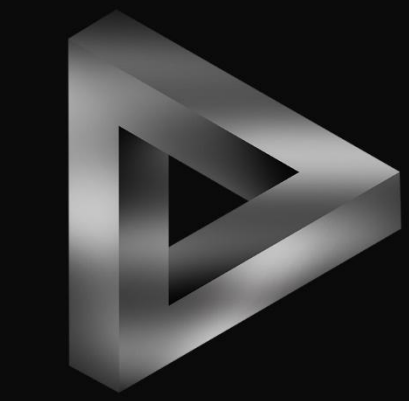


DOMAIN

WHITE PAPER 1.0

Preface

Due to the limitation of individuals' ability to obtain information and productivity during the development of human civilization, human beings established centralized institutions and organizations, as well as benefited from the high efficiency provided by them, so that the social economy can develop rapidly. But with their gradual growing and expansion, the managers often collude with each other change data privately and damage the interests of customers for their own benefits. As a result, the crisis of confidence has become more and more violent. In addition, Central Bank in various countries caused inflation by printing money infinitely, while personal information was sold by institutions in a package as a means of profit. Numerous cases of trust collapse have emerged between institutions and individuals, thus greatly hindering the progress of social civilization and development of economy. Therefore, it has become an urgent demand for many people that establishing a transparent and stable new consensus system is urgently needed as the basis of trading.

Fortunately, the rapid development of science and technology has brought hope to this longing of human beings. In 2008, Satoshi Nakamoto wrote a white paper on Bitcoin in combination with the wisdom of predecessors, proposing a peer-to-peer cash payment system and bringing block-chain as its technical basis into the public's vision. Moreover, the peer-to-peer, decentralized and non-tampered mode of payment makes it possible to avoid the drawbacks of centralized transaction modes. Instead of being issued by any monetary institution, Bitcoin can only be generated through a large number of calculations on the basis of a specific algorithm, and there are many nodes in the whole P2P network to confirm and record all transactions. In this way, no one can manufacture and issue a large number of currencies and each Bitcoin user can calculate and confirm every transaction. Finally, this perfect decentralized transaction mode has catapulted Bitcoin to stardom. However, the acquisition of Bitcoin has become a game of a few "old miners" after a period of development, while a new "miner" cannot compare with it in terms of economy

or experience. This violates the definition of decentralization. Some nodes cannot be selected as the center, while only a few earlier nodes can become the center. As a result, Bitcoin has been become a game such as the stronger can keep strong and stronger constantly, in which the strong can easily occupy global wealth, even change the game rules through their absolute dominance of hash rate.

Although Bitcoin is not perfect in building a decentralized consensus system, the block-chain as its technological base has left us with clues to solve the problem. On the one hand, block-chain is a distributed database of growing data records and there is no central node, so that all information can be sent, edited and stored peer-to-peer; On the other hand, the data interaction relies on a fixed algorithm and correlate with all data previously written through cryptography technology, thus making it difficult for the owner of a single node to tamper. To some extent, block-chain technology makes it possible to establish an open and transparent consensus mechanism for transaction, no longer relying on the traditional credit system. If it can be applied in the fields, such as financial business, entertainment culture and intellectual property, etc., we will have the chance to experience the social trend brought by block-chain, thus fundamentally breaking through the bottleneck of modern human civilization development and restarting the rapid development of human society, economy and civilization. Furthermore, the implementation of block-chain technology is an innovation revolution worthy of attention and constant exploration and practice by all mankind. As everyone knows that finance is the blood of survival and development of human society, and crypto-currency is an emerging medium of value delivery, both of which are obviously the places of strategic importance for the tide players of the times.

According to the basic concepts of decentralized, peer-to-peer and non-tampered block-chain, we created “Domain”, which has the most fair and advanced issuance mechanism to date, and can exert the power of consensus to the utmost. In the system of Domain, capital will become pale and weak, while no one and no institution can control Domain. It will continue to operate in

accordance with the established mechanism. In the world of Domain, talent is the embodiment of value. Each person who has a consensus on Domain will successfully get a private domain. Finally, the consensus of countless private domains will build a brand new, fair and bright future Domain.

We all know that the Internet of Information has accelerated the digitization of global financial assets. But in this process, people are constrained by the opacity of centralized institutions and the limitation of Internet technology. At present, asset security and crisis of confidence have become the biggest threat to personal assets. As a brand-new crypto-currency, Domain actively solves the global crisis of confidence with block-chain technology and devotes itself to redefining trust, creating a transparent and stable value Internet, and opening up a way for the safety of human assets. If the emergence of Bitcoin is an innovation, then the birth of Domain will be the singularity during the development of the whole human society. From now on, you will have the opportunity to hold the key to open the future world with us.

Catalogue

1. Project Background

1.1 Current social situation -- breaking faith of fiat currency

It is well known that the US subprime mortgage crisis triggered Wall Street Storm in 2008, and then the economic crisis swept the world, still with a certain impact until now. In the face of a series of economic recovery actions by the Federal Reserve, people gradually realized that the bankruptcy of fiat currency credit is almost inevitable under the conditions of market economy. Actually, during the financial crisis occurred in Roosevelt era in 1929, President Roosevelt banned the exchange of private gold to US dollars, and issued the decree of only promising the exchange of gold to US dollars for foreign governments. And in the 1970s, President Nixon completely abolished the exchange between gold and US dollar, thus initially showing the policy of completely abandoning the gold standard. Among the two official defaults in the history of the birth of US dollar, one was against the American people, and the other was against the people of the world. Such actions could alleviate the US financial crisis for a while, but in the long run, it implied that the fiat currency credit would certainly go bankrupt at some point. Unlike the people's helplessness for official defaults against US dollar in the previous two financial crises, the concept of Bitcoin was proposed in 2008 and emerged in 2009, meaning that there would be always a group of forward-thinking and intelligent people who were eager to find a method in mechanism for dealing with the breaking faith of fiat currency.

1.2 Current situation of industry

1.2.1 Current situation of Bitcoin

Undoubtedly, the birth of Bitcoin is a singularity during the development of human society and economy, which is characterized by a peer-to-peer trading system that does not require a third party, an irreversible transaction, the transaction result that can never be tampered with and the

electronic cash that will never increase issuance. It is nine years old now, while the first-mover advantage of early participants has gradually formed an insurmountable gap that the latecomers cannot surpass it easily. In addition, Bitcoin has been completely controlled by institutions and capital and become a highly controllable financial product that can continuously generate revenues due to the intervention of various capitals in recent years. It cannot be denied that Bitcoin, a product born in 2008, is almost perfect as of today. But as mentioned in the preface, the dark hour will come to mankind in case of replacing the global fiat currency with Bitcoin.

1.2.2 Collapse of the consensus system

If you are just holding Bitcoin to rise, it can still be barely understood as a kind of consensus. However, the speculators have been no longer content to be mere holders for a long time, so they made thousands of projects emerge in the name of decentralization. Even just having a glance at these projects, you will find how the concept is outrageous, how the logic is chaotic, how the temptation is huge and how the means is ridiculous. But amazingly, these projects can still attract a large number of investors. Actually, the concentration of chips in these projects and the high degree of control by dealers are contrary to the concept of decentralization, so where is the consensus for investors entering at different stages? The whole industry has been plagued by block-chain projects one after another, while most investors are very miserable. Moreover, the contract product has faintly become the prevailing trend in the market, the high unit price of Bitcoin inevitably makes people feel short of staying power, the successive but flashy projects are constantly consuming the remaining patience of investors, and the freshly injected blood is obviously insufficient. As a result, this must be a disaster for both Bitcoin and block-chain, while there will be no hope to establish a consensus system if it goes on like this. So how long this industry last can last if there is no new product to reverse the industry trend and no pure innovation project that shapes value with consensus to change the situation?

2. Project Introduction

2.1 Domain brief

Based on the block-chain technology and the basic principles of fairness and universal benefit, we created a value Internet with people's consensus as the only standard by taking the decentralized anonymity as the design concept and combining with the advantages of Bitcoin and ETH in the issuance and operation. As a result, people and countries of any color can build a consensus and create values through this value Internet. Moreover, we always believe that the manifestation of value is originated from consensus and being prosperous from co-governance and honorable due to sharing. We call this absolutely fair and consensus-based value Internet system "Domain".

It is a sustainable process to issue Domain, while consensus is the only condition for the generation of DM. Those who become the consensus person of domain will have fair conditions of acquiring DM. The value of Domain will depend on the quantity and quality of consensus population, and its issuance mechanism has completely killed the possibility of large capital gains from the beginning of its design, rejecting speculation at any time.

Domain will put all the DM into the public domain mining pool, while each participating consensus person will receive his/her private domain mining pool from the public domain mining pool. All DM will be mined from the private domain mining pool with the dual-consensus mechanism of POS and POW, with 50% to be permanently destructed.

First of all, Domain provides the consensus persons with a decentralized OTC trading system that supports fiat currencies and mainstream digital currencies; Second, we set a the price limit

trading rule of up or down less than 1% in a single day to prevent speculators from affecting the operation of the whole Domain and causing the consensus persons to panic, and to eliminate the possibility of capital intervention; Third, when there is a certain number of consensus persons, Domain will become an absolutely reliable credit granting platform based on pledge for consensus. At this moment, Domain ecological empire will be opened.

- Peer-to-peer loan service among consensus nodes based on pledge
- Global trade exchange settlement system based on pledge
- Create the strongest public chain ecology in the world based on the strong consensus.

Domain is a consensus area jointly created by consensus persons based on the starting point of consensus, co-construction, co-governance and sharing, which is generated and grows only by consensus, with nothing to do with region, nationality, skin color and country. It spans both space and time. The consensus person of Domain is also the forerunner of the future world, while Domain will become the absolute master of the future world together with its consensus person.

2.2 Project philosophy

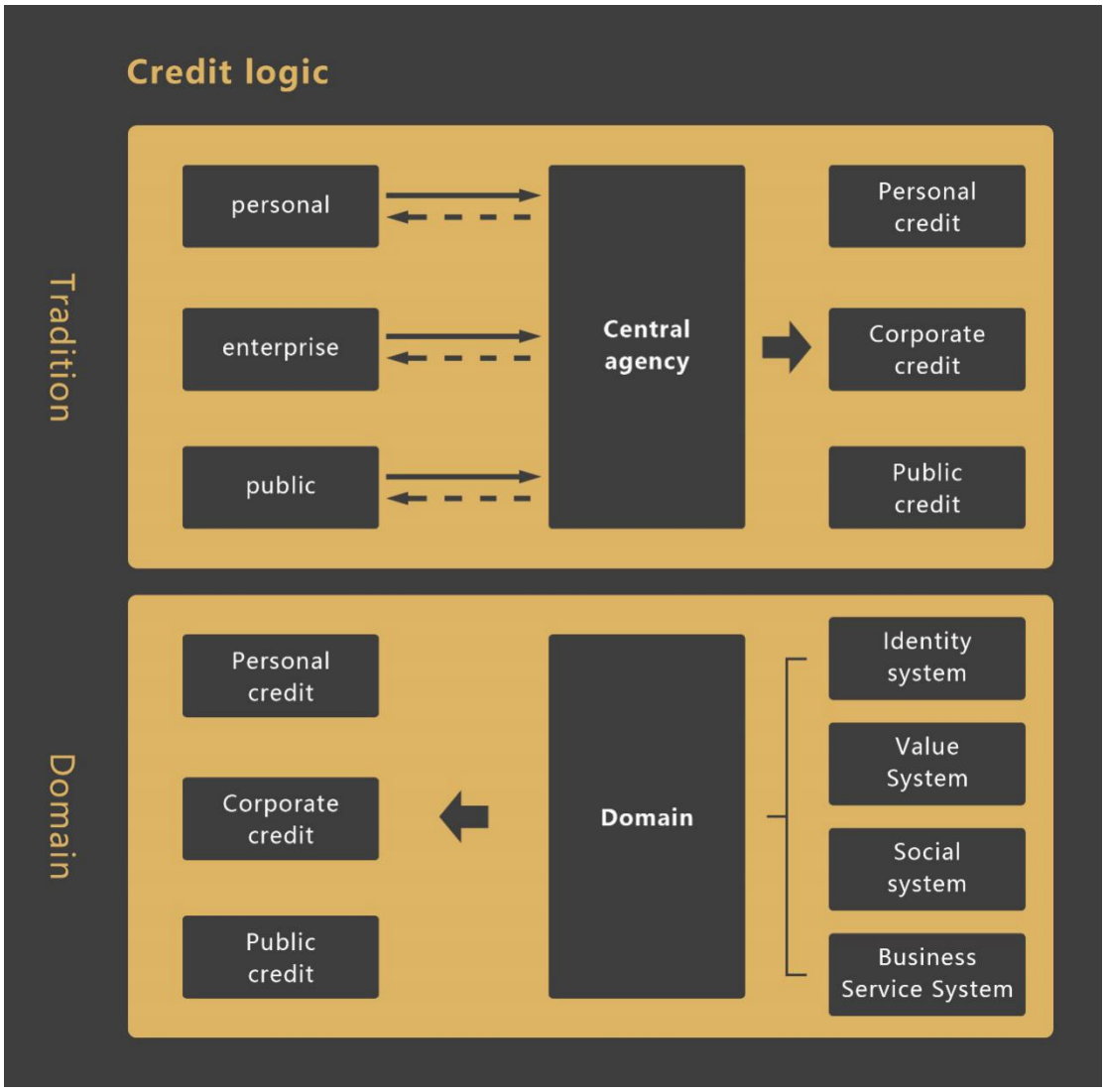
Domain aims to create a decentralized and absolutely fair value Internet that everyone can participate in. Based on the unique issuance mechanism, Domain creates the most reliable personal credit granting platform and develops a series of business ecology based on credit granting, thus making an asset play its value multiple times while maintaining value and increasing income. Meanwhile, an absolutely fair mechanism can allow Domain to accept more consensus persons in the world. Domain will become the key to enter the future world and the trading medium with the most consensus basis in the four-dimensional world.

