be limited to recording such small amounts of micro data?

In view of the status quo, the industry introduces IPFS, which is called Interplanet File System. Chinese can be called Star File System and is developed by Protocol Labs. It is currently the most promising solution to solve this problem. IPFS is a peer-to-peer transport protocol where each node stores a series of files indexed by hash. When a client needs to access these files, it only needs to pass the hash value of the file through an ingeniously wrapped abstraction layer. IPFS will use this hash value to find the corresponding file from the active node and return the file content to the client. This approach makes us access data faster, safer, and more open.

The reason why IPFS is so worthy of attention is that it is different from the traditional HTTP protocol and other centralized storage methods. IPFS implements

true distributed storage, which will become the data storage foundation for all blockchain projects in the future, providing strong support for the development of the entire blockchain industry. Therefore, the development space of the IPFS protocol has great potential, and it is likely to gradually become the mainstream data storage method in the future, and build a new era of faster, safer and more free Internet.

IPFS, like all blockchain technologies, is based on P2P and forms a peer-to-peer transmission network. People can more easily connect together to form a global network. There is no central node in this network, and the resources you need may be in your neighbors or on the other side of the globe. The resources stored in the IPFS may be scattered around the world, and more likely to be concentrated in a hot spot depending on the popularity of the resources. Hotspot resources will be easier to access and faster to access. In the near future, the IPFS protocol is likely to completely replace the traditional HTTP protocol.

If the blockchain is a reshaping of traditional Internet technologies, then IPFS is a reshaping of the traditional HTTP transport protocol.

In fact, IPFS is not perfect in its application. Anyone who gets this hash value can easily download it from IPFS. For files with sensitive information, it is not suitable for direct sharing. Based on this security vulnerability, we introduced SFIS - equivalent to version 2.0 of IPFS. When we need to share some sensitive files on SFIS, we need to do some processing on these files in advance.

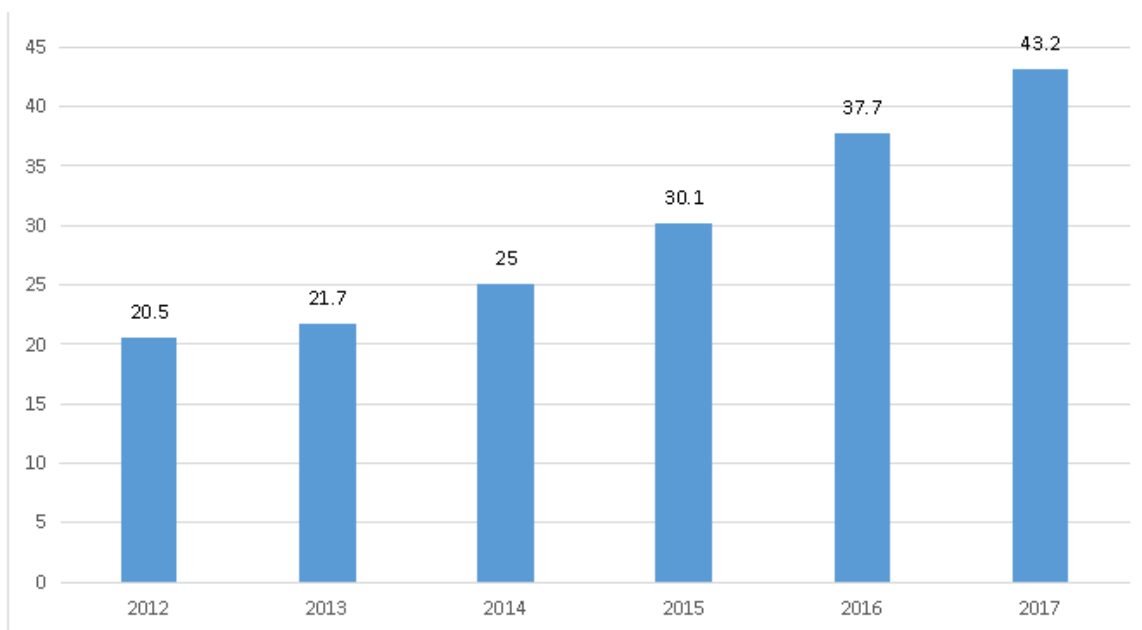
二、 Industry analysis

The continuous improvement of the network has made the problem of idle network resources more serious. Whether it is measured from the daily demand of the network speed or the length of the network, a serious waste of resources can be drawn: 90% of the bandwidth is idle.

As of June 2017, the total number of Internet users reached 3.89 billion, with a penetration rate of 51.7%, while 3.89 billion netizens had an average of 43.2 hours per week, which is equivalent to 3.89 hours of Internet access per day and 20.11 hours of idle time per day.

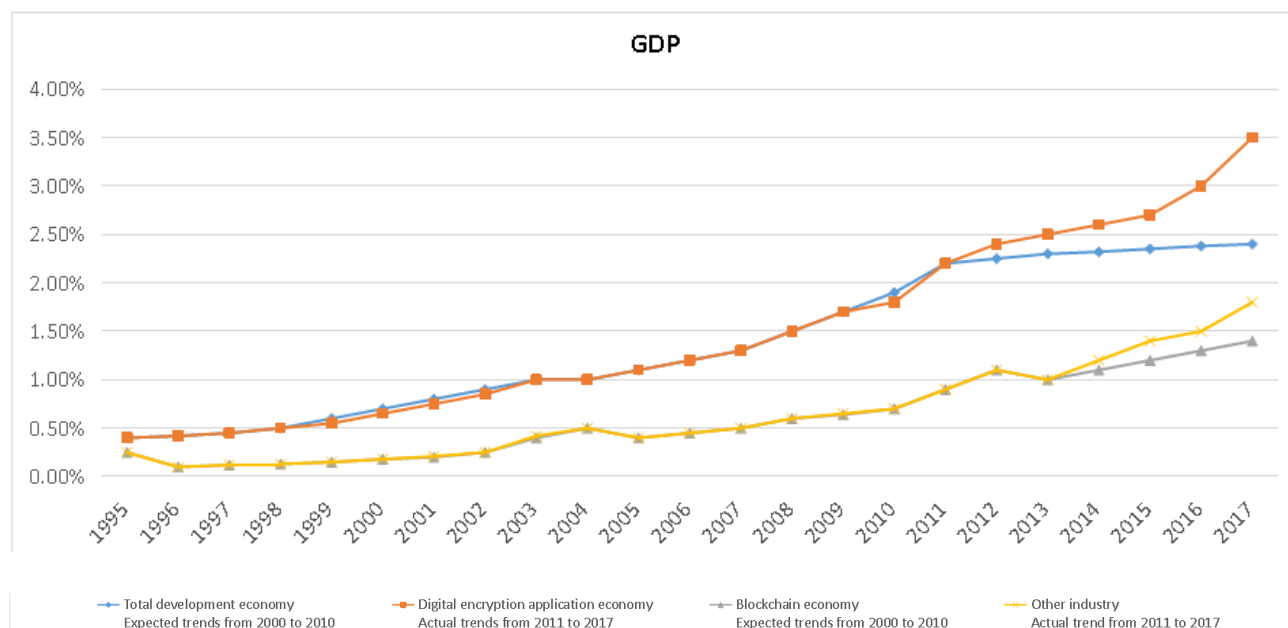
Average Internet time per week for global netizens

Driven by technology and price, the global cloud computing market continues to



grow. According to Gartner, the cloud computing market, including IaaS, PaaS, SaaS, process services, and advertising marketing, was \$219.6 billion in 2016. By 2020, the overall size is expected to reach \$411.4 billion, a compound growth from 2016 to 2020. The rate is 17%.

Percentage of GDP



Chapter II Advantages of SFIS

In IPFS transmission, data still has security risks. This simple, centralized decentralized storage transfer method minimizes the cost of publishing information, but at the same time it creates an innate lack of selectivity. For example, anyone who gets this hash value can easily Download it on IPFS. For files with sensitive information, it is not suitable for direct sharing.

In SFIS, we have used a lot of technical results of blockchain. It mainly includes: hash algorithm, symmetric encryption, asymmetric encryption, digital signature, digital certificate, homomorphic encryption, zero-knowledge proof and so on.

This chapter briefly introduces the application of security and cryptography techniques in blockchains from the perspectives of security integrity, confidentiality, and identity authentication.

一、 the functional advantages

1. Integrity (tamper proof)

The blockchain uses cryptographic hash algorithm technology to ensure that the integrity of the blockchain account is not destroyed. The hash (hash) algorithm can map binary data into a string of short strings and has input-sensitive features. Once the input binary data is slightly falsified, the hashed string will occur very much. big change. In addition, the excellent hash algorithm also has a collision avoidance feature, inputting different binary data, and the obtained hash result string is different.

