North Star **Chain**

Block Chain Data Privacy Service Platform

-

From the deep net
to illuminate the future

TABLE OF CONTENTS

ORIGINATING FROM POLARIS

ORIGINATING FROM POLARIS

North Star Chain

From an explosion 17. 3 billion years ago, the stars of all things appear, burning in the ashes, the war song of life recovery from nothing, into all, is the power of the universe. The ruins after the wind and the sand tell of the glorious past, like life as time, we can not escape the judgment of the universe. in the central world, the thought of fate is written in advance. Life is nothing but the practice of the traces of history, democracy is nothing more than the rhetoric of hegemony. At a time when we are about to assume that centralisation is the rule of the universe.

Blockchain was born from the deep net. in a central world, our destiny is not ours. Strive to hope that the dream of peace will be destroyed by one central right at a time. The greatness of decentralization lies in the fact that it enables each person to take control of his or her own destiny, to contend with the power of the masters of the universe, and to perpetuate the development of civilization and thought. He can make civilization and ideas sustainable, make them like stars, and make them agree on rules. Only 10% of the world's people hold 90% of the wealth. with the progress of mankind, the gap between the rich and the poor has become more apparent.

A lot of resources are in the hands of a small number of people, and the fate we think we can break is a predetermined procedure. The vast majority of human beings had difficulty changing their destiny until blockchain appeared. Blockchain's appearance is accompanied by hope, but there are many obstacles to crossing hope. Different block networks are difficult to interconnect, making each block network become an independent closed world. Even though we have gained the freedom and openness of the block world, we are still confined to a limited space.

ORIGIN

From exploration to discovery, from changing the world

Password punk (Cypherpunk)

- Speaking of the origin of Bitcoin, you have to talk about a slightly mysterious group: Cypherpunk.This group is a loose alliance of password geniuses, and Bitcoin innovation draws heavily on the contribution of password punk.Part of the word password punk comes from the cipher (Cipher), which in cryptography means the algorithm used for encryption and decryption; part of it comes from Cyberpunk, which refers to a sci-fi genre popular in that era.This combination has a subtle meaning and exudes a radical ideal of changing society.

  The idea of password punks is that society is now spreading its erosion of personal privacy and rights.They exchanged their concerns about this issue and believed that protecting privacy in the digital currency era is critical to maintaining an open society.This concept is reflected in Bitcoin: the pursuit of decentralization, the embrace of anonymity, the principle of liberalism.

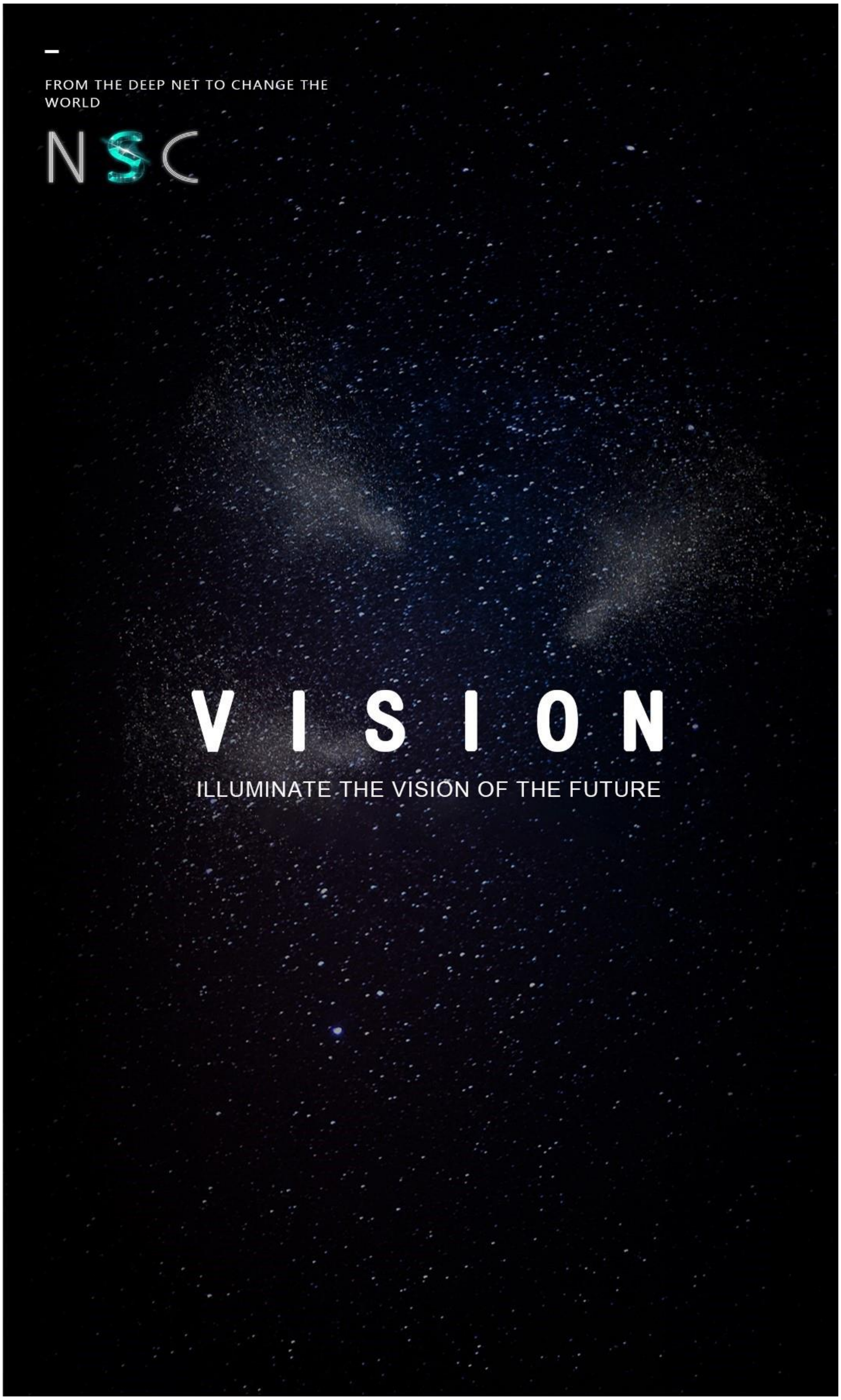
  Password punk itself is the earliest communicator of digital currency. In its email group, there is a common discussion about digital currency, and some ideas are put into practice.For example, David Johm, Adam Baker, Dai Wei, Hal Finney and others have made a lot of exploration in the early days of digital currency.

- Early digital currency exploration

  Bitcoin is not the first attempt at digital currency.According to statistics, before the birth of Bitcoin, there were dozens of failed digital currency or payment systems.It is these explorations that provide a lot of experience for the birth of Bitcoin.

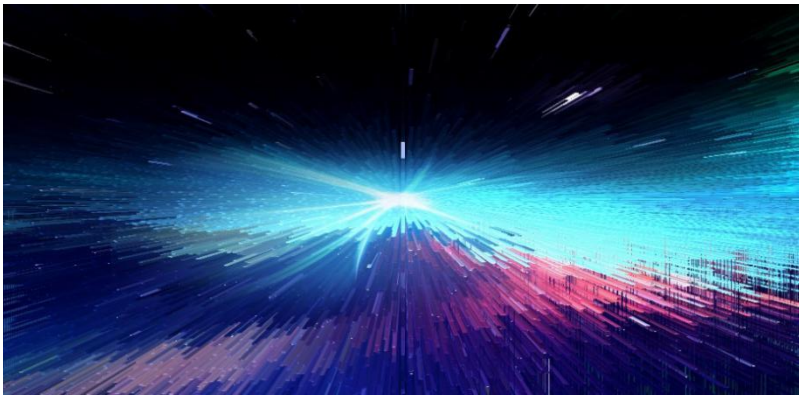
Many people did not believe it before the change took place.

--Nelson Mandela


FROM THE DEEP NET TO CHANGE THE WORLD
NSC
VISION
ILLUMINATE THE VISION OF THE FUTURE

Ignite the spark of the new world civilization

The original appearance of the universe is a very high temperature, extremely high density fireball.A big bang produced the universe, produced elements, produced life, and produced everything in the world.The universe is a prototype of nothing.



