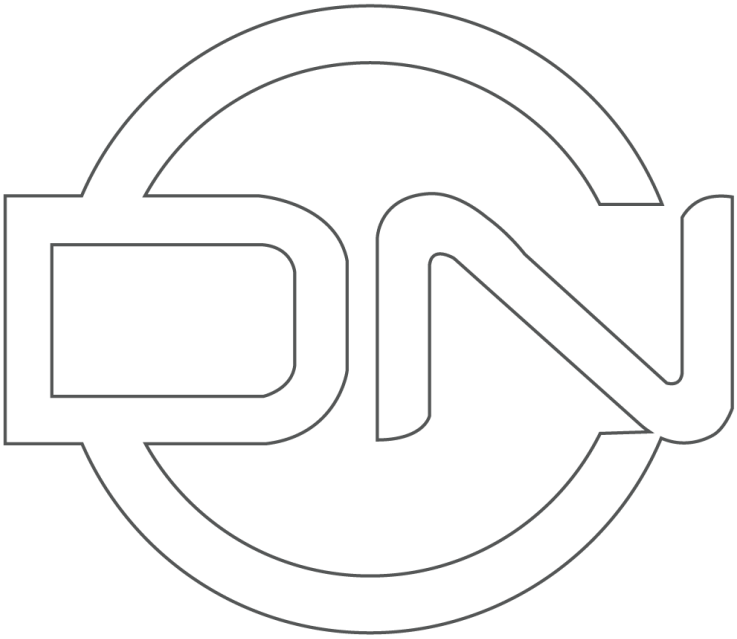


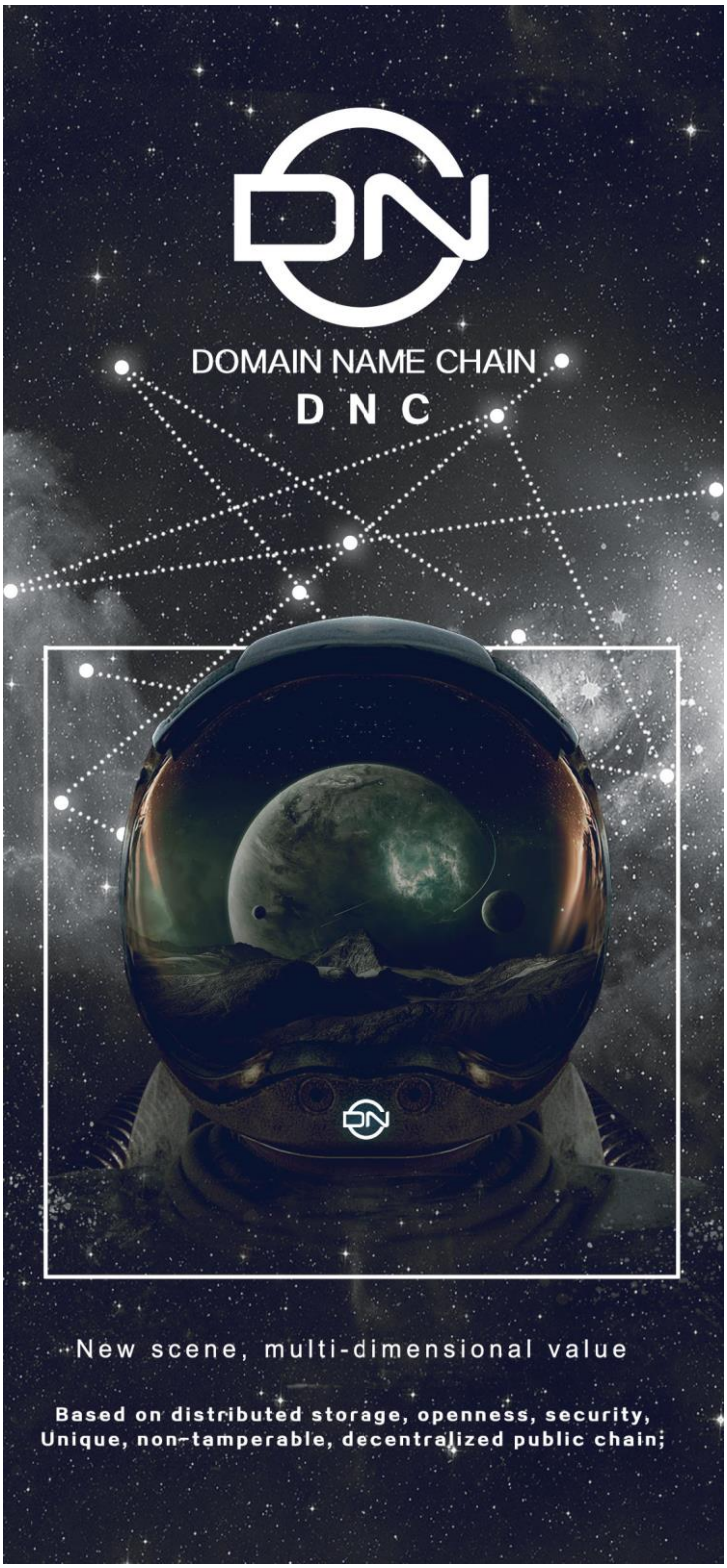
DNC

DOMAIN NAME CHAIN

Project White Paper

dnchain.io

01 Project background and goals



A new generation of fully functional public chain project based on distributed storage

Summary

In the 1960s, ARPAnet (predecessor of the Internet) appeared in the United States. In 1983, Paul Mockapetris (Paul Mockapetris) invented the DNS system, which is a distributed database to solve the problem of IP addresses difficult to remember. In 2009, a self-proclaimed SATOSHI NAKAMOTO guy released the BTC node code, and then the concept of blockchain appeared, which affected the entire financial world. In 2020, DNC (Domain Name Chain) emerged, 88 versions of the world's top communities synchronously launched version 1.0, participated in the DNC super node election, used the massive USDT fund pool as a guarantee for exchange, and cooperated with many overseas listed companies. Realize the free exchange of the same rights of currency stocks, reserve multi-country DCEP ports, serve 1 billion-level end users, and expand the application field of blockchain to e-commerce, games, tourism, and finance.

DNC is the basic currency of the DNC chain. It can be composed of a series of names separated by dots. It circulates throughout the DNC ecosystem. The total number is 1 billion, and it gradually decreases (incends) as transactions increase. DNC ' s The operating company is Starlink (Starlink is a new company independent from SpaceX in the United States), provided security by the IMB, SpaceX invested 1 billion US dollars to support DNC global broadband Internet access satellite

network.

DNC and US SpaceX successfully launched 400 Starlink satellites. In the live webcast about the launch, SpaceX revealed a series of upgrade details for these satellites, including increased bandwidth and complete decomposition. DNC inherited the initial design ideas of the Internet, creating a personal free communication platform, resisting oligopoly and creating a private and safe Cyber Space. The domain name is unique, and the personal identity of the blockchain is also unique, connecting online and offline, and on-chain and off-chain.

DNC will be a cross-chain hybrid structure, covering DPOS + PBFT + POW consensus algorithms, perfectly docking transaction sharding and storage sharding, and providing 2 stable cloud VMs at the bottom to developers worldwide.

The general trend of the future development of the Internet is from centralized to distributed development. The emergence of blockchain has greatly promoted the cooperation of distributed resource providers to provide storage, bandwidth, payment and other services. Due to the lack of readable and writable distributed storage and scalable distributed accounting, current blockchain applications are greatly limited in their application scope. The current blockchain is mainly used in transfers, deposits, gambling, etc. In addition to the inefficient function of world state (transaction data saved by all miners), storage and accounting

cannot handle large-scale transactions and big data storage. This greatly limits the popularity of blockchain applications.

DNC planning is the integration of distributed ledger, distributed storage and distributed communication.

Any user can use the private key to control their own distributed cloud space, and build their own file system and file-based database system on it, so as to provide the "missing hard disk" for the blockchain system and make the distributed system Developers can use it to build a variety of practical DApps. This may also be a major change to the Internet's infrastructure, which will have a profound impact on the Internet.

Distributed communication is also a function that distributed systems must have. Information exchange, whether it is a two-person conversation or a multi-person conversation, whether it is text, voice or video, is extremely important for various types of transactions before, during and after the event. The traditional blockchain lacks a readable and writable distributed storage space, which makes it difficult to establish a distributed communication system. The project has a distributed storage function. Communication data can be used as a relay through a distributed cloud to achieve a true point-to-point distributed communication function. .

Bitcoin, which implements the peer-to-peer transfer function, is the

first-generation blockchain. It mainly builds a distributed system through an incentive mechanism; Ethereum, which implements smart contract functions, is the second-generation blockchain, which mainly uses Turing-complete virtual The machine realizes programmable transfer; and the DNC-like public chain has functions such as distributed storage, infinitely scalable transactions, and distributed communication. It is a fully functional blockchain. A fully functional DApp can be built on it and can be considered It is the third generation blockchain.

Starlink is a new company independent from the American space exploration technology company SpaceX. It is an industry leader in recycling technology, which is much higher than the industry standard. When the service life is reached, the satellite will use the integrated propulsion system to get out of orbit. Even in extreme cases where the propulsion system fails, the satellite will use atmospheric friction to self-destruct, which is much better than other high-orbit satellites. (Everyone knows that high-orbit satellites make a lot of space junk)

Share a Russell's poem, which coincides with DNC's vision, and worship the power admired by Pythagoras-that is, digital control of ten thousand logistics.

I have wished to understand the hearts of men. I have wished to know why the stars shine. And I have tried to comprehend the Pythagorean power by which number hold sway above the flux.

Love and knowledge, so far as they were possible, led upward toward the heavens.

But always pity brought me back to earth. Echoes of cries of pain reverberate in my heart.

Children in famine, victims tortured by oppressors, helpless old people a burden to their sons, and the whole world of loneliness, poverty, and pain make a mockery of what human life should be. I long to alleviate this evil, but I cannot, and I too suffer.

–Bertrand Russell

Figure 1 Bertrand Russell

1: Project endorsement, goals, vision

1.1: The driving force, current situation and dilemma of the development of human civilization

The power of a single person is insignificant, and the progress of human civilization stems from the breadth and depth of human cooperation. The progress of human cooperation mainly benefits from institutional progress and technological progress. The system mainly refers to the system related to various organizations, and the technology mainly refers to the technology related to human exchanges and transactions.

The basic method of human cooperation is the distributed market. Social division of labor cooperation based on distributed markets is the most basic and natural method of human cooperation. The ingenuity of market mechanisms is praised by Adam Smith as "invisible hand". However, human cooperation faces obstacles such as opaque information, asymmetric information, conflicting concepts, and a lack of program interfaces in the brain. The fully distributed market has limited capabilities in solving trust issues. Therefore, society has invented various centralized organizations to Resolve trust issues. At present, the system of human cooperation is mainly built around centralized organizations (states, religions, enterprises, etc.). With the development of the Internet, more and more people can communicate and cooperate

online, and the cost of contracts is greatly reduced. Internet platforms such as Google, Apple, Facebook, Tencent, and Ali, as the new centralized organizations in the era of online cooperation, play an important role in human online cooperation.

Centralized organizations have made great contributions to human civilization, but they have also brought various resistances and major risks to civilization. All kinds of centralized organizations are becoming more and more centralized in terms of geography, culture, religion, system, information system, etc., which not only cause obstacles to exchanges and transactions, but also become the main source of various conflicts. The stronger the centralized organization, the more severe the gap and confrontation between the organizations, the more obvious the pressure within the organization, and the greater the impact of organizational failure. World wars, regional conflicts, trade protection, and corporate monopolies have greatly affected human cooperation and may have stalled. Centralized organizations also face dilemmas such as single-point risk, class differentiation, and organizational conflict when solving trust issues. The so-called single-point risk of a centralized organization means that the more successful the centralized organization is, the more power, capital, talents and data are concentrated in the hands of a few institutions or a few people. Once these institutions are breached by the outside or internally altered,

the consequences are unimaginable. . Secondly, the increasing concentration of resources in the hands of a few people also results in the formation of different strata within the organization. Stratum conflicts are unavoidable and mutual squeezing is also common. Finally, various methods of increasing cohesion within an organization are called methods such as patriotism, corporate culture, religious belief, etc., which just makes the conflict of ideas between organizations difficult to avoid, and the opaque information between organizations makes the The problem of trust is also difficult to solve, even making brutal competition the norm.

From a large time scale, human civilization is still at a very preliminary stage. According to the calculation of the Kardashov index, human civilization is currently in the 0.73 type civilization (Sagan, 2000), that is, human civilization still only belongs to the category of 0 type civilization. It can be said that human beings are extremely vulnerable to the vast universe, just like children in their infants. But such a child who is in need of a long body is choked by the limitations of the centralized organization.

It has to be pointed out that the drawbacks displayed by the current centralization scheme continue to expand, which is particularly obvious in the Internet era, which has caused human development to fall into a certain dilemma. When the Internet first appeared, we saw

that the Internet played an important role in information dissemination and media transparency. However, with the development of the Internet, various centralized Internet platforms have also formed an oligopoly, and the data of large Internet platforms is increasingly More and more concentrated in the hands of a few centralized organizations, traffic monopoly, data monopoly, and technology monopoly are becoming more and more serious, so that a large number of individuals or small businesses can only rely on a few large groups, and small startups are increasingly difficult to succeed , This has constituted a great obstacle to human innovation. Human cooperation based on large-scale Internet platforms greatly promoted the progress of human civilization in the first stage of Internet development, but with the deepening of Internet development, the power of the Internet is becoming more and more unequal, and the platform monopolizes resources.

Figure 1 DNC and US SpaceX successfully launched 400 Starlink satellites

1.2: The rise of blockchain and the hope it brings

The Bitcoin white paper published by Satoshi Nakamoto on November 1, 2008 has enabled mankind to realize the pioneering issuance of private currency through the Internet, and the blockchain technology behind it has great potential in solving the problem of trust between partners. This is why the blockchain is called "the machine of trust" by the cover article of The Economist. Most of the existing technology mainly promotes the progress of "productivity", and blockchain is an innovation of people's "cooperation mode" and a technological revolution of production relations. Before the advent of the blockchain, human cooperation can only be achieved through a centralized solution. The Internet is to use a centralized server and a C / S or B / S architecture built on the TCP protocol. The blockchain allows us to see the possibility of transforming a centralized transaction matching platform into a distributed matching platform. This will not only maximize the efficiency of the distributed market economy, but also avoid the problems caused by the centralized organization. Earth reduces the cost of trust in distributed markets. In fact, for the main obstacles such as opaque human cooperation, irrationality, conflict of ideas and lack of program interface, the blockchain can give a reasonable distributed solution, the main reason is that the blockchain has distributed accounting and consensus And token incentives, assets

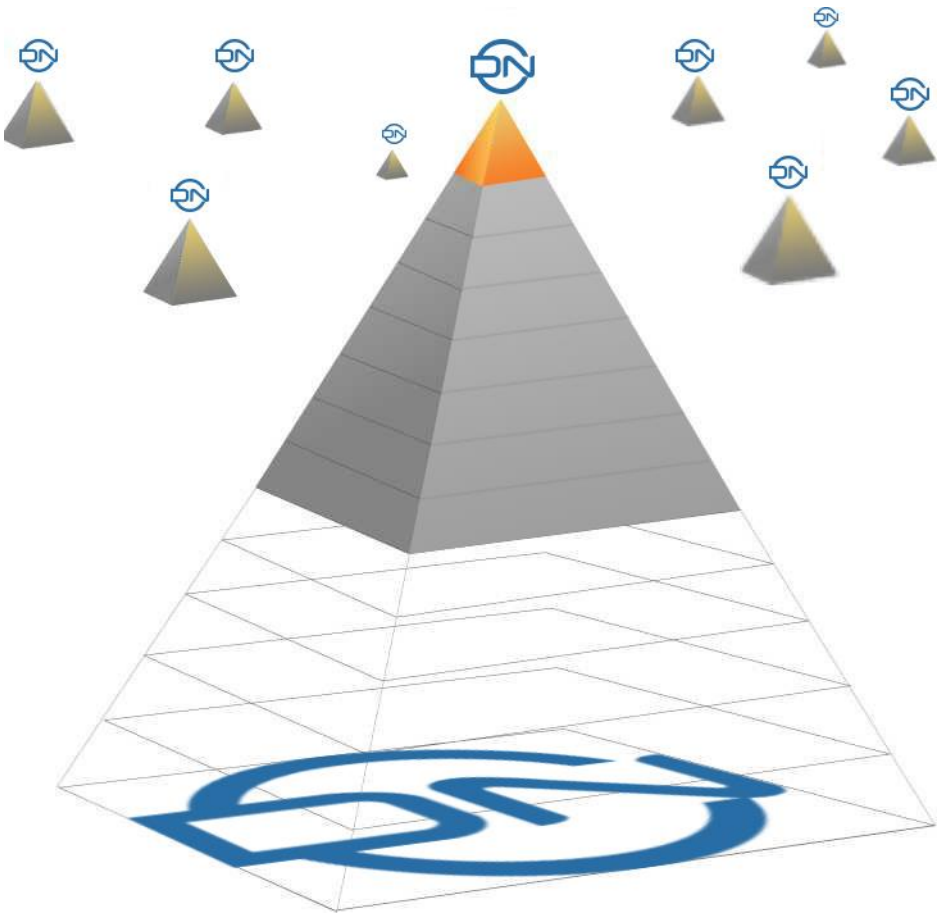
based on address and private key control, smart contracts, trusted data, distributed communication, etc.

The industry with the biggest changes brought by blockchain is finance first. Bitcoin pioneered non-governmental issuance of currency and non-intermediary electronic transfers. The ICO boom in 2017 allowed us to see the broad prospects for various assets to be digitized, distributed bookkeeping and programmable through tokenization. It is conceivable that various assets including securities, land, real estate, automobiles, oil, etc. will be mapped on the chain in large numbers in the future, so as to realize asset digitization, distributed bookkeeping and programmable.

But in the future, if the blockchain can achieve distributed storage and distributed communication, the blockchain has the potential to form a distributed Internet infrastructure, thereby providing unlimited possibilities for human-based centralized organization cooperation to distributed organization cooperation . The first generation Internet is a centralized information Internet, which has brought great changes to society, and the rising distributed information Internet and value Internet are the deepening and inevitable trends of Internet development.

More importantly, for the first time in human history, blockchain has given human core problems, a distributed solution to the trust

problem, that is, trust will be delivered to the code. The smart contract based on the blockchain replaces the paper contract, which not only makes the automatic execution of the contract possible, but also allows strangers to conduct transactions based on the trust of the code. Through distributed accounting and smart contracts, humans can automate distributed market transactions without relying on centralized institutions, allowing humans to achieve a qualitative leap in cooperation technology for the first time since going out of Africa. Times, that is, human organization and cooperation based on distributed Internet. It is foreseeable that the distributed technology based on the blockchain will gradually solve the disadvantages of the centralized organization, open the curse of the centralized organization on the human throat, and start a new journey of human civilization to a more advanced stage.



1.3: The current defects of the blockchain and the problems to be solved: from Turing complete to complete functions

The application of blockchain in the field of payment started from Bitcoin in 2009. The proposal of Ethereum as a Turing complete blockchain was from 2014, but so far, except Bitcoin and Ethereum, there are more than 100 In addition to 10,000 users, other blockchain applications have basically not reached this order of magnitude, and daily activities are even less, only a few hundred thousand, but centralized application users reach 10 million everywhere, and hundreds of millions are not uncommon. Blockchain projects not only lack killer applications, but also have less implementation in all walks of life.

Centralized platforms generally have functions such as registration and identity authentication, data storage, communication, and order transactions. The platform is also superior in scalability and user experience. The blockchain is almost vacant or incomplete in these functions. The following lists the main imperfect aspects of blockchain functionality.

1: Capacity expansion. Capacity expansion refers to the confirmation efficiency of blockchain transactions. At present, the average TPS of Bitcoin is less than 10, and the average of Ethereum is less than 20. The speed of EOS single chain with super node capacity is only thousands. At present, blockchain expansion is working hard through sharding, layering and consensus mechanisms, but they are still immature.

2: Storage. The development of the Internet is accompanied by the development of data storage technology, but the current blockchain basically uses data blocks to broadcast to the entire network, which is not only inefficient, but also difficult to produce various data-based applications.

3: Communication. At present, important applications, whether Airbnb, Uber or Taobao, have built-in communication functions, not to mention social applications, because most transactions have communication requirements before, during and after transactions. The current blockchain is building a value Internet, but it has failed to

integrate the functions of the information Internet, and future blockchain projects need systematic solutions that can efficiently integrate human communication and transactions.

4: Cross-chain. We expect that blockchain can express a large amount of value on the chain and form a value Internet through the blockchain, but at present it seems that each blockchain has formed its own value interaction, but it is difficult to value between the blockchains Interaction, which actually forms an archipelago of blockchain, but there is no connection between islands. To this end, there are now tens of thousands of exchanges, but exchanges are centralized institutions that can only exchange value, and it is more difficult to achieve multi-currency programmable interaction, that is, multi-currency smart contracts.

5: Identity management. People's identities are closely related to their activities, including socializing and trading, as well as self-identity revealing and identity authentication from third parties. In addition, identity use is related to usage scenarios, and people have different identities in different situations. The existing blockchain lacks comprehensiveness and depth of identity management, and lacks integration with business scenarios.

6: User experience. When existing blockchain projects are made into products, the user experience is often poor. For example, the management and use of private keys and addresses are not friendly, and

lack of integration with artificial intelligence.

It can be seen that the current blockchain has not been applied on a large scale, mainly due to the above-mentioned imperfect functions. Melanie. Swan divides the application of blockchain into three stages in "Blockchain: Blueprint and Guide to the New Economy" (Swan, 2015): Blockchain 1.0 is the application of blockchain to payment, technical characteristics It implements distributed bookkeeping; blockchain 2.0 is the application of blockchain in finance, and the technical characteristics are the realization of Turing complete smart contracts; blockchain 3.0 is the application of blockchain to all aspects of society. Realize various functions possessed by the current centralized platform. At present, the reason why the blockchain cannot develop applications for tens of millions of users is mainly because the existing public chain does not have all the above-mentioned functions, and there is no way to develop distributed applications commonly used by the public. To realize Blockchain 3.0, it is necessary to make the public chain system evolve from Turing completeness to complete function.

The so-called "complete function" refers to the specific key functions required for blockchain-based applications to achieve an experience comparable to existing centralized apps. The public chain 3.0 is similar to the distributed version of the current centralized platform. To enable it to develop complex distributed applications on it, it needs to have sufficient

functions itself, which requires the newly emerging blockchain to be able to specifically Features. However, when we look at almost all public chain projects that are now appearing, it is difficult to meet the requirements of "complete functions". They either lack communication, or lack storage, or lack identity management functions. Therefore, at present, there is no real public blockchain of blockchain 3.0 on the market. The real landing and large-scale application of the blockchain is precisely the need for the public chain platform to evolve from "Turing complete" to "function complete", that is, to have various functions that can realize heavy distributed applications, not just Turing complete payment. That's it.

Figure 2: DNC simulation scenario

1.3.1: Features that humans need to have in an automated cooperation system based on blockchain

A distributed market is the most natural way for humans to cooperate, but due to the limitations of communication technology and automated trading technology, humans have used a large number of centralized organizations to alleviate market failures. The centralized solution solves a large number of problems, but it also has inherent defects. The centralized Internet platform allows us to see the possibility of human cooperation automation, and the blockchain allows us to see the prospect of human distributed automatic cooperation. Internet-based distributed automatic cooperation system will be the main development direction of human future cooperation technology. The automatic human cooperation system based on blockchain has its completely different characteristics from the centralized platform. To sum up, the human cooperation system based on blockchain needs to have the following characteristics:

1: The public chain is sufficiently distributed. The distributed system breaks down the cooperation partners into smaller particles, making the cooperation granularity smaller, and has the potential to avoid various negative problems caused by centralization and increase the number of participants who can participate in cooperation. This requires that the blockchain is a very distributed public chain.

2: Automation system based on code cooperation. Automation is not only the automation of machine systems, but also the future of human

society cooperation. People cooperate based on procedures to enable future cooperation systems to operate efficiently. The advantage of this cooperation method is that it can reduce the problems caused by mistrust by increasing code transparency and automatic execution. This code-based cooperation mechanism is the most critical solution to the obstacles in human cooperation. This requires the public chain and the smart contracts on it to be open source systems.

3: Ability to integrate communication and transactions. Communication is the most critical means to reduce information asymmetry. Before, during and after the transaction, both parties must be able to establish contact at any time, so the distributed automatic system can integrate communication and transactions. In the Internet era, this requires integrating the information Internet and the value Internet on a distributed network.

4: The data is controlled by the producer, that is, distributed cloud storage is required. A big problem with the centralized solution is that the data is occupied by the centralized organization, which is not only unreasonable, but also easy to leak privacy. The reasonable way is that the data is controlled by the producer, which requires the distributed system to solve the problem of distributed storage of data, so that once the data is generated, there is private space and the power can be confirmed.

5: Have identity verification and reputation proof mechanism. The mechanism of identity verification and reputation proof is the most important mechanism to solve the information asymmetry and the distrust of the transaction subject. Distributed systems must integrate the two.

6: It enables various participating subjects to enjoy services or make money. The system enables individuals, organizations, and intelligent programs to participate equally in transactions. At the same time, this requires that the public chain can empower participants, including code developers, product providers, and users, and benefit from a larger platform than a centralized platform.

7: Ability to empower developers. The most important creativity of mankind comes from entrepreneurs, and a system can only release vitality if it attracts strong support from various entrepreneurs.

In summary, the existing human cooperation is mainly based on the semi-automatic system of centralized organizations, which can be called the first-generation cooperative system. The second-generation human cooperative system should be mainly based on the distributed automatic system. Such a system should have the ability to allow various trading entities to trade more equally and efficiently.