The blockchain utilizes the input sensitivity and collision avoidance characteristics of the hash algorithm. Within each block, a hash value containing the previous block is generated, and the Merkle root hash value of the verified transaction is generated within the block. Once some blocks in the entire blockchain have been tampered with, the same hash value as before the tampering can not be obtained, so that when the blockchain is tampered with, it can be quickly identified, and finally the integrity of the blockchain (tamper-proof) is guaranteed. .

2. Confidentiality

The encryption and decryption technology is divided into two categories from the technical composition: one is symmetric encryption and the other is asymmetric encryption. Symmetric encryption encryption and decryption keys are the same; non-symmetric encryption encryption and decryption keys are different, one is called public key, and the other is called private key. Public key encrypted data, only the corresponding private key can be unlocked, and vice versa.

The blockchain, especially the alliance chain, requires TLS (Transport Layer Security) encryption communication technology to ensure the security of the transmitted data during the whole network transmission process. The TLS encrypted communication is the perfect combination of asymmetric encryption technology and symmetric encryption technology: the two sides use the asymmetric encryption technology to negotiate and generate the symmetric key, and then use the generated

symmetric key as the working key to complete the data encryption and decryption. The technology comprehensively applies the advantage that asymmetric encryption does not require the shared key of both parties, and the symmetric encryption operation is fast.

2. Authentication

Simple TLS encrypted communication can only guarantee the confidentiality and integrity of the data transmission process, but it cannot guarantee the trusted end of the communication peer (man-in-the-middle attack). Therefore, we introduce a digital certificate mechanism to verify the identity of the peer end of the communication, and thus ensure the correctness of the peer public key. This process is a digital certificate, which is issued by an authority. The side of the communication holds the authority public key, which is used to verify whether the communication peer certificate is trusted by itself (that is, whether the certificate is issued by itself), and confirms the identity of the peer according to the content of the certificate. In the case of confirming the identity of the peer, the public key in the peer certificate is taken out to complete the asymmetric encryption process.

In addition, the latest research results of modern cryptography are applied in the blockchain, including homomorphic encryption and zero-knowledge proof. In the case of a blockchain distributed ledger disclosure, it maximizes privacy protection. The application of this technology can be continuously developed and improved.

Blockchain security is a systems engineering. System configuration and user permissions, component security, user interface, network intrusion detection, and anti-attack capabilities all affect the security and reliability of the final blockchain system. In the actual construction process, the blockchain system must reach a reasonable balance in the dimensions of security, system construction cost and ease of use, on the premise of satisfying user requirements.

二. Performance advantage

1. Rich experience in high concurrent processing

SFIS's existing system handles more than 200,000 concurrent transactions per second. SFIS draws on FiT's high-concurrency, distributed account management experience, and supports tens of thousands of processing per second through various model analysis and compression tests.

2. Efficient adaptive consensus algorithm

In enterprise blockchain solutions, the ability to handle concurrent blocks of a single blockchain is primarily governed by consensus algorithms. In the actual alliance chain application, the network status between nodes is good for most of the time, and the probability of node failure or Byzantine node is small. Most of the time, you only need to solve the data consistency of multiple nodes and complete the transaction efficiently. When it is found that there is a node failure or fraud, it can automatically switch to a Byzantine fault-tolerant algorithm to ensure the smooth running of the business. The adaptive blockchain consensus algorithm provided by SFIS is highly efficient in the case of good network conditions, no node failure or fraud, and can accurately detect node failure or node fraud. When a node failure or fraud is detected, the system automatically enables Byzantine fault-tolerant algorithm feature, in a network with a total number of nodes of $3f+1$ (where f is the number of Byzantine error nodes), when the fault-tolerant node does not exceed f , the system normally provides external services; when all bad nodes are repaired or Byzantium After the fault-tolerant node is solved, when all the nodes have the same data, they automatically switch back to the efficient algorithm. The advantage of the adaptive algorithm is to ensure that the alliance chain can process concurrently and efficiently for most of the time, and accurately handle the problem of node errors.

3. Mass storage

SFIS supports multiple ways of local database storage, file system storage, and cloud storage. Local storage implements hot and cold separation, database storage uses a sub-database partitioning model, and cloud storage supports expansion according to cloud clustering rules.

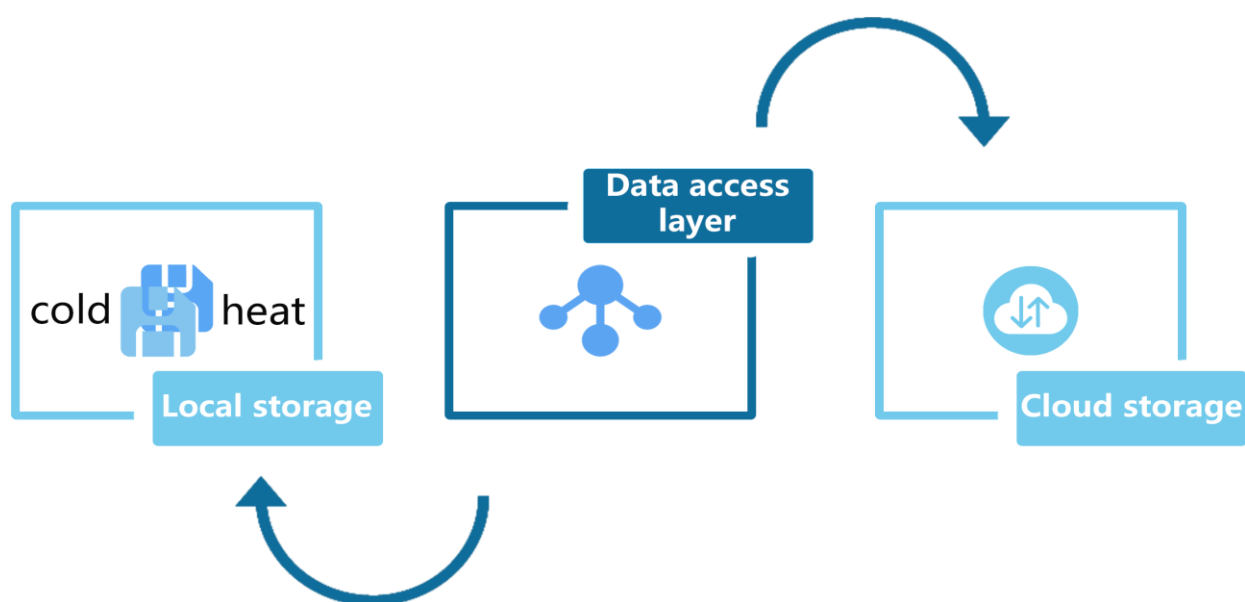
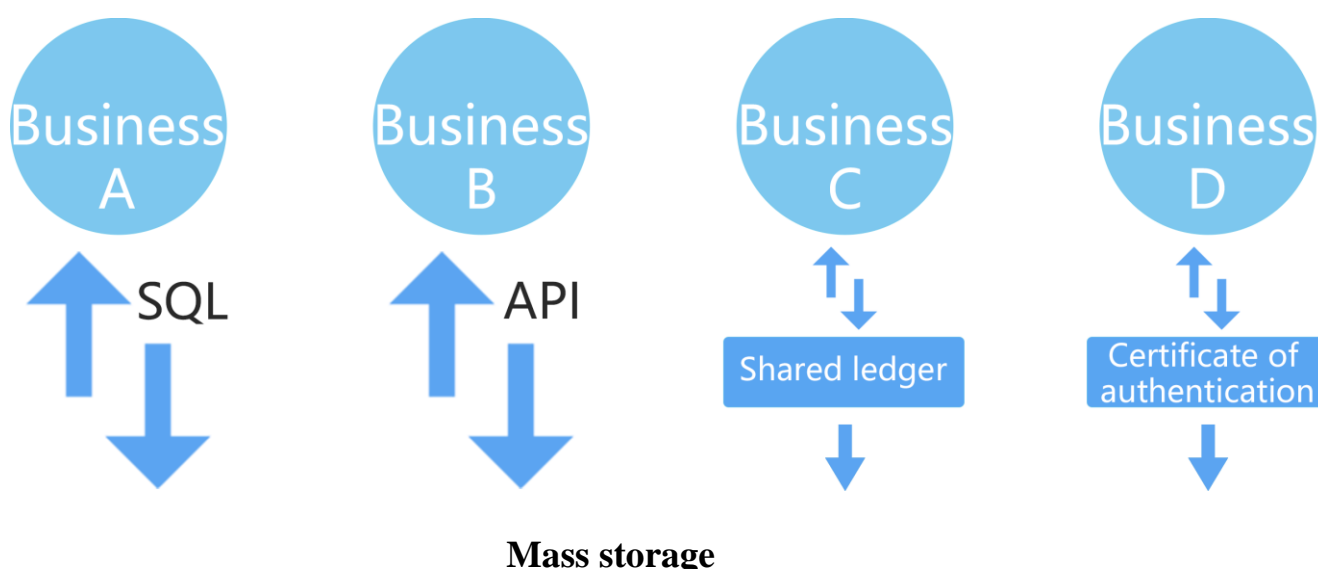


