2022

Coopunion Network White Paper

A high performance Layer 1 Network that continually evolves from Ethereum

Abstract

Blockchain is a decentralized ledger technology. It is another revolutionary innovation of Internet technologies after artificial intelligence, big data, cloud computing and Internet of things. Blockchain technology promotes the transformation of production relations in the development of digital economy. With the consecutive waves of digitization in recent years, network applications such as Ethereum and Bitcoin have sprung up in the global digital economy system, promoting the rapid development of blockchain technology. In the continuous innovation and evolution, after iterations during more than a decade, blockchain technology has gradually become pivotal in digital economy globally after COVID-19. The Internet enters a new era.

Coopunion Network, abbreviated as CUN, is a distributed network infrastructure that evolves from Ethereum. It aims to build a blockchain network and ecosystem with high-performance, high stability and low cost, to improve users' experience, to reduce use cost, and to protect users' assets in digital world. Ultimately CUN will be a DAO-governed network.

Innovate from the underlying technology, CUN has made technical improvements in consensus mechanism, incentive mechanism, privacy protection, identity verification and multichain cross-chain respectively, which characterize CUN with high performance, high flexibility, high decentralization and incentive balance. Join and maintain CUN, users will receive Coopunion Network Point

（abbreviated as CUNP, which can be used to pay Gas on CUN, and is also the perpetual certificate that quantifies users' contributions , as well as the tool for community governance) . Compared with other main blockchain projects, its incentive rules and election mechanism imply higher efficiency and equity.

Content

CUN Vision

Coopunion Network, abbreviated as CUN, is a distributed network infrastructure that evolves from Ethereum. It aims to build a blockchain network and ecosystem with high-performance, high stability and low cost, to improve users' experience, to reduce use cost, and to protect users' assets in digital world. Ultimately CUN will be a DAO-governed network.

1.Innovation and Performance

1.1 Consensus Mechanism

Coopunion Network (CUN) innovatively adopts a periodically hybrid consensus mechanism to realize the block consensus. The consensus mechanism is of high performance, high flexibility, high decentralization and balanced incentive.

① **High Performance**

Hybrid consensus mechanism adopts Proof-of-Authority (POA) [1] and Proof-of-Stake (POS) [2] as the access, and the algorithm of Practical Byzantine Fault Tolerance (PBFT) [3] is used in the validator cluster for high-throughput, low-delay consensus. In the meantime, layered architecture is applied to improve the PBFT algorithm to optimize hierarchical consensus communication, which can improve the scalability while ensuring the performance.

② **High Flexibility**

Different access mechanisms and leader election algorithms are selected in different stages of the project to conduct the dynamic network node addition and deletion. Besides, incentive parameters, CUNP distribution proportion and consensus network scale are dynamically adjusted in the light of network operation to build an infrastructure with great flexibility.

③ **High Decentralization**

Following the core concept of blockchain, CUN network moves gradually towards decentralization. Incentive measures for ordinary nodes to maintain the network and voting are set to encourage more nodes to enter the network. In addition, to build a network with fairer consensus, centralized behaviors such as taking the lead in voting and building mining pools are not advocated.

④ **Balanced Incentive**

In the early stage, identity verification is chosen for nodes' access and 5000 CUNPs are staked to prevent malicious actions from nodes. Then, in the middle and later stage, the quantity of staked CUNPs will increase and enter into the incentive pool. The amount of incentive rewards obtained is in direct proportion to the node' s staking ratio and staking time. With the identity access setting, the incentive becomes more balanced to attract more nodes to join in and maintain the network, promoting it's positive development and scaling. Moreover, incentive mechanism of CUN is more equitable and rational that both network maintenance and business contributions are recorded on blockchain.

1.2 Privacy Protection

The privacy of CUN users is in all-round protection via varieties of encryption algorithms. Simultaneously, the modular and pluggable design of CUN network facilitates the usage of developers, system upgrade and maintenance.

① **Modular Design**

For the privacy security of developers, merchants and users, CUN introduces a special privacy protection module which includes three submodules of CUNZKLib (Coopunion Network Zero-Knowledge Proof Library), CUNHELib (Coopunion Network Homomorphic Encryption Library) and CUNTEE (Coopunion Network Trusted Execution Environment). The three submodules provide the functions of zero-knowledge proof, homomorphic encryption and trusted execution environment respectively for the higher-layers. And they are compatible with each other while performing their duties respectively at the same time. Developers are able to develop high-performance and secure business programs easily by calling pertinent interfaces or functions of the privacy protection module.

② **Pluggable Design**

As CUN seeks to ensure the upgradability and easy maintenance of the system, it will add the privacy protection module and corresponding submodules to the network in the form of components.

1.3 Identity Verification

Users can manage their own identity information in CUN by the digital identity verification function which is specially designed .

① **User Privacy Protection**

The basic personal information of users is encrypted on the chain to avoid privacy leakage. As for users' advanced personal information, it is stored in the

ledger center in a verifiable declaration way and cannot be viewed by any other people without the user's permission. This measure minimizes the leakage of personal privacy and avoids the fraudulent use of identity.

② **User-Friendly**

Users can sign up via PointBox and manage their own CDID account, ledger center and assets without the need to save UTXO and other data complicatedly, which minimize their use cost.

2.Technology

2.1 Overview

CUN aims to build a blockchain network and ecosystem with high-performance, high stability and low cost, to improve users' experience, to reduce use cost, and to protect users' assets in digital world.

According to design principles, CUN makes innovation in consensus mechanism, incentive mechanism, identity authentication, privacy policy and cross-chain. In terms of consensus mechanism, for a long-term consideration, a phased hybrid consensus mechanism is adopted to match the various needs in different development stages, which guarantees the gradual scaling of CUN with high performance and TPS (Transactions per Second). The incentive mechanism is adapted to the consensus, the rules are designed from the perspective of community cooperation, and the overall design is ordinary-node-friendly. CUNP-staking voting mechanism will be introduced in the second stage to incentivize ordinary nodes to maintain the network and realizing the PoA + PoS consensus. To resist centralized behavior, CUN encourages ordinary nodes to participate in the maintenance of the network. In terms of identity authentication, a decentralized identity authentication system CDID is created to realize a secure and standardized identity management and to protect users' privacy. Finally, in terms of the privacy policy, the privacy protection system of CUN is modularized as an

underlying technology for developers in the condition of guaranteeing the security of private data and offering efficient development with the tools of Zero-Knowledge Proof, Trusted Execution Environment and Homomorphic Encryption Library.

2.2 Design Philosophy

(1) Sophisticated and advanced: Adopting blockchain as the underlying technology and creatively equipped with the phased consensus mechanism which faces large-scale and high-concurrency blockchain applications, CUN possesses a sophisticated system structure that integrates advanced technologies, achieving a network with high-concurrency, low latency, high throughput, high decentralization and well-balanced incentive mechanism.

(2) Easy to use: The underlying blockchain system is packed and easy-to-use interfaces are provided for developers to access the whole system, making them concentrate on the innovation and development of applications. Users are able to enjoy the one-stop business processing through PointBox.

(3) Secure and reliable: Built upon the deep-going research on consensus algorithm, cryptography, smart contract and other technologies, CUN provides decentralized, traceable, reliable, secure and stable services for users. It can share information securely and improve the system efficiency.

(4) Open access: CUN is equipped with side chain, which is an open cooperation

platform for various businesses including certificate of deposit, asset management and transaction. The main and side structure creates more opportunities for members and users to participate in the open business cooperation, to develop an open and win-win CUN ecosystem.

