MOS

MOS

Public Chain Technology Whitepaper

New generation of Public Chain based on DAO 2.0 Distributed Autonomous Community Structure

Every consensus is a drving force

NOTICE AND DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "NOTICE AND DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER MOS FOUNDATION LTD. (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS (THE DEVELOPMENT TEAM) WHO HAVE WORKED ON THE MOS PUBLIC CHAIN (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE MOS PUBLIC CHAIN IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR/VENDOR OF MOS TOKENS (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE PROJECT WEBSITE (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

The Whitepaper and the Website are intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Foundation, the Distributor, and/or the Development team have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Foundation nor the Distributor is under any obligation to update or correct this document in connection therewith.

Nothing in the Whitepaper or the Website constitutes any offer by the Foundation, the Distributor or the Development team to sell any MOS token (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of the MOS Public Chain. The agreement between the Distributor and you, in relation to any sale and purchase of MOS token, is to be governed by only the separate terms and conditions of such agreement.

By accessing the Whitepaper or the Website (or any part thereof), you represent and warrant to the Foundation, the Distributor, its affiliates, and the Development team as follows:

(a) in any decision to purchase any MOS token, you have not relied on any statement set out in the Whitepaper or the Website;

(b) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that MOS token may have no value, there is no guarantee or representation of value or liquidity for MOS token, and MOS token is not for speculative investment;

(d) none of the Foundation, the Distributor, its affiliates, and/or the Development team members shall be responsible for or liable for the value of MOS token, the transferability and/or liquidity of MOS token and/or the availability of any market for MOS token through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to purchase any MOS token if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of MOS token would be construed as the sale of a security (howsoever named), financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, New Zealand, People's Republic of China (but not including the special administrative regions of Hong Kong and Macau, and the territory of Taiwan), Thailand, and the Socialist Republic of Vietnam).

All contributions will be applied towards the advancing, promoting the research, design and development of, and advocacy for the application of blockchain technology in the financial services industry. The Foundation, the Distributor and their various affiliates would develop, manage and operate the MOS Public Chain. The contributions in the token sale will be held by the Distributor (or its affiliate) after the token sale, and contributors will have no economic or legal right over or beneficial interest in these contributions or the assets of that entity after the token sale.

The Foundation, the Distributor and the Development team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of the Whitepaper or the Website, or any other materials published by the Foundation or the Distributor). To the maximum extent permitted by law, the Foundation, the Distributor, their affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of MOS token should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the MOS token sale, the Foundation, the Distributor and the Development team.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of MOS token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for sale and purchase of MOS token and/or continued holding of MOS token shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of MOS token (the Terms and Conditions), which shall be separately provided to you or made available on the Website. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and Conditions shall prevail.

No regulatory authority has examined or approved of any of the information set out in the Whitepaper or the Website. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation, the Distributor and/or the Development team, may constitute forward-looking statements (including statements regarding intent,

belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicted in the Whitepaper, and the Foundation, the Distributor as well as the Development team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

The Whitepaper and the Website may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.

1. Abstract

Since Satoshi Nakamoto published his paper “Bitcoin: A Peer to Peer Electronic Cash System” in November 2008, the crypto digital asset market represented by Bitcoin has emerged from scratch and has developed into a market with **a total market value of over 200 billion US dollars and daily trading volume of nearly 80 billion US dollars**. At the same time, with the rise of Blockchain technology, companies and organizations, including traditional IT suppliers, financial institutions and public sectors, are trying to find solutions based on distributed ledger technology (DLT) to upgrade existing products or services, especially in the application fields of supply chain, information management system, financial clearing, settlement and trusteeship services. **Blockchain technology has the potential to radically change the way financial transactions are structured and completed in both domestic and international business environments. It is the biggest change in the global financial sector in the past decade.**

In short, Blockchain is a growing list of records that are linked and protected using encryption techniques. Blockchain can be used as an open distributed ledger to effectively record transactions between two parties in a verifiable and permanent manner. Blockchain is usually managed by peer-to-peer networks (P2Ps) and adheres to the protocol for verifying new blocks (i.e., consensus protocol). Once recorded, no data in any given block can be retrospectively changed without changing all subsequent blocks, thus avoiding fraud, reducing trust costs, and realizing a series of potential applications. **Blockchain solves the problem of "too big to fall" and "centralization" in traditional finance and provides a basis for decentralized and distributed financial organization.**

As the famous Convey's Law reveals, "**The function of a system is ultimately limited to the form of organization that designs it.**" The development and application of Blockchain technology also requires its organizational structure to change from the traditional and centralized form of company system to an open and distributed organizational model. This led to the birth of DAO, namely "Distributed Autonomous Organization". In the autumn of 2013, Daniel Larimer (the founder of BitShares and EOS) put forward a concept similar to DAO in the book titled “Overpay for security”.

The community building Bitcoin and Ethereum is a typical DAO, that is, through a series of open and fair rules, it can operate independently without intervention and management. These rules often come in the form of open source software, and everyone can become a participant in the organization by purchasing stakes in the organization or providing services.

- **From the point of view of computer science, DAO is like a fully automated robot, when all its programming is completed, it will operate according to established rules.** It is worth mentioning that in the process of operation, it can also continuously self-maintain and upgrade according to the actual situation, through continuous self-improvement to adapt to its surrounding environment.
- **From an economic point of view, DAO is a self-organized and coordinated organization using economic incentives and self-execution criteria and operating around common goals.** Supported by the network effect, DAO provides an income model and incentive mechanism for open and shared resource production. With the integration of more open resources, DAO will be able to expand its scale indefinitely, while maintaining agility and consistency, avoiding dependence on the "center", thus surpassing the existing corporate structure in many dimensions.

In fact, DAO has a very wide range of forms. It may be a digital currency, a system or an institution, or even an auto-pilot car. They provide valuable services to customers. Such services can be currency transactions (such as Bitcoin), application development platforms (such as Ethereum), or any business model. Each DAO has its own terms and conditions. Each member will always have the right to view his/her own, disposable, digital currency form of DAO rights and interests, and it is possible to obtain the corresponding returns. At present, because of the advantages of traceability, anti-tampering and decentralization, Blockchain technology has been widely used in the management, trading, liquidity and other financial fields of digital assets, and has generated the need to establish DAOs for the financial field. However, when building DAOs for specific financial sectors, the following pain points begin to emerge, and innovative solutions are urgently needed:

- DAOs need community members to agree on important decisions with certain mechanism, the so-called "decision-making consensus". For example, Bitcoin community's discussion about "expansion" or Ethereum community's controversy about bifurcation after being attacked can be interpreted as a case of consensus in decision-making. **How to reach "decision-making consensus" efficiently and cheaply and reduce internal friction is the core organizational problem faced by DAO in the practice of financial field.** In the past corporate governance, this approach was often decided from the top down, but in distributed DAO, it is necessary to establish some rules that can be implemented uniformly and customized flexibly according to individual needs. At present, the DAO model needs to be strengthened and improved. The characteristics of these rules include:
    - Meeting the Individualized Needs of Different Interest Groups
    - Establishment of governance structures and rules of procedure
    - Conciliation of conflicting interests or opinions
    - Group decision making with universal constraints on members
- The development and growth of DAO depends on the active participation and contribution of members of the community, which stems from the recognition and reward for the contributions of members. In the past development history of Blockchain, there are many mechanisms such as PoW (Proof of Work), PoS (Proof of Stake) and DPoS (Delegated Proof of Stake) based on specific computer algorithms, namely the so-called "**algorithm consensus**". However, in view of the unique needs of various sub-sectors of the financial sector, including token financing, point-to-point mortgage lending, stable currency, decentralized derivatives market, large OTC collaboration and so on, the needs of participants in each business are different, and the requirements for incentive mechanisms are also different. Therefore, if only a single algorithm consensus is adopted in a DAO system, the participation of the whole industry will not be cohesive. In fact, many blockchain projects in the financial field fail to take account of the specific needs of members from different fields and different professional communities, thus limiting the scale of social expansion.
- The core idea of DAO is to "de-centralize", that is, to promote the development and growth of projects, services, systems and so on by the consensus of the members of the community. Only the real "de-centralization" can avoid the disadvantages of centralized management, including poor information communication, abuse of rights and so on. This is also the biggest difference between Blockchain technology, DAO and all traditional financial systems and systems. However, at present, in most DAO projects, including Ethereum, some individuals and institutions with specific "voice power" through organization, resources and computing power, control the dominance of the

whole project. The members of the general community can neither participate in decision-making equally nor enjoy the legitimate benefits brought by the development of the project. Such de-centralization, in fact, is "pseudo-de-centralization", which deviates from the fundamental principles of DAO.

In order to solve these long-standing pain points, MOS team combined the industry's top computer algorithm talents, Blockchain technology elites, Token Economy experts and software research and development gurus, gathered many years of rich experience in the financial field, and proposed a new financial chain based on DAO 2: **MOS Public Chain**. It has the following characteristics:

- In view of the shortcomings of DAO at present, a new **DAO 2.0** system is proposed in MOS Public Chain, which includes a set of procedural settings from organizational construction to voting mechanism and focuses on solving the problem of " decision-making consensus ". Starting from the distributed rules, it can innovate all the existing DAO modes and realize the real network of nodes, so that the flexible and stable operation of various distributed financial transactions can be ensured by removing the restrictions, and each member of the community can use various financial applications independently.
- In view of the common phenomenon of "pseudo-de-centralization", the MOS Public Chain innovatively applies VRF (i.e. Verifiable Random Function) to community management and construction, periodically chooses community leaders and committees by VRF, and completely transfers management power and autonomy to community control, so as to achieve a flat and transparent management mechanism.
- **PoFC** (Proof of Financial Contribution) is adopted as the consensus mechanism of algorithm. "Financial contribution" includes the combination of financial transaction resources (circulation) and community contribution (workload). It allows various applications in the Public Chain to adopt different weight allocation according to diverse needs, based on these two contributions' proportion in the general consensus mechanism. It is implemented into the Smart Contract to achieve a code-based **dual incentive system**. In addition, under the guidance of PoFC mechanism, the special incentives for technology developers in the community also conform to the design concept of endogenous economic growth model: technology progress is one of the important dimensions to promote overall economic growth.
- The MOS Public Chain refers to the "**endogenous economic growth model**" established by Paul Romer, the winner of the 2018 economic prize, and transplants the GDP estimation model of the general economic system to the DAO 2 organization, thus establishes a unified evaluation system for the value generated by the distributed organization. The endogenous economic growth model considers the important parameters such as savings rate, population growth rate and technology progress as endogenous variables, and the long-term economic growth rate can be determined by the interior of the model. Furthermore, the number of tokens, nodes and technology progression of distributed organizations are taken as similar parameters in the MOS Public Chain. Through certain transformation and analysis, the value of DAO can be quantified, and its long-term growth rate can be predicted.
- In response to the special needs of financing, lending, agency and derivatives in the financial field, the MOS Public Chain has developed a DAF (Decentralized Autonomous Finance) protocol group specially for eliminating various pain points in the financial field and developed corresponding MOSDAO DAPPs. These agreements include:
    - Token issuance and financing based on Smart Contracts

  - Distributed order submission and matching
  - Lending interest rate and mortgage method based on automatic discovery mechanism

Therefore, whether it is a member of the community, a project participant or a Blockchain project who develops applications on the MOS Public Chain, it can achieve the following objectives by means of the distributed rules, consensus mechanism, infrastructure and Smart Contracts it provides:

- Enhanced circulation of currency assets transactions based on community autonomy
- Issuance of new tokens
- Construction, collaboration, management, voting and decision-making of a specific crypto currency community
- Developing a Smart Contract system for the dual factors of community node rights and workload
- Self-defined incentive criteria for nodes with different rights and interests

This Whitepaper will give an in-depth introduction to the problems to be solved, the solution path to be adopted, the overall architecture design, technical innovation, team composition, development vision and roadmap of the MOS Public Chain.

The platform token used in the MOS Public Chain is called the MOS Token. For the operation, circulation and sales rules of the MOS Token, please refer to the "MOS Commercial Whitepaper" released same time as this Whitepaper.

2. Ideology of MOS Public Chain project

2.1 Development Status of Blockchain Technology: From 1.0 to 2.0

Blockchain is a new application mode of computer technologies in the Internet era, such as distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and so on. Blockchain technology is considered to be a subversive innovation of computing mode after the developments of mainframe, personal computer and Internet, and is bringing about a new technological innovation and industrial transformation all over the world. The United Nations, the International Monetary Fund, the United States, the European Union, Japan and many other developed countries have paid great attention to the development of the Blockchain and actively explored the application of it. At present, the application of Blockchain has extended to financial transactions, Internet of Things, intelligent manufacturing, supply chain management, digital assets and other fields.