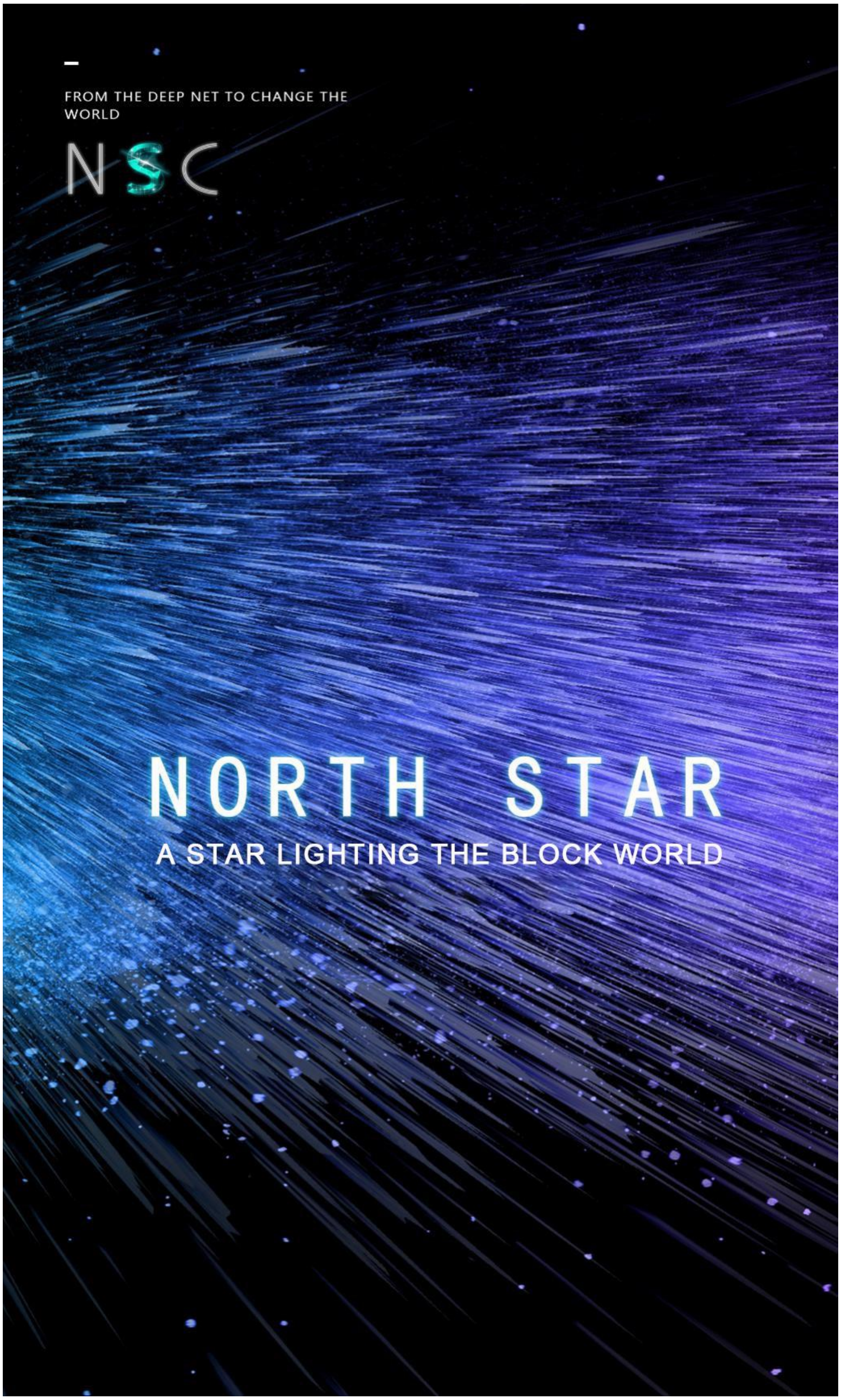
Since the birth of mankind, the world has been constantly changing, we seem to have never experienced a long-lasting prosperity. We have worked hard to build a beautiful society/nation. After the years of sandstorms, it is a fragment of the wall.Because of the lack of trust and democracy, the civilizations that were formed once and for all were broken again and again.

There is an old saying in China that "the long-term must be divided, the long-term must be combined." People seem to have accepted this situation. We think this is the nature of the universe itself.

Although we have been expecting good times countless times, we have only had a moment of peace in the melody of religious singing.

When we soon think that this is the rule that the universe dominates everything, the blockchain was born from the deep network.Originated from the deep network, illuminate the future.The birth of the blockchain has rekindled hope.

In a centralized world, our destiny is not dominated by us.Efforts to hope that dream peace will be destroyed by a centralized right.The greatness of decentralization lies in enabling everyone to control their own destiny, to compete with the power of the universe, and to allow civilization and thought to develop in an eternal and orderly manner.He can make civilization and thoughts perpetuate, making them like stars, and let them reach consensus under the rules, so that the human and human thoughts and actions can reach an unprecedented height.


FROM THE DEEP NET TO CHANGE THE WORLD
NSC
NORTH STAR
A STAR LIGHTING THE BLOCK WORLD

NSC

Illuminating the stars of the block world

From birth to development, there is an invisible line that involves everyone.Only 5% of the world's people have mastered 95% of their wealth. As productivity increases, the gap between rich and poor is growing.The social class is becoming more and more obvious. A large number of resources are in the hands of a few people. The vast majority of human beings are unable to change their own destiny.

The emergence of blockchain has ignited hopes in human society.

The emergence of blockchains is accompanied by hopes, while across hopes there are major obstacles.

The different point-to-point networks constructed by cryptography and mathematical algorithms make each block world an independent world. Similar to the LAN in the Internet era, we have gained the freedom of the block world. Open, our ideas are still imprisoned in a limited space.

Nsc- illuminates the stars of the block world and opens the door to the world block.

NSC is born for the link block civilization. NSC uses the asynchronous data synchronization and relay node idea to form a compatible transport protocol between different block networks through the Polaris Cross-Chain Protocol. Different blockchains will be used. Network interconnection makes the blockchain network change from the local area network to the Internet.And our thinking will be sustainable throughout the block network.

Polaris Light

Nsc full name "north star chain", Chinese translation for the North Star chain

Cynosure, the western name of the North Star, is in English, Cynosure has the meaning of attracting the center.The position of the polar star is relatively stable and difficult to change, so it gives people the feeling of being loyal and having their own position.From a life perspective, Polaris has the meaning of guiding us to the goal, just as it allows us to tell the same direction.

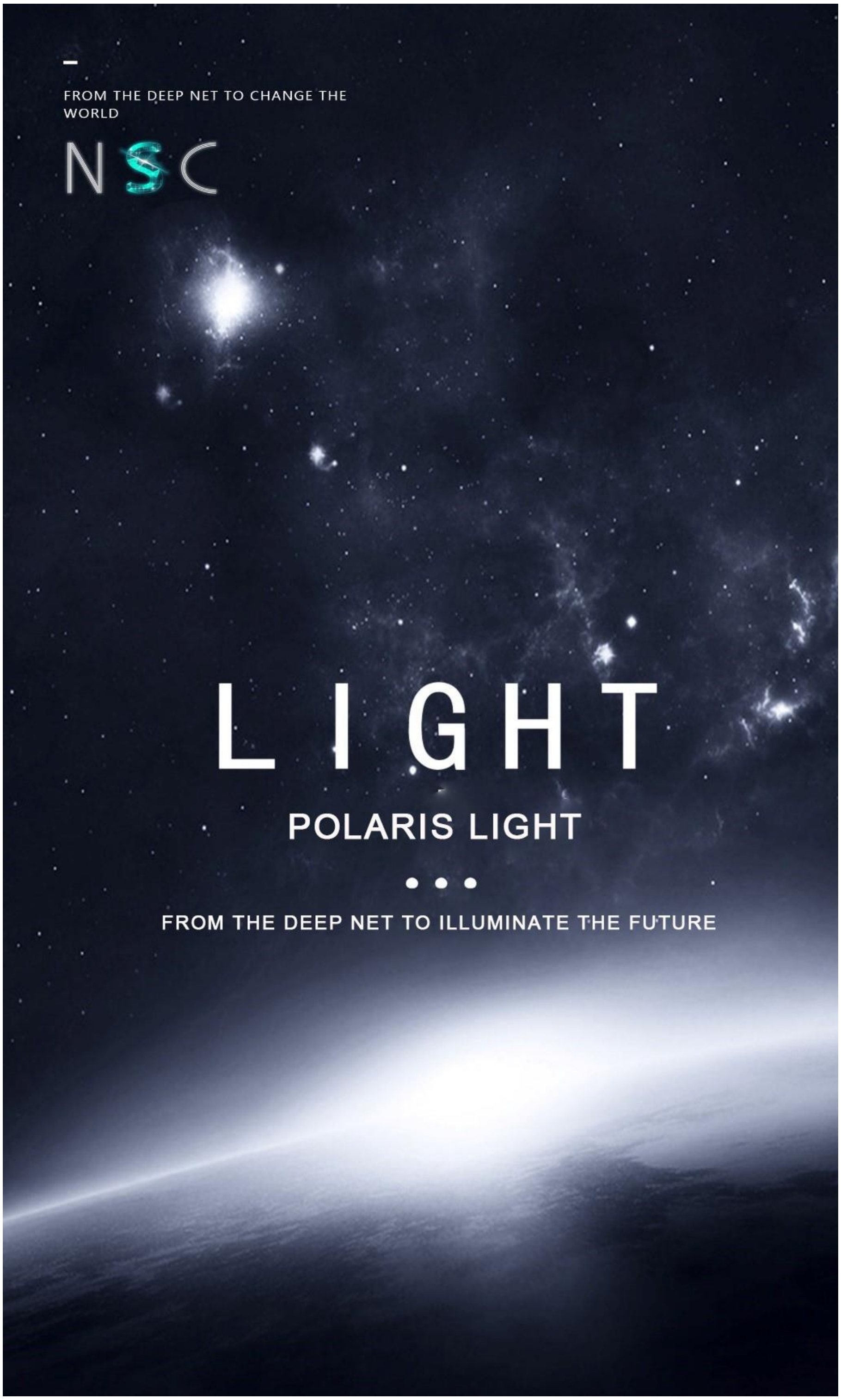
In the Chinese tradition, the North Star has an extraordinary significance. The ancients recognized the Beidou and the Polar Star as a whole. They are called "Douji", and the Douji is at the center of the rotation of the stars. The stars rotate around it, as if the sky dominates. The ancients used the four struggles to determine the time, and Beidou became the creator of the order of the heavens and the earth. The spring and summer, the long autumn and the winter collection seemed to be coming with the Beidou, and the Beidou became the center of the universe.

