

Delta White Paper

Introduction

The birth of a decentralized encrypted digital currency called Bitcoin marks that human society is gradually moving towards the era of decentralized super-sovereign digital currency. It is the aspiration of the people of the world that a new digital currency that is fair, safe, value-preserving, fast, and green becomes a daily payment currency.

Our mission is to build a digital currency and decentralized application platform that allows every ordinary person to freely participate in minting and operating.

Our vision is to work with everyone in the world to create a super-sovereign digital currency that is fair, secure, fast, green, and inflation-free. We are committed to establishing a relatively free peer-to-peer ecosystem and online application environment, allowing everyone to participate freely and jointly promote the development and application of Delta.

1. Brief introduction to the sovereign currency issue

1.1 The sovereign currency issuing country that acts as the world currency can obtain huge international seigniorage and international inflation tax benefits. This single world currency structure is an unfair structure.

1.2 The prerequisite for the function of international currency payment means is the strong credit guarantee of the currency issuing country. However, the Triffin Dilemma makes sovereign currency issuing countries face a dilemma. The single world currency pattern is an unstable structure.ⁱ

1.3 The duality of currency value scales determines that only one currency can perform the functions of a world currency in the international market. The multi-polar world currency structure will lead to friction among currency-issuing countries and is detrimental to the peaceful development of the world economy.

1.4 centralized currency issuance power in order to stimulate the economy and increase fiscal revenue may lead to severe over-issuance of currency and high inflation. This will seriously affect the value of the existing currency in ordinary people's pockets and increase the economic pressure for survival .

2. The current status and drawbacks of cryptocurrency

Bitcoin is the earliest cryptocurrency. The concept was first proposed by Satoshi Nakamoto on November 1, 2008, and was officially born on January 3, 2009. The open source software designed and released based on Satoshi Nakamoto's ideas and the P2P network built on it. Bitcoin is a P2P form of digital currency. Bitcoin's transaction records are open and transparent. Peer-to-peer transmission means a decentralized payment system. Unlike most currencies, Bitcoin is not issued by a specific monetary institution. It is generated through a large number of calculations based on a specific algorithm . Some encrypted digital currency products subsequently invented by humans also basically refer to the model and technology of Bitcoin.

Such models and technical solutions have many excellent benefits and have brought many inspirations to the subsequent development of digital currency. for example:

Decentralization and immutability - these features ensure that the funds held by people are not controlled and supervised by any third party, while giving people a complete sense of ownership. Holders don't have to worry about their funds being frozen or wiped, which is reassuring.

Independence, fairness - Cryptocurrencies are not controlled by any country, bank or financial institution, and they are based on a decentralized network. Theoretically, it avoids to a certain extent the competition and conflicts caused by countries pursuing advantages in monetary policies and financial systems.

However, it also brings about many practical problems. Related issues will be discussed below.

2.1 Security

There are two main aspects of cryptocurrency security issues designed based on the above principles:

① Private key cracking - The theoretical difficulty of cracking a Bitcoin private key is equal to cracking a 256-bit key. In other words, the attacker needs to exhaust the problem approximately 10^{77} times at most. Although this chance is very slim, no one can guarantee that a successful collision will definitely happen for the last time. At the same time, with the emergence and development of quantum computers, it will bring greater worries to holders.

② Private keys are lost or stolen - Keeping the private keys of cryptographic currencies is an important problem faced by holders. Regardless of whether you choose to use a cold wallet, paper wallet or brain wallet, there is a possibility that the private key will be lost or stolen, which makes people feel very anxious. Everyone in

the world has had something lost or stolen, or forgotten important information. Therefore, no one can guarantee that this will not happen when it comes to managing private keys or mnemonic phrases. The worst part is that once lost or stolen, it cannot be retrieved or reset by any means, which brings huge risks to the holder.