Blockchain technology originated from the founding paper "Bitcoin: A Point-to-Point Electronic Cash System" published in 2008 by a scholar aliased as Satoshi Nakamoto. In a narrow sense, Blockchain is a kind of chained data structure, which combines data blocks in a sequential manner in accordance with the time order, and ensures it is a nontangible and unforgeable distributed ledger in a cryptographic manner. Broadly speaking, Blockchain technology is a new distributed infrastructure and computing paradigm. It uses Blockchain data structure to verify and store data, uses distributed node consensus algorithm to generate and update data, uses cryptography to ensure the security of data transmission and access, and uses Smart Contracts composed of automated script code to program and operate data.

At present, Blockchain technology is regarded by many large organizations as a major breakthrough technology to completely change the business and even the operation mode of the organization. At the same time, like the new generation of information technology such as cloud computing, big data, Internet of Things, Blockchain technology is not a single information technology, but relying on existing technology, and adding with innovative combinations, so as to achieve previously unrealized functions. So far, Blockchain technology has gone through three stages of development, as shown in Figure 1.

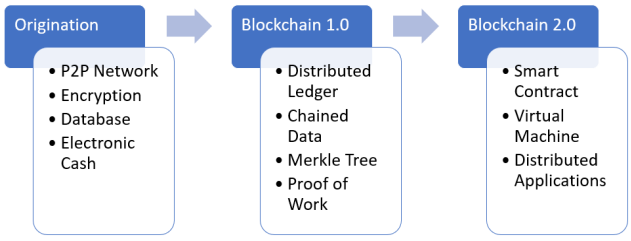


Fig. 1 Development Phases of Blockchain Technology

The core foundation of Blockchain 1.0 includes:

- P2P network technology is a networking technology in which a Blockchain system connects peer nodes. The academic community normally interprets it as a peer-to-peer network. In most media, it is called a "peer-to-peer" or "end-to-end" network. It is a kind of connection

network on the Internet. The left side of Figure 2 shows a P2P network mode, and the right side is a typical centralized network mode.

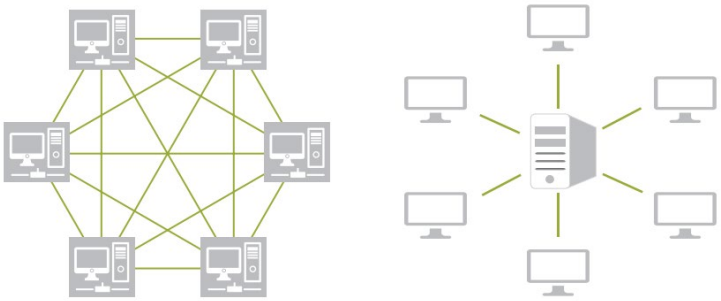


Fig. 2 Comparison of P2P networks and centralized networks

Different from the centralized network mode, the nodes in the P2P network have equal status, each node has the same network power, and there is no centralized server. All nodes share part of the computing resources, software or information content through a specific software protocol. Prior to the advent of Bitcoin, P2P network computing technology has been widely used to develop applications such as instant messaging software, file sharing, software downloading, network video playback, and computing resource sharing software.

- Asymmetric encryption algorithm refers to the use of public and private keys to encrypt and decrypt data storage and transmission. The public key can be publicly released for the sender to encrypt the information to be sent, and the private key is used by the receiver to decrypt the received encrypted content. The public-private key pair takes a long time to calculate and is mainly used to encrypt less data. Commonly used asymmetric encryption algorithms are RSA and ECC. The process of the asymmetric encryption algorithm is shown in Figure 3. Blockchain uses asymmetrically encrypted public-private key pairs to build trust between nodes.

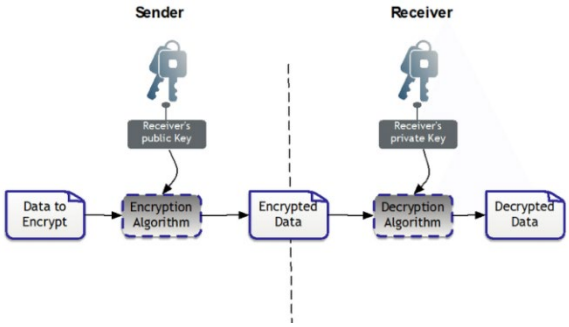


Fig. 3 Asymmetric encryption algorithm illustration

- Chained data structure in blocks: Each node of the Blockchain system selects a block node with packaged transaction authority through a certain consensus mechanism. The node needs to hash the previous block of the new block, the current timestamp, the valid transaction that occurred during a period of time, and the Merkel root value, then package them into a block and broadcast to the entire network. Since each block is linked with the previous block by cryptographic proof, when the Blockchain reaches a certain length, to modify the transaction content in a historical block, the transaction records and cryptographic proofs of all the blocks before the block must be reconstructed, thus effectively preventing tampering.

- Full network shared ledger: In a typical Blockchain network, each node can store a complete and consistent ledger of historical transaction records occurring on the entire network. This means, tampering and attacking of individual ledger data will not affect the security of the general ledger. In addition, since nodes on the entire network are connected in a point-to-point manner, there is no single centralized server, so there is no single attack portal. At the same time, the feature of sharing the ledger on the whole network also makes it possible to prevent double payment from becoming a reality.

The combination of the above technologies generates a typical implementation of the Blockchain 1.0, and its complete technical architecture is shown in Fig.4.

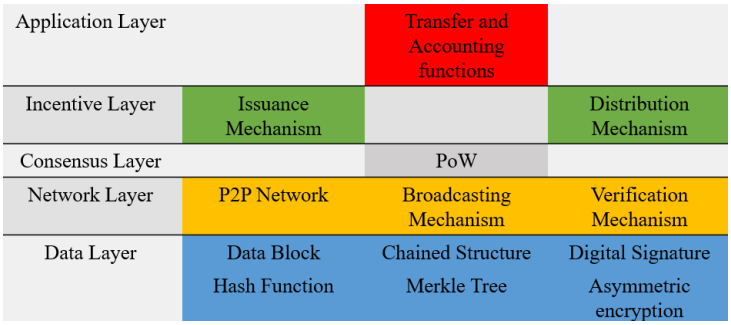


Fig. 4 Technical architecture of Blockchain 1.0

Around 2014, the industry began to recognize the value of Blockchain technology and use it in areas other than digital currencies, such as distributed identity authentication, distributed domain name systems, and distributed applications (DAPP). Building a DAPP from scratch with a Blockchain technology architecture is very difficult, but different DAPPs share many similar components. Blockchain 2.0 attempts to create a shareable technology platform and provides BaaS (Blockchain as a Service) services to developers, greatly improving transaction speed, reducing resource consumption, and supporting multiple consensus algorithms such as PoW, PoS and DPoS. To make DAPP development easier. Typical characteristics of Blockchain 2.0 are as follows:

- Smart Contracts: Applications in Blockchain systems are coded, automatable business logic that typically has its own token and proprietary development language.
- DAPP: Applications that include a user interface, including but not limited to various cryptocurrencies, such as Ethereum wallets.
- Virtual Machine: The code used to execute the compiled Smart Contract. The Ethereum virtual machine is Turing-complete and can perform self-consistent logic calculations.

Technical architecture of Blockchain 2.0 is shown as below:

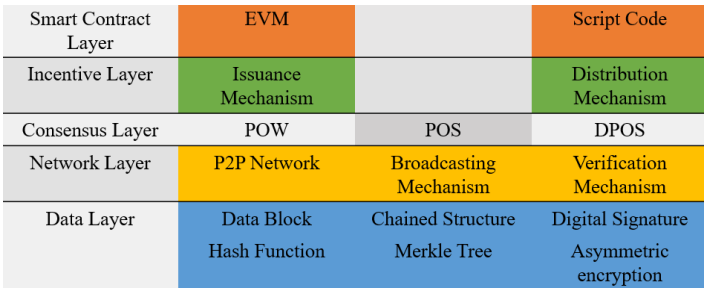


Fig. 5 Technical architecture of Blockchain 2.0

With the continuous progress of Blockchain technology and applications, the Blockchain 2.0 represented by Smart Contracts and DAPP will not only support the architecture system of various typical industry applications. Behind the various forms of organization, company, society, etc., people may be able to see the shadow of this distributed collaboration model of Blockchain. It can be said that the Blockchain will definitely change people's lifestyles extensively and profoundly. At present, the application of Blockchain has extended from a single digital currency application, such as Bitcoin, to various fields of economic society.

Considering the feasibility, maturity and importance of various industry applications, in addition to the relatively mature application of the financial services industry, the application of other industries is still in the initial stage of exploration. This project focuses on the application of Blockchain technology in the financial services industry.

2.2 Introduction to Distributed Autonomous Organization (DAO)

In 1967, American computer scientist Malvern Conway proposed the famous Convey's Law: "**The function of a system is ultimately limited by the form of organization that designs the system.**" That is, a system's design reflects the organizational form of each member in the ecosystem in which the system is developed. The way of communication and cooperation between the various nodes of the system also reflects the flow of information and cooperation between members.

Based on Conway's law, the following principles were derived for system design:

Communication between people is very complicated. One person's communication energy is limited, so when the problem is too complicated, and many people need to solve it, the management needs to split the organization to achieve the improvement of communication efficiency;

- The way people communicate with each other in the organization determines the system design in which they participate. Managers can bring diverse ways of communication between teams through different splitting methods, thus affecting system design;
- If the subsystem is cohesive, and the external communication boundary is clear, the communication cost can be reduced, and the corresponding design will be more reasonable and efficient;
- Complex systems need to be continuously optimized through fault-tolerant resiliency. Don't expect a large and comprehensive design or architecture. Good architecture and design are slowly iterative.

Fig. 6 Paper published on Conway Law in 1967

The development and application of Blockchain technology essentially has the characteristics of a distributed system, that is, a system in which all nodes are distributed on a networked computer, and nodes communicate between each other by transmitting messages. A node here can be roughly thought of as a piece of software, or a part of a software that can be run independently.

This distributed feature, in accordance with Conway's law, requires an organizational structure of its ecosystem, from a traditional, centralized corporate form, move to an open, distributed organizational model. This led to the birth of the Decentralized Autonomous Organization (DAO).

In the fall of 2013, Daniel Larimer (the founder of BitShares and EOS) first proposed a DAO-like concept in the article "Overpaying for security." Initially, its name was DAC, which means "Decentralized Autonomous Corporation". As the name implies, Daniel identified it as the organizational form of the enterprise, and the difference with traditional ones is “decentralized/distributed”. He pointed out that in the DAC, the crypto asset is the share, and the relevant regulations are determined by the source code. The purpose of the DAC is to make a profit for shareholders by providing valuable services to the free market.

In the same year, Daniel founded BitShares to implement his DAC concept, which is also considered to be the governance model of the subsequent Steemit and EOS projects, as well as the DAC concept. In 2014, Daniel further expanded the concept of DAC and identified its four core features:

- Must have interests available for trading (i.e. Token/Coins)
- Its value must not depend on an individual or company;
- The organization must be transparent and must not control any private keys;
- Do not rely on any legal contract, such as copyright and patents

During the same period, Vitalik Buterin explained his concept of DAC in his blog and Bitcoin Magazine, and inspired by Daniel Suarez's book “Daemon”, he created the vocabulary of DAO in the context of Blockchain.

Next, with Vitalik's release of Ethereum and Smart Contracts after 2015, DAO's programmability has been greatly improved, and the rules and values it can carry have also increased. After the DAO theft event in 2016, the security of DAO projects has gradually increased, and the number of hacker attacks has decreased. The attention of the Blockchain industry has shifted to how to implement DAO governance and how to provide DAOs with business value.

The community that builds Bitcoin and Ethereum is a typical DAO, a form of organization that can operate autonomously without intervention and management through a series of open and fair rules. These rules often come in the form of open source software, and everyone can become a participant in the organization by buying shares in the organization or providing services.