1.3.2: Project objectives

Blockchain technology allows us to see the prospect of all human beings building an automated society on an automated transaction matching system, and it is possible to form a global village based on blockchain. To upgrade human civilization as soon as possible, it is necessary to establish a fully functional and infinitely scalable public chain system, so that the exchanges and transactions between individuals, individuals, organizations and organizations, and individuals and organizations can cross geography, institutions, organizations, Restrictions on beliefs, races, etc. promote human cooperation on a global scale, and integrate information Internet and value Internet through blockchain to promote human cooperation in a manner that promotes human communication and transactions.

We see that the number of users of some apps can reach more than 1 billion, and the total number of humans is less than 10 billion. If it is an infinitely scalable public chain, it is entirely possible that it will encourage all humans to establish cooperation on it and promote The realization of the global village of blockchain. Although it is not easy to achieve this goal, we can already see the dawn of such a prospect.

With such a mission and vision in mind, the project will have the direction of persistent efforts. But direction alone is not enough. The project needs a specific goal. Based on the above analysis of human-centric cooperation and the analysis of the current shortage of blockchain,

the most important thing that humans currently need is a distributed automation cooperation system, and this system should be based on a public chain. Our goal should be to develop a public chain that can overcome the deficiencies of the current blockchain and establish various DApps on it to promote human cooperation. Such a public chain should have the following characteristics: infinitely extensible, full-featured, and address-centric for data confirmation. Therefore, the goal of DNC is to develop a public chain with address as the core for data confirmation, complete functions and infinite scalability, and promote the continuous improvement of the DApp ecosystem on it.

Figure 3 DNC simulation scenario

So the DNC project has the following goals:

1: Establish an information Internet based on a peer-to-peer network.

The data is stored in the private space of the producer, and the right is confirmed when the data is generated. The famous scientist Professor Zhang Shousheng put forward the following points when discussing the development of artificial intelligence and big data: "Most big data is related to personal information. Personal data and information often go to the central platform. Individuals are not protected by privacy. There is no reward for providing personal data. These two problems are solved by the blockchain at the same time, so the blockchain and artificial intelligence must have a complementary relationship. "And this project is based on distributed personal data space for personal data. Confirm power.

2: Establish a value-based Internet based on peer-to-peer networks, with transaction scalability capable of supporting 1 billion users.

3: Establish a multi-dimensional identity and reputation system, so that the human cooperative ecology can generate a mechanism for good currency to expel bad currency.

4: Serve developers, so that developers can focus on data services instead of data possession.

02 Project architecture

2. Project architecture

2.1. Project design ideas

2.1.1. Point-to-point communication, distributed information Internet and space-based storage

Space-based storage is the key to project design. It is necessary to meet the design conditions. Only on this basis can point-to-point communication and distributed information Internet be realized. At present, IPFS technology needs to do transactions every time it uploads and downloads files, which will make the file system itself occupy a lot of transaction resources, making it difficult to be applied to data storage that needs to be dynamically updated, and dynamically updated data is the most time-sensitive And the most valuable. IPFS is actually "file-based" storage, while our traditional Internet storage is actually space-based. Almost all cloud services are charged according to the size and time of space usage, but the space in the blockchain world is not charged according to the time and space used by storage space. This is what blockchain storage needs to reverse most.

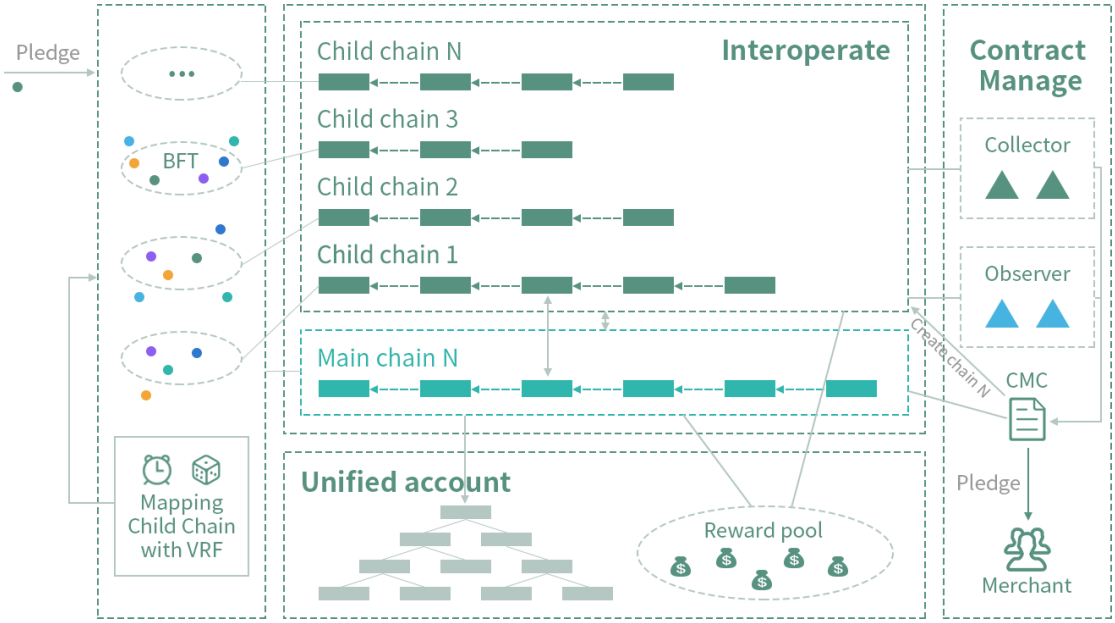
At the same time, space-based storage can enable everyone to have their own "distributed personal cloud", which makes it possible to establish data communication, authorization and transactions on the personal cloud, and also allows various applications to choose to generate applications The data is returned to the user, that is, the data is

not stored on the platform, but stored in the personal cloud.

2.1.2. Settlement of transaction scalability

To enable the project to be used by a large number of people, it is necessary to expand the existing blockchain transaction capabilities. How to expand transaction capabilities is one of the main topics of blockchain development.

The essence of the blockchain is a distributed ledger. It needs to perform the next operation after the state synchronization, and then synchronize the new state, otherwise it will be difficult to avoid the double-spend problem. To achieve the state synchronization of the peer-to-peer network, you need to select a trusted accounting node in each state synchronization cycle, and then broadcast the records to all nodes, and so on.



Parallel fast multi-chain sharding

According to this, the bottleneck of transaction ability lies in two points: the efficiency of electing the bookkeeper; the efficiency of data synchronization.

Efficiency of election bookkeeper: The bookkeeper selection is mainly achieved through a consensus mechanism. At present, there are mainly proof of work, Byzantine agreement, and proof of rights and interests.

The proof of work of POW is the most concise and safe, but it is also criticized because of the slow block generation speed, unfavorable environmental protection, and monopoly of mining pool computing power. It is a consensus mechanism that can be avoided if it is necessary.

The PBFT Byzantine agreement needs to collect the signatures of more than two-thirds of the nodes. With the increase in the number of nodes, it is almost impossible to do it, only through super nodes, but this will seriously damage the decentralization.

Proof of POS equity can be produced relatively quickly, but it is considered to widen the gap between the rich and the poor and be easily monopolized by the rich, and problems such as finality are difficult to prove mathematically. However, in fact, the proof of workload is also to widen the gap between rich and poor and easy to be monopolized by the rich, because purchasing computing power also requires more financial resources. At the same time, proof of rights is not impossible to

contain the gap between rich and poor through new design.

Therefore, when designing a consensus mechanism, this project hopes to absorb the strengths of various consensus mechanisms, avoid the weaknesses of various consensus mechanisms, and adopt a hybrid consensus mechanism will be a more reasonable choice.

Data synchronization efficiency: sharding

The synchronization efficiency is mainly related to the hardware performance, the size of each block, the block generation cycle, and the scale of the nodes that need to be synchronized. Hardware performance, including broadband, needs to wait for the development of the entire Internet hardware infrastructure. The size and block generation period of each block are directly related to TPS and cannot be optimized. The size of the nodes that need to be synchronized is related to security and to decentralization, and it is in this regard that most current blockchains are unreasonable. The current number of blockchain nodes can be infinitely increased, but all need to synchronize a piece of data, which makes the system performance become worse and worse as the number of hardware increases, but the distributed level reaches a certain level and then increases its marginal utility is decreasing of. Although the distributed level increases security, security and distribution also require a certain degree, and it is not necessary to expand indefinitely.

Therefore, the best way to increase synchronization efficiency is

currently sharding, which is to divide nodes into multiple groups. As the number of nodes increases, the number of shards gradually increases, and each shard has enough nodes to maintain "sufficient distribution" Type ". This approach allows the size of each shard to be controlled to a certain extent, which increases the synchronization efficiency. On the other hand, multiple shards simultaneously produce blocks, so that there is a realistic way out for infinitely expanding blockchain transaction capabilities. Therefore, although the shard design has certain difficulties, the shard design, including inter-slice transactions, split mechanism, etc. will be an inevitable choice for this project.

2.1.3. Multi-dimensional identity verification and reputation proof mechanism

Although the blockchain provides a way of anonymous transactions, more transactions require the parties to continuously improve understanding to reduce information asymmetry and transaction costs, and facilitate more transactions. Therefore, the identity verification and reputation proof mechanisms are necessary designs.

Because it is difficult to achieve mandatory disclosure in the blockchain world, it is difficult to verify the authenticity of the data even in the distributed world. However, the blockchain has the characteristics that data cannot be tampered with. As long as the disclosure information is provided to individuals, time stamps are added, and the data cannot

be tampered with, then voluntary disclosure or self-reputation certification will become the choice of many people.

Since a person has multiple identities, similar to family, school, company, country, part-time occupation, etc., there will be different identity characteristics in different occasions, so multi-dimensional identity verification is required. Similarly, the reputation proof mechanism also needs multi-dimensional data to support it. Only when a person keeps his various data on the tamper-proof network can he leave more and more traces in time, thus presenting himself with more and more credibility, and making identity and credibility his own assets.

Therefore, many people use the personal cloud on the blockchain for identity verification and reputation proof.

2.1.4. Serve developers

This project is to promote the productivity of entrepreneurs, thereby promoting the efficiency of human exchanges and transactions. This is the fastest way to promote human exchanges and transactions, so this project is designed for developers everywhere. Platform entrepreneurs don't necessarily want to own user data, but they are guilty of injustice. Platform entrepreneurs actually lack options, and current data cannot be stored by everyone. If the blockchain can provide everyone with a cheap personal cloud space, then the entrepreneur may have a fully functional blockchain and establish various types of DApps to start a business.

Because the distributed network built by the fully functional blockchain has many irreplaceable advantages, and can better provide better start-up services under the shadow of the Internet giants.

A fully functional blockchain can better perform data confirmation, rule making and self-certification innocence.

Most of the current entrepreneurship needs to use the Internet to develop mobile applications or websites, but new entrepreneurs are faced with the challenges of the huge cost of Tuoke and the replication of their business models by large Internet platforms. Because large Internet platforms have advantages in terms of development power and traffic import, and Internet platforms with big data are easier to optimize customer experience, and small entrepreneurs have higher development costs and customer acquisition costs, so the current Entrepreneurs can easily encounter bottlenecks in entrepreneurship. Their best way may be to develop and sell to large Internet platforms, thereby further enhancing the monopoly power of Internet platforms.

How to give entrepreneurs the ability to challenge large platforms? At present, the most criticized by large platforms are the monopoly of user data, the monopoly of trading rules, and the lack of transparency. They claim to be innocent, but it is difficult to prove themselves innocent. If starting a business on the blockchain allows the data produced by the user to be authorized to the producer, the transaction rules are controlled

by the user, and the developer can prove himself innocent, then the developer has the ability to challenge the large Internet platform.

A fully functional blockchain can make better use of development tools and development ecology

The blockchain-based Internet is very different from the traditional in architecture. The blockchain has a thick protocol layer and a thin application layer, and the traditional Internet has a thin protocol layer and a thick application layer. This makes the traditional Internet development more difficult, and the smart contract suite can be used in the blockchain world to start a business, even without renting a server, which allows developers to better help each other, and better share development tools. Development difficulty Also reduced accordingly.

Full-featured blockchain can better share traffic and reduce customer acquisition costs

The traditional Internet platform has a lot of data, which makes the platform more and more powerful, and it is more and more difficult for entrepreneurs to import traffic or obtain customers. However, users on the blockchain platform can use the address as the ID of any application, which makes it possible to share traffic between DApps on the blockchain and greatly reduce the cost of customer acquisition.

A fully functional blockchain can better perform data sharing and customer portraits.

The biggest feature of a fully functional blockchain is that data is stored in personal space, and these data can be selectively opened. Therefore, most people have open data that can be used by new entrepreneurs on the blockchain, thus achieving data sharing and providing convenience for customer portraits and targeted recommendations for the first time using an application platform.

2.2. Features of the project

2.2.1. Serving developers: Empowering entrepreneurs as the main entry point for ecological construction

DNC strives to become a human-based blockchain-based automated cooperation system, which consists of a basic public chain, Pyramid structure composed of DApps, merchants and customers. as the picture shows:

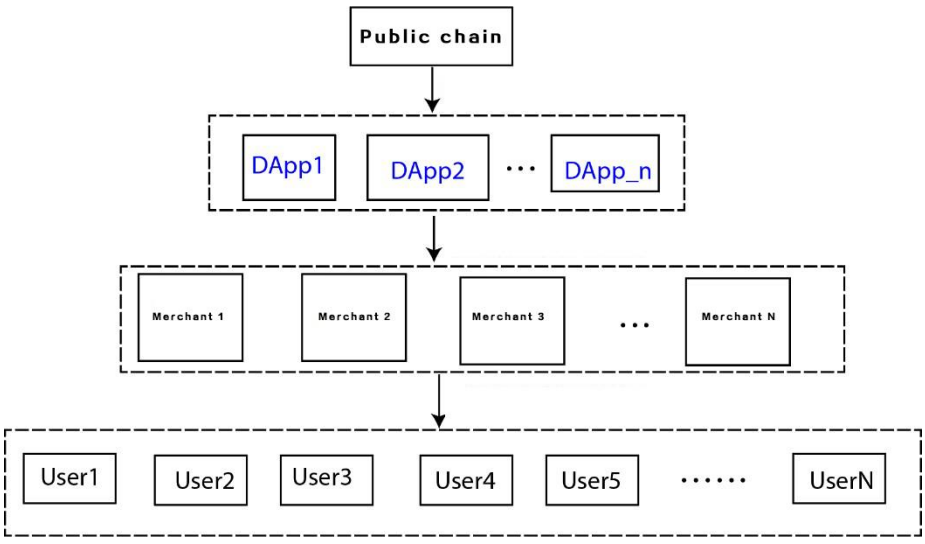


Figure 1. Blockchain ecological pyramid

It can be seen from the above figure that the direct service object of DNC is DApp. If DApp is mainly regarded as a developer (D end), and D end will be an entrepreneur in a human automation cooperation system, so the main service object of DNC is an entrepreneur. For this reason, DNC mainly accomplishes the following:

1: Provide the necessary functions for developers: For this, the blockchain needs to be fully functional and infinitely scalable.

2: Reduce the cost of developers: To this end, it is necessary to establish perfect support, including multi-language support, good documentation, test network, and a lot of open source code.

3: Importing traffic for developers: This requires users to be able to share. For this purpose, user information needs to be placed on the public chain.

4: Storage space can be subject to object management: the function of the database is the most basic function of various applications, and the readable and writable, space-based storage function will be necessary for developers.

5: Avoid developers from forming unfair competition: This requires that the data is not attributed to the developers, so that the developers can truly provide algorithm services. For this, the data needs to be placed on the public chain.

6: Add transaction objects that can enter smart contracts: This

requires the blockchain to have cross-chain functions.

7: Make the smart contract smart enough: This requires the smart contract to have the function of a prophet.

2.2.2. Space-based data storage: readable and writable storage space

The traditional Internet is based on the TCP protocol and C / S or B / S architecture, and has various vertical applications. However, because the server is at the core, and there is a lack of communication mechanisms between servers in different organizations, there is no way to establish intelligent and automated cooperation across organizations. The blockchain is built on the P2P network. Due to the equal status of the nodes, intelligent and automated cooperation across subjects (including individuals and organizations) is possible. The traditional Internet has a complete database system on which large-scale applications can be built. However, the blockchain system lacks a database system that can support large-scale applications, which makes it difficult to establish even large-scale cross-subject cooperation on the blockchain. . Therefore, the function that DNC must do is the function stored on the chain. In addition, in order for the data producer to become the controller of the data, the data needs to be stored in the storage space owned by the address. Therefore, the address needs to have the ability to apply for data storage space.

From the perspective of developers' data storage needs, these spaces need to be managed based on objects rather than files, so that the data can be defined differently when it is generated, and the management method is designed. A large number of applications need to update data at any time, such as communication, social networking, self-media and online stores, etc., and need to establish a readable and writable storage space in the background. Therefore, the readable and writable, space-based, object-managed storage sub-chain will be the first technical problem that DNC needs to break through.

At present, a large number of storage-oriented blockchain projects are based on IPFS and are managed on a file basis. They upload text encrypted and the public chain manages it in slices. The main purpose is to store certificates, not for developers. In this file-based management system, it is difficult to implement storage management based on storage space with high availability, readability, and objectification, and it is also difficult to implement a database system on it. Of course, space-based management requires space contribution management, space application management, and space read-write management. The complexity of setting up such a cloud service on a distributed system can be imagined, but it is based on space distribution. The storage system is a difficult problem that the blockchain must break through.

In the distributed cloud world, the space contributed by all the space

contributors will form a "world hard disk", which will be a large cloud space for the public chain, and the applicant only applies to use part of it, which requires design. A set of incentive mechanism, payment mechanism and management method make the reading and writing of data achieve high security and high availability.

The basic function of the blockchain in the future should be distributed storage, and distributed computing is not the most important part of the blockchain (although multiple calculations have a check function). A large amount of data can only allow individuals to master the data by using distributed storage, and the real realization of data is owned by the data producer when it is produced, and the real empowerment of individuals is realized. On the contrary, the centralized data storage makes the centralized platform occupy all kinds of data, which not only enables them to obtain benefits through the data, but is also at a single point of risk. Establishing a personal file system on a distributed cloud service not only allows the data rights to be generated by the generator, but also makes it possible for individuals to propose authentication and data transactions based on this space, and makes the social communication and transaction granularity smaller. For entrepreneurs, it is easier to build large DApps on it, which may lead to major changes in the way human society is organized. DNC needs to develop its own storage subnet, using space as the management object

and files as the object management, so that each user can easily establish his own data system, identity reputation system, communication system and transaction system on it.

2.2.3. Data confirmation based on address: Address is at the core

The blockchain system makes it possible for an address to have various functions. In the traditional world, when people want to interact with each other, they need to apply for accounts on different Internet platforms, and for value interaction, they need to apply for bank accounts. On the blockchain, people can have not only information interaction but also value interaction. Not only that, but also can easily publish various smart contracts for programmable value interaction. In addition, people can also bind their identities and addresses to assist in biometrics and establish their own identity system. However, in various centralized systems, people need to register multiple accounts, and the data is also divided and occupied by each centralized service organization. The interaction between organizations is difficult to achieve. Such a cooperative system is neither efficient nor reasonable, and There is a single point of risk.

In DNC, users can register their real-name addresses, such as michael.lin, and can also register some anonymous addresses such as john.smith for some anonymous social activities. We can make the

address be used as a communication account, social account, bank account, and personal cloud account, and use the immutability of the blockchain to make the blockchain data facilitate the establishment of identity and reputation certificates. Therefore, as long as the distributed storage and communication of address-based data can be realized, all these functions can be integrated into one address, so that the address plays a central role in human communication and transactions.

Address-based data storage and control also makes data authentication and flow sharing extremely convenient. Because the addresses of different DApps and the data related to the addresses are distributed storage based on the addresses, that is, these data can be stored in the user's own space. In this way, the data generated when the user uses the DApp can be confirmed when it is generated, which not only makes the value of the address more and more big, but also allows different DApps to read the data of the other user, which makes traffic sharing possible. Doing so also gives DApp the ability to challenge centralized platforms. The original center

The platform continues to occupy data through the "overlord clause" to enable itself to earn income mainly from data rather than services, and the new DApp can provide traffic for the original DApp when it is developed on DNC, and the new DApp It can also bring traffic to the original DApp. The data sharing about DApp is shown below:

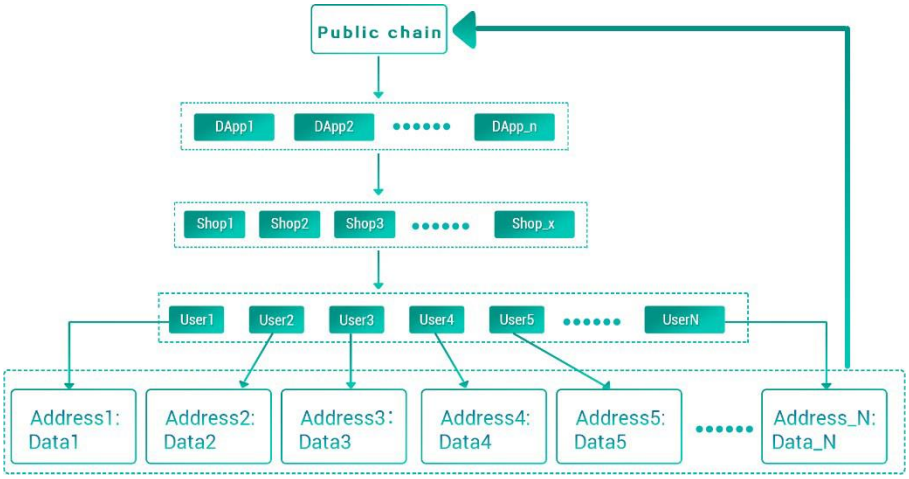


Figure 2. Customer and data sharing between DApps

DNC, on the basis of implementing distributed data storage, enables any DApp to have the ability to give address data storage, information exchange, value interaction, and identity verification, etc., so that any individual, organization, or even intelligent program, as long as there is an address Conveniently establish communication and transaction relationships with any other subject. Not only that, with the accumulation of data with the address as the core, it is also possible to establish a credible proof system of "good money drives out bad money" to make human cooperation move toward a virtuous circle. From the perspective of the subject of communication and transaction, as long as they have the ability to operate addresses, any subject can participate in the DNC system for communication and transactions. They may be individuals, organizations, or intelligent programs. The current world is a world dominated by various centralized organizations.

Blockchain is making individuals rise, and in the future intelligent programs will become more and more important subjects, but in fact it is not necessary to distinguish between people or intelligent programs behind the address, whether they are individuals or Organizations, as long as they apply for and own an address, they can achieve equal exchanges and transactions between these subjects.

According to Metcalfe's law, the more participants participate in a system, the more progress can be promoted. Participants, whether they are individuals, businesses, or smart programs, through the underlying blockchain code, they can freely express their views, sell products, and purchase products without restrictions from geography, institutions, and organizations, and make transactions more automated through smart contracts And intelligent, so that humans gradually establish large-scale, automated and deep cooperation.

2.2.4: Data sharing based on data routing: information exchange is fully supported by the protocol

The storage function of DNC enables data to be stored on the chain, and data routing is required when data is acquired. DNC designs a special data routing function that allows data to be accessed at any time and also enables information exchange between any addresses. In order to be able to achieve a smooth chat experience, current solutions

all require centralized storage or routing. DNC's distributed storage has been specially optimized for chat. Using specially designed readable and writable storage space and file database can achieve chat without going through a centralized server.

Information exchange, whether it is a two-person conversation or a multi-person conversation, whether it is text, voice or video, is extremely important for human transactions before, during and after the event. The characteristic of the information Internet is information interaction, and the value Internet is characterized by value interaction, but DNC, as a new generation of public chain, will break this boundary and integrate information interaction and value interaction.

DNC provides protocol-level communication support for DApps, so that everyone can encrypt and decentralize free communication with the world through the address. The communication data will only be owned by the producer. Anyone can establish a peer-to-peer rich media chat, multi-person group chat, and can transfer funds and interact with smart contracts during the exchange. It is important to integrate the communication function into the blockchain: before the transaction, you can contact the other party to negotiate the transaction, and you can easily establish the smart contract of the transaction in the session; during the transaction, the two parties can establish the transaction-related situation Chat, communicate the delivery situation or modify the

smart contract; after the transaction, all the objects that have been traded can be divided into different groups to facilitate customer relationship management.

DNC will support sub-real-time chat at the protocol layer, while DApp is based on Email and distributed storage functions, which can establish a point-to-point or point-to-multipoint relationship and conduct point-to-point or group chat.

2.2.5: The system is fully distributed and infinitely scalable

DNC V2.0 is completely distributed. DNC V2.0 is similar to Bitcoin and Ethereum, does not require any election of super nodes, anyone can participate in mining, and have the opportunity to receive mining rewards. Participants can choose to obtain resources from each shard participating in the consensus main chain or applying to participate in the functional sub-chain.

Whether it is a Windows system, a Pingguo system, or an Android system, you can share disks or participate in mining through DNC software, which greatly expands the distribution and scalability.
DNC is infinitely scalable. The so-called infinite scalability means that the blockchain system can continue to expand with the increase of miners and can support more users. DNC will use a sharding mechanism, so as the number of participating miners increases, each

function will be continuously expanded.

2.3: Address-based data system

2.3.1: Credit verification based on personal cloud space identity

verification, circle of friends and transaction records

People-to-people exchanges and transactions are inseparable from the reputation mechanism. Because people's communication and transactions often need to know who is the object of communication and transactions, so that the information can be more symmetrical in order to reach a transaction efficiently. For a well-functioning market, credibility is the most important mechanism for "good money drives out bad money". The blockchain should provide an interface for the reputation mechanism, so that people's reputation can change dynamically over time, and promote address owners to maintain their reputation.