Figure 4-4-1-4 Mass storage

3. Access in a way that satisfies multiple user habits

The SFIS platform product layer (Trust Platform) provides a rich application development framework. The application types include basic application models such as digital assets, shared ledgers, forensic certificates, share crowdfunding and ownership transactions. Users can develop their business based on these application development frameworks, or they can develop directly based on the SQL and API provided by SFIS underlying Trust SQL. It provides multi-language support for the library of the underlying API used in business development, which can meet the development habits of different users and reduce the difficulty of user access.



4. Optional key management docking mechanism

SFIS provides the original key system association, partial trust and full trust three types of docking mechanism. When connecting with the existing system, the appropriate docking mechanism can be selected according to the actual situation of the key management system of the existing system. If the original key system is highly secure, it can be reused directly using the original key association method; the new service can choose the key management full trust mode; or the partial trust mode can be selected according to the business situation.

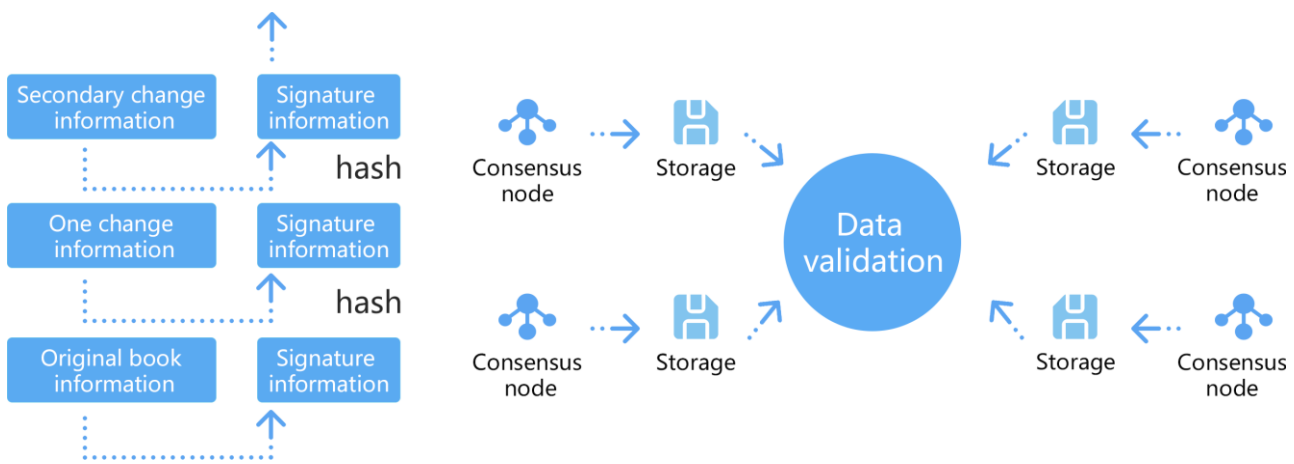
5. Reliable and consistent record storage

SFIS is to ensure that the service request cannot be tampered with during the transmission process through the asymmetrically encrypted digital signature, and the other is to ensure that the data of each node is consistently stored through the consensus mechanism. The data records already stored are guaranteed by the self-checking and quasi-real-time multi-node data check in the node to ensure that the stored data records cannot be modified.

Self-checking of nodes: SFIS uses a blockchain structure to store data records. The modification of some records destroys the integrity of the blockchain structure and can be quickly verified and restored from other nodes. In addition, each

accounting node of SFIS has its own private key. Each block header contains the signature of the private key of the node, and the modification of the data in the block can be verified by signature. Multi-node quasi-real-time data verification: When the private key of the node is stolen, the malicious user is present on the modified ledger chain.

For all data possibilities, SFIS provides a quasi-real-time data comparison mechanism between multiple nodes, which can timely detect the tampering of a node's book data.



6. User privacy

User information and blockchain addresses in SFIS are isolated. From the record storage of each node, the associated user information cannot be obtained. User information storage has multiple layers of protection such as access control, access authentication, and encrypted storage.

7. Secure key management system

In the SFIS key management solution, the key safe and user account delegation functions are provided to ensure the security of the key. The key safe uses the user information to encrypt and divide the key and store it on multiple different nodes. Under the normal business process, the key safe is not accessed. When the user key is lost, the key can be found after the user information is authenticated. Back. The account entrustment is to realize the account retrieving function by entrusting the

account to operate the entrusted account. All SFIS entrusted account operations are independently recorded on the blockchain, and there are strict frequency restrictions and independent risk control on the operation of the entrusted account. The strategy can strictly control the operational risk of the entrusted account.

Chapter III SFIS Technology Architecture

—. SFIS underlying platform

1 User Management:

Responsible for the identity information management of all SFIS participants, including maintaining public and private key generation, key storage management, and maintaining the user's true identity and blockchain address correspondence, and supervising and auditing certain real identities under authorization. For the application of financial transactions such as digital assets, the rules of risk control are configured to ensure the security of system transactions.

2 Basic services:

The base service is deployed on all nodes to verify the validity of the transfer request and to record the valid request and record it on the storage. For a new transmission request, the basic service first analyzes the interface adaptation, authenticates the transaction, and after signing and encrypting the transaction or contract through the consensus algorithm, it is completely and consistently stored on the shared ledger. In the self-adaptation mechanism, the consensus mechanism has high concurrency under normal conditions of both the network and the node, and is highly fault-tolerant in the case of network anomaly or node spoofing.

3 SFIS application service layer:

SFIS provides the basic capabilities and implementation framework for typical applications. Based on these basic capabilities, users can superimpose the unique features of their own services and easily implement the blockchain implementation of business logic. Helps to solve problems that were difficult to solve before using SFIS's non-tamperable and non-repudiation features.

Forensic service:

For intellectual property, policy preservation (certificate of equity), personal and corporate qualification certificates, etc. Application scenarios, SFIS fully exploits the ability to be erased and publicized, allowing organizations and individuals to post copyright information, insurance information, qualification certificates, etc. to the blockchain through a simple interface or APP client, allowing all accounting The nodes collectively testify for themselves.

4 Basic services:

The basic service module consists of interface adaptation, consensus management, network communication and record storage, as shown below:

Interface adaptation		Consensus management		
Protocol resolution	Consistency judgment	Adaptive	Algorithm configuration	
Authentication	Switch management	bft-raft	t-raft	PBFT
Record storage		Telecommunication		
Database	Cloud storage	Route management	P2P	

4.1 Interface adaptation

SFIS integrates Internet idle computing power through blockchain, and IPFS-based distributed supercomputers make rational use of idle computing power. SFIS forms a big data application platform through various data docking channels to obtain user behavior trajectories. It provides SQL and API interfaces to the application layer for user convenience and low-cost access to SFIS. The API interface supports both synchronous and asynchronous modes. After the interface adaptation layer parses the service request, after the authentication and signature verification, the service request is recorded to the account book through the consensus algorithm. As a client of the consensus management module, the interface adaptation module also participates in consensus management. The interface adaptation module is mainly responsible for the summary and consistency judgment of the results returned by each consensus node.

4.2 Consensus management

The consensus mechanism is the technical point of the SFIS core. The process of agreeing on data, behavior, or process through the interaction between nodes under the pre-set rules of nodes participating in multiple parties is called consensus. The consensus mechanism refers to the algorithms, protocols, and rules that define the consensus process.

4.3 Telecommunication

The network communication module is responsible for message data transmission between nodes and on the service side. SFIS uses a dynamically self-organizing network that can be multiplexed and connected for sharing. It can be compatible with existing security facilities such as firewalls and proxy servers, providing peer-to-peer networking and secure and reliable data transmission.

