Multiple-AC (MAC)
Technical White Papers

Blockchain Bottom Layer Technology
and Scenario Application Service Provider
World Multiple Atomic Research Centre
Foundation LTD.
September, 2018

Catalogue

I. Abstract 01

II. Introduction of MAC 03

2.1 Multiple Hybrid Consensus Mechanism and Cross-chain Atomic Operation 03

2.2 Development Background and Business Application Prospect of MAC 04

III. The Reason of Developing Multiple-AC (MAC) 07

3.1. Transaction performance 07

3.2. Broadcast communication 08

3.3. Information encryption and decryption 08

IV. Design Principals of MAC MAC 09

4.1. Transaction 09

4.2. Privacy 09

4.3. Supervision 10

V. Features of MAC 12

5.1 Cross-chain query and retrieva 12

5.2 High security 13

5.3 Strong commonality 13

5.4 Full interoperability 14

5.5 Advanced traceability technology model 14

5.6 Minimum threshold 14

5.7 Industrial development 15

5.8Industrial development 15

VI. MAC Innovation Implementation Plan 15

6.1 CHNN random sampling replaces traditional discrete consensus algorithm 15

6.1.1 Definition of CHNN and discrete data 15

6.1.2 Description of the dispersion tendency statistics 17

6.1.3 Inter-Quartile range 18

6.1.4 Average deviation 19

6.1.5 Square deviation and standard deviation 20

6.2 synchronous sorting technology transforms the consensus 22

6.2.1Implements RungeKutta asynchronous parallel algorith in Transputer-oeeAM environment 23

6.2.2 Efficiency analysis 24

6.3 Multi-language development programming 24

6.4 Implement of data migration 25

6.5 Neuron system simulation, Joint decision-making 26

VII. Development Process of the Consensus Mechanism 27

7.1 Blockchain Consensus Mechanism: POW, POS to DPOS 27

VIII. Application of NDPOS-based hybrid consensus in MAC 30

IX. Business Application Development of MAC 30

I. Abstract

Multiple Atomic Chain (MAC) is the third blockchain underlying ecosystem that being developed beside of Bitcoin and Ethereum. It is committed to expanding the application boundaries and technology boundaries of blockchain technology, thus to enable the common internet users to feel the value of blockchain technology, and let blockchain not be stuck in the academic theory level but more directly applied to the practice of application development. The development of MAC will be the spark of business application and blockchain technology collision, as well as a challenge to the existing blockchain technology. It jumps out of the conventional thinking of the existing technical field, and will be the pioneer of blockchain 3.0 application ecosystem.

In MAC system, P2P value transfer can be implemented through the Value Transfer Protocol; High concurrency performances, high throughput, fast and secure are the characteristics of MAC. So by applying the MAC underlying structure, a decentralized application development platform that supports multiple industries (finance, IOT, supply chain, social media, game, e-commerce, etc.) can be built.

In the MAC public blockchain system, the blockchain can be read by anyone in the world, transactions can be sent by anyone with valid confirmation, and anyone can participate in the consensus process (consensus process decides which block can be added to the blockchain and clarify the current state). As a substitute for centralized or quasi-centralized trust, the security of the public blockchain is combined with economic incentives and encrypted digital verification by means of “Cryptographic Digital Economy” with PoW or PoS mechanism; and follow the below general principle: The economic rewards that each person receives are in direct proportion to the contribution to the consensus process. These blockchains are often considered to be "completely decentralized."

In the MAC consortium blockchain, we will apply the Proof of Time consensus agreement which is integrated with Raft raised by the MAC developer; It will significantly shorten the time for realizing the consensus in consortium blockchain and private blockchain. In the MAC system, the blockchain Contract is divided into Smart Contract and Master Contract; besides the Smart Contract, via introduction of off-chain factors, we will establish the blockchain Master Contract that in line with the world business logic

In the MAC system, via the design of Oracle and Data Feed, plus improvements and optimizations on such basis, as well as realizing the diversification and rationalization of the smart contracts, we could make the blockchain more compliance with the needs on business level, and build the bridge from the real world to the blockchain world. In addition, in the MAC system, the ID information of the participants can be managed through Smart Contracts, which will provide better support for various industry services based on the MAC public chain system. Furthermore, the mobile-oriented strategy is also particularly valued by MAC. In the MAC ecosystem, we will work with third-party developers to provide mobile services which including: mobile wallet, mobile DAPP application and mobile intelligent contract service. We also encourage third-party developers to join the MAC Developer Eco-Community, to develop the mobile service of the blockchain together, and jointly promote the implementation of blockchain technology.

MAC has made a number of innovations, breaking the traditional consensus-level thinking, conducting in-depth research and mining from the core algorithm level, and creating independent IP technologies, such as “Asynchronous Sorting”, “CHNN-Consensus Mechanism”, “Neuron” and many other core breakthrough technologies of algorithm, which enable to achieve high-speed TPS and stable system concurrency performance. The MAC development team firmly believes that only good performance can transform the real implementation of blockchain technology from the theoretical stage to the application stage. The MAC team has been constantly pursuing performance in the development stage, and has created a high-performance and underlying public chain – MAC, which can realize multiple business application developments. MAC has reshaped the blockchain ecology and created a new era of blockchain 3.0 development and application.

II. Introduction of MAC

2.1 Multiple Hybrid Consensus Mechanism and Cross-chain Atomic Operation

MAC is a main chain developed based on Bitcoin and Ethereum system; using multi-chain consensus, multi-chain parallel, multiple hybrid consensus 【1】 and cross-chain atomic operation 【2】 to construct the cross-chain asset circulation highway; The consensus mechanism integrated the advantages of NDPOS, DPOS, POS, POW and PBFT; break the consensus mechanism via algorithm-inverse method and select the best through asynchronous sorting and discrete-to-continuous method. It is not necessary to connect with most nodes in the consensus process, nor to obtain voting, data transmission of the system can be cut down, dependence on the network of nodes can be reduced; nodes are randomly selected, using random computable functions, and the user knows whether it is selected according to the calculation, and feedback and broadcast results to other users. Multiple hybrid consensus mechanism amplifies the advantages from the consensus level and increases the speed of TPS. When our team was conducting research and development, we have found that it is limited to improve the TPS via traditional consensus level. The traditional consensus mechanisms, no matter it is POW/POS/DPOS/NDPOS or PBFT, after many calculations it is proved that single consensus mechanism can't achieve the breakthrough, so through the algorithm-inverse method and application of our exclusive technology [1] and [2] to break up the consensus and select the best part, and eventually realized the breakthrough of TPS speed. Some people say that the TPS can't be the only proposition of blockchain development, our MAC team firmly believes that blockchain as a technology must be implemented in practical applications, which includes a large number of commercial applications, and for a commercial application, no matter it is traceability or logistics tracking or payment, there are corresponding requirements for TPS. At least the TPS theory value should be above 5000, and the existing consensus mechanisms such as POW (TPS stays in single digits and can only used for mining), POS (can only do simple wallet and application development), and

even DPOS is NOT realistic to achieve TPS breakthroughs, because they cannot solve the concurrency problem at peak concurrency time, thus lead to the TPS fail to support at multi-user and multi-node situations. Even the TPS value that meets Turing-complete PBFT fault tolerance rate of 33% is far from being able to reach commercial level application, it is far from the traditional VISA TPS value.