The north star chain was born in the blockchain, and it continues to inherited the wisdom of the blockchain during its growth and reproduction, and will continue to evolve, making the whole system more perfect.

We hope that the Tongbeidou cross-chain agreement can be the first to push the blockchain field from the "LAN era" to the "World Wide Web era."

Born from the blockchain, link the blockchain to guide the future, just like the North Star.

We hope that the Tongbeidou cross-chain agreement can be the first to push the blockchain field from the "LAN era" to the "World Wide Web era."



FROM THE DEEP NET TO CHANGE THE WORLD
NSC
LIGHT
POLARIS LIGHT
● ● ●
FROM THE DEEP NET TO ILLUMINATE THE FUTURE

Second, North Star Chain Introduction

2.1 Characteristics of blockchain

Equal value distribution network:

Due to the use of distributed computing and storage, there is no centralized hardware or management organization, the rights and obligations of any node are equal, and the data blocks in the system are jointly maintained by nodes with maintenance functions in the entire system.All participants have equal rights.The mathematical algorithm will guarantee the fairness and fairness of each participant's income distribution and system dividend distribution.The entire ecosystem will receive distribution based on value contributions.

Information cannot be falsified and irreversible

Once the information is verified and added to the blockchain, it is permanently stored.Because it is a distributed point-to-point storage method, unless the node can control more than 51% of the nodes in the system at the same time, the modification of the database on a single node is invalid, so the data stability and reliability of the blockchain are extremely high.

Anonymous and trustworthy

All participants are free to participate in the construction of the entire ecology, and everyone can use it freely and autonomously.There is no need for mutual authentication between nodes, and participation does not require centralized approval.In the network built with mathematical and cryptographic algorithms, the basic "constitution" that all participants will follow is the consensus algorithm.And through the encryption algorithm and hash algorithm, each participating address is first and anonymous, and protects the privacy and freedom of each participant in the public data.

2.2 NSC Chain's mission

NSC Chain is the world's first anonymous cross-chain data technology platform. Through the Beidou cross-chain technology and quantum file slicing technology, the current blockchain block storage cost is high, the transfer cost is high, the centralized cross-chain transaction cannot be decentralized, the assets cannot be cross-chained, and the data security risks are large.

NSC Chain is committed to making data retention and cross-chain asset transactions safer and more efficient; allowing more participants to protect their privacy; making cross-chain applications possible.

Through cross-platform development, NSC Chain will link the ecology of NSC Chain and IPFS, and concentrate more on the problem of block data storage.Of course, we do not rule out compatibility issues that may arise in the future, so the possibility of a consensus algorithm upgrade is not ruled out in the future.In the future, NSC Chain will protect the privacy and security of each participant's data, helping more creative developers to develop cross-chain applications such as decentralized exchanges. NSC Chain's file system will also be more enterprises and individuals. Provide services to protect information from misappropriation and monitoring by malicious third parties.

2.3 Innovation of NSC Chain

Technological Innovation 1: Beidou Cross-Chain Agreement

The Beidou cross-chain protocol guarantees the transmission of different blocks through the asynchronous elastic algorithm through the technical idea of the distributed relay super-operation node.Different from pow mining, the nsc miner's computing power will no longer perform meaningless random hash collisions. The miner encrypts the data by executing the slicing algorithm and encryption algorithm, and guarantees the data transmission between the links through the asynchronous algorithm. .The Beidou agreement will be the starting point for cross-chain transactions and cross-chain payments.

Technological innovation 2: Anonymity, privacy protection mechanism

All ordinary data transmission and transfer information, transfer amount and other data inside nsc are encrypted and transmitted.It is impossible for non-trading parties to obtain any valuable information such as address, amount, and transmission content.The use of advanced algorithms in mathematics and cryptography to guarantee anonymity and privacy can effectively guarantee the freedom of participation of the nsc ecosystem.

Technological Innovation III: Unique Ecology

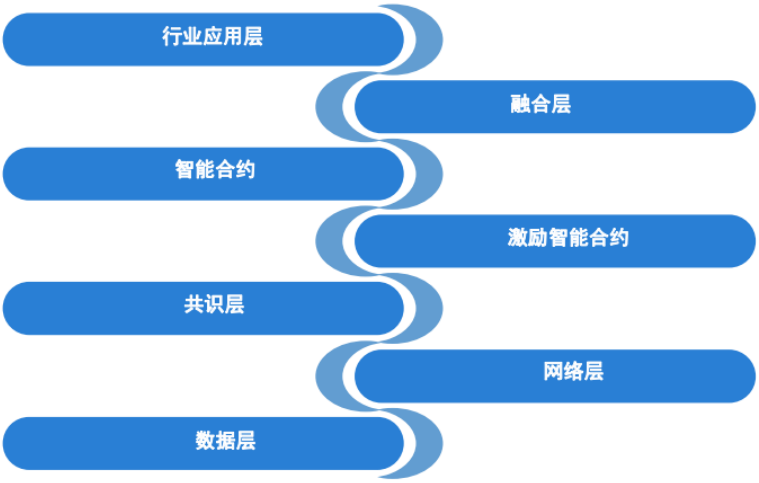
Through the incentive mechanism and the revenue intelligent dynamic algorithm, the value distribution is completed by the intelligent contract dao architecture.Use a transparent and transparent value distribution incentive to form a huge ecological network.Let the value carrier have stronger dispersion and circulation, and complete the exponential fission and linear growth of the ecological in the circulation of the value carrier.The dao architecture guarantees system dividends for each participant's distribution.

Technological Innovation 4: Quantum Holographic File Slice Encryption Technology

The unique holographic file slicing technology will upload tens of thousands of slices of encrypted large files.The encrypted file fragment distribution is stored in the ipfs interstellar network.The private key generated by the 256-bit asymmetric encryption will be saved by the data source.All third parties that are not authorized by the data source will not be able to steal data.The holographic intelligent algorithm can prevent the loss of files in the process of transmission and distributed storage. Only three-quarters of the file fragments can be used to restore the complete file.

Third, NSC Chain implementation

3.1 Technical Architecture



3.3.1 Data layer

The base DAG data structure NSC Chain uses the underlying DAG structure to store transaction data in the first phase.At present, many projects such as IOTA and Byteball have successfully built a public chain that can run stably with DAG, which proves the technological advancement and performance of the DAG chain.In the NSC Chain, the transaction information is encapsulated into units, and the units are linked together to form a DAG map.Since the unit can be linked to any one or more of the previous units, there is no need to pay more computational cost and time cost for the consensus problem, and there is no need to wait for strong data synchronization between the nodes, or even the concept of assembling multiple blocks of data units. Therefore, the amount of concurrency of transactions can be greatly increased and the confirmation time can be minimized.The DSG data structure of NSC Chain is shown in Figure 3-1. The directed edge between cells indicates that there is a reference relationship between the two cells. There is a directed edge from B to A, indicating that B refers to A, A. Is the parent unit of B, B is a child of A. At the same time, we call unit C indirectly refer to A, A is the ancestor unit of C; unit G does not have any parent unit, called creation unit, creation unit is unique Units X, Y do not have any subunits, and such units are called top units.

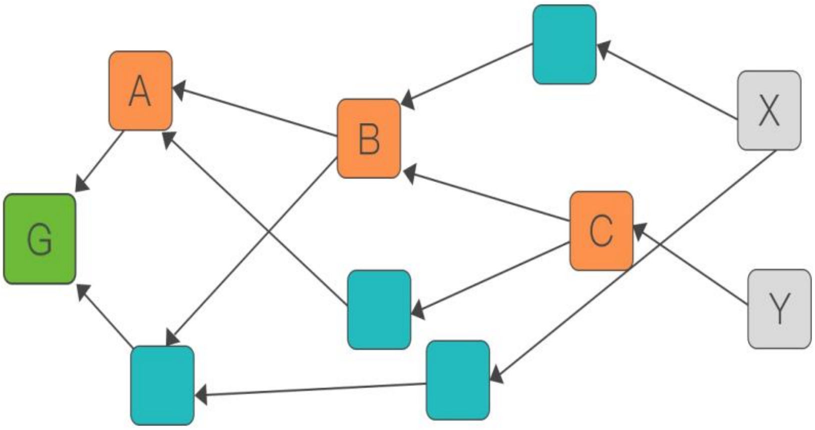


Figure 3.1.1—NSC Chain directed acyclic graph

HashNet data structure based on enhanced DAG HashNet is a directed acyclic graph (DAG) consisting of an infinite number of vertices and directed edges connecting vertices.As shown in Figure 3-2.The figure records what data is sent to other nodes in what order by all nodes in the network. Each node has such a HashNet copy in memory.