2.3 General Framework

Guided by the design principles of "easy to use, secure and reliable, open and shared", the overall architecture of the CUN system is divided into four layers from top to bottom, namely the interface layer, the management layer, the consensus layer and the basic service layer. The interface layer is the top layer of the entire system, responsible for providing a series of development tools and interfaces to business developers. It is also the first and most frequently contacted layer for developers, containing modules such as gRPC, JavaSDK, and CLI. The management layer is the second layer of the CUN system, responsible for a series of affairs such as the authority division including access management, contract management, authority management, parameter management, certificate management and other modules. The consensus layer is the core layer of the entire CUN system, which ensures the smooth system operation and the consistency of system nodes. It includes four modules: consensus adapter, consensus node election, consensus algorithm implementation, and consensus reward and punishment mechanism. The basic service layer is the bottom layer of the entire network that provides multiple modules such as privacy protection and CDID system. The overall frame structure is

shown in Figure 1:

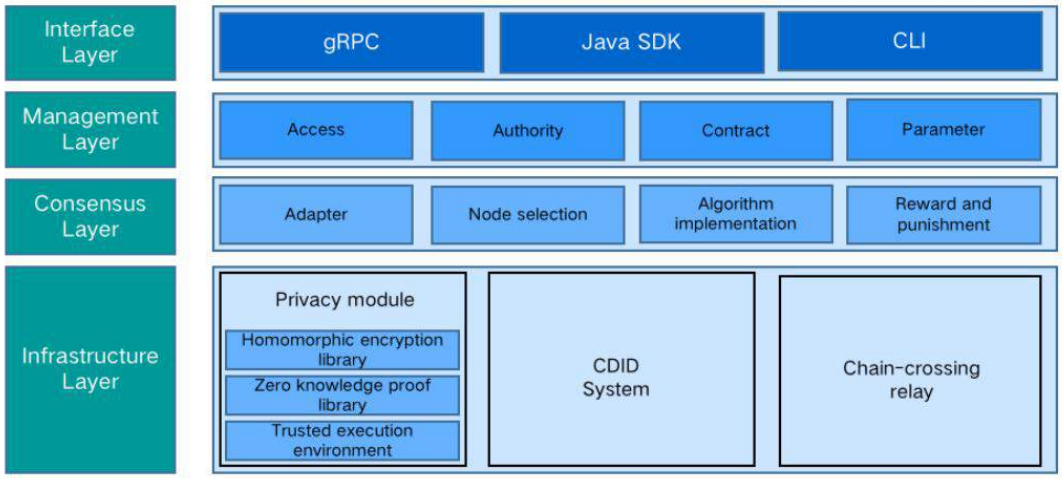

Figure 1. CUN System Architecture

The consensus layer and basic service layer are the core parts of the system, they will be introduced in detail in the later chapters. The following only introduces the functional modules of the interface layer and management layer.

RPC module: This module is based on HTTP/2 protocol transmission and uses Protocol Buffers as an interface description language. It is a set of protocols and interfaces for the client to interact with the blockchain system. Users can query blockchain-related information (such as block height, block, node connection, etc.) and send transactions via the RPC interface.

JavaSDK: a basic JAVA language toolkit for upper-layer application developers. The CUN system opens an interface outwards so external business programs can be written in Java language. Developers only need to select the SDK of the corresponding language per requirements of their own business programs and use

the API provided by SDK for programming to realize the operation on the blockchain. Besides, some SDKs have a built-in console that developers can directly use the command line to perform the above-mentioned functions such as compiling contracts, deploying contracts, sending transactions, querying transactions and chain management.

CLI module: an important interactive client tool of this system acting as the role of rich control and automated system management. CLI establishes a connection with blockchain nodes to implement read and write access requests to blockchain node data. The console has a abundance of commands, including querying the state of the blockchain, managing blockchain nodes, deploying and calling contracts, etc.

Access management: responsible for the access management of Validator, the verification node of the entire CUN system.

Permission management: set different permissions for nodes to ensure the system security.

Contract management: responsible for operations such as contract update and iteration on the chain.

Parameter management: In the CUN system, a part of parameters closely related to the operation of the blockchain are always in dynamic adjustment, so unified management through parameter management is required. The adjustment

of these parameters is usually determined by voting of the DAO organization in the CUN system using the multi-signature technology. Only after all nodes agree and sign can the parameters be modified, thereby ensuring the security of the parameters.

2.4 Consensus Mechanism and Incentive Mechanism

The CUN on-chain system adopts a phased consensus and incentive mechanism. In terms of the consensus mechanism, CUN adopts PoA as access consensus in the initial stage. The PoS + PoA consensus is adopted in the second stage of the mid-term to achieve an access consensus with a stake voting mechanism. And in the third stage, as the number of nodes and CUNPs held by nodes increase, the consensus network will upgrade to PoS + Practical Byzantine Fault Tolerance (PBFT) consensus to ensure the performance efficiency. In different consensus stages, different incentive mechanisms will be selected to enhance the enthusiasm of nodes.

2.4.1 PoA and PoS Consensuses

PoA, Proof-of-Authority, authorizes a group of nodes as validators at initial stage. The task of these nodes is to check and verify newly added identities, verify transactions, and organize blocks added to the network. To ensure the efficiency and security of the network, the number of validators is usually kept at a small scale.

PoS, Proof-of-Stake, is an alternative algorithm proposed to solve the problem of massive waste of resources in the PoW algorithm. In this algorithm, the accounting right is obtained by the node with the highest stake rather than the highest computing power in the system. Nodes holding more shares have a higher probability of deciding the next block and obtaining block rewards. Determining the accounting right by the size of stake can effectively avoid waste of resources, hence shortening the block generation time and transaction processing time.

The PoA stake identity while the Pos stake equity. For the CUN application scenario, small-scale nodes will be authorized to enter the network in the early stage of the network. Since there is no CUNP accumulation in the beginning, each node cannot quantify its holdings. Therefore, at this stage, the PoA consensus which stake identity is considered as the basis for the election of proposed nodes. When the network nodes grow to a certain size, they will be transformed into a PoS consensus, and all consensus nodes will conduct a PBFT consensus when the network upgrades to the main chain.

2.4.2 PBFT Consensus

In the third stage, CUN combines the Practical Byzantine Fault-Tolerant protocol with the blocker election consensus to form a hybrid consensus protocol. The hybrid consensus is divided into two main components: blocker election and main chain consensus. In the blocker election component, PoA is adopted in the early stage and PoS is adopted in the later stage, while the main chain consensus component will use PBFT consensus to improve performance.

The communication complexity of the currently widely used PBFT consensus protocol is O(n^2). The number of nodes in the later period will continue to increase, the consensus efficiency will drop by a quadratic level after the final node scale reaches 100 or more. In response to this problem, CUN will improve the PBFT consensus in the transition phase to enhance its scalability, security and performance. CUN intends to choose the following PBFT improvement measures:

(1) Hierarchical PBFT

The nodes in consensus network are divided into multiple levels according to its credit identity and holding CUNP equity. When proposing a block, a consensus will be firstly made within the sub-cluster to which the proposer belongs. After the consensus is passed, it will be signed using the multi-signature technology. The block is sent to the upper-level cluster for another consensus in the reply stage. After the upper-level cluster receives the proposed block, the signatures are verified and PBFT is chosen for consensus. The above process is looped until the

block reaches the top cluster and the verification is completed. In the end, the block will be broadcast to the nodes not participating in the verification for data synchronization and sharing. The schematic diagram of the hierarchical PBFT architecture is shown in Figure 2.