2.2.1 Redefinition of trust

During the development of human civilization, the problem of lacking trust has been particularly prominent all the time, while the trust system of modern society has been on the verge of collapse and in crisis. Moreover, such crisis has caused impact between institutions, between institutions and individuals, and between individuals. As a result, the more progress a society makes the less trust it has. The unlimited printing of money by central banks of various countries has made us lose trust in centralized institutions, so some people attempt to improve this situation with Bitcoin. Followers all yearn for the day when Bitcoin is used to benchmark the sum of global wealth. However, the mechanism of Bitcoin determines it to be a game of the strong who can keep strong constantly, in which the strong can easily occupy global wealth, even change the game rules through their absolute dominance of hash rate. Then, some people attempt to use the previous business performance records to judge the credibility of institution or individual. But everyone knows that even if the coin flips heads 100 times, but what about at 101st time? Of course, the answer is no. In the logic of probability, no matter how many times you flip a coin and when you flip it, there's a 50% chance that it will come up heads or tails. So no matter how perfect the previous performance record of this institution or individual is, it cannot ensure that it will perform in the future.

But in consensus world of Domain, we only judge whether the consensus person has sufficient performance ability according to the number of DMs in his private domain mining pool for participation in mining. Certainly, we will also provide the credit granting of his number of DMs to the third-party institution or individual. Therefore, performance is inevitable in the Domain ecology, rather than a matter of probability, regardless of the objective environment. In a word, in the Domain world, how much credit you have depends only on the assets in your private domain mining pool, and having nothing to do with anything else. Therefore, our consensus persons can indirectly obtain Domain's absolute guarantee of the consensus persons' credit while

constantly participating in mining in Domain world.



2.2.2 Token of the future world

At the beginning, Domain was designed based on the concept of fairness, justice and openness. We will never allow any organization or individual to dominate Domain, with the same effect on the initiator. Moreover, we believe that no one in the world can own more than 1,000 DMs. This is not to question the power of capital, but we have not granted any right to Domains with more than 1,000 DMs. In other words, the parts exceeding 1,000 DMs cannot generate any

value in the Domain world. Our philosophy is that making Domain becomes the token of the future world and owning Domain is a necessary condition for you to do business or live in the future society. Instead of lacking a leader, this society lacks a fair dominant mechanism that allows most people to participate in.

Owning Domain will become a prerequisite for your all social activities in the future society, so at that time you will not be able to prove your good credit to a social participant from different civilization and different dimension with your credit card record. The number of assets in your private mining pool is the basic condition for consensus building. Maybe you feel that the vision of the future society is far from you, but this will soon form a basic consensus in the early Domain consensus groups.

We will encourage the consensus persons of Domain to jointly establish a new commercial institution that can subvert the tradition. Because it is jointly established by consensus persons, the assets in their private domain mining pools will be a strong endorsement of the credit and strength of this institution, and all the consensus persons in the Domain world will be its first customers. Under the premise of exercising power and sharing benefits together, different consensus person will play different role in the institution.

2.2.3 Magician for the reconstruction of wealth order

During the development of human society, the refresh rate of your cognition will determine whether you can enter the first echelon of wealth. With less cognition, you will inevitably pay for it. Then, the global wealth order will be reconstructed in the event that most people have to pay for cognition. The same is true in the Domain world. Even if we try to balance the input-return ratio of early participants and later participants with mechanism, it is certain that the entry barrier of later participants will be several times that of early participants. After all, the time is one of the

variables. Therefore, with the increase in the number of Domain consensus persons, the wealth order will be reconstructed and the 28 principles that have dominated human society for thousands of years will be rewritten.

But in the Domain world, there is a second variable, namely, human nature. It can make the process of reconstructing wealth order as changing and elusive as a magic. The issuance mechanism of Domain is absolutely deflationary, keeping demand exceeding supply. Hence, the consensus persons will always face the choice of keeping on moving or giving up whenever they participate in Domain, without the third choice. Actually, it is a cruel process that some consensus persons must give up to support those who choose keeping on moving, but it is also necessary. Furthermore, those who choose to give up can rejoin Domain at any time, while the investment will be multiplied by the variable of time, which is several times that of the early days.

No one in the world will cherish items at his fingertips, so perseverance will become meaningless you if there is no price to pay for giving up. In the Domain world, no DM is generated for no reason, while the new consensus power join each time DM is generated. The two triangular models of the absolute deflation of DM and the absolute deflation of the number of people and demand determine the Domain market in which demand exceeds supply. It can be said that each consensus person who can complete power confirmation is the lucky one chosen by God, and the elimination of each consensus person will support those who choose keeping on moving.

3. Issuance Mechanism of Domain

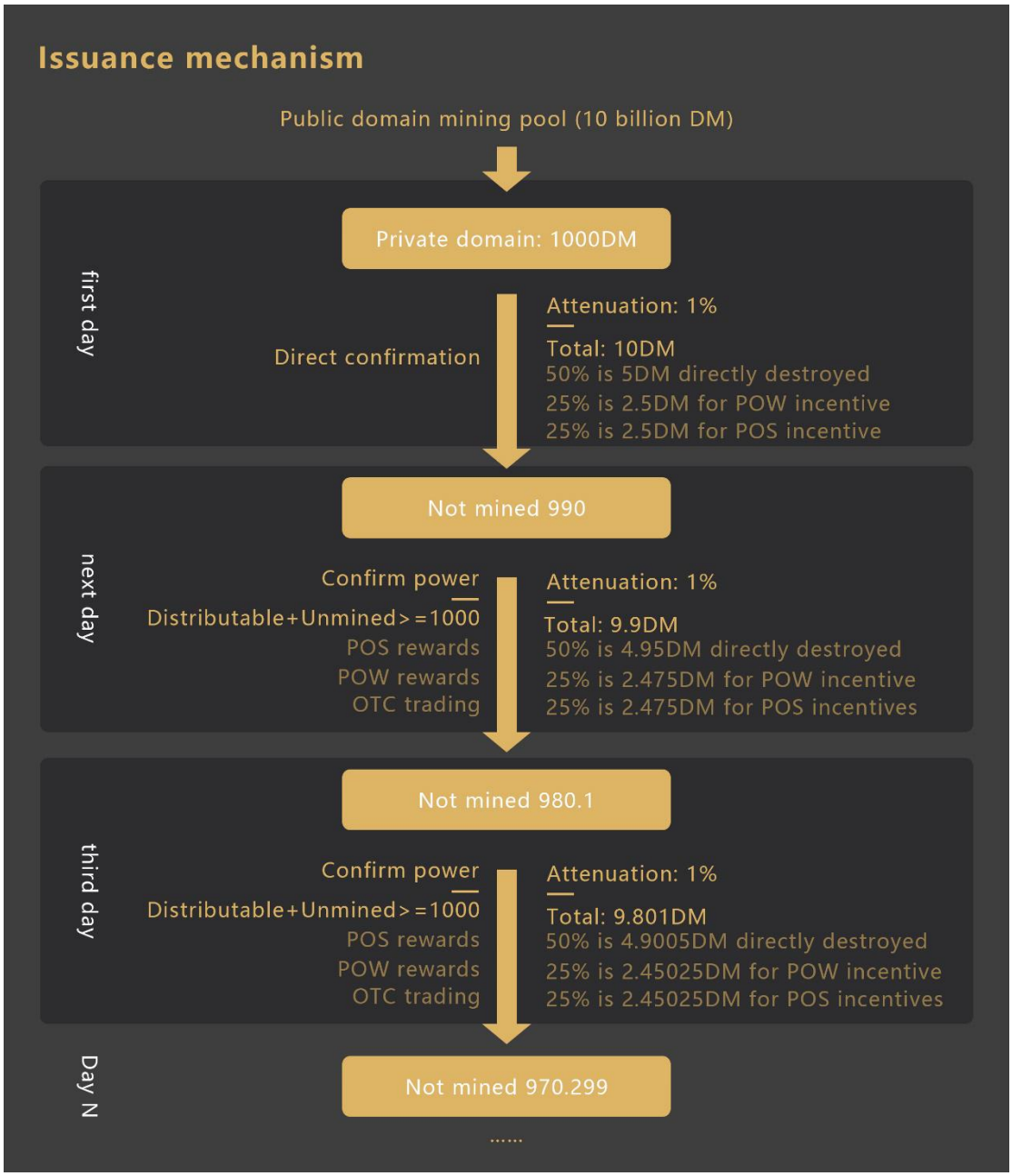
3.1 Issuance mechanism of DM

There are a total of 10 billion DMs to be put into the public domain mining pool of Domain. Each time a consensus person joins, the public domain mining pool will put DM into his private domain mining pool, and then it is generated by means of mining through POW or POS. And in the initial period, Domain will pre-mine 100,000 DMs for market circulation and set up 200 TOP accounts, with each account holding a quota of 100,000 DMs.

The first day

When issuing DM, all consensus participants will receive a private domain mining pool with 1000 DMs to be mined before the first power confirmation in the whole network. Participants on the first day can complete the power confirmation without any operation. All private domain mining pools with successful power confirmation will be attenuated by 1%. Among them, 50% of the attenuated DMs will be permanently destroyed, 25% will be used for POS mining rewards and 25% will be used for POW mining rewards. At this moment, the residual number of DMs to be

mined in the private domain mining pools of all participants on the first day will be 990. (1000 - 1000×1% = 990).



The second day

After the attenuation on the first day, there are 990 DMs to be mined in all private mining pools of consensus persons. At this moment, the newly joined consensus persons can only receive a private domain mining pool with 1000 DMs to be mined. The power confirmation of the consensus person's private domain mining pool can be completed when the sum of DM number to be mined in the private domain mining pool and the tradable DM number is greater than or equal to 1000.

But in order to complete the power confirmation, this round of consensus persons are required to obtain no less than 10 tradable DMs through the methods, such as OTC transaction, POS and POW rewards on the first day, etc.

All private domain mining pools with successful power confirmation will be attenuated by 1%. Among them, 50% of the attenuated DMs will be permanently destroyed, 25% will be used for POS mining rewards and 25% will be used for POW mining rewards. At this moment, the residual number of DMs to be mined in the private domain mining pools of all participants on the first day will be 980.1. (990 - 990×1% = 980.1)

The third day

After the attenuation on the day before, there are 980.1 DMs to be mined in all private mining pools of consensus persons. At this moment, the newly joined consensus persons can only receive a private domain mining pool with 980.1 DMs to be mined. The power confirmation of the consensus person's private domain mining pool can be completed when the sum of DM number to be mined in the private domain mining pool and the tradable DM number is greater than or equal to 1000.But in order to complete the power confirmation, this round of consensus persons are

required to obtain no less than 19.9 tradable DMs through the methods, such as OTC transaction, POS and POW rewards in the first two times, etc.

All private domain mining pools with successful power confirmation will be attenuated by 1%. Among them, 50% of the attenuated DMs will be permanently destroyed, 25% will be used for POS mining rewards and 25% will be used for POW mining rewards. At this moment, the residual number of DMs to be mined in the private domain mining pools of all participants on the first day will be 970.299. (980.1 - 980.1×1% = 970.299)

By analogy, each time the consensus person completes the power confirmation, the DMs to be mined in the private domain mining pool will be attenuated by 1%.When there are less than 950 DMs to be mined in the private domain mining pool of the first batch of consensus persons, all newly joined consensus persons will receive a private domain mining pool with 950 DMs to be mined, with the same attenuation rule.

3.2 Pre-mining

The absolute deflation issuance mechanism of Domain is one of the fundamental reasons for ensuring its long-term running, but it will also cause some early Domain users to fail to obtain DM for power confirmation. For this reason, Domain system will pre-mine 100,000 DMs from the public domain mining pool and put them into the market through OTC transaction in the Domain network, so as to run the project better in the early stage and allow more early participants to conduct power confirmation and get return. For the sales of DMs in this part, the individual can only purchase 50 DMs at a unit price of 1 USDT. Through the pricing below the market and the setting of limited purchase, it will ensure that DM can be put into the market correctly.

3.3 Eight advantages of the issuance mechanism of DM

Absolute deflation issuance mechanism

The issuance process of DM coincides with its destruction process, while the generation of each DM is accompanied by the permanent destruction of another DM.

Scarcity throughout

The issuance mechanism of DM determines that the generation of each DM will generate a new round of consensus, while each round of new consensus will create twice as much demand as the generation of DM in the last round. Moreover, there will be more and more new consensus persons to join, so DM will always be popular.

Low participation barrier from scratch

On the first day of issuing DM, all consensus persons can participate in Domain at a cost of 0 and receive token rewards. Even after Domain runs for a period of time, we will adjust its participation barrier to only 50 tradable DMs, which is better than 90% of block-chain products on the market. Furthermore, the lower barrier allows Domain to get more consensus persons more quickly, thus ensuring that the value of Domain will rise steadily.

