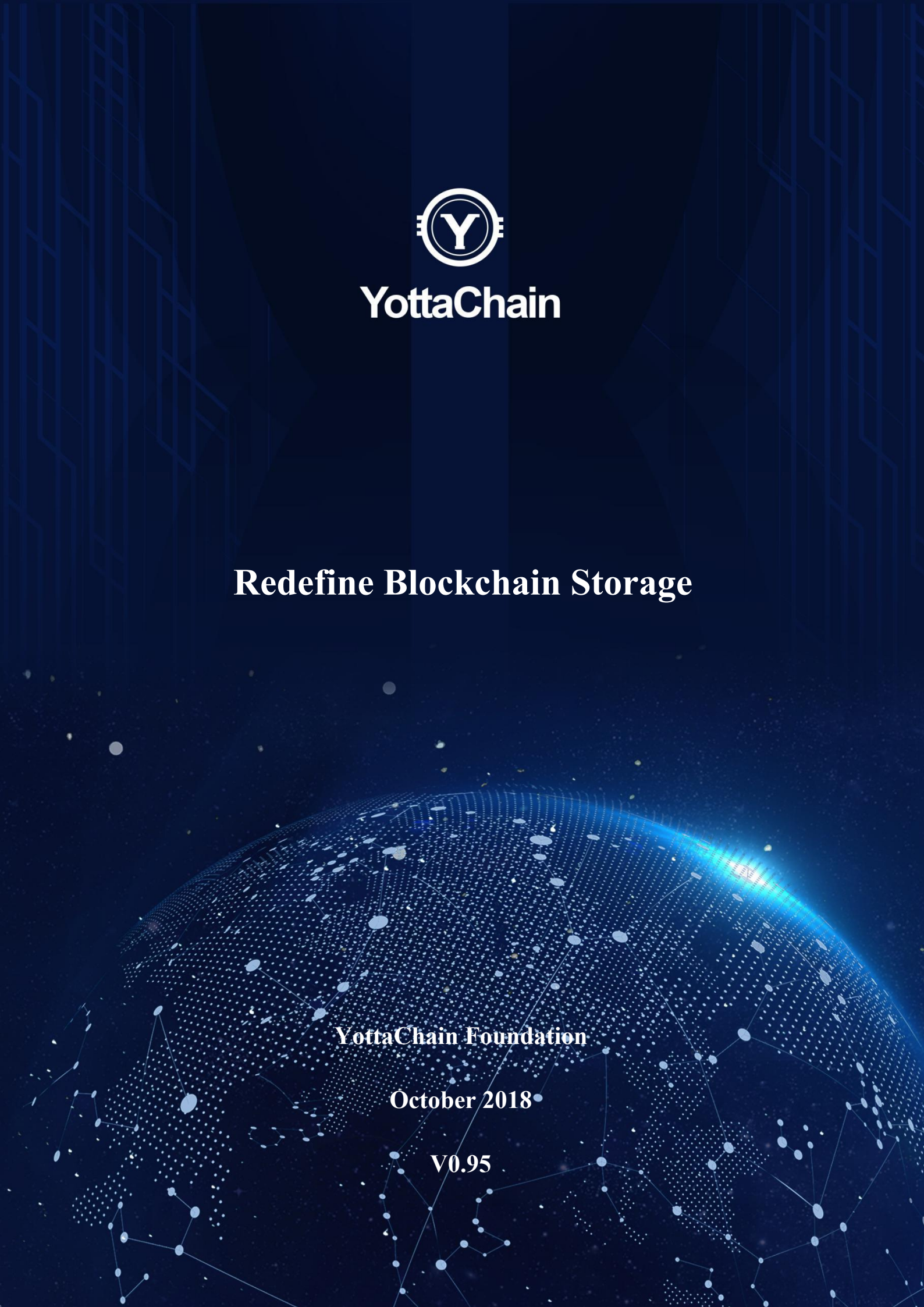


Redefine Blockchain Storage

YottaChain Foundation

October 2018

V0.95

CONTENTS

ABSTRACT

Storage is the best application scenario for blockchain, and YottaChain is a top public blockchain for the best applications of blockchain.

YottaChain redefines the blockchain storage industry with its unique core technology, enabling blockchain storage to break through and develop into a new pattern, establishing an open platform to play a key role in the development of blockchain storage.

On the technical level, YottaChain has an exclusive patented technology of “de-duplication after encryption”, that ensures blockchain storage is safe enough for personal and enterprise data, while enlarges the data storage space by 5-10 folds by dedup bonus.This technology has subverted the blockchain storage industry and for the first time made it possible to use it in both ways.

From the point of view of economic model, YottaChain rewards who contributes resources, instead of who wastes resources like BTC/ETH.

Furthermore, YottaChain's double layers token design combines both stability and liquidity. From the point of view of double layers token design the asset backed tokens anchor physical resources,there is unearned increment by 50%+ every year; and the liquid cryptocurrency's price can be mined by market, but model design can guarantee long term appreciation;

From the point of view of governance structure, YottaChain for the first time proposed an entirely decentralized governance structure to solve the problems of “who makes the rules”, “how the rules are implemented” And “who will manage the rules when any person is evil or does nothing.”

YottaChain's unique incentive model allows storage resource owners to contribute more space to their YottaChain, and instead gain more storage space and receive additional cryptocurrency rewards.Moreover, this model does not require any subsidy,it can work forever.

In the business model, YottaChain not only forms a commercial closed loop, but also is more reliable than any centralized storage (more than 10,000 times more reliable data), lower cost, and comes with network acceleration, anti-DDos and disaster recovery features. As a typical representative of the main business, we have a deep understanding of market demand and user pain points. With deep industry resources, strong industry partners, and perfect market entry solutions, we can directly and seamlessly migrate the market of tens of billions of dollars;

In terms of ecological development, YottaChain can directly migrate millions of existing IT applications, on the other hand, it provide an open platform to open its own core capabilities and allow blockchain storage on open platforms. The system can share the weight loss

bonus. The third-party blockchain storage system can join the YottaChain ecosystem to gain key technical capabilities, and can immediately realize double revenue. It has now received major support from the IPFS ecosystem.

1. BACKGROUND

1.1. Storage is the best application scenario for blockchain

1.1.1 What is blockchain storage?

Blockchain storage is not about storing data on the blockchain, but it is decentralized storage plus blockchain incentives, using blockchain incentives to allow more nodes and users to join the system, thus building a more reliable , lower cost and larger storage systems.

1.1.2. Storage itself has decentralized requirements

The reliability of centralized storage has reached an extreme. It is difficult to solve the impact of factors other than technology on data reliability and service stability. For example, Tencent Cloud, which broke out in August 2018, completely lost user data events (hardware failure plus operation and maintenance personnel mistakes). In September 2018, Microsoft's Texas data center stopped serving for more than 20 hours (because lightning damaged the refrigeration) Equipment), as well as 2017 AWS object storage service failure (Operation and maintenance personnel operation error) and Alipay stop service event (fiber is cut), not to mention 911 directly destroyed the headquarters of many large companies.

In order to improve the reliability of persistent storage, it is necessary to establish storage nodes scattered around the world. The

more the number, the more the dispersion, the higher the reliability of data;

In order to accelerate the network, it is also necessary to decentralize and establish CDN nodes scattered around the world. The more the number is closer to the end users, the better is the network acceleration effect.

1.1.3 Amplification effect of data deduplication

Data deduplication (discussed in detail in the subsequent chapters of this white paper) is a key technology for storage, which can amplify the data storage space, which is characterized by more users,. The more the data, the greater the amplification effect, that is, the same storage Space can store more data.

1.1.4 Storage can be directly TOKENIZE on the chain

In other application scenarios of the blockchain, such as tracing ability, the blockchain can only ensure that the data after the upper chain will not be tampered, but cannot guarantee that the data on the upper chain is true. On the contrary, storage is both physical world (referred to as a large-scale use in the real world) and the digital world (meaning that it can be directly processed by the blockchain program without a third-party organization), which can be directly tokenized on the chain.

1.1.5 chemical reactions of blockchain + storage

By using the incentive function of the blockchain, it is possible to quickly recruit a large number of miners to join the blockchain storage system and attract a large number of users without requiring huge investment. It quickly forms a scale, and the number of nodes is large, geographically dispersed, which is away from the terminal. And close to the user. As user is more, the data is more, thereby improving the storage quality, increasing the storage space, and reducing the cost.

Conversely, due to the needs and characteristics of the storage itself, the value of the blockchain can be more prominently reflected. Therefore, blockchain storage not only has practical application scenarios, rigid market demand and huge market space (nearly $100 billion per year), but also the best application scenario for blockchain.

For example, Airbnb, as a decentralized hotel, quickly became the world's largest hotel, surpassing historic hotels such as Hilton. Airbnb is spending a huge amount of marketing dollars to achieve this. With the help of blockchain, decentralized storage is also expected to surpass AWS/Google as the world's largest storage pool.

1.1.6 User value of blockchain storage

Before the development of decentralized applications (DApps), blockchain storage could compete for marketplaces from existing

centralized storage, and it is very rare in blockchain applications to compete for market quality and price with centralized applications.

For users, blockchain storage as a persistent storage, has more than 10,000 times more data reliability and service stability than centralized storage, and it also contains very expensive disaster recovery and anti-DDos features. The price is only a fraction of the centralized storage without disaster tolerance and anti-DDos features. In other words, the quality exceeds the luxury goods, and the price is lower than the knockoff goods.

There is also a disadvantage of using blockchain storage as a persistent storage, which is poor performance, mainly reflected in the Latency indicator (the total system throughput index can be built up by the number of nodes), which is due to the existence of large network transmission delay. However, it does not prevent blockchain storage from having an overwhelming advantage in the field of persistent storage. This is because storage is inherently layered. Each layer acts as a cache for the next layer. The better the performance, the higher the unit price, the smaller the capacity. And lower the performance, the lower the unit price, and the larger is the capacity. The blockchain acts as the last-level persistent storage layer, and there are several layers of centralized storage as local caches (hard disk, SSD, 3DXPoint, memory, L3 cache, L2 cache, L1 cache, etc.). This tiered storage system is already existing. After the blockchain is

stored, it is nothing more than adding the most reliable, cheapest, largest and slowest layer, for example, from 7 to 8 layers.

In the field of network acceleration (CDN), blockchain storage has incomparable performance advantages due to the large number of nodes and proximity to users, and the cost is also lower.

At present, the market for enterprise-class storage represented by Dell-EMC/NetApp/HDS/IBM/HP and the cloud storage represented by AWS/Google/Microsoft is more than $60 billion per year, and the total global data is The amount is doubled every 27 months (Gartner above). Blockchain storage has an overwhelming advantage over existing centralized storage in both persistent storage and network acceleration, with a market size reaching tens of billions of dollars.

1.2 IPFS

IPFS (Inter Planetary File System) is a star project for blockchain storage. IPFS is a decentralized storage system, released in 2015, with the slogan “Replace HTTP”. Its corresponding blockchain incentive layer FileCoin raised US$257 million at ICO in 2017, which was the largest ICO at that time and is expected to be Go online in 2019.

1.2.1 What IPFS Resolved

1.2.1.1 Decentralized storage

IPFS provides an excellent decentralization storage mechanism, connecting numerous untrusted nodes, forming a very reliable storage system, which is much more reliable than your own storage, just like bitcoin connecting unreliable nodes to form a more reliable financial system than banks. At present, IPFS still lacks redundant coding mechanism, so there is still the problem of data loss, but it will be added to the fileCoin development as planned.

1.2.1.2 Healthy and Sustainable Mining Model

The mining method of IPFS/FileCoin is to contribute storage space to the community: Whoever provides the larger storage space, more stable services, faster bandwidth and being closer to the central cities will get the more FileCoin as a reward. This novel consensus mechanism provides incentives for social contributors, who contributes more will be rewarded more. Thus, the problem of excessive consumption of resources for mining in traditional blockchain is solved, and a healthy and sustainable model is formed.

1.2.2 Deficiency of IPFS

1.2.2.1 Lack of Data Security mechanism

The underlying layer of IPFS does not provide a data security mechanism, and anyone who knows the hash value of a file can access the file. Such design is more suitable for storing public information, such as web pages, than for storing personal and

corporate data. Because both personal and corporate data are intended to be stored in a more secure way, rather than being made public.

In fact, IPFS's iconic "Replace HTTP" slogan also reflects this helplessness, that is, IPFS is designed to store public data such as web pages, rather than personal and corporate data.

IPFS recommends that part of the security problems should be solved at the application layer through file encryption, but this is not the fundamental solution to the data security problem. Data security is highly professional, and it is difficult for the application layer to do well. Moreover, the file encryption at application layer cannot solve the problem of file deduplication by encrypting, which will affect the efficiency and cost of the whole system.

1.2.2.2 Unsupported Dynamic web pages

IPFS is designed as a replacement of the HTTP protocol, stored static files by means of decentralized model, but currently most of Internet web sites use dynamic web page technology, IPFS protocol will not be used for direct entry of site visit, but only as a dynamic web site of the underlying file storage agreement, if lack of computing power, which is not consistent with IPFS protocol’s original purpose. If the browser uses the IPFS protocol as a way to access the site, IPFS needs to include supporting ofprocessing mechanisms of dynamic web page, which must have the computing power.

1.2.2.3 Insufficient Data reliability

Since the data is not encrypted, for ethical issues, IPFS is designed so that each storage node can only obtain a copy of the file if it is actively pinged (to prevent violent pornography from violating religious beliefs and other files that the storage node owner is unwilling to accept into the node), that is, if there is no other node ping after uploading a file, there is still only one copy in the whole network, which is easy to lose. This mechanism guarantees that many copies of hotspot files (such as popular music) will not be lost, but unpopular files may be lost, thus losing the possibility of making persistent storage.

1.2.2.4 Insufficient Service Stability

IPFS/FileCoin motivates all nodes indiscriminately according to a unified incentive algorithm, resulting in a large number of individual nodes that cannot guarantee stable services, this will drag down the service quality of the entire system. In order to cope with these problems, FileCoin adopts the mortgage penalty mechanism, and other nodes can reconstruct the lost data when the node is offline, but this will inevitably affect the quality of FileCoin's commercial delivery.