2.2 Fairness

an example, although its decentralized nature allows anyone to participate in verifying transactions and mining blocks, in the early days, only a few people devoted themselves to this and thus obtained a large amount of Bitcoins. With the rise of the Bitcoin network, a large amount of computing power has been concentrated in the hands of a few mining farms, resulting in large-scale centralization of Bitcoin production and wealth distribution. Currently, 87% of Bitcoins are owned by 1% of the network, making it difficult for most ordinary people to get involved. People who want to own Bitcoin in the later period can only buy it in the secondary market at high prices or invest huge sums of money to purchase computing power. This situation makes it difficult for most ordinary people to have the confidence and strength to join. Therefore, fairness is an issue worth thinking about in cryptocurrency networks such as Bitcoin.

2.3 Energy consumption and environmental issues

According to real-time Bitcoin Electricity Consumption Index (CBECI) data released by the Cambridge Center for Alternative Financeⁱⁱ, the energy consumption of global Bitcoin mining is staggering. Currently, this figure is approximately 131.73TWh, which is comparable to the annual electricity consumption of countries such as Argentina or the Netherlands. In addition, Bitcoin mining also produces a large amount of carbon emissions, accounting for about 0.10% of total global emissions. This has exacerbated global environmental problems, especially climate change and environmental pollution.

mining on Bitcoin and similar networks continues to expand, so does energy consumption and carbon emissions. However, although the energy consumption and carbon emissions of these mining have attracted much attention, it has also promoted the development and application of greener and more efficient encryption technologies.

2.4 POS dilemma

The emergence of the POS (Proof of Stake) mechanism has indeed solved to a certain extent the problems of energy consumption and transaction speed of cryptocurrencies such as Bitcoin. However, there are also some difficulties in the POS mechanism. The main problem is that in the POS mechanism, the validators with the most staked tokens can obtain verification qualifications and receive rewards faster. This mechanism may lead to "the rich getting richer and the poor getting poorer", thus raising the issue of distribution fairness. This further hinders the circulation and popularity of cryptocurrency.

Under the POS mechanism, validators with a large number of tokens are able to obtain more rewards, which makes rich validators richer and poor validators poorer. This model may exacerbate the gap between the rich and the poor in society, reduce the participation of ordinary people, and thus hinder the popularity and development of cryptocurrency.

In addition, there are some other problems with the POS mechanism. For example, staking tokens can create risks, and validators may suffer losses if the price of the token drops. In addition, the verifiers in the POS mechanism may be maliciously attacked by attackers, thus affecting the security and stability of the entire network.

Therefore, although the POS mechanism solves the problems of energy consumption and transaction speed of cryptocurrencies such as Bitcoin to a certain extent, it also brings some new problems and challenges. In order to solve these problems, further research and exploration of more fair, secure and effective consensus mechanisms are needed.

Of course, in addition to the security, fairness, energy consumption and POS issues mentioned above, there are other problems with various existing cryptocurrencies. For example, there are problems such as slow transaction speed, high transaction costs, large price fluctuations, lack of application scenarios, and exchange gaps. These problems will not be discussed here for the time being. The subsequent delta design description chapters will discuss how to solve and avoid these problems through some effective methods and strategies.

3. Delta is a more ideal digital currency system

In order to design and develop a more ideal digital currency, we stand on the shoulders of our predecessors, learn from their advantages, and avoid making the same mistakes. At the same time, combined with the current social conditions and technological foundation, we take humanistic currency as the basic concept and are committed to designing and building an ideal digital currency system in the future society.

3.1 Nouns and definitions

written explanations of some necessary terms and definitions at the front .

- **DTC:** This is the abbreviation of Delta Coin and the code for this digital currency.
- **DTCT:** This is the abbreviation of Delta Credit, which means DTC that has not been activated and released.
- **δ:** This is the currency symbol of Delta Coin, such as 10δ, 100δ, 1000δ, etc.
- **Mining:** In the Delta application, through specific allocation rules and modes, users obtain the behavior of DTCT through click operations.