For this new form of organization, we can compare it to the traditional form of organization:

- Traditional organizations follow a top-down governance structure, while DAO is an autonomous, distributed network of various stakeholders, and any member can submit proposals and initiate improvements.
- Traditional organizations are a legal entity, while DAO does not have a centralized legal entity.
- Traditional organizations provide their employees with legal contracts that are enforced by humans, while DAO uses Smart Contracts as operational rules.
- The operation of traditional organizations requires a lot of maintenance and management, and most DAO rules and policies are set up at the beginning of the operation. Once the rules are established, DAO operations no longer need to be managed, achieving high efficiency and automation.
- The traditional organization's interest distribution mechanism and stakeholder information are centrally managed and controlled. In DAO, each member will have the right to view their own rights and interests at any time through the Blockchain, thus greatly improving the transparency of the entire organization.

As the name implies, the core features of DAO are:

- **Autonomy**

The basic characteristic of DAO is that DAO is programmed to execute specific operational rules, which means that when the conditions specified in the program are met, DAO will automatically perform the corresponding operations. In traditional organizations, someone must specifically explain and guide specific rules. Suppose that in real life, members of an organization want to allocate funds to various projects through expert committees. For traditional organizations, once the expert committee gives advice, the executor must go through many steps to release the funds. For DAO, funds are transferred as soon as the committee approves. Neither internal stakeholders nor banks can stop it.

In order to fully automate the DAO's operating rules and the safe and efficient execution of operations, DAOs must be run on a public, permissionless Blockchain, such as Ethereum.

There are two main reasons for this:

1) Traditional software platforms cannot process funds directly. They can only send orders to financial institutions responsible for transferring funds. By using a common Blockchain, DAO can place cryptocurrencies or other digital assets under the direct and unique control of Smart Contracts, and DAO can express the organization and its specific operational rules in software code.

2) Traditional software relies on third-party infrastructure. If the software platform runs on the cloud service platform, the specific expression of the operation rules depends on the cloud server. The cloud server is prone to interruptions, errors, or external factors that prevent the software from running properly. The public Blockchain never has these problems.

In short, DAO is autonomous because DAO is self-executing according to the rules, no one can stop it, and no one can change it from the outside.

- **Decentralization**

Decentralization can be understood from two levels, and it can also explain the relationship between “decentralization” and “autonomy”.

DAO is decentralized because it runs on a decentralized, permissionless Blockchain. Blockchain expert Yalda Mousavinia defines DAO as: "Organizations that operate under the rules of digital rules." Similarly, Tim Bansemer pointed out: "DAO is essentially a combination of Smart Contracts that run on permissionless Blockchains (such as Ethereum)."

DAO is decentralized because it is not organized around the ranks of executives or shareholders like traditional companies. The execution of DAO's power is carried out collectively. Based on the non-affiliated cooperation mechanism, the power structure is “distributed”. Compared to the traditional, rigid hierarchical structure, DAO's innovation is that it can coordinate many people and can be scattered around the world. This feature makes DAO fundamentally different from traditional organizations.

Basically, all DAO projects are built around these two layers. Aragon's positioning is mainly on the first layer, emphasizing "fighting for freedom." Tim Bessemer is defined as “the future of cooperation” and perfectly expresses the meaning of the second layer.

If the essential feature of DAO is to avoid the power being seized by a third party, these two layers are complementary.

- **Organization**

The first DAO project was “The DAO”, created in 2016 to fund projects that benefit Ethereum. The idea of using DAO instead of foundation or venture capital is in line with the decentralized spirit that the Ethereum community cherishes. In fact, The DAO is a fund whose decisions are made directly by individual community users rather than being delegated to a specific manager.

The concept of DAO was proposed by Dan Larimer (founder of EOS) in 2013. He coined the term “DAC” – a decentralized autonomous company. Dan Larimer likens Bitcoin to a company whose shareholders are Bitcoin holders and whose employees are miners. In the same year, Vitalik Buterin asked a question: How does a company operate without a manager? This summarizes the concept of DAO. Business automation is often seen by the public as the process of replacing low-skilled people with robots or computers and allowing more qualified employees to manage. However, Vitalik made the opposite suggestion of replacing management with a software technology that recruits people and pays salaries to drive tasks that help the company's mission. “DAO” clearly indicates something broader than the typical definition of “organization” “a social group that brings people together and works towards a common goal.” Therefore, Vitalik defines DAO as “an independent existence attached in the network, but also heavily rely on hiring individuals to perform certain tasks that DAO itself cannot do."

In summary, DAO has become an organizational form between industry and enterprise under the joint action of consensus mechanism and distributed network. On the one hand, it realizes the efficient allocation of capital in a distributed network and solves the problem of information asymmetry. On the other hand, the establishment of a credit system that transcends simple acquaintances through a consensus mechanism can form a new economic model that is based on shared economy, thus breaking a series of restrictions on the relationship between enterprises and markets in the neoclassical economy, creating a new organizational structure.

2.3 The development direction of the distributed autonomous organization Public Chain

Since the attack on The DAO based on Ethereum in 2016, DAO has gradually moved away from people's attention. However, the development and testing of DAO has never stopped. By 2019, with the

further improvement of related technologies and theories, the development of DAO began to re-emerge. For example:

1. Aragon, DAOstack and Colony have already supported the creation of DAO contracts on the main network.
2. Projects such as KyberDAO (Kyber Network), PolkaDAO (Polkadot) and dxDAO (Gnosis) have been trying to use DAO for protocol governance.
3. DAO projects such as Kleros and Aragon Court can provide decentralized arbitration services. In the real world, Vermont, Malta, and the United Kingdom have issued corresponding licenses for the creation of jurisdictions for DAO.
4. The UK-based Nexus Mutual is the first DAO-driven decentralized mutual insurance company to issue insurance-backed policies designed to cover other types of risks typically covered by traditional insurers.
5. In France, La Suite du Monde plans to use DAO to manage its funding and project plans. Very different from other projects, the project was established to provide land, financial and legal support to the "community" on the premise of the collapse of the current industrial civilization. These "communities" are local, self-recovering, independent, self-organizing cooperatives.

All in all, from Prague to Curaçao, from Athens to New York, new DAO projects can be found everywhere. These projects are highly discoverative and experimental, more decentralized, in order to create a more equitable system. The goals and operations of these projects are very diverse, which also illustrates the breadth of DAO's future applications.

The biggest difference between DAO and traditional organizations is its support for automated rules based on Smart Contracts. Currently, the most common Smart Contracts are various cryptocurrency contracts, which means that developers can easily deploy and distribute new crypto tokens running on Ethereum or other Public Chains by deploying a Smart Contract. If the Smart Contract is compatible with the ERC20 standard, the developer does not need to re-develop the entire token ecosystem from mining to trading. The new encryption token can be directly used to support Ethereum's e-wallet, greatly reducing the threshold bar for establishment of new encrypting tokens.

Smart Contracts can also be used to operate a variety of open and fair automated service agencies. Through Smart Contracts that operate across multiple nodes around the world, all operations and decisions are open and transparent, reducing transaction uncertainty.

DAO has some important latest trends in the support of Smart Contracts:

• Multi-protocol compatibility, that is, not only support ERC20, but also extend to other protocols;
• Realize distributed operation in combination with random mechanisms such as VRF, avoiding "pseudo-de-centralization" and "pseudo-intelligence" which has occurred previously;
• Reduce transaction costs and increase transaction speed (TPS).

In addition, the current DAO-based Public Chain has strong support for cross-chain technology. The so-called cross-chain refers to the interaction, communication and support between different Public Chains. Current mainstream cross-chain technologies include:

- Notary schemes
- Sidechains/Relays
- Hash-locking
- Decentralized private key control

The notary mechanism is the simplest and most commonly used cross-chain technique. There are many similarities between sidechains and relays, and only a few subtleties are slightly different. Hash locking

is much like a lightning network, and it is a relatively more technical way. It has been mathematically proven to be an atomic-scale exchange model. Distributed private key control is to strengthen the security of assets on a single Public Chain by jointly storing private keys by multiple Public Chains.

Early cross-chain technologies, including Ripple and BTC Relay, are more concerned with asset transfers; existing cross-chain technologies, Polkadot and Cosmos, are more concerned with cross-chain infrastructure; new emerging cross-chain technologies can support multi-currency Smart Contract, on which a lot of cross-chain financial applications can be generated.

In the earliest projects, DAO was proposed as a decentralized infrastructure. Up to now, nearly three years have passed, and some major infrastructures have been established. This is not only reflected in the number of projects related to DAO, but also in the continuous expansion of the entire DAO ecosystem. DAO has gradually transitioned from a centralized beneficiary platform to distributed storage, interactive interfaces and a broader decentralized financial services platform. Not only has the security of Smart Contracts been greatly improved, but the development focus has also been changed from single guide to the construction of decentralized infrastructure, to the management and use of existing systems, protocols and platforms.

In summary, the DAO Public Chain can make immediate and transparent decisions that are beneficial to the entire society based on logic and facts. They allow expert members to make decisions for the community and can play a very important role in the financial services industry and even the broader service industry.

2.4 Integration of Decentralized Self-Organized System and Cryptocurrency Financial Industry

At present, Blockchain technology has been widely used by financial institutions around the world in the financial fields of digital asset management, trading, and liquidity because of its advantages in traceability, non-tamperability, and decentralization. This trend established the demand for DAO in the financial sector and derived the concept of DeFi, namely decentralized finance, which mainly refers to decentralized financial derivatives and related services, which are based on distributed ledgers and Blockchains. technology.

From stable coins, decentralized token exchange platforms to credit lending, there are currently thousands of DeFi projects, and the entire ecosystem is booming. Among them, the most representative DeFi project is Bancor and MakerDAO’s DAI. The former is to reform the existing exchanges, and the latter is to reshape the traditional central bank and the stable currency.

The Bancor Agreement transforms traditional human-to-human transactions into human-machine transactions through a variety of Smart Contracts. The project team can issue tokens through one of the BNTs as a mortgage. The token market price is directly related to the supply and demand relationship. However, as far as the current cryptocurrency market is concerned, Bancor's drawbacks have been exposed in the rise and fall of the mechanism-like DAPP games FOMO3D and P3D.

At the same time, according to the data provided by Delphi Digital, MakerDAO, as a lending platform based on Ethereum, “currently accounts for 90% of the total value of locked tokens in decentralized financial projects”, often referred to as “decentralized central bank”. Other stable currencies, such as Tether (USDT), are only implemented by IAUs that issue redeemable assets through a centralized organization and are not in the DeFi category. The MakerDAO user can obtain the stable currency DAI anchored with USD 1:1 through locking-up ETH. This process is completed by the user through Maker's core Smart Contract CDP, and the MakerDAO team also directly indicates: “The core and advantages of DeFi is, users can participate without approval."

Whether it is DAI or Bancor's transformation, the core way of its implementation is to adopt complex Smart Contracts, supplemented by considerable governance capabilities and community consensus to solve problems outside the Smart Contract. The booming of these DeFi projects may mean that Blockchain finance has gradually moved from experimentation in the game to actual implementation.
In summary, Blockchain technology has been widely used by financial institutions around the world in the financial fields of digital asset management, trading, and liquidity because of its advantages in traceability, non-tamperability, and decentralization. And it triggered the need to establish DAO for the financial sector. However, when building DAOs for specific financial sectors, all project parties, token holders, and community members face the following challenges:

- How to achieve “decision-making consensus” efficiently, conveniently and quickly, avoiding losses caused by differences of opinion and difficulty in reaching agreement;
- How to reward the contribution of community members (including miners and other nodes) to the entire community fairly and flexibly, and form “positive feedback” that can actively expand the size of the community;
- How to truly “decentralize” and prevent the community and platform from being controlled by some elites or nodes with important resources, which causes ordinary members to be unfairly excluded from enjoying the benefits of community growth.

2.5 Design Ideology of MOS Public Chain

The MOS project team has been rooted in the financial field for many years, has accumulated rich experience in financial applications, and has a professional Blockchain technology development team. By combining technology and finance, it has proposed a solution to solve the current difficulties that the financial industry faces. The solution is a new generation of Public Chain platform: **MOS Public Chain**. The platform has brought up the following innovations:

- The MOS Public Chain has designed a new organizational structure that includes community members, Committee, community leaders, development teams, etc. These roles are interrelated and mutually motivated by distributed rules, avoiding the traditional DAO architecture’s drawbacks, such as the lack of automatic enforcement mechanisms, lack of effective incentives, and community being controlled by few individuals. It has laid a solid foundation for the operation of various distributed financial applications, thus forming a new DAO 2.0.
- In the DAO 2.0 architecture of the MOS Public Chain, a random mechanism based on VRF (Verifiable Random Function) is used for the screening process of the Committee. Each time the issue, project, and voting are decided, by adding certain random factors, this method can avoid the reliance on specific members and the possibility of stakeholders paying bribes to known members, truly achieving "decentralization."
- The development of a decentralized organization depends on the support of miners and nodes, which requires corresponding rewards for their contributions. In the past DAO 1.0 project, it relied only on a single mechanism such as workload (PoW), stakeholding (PoS), etc., which limited the flexibility of various applications derived from the organization. Therefore, in the MOS Public Chain, a consensus mechanism called Prof of Finance Contribution (PoFC) is innovatively applied. For the first time, two diverse types of incentives were combined in the form of weights: one is to encourage members to have more financial transaction resources, another is to provide a return on their contribution to the community. Each project and community can adopt different combination

strategies for all of its implemented financial applications, which greatly enhances the flexibility of the applications derived from the MOS Public Chain platform.