4.4 Record storage

The SFIS record storage can support the storage of a variety of media. The storage medium can be a database, a file system, or a cloud storage medium such as cloud DB, cloud KV, and the like. Record storage uses a blockchain structure, any tampering with historical data can be found by self-checking, and warnings and automatic corrections.

二. User Management

User management mainly solves the mapping relationship between user identity and blockchain address, and the privacy of user privacy. And the traceability of regulatory audits. From the business scenario, some scenarios require anonymity and transaction irrelevance. Such as stock trading, digital currency, etc. Some scenarios do not require anonymity and irrelevance, such as mutual insurance, source tracking, and so on. To balance these two scenarios, key management requires strong adaptability and compatibility.

SFIS offers a variety of configurations that users have the flexibility to choose. From the perspective of user access, one is the original system transformation access blockchain, and there is a key security management system with high security level, such as institutional clearing, bank factoring, etc., and the other is a new application scenario. There is no perfect key management system for access blockchain or legacy systems, such as some supply chain services and some B2C services. In order to inherit the key security management system with high security level and retain the usage habits of the original users, SFIS provides three types of traditional key system integration, full hosting and partial hosting.

1 Traditional key system integration:

Applicable to users with high security level of the original private key system, such as financial institutions, original U shields, electronic signatures, etc. For such users, SFIS only needs to use the private key system and blockchain of the original users. The addresses can be associated.

2 Partial hosting:





Some subjects that are suitable for accessing the blockchain service have a higher security level key system or a plurality of blockchain technology interworking scenarios. In the case of partial hosting, SFIS guarantees the multi-party blockchain address association and consistency of participation.

3 Fully managed:

Suitable for new access scenarios and scenarios where the original Internet has a higher degree of habit. The original system of user name and password is associated with the secure key generation and management system to isolate the user information from the blockchain address and protect the privacy of the user.

4 For fully managed mode:

The user management system of SFIS consists of four parts: account management, key management, authority management and risk control audit.

 Account management	 Key management	 Authority management	 Wind control audit
Registration Login Cancellation Irrelevance	Generation Association Safe Signature chain	Privilege rating Access control	User association Audit control Wind control management

4.1 Account management

Account management is responsible for user account management, including account registration, login, logout, and account and key irrelevance processing. When the account is registered, the identity information such as the username and password

that the original user is accustomed to is mapped to the SFIS address. After the account is logged in, the service request related to the blockchain can be sent. In the scenario where the transaction is highly confidential, the user can select the SFIS address irrelevance processing, so that different transactions of the same user are not related in the block record storage, thus improving user security and transaction confidentiality.

4.2 Key management

In the fully managed mode, the key management system is responsible for the association of the user key with the account, key security management, and loss recovery. The user key is generated on the client, and the user can choose to save the key in the key safe or delegate to the associated account so that the key is lost and retrieved. In order to ensure the reliability of the association relationship between the user account and the key, the key management system uses the multi-node chain storage for the signature of the association relationship.

4.3 authority management

The rights management module is responsible for the control and management of user accounts, key systems, node joins and exits, and data access. Including audit permissions, account delegation permissions, node consensus permissions, and user data access permissions. Auditing authority is to provide auditing functions for the regulatory authorities, and to strictly control the access rights and data scope. Users who are not related to transactions on the shared ledger can be associated with users. The account delegation authority is used to control the access control of the user account delegation relationship. Consensus authority for consensus authority management for participating or newly joining nodes. Access rights are used to manage client-side data query permissions on the blockchain.

三. Smart contract

The SFIS contract section includes both standard contracts and contract types for business customization. Standard contracts include asset consistency check, automatic transaction matching, multi-party confirmation transfer, and automatic clearing of contracts, which are relatively simple contracts. They are built-in contracts of the SFIS blockchain and can be directly linked to the blockchain. User-customized smart contracts that modify configuration and add other business logic through contract templates can also support more complex user-programmed contracts that run in a stand-alone environment.

The smart contract includes the registration, triggering, execution and cancellation of the contract, as shown below.:



Chapter IV Algorithm Optimization and Network Layer Design

—. Principles and objectives

1 Optimization and design goals:

Design needs to consider the three elements of discovery, retrieval and consensus.

Consensus Consensus:

The efficiency of existing consensus algorithms (TPS) is mainly restricted by the network layer structure. The introduced super point (DPOS), layering, sharding and other technologies are passively improving the network layer structure.

Search Searching:

IPFS does not have a clear search algorithm. Existing search engine algorithms do not support the decentralized system very well. Efficient retrieval determines the mining revenue.

Discover Discovery:

IPFS adopts the classic kademila network structure. There are flaws in the classic network design of P2P systems. It needs to be optimized and upgraded on the Kad network structure. The new network layer design should improve the efficiency of consensus, retrieval and discovery.

2 Optimization and design principles

Classic DHT network, must be considered:

1) Physical proximity: The neighbor relationship represented by the IP address is dispersed by Hash, which generates a large amount of invalid cross-network traffic, wastes bandwidth resources and impacts the backbone network.

2) Node heterogeneity: There is a big difference in node performance in P2P networks. The stability of the nodes determines the efficiency of the discovery; small nodes (memory, bandwidth, online duration) can not implement the sorting, caching, calculation and other algorithms in the retrieval, which becomes the bottleneck of retrieval, and thus reduces the performance of the consensus algorithm.

3) Network fluctuations Churn: Nodes join and exit the network arbitrarily, causing a large maintenance load on the network and risk of data loss, reducing network availability. Separating stable nodes from small nodes by layering is a proven solution.

4) DHT does not support semantic retrieval.

Therefore, optimization and design principles must be followed :

1) Compatibility: The IPFS version is continuously iteratively upgraded. In order to be compatible with future versions and IPFS networks, the IPFS code is changed as little as possible. The new optimization and design algorithms are compatible with IPFS, that is, the IPFS common version and the enhanced version.

2) Hierarchical design: IPFS network and super node network are generated through layered design. In the super node network, the above DHT problem is solved, and the super node undertakes more discovery, retrieval and consensus tasks. The layered design can support consensus mechanisms such as DPOS and DPBFT.

3) Super-node election: The super-node algorithm considers the locality, churn and DPBFT consensus mechanisms to form a stable super-point network with strong computing power and large bandwidth.

4) Super node maintenance: The super node network needs to exchange a large amount of core data. The existing Gossip, random-walk and other maintenance algorithms are inefficient, and the DHT multicast algorithm needs to be considered to solve the maintenance problem.

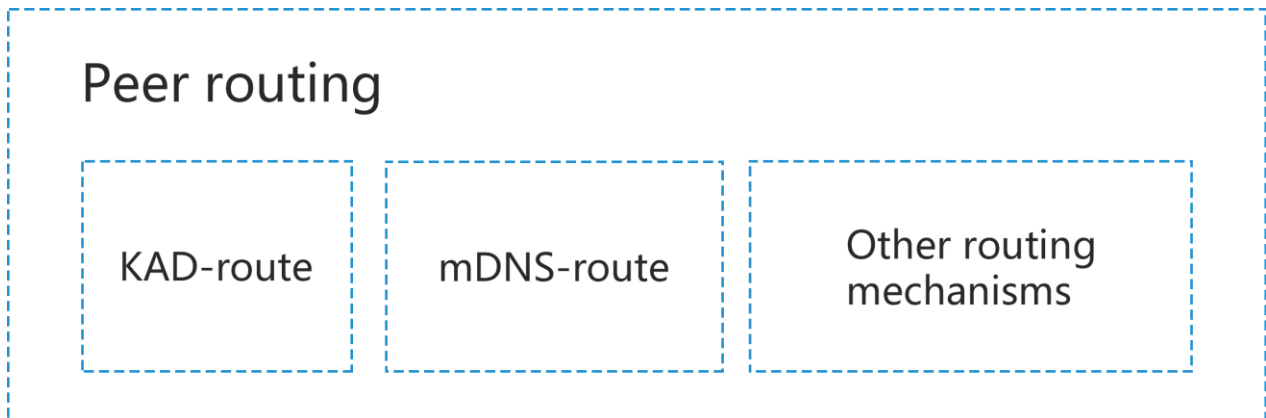
二. SFIS design

1. IPFS network layer status (libp2p)

1.1 IPFS uses Kademila and S/Kad structures

1.2 Adopt mDNS network layer multicast protocol in LAN

1.3 And provides an interface to other discovery algorithms



1.4 In order to resist attacks such as witches, Byzantium, DDOS, etc., the use of random-walk to improve the DHT algorithm

1.5 Did not see the Coral network first mentioned in the white paper, Coral is a layered DSHT algorithm

2. SFIS main content

2.1 Cluster Cluster: At present, the alliance has established an enterprise server room (mine pool) to build a super point based on the machine room.