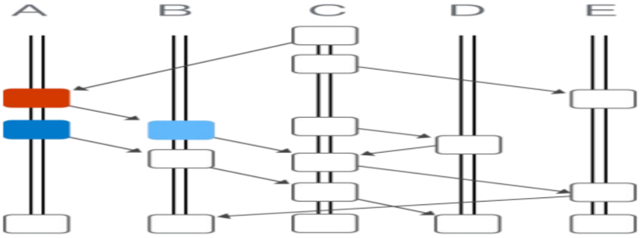


Figure 3.1.2: HashNet Data Structure Diagram

In the figure above there are 5 computer nodes a, b, c, d, e, each node has a placement vertex

The pillar of vertex (also called event).The latest events will be placed at the top of the map.

HashNet is growing upwards over time.

3.1.2 Network layer

The underlying communication network of the NSC Chain adopts the P2P architecture, and then an anonymous access mechanism between nodes is added to ensure the privacy protection of the information service.P2P is the abbreviation of English Peer-to-Peer, called "peer-to-peer" or "peer-to-peer" technology.IBM defines P2P as: “P2P systems consist of several interconnected computers and have at least one of the following characteristics: The system relies on the active collaboration of marginalized (non-centralized servers) devices, each member directly from other members instead of Benefit from the participation of the server; the members of the system play the role of the server and the client at the same time; the users of the system application can recognize each other's existence and constitute a virtual or actual group." In the P2P system, each node (Peer) They are equal participants, taking on the two colors of service users and service providers.The ownership and control of resources are distributed to every node in the network.P2P technology makes communication on the network easy and straightforward, and minimizes reliance on intermediate servers.P2P technology changes the location of the “content” from “center” to “edge”.In other words, it changes the state of the Internet that is now centered on a centralized website. Resources are not stored on the server and are stored on all users' PCs.P2P technology makes the terminal no longer a passive client, but becomes a device with dual features of server and client.Therefore NSC Chain has the characteristics of decentralization.

3.1.3 Consensus layer

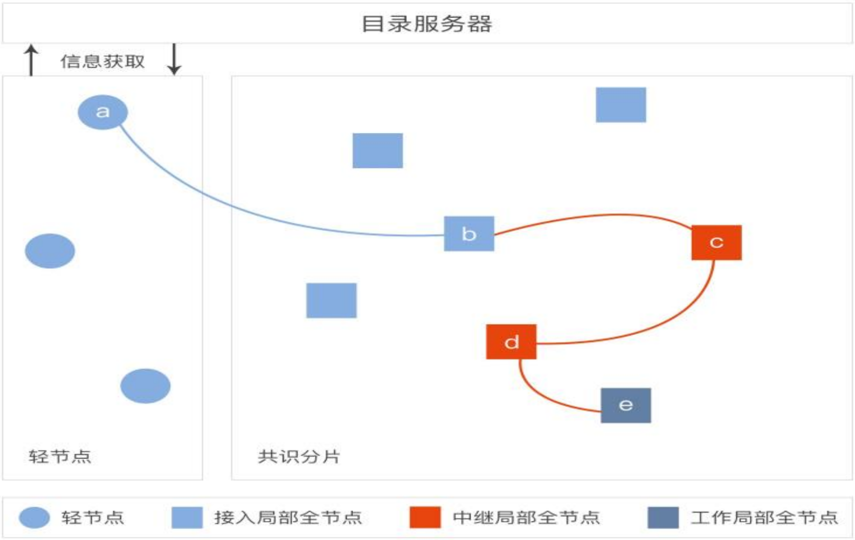


Figure 3.1.3: Basic schematic diagram of the NSC Chain anonymous communication network

NSC Chain uses DPOS to implement a consensus mechanism for blockchain accounting and data exchange.The Chinese name of DPoS (Delegated Proof of Stake) is called the share authorization certification mechanism (also known as the trustee mechanism). Its principle is to let the whole network token holder vote, thus producing at least 21 representatives as the system block production. We can understand it as 21 (infinitely expandable) super nodes or pools, and the 21 super nodes have the same rights to each other.From a certain perspective, DPoS is a bit like a parliamentary system or a people's congress system.Only one representative of the NSC Chain has the right to produce the block. If the representative cannot fulfill their duties (the block cannot be generated within a predetermined period of time), they will be delisted and the network will select the new super node. To replace them.

The main consensus mechanisms of the existing blockchain projects are PoW (Proof Of Work) and PoS (Proof of Stake), and a small number of projects adopt a revised BFT (Byzantine Fault Tolerance) consensus mechanism. Bitcoin is the most successful cryptocurrency under the PoW mechanism. Although the PoW mechanism has successfully proved its long-term stability and relative fairness, its efficiency is relatively low. In the case of Bitcoin, it can only process about 6 transactions per second and consumes it. A large amount of energy is not enough to meet the high performance requirements of the basic chain; while the PoS mechanism introduces the concept of “coin day” to participate in random operations relative to PoW, since there may be a small number of large households holding most of the generations in the entire network. In the case of the currency, the entire network may become more and more centralized as the running time grows. The PoS mechanism saves energy but does not improve performance and security.In order to achieve performance improvement based on security and decentralization, the DPoS mechanism emerges.The DPoS mechanism requires that the previous block must be signed by the trusted node before the next block is generated.Compared to PoS's "national mining", DPoS uses a system similar to "representative assembly" to directly select trusted nodes, and these trusted nodes (ie witnesses) replace other holders to exercise power, witnesses. The node requires long-term online, thus solving a series of problems such as the block delay caused by the fact that the PoS signing block is not always online.The DPoS mechanism typically achieves 10,000 transactions per second and can reach 100,000 times per second with low network latency, making it ideal for enterprise applications.

3.2 Anonymous algorithm

3.2.1 Zero Knowledge Proof Algorithm

Zero-Knowledge It means that the prover can believe that a certain assertion is correct without providing any useful information to the verifier.And NSC Chain is using a zero-knowledge proof technology to complete a truly anonymous blockchain network.

In order to achieve true anonymity, we need to first use an address as an intermediate address, and both parties need to verify each other's information.So how do you ensure that both parties have completed the verification they deserve, and they will not leave information on each other? Therefore, in order to solve this problem, the conversion of the interactive protocol to the non-interactive proof system is required.We will use elliptic curves, and we can get a limited, but enough, way to support the homomorphic hiding of multiplication.This will show this homomorphic concealment with restrictions, just enough to convert our protocol to the non-interactive system we want.

Constructing a curve of prime order with k = 12

```
  Input:    the approximate desired size m of the curve order (in bits).
  Output:    parameters p, n, b, y such that the curve y2    = x3 + b has order n over Fp    and
the point tt = (1, y) is a generator of the curve.

  Let P (x) ≡ 36x4 + 36x3 + 24x2 + 6x + 1
                                                                    2
  Compute the smallest x ≈ 2m/4 such that flog 3: loop
     t ← 6x2 + 1
     p ← P (−x), n ← p + 1 − t 6:    if p and n are prime then 7:           exit loop
     end if
    p ← P (x),        n ← p + 1 − t 10:        if    p and n are prime then    11:   exit loop
     end if
     x ← x + 1.
   end loop
   b ← 0
   repeat
     repeat
     b ← b + 1
     until b + 1 is a quadratic residue mod p
  Compute y    such that y2 = b + 1 mod p
       tt ← (1, y) on the curve E : y2 = x3 + b
   until ntt = ∞
   return p, n, b, y
```

In some cases, a fairly small auxiliary factor may be quite acceptable.For example, if a 256-bit prime field has no substantial impact on bandwidth usage, the encapsulation of the array will be affected.The curve y of k=8 and ρ5/4 can provide a group order of about 200 bits and map the discrete logarithm of the curve to the 2048-bit finite field.Furthermore, as we have already pointed out, even Value of k is advantageous from the perspective of effectively implementing the pairing algorithm.Therefore, it is interesting to study how to generate more curves that satisfy k as an even condition.ρ>1 is as small as possible (say, p ≤ 5 ≤ 4).

A practical method for solving the norm equation dV2=4hΦk(T1)(T2)2, that is, by selecting t and hoping to process the obtained D, it is generally inevitable since D∼tϕ(K), where ϕ(K)) is the Euler function.

For example, for k=2q, where q is an odd prime, we expect to find D∼tq−1.

However, if we can handle a CM discriminant D as large as tq−3, then the curve with k=2q is very simple, resulting in ρ≡log(P)/log(R)∼q/(q− 1).For some u (note that t is negative), the trace of Frobenius is t=−4u2 2, let x=t−1.

Suppose Φk(X) takes a prime number.

h = −(x − 1)/4,

r = Φk(x)

= xq−1 − xq−2 + xq−3 − xq−4 + xq−5 − · · · − x + 1

= xq−1 − xq−3(x − 1) − xq−5(x − 1) − · · · − x2(x − 1) − (x − 1), p = hr + t − 1,

DV 2 = 4hr − (t − 2)2

= −(x − 1)xq−1 + xq−3(x − 1)2 + xq−5(x − 1)2 + · · · + (x − 1)2 − (x − 1)2

= −(x − 1)x2[xq−3 − (x − 1)(xq−5 + xq−7 + · · · + 1)].