1.3 Data Encryption and Data De-duplication

1.3.1 Data Encryption

Data security is very important to everyone. However, since centralized storage is usually provided by large companies, such as AWS, Google and Dropbox, data encryption is only a sales point, it is not a “must have” feature. Most users trust the branded company’s internal control system to guarantee their data security, and it is expected that big companies will not do evil to user’s data, or at least the evil is within acceptable degree.

For decentralized storage, data encryption is a must for storing personal and corporate data. Since the node of decentralized storage is untrusted, in addition, the source code is open and each storage node can be freely accessed. If data is not encrypted, the decentralized storage is only suitable for storing public data such as web pages, and is not suitable for storing personal or corporate data related to privacy/trade secrets.

Therefore, the general purpose blockchain storage must encrypt data by “zero knowledge” data encryption.That is, anyone other than the data owner or its licensor knows nothing about the data, neither the owner of the storage node, the designer of the system, and the system developer.

1.3.2 Data Deduplication

If multiple people have the same data and they do not store it repeatedly but merge and share the same space, it is called deduplication (that is, removing duplicate data) or re-deletion (that is, deleting repeated data).

Data deduplication and redundant storage are concepts at different levels. Even if only one piece of data is stored after deduplication, this data must be divided into many fragments by redundant coding, which are stored on different nodes, even if some of the node data is lost, the data integrity is not affected. The fragments stored on such multiple nodes are collectively referred to as one piece of data.

These two concepts are sometimes misleading or confusing because one of the simplest redundancy algorithms is multi-copy storage, such as IPFS. In this case, the same data owned by multiple users will be saved by deduplication, but this one has multiple copies.

The data repetition rate is positively related to the number of users and the amount of data. The more users and the larger amount of data, the higher repetition rate. According to a reference data, the average repetition rate of a typical large scale cloud storage application is 5, that means every file is repeated 5 times in average. This is the average repetition rate of a single application and the data repetition rate of the whole blockchain storage is definitely far beyond this number.

The higher the data repetition rate, the lower the average storage cost. Suppose the average data repetition rate is 10, the 1GB physical space can store 10GB of data in average, and the average storage cost is reduced by 10 folds, thus forming a strong competitiveness of blockchain storage.

In addition to significantly reducing costs, blockchain storage can also leverage the data deduplication feature to build powerful stimulus models. Assume that a person with 100GB of storage can only store 100GB if he use to save his own data. However, if the storage resource is used for mining, and then use the cryptocurrency to purchase storage space, he will be able to store 200GB data, and a lot of cryptocurrency. This method can store more data and get a lot of extra digital currency, which can effectively encourage the owner of the storage resource to join the system mining. The entire process does not require subsidies, and the system can even collect taxes, which is long-term sustainable. The mystery of this "magic effect" is that 100GB of space can store an average of 500GB or more of data.

1.3.3 Data Encryption OR Data Deduplication, which one to sacrifice?

As mentioned earlier, zero knowledge data encryption and data deduplication all play a decisive role in block chain storage. However, it is commonly known that data can’t be de-duplicated after

encryption, that is, one of zero knowledge data encryption and data deduplication must be sacrificed, it is a hard choice.

Some people think that this is because the data becomes garbled after encryption, and data deduplication cannot be identified. That's not really the point, the hash value of the plaintext can be used to identify duplicated data with no risk to data security.

The main problem is the authorization of data.That is, user A stores data X, when user B also stores the same data X, how to authorize A's data to B without affecting A's data security? It is generally believed that this problem is unsolvable, so there is only one can be survived between zero knowledge data encryption and data deduplication.

For instance, IPFS chose data deduplication and sacrificed data security, which is the actual reason why IPFS is designed to store public data such as web pages etc. IPFS proposes to encrypt data at the application layer, which will force the application to bear the consequence of increasing cost a lot. Some blockchain storage projects have chosen data encryption, sacrificing data deduplication. Although data security is guaranteed, storage costs have risen dramatically and an extremely effective incentive model has been sacrificed.

The founder of YottaChain is a well-known cryptography and storage scientist who broke the "common sense" and used the rigorous

scientific research method to invent the TruPrivacy technology that can achieve “deduplication after encryption”, thus subverting the blockchain storage industry.

2. INTRODUCTION TO YOTTACHAIN

2.1 Introduction to YottaChain

YottaChain is a blockchain storage public chain based on disruptive technology and deep industry resources. It breaks through the limitations of IPFS, providing not only a strong incentive for miners, but also end-to-end seamlessness for users of the original centralized storage. Connected high-quality, low-cost, persistent storage and network acceleration solutions, and also developed a blockchain storage protocol BSP to create an open platform for blockchain storage, providing DAPP with reliable, inexpensive, high-capacity, high-performance decentralized storage. It provides core capabilities and shares de-duplication effects for other blockchain storage systems.

Compared to IPFS/FileCoin, YottaChain’s improvements on IPFS include:

2.1.1 Data Security Mechanism that does not affect de-duplication

TruPrivacy is the only technology in the world that can achieve “deduplication after encryption”, thus achieving zero knowledge data encryption and data deduplication at same time. In 2015, TruPrivacy technology publicly offered a reward at DefCon, the world's largest hacker conference. Under the premise of opening the server as a hacker freely and providing hackers with administrative account rights, the world's top hackers failed to steal the user data stored on the server. No one receives a high cash prize.

TruPrivacy's global patents have been formally authorized to take effect, and the technical details can be found in relevant patent documents of various countries(US patent No. 9164926B2, issued on October 20, 2015, Chinese patent No. 2024272, issued on April 13, 2016, and EUpatent No. 2830282,issued on September 19, 2016). A brief description is also available in section 5.2 of this white paper.

YottaChain has exclusive TruPrivacy technology. It add the data security mechanism based on the inheritance of IPFS existing storage design, mainly in three aspects:

1) Zero-knowledge encryption is performed on data and then data deduplication is performed, so that the final storage is non-repeating encrypted data, the person without permission (including the owner of the storage node, system designer / maintainer) is absolutely unable to know the data content;

2) Implements the file's permission system, defines the file access rights according to the file's Owner, Group and Everyone;

3) Implements the file authorization mechanism at the data level, so that the file can only be opened by the authorized person, and no matter how the nodes do evil (including malicious modification of the code), the authorization mechanism cannot be broken. The reliability of this mechanism, like the blockchain, is guaranteed by cryptographic-based mathematical formulas.

After adopting TruPrivacy technology, data de-duplication can be realized under the premise of ensuring data security. YottaChain is equivalent to become a “magic space”, just like a miner contributes 1 GB space, YottaChain can generate 5-10 GB storage capacity. It leads to a miracle effect that the purchasing power of the digital currency acquired by the contributor exceeds the resources it contributes. Instead of storing their own data, people with storage resources should use the storage space forYottaChain mining, and then use the cryptocurrency obtained by mining to buy storage space to store data. This process not only can store more data, but also left some cryptocurrency. This mechanism can inspire more people to participate in mining and contribute their own storage resources.

2.1.2 Data reliability assurance mechanism far beyond centralized storage

- YottaChain's persistent storage service uses redundant coding, and data is automatically encoded into N (for example, 100, the specific number will be determined by the Community Governance Committee in the future), and any M (for example, 70) fragments can be recovered. Data is output, and then the N pieces are stored in N storage nodes, and each node stores a fragment, so that as long as there is no N-M+1 (31 in this case) node failure, data integrity is guaranteed not to be lost.

- When any node fails, the system will immediately select another node to reconstruct the data of the failed node. In this case, as long as the remaining 30 nodes are not completed before the first failed node is completed, it can guarantee that the data can be will never lost.

- Each node monitors and verifies each other, and any node can be quickly discovered once it fails.

- To rebuild data of a failed node, it will be divided into many nodes and reconstructed at the same time to speed up the reconstruction. For example, the failed node stores one fragment of 10,000 files. It takes an average of 0.5 seconds to reconstruct a fragment (mainly the network transmission time), and 100 nodes are involved in the reconstruction. Each node only needs to

reconstruct 100 fragments. An average of 50 seconds to complete all reconstruction work. As long as the other 30 nodes of the same file do not expire at the same time within 50 seconds, the file data will not be lost.

- Because of the good redundancy and geographical dispersion, there is no need to worry about the damage of the hard disk and the operation and maintenance of the individual nodes. (In August 2018, Tencent Cloud lost user data due to operation and maintenance errors) and lightning weather (September 2018, Microsoft was struck by lightning). Data failure caused by Azure service shutdown in some areas for more than 20 hours), power outages, fiber cuts, earthquake fires, etc.
- Due to the scattered nodes and good redundancy, they is no afraid of DDOS attacks.

2.1.3 Mechanism of seamless migration of centralized storage applications

YottaChain's founding team is a veteran of the storage industry and will provide binary compatible interfaces to centralized storage, including but not limited to block storage, NAS storage and object storage, enabling centralized storage applications without re-development, no code modification, no recompilation, Seamless migration can be done directly using YottaChain storage. For these

applications, it is thought that traditional storage such as AWS/EMC is still being used, although it has actually switched to YottaChain storage.

In this way, all existing centralized storage applications are YottaChain's ecological applications, and its storage market is tens of billions of dollars per year.

2.1.4 Open platform for blockchain storage

YottaChain adheres to the philosophy of hang, which regards all blockchain storage systems (including but not limited to IPFS) as a peer to jointly create a blockchain storage ecosystem, which provides strong technical support for each DApp together to snatch the nearly $100 billion market for centralized storage.

To this end, YottaChain has established an open platform for blockchain storage, opening its own unique core technology to industry peers including IPFS. Other blockchain storage systems connect to the YottaChain blockchain storage open platform through a blockchain storage protocol BSP. All blockchain storage systems based on BSP protocol have the following values:

1. Enjoy the core technology empowerment of YottaChain, including the data encryption deduplication technology that all blockchain storage systems are eager for.

2. Applications for nearly $100 billion in centralized storage

3. Share data to pay dividends. The more blockchain storage systems that support the BSP protocol, the more the data deduplication has on the storage space, and all blockchain storage systems can enjoy this magnification.

YottaChain's BSP agreement will become an international industry standard. The founder of YottaChain is the chairman of a technical committee of the internationally authoritative industry standards organization OASIS. He has built China's first internationally recognized international software standard. In addition, the CEO of OASIS is also a member of Yotta Chain's advisory group and will have sufficient capabilities, and a wealth of experience to build this standard.

After joining the YottaChain ecosystem, the third-party blockchain storage system not only gains the missing key capabilities, but also shares the “data deduplication” bonus. (The data deduplication magnification follows the law of “The more users, the larger the amount of data, the higher the magnification”), immediately earn more than a few times. For example, a blockchain storage system has 10,000 mining machines, 10PB storage space (capacity after redundancy), and its own data repetition rate is 2. After using the encryption and deduplication capability of the YottaChain open platform, it can sell 20PB of data space. After sharing the "data de-duplication" bonus with the YottaChain ecosystem, the

amplification factor is increased to 5 times, that is, 50PB of data space can be sold.

2.1.5 Economic model with both stability and fluidity

In order to ensure the stability of the currency, and also provide a market-based mechanism to facilitate the discovery of prices through the market, YottaChain uses a two-tier currency model. One of them is a market-based currency, and the other is a resource token for asset endorsement. The resource token anchors the resources contributed by the miners, never oversells, adopts the mechanism of system pricing, automatic value-added every year and automatic growth of de-duplication coefficient to ensure stable and value-added resources, which is a very good stable currency. The price of the currency and the exchange rate with the resource token are completely market-oriented, allowing moderate speculation to maintain liquidity, but the slower mining rate corresponds to more and more resource clearance, from the design mechanism it also ensures that it has long-term value.

2.1.6 Decentralized Governance Structure

YottaChain first time proposed an entirely decentralized governance structure. The YottaChain constitution proposed by YottaChain will draw on the theoretical and practical results of human social economics and political science, and creating a parallel world of

democratic checks and balances, transparency and automation, balancing fairness and efficiency.

The execution of YottaChain Constitution and Rules is implemented by code. The exact expression of “Code is law” should be “Law is implemented by code”. Ensuring that the new developed code perfectly implement the established rules is one of the key point of the YottaChain governance structure.

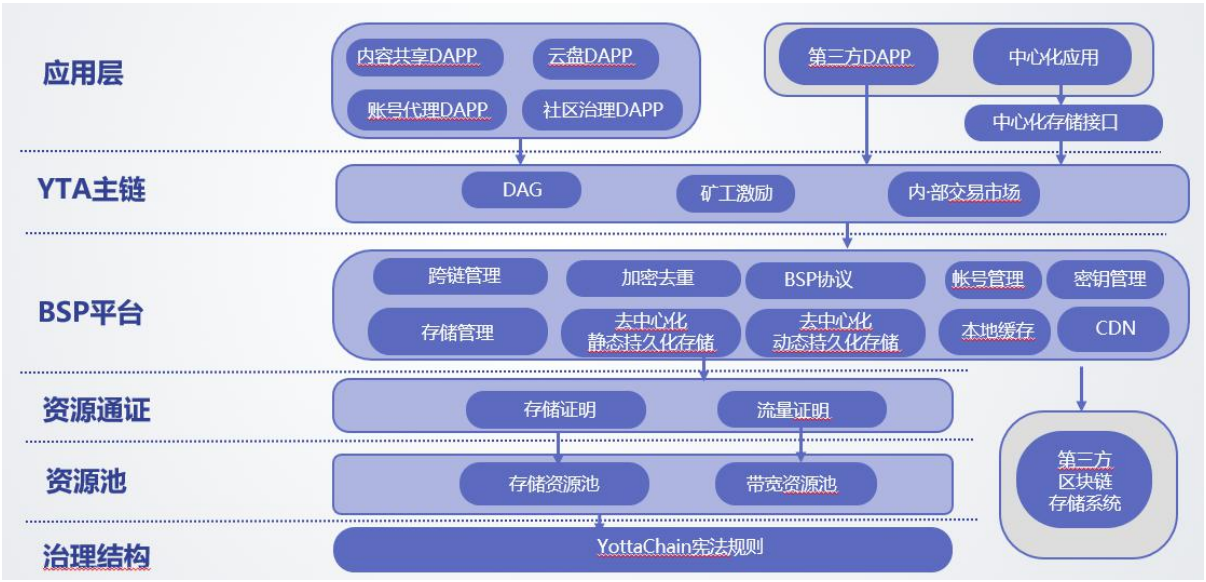
2.1.7 Other Important Improvements

In addition to storage service services, YottaChain also comes with four DAPPs: content sharing, cloud disk, account agent and account proxy DAPP. These four DAPPs not only demonstrate the application on YottaChain, but also play a role for running and operating and promotion of YottaChain. Content sharing DAPP can expand the scale of YottaChain by means of content marketing; Cloud storage DAPP is helpful for consumer user; The account agent DAPP provides the account system with different levels of security and convenience, and can be connected with other account systems (such as bank’sU-key and enterprise employee identity), allowing users to log in at a single point. Community Governance DAPP achieves a complete decentralized community governance (see Sections 2.1.7 and 8), making YottaChain a true community autonomy public chain that can attract eco-related parties to join.