Absolutely free retention mechanism

Domain does not set any coercive measures for all participants. At any time, the consensus persons can freely determine whether or not to continue to participate in Domain. Unlike other block-chain products, Domain participants can take away total investment and profits (after deducting service charge) through OTC transaction system at any time when they leave.

Super high consensus stickiness brought by high rate of return

Each consensus person will receive a super high POS mining reward for each power confirmation. POS mining reward is calculated and equally distribute to each DM, so that the consensus person can get high reward steadily in case of contiguous power confirmation. Moreover, the phasic power confirmation reward can motivate the consensus persons to continue to complete the power confirmation. In order to prevent excessive speculation and capital control, Domain has set a price limit trading rule of up or down less than 1% in OTC transaction, but the long-term and stable currency price increase can make the consensus persons of Domain obtain the increase in value brought by the steady rise of currency value while enjoying the increase in the number of DM in the process of mining.

Scientific cost structure

According to the issuance mechanism of DM, the consensus persons should participate in the transaction to complete power confirmation every day. With the increase in the value of DM, the actual cost of holding coins will gradually increase, while only the holding cost structure infinitely close to the current price can ensure a stable rising of the DM value. Since the tradable DM with POS exceeding 1000 is not counted in the scope of equity calculation, even the consensus persons who have obtained a lot of DMs through POW mining rewards in the early days will sell them through OTC in a timely manner. Therefore, the situation that a large number of low-cost chips hit the market in the early days will never appear.

No pain, no gain

In the Domain world, no pain no gain. You can either purchase DM through OTC to complete power confirmation to earn POS mining rewards, or invite more consensus persons to expand the

consensus group to obtain POW mining rewards. Whenever you gain in Domain, you will be rewarded for your efforts.

Whenever you stop paying, there will be no returns in Domain. You can get returns only when paying again. Please remember that the value of DM at any time is from the contribution of all consensus persons, rather than pennies from the heaven.

Eliminate the possibility of any manipulation of Domain

Domain will publish the public domain mining pool address, permanent destruction pool address and service charge destruction pool address for supervision by consensus persons. All mechanisms are completely open and transparent; the same is true for initiators. The only way to obtain DM is mining through POS or POW. There is no exception to this principle.

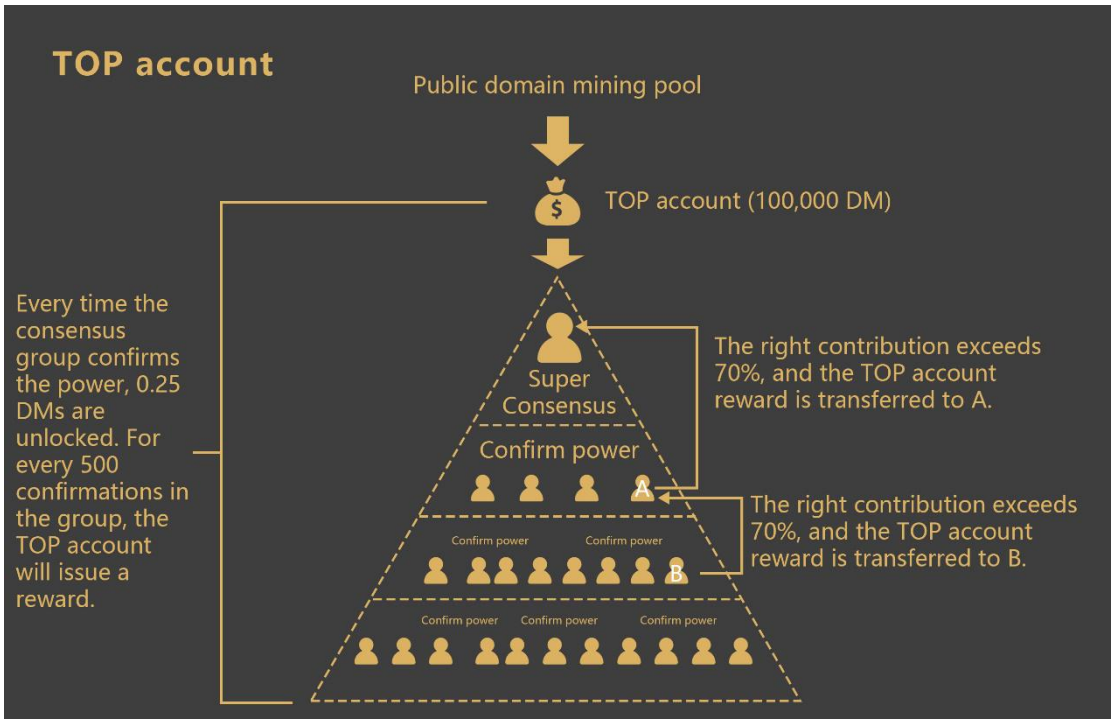
3.4 Service charge system

In the Domain world, the withdrawal fee is charged in a decreasing manner. All the fee incomes will be destructed and the destruction address will be published for joint supervision by all consensus persons. Each new consensus person should pay 25% of withdrawal fee, while the withdrawal fee will be reduced by 1% each time he completes power confirmation of the private domain mining pool. Until his withdrawal fee is reduced to 1%, it will stop reducing and maintain this withdrawal fee rate forever.

3.5 Reward mechanism of super consensus person's TOP account

In order to better promote Domain, we will openly recruit 200 super consensus persons from all over the world through our official website in advance. Each of them will receive a TOP

account with 100,000 DMs injected by the public domain mining pool. Moreover, every time the member in the consensus group formed by super consensus persons confirms the power, additional 0.25 DMs rewards will be given to the super consensus persons in addition to the normal POW mining rewards. For every 1000 DMs in the TOP account rewards, it will be deducted from the balance of TOP account reward.



In order to ensure that the consensus person who has truly made outstanding contributions to the promotion of Domain can receive more rewards, Domain will evaluate the situation of the consensus group compose of those who directly join through the sharing of this super consensus person each time the TOP reward is issued. If more than 70% of the 125 DM rewards of this super consensus person are generated by the contribution of a consensus person in the consensus group, we will cancel the identity of this super consensus person and transfer the remaining rewards to the consensus person who has truly made outstanding contributions to Domain.

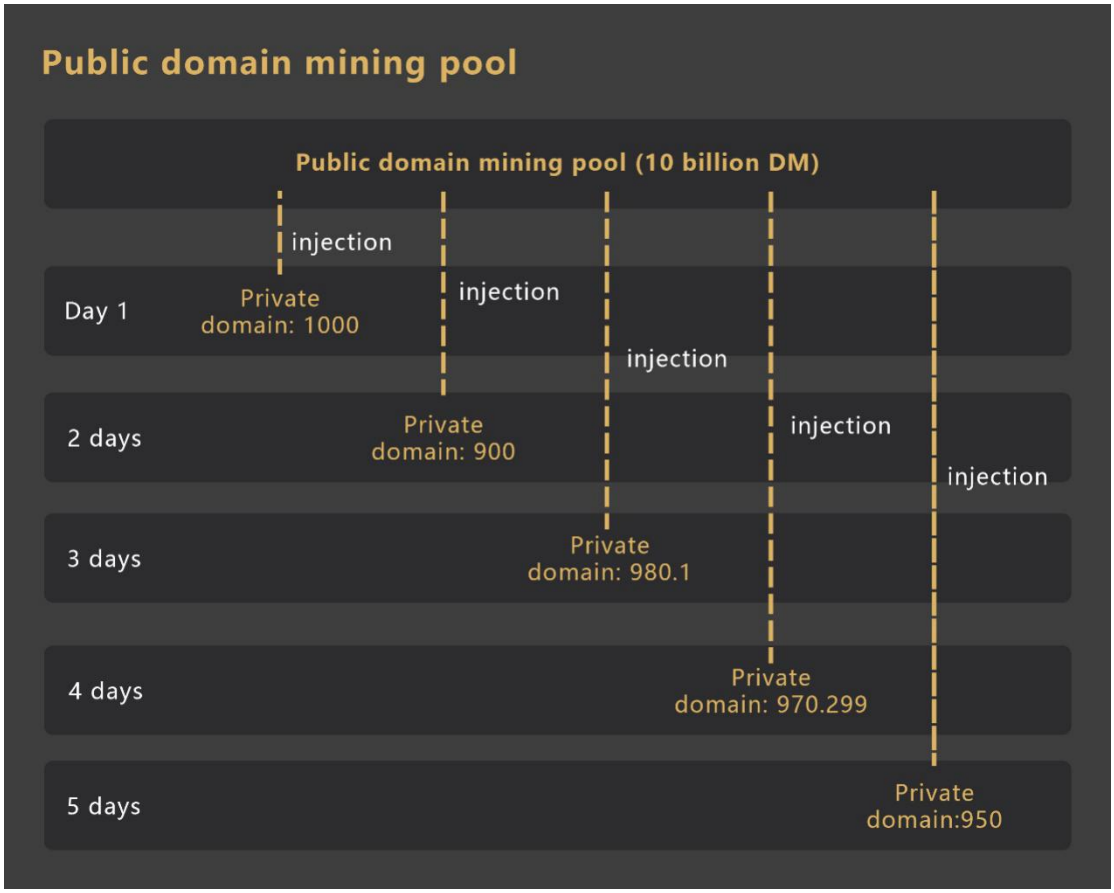
4. Interpretation of Terms

Domain token

The network token Domain is DM, which is the reward obtained by all consensus persons who participant in Domain and the only tradable token in the whole Domain.

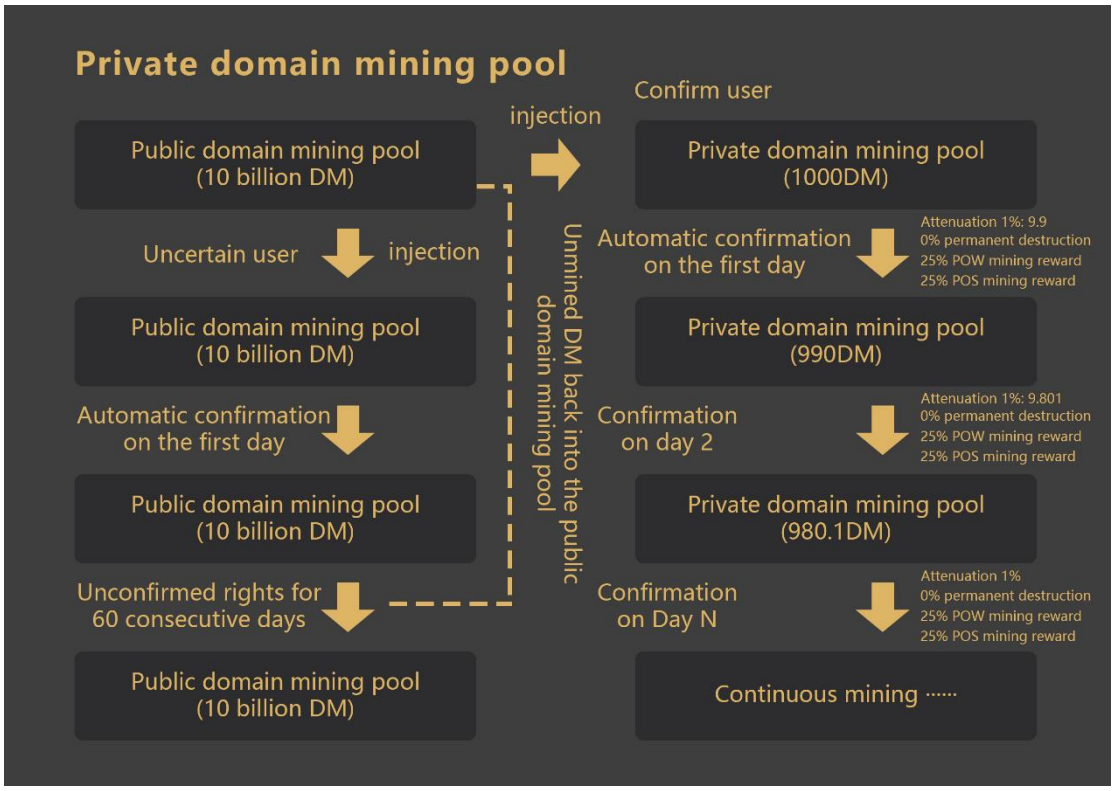
Public domain mining pool

The public domain mining pool will be responsible for storing all unmined DMs and injecting a certain amount of unmined DMs into the qualified private domain mining pools. The number of DMs in the public domain mining pool will decrease as DMs are put into more private domain mining pools, until all DMs are put into the private domain mining pools of consensus persons. In addition, the public domain mining pool belongs to all consensus persons of Domain and is supervised by them.