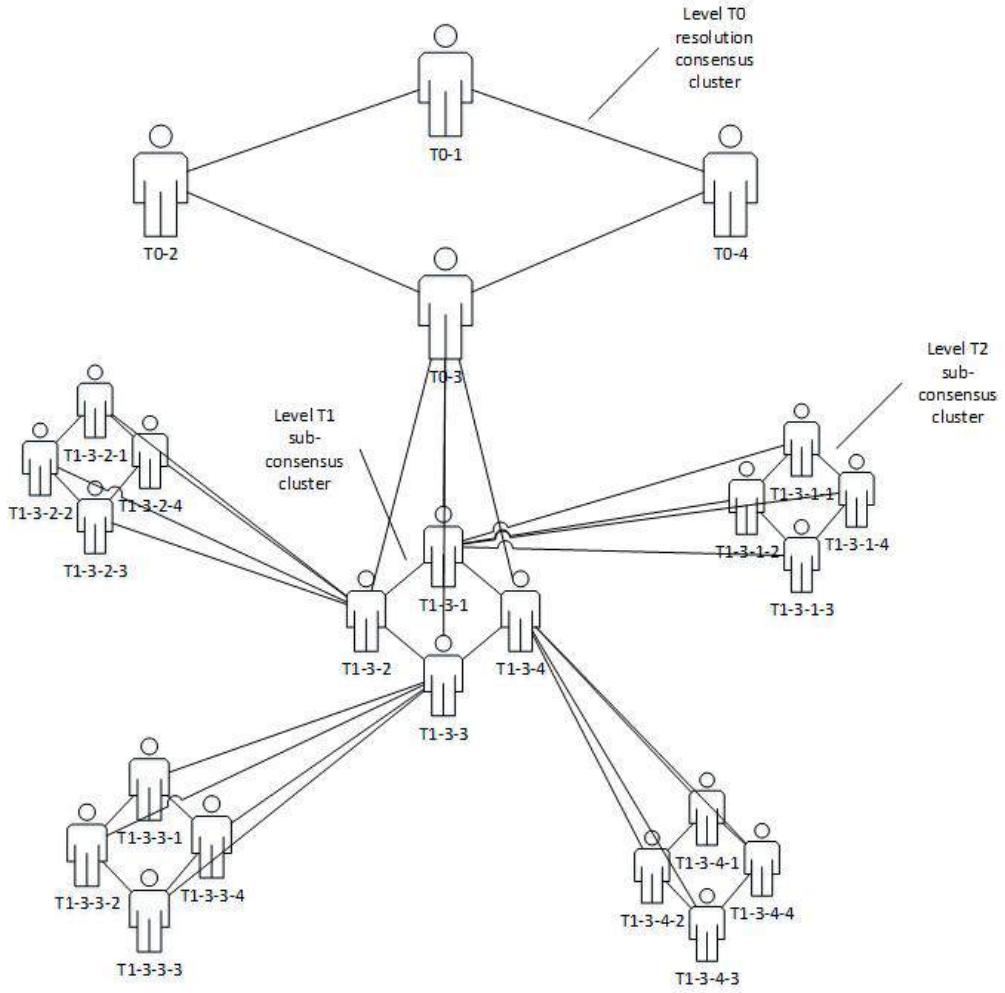

Figure 2. Hierarchical PBFT Architecture

According to the PBFT algorithm process, the master node in the pre-prepare stage will send pre-preparation messages to other nodes. At this time, the number of communication times is N-1. Then, after all nodes enter the prepare stage, all

nodes except the master node will send a ready message to other nodes except themselves. At this time, the number of communication times is $(N-1)^2$. When finally entering into the commit phase, each node needs to send a commit message to other nodes except themselves. At this time, the number of communication times is $N*(N-1)$. Therefore, the number of single consensus communication times in the traditional PBFT algorithm is shown in the following formula (1):

$$(N-1)+(N-1)^2+N*(N-1)=2N*(N-1) \quad (1)$$

The communication times of the second-layer and third-layer PBFT consensus processes are deduced according to the above derivation process. In the formula (1), if setting K to be the number of sub-cluster nodes, the communication time of the second-layer and third-layer PBFT can be deduced as shown in the following formulas (2), (3) :

$$2*(\frac{N}{K}\text{-}1)*(\frac{N}{K}\text{-}2)+2*\mathrm{K}*(\mathrm{K}-1)+\mathrm{K}*(\frac{N}{K}\text{-}1) \quad (2)$$

$$2*(\frac{\frac{N}{K}\text{-}1}{K}\text{-}1)*(\frac{\frac{N}{K}\text{-}1}{K}\text{-}2)+2*K*(K\text{-}1)+2\mathrm{K}*(\mathrm{K}-1)+\mathrm{K}*(\frac{N}{K}\text{-}1) \quad (3)$$

Through the above formulas (1), (2), (3), it can be concluded that when the number of sub-cluster nodes K=4 and the total number of nodes N=20, the number of PBFT communication time will reach 760 and the number of second-layer PBFT communication time is 64. When the number of nodes expands to N=84, the number of PBFT communication time will reach 13,944, while the number of third-layer PBFT communication time is only 152.

(2) Concurrency Mechanism

In the third stage, CUN will improve partial synchronization model of PBFT so that the PBFT consensus can be carried out concurrently in several stages such as view-change, block proposal, and main chain consensus. In a certain round of the main chain consensus process, the next round of block proposal or election voting process can be executed concurrently. When there is a problem of evil or failure of the master node during the consensus process, the view-change is triggered and the system will re-elect the master. In this process, other master nodes can perform concurrent block consensus that was not completed in the previous round, making full use of the fragmentation time to improve consensus efficiency and increase throughout capacity.

(3) Communication and Signature Optimization

As PBFT-type consensus involves a large amount of communication and broadcasting, the communication in a specific network will cause network congestion when the nodes reach a certain scale. So, in the third stage, CUN considers using communication protocols such as Gossip to optimize the consensus. Since there are multiple stages in the PBFT-type consensus and each stage requires different nodes to sign and send phased messages, a large number of signature verifications are involved in the consensus process. If signature algorithms such as elliptic curve encryption and RSA are used, the delay of multiple signature verifications will affect the overall consensus delay. However, the use of

multi-aggregated signature mechanism can aggregate multiple signatures into a short signature that the signature verification delay is unrelated to the number of signers and the space occupied by the block can be saved. At present, the use of BLS [4][5] and Schnorr [6] signatures to improve the consensus signature will have been incorporated into the proposed schemes of mainstream public chains such as Bitcoin and Ethereum, and both of them can resist the attack of rogue keys. CUN will consider the usage of high-efficiency multi-signatures such as BLS and Schnorr to improve the efficiency and security of signature verification, as well as realize the optimization of the signature part.

2.4.3 Phased Consensus

The adoption of a phased consensus mechanism by CUN is conducive to improve Pow. Phased consensus mechanism integrates the advantages of PoA, PoS, and hierarchical PBFT algorithms, and conforms to the concept and features of cooperation of CUN community.The consensus mechanism is mainly divided into three stages. The first stage adopts the access-designated PoA algorithm as the consensus mechanism during the initial operation of the public chain. The second stage uses the voting-access PoA algorithm and PoS algorithm as the consensus mechanisms during the transition period. The third stage selects the PoS algorithm and PBFT algorithm as the consensus mechanisms during the mature operation of the public chain. The specific model structure is shown in Figure 3.