Roles and functions:

Roles and functions constitute an organic whole of currency casting, consensus building, and system security. In the Delta system, there are three core roles: miners, ambassadors, and validators.

- **Miner:** A participant in the Delta system will obtain miner status when performing mining operations for the first time. Its main function is to conduct mining operations on Delta's mobile application to generate DTC. This design is very interesting and practical because it consumes no additional power, is environmentally friendly, and does not cause time anxiety or affect personal health. In the construction process of Delta Consensus, miners are the main force.
- **Ambassador:** Any miner can recommend people around them to join Delta by using their own DID (Digital Identity Identifier) and build a micro-community network. Those who successfully recommend others to join will automatically receive ambassador status. The role of the Ambassador is to teach new members how to conduct mining operations and help them understand how Delta works. Therefore, ambassadors are a key force in Delta consensus building.
- **Validator:** The unique design of the Delta system makes it a digital currency system that requires no password, no private key, and no mnemonic phrase. In this system, the role of the verifier is to provide account authentication services to unspecified users through verification terminals. Any miner has the opportunity to become a validator through the election process, and they play an important role in ensuring the security of the system .

3.2 Mobile phone mining

Introducing the concept of mining into cryptocurrency can help solve the problem of distribution fairness in currency issuance. Pi Networkⁱⁱⁱ pioneered the innovative design of mobile mining, which is environmentally friendly and effectively avoids energy consumption issues without occupying the computing power of the device and additional networks. Today, when mobile phones are highly popular, it has become

possible for ordinary people to participate in digital currency mining. Delta inherited this design. It should be noted that **the essence of mining lies in distribution, not calculation.** In the design of Bitcoin, Satoshi Nakamoto used the computing power of participants to calculate mathematical problems to compete for accounting rights and reward Bitcoins. It can be seen that computing power is only used in the game to compete for accounting rights, and it is not directly related to accounting. Judging from the working principle of the computer, it is just the process of writing data to the disk, and this process consumes very little energy. Therefore, abandoning computing power mining is completely reasonable and feasible under the current technical background.

3.3 Proof of People (POP)

If we use the amount of computer work computing power to prove the contribution to the network is called POW mining (Proof of Work), and the amount of pledged currency to prove the contribution to the network is called POS mining (Proof of Stake), then we can Proving the contribution to the network through the authenticity of the people themselves is called POP mining (Proof of People). When we enable the Delta program on the mobile phone for mining, it is not the mobile phone itself that is performing the mining process, but the mobile phone as a carrier used to verify the authenticity of the individual. Therefore, the essence of Delta is to hand over the power of minting money to the people, which is a concept of humanistic currency.

3.4 3-No-Verification

The creative design makes Delta an encryption currency system that requires no password or private key.

Passing **3-No-Verification is the only way for users to enter the Delta system.** In order to solve the cryptocurrency security issues mentioned in [Chapter 2.1](#), we propose and use 3-No-Verification in the Delta account authentication design.

The meaning is:

- No password
- No private key
- No mnemonic words

The reason why we do not need passwords, private keys, and mnemonics is that if the system is still designed in the form of account + password, password protection will be required via email or SMS, which will lead to decentralization and service continuity. seriously questioned. Specifically, email authentication requires a dedicated outbox address, and SMS verification requires an SMS access number or sending port applied for at a telecommunications company. Not only do these resources require ongoing maintenance, they also require payment. These tasks need to be performed by centralized human operations, which will lead to user distrust and

is contrary to the core concept of decentralized applications.

After the birth of Bitcoin, asymmetric private keys were used as a means of authority authentication, which is a completely decentralized authentication scheme. Later, in order to facilitate users' memory and management, developers derived mnemonic solutions and were widely used in decentralized applications. However, these solutions all involve the risk of losing, forgetting, or stealing the private key or mnemonic phrase, and cause users a certain amount of anxiety. Therefore, we need a more secure and convenient authentication method to replace traditional passwords, private keys and mnemonic phrases.