By construction, the −(x − 1)x2 factor is a square, so D is the square-free part of z = xq−3 − (x − 1)(xq−5 + xq−7 + · · · + 1). Since p = hr + t − 1, it is also clear that ρ ∼ q/(q − 1). For instance, if k = 10 (i.e. ρ ∼ 5/4) we get z = x2 − x + 1, and a simple search produces parameters like these:

t = −931556989582: 40 bits

r = 753074106157227719531468778253698105623799226081: 160 bits

p = 175382861816372173247473133505975362972517516867279787545493: 197 bits

ρ ∼ 1.237425

D = 867798424841873127503473: 80 bits

Another example, now for k = 14 (i.e. ρ ∼ 7/6) where z = x4 −x3 +x2 −x+1:

t = −82011134: 27 bits

r = 304254450525046050085067914513460261078757135361: 158 bits

$p = 623806328015370575494732907659994082548136453468333889$: 183 bits

$\rho \sim 1.153987$

$D = 452367394849464569357932435353 61$: 106 bits

The anonymous issue of verification can be solved by a non-interactive proof system.

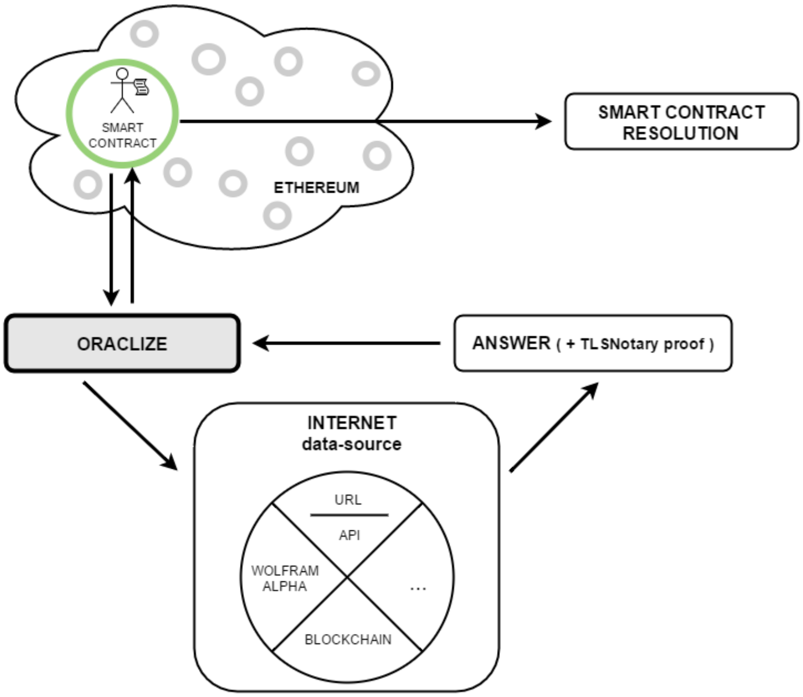
3.2.2 Carter system

Carter (Carter System) is the world's first blockchain system that realizes the privacy protection of Turing's complete smart contract through non-interactive zero-knowledge proof (NzK), compared with the existing blockchain privacy protection technology. Carter not only protects the privacy of account information and transaction information, but also protects the security of Turing's complete smart contract input and output. In addition, developers can also issue anonymous digital assets based on smart contracts on NSC Chain (Token), and the communication information with the smart contract will also be protected by privacy.Carter redesigned the blockchain structure and various underlying protocols, making the privacy-protected Turing-complete smart contract a reality, not only enabling privacy protection for a wider range of applications, but also because of its advanced NzK cryptography. The algorithm also further enhances the difficulty of attacking user privacy data.In addition, in the upcoming version 1.0, the practicality of the current NzK encryption algorithm is improved, the memory resources required to be consumed are greatly reduced, and the computational efficiency is improved.In addition, compared with the mainstream anonymous blockchain system on the market, Carter's support for Turing's complete smart contracts and privacy protection measures for its related decentralized applications have greatly expanded the usage scenarios. Chemical.What's more worth mentioning is that the team not only considers the privacy protection measures required by the decentralized application itself, but also plans to provide solutions from the point of view of the peer-to-peer network transmission security and the privacy of the account's physical network address. The solution allows for strong privacy protection when interacting with a centralized application or when interacting with a consumer client.

3.2.3 Difiniti Protocol

Difiniti Protocol (Difiniti Protocol): A distributed DNS system that can utilize existing P2P network interaction information, with automatic switching and dynamic addressing functions, and is resistant to attackers, enabling the entire data transmission network to have Very stable security.

3.3 Data Processing



```
    function GetTicker() {
        oraclize_setProof(proofType_TLSNotary | proofStorage_IPFS);
        update();
    }

    function __callback(bytes32 myid, string result, bytes proof) {
        if (msg.sender != oraclize_cbAddress()) throw;
        ETHXBT = result;
        update();
    }

    function update() {
        oraclize_query(60,                                                    "URL",
"json(https://api.RXChainoracle.xx/0/public/Ticker?pair=ETHXBT).result.XETHXXBT.c.0");
    }

    function kill(){
        if (msg.sender == owner) suicide(msg.sender);
    }
```

3.4 Quantum Slice Algorithm

3.4.1 Elliptic Curve Encryption Algorithm

Using the ellipse algorithm to encrypt the uploaded data The public key will be used to store the token and permanently write to the NSChina block record, which is returned to the user as a read credential.For example, RSA is based on the fact that two prime numbers p and q are easily multiplied to obtain n, while factoring for n is relatively difficult.What is the problem with the elliptical curve?

Consider the following equation:

K=kG [where K, G is the point on Ep(a,b), and k is an integer less than n (n is the order of point G)]

It is not difficult to find that given k and G, it is easy to calculate K according to the addition rule; but given K and G, it is relatively difficult to find k.

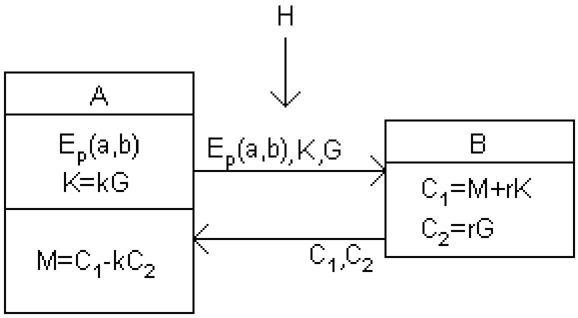
This is the problem with elliptic curve cryptography.We call the point G the base point, k(k< p style="word-wrap: break-word;" >

Now we describe a process for encrypting communications using elliptic curves:

1. User A selects an elliptic curve Ep(a,b) and takes a point on the elliptic curve as the base point G.
2. User A selects a private key k and generates a public key K=kG.
3. User A transmits Ep(a, b) and points K, G to User B.
4. After receiving the information, user B encodes the plaintext to be transmitted to a point M on Ep(a,b) (the encoding method is many, not discussed here), and generates a random integer r(r).
5. User B calculates point C1 = M + rK; C2 = rG.
6. User b passes c1 and c2 to user a.
7. After user A receives the information, it calculates C1-kC2, and the result is point M.

Since C1-kC2=M+rK-k(rG)=M+rK-r(kG)=M, the plaintext can be obtained by decoding the point M.

In this encrypted communication, if there is a voyeur H, he can only see Ep(a,b), K, G, C1, C2 and find K through K, G or R from C2 and G. of.Therefore, H cannot obtain the plaintext information transmitted between A and B.



In cryptography, describe an elliptic curve on an Fp, commonly used to six parameters:

T=(p,a,b,G,n,h)。

(p , a , b are used to determine an elliptic curve, G is the base point, n is the order of point G, and h is the integer part of the number m of all points on the elliptic curve divided by n)

The choice of these parameters directly affects the encryption.SafetySex.The parameter values generally require the following conditions to be met:

1, p is of course larger and safer, but the larger the calculation speed will be slower, about 200 can meet the general safety requirements;

2、p≠n×h；

3、pt≠1 (mod n)，1≤t<20；

4、4a3+27b2≠0 (mod p)；

5, n is a prime number;

6、h≤4。

3.4.2 Fragmentation Storage System

After the slice information is written into the NSChina block, the super node will send all the fragments to the IPFS storage node for storage and return the IPFS storage information.After the information is subjected to secondary asymmetric encryption, the public information is written to the block for permanent storage, and the private key is returned to the data source.

IPFS is a peer-to-peer distributed file system that attempts to connect to the same file system for all computing devices.In some ways, IPFS is similar to the World Wide Web, but it can also be viewed as a separate BitTorrent group that exchanges objects in the same Git repository.In other words, IPFS provides a high-throughput, content-addressable block storage model with content-related hyperlinks.This forms a generalized Merkle directed acyclic graph (DAG).IPFS combines distributed hash tables, encouraging block swapping, and a self-certifying namespace.IPFS does not have a single point of failure, and nodes do not need to trust each other.Distributed content delivery can save bandwidth and prevent DDoS attacks that HTTP scenarios can encounter.

Powerful network data distribution mechanism:

A hash fingerprint means that each file and all the data blocks it contains are converted to a hash string.Each node maintains a DHT (Distributed Hash Table) containing the corresponding mapping relationship between the corresponding data block and the target node.The entire hash table is organized into a binary tree, and the average query contact node complexity is O(log2N).For example, to query 10 million nodes, only 20 hops.

Based on content addressing rather than domain name addressing.Only through the hash of the file or data block, ipfs can automatically find the node that owns the data block in the whole network node and pull the data from the node.