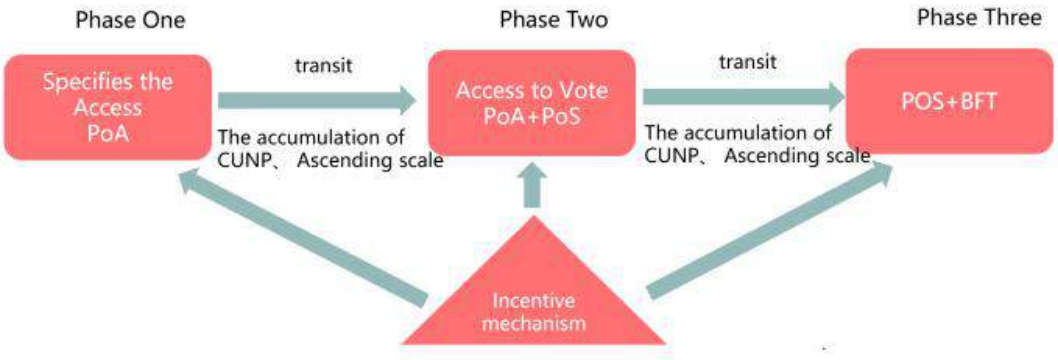

Figure 3. Phased Consensus

(1) The First Stage: Origin Network

At the launch, CUN "Origin" network is a Layer1 network with mainnet Coin, with PoA consensus as access mechanism to directly elect multiple trusted nodes to participate in the launch and maintenance of the network, forming a collection of nodes. These nodes need to stake a part of CUNPs, and block collection, packaging, consensus and verification are all performed by nodes in the set.

CUN evolves from Ethereum and the official network is launched after it has run stably on the test chain. In the first stage, CUN is of great network stability. In addition, since there are only 21 network nodes in the first stage, high consensus performance is also a pivotal feature of this stage.

(2) The Second Stage: Cape of Good Hope Network

When the network node scale and the CUNPs held by the community are accumulated to be eligible for stake voting, CUN will enter Cape of Good Hope

Network from Origin Network. The Cape of Good Hope Network is a transitional network to Next Generation Network, with PoA+PoS as the access mechanism. In the Cape of Good Hope stage, nodes that joined by PoA mechanism at the Origin Stage still need to stake a portion of CUNPs, to maintain the network and obtain incentives for network maintenance. One difference of the Cape of Good Hope network is the introduction of the PoS mechanism. At this stage, the nodes joined by the PoS mechanism are community nodes, they need to stake more CUNPs to have node election qualification. According to the number of votes obtained by candidate nodes, the top n nodes will enter the set of verification nodes, maintain the network together with PoA nodes, and benefit from network maintenance and staking. CUNPs engaged in voting will also benefit from staking. At this stage, a large number of community nodes will be added to the network, and more long-term participants in the CUN ecosystem will be added by the staking incentive mechanism. By combining the PoA+PoS consensus, while expanding decentralization, the stability and high performance of the network are guaranteed.

(3) The Third Stage: New Generation Network

When the network scale and CUNP distribution gradually stabilize, and the node scale and community scale further expand, CUN will enter the third stage. In this stage, PoS is used as the access consensus, and a random algorithm with equity as the weight is used to determine the block producer. In the consensus phase of

the main chain, an improved PBFT algorithm is used to achieve Practical Byzantine fault tolerance. At this stage, as the network scale is large enough and the PoS+PBFT consensus is adopted, CUN allows community users to jointly dominate the network. The most significant feature of the network is the high degree of decentralization, and is planned to be DAO-governed at this stage.

3.4.4 Incentive Mechanism

The blockchain system uses a specific economic incentive mechanism to ensure that all nodes in the decentralized system are motivated to participate in the generation and verification processes of data blocks. The consensus mechanism and incentive mechanism are an inseparable whole which are closely related and coupled. For the consistency of node ledgers, the consensus mechanism defines various node behaviors and stipulates the behavioral norms and sequence of actions that the nodes must comply with to maintain the security, consistency and vitality of blockchain ledgers. The incentive mechanism is deployed to encourage nodes to participate in the consensus, give active nodes certain rewards, give malicious nodes certain punishments, and encourage nodes to faithfully and efficiently verify the blockchain ledger data. They are coordinate with each other to guarantee the block quality.

Coopunion Network Point, abbreviated as CUNP, can be used to pay Gas on CUN, and is also the perpetual certificate that quantifies users' contributions , as well as the tool for community governance. Both maintenance of CUN and

contribution to the application on the chain can obtain CUNPs. 65% of the CUNPs will be mainly utilized to encourage the following two actions:

(1) Network maintenance: All the nodes participating in the network consensus can acquire incentives to increase the number of ordinary nodes and the enthusiasm for network maintenance, as well as scale up the network.

(2) Business contribution: Nodes or users participating in the business contribution will obtain CUNPs based on the value they have created and the cost they have invested in.

Following the design philosophy of the Network, the CUN system does not advocate the passive phenomena such as taking the lead in voting and the formation of mining pools.

In the second phase, a stake voting incentive is added, and the community votes to elect verification nodes. After the verification node produces the correct block, the community users who voted will receive part of the CUNP as reward.

2.5 Privacy Protection System

In the Internet era, countless data are generated, transmitted, stored and calculated on the network all the time. The principle of blockchain determines that all data stored on it are public, which is a significant challenge to ensure the data privacy. As a consequence, CUN takes the privacy protection system as the infrastructure of the whole network and provides it to developers in the form of

modules, not only making sure that the privacy data can be well-protected but also bringing developers higher work efficiency on CUN.

As shown in Figure 4, CUN privacy protection module can be divided into three submodules, including CUNHELib which provides homomorphic encryption function, CUNZKLib which provides zero-knowledge proof function, and CUNTEE which is a trusted execution environment module.

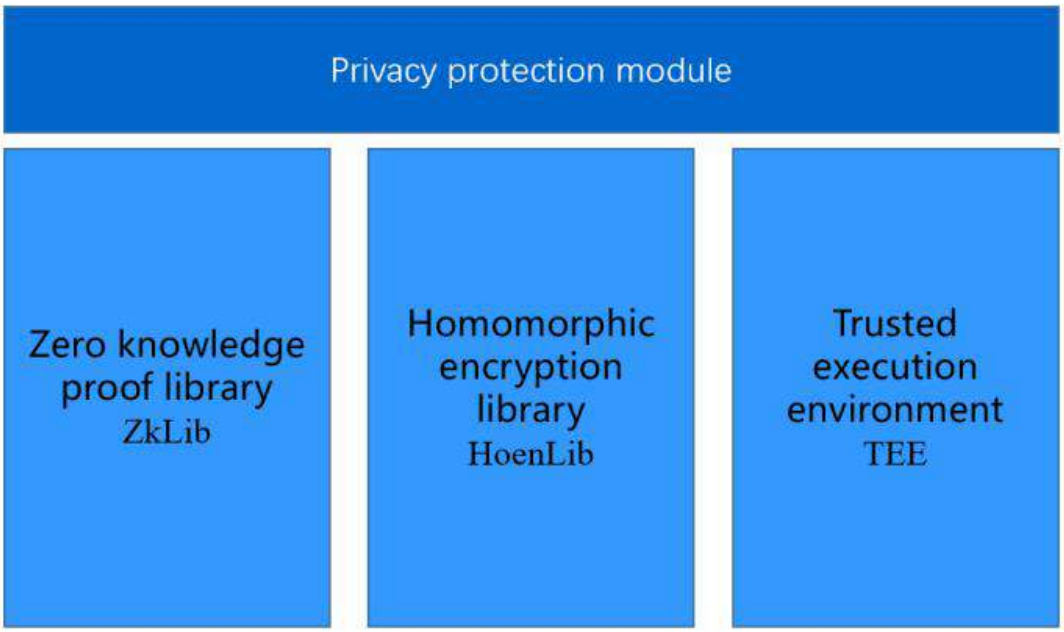

Figure 4 Privacy Protection Module

2.5.1 CUNHELib

There are numerous important and private data generated in our actual production and life which, in the past, could only be saved in the local database. The data separated from the Internet are obviously in great privacy, but the problem is that these data are often not static and need to participate in the