YottaChain divides nodes into commercial nodes and ordinary nodes. There are certain threshold requirements for commercial nodes, such as 7x24 hours online, node size, performance, reliability, stability and behavioral specifications to meet basic requirements. Storage and computing servicesare provided by commercial nodes to guarantee the reliability and stability of services. For ordinary nodes, the threshold should be as low as possible to ensure universality.

YottaChain divides users into individual users, family users, and enterprise users, providing an authorization management mechanism for enterprise users and a transparent mechanism for family users.

2.2. YottaChain System Structure



As shown in picture, the YottaChain commercial node consists of six layers. The blue bottom is what YottaChain itself wants to achieve, and the gray bottom is a third-party system that incorporates the YottaChain ecosystem.

The bottom layer is the YottaChain Constitution Client, providing code-based governance rules for the entire system.

Resource pools are various types of resources that miners use for mining, including storage resource pools such as hard disks, flash memory, and memory, and bandwidth resource pools.

The resource token-through layer is a mechanism for issuing resource certificates after tokenizing all kinds of resources, and can verify whether the miners actually provide the corresponding types of resources. For the storage resource, the storage certificate (the equivalent form of the FileCoin PoSt algorithm) mechanism is used to issue the resource token of the storage class, and the traffic certificate mechanism for the bandwidth resource is used.

The BSP open platform provides core technology enabling for each blockchain storage system and provides various storage services for upper-layer applications, including critical encryption and de-duplication technologies, decentralized static persistent storage, decentralized dynamic persistent storage, and local Storage functions such as caching, CDN, storage management, cross-chain scheduling, and other data security mechanisms such as account management and key management. All of this is open to all blockchain storage systems and upper-layer applications through the BSP blockchain storage protocol.

Decentralized static persistent storage is suitable for storing static data. The stored data adopts the data reliability guarantee mechanism as described in 2.1.2, and the reliability is much higher than the best centralized storage, which is accessed by the hash value of the data;

Data reliability for decentralized dynamic storage is similar to decentralized static storage, but needs to be accessed by ID. The ID of a file does not change regardless of how much content changes. For the same ID file, the new content will overwrite the old content;

The local cache uses local storage resources and has high performance but cannot be used for persistent storage;

CDN is suitable for network acceleration, only saves the most popular content, and returns the content without hits;

The storage management automatically allocates the storage resources occupied by each storage service according to the market supply and demand situation to ensure the maximum benefit of the miners and the interests of the users, and repeats according to the market conditions of the resource token and the third-party blockchain storage system and the current average data. Rates and tax automatically calculate quotes for each storage service.

Cross-chain scheduling allocates storage traffic according to user requirements, evaluates the reliability of each storage system, and manages cross-chain storage as much as possible under the premise

of user license, to isolate the fault domain to the greatest extent, improve system redundancy, and improve data reliability.

The data security mechanism is based on the TruPrivacy technology, includes encryption and key management for the persistently stored data, ensuring that only the owner of the data and its grantee can access the data, and no one else can see the data. Furthermore, the read and write access can be separately licensed.

The BSP protocol module connects the blockchain storage systems through the standard BSP protocol, and if necessary, digital currency exchange (for example, YTA exchange FIL for purchasing FileCoin storage space);

The YTA main chain implements the DAG-based blockchain system, and implements incentives for miners through the POR consensus algorithm (see Section 3.3), and provides YTA two-way exchange of various resource tokens and users to use the resource token to purchase various storage services or Calculate the internal trading market for the service.

YottaChain provides four demonstration DAPP applications for content sharing, cloud disk, account proxy and community governance. These four applications are also the basic and general requirements for individuals and businesses to use YottaChain. Third parties can develop standalone DAPP applications based on YottaChain. In particular, YottaChain provides storage interfaces

such as block storage, NAS storage and docking storage compatible with centralized storage through a centralized storage interface module, and corresponding storage management functions, so that existing centralized storage applications can be modified without using code. Compiled binary compatible for seamless migration to blockchain storage.

2.3 BSP protocol and BSP open platform

YottaChain's unique core technology, which plays a decisive role in the blockchain storage, is opened by the BSP (Blockchain Storage Protocol) protocol. The BSP protocol is used to build an open platform for the entire blockchain storage industry, called the BSP open platform. .

A blockchain storage system, through the docking BSP protocol, can enjoy all the functions of the BSP open platform, including encryption and deduplication and other exclusive technologies that play a decisive role in blockchain storage, directly bringing market benefits to the centralized application. Seamless docking, including very professional various types of storage services, professional key management and account management functions. In addition, all blockchain storage systems running on the BSP open platform can share the "deduplication" bonus and get a storage amplification factor much larger than itself (this is because the more users, the more data

The higher the magnification factor, so you can sell more data storage space and earn more than a few times.

Whether it is YottaChain's own storage system or a third-party blockchain storage system, it is the same for the BSP open platform, which can be verified by open source code. And as a public chain of complete decentralized governance, YottaChain's functional definition, algorithm, code implementation and deployment are all open and transparent, community-autonomous, third-party blockchain storage systems can even run through the election of YottaChain community governance the committee is involved in management.

Calling the BSP open platform requires a certain amount of YTA, but the number is very small, which is equivalent to the need for various ERC20 tokens to consume a certain ETH as a Gas on the Ethereum platform. Compared with the benefits brought by the BSP open platform, the proportion is very low, so as to achieve the goal of common development of ecological common development. The specific scale factor is set by the Community Governance Committee before the main chain goes online.

3. THE TOKEN DESIGN

3.1 Overview

In order to ensure that stability of the value of token and also provide a market-based mechanism to facilitate the discovery of prices through market, YottaChain uses double layers token model. One of them is a single market-based cryptocurrency and the other is many kinds of asset backed tokens.

The cryptocurrency of YottaChain is YottaCoin, its symbol is YTA. YTA is the system equity currency, mainly used for trading on the major exchanges.

YottaChain issues a type of token for each kind of resource (such as hard disk storage resources, bandwidth resources, x86 CPU virtual machine resources), YottaChain provides trading services among different types of resource tokens by the internal exchange.The transaction price between each resource token and YTA is determined entirely by the market's fluctuation.

YottaChain miners contribute resources to mine and obtain the corresponding tokens and then convert it into YTA. Users who need to use the resources in the YottaChain system purchase YTA, which is then converted into corresponding resource tokens to purchase the corresponding resources.

3.2 Resource Token

YottaChain issues a kind of token for each type of resource, called Resource Token. For example, hard disk storage resources, flash

storage resources, memory storage resources, and bandwidth resource four types of resource tokens are issued separately. The number of resource token issued will be decided by the Community Governance Committee.

The circulation of all resource tokens depends on the amount of resources of this type contributed by the miners. The more resources miners contribute for mining, the greater the amount of resources token are issued. The resource token will not exceeds the amount of correspond resource. The ratio between the amount of resource tokens and the amount of resources used for mining is relatively fixed, however, the difficulty of mining is increased by 50% every year, so that the earlier miners can get more resource tokens with the same amount of resources. The ratio is also much higher than the price reduction of hardware, ensuring the possession of resources. Users have good value-added benefits.

For resource users, you can use the resource token to purchase the corresponding resources. Due to factors such as data de-duplication and CPU virtualization, the amount of resources available to users is many times the amount of resources contributed by miners, which greatly reduces the cost of purchasing resources and also constitutes anmagic economic model for everyone.

The following is an example of static persistent hard disk storage to illustrate the resource token mechanism of YottaChain. Assume that

the token for static persistent hard disk storage resource is YTA-HDD (the specific name is finalized by the Community Governance Committee when the token is created). In the first year of the main chain online, a miner can get 1YTA-HDD by storing 1GB data from YottaChain for 1 year, get same 1YTA-HDD by storing 1.5GB data for 1 year in 2nd year, get same 1YTA-HDD by storing 2.25GB data for 1 year, and so on, with a constant increase of 50% per year.

If you do not consider the data de-duplication factor, then 1GB of data storage requires about 2.95 (that is, $1+1/1.5+1/1.5^2...+1/1.5^9$) SPH for 10 years. But with the addition of data de-duplication to the factors a very special model will be produced.

According to our research, the average data repetition rate of a medium-sized cloud storage application is about 3 times, and the average data repetition rate of a large cloud storage application is about 5 times. The more people use the data,the larger the data volume, the higher the repetition rate is. So we can estimate the average repetition rate of YottaChain is about 7-10 times. In other words, if the entire system stores 1 EB of data, the actual physical storage space is between 100PB and 200PB. Considering that data storage also requires redundant coding, we illustrate with a 5x average repetition rate (this is the number after counting the data redundancy rate caused by redundant coding).

In the case of a 5x average repetition rate, 1GB of data requires only 0.2GB of space on average. Even with the transaction cost, only about 0.6YTA-HDD is needed to buy 1GB of data for 10 years of storage. This creates a magical stimulating effect: if a user have 1GB of hard disk space for self-use, he can store 1GB of data, but if used for mining, he can get 1 YTA-HDD by contributing same space to store data for others for one year, and then use 0.6YTA-HDD to buy 1GB of data for 10 years of storage service, and 0.4YTA-HDD still left in hand. This will not only help others, but user himself will get benefit from it.This model is sustainable for infinite time. The system operators not only do not subsidize but also can collect tax from transactions for long-term ecosystem construction, which fully reflects the superiority of the blockchain model.

After a miner contributes resources to mine and obtains YTA-HDD, he can handle these YTA-HDDs as follows:

1. Use these YTA-HDDs to buy more space to store his own data.
2. Convert YTA-HDD to other resource token (via YTA as an intermediary) and purchase other type of resources (such as CPU resources)
3. Hold YTA-HDD and wait for 50% of the annual value added
4. Convert to YTA and redeem it into legal currency.

5. Convert to YTA and hold YTA, Exchange into YTA, hold YTA, through voting or election participate in YottaChain community governance

The above is an example of YTA-HDD. No matter what kind of resource token, its value is directly related to the corresponding resources, to ensure that the corresponding resources can be purchased, and never have to worry about the price falling to zero, but it will not increase the value by ten times in the short term, which ensures a long-term stable value-added. As time goes by, its purchasing power is getting stronger and stronger.

3.3 Crypto-currency

3.3.1 YTA Overview

YTA is the crypto-currency traded on major exchanges and an intermediary for the exchange of various resource tokens within the YottaChain system. All resource tokens can be exchanged freely with YTA within the YottaChain system, and transfers between different accounts are not allowed except for YTA exchange. while the exchange rate between Resource Pass and YTA is floating and entirely determined by the market. When the demand for purchasing a certain resource token is greater than the quantity for selling the resource token, when the demand exceeds supply, the price of the resource token will rise, and vice versa. A similar situation exists

between different types of resource tokens. When a resource is surplus and another resource is shortage, the exchange rate between the two (via YTA) will also change.

The value of the resource token is relatively stable, but since the exchange rate of YTA and the resource token is floating, the value of YTA is also floating. But the price of YTA is positively correlated with the exchange rate of YTA resource token, In other words, the more resources that YTA can buy, the greater its value and the price will increase as the value increases.

3.3.2 Issue quantity and lock position

YTA initially issued 4 billion, allocated in three parts:

- The founding team allocated 1.5 billion YTA
- YottaChain Foundation allocates 1.2 billion YTA
- Investors allocate 1.3 billion YTA

In front of the YottaChain main online line, YTA will use the ERC20 smart contract in Taifang to go online, and the YottaChain main online line will map YTA's ERC20 token to the main network through mapping.

After YottaChain's main online line, an additional YTA is added each year to reward the nodes of the book keeping. As time goes on, the

price of the coins is getting higher and higher (see section 3.5). The number of additional issuance is less and less, and the cumulative number is less than 1 billion, that is, YTA issuance. The total amount does not exceed 5 billion.

The first exchange transaction on YTA's ERC20 token is recorded as the token listing date.

Team lockout: unlock 20% before the listing of the token (used to pay employees for the purpose of paying), starting from the listing date of the token, unlocking 20% every 6 months, all unlocked in 24 months.

YottaChain Foundation Locks: 20% unlocked before the listing of the token (for hiring consultants, marketing, community operations, etc.), starting from the listing date of the token, unlocking 20% every 3 months, unlocking all 12 months.

Investor locks the warehouse: unlock 20% before the token is listed. Starting from the listing date of the token, unlock 20% every month and unlock all 4 months. For strategic investors with high investment quotas, the same lock-up period as the team or foundation is used.

The YottaChain team has developed a smart contract for YTA automatic lockouts, which are enforced through smart contracts.

3.3.3 Consensus mechanism and mining rate

YTA adopts the DPOS consensus mechanism, and sends a certain YTA to the nodes for accounting every year, including 21 super nodes and no more than 100 standby nodes.

The mining rate within 60 years after online of YTA is shown in the following table:

Time interval	Mining rate	Mining amount during the period	Turnover at the end of the period
1st year	100 million/year	1 billion	4.1 billion
2nd year	900 million/year	900 million	41.9 billion
3rd year	800 million/year	800 million	4.27 billion
4th year	700 million/year	700 million	43.4 billion
5th-6th year	600 million/year	120 million	4.46 billion
7th-8th year	500 million	1 billion	45.6 billion
9th-10th year	400 million	800 million	46.4 billion
11th-12th year	300 million	600 million	47 billion
13th-15th year	200 million	600 million	47.6 billion
16th-18th year	100 million	300 million	47.9 billion
19th-21st year	99 million	27 million	48.17 billion
22nd- 24th year	8 million	24 million	48.41 billion
25th-28th year	7 million	28 million	48.69 billion
29th-32ndyear	6 million	24 million	48.93 billion
33rd-37th year	5 million	25 million	49.18 billion
38th-42nd year	4 million	20 million	49.38 billion
43rd-47th year	3 million	15 million	49.53 billion

48th-52st year	2 million	10 million	49.63 billion
53rd-57th year	1 million	5 million	49.68 billion
58th-62nd year	9,00,000	4.5 million	49.725 billion

3.4 Economic Model

The number of issued resource tokens is related to the amount of resources contributed by miners and the total amount of data actually stored by users. Specifically, for each new miner at YottaChain, YottaChain has issued a small amount of storage resources to purchase its storage space as inventory. When the space is purchased and saved by the end user, the system will issue a new resource token. The miner buys space until the miner's space is filled by data.