Reputation is actually an evaluation of information (including identity information) of the address owner. To this end, as much information as possible should be integrated into the address, and DNC is based on the address as the core data storage, it is easy to pass a variety of information Proof of reputation (PoR). People can record their relationship with the world through voluntary information disclosure, or they can adopt a third-party identity verification mechanism to establish

their credibility. Different ways of proving the effectiveness are different. DNC proposes three types of proofs: weak proof, semi-strong proof and strong proof:

1: Weak proof: By publishing information by yourself, let the virtual world and the real world continue to establish contact, and prove yourself through the dynamic information of your life that is continuously deposited on the timeline. This is mainly achieved through social functions.

2: Semi-strong proof: Prove yourself by transacting with other addresses and providing transaction-related information (including comments from the transaction party).

3: Strong proof: establish a credible association between your address-related information and the real world to prove yourself. This method is mainly achieved by publishing its relationship with the address through a trusted channel or through third-party verification. For example, an organization can publish its own blockchain address on its official website, or a person can verify it by a special verification agency, and the verification agency can publish the identity of the real person corresponding to the address in its own information release channel. At the same time, the address owner can publish relevant verification information on his address to facilitate verification from other trusted subjects.

In order to complete the credibility certification, individuals can choose to store personal information, life dynamic databases and transaction data in their own spaces, and authorize them to different people for use. In the future, more and more people may deposit data in private data identified by addresses, such as:

1: Address book data: Give the address permission to manage the address book, one of which is to authorize relevant personnel to help transfer the data in the address to a new address, which can be used in emergency situations such as the loss of private keys;

2: Life dynamic data: endow the address with the ability to publish an immutable life dynamic;

3: Multimedia data: give the address the ability to publish text, pictures, voice, video and other media, and give the address the ability to customize tags and custom tamperable attributes

4: Product data: Give the address the ability to publish various products, including resources that can be shared, and store these data in the product database;

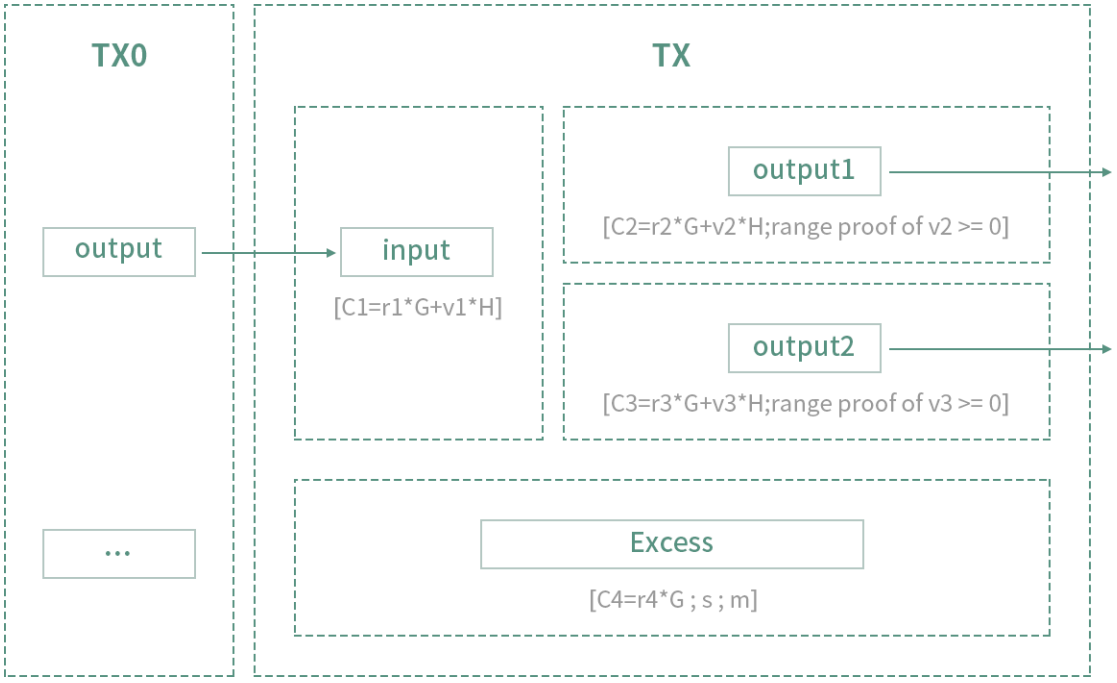
5: File storage space: Give the address application space and the ability to save various data. Since the file exists in the form of an object, the address can define its own database, which paves the way for the establishment of various DApp databases

6: Multi-currency wallet data: Give the address the ability to map

various tokens to the chain through cross-chain transactions to form its own multi-currency wallet database;

7: Coin issuing data on the chain: giving the address the ability to issue coins with one click and storing the relevant data in the coin issuing database;

8: Smart contract data: Give the address the ability to generate smart contracts, and save the relevant information in the smart contract database.



Reliable privacy protection and permission control

Since the data is stored in a private data set after it is generated, this solves the problems of data privacy protection and confirmation, and also paves the way for data transactions. Only the data that the address

is willing to open will be disclosed. The address can also selectively open the data to the specified address and form its own data sharing circle. For example, the life dynamic data can only be seen by the specified friends. These shares can also set the time limit of access or pay to view, thereby forming various types of data exchanges and transactions.

In the future, there may be specialized data second traffickers, who are constantly acquiring various types of desensitized data from individuals, thus making data truly a service industry.

2.3.2: Address alias, communication account and help recovery function

The main function provided by DNC is user-oriented communication and communication, and user communication and communication need to bind users with a memory-friendly ID, rather than boring binary address strings. So DNC provides address aliases as a more friendly interface.

Since the communication requires the other party's public key encryption, the address will also be able to apply for a special communication account and the communication account can be in the world state for encrypted communication of data.

If you have the private key, you will have everything, but if you lose

the private key, you will lose everything. To avoid this tragedy, DNC will design the address to specify other addresses to join the multi-signature, so that when the private key is lost, the private key of other addresses will be lost after a certain period. Can help authorize the ability to transfer data or account balances to other addresses.

2.4: Design goals

Although blockchain has been considered to have the potential to subvert the existing business model in recent years, the underlying technology of the public chain is not enough to support large-scale commercial applications. The most prominent technical problem of the blockchain is the low system performance. Taking Ethereum as an example, all the applications running on the entire network can use about 10 transactions per second, but for an application with a daily activity of 10 million levels, the peak TPS requirement is generally around 2000-3000, so now Some blockchain 1.0 and blockchain 2.0 systems represented by Bitcoin and Ethereum are completely unable to support large-scale commercial applications.

And why is it so difficult to break through the limitation of TPS? Just like the “impossible triangle” problem that all distributed systems will face in design, blockchain systems will also face their own impossible triangle: decentralization, security and high performance.

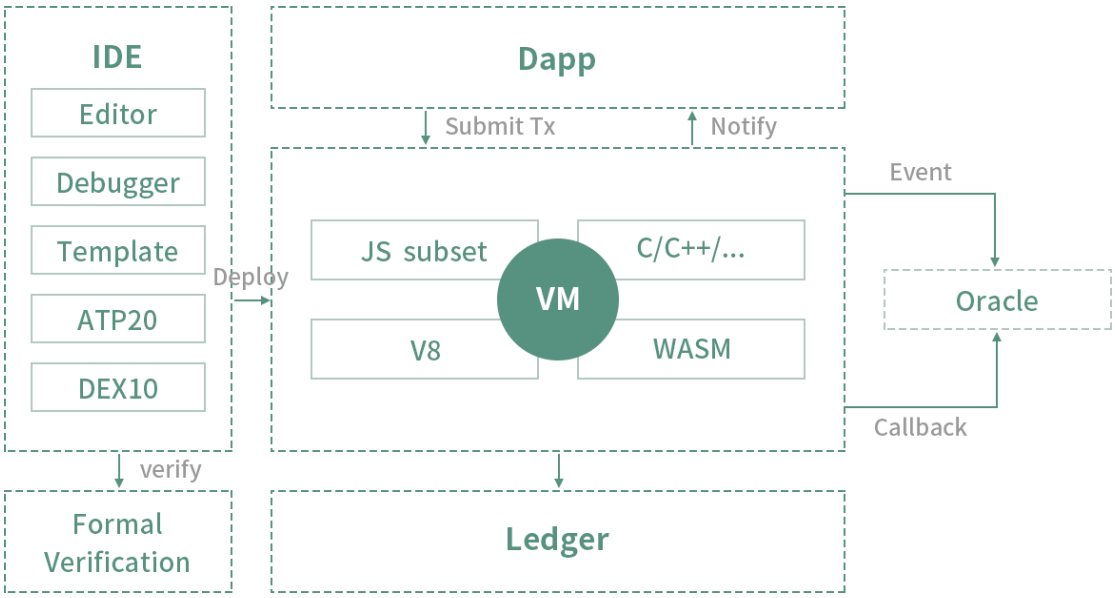
1: The decentralized design challenge is how to ensure the

decentralization of the network. This requires that the network needs to be a peer-to-peer network. The status of the machines in the network is equal, and there is no special central node. At the same time, in order to ensure the decentralization of the network, the network needs to be an open network without access, so that everyone can join the network, and the network will not be controlled by one or more centers;

2: The design challenge of security is to ensure that the network is secure enough to be easily destroyed by others. In an open and economically linked network, not only will good people buy machines to join the network, but there will also be more bad people trying to profit by destroying the network. So, how to ensure the security of the network when there are bad people inside the network, which has broken through the traditional security architecture and is a challenge for security design;

3: The high-performance design challenge lies in ensuring that the network is adequately decentralized and secure as much as possible, ensuring the best performance and lowest network energy consumption.

In the impossible triangle of blockchain, Bitcoin and Ethereum have chosen enough decentralization and security, while EOS has biased efficiency and sacrificed some decentralization and security.



Application development friendly smart contract

The goal of DNC is to build a communication and trading platform with blockchain technology. On this platform, data assets, multiple tokens, goods and services can interact freely through smart contracts, balancing the three corners of the impossible triangle in a good balance. Under the circumstances, to realize value intercommunication. Specifically, it includes the following technical requirements:

System functions

With infinitely scalable transactions and Turing complete smart contract functions.

With convenient data saving function.

With convenient asynchronous communication function.

System characteristics

The system is stable and highly concurrent.

Distributed applications are easy to develop and deploy.

Can be as modular as possible to facilitate system upgrades and maintenance.

Scalability

It can meet the needs of large-scale communication and transaction applications.

It can maintain a reasonable energy efficiency ratio when the system reaches a large scale.

In the case of the expansion of the system's own scale and application scale, the block generation efficiency, storage efficiency, and communication effect can be maintained well.

With the addition of more resources, the system can be infinitely scalable.

Safety

Can prevent double-flower attacks.

Can prevent witch attacks.

Can prevent other attacks that reduce efficiency or system paralysis.

2.5. System architecture

Based on the above analysis, the system must have at least one storage subnet, shard transaction sub-chain, coordinating shard main chain, smart contracts running on each shard and address-centric user

support system. The following diagram can summarize the main architecture of this fully functional blockchain.

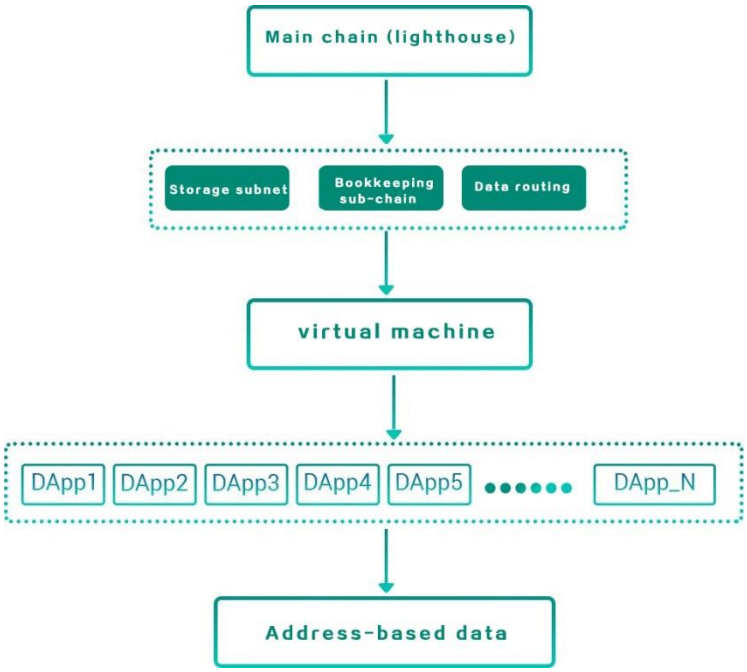


Figure 3. System architecture

The following chapters, in terms of technology, will mainly discuss how to implement space-based storage, how to implement sharding, and how to implement personal cloud-based communication. The economic model will discuss the token economic model and the future plan of the project.

03 Space-based storage

3. Space-based storage

3.1. Storage based on peer-to-peer network

3.1.1. Architecture of the storage chain

Traditional blockchains mostly belong to the status block chain (Status BlockChain), from the single state of the number of bitcoins in Bitcoin, to the state of the smart contract world of ethereum. All follow the logic of state storage.

Starting from IPFS, a data block chain (Data BlockChain) has emerged. The data block chain uses the attributes of data as a state to conduct transactions and storage. From a storage perspective, IPFS implements object storage, and its object is a file . Two kinds of miners are proposed, one as a storage miner to save file data; one is an index miner, which is mainly used to save file description information (file owner, number of shards, shard hash and other attributes)

The concept proposed by DNC is not object storage, but a pure spatial storage. It does not target specific storage objects, but provides available storage space. Users can use the storage space like a local hard disk and use it to store various data objects, and this space is provided by distributed miner nodes.

The following figure is the architecture of DNC's storage subnet:

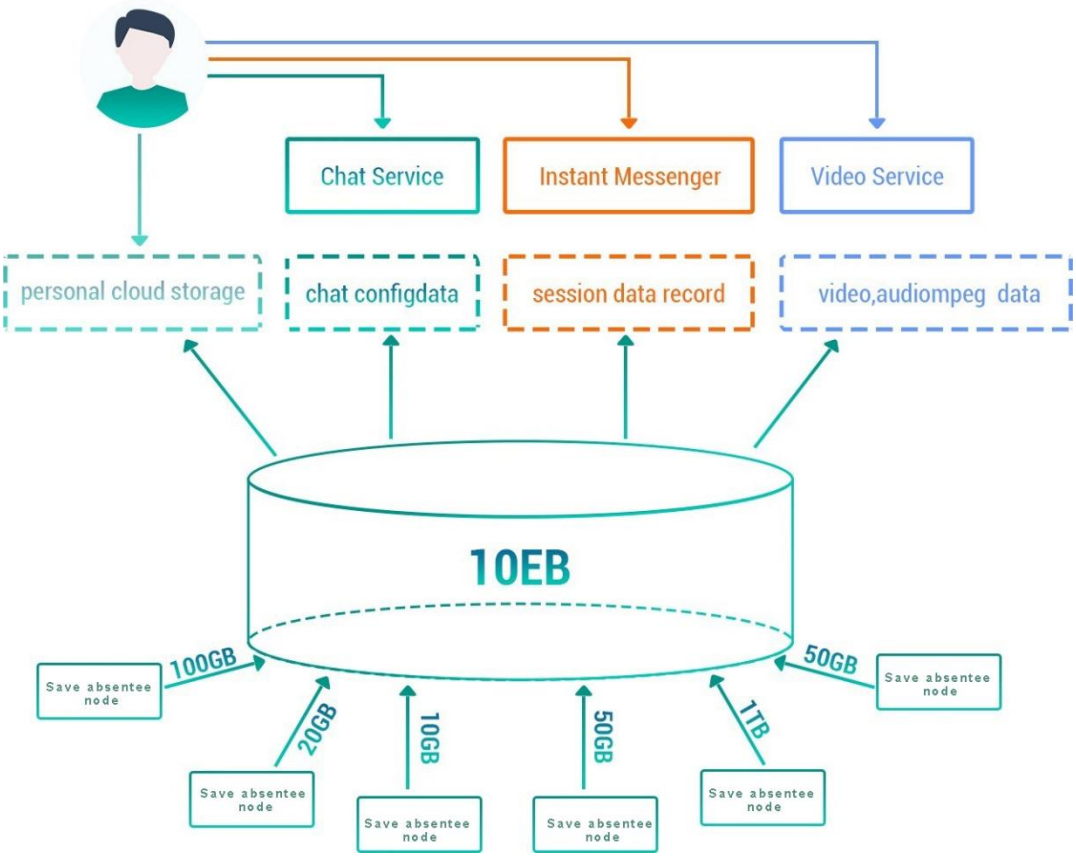


Figure 4. DNC storage function

As shown in the figure above, storage contributors (storage miners) provide their own hosts or nodes with free storage resources. DNC aggregates the miners' resources to form a large-scale storage cloud.

With a large-capacity storage cloud, wallet (terminal) users can extract a virtual storage space (such as 1GB) from the cloud to form their own cloud disk. Users can plan to store files in the space themselves, and can save large-volume files. For example, audio and video data can also save a large number of small files. The uploading and downloading, addressing, using, managing and maintaining of

these files or data are all planned by the users themselves in the virtual cloud disk. There is no need to perform complex market transactions like IPFS to complete the storage of a small number of files.

In addition, with the distributed storage cloud, we can construct more complex distributed services on it, such as chat rooms, instant messaging, audio and video services, and so on. These traditional centralized services have the opportunity to achieve decentralization after solving the storage pain points.

The main task of storage miners is to maintain and maintain the physical space provided by them and the virtual space of mapping management, so that they can continue to provide services online to continuously obtain mining income.

The role of the storage sub-chain is shown below:

From the above figure we see four roles, Wallet means front end, Farmers means storage space service provider (also known as landowner, ie landowner), Miners means blockchain service provider, and there is also an important role It is a "Data Gateway", also known as a data agent, which provides the function of data routing.

3.1.2. Data agent

If there is no data agent, when users want to write data, they need to take a complicated network path to establish information query before

they can start transmission. This will undoubtedly bring a very severe test for the user experience. In order to make users take shortcuts (Shortcut), you need to help the agent to complete in advance, and every visit in the future will be familiar. The agent prepares various information queries and paths for the data objects frequently accessed by the user. When the user makes a request, the waiting time will be greatly shortened and the experience can be greatly improved. Taking the Email service as an example, the agent can provide reading and writing of the mailing list space belonging to the user, thereby greatly speeding up the delivery speed of the mail.

Therefore, a "centralized" private employment service is formed between the user and the agent, which is equivalent to the user being able to find a data service provider providing exclusive data services on the network through transactions (spending DNC currency). The service provider is mainly responsible for the construction, transmission and simple list management of the data access path of the employer.

3.1.3. Storage miners mining

DNC divides the virtual storage space into Chunk. After the storage miner determines to provide a certain amount of storage, he can claim the Chunk that provides space. For example, Miner A determines to provide 1GB, which is allocated to Chunk N by the algorithm.

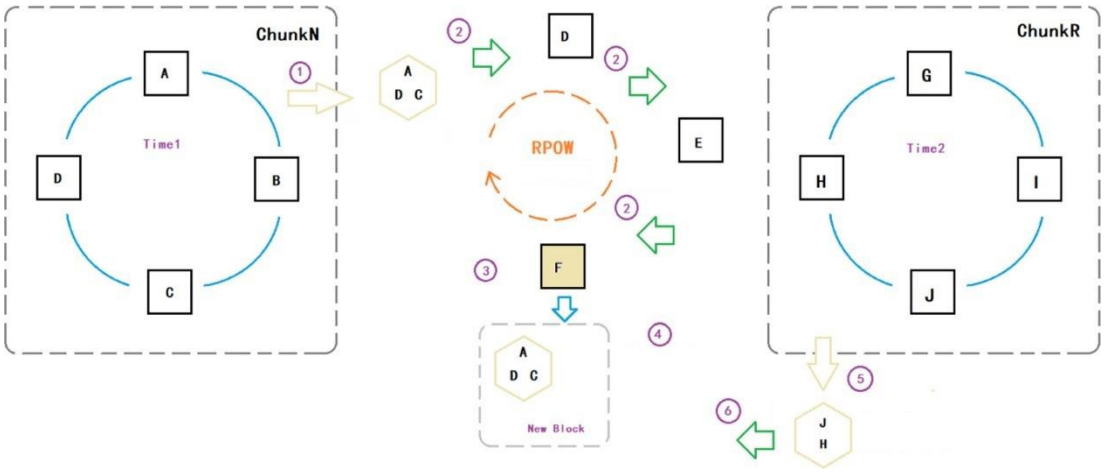


Figure 6. Schematic diagram of storage miners mining

(For example, Chunk N is 3GB 4GB range of virtual space). Miners claiming the same Chunk form data copies with each other, which we call a copy group (Chunk Copy Group). As shown above, claiming storage nodes A, B, C, D and G, H, I, J in different virtual spaces form ChunkN and ChunkR's two copy groups.

At Time1, the four nodes ABCD of the ChunkN copy group mutually verify the data. They provide each other with the Chunk on-chip data offset and data size calculation hash associated with their own Id and the current block hash, and hand the hash to other nodes for verification. , Sign and continue to pass after verification, and discard if not passed. When the number of signatures reaches 2/3 nodes, the authentication can be considered as passed. In the figure, three nodes A, C, D in ChunkN pass each other's data verification and successfully sign. So the signature was packaged into a "spatial verification transaction". Broadcast this transaction among all miner nodes.

In the end, the "spatial verification transaction" is packaged by the miner determined by RPOW in a new block. The new block packages this verification transaction into the block and then broadcasts the whole network. The node that receives the new block rewards tokens based on the accounts associated with the three storage nodes A, C, and D included in the space verification transaction in the block. So keeping the storage space online can generate revenue.

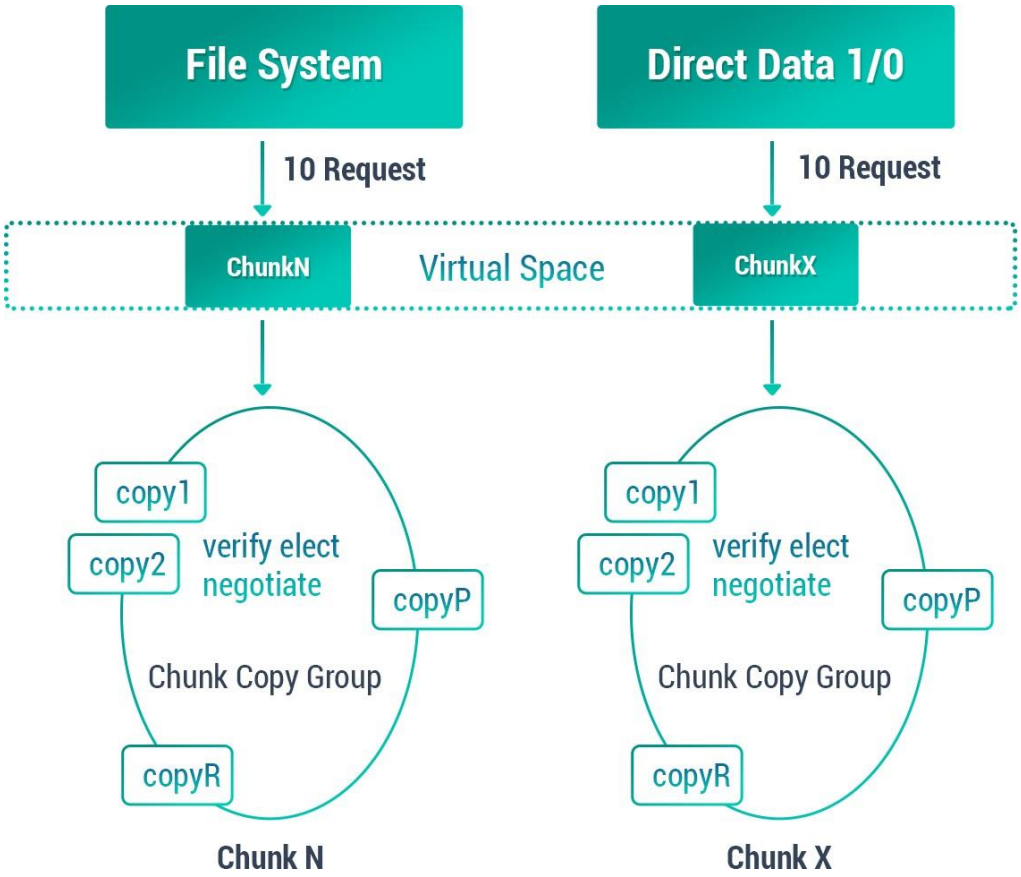


Figure 7. Schematic diagram of storage miner verification

3.1.4. Fragmentation and encryption

The storage sharding adopts the spatial sharding mode, which is

different from the file sharding of most public chains today: traditionally, the file is divided into several equal-length fragments and distributed on the network. When downloading and reading, it is read in parallel to local splicing. The advantage of this method is that it is simple and straightforward to implement, Merkle integration of file fragment content hash to ensure the consistency of file data. Multi-segment downloading at the same time downloads also improves the reading speed; The large number of large file fragments is relatively difficult to maintain; while the file size is fixed, its storage mode is limited to read-only. Generally, file modification is not supported, and it can only be applied to archive scenarios. From a functional perspective, the description is equivalent to network file storage, which is consistent with the traditional P2P file model. The benchmarking centralized service is similar to FTP.