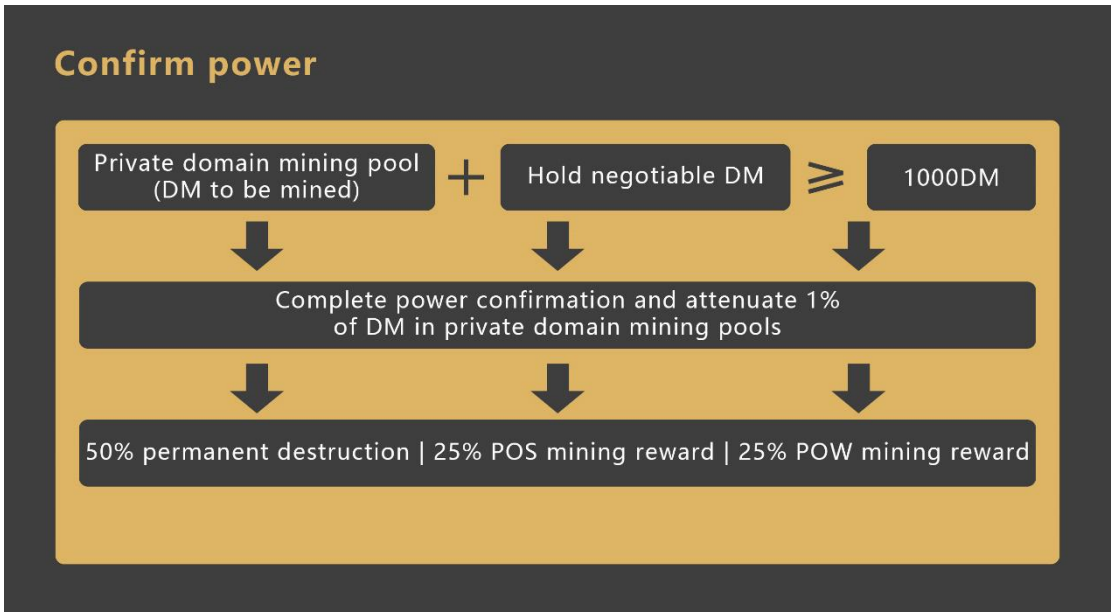
Private domain mining pool

The private domain mining pool is the consensus person's reservoir of DMs to be mined. In principle, all all DMs produced by POS mining come from the private domain mining pool of each consensus person. Every time the consensus person completes the power confirmation, 1% of the total remaining DMs in the private pool can be mined. For the mined DMs, 50% will be permanently destructed, 25% will be allocated for POS mining rewards and 25% will be allocated for POW mining rewards. All destructed DMs will disappear forever and the destruction address is supervised by all Domain consensus persons. If the consensus persons do not confirm the power for 60 consecutive days, the remaining unmined DMs in his private domain mining pool will be re-injected into the public domain mining pool.



Power confirmation

Power confirmation is a necessary condition for all consensus persons to get POS mining rewards. When the sum of the number of DMs to be mined in the private pool of the consensus person and the number of tradable DMs is greater than or equal to 1000, the “power confirmation” can be completed. After power confirmation, the consensus person will get POS mining rewards according to the number of tradable DMs held by him. Domain will take a snapshot of the consensus person’s account at a certain time, while it is deemed to be “power confirmation” when the result of snapshot meets the requirement of power confirmation.



POS mining reward

POS mining reward means that 25% of all mined DMs in the private domain mining pools that meet the requirement of power confirmation are equally rewarded to the DMs in the private domain mining pools that meet the requirement of power confirmation. The amount of POS mining rewards depends on the number of DMs held by the consensus person. If the sum of unmined DMs in the private pool of consensus persons and the tradable DMs is greater than 1000, the tradable DMs exceeding 1000 will not receive POS mining rewards.

$$f = (y * 25\%) * \frac{n}{m}$$

POS reward for a single node: f

The total DM of attenuation in the private domain mining pool after "authorization confirmation" of all nodes: y

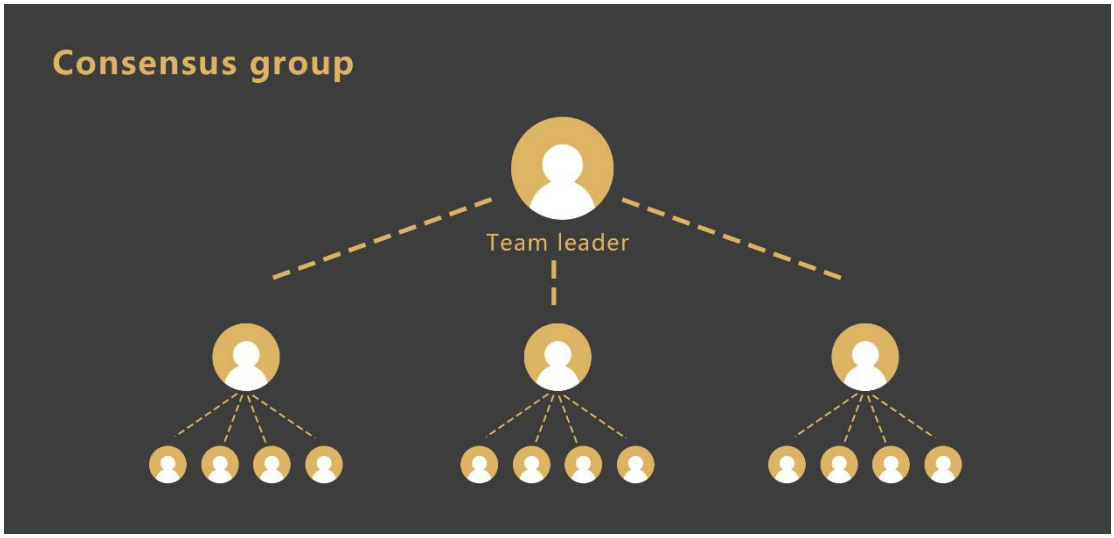
The total tradable DMs in the node account: n

The total tradable DMs of all consensus persons after authorization confirmation: m

(For example, when there are 1100 DMs in the private domain mining pool of consensus persons, including 900 DMs to be mined and 200 tradable DMs, the number of DMs used for participation in POS mining rewards by the consensus persons is only 100 (1000 - 900 = 100). That is, the additional 100 DMs cannot obtain POS mining rights, thus no rewards.)

Consensus group

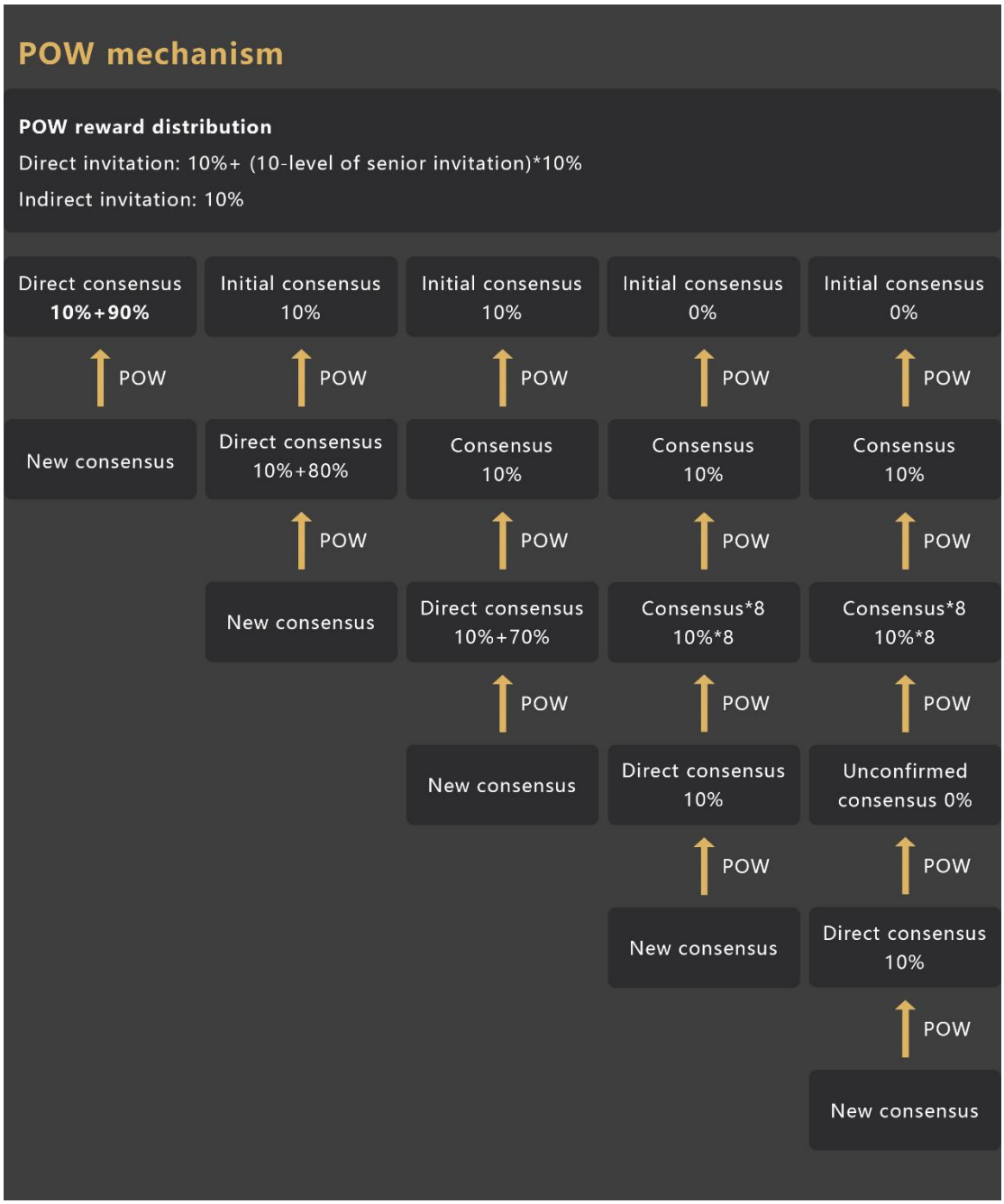
In the Domain world, each consensus person is obliged to share Domain. And then we will form a consensus group compose of you and all other consensus persons who joined Domain because of your sharing. After each member of your consensus group completes the power confirmation, Domain will help you get POW mining rewards. Certainly, you should help each member of your consensus group better understand Domain to constantly receive POW mining rewards.



POW mining reward

Domain will give you (the team leader) the DMs equivalent to 10% of POS mining reward obtained by the consensus group members as POW mining rewards. The primary condition to obtain POW mining reward is that the consensus person must complete the current power confirmation, while the number of consensus persons who are developed directly will determine the upper limit of POW revenues obtained by this consensus person.

POW mining rewards = number of POS mining rewards for a single consensus group * 10%



Phasic power confirmation reward

Each power confirmation by the consensus person is a promotion of Domain. Therefore, Domain will issue phasic power confirmation reward to those who have completed power

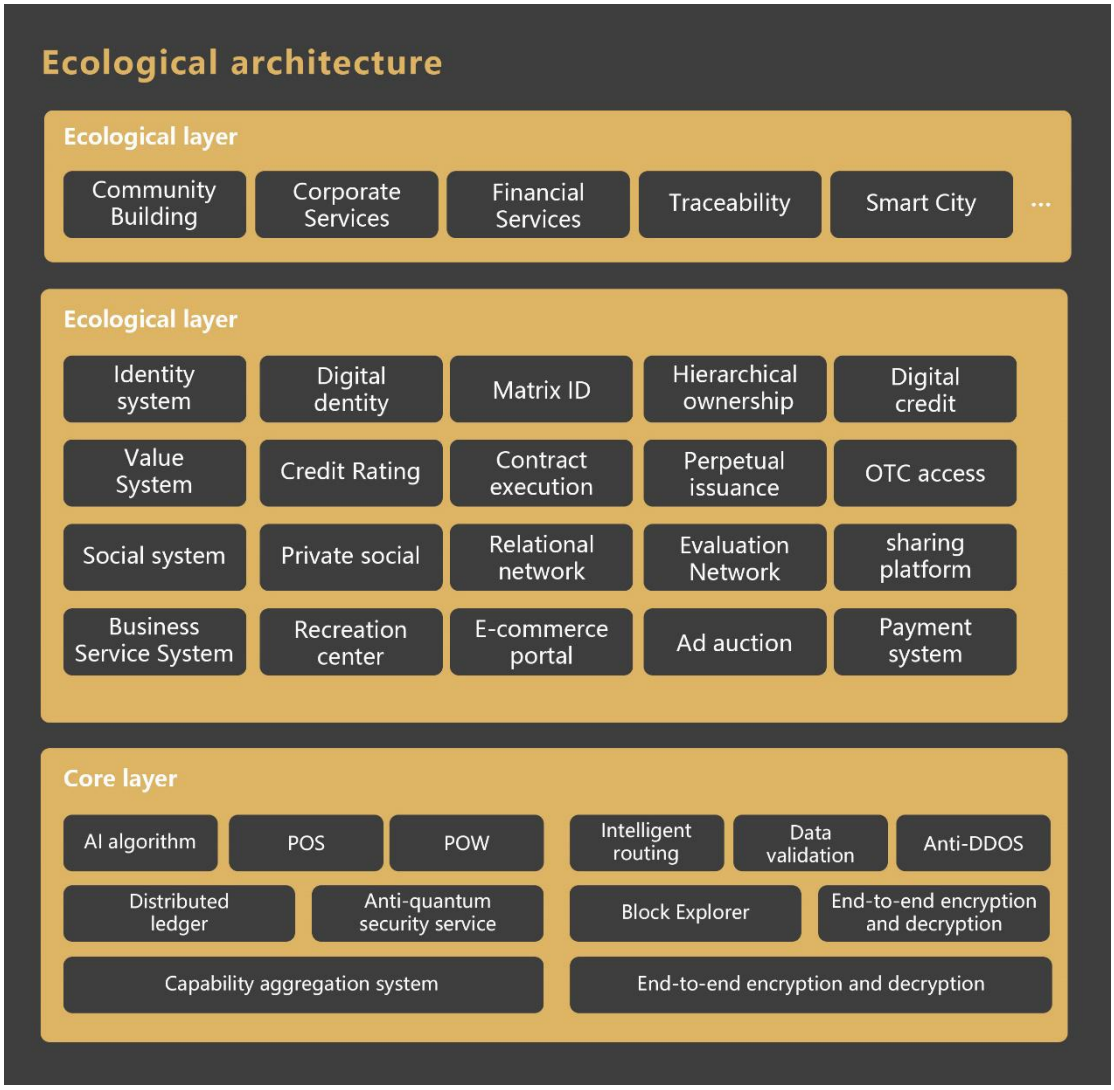
confirmation for certain times.