The reason why we must design a certain system inventory is because when the main chain is just started, there is no user to purchase storage space and other resources, the miners have no resource tokens. At this time, there is no resource circulation in the trading market. Users can't use YTA in exchange for resource tokens. In order to break this strange circle, YottaChain took the system to purchase part of the inventory to solve the problem, that is, the system pre-purchased some storage space and other resources to all miners as inventory sold to the user (the size of the inventory is determined by the Community Governance Committee), so that the miners With partial resource clearance, users can switch to resource token with YTA, and the entire economic system will be operational.

Even with the addition of stocks, the amount of resource tokens issued by YottaChain is lower than the total amount of resources owned by the miners, so that users can always buy the corresponding storage space through the resource token.

The price at which the user purchases the storage computing service using the resource token is uniformly priced by the system, and the system calculates the price in real time according to the amount of resources consumed by the service plus the appropriate tax. Take the persistent storage service as an example, the unit price is (1 + tax rate) / (digging difficulty * average de-duplication coefficient), As the difficulty of mining is increasing year by year, the de-duplication coefficient is also increasing gradually with the increase of the number of users and the amount of data. The mechanism guarantees the relative stability of the price, the storage space that the same amount of resources can be purchased is steadily rising (that is, the price of the unit storage space is steadily decreasing), which is beneficial to the user. A stable expectation of the purchase price is conducive to the budget management of the user unit, and the community can also receive appropriate tax guarantees to ensure that the community has sufficient resources to continue to develop. The tax rate is stipulated by the Community Governance Committee, and the ratio will be much smaller than the income that the user receives.

Through the above mechanism is designed to enable miners make money constantly, and allow users to purchase storage and computing services at a stable and low price.

From the economic model, YottaChain storage provides the quality of far beyond centralized storage (data reliability, disaster tolerance, anti-DDos), and the cost is greatly reduced, thus forming a source of profit space for miners and users.

Relative to centralized storage, the cost reduction of YottaChain storage lies in the following factors:

- YottaChain adopts TruPrivacy technology, which can safely realize data deduplication, and reduce hard disk space occupied by the same data by 5-10 times.
- Most storage nodes have very few storage devices and do not require a dedicated cooling system (which accounts for one-third or even half of the data center's power consumption). It can be cooled by natural ventilation, and both CapEx and OpEx are greatly reduced.
- Home storage mining machine does not need to spend extra bandwidth, no need to pay rental costs. Household electricity is also cheaper than industrial electricity.
- YottaChain’s most storage nodes do not require professional operation and maintenance engineers to be on site. Each node is

automatically operated and other nodes are automatically placed in the event of an unexpected failure, saving expensive operation and maintenance costs.

- YottaChain massive storage nodes are using idle hard disk space, belonging to sunk cost, marginal cost is close to zero.

3.5 Stability and mobility

The amount of issued token of YottaChain's own resource token is strictly equal to the amount of resources contributed by miners. It is never over issued, the value of resource token is relatively stable and there is 50% automatic value-added every year. After offsetting the decline in hardware costs, there is still a considerable steady return. It is suitable for users who need to use the corresponding resources, also suitable for risk-averse conservative investors. It has a higher yield than the wealth management fund and is a very reliable and stable digital currency.

YTA is not directly anchored to the physical resources. The value of the YTA can be adjusted by adjusting the exchange rate between YTA and the resource token. In the short run, this mechanism can provide more speculation, but it can also guarantee value increasing in the long run. This is because YTA's mining rate is relatively constant (except for the small amount of YTA newly issued by the rewarding billing node every year). As time goes on, the amount of

resource tokens is more and more while the resources in the system are increasing. The resource corresponded to each YTA is increasing and its value will increase accordingly. Therefore, the price of YTA is affected by factors such as supply and demand, market manipulation and speculation, but in the long term it must be greatly increase, and there is never a risk of becoming to zero.

In order to ensure the liquidity of the two-way transaction between YTA and Resource token, the YottaChain Foundation will conduct the internal transaction in the city if necessary, and ensure that the resource token obtained by the miner can be exchanged for YTA. After the user purchases YTA, it can be replaced with the resource. token. The YottaChain Foundation can do this by leveraging the mastery of YTA and the resource token for collecting transaction fees.

3.6 blockchain storage ecosystem

For the blockchain storage that joins the BSP open platform, the currency issued is equivalent to a resource token of YottaChain, and has a certain exchange rate relationship with YTA. The resource adjustment between each other is carried out through YTA as an intermediary.

For IPFS or other large blockchain storage systems, a bench marking system that conforms to the YottaChain platform protocol can be

developed, and the corresponding resource token is issued on YottaChain. The resource token and the digital currency of the bench marked system are side chained. 1:1 anchor.

Through the above method, a huge blockchain storage ecosystem can be formed on YottaChain, including all the blockchain storage systems on the market.

4. YOTTACHAIN ACCOUNT MANAGEMENT

4.1. Overview

Other blockchain applications often use public keys or their variants to uniquely identify users, but their readability is not strong. Use a more readable account name in YottaChain to uniquely identify the user. The account name consists of 10-32 characters. The account is associated with the user's YTA account balance, in addition to the user's public and private key pairs, and the routing information in the P2P network.

4.2 Account Creation

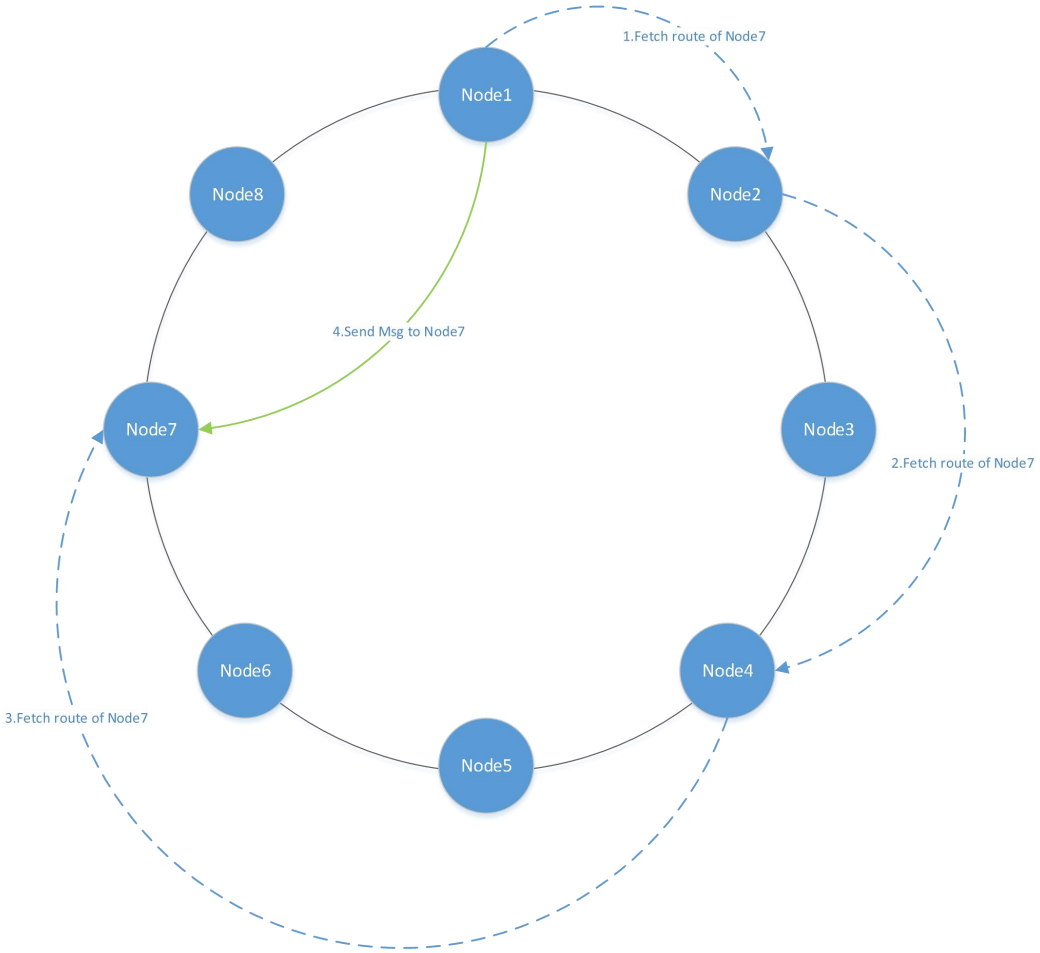
The account is created by the YottaChain account proxy service. The account proxy service canberun on aordinary node (only the account used by the local user is managed), or it canberun on the commercial node (the service is provided to the public). When creating an account, the user needs to provide the YottaChain global unique

account name, three pairs of random public and private key (a pair of login keys, a pair of signature keys, a pair of encryption keys) will be automatically generated, and then save the account name and public keys to YottaChain. The backbone network is not responsible for keeping the private keys, the account proxy application is. For the account password login method, the private keys can be encrypted by password and saved to the account proxy's storage area, such as the persistent storage layer of YottaChain. When the user logs in for the next time, the account proxy application will verify the password and then use the password to decrypt the private keys, then connect to any commercial node, use the challenge response method to verify, and prove that it owns the login private key without showing the private key.

4.3. Message Mechanism

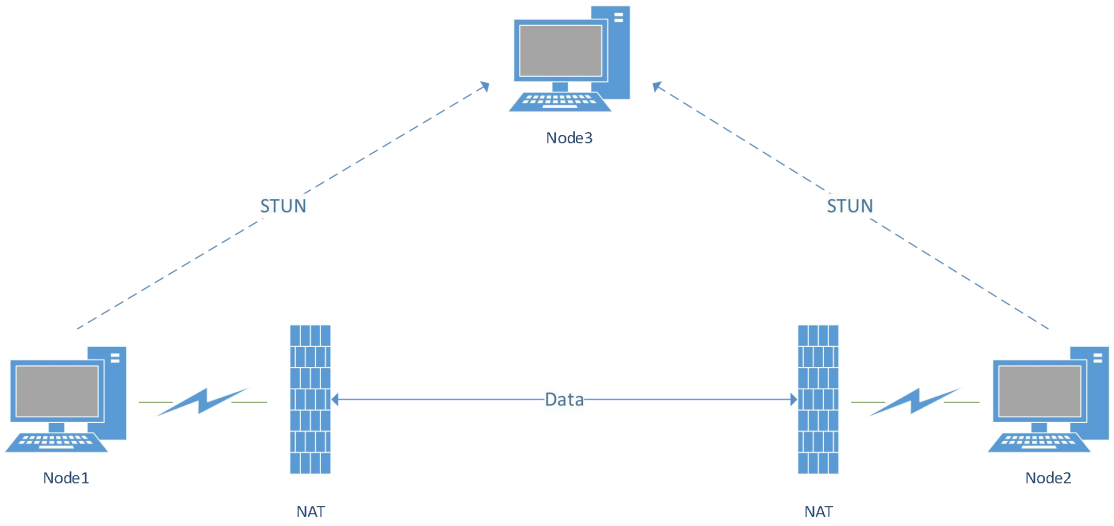
The account can send structured messages to other accounts, and the messages are divided into predefined messages and user-defined messages. Predefined messages are handled by the internal mechanisms of the YTA node (such as messages sharing files), and custom messages can be processed by user-defined processor code. The message is routed between Kademlia DHT networks based on YTA nodes, and the routing information is stored in the global routing table in the DHT network. Due to Kademlia's query efficiency, the average complexity of a route query is log2 (n), where

n is the number of YottaChain nodes. In the following figure, the whole process of sending a message from node 1 to node 7, node 1 queries the nearest node of node 7 in the local routing table, and obtains node 2, which forwards the message to node 4 according to the same rule, and finally arrives. Node 7, node 7 returns its own address to node 1 through the previous node, and finally node 1 and node 7 establish a connection and exchange information.



Due to the prevalence of NAT devices in the Internet, NAT penetration technology is an important technical support for P2P networks. YottaChain uses the ICE NAT traversal framework to ensure that YottaChain nodes can be properly connected to each other

behind various types of NAT devices. The following figure shows how the YottaChain nodes are connected in the presence of NAT.



Node 3 is a YottaChain node located on the public network. Node 1 and Node 2 are both located behind the NAT device. Node 1 wants to communicate with Node 2. With the help of Node 3, the STUN protocol is used to exchange the address and port information mapped to the public network. And use this information to make a hole in the NAT device. After the hole is successfully created, node 1 and node 2 can directly establish a connection and exchange data. If the hole fails, the communication between node 1 and node 2 needs to be utilized by node 3 through the TURN protocol.

4.4. Group Management-

The YottaChain account system defines group, which is similar to the user group in the Linux operating system. Each user can create multiple groups, and the default group of a new account is “Everyone”.

Each group simultaneously generates a public-private key pair corresponding to the group for file sharing in the group. The group information and the group public key are stored in the YottaChain blockchain, and the group private key is stored in the proxy application layer of the group creator, and the group member information is stored in a distributed form in the DHT network for easy searching.

When other accounts want to join the group, they request the group private key from the group creator, and write the account and group correspondence into the DHT network.

4.5. Authority Mechanism

Access to data is controlled by keys. Each data has its own unique encryption key to ensure different data using different encryption key. So that data is encrypted with a randomly generated symmetric key (the role of the random key is to ensure that the key is unknown to anyone), and the key is called the storage encryption key for the data. People who have access right to this data use their encryption public key to encrypt the storage encryption key, which is then stored in the YottaChain system area. Later, when the user needs to access the data, the storage encryption key is decrypted with user's own encryption private key, and then data can be decrypted to obtain the data plain text. The data shared to the group is also a similar mechanism, just use the group key instead of the aforementioned user keys, and the

user belonging to the group can obtain the private key of the group by encrypting the group private key with the user's encryption public key and saving the encrypted key. When the user wants to access the file, the user can decrypt the said encrypted key with his encryption private key to obtain the group private key, and then can access all data that the group owns access rights. The same mechanism is used for data shared to Everyone, and Everyone is defined as a special group set by the system (all users automatically join the group when creating an account).