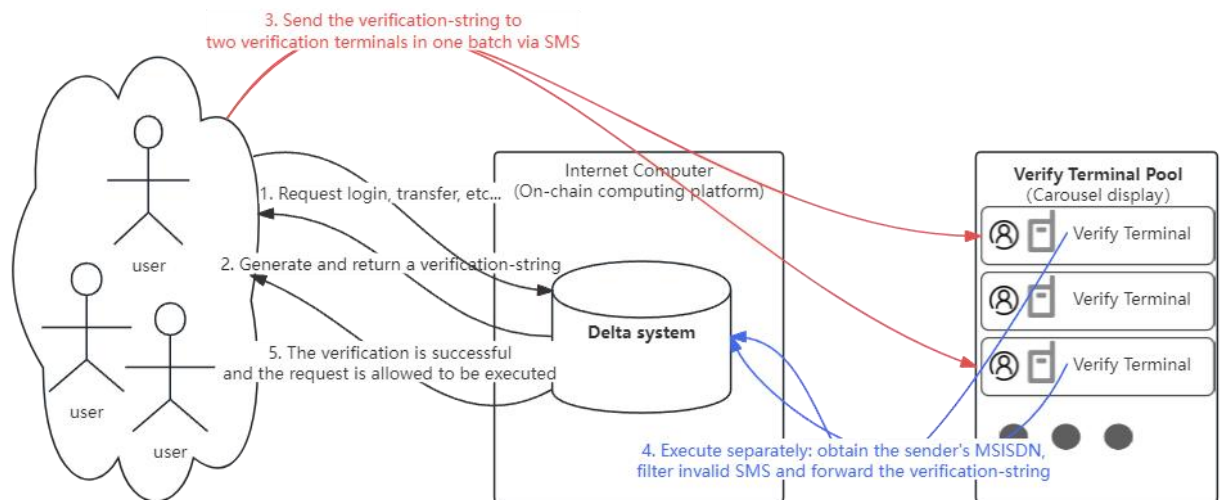
Since passwords, private keys, and mnemonic phrases are at risk of being cracked, lost, and forgotten, it is not impossible to abandon these three verification methods to achieve decentralized account verification. Delta has successfully achieved three-no verification, which is mainly due to the powerful functions of the blockchain-based Internet Computer and the world's highly mature mobile communication network. MSISDN is the only number that can identify mobile users in the mobile communication network, so three-no verification is also called decentralized SMS authentication. Delta developers have designed a "Decentralized SMS Authentication Protocol" framework, which is a completely reliable and decentralized solution. The technical background and more detailed description of Internet Computer will be introduced in the subsequent technical solution chapters.

3.3.1 Verification process and rules . An overview of the verification process and rules is as follows: First, we allow users who meet specific conditions to apply for verification terminal permissions to become verifiers. Verifiers can use their idle MSISDN (mobile phone number) and smartphone to download and install the delta verification application. Use the MSISDN as the access number to receive and forward the verification string. The verifier only needs to ensure that the mobile phone power and network connection are stable, and the verification process will be completely automated by the Delta system. When a large number of users apply and become verifiers, a verification terminal pool will be formed. Later, when a user performs operations that require identity verification such as registration, login, or transfer, the Delta system will generate a verification string. The user will select a well-functioning terminal from the verification terminal pool and send the verification string to the terminal's access number in the form of a text message. After receiving the verification string, the verification terminal extracts the sender number at the same time and then forwards it to the Delta system. Finally, the Delta system performs a verification comparison and the legitimate user's request will be allowed to pass. For more detailed information, see the [Decentralized SMS Verification Protocol^{iv}](#) Framework.

In addition, additional explanations are needed: First, in the early stage when the system has not yet formed enough verification terminals, developers will access a globally accepted virtual access number to provide early users with verification access.