The reward criteria are as follows:

Number of power confirmation	Number of rewards (DMs)
5	5
15	10
35	20
N+20	20

5. Domain Ecology

Based on the foundation of opening source co-governance, Domain takes energy-gathering and co-construction as the means to construct the whole value Internet for future development. It includes three logical layers from bottom to top: core competence layer, platform service layer and ecological industry layer. The competence of each layer is logically coupled and complements each other, thus forming a multi-dimensional ecosystem in pursuit of win-win results and prosperity.

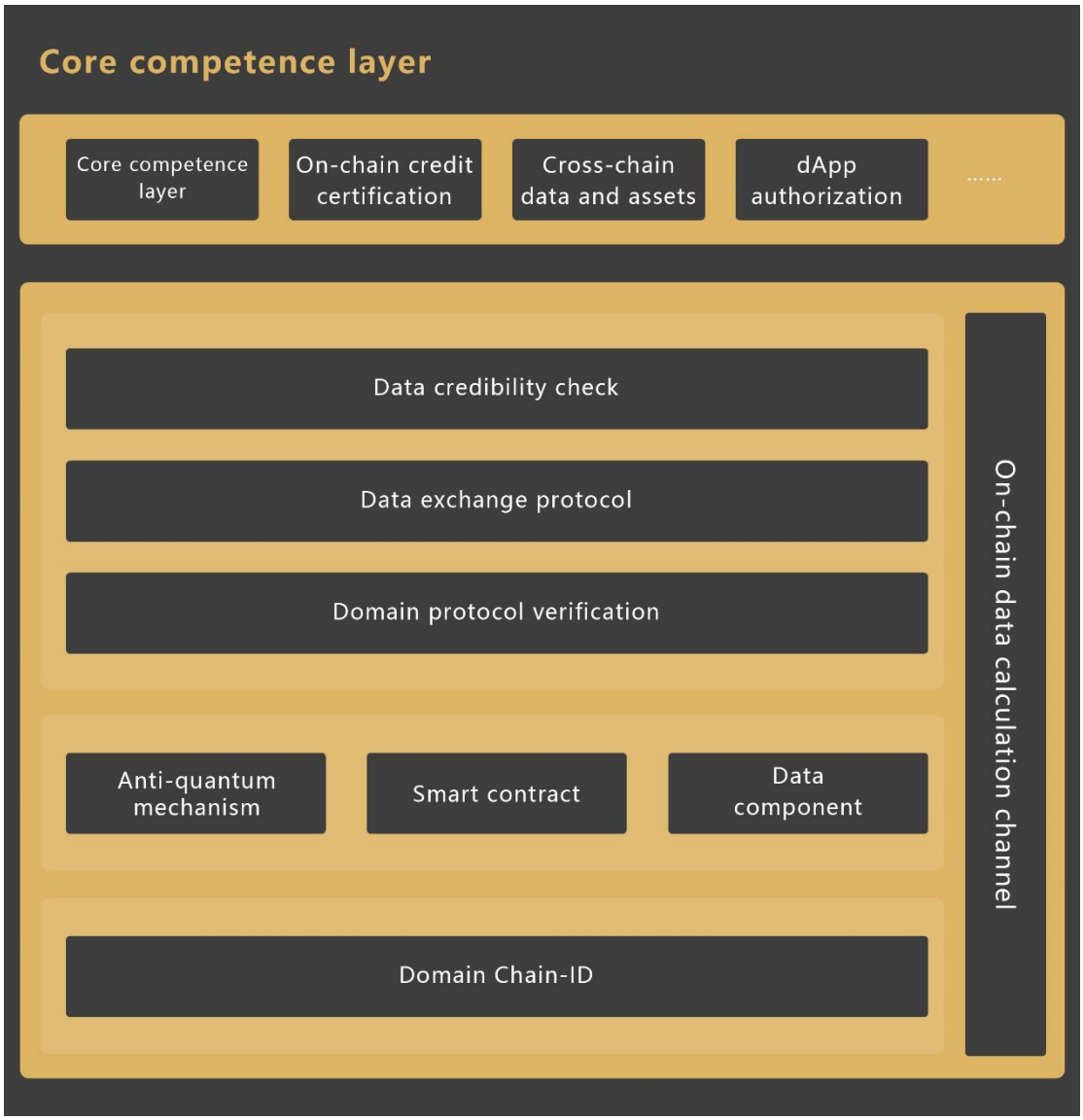


5.1 Core competence layer

All platform services of Domain are based on the construction of core competence layer. The core layer is designed to provide the best infrastructure and support means for the value Internet created by Domain. In addition to ensuring the basic elements, such as reasonable technology and consistent security, one of the main objectives pursued by the architecture is to make all resources and competences to be accessed and measured.

The purpose of competence aggregation system is to integrate the advanced technologies, such as AI, algorithm and hash rate, distributed data and anti-quantum security service, etc., into the competence system. In addition, it can be acquired and used with unified interface protocol in the development of platform. All basic competences are coordinated with data and status support tools, such as block data browser, operation status monitoring of each competence, network state, intelligent routing and resource management.

When building Domain block-chain architecture, the underlying technical logic follows the principle of system safety first and ensures that all operations cannot be tampered with, transactions are well documented, privacy protection is paramount and sensitive data is desensitized. At the application layer, the usage experience of ordinary users and developers is opened and improved to the greatest extent, and the system is scalable and adaptable.



5.2 Platform service layer

As an open platform for supporting the business development and operation collaboration of builders, the platform service layer can provide a convenient and high-performance block-chain construction environment and supporting services for all consensus person. The construction of platform layer includes six systems, including three basic systems: identity system, value system and collaborated system; and three major value-added systems: social contact system, security system and business system.

5.2.1 Identity system

n order to achieve the platform community expansion and the smooth information flow in Domain Value Internet, Domain establishes a digital identity for each individual in the ecosystem. It assigns the matrix ID and expands the hierarchical and grading ownership status on the unique identity key, and adds the verifiable social attribute and traceable digital credit investigation on the basis of digital identity. In addition, the identification guarantee is provided to individuals, enterprises, organizations, associations and even AI people, supporting them to participate in community co-governance as community members. The community member system includes many subsystems, such as identity system, credit investigation center and voting service, etc., which can fully satisfy the requirement of social people's free passage in the co-governance matrix digital community as a digital person.

5.2.2 Value system

Domain is designed to establish a decentralized value Internet through consensus, build a consensus identity system through the advantage of a sustainable DM issuance mechanism throughout the Domain Value Internet, and provide the individual of the third-party organization with fully true credit evaluation in accordance with the real DM assets held by consensus person. Such credit evaluation is different from those generated by conventional Internet based on the previous performance records. The credit evaluation of Domain is only generated based on the amount of consensus person's DM assets. As a result, breaking faith for any reason can be completely eliminated, and any commercial activity carried out in Domain Value Internet can be strictly executed in accordance with the agreement between both parties.

5.2.3 Social contact system

The social contact system of Domain mainly includes private social contact, relationship network, evaluation network and sharing platform. In view of the sensitivity of personal privacy,

an end-to-end encrypted data chat is built in combination with the natural advantages of block-chain technology applied to social contact platforms. Furthermore, all data will be stored in the free database controlled by the user, while the user has the right to decide how to process the data. By introducing distributed encryption technology and Micro-Cloud Service, the consensus persons can freely choose the information flow path, storage method and spreading scope, solve the information exchange in the process of community development, improve communication efficiency and weaken the trust of strangers.

5.2.4 Business service system

On the basis of the unique identity system in Domain, all consensus persons will provide commercial service, enjoy others' services and survive the fittest under the value and evaluation system. As the basic competence of Domain, the entertainment center, e-commerce portal and advertising bidding will be open to the community to create value and provide service docking for consensus persons.

5.3 Ecological industry layer

As the uppermost layer of Domain, ecological industry layer combines platform competences with various industry scenarios to achieve multiple value exchanges and ecological prosperity. On the one hand, it combines with the traditional industries to improve efficiency and survive the fittest; On the other hand, it meets the ecological environment of the same industry to complement each other's strengths and grow together.

In fact, the credit generation logic of the value Internet of Domain is like the real estate mortgage loan in the society currently. As everyone knows commercial banks take the borrower's house property as a risk mortgage and lend cash to the borrower to earn interest. In this way, the bank will return the house property if the borrower performs the repayment, and will

auction it to ensure the safety of the bank's principal and interest if the borrower fails to perform the repayment. It is a win-win business model. One the one hand, although the borrower mortgages the house property to the bank, he still have the right to use the house and get the incremental benefit and rental income generated by the house property. Moreover, the borrower receives a loan from the bank to solve the funding problem. On the other hand, the bank can greatly reduce the loan risk by the borrower's house property as a mortgage and earn the interest on funds.

Similarly, in the value Internet of Domain, any commercial activity should be carried out based on the number of consensus person's DMs. Domain will freeze the corresponding DMs according to the asset value involved in the consensus person's commercial activity, but the consensus person still enjoys POS and POW mining income brought by DM and the income of increased DM value. If the consensus person can fulfill the contract, Domain will unfreeze the frozen DMs, while if he cannot, Domain will transfer his DMs to the damaged party according to the content of smart contract.

Due to the characteristics of Domain: decentralized block-chain, inability to tamper with and low transaction cost, the credit identity is obtained through Domain and the credit evaluation is generated based on Domain. Besides, the efficient and low-cost business model executed through smart contract will be applied to various commercial activities of human beings, thus fundamentally solving the problem of high trust cost in the current society.

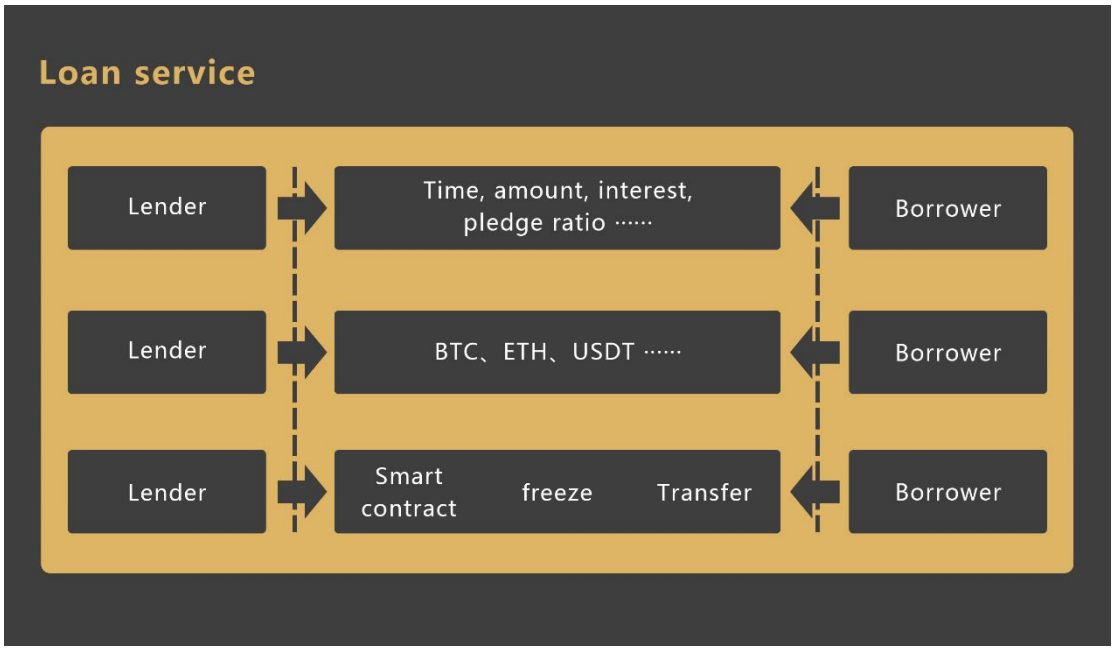
In terms of the architecture of ecological industry layer, Domain advocates open docking, strives to build an advanced and effective ecological access capability, serves various business forms participating in ecology, and completes the docking on the basis of identity system and value system. While sharing the competence service with the overall ecological environment, it

can also share other open capabilities of Domain ecosystem, so as to jointly promote the ecology and increase the value.

Based on the three major systems of Domain: identity, value and ecology, we will successively carry out the following ecological application demonstrations:

5.3.1 Loan service based on pledged DM

This service will be issued after the launch of Domain 2.0 Dapp version, aiming to solve the dilemma of consensus persons who have to face the difficulty of cash flow in life while wanting to stay in Domain for continuous mining to earn income. After the issuance of loan service, the consensus person can borrow the digital currencies, such as BTC and ETH, etc., so as to solve the problem of temporary funding difficulty by means of pledged DM while not affecting his income in Domain. Of course, the borrower is required to pay the lender an agreed amount of DM as interest. If the borrower fulfills the contract and repays the arrears and interest, Domain will unfreeze the borrower's DMs, while if the borrower fails to do that, Domain will transfer the frozen DMs of the borrower to the lender's account according to the pledge proportion and the agreed interest, thus ensuring that the lender's rights and interests will not suffer losses. All items, such as pledged loan proportion, loan time and loan interest, etc., shall be negotiated and established by the borrower and the lender. Domain shall be only responsible for the supervision and execution of the contents agreed by both parties.