- Community members and token holders, in assessing the development prospects of each project, used to rely on their own experience, resulting in a lot of uncertainty and risk. To this end, the MOS Public Chain uses the Endogenous Growth Theory (EGT) established by Nobel Prize-winning economist Paul Romer to analyze the future development trend and growth rate of each project. The parameters used include the number of tokens of the project, the number of miners, the number of nodes, and the development funding. After the EGT-based empirical formula is transformed, the quantitative growth curve of each project is obtained, thereby greatly avoiding the blindness of the members in selecting the project.

The MOS Public Chain is designed with a variety of features which would facilitate the development financial applications thereon, including but not limited to financing, sales, agency, commissioning, credit, and more. To this end, the MOS Public Chain platform provides a set of "DAF" (Decentralized Autonomous Finance) protocol group for various application projects, and developed the corresponding MOSDAO DAPP. In this way, application projects can easily use these protocols and infrastructure to develop application scenarios and services required by them and their members.

2.6 Design Vision of MOS Ecosystem

As the opening statement of this Whitepaper reveals: "The community is self-governing, and finance is empowered by consensus."

DAO is one of the most anticipated applications of Blockchain technology. After all, this is the first time in history that we have the ability to coordinate in a non-religious and anonymous way to make decisions collectively for something. This decentralized community governance model has far-reaching implications for promoting industry development, strengthening corporate governance, and even facilitating communication and coordination among all human beings. In the financial field, represented by DeFi, DAO is getting more and more attention and application.

The vision of the MOS Public Chain project is to enable each community member to have equal access to the autonomy of financial services, to jointly build the new generation of distributed autonomous organization, that is most suitable for members of the community, and encourage contributions through reasonable incentives, and is independent of any single “central”.

MOS Public Chain projects will rely on careful architecture design, advanced technology, careful logic settings, strong Smart Contract support and unique cross-chain, sidechain technology to meet the needs of various financial industry applications and derivation, and then become the preferred Public Chain in the financial services industry.

3. Implementation Framework of MOS Public Chain project

3.1. Architecture Design of Distributed Autonomous Community DAO 2.0

So far, dozens of diverse types of DAO organization forms and Public Chains have appeared, including Bitcoin, DashDAO, The DAO, etc. According to Blockchain expert Vu Gaba Vineb, all DAOs can be measured on three aspects:

- Decision-making methods
- Participation incentives
- Level of Decentralization

Existing projects have their own advantages in all three aspects, but they have not been able to maintain a relatively balanced state in all three aspects and can be classified as DAO 1.0. In response to the various pain points of the current DAO system, MOS innovatively proposed the DAO 2.0 autonomous community architecture design plan, and carried out comprehensive improvement from the above three perspectives.

In the past DAO 1.0, the community's decision can basically be divided into the following steps:

- Distribute DAO's rights and manage tokens through airdrops, crowdfunding, private placements, public offerings, etc. Only those who hold these tokens are considered members of the community.
- For a specific topic, a discussion is held by a subset of community representatives and then the conclusion is submitted to the development team. The discussion topics include but not limited to:
    - Is a project suitable for issuing tokens in the community?
    - Is a new development mechanism recognized?
    - Does a key algorithm need to be adjusted, such as mining, incentives, etc.?
- The development team sets up a voting interface (web or DAPP) for all community users to complete the vote within a certain period.
- Make decisions based on the final bid results.

There are several potential problems here:

- It is obviously not feasible to submit all proposals to the voting process, but which topics to choose to vote for? At present, most of the proposals are controlled by some community representatives, who are mainly initiators of DAOs, the main token holders (i.e. institutions or users with large number of tokens) and some KOL (community leaders). This not only weakens the “decentralization” of DAO, but also gives these “discourse rights” owners the opportunity to manipulate the main trends of the community. More importantly, they may exclude issues that have an adverse impact on their interests, and only submit issues that are beneficial to them.
- The voting participation of community members is not motivated. The prevailing situation is that most DAOs have very low voting rate on a certain topic, which further leads to the intensification of centralization, and cannot reflect the demands of ordinary community members and token holders for self-governance and collaboration. There are many reasons for

this. On the one hand, it is inconvenient to vote, but more importantly, there is a lack of effective voting incentives. Community members cannot directly benefit from voting, which naturally reduces interest in voting.

- There are artificial steps in the entire voting process, and there is no automatic execution mechanism. The participation of the development team may introduce the influence of human factors, for example the development team may have some preference on the design of voting page and options, and also the voting topics, which will affect the whole DAO's decentralization level.

Therefore, the MOS Public Chain has designed a new mode DAO 2.0 in the decision-making aspect, which can solve the above problems perfectly. Its structure and process are as follows:

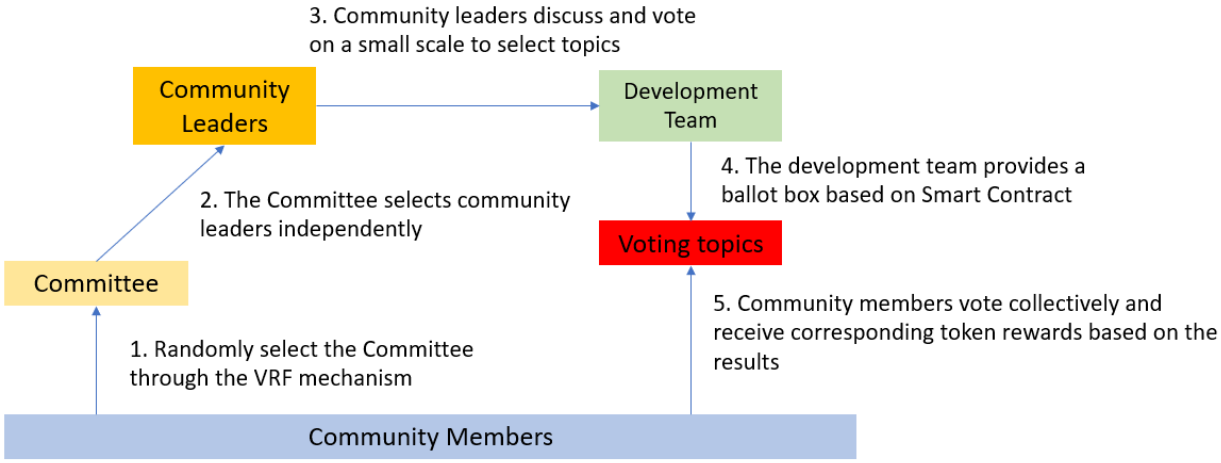


Fig.7 Decision process of DAO 2.0

It can be seen that the process is divided into the following roles:

- Community Member: A user who owns the MOS Public Chain platform token MOS is called a community member. Community members need to lock a certain number of MOS tokens before they enter the candidate pool of the randomly selected Committee.
- Committee: The community members automatically select some members to become members of the Committee through the VRF algorithm. For each topic, the calculation will be repeated. Members of the Committee will be continuously updated.
- Leader: A randomly generated Committee will vote for community leaders with influence, judgment, and execution ability, who will propose a proposal regarding changes to features of the platform for voting on behalf of all token holders.
- Developer: The development team is responsible for the construction, development and maintenance of the Public Chain, as well as the design and production of DAPP for voting.

Here's a step-by-step breakdown of the entire decision process:

1) Community members randomly select the Committee through the VRF mechanism

For several topics that need to be discussed, the development team will first set a voting period (T). During this period, the first step is to randomly screen out the Committee from all community members who choose to lock-up MOS.

In response to the general "pseudo-de-centralization" phenomenon, the MOS Public Chain innovatively applies VRF (Verifiable Random Function) to the Committee election, and periodically selects Committee members by using VRF. The management and autonomy are completely controlled by the

community, and a flat, transparent management mechanism is realized. This involves the principles of VRF and random number generation.

Relying on random numbers to allocate social resources has been applied to all aspects of daily life. From an economic point of view, random numbers are widely used in cryptography, numerical simulation, statistical research, lottery gambling, game lottery, etc., and have extremely high commercial value.

In order to generate random numbers, people also invented statistical methods such as dices, turntables, and coin flips. Computer generated pseudo-random numbers and quantum mechanics were used to obtain random numbers. Although these methods solve the problems of randomness, uncontrollability and unpredictability of random numbers, they lack the decentralization and provable fairness. Naturally, people want to find a more equitable random number generation and distribution mechanism. As a decentralized platform, the Blockchain provides a natural basis for the generation of fair and random numbers.

However, it is more difficult to design a usable random number generator on the public Blockchain. In addition to the basic random number statistics requirements, a random number generator available on the Public Chain must meet at least the characteristics of unpredictability, uncontrollable, difficult to collude, fair and auditable.

Pseudo-random numbers are generally generated by a certain algorithm, and their distribution functions and correlations can all pass statistical tests. But compared to true random numbers, they are generated by algorithms rather than a real random process. The pseudo-random number is also as close as possible to the randomness it should have, but because of the "seed value", the pseudo-random number is somewhat controllable and predictable. The pseudo-random number can be generated by using the middle method, the congruence method, the shift method, the Mason rotation algorithm, and the like.

The generation of true random numbers is unpredictable, and it is impossible to repeatedly generate two identical sequences of true random numbers. True random numbers are typically generated using physical phenomena such as throwing coins, rolling dice, shaking the mouse, turning wheels, using electronic components, using atmospheric noise, nuclear fission, and the like. The technical requirements of the true random number generator are generally high, and the production efficiency is generally lower than the pseudo random number. In addition, if the amount of information entropy is very limited, it is not always possible to generate a true random number. True randomness can be further distinguished by statistical randomness and randomness in quantum effects. It is generally believed that due to the inherent randomness of quantum mechanics, the random number generated by it is more "true" than the random number generated by statistics in traditional physics.

The Linux kernel provides a statistically random number generator. It uses the noise of the machine to generate random numbers. The noise source includes various hardware running speeds, and the interaction speed between user and computer, the interval of keystrokes, the speed of mouse movement, the interval of specific interrupts, and the response time of block IO requests. In addition, by listening to the noise generated by the quantum fluctuations of subatomic particles in the vacuum, scientists at the Australian National University has built random number generators and made them available to Internet users.

Quantum phenomena makes use of the randomness of particle behavior at the atomic scale, and its nature has not been discovered by humans, so it can be regarded as an entropy source with good uncertainty; chaotic phenomenon refers to the initial in chaotic systems. Minor differences in quantity

can lead to very different future developments, so unless you get all the accurate information at the initial moment, you cannot predict future trends.

Therefore, how to design and implement a plausible fair random number generator on the Blockchain has become an important research issue in recent years. Since the Randao team proposed the use of the Commit Reveal solution in 2015, the Randao++ solution proposed by Vitalik Buterin is published to developers. And, some DAPPs use Oracle to obtain random numbers from the under-chain service to implement Blockchain random number generation.

Regarding the measurement of random number generation schemes, the following indicators should be considered:

- Unpredictable: Unpredictable is for all participants. Neither producers nor consumers can predict the possible value of the next random number based on historical data. Even slightly increasing the success rate of prediction is also impossible. It means the scheme has Markov property. In the public random number scheme, it is also required that no one can improve the prediction probability based on any public information. For example, in Bitcoin Beacon's scheme, even if the historical data of the block, the public key of the mine pool, or the transaction list to be packaged etc. is known, he/she still can't get the advantage of prediction.
- Non-collusion: In the process of generating random numbers, some participants join together to exchange their private information, which does not affect the random number generation process or the result of changing random numbers, or has other comparative advantages, such as getting the results of the random number to be generated in advance of others.
- It is not possible to be known in advance: All the participants of the random number generation process know the random number at the same time, and neither party can know the result in advance.
- It cannot be falsified: the producer of the random number cannot forge a random number, and when a random number is generated, the random number cannot be modified by anyone.
- Not selectable: The production process of random numbers may have many random numbers generated at the same time. The producer cannot choose to provide one of them, or replace one with the other.
- Cannot be hidden: The producer cannot refuse to disclose the random number after the random number is generated. That is, the produced random number must be made public and cannot be hidden or withdrawn.
- Easy to participate: During the generation of random numbers, the parties to the random number can be easily involved. The random number generation scheme should facilitate the broad participation of the average person, reduce or eliminate the participation threshold, and the right to participate should not be deprived.
- Auditable: After the random number generation process is over, the overall process can be reviewed and checked.
- Cost: The production cost of a random number should be as low as possible.
- Response speed: The random number generation process should be fast enough.