For dynamic storage, write permissions should be limited, otherwise anyone can go and modify other user's files, which will cause confusion. The mechanism is as follows: When creating dynamic persistent storage data, a pair of public and private keys are randomly generated, which are called write permission private key and write permission public key. Only the user who owns the write permission private key has the right to write/ modify the data. To verify this, the write permission public key is saved as meta data for the data. When modifying the data, the new data must be signed with the write permission private key. All nodes that store a fragment of the data must use the write permission public key to verify the signature when accepting the write request and the data is modified only after the verification is OK.

5. YOTTACHAIN STORAGE SYSTEM

5.1. File Security

5.1.1 Requirements

From the perspective of user requirements, when a user selects a storage medium to store their own files, it is desirable that their files are kept secret, rather than fully public. The storage system itself should embed data protection mechanism for the files it stores. From the perspective of social needs, there should also be means to block contents that promote extreme violations of human society, such as extreme terrorism.

5.1.2 Problems

Currently, the unique index identifier Hash of the file in the IPFS storage network can be obtained by the Get (Hash) method, and no authentication is required, and the file is difficult to be destroyed. It neither meet individual needs nor meet social needs.

5.1.3. Solution

YottaChain encrypts the file and upload it at data source side. Before the file enters the DSN (Distributed Storage Network), it is already encrypted, and other people can't decrypt it except the owner or its grantee.

5.2. Encrypt DSN

Encrypted DSN protocol:

Before Put data, the storage encryption key (St_k) of the file is randomly generated, the file is encrypted by St_k, the storage encryption key is encrypted by the user's encryption public key, and the Hash of the plaintext and ciphertext is separately calculated, stores ciphertext, the encrypted storage encryption key, the plaintext Hash, and the ciphertext Hash.

1.Hash(Data)→H_{data} Calculate plaintext hash

2.RandomSym()→St_k randomly generates a symmetric key as the storage encryption key of the file.

3.Enc(St_k, Data)→EncData Encrypts the file with the storage encryption key.

4.Hash(EncData) →H_{enc} Calculate ciphertext Hash

5.Enc(S_{pub}, St_k) →$EncSt_k$ Encrypts the storage encryption key with the user's encryption public key

6.PutIPFS (EncData) stores encrypted data to IPFS

7.PutPri (H_{data}, H_{enc}, $EncSt_k$) The encrypted storage encryption key, ciphertext Hash is stored in the user permission list, recorded under the plaintext Hash item.

When Get data, the corresponding ciphertext hash is extracted through the plaintext hash, and the ciphertext and the encrypted

storage encryption key are extracted from the IPFS through the ciphertext hash, and the encrypted storage encryption key is decrypted by the user's encryption private key. The key is stored, and the encrypted data is decrypted by the storage encryption key to obtain the plaintext of the data.

1.GetPri(H_{data})→H_{enc}, EncStk Get the ciphertext hash and encrypted storage encryption key from the permission list through plaintext hash

2. GetIPFS(Henc)→EncData Use ciphertext hash to retrieve ciphertext from IPFS

3.Dec(Sprv, EncStk)→Stk decrypts the encrypted storage encryption key with the user's encryption private key to obtain the storage encryption key.

4.Dec(Stk, EncData)→Data decrypts to obtain plaintext

The optimized DSN solution effectively guarantees the security of the data.

Security: Only the ciphertext appears outside the data source. Only the user's encryption private key can be used to obtain the plaintext of the data. Users don't need to worry about the data being compromised if they keep their own encryption private key securely.

Integrity: The data D corresponding to Hash will not get D1 through Get(hash), where D1≠D.

Data recoverability: Put data D successfully, there must be a successful Get request to get the data.

The above solution cannot solve the problem of data de-duplication. Traditionally, it has been recognized in the industry that encryption cannot be de-duplicated. If the server side wants ZeroKnowledge, repeated data can only be saved repeatedly because the same data becomes different after encryption. This is why all large cloud storage service providers do not provide ZeroKnowledge storage, and IPFS simply does not provide encryption.

YottaChain provides a special mechanism to prevent the storage of duplicate data while ensuring the same security, breaking the industry's "common sense" to have the cake and eat it too.Within this mechanism, in addition to the user permission table, maintain a global metadata table, record the correspondence between plaintext hash and ciphertext hash, and first query whether there is data of the same hash when writing data, if not Re-save the item:

Hash(Data) →Hdata Calculate plaintext hash

If CheckDup(H_{data}) = TRUE goto 11 If the same data already exists, go to step 11

RandomSym()→St_k randomly generates a symmetric key as the storage encryption key of the file.

Enc(St_k, Data)→EncData Encrypts the file with the storage encryption key

Hash(EncData) →H_{enc} Calculate ciphertext Hash

GenKey(Data)→S_{data} Generates a symmetric key from the plaintext of the data, which can be generated by calculating the hash value after the data is plaintext plus salt. The reason why salt is added is because the plaintext Hash is a public value, without the salt those who do not have the data can obtain the key. To ensure consistency, the salt value can be a fixed value.

Enc(HData, Stk) →EncStk' Encrypts the storage encryption key with the symmetric key generated in plain text. This is a very strange step. The plaintext is used as the key and the key is encrypted as plaintext. Most people would think that this formula has a typo, reverses key & plaintext by mistake. In fact, it is designed specifically, and this step is the core step of TruPrivacy.

PutIPFS (EncData) saves encrypted data to IPFS

PutMeta(Hdata, Henv, EncStk)records the ciphertext hash and plaintext encrypted storage encryption keys in the global metadata table, recorded under the plaintext Hash

Goto 14

GetMeta(H_{data}) →H_{env}, $EncSt_k$' to retrieve plaintext encrypted storage encryption key from the global metadata table

GenKey(Data) →S_{data} generates symmetric key from data plaintext according to same algorithm

Dec(S_{data}, $EncSt_k$') →St_k Decrypts plaintext encrypted storage encryption key to obtain storage encryption key

Enc(S_{pub}, St_k) →$EncSt_k$ Encrypts the storage encryption key with the user's encryption public key

PutPri(H_{data}， $EncSt_k$) stores the encrypted key from last step into the user permission list, recorded under the plaintext hash item.

When getting the data, the corresponding ciphertext Hash is extracted from the plaintext hash item of the global metadata table, the ciphertext is retrieved from the IPFS through the ciphertext hash; the encrypted storage encryption key is retrieved from permission list and decrypted by the user's encryption private key. The encrypted data is decrypted by the storage encryption key to obtain the plaintext of the data.

GetMeta(H_{data})→H_{enc}

Get ciphertext Hash by plaintext Hash from the global metadata table

GetPri(H_{data})→$EncSt_k$

Get encrypted storage encryption key by plaintext Hash from the permission list

GetIPFS(H_{enc})→EncData

Get ciphertext by ciphertext Hash from IPFS

Dec（S_{prv}, $EncSt_k$）→St_k

Decode the encrypted storage encryption key by the user's encryption private key.

Dec(St_k, EncData)→Data

Decode the cyphertext to get the plaintext.

The optimized DSN scheme can not only guarantee the security of data effectively, but also achieves encryption and de-duplication at same time.

In order to achieve a better de-duplication effect, the data can be divided into fixed length blocks and each block can be de-duplicated separately.

The above scheme can only be used to store static data. When storing dynamic data, not only the data identification should be ID which is changeless instead of Hash, but also writing permission validation is needed to prevent data from being overridden and tampered with by others.

The creation process is as follows:

RandomAsym()→Sw_{pub} ,Sw_{prv}To generate asymmetric key randomly as the writing permission key

Create(Sw_{pub}) →ID To create a dynamic data and get a unique ID, then record the corresponding writing permission public key under that ID item

RandomSym()→St_kTo generate symmetric key randomly as storage encryption key

Enc(S_{pub}, St_k) →$EncSt_k$ To encrypt the storage encryption key with the user's encryption public key

PutPri(ID，$EncSt_k$)To store the encrypted storage encryption key into the user permission list under ID item.

The process for writing data is as follows:

GetPri(ID) →$EncSt_k$

To extract the encrypted storage encryption key from the user permission list

Dec（S_{prv}, $EncSt_k$）→St_k

To decode the encrypted storage encryption key by the user's encryption private key.

Enc(St_k, Data)→EncData To encrypt data with storage encryption keys.

Hash(EncData) →Henc To calculate ciphertext Hash

Enc(Swprv, H_{enc}) →$EncH_{enc}$ To sign ciphertext Hash with writing permission public keys of that ID.

PutDyn(ID, EncData, $EncH_{enc}$)

To write the dynamic ciphertext, the signature represents the writing authorization.

Whilewriting dynamic data by node which stores fragment of dynamic data, verification and permissions need to be done first.

GetKey(ID) →Sw_{pub}

to get the writing permission public key of ID

Hash(EncData) →H_{enc}

To calculate ciphertext Hash

If Dec（Sw_{pub}, $EncH_{enc}$）= H_{enc}Write(ID, EncData)

If the signature is verified, data can be written.

The reading process of dynamic data is as follows:

GetPri(ID)→$EncSt_k$

To extract the encrypted storage encryption key through the ID from the user permission list

GetDyn (ID)→EncData

To read ciphertext from dynamic data storage area with ID

Dec（S_{prv}, $EncSt_k$）→St_kTo decode the encrypted storage encryption key by the user's encryption private key.

Dec(St_k, EncData)→Data To decoded data.

5.3.Byzantine Fault Tolerance

The main background of the Byzantine general problem was： The Byzantine Roman Empire was vast. The armies were far apart, so communication between them could only be made by messenger. Furthermore, any strategic deployment needs to be unified before it can be carried out. If there is an untrustworthy general or messenger in the army, it will disrupt the war plan and fail to reach an agreement. Because with the known presence of rebels, how to reach a consensus becomes a question for Byzantine generals

A storage malfunction is called a Byzantine malfunction, that is to say dishonest and unreliable miners lose their data, so the filefails to extract.

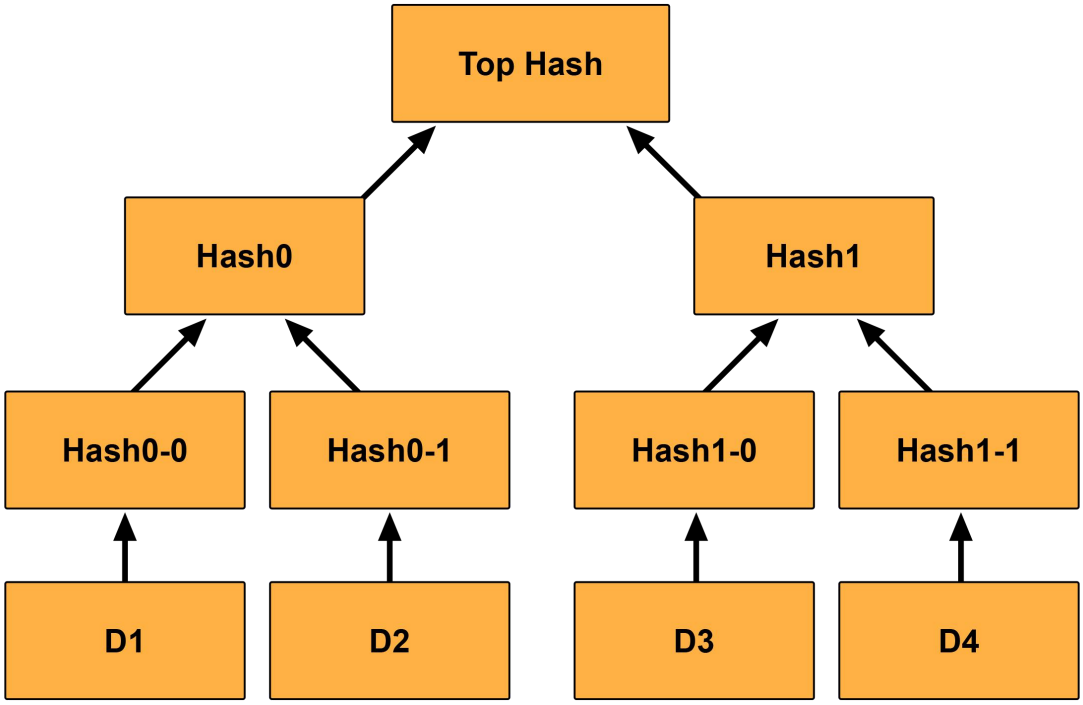
Byzantine fault tolerance scheme: Put(D,n,m), When the data is uploaded, using redundant code to split data into n segments under condition of allowing max to m segments not available. Specify n nodes to store these segments, so that tolerates m nodes' failure. That is when the number of failure nodes is less than m, the file could survive. Inthis case, new node will be re-selected to store data segment instead broken node through the repair mechanism.

The choice of node n and fault-tolerant node m can be made by the user himself. The system will default to a value, n>3m+1.

5.4. Standard Format File StdFile

With the function of self-description, the related information of the file can be obtained by obtaining the HeadHash of the file.

What is the HeadHash? First, a brief look at the merkel tree.