2.2 Short-chain Shortcut: Physical neighbors of the machine in the equipment room, using large routing table technology, establishing short connections between nodes

2.3 Hot Data Backup Hotrep: Establish hotspot routing table for high frequency search to improve retrieval efficiency

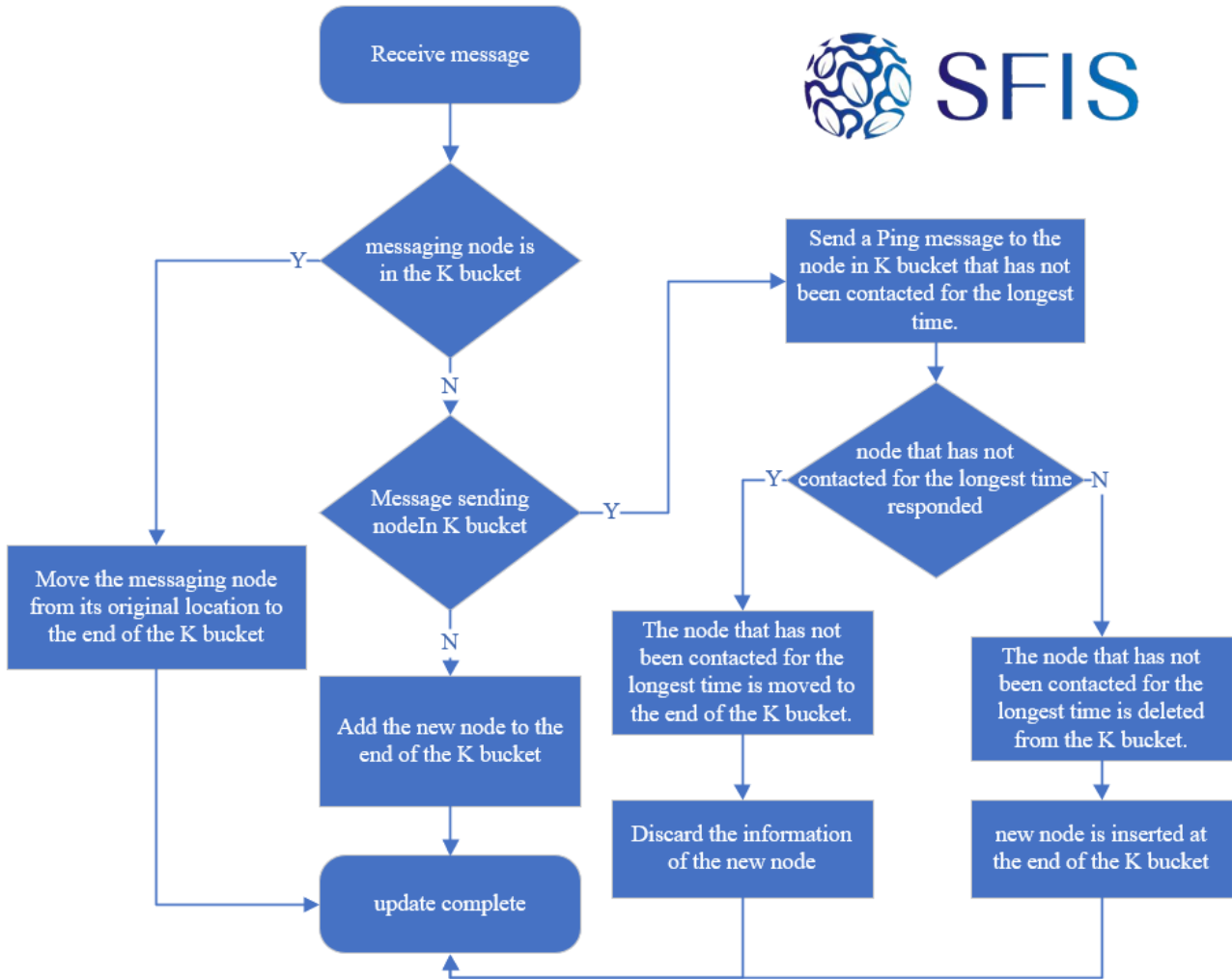
2.4 Consensus TPS: Based on the super-point network, PBFT can be directly optimized to DPBFT, and the consensus TPS is improved.

3. SFIS design is as follows :

Kad algorithm optimization

The kad protocol tends to leave the old node with long online time in the K bucket. Only when the old node in the K bucket actively exits the network or fails, will the new node be added to the K bucket. In order to prevent the K bucket from aging, Kad introduces a refresh mechanism. In a certain period of time, Kad will clear the old node that is invalid in the K bucket and add a new node. This method greatly improves the stability of the K bucket and reduces the network maintenance cost. However, only the old node exits or fails to have a new node to join, which will leave many high-performance nodes out of the bucket.

Therefore, it is necessary to make a new adjustment to the update mechanism of the K-bucket. The goal is to preferentially add a new node with excellent performance to the K-bucket under the premise of ensuring the stability of the K-bucket, instead of the old node with poor performance in the K-bucket. Therefore, the nodes in the K bucket are guaranteed to be nodes with better performance.



K barrel update flow chart

1) Excellent node (super point) evaluation model

There are large differences in heterogeneity between nodes in the Kad network, and the performance of each node is quite different. The excellent node evaluation model sets the Cap capability value for each node to reflect the node processing capability. By evaluating and calculating the processing power of the node, the node value of the Kad network can be referenced to the Cap value of the node, and the node with the high Cap value is added to the K bucket, and the Cap value is sorted according to the Cap value in the K bucket. The high node is placed at the head of the K bucket.

The data structure of the Cap value is as follows:

```

Typedef struct capinfo{
    Uint256 node_id; //node ID
    Double U; //Node remaining computing power
    Double M; //The remaining memory of the node
    Unit8 T; //node continuous online time
    Unit8 TTL; //Physical hops
    Unit8 RTT; //round trip time
    Double cap; //node cap value
}K_capinfo;

```

When the K bucket selects a node, it obtains the U, M, T, TTL, and RTT parameters of all nodes, obtains the maximum values of U, M, and T, and the minimum values of TTL and RTT, and calculates the cap value according to the normalization function.

$$\text{Cap} = f(a * (\min_TTL / TTL + \min_RTT / RTT) + b * (U / \max_U + M / \max_M + T / \max_T))$$

a b select the value of <1 to achieve normalization

The cap worth size is used as an indicator of the overall performance of the node. The larger the cap value, the higher the overall performance of the node, and the K bucket is preferred. The smaller the value, the smaller the overall performance of the node and should be selected last.

2) K barrel update strategy adjustment

The K bucket selects the candidate nodes according to the DHT algorithm, then calculates the cap value according to the evaluation model, and sorts the candidate nodes according to the cap value, preferentially selects the node with the high cap value to be inserted into the k bucket, and deletes the intra-bucket node with the low cap value to complete the K bucket. Adjustment.

By modifying the order of nodes in the K bucket, it can be ensured that the performance of the node is prioritized in the selection of the node, and the success rate of resource positioning is higher. According to the performance of the nodes from

large to small, the node with higher comprehensive performance is guaranteed, and the probability of being selected is higher. This kind of structural adjustment of the K bucket can ensure that when the Kad is used for resource location, under the premise of ensuring a high resource location success rate, the service provided by the node with higher comprehensive performance of the node can be obtained preferentially.