5.3.2 Global trade exchange settlement system based on pledged DM

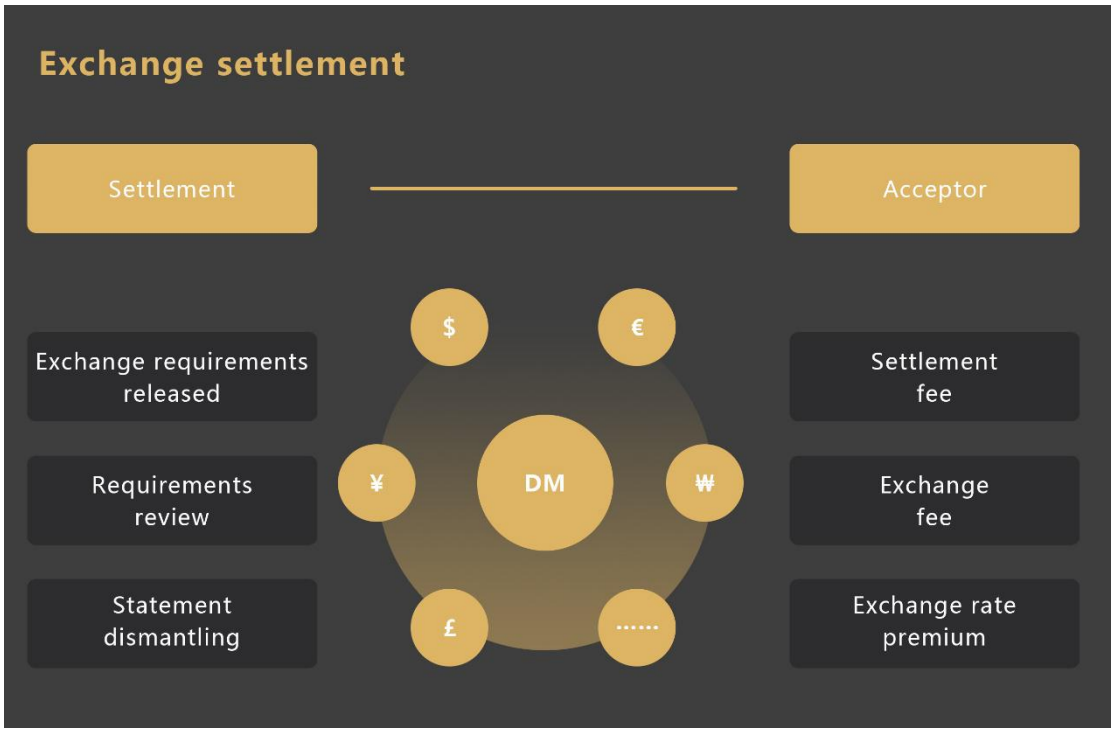
Because of the independent fiat currency system in each country and different foreign exchange control policies in different countries, high rates and low efficiency are very common in global trade settlement, resulting in a lot of resentment. Later, Bitcoin is used as a settlement currency in some cross-border trades after its birth, but the extremely unstable price and large volatility makes it riskier to use Bitcoin as a settlement currency.

Fortunately, a global trade exchange settlement system based on pledged DM will be launched after the number of consensus persons and distribution area of Domain value Internet form a scale effect. The system can perfectly satisfy the diversified trade demands of using different fiat currencies in different countries. No matter whether the settlement demander understands or participates in the investment of block-chain digital assets and whether he is

consensus person of Domain, he can complete the global trade settlement through Domain with low cost and high efficiency.

At the scheduled time, each consensus person of Domain will become an acceptor of global trade settlement, while the acceptance capacity is determined by the number of DMs held by him. For too large single settlement amount, Domain will automatically dismantle the amount and find more qualified consensus persons to act as the acceptors together.

The settlement demander can customize the settlement requirements when releasing a task. For example, exchange the paid US dollars into the designated digital currency, and then transfer it to the address designated by acceptor, with the number of DMs that he is willing to pay for the settlement. After releasing, this task advertisement will be conveyed to all domain consensus persons who meet the requirements in an instant, and then the one who completes the task first will earn the reward for this task.



5.3.3 Creation of the strongest public chain ecology in the world based on a strong consensus

It is well known that traffic is power and user is “God” in the era of mobile Internet. Therefore, you will have users after mastering traffic, and may have it all after having users.

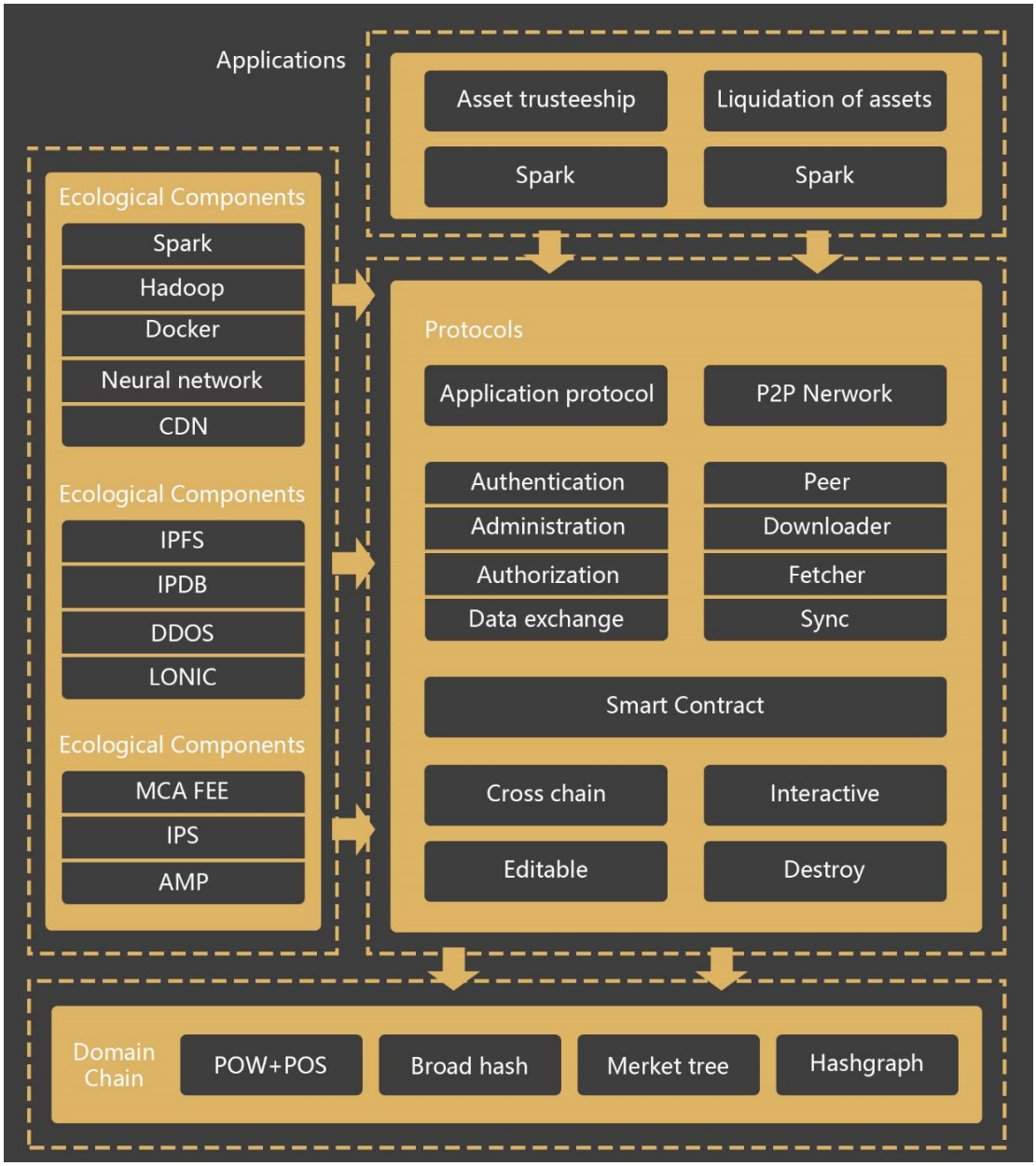
The same is true in the value Internet world built through block-chain technology. Only with the basic traffic, good innovations, good applications and good public chains can produce value and get better development.

Domain will generously output the traffic for all block-chain applications and side chains developed on the Domain public chain, and all consensus persons of Domain will jointly promote the excellent applications and projects. As a result, every valuable project can get the support of a

huge amount of traffic at the beginning, and can be implemented at the fastest speed. For high-quality projects, we can initiate crowdfunding through Domain to acquire the initial research and development funds by raising DMs. The consensus persons of Domain can reap a high payoff through the investment in superior block-chain projects.

In addition, Domain will take the strong consensus foundation to welcome the valuable block-chain application to develop based on Domain public chain with an open attitude, as well as guide all Domain consensus persons to promote it, thus jointly creating the safest, most convenient and most efficient world-class public chain with the riches application to date.

6. Technical Architecture

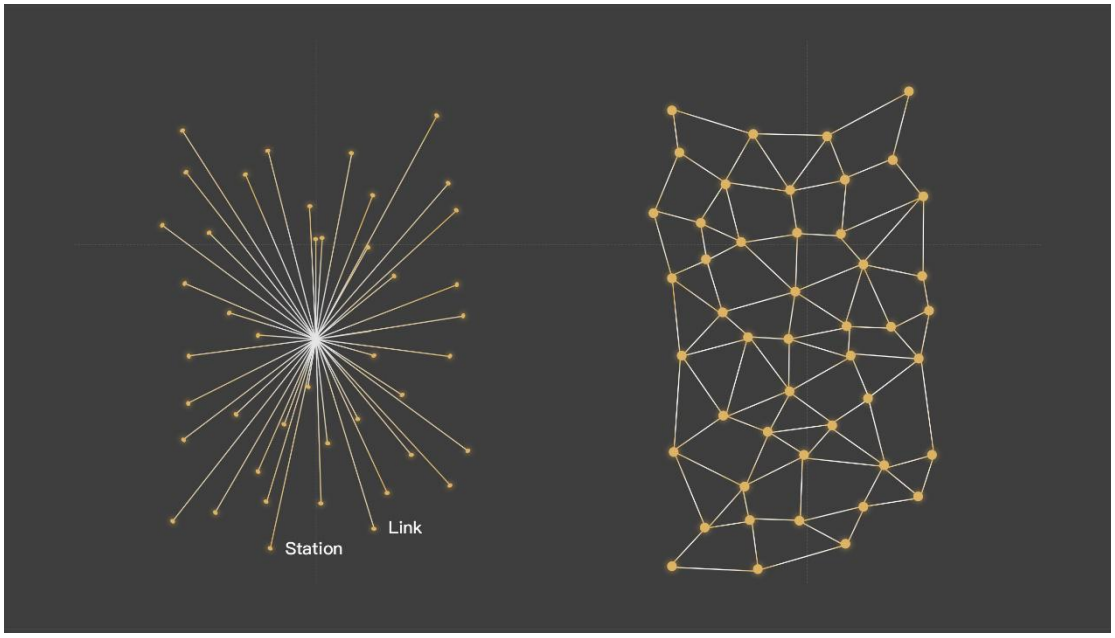


Domain is a value public chain with fairness and universal benefit as its basic design philosophy. On the one hand, it follows the principles of security, fairness, autonomy and decentralization in the construction of technical architecture. On the other hand, it guarantees that

all block data cannot be tampered with, transaction data can be documented, and privacy and security are paramount, so as to achieve the absolute safety, and stable and sustainable operation of the whole block-chain network. Its underlying system architecture includes network layer, consensus layer, data layer, contract layer and application layer.

6.1 Network layer

In the network layer of Domain, all data transmission, verification, block packaging, and security maintenance in the whole network are completed by 23 nodes. The nodes are interconnected to form a network, and each node has the functions of data transmission and verification. The functions of node are as follows: First of all, every two nodes are interconnected to form a loose network without a fixed topological structure through peer-to-peer; Second, each node has a flooding routing function to ensure that the information can be interacted and the blocks can be spread throughout the network; Third, the node has the function of verification, thus ensuring the correctness of the received data, and the correctness and reliability of network information; Fourth, Domain nodes can freely join or leave the block-chain system, without affecting the normal operation of block-chain; Fifth, the nodes of the whole network can be communicated equally, without passing through intermediate entities; Sixth, the node has the right to independently process the received data, and each node can independently verify all blocks and transactions.



Each node in the peer-to-peer network stores an interaction record pool and a copy of the block-chain. It can independently verify the validity of the received interaction records or blocks, and decide whether to retain the transaction blocks or not by itself. The verification is as shown in the following formula. In case of receiving information, it is put into the record pool or connected to the end of the block-chain, and then starts the new record collection or block mining.

$$Verify\ (\varepsilon,\ \vartheta,\ \phi,\ \delta)$$

Wherein, ε indicates the data structure of transaction or block; ϑ indicates whether the field value is within a reasonable range; φ indicates whether the corresponding relationship between the input and output in the transaction or block is correct; δ indicates whether the transaction or block has existed.