DNC does not aim at files, but proposes a way to access storage space. Storage chain miners obtain tokens by sharing the free storage space in the disk. Different from the idea of IPFS and other storage products, no matter whether there is file upload or not, the space can bring value to the miners. Countless storage on the network together builds a huge virtual disk. Divided into spatial slice Chunk collections, the resources of the storage miners on the chain are associated with Chunk to form a huge storage pool. Why is it providing a storage pool?

With this distributed virtual cloud storage pool, users can allocate the space they want, and they can freely read and write files or data in it. From this perspective, it is for users. It is more like a cloud storage device than an FTP server. On the block storage device (Block Device) in this chain, we can construct a simple File System on the storage terminal and use it for storage.

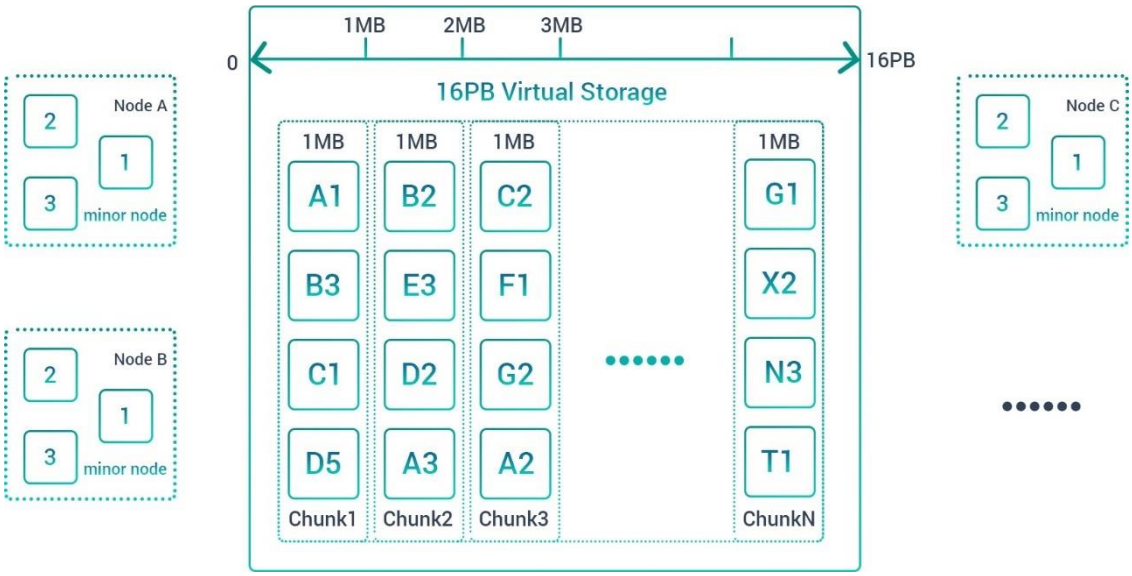


Figure 8. Fragmentation and encryption

As shown in the figure above, there are many chunks in the 16PB virtual space. Each chunk is a fixed capacity (such as 1MB). For storage miners, the way they contribute space is to contribute block copies. Each chunk in the figure has It is composed of block copies contributed by multiple miners, so Chunk is a logical concept, it represents a segment in the virtual space, for example, Chunk1 represents the 0-1MB

segment in the virtual space, and Chunk2 represents 1MB in the virtual space -2MB of space ···; each chunk can be constructed by 1MB blocks provided by multiple miners, the number of copies is scalable, and different claim strategies are made according to different thresholds.

3.1.5. Grouping of miners

Storage miner grouping involves two levels:

1. Using Chunk management, gather all nodes involved in maintaining the same data together to become a Chunk maintenance group

2. In order to ensure high availability of data, the number of Chunk space copies is relatively large, which means that Chunk management information also needs to occupy a relatively large management space (memory and storage).

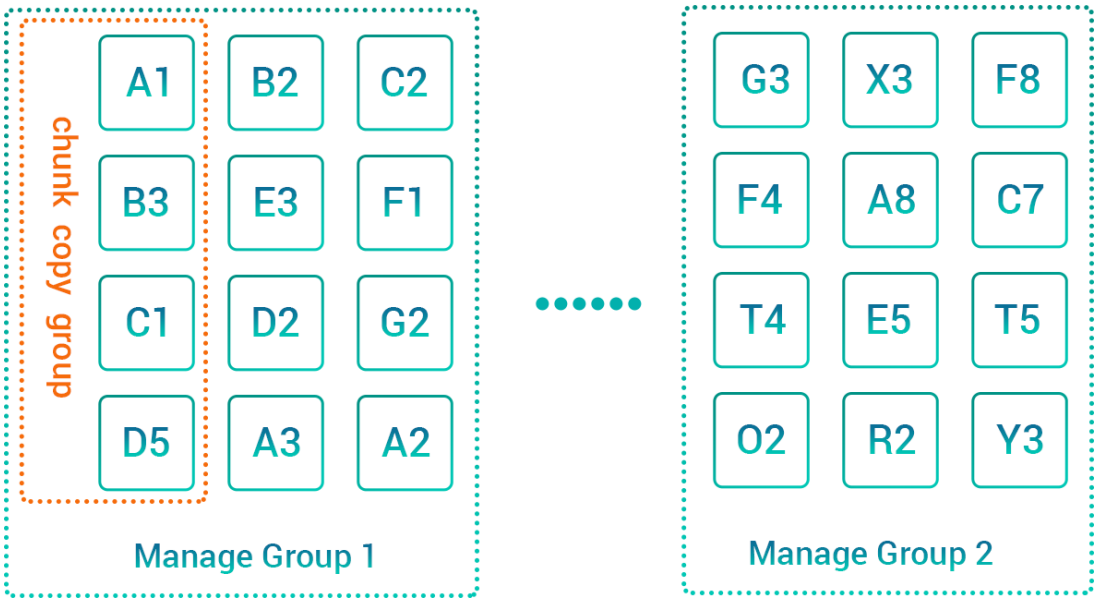


Figure 9. Fragmentation and encryption

For the same miner node, it is the space carrier provider of each chunk. It participates in all the chunk copy groups that it claims (provides space). In this group, it synchronizes data with other nodes participating in the same chunk. Maintain high availability of the same chunk.

For each chunk, it is necessary to record the status of their replica participating nodes. According to the correspondence between the ChunkId and the NodeId of the miner node, DNC divides all the Chunks into a number of Manage Groups, which are handed over to a group of miner nodes for information recording and management . This allows miners to form a management shard for Chunk and a sharding mechanism for the storage blockchain.

The sharding mechanism of the blockchain is to improve the overall operation efficiency of the blockchain, so that more information and transactions can be processed in parallel.

3.1.6. Data download

For data download, user nodes request data from a group of Chunks based on data requests (from File System, or direct data access from the upper layer).

For all nodes in the same Chunk Copy Group, the requesting node sends a command to request the Id and current status of the current

update block. After the request is successful, the nodes with the largest and equal Id and status "status online" are classified as data The providing node divides the download request into different fragment requests according to the data size requested from the chunk. At the same time initiate a data transmission connection to them.

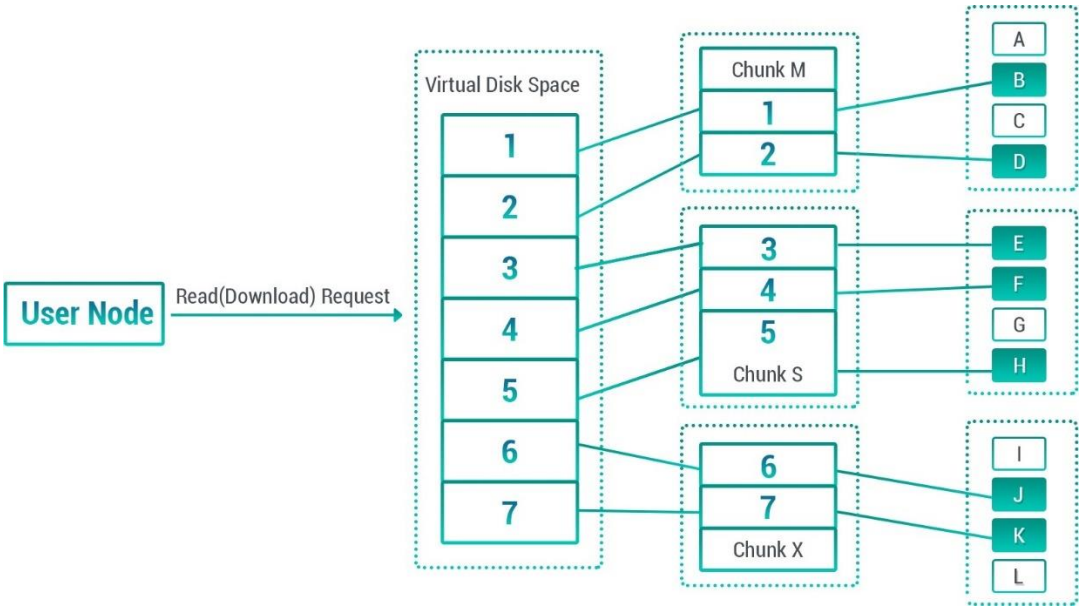


Figure 10. Data download

3.1.7. Data upload

As shown in the figure above, there are many chunks in the 16PB virtual space. Each chunk is a fixed capacity (such as 1MB). For storage miners, the way they contribute space is to contribute block copies. Each chunk in the figure has It is composed of block copies contributed by multiple miners, so Chunk is a logical concept, it represents a segment in the virtual space, for example, Chunk1 represents the 0-1MB segment in the virtual space, and Chunk2 represents 1MB in the virtual

space -2MB of space ···; each chunk can be constructed by 1MB blocks provided by multiple miners, the number of copies is scalable, and different claim strategies are made according to different thresholds.

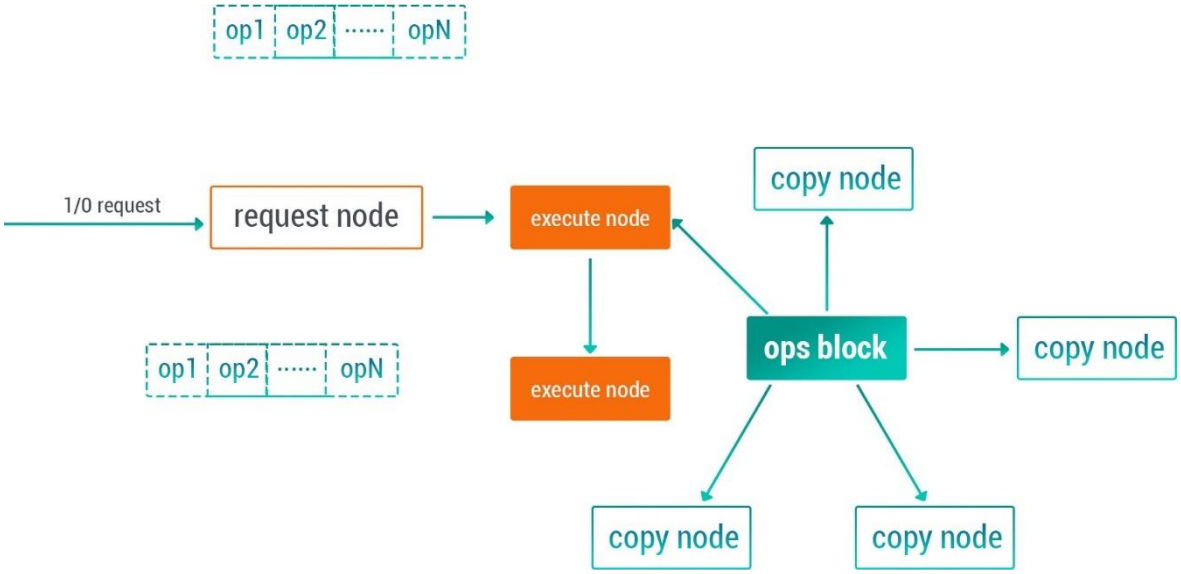


Figure 11. Data upload

Data writing process description:

We divide Chunk into several slices, and slice is the basic unit of user-side operation. Slice's OwnerId is the tenant and user of this slice. Only he has the authority to update and write this slice. The service model is like this:

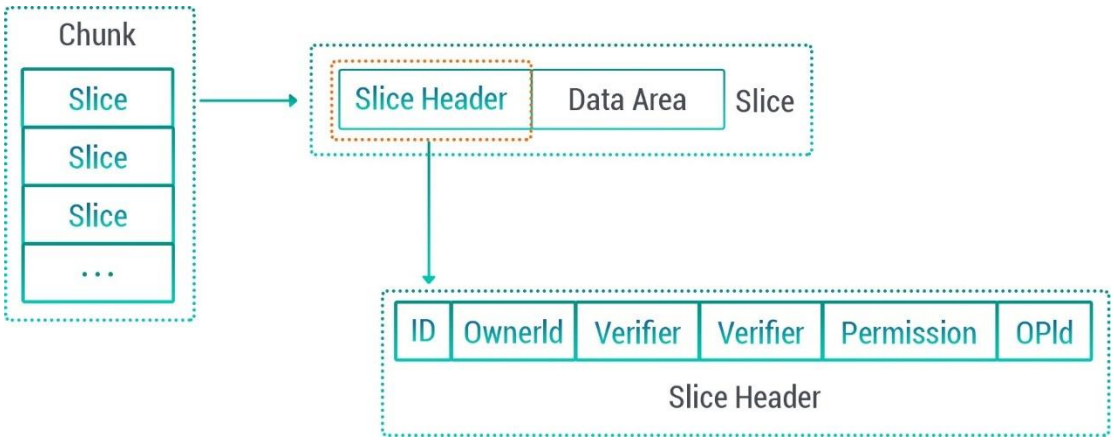


Figure 12. Data upload (continued)

Figure 13. Data writing

For Chunk, users directly access the slice on the storage node, so there are no obstacles and deception. For session services, the service model becomes as follows:

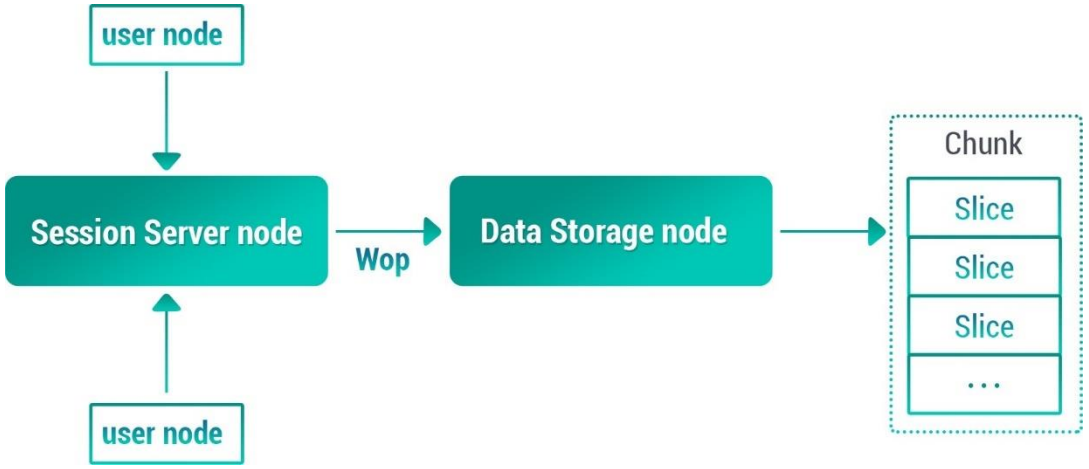


Figure 14. Data node access

As shown in the figure, all users must communicate and communicate on the channel server of the session service node, and the session file data needs to be submitted to the storage node by relying on the session service node.

The session service node is a node randomly selected from the channel blockchain based on dynamic routing, and its behavior is

unpredictable, so we cannot fully trust that it will not do evil. Although the session content is transmitted encrypted, although it cannot spy on the session content, it can maliciously destroy the session data on the storage node when writing.

The requesting end broadcasts to the member nodes of the same block replication group by constructing an initiating inquiry instruction broadcast, and notifies them of the operator Id. Each node receives an instruction, and if no one is currently using it or the most recent operation has timed out from the current time, the signature is accepted. Send the signed response message to the requesting end through active path finding or return to the requesting end according to the original path of the broadcast path. After receiving a sufficient number of signatures, the requesting end packs all the signatures to form an Open command and broadcasts again. Each node checks the verification signature And confirm the quantity, if you agree with 2/3, then set the operator ID to the memory.

Design of block copy synchronization: treat all participating nodes of the same block data group as a micro-blockchain for this data block. The blockchain uses a semi-cached synchronization strategy. Each group node can be collected from each The Wop request on the requesting end, after collection, starts broadcasting these Wops to the execution node of the current block; after the execution node collects the request, it packs

them into operation blocks according to the receiving order (using sorting to eliminate the possibility that multiple nodes may generate the same virtual write Conflict), packing and filtering out operations that do not meet the shard permission setting

Each group node can be called a copy miner. It collects Wop requests from other group nodes. When the number of Wops meets certain requirements (N> 0) and the collection time meets certain requirements, it sends the original Or, the Ids of the Wops received from other nodes are packaged into block broadcasts to other nodes, and at the same time, each Wop is executed locally according to the order of the Wops in the block.

If a group node creates and executes its own generated block, and then receives a broadcast block from its group node, it needs to first determine its own priority. If a node is down, then no block can be generated within its time window as an execution node, and all operations will have a certain delay. Aiming at this high delay characteristic.

Figure 15. Sequential execution

The upper-layer application should first buffer the data before

loading it, try to reduce the number of loading times, and merge most operations together.

For the newly added group node, a data download process is required. It selects a smooth communication node from the group node as the data service node and starts to download the complete data of the chunk from the beginning; at the same time, it also needs to Join this cluster and become a quasi-cluster member node (semi group node). It needs to save all the blocks in the download process while downloading the data. After downloading the data, execute all the blocks locally, so that the overall synchronization can be completed and keep up with the rhythm of other replica nodes. .

The implementation node election rules are more particular, and all group nodes may have a larger number, such as 32. If a simple round robin strategy is adopted, in most cases, the node that receives the IO operation request is a few nodes bound to the app node (a chunk may be used by multiple tenants at the same time, and the operator is not unique); A leader needs to be elected as the execution node of this replica synchronization group. Election process: When the tenant writes data to the virtual disk, it will first call an Open method. The Open method will query all the replica node nodeIds where all participating Chunk information is located, and send Open messages (with chunk, slice), The storage node finds the corresponding local storage record

from the local disk according to the (Chunk, slice) information carried in the message and compares the owner and attributes (read and write permission attributes, etc.). Action; if the verification is successful, add this node to the execution node group of the (Chunk-Slice), and make the message known to all the nodes, and the members of the execution node group in a slice will rotate out of blocks Block success is division of labor broadcast: the broadcast mechanism can be set to query delivery mode, because it involves bandwidth and traffic, so communicate before sending, instead of directly throwing data, for the group node, try to select only 1-2 subordinate nodes Data transmission, and then further transmission by the lower node.

From the above description, the write operation process is more complicated, if the application layer uses synchronous waiting, it will make efficiency

The application layer should use the cache operation method. After submitting all the cache operations at once, on the one hand, it continues to wait and add new operation instructions into the cache area. Zone cleared.

3.2. Proof of space-time, proof of existence, and proof of availability

3.2.1. Proof of space-time and existence

atial synchronization is divided into three types of synchronization:

1: No space-time proof is used. In this case, the space only exists as a resource, and it has not been rented by the user or has not been written yet, so it cannot be verified by a certain set of data. Self-verification mechanism.

2. The space-time certificate that is already in use indicates that the space is already in use, indicating that the Chunk has been leased by the user and has submitted (file) data to the space, so synchronization and verification are based on these data.

3: The space that is being read and written proves that the group node that is being read and written is recognized only after the majority of the nodes are updated.

The space provided by any space provider is filled with data, which may be user data or automatically generated fill data. The blockchain will periodically initiate (for example, every 20 blocks) a random spot check to allow mutual verification within a data group, and the majority is considered to be a trusted node and can receive space rewards.

3.2.2. Proof of availability

The user of the data space will submit a service data during the use of the data agent every time it is completed, and write it to the world state. The mainnet will automatically blacklist the space miners with poor service experience. The worse the service quality, the faster the

submission speed of the service quality, the quicker it is to find out the black sheep. Over time, it is difficult for untrusted space miners to cause harm to the system.

3.3. Incentive mechanism and payment mechanism

3.3.1. Space usage mechanism

The space usage mechanism is as follows:

1: First space usage: Users use DNC to pay for their storage objects according to the length of time and space size according to the built-in price formula, pay to deposit in the fund pool, and confirm the storage object expiration time stamp when the block is packed.

2: Spatial adjustment: When the object expands or shrinks, the timestamp is changed according to the pricing formula according to the object change and additional DNC.

3: Space lock: After the timestamp expires, the space access right is automatically locked, and the space will be used as an application space mark.

4: Space reclamation: When new space is claimed, the free space will be used first, and then the space that expires earlier will be used.

5: Space unlock: When the user applies for renewal, if the original space is not recovered, it can be recovered again, but the space cost from the expiration to the current time needs to be paid.

6: Landlord Reward: Multiply the price by the amount of each block that has been purchased and used to cancel each time to obtain the total reward, and confirm to the verified landlord through a random verification mechanism.

3.3.2. Relevant variable conventions

All paid transactions for space purchases will be completed by special algorithms and recorded on the main chain. The payment will go to a special account called "fund pool". The fund pool records space purchase behavior. The following uses mega-days (MD) as the unit of measurement for space usage rights. Mega-days represent the usage rights for one mega-space per day.

Variable assumptions are as follows:

1: W: Assume that the total space of the world hard disk that the user can use is WD, and the unit is MB bytes. This data is corrected once per block and recorded by the block header. Worlddisk first letter.

2: t and T−1: Represent the timestamp of this block and the timestamp of the previous block, respectively.

3: T: is the total number of trillion days in the current block. Here, the maximum storage period that a space object can apply for is within 365 days from the time of transaction, so the maximum number of megadays that can be provided by each block cycle is 365W. We use T

to represent the right to use this space. Block correction once. T = T−1 + (W − W−1) ∗ (t − t−1) / (24 ∗ 60 ∗ 60). T−1 is the total number of mega days in the previous block, and W−1 is the total space of the world ' s hard drives in the previous block. (W0 − W−1) ∗ (t − t−1) / (24 ∗ 60 ∗ 60) adds or subtracts mega days to the current block. T is the first letter of Total.

4: B: It is the number of mega days that the current block has been purchased and is still usable. This data is corrected once per block and recorded by the block header. B = B−1 − B−1 ∗ (t − t−1) / (24 ∗ 60 ∗ 60) + ΔB. Where B0 is the number of mega days that have been purchased and still available for the current block, and B−1 is the number of mega days that have been purchased and still available for the previous block, B−1 ∗ (t − t−1) / (24 ∗ 60 ∗ 60) indicates the used megadays that need to be cancelled in the current block. ΔB is the number of new purchases in the current block. B is the initial letter of Bought.

5: R: indicates that the current block is not enough to buy trillion days, including free space and space that has expired. Residual initials. R = T-B

6: M: indicates the number of DNC tokens in the current block fund pool.

7: p: indicates the current block storage unit price, the use price per

trillion days, the unit is DNC, here represents the hard disk user, that is, "citizen" "rent" fee per trillion days.

8: r: Represents the unit rent of the current block, the rental income per mega-day, the unit is DNC, here represents the hard disk provider, that is, the "landlord" income of "rental" per mega-day.

3.3.3. Requirements for the price function of space use rights

Terabytes price is the key to adjust the use of storage space, the price adjustment should be satisfied with the following conditions:

1: As the demand for use increases, prices continue to increase in a non-linear manner, so that the space is always in a surplus state.

2: As the demand for use increases, the rewards for space-time verification increase to encourage more landlords to stay.

3: The space rental price is within a reasonable range.

4: The space rental price is in a relatively stable state.

3.3.4. Bancor payment mechanism

If the time that each storage object can store is unlimited, it is difficult to manage the inflow. If it is stipulated that the storage time of each object is at most 365 days, and the excess needs to be renewed, the total number of mega days that can be purchased is T = 365W. Since there is a fixed total number of mega days in each block

generation cycle, it is possible to use a Bancor-like mechanism to price mega days in each block generation cycle.

Bancor is a project of Ethereum, a currency system that provides continuous liquidity for digital currencies through smart contracts. Bancor solves the liquidity of digital currencies with small transaction volume. It does not require third-party institutions or second parties, and can buy and sell tokens through smart contracts. But at the same time, Bancor's automatic adjustment mechanism makes automatic price discovery and autonomous flow mechanisms possible, and also makes it never sell out.

The following uses the Bancor mechanism to price trillion days in a certain block generation cycle.