In summary, the MAC team has jumped out of the traditional way of thinking blockchain. We broke through the traditional way of thinking consensus mechanism which is the consensus mechanism determines the TPS thus to determine the performance. MAC's breakthrough at the underlying has broken the traditional thinking. The algorithm is the core of breakthrough, and the consensus mechanism is used as corresponding cooperation, thus achieving significant effects and getting measured data of TPS. Therefore, the focus of MAC is on the core part of algorithm, at this level, we have done a lot of work and innovations, and have achieved remarkable results. After multiple calculations and authoritative super-computing center tests, our TPS value has exceeded tens of millions, which has profound influence to the development of traditional high-performance development platforms, no matter it is based on consensus mechanism or DAG. In the future, MAC will become a real commercial application chain, satisfying the physical application of finance/payment/e-commerce/trace source/logistics and many other industries; it will effectively implement the blockchain technology in various fields of the entity, and truly solves the VHT pain points that the existing decentralization cannot solve, and build a very easy and friendly world-class block chain infrastructure. At the same time, on MAC, users can access to the big user ecosystem of the blockchain world via the shared and unified multi-chain user system, transaction time, privacy protection, progressive node consensus, and improve the efficiency of trust, also in the concurrent response we have done a lot of breakthroughs.

2.2 Development Background and Business Application Prospect of MAC

Looking at the background and basis of MAC development - development from

nothing, the purpose of Internet is to reduce the cost of information transmission and improve the efficiency of collaboration. However, the cost of information transfer between organizations is still very high. The Internet has established a complete ecosystem and solved the zero cost information transmission problem, it enabled the information to be transmitted to every corner of the world in just one blink; later the world transitioned to the era of big data and cloud computing, of which the data is too centralized which lead to central control too powerful, thus increase the risk of collective data leakage; besides, all data have to go through the cloud, which is inefficient and costly. While the blockchain technology can achieve decentralized storage of data under the premise of ensuring that content is not falsified, and fundamentally solve the above problems. At this stage, trust is the issue. Almost all internet trades shall require a qualified third-party credit agency to handle the payment process. Such systems are still subject to a "credit-based model." Digital currencies that derived from the blockchain have overturned the situation of making payment through a third-party credit institute, it facilitates the direct payments, and third party is not needed. Since the blockchain is a distributed ledger, a technical solution for collectively maintaining a reliable database through decentralization and de-trusting. Blockchain is not a single technology, but the result of multiple technology integrations. These technologies are combined in new structures to create a new way of data recording, storage and presentation. Many nodes together form an end-to-end network. There is no centralized device and management organization. The nodes are verified by digital signatures, with no need of mutual trust. Then the nodes will record the data to the nodes of the entire network. It will never lose but always traceable. Since the nodes are trustless, there is no need to disclose the identity, so nodes are all anonymous.

The emergence of P2P value transmission networks has historical inevitability. From the development of TCP/IP protocol in the 1980s to the application of web browsers and server applications in the 1990s, Internet technology has changed the pattern of data exchange and human life from different aspects and dimensions. The development of Internet technology has benefited from the improvement of infrastructure. From the early information super highway and

the popularity of various smart terminals, these also constitute the basis for the infinite expansion of the application layer in the seven-layer model of the Internet OSI.

Among the various Internet protocol stacks, most commonly used protocols includes TCP/IP, HTTP, HTTPS, FTP, TELNET, SSH, SMTP, POP3 and etc. With these protocols we have built a variety of Internet services. But if think deeper, we will find that before this, we have been unable to properly implement the P2P value transfer and transmission without the help of third parties. In fact, we are not lacking a specific method, but lacking the Value Super Highway that based on the Information Super Highway and how to implement the Value Transfer Protocol (VTP protocol) of Value Super Highway. Blockchain is the first VTP protocol running on the Information Superhighway. With the development of interconnected technologies (Internet, Internet of Things, VR/AR), the interaction between people and objects, people and information is more diverse, and more entities are digitized (Digitalize) and tokenized and symbolized, once the entity is digitized or tokenized, the mapping and segmentation of physical assets on the Internet is completed. While one immediate problem occurs is: how to transmit these assets and values via P2P? Therefore, it can be speculated that as the Internet service deepens, the physical and virtual boundaries will begin to blur, and the demand for P2P value transfer will be highlighted. Therefore, the Value Super Highway and Value Transfer Protocol on the Internet will inevitably appear. Blockchain accelerates this historical process. The blockchain is active in a wide range of fields, including banking, auditing, internet of things, personal health, notary, social, shared economy, and copyright management. Take the personal medical health solution for example: service of reading the user's medical-related data after been personal authorized, using blockchain storage and asymmetric encryption technology, users can enjoy the featured functions of network-wide sharing, health data monitoring, etc. and provide quality basic data services for major hospitals, insurance and other institutions; and on the social aspect: Blockchain technology is used on social networks, which is a trusted peer-to-peer equal social platform that can be completely anonymous and protect strangers socializing;

In the area of shared economy: without the blockchain, the sharing economy is not shared enough. Used car transactions that based on the blockchain is using the VIN code as the unique ID of the car. The blockchain records all the information of the car from the factory till to the second transaction: such as repairing, maintenance and other information, which makes the used car information much more transparent. People choose blockchain-based digital currency for renting transactions, reducing the problem of information asymmetry caused by the centralized platform, as well as the transaction transparency issue. If what the Internet technology solves are communication problems, then blockchain technology solves the problem of trust, which can be widely applied to all areas where trust problems exist.

III. The reason of developing Multiple-AC (MAC)

Developers and users have witnessed the rapid development of blockchain technology. But the blockchain industry still faces many challenges from both the technical and industrial application perspectives. Many companies still have concerns about the application of blockchain, because there are still many problems for traditional blockchain technology to be applied to business applications. For blockchain to have breakthrough development in the future, combination of technology and application is inevitable. When our MAC team develops the multiple atomic chains, we could not find the underlying public chain that meets our requirements to dock with most of the business applications, so we believes that the real push of technology needs to be tested in reality, the performance is the most important part of it. Whether to stay at the theoretical level or the mining level or the performance level, it is a very important part, we can only meet the development needs of existing business applications by enhancing the real performance.