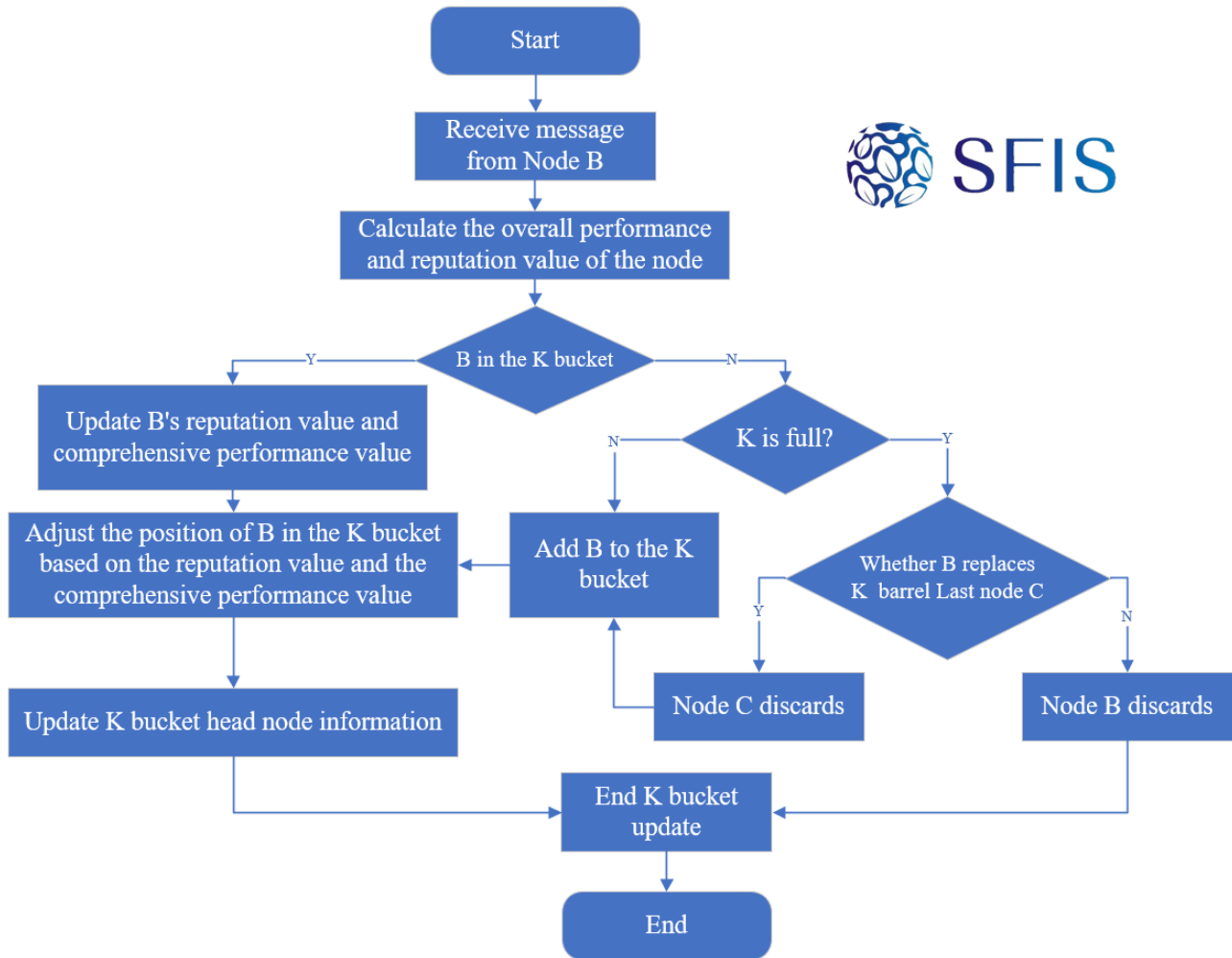
It can be said that the adjustment of this algorithm has the least modification to the existing libP2P_DHT algorithm and is more convenient to apply.

3) K bucket random selection strategy

The Kad network does not consider attack problems such as sybil and DDOS. If a malicious node forges a cap value to become a good node or obtain more search tasks and may implement a power attack and then an IPFS network; On the excellent nodes, hot spots will occur, that is, hotspot bottlenecks and routing tree congestion. In order to solve the above problems, we add a random selection strategy in the routing algorithm, improve the routing link to enhance the Kad network to resist the attack capability, and improve the hotspot problem.

The steps to randomly select nodes based on probability are as follows:

- A. Read the cap value of the head node in the k bucket
- B. Calculate $choose = rand() \%$
- C. Pointer pointer traverses all nodes of k bucket
- D. Add the cap of the node every time a node pointer is passed, $temp += point - > cap$
- E. When temp is greater than choose for the first time, the node pointed to by the pointer pointer is the node selected in this operation in the K bucket, and the nodes are arranged in descending order of cap. The random selection of the seed can be avoided while ensuring routing efficiency. The generation of system hotspots.



K-bucket algorithm based on cap evaluation model

Hotrep Hot Data Search

Searching for hotspots: Some time in the Internet, there will be some resources that are searched more. The higher the degree of attention of a certain resource, the higher the frequency of searching. In view of this phenomenon, a hotspot routing table can be added to the super node in the system to record the most frequently searched node information, and the resource hash key value and the node address of the resource are recorded in the table. The routing table, if the information of the resource exists in the table, directly routes to the destination node to complete the query; otherwise, according to the normal resource node retrieval method.

Adding a hotspot routing table to the super node can greatly enhance the efficiency of IPFS retrieval while reducing the network load, and at the same time let

the node with strong performance (super point) take on more tasks, reflecting the greater the ability of the Internet to be more responsible.

There are two options for confirming hotspot data:

Option 1: Provide a search layer or retrieve a DaPP interface, and retrieve data from the upper layer to calculate hotspot resources through Top*K and Hits algorithms.

Option 2: The history of all super points storage routes, using the smart contract to implement the Hits algorithm to calculate hotspot resources.

The length of the hotspot routing table is the same as the length of the Kad routing table. There are three data fields, which are the hash value of Resources_key to find the resource, Node_id to store the IP address of the resource node, and the number of times the Count resource is retrieved. The hot rep data structure and query algorithm are described as follows:

Struct hot table

{

Char Resources_key[];

Char Node_id[];

Int Count;

} ;

//Find the keyword K in the hotspot table

If(Find hot table(K))

{

Count+1;

Return Node_id;

//Find the keyword K in the hotspot table, increase the number of

Counts by 1, and return the IP address of the node where the keyword is located.}

Else//No keyword K found in the hotspot table

{


```
Update (hot table);  
//Update hot table with the most recently unused replacement algorithm  
Find K table(K);  
//Continue to look in the improved K bucket  
}
```

Cluster short chain shortcut (base hotspot)

A considerable number of nodes in the IPFS network are enterprise servers. Installed in the equipment room, the high-performance machine configuration is similar, the physical location is close, the operation is stable and the online time is long, and it has the characteristics of public network IP and symmetric uplink and downlink bandwidth. We define it as a super node cluster. Kad is used in the super node cluster, but the algorithm retrieval time is long, the routing link is complex, and a large amount of computing resources are idle. In order to improve the efficiency of cluster use, we design a two-layer DHT network in the cluster, and the nodes form a full connection to achieve "one-hop" routing (on hop), which greatly shortens the retrieval time and is equipped with a hotspot routing table to improve the retrieval hit rate. This kind of cluster DHT network, we call it: base hotspot.

1. Double-layer DHT network design

In the physical computer room, each computer room constitutes a DHT network; each computer room elects K nodes as front-end machines, and the front-end machines of n computer rooms form an $n*K$ DHT upper-layer network to realize cross-cluster forwarding. This double-layer DHT network can achieve $o(d)$ routing efficiency ($d \leq 3$), the upper DHT network maintains the routing table $o(n*k)$, the lower routing table maintains $o(M)$, and M is the number of machines in the equipment room. .

2. Double layer DHT maintenance algorithm

Each layer of the network uses a classic Chord network, and all nodes form a

fully connected network. In order to resist broadcast storms, data exchange between nodes uses a power-order multicast algorithm.