Taking all these factors into consideration, the MOS Public Chain platform decided to choose VRF as the basis for random selection. The VRF (Verifiable Random Function) algorithm was proposed by Professor Mokari in 1999. Due to its better security and efficiency, more and more Blockchain projects have used it to optimize the consensus process, so that the random number generation part of consensus

mechanism occupies less resources, and more resources can be used for the transaction and the operation of the contract.

To understand the principle of VRF, first need to explain what is meant by "random" here: an ideal hash function whose value range should be discrete and evenly distributed. Given different input values, the output value should not be regular, randomly spilled and distributed within the range of values.

Let's look at a simple variant of the hash function, which combines the keys, such as

result = SHA256（secret，info）

Then to get the result, just having **info** is not enough, we must know the **secret** to calculate, which is the key. Or user may already have the result and info, but user must know the secret to verify that info and result are the corresponding matches.

This is the hash function with a key. However, there is a question here: Is it possible to verify that result and info match correspondingly without presenting the key? Then there is a verifiable random function (VRF).

In short, it is a hash function that combines asymmetric key technology, such as result = VRF_Hash(SK, info), SK is a private key, not public, secretly saved, and the PK paired with SK is a public key, which needs to be publicized to the verifier. The specific operation process is as follows:

1) The prover generates a pair of keys: PK, SK;

2) The prover calculates: result = VRF_Hash(SK, info);

3) The prover calculates proof = VRF_Proof(SK,info);

4) The certifier submits result and proof to the verifier;

5) The verifier calculates whether result = VRF_P2H(proof) is valid. If it is valid, continue with the following steps, otherwise it will be suspended;

6) The certifier submits PK, info to the verifier;

7) The verifier calculates True/False = VRF_Verify (PK, info, proof). True indicates that the verification passes, and False indicates that the verification fails. The so-called verification pass means that whether proof is generated by info, whether the result can be calculated through proof, so as to confirm whether the info and result match, and whether the material given by the prover has a problem.

Throughout the operation process, the certifier never presents his or her private key SK, and the verifier can deduce whether info and result match, which is the function of VRF. Thus, after the result is generated by the private key, the value can actually be regarded as a large positive integer. If it is 256 bits, its value range should be between 0 to 256th power of 2.

Dividing it from the 256th power of 2 gives a value between 0 and 1. By placing this value in the cumulative distribution of the binomial distribution for comparison, the corresponding value can be obtained. If this value is greater than zero, it is equivalent to drawing a sign that can proceed to the next step. Put this value together with the previous VRF generated, broadcast to other users, and any other received users combined with the broadcaster's public key and the value known to the entire network, they can verify whether the following two conditions are true:

1) The verification result is correct

2) The j' is equal to j through the binomial distribution function, as shown in the following figure:

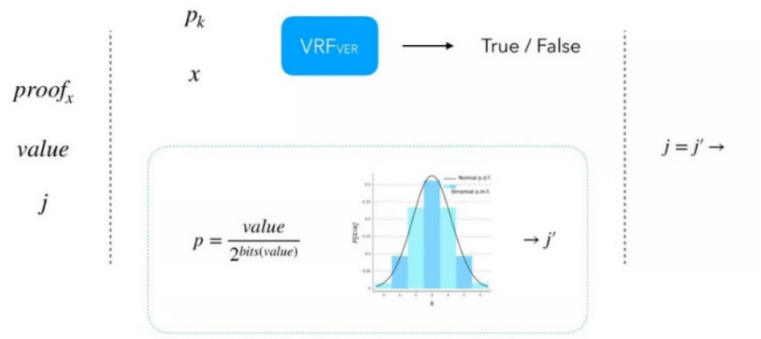


Fig. 8 Verification Mechanism of VRF

Assuming that both conditions are true, then the results of this lottery are correct and credible. So far, the process from lottery generation to verification is completed.

The advantages of VRF are:

1) First of all, its lottery process does not need to communicate with other parties. It is possible to go to this lottery result directly in this machine, and this x input is recognized by everyone. The output value for the same x is fixed, so the lottery result cannot be changed no matter how many trials.

2) After a node receives the lottery information of other nodes, it can use the attached certificate to prove the correctness of the random number and ensure that it is calculated by the owner of the private key. Therefore, the result of this drawing cannot be forged.

3) VRF is mainly used to derive a pseudo-random number. The part of the lottery is mainly responsible for a binomial distribution function. By constructing the parameters of the binomial distribution, users can conveniently control the winning stakes that need to be drawn. The number can be adapted to different scenarios that require lottery.

Therefore, through such a truly random method, the Committee can be fairly and justly selected, avoiding any human factors interference.

2）The Committee selects community leaders independently

Next, a randomly generated Committee will have the opportunity to choose a community leader. The key to this is how to motivate the Committee to select truly outstanding and qualified community leaders. To this end, MOS team has designed the following incentives:

First, each Committee member lock-up a certain amount of MOS tokens as a prize pool. Based on this prize pool, the incentives received by each Committee are divided into three parts:

- If the leader of the Committee votes for the leader and passed the Committee's vote to become a community leader, the member can receive several MOS tokens from the prize pool as a reward.
- Incentives from community leaders: If the proposal by the community leader is voted for by all community members, and the majority of users approve it, the Committee members will receive a few more MOS tokens as a reward.

Specifically, the rules are as follows:

1) Each Committee member first locks-up a certain amount of MOS tokens as a prize pool.

2) Each Committee member can nominate a limited number of community leaders and explain the reasons.

3) All Committee members vote online for all nominated community leaders.

4) Each Committee member can vote for a limited number of leaders (i.e., If only three leaders are selected, it means only three votes per person).

5) Track the total number of votes for evaluation. If the members of the Committee vote to select the leader, they will become the community leader through the voting of the Committee. Members can get several MOS tokens as rewards.

6) After that, if the proposal by the community leader is selected and the final vote of all community members is passed, which means the permission of most users is obtained, then the Committee members who choose the leader will also receive several MOS tokens as incentives.

The entire process is automatically controlled by the Smart Contract written by the development team, without any human intervention, avoiding the possibility of individual Committee members and community leaders manipulating the entire choice.

Please note that the specific number of reward MOS tokens, the number of Committee members, and the number of community leaders will be explained in the updated Whitepaper after the Mainnet gets online.

3) Community leaders discuss and vote on a small scale to select topics

In this step, a number of community leaders selected by the Committee will discuss the topics that need to be discussed during the voting period T and decide whether to submit them to the development team. As an important node for screening high-quality assets and conducting community tokens, community leaders will carefully screen proposals for the benefit of the community.

During a voting period, there are often multiple topics and projects that need to be screened, so community leaders need to rate these topics and projects. The MOS Public Chain has developed a rating framework for financial projects, and extracted 109 evaluation indicators (KPI) in five aspects, as shown in the following table:

Criteria	Weight	Detailed Criteria	Weight	Number of KPI

Table 1 Rating system of Projects on MOS Public Chain

Project overview	16%	Basic situation of the project	22.5%	8
		Basic situation of the team	20%	6
		Capital market recognition	12.5%	3
		Project promotion	22.5%	2
		Project popularity	22.5%	3
Project team	26%	Founder background	49%	10
		Core management team	25%	5
		Core development team	26%	5
Project plan	20%	Project market analysis	28%	4
		Project plan analysis	34%	4
		Project governance structure	18%	3
		Project Information Disclosure and Risk Management	20%	4
Project technology	20%	Blockchain technology	40%	10
		Application innovation	6%	1
		Technical applicability	6%	1
		Technical maturity	16%	2
		Technical health	32%	7
Token economy	18%	Basic situation of tokens	20%	8
		Token distribution plan	24.5%	8
		Token release mode	20%	5
		Token liquidity	11%	5
		Economic model design	24.5%	5
Total	100%			109

And based on this system, the risk level is defined in the following table:

Risk Level	Description
Low	These are high-quality projects, having strong competitive advantages in the market, standardized management system, true and timely information disclosure, strong development strength and operational strength, good development prospects, and strong ability to resist and withstand major internal and external unfavorable factors.

Middle	The project has certain competitive advantages in the market, relatively standardized management system, true and relatively timely information disclosure, certain development strength and operational strength, and certain ability to resist and withstand internal and external unfavorable factors, but the potential internal and external disadvantages may affect the development of the project to some extent.
High	The performance of the project is still acceptable or poor, the management level is general, the information disclosure is real but not timely, the development and operation are under certain pressure, and the project development has high uncertainty. Once there are internal and external unfavorable factors, the project can be rapidly deteriorated at any time.
Not Recommended	The project management level is very poor, development is stagnant, it is almost impossible to continue operations, or project is already failed, or information disclosure is not true, and there is possibility of fraud.

表 2 风险等级划分

The final project rating is listed below:

Rating Mark	Risk Level	Rating Range
AAA	Low (Lowest)	[90, 100]
AA	Low (Low)	[80, 90]
A	Middle (Low)	[70, 80]
BBB	Middle (High)	[60, 70]
BB	High (Low)	[50, 60]
B	High (High)	[40, 50]
CCC	Not Recommended	[30, 40]
CC	Not Recommended	[20, 30]
C	Not Recommended	[10, 20]
D	Not Recommended	[0, 10]

Table 3 Guideline for project rating

If the topics and projects recommended by the community leaders are not performing well, they will face the risk of being eliminated in the next round of Committee votes. Therefore, they will actively review, audit and evaluate the topics and projects that need to be submitted to the vote. In addition, the MOS Public Chain will establish a corresponding reward and punishment mechanisms for them:

- Before submitting an issue, community leaders need to lock-up a certain MOS token as a prize pool.
- If the submitted topic is approved by the member's specific vote, the community leader will receive the MOS token reward from the prize pool.
- Each community leader's rating for each topic is recorded in their personal record.
- However, if the submitted topic is not approved in the specific vote of the member, i.e. it is not recognized by most members, the community leader’s personal record will be greatly discounted.
- The Committee can see the ability of each leader when voting for community leaders. Obviously, the better their person record are, the more likely they will be elected.

4）The development team provides a ballot box based on Smart Contract

The MOS development team will provide a “ballot box” for all community members to vote based on topics recommended by community leaders. Similarly, the entire voting process will be presented in

the form of a Smart Contract. Users only need to view information about the voting topics in the MOSDAO wallet, as well as information about all community leaders who have proposed the proposal. Choose support or objection (i.e. YES or NO), members can complete the vote.

The key to voting through Smart Contracts is how to assign rights to the right voter, block illegal voters, and allow proxy voting between users, while automatically counting votes and keeping entire voting process completely transparent. Below is an example of “ballet box” Smart Contract based on Solidity developed by the MOS development team.