3.1 Transaction performance

the Bitcoin blockchain TPS is about 6.67 times / sec, each transaction requires 6 blocks to confirm, 10 minutes to generate one block, for the entire network to confirm one transaction takes 1 hour; although Ethereum of blockchain 2.0 have made some improvements, if looking from the TPS alone the changes are still not significant, Ethereum's TPS is about 21, such performances will make most application scenarios suffer. MAC has optimized the transaction performance, broadcast communication, information encryption and decryption, consensus mechanism, and transaction verification mechanism are the main factors that affecting the transaction performance of the blockchain.

3.2 Broadcast communication

Since one of the core technologies of the blockchain is the P2P network, the efficiency of P2P network communication is very important to the performance. First, in order to maximize the performance of the transaction, we adopted a variety of hybrid consensus mechanisms to ensure the optimization on the consensus level. At the same time, we broke through the traditional way of blockchain thinking and made a breakthrough in the core layer of the algorithm. Therefore, the nodes can be connected with high-speed network as much as possible, and the transaction performance of the blockchain can be greatly improved.

3.3 Information encryption and decryption

Information encryption and decryption are the key parts of the blockchain; mainly involve the hash function and the c encryption algorithms. The hash function currently mainly includes SHA family algorithm, MD5, SCRYPT, RIPEMD, WHIRLPOOL, CUCKOO HASH, HAVAL, Tiger, LYRA2, Equihash, Hashimoto, Dagger, Ethash (the algorithm of Ethereum's current Pow mechanism) etc. also there are series and parallel uses of the algorithm. Since commercial applications generally do not consider mining and pay more attention to performance, here we mainly use the commonly used SHA256 algorithm. The asymmetric encryption part mainly includes RSA, DSA, elliptic curve algorithm, etc. (the signature algorithm used by Bitcoin is ECDSA, and the verification speed of Schnorr signature is faster than that of ECDSA signature), and this signature volume can be Smaller, protogenous support multiple signatures.

IV. Design Principles of MAC

4.1 Transaction

From the perspective of the transaction verification mechanism, at present, our MAC does the following optimization methods:

A. Sharding, the general idea is that each node only processes a part of the transaction, such as a transaction initiated by some of the accounts, thereby reducing the computing and storage burden of the node.

B. Lightning Network and State Channels, these two strategies are to keep the underlying blockchain protocol unchanged, put the transaction out of the chain as much as possible, and solve the scalability issue by changing the protocol usage. Under this strategy, the distributed ledger only records the coarse-grained ledger, while the truly fine-grained bilateral or limited multilateral transaction details are not recorded as transactions on the distributed ledger.

C. MAC has designed a unique account blockchain and transaction blockchain. When a new bank is established or the original bank needs to be expanded, an account blockchain can be established to solve it; when the transaction volume is large, the system can increase the transaction blockchain to speed up the processing, and solve the scalability requirements through these two ways. Through the innovation of algorithm and the deployment of consortium chain, the performance such as throughput is greatly improved. The current delay can be controlled at the second level, the throughput is up to 10,000 per second, and the storage space requirement of a single node can be optimized and compressed accordingly, the performance bottlenecks have been broken.

4.2 Privacy:

In the public blockchain, each participant can get a complete data backup, all transaction data is open and transparent, this is the advantages of this type of blockchain, but on the other hand, this feature is fatal for many blockchain applications. Because in many occasions, not only users themselves want his account privacy and transaction information to be protected, also for the business institutes, the business accounts and transaction information are important assets and trade secrets for them, and they do not want to share them publicly. In order to solve the privacy protection problem of blockchain, we adopt homomorphic encryption and ring signature.

Homomorphic Encryption: Homomorphic Encryption is a method of performing computations without prior decryption of encrypted data. It provides a much-needed method of using blockchain technology on the original basis. By using homomorphic encryption to store data on the blockchain, a perfect balance can be achieved without any major changes to the blockchain attributes. In other words, the blockchain is still a public blockchain but the data on the blockchain will be encrypted, thus the privacy of the public blockchain is being taking care of; this enables the public blockchain to have the privacy effect of a private blockchain.

Ring Signature: A ring signature is a simplified group signature that gets its name because it consists of a rule that forms a ring. In the ring signature scheme, one member of the ring uses his own private key and other members public key to sign, but does not need the permission of other members, and the verifier only knows that the signature comes from this ring, but don’t know who is the real signer. Ring signatures solve the problem of full anonymity for signers, which allow a member to sign on behalf of a group of people without revealing the signer's information. In the darknet currency, its ring signature is a mixed coin service on the blockchain. Such mixed coin has the same amount of input and uses multiple other people's public keys, only knowing that it is sent from one of the groups. However, it is impossible to identify which one it is, and impossible to judge the input and output pairs by amount analysis.

4.3 Supervision

The transparency and decentralization characteristics of blockchain are difficult to be fully accepted by the government, supervisor and even at the transaction level. So how should the blockchain allow governments and supervisor to properly participate in the supervision without compromising the interests of commercial organizations and avoiding low efficiency? The general ledger can audit all or part of the general ledger entries in accordance with the prescribed

rules. In collaboration with the participants, the auditor can obtain a view of the general ledger through a time-based certificate and connect the transaction to provide the actual asset operations. The use of a hierarchy of keys can control the auditing authority that will be given to the auditor to check certain transactions, or a group of transactions, and only disclose the most relevant keys to the auditing entity to provide the possibility of control the auditing. Application auditors who are not members of the system can be given passive means of observing blockchain data while ensuring that they are only given transactions related to the audited application. In the accounting, management and synchronization processes of financial agreements between regulated financial institutions, the nodes responsible for supervision and observation operations have been designed, the supervisors are also on the ledger, the transaction information is verified by a specific transaction party, no need of a large group of verifiers that unrelated to the transaction. The supervision of the blockchain is to some extent promotes the commercial application of the blockchain to be better implemented and provide compliance protection, but over-supervision may also destroy the blockchain, it is necessary to grasp the scale. Meanwhile, supervising institutes should also follow the pace of innovation and conduct effective new forms of supervision in an open and inclusive manner. Comparing the development path of Internet technology, we find that both the blockchain technology itself and the application based on blockchain technology are in the early stage of industry development, and there are many directions worth exploring. Therefore, we hope to build a new blockchain ecosystem as an option for the future world's Internet value transfer protocol, and push the usability of the entire blockchain industry forward. This is the reason why we design the multiple atomic chains. MAC is dedicated to expanding the application boundaries and technology boundaries of blockchain technology, enabling ordinary Internet users to feel the value of blockchain technology and building a new ecosystem of developers and users based on blockchain technology.

V. Features of MAC

5.1 Cross-chain query and retrieval

Similar to the sharding mechanism of any distributed database, the sharding mechanism of NDPoS is based on the DHT mode, which is segmented according to the hash value of the partition key. In this mode, the precise query operation performance of the specified partition key is extremely high, and generally the data of the entire cluster can be evenly distributed for uniformly distributed partition keys. However, if the partitioning key is not included in the query criteria, the query must be broadcast to all shards to get eligible records in all partitions.