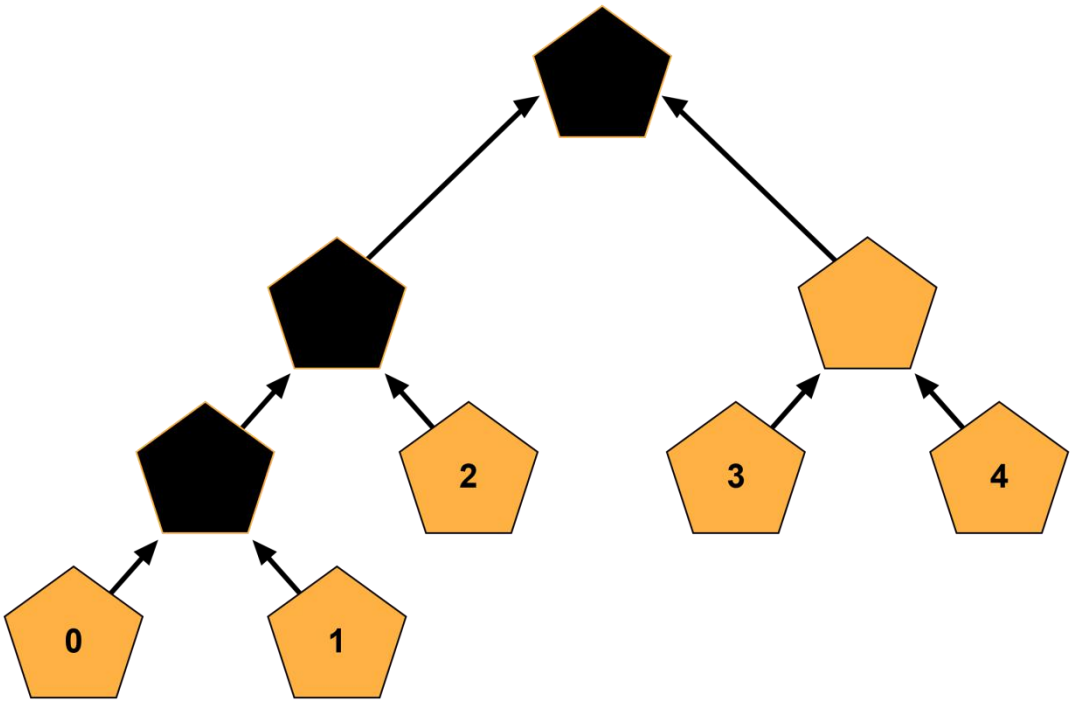


It's a tree structure that shows a Hash list. At the bottom of the tree is a fixed - sized chunk of data except the smallest one on the right side. Each chunk has a Hash that corresponds to it. Two adjacent pieces are combined to a new Hash, until top Hash called Merkle root.

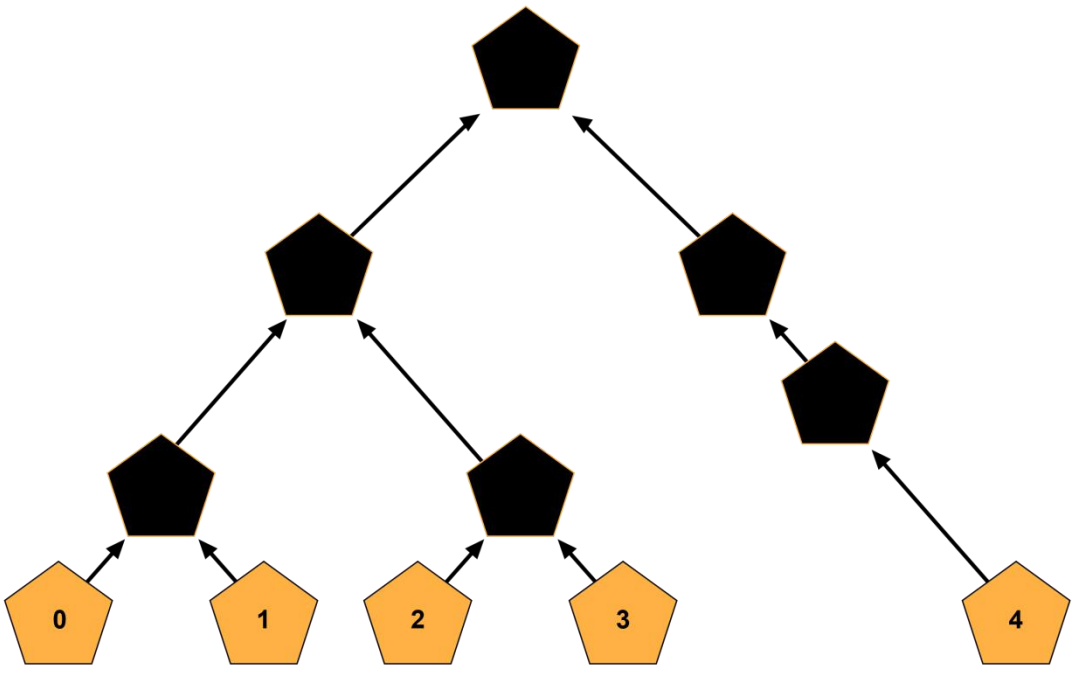
File index: By getting the Hash of the file(top Hash)to obtain the leaf Hash, finally to the smallest piece of data.

Merkle Tree

Merkle Tree insert



The Merkle Tree is changed by inserting a Data Block 0 of a fixed size and a fixed format, but the structural relationship is essentially unchanged. Because the contents of 1,2,3,4,5 data blocks have not changed. The inserted Merkle Tree is:



Here the data block 0 is going to be studied.

Because when getting the file data, 0 could be used as file Head. The data block that is more than 0 could act as the file content Data. The data block 0 is the self-description of the file, which may contain metadata like file encoding format, creation time, file format, filename etc.. Recording these metadata in certain format and use Convert(HeadInfo) to convert them to HeadBlock which is file head information with fixed block size, Stores HeadBlock together with content data.

SFILE: Hash（HeadBlock（Finalsize）+Data）-->Top Hash

It doesn't affect the overall structure of the data in the Merkle Tree, and if the number of bottom data blocks is even, then when block 0 is inserted, orphans are created. But the orphan will be always at the end of the right side.

SFILE file index: to inquire leaf nodes from the Top Hash, when go through to the bottom of the data block, you will always know the first chunk is the head information. It describes the file, but not part of the file content. So it could be ignored when organizing data.

SFILE is designed to create a standard format file with self-describing function, so as to realize some information exchange of the file.

5.5. File Sharing

In a YottaChain system, files are encrypted and stored securely. To get a file, you must have the storage encryption key for the file to be decrypted. For example, user A wants to share his/her files with B, so what A file needs to do is YottaChain.share(EncD, St_k, ObjectB) to share storage encryption key with B. Only when getting storage encryption key St_k, B can declassified encrypted file encD. But there is also a problem. There is a risk of leakage during transmission. Also, in the YottaChain key management system, there is no plaintext storage encryption key St_k, only existing encrypted storage encryption key $EncSt_k$. The exchange of storage encryption key here uses an asymmetric encryption algorithm.

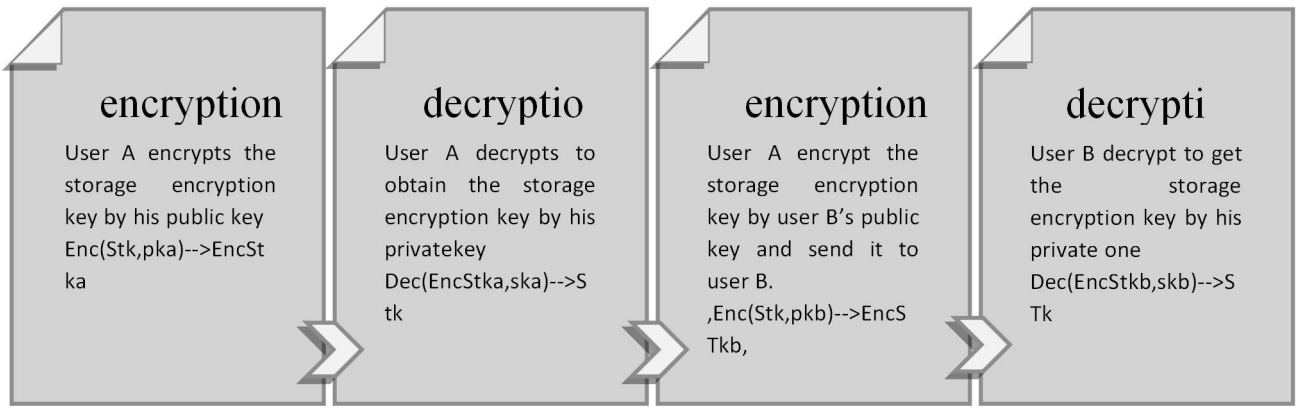
The concrete build process is shown as follows:

pka---A public key of user A

ska---A private key of user A

pkb---B public key of user B

skb---B private key of user B



By message passing mechanisms of account management, user A sends the formatted message

YottaChain.setMes(EncHashD,$EncSt_{kb}$)-->Mes

To user B,

YottaChain.sendMes(A,Mes,B)-->MesID ,

UserB receives the message and uses its own processing script to get the message content.

YottaChain.getMes(MesID)

Then by storage encryption keys encrypted by user B's public keys, user B can get the plaintext storage encryption key by his own private key.

6.YOTTACHAIN STORAGE AND TRADING MARKET

6.1.YottaChain Storage Network

6.1.1. Overview

In the market of traditional centralized storage providers, users choose storage providers and pay for the storage of data. When users need to obtain data, they can get them directly through storage providers. Storage providers do not need to provide users with real-time proof that they are storing their data (it must store user data, and user trusts it). Whena user needs the data, it is always available.

In this market, centralized storage providers are open for users to choose, users can choose the storage providers they trust.

YottaChain is a decentralized storage network, in which users pay to store data in storage certain areas in the YottaChain storage and trading market. Users and storage providers are "anonymous", which requires the storage provider to provide valid proof for the YottaChain network to verify that it is indeed safe to store data.

6.1.2.Requirements

The storage certificate (POS) must be able to prevent three types of attacks: Sybil attack, outsourcing attacks, generation attacks.

Sybil attacks: Malicious miners could pretend to store (and get paid for) more copies than the ones physically stored by creating multiple Sybil identities, but storing the data only once.

Outsourcing Attacks: Malicious miners could commit to store more data than the amount they can physically store, relying on quickly fetching data from other storage providers.

Generation Attacks: Malicious miners could claim to be storing a large amount of data which they are instead efficiently generating on-demand using a small program. If the program is smaller than the purportedly stored data, this inflates the malicious miner’s YTA reward, which is proportional to the miner’s storage currently in use.

6.1.3.Safety-based Replication Proof and Space-time Proof

This part mainly refers to FileCoin'sreplication proof (PoRep) and space-time proof (Post). PoRep has improved PDP and PoR scheme, effectively preventingthree kinds of attacks.

1. SealSealing Operation

Absenteeism storage data by method $Seal^{\tau}_{AES\text{-}256}$ to store data and generate a copy, so that storage absenteeism can honestly store the independent N copies of data D, and make sure that Verifier V has enough time to generate a random validation to challenge R_C.

2. Replication Proof

Definition: replication proof (PoRep) allows storage providers to provide copy(π) to persuade the verifier. When the verifier issues a random challenge, storage providers should be able to provide evidence, proving that the data D relative to the certifier's specific copy R has already been stored in the exclusive physical storage area. This scheme is an interactive protocol.

Three construction phases of replication certificate (PoRep) :

PoRep.setup() -->Copy R, copy of the Hash tree roots, Merkel root of R, encapsulation proof πSEAL

PoRep.prove() --> storage proof πPOS

PoRep.Verify() -->bit b （ Storage valid certification b1（ π_{POS} ）^ encapsulation valid certification b2（ π_{SEAL} ））

3.Concrete Construction Practice

PoRep.setup()

inputs：

--prover key pair (pk_P , sk_P）

--prover SEAL key (pk_{SEAL})

--data D

outputs: replica R，Merkel root rt of R，proof π_{SEAL}

Processes:

calculate hD=CRH(D)

calculate R=$SEAL^{\tau}$（D，sk_P）

Calculate rt = MerkleCRH(R)

Set $\vec{x}$ = (pk_P, h_D, rt)

Set $\vec{w}$ = (sk_P, D)

Caculate π_{SEAL} = SCIP:Prove($pk_{SEAL,}$ $\vec{x}$, $\vec{w}$)

Output R, rt, π_{SEAL}

PoRep.Prove()

inputs：

--prover Proof-Of-Storage key pk_{POS}

--replica R

--random challenge c

outputs: a proof π_{POS}

process：

· calculate Merkel root rt=MerkelCRH(R)

· calculate path = Merkel path from rt to leaf R_c

· set $\vec{x}$ =（rt, c）

· set $\vec{w}$ = (path, R_c)

· calculate storage proof π_{POS}=SCIP.Prove（pk_{POS}， $\vec{x}$， $\vec{w}$）

· output storage proof π_{POS}

PoRep.Verfy()

inputs：

--prover public key ， pk_P

--verifier SEAL and POS keys vk_{SEAL} , vk_{POS}

--hash of data D, h_D

--Merkel root of R， rt

--random challenge ， c

--tuple of proofs， （πSEAL，πPOS）

outputs: bit b =1 stands for effectiveness

Process:

· set $\vec{x}$ =（pk_P，h_D，rt）

· calculate b1=SCIP.Verify(vk_{SEAL}, $\vec{x}$,π_{SEAL}）

· set $\vec{w}$ =（rt，c）

· calculate b2=SCIP.Verify(vk_{POS}, $\vec{w}$,π_{POS})

· calculate b1^b2

4. Space-time Proof

Space-time proof allows the storage provider to provide evidence that data is stored effectively during a period of time (t). There is no specified verifier for Space-time proof (Post), and any privileged node can validate it.

Construction plan of PoSt

PoSt.Setup(1^λ, D) → S_P, S_V, where S_P and S_V are scheme-specific setup variables for P and V, λ is a security parameter. PoSt:Setup is used to give P and V the necessary information to run PoSt:Prove and PoSt:Verify. Some schemes may require the prover or interaction with a 3rd party to compute PoSt:Setup.

PoSt:Prove(S_P, D, c, t) →π^c, where c is a random challenge issued by a verifier V, and π^c is a proof that a prover has access to D for some time t. PoSt:Prove is run by P to produce a π^c for V.

PoSt:Verify(S_V, c, t, π^c) →b, b is a bool value which checks whether a proof is correct. PoSt:Verify is run by V and convinces V whether P has been storing D for some time.

6.2. YottaChain Trading Market

Various resources on YottaChain will be publicly traded in the YottaChain trading market; the trading market will match the transaction according to the number of resources, bandwidth, network latency, quotation and other factors that are offered by nodes.

Each kind of different resource has its own resource token, and the user needs to use the corresponding resource tokento purchase the required resources. All resource tokens can be freely exchangedviaYTA. When users want to use the resources on YottaChain, they need to convert YTA to correspondedresource token. The trading market will provide the quotation of each kind of resource token and automatically arrange the transaction for matched bidding.