Bancor requires a constant term: $c = M / (p * T)$

The price formula can be deduced by the above two formulas: $p = M / cR$

When the value of parameter c is different, the price curve changes as follows:

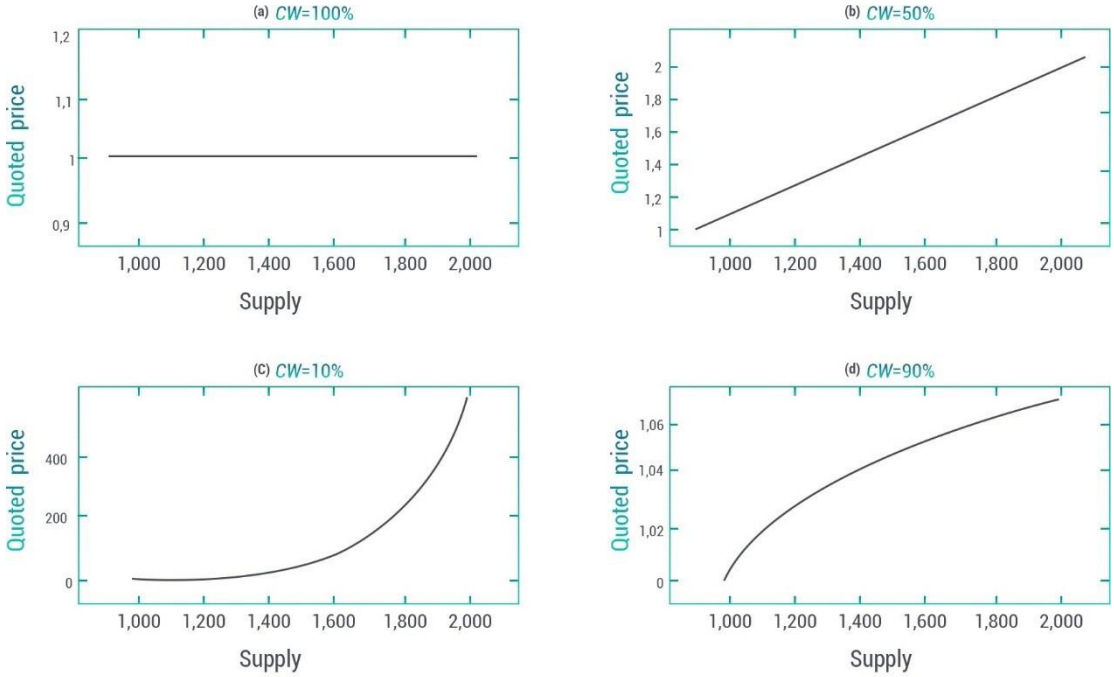


Figure 16. Price charts with different constants

Where CW represents a constant:

- When CW = 100%, it can be considered that the issued token is an alias of the connector token. No matter how the demand changes, the price of the issued token is always equal to the price of the connector token.
- When CW = 50%: the issued tokens have a linear relationship with their supply.
- When CW <50%, CW = 10% in the figure, as the supply increases, the price increases rapidly.
- When CW> 50%, CW = 90% in the graph, as the supply increases, the price changes little.

We can set the constant in the reference Bancor, package c to about 20%, so that when there are few people using storage, storage is cheap, but the more users, the more expensive it is, and it increases nonlinearly.

Since every purchase of a mega-day in the Bancor protocol will cause price changes, we use a simplified algorithm, that is, the price is the same every time the block is produced.

3.3.5. Landlord rent, landlord subsidy, and donation channel

Landlord rent

Since the world hard disk utilization rate is B / T, but the cost of the entire hard disk needs to be borne by real users, it should be paid by the fund pool.

Since each block has freely destroyed the expired right of use according to the time stamp, these destroyed parts should be paid to the hard disk provider. The number of mega days it needs to pay is:

$$r = (t - t-1)/(24 * 60 * 60)$$

For the liquidation of the previous block, the megabytes sold in the previous block are B−1, and the tokens that have been earned are M−1, so this part of the megabytes should be paid proportionally from the asset pool, which should be The rental cost is:

$$r = M-1 * ((t - t-1)/(24 * 60 * 60))/B-1$$

These fees will be distributed at each block time to reward verified l andlord wallets.

Landlord subsidies

In order to make the space always have a certain surplus and make the storage space in the early stage of the project relatively cheap, within a certain period, a certain amount of capital is regularly added to the capital pool so that the entire ecology can subsidize the landlord.

Donation channel

Distributed storage is the foundation of the project and the dream of many people. We can add a donation channel so that currency holders can donate funds to the fund pool.

04 Distributed communication based on distributed storage

4. Distributed communication based on distributed storage

4.1. Asynchronous communication: Email

Distributed Email mainly uploads short messages (currently defined as less than 1k) to the state of the world by doing transactions, and large messages are used as attachments to be downloaded from the personal cloud space of the recipient to the sender. The download is divided into free and paid, and the data is encrypted and protected by the public key of the recipient. In the case of payment, only paying the fee can have access. In this way, data transactions can be realized. Because of the need to know the public key, any address can apply for an additional email address and email alias, and write the public key of this address into the world state.

4.2. Framework of data routing

Distributed social networking, as the name implies, is mainly manifested in the form of instant messaging. The oldest instant messaging appeared in the 1990s. The peer-to-peer technology used by the conversations established between users does not provide server forwarding in the middle, which is what we often mention. To point-to-point technology. The server only serves as a bridge between users' computers to find and locate each other. Although most of the functions of instant messaging will be mainly implemented by DApps on it, DNC has the ability to provide distributed communication

because of its distributed storage function.

As shown in the figure above, the AB node only transfers its IP: Port to the Server by logging in to the Server. When establishing a Session session, it obtains the address of the other party from the Server and they establish direct communication. The advantage of this is that the communication between the two parties of the AB is independent of the server, and there is no privacy disclosure.

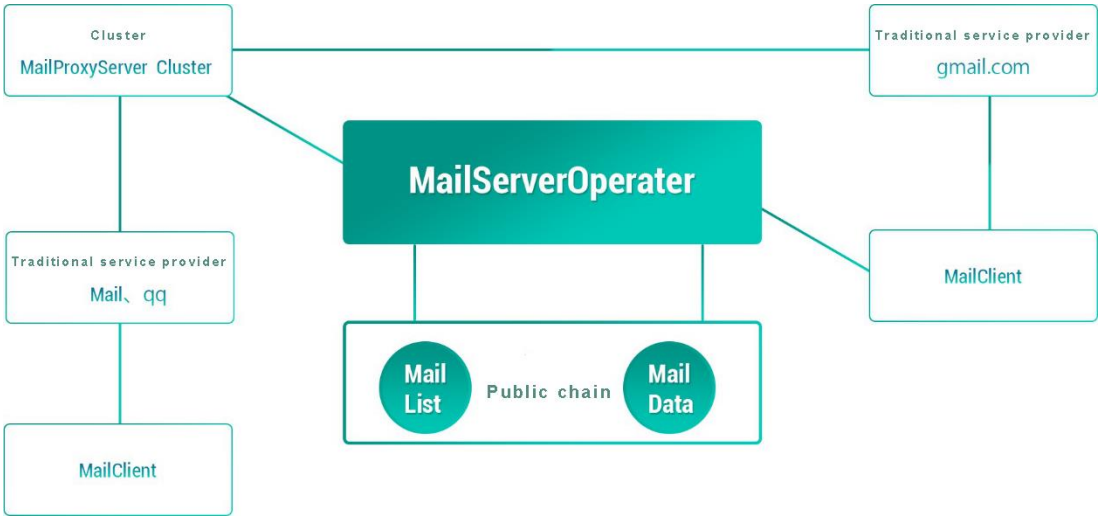


Figure 17. DNC distributed data routing framework

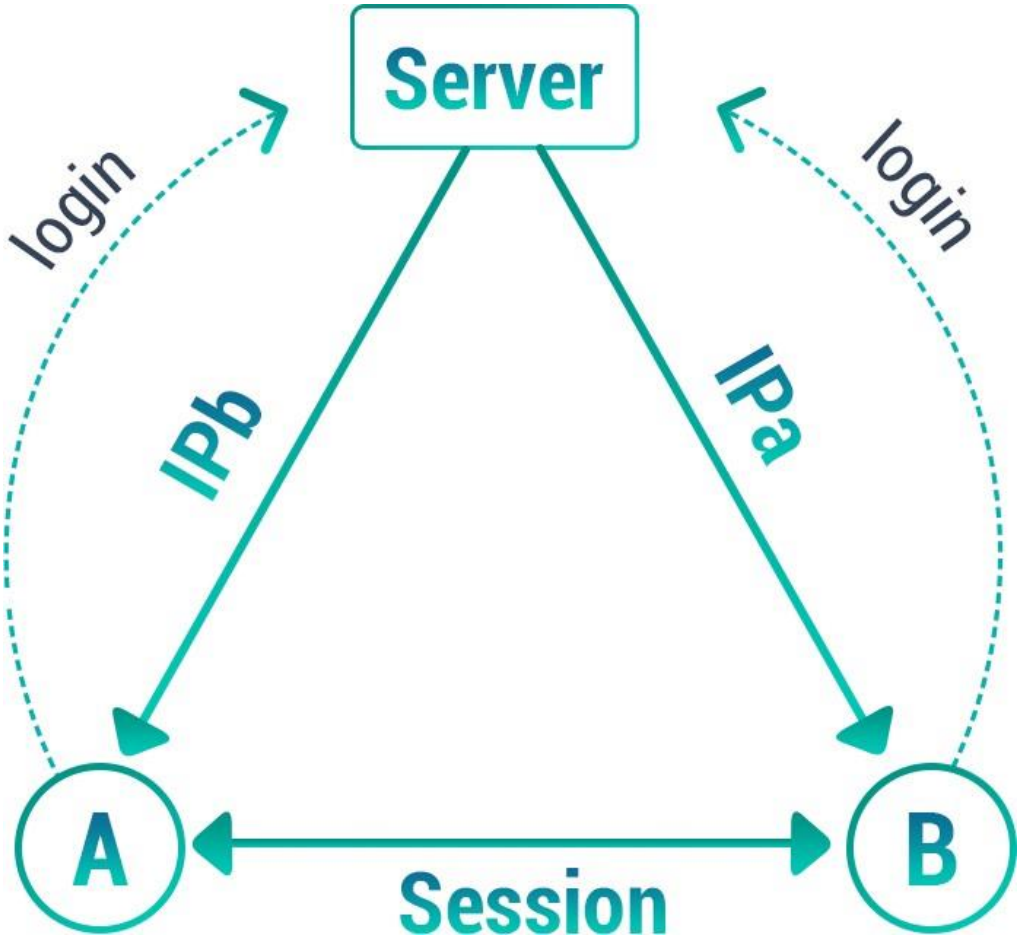


Figure 18. Point-to-point dialogue

The shortcomings of this model are also obvious, that is, it is impossible to establish a conversation in which multiple people participate at the same time, and the simultaneous participation of multiple people requires the establishment of a complex mesh structure. If a star structure with a certain user as the core is used, then when this user goes offline, the communication connection of others needs to be re-established. Moreover, this mode of purely relying on user nodes is not conducive to the preservation of the list of participants in the conversation and the preservation of conversation

content.

So in the end instant messaging returned to the centralized chat room model. The central node provides a stable online service, relays the conversation content, saves, and manages the manager. These powerful technologies and experience advantages are unmatched by pure peer-to-peer.

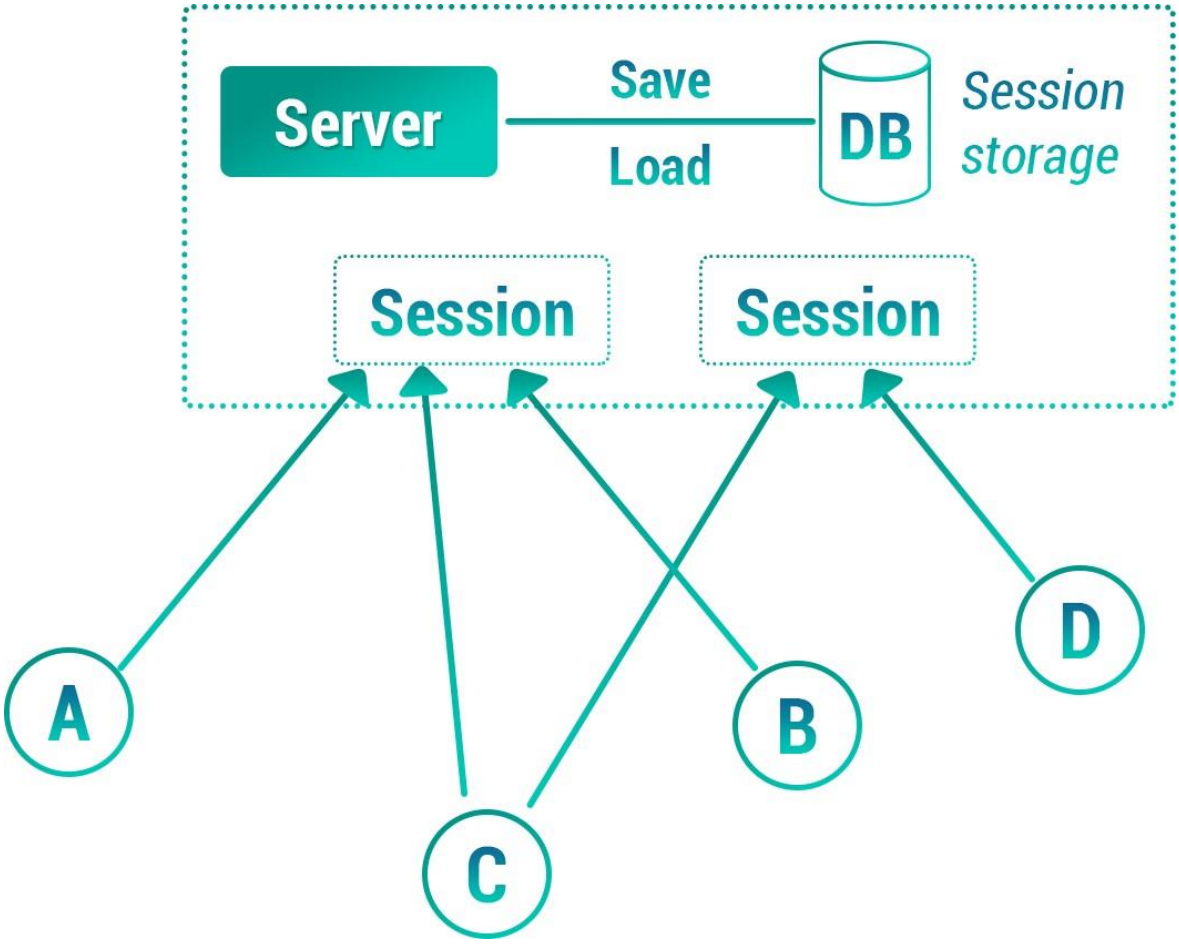


Figure 19. Centralized conversation service

The session content storage service and stable channel availability provided by the centralized node make the user session function very reliable and powerful.

Comparing the above two modes, we can see that for the user node, they need to experience the normal session service, there are two necessary conditions: 1. The maintenance of the session; 2. The high availability of the communication channel service; This On the two conditions, pure peer-to-peer is difficult to meet, and the instability of the node online causes the instability of the topology. Keeping the content and configuration of the Session is more complicated for ordinary user nodes (if they are stored in themselves, they face complex synchronization problems) . Both of the centralized services can be perfectly solved. Therefore, traditional IM services are all provided by the central server. The advantages of the central server are that the logical processing is coordinated, the storage services are uniform, the service cluster communication is efficient, and it is easy to implement complex and large-scale data processing.

Centralization of service clusters also has its inherent disadvantages: 1. User data rights are in the hands of centralized institutions and cannot be handled independently; 2. Service provision may be affected by regional network problems and technical maintenance issues; 3. Communication content is subject to institutional supervision , Or even private monitoring.

DNC believes that communication is a means of communication between the human world, it should be a free tool under its own

control. DNC constructs a completely distributed conversation place, which is decentralized, so that any one or several service nodes on the network have the opportunity to become a communication bridge (communication routing) between user terminals. The group key encryption of the communication content makes these service nodes that provide routing channel services unaware of the content.

Adhering to the advantages of centralized services, DNC conceptually separates storage and channels. Form an architecture in which the storage blockchain and the channel blockchain cooperate with each other:

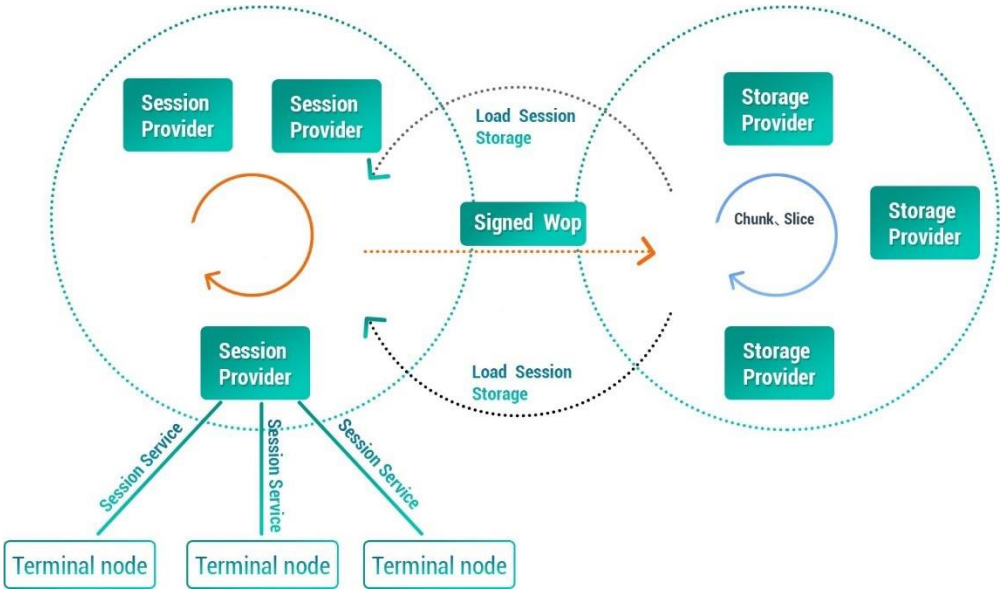


Figure 20. DNC distributed data routing framework

Comparing the above figure with the centralized session service diagram, we can find that DNC replaced Server and Storage in the centralized session service diagram with two blockchains:

1: The storage blockchain is composed of highly available distributed storage miner nodes, using the huge storage space provided by participating miners to construct a highly available storage network;

2: The channel blockchain is composed of highly available distributed Relay miner nodes, which mainly provide dynamic data routing to help users construct a service node connection topology based on Session participating members that all members can connect to provide data Relay At the same time, the service nodes participating in the data relay can access the Session Storage of the storage blockchain to continuously save the session content so that the nodes can be loaded online in the future.

For the user Terminal node (wallet terminal), the functional interface and experience it gets are no different from the centralized session service, and the server side has completely evolved into a decentralized distributed system using distributed blockchain technology.

4.3. Session related storage definition

Group

Group is a concept of user conversation in our daily communication. A group of users who communicate frequently will maintain a public session temporarily or for a long time. This public session body is called a group, and they are all called group members. All users exit the group before the group is closed, otherwise it will

remain open.

The concept of maintaining groups on the blockchain is the core content of distributed instant messaging. The elements contained in a group are:

A. Participant list

B. Their most recent chat history

C. They provide shared files in the group

This group of elements requires that regardless of whether the group members are online or not, they must always be able to keep the service online when the session is established. This puts forward storage requirements for distributed communications. And all these need to provide encryption mechanism,

It is guaranteed that the plaintext of the content is not known by the intermediate nodes that provide service support. In the following, we will introduce the related designs of session establishment, session encryption, group members and content storage.

<Jiatu represents account contact space, account conversation list space, conversation space>

The storage blockchain mechanism is not introduced much. The previous description is more. As shown in the figure, we cut a predefined virtual space on this huge storage cloud to provide user

account information, session information and other data The storage is pre-defined to facilitate DNC's distributed communication services to be executed more quickly and managed more conveniently. If these resources are applied dynamically, the execution efficiency will cause user experience problems.

4.4. Dynamic routing

Completely distributed design, the service quality of communication miner nodes has some chances. They may go offline at any time, or affect the quality of service because of other transactions, and even IP addresses and communication ports may not guarantee stability. Under this condition, the terminal needs to provide dynamic routing guarantee when requesting to establish a session service and execute the session process.

4.5. Design of session establishment process

The user requests to establish a session. The request obtains a miner node with service qualification by broadcasting on the channel blockchain node network (specifically with a forward hop limit). Miners perform shard management based on Session, and user nodes will broadcast to several shards that match the current BlockHash at the same time. The miner node recommends idle session resources based on the SessionId information recorded by its local block shards, and

promises to be able to provide services for the session. The user node collects a list of self-recommended miners, and selects from them the resources that can support the same Session sharding

The miners group, package their NodeId and recommended SessionId into a transaction TxNodeId, and broadcast the SessionId to the group for RPOW. Decide the miners to mine to determine the final assigned SessionId and the group of miners participating in the session service.

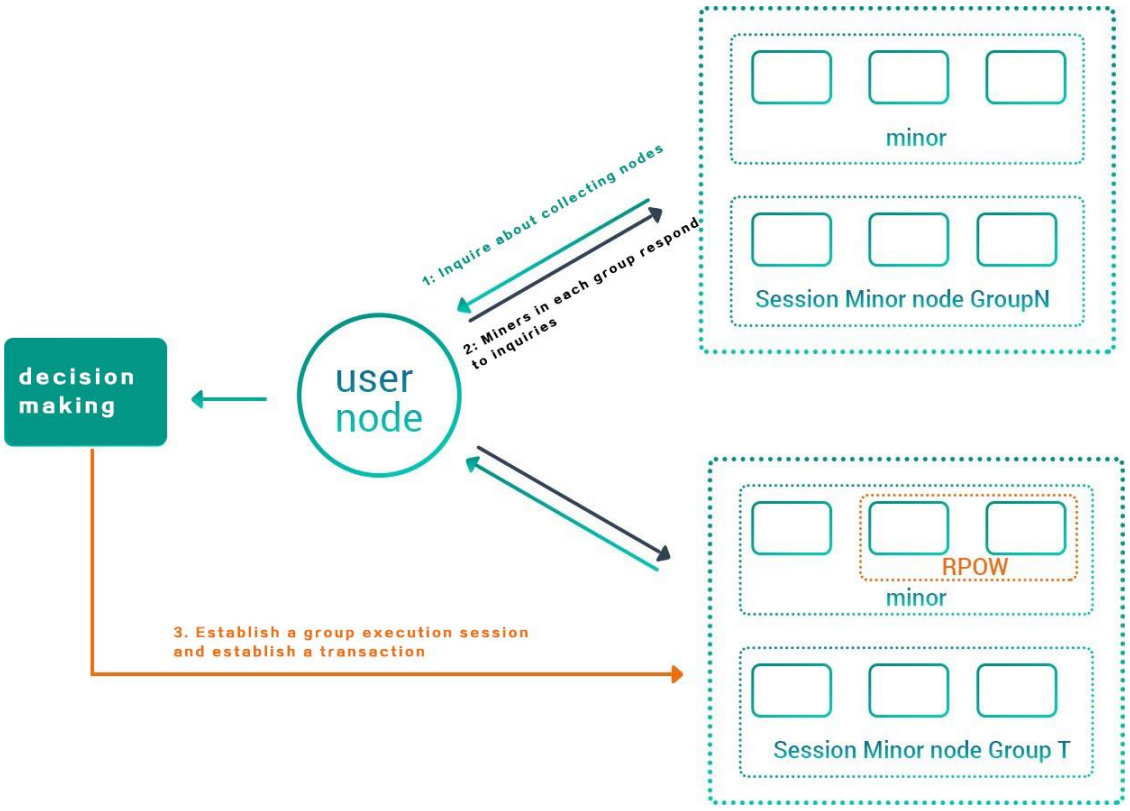


Figure 21. Establishing a session

The service node group selects one of them as an Executor node

based on a random algorithm (such as (NodeId% BlockHash) & 0xff to take the minimum value), which is responsible for the read and write operations of the SessionId data area of the storage blockchain.

As can be seen from the above establishment process, establishing a session, from applying for resources to determining miner sharding, to RPOW final synchronous selection, these series of operations are relatively time-consuming. Such steps are basically inevitable for a distributed service .

In order not to affect the user experience. We can optimize some of these steps.

To this end, DNC considers to select a minor node with a high score (more self-reported resources) to communicate after selecting the miner group in the first step. If it can communicate successfully, it is defined as the session server (Executor node) to start providing directly. Session Relay data forwarding service. Executor directly contacts other nodes of this group of miners list involved in the transaction, and simultaneously encapsulates a message broadcast with all target user ids and service node lists to find all session participants. After all participants (wallets) terminal nodes receive the message , Just try to connect to each service node and participate in the conversation.

The process of constructing a transaction to apply for the RPOW of SessionId and the process of connecting the storage blockchain are

slowly completed by Executor in the background (the initial session does not need to read the content from the storage chain, so it can be directly at the service node Memory construction). This will greatly improve the user experience for establishing a session.

The service topology diagram after the session is successfully established is as follows:

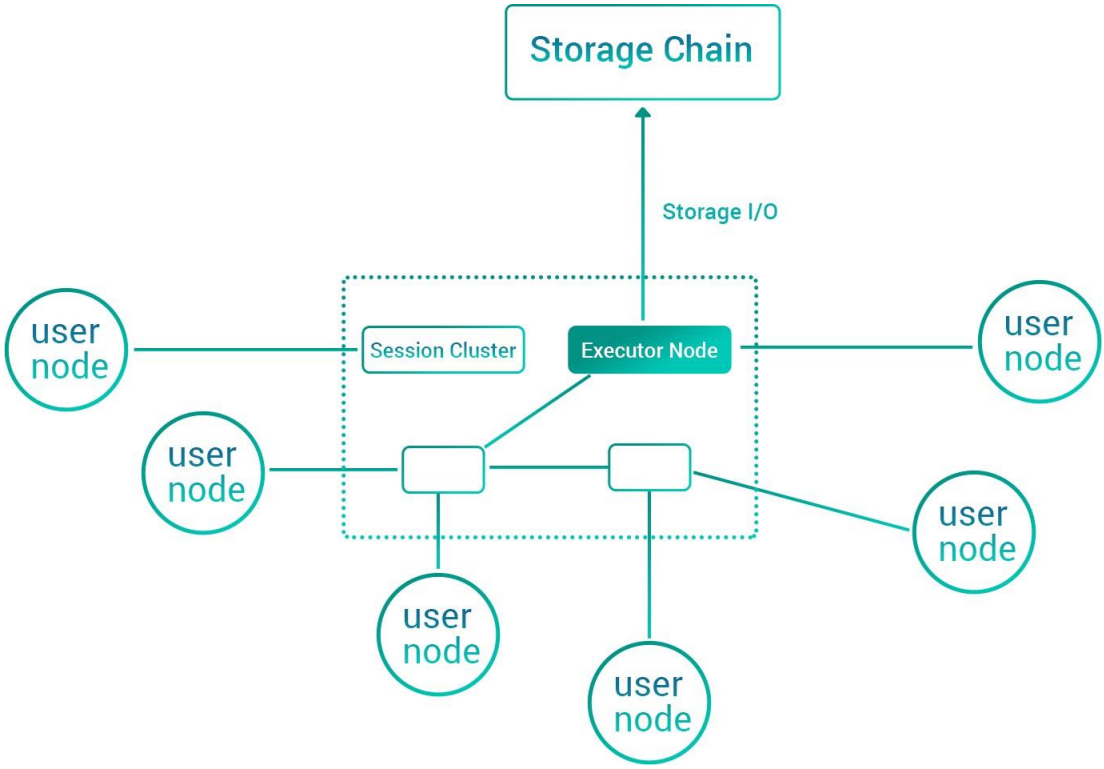


Figure 22. Session service topology

There is a special design here: we must choose more than 3 conversation servers to participate in the service. Mainly one of them, the rest of the services exist as signature supervisors. The signature supervision proposed here is a mechanism for monitoring a centralized

function.