computation. It is difficult for the owners of these data to buy local computing equipment at a high cost. However, in contrast, blockchain network can provide huge computing power via connecting computing devices around the world in the form of P2P. So the cost can be greatly reduced if the private data is calculated on the blockchain network. But it is inevitable for the data to be shared in each node as a result of the distributed characteristic of blockchain, which is undoubtedly unacceptable. To address the contradiction between privacy and computability, CUNHELib is provided by CUN in the form of precompiled contract for all its developers. With just a certain consumption of Gas, developers are able to call these precompiled contracts[7] in their own solidity procedures.

CUNHELib is a homomorphic encryption library providing mainstream homomorphic encryption algorithms in the market. As a cryptology primitive[8], homomorphic encryption refers to a kind of cryptography technology based on the computational complexity theory of mathematical problems. Decrypting the output gotten from the processing of homomorphically encrypted data, the output result is the same as processing the original data which is unencrypted in the same way. In substance, homomorphic encryption refers to such an encryption function that the result of re-encrypting the additive and multiplicative operations on the plaintext is equivalent to that of performing corresponding operations on the ciphertext after encryption. Because of this, it is feasible for people to entrust a third party to process the data without information leakage. Encryption functions

with homomorphic properties refer to two encryption functions that plaintext a and b meet the formula of Dec(En(a) ⊙ En(b))=a ⊕ b, in which En is short for encryption operation, Dec is short for decryption operation, and ⊙、⊕ are corresponding to the operations on plaintext and ciphertext domains respectively. When ⊕ represents addition, it is called additive homomorphic encryption; when ⊕ represents multiplication, it is called multiplicative homomorphic encryption. Fully homomorphic encryption refers to the encryption function which can perform several additive and multiplicative operations arbitrarily if it satisfies both additive and multiplicative homomorphic properties, namely Dec(f(En(m1)，En(m2)，…，En(mk)))=f(m1，m2，…，mk) or f(En(m1)，En(m2)，…，En(mk))=En(f(m1，m2，…，mk)). In this formula, if f represents arbitrary function, it is called fully homomorphic encryption. Based on the precompiled contract, CUNHELib compiles the mainstream and efficient fully homomorphic encryption algorithms in the market into CUN in the form of underlying smart contract library. Among them, the general multiplicative and additive homomorphic encryption algorithms such as Paillier algorithm (additive homomorphism) and ElGamal algorithm (multiplicative homomorphism) are mature and efficient, enabling the on-chain privacy data to conduct a certain extent of operations without decryption. In addition, although the fully homomorphic algorithm with broader prospect is not mature currently[9], there are still many available function libraries, including the C++ library Helib (sub-BGV algorithm and integer domain) with IBM as the open source and C++

library SEAL (sub-BFV algorithm, integer domain, CKKS algorithm and floating-point number field) with Microsoft as the open source.

2.5.2 CUNZKLib

With the advancing of blockchain projects, it is found that trusted verification of data is required in many scenarios. The verification of plaintext data is simple since the data verification can be easily completed by setting reasonable verification protocols. Nevertheless, the key point is that the private data is likely to be leaked. For example, many mobile Apps now use SMS verification code, which will reveal the phone number of users and bring them plenty of spam messages and advertisements. It seems that there is no better solution and users are just forced to exchange privacy for trust. If we adopt this mode in a blockchain system, we will face a higher risk of privacy leakage because the blockchain is a multi-node, distributed P2P network. And the privacy of user information will be more difficult to guarantee on condition that users continue to upload plaintext to the blockchain network for verification. Therefore, we offer the CUNZKLib to help developers create blockchain applications[10] with functions such as privacy data verification.

CUNZKLib realizes and provides a variety of mainstream zero-knowledge proof algorithms. Zero-knowledge Proof, proposed by S.Goldwasser, S.Micali and C.Rackoff in the early 1980s, means that the certifier can make the verifier believe that a conclusion is correct without providing any useful information to him. It is essentially a protocol involving two or more parties, that is, a series of steps

demanded for two or more parties to complete a task. The certifier makes the verifier to believe that he knows or owns a message without leaking any information being proved to the verifier. Given that a lot of facts have proved the practicability of zero-knowledge proof in cryptography[11], it can be used for verification to solve many problems effectively.

2.5.3 CUNTEE

With the achievements of storing user information and assets, as well as handling operations such as payment, the functions of mobile devices are more powerful now. But whether it is a mobile device, traditional laptop or desktop computer, there are more or less security risks when running operation systems like Android, IOS, Linux and windows. For instance, bugs are often found, attacks always occur, and it is difficult to verify whether the OS has been tampered since it has access to all data of the application. All these situations may lead to the leakage of user privacy data, and even directly threaten the asset security of users.

CUNTEE module, the trusted execution environment (TEE) module of CUN, is established to help users to protect their privacy. TEE is an area on the CPU to provide a more secure space for the execution of data and code and ensure their confidentiality and integrity. CUNTEE builds a secure and private data computing environment for users. The end-to-end privacy protection offered by CUNTEE makes it possible for the user to be the only person qualified to view the data and computing results. Meanwhile, the trusted environment provided by CUNTEE

guarantees that the smart contract code cannot be tampered and is able to run in the way designated by the blockchain protocol, thus bringing the security to the whole blockchain network.

2.6 CDID System

CDID (Coopunion Decentralized Identity) system, building on the CUN main chain, is constructed for a secure and standardized management of users' personal identity information in the CUN ecosystem. Different from the early blockchain network which did not have the concept of account and used UTXO to record the balance, and the traditional centralized identity of which the privacy is easy to be leaked, decentralized digital identity can effectively protect the user privacy and meet the scenario needs of identity information. Users can register their own CDID after KYC (Know Your Customer) verification. CDID is unique and composed of two parts:

① CDID Identifier: the unique identifier representing user information, equivalent to users' on-chain ID.

② CDID Document: retrieved via CDID identifier. The content stored in CDID document is as below:

- Public key of users: used for application interaction among users or signature verification by organizations;

- Account types of users: institutional users and individual users have different

account types;

- Personal basic information of users: name, gender, contact information, etc.;

- Encrypted user assets: digital assets held by users;

- Account priority of users: the priority of account when handling businesses;

The overall architecture of CDID system is shown in Figure 5.