Therefore, the DHT sharding algorithm on which NDPoS is based must be optimized to meet the real-time efficiency of non-primary key query and retrieval. A simpler and more intuitive way, i.e. to introduce the concept of global indexing; In the field of distributed databases, the so-called global index is a secondary index, but the partitioning key of the index uses index keys instead of table partitioning keys. In this mode, the user can partition the index key field by using a hash partition or a range partition, enabling the querier to obtain records that match the query conditions while accessing only a limited number of partitions.

But one of the big drawbacks of this model is consistency. Since the partition key of the global index is different from the data table partition key, the index corresponding to a record is often not in one sharding. Therefore, the introduction of a strong consistent global index often brings a large amount of distributed transaction overhead; so generally speaking, it will not be adopted on large scale by traditional databases. However, for some scenarios that meet the final consistency, using a non-strong consistent global index can often yield unexpected effect. The core essence of NDPoS is to split the main data in the form of DHT sharding, but can establish a final consistent global index for other attributes that need to be retrieved. This mechanism needs to implement a database "table" and "index" and similar mechanisms for each account node, and store the data of different business attributes separately. NDPOS meets the

strong consistency data communication of quasi-real-time cross-sharding on the basis of DPoS. Unlike the eventual consistency of the unpredictable transaction confirmation time of the DAG structure, NDPOS provides strong consistency across inter-chain transactions through the peer-to-peer multi-activity mechanism. In the structure, the ledger in each chain is divided into two roles: the proxy node and the follower node. The proxy node is responsible for the consensus negotiation within a small scope, while the negotiation result informs the following node to perform accounting.

5.2 High security

Based on the symmetric and asymmetric double encryption algorithm in cryptography theory, it has integrated the irreversible quadruple encryption (Token + public key + private key + dynamic failure re-reconstruction) + unique core algorithm created by MAC team, and make the contract transmission, transaction and data more secure, and make the cracking become history.

5.3Consensus privacy is more protective

The MAC realizes the network chain + related node + subscription mode + smart screening storage, encrypted transmission of the private transaction to the node with decrypted private key, and the transaction hash is packed into the block. The private transaction data is only saved on the relevant node that has the decrypted private key. The relevant node decrypts and executes the transaction first, and the transaction data is not sent to unrelated node; the relevant party has the right to see the plaintext data, and other parties have no right to see the plaintext data but can verify the authenticity of the ciphertext data only. In addition, nodes that subscribe to the same channel can maintain and share the same ledger, forming a confidential communication link. Batch isolation between the ledgers has formed consensus channels for privacy, completely eliminating the possibility of information leakage. Compared with the privacy protection f Ethereum and EOS that basing on pseudo-name protection and without more extension, MAC's advantages are more than obvious.

5.4 Strong commonality

The analysis draws on the logic concepts of major public platforms, and the MAC tech team has independently developed the JSON synchronous + asynchronous data API interface calling method which can be used by the whole network. Multi-channel and multi-protocol to transmit the same data; cease transmission as soon as data received, ensure the accurate receipt and arrival of data.

5.5 Full interoperability

The MAC tech team has created a full interoperability communication protocol; authority DIY, one can develop its own internal peer-to-peer communication, linear communication between application packages, and application A internal and application B internal linear communication under the premise of following the MAC platform protocol, bridging communication via public chain. To achieve the diversity and flexibility of contracts, tokens and business processes.

Because of independent underlying structure, cross-chain transaction is simplified. For example: A is the store of the X platform, B is another store of the X platform, and C is a store of Y platform. To realize the transaction between A and B, it can be realized by the data circulation in the T-mall platform. If want to realize the transaction between A→C or B→C, you need X merchant platform and Y merchant platform to exchange data through API or other bridges. The data circulation process will be more complicated, and it need to be implemented through two platforms together. The transaction between A→B is realized inside MAC internally.

5.6Advanced traceability technology model

MAC focuses on the research and development of the traceability technology and the domestic closed-loop work, and has the original technology of plaintext + ciphertext + authority allocation compared with other underlying structures. It can intelligently judging if it is plaintext or ciphertext, full traceability and fact verification of the circulation process makes the application can be applied to more scenarios, and supports the DAPP customization mode.

5.7Minimum threshold

At present, blockchain technical talents are difficult to find, because most of them use small computer languages for development and face trans-disciplinary technical obstacles. MAC breaks the limitation of this industry. Application API development accepts all current computer languages for development, any ordinary programmers who are proficient in one certain language can quickly develop and implement applications on MAC.

5.8Industrial development

After the in-depth discussion of the adaptability of products and technologies between the hardware and software vendors, the MAC underlying platform products introduced by MAC tech team pays more attention to the mutual adaptation of databases, middleware and operating systems during the architecture development and deployment process. From chip, server, storage, network, to operating system, database, middleware and application layer have all been replaced, MAC has integrated all powers of the information technology to provide customers with a better one-stop blockchain application solution. Let the blockchain system be truly implemented, and become an accelerator to promote the transformation and upgrading of the global software industry.

VI. MAC Innovation Implementation Plan

6.1 CHNN random sampling replaces traditional discrete consensus algorithm

6.1.1 Definition of CHNN and discrete data

The continuous quantity is usually called the analog quantity, which is a continuous physical quantity in time and quantity. Like the mercury length in thermometer to indicate the temperature. Its feature is that the numerical value is represented by a continuous quantity, and its operation process is also continuous. A graph of the continuous quantity of temperature change is shown in Figure 1.

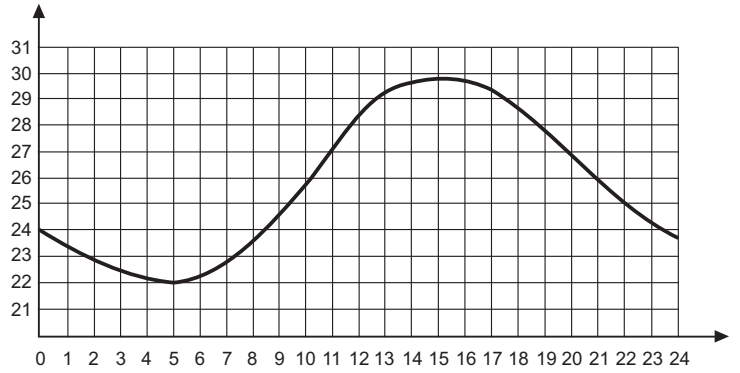

Figure 1 CHNN nodes distribution diagram

Discrete quantity, also known as digital quantity, is the physical quantity obtained by discretizing the analog quantity. That is, any instrumentation device cannot have a completely accurate representation of the analog quantity because they all have a sampling period in which the physical quantity values are constant, while the actual analog quantity is changed. . This discretizes the analog quantity and becomes a discrete quantity. If the value of the temperature is measured in each hour of one day, the temperature value at discrete time points within 24 hours is obtained, as shown in Figure 2.