Blockchain 1.0 and 2.0 are basically state synchronization mechanisms. All states are stored in nodes across the network. There is no trust relationship between nodes. All operations must be self-calculated and authenticated by the nodes to form a unified consensus. This mechanism is beautiful and complete enough; and its limitations are also very strong, that is, it is impossible to realize business scenarios with high complexity and large data throughput; this scenario used to be efficiently coordinated by a centralized service (cluster) The realization is also the pain point of the blockchain application.

In order to achieve complex data storage and communication services, DNC uses a small range of verification between nodes. A mechanism of mutual trust between nodes is added, that is, a small number of nodes are engaged in highly transactional and data processing. These nodes verify and sign each other in a small range, and the signature results are agreed to the miner nodes of the entire network. This model is suitable for performing small-area transactions. In order to prevent witch attacks, the members who make up this small circle need to adopt a sufficiently random entry mechanism. It is best to randomly change the composition of the members according to the passage of time. If the business composition cannot be dynamically

changed due to certain business needs. Then the remuneration model obtained by the transaction they signed together (other nodes are not aware of) can not be a fixed calculable (time) and quantity model.

05 Consensus mechanism

5. Consensus mechanism

5.1. Overview of consensus mechanism

Since the essence of the blockchain is a distributed ledger, how to select the bookkeeper, how to keep accounts, and how to synchronize and verify becomes the core problem to be solved. The consensus mechanism refers to reaching consensus in these aspects. At present, the mainstream consensus mechanisms of the public chain are POW, POS and PBFT.

POW

Proof-of-work was originally proposed as a proof-of-work system. This concept came from an academic paper published by Cynthia Dwork and Moni Naor in 1993. It is a countermeasure against denial of service attacks and service abuse, requiring the initiator to consume a certain amount of computers Resources to perform calculations. The word POW was formally proposed by Markus Jakobsson and Ari Juels in their articles in 1999.

Bitcoin uses the POW mechanism in the process of generating Block. A block hash that meets the requirements needs to be composed of N leading zeros, and the number of zeros depends on the difficulty value of the network. It takes a lot of trial and error to calculate a reasonable block hash, and the calculation time depends on the hash

speed of the machine. When a node provides a reasonable block hash value, it indicates that the node has indeed undergone a large number of attempts to calculate. Of course, it cannot obtain the absolute value of the number of calculations, because finding a reasonable hash is a probabilistic event. When a node has n% of the computing power of the entire network, the node has a probability of n / 100 to find a block hash value that meets the requirements.

POS 1.0

Proof of Stake (POS) is proposed by a digital currency enthusiast named Quantum Mechanic in the Bitcointalk forum in 2011. The POS qualified block can be expressed as: F (Timestamp) <Target * Balance. Compared with POW, the search space on the left side of the formula changes from Nonce to Timestamp. The Nonce value range is unlimited, and Timestamp is extremely limited. The block time of a qualified block must be within the specified range of the previous block time. Blocks that are too early or too early will not be accepted by other nodes. The target value on the right side of the formula introduces a product factor balance. It can be seen that the larger the balance, the larger the overall target value (Target * Balance), and the easier it is to find a block. Because Timestamp is limited, the success rate of POS casting blocks is mainly related to Balance.

POS just represents a concept of a consensus mechanism, and there

are quite a few areas that can be optimized in specific implementation methods. There are currently two classic implementation ideas, one is Peercoin and the other is Nextcoin. They have introduced many security mechanisms.

Peercoin was proposed by Scott Nadal and Sunny King in August 2012. In the project, the miner needs to select one from all his UTXOs as the Kernel, construct coinstake, and calculate the hash. If it fails, reconstruct coinstake, the timestamp Time will be changed during reconstruction, and the Kernel can also be changed to obtain different Coinstake , And so on, until a qualified block is found. Peercoin is calculated in terms of currency age rather than balance. Once a UTXO is spent, its currency days are cleared, and the new UTXO currency age starts from 0.

Peercoin's successful operation soon attracted a group of followers, of which more famous ones include Nova-coin (NVC), blackcoin (BLK), etc. The black coin community believes that the coin age may be abused by malicious nodes to obtain a higher network weight and successfully implement a double-spend attack. So it released a POS 2.0 white paper and made several details of PPC optimization to solve some potential security issues. One of the most important improvements is to replace the currency age with the balance. The conditions for a qualified block change from: F (Timastamp) <Target * coins * the age of coins, to:

F (Timastamp) <Target * coins. Because a UTXO's ability to forge blocks remains the same no matter how long it is placed, this action can incentivize nodes to keep more coins online, improve system security, reduce attack paths to a minimum, and significantly improve the network to keep running The number of nodes.

In September 2013, a user named BCNext launched a post on the Bitcointalk forum, announcing that a new pure POS currency will be issued, which was later named Nextcoin, or NXT for short. NXT abandons Satoshi's UTXO design scheme and adopts an account balance scheme, with each account corresponding to a private key. Each block has a generation signature (generationSignature) field. Each miner signs the generationSignature of the previous block with his own private key, obtains his own generationSignature of the block, and performs SHA256 operation on this field to obtain hashdata. , Take the first 8 bytes of hashdata the unique hit variable of the miner in the block.

NXT's POS implementation is completely different from PPC. The qualified block judgment method is: hit <baseTarget * effectiveBalance * elapseTime, where baseTarget is the benchmark value of the difficulty of the entire network, this difficulty is adjusted according to a block target per minute, and effectiveBalance is the effective balance of the account , ElapseTime is the time interval between the current time and

the previous block. Because hit is the result of users signing with their own private keys, it is very random for different users. Even users with small balances, if luck is good enough and the hit value is small, it is possible to quickly forge blocks.

Peercoin and NXT opened up ideas for the design of POS. Although there are still shortcomings, it proves that POS works.

The DPOS bitshares (Bitshares) project started in August 2013. Bitshares invented a new consensus mechanism-Delegated Proof Of Stake (DPOS), which is the proof of share authorization. Its principle is to let everyone who holds bitcoin shares vote, resulting in 101 delegates, who will rotate out of the block. If a currency holder wants to become a representative, he must first use his public key to register on the blockchain to obtain a unique identity identifier with a length of 32 bits. The top 101 are selected as representatives. Delegates generate blocks in turn, and the revenue (transaction fee) is divided equally. If a representative does not honestly produce the block, it is easy for other representatives and shareholders to find out that he will be immediately kicked out of the "board", and the vacant position is automatically filled by the representative with 102 votes. From a certain perspective, DPOS can be understood as a multi-center system, which has the advantages of decentralization and centralization.

PBFT

PBFT (Practical Byzantine Fault Tolerance), a practical Byzantine fault tolerance algorithm, was proposed by Miguel Castro and Barbara Liskov in 1999, and can ensure the correctness of the system (avoiding bifurcations) when the malicious node is less than one third. PBFT needs to collect signatures of more than two-thirds of all nodes
The block can be confirmed, which is almost not feasible under large-scale nodes, so the number of nodes must be limited to a few nodes using this algorithm, which causes the problem of sacrificing distribution. It is generally believed that it is contrary to the core feature of the blockchain, distributed.

In order to apply PBFT to the blockchain, the NEO project (delegated BFT, DBFT) is an improved algorithm based on PBFT. NEO mainly designed a set of voting mechanism based on the proportion of equity held for the generation of consensus participating nodes. Through voting, consensus participating nodes (accounting nodes) were determined, and digital certificates were introduced in the blockchain to solve The authentication problem of the true identity of the accounting node. These practices all require the intervention of centralized institutions, and are relatively centralized.

BFT-DPOS

The EOS that appeared in 2017 combined BFT and DPOS, first selected 21 super nodes (main witness nodes) and 100 alternative

witness nodes, and changed the original random block order to the one determined by the witness after consultation. The order of block generation, so that witnesses with low network connection delay can generate blocks adjacent to each other. When 15 main 21 witnesses confirm the transaction, the transaction is irreversible. According to the design of EOS, the block can be produced in 0.5 seconds, and the whole network can be confirmed in 1 second. Each witness produces 6 blocks in a row, that is, each witness is still responsible for 3 seconds of block production, but from the initial production of only 1 to 6.

After each block is produced, the whole network is broadcasted immediately. The block producer waits for 0.5 seconds to produce the next block, and will receive the confirmation result of the previous block from other witnesses. The production of the new block and the receipt of the confirmation of the old block take place simultaneously. In most cases, the transaction will be confirmed within 1 second (irreversible). This includes 0.5 seconds of block production and the time required for confirmation by other witnesses.

Casper

Although Ethereum's POW efficiency is higher than that of Bitcoin, and it also has a certain mechanism to resist dedicated mining machines, its TPS averages not more than 20. In order to improve efficiency, Ethereum developer Vlad Zamfir? Has proposed a new POS

The mechanism, Casper, is similar to Tendermint. Although Casper may not be implemented until 2020, the security-deposit based economic consensus protocol proposed by it is worth discussing.

The nodes in the Casper protocol, as "bonded validators", must pay a deposit (this step is called a "locking deposit") before they can participate in block generation and consensus formation. The Casper consensus protocol restricts the behavior of validators through direct control of these deposits. Specifically, if a validator does anything that Casper considers "invalid", his deposit will be forfeited, and the right to generate blocks and participate in consensus will be cancelled. The introduction of margin solves the problem of "nothing at stake", which is the low cost of doing bad things in the classic POS protocol. Now there is a price, and the verifier who is objectively proven to do something wrong will pay this price.

Casper's consensus is called Gambling on Consensus. Casper requires the validator to bet most of the deposit on the consensus result. The consensus result is formed by the bet of the validator: the validator must guess which block others will bet on and win, and also bet this block. If the bet is right, they can get back the deposit plus transaction fees, and there may be some new currency issued; if the betting is not quickly agreed, they can only get back part of the deposit. Therefore, the verifier's bet distribution will converge after several

rounds.

The block in Casper requires a lock deposit. The vast majority of validators who reach 67% to 90% of the validators bet on this block and the probability reaches more than 99% to confirm. If no consensus is reached, multiple rounds of betting are required. When all blocks smaller than height H have been finally confirmed, it can be said that the state of H-1 height has been finally confirmed.

In order to resist the majority alliance attack, Casper needs to design a cooperative game mechanism to ensure that each node can only get the maximum benefit in the alliance of all nodes, that is, if p% of the validators participate in the consensus game, then they will get f (p) p% of the gain, and if 100% of the validators participate, you can get more returns. This design is the difficulty of Casper.

5.1.1. Summary of advantages and disadvantages

From the above analysis, it can be seen that BFT is mainly suitable for alliance chains or supplementing other consensus machines. The main choices of public chains should be POW and POS. In the long run, especially from the perspective of blockchain applied to all aspects of life, POW is unreasonable, and there is little room for improvement, and POS will become the mainstream of public chain through continuous improvement. The following compares POW and POS in terms of decentralization, energy consumption, security, consensus speed,

transaction capacity, selling smoothness, gap between rich and poor, and finality.

Decentralized. POW makes it possible for those with computing power to obtain accounting opportunities. At the beginning of their design, they hoped to achieve maximum decentralization, but the emergence of special chips for specific hash algorithms has changed this pattern. It makes ordinary computers It is difficult to participate in the accounting competition, and the emergence of the mining pool has further affected the distributed topology, which makes it even impossible for SOLO mining even for dedicated mining machines. Therefore, POW is not very sufficient in hardware decentralization. POS makes it possible to obtain accounting opportunities as long as you hold tokens, and the more opportunities you hold, the greater the chance that randomness can be increased through a certain design to improve decentralization.

Security The biggest advantage of POW is security. First of all, there is a complete mathematical proof of its security. This is the unparalleled advantage of POS and DPOS. The blockchain consensus mechanism generally needs to consider resisting both DDOS attacks and double payment attacks at the same time. There is a threat of 51% computing power attack in POW. Bitcoin's current super computing power makes it costly to destroy the system. However, for a new project, the use of

POW may be very dangerous, because the current computing power may be used to attack, but for new projects, POS is more secure. The NXT project can theoretically achieve fast transactions, but it needs to forge nodes to expose their own IP, so that it is easy to be the target of DDOS attacks, and DPOS representatives are also easy to be the targets of DDOS attacks. Although there will be a 51% coin age attack on POS, and DPOS security depends entirely on the honesty of the representative, but it is not impossible to design, Casper's mortgage opportunity can increase the cost of doing evil.

Energy consumption POW not only consumes a lot of energy, but also requires a lot of CPU and peripherals. The waste is very large, but POS does not have this problem.

Consensus speed POW is difficult to shorten the block time. POS can shorten the block time relatively. In particular, NXT will be faster than PPC. DPOS can also reach consensus in a short time. Bitshares currently generates a zone in 30 seconds. Piece. However, POS is more prone to forks, especially NXT, so transactions need to wait for more confirmation to be considered safe.

Transaction capacity. This is the core problem that needs to be solved in the future development of the blockchain. Huge transactions easily mean huge bandwidth and storage space. The transaction capacity of POW is difficult to expand, and NXT can predict who will

forge the next block because each node , Can directly send transactions to the forging node, so NXT transaction capacity has great scalability. From a certain perspective, DPOS can be understood as a multi-center system, which has the advantages of decentralization and centralization. If the representative nodes run powerful servers and each other has enough bandwidth, the transaction processing capacity can theoretically be comparable to traditional centralized Systems, such as Visa.

Block smoothness POW Due to the characteristics of the hash algorithm, you can get a smooth block speed, and you can adjust the difficulty of the entire network at intervals. The block generation of POS is mainly related to the balance, and the gradient of user balance gap is relatively large, so POS generally Blocks have to adjust the basic difficulty of the entire network. DPOS relies on the synergy of limited representatives. If the representatives do not come in and out frequently, they can almost fix the block spacing.

The gap between rich and poor. With POS, the more opportunities to hold coins, the greater the chance of earning, and the greater the opportunities, which will widen the gap between the rich and the poor, so that hoarding coins can generate income. This is considered to be an important point that POW is better than POS, but in fact, POW is richer will hoard more machines and earn more coins. From this point of view,

POW is like POW. The more investment, the greater the opportunity, but POW The resources invested are used for hash collision, and the resources invested by POS are to buy coins, so POS is better in this respect.

Finality. POW reaches consensus through competition, and there is no finality. In theory, if there is enough computing power, the Bitcoin blockchain can now be dug from scratch, but the finality can be achieved by relying on detection points. NXT and DPOS are strictly dependent on the time axis, and rely on real-time online detection of nodes, so there is ultimateness.

The issue of nothing at stake. Casper solves the problem of unsecured, increasing the cost of evil. But most current mechanisms still have this problem.

Based on the advantages of all parties, when decentralization, security, efficiency, and energy consumption cannot be achieved at the same time, POW completely abandons the need to save energy and maintains system security and decentralized features through huge computing power. POS costs almost no extra power, but requires sacrifices in two other features. POW has been proven to make excessive sacrifices in energy consumption and efficiency for safety and decentralization, especially when the blockchain needs to be applied to all aspects of social life, POW is almost not feasible. The design of a

blockchain system originally needs to balance decentralization, security, efficiency, energy consumption and other aspects, rather than only pursuing performance on one side, but the characteristic of POW is that once a POW is opened, It may cause a computing power war, which makes the POW transformation space very small. POS has more space in design, can balance the performance of various aspects through design, and is more suitable for public chain. In addition, Casper represents the latest achievement of POS and can be designed on the basis of it.

5.2. POS mechanism of DNC

5.2.1. DNC requirements for POS design

The above analysis shows that POS has many advantages over POW. DNC should choose POS as the consensus mechanism, but the design needs to balance various aspects of performance according to the demands of different public chains. So what are the needs of DNC in terms of importance?

The first place is distributed. The goal of DNC is to promote human exchanges and transactions, so that humans can cooperate with the smallest particles, which requires any individual, organization, intelligent program can join to provide resources or become users, they can break through countries, systems, races Cooperation, only a sufficiently

distributed system can achieve the lowest entry and exit threshold.

The second place is security. Only with sufficient security can the system be able to run for a long time. Security includes two categories: one is major security, which means that the impact is global, and once the system appears, the system faces a crash, which must be avoided; the other is secondary security, which means that the system can continue to operate after it appears , The impact is local. In system design, we must eliminate major risks, eliminate secondary risks as much as possible, and design a recovery mechanism after system risks appear. The recovery mechanism is relatively easy to design a plan in a centralized system, but how to recover in a distributed system is more difficult to design. Generally, it needs to appear automatically through community behavior and economic games.

The third place is efficiency, including consensus speed, transaction capacity, and block smoothness. As transaction capacity is limited by network broadband, the key need to design is consensus speed and smooth selling. The expansion of transaction capacity can only be carried out through sharding under certain circumstances of Internet broadband, which will be specifically introduced in the "Sharding Mechanism" chapter.

The fourth place is to avoid injustice. In the design, avoid the situation of not gaining without paying and paying no gain. In addition,

the balance between pay and benefit should be balanced.

The fifth-ranked resource consumption includes equipment and energy consumption. The elimination of POW greatly controls resource consumption. In the design of POS, excessive search space and POS degradation of POW should be avoided.

According to the above requirements, DNC has the following characteristics in the design of POS:

- In terms of distribution, any willing participant will have the opportunity to obtain contributing resources. It is possible for any referrer to reach the most basic condition that is easy to achieve in the block generation.
- In terms of efficiency, a certain period of time will focus on certain nodes to generate blocks, and after a period of time, the block list will be re-decided.
- In terms of security, special designs will be made for possible witch attacks, 51% attacks, DDoS attacks, etc.

In addition, a well-functioning consensus needs to be optimized in the following areas.

Randomness

To make it possible for all participants to obtain the opportunity to produce blocks, at the same time, because each miner on the peer-to-peer network may choose a result that is beneficial to itself, thereby

manipulating the next generation of blocks, it is necessary to introduce some randomness.

The introduction of a random mechanism must also reach consensus, which is the difficulty of introducing a random mechanism on a peer-to-peer network. At the same time, there is another difficulty. If the entire main network relies on algorithms, it is already very difficult to have randomness. The so-called randomness generated by the calculation itself is pseudo-random and may be cracked.

Proof of work is done by hash calculation to achieve randomness. Proof of stake promises to be able to select bookkeepers at a lower cost, but randomness requires special design. It may be a search space like Peercoin, or Nextcoin is related to each miner's private key.

We found that it is difficult to reach consensus by introducing a random number that is not proof of work, and the random number generated by calculation is pseudo-random. If it is possible to introduce random numbers from nature, but this requires a mechanism to collect random numbers and send random numbers, which is difficult to achieve with a decentralized method.

The only thing we can choose is animals with randomness, such as humans, to obtain randomness through the uncertainty of their game results. Since the actual operator behind each miner node operator is a human, it is possible to achieve a goal by designing a collective decision

with randomness.

Convergence

Convergence means that the bookkeeper can be selected in the end.

Interest relevance

If the block producer of a system has no collateral, its attack cost will be reduced.

Finality

If there are enough resources to dig a chain from scratch, you will get a longer chain and make other miners think that the chain is legal, you can carry out a long-range attack, and such a chain lacks finality.

Objectivity

One goal of the consensus mechanism is to allow new entrants to assess the current status of peer-to-peer network systems through information received from peer nodes. This feature is more important when resisting witch attacks.

Objectivity means that new entrants can independently obtain the same knowledge of the current status of the system as other nodes of the network through the protocol rules (for example, the definition of the genesis block) and the information broadcast throughout the network.

POW is an example of objectivity, as long as a node is connected to

at least one "honest node", it can choose an effective blockchain, because this chain has the greatest cumulative difficulty.

Unlike PoW, the proof of rights and interests is not objective. Weakness can only be achieved by increasing the randomness of people (Weak Subjectivity). If a node needs the latest status information in addition to the protocol rules (for example, the definition of the genesis block) and the information broadcast throughout the network to judge the current status of the system, such a consensus mechanism is weakly objective. Although weak objectivity sacrifices decentralization and mathematical completeness because of the randomness of introducing people, it is a better way to combine computer and social drives (Buterin, 2014).

5.2.2. Preventing possible attacks

Based on the importance of security, a good system should be able to prevent various attacks. This section specifically discusses the attacks that need to be focused on.

Prevent witch attacks

Witch attacks are difficult to avoid completely in any peer-to-peer network system. What can be done is to increase the difficulty of their attacks. POS can prevent witch attacks by using mechanisms such as time, randomness, and deposits.

Prevent DDos attacks

If the next or several block producers can be predicted, as long as the DDoS attack is carried out, the system can be paralyzed. The introduction of randomness and charging mechanisms can effectively prevent DDoS attacks.

Pre-dig double spend attack

The double spend attack requires the attacker to privately prepare a relatively long chain of private mining after spending a sum of money, and after the other party 2 confirms the receipt of the funds, the private mining chain is released. The funds on the private mining chain are Go to another place.

2 This type of double spending requires a large sum of money to be prepared and a place that is willing to accept it. Generally, the exchange is willing to accept a large amount of funds through trading

The Institute is also easy to cash out.

Bribe Attack

In order to allow miners to abandon the existing chain and use the chain prepared by themselves, the attacker only needs to provide a greater benefit to achieve double spending.

If the attack fails, the attacker will not lose anything, as long as his bribe is less than Shuanghua income.

Coin age accumulation double spend attack

For Peercoin or other consensus mechanisms that use coin age as a

basis instead of wealth, in theory, as long as you wait long enough, an attacker may accumulate enough coin age to subvert the system.
If you master 5% of Peercoin's unspent output (UTXOs) and divide it into different outputs, waiting for its coin age to be 10 times that of other coins, it is possible to achieve a double spend attack. So in later versions of Peercoin and BlackCoin, the age of coins will be multiplied by a weight. Long Range Attack

In the Nxt system, chains with more than 720 blocks will not be accepted by the system, which is about 12 hours in this system. But on the one hand, it is more difficult for new entrants to achieve because there is no historical knowledge for comparison.

5.2.3. DNC consensus mechanism

Reasons for choosing Casper as the basic framework

There is no absolute good or bad consensus mechanism, the key is to be able to meet the needs of the economic model. DNC requires a balance of distributed level, security and efficiency. The current consensus mechanism Casper is the most suitable choice.

First of all, in terms of distribution, Casper has hundreds of validators, which is very difficult to collude, and the entry and exit of validators does not require human intervention and can be sufficiently distributed.

Secondly, in terms of efficiency, Casper narrows the scope of consensus, and it is easier to reduce network burden through directed broadcast.

Finally, in terms of security, Casper has the following advantages:

1: Randomly select validators to be allocated to each shard through the main chain of the lighthouse, which can make the security of each shard consistent with the security of the entire network.

2: The deposit mechanism increases the difficulty of the attack.

3: Introduced many individuals, the combination of these individuals formed a relatively large randomness, making various attacks difficult.

PoW + Casper + PBFT

DNC's consensus mechanism uses a PoW mechanism similar to Ethereum on the main chain to ensure security and randomness. The PBFT mechanism is used on shards to ensure block generation. To ensure the security of PBFT on shards, Casper will be used. The mechanism of pre-selects the block producer pool, and uses PoW to periodically rotate the block producers of each shard.

By increasing the difficulty of entering the PBFT miner pool and the difficulty of exiting, and increasing the randomness of selection, it will be difficult to damage the shards through witch attacks.