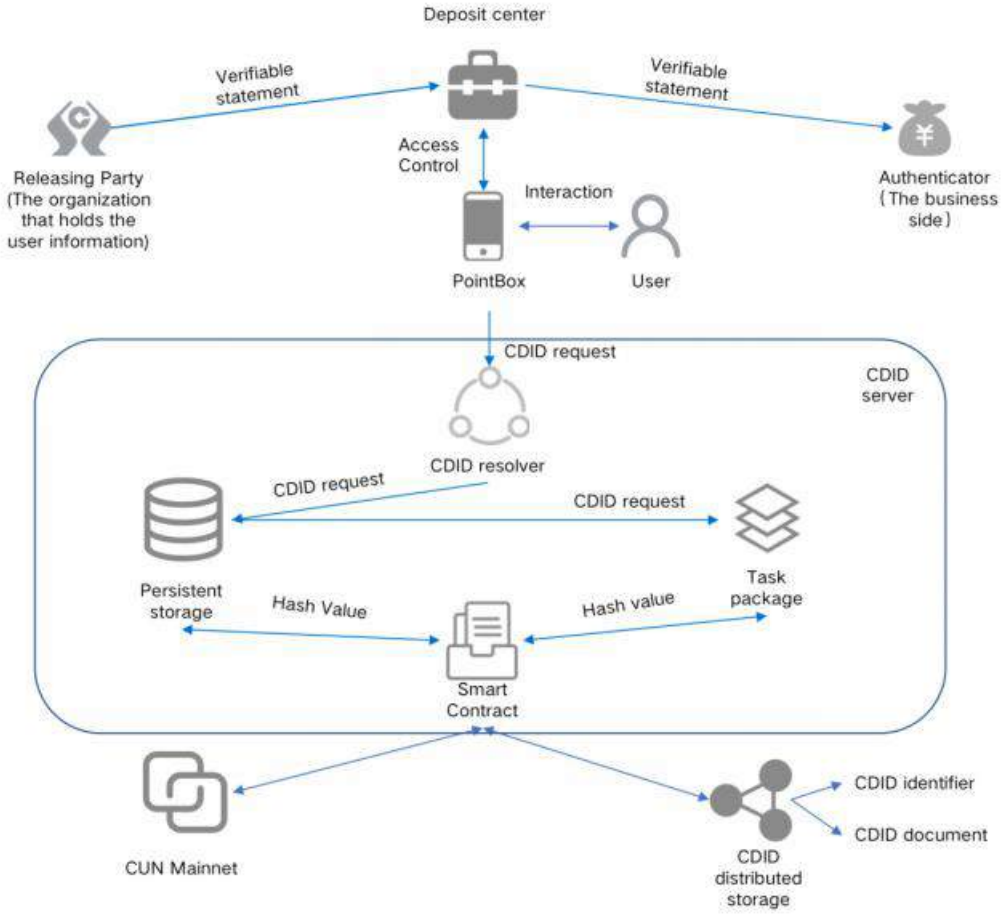

Figure 5. Overall Architecture of CDID System

2.6.1 CUN Decentralized Digital Identity (CDID)

To create CDID, individual users need to submit personal information through

PointBox for KYC verification while institutional users need to provide corresponding qualification documents issued by certifying authorities. After receiving the CDID creation request, CDID server sends the request to CDID parser. Once the request been verified and signed, it returns to the CDID server database. Subsequently, CDID packer interacts based on the smart contract deploying CDID server following the collection of CDID tasks for a period of time, writes the CDID information into distributed storage via smart contract, and writes the hash value of packed tasks into the mainchain of CUN to put it on chain. The CDID system can realize the highly concurrent CDID request-response under the condition of ensuring the security of user identity information without generating pressure to the main blockchain.

2.6.2 Verifiable Claim

The user CDID is in the general priority after the user’s submission of his basic identity information for signup. If the user wants to get higher priority and meet the requirements of some applications for user identity information, he can conduct the KYC verification of advanced personal information by the verifiable claim.

The data of credit, education, work, social activities, etc. are involved in the KYC verification of advanced personal information. The user can send an authentication request to the organization possessing his data such as a bank, school, enterprise or credit union. After receipt of the request, the organization will verify his identity

information, issue a verifiable claim to prove his identity, and send it to his ledger center. The user can also submit physical proof of the information in question and the corresponding verifiable statement will be stored in the ledger center after verification. In terms of the ledger center, it is a private storage space located in the server or PointBox that is completely controlled by users. Nobody else can view the verifiable claim in the ledger center without authorization.

When processing relevant businesses or using certain applications, the user can allow the business side to view his corresponding verifiable claim by visiting his ledger center via the QR code or authorization, hence increasing the priority of his CDID account to a higher degree and obtaining better services, such as more functions, fast handling channel from the business side or applications. Given that different business sides may have different KYC verification requirements, users can request different verifiable claims aiming at different personal information and reuse them without repeated application.

In addition to guarantee the security of user privacy, CDID verifiable claim can also perform KYC verification in high efficiency and flexibly applied to many practical business scenarios such as credit as well.

2.7 Cross-Chain Architecture

CUN executes the function of cross-chain asset exchange in PointBox to facilitate cross-chain transactions and increase information interaction with other

chains. This function will be implemented by using the cross-chain technology of Hash Time Lock Contract (HTLC). Hash time lock, a combination of hash lock and time lock, forces the recipient of the transaction to provide a proof of receipt that both parties agree within the specified time, and then the sender’s assets can be obtained. Otherwise, the assets will be returned to the sender’s account after the end of the specified time[12] . The proof of receipt usually needs to ensure that the receiver has paid a certain amount of work or that the sender can also obtain equivalent assets on its blockchain.

The condition for the hash time lock to achieve cross-chain asset exchange is that both parties can parse the data in the other's smart contract. Under this premise, the two parties of the transaction need to create a smart contract separately when they exchange assets. Each side's contract stipulates the conditions and time limits for the transaction, and the two parties will lock the assets they want to exchange. After completing a series of preparations, the sender will firstly send to the receiver the conditions of obtaining his assets , and then the receiver will send the receipt proof to the sender’s smart contract in accordance with the conditions agreed by both parties, and the receiver will verify the sending. After the certificate provided by the party is passed, it will automatically transfer its assets to the sender, and the receiver will also obtain equivalent assets from its contract based on the certificate provided by the sender. In this process, both parties can terminate the transaction at any time, but the party that proposes to

terminate the transaction needs to wait for the other party to confirm that the assets have been unlocked and returned to PointBox before unlocking the assets of the party. If the asset cannot be unlocked within a certain period of time after the proposed termination of the transaction, the transaction will be verified per the pre-agreement conditions in the contract between the two parties. If the transaction is legal, the assets of both parties will be automatically unlocked; if a fraudulent transaction is detected, the locked up assets of the fraudulent party will be paid to the other party as compensation.

For example, if Alice on the CUN chain and Bob on the Bitcoin chain want to make an asset exchange, both of them need to set up a hash time lock contract on the two chains at first and then perform the following steps:

1. Alice randomly generates a key R, calculates its hash value H = hash(R), and sends H to Bob.

2. Alice locks the 100 CUNPs she wants to exchange and sets a longer lock time t1 with the condition that whoever can provide the original value R of H within the specified time can get 100 CUNPs.

3. When observing that 100 CUNPs are locked in Alice's contract, Bob locks 2 BTCs and sets a shorter time t2 (t2<t1) in his contract with a same condition that whoever can get the original value of H within the specified time can get 2 BTCs.

4. After finding Bob's locked assets and the corresponding acquisition

condition, Alice sends the key R to Bob's contract. After the verification is passed, she can obtain 2 BTCs.

5. Bob gets the original value R of H from the contract he set up and sends it to Alice's contract. After the verification is passed, he can get 100 CUNPs.

When Alice and Bob both have received the corresponding assets, the transaction between the two parties is finished and the contracts set by them will automatically become invalid.

3.CUNP Value Model

The value of CUNP comes from the CUN network effect. By bringing together all the institutions and individuals around the world who wish to do business on blockchain via CUN, they voluntarily provide services and access services based on CUN, and form a global on-chain market matched by CUN.