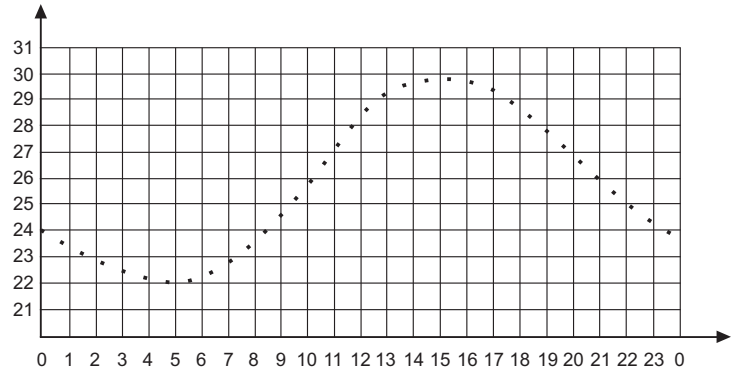

Figure 2 DHNN nodes distribution diagram.

6.1.2 Description of the dispersion tendency statistics

Although the concentrations can well describe the characteristics of a set of data, but using these statistics alone is not enough. It is also need to consider the dispersion of data. Sometimes, the average and median figure of the two sets of data may be identical, but there is a big difference between the two sets of data. Please see the following two sets of data:

Group A: 79 79 79 80 81 81 81

Group B: 50 60 70 80 90 100 100

The average and median figure of the two sets of data are both 80, but it is not easy to assume that the levels of the two groups of students are the same. There is obviously a difference between the A group data and the B group data. First, the data in Group A is relatively concentrated, and the value of each data is almost the same as the average of 80; while the data in Group B is relatively scattered and uneven, it reflects another important feature of data distribution - Variability. The statistic that describes the discrete trend of the data is called the measure of dispersion, or difference quantity.

Concentrations describe the typical case of a set of data, and measure of dispersion reflects the special case of the data. When studying the characteristics of a set of data, it is necessary to understand not only the typical situation, but also the special case. In the previous example, the concentration of Group A data and Group B data are the same, but the measure of dispersion is definitely different. We can only understand the difference between the two sets of data by understanding the concentration and measure of dispersion of these two sets of data. Commonly used statistical indicators that represent dispersion tendency in data are full-range, inter-quartile range, average deviation, square deviation, and standard deviation [3].

Full range is the simplest statistic that illustrates the degree of data dispersion. Arrange a set of data in ascending order, and subtract the lowest score from the highest score. The resulting value is the full range, that is, the range between the highest score and the lowest score. The full range of the above group A data is

81-79=2

the full range of the B group data is

100-50=50

Small full range value indicates that the distribution of data is relatively concentrated; Large full range value indicates that the distribution of data is relatively scattered. The advantage of full range is that the calculation method is simple and easy to understand. The disadvantage is that since it only takes into account the values at both ends, it does not take into account the difference in the intermediate values, and is not stable to describe the data.

6.1.3 Inter-Quartile range

The median can be used to represent a concentrated trend in the distribution of a set of data. The median just splits a set of data into two. If to divide the left and right sides of the median into another two parts, four equal quartiles are obtained. The value of the first quartile (i.e. 25% of the position) of this set of data is exactly one quarter of the data distribution, the median is exactly the value of the second quartile, and the third quartile value is just three-quarters of the data distribution of the group. Subtracting the value of the first quartile from third quartile, the resulting value is called the inter-quartile range (IQR), which is statistically used to represent the data discrete situation. As in the above group A data, the inter-quartile range is

As in the above group A data, the inter-quartile range is

81-79=2

the Inter-Quartile range of the B group data is

100-60=40

In addition to the inter-quartile range, there are statistically decile intervals and percentile interval, which are the same. After sorting the data from large to small or from small to large, the decile uses 9 points to divide all the data into ten equal parts, and the variables corresponding to the 9 point positions are called decibels, which are respectively recorded as

D1,D2,...D9

Data represent 10% falls to D1, Data represent 20% falls to D D2... data represent100% falls under D9. The range between the percentile and the range

between the deciles are the same. The data is divided into 100 equal parts. The corresponding variables at the 99 points are called Percentiles, which are recorded as P1, P2,... , P99, data represent 1% falls to P1... 99% falls to P99 [3].

6.1.4 Average deviation

Compared to the full range, the inter-quartile range is slightly better in expressing the discreteness of the data, but since it does not take all of the data into account, its stability will be worse. For example, we get two sets of data. The values of the two sets of data are not exactly the same, but the value of the resulting inter−quartile range may be exactly the same. This is the disadvantage to use the inter-quartile range to represent the data distribution. The ideal way is to take all the data into account to calculate the degree of distribution. The reason is simple: the average figure represents a concentrated trend of a set of data. We compare each of the data in a set of data with the average figure to know the extent to which each data deviates from the mean, or the difference from the mean. If you add up the difference between each of the data and the average figure of the set of data, then the difference in all data can be seen at a glance. Divide this value by the number of data, and the resulting value is called the average deviation. Its calculation formula is:

average deviation =

$$\frac{\sum \left| X - \overline{X} \right|}{N}$$

Among which

X

= value of each data

$\overline{X}$

= population average

N

= observed data amount

As can be seen from the above equation, the average deviation is the average of the absolute values of all raw data and mean value in the data distribution. The absolute value is used in order to avoid negative numbers. Since the average deviation is calculated from each observation value in the distribution, it better represents the degree of dispersion of the data distribution. However, since the calculation of the average deviation requires an absolute value, which is not conducive to further statistical analysis, the average deviation is not commonly used in statistical practice.

6.1.5 Square deviation and standard deviation

According to the above formula, if do not calculate the absolute mean value of the difference between each raw data and the mean value, but the square between them, there will be no negative numbers. Then add the value of the square of the difference between each raw data and the mean value, and get the sum of the squares of the difference between each raw data and the mean value

$$S = \sqrt{\sum \left(X - \overline{X} \right)^2}$$

Using this sum of squares and dividing by the number of data observed, the resulting value is called the square deviation. In equation,

$$S^2 = \frac{\sum \left(X - \overline{X} \right)^2}{N}$$

Since the value of the square deviation is relatively large, the standard deviation is generally used to represent the degree of dispersion of the data. The standard deviation is the square root of the square deviation and its equation is:

$$\sum \left(X - \overline{X} \right)^2$$

The concepts of standard deviation and square deviation are easy to understand. Both of them are actually a measure of difference: the square of the standard deviation is the square deviation, or the square root of the square deviation is

equal to the standard deviation, both of which reflect the distribution of a set of data around the mean value. The larger of the standard deviation value, the greater the degree of dispersion of the data, i.e., the more uneven the data, the wider the distribution; the smaller the standard deviation value, the smaller the dispersion of the data, i.e. the more the data are concentrated, in order, and the smaller the distribution range. When there is no difference in the data at all, all values are equal to the mean value, and the standard deviation or square deviation is equal to zero.