7.YOTTACHAIN DEMONSTRATIO APPLICATION

7.1. YottaChain Content Sharing Application

YottaChain will build a content exchange application where the content provider stores the content of the file into the YottaChain storage network and encrypts the file. Content visitors can request authorization from the content provider. After the content provider authorizes, content visitors can view or play related content.

The content provider encrypts the content of the file through the TruPrivacy technology and saves the file to the storage network. When a content provider saves a file to a storage network, he will pay to save it through the storage market. In order to encourage more content providers to upload content, YottaChain will provide a certain amount of YTA to encourage content providers to upload content to the storage network free of charge.

Content visitors retrieve content through content applications and initiate access request transactions through the YottaChain backbone network. Transactions are completed automatically according to the price set by the content provider and access authorization is generated for content visitors automatically through smart contracts. Content visitors are authorized to download and use file content.

TruPrivacy will solve the problem of the same file content being repeatedly uploaded to the storage network space through a post-encryption de-duplication mechanism.

Content uploaders will automatically register their identities in the content sharing application and can confirm rights based on the registration information when there is a copyright dispute.

Documents encrypted with TruPrivacy can be blocked and accessed at the request of regulators if they are in violation of laws and regulations.

7.2. YottaChain Cloud-storage Application

7.2.1.Requirements of Cloud-storage Application Users

1.Office significance of data file sharing

Small and medium-sized enterprises and entrepreneurial companies also have a strong official need for file sharing, data backup and other aspects. However, due to their limited size, these companies are not able to purchase professional storage and backup facilities like large enterprises, nor can they arrange special personnel for daily configuration maintenance. If they have YottaChain, they can achieve collaborative work among members, quickly improve work efficiency, facilitate enterprise management, and facilitate the storage and integration of enterprise data.

Cloud plate application based on the above challenges, to provide a cost-effective, and easy to management solutions, for the enterprises through the provision of data backup, security distribution, rapid sharing important functions, such as to achieve a safe and reliable,

simple and convenient management of enterprise digital asset management platform, improve the level of enterprise digital asset management and efficiency, and satisfy the business enterprise of all departments border less coordination office and the demand of the information sharing and resource management, implement the office of the cloud, and help users to improve the work efficiency, reduce operating costs.

Enterprise cloud storage application is a product designed for enterprise users, aiming to meet the needs of enterprise collaborative office. At the same time, it also provides space for personal use, ensuring the privacy and security of file storage. Multiple employees can create a collaborative office folder, and when one of them changes the document, the updated document is displayed in the collaborative office folder. Support document direct online browsing, cloud office. Improve document distribution and sharing ability, enhance collaboration, and improve office efficiency.

2. The ubiquitous Internet environment trend has created virtual mobile storage

With the development of big data and mobile Internet, cloud storage service is becoming a new growth point of IT economy. According to IDC, the market size of cloud services will increase from 17.4 billion US dollars to 44.2 billion US dollars in the next four years. Among them, the market share of cloud storage services will increase from

9% to 14%, which means the market size of cloud storage services will be close to 6.2 billion US dollars.

Many Internet enterprises have followed the development of the market by launching free personal cloud storage service with large capacity, which has been widely used. For enterprise users, they also hope to protect their existing digital assets, facilitate information communication, reduce data management and maintenance costs, and adapt to the rapid development of business through cloud storage services.

At present, the enterprise important data is often scattered among the staff in all kinds of terminal equipment, due to the lack of data backup protection system, when a file is unavailable, unable to recover, causing unnecessary loss data, with the growth of the enterprise scale and the opening of the branch, the enterprise has a strong data exchange and distribution requirements, is currently widely used E-mail or QQ methods such as transmission, lack of regulatory process, it is easy to cause disclosure or loss of data; For large file transfer, limited by the existing network bandwidth, the transmission efficiency is low and the success rate is low, which hinders the daily business of enterprises.

Cloud storage application based on the above challenges, for the enterprise to provide a cost-effective, and easy to management solutions, through the provision of data backup, security distribution,

rapid sharing important functions, such as to achieve a safe and reliable, simple and convenient management of enterprise digital asset management platform, enterprise IT procurement to reduce costs, improve enterprise digital asset management level and efficiency.

7.2.2 Characteristics of Cloud-storage Application

1. Sharing Express distribution

Cloud storage can be distributed quickly. After uploading the documents by the higher authorities, the sub-departments and subordinate branches can obtain the documents immediately.

Through the sharing function, team materials can be quickly shared to colleagues and members, Significantly improving the efficiency and quality of distribution and management.

Through the function of external link, after extracting the external link of the file, the file can be quickly distributed to the customer by mail, QQ, WeChat, etc.

Quick summary

Through the sharing mechanism, data collection and summary can be completed quickly by groups and team members. One person creates folders and shares team members. After the team members upload the

data, the team leader can collect all the data and make summary statistics immediately.

Collect customer data quickly. After setting up the Shared folder and distributing the folder connection, you can quickly collect customer data to facilitate communication without losing customers.

Efficient sharing

Enterprise cloud storage supports multiple forms of sharing.

Cloud storage users can quickly share personal materials with their partners and colleagues to facilitate communication and collaboration. It also supports more flexible group mechanisms.

External link sharing can pull customers into the communication team by means of external link to achieve interaction and sharing. Keep abreast of customers and partners.

2. Ease of UseEasy to carry

By setting up automatic synchronization, files can be saved in the cloud at any time,Mobile phone, computer, pad and other multiple terminals to check and read at any time. Travel, go home, visit customers, no more usb drives, hard drives, CDS, laptops, etc. Visiting clients is easy to do with your phone. You can also check various company documents at any time during your trip.

L more terminal

Support mobile terminal to view materials, share Settings and distribute. Use mobile phone to retrieve files from the network storage at anytime and anywhere, generate access to the external link, no upload time, and improve work efficiency.

All product materials are stored in the network storage, and no longer need to print or carry paper materials. The salesman only needs to carry a tablet computer or use a mobile phone.

L more interface

The open OpenAPI is compatible with the international industry standard Amazon S3 interface and provides the stored API for developers to call in their own applications.

Open a comprehensive API interface to meet all integration requirements of the enterprise.

L more scenes

Use mobile phone to take photos at the construction site and project site, and upload the cloud storage directly. The construction site USES a tablet computer to directly view the construction drawings on the cloud storage.

Cloud storage iOS, Android and PC clients can also handle work tasks in a timely manner during the journey. The client supports online playback of images, audio and video in various formats, as well as online preview of working documents.

3. The security

Controllable

Cloud storage applies the most advanced security technology in the use, transmission, storage and other aspects of documents to ensure the reliability of the company's documents.

Encryption safety

Cloud storage applications are designed to protect the complete control of enterprises' digital assets from loss or leakage due to personnel changes, computer replacement or loss, reinstallation of systems, hard disk failures, virus Trojan intrusion and other factors. By restricting the authority of the system administrator, the system administrator cannot see any files and cannot peek into enterprise secrets.

Transmission safety

Cloud storage is encrypted on the client side and decrypted on the client side. No key and plaintext are stored in the cloud. The whole transmission USES ciphertext transmission any link does not disclose the company secret.

Operational control

Cloud storage application sets up the role authority management system, which supports customized roles except for keeping roles. It

can assign different role rights to different people and guarantee the security of files from file operation.

A multi-file deletion mechanism has been set up, so that files can be recovered safely even if employees delete them maliciously. A variety of treatment schemes have been set up for employee demission to ensure the pass ability of documents.

Containment

Cloud storage supports the sharing of documents, so that distributors can freely choose the personnel and departments to join, so as to control the scope of visitors.

Shared files support department inheritance sharing, and can control whether sub-departments can inherit access to folders from higher departments, thus further enhancing scope control.

Comb storage

Establish a Shared perspective, a Shared perspective, an external link perspective and other perspectives to organize documents. Ensure that users can sort through files from different angles.

The superior department may set up folders as required and grant corresponding authority to different sub-departments. After subdepartments submit the corresponding materials, the parent department will automatically complete the summary according to the subdepartments' classification to form a clear directory structure.

Easy to check

The historical version function ensures that the same file is recorded in the update order and that all files exist. You can return to the desired version at any time.

7.2.3 Cloud-storage Application System Structure

YottaChain cloud storage application DAPP, based on YottaChain account management system, YottaChain storage network supports the opening of cloud disk application in groups, which is equivalent to the opening of cloud storage application in a Shared space by an enterprise, department or organization.

The launching of cloud storage DAPP requires three steps: 1. Set up the group of cloud storage application, only the group manager can launch the cloud storage application; 2. Use the YottaChain computing network to provide computing resources for cloud storage DAPP. Cloud storage DAPP will complete the purchase of computing resources through the YottaChain trading market; 3. Use YottaChain storage network to provide storage service for cloud storage DAPP. Cloud storage DAPP will complete the purchase of storage resources through the trading market.

8. YOTTACHAIN GOVERNANCE STRUCTURE

The YottaChain project proposes a decentralized governance structure to solve the governance structure problem of block chain.

8.1 Source of Law

First, we define the source of law of YottaChain with reference to the research results of jurisprudence. In human society, the source of laws of the centralized system (such as the feudal dynasties of China) can be traced back to the individual will of the monarch, while the democratic system values the referendum #1 priority. In the YottaChain, as a decentralized governance structure, the source of law can be traced back to the votes of all the YTA holders.

Like EOS, holders should vote as “one coin, 30 votes”, not “one account, one vote”, nor one coin, one vote.

8.2YottaChain Community governance committee

YottaChain implements a representative system, and the community governance committee, which is voted by all YTA holders, formulates the rules of the YottaChain. This is because:

For the sake of efficiency, If everything is voted by all the holders, there will be no operability.

For professional reasons: Rules need to be formulated by by people with professional competence, not to mention the substantive issue like how to define legal provisions to achieve purpose, even to keep consistency between laws and articles is not easy.

For professional reasons. Rules need to be formulated by people with professional competence.

Other problems such as to block legislative loopholes and achieve appropriate punishments for law breaker, are all very professional. It is also an inevitable choice to legislate by people with professional competence. In addition to the Constitution, the Community governance committee, including but not limited to mining algorithms, whether to roll back, the appointment of committee members, and the growth of the total amount of digital currency, etc, formulates all rules of the YottaChain.

If the rules set by the Community governance committee violate the interests of most of the YTA holders, the holders of the currency can vote to ban its right. A referendum can be automatically held as long as there are a certain number of holders propose. The blockchain ensures that such a mechanism can be performed efficiently and fairly at low cost. From the initiation, holding and performance of the voting are automatically performed by the program. Similar to the EOS election BP, it is difficult for anyone to block and cheat. This mechanism can guarantee that the Community governance committee is generally in the interests of all the YTA holders. The reason why this is "generally" is the result of a because the compromise between fairness and efficiency. Community governance committee cannot be reelected just because of occasional non-critical errors.

8.3 From Rule to Code

In YottaChain's point of view, the true meaning of “code is law” is that “law is implemented by code”. We divide the transition process from rule to code into three major steps, and design a complete system to ensure that each role has to perform its duties as designed. These three steps are: the conversion from rules to product specifications, the conversion from specifications to codes, and the issuance of codes.

8.3.1 Code Specification Committee

The YTA sets up a Code Specification Committee that is responsible for converting the rules established by the Community governance committee into product specifications. Members of the Code Specification Committee are appointed and controlled by the Community governance committee. The specifications written by Code Specification Committee must strictly abide by the rules set by the Community governance committee. Except fixing bugs and performing upgrades that do not undermine the rules, the Code Specification Committee cannot arbitrarily propose new requirements.

The reason why the Code Specification Committee was set up separately is because the writing of product specifications is also professional, and its professional requirements are different from the

professional requirements of the Community governance committee. However, if the requirements specification written by the Code Specification Committee is inconsistent with the rules, the Community governance committee has the right to change its members to correct the error.

Since the whole process is open and transparent, the YottaChain community will report to the legislative council in case of any inconsistency between the requirements specifications written by the code specifications committee and the rules generated by the Community Governance Committee's voting. If the deviation of such requirements, specifications and rules is intentional, it is a very serious violation of the law whether it causes adverse consequences or not. It violates the responsibilities of its post and violates the trust of the Community governance committee, which will naturally be seriously dealt with by the Community governance committee. If the Community governance committee turns a deaf ear to this, the Community governance committee will also constitute a very serious violation of the law, which will violate its duties and trust of the holder of the currency and all the holders of the currency will naturally deal with it seriously. Under such an interlocking system, it is possible to ensure that everyone must conscientiously perform his or her duties.

8.3.2 Coding Committee

The coding process can also be divided into architecture design, coding according to architecture, testing, and merging code. But these are all done in accordance with the norms of the open source community. Developers around the world (even not YTA holders) can contribute code to achieve decentralized coding. If necessary, we can also set up a Coding Committee to take the lead in organizing the coding process. Similar to the Code Specification Committee, the Coding Committee is also appointed by the Community governance committee and is accountable to the Community governance committee.

8.3.3 Code Launch Committee

The last step is the release of the code. This is a final step to check and review. Before releasing, it must be confirmed that the code developed meets the specifications and there is no serious bug.

The mechanism of YottaChain is: the bottom layer of all nodes is the YottaChain constitutional client part whose main function is to automatically update new version of YottaChain software, i.e. automatically downloads and installs the software which has specific signature.

YottaChain establishes a Code Launch Committee. When members of the committee vote to approve a code, the code is automatically signed with the said specific signature, and all nodes are

automatically updated immediately. From voting to all node updates, the process is fully automated to launch the code. Similarly, the Code Launch Committee is also appointed by the Community governance committee and is accountable to the Community governance committee.

8.3.4 Brief Summary

The professional capabilities required by the Code Specification Committee, the Coding Committee, and the Code Launch Committee are similar. The reason why they are divided into different organizations is mainly because they need to be checked and balanced. If the specification submitted by the Code Specification Committee is inconsistent with the rules set by the Community governance committee, the Coding Committee can find error and raise objections. It is more efficient than waiting for the Community governance committee to take action to stop it. If the code submitted by the Code Committee does not meet the specification, the Code Launch Committee will not approve it and it will not take effect. Conversely, in case the Code Launch Committee wants to do something illegal, but because the code was not written by itself, it's impossible for it to issue its malicious codes.