Ipfs uses a distributed naming system called ipns to map hard-to-remember data hashes into easy-to-remember strings.This can be analogous to the mapping between domain names and ip addresses.

Ipfs has the following features:

相同 The same data content is given a unique hash fingerprint. By comparing the hash fingerprints, it can be judged whether the data blocks are consistent, and the data storage space is prevented from being wasted;

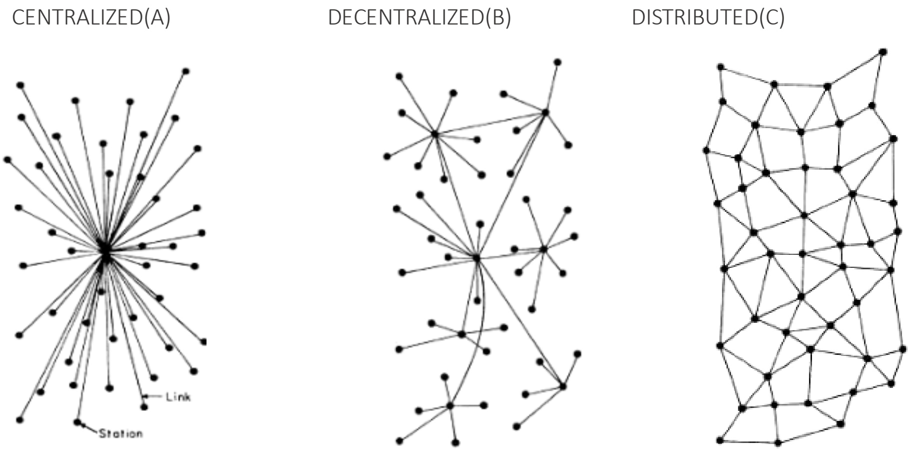
节点 The node itself uses a git-like version control system to manage local files and data blocks.This not only ensures the redundancy of the data block, but also provides a traceable historical version;

√ IPFS nodes need to use blockchain technology in maintaining hash routing table and account consistency. On the one hand, they reach consensus on the content and nodes in dynamic addition and subtraction; on the other hand, they are NSC Chain in the incentive mechanism. Document data storage management construction base platform;

刺激 The node is excited to store rare data blocks by issuing tokens.The node can not only pull the required data from other nodes, but also store the new data in its own node for other nodes to download;

数据 The data stored in ipfs will be permanently saved and cannot be deleted by any third party. Only the data producer has its own modification authority;

√ In the process of IPFS storage and data transmission, due to the distributed node storage mode, there is a very small probability event that the node will lose data. NSC Chain's holographic file slicing technology ensures the security of each user's data thoroughly. It solves the file loss phenomenon of IPFS storage transmission and guarantees complete data integrity and security.



CENTRALIZED(A)

DECENTRALIZED(B)

DISTRIBUTED(C)

Ipfs is a hypermedia protocol based on content and identity addressing, unlike traditional location addressing

At the level of the IPFS protocol, this system is completely transmission neutral.This means that nodes can run on any transport protocol.In fact, IPFS nodes do not need to be referenced by a centralized IP.IPFS nodes can run in a variety of network architectures, and IPFS is an innovative paradigm shift decentralized storage.No part of the platform will be stored on a centralized server.Therefore, no organization, anyone or even NSC Chain can check or restrict the data source to publish works on the IPFS platform.The identity information generation and verification node is uniquely identified by the NodeId.It is usually a public key created using S/kademlia's static encryption puzzle.The node will store its public-private key pair, and the user can start at each

Registering as a "new" node at the time of initialization, but this leads to the loss of accumulated network revenue.

```
type NodeId Multihash
Type Multihash []byte // Self-describing cryptographic hash summary
type PublicKey []byte
Type PrivateKey []byte // Self-describing private key
type Node struct {
NodeId NodeID
PubKey PublicKey
PriKey PrivateKey
}
Difficulty = <integer parameter>//Based on S / Kademlia's IPFS identity generation:
n = Node{}
do {
n.PubKey, n.PrivKey = PKI.genKeyPair()
n.NodeId = hash(n.PubKey)
p = count_preceding_zero_bits(hash(n.NodeId))
} while (p < difficulty)
```

On the first connection, the peer exchanges the public key and checks if the peer's NodeId is equal to the public key's hash.
If no, the connection is terminated.

3.5 Account System

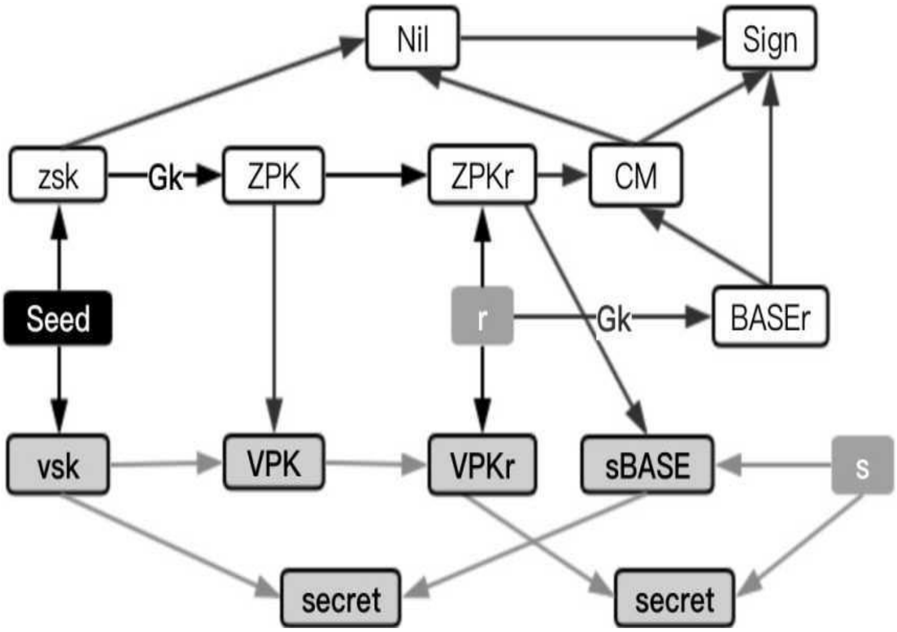
The account system is divided into two categories: user accounts and contract accounts.The user account is that the user selects a 32-byte seed and the contract account generates a 64-byte address according to the environment in which the user installs the smart contract. Both are unique to the system and cannot be duplicated.

The user account can generate a 64-byte private key SK and a 64-byte public key PK, which is the user's payment address.When installing or invoking a smart contract, the wallet will generate a temporary storage address PK based on the current situation. This temporary storage address cannot be associated with the user's private and public keys in any way and will only be used once.

When the smart contract is installed, the wallet will convert the scratch address to a 64-byte smart contract address (CADDR) according to the current situation.When the node receives the address, it needs to ensure that the smart contract address has not appeared before.

Let:

Gk = NewEccQ



seed = New(Byte32)

r = RandFrQ

s = RandFrQ

a = RandFrQ

m = Message

SK:

zsk = HASHzsk(seed)

vsk = HASHvsk(seed)

sk = (yskt zsk)

zvsk = zsk • vsk

PK/TK:

ZPK = zsk-Gk

VPK=vsk-zsk-Gk

PK= QPK,VPK)

TK=(ZPKtvsk)

PKr:

BASEr = r • Gk

ZPKr = r • ZPK

VPKr = r • VPK

PKr =(yPKr,ZPKr,BASE^

Trace :

VPKr = = vsk • ZPKr

Enc :

BASEs = s • ZPKr

SECRET = s * VPKr

key = Hashs(SECRET)

M = Encvk(m, key)

Dec :

SECRET = vsk- BASEs

m — Decvk^M, key)

Sign :

k = Hash^a, zvsk, ni)

sO = k • BASEr

h = Hash2(S0,m)

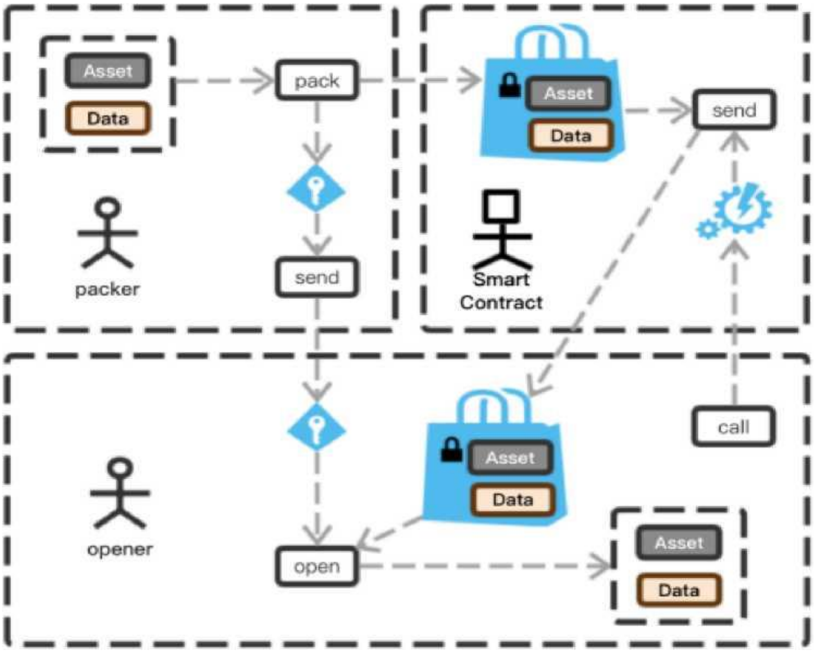
si = k + zvsk • h

sign = (sO,sl)

Verify :

si • BASEr = = SO + h- VPKr

Seed is the account seed and the user must keep it.SK is a private key that is not persistent storage, where TK is a tracking private key that can be provided to a trusted third party for auditing the account.PK is the transaction target address provided by the public key to other users is the temporary storage address, which is provided to the smart contract to temporarily receive the target address of the asset.