One thing to note is that in the above formula we use N as the divisor and the results are not very accurate. This is because, in general, the overall parameters are unknown, and only the sample statistic can be used as an estimated value, for example using the sample standard deviation (S) as the estimated value of the population standard deviation (σ) , it can be shown that when N is used as a divisor in the formula (especially when N is small), the resulting sample standard deviation as an estimated value of the population standard deviation is not accurate. When use

$$N-1$$

as the divisor and the results have no deviation. So the safer way is to use

$$N-1$$

as the divisor. When N is very big, use N or

$$N-1$$

as divisor would not have much difference.

Discrete-to-continuous: It is confirmed by the traditional discrete consensus algorithm, and upgraded to CHNN random sampling. Select only a portion of all nodes to get one result, via multi-round sampling to achieve full coverage. When the result of the random sampling converges to a trusted value, the consensus is reached. The synchronous consensus improves the operating efficiency of the asynchronous system, and it cooperates with the multi-node design of the asynchronous system to further improve the concurrency performance of the system.

It is not necessary to connect with most nodes in the consensus process, nor to obtain voting, data transmission of the system can be cut down, dependence on the network of nodes can be reduced; nodes are randomly selected, using random computable functions, and the user knows whether it is selected according to the calculation, and feedback and broadcast results to other users. Linear scalability, i.e. the performance is linearly accelerated as the node scale increases. The larger the node scale, the faster the convergence and the better the performance.

6.2 Asynchronous sorting technology transforms the consensus

The exclusive asynchronous sorting technology transforms the consensus into dealing with large-scale concurrent requests to asynchronous systems and the data sorting issues. The overall connectivity is better than the network, it can run as normal in a non-fully connected network environment, even in systems with a network connection ratio < 50%.

Multiple hidden layer networks, using a hidden layer network to approximate any continuous function. The framework replaces the single hidden layer by a deep network, and the result can be converged and normalized more quickly during the fitting process.

BPTT, multi-layer partitioning, fog algorithms, switching network topology structure between weak centralization and decentralization; Combination of super node and supervising node.

Asynchronous communication strategy in parallel processing technology, information communication between tasks usually adopts two strategies, asynchronous communication strategy and synchronous communication strategy, which leads to asynchronous parallel algorithm and synchronous parallel algorithm. The so-called synchronous parallel algorithm is in the process of execution of few tasks, there will be a task at waiting state in a certain, it can only be activated until another task completes a certain operation, but in the asynchronous parallel algorithm, there is no such phenomenon, the communication between tasks is Through global variables (shared data), unlike the dependencies between tasks in the synchronization algorithm, each task does not have to wait for input, but can continuously perform tasks and interrupt acquisition according to the information currently

obtained from global variables. So the asynchronous algorithm can bring the advantage of avoiding the synchronous communication overhead between tasks, thus improving the speedup ratio. However, the blockchain environment only supports the synchronous communication mechanism, and the two node processes (tasks) connected in the same channel can only communicate when they are at input/output ready state respectively, otherwise the process (task) that is already in the ready state (whether it is input or output process) will always at waiting for communication status.

Specifically, since the tasks assigned to the processors are always unbalanced, it may occur: 1 the task output phase delay too long to respond to the data input request of input phase; 2 task output phase requests to send data waiting for the task input phase response is too long, may lead to potential data lose.

Furthermore, due to communication waiting, the task cannot enter the next recursive operation. Therefore, it is very necessary / must to design a communication strategy to make Trasnputer-OCCAM multiprocessor system realize asynchronous communication data exchange, consider adding a OCCAM process (Commu-niCationprOCessing) to function as cache.

In the memory variable, the user enters the next recursive operation; ②when the task input phase requests data input, the data temporarily stored in the memory variable is assigned to the task; ③ when ① and ② occur simultaneously, transfer the stored data in memory variable 1 in the CP to the task, at the same time, store the newly sent data in the memory variable 2; ① when there is no request, the CP will not function.

6.2.1Implements RungeKutta asynchronous parallel algorith in Transputer-oeeAM environment

The RungeKutta asynchronous parallel algorithm is implemented in the Tarnspuertr-() ccAM environment. The Tarsnputer is a single-chip computer that integrates various functional blocks such as CPU, memory, and high-speed interconnect communication links. It has 4 pairs two-way communication links to be used for processing links between processors, so as to form a multiprocessor system of various topologies.

The OCCAM language is the programming language of the Tarsn-puter parallel

multiprocessor system. It can describe the parallel multiprocessor system structure constructed by Tarsnputer and write applications.

According to the foregoing task assignment principle and communication strategy, the Runge•Kutat asynchronous parallel algorithm model can be divided into several types of tasks, one to complete the recursive calculation and the other to act as a buffer. On the Tarnspiter multiprocessor, each of the task corresponds to an OCCAM process. Taking the third-order RungeKutat asynchronous parallel algorithm as an example, it can be divided into six concurrent execution tasks, three of which complete the recursive operation of the tier one, tier two and tier three approximation, and the other three (CPI:, CP2, CP3) are used to realize the process information communication, and the process of distribution and communication settings on the Tarnsputer network.

6.2.2Efficiency analysis

The efficiency analysis uses time series chart to represent the execution order of a process on the straddle. What being shown is the time series of each process executed by the third-order Runge Kutta asynchronous parallel algorithm.

6.3. Multi-language development programming

If you are a developer and want to implement a certain application scenario with a blockchain, you can use MAC to develop the application as follows: The following steps are performed on the MAC development platform:

(1) Register as a developer: Get the APP ID and KEY, which are two parameters that must be available for a MAC application.

(2) Parameter setting:

A. Asynchronous calls: Some other API functions can't be returned in real time. It takes a certain amount of time (a few seconds) to return the final result. If the waiting time is too long, the user experience will not good. We can set the API to return immediately without waiting for the result, which we call asynchronous calls (such as asynchronous mechanisms of Alipay, WeChat payment, etc.).

B. Set the callback URL: In the case of asynchronous call, it is necessary to set a callback URL. After the transaction is confirmed by MAC, the final

result of the API call will be notified to that URL (if the developer determines that no callback is required, then This step can be omitted). The URL specified by the developer needs to have program logic to process the result notification.

Set blockchain: The developer can set the default blockchain, and the API interface uses the default blockchain if no blockchain type was specified.

(3) Familiar with API, SDK: MAC will provide detailed API interface description and SDK source code. The developer is easy to develop blockchain applications by refer to the API and SDK. Developers can run the application directly, which greatly simplifying the entry process.

(4) Develop blockchain application: Developer selects the application scenario and develops its own blockchain application. The presentation interface can be a webpage, a desktop client, a mobile APP, etc.