The development team will create a contract for each proposal and provide an abbreviation. The creator of the contract, which is the development team, assigns voting rights to the address of each qualified member based on the MOS token lock-up. The people who hold the addresses to which the voting rights are assigned to, may choose to vote on their own, or delegate the voting rights to the person they trust.

```
pragma solidity ^0.4.4;
// Delegated voting



contract Ballot{
    //Delegated voting entity
    struct Voter{
        uint weight;// accumulated weight
        bool voted;//if Ture, means the voter has already voted
        address delegate;// Delegated voter
        uint vote;// index of the proposal that voter selects
    }

  //Type for independent proposal
  struct Proposal{
        bytes32 name; // abbreviation（32 bytes）
        uint voteCount;//accumulated votes
  }

  // State variables and other parameter declarations
  address public chairperson;
  // Declare a state variable here, save the structure of the Voter for each independent address.
  mapping (address => Voter) public voters;
  // A dynamic array that stores the Proposal structure
  Proposal[] public   proposals;



  // Create a new vote to choose a proposal name proposalsNames
  function Ballot(bytes32[] proposalNames) {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
  // Create a new proposal for each proposal name provided
```

```
// Object added to the end of the data
for (uint i= 0;i<proposalNames.length;i++){
// Create a temporary proposal object
// Add to the end of a proposal array
proposals.push(Proposal({
                name:proposalNames[i],
                voteCount:0
    }));
    }
}

// Providing voting rights to voter
// Can only be called by the voting host chairperson
function giveRightToVote(address voter) public{
    if(msg.sender !=chairperson || voters[voter].voted)
    throw;
    voters[voter].weight = 1;
}



// Entrust your voting rights to a voting representative
function delegate(address to){
    // Specify reference
    Voter    storage sender = voters[msg.sender];
    if (sender.voted)
    throw;
// When the voting representative to also delegates to others, need to find the final voting representative.
  while (voters[to].delegate !=address(0)&& voters[to].delegate !=msg.sender)
    to = voters[to].delegate;
// This is not allowed when the final voting representative is equal to the caller.
  if (to ==msg.sender)
      throw;
    // because sender is a reference
    //Here it actually edits voters[msg.sender].voted
            sender.voted = true;
            sender.delegate = to;
            Voter delegate =voters[to];
      if(delegate.voted){
    // If the delegated voting representative has already voted, directly modify the number of votes
          proposals[delegate.vote].voteCount +=sender.weight;
    }else{
    // If the voting representative has not voted yet, modify the weight of his/her vote
          delegate.weight += sender.weight;
```

```
        }
    }

  // Cast a vote (including the votes entrusted to the user)
  //To proposals[proposal].proposalNames
function vote(uint proposal){
        Voter    storage sender = voters[msg.sender];
        if (sender.voted)throw;
        sender.voted = true;
        sender.vote = proposal;
  // If the proposal index is outside the given proposal data range
  // Will automatically throw an exception and undo all changes
        proposals[proposal].voteCount +=sender.weight;
  }


  // Calculate the current winning proposal based on all current votes
  function winningProposal() constant returns (uint winningProposal){
        uint winningVoteCount = 0;
        for(uint p =0; p<proposals.length;p++){
              if(proposals[p].voteCount >winningVoteCount){
                    winningVoteCount = proposals[p].voteCount;
                    winningProposal = p;
        }
    }
  }
}
```

5）Community members vote collectively and receive corresponding token rewards based on the results

Finally, all community members who have locked-up a certain amount of MOS tokens will vote. In order to improve the voting rate of community members, they are encouraged to actively participate in ecosystem operations. The MOS Public Chain has designed the following incentives:

- Once the proposals available for voting are approved by most community members, members who have voted will receive a certain amount of token rewards from the prize pool.
- If the option members voted for fails, the tokens collateralized by the member will be distributed to other members who have passed.

This will not only encourage members to vote, but also encourage them to carefully analyze each topic, the actual value of each option, and make choices that are appropriate for the community. The incentive mechanism achieves “interaction” with its own interests and achieves positive feedback.

In summary, this is the DAO 2.0 “Decision-making Consensus” process proposed by the MOS Public Chain. The whole process is completely based on Smart Contracts, and the VRF random screening and incentive mechanism effectively reduces the possibility of centralization and improves the enthusiasm and efficiency of community members in decision-making.

3.2. Algorithm Consensus Mechanism of MOS Public Chain

The development of a Public Chain depends on the active participation and contribution of miners and nodes, which stems from the recognition and reward of contributions to these members. In the past history of Blockchain development, there are various mechanisms such as PoW (Proof of Work), PoS (Proof of Stake) and DPoS (Delegated Proof of Stake) based on specific computer algorithms, so-called "algorithm consensus".

The Blockchain is a public ledger, an open database, and a peer-to-peer collaborative network. Collaborators (nodes) work together to maintain data. Each node has a complete data backup. The data content of all nodes must be identical. Each node can find transaction records locally, and each node can also add transactions locally. Without a center to command and coordinate, to complete this collaboration, the Blockchain must have a consensus mechanism that must address two basic issues:

- Who has the right to write data – only one person can add accounting data at a time;
- How other people synchronize data – because the consistency of the ledger needs to be maintained.

The process of data writing (block addition) is as follows: the node that has the right to package the transaction, put the packaged transaction (block) on the existing database (Blockchain), and broadcast to the whole network. Upon other nodes receive the message and verify the block, the newly packaged transaction will be synchronized. Each packaged transaction is called a block, and the blocks are constantly superimposed to extend the Blockchain. One problem with synchronizing data is how to agree on the order of transactions that occur within a certain period of time. Since each node is recording transactions spontaneously or keep synchronized, there is a high network delay in the case of peer-to-peer communication. Therefore, the order of data received by each node is inconsistent. Thus, how to keep the consistency of each node's replica data has become a very important issue.

The consensus of the Blockchain is: the longest chain is the main chain, that is, each node always selects and tries to extend the main chain. This means each node uses the chain with the most blocks as the choice to add and update the block. Thus, multiple nodes can synchronize an authoritative public ledger. Then, the Blockchain consensus mechanism focuses on solving the first problem: who has the right to write data. With the development of Blockchain technology, there have been many ways to solve this problem. Here are three main ones: PoW, PoS, and DPoS.

1） PoW (Proof of Work)

The workload here refers to the process of computer computing Nonce (random number). Each node calculates a random number. Within a certain period of time, the difficulty of finding a random number is certain, which means that it takes a certain amount of work to get this random number. The node that first obtains this random number adds the packaged transaction block to the existing Blockchain and broadcasts to the entire network, and then other nodes verify it and synchronize.

Advantage:

- Safety: Because the miners are spending money to buy mining machines to participate in mining, the cost of the mining machine is the actual sunk cost, so the possibility of concentrated fraud (such as collective accounting falsely to deceive the whole network, etc.) is less likely. In the past 10 years, there have never been any errors or omissions or attacks to Bitcoin. It is enough to prove the most superior security of the PoW algorithm. Other mechanisms such as PoS and DPoS are new consensus mechanisms that have emerged in recent years and have not been tested by time.

Even if there are no major problems or loopholes in the short term, it is impossible to assert that there will be no major security problems in the future.

- High quality projects tend to attract early miners. Because early participants are more likely to get larger rewards and do not need specialized mining machines, miners tend to be more involved in this high quality PoW projects in early phase, and if the project is well developed, it can generate better income. This advantage is only for today, because of the success of Bitcoin PoW, the graphics card miners are looking for high-quality project mining, which has contributed a lot to the early projects, but when Bitcoin came out, the above two advantages actually didn't exit. Thus, this consensus mechanism will become more and more safe and attractive with time.

Disadvantages:

- Waste of resources: Due to competing computing power, participants are constantly upgrading hardware (graphics cards) for greater computing power, and even producing machines (mine machines) dedicated to calculating SHA-256 or other mathematical problems. The production and operation of these machines cause huge manpower and electricity waste, just to calculate a meaningless encryption math problem, which is the most criticized point for Bitcoin.
- Upgrading is difficult: Since the entire calculation and competition process is written in a variety of mining machines, any upgrade to the original consensus mechanism is difficult to notify and implement, to apply changes for all participants in a short period of time. And because of participators have different personal wishes, it is difficult to achieve a smooth upgrade of the entire mechanism and system, resulting in divergence and impact to security is almost difficult to avoid.

2）PoS (Proof of Stake)

PoS is that the system allocates the corresponding block generation rights according to the product of the number of tokens (tokens) held by the node and the time (token * days). The more tokens users have, the greater the probability of obtaining the block generation rights. Token is equivalent to the Stake of the Blockchain system and is therefore called a proof of stake.

Advantage:

- No waste of resources, no mining machines, and the way to get high gains is to become a bigger stakeholder.
- Upgrades are relatively easy and are performed on the software and online via a computer, without involving hardware rewrites.

Disadvantages:

- Security cannot be completely determined. Some holders may use other digital currencies to exchange with PoS currency. There is no substantial sunk cost, the cost of fraud is relatively low, and the mechanism is not time-tested, and the safety cannot be determined in the short term.
- Inflation and wealth concentration are more pronounced. Because of the issuance mechanism, there is inflation every year before the currency is fully issued, and wealth will tend to be centralized.

3）DPoS (Delegated Proof of Stake)

In PoS mechanism, users can get block generation rights with Token, while DPoS means that people with Token vote for fixed nodes, and these nodes act as agents of the token holders to exercise the right to generate blocks. These representatives elected by votes obtain block generation rights in turn according to certain algorithms. Different from PoW and PoS, the whole network can participate in block generation rights competition. The DPoS block generation node is determined within a certain period of time. The proof of stake authorization enables each node to first elect n block generation

nodes through stakeholding, like the board system in the company, and subsequent proposals are processed in turn by these selected nodes. The proof of stake authorization does not theoretically require that the elected representative individual be a stakeholder, and thus appears to be more democratic and open. If the elected representatives do not act (which means they don't generate blocks in their turn), or don't act properly, they can be screened out and punished if necessary (the voters who select them may also be punished). The stake authorization certification mechanism greatly improves the efficiency but reduces the number of block generating nodes and is weakly centralized.

Advantage:

- Ease of use is optimal, the number of special nodes is small, the verification efficiency is high, and the user experience is good.
- Special nodes are often highly related to groups or individuals with enormous amounts of money and have higher social influence. As the price of the currency rises, the block generation reward will bring huge benefits to the special nodes, so the promotion willingness of special nodes is the strongest than the above mechanisms.

Disadvantages:

- The security is weak, the number of verification nodes is too small, and the ease of use sacrifices the security. It is not a decentralized block generation method. The essence of the special nodes may only be few servers distributed around the world. Thus, the security risks are large.
- The right of a special node is too large, and it is difficult to achieve complete anonymity. The possibility of collective evil or collective coercion cannot be ruled out.
- The individual's willingness to vote is weak, and since the special node itself is also a holder of a large amount of money, it is inevitable that the voting process becomes a game between interest groups. The possibility of community division is high.

4）PBFT（Practical Byzantine Fault Tolerance）

The practical Byzantine fault-tolerant algorithm is a message-based consistency algorithm. Different from the previous three, PBFT is based on calculations, and there is no token reward. When everyone in the chain participates in the voting, less than (N-1)/3 nodes are opposed, the right to publicize the information is approved. The algorithm achieves consistency through three stages: Pre-prepare, Prepare, and Commit. These stages may be repeated because of failure. After the practical Byzantine fault-tolerant algorithm information is exchanged between nodes, each node lists all the obtained information and finally uses most of the results as a solution.

The Byzantine general issue was proposed by Leslie Lamport in 1982, as described below: The Byzantine Empire sent m troops to besiege an enemy. Since the Byzantine army is spread in various locations, it must start attack simultaneously in a separate enclosure. Each of their armies has no chance of attacking alone, unless more than n troops attack at the same time to attack the enemy, and the military can only rely on the communication soldiers to communicate with each other to negotiate the offensive intention and attack time. But there may be traitors between the Byzantine generals. The purpose of these traitors is to obstruct other loyal generals to reach a consensus plan by deliberately transmitting false news or not sending out any news.

The Byzantine General problem is the modeling of a realistic distributed system in which the military corresponds to nodes in a distributed network, whether it can reach an operational agreement and eliminate the enemy, corresponds to whether a distributed network can achieve consistency, and the behavior of traitor in the generals corresponds to a situation in which the faulty node of the computer

exhibits inconsistency, such as channel instability causing the node to send wrong message to other nodes, or message corruption. The above distributed system failure is also called a Byzantine error. A situation in which a message is lost or duplicated in a distributed system, but no content corruption occurs is called a non-Byzantine error. Fault tolerance refers to the protocol that handles these anomalies or failures. An algorithm capable of dealing with Byzantine errors is called Byzantine fault tolerance, while an algorithm that can deal with non-Byzantine errors is called non-Byzantine fault tolerance.

Advantage:

- Save energy without the need to mine.
- It is very fast to determine the correctness of the information.

Disadvantages:

- When nodes are added, a large amount of information interaction is required, and the burden on the entire system is greatly increased, resulting in poor scalability.
- Poor security (failure tolerance is only 1/3).

In summary, the Blockchain solves the problem of transmitting trusted information and value transfer on untrusted channels, and the consensus mechanism solves the problem of how the Blockchain achieves consistency in a distributed scenario. Targeting the unique needs of each segment of the financial sector, including fund raising using tokens, peer-to-peer mortgage lending, stable currency, decentralized derivatives market, bulk OTC collaboration, etc., the needs of each business are different, and the requirements for incentive mechanism are also different. Therefore, if a single algorithmic consensus is used in a public chain system, it is very difficult to aggregate the participation of the entire industry. In fact, many Blockchain projects in the financial sector have failed to take into account the specific needs of members of different fields and different professional communities, thus limiting the scale of community expansion.