Fourth, NSC Chain Ecology

4.1 Ecological structure

Super computing node ecology:

Based on a unique technical algorithm, NSC Chain's super-computing nodes will work together to form a super-computing center that does not require interference and automatic operation. All received data is encrypted and distributed and stored. NSC Chain has an automatic error correction trace and correction system. Data synchronization is performed between each node by running an asynchronous protocol.All SuperNodes need to meet the minimum computing power and storage performance review before applying.After submitting the application, all the nodes will vote.

Application Ecology:

NSC Chain's cross-chain technology will attract many decentralized DAPP calls.NSChain plans to use the community to guide participants to actively participate in the maintenance and fission of the applied ecology.For creative freelance developers, creative apps will be demonstrated in the app ecosystem.Creative applications are in the application ecosystem of a large number of participants.

In the future, there will be a variety of beautiful cross-chain applications in the NSC Chain application ecosystem, such as distributed decentralized exchanges.

Developer:

Global companies and all participants are free to develop.Based on NSC Chain cross-chain data transmission technology, deploy applications to the NSC Chain application ecosystem.The NSC Chain development platform will significantly increase development efficiency and lower the developer's technical threshold. At the same time, the NSC Chain ecosystem provides a large number of community users for each application developer, allowing developers to focus on operational and application ideas.

Arbitration Commission:

The work of the Arbitration Commission is to act as a supervisor of the Foundation. The Arbitration Commission will arrange 16 seats to vote in accordance with the 180-day rotation cycle.The token used for voting will be locked for 180 days.Members may be re-elected.Three of the 16 seats have one vote veto. The three supervisory seats will be voted by 16 members to generate two seats. The Foundation will vote for one, with a rotation period of 360 natural days.Each vote will be publicly held on the official website.The Arbitration Commissioner will be entitled to the Foundation’s token for the construction of the Arbitration Commission.

4.2 Mine release

1. Ecological development Tokens with a total amount of 130 million to be dug will be distributed by value for all nodes after an 80-year cycle.

2. The number of tokens in the pool is halved every four years.Each delivery billing cycle is a block interval with a starting value of 139.4225 per cycle.

Proportion of different types of mining pools:

time	Total output	Mine pool 1	Mine pool 2	Mine pool 3	Mine pool 4	Mine pool 5
First 4 years	25003052.1	6250763.0	5000610.4	5000610.4	1250152.6	7500915.6
9-12 years	6250763	1562690.7	1250152.6	1250152.6	312538.1	1875228.9
13-16 years	3125381.5	781345.3	625076	625076	156269.0	937614.4
17-20 years	1562690.7	390672.6	312538.1	312538.1	78134.5	468807.2
…						
80 years	6104.3	1526.1	1220.9	1220.9	305.2	1831.3

(The specific algorithm is based on the main online line, and the NSC Chain Foundation reserves the right to adjust the algorithm during the system development phase)

2.3 income algorithm

Storage node revenue calculation:

1 Mine pool income: time period t (positive integer multiple of 30s), total pool period c, total task coefficient m in the period, task coefficient m1 of the task involved, task participant number p.

All the tasks in the system participate in the number Z1 during the period, and all the participating numbers Z in the period (time period).Formula: 0.6CT / 30 * M1/M/p + 0.4Z1/Z

Developer revenue calculation:

1 Mine pool income: time period t (positive integer multiple of 30s), total pool period c, total participation number p (one person participates in an event recorded as one person), and the number of application participation is recorded as p1

Formula: ctp / 30p1

2 application revenue: total application income z

Formula: 0.4z

3 development fund raising algorithm

The creator releases y% of the proceeds of the work, recruits M NSC Chains for authoring, and completes Q(Q...Q) NSC Chain recruitment (Q<=M) by the end time.

All behaviors that earn NSC Chain require time series T competition, and time is a factor that affects returns. The earlier the time, the higher the return.

Formula: $\Sigma_{k=1}^{x} k$ S=(x+1)-u /

If the developer's income is A, the income of the Nu investment creation = A * y% *.

The y% share of the proceeds, the collection of M RXChain for the declaration, the proceeds from the Nu investment announcement

= A * y% * S* QU/ $\sum_{k=1^{QU}}^{x}$

Calculation of mining revenue: the computing power of the whole network is recorded as o, and its own computing power is recorded as o1, the total amount of computing power pool c

Formula: c*o1/o (the test algorithm will be published after the main online line)

V. NSC Chain application scenario

5.1 cross-chain application

a. Scenario 1: Cross-chain financial tools

At present, the traditional financial market matching trading system has many shortcomings: high agency costs, poor expandability, and low efficiency.NSC Chain's cross-chain technology can help developers build a decentralized digital asset trading platform (decentralized exchange) and eliminate agency fees, remove professional thresholds, easily expand, improve accuracy and efficiency.

Scenario 1: Cross-chain financial tools

b. Scenario 2: Go to Center Insurance

Insurance is an industry that is closely related to the public.Due to the centralized management of the traditional insurance industry, there have been criticized problems such as the process is too long and the claims procedures are complicated and slow.At the same time, the huge insurance company agent system also makes a large part of the insurance income used for business operations.The decentralized insurance through the NSC Chain cross-chain can solve these shortcomings perfectly.For example, an NSC Chain platform can be used to create an aviation delay risk.Users who want to purchase aviation insurance can purchase it with tokens before taking the flight.In most cases, the user's flight will be on time, so the user's token will be locked in the smart contract corresponding to the aviation insurance incident.When a flight is delayed, the smart contract will write the flight number of the delayed flight to the claims insurance smart contract of the aviation insurance.The Claims Smart Contract will be able to automatically return different types of token claims for customers who have purchased the flight insurance for the flight number.The entire process is fully automated and requires no human intervention. All users' tokens will be used for customer claims in addition to a small portion of the miners' fees.

4.2 Distributed applications

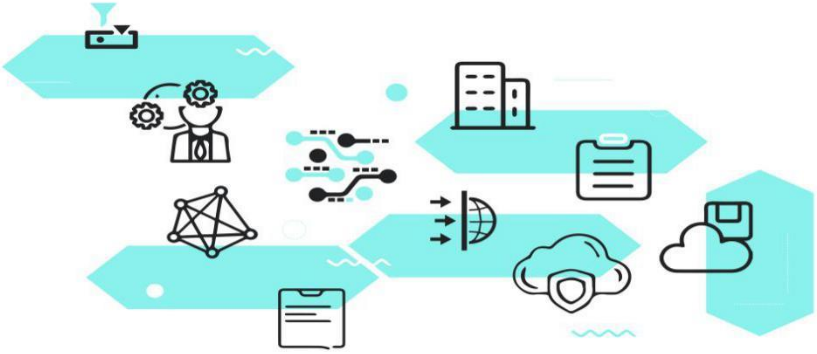
Scene 1: Distributed Network Disk

The existing network storage space service provider adopts the centralized storage of the enterprise. After each file uploaded by the user retrieves the MD5 value, the non-repeating data is uploaded and stored.In order to prevent accidental loss and damage of data, large-scale network storage service providers will repeatedly store (backup) each data file, which further increases the cost of storage.Moreover, due to the influence of different regions, some service providers will destroy user files without the user's permission.This also leaked another problem. Among the existing data service providers, some data service providers did not protect the privacy of users. The service provider did not encrypt the original data. The service provider and any third party bypassing the firewall. Users can view and read and write user's private data without permission from the user.Distributed network storage applications based on NSC Chain storage technology will completely address issues such as privacy, security and cost.All data is sliced and stored in a distributed manner across geographically dispersed nodes.Any service provider and third party that is not authorized by the user will not be able to access and read any data.The development of data storage applications through NSC Chain is efficient and low-cost, and service providers' storage costs are only one-fifth of the current cost.

Scene 1: Distributed Network Disk

Scenario 2: Enterprise Big Data Storage Solution

At present, big data within the enterprise is stored in a centralized manner, especially for some Internet companies.User information and user privacy have huge security risks. Facebook's user information disclosure has caused people around the world to worry about the security of private data and personal information.NSC Chain will be an open distributed data storage and application development platform in the future.Enterprises can address data storage efficiency and data security issues based on NSC Chain's approach.