6.2 Consensus layer

The distributed database of Domain mainly adopts Paxos and Raft algorithm to solve the distributed consistency problem. These databases are jointly maintained by all credible nodes, and the algorithm supports Crash Fault-Tolerant (CFT). The decentralized block-chain is jointly managed and maintained by multiple parties, the network nodes of which can be provided by any party. Besides, Byzantine Fault-Tolerant (BFT) solution is adopted for processing due to some incredible nodes.

Assuming that there are at most f incredible nodes in the network compose of n nodes, Byzantine failures can be solved under the condition of n>=3f+1 for a reliable network with synchronous communication. But for asynchronous communication, Fischer, Lynch and Paterson prove that the mechanism of certainty and consensus cannot tolerate any node failure. The complexity of Federated Byzantine Agreement is reduced from exponential level to multiple levels, thus making it become optimal solution in the application of a distributed system.

Domain adopts “POW+POS” to realize block-chain accounting and data exchange, and achieve the consensus of nodes in the whole network through the proof of workload and the equity allocation mechanism. The workload proves that the rights and interests at evenly divided and fairness and universal benefit are achieved in the whole network by inviting more nodes to participate in the construction and maintenance of the block-chain network, thus encouraging more nodes to attend and achieve an equal division of distributed accounting right. Meanwhile, more tradable tokens will bring the early participants more equity divisions and enable nodes to form sustainable work accounting behaviors.

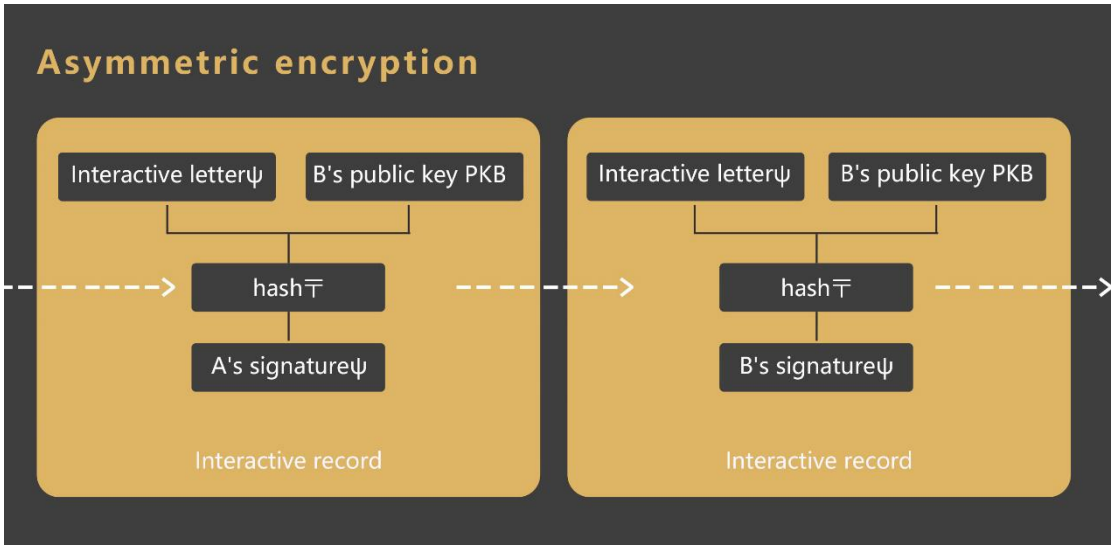
The integration of the two mechanisms can not only ensure the security and decentralization

of the block-chain network, but also allow the whole accounting process flow smoothly, reaching a trading speed of tens of thousands of levels per second, high TPS and unobstructed transactions. Actually, it is very important for the Domain block-chain network that requires many nodes to attend to achieve low latency, high transmission and long-term stability.

6.3 Data layer

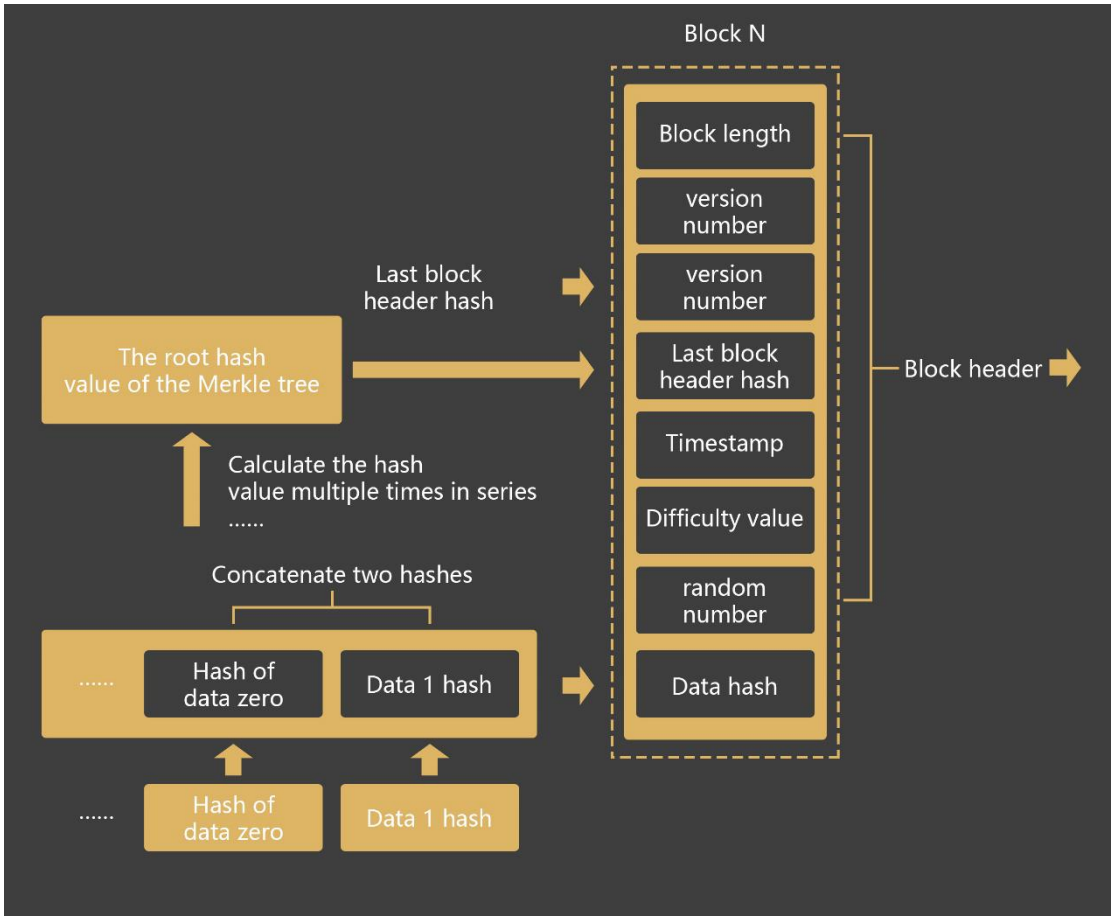
6.3.1 Interaction record

Interaction record is a data structure used to record interaction information, containing the signature of interaction responder A, the public key of initiator B, input information and output information, etc. But it does not specify the interaction records of predecessor and successor in the data structure, only determines the logical authorization relationship with the interaction public key and signature. Therefore, each interaction is independent and only forms a chain relationship at the logical level.



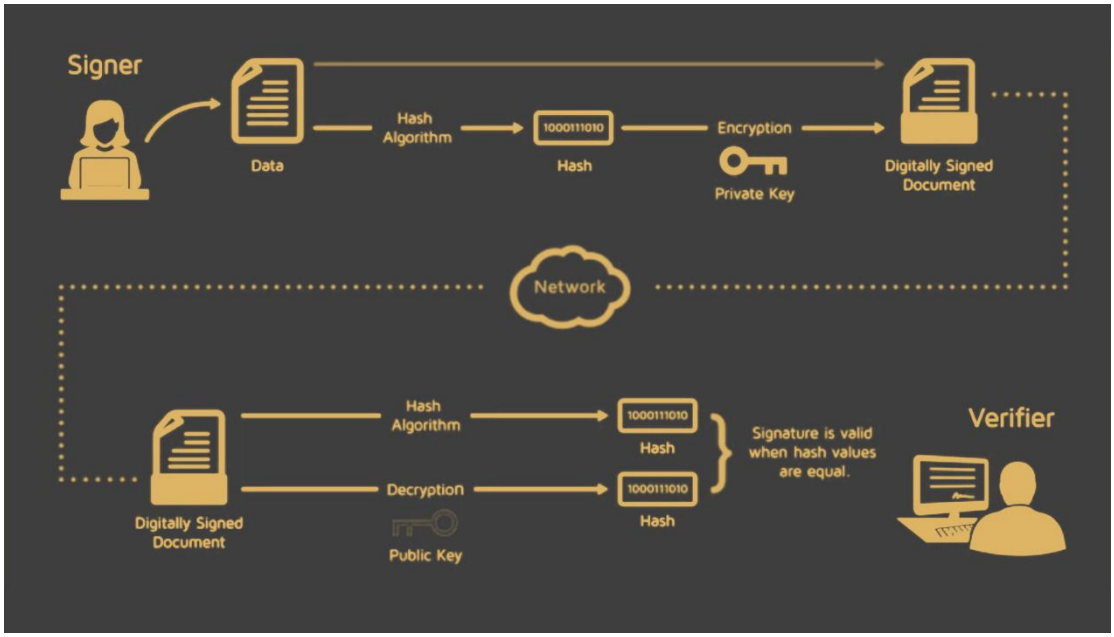
6.3.2 Block structure

As a component unit of block-chain, block consists of a block header and a block body. The block header can be divided into three parts: the predecessor block hash, the basic information part (containing the information, such as version No., timestamp, difficulty value and random value, etc.,) and the Merkle tree hash. Specifically, the predecessor block hash in each block indicates the information of the previous block, which is included step by step to form a block chain structure; The timestamp in the basic information determines the block generation time. The generation time of Domain network block is 10 seconds. That is, one block is generated every 10 seconds; The Merkle tree is the main data part located in the block body, while the leaf node refers to the recorded information and the intermediate node is the hash of the lower two nodes. Merkle tree structure guarantees the authenticity, security and non-repudiation of the data.



6.3.3 Asymmetric encryption algorithm and hash algorithm

As the foundation of block-chain technology, asymmetric encryption algorithm and hash algorithm ensure the security and verification requirements of incredible networks. In order to guarantee the privacy and security of Domain users' accounts and the long-term operation of the whole block-chain network, Domain adopts asymmetric encryption algorithm and hashing algorithm for the network verification nodes in the data layer. Generally speaking, hash algorithm is used to generate the predecessor block address, summary of the recorded information and interaction address, and construct record data structure. Asymmetric encryption algorithm is used to encrypt information, sign, authenticate and verify each transaction. At present, elliptic curve encryption algorithm is considered as one of the most secure encryption algorithms. Elliptic curve modulo forms a limited set of discrete points, while ECC is an asymmetric encryption algorithm on the basis of discrete set logarithm problem.



6.3.4 DO zero-knowledge proof

Zero-knowledge proof algorithm plays an important role in cryptography. It refers to that the

certifier can still prove the correctness of a conclusion without providing any useful information to the verifier. In a block-chain application scenario, zero-knowledge proof can meet the verification requirement of encrypted data.

Based on the concept of zero-knowledge proof, Domain innovated and developed the DO zero-knowledge proof technology. It can conduct verification across multiple different encrypted ledgers and support full homomorphy relationship verification for encrypted data under zero knowledge when all ledgers are in the state of full cipher-text, including the operations of adding, subtracting, multiplying and dividing for encrypted data, and the verification of data size relationship, etc. The verification time is less than 3 milliseconds.

The emergence of DO zero-knowledge proof technology provides a cross-validation of encrypted data, especially the data under complex business logic, thus ensuring legal compliance in the transaction flow process, greatly improving the risk control capability of business flow among multiple agents and making it possible to apply multi-level business scenarios on the block-chain.