The following figure is the architecture of DNC's consensus

mechanism:

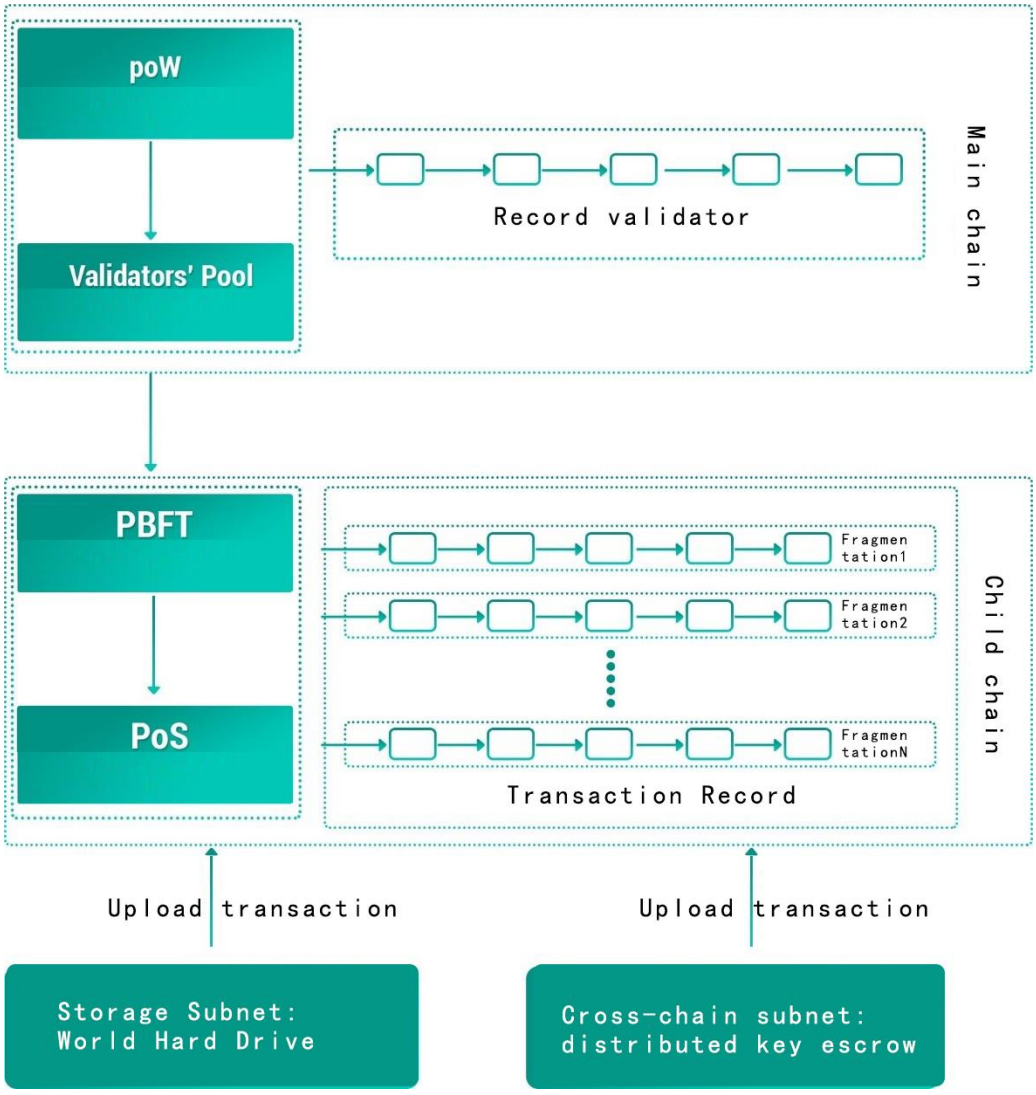


Figure 23. DNC consensus mechanism

06 Sharding mechanism

6. Sharding mechanism

6.1. Sharding overview

6.1.1. Overview of capacity expansion

To achieve a practical level of transaction efficiency on the blockchain, a TPS of 10,000 transactions per second is required. This is actually just a need. Currently Bitcoin is 5 to 10 pens per second and Ethereum is 10 to 20 pens. Even if Ethereum is upgraded to Proof of Stake, its TPS will be difficult to exceed 500. What the blockchain needs is a plan to expand a thousand times from the current ten.

The structure of a single chain is very difficult to reach the order of 10,000 per second, which is mainly due to the limitation of broadband. Because 10,000 transaction packets per second must be synchronized to the entire network in time, otherwise it will cause a large number of soft forks and make the system tend to collapse. As the scale of the single chain is larger, that is, the distribution is stronger, the synchronization efficiency is lower, and the TPS is lower.

Bitcoin's efforts are still based on a single chain:

- Currently, the main effort is to increase the block size. Expanding from 1M upwards, such as the Bitcoin Cash fork, expanding from 1M to 8M is only an 8-fold increase. The increase is 8 times and there is no improvement in other aspects. Its application scenario can only be a large

amount of transfer. This is the key factor for the original bitcoin computing power and everyone's recognition, so the forks have not exceeded the original Bitcoin.

- Or by reducing the block time, this period is similar to increasing the block size, because the block data is always broadcast throughout the network. Whether it is increasing the block size or reducing the block time, you will encounter synchronization efficiency bottlenecks. Litecoin is reducing the time from 10 minutes to 2.5 minutes, but this speed increase is limited.

- Although SegWit may reduce the broadcast volume of the same number of transactions, this technical innovation has limited help for capacity expansion.

- Finally, the offline expansion scheme, such as a side chain like the Lightning Network, cannot be counted in the transaction efficiency of the blockchain, because it is a scheme with very limited usage scenarios.

NEO uses the dBFT consensus mechanism, but its improvement in efficiency is limited. IOTA uses DAG technology, it is no longer a blockchain, it is difficult to prevent double spending. In comparison, Ethereum's efforts may be more reasonable. It chose a consensus mechanism from proof of work to proof of rights and interests, and transformed a single-chain mechanism into a multi-chip mechanism through sharding.

6.1.2. Ethereum sharding overview

Sharding is much more advanced than blockchain technology, and it is widely used in optimizing commercial data to Google's global relational database. The main part of sharding is to use some special methods to split the data in a database in parallel. Generally speaking, these split data are called shards.

In a blockchain distributed network, the network consists of a series of peer-to-peer network nodes that are interconnected in a certain way. At present, each node stores all the data of the network and transactions, which will cause serious problems in terms of scalability.

Ethereum stores all blockchain data, including account balances, storage, and contract codes. The limitation of the whole system comes from the communication bottleneck that forms a consensus between nodes. Since each node has no privileges, the speed of the entire network node is only as fast as a single node.

The idea of Ethereum's sharding is not to shard the data but to group the nodes, so as to eliminate the scalability bottleneck of the system by processing the data in parallel, thereby greatly improving the transaction performance. Ethereum even thinks that each shard can have its own characteristics, and the shards communicate through a certain protocol. Ethereum groups all transactions and smart contracts, and each group will have a data header and data body. The data subject is all transactions

of this group. The data header includes:

- Shard number;
- Random sampling (random sampling) to divide the verifier into pieces;
- Shard Meckergen.

All transactions occur between accounts within the shard, and the consensus mechanism within the shard is proof of stake. Each block of Ethereum will include the root of the global state and the root of the transaction group. The former is the Merkel root of all the latter.

In order to avoid attacking other shards through a single shard, random sampling generates that the verifier is cross-shard, so that the attacker is difficult to carry out the cross-slice attack because the attacker is not sure which shard the verifier will be divided into.

The difficulty of Ethereum's design is the inter-chip communication protocol. Its design is very complicated and the cost is high, so it is only used when necessary. When the information requested by a node is not stored in this shard, cross-shard communication is required.

Cross-chip communication is achieved through transaction receipts. The transaction receipt is stored in Merkel root, so it is easy to verify, but it is not part of the state root. When one shard receives another shard's transaction, it will check Merkel root to ensure that the receipt is not spent. The receipt is stored in shared memory, which can be verified by

other shards, but not modified. Therefore, through the distributed preservation of receipts, shards can communicate with each other.

The Ethereum sharding method includes a main chain and a sub-chain. The main chain is responsible for managing the verifier, and the sub-chain is responsible for transactions. The sub-chain contains 100 sub-chains, and account transaction information is stored on the sub-chain. The specific practices are as follows:

1: Participate in the main chain: deposit to the equity pool, send 32 ETH deposits to the Casper account, with a public key and a withdrawal address. After waiting for a day, the agreement will include this transaction information in the verifier pool.

2: The work of the main chain: track the blocks on the sub-chain, randomly assign validators to shards, and track the information of the verification nodes, including what shards are allocated, whether there are rewards and penalties.

3: The work of the verification node: block generation on the main chain; verification of block generation, transactions, rewards and fines on the verification chain on the main chain; verification and confirmation of transactions between shards; block generation on shards.

4: Reward: When the online normal operation status sends out the information that should be sent, all are normal. In this case, you will find that the other two-thirds of the nodes are normal and you can get

interest.

5: Penalty: However, at least two-thirds of the nodes are running normally, and there will be some small penalties. However, if most of the nodes are offline, there will be a big penalty. In the worst case, the signature is wrong or there is conflicting information with yourself. This may be that you want to attack the network, or you are hacked. If this happens, you will have some punishment. This penalty is proportional to the number of other verification nodes that make mistakes, because the attack requires multiple nodes to participate at the same time. The cost of attacking the system is very high. If you have a problem as a personal verification node, the cost is not so high and it is fair. This mechanism hopes to motivate everyone to do the verification node, and also hopes that everyone can better protect their mechanism when setting up, and try not to fail at the same time as the security protection of other nodes. 6: Withdraw from the main chain: withdrawal, private key or withdrawal address can trigger the withdrawal process. Once triggered, your verification node will be closed in about 7 days. After you exit, you need to wait 4 months to withdraw Ether .

Because the upgrade of Casper itself is difficult, because it takes a long transition time from PoW to PoS, otherwise many PoW mining unions will be greatly affected, so the implementation of Ethereum's sharding may need to wait a long time.

6.1.3. Overview of other shards

The other project that uses sharding is more famous is Zilliqa, which currently does not implement state sharding, only transaction and calculation sharding. It claims that it can reach thousands of transactions. It uses the PBFT consensus mechanism in each shard. The reason is that POS is not as important as PBFT. Zilliqa uses POW when it needs to vote for a long time.

Because each shard performs transaction calculations to form small blocks, and then these blocks are merged into a large block, so its state is not divided. This approach is difficult to deal with the scalability bottleneck of the blockchain.

6.1.4. Difficulties of sharding

So multiple chains in parallel is an inevitable design. But it also raises the following questions:

1: How to keep the data mainly in a single piece, without broadcasting all to multiple pieces, otherwise the main meaning of fragmentation will be lost.

2: In the case where the data is mainly on a single chip, how the native tokens are unanimously accepted throughout the network.

3: How to conduct inter-chip transactions.

4: How to balance the load among multiple chips.

5: How to avoid attacking the entire network from one slice.

Discussing sharding cannot but discuss the triangle paradox. Distribution, security and efficiency constitute an impossible triangle, and the three need to be balanced. But in the case of a public chain, the efficiency has not improved as the number of nodes increases, and synchronization is more difficult. There may be no more than 10,000 machines in collusion than a thousand machines. It is unreasonable to insist on distribution. Therefore, as the number of nodes increases, the design of splitting a chain into multiple pieces is reasonable.

Sharding includes three aspects, one is the calculated shard, the second is the data shard, and the third is the transaction shard. Smart contracts are distributed in different slices, which can save computing resources, while data is placed in different shards to save broadband resources, and transactions are placed in different shards.

6.2. DNC's sharding and splitting mechanism

DNC adopts independent block generation on-chip, and inter-chip transactions are divided through main chain transfer. For the security of inter-slice transactions, cross-slice transactions will introduce a "police mechanism" to verify the data.

DNC does the sharding of transactions, data and calculations. Each shard is independent, and mutually recognizes the data on the other

side's chain, and can initiate cross-shard transactions.

Sharding will be automatically upgraded, that is, the split mechanism. When the number of nodes reaches a certain number, the child chain will split, thereby forming multiple shards. The mechanism of splitting must consider certain randomness. The data after the split will have an inherited relationship with the data before the split.

6.3. Smart contracts

DNC is developed based on the go language version of Ethereum, and will have and be compatible with various functions of the Ethereum contract, and will expand its functions to have data reading and writing and communication functions.

Such a smart contract will have the function of a prophet, that is, data can be read in from outside, and various

Email to trigger the notification.

Smart contracts will be conducted in shards, and inter-slice transactions can also be initiated.

6.4 Distributed File Storage Engine

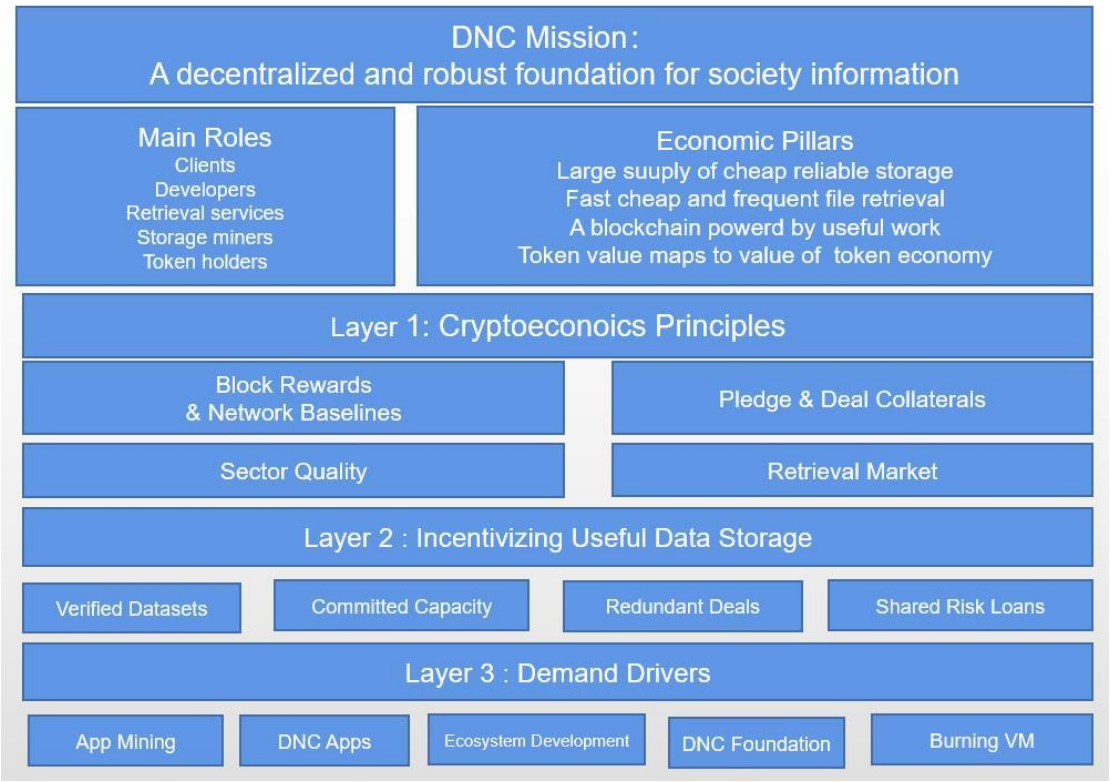


Figure 24 DNC Mission:

A decentralized and robust foundation for society information

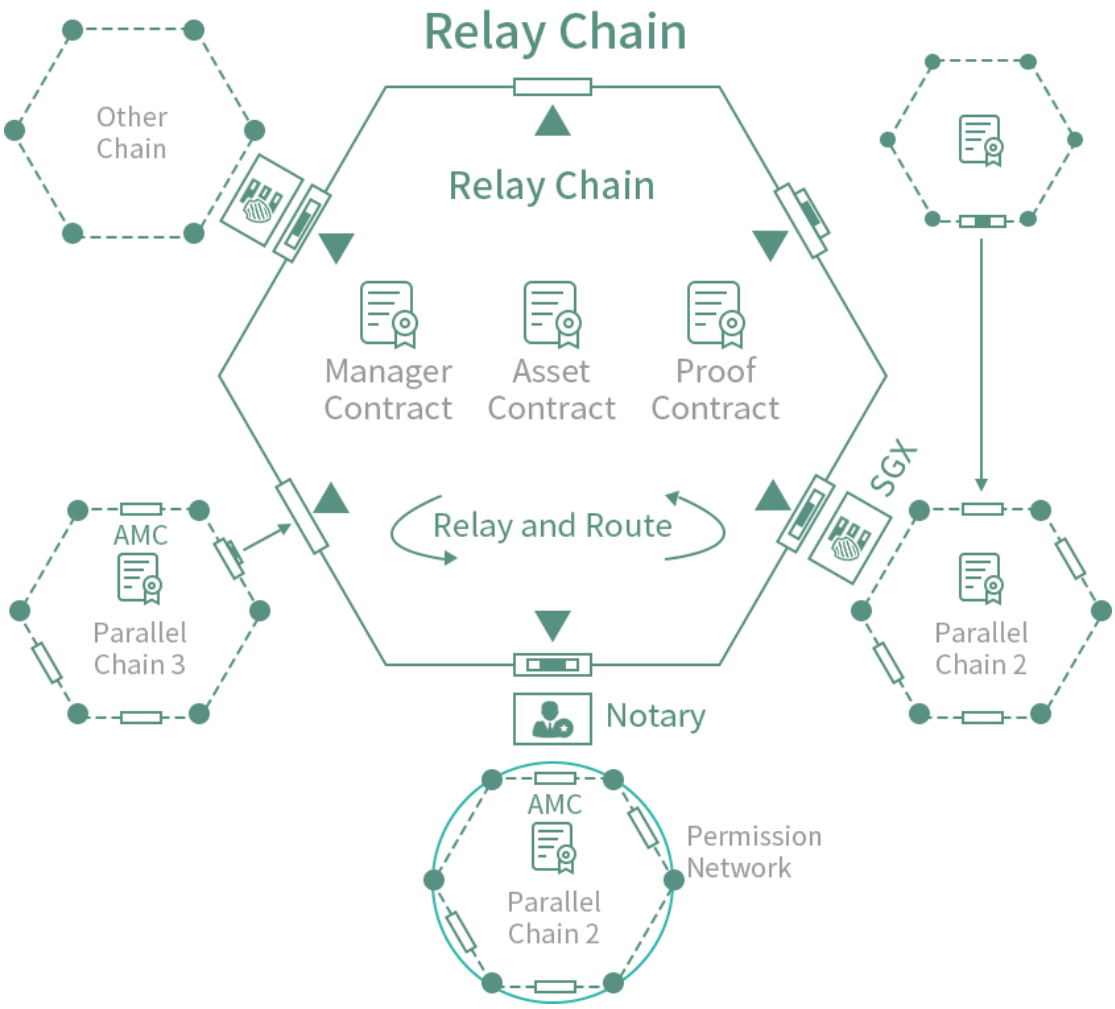
07 Blockchain society, data service providers and application scenarios

7: Blockchain society, data service providers and application scenarios

7.1: From Turing completeness to functional completeness: apply blockchain to all aspects of society

According to Melanie Swan, founder of the Blockchain Science Institute, the development of blockchain technology is divided into three stages: 1.0 for programmable currency, 2.0 for programmable finance, and 3.0 for programmable society. Bitcoin and various competing currencies belong to Blockchain 1.0. Ethereum is Turing complete and implements Blockchain 2.0. However, because Ethereum lacks storage, cross-chain, communication and other functions, it is not fully functional and difficult to use in many aspects. Since other existing blockchains do not have fully distributed, infinitely scalable, communication, storage, cross-chain and other functions at the same time, it is also difficult to apply to all aspects of society. Reasons for DApp replacement.

DNC is completely distributed and infinitely scalable, and has functions such as communication, storage, and cross-chain. This is that DNC has the ability to be applied to all aspects of society, and it is a real blockchain 3.0 project. DNC can be applied to almost any scenario, only a few application scenarios are listed below for explanation.



Scalable homogeneous / heterogeneous cross-chain interoperability

7.2: Data service providers

The data service provider is actually a DApp entrepreneur. Most of the user's data is not owned by themselves. What they do is collect data tags and instructions, analyze them, and do data mining and data push services.

7.3: Blockchain search

The master's data will be accumulated in the distributed storage system, and exploring these data becomes an important task. Blockchain search refers to the search for all open data on distributed

storage.

7.4: Distributed cloud storage service

The storage sub-chain of DNC constitutes a large "world hard disk", which is infinitely scalable and provides distributed cloud storage services for individuals and enterprises. Users can also generate hash uploads at any time to prove that they cannot be tampered with and can become distributed. Dropbox. Especially for enterprises, there is a greater demand for data security and privacy protection, DNC's elephant storage is very attractive to them.

7.5: Distributed communication and online live broadcast

DNC gives the ability to communicate between addresses. It is actually a distributed communication tool. The communication data will not be reviewed or mastered by anyone other than the conversation. It may become a distributed WeChat and provide various online live broadcast services. Due to the convenience of blockchain payment, it is easy to reward in the session.

7.6: Blockchain identity service

The address can upload its own identity information, including resume, in its own space, can become a distributed Linkedin service,

and be used in various scenarios requiring identity services. Identity can be combined with any other application, and may need to provide corresponding data to evaluate its eligibility and payment when participating in other services, such as the typical loan application, lenders need to open their own identity information and private data for credit evaluation .

7.7: Blockchain self-media, blockchain pan-entertainment and blockchain advertising market

The address can upload articles, voices, videos and other materials in its own space, and can become distributed Facebook, Instagram, Himalayan, Youtube, Douyin, etc., through the recommendation system can form a service similar to today's headline, and in DNC In the above, all kinds of programs can be paid by users without intermediaries. In addition, each address can publish its own advertising smart contract, and can also embed advertising smart contracts at other addresses, so that it can advertise itself or advertise for them.

7.8: Blockchain sharing economy, blockchain mall and blockchain logistics

Since everyone has their own private space and can define their own labels and descriptions, they can publish product sales information

in their own space. If there is a vacant house for rent, an Airbnb will be formed. If there is an vacant car seat sharing and Taxi formed by updating GPS at any time. Coupled with proof of identity and credibility, and reviews of transactions, a virtuous circle can be formed. The communication module allows both parties to the transaction to communicate with each other in text, voice or video.

Since any merchant can publish and update product information in its own data space, the merchant can settle in DNC and form a three-party smart contract with the logistics enterprise, which can complete the transaction very automatically. The communication module of DNC makes bargaining and after-sales service very convenient. The digital field of the transaction contract allows both parties to the transaction to evaluate the transaction after the fact.

7.9: Blockchain IoT and supply chain management

Since every company or even every smart object in the supply chain system can choose to upload its own data to its own address, these manufacturers or smart objects can use these data to build a smart contract system to form a complex, mutually triggered supply Chain management system.

With the distributed cloud space of the enterprise, supply chain dynamic maintenance and data upload, supply chain data transactions

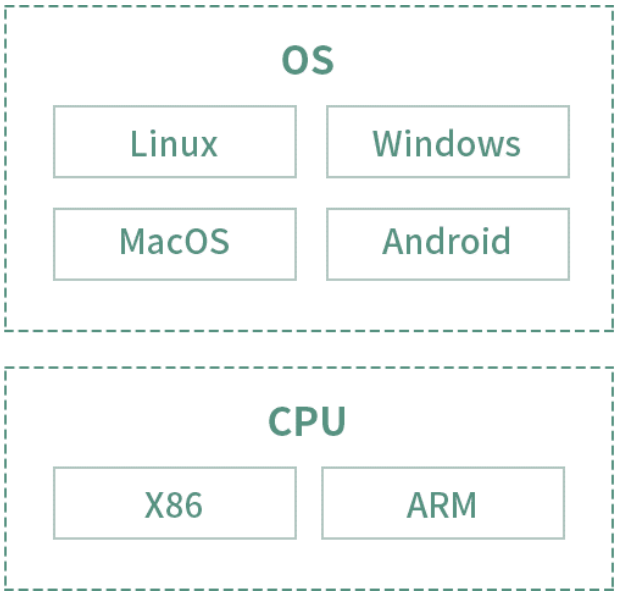
and B2B transactions will become easier. And the data reading function of smart contract makes the management society AI and order-driven automation society possible.

7.10: Blockchain big data transactions, data services and artificial intelligence training

Since each participant with an address has its own data set, these data sets can be easily traded through smart contracts, and all purchased and public data can be collected by the data service provider and provide data services, if used for Artificial intelligence training these data can play a greater role.

7.11: Blockchain games

People in the future will live in various real-life game scenarios composed of big data, but because data is difficult to save on the chain, blockchain games can only be used for some very simple applications. On the DNC, by storing the data of the game developer on the chain, storing the data of the game player in the player's private space, running heavy calculations with a dedicated server, and conducting transactions with the main chain, it can solve the development problem of heavy game scenarios .