Scenario 2: Enterprise Big Data Storage Solution

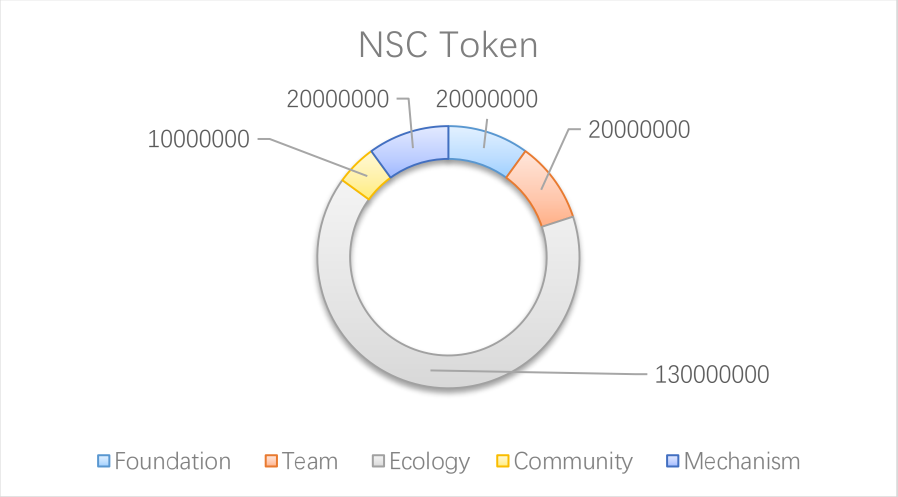
V. NSC Token Distribution

Issue Name: NSC (North Star Coin)

Number of issues: 200000000

Issue type: erc20

Distribution ratio: 10% of the team, 5% of the community construction, 10% of the organization, and 65% of the node ecology



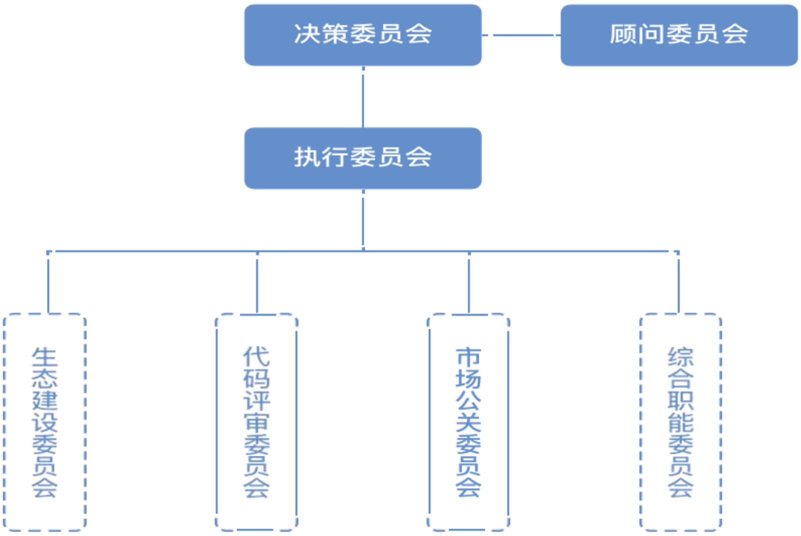
Description:

1. The technical team locks the warehouse, and releases 5% monthly after the

main online line, and the release is completed in 20 months;
2. Foundations using tokens must be reported and passed through the decision-making committee and publicized;
3. Community rewards are not locked in the circulation of Token.
4. The ecological release of the self-initiated online line began to be halved every four years, and the release was completed in about 80 years.Super nodes and storage nodes used to reward computing power to the main network.

6. Foundation and team introduction

6.1 Foundation Architecture



The nsc Foundation (hereinafter referred to as the “Foundation”) is a legally incorporated management body established in Singapore.The Foundation is committed to the development, construction and governance of nsc and promotes the establishment, evolution and formation of ecological communities.In order to avoid the direction of community members, the inconsistency of decision-making, and even the resulting division of the community, the Foundation explains the generalities and privileges of the management community by establishing a good governance structure.The foundation's governance structure is designed to maintain a balanced ecological sustainability, decision-making efficiency, and money management compliance.The Foundation exercises daily powers from the decision-making committee.

6.2 Team Introduction

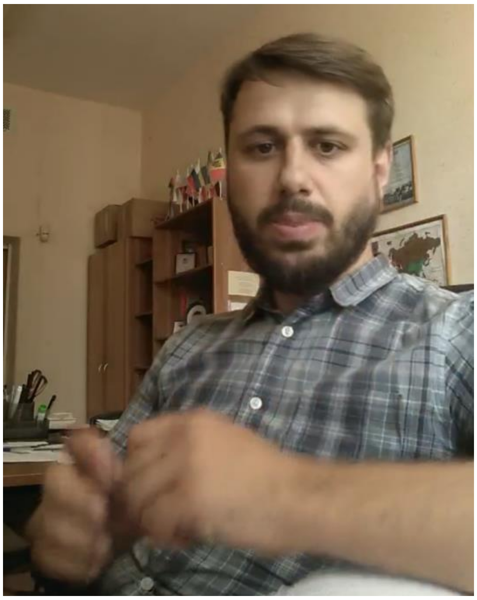
1.alex(CEO)

Alex, graduated from Yale University, focuses on the world currency system and financial system, and has his own unique insights into the blockchain industry and the virtual currency market. He led the Yale University monetary and international relations research project.Currently co-founder of the British data technology company Blis. NSC Chain co-founder, CEO.

2.Daniil(CTO)

Graduated from Stanford University with a master's degree in computer science and a network security consultant from the American Computer Society. The computer has long been engaged in cryptography and P2P peer-to-peer encryption network transmission technology research. G2G co-founder of well-known game trading website, has many years of experience in distributed network security, NSC Chain co-founder

People, CTO.



Tammo Weiss(CMO)

He holds a master's degree in communication from Heidelberg University. He has worked for Unilever, the chief operating officer of Garena, and is currently the co-founder of NSC Chain.

Disclaimer

Nothing in this white paper constitutes legal, financial, commercial or tax advice, and you should consult with your own legal, financial, tax or other professional adviser before engaging in any activity related to this white paper.Neither NSCChainFoundation Ltd. (hereinafter referred to as the “Foundation”) nor any project team member working on the RXChain platform or any related project (“NSCChain Team”), nor any third-party service provider, should respond to you. Responsible for any direct or indirect damages or losses suffered in connection with obtaining this material, materials provided by the Foundation, or accessing the Site or any other material published by the Foundation.

All contributions will be used for Foundation's goals, including but not limited to upgrading and supporting the research, design, development, and implementation of decentralized passwords or blockchain solutions to build a transparent, free, and reliable data market.

This white paper is for informational purposes only and does not constitute a prospectus, an offer document or a securities offer or investment solicitation.The information below may not be exhaustive and does not imply any element of contractual relationship.The accuracy or completeness of such information is not guaranteed and it is not intended to provide any representation, warranty or promise as to the accuracy or completeness of such information.In the event that this white paper contains information obtained from third parties, the Foundation and/or the NSCChain team do not independently verify the accuracy or completeness of such information.The accuracy or completeness of such information is not guaranteed and it is not intended to provide any representation, warranty or promise as to the accuracy or completeness of such information.

This white paper does not constitute an offer by the Foundation or the NSCChain team to sell any NSCChain Token (as defined in this white paper), and the whole or any part thereof, and the facts stated therein, do not form the basis of any contract or investment decision. Associated with any contract or investment decision.Nothing contained in this white paper is nor can be cited as a commitment, representation or promise to the future performance of the Platform.Any agreement between the Foundation (or its affiliates) and you that purchases or sells NSCChain is governed solely by the terms and conditions of the agreement.

The Foundation and the NSCChain team do not and do not wish to make any representations, warranties or promises to any entity or individual, and declare no liability.Prospective purchasers of Token should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the Token Sales, Foundation and NSCChain teams. By accessing this white paper or any part of it, you make representations and warranties to the Foundation and the NSCChain team as follows:

(a) You acknowledge, understand and agree that NSCChain may be of no value, that there is no assurance or representation of the value or liquidity of NSCChain and that NSCChain is not used for speculative investments;

(b) You are not making any decision to purchase any NSCChain in accordance with any of the statements in this white paper;

(c) You will and at your own expense to ensure that all applicable laws, regulatory requirements and restrictions (as the case may be) are applicable to you;

(d) You acknowledge, understand and agree that if you are a citizen, resident or green card holder of the United States of America, or if you are a citizen or resident of the People's Republic of China, you are not eligible to purchase NSCChain.

All statements contained in this white paper, statements in press releases or from public access, and statements that may be made by the Foundation and/or the NSCChain team may constitute forward-looking statements (including information about market conditions, business strategies). And the intentions, beliefs, or current forecasts of the plan, financial situation, specific regulations, and risk management practices).You are kindly requested not to undue reliance on these forward-looking statements as they involve known and unknown risks, uncertainties and other factors that may cause actual future results. With the aforementioned prospects

The results described in the sexual statement are quite different.These forward-looking statements speak only as of the date of this white paper, and the Foundation and the NSCChain team expressly disclaim any obligation, whether express or implied, to modify these forward-looking statements to reflect events after this date.

This white paper may be translated into a language other than English. If there is a conflict or ambiguity between the English version of this white paper and its translated version, the English version shall prevail.You acknowledge that you have read and understood the English version of this white paper.

No part of this white paper may be copied, reproduced, distributed, or transmitted in any way without the prior written consent of the Foundation.