CUN eco-services will be developed in parallel in the three stages of CUN evolution. In the early stage, the operation team will develop some CUN-based network applications to better support the eco-development. In the later stages,operation team will gradually focus on the network development and ecosystem construction.

CUNPs provide an important basis for distribution. On the one hand, CUN generates a limited amount of CUNPs on demand to award contributors. On the other hand, the applications operating on CUN network and profits generated assign value to CUNP. In theory, the value of CUNP will increase as the number of users, assets and trading volume on CUN increase.

3.1 CUNP Generation

In the first stage of CUN(Origin Network), the ecological participants of CUN include community supporters, CUN operation team, validating nodes, DAOs and blockchain technology believers. CUN will generate a certain number of CUNPs to

record the contributions of community supporters, validating nodes, operation team, as well as to motivate early users and application developers. For the long-term sustainable and stable development of CUN, the CUNPs generated in this stage is only of a minimum value in the total amount.

In the second stage of CUN(Cape of Good Hope Network), the network will generate a certain number of CUNPs to record the contributions of community supporters and validating nodes: to stimulate the network transition and due to the increase in the number of validating nodes, the amount of CUNPs generated for the validating nodes increases by 50%, as shown in formula (4).

After the network switching, a staking incentive pool is generated to encourage CUNP holders to participate in the network governance voting. If the number of CUNPs that have obtained governance right by staking is N, the CUNPs generated in the staking incentive pool will be N * 12%. These CUNPs will be transferred to stakers on a daily basis based on the proportion of staking quantity [as shown in formula (5)]. To stimulate the eco-system development, the CUNPs generated in this stage is ten times as much as the CUNPs of the Foundation. They will be automatically transferred to the dedicated address of the Foundation.

$$C_2 = C_1 * 150\% \qquad (4)$$

$C_1$and C_2 in formula (4) refer to the quantities of CUNP rewards available to the first-stage and second-stage validating nodes, and the 50% rise parameter can be

adjusted dynamically according to the actual situation.

$$C = N * 12\% * (a * p_1 + b * p_2) \quad (5)$$

In formula (5), *C* refers to the CUNP rewards that the staker can get in the incentive pool; *N* refers to the total amount of CUNPs having obtained the governance right by staking; *a* and *b* refer to the number of CUNP staking days and the proportion of CUNP staking in the incentive pool; p_1 and p_2 refer to the number days and the weight of staking proportion (which can be adjusted dynamically). The rewards received from the incentive pool are in direct proportion to the staking time and ratio of CUNP.

Theoretically, the number of staking incentive pool scales up with the increasing staking quantity of CUNP. More CUNPs can be acquired as a result of the relatively small number of early stakers. Subsequently, the proportion of staking incentive pool distributed to each CUNP is on the decrease with the increasing number of staking CUNPs. All the released CUNPs will participate in the staking in theory and the APY earnings will be stable at 12%. However, the incentive part generated by staking cannot be staked repeatedly within 90 days after being extracted so as to prevent the system stability from being destroyed owing to the obtainment of compound return.

In the third stage of CUN(New Generation Network), users will have accumulated a lot of CUNPs from participating in the early network governance,

the network upgraded to the improved consensus algorithm of PoS + PBFT, and the Mainnet accumulated a large number of users and become more decentralized with verified security. In addition to community supporters, CUN operation team, validating nodes, DAOs, blockchain technology believers, the participants of CUN ecosystem also contain many mature CUN network application providers, including but not limited to the asset generation, exchange and management based on CUN standard.

Most of the CUNPs will be generated in Cape of Good Hope Network and New Generation Network to record the contributions of relevant parties to CUN development: node maintenance contribution accounts for 45%, business contribution accounts for 20%, the Foundation accounts for 10%, community supporters account for 10%, and the CUN operation team accounts for 15%.

CUNP holders are entitled to participate and vote in the nodes election campaign by staking CUNP. The voting will be carried out according to the principle of "voting weight by person: voting weight by the number of holding CUNPs = 6:4" to weaken the influence of mine pool and ensure the decentralized nature of network， but each CUNP staked still is entitled to have the full right of yields. To ensure the stability of the CUN economic model and to avoid the exponential generation of CUNPs through repeated stakings of CUNPs, it will take 90 days before all additional CUNPs generated through staking can be withdrawn and circulated again.

After the listing on DEX, the CUNP incentives to CUN operation team will be generated and released linearly over 12 months; the CUNPs generated in the Foundation will be 1/10 of the number of CUNP in circulation, and will be automatically allocated to the dedicated address of the Foundation.

In conclusion, CUNP generation follows the on-demand principle, and the total quantity will stop to increase when it reaches 1 billion. The generation rules of CUNP take into account the contributions of operation team, nodes, governance, Foundation as well as the business contribution after the launch of Mainnet. CUN network encourages long-term behavior rather than short-term speculation until the application ecosystem becomes prosperous and all CUNP holders are greatly fed back. To stimulate the network upgrading, CUNP incentive parameters are taken into consideration every time when getting into the next stage.

In the CUN Origin Network , CUNPs are generated as shown in Figure 6.

Unit: point

CUN Contributors	Generated	Expected	Total2 (Contributors)	Total 2 in All
Nodes	110,000	449,890,000	450,000,000	45%
Business	10,000,000	190,000,000	200,000,000	20%
Eco-Fund	930,000	99,070,000	100,000,000	10%
Community Support	750,000	99,250,000	100,000,000	10%
Operation team	7,500,000	142,500,000	150,000,000	15%
Total1 (generated and expected)	19,290,000	980,710,000	1,000,000,000	100%

Figure 6. CUNP generation in Origin Network

3.2 Governance and Staking

The governance principle of CUN is to keep CUN in a healthy and steady development, make on-chain ecosystem play a valuable role to the digital economy, ensure that users can enjoy services provided by the CUN ecosystem, and all stakeholders can get due benefits according to the distribution principle of blockchain economy. Considering that the CUN consensus mechanism is divided into three stages of PoA, PoA+PoS and PoS+PBFT, the governance mechanisms are somewhat diverse in different stages.

In the three stages of CUN networking, as a necessary component of CUN governance, a certain number of CUNPs need to be staked for the validating node and can be released when it no longer serves as the node. The corresponding staking quantities are: 5000 in the first stage, 10000 in the second stage and more in the third stage (the staking quantity will be determined by community vote). Except for the first stage, corresponding staking will be rewarded with additional CUNPs.

Just like air and water, the Internet is open and equal to everyone as an infrastructure. CUN does not set restrictions on applications to avoid making irrational and unfair decisions due to personal likes and dislikes under a specific environment. Although validating node is the mainstay of network, it cannot stop anyone from entering the network. On the contrary, given that there may be some validator node problems, the validator mainly stakes his own identity in the first

and second stages of the network, putting the network operation under the supervision of all users. And then in the third stage, the validator will stake his own assets. When the validator cannot support the network operation, the system will deduct part of the staked CUNPs as a punishment.

4. Ecosystem Construction

In the CUN mainnet , CUN Foundation plays the roles of CUN treasury and eco-investor to gain investment profits and redistribute them.

In Origin Network and Cape of Good Hope Network , the Foundation is managed by the operation team. In New Generation Network, the treasury will be managed by DAO.