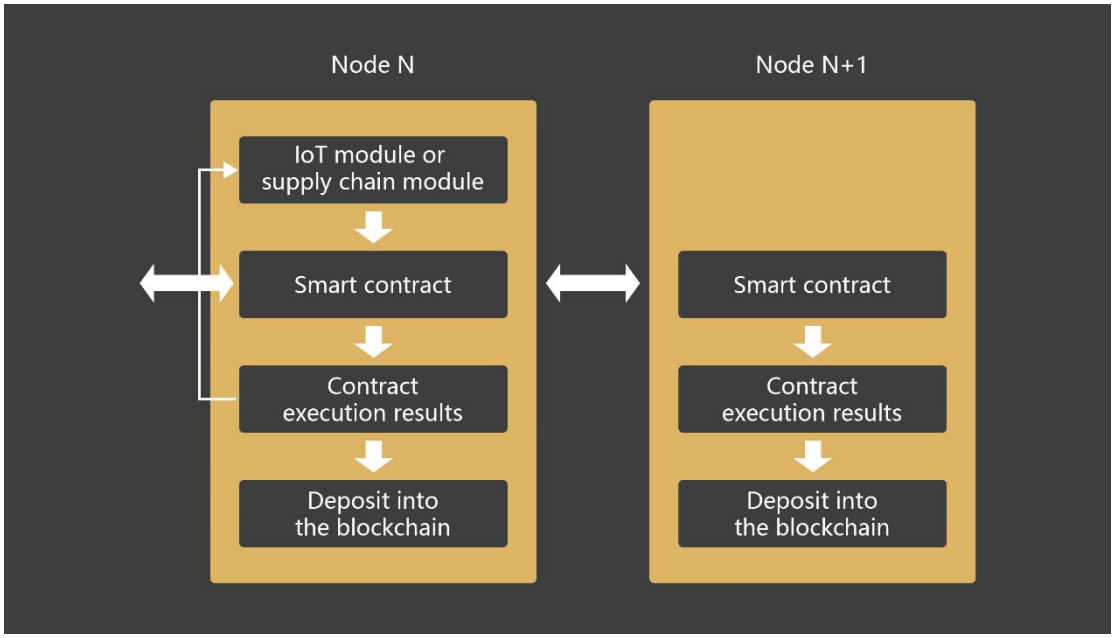
6.4 Contract layer

The contract layer of Domain has a smart contract set defined in the genesis block, including the main functions, the consensus mechanism of chains and the contract set update mechanism, etc. On this basis, cross-chain relay is realized to make Domain achieve credible cross-chain interaction with homogeneous and heterogeneous chains. In fact, it is of great significance for asset exchange and application docking in more and more public chain ecological environments.

6.4.1 Smart contract

The smart contract application in the Domain system is based on block-chain technology. The contract code, execution process and execution result are open and transparent to all topics of the supply chain, and the results cannot be tampered with, thus effectively improving the credibility of the system and facilitating the nodes to participate in maintenance and supervision.

Domain executes the smart contract with WebAssembly (WASM). Moreover, developers can use their familiar programming languages to write smart contracts with the help of WebAssembly. Therefore, Domain will support more programming languages to lower the barrier for developers to write smart contracts in the future.



In addition, developers can use the compilation tool provided by Domain to compile high-level language codes, such as C++, etc., into byte-code with WASM format, and then call the

contract deployment interface to deploy the code on the chain. A successfully deployed smart contract can create a smart contract account on the block-chain, which stores the contract byte-code and the corresponding Application Binary Interface (ABI). Unlike ordinary Domain accounts, the contract account and asset are controlled by contract code, without private key.

In order to call a smart contract, the user is required to specify the contract account name and contract method, and use ABI to interact with the smart contract. ABI is generated by the compilation tool provided by Domain, containing the information, such as contract interface, interface parameters and persistent storage structure, etc. The smart contracts can be persistently and sequentially stored in memory in the form of objects, while the storage fields and types of objects are customized by developers according to business needs.

6.4.2 Data customization contract

Domain supports a Turing complete smart contract language, and the powerful smart contract language makes the original complex business logic and application in the real world implement on the block-chain easily. But due to the operation mechanism of the block-chain, the operation of smart contract, even its abnormal operation, will be independently and repeatedly on all block-chain nodes. Therefore, it is very expensive to run the smart contract on the Domain block-chain (including computing and storage resources).

In this regard, we established a unique Data Pattern for Smart Contract, which takes the business event drive as the origin. We try to keep the smart contract language with data characteristics as simple as possible and reduce the calculated amount of fuel consumption, standardize many operations, such as data reading and event trigger, etc., output in a standard data format, such as JSON, and reuse and inherit these smart contracts.

In fact, many operations, such as writing data to the main chain block of Domain, are not suitable to be performed directly on the main chain. Therefore, the contract supports the event at the language level to directly notify the relevant parties to process when the expected event occurs. At the same time, the developer of the contract is required to repeatedly implement the same logic to achieve standardized cross-chain data transmission in the ecological system.

Furthermore, we will design and build many smart contract libraries. Through the event function index, these contracts can be quickly queried, called, inherited and reused, and the relevant data can be generated by itself. After getting the relevant standard data files, the developer, user, or enterprise can realize the interaction between the application program and the data of other sub-chain systems.

- The consistency, normalization, accessibility and circulation of data in the Domain value block-chain ecosphere are gradually realized as follows.
- Consistency: The core of consistency lies in consensus. Due to the mass data in the field of Internet ecology, there is a problem of different cognition among the data of different industries, devices and attributes, so the unique mechanism of the block-chain is set to solve the problem of data consistency.
- Normalization: The diversification of data leads to its lack of standards or uniformity, but the basic condition for establishing uniformity actually lies in the circulation of data. Only when data is able to be circulated on more levels can it establish its normalization in the social network.
- Accessibility: The circulation of data has its value, while its value lies in its usability. Only by enabling more people to access data in different environments and devices can it truly realize its value.

- Circulation: Data is like scattered beads, with fragmented space of existence. Therefore, we should sort out and combine these scattered data to truly realize, or even develop their values, thus completing the process of transaction and exchange in social networks.

6.5 Application layer

The application layer of Domain block-chain architecture encapsulates various application scenarios and customized adaptation components to facilitate developers for in-depth development and access based on Domain block-chain. It provides an interface for application software and supports client-side encapsulation of multiple computer languages, thus simplifying the language calling process.

The application layer mainly includes the following parts:

DOClient: built-in contract, smart contract, oracle machine and cross-chain interaction components for the calling of application programs;

DES-SDK: credible data exchange interactive component for the calling of application programs;

BaaS-SDK: credible data storage interactive component for the calling of application programs;

Domain Wallet: command line wallet for the encapsulation of the main chain interactive API;

DOM: the smart contract compilation tool of Domain that can compile smart contract into Web-assembly byte-code.

Domain mainly provides two methods to realize interaction between the application layer and

the underlying block-chain. The first one is that the client-side initiates a request through the application layer, and then the application layer sends the information to the block-chain (information co-chain). After that, the application layer captures the processing result to return it to the client-side. The second one is that the client-side initiates a request through the application layer, and then the application layer sends the information to the co-chain. After that, the application layer does not capture the processing result, but the client-side obtains the processing result on the block-chain by querying. According to the specific scenario requirements of the application, different modes can be deployed to meet the requirements of customized scenario business.

7. Technical Advantages of Domain

7.1 Improvement of network performance

The core principle of Domain is to solve practical technical problems with mature and efficient technologies. Instead of the concept of “optimizing” the block-chain, we are more concerned about how to provide a reliable configuration that can run business applications stably.

Domain nodes are classified according to different functions, thus conducting open source for the nodes that run on the cluster and provide standard service, and reaching consensus on the main chain through the “POW+POS” mechanism. The delegated mining nodes can protect the side chain to the greatest extent and share the strong consensus on the main chain. This method increases the pressure on each node, but the efficiency will increase with the addition of more side chains, because the delegated mining nodes can run on the cluster. The side chains are independent of each other, so each additional side chain can increase the efficiency of the whole system and the efficiency of each side chain can be improved due to parallel processing.

7.2 Upgradeable contract

At present, Ethereum smart contract is designed to be unchangeable once the codes are deployed. In other words, the code logic will never have the ability to upgrade from the time of deployment. As an agreement, the smart contract requires immutability, which represents a kind of agreement, with determined operation behavior. But as smart contracts are used more frequently, their processes and codes become more and more complicated. Moreover, like the contracts in real world, there will inevitably be man-made loopholes in the process of design and coding if there is no serious review. As a result, once they are hacked, there will be a huge loss.

Aiming at the current design program of most smart contracts in the industry, we adopt a simple smart contract upgrade program. In terms of language, we support the state variable of one contract to provide direct reading and writing of another contract (in compliance with security constraint).

```
    contract Token {
mapping (address => uint256) balances shared;

function transfer(address _to, uint256 _value) returns (bool success) {
        if (balances[msg.sender] >= _value) {
            balances[msg.sender] -= _value;
            balances[_to] += _value;
            return true;
        } else {
            return false;
        }
}
```

When deploying the contract, the balances variable is identified with the keyword “shared”. When compiling it into byte-code for running, the virtual machine will design a separate storage area for this variable. Furthermore, all variables declared without the keyword “shared” cannot be directly accessed by other contracts. Suppose that the transfer function of the source code needs to fix a bug, check the _value and deploy a new smart contract code.

```
    [baseContractAddress="0x5d65d971895edc438f465c17db6992698a52318d"]
    //baseContractAddress 是旧合约的地址
    contract Token {
mapping (address => uint256) balances shared;

function transfer(address _to, uint256 _value) returns (bool success) {
        if (balances[msg.sender] >= _value && _value > 0) {
            balances[msg.sender] -= _value;
            balances[_to] += _value;
            return true;
        } else {
            return false;
        }
```

After deploying the new contract, choose self-destruct for the old contract. And then, it can no longer be accessed, but the shared variable is still retained forever. The new contract can completely inherit the balances asset of the old contract and all the states are not lost, so it is not necessary to do additional migration work. But when developing a smart contract, it is necessary to declare the key state variable as “shared”, while the compiler will perform special processing for the storage area of the variable to ensure that it can be accessed by other authorized contracts.

In order to ensure safety, the upgraded contract and the old contract must be the same creator, otherwise there will be an abnormality during operation. Actually, it is not moral conduct this design, because once the terms and conditions of the contract are drawn up, they shall not be modified, or at least the contract audience must be consulted before modification. Therefore, we introduced a voting mechanism to approve the upgrade of smart contract, rather than being modified directly by the contract creator.

7.3 Upgrade design of core protocol

Domain node can get the compiled virtual machine byte-code from the Code storage area of the current latest block-chain. If there is no Code data in the current latest block, the core protocol has not changed. Then, it is necessary to trace back to the code of the latest block. All core protocol behaviors of the block-chain are determined by Code, including verification algorithm, packaging rules, NR algorithm and reward mechanism, etc.

In order to upgrade the core protocol, Domain team will develop and put the code in the open channel to discuss and vote by the community. Voting can be conducted in the form of smart contract or forum. When most community members agree to upgrade the protocol, Domain development team will package the latest code into a Code for transaction, and then release it to the nodes in the whole network. As long as the accounting node includes it in the block, it can take effect at the height of the customized block.

7.4 Dynamic adjustment of global parameters

Domain can dynamically adjust the global parameters of the system without branching, which is called DGP (Dynamic Global Property). The board of directors in charge of governing on the chain can initiate proposal and voting to decide the dynamic adjustment of global parameters, such as block size, block generation speed and transfer charge, etc. Such DGP program can avoid

the branching of the public chain, so that all ecological participants on the chain can consistently develop trade and build the ecology on the main chain.

7.5 Processing of mass data

The data co-chain and data exchange components of Domain support full domain data co-chain and exchange. The developer can trade and use these data after they are authorized by data source in a credible execution environment. All applications developed on Domain can use the user's personal data after being authorized by the user. Based on this, the developer can provide products and services that are more in line with the user's habits and needs. In the data exchange system, we should always focus on the data privacy protection and data leakage prevention. Moreover, an authorization mechanism is designed in the trust ecosystem established by Domain. That is, for any transaction involving data related to the data subject, it is necessary to notify the data stakeholder to authorize the transaction, so as to guarantee the data ownership in the process of developing application ecosystem and protect the rights and interests of each consensus person to the greatest extent.

7.6 Cryptography technology and data protection components

In the links, such as multi-dimensional entity identity authentication, distributed data exchange and distributed process protocol, etc., Domain provides the supports of a series of cryptography and data security components, including data encryption transmission, key sharing protocol, multi-party key management, ring signature component and blind signature component. In the link of identity and data verification, it provides zero-knowledge proof and homomorphy encryption scheme. In the link of data collaborative application, it provides secure two-party computation and further explores multi-party technical solution later. In addition, Domain provides specific security components for specific scenarios and supports the upper-layer

application implementer to build an applicable security application protocol on the basis of security components. These security components will be constantly developed and expanded according to scenario requirements, thus satisfying the needs of the community users expanded by Domain.

Citation

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

2.Vitalik Buterin. Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform. 2013.

3. Melanie Swan. Blockchain: Blueprint for a new economy "O'Reilly Media, Inc.", 2015.

4. Frederick P. Brooks. The Design of Design: Essays from a Computer Scientist. "Addison-Wesley", 2010.

5. Andrew S. Tanenbaum. Modern Operating Systems "Pearson", 2007

6. Joseph Poon and Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016

7. Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. 2014.

8. Hyperledger Whitepaper. 2016

9. Muhammad Saqib Niaz and Gunter Saake. Merkle Hash Tree based Techniques for Data Integrity of Outsourced Data. 2015

10. Sunny King, Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012

11. David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5, 2014.

12. Leslie Lamport. The Part-Time Parliament. ACM Transactions on Computer Systems,21(2):133-169, May 1998.

13. Leslie Lamport. Time, Clocks, and the Ordering of Events in a Distributed System. Communications of the ACM, 21(7): 558-565, Jul 1978.

14. Paul Tak Shing Liu. Medical record system using Blockchain, big data and tokenization. Information and Communications Security, pages 254-261. Springer, 2016.

15. Robert Love. Linux Kernel Development. "Addison-Wesley", 2010

16. Shawn Wilkinson and Tome Boshevski, Storj: A Peer-to-Peer Cloud Storage Network. 2016.

17. A. Back, Hashcash -- a denial of service counter-measure, Hashcash.org, 2002.

C. LeMahieu, "Raiblocks distributed ledger network", 2014

DOMAIN

FUTURE DOMAIN

Twitter：@Domain2045
Web：https://www.domainss.io