The nodes form a one-way circular linked list. Yes, order. Then the i -th power neighbor is . Where is the largest integer less than. The multicast space is the upper limit of the initialization time. Description of the multicast algorithm of node s :

```

s.PowerMulticast(update, upbound){ //updateFor data that needs to be
updated
    for (i=0, i<m; i++){
        if (list( $b^i$ ) ∈ (s, upbound) ){
            new = list( $b^i$ ); //Set the next multicast point in power order
            if (list( $b^{i+1}$ ) ∈ (s, upbound) ) new_upbound = list( $b^{i+1}$ );
            else new_upbound = upbound ; //Set the next multicast

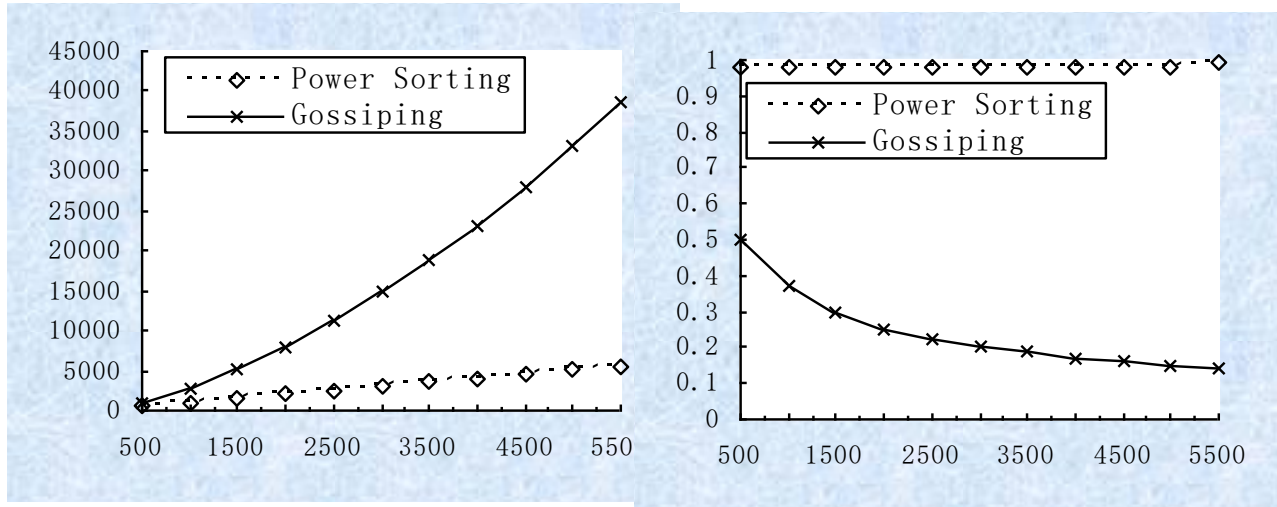
forward (update, new_upbound) to new; //Send a multicast message
        else exit;//Exit without qualifying points}
    }

```

Among them, it is the base of power order multicast. Each node can be determined based on its own bandwidth and the number of child nodes it is responsible for distributing:It can be estimated from the multicast space that it is responsible for and the ID value in DHT.

The concept of the Gossip protocol diffusion round and the number of spread messages per round determines the round of message diffusion and the number of messages spread per round. According to the definition of the Gossip protocol, in the power order multicast algorithm. Compared with the Gossip algorithm, the power order multicast algorithm does not generate duplicate messages, the probability of all nodes getting messages is high, and the number of messages spread per level and the

number of expansion rounds are the lowest.



3. Join and exit of base hotspots

When a node in the base joins or exits, it will affect all nodes in the base; when the current setup joins or exits, it will affect the upper DHT network, and the maintenance cost is high. However, the nodes in the base are quite stable, so the network churn is very small, so the maintenance cost is high but the maintenance frequency is very low. This design can effectively exert the performance advantages of the base super node.

3.1 Node join maintenance

When a new node is added, a double-layer DHT routing table can be obtained by randomly selecting a node through the bootstrap list, and the size is $M+n*k$.

The new node broadcasts its own information using a power order multicast algorithm, and all nodes update the routing table.

3.2 node exit

When the node exits, the front-end machine detects that the node fails, broadcasts with a power order multicast algorithm, and all nodes update the routing table.

DPBFT consensus

At present, the TPS of the public blockchain based on the proof of work (POW)

and the certificate of interest (POS) is only less than 7 times. The average confirmation time of a transaction is 10 minutes, and the time when the transaction cannot be falsified is 1 hour. Moreover, the consensus algorithms such as POW and POS are inefficient and consume a lot of energy, which can not meet the performance requirements of blockchain system. The traditional distributed consistency algorithm represented by Paxos and Raft does not consider the Byzantine fault tolerance problem, and it is not applicable to honest and malicious nodes. Coexisting blockchain system; the practical Byzantine fault-tolerant algorithm was originally designed for distributed system messages and system instruction execution order problems. It adopts C/S architecture. The three-stage broadcast protocol seriously wastes bandwidth and static. The network topology cannot meet the system characteristics of the block chain dynamic equivalence. The DPOS consensus represented by EOS is valued by the blockchain. After studying the principle of DPOS consensus algorithm, we apply the authorization mechanism of DPOS algorithm to PBFT, and improve the PBFT, and propose dynamic authorization for blockchain application. The Byzantine fault-tolerant algorithm DPBFT has three advantages over PBFT:

- 1) Authorize the election mechanism, specialize the consensus accounting node and supplement the "lifting level" mechanism to dynamically update the consensus accounting generation
- 2) Streamlined consensus state, reducing network overhead caused by the consensus broadcast mechanism in the PBFT phase
- 3) Layered P2P structure, fully in line with the characteristics of the blockchain system

1. DPBFT consensus algorithm

The traditional PBFT consensus algorithm requires three stages to broadcast on the whole network, and the instability of the consensus node will cause the network segmentation (Partiton). In order to improve the efficiency of PBFT, there is a problem that nodes are few and nodes are stable and fully trusted. We use a two-tier DHT

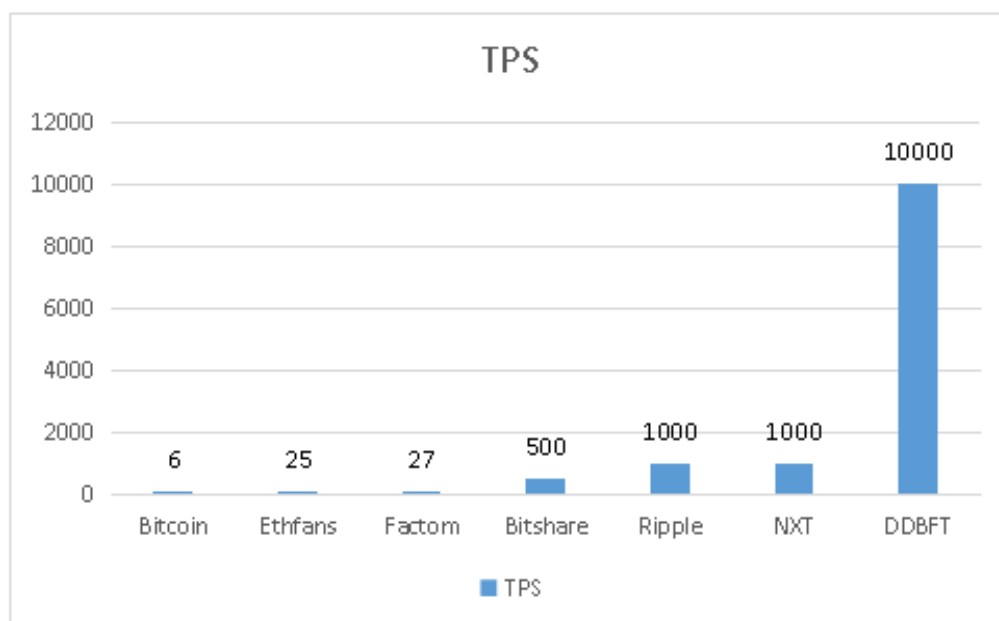
network to build a dynamic authorization DPBFT consensus to solve the above problems. The specific process is:

- 1) K front-end machines of each base are authorized nodes
- 2) Authorized nodes form a DHT fully connected network, multicasting all consensus messages in power order multicast
- 3) All authorized nodes complete the three-phase PBFT consensus
- 4) Send consensus results to the originating node

2. Judgment of legality of transactions

The rules for determining whether a transaction is legal are as follows:

- 1) Whether the transaction conforms to the rules for the composition of the transaction, if it is met, it is legal, if it is not, it is illegal.
- 2) Whether the transaction already exists in the blockchain, if it does not exist, it is legal: if it exists, it is illegal.
- 3) Whether the transaction is a double transaction, judging whether the double transaction is based on whether the last block of the current block is the end of the blockchain, and if so, it is legal. If not, the blockchain is forked, and double payment is very likely. , judged to be illegal.
- 4) Whether the script in the transaction is correctly executed, which means that the property in the transaction is legally transferred from the initiator to the recipient. If it is executed correctly, it is judged to be legal: if the execution result is false, it is determined to be illegal according to the algorithm. Simulation test and theoretical evaluation, DPBFT has more than TPS in the case of 1000 consensus nodes.



Chapter V Credit Endorsement

In order to ensure that we are not fictitious, exaggerating the authenticity of the financing project, the prospects of earnings, concealing the risks and risks of financing projects, making false one-sided propaganda or promotion, such as ambiguous language or other deceptive means, fabricating or distributing false information or Incomplete information harms the business reputation of others and misleads investors. We have joined a foundation for credit endorsement. Morgan Stanley (NYSE: MS) is known as the “Da Mo”, an international financial services company based in New York, USA, which provides a variety of financial services including securities, asset



management, corporate restructuring and credit card. It currently has representatives in more than 600 cities in 27 countries and employs more than 50,000 people.