6.4 Implement of data migration

Here is one scenario: A developer develops a blockchain application, manages 1000 users with B, and issues 10 assets. One day the developer wants to switch the application to E. The question is: What should be done with the user and asset data originally on B? MAC systems support the switching of heterogeneous blockchains. Developers can manually switch the default blockchain on the developer management platform and perform data migration.

Rules for data migration: For user and asset data, MAC will keep their final state; when switching to other blockchains, MAC will restore the final state of users and assets to the new blockchain, but do not restore historical transactions. The state restoration process includes operations such as registering a user on a new blockchain, and issuing the type and amount of assets owned by the user.

The time of data migration depends on the size of user and asset data. When migrating from the consortium chain or private chain to the public chain such as B and E, the transaction fee required for sending transaction is paid in cryptocurrency. The smart contract uploaded by the developer itself, as well as the custom data of the developer, cannot be migrated from the source blockchain to the target blockchain, because of the blockchain smart contract systems are different. However, MAC provides the ability to access multiple blockchains at the same time. Developers can deploy newly written smart contracts in the target blockchain, and then extract custom data from the smart contracts of the source blockchain and store them in the target blockchain, and then the data migration process is completed.

6.5 Neuron system simulation, Joint decision-making

Artificial Neural Networks (abbr. ANNs) is also referred to as neural networks (NNs) or connection models; it is an algorithmic mathematical model that simulates animal neural network behavior characteristics, and processing distributed parallel information. This network relies on the complexity of the system achieves the purpose of processing information by adjusting the interconnection between a large number of internal nodes.

Through modeling and interlinking of neuron-the basic unit of human brain, the neural network explores the model that simulating the function of the human brain nerve system, and to develop an AI system that has information processing capabilities of learning, association, memorizing and pattern recognition. An important feature of neural networks is that it can learn from the environment and store the results of learning in the synaptic connections of the network. The learning of neural network is a process. Under the excitation of its environment, it successively inputs some sample patterns to the network, and adjusts the weight matrix of each layer of the network according to certain rules (learning algorithm), and the learning process ends when the weights of each layer of the network are converged to a certain value. Then we can use the generated neural network to classify the real data.

MAC is the first one to combine the AI Neuron network neuron system to the main chain, rational decision-making, identify congestion to achieve balance, data value shared decision making. Numerous independent decision-making individuals form a conductive structure to simulate Neuron, and make decision jointly

VII. Development Process of the Consensus Mechanism

7.1Blockchain Consensus Mechanism: POW, POS to DPOS

In the blockchain system, there are many screening programs, such as PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegate Proof of Stake), PBFT (Practical Byzantine Fault Tolerance); starting from the PoW proposed by Satoshi, people have made deep thoughts and innovation on the data consistency problem of large-scale distributed peer-to-peer network nodes. Both PoW and PoS can be categorized to the scope of synchronous consensus algorithms. The original intention of PoW and PoS is to periodically elect a "lucky node" as the benchmark node of the log (ie, accounting) in all peer-to-peer network nodes through certain mechanisms, and the node will write the transactions recorded by itself to the log and send the file (ledger) to other nodes. This mechanism extends the Client-Server architecture of the traditional database to the multi-node peer-to-peer structure (multi-active), and the entire cluster can guarantee the strong consistency of the accounts written into the ledger and confirmed by multiple parties.

However, this mechanism faces many problems when the number of nodes in the cluster network increases significantly. For example, Bitcoin's average frequency of 1MB data blocks in ten minutes makes the overall throughput extremely limited; whether it is to increase the block size or shorten the block time, it will introduce more complex issues from multiple levels such as bandwidth or fork. Therefore, besides enhancing the clustering capability by using a series of additional measures, another typical idea is to improve the overall performance, throughput, and responding speed of the cluster by reducing the number of node that participate the consensus protocol. The DPoS is a typical architecture. It elects a certain number of proxy ledgers by voting between ledgers, and a consensus network is formed between these ledgers, while other unelected ledgers are synchronized with the proxy ledgers, thus to meet the reduction demand of consensus node participation. However, regardless of any form of consensus algorithm, the overall throughput of the

entire cluster is still limited by the network bandwidth between participating consensus nodes. For example, in a typical public network environment, the upload and download bandwidth between two common devices often reaches up to 5-10MB/s (100 Mbps bandwidth). Assuming each record is 100 bytes, the minimum network throughput of that the two nodes participate which physically limited is no more than 10MB/100/2=50,000/s (requires double data transmission due to the need to send the ledger and real-time transaction data). When the number of nodes participating in the consensus increases, assuming that the each ledger is averagely connected to 10 other ledgers through the P2P protocol, then the throughput is basically no more than 5,000/s. Thousands of transactions per second across the network may be sufficient for private chains or even consortium chains, but for a typical public chain it is far from the demand. Therefore, basically for any public chain project, the single-chain DPoS architecture cannot meet the future business expansion needs.

POW as a digital currency consensus mechanism was proposed in the B-money design in 1998. In 2008, Satoshi published a white paper on Bitcoin. Bitcoin applies the POW consensus, to guess a value (nonce) by calculation, and solve the specified hash problem (two times SHA256). It is guaranteed that only a few legitimate proposals will appear in the system for a period of time. At the same time, these small amounts of legitimate proposals will be broadcast on the network, and the users who receive the broadcast will verify and continue the calculation basing on the longest chain that it believes. So even there may appear Forks of the chain, but eventually there will be one chain that becomes the longest. POS – proof of stake, from Bitcoin to Ethereum. After all, the POW algorithm relies on the consumption of a large amount of resources to ensure the achievement of consensus. Is there a consensus mechanism that does not need to be secured by stacking of computer resources? In 2011, a digital currency enthusiast named Quantun Mechanic presented the Proof-of-Stake (POS) certification mechanism at the Bitcointalk Forum, which was fully discussed and proved to be feasible. If the POW is mainly competing the calculation power, then the POS is a competition of balance. Generally speaking, the more coins you have in your hand, the greater the probability of

digging into a block. However, there is a huge loophole in the POS consensus algorithm, which is the Nothing-at-Stake attack. Miners can mine at the same time on more than two branch chains, and can initiate a fork attack without holding 51% of the coin amount. DPOS proxy proof of stake, to against the low efficiency of POW, POS and the issue of become more and more centralized, BM's BitShares project launched in August 2013 adopted the DPOS consensus algorithm. BitShares is a typical representation of the DPOS consensus algorithm. DPOS is similar to the modern corporate board system. The BitShares system calls the token holders as shareholders, and the shareholders vote for 101 representatives, who then are responsible for generating the block. The core issues that need to be resolved are: how the representative is elected, and how to freely withdraw from the “board”. How to cooperate to generate blocks, etc. If the holder of the coin wants to be a representative, he needs to register his own public key to the blockchain to obtain an unique ID of 32 digits. The user can vote on the ID in the form of transaction. The top 101 users will be selected as representatives. Representatives take turns to generate blocks, and the income (transaction fee) is divided equally. If there is a representative is unproductive on block production, it is easy to be discovered by other representatives and shareholders, he will be kicked out of the "Board" immediately, and the vacant position will be automatically filled by the representative rank in 102. In a way, DPOS can be viewed as a multi-center system with both decentralization and centralization advantages. DPOS consensus, EOS elects 21 super nodes by voting. Each node has a 3 second time sharding and takes turns to record the account. If one node fails to generate block on its turn, that node may be voted out and replaced by another candidate node. The block generating speed is 0.5 seconds! In such case, the unlimited nodes and random block generating problems in the POW or other POS consensus are now changing to the issue of solving the Byzantine problem of fixed number and fixed block order only, of which the difficulty level is greatly reduced.