8.4 De-founder

"Decentralization" means "de-founder", but for a founder it is very difficult to leave a project for which he has made many efforts to

create a big project from nothing, why should he leave? This problem is similar to transition path from centralized to democratic. At the start of the project, the project is controlled by the founder. When the project is mature, it is necessary to be “de-founded”. This conversion is not so easy to achieve. From another perspective, it is not necessarily a useful thing for the founder to leave completely.

Generally speaking, no one has more emotions about the project than the founder. No one knows the project better than the founder. No one wants to run the project better than the founder. The departure of the founder is obviously not a reasonable solution.

A reasonable solution is to refer to the constitutional monarchy of human society, giving the founder a ceremonial treatment and limited rights in an emergency, but under normal circumstances the founder has the same rights as ordinary YTA holders.

In this scheme, after the founder launches the project and the 1st Community governance committee is elected, the Community governance committee takes over the community, the original foundation will be dissolved, and the founder only served as a ceremonial community leader, equivalent to the constitutional royal family. This ceremonial treatment includes giving a ceremonial position in the constitution, speak on behalf of the community (but cannot make any decision or promise anything) and so on. The only

special right is that in an emergency, the founder has the right to initiate a referendum (while other YTA holders initiating a referendum require a certain threshold). In short, the community gives founder opportunity to appeal but has no right to make any decisions for the community.

8.5 Conclusion

Through the above institutional design, YottaChain can be guaranteed to be a self-evolved project. All powers are belong to all YTA holders. Rules can be formulated efficiently and professionally. All rules are implemented by code. If anyone makes mistake, there is always a corresponding remedy mechanism. In this way, a completely decentralized blockchain project can be constructed, while its operation is professional and efficient.

9、APPLICATION SCENARIO

9.1 Compatible with all IPFS Application Scenarios

YottaChain itself uses IPFS as a decentralized static persistent storage module, which can be compatible with all application scenarios of IPFS, including static web pages, CDNs etc.:

- Mount the global file system for decentralized persistent storage
- File version management

- Versioned package manager for all software （already implemented：https://github.com/whyrusleeping/gx）
- Can be used as the root file system of the virtual machine
- Can be used as a database: Applications can directly operate Merkle DAG, with versioning, caching and distributed features
- Can serve as communication platform
- Various types of CDN
- Permanent static web access, there is no link that cannot be accessed

9.2 Secure, Low Cost Storage for Personal and Corporate Data

YottaChaintigg provides comprehensive data security mechanisms to ensure that no matter how untrusted nodes store the data, there is no need to worry about data being leaked. Even the world's best hackers cannot easily break through. In any case, only data owner or its licensors can see the data, which is garbled for anyone else (including YottaChain's designers and implementers), without the risk of being compromised. Practically it can be considered absolutely safe.

Therefore, personal and corporate data, no matter how private or confidential, can be safely stored on YottaChain without any fear of security issues. It is much more secure and reliable than compare to the data stored to AWS, Google, and even your own computer.

At the same time, as YottaChain does not sacrifice any storage efficiency while encrypting security especially with the ability to de-duplicate data, you can reduce to storage by 5-10 times compared to any vendor's storage device in the market. Whether it's cloud storage, enterprise storage or distributed storage, whether it's a first-tier vendor or a low-quality product, it's much more expensive than YottaChain's storage.

9.3 To Build a Real Sharing Economy Using Idle Resources

Sharing economy refers to a new economic model based on strangers and the transfer of the right to use of goods with the main purpose of getting a certain reward, whose essence is to integrate idle resources, which is a model where people enjoy social resources fairly, pay and benefit in different ways and get economic dividends together. Previously, the existing sharing economy is usually realized through the internet platform.

The sharing economy involves three main bodies; namely, demand side, supply side and sharing economic platform of goods or services. The sharing economic platform serves as a link between the supply and demand sides, enabling the demand and supply sides to trade through the shared economic platform.

Airbnb, which aggregates the resources of idle accommodation in the world, is a representative enterprise of the sharing economy. It

becomes the largest hotel very quickly based on the power of sharing economic.Trying to aggregate the dripping of idle vehicles, Moby has also been regarded as a representative of the sharing economy. But in practice, companies such as Didi and Moby are not active. So it is not a real sharing economy, and does not play a role in activating idle resources.

YottaChain uses blockchain technology to create a shared economic platform that aggregates idle storage resources and computing resources around the world for use. It is a true sharing economy.

According to Gartner, there are now more than 3 million enterprise data centers in the world. Each enterprise data center has a large amount of storage resources and computing resources. If you add personal home resources (routers, home NAS, TVs etc.), it is even more than this. These storage and computing resources basically have idle parts (there is almost no way to use 100% of all the hard disk space). How to reasonably utilize a large amount of idle resources is a very significant issue.

YottaChain utilizes the unique block chain incentive model to mobilize the owners of storage space and computing power to contribute the temporarily idle resources to mine for others' use and fully share social resources, thus realizing a very huge scale shared economy system.

9.4 Self-Used Storage Space for Mining

For YottaChain, in addition to the use of idle resources for mining, the storage resources that are being used and will be used can also be used to mine and exchange rewards, and the data storage and mining can be used to exchange rewards.

For example, if a user has 1TB of storage space, which is originally used to store 1TB of data, now use this 1TB of storage space to join YottaChain to mine, and the YTA backhand to buy storage space, user can store 2TB of data, still there are some YTAs left.

This miraculous effect is because of YottaChain's data de-duplication technology that allows 1TB of storage space to store at least 5TB of data, so YTA mined with 1TB of storage space far exceed the cost to purchase 2TB of data storage space.

Sowith YottaChain, even if there is no idle storage space, you can use the used resources to mine, in this way, you can get extra digital currency as a reward.

9.5 Infrastructure of other Block Chain Projects

As an infrastructure public chain, YottaChain will provide solid, secure and low-cost infrastructure support for other blockchain projects, including but not limited to:

- Quickly provide a large number of nodes for other block chain projects: when each new chain goes online, it often requires a large number of nodes. The more nodes, the more reliable the distributed ledger of the blockchain. If depends on early users to establish blockchain nodes, it takes a long time to reach a relatively large number of nodes. If using virtual machines of public cloud service such as AWS to quickly establish a blockchain node, the important value of the decentralization of the blockchain is lost because the fault domain is not isolated. If nodes are established on YottaChain, nodes can be established rapidly and at low cost, and these nodes are built on the blockchain nodes, which naturally meet all requirements of block chain on decentralization and fault domain separation.

- The distributed ledger stored in the blockchain itself is completely stored by all the full-book nodes. Each node stores the information of all the blocks, which is equivalent to a multi-copy redundant storage mode. For example, Bitcoin has more than 10,000 full-book nodes, and the same data is stored in more than 10,000 copies. Although this model is very reliable, it is also very redundant. It is acceptable for very small but important cryptocurrency transaction records, but it can be very costly to store other types of data. YottaChain provides a more efficient storage mode for other blockchain

projects, which uses redundant coding to store data, reduces the redundancy of data storage to an economically reasonable level and is not limited by the block capacity, which can store nearly unlimited data.

- Blockchain transaction recordsneed to be packaged in blocks. The number of transaction records that can be packaged in each block is limited, which leads to congestion blocking at the peak of transaction, sometimes even more than one day is required to confirm the transaction. With the help of YottaChain, transaction records can be stored in YottaChain, and each block only needs to record dozens byte of hash value. Thus a small block can store countless transactions, and it is also equipped with anti-cheating and anti-node fault features, so it is no need to expand the block capacity.

9.6 Storage as Low Cost Object

Object storage is an API-based storage model provided by cloud storage service providers that handles and solves storage problems that were once considered tricky: continuous scalability, reduced flexibility, limited data persistence, unlimited technology updates and out-of-control costs. The API protocol for AWS's S3 Object Storage Service is the de facto standard for object storage.

YottaChain will provide S3-compatible object storage services at much lower costs so that users of AWS/S3 or other cloud platform object storage can immediately reduce their monthly costs without changing their code.

9.7 As a Persistent Storage with Disaster Recovery Feature

YottaChain's decentralized storage is naturally disaster-tolerant. YottaChain will provide standard block storage interfaces and NAS storage interfaces, which can be used as a low-cost solution for conventional enterprise storage (approximately $60 Billion per year) with disaster recovery capability!

In the future, all centralized storage (including AWS, Alibaba Cloud, EMC, Huawei) will not be considered as persistent storage, but can only be used as a local cache. Only decentralized storage can be used as a persistent store. An obvious example is that in August 2018, Tencent Cloud completely lost user data, and AWS and Alibaba Cloud have repeatedly experienced global failures.

10. TEAM MEMBERS AND ADVISORS

YottaChain is a blockchain project operated by YottaChain Foundation in Singapore. The founding team and advisory team are very professional and experienced.

10.1 Core Team Member of Sursen Interplanetary

- Alex Wang Founder

Top international IT scientist, a well-known entrepreneur, and has rich experience in social governance.

Alex has more than 20 years experience in cryptography application and nearly 10 years of experience in distributed storage system, all his technologies have reached world's top level. He has invented more than ten internationally leading technologies, and he was named China's Top 10YoungScientists (one of the national official highest honors), the first China Outstanding Engineers (selected by the Ministry Of Science and Technology of China, and the only one in the software and Internet industry) and the Top 10OutstandingYouth of China Software Industry (jointly selected by the Ministry of Industry and Information Technology and the Central Committee of the Youth League of China, with the sole unanimous vote), have invented more than a dozen global leading technologies, created many milestones in the Chinese IT industry, and owned more than 100 patents in US, Europe, Japan and China.

As a entrepreneur, Alex Wang founded the internationally renowned Sursen Group, a well-known Chinese IT leading enterprise. And once sold a company for several hundred million yuan.

As a company with technology genes, Sursen Group has always stood at the front of technological innovation in many eras of IT industry. Its data security products based on cryptography (security documents, secure storage, secure cloud disk, secure communication) are widely used. Applications, customers include 100% of China's central ministries, 100% of provincial governments, 100% of central enterprises, 100% of banks and a number of top secret institutions, involving billions of confidential documents have never had a security responsibility incident.

TruPrivacy, invented by Alex Wang, is the only technology in the world that can achieve data deduplication after encryption, and has patent protection worldwide. TruPrivacy technology relies on a complete password system. Even if the network is compromised, the server is controlled, and key personnel are bought, the user data can be secured and the hacker cannot steal it. At DefCon, the world's largest hacking conference in 2015, Sursen Yunkai opened the server and handed over control to hackers, with high cash rewards, but no one could steal user data and withstood the most demanding public verification.

The SurFS distributed shared storage system invented by Alex Wang is a major innovation in distributed storage technology. The unique technology has greatly shortened the data path, greatly improved the data transmission performance between nodes, and greatly reduced the system cost. Received the "Cloud Storage Excellence Award" from the US "Cloud Computing" magazine.

Alex Wang also serves as the chairman of the UOML-X technical committee of the OASIS International Industrial Standards Organization. He has extensive experience in managing multinational organizations with rules; he has deep experience in legislation.

- Will Hou Co-Founder /CEO

Hou Yuewen is an entrepreneur with technical background. He was once the director of software engineering of Sursen Electronics Corp.He is proficient in cryptology related technologies, and has undertaken many data security projects of the top national confidentiality related institutions in China. As a serial entrepreneur, he has set up his own start-up companies, such as Mobao Times, and

has rich practical experience in Internet product research and development, community operation and other aspects.

The cloud storage business that Hou Yuewen is in charge of has more than 10 million users in the world since it was launched for 2 years, among which the enterprise cloud storage product is one of the leading mainstream manufacturers in China.

- Peter Junge,Europen team leader

Peter Junge got his master degree from university of Hamburg, Germany, served successively as senior engineer of Sun Microsystems and project manager of OpenOffice.org, a well-known open source community, with rich front-line experience in IT technology and open source community management.

Peter has preciseness and conscientiousness of German characteristics, and has the outstanding specialty in compliance.

- Yvonne Li US team leader

Graduated from the university of Houston, Yvonne Li worked as an engineer at Lockheed and NASA, and served as director of

international operations for semiconductor giant KLA-Tencor. Later, she worked as a mobile Internet entrepreneur in Silicon Valley.

Yvonne has a good technical background and extensive contacts in Silicon Valley.

10.2 Advisors Group

- Laurent Liscia, Chairman of OASIS

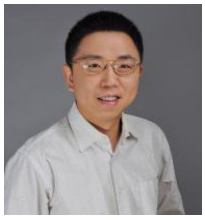
OASIS is an authoritative international industry standards organization, which is composed of more than 100 major IT manufacturers, users and academic research institutions in over 100 countries around the world.

Mr Laurent was a former officer of French foreign ministry.

- Louis Suárez-Potts, Leader of OpenOffice.org

Louis has long been responsible for managing the OpenOffice open source community and has served as director of operations for the Oracle community.

- Tao Jiang, Founder of CSDN



Founder of CSDN, the world's largest developer community

Tao is also founding partner of Geek-Bang venture capital.

- Fred Wang, Founder of Mars Finance/LineKong(hk.8267)

Founder of Mars Finance and Economics, a mainstream media in the blockchain

Founder of LineKong Interactive, a listed company

Founding partner of GeekBang venture capital

- Xiao Zhao,China's famous economist

He served as director of the research center of SASAC's macro-strategy department; expert member of the China economics

award, and core member of the famous economic group "doctor's coffee".

- Michael ZengMicrosoft Partner Director of Engineering

More than 20 years in Microsoft, successively engaged in operating system, search engine, artificial intelligence and other Microsoft mainstream technology research work.

11. RISK AND DISCLAIRMER

This document is a conceptual document of the YottaChain project [white paper] and is not intended to sell or solicit the shares, securities or other regulated products of the company.

This file cannot be used as the prospectus or any other form of standardized contract documents, and does notconstitute advice or solicitation of investment proposals for securities or any other regulated products in any jurisdiction.

This document shall not become any sales, subscription or invitation to others to purchase or subscribe to any securities, as well as any form of contactor commitment based on this.

Any information or analysis presented in this document shall not constitute any proposal to participate in the investment decisions and shall not make any specific recommendation that is biased.

The YottaChain foundation shall not be liable for any direct or indirect loss of assets resulting from participation in the project.

This document may be amended or replaced at any time, but we have no obligation to update this version of the white paper or provide additional information to our readers.