Adherence to business ethics, compliance with international conventions and relevant national laws and regulations is the cornerstone of SFIS's global compliance operations. The industry strengthens the management and supervision of global business operations through the establishment of specialized compliance and regulatory organizations, and continuously strengthens employees' legal awareness and normative awareness through training, publicity, assessment, and accountability.

Continue to work on the compliance construction of blockchain technology, network security, data and privacy protection, anti-commercial bribery, trade secret protection and other business areas. We have continued to ensure a compliance system that meets industry best practices by increasing the investment in organization and resources.

The core of the fund partner



Anthony

Morgan Stanley Global Partner
Wall Street Financial Specialist
Senior fund management expert



Carol

CEO of Zhichuang Technology Group
Co., Ltd.
Former Senior Manager, UBS Group
Partner of Morgan Stan Financial
Services

Chapter IV Introduction to Tokens

Issuance method

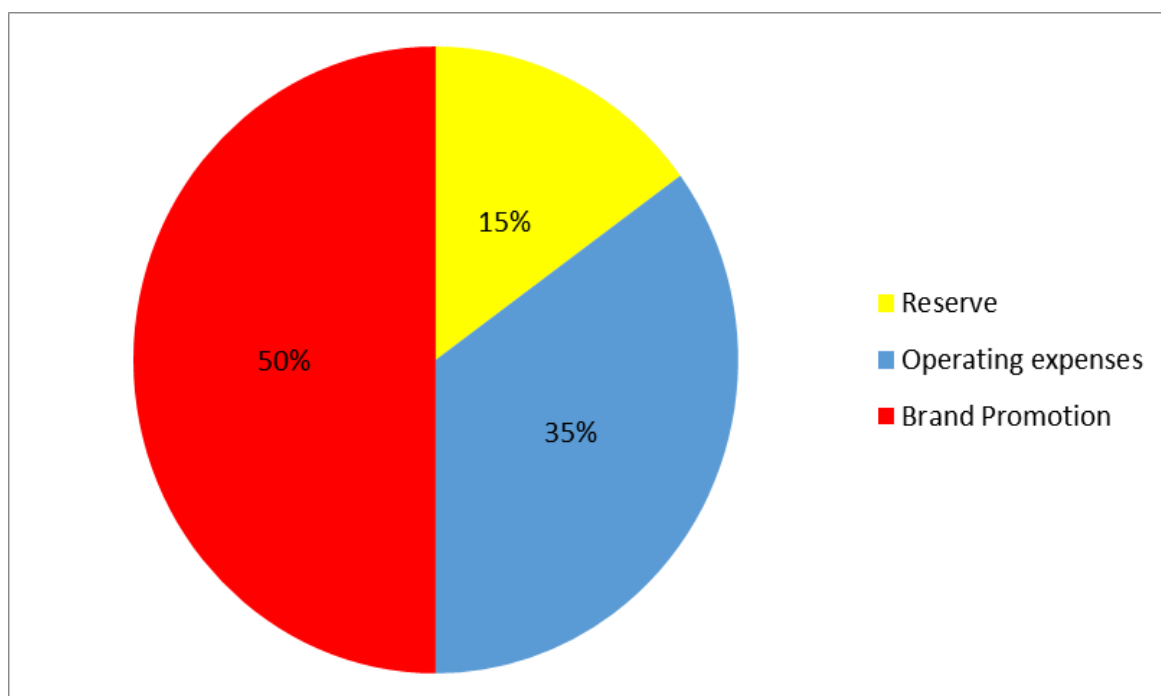
The name of the currency; English (SFIS), Chinese (super star file)

mode	plan
Total amount of issuance	3 billion pieces (5% private placement, 15% team, 20% fund, 60% mining)
Private placement	5%, 150 million pieces
Private placement price	5 yuan / piece
Private placement time	August 15 - October 31, 2018
Estimated time of the market	November 18
Expected price	13 yuan
Release mechanism	After 30 days on the line, 15% of each month is released.
Accepting assets	ETH Ethereum

time online

date	jobs
2018/08	Online trading venue
2019	Full online line
<p>This online launch will be started on the official website in August 2018 and will be released on other platforms.</p>	

Fund use plan



35% of the funds raised from the public offering will be used for the functional development and system operation and maintenance of the platform, including providing incentives for team members, research and development funds, etc.

50% is used for brand building and operation promotion of the platform, including continuous promotion and popularization of the platform for the traditional industry and blockchain industry, providing financial support for various market activities, ensuring that the Bofa platform quickly gains market recognition and rapid Accumulate trading users

Chapter VII Team Introduction

Adi Ben-Ari

Blockchain expert

Worked at Applied Blockchain 2015.4 - now

Co-founder/Agent CTO: During his tenure, he launched an international website, futures trading platform and algorithmic trading orders.



Education background

MBA (Master of Business Administration), Tel Aviv University School of Business Administration, 2000 - 2003 B.Sc. (Bachelor), Department of Computer Science, University of Bristol.

Mario Gemoll

Financial Specialist / Freelance Programmer and Consultant



Previously, he led Mario Gemoll 2008.8-2015.10

The R&D team of the entire team's futures trading platform is responsible for futures trading systems with annual revenues of more than \$300 million.

Education background

Master of Science in Computer Science, Oxford University, 2013 - 2016.

Bachelor of Computer Science, Technical University of Munich, 2003-2007

Chris Lavery

Community Expert /

Vice President of Business Operations and Finance at Bofa 2015.2 - Present. Vice President of Finance and Internal Consultant: Working at GoPago 2012 - 2014



Education background

Master of Business Administration in Finance, Wharton School of the University of Pennsylvania, 2009 - 2013

Philip Welber

Password Expert /

UX Engineer: Working at Blockchain 2016.11 - Now. Full-end engineer: Working at Targeted Social 2015.12 - 2016.11



Xen Baynham- Herd

Mathematical expert

Strategy Leader and Chief Economist: Previously Blockchain 2017.5 - Present Board Member: UBS 2015.3 -



2017.5.Strategic Planner: Working at UBS 2013.4 - 2015.2 Analyst: Working at UBS 2010.11 -

Education background

Master of Science (MSc), Department of International Banking and Finance, Durham School of Business, 2008-2009 Bachelor of Arts (BA), Department of Economics and Politics, Durham University

Daniel's CV

High-tech-driven entrepreneurial professionals

Has many years of experience in the field of technology, in the foreign exchange market Experienced in trading, using foreign exchange personally and professionally. Enthusiastic about financial markets, cloud integration in sales and data protection processes, is currently monitoring the development of multiple financial modulo solutions for customers.



Dr. Imran CV

Blockchain and cryptocurrency traders, and more than 3 years of experience in related fields and transactions, always actively discover new machines .Meeting and cooperation areas.



Chapter VIII Risk Warning and Disclaimer

Disclaimer

This document is for informational purposes only and does not constitute an opinion regarding the sale or purchase of SFIS shares or securities. Any similar offer or levy will be made under a trusted term and with the applicable securities laws and other relevant laws, and the above information or analysis does not constitute investment decisions or specific recommendations. This document does not constitute any investment advice, investment intention or instructed investment in the form of securities. This document is not intended to be an understanding or offer of any purchase or sale, or any invitation to buy or sell any form of securities, nor is it a contract or commitment of any kind.

SFIS clearly stated that the relevant intention users clearly understand the risks of the Bofa platform. Once the investors participate in the investment, they understand and accept the risks of the project, and are willing to personally bear all the corresponding results or consequences.

Bo invention does not assume any direct or indirect losses caused by participating in the Bofa project, including:

1. Economic loss due to user trading operations
2. Any errors, omissions or inaccuracies arising from personal understanding;
3. Loss caused by individual trading of various blockchain assets and any resulting behavior.

risk warning

Safety:

Many digital asset exchanges cease to operate due to security concerns. We attach great importance to safety, but there is no absolute 100% safety in the world, such as: various losses due to force majeure. We are committed to doing everything possible to ensure the security of your transactions.

Competition:

We know that the exchange is an extremely competitive field. Thousands of teams are planning and developing trading platforms. Competition will be cruel, but in this era, any good concept, startup, or even mature company will face the risk of such competition. But for us, these competitions are the driving force in the development process.

to sum up:

In summary, today, blockchain assets are highly sought after, we have created a unique star lineup team, committed to the long-term sustainable development of blockchain assets, designed to provide investors with a safer, more efficient, Trustworthy trading platform, the best investors regard the team and experience as the core considerations, and we are the choice of countless excellent investors; together with the excellent people you will be better, sincerely invite you to join us, Be part of our team and share the most efficient return on investment in this era – digital wealth.