VIII. Application of NDPOS-based hybrid consensus in MAC

The core mechanism of NDPoS is to atomize operations between multiple chains, abstracting it with a logically higher-level chain, and using the DPoS algorithm in the high-level logical chain to guarantee the atomicity of operations between each member. The members in the high-level logical chain are also one or more proxy nodes in each partition chain. The node use the consensus reached in the high-level logical chain, and filters out the modified data contained in its own chain, and execute within the chain as an atomic operation to achieve the purpose of inter-chain atomic operations.

In the NDPoS structure, the ledgers in each chain are divided into two roles: the proxy node and the following node. The proxy node is responsible for the consensus negotiation within a small scope, and the negotiation result informs the following node to perform accounting. When there is a nested structure, the proxy nodes in the underlying chain are elected as ordinary accounting nodes in the upper virtual chain, and some of the nodes serve as the proxy nodes in the upper virtual chain to negotiate communication between the chains and work as consensus. Therefore, any one of the ledger nodes can have one or more states at the same time. It can be used as an independent following node, or as a proxy node of the underlying chain and a following node of the upper virtual chain, or as a proxy node of the underlying chain and a proxy node of the upper virtual chain. When there are three or more nested architectures in the network, each of the ledger nodes may have several roles at the same time. Taking a three-party transaction as an example, assume that there is a transfer transaction between X, Y, and Z records of three sharding chains, where record X is from sharding A; record Y is from sharding B; record Z is from sharding C. It can be seen that the sharding chain A, B, and C are completely independent, and there are one or more proxy nodes in the voting node of each sharding, forming a virtual chain between the sharding chains. All nodes in this virtual chain also use the DPoS mechanism for consensus. When there is a transaction that transfers from X to Y and Y to Z, the transaction is first initiated by the sharding in which X is

located. At this time, the accounting node receiving the transfer operation forwards the operation to the proxy node according to the DPoS rule for consensus. If the proxy node finds any record in the transaction as a cross-sharding operation, it will forward the operation to the proxy node in the upper virtual chain for cross- chain consensus. In the process of cross-chain consensus, the proxy node that initiates the sharding also forwards the transaction to the upper proxy node in the upper virtual chain according to the DPoS principle, and the upper proxy node first initiates the upper layer in the upper virtual chain. After the coordination nodes in the virtual chain reach a consensus, they will notify other following nodes (i.e. the common proxy nodes in the sharding chain) in the upper virtual chain according to the DPoS principle. Then, in each sharding chain, it broadcasts to its own following nodes according to the respective DPoS rules, and achieving cross-chain consensus. The core idea of NDPoS is to first reach a consensus in the top-level virtual chain and then communicate the results to the underlying sharding chain. When there are more than two layers of virtual chains, the pattern is passed down from the top layer in a recursive manner. When a business negotiation occurs, if the parties involved are all in the same department, all negotiations need only reach a consensus among the internal management of the department. If the two parties in need of negotiation are in different departments of the same business unit, all the negotiation need to be carried out between the management team of the business unit, and the results of the negotiation will be notified to the affected departments. If the negotiated parties are located between departments of different units of the branch company, the decision must be made by the branch management team, and then the respective units are notified, and the units informs the underlying departments to execute. The election strategy can be implemented according to the business characteristics of each project, but the core is to ensure that each of the underlying chains must have one or more proxy nodes as the nodes of the upper virtual chain to participate in the cross-chain consensus. Otherwise, the communication involving the underlying chain cannot be communicated to other following nodes in the chain.

Therefore, each time the upper-layer virtual chain consensus occurs, it must

first calculate whether there is at least one member in all the underlying chains involved in data block, and the initiator of the consensus must be approved by more than 2/3 members (take BPFT as example), and In all the underlying chains involved in the data block, after the consent agreement between the proxy nodes of each bottom chain is agreed upon, then the consensus can be considered successful.

In the NDPoS multi-layer architecture, the total general ledger supporting number and throughput volume can be infinitely elastically expanded as the number of layers increases. For example, suppose a typical single-chain DPoS maximum ledger support is 10,000, the number of proxy ledger is 101, and the single-chain design ideal throughput is 5000/s, then the two-layer structure can support about 10,000*(10,000/101)~= With 1,000,000 nodes, the theoretical ideal throughput is 5,000*(10000/101)~=500,000/s. The three-layer structure can reach 10,000*(10,000/101)^2~=1,000,000,000 nodes, and the theoretical ideal throughput is 5,000*(10000/101)^2~=500,000,000/s.Through the hierarchical nested DPOS mechanism, the infinite elastic expansion of the network sharding is realized, so that the follow-up elasticity of throughput is increased.

IX. Business Application Development of MAC

Decentralized commercial application (DBAPP)

Decentralized transaction platform and other decentralized application underlying development, using the underlying technology of MAC to develop the decentralized platform. The most important problem for decentralized applications is the performance problem. The high-performance MAC can solve this problem. High TPS can solve the needs of like finance, logistics and tracing industries, and truly realize business-grade applications, enable the blockchain truly enter the 3.0 era; MAC lets blockchain decentralization technology from technical theory level to practical application level; business application is the biggest assessment standard for technical performance. At present, we already have some application developers based on MAC, and we

will also access more in the future; starting from the all-ecological industrial chain, to build the underlying structure of the full industry chain. The current blockchain 2.0 era is stuck in the simple applications like issue TOKEN, develop wallets etc, which cannot truly dock with the application of the real economy, e. g. financial / logistics / tracing / e-commerce / payment / social / production lines and many other entities, the key reason is the business application is very important for the development of blockchain performance. MAC has such qualifications of business application development..

Quotes:

[1] Vitalik Buterin. Ethereum , April 2014. URL https://ethereum.org/.

[2]Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system

[3]Andrew Miller, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. Sprites: Payment channels thatgo faster than lightning.

[4]Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for c:Verifying program executions succinctly and in zero knowledge. In Advances in Cryptology–CRYPTO2013,Springer, 2013.

[5]Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments.2015

[6]Wang Tao, https://www.8btc.com/article/172587

[7]Christian Nagel Bill Evjen Jay Glynn.Professional C# 4.0 and .NET 4.

[8]GLOBAL ASSESSMENT CERTIFICATE.Mathematics II:Probability,