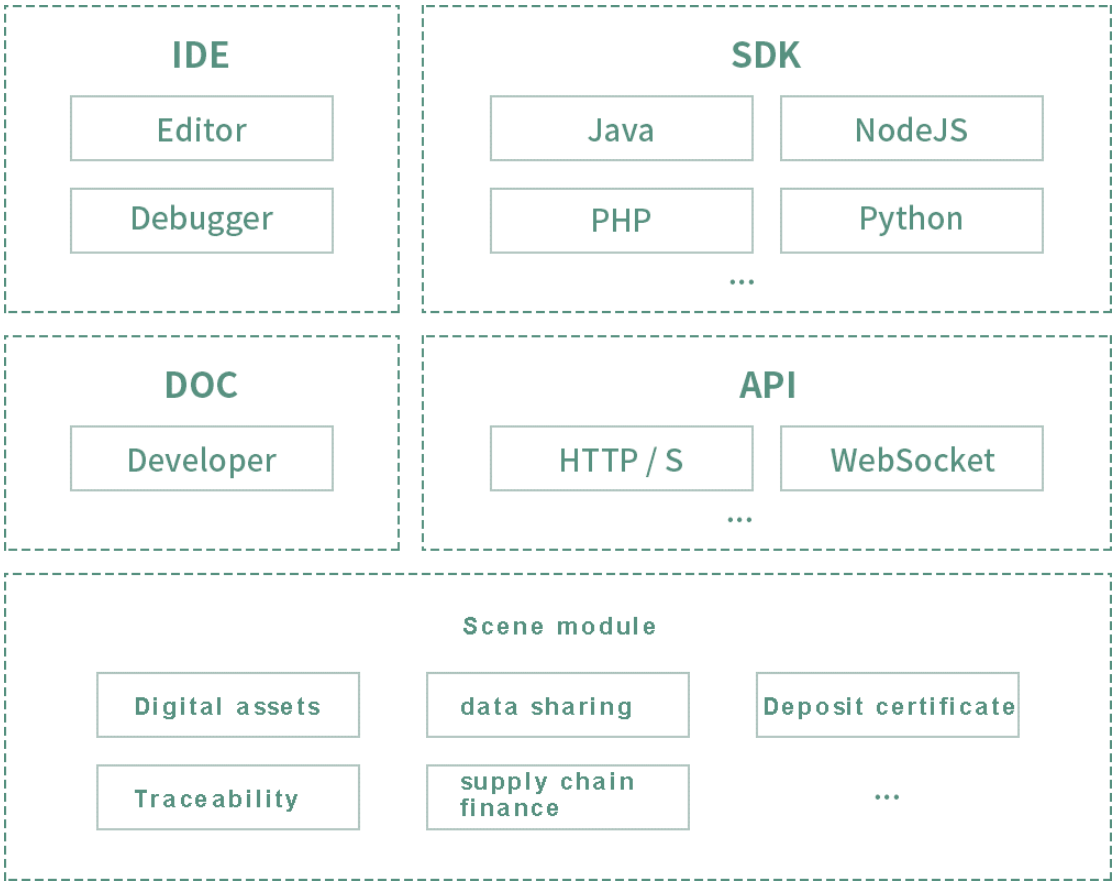
Visual O & M

Provide a comprehensive visual monitoring platform for the blockchain

Blockchain browser providing multi-dimensional statistical analysis

Node supports local and cloud deployment

Multi-platform support: Linux / Windows / MacOS / Android



Ease of use

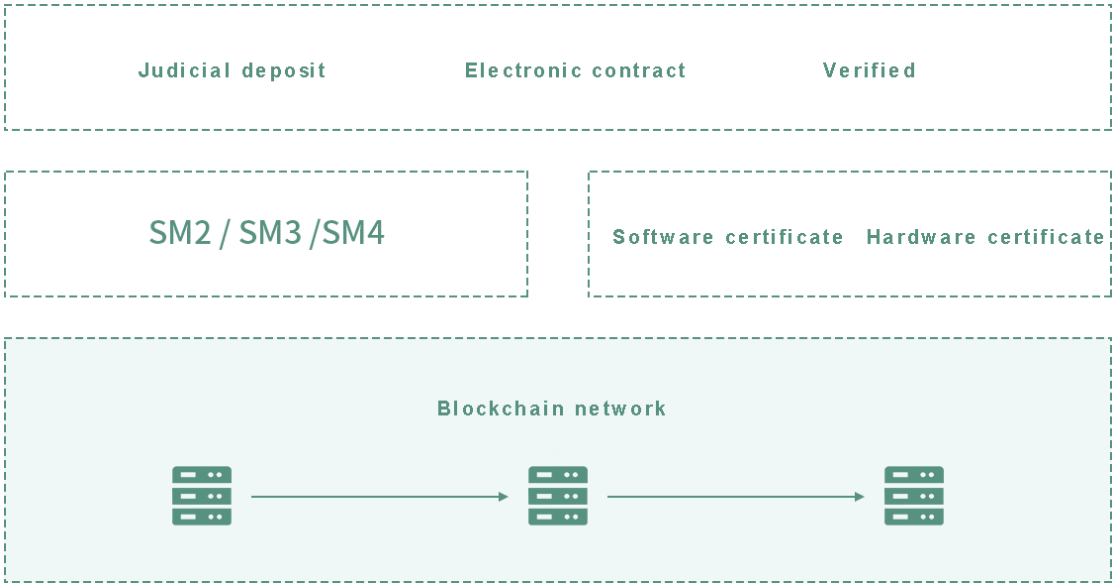
API supports short connection HTTP and long connection WebSocket protocol

SDK supports development languages such as Java / NodeJs / Python / PHP

Smart contract supports JS / C / C ++ mainstream development language

Smart contract IDE integrating development, testing and deployment

Complete and detailed development documentation



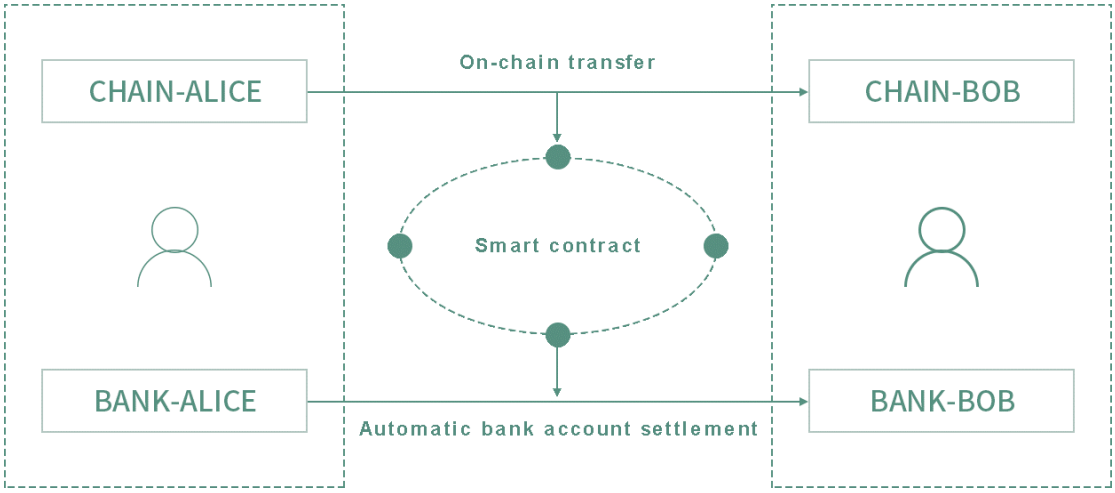
Legal effect and compliance

Support electronic contracts and judicial deposit

Support national secret algorithm SM2 / SM3 / SM4

Blockchain users use CA real-name authentication

Blockchain nodes use CA to access the network



Accounts on the chain can be linked to bank accounts

There is no "money" problem on the chain in commercial applications

Integration of on-chain accounts and bank accounts

Smart contract realizes automatic liquidation of funds

The liquidation process depends on the signature on the chain, not on the administrator

Global settlement via VISA debit card

08 Project governance mechanism Project development planning and token distribution

8: Project governance mechanism, project development planning and token distribution

8.1: Project governance mechanism

8.1.1: Governance philosophy

Community is everything

The DNC platform is a public chain. As the initiator of the project, the DNC Foundation is a non-profit organization. The DNC platform, as a public chain of various token holders, developers, and users, does not belong to any organization or individual, but belongs to the entire DNC community. In order to realize the mission of DNC to promote efficient human cooperation, the DNC Foundation, as the initiator, needs to attract as many participants and resources as possible into the community and try to condense the power of the entire community, by continuously iterating its products and enriching its ecology to promote DNC The system is used in real scenes and improves people's lives.
The DNC platform is a public blockchain. As the initiator of the project, the DNC Foundation is working for a promising blockchain ecosystem, not for the company's profit like the traditional enterprise project operation. The DNC platform, as a basic DNC platform for all kinds of token holders, does not belong to any organization or individual, but belongs to the entire blockchain token community. DNC makes the use of tokens more flexible, the circulation is more convenient, and more

importantly, it gives the function of token DNC services. Make all tokens have greater value. In fact, the value Internet cross-chain ecology is a big business, which needs to be initiated by the DNC Foundation, the entire community joins and participates together, and generates more and more perfect blockchains through continuous iterations. This is exactly the characteristics of blockchain projects. The blockchain project starts with an important need or a problem to be solved, which needs constant exploration by these demanders and participants during the development process. At the same time, more people in the community are attracted to participate, and then the demand develops in a more perfect direction, and further promotes technological progress. Therefore, the idea of project operation must be community-based from the beginning, and community operation is related to the success or failure of blockchain.

The community consists of:

The DNC Foundation and the development team are the initiators and promoters of the project platform.

Programmers interested in the project. They are interested in the project or project technology and can join the foundation development team or independently develop and optimize the DNC as a third party. DNC participating node. Obtain revenue through bookkeeping and maintain DNC operations.

Users of the DNC platform can obtain DNC services by using the DNC platform.

DNC service providers on the DNC platform, such as payment platforms, centralized or decentralized exchanges, lending platforms and other financial service providers.

DNC token investors. Including private equity institutions, early investors, late investors and potential investors.

Other stakeholders. Including media, government, etc.

The above persons or organizations play an important role in the future development of DNC. The purpose of community operation is to mobilize as much power as possible and organize it in the most effective way, so that DNC can continue to iterate, form influence, and serve a larger community.

The growth of the community is actually related to both the core community and the peripheral communities, and the two are complementary. The core community is the core, but the formation of key communities requires the peripheral communities to continue to attract people to enter, because the core community's people come from external communities, but the peripheral communities also need the support of the core community's resources. We found that the growth of projects such as Bitcoin and Ethereum has followed this rule.

We position the core community as the initial founder, blockchain technology community, blockchain investment community, and the peripheral resources are other investors, users, developers, media, etc. who are interested in the project.

Technology first

Value Internet currently has bottlenecks in usability, and needs continuous efforts in the future to continuously promote its usability. The DNC project is closely related to the availability of the Internet of Value. We will launch the "Blockchain Technology Promotion Movement" to contribute to the progress of blockchain technology in usability. This will be a long-term work of the foundation.

The sports line will continue to gather talents and technical materials in the form of technical salons, training camps, and seminars. We will promote the content provided by offline participants, and promote the content in the form of various websites and various media. It also attracts traditional Internet personnel and other technical personnel through irregular classes to expand the reserve force of the technical community.

The blockchain technology promotion movement will unite all forces that can be united, including universities, research institutes, enterprises, institutions, governments, alliances, etc. to establish cooperative relations, and gather resources to jointly promote the

progress of blockchain technology.

8.1.2: Foundation and decision-making committee

The members of the DNC community include foundations, developers, participating nodes, users, service providers, token investors, etc., among which the DNC foundation as a core community member will operate in a completely transparent manner. The private keys of all the tokens of the foundation will be collectively held by the foundation's decision-making committee through multiple signatures and managed securely. The decision-making committee is composed of core partners, and the partners have perfect entry and exit rules to avoid dictatorship or single-point risk, and promote the decision-making committee to adapt to the project development.

8.2: Project development planning

8.2.1: Five stages of development

The development of DNC is divided into five stages.

1: V1.0: Complete the transaction sub-chain from 2018 to 2020. At this stage, DNC will complete the project to start 23 transaction super nodes + 46 transaction alternative nodes, and develop to a scale of more than 200,000+.

2: V2.0: From 2020 to 2022, complete the social sub-chain that

supports distributed file and application deployment, develop more than 1000+ miners, and the community size grows to more than 1 million +.

3: V3.0: From 2022 to 2024, the home robot Internet of Things sub-chain will be completed, and the community will grow to more than 10 million +.

4: V4.0: From 2024 to 2026, complete the super node satellite on-chain, realize global free point-to-point communication plus full ecological upgrade of payment, and achieve a community size of 200 million +.

5: V5.0: After 2026, we will explore the in-depth evolution of DNC in various fields, hoping to help humanity enter a new stage of civilization.

8.2.2: Project promotion methods

This project divides community operations into two areas: core communities and peripheral communities. The former mainly adopts offline mode, and the latter mainly adopts online mode. Plans for core community operations are:

DNC Foundation team: We will give the team certain token rewards. One is to compensate the resources invested in the early stage, and the other is to enable it to become a stakeholder, hoping to continue to invest in the future and continue to participate in the development of

DNC.

Blockchain technology community: Technology is the core and difficulty of blockchain development. We will use the technical strength and social resources of the founding team to explore and cultivate a group of top-notch talents in both online and offline ways to promote the growth of the technical community.

Blockchain investment community: Relying on the blockchain technology community, through the form of investor meetings, we can not only popularize blockchain knowledge to private equity and other investment communities, but also enhance the cooperation opportunities between the two parties.会。

8.2.3: Foundation management and token model

The project has established a non-profit organization DNC Foundation in Singapore, whose goal is to improve the project ecology and promote the realization of the project vision. Tokens are an indispensable component of the public chain ecosystem. As the incentive mechanism of the public chain economic system, it is like a lubricant of a mechanical device, but also like the blood of the living system. It is the token-based consensus mechanism that brings community members together to achieve a virtuous cycle of the blockchain ecosystem. For project starters, tokens are the necessary

compensation for them and the motivation to continue to participate in the future; for users, tokens are passes; for investors, tokens are tickets to the future; for developers, tokens Let them become shareholders; for the bookkeeping node, the token is the compensation they have worked hard for. All the people who hold tokens can be the above multiple identities. They are closely related to the public chain project, and become users, propagandists, developers, investors, grow together with the project ecology, and achieve the great mission of the DNC platform. The private keys of all foundation tokens will be held collectively by the foundation's decision-making committee. On the one hand, avoid dictatorship; on the other hand, avoid single points of risk. The foundation's decision-making committee is the highest decision-making organ of the foundation.

In order to realize the mission of the DNC platform, the DNC project has designed DNC (DNC) tokens, and designed the distribution structure of DNC tokens to make the project sustainable development. The token design mainly considers five aspects:

1: Quantity. The total supply of tokens is 2 to the power of 30, totaling 1073741824, about 1 billion. This number happens to be the world's hard disk management unit of DNC, that is, the size of the space maintained by a storage group is one G. This quantity can also make the tokens have a reasonable price when they go online, and grow steadily

on this basis, and make the quantity in line with the people's habits in the period of the global village.

2: Token issuance mechanism. There should be an upper limit on the supply of tokens to realize the concept of non-inflation. This makes the earlier the participants more favorable, and also makes the system more stable.

3: Token distribution. The distribution of tokens must be well balanced to realize the non-central concept. The DNC team needs to make great efforts in communications, data storage, cross-chain and cross-data sources. We allocate 10% to the core team to support development and operations by 2030. In addition, because the DNC accounting node task is relatively heavy, it can account for nearly one-third. The rest will be used for ecological construction.

4: Ecological construction. More than half of the tokens will be used for the foundation to promote the continuous growth of the project, especially the construction of DNC publicity and application ecology requires a lot of funds.

5: Miners and fuel. Various values will enter the DNC in the form of distributed node control, which requires a large number of distributed node control tokens. The more nodes, the higher the security. And the greater the value of running on the chain, the more nodes are needed. To maintain the number of nodes and computing power, it is necessary

to give miners a bookkeeping reward and service fee.

The distribution of tokens is as follows:

1: Partner incentive: 10%. Most of the incentives used to participate in the creation of the project from scratch, and the partners who join the strategic significance of the project in the next 20 years will be locked for a long time;

2: Developer community: 5%. In the future, the project will be transferred to community development to attract top developers to join. This part of the token will be allocated to important developers in the next 20 years as a reward for the continuous progress of the project, and most of it will be locked for a long time;

3: Token swap: 5%. Allocated to participants willing to exchange DNC for other tokens, so that the team can obtain more liquid tokens to support early development and operation;

4: Ecological construction: 10%. It is used for cooperative development of the foundation and ecological construction with the blockchain community. It will be gradually released in 20 years, and the distribution method is initially expected to be 2% in V1.0, V2.0, V3.0 and other stages;

5: Miner reward: 70%. It will be used for resource proof incentives, with storage mining and accounting mining accounting for 35% each. Completed in 20 years, it is expected to adopt a gradual reduction in

inflation rate, the specific method will be determined after the public test.

Release Notes

DNC is a universal currency for global centralized finance. The name DNC combines the Domain Name Chain to form a new term, marking the goal of DNC is to become a common "free and stable product" in the future decentralized global finance

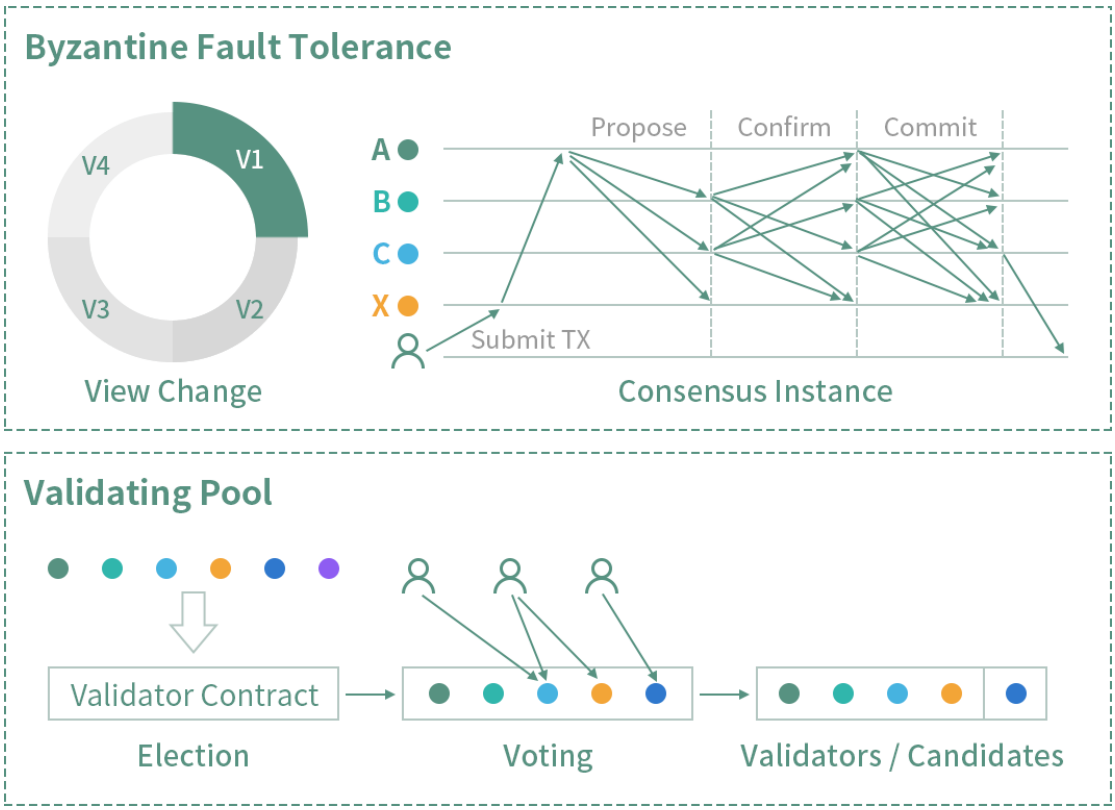
Basic Information:

Circulation: 1,000,000,000 DNC

Consensus algorithm: DPOS + PBFT

Block interval time: 3 seconds

Output per block: annualized rate (12 * 31 * 24 * 60 * 20) The annualized rate is determined by super node voting



Safe and efficient consensus algorithm

Innovative two-layer consensus algorithm Validationg Pool + Bubi-BFT

Safe and efficient verification pool election algorithm

High-performance Byzantine fault-tolerant algorithm Bubi-BFT

High throughput, second-level confirmation, provable security

09 in conclusion

9： in conclusion

Human civilization is still at a very preliminary stage, and its rapid progress cannot be achieved without the in-depth cooperation between the trading entities to break through the restrictions of geography, system, country, organization, etc. The development of the Internet has given people hope to break through these restrictions. The information Internet has enabled people to break various restrictions for information communication, but the increasingly centralized information Internet needs to transform into a distributed information Internet. The Internet of Value allows people to see the hope of breaking various restrictions for value interaction, but the data storage, cross-link interface, and scalability of the blockchain are not enough to support heavy applications. complete.

DNC is committed to becoming a fully distributed, fully distributed and infinitely scalable public chain system that can integrate the Internet of Information and the Internet of Values with addresses as its core. It enables the transaction to be infinitely scalable through the main chain layered sharding, and the function is complete and infinitely scalable through multiple functional sub-chains and its sharding. It is based on the readable and writable storage function sub-chain, so that any subject can publish their own identity information, social

information, rich media, products and smart contracts by establishing their own private data sets, and build on it in this way Various distributed applications.

DNC is a fully functional third-generation blockchain that can apply blockchain to all aspects of society. The foundation is based on the community and adopts a distributed governance mechanism, which will surely prompt DNC to continue to approach its mission-to promote human efficiency through the establishment of a fully functional, fully distributed and infinitely scalable blockchain with address as the core Cooperation.

DNC is an open payment network. It is a network established for financial payments, just like an e-mail message for information transfer.

The agreement can be used to transfer money to any corner of the world in any currency quickly and for free.

The DNC protocol is compatible with all legal currencies and virtual currencies, and can realize the free circulation of value worldwide.

Independent systems can be interconnected like mail systems. Just as SMTP created a shared standard environment for email, DNC also created a shared standard for payments.

The functions of the DNC network far exceed that of Bitcoin. It includes: bidirectional flow of real and virtual currencies, multi-currency P2P exchange and payment, and P2P network credit personal network

clearing. The combination of these four functions has already constituted a basically complete decentralized all-currency financial system.

DNC is a secure payment network.

This security is not only the security of funds, but also the security of protecting payments from power.

DNC is built on a P2P network and is different from the traditional centralized financial network. The DNC payment system is distributed on all nodes around the world. These nodes connected through the P2P network constitute the entire DNC financial database. Therefore, financial transfer payment is only a matter of seconds. DNC's decentralization has another manifestation. Although SWIFT is nominally an inter-bank organization, it is, after all, dominated by the United States. The United States has a large voice in it, and DNC does not have such a situation. DNC can minimize the impact of power on payment.

DNC optimizes the payment system, performs distributed processing of settlement functions, and completes instantaneous and peer-to-peer payments and transfers. For users, DNC's instant payment enhances the payment experience.

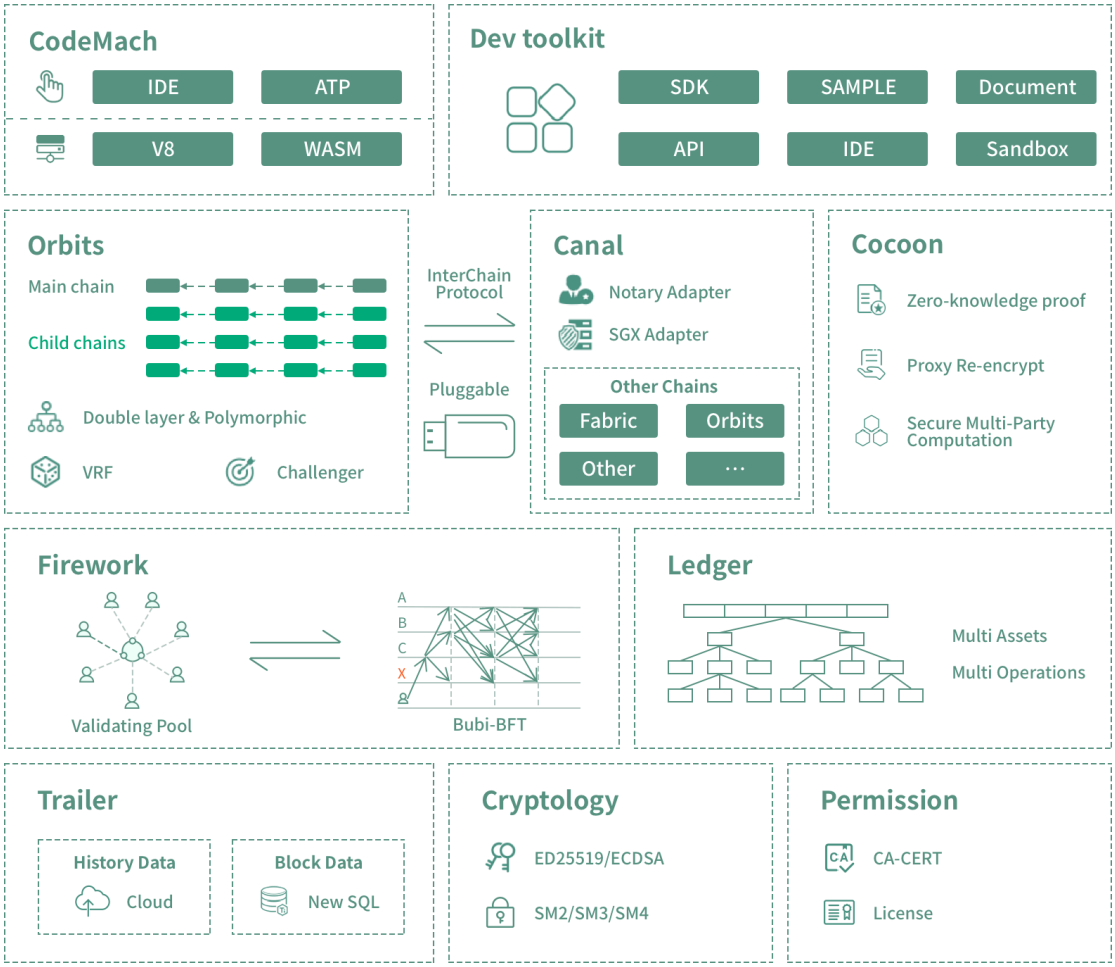
DNC makes payment as easy as breathing

DNC has established a shared payment network that can be used anywhere in the world at any time. This makes DNC more approachable and convenient. You can easily find the DNC transaction entrance on the Internet, but with the development of DNC, you can find the entrance anywhere in stores, hotels, gas stations, etc., which makes people's financial payment as free as breathing. You can easily transfer your banknotes to any corner of the world within a few seconds. You can use the DNC entrance system to get local currency anywhere.

DNC makes your currency exchange so convenient

Because of the existence of DNC, it is not necessary for people to get involved in the foreign exchange market when conducting global transactions, because DNC's internal mechanism already supports foreign exchange. Similarly, people do not need a multinational financial institution to complete financial payments, you only need a simple payment portal to complete everything.

For financial institutions, the settlement risk is reduced. This is the significance of DNC innovation.



Domain Name Chain 1.0