- To this end, the MOS Public Chain first proposed the use of PoFC (Proof of Finance Contribution) as an algorithmic consensus mechanism. "**Financial contribution**" includes a combination of financial transaction resources (i.e. "participation in economic activities") and community contribution (i.e. "provision of computing workload"). It allows various applications in the Public Chain to adopt different weight allocation according to diverse needs, based on these two contributions' proportion in the general consensus mechanism. It is implemented into the Smart Contract to achieve a code-based **dual incentive system**. Note that the "**financial trading resources**" here are not limited to the number of tokens owned, but also include:
  - Trading volume; the more frequent the transaction, the greater the contribution.
  - Amount of commissioned sales and entrusted purchases
  - Number of invited mining nodes
  - Number of tokens issued

The purpose of recording these resources is to encourage miners and nodes to actively participate in the financial activities and transactions within the community, thereby improving the community's activity and financing efficiency. **The contribution of the community** (i.e. "workload") needs to be calculated according to the existing mining algorithm, and according to the computing power of each miner and node, provide corresponding mining opportunities and token rewards.

MOS Public Chain comprehensively considers these two factors, and allows each project, community, according to their own needs, to tailor the corresponding consensus mechanism for the actual needs of

financial applications, that is, to assign the weight of these two factors, to achieve one specific consensus setting for one specific project. The relevant process is shown below:

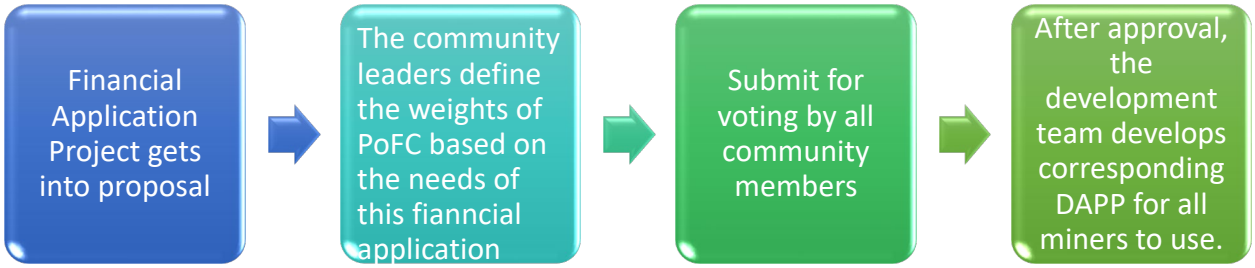


Fig.9 Algorithm Consensus Mechanism of MOS Public Chain

3.3. DAO 2.0 Development Model based on Endogenous Economic Growth Model

The MOS Public Chain draws on the Endogenous Growth Theory (EGT) established by Paul Romer, winner of the 2018 Nobel Prize in Economics, to transplant the GDP estimation model of the general economic system to the DAO 2.0 organization. Thus, a unified evaluation system for the value generated by distributed organizations has been established.

Since Adam Smith, the entire economics community has debated the factors driving economic growth for more than 200 years. The resulting consensus is that for a long period of time, a country's economic growth depends mainly on the following three elements: (1) the accumulation of productive resources over time; (2) the efficiency of the use of resource stocks in the case of a country's technical knowledge; (3) technical progress. However, the most popular neoclassical economic growth theory since the 1960s is based on the growth model established by the Cobb-Douglas production function with labor input and physical capital input as independent variables, and technological progress as an exogenous factor to explain the economy growth, therefore, the conclusion is that long-term economic growth stops when the factor returns decline.

However, the "new economics" formed in the early 1990s, the endogenous growth theory, argues that long-term growth rates are explained by endogenous factors. This means, in the process of labor input, there is the human capital formed by formal education, training, and on-the-job; in the process of physical capital accumulation, there is technical progress formed by the activities of research, development, and innovation, so that the elements such as technical progress are endogenous, and the conclusion is made that, the return from the existing factors caused by technical progress will keep increasing and long-term growth rates are positive. Of course, many economists have long seen the effects of human capital and technical progress on economic growth, but they all see them as exogenous factors.

Thus, the policy implications of the two theories differ: although fiscal economists have always believed that fiscal policy can influence economic growth (because the intrinsic link between fiscal policy and economic growth is manifested in many ways, such as the negative effects of distorted taxes, the negative impact of progressive tax on the propensity to save, and the increase in taxes to use

additional resources to increase the level of public spending, etc.), but neoclassical growth theory believes that long-term economic growth is entirely determined by the exogenous factors of the theory itself, so no matter what Policy, long-term growth is unchanged, or fiscal policy has only a short-term effect on economic growth, but cannot affect long-term growth; while endogenous growth theory believes that a country's long-term growth is determined by a series of endogenous variables. These endogenous variables are sensitive to policies (especially fiscal policies) and are influenced by policies. If the growth rate is determined by endogenous factors, then the question is how the economic entities, especially the government, can influence the growth rate. Therefore, the impact of fiscal policy on economic growth has once again become the focus of attention.

The Romer model, the Lucas model, and the Grusman-Heptman model are just the most famous endogenous growth models, and many others focus on different growth aspects, such as the knowledge-growth endogenous growth model of Kim and Robertson, Agger and Howett's imitation and creative digestion of endogenous growth models and Yang's international trade endogenous growth model. An important idea expressed by all these models is that, **enterprises are the ultimate driver of economic growth, especially as they attempt to illustrate how enterprises accumulate knowledge, which broadly includes human capital and technical change.** This accumulation of knowledge is expressed in terms of increasing human capital, producing new products, and improving product quality. These models suggest that externalities or knowledge spillovers occur in the knowledge and accumulation process and require government policy interventions: policies to support research and development, innovation, human capital formation, and even key industrial sectors.

In summary, the following simple non-technical statements can be made about the reasons for the economic growth expressed by the endogenous growth theory:

1) Technical innovation is the source of economic growth

2) The degree of labor division and the accumulation of specialized human capital are the most crucial factors determining the level of technical innovation.

3) Certain economic policies implemented by the government have an important impact on a country's economic growth.

Similarly, the MOS Public Chain will use each financial application, the number of tokens, the number of miners, the number of nodes, and the technical costs (the development spending of the MOS Foundation development team for each project) as a similar parameter, through certain transformations and analysis, to quantify the value of each financial project and predict its long-term growth rate in the future.

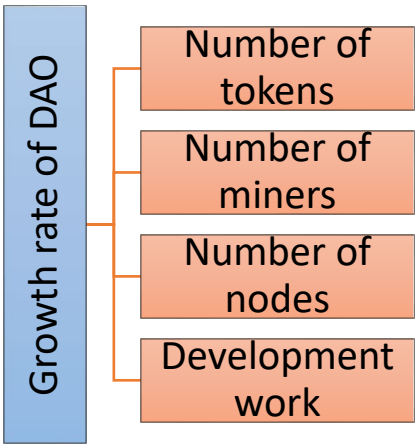


Fig. 10 DAO Grow rate prediction based on Endogenous Economic Growth Model

3.4. DAF (Decentralized Autonomous Finance) Protocol Suite

As a platform, MOS Public Chain has formed a community consensus through the innovative design of DAO 2.0, and would be able to support a variety of financial applications based on this.

First, in response to the special needs of financing, lending, agency, and derivatives in the financial sector, MOS has developed a "DAF" (Decentralized Autonomous Finance) protocol suite specifically designed to eliminate various pain points in the decentralization of the financial sector.

Finally, the MOS Public Chain will continue to strengthen the characteristics of various aspects, including cross-chain, side chain and other support, improve the Public Chain ecology, and gradually become the first Public Chain of choice for the financial industry.

3.4.1 Decentralized Autonomous Community Token Issuance based on Smart Contract

The primary application of the DAF protocol suite is to allow projects to utilise the MOS Public Chain to implement a truly Smart Contract-based, decentralized autonomous community token issuance. The core idea of this issuance mechanism is that as long as several nodes reach a consensus, it is possible to issue tokens based on Smart Contracts by setting node rights and decision-making consensus rules (such as voting, random, etc.). Members of the community interested in this token can purchase tokens directly from these nodes, or they can purchase them through other agents. Via secondary smart contracts, the income generated by token sales may be distributed among all nodes and members according to the consensus fairly reached between the nodes.

This model has the following advantages over traditional Blockchain fund raising methods:

- MOS ecosystem believes that the community consensus led by more community leaders and quality nodes can truly identify the pros and cons of the project, without the need for a centralized organization to endorse the trust of the project. Any centralized organization will definitely be based on its own interests and cannot be responsible for each individual participant.
- For token holders, because this process is based entirely on transparent and traceable Smart Contracts, it avoids project-based malpractice and greatly reduces project risk.
- For the issuer, the entire process does not need to rely on any third parties or exchanges, etc., avoiding the intermediate architecture to earn high commissions.
- The issuer and the project side can focus on the value increasing of the project and the construction of the community and leave the specific matters of the token issuance to the community autonomy.
- Ensure that the secondary market value of tokens stems from the power of community consensus. Issuing tokens really through the community consensus, will stimulate the self-regulation of market prices, so that the price of open secondary market transactions tends to stabilize.

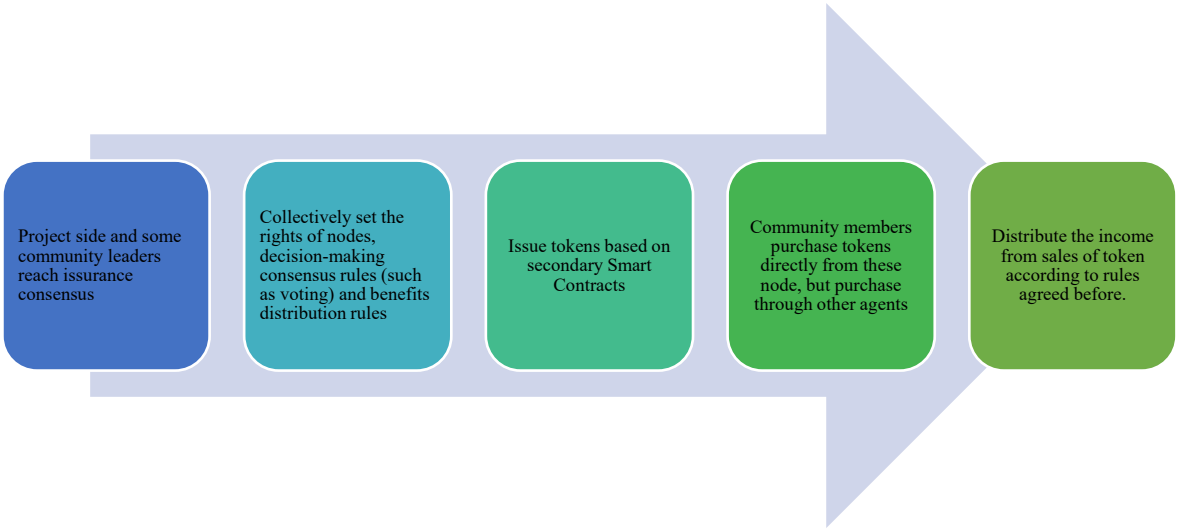


Fig. 11 Process to issue token though DAO 2.0

3.5. Ecosystem

In summary, a new ecosystem for the financial industry has been built throughout the MOS Public Chain. The system mainly includes the following elements:

- Foundation: As the organizer and operator of the entire Public Chain, the MOS Foundation undertakes the functions of building infrastructure, organizing development teams, updating Smart Contracts, providing core services, and providing all-round support for users and community members. The Foundation will receive upfront funding (via sale of MOS tokens) for the development and maintenance of various systems, products and contracts.
- MOSDAO: The MOSDAO wallet runs in the terminal of each member and is the core means of linking all members. MOSDAO has the following features:
    - Support cloud services, multi-point backup, highly secure and reliable
    - Support HD wallet function
    - Support multiple signatures, when enabled, members can choose to be unlocked by several other members in coordination, thus avoiding individual members losing account ownership due to key loss
    - Community consensus functions, including commissioning, voting, lock-up, rewards and punishments, etc., will be completed through Smart Contracts supported by DAPP to achieve financial transactions based on community autonomy.
- MOS Token: See Chapter 4 for details.
- Community Autonomous Management System: Community leaders in each community can customize the community's autonomous management system, which includes a series of Smart Contracts based on DAF, such as:
    - Part of community sales can be used as incentives for the community
    - Each member can pay a membership fee, and all contributions are used as a prize pool to motivate members of the community. The specific network settings and the proportion of node incentives are all customized by the community organizers

through the contract, and then all members vote collectively (through the "decision-making consensus" mechanism).