As CUN evolves, for a prosperous CUN ecosystem, the CUN Foundation will be mainly used to fund or incubate, among other things, the following:

① Developer funding or application development investments related to blockchain industry;

② Financial support for academic theory researches about blockchain technology;

③ Funding or investments in technological researches related to blockchain technology;

④ Commonweal donations;

⑤ Other matters resolved by the community

5.Risk Disclosure

Apart from those stated in the white paper, CUN operation team makes no statement or assurance (especially regarding the marketability and specific functions) to CUN or CUNP. Participants need to confirm that they will join in voluntarily and are ready to take risks, responsibilities and expenses before entering the CUN network and ecosystem. It is essential for users to be aware of and assess whether they have the ability and willingness to take the following risks:

① Information Disclosure

As of the release date of this white paper, CUN Cape of Good Hope Network and New Generation Network is still under development and technology reserves, with relevant development philosophy, consensus mechanism, algorithm, code and other technical details and parameters may be adjusted per the project progress. The information of CUN described in this white paper is crucial and the latest but not absolutely complete. Although CUN tries to better fulfill the obligation of information disclosure, it cannot guarantee that all information is transmitted to each user in real time.

② Policy Changes

Blockchain and digital assets are getting increasing attention in major countries and regions of the world under ever-improving compliance regulation.

Nevertheless, as an emerging industry, blockchain may still face policy changes in many countries. It is of great necessity to confirm local regulatory policies before entering the CUN network and ecosystem.

6.Terms and References

6.1 Terms

Coopunion Network（CUN)

Coopunion Network is a distributed network infrastructure that evolves from Ethereum. It aims to build a blockchain network and ecosystem with high-performance, high stabibilty and low cost, to improve users' experience, to reduce use cost, and to protect users' assets in digital world.

Coopunion Network Point（CUNP)

CUNP can be used to pay Gas on CUN, and is also the perpetual certificate that quantifies users' contributions , as well as the tool for community governance.

DAO

Distributed Autonomous Organization (DAO) is a form of blockchain-based organization structure that operate independently under open and fair rules, free from any intervention and management. These rules often appear in the form of open source software and anyone can become a participant in the organization by purchasing its equities or providing services.

PoA Consensus

Proof-of-Authority (PoA) is an improved algorithm based on proof-of-stake

which is capable of providing relatively fast transactions via the identity-based consensus mechanism for shares. The set of validator nodes is elected by identity staking. And then, the collection, packaging, validation and on-chain operation of blocks are all completed by the internal nodes of the set while other ordinary nodes are only responsible for the data synchronization.

PoS Consensus

Proof-of-Stake (PoS) is a consensus mechanism of stake. In this mechanism, the creator of the next block is decided by a combination of many factors such as random selection and the number of holding Token. The PoS mechanism can be used to solve the problem of massive resources waste in the Proof-of-Work.

PBFT Consensus

Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism for fault tolerance formation against the distributed BFT problem. In the specific blockchain network, PBFT consensus can allow the existence of PBFT nodes with different proportions.

Gossip Protocol

Gossip Protocol, the inspiration of which originates from plague, social network, etc., is a kind of communication protocol serving as a way to spread information. It is mainly applied for the data synchronization of each replica node in the distributed database system. One of the most important feature of this scenario is

that all nodes of the network are peer nodes and unstructured networks.

BLS Signature

An encrypted digital signature scheme for users to verify the authenticity of signers. The verification is realized by bilinear pairing and the signature is an element of elliptic curve group. The scheme possesses the functions of signature aggregation and multi-threshold signature.

Schnorr Signature

A digital signature based on discrete logarithm problem. Schnorr signature supports multiple signature and batch verification, as well as generates short signature by efficient aggregation. The verification speed of this digital signature is extremely high.

Homomorphic Encryption

Homomorphic encryption, a cryptography primitive, is a type of cryptography technology based on the computational complexity theory of mathematical problems. An output is acquired by processing the homomorphic encrypted data, and the result after decrypting the output is the same as that by processing the unencrypted original data with the same method. In essence, homomorphic encryption refers to such an encryption function: the result of re-encrypting the addition and multiplication operations on the plaintext is equivalent to that of conducting corresponding operations on ciphertext after encryption.

Fully Homomorphic Encryption

Fully homomorphic encryption, a cryptography primitive, is an encryption function which allows additive homomorphism and multiplicative homomorphism at the same time and can implement arbitrary multiple additive and multiplicative operations. In mathematical formula, that is, $\mathrm{Dec}\left(\mathrm{f}\left(\mathrm{Enc}(\mathrm{m}_1), \mathrm{Enc}(\mathrm{m}_2), \ldots, \mathrm{Enc}(\mathrm{m}_n)\right)\right) = \mathrm{f}(\mathrm{m}_1, \mathrm{m}_2, \ldots, \mathrm{m}_n)$, where f is an arbitrary function.

Zero-Knowledge Proof

Zero-knowledge proof, a cryptographic primitive meaning that a prover can interact with a verifier to make sure that an assertion is correct while the verifier knows nothing else about it. The definition of the so-called zero knowledge is that the verifier cannot get any additional information except the result of judgment (correct or incorrect).

Trusted Execution Environment (TEE)

Trusted execution environment (TEE) is a secure area in the main processor which runs in a separate environment parallel with the operating system. It ensures that the confidentiality and integrity of code and data loaded in TEE are well-preserved. By using both hardware and software to protect the data and code, the parallel system is more secure than the traditional system (namely REE, Rich Execution Environment). Trusted applications running in TEE are able to access all functions of the device's main processor and memory while hardware isolation

protects these components from the influence of user installed applications running in the main operating system. The software and encryption isolation in TEE can protect different trusted applications from each other.

Decentralized Digital Identity

An identity information based on the distributed technology that is stored in the forms of DID document and DID identifier. It protects the privacy of personal information and share information across institutions.

PointBox(Wallet for digital assets on Coopunion Network)

A visual application software for users' identity management, transactions and application participation.

Hash Time Lock

A cross-chain technology based on hash lock and time lock. It supports the atomic exchange of assets by users on different chains. The advantage of hash time lock is that it complete the exchange of cross-chain assets under the premise of mutual distrust.

6.2 References

[1] Hasan O, Brunie L, Bertino E. Privacy Preserving Reputation Systems based on Blockchain and other Cryptographic Building Blocks: A Survey[D]. University of Lyon; INSA-Lyon; CNRS-LIRIS-UMR5205, 2020.

[2] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19: 1.

[3] Castro M, Liskov B. Practical byzantine fault tolerance[C]//OSDI. 1999, 99(1999): 173-186.

[4] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[J]. Journal of cryptology, 2004, 17(4): 297-319.

[5] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2003: 416-432.

[6] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2001: 552-565.

[7] Tong Qinwei, Li Jie, Wang Jie, Hu Xinsen, Hu Kai. *A Fully Homomorphic Encryption Method Based on Smart Contract* [J].*Cyberspace Security*, 2020,11(09):32-38.

[8] Ananth P, Jain A, Jin Z, et al. Multikey FHE in the Plain Model[J]. IACR Cryptology EPrint Archive, 2020: 1–34.

[9] Gai K, Qiu M. An Optimal Fully Homomorphic Encryption Scheme[J]. Proceedings - 3rd IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2017, 3rd IEEE International Conference on High Performance and Smart Computing, HPSC 2017 and 2nd IEEE International Conference on Intelligent Data and Securit, 2017: 101–106. DOI:10.1109/BigDataSecurity.2017.43.

[10] Reitwiessner C. ZkSNARKs in a Nutshell[J/OL]. Ethereum Blog, 2016: 1–15. https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/.

[11] Bernhard D. Zero-Knowledge Proofs in Theory and Practice[J]. 2014.

[12] Joseph Poon, Thaddeus Dryja "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments"[OL]2016.
https://lightning.network/lightning-network-paper.pdf