- Communities: Communities are a vital part of the MOS ecosystem, including community members, community leaders, and trusted agents.
- Development Team: The development team is managed by the Foundation and is responsible for providing technical support to all communities, including Smart Contract development and maintenance, and public infrastructure management.
- DAPP: For each type of financial application, including mortgages, loans, commissions, etc., each project can develop DAPP based on the MOS Public Chain. The MOS Foundation provides a powerful SDK (software development kit) and API interface to facilitate the development of innovative financial applications.
- Cross-chain support: MOS Public Chain not only supports financial applications in its own ecosystem, but also supports the mainstream cryptocurrency Public Chain (including Bitcoin Public Chain, Ethereum, etc.) through cross-chain support, thereby greatly increasing the types of financial derivatives supported, allowing application projects and community members to build trade pairs and derivative mortgage/lending services that combine MOS tokens with mainstream currencies.

4. Introduction to MOS Token

4.1. Attributes explanation

The native digital cryptographically-secured utility token of the MOS Public Chain (**MOS token**) is a transferable representation of attributed functions specified in the protocol/code of the MOS Public Chain, designed to play a major role in the functioning of the ecosystem on the MOS Public Chain, and intended to be used solely as the primary utility token on the network/protocol.

MOS token is a non-refundable functional utility token which will be used as the medium of exchange between participants on the MOS Public Chain. It is a type of utility token similar to platform tokens of other leading projects, with multiple functions and can be used for community voting (as described above), staking or security deposits to indicate service standard guarantees, and purchase of various rights and services, as well as the platform currency for secondary applications within the ecosystem related to user rights in financial scenarios.

The goal of introducing MOS token is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on the MOS Public Chain, and it is not, and not intended to be, a medium of exchange accepted by the public (or a section of the public) as payment for goods or services or for the discharge of a debt. MOS token does not in any way represent any shareholding, participation, right, title, or interest in the Foundation, the Distributor, its affiliates, or any other company, enterprise or undertaking, nor will MOS token entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. MOS token may only be utilised on the MOS Public Chain, and ownership of MOS token carries no rights, express or implied, other than the right to use MOS token as a means to enable usage of and interaction within the MOS Public Chain.

In the early stage, MOS Tokens will only be used in some MOS Public Chain series exchanges, but will gradually be listed on the mainstream exchanges. It has more attributes and rights than regular cryptocurrencies. To the extent a secondary market or exchange for trading MOS token does develop, it would be run and operated wholly independently of the Foundation, the Distributor, the sale of MOS token and the MOS Public Chain. Neither the Foundation nor the Distributor will create such secondary markets nor will either entity act as an exchange for MOS token.

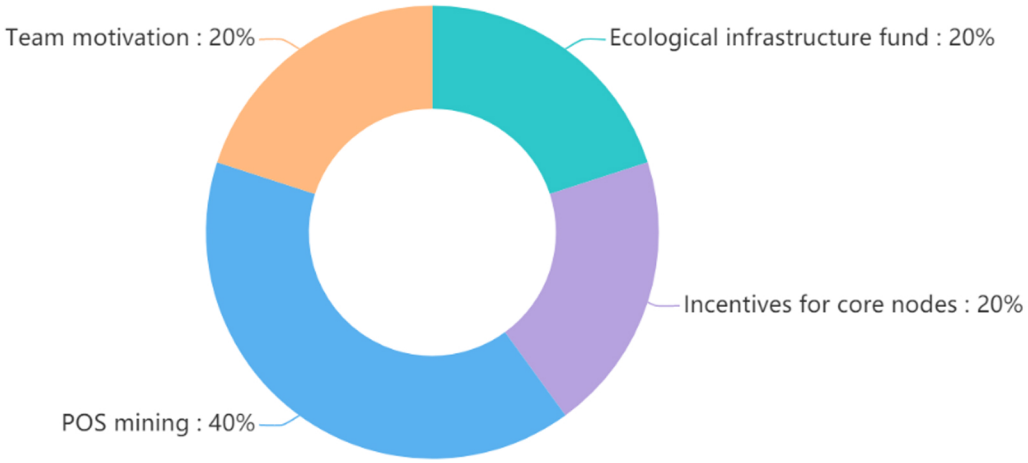
Compared to other platform tokens, MOS tokens have the following characteristics:

- Holders can use it for various interests within the MOS Public Chain, such as voting, VRF screening, as the unit of exchange for mortgages, payment of platform commissions etc.
- Holders would have access rights to the MOS ecosystem and applications developed thereon, as well as may participate in community governance (for the avoidance of doubt, the right to vote is restricted solely to voting on features of the MOS Public Chain; the right to vote does not entitle MOS token holders to vote on the operation and management of the Foundation or its affiliates, or their assets, and does not constitute any equity interest in the Foundation or its affiliates).
- MOS token is required as virtual crypto "fuel" for using certain designed functions on the MOS Public Chain, providing the economic incentives which will be consumed to encourage participants to contribute and maintain the ecosystem on the MOS Public Chain. Similarly, users which exhibit greater participation in economic activities conducted on the MOS Public Chain would also receive a greater amount of token incentives under the algorithmic consensus mechanism. MOS token is an integral and indispensable part of the MOS Public

Chain, because without MOS token, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on the MOS Public Chain.

- Computing resources are required for running various applications and executing transactions on the MOS Public Chain, as well as the validation and verification of additional blocks / information on the blockchain, thus providers of these services / resources would require payment for the consumption of these resources (i.e. "mining" on the MOS Public Chain) to maintain network integrity, and MOS token will be used as the common unit to quantify and pay the costs of the consumed computational resources.
- Users of the MOS Public Chain and/or holders of MOS token which did not actively participate will not receive any MOS token incentives.

4.2. Issuance Method



20% of MOS tokens as an ecological infrastructure fund will be used for development, business operations, legals, research on blockchain technology that includes enhancing system and applications such as wallet, payment gateway, financial derivatives within MOS ecosystem and contingency over the next few years to deliver on the roadmap milestones.

20% of MOS tokens will be allocated to ensure that liquidity and incentives will be available to distribute to core node members and affiliates to grow the network, especially those who help to do marketing, advertisement, technology development and other forms of activities in order to ensure continuous acknowledgment of MOS from the public.

40% of MOS tokens are produced through POS mining.

20% of MOS tokens will be allocated to the MOS Team (advisors and core team) and vested to align the Team with project delivery. This part will be released within two years.

In particular, it is highlighted that MOS token: (a) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the Distributor or any affiliate, (b) does not represent or confer on the token holder any right of any form with respect to the Foundation, the Distributor (or any of its affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the MOS Public Chain, the Foundation, the Distributor and/or their service providers, (c) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss, (d) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument, unit in a collective investment scheme or any other kind of financial instrument or investment, (e) is not a loan to the Foundation, the Distributor or any of its affiliates, is not intended to represent a debt owed by the Foundation, the Distributor or any of its affiliates, and there is no expectation of profit, and (f) does not provide the token holder with any ownership or other interest in the Foundation, the Distributor or any of its affiliates.

Risk Disclosure

Nothing in this Whitepaper constitutes legal, financial, business or tax recommendations. Before participating in any activities in this Whitepaper, please consult relevant legal, financial, tax or other professional consultants. In view of the nature of the business model of the project and the fact that the project is at an early stage of development, the MOS token in this Whitepaper should be regarded as a high-risk project. The purchaser should be aware of the potential risks of this project, and this project is only suitable for purchasers who can withstand the risks of this project. In addition, purchasers should consider other risks before purchasing MOS tokens and advise professionals to consult on income tax, law and other related matters before purchasing. **IF YOU DECIDE TO PURCHASE MOS TOKEN, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:**

Risks related to judicial supervision

Blockchain technology has become the main object of supervision in the world's major countries. The existing regulatory license or tolerance for MOS tokens or this public sale in any country may only be temporary. From time to time, the project may receive inquiries, notifications, warnings, orders or rulings from one or more authorities, or may even be ordered to suspend or terminate any action regarding the public sale or the development of MOS tokens. The development, marketing, publicity or other aspects of MOS tokens, as well as the current public sale, may therefore be seriously affected, hindered or terminated. At the same time, MOS tokens may be defined as virtual goods, digital assets or even securities or currencies at any time. Therefore, in some countries, according to local regulatory requirements, MOS tokens may be prohibited from trading or holding. In addition, procedures prohibited or restricted in specific jurisdictions, such as those involving gambling, betting, lottery, pornography, etc., may be developed, promoted, marketed or operated using the permissionless requirements of the MOS Blockchain. Supervisory authorities in specific jurisdictions may take corresponding administrative or judicial measures against specific applications or even their developers or users. Punishment, sanction, repression or other regulatory measures by any government authority will more or less intimidate or deter existing or potential users of MOS tokens to use the platform of the MOS Public Chain and hold the MOS tokens, which will have a significant adverse impact on the future of the MOS Public Chain.

Hacking and Theft Risk

Hackers or other organizations or countries may attempt to interrupt the functioning of MOS Public Chain in any way, including DoS attacks, Sybil attacks, guerrilla attacks, malware attacks, or consistency attacks.

Vulnerability and Rapid Cryptography Development Risk

The rapid development of cryptography and science and technology, e.g. quantum computers, imposes the risk of cracking the cryptocurrency tokens and MOS Public Chain platform, which may lead to loss for users of MOS Public Chain.

Failure risk in application

MOS Public Chain platform may fail due to various reasons, and it may not provide services normally. In serious cases, users may suffer losses. The neglected fatal flaw in open source software or the risk of large-scale failure of global network infrastructure. While some of these risks will be significantly mitigated over time, such as fixing loopholes and breaking computing bottlenecks, others remain unpredictable, such as political factors or natural disasters that may lead to partial or global Internet disruptions.

Market risk of token sales

Because the environment of token sales market is closely related to the situation of the whole digital currency market, such as the overall market downturn, or the influence of other uncontrollable factors, it may cause the digital currency itself to be undervalued for a long time even if it has good prospects. In addition, tokens are traded on the open market, usually with sharp price fluctuations. This fluctuation may be caused by market forces (including speculation), changes in regulatory policies, technological innovation, the availability of exchanges and other objective factors. This fluctuation also reflects changes in the balance between supply and demand. Whether or not there is a secondary market for MOS tokens trading, the project side is not responsible for the transaction of MOS tokens in any secondary market. Therefore, the risk involved in the transaction price of MOS tokens should be borne by the MOS token traders themselves.

Risk of Incomplete Information Disclosure

The MOS Public Chain project is still in the development stage, and its philosophy, consensus mechanism, algorithm, code and other technical details and parameters may be constantly updated and changed. Although the Whitepaper of the MOS Public Chain project contains the latest key information of the MOS Public Chain project, it is not absolutely complete and will be adjusted and updated by the project side for specific purposes from time to time. The project side is incompetent and has no obligation to keep informed of every detail of the MOS Public Chain project development (including its progress and expected milestones, whether or not delayed), so it does not necessarily allow participants to get timely and sufficient information about the MOS Public Chain project development from time to time. The inadequacy of information disclosure is inevitable and reasonable.

Risk of Private Key Loss

Buyer's digital currency, MOS token, is the only way to manipulate the content contained in the address after extracting its own digital wallet address, which is the buyer's relevant key (i.e. private key or wallet password). The user is personally responsible for protecting the relevant key for signing transactions that prove the ownership of the asset. Users understand and accept that losing or destroying the private key necessary to access MOS tokens may be irreversible. The MOS token can be operated only by occupying the relevant unique public key and private key through local or online wallets. Each purchaser should keep the private key of his/her wallet properly. If the private key of the MOS token purchaser is lost, lost, leaked, damaged or endangered, the project party or any other person cannot help the purchaser to access or retrieve the relevant MOS token. In addition, only by keeping the wallet safe (especially the private key) can the users enjoy the benefits such as rewards and gifts attached to the purchase of MOS tokens. MOS tokens should be withdrawn into wallets that are absolutely controlled by users. Once the MOS tokens are transferred or transferred for any reason, the unrealized rewards and gifts attached to the MOS tokens will not be available. The best way to safely store logon certificates is to separate the key to one or more places and store them safely, and it is best not to store them on public computers. Anyone who gains access to the purchaser's registered mailbox or registered account by decrypting or cracking the password of the purchaser of MOS tokens will be able to maliciously claim the stolen MOS tokens.

Other unforeseen risks

In addition to the risks mentioned in this Whitepaper, there may also be risks that the MOS Public Chain team has not mentioned or anticipated.

Copyright of this article

THANKS!