This virtual access number will be removed once the number of validators is sufficient to meet basic needs. Second, in order to avoid users incurring higher international SMS charges, the system will prioritize the home country verification access number for users who need verification.

Chart 1 (Illustration of verification principle)



3.3.2 For the verifier rules part , our design includes the following items:

- (1) The upper limit of the number of verifiers allowed in each region (districted according to the E.164^v country code) is one ten thousandth of the total registered population, and the minimum number of people allowed is 1,000.
- (2) Staking election: To become a validator, you must pass the staking election. Candidates need to invest a certain amount of Delta Coin into the campaign pool and download the Delta verification terminal to ensure a normal connection with the Delta system. According to the election rules, the system will automatically select a certain number of winners from the election pool to become validators in each election cycle (one day). A maximum of 30 people will be selected in each cycle. At the same time, the total number of people screened cannot exceed the upper limit specified by the region. Successful validators will receive a 90-day working period.
- (3) Offline slashing: Within the working cycle (90 days), the verifier must not be offline for more than 1 hour for any reason, otherwise its pledged funds will be slashed and transferred back to the community mining fund pool.
- (4) Attack penalty: For verifiers who attempt to gain access to others through attacks (such as packet capture, tampering, etc.), the system will confiscate their pledged funds and mark them as dishonest users.
- (5) Election renewal: After the 90-day work period expires, validators can choose to continue participating in the staking election to maintain verification services. The pledge amount can be calculated superimposed on the amount in the current service period.

In addition, a reward mechanism is provided for honest verifiers, and detailed measures regarding rewards will be elaborated in the economic model section.

3.5 Safety Circle

After the introduction of the 3-No Authentication security verification model, the use and management of digital assets will become safer and more convenient. However, under special circumstances, this single verification mechanism may lose its security. For example, when a mobile device is lost or stolen by others, the other party may have full control of the device, including sending verification SMS messages. In order to prevent this from happening and protect the security of account assets, we have added a security circle function to the system design to provide secondary identity verification for accounts to enhance account security.

The security circle is a verification model based on user social relationships, and this function is completely decentralized. It helps users achieve security verification through their social relationship circle. The security circle function can effectively increase the difficulty of malicious attacks and reduce the risk of accounts being obtained by others.

The working principle of the safety circle is as follows: First, users can add trusted people (usually relatives and friends) to their safety circle member list, usually 3-5 people. When an account requires security circle verification, the Delta smart contract program will randomly select a member from the security circle member list to assist the current user in confirming their identity by providing a security code. When the current user asks the member for the security code, the selected security circle member will be able to help confirm whether the user is the user. At the same time, the program will prompt: "Refuse to provide the security code if it is not a relative or friend" to protect the security of the account. Therefore, any Delta user should ensure that the people on their security circle member list are trustworthy.

Under what circumstances is it necessary to use a safety circle?

① When a user's mobile phone with the Delta program installed is lost, the user should use a new device to forcefully log in to the Delta application. In this case, users need to use security circle verification to ensure the security of their account. Due to the loss of the phone, the original verification status has become invalid, and the user needs help from security circle members to verify their identity and log in to the app .

② When the account performs sensitive operations, such as changing mobile phone numbers or updating security circle members, in order to prevent these operations from being performed by others, security circle verification also needs to be enabled .

3.6 Economic model

In [Chapter 2.2](#), we mentioned fairness issues in the distribution of existing cryptocurrencies. Therefore, the design of delta distribution rules needs to avoid a distribution method similar to Bitcoin, that is, allocate most of the currency to early participants. This distribution method may result in late-stage participants needing to purchase at a high price, thus turning it into a speculative tool. This not only hinders the formation of human currency consensus, but may also lead to the failure to realize circulation value. Therefore, the delta allocation rule needs to be implemented in a more reasonable way.

First of all, we define the initial total amount of Delta Coin as 300 billion. Compared with other cryptocurrencies, Delta uses such a large total amount to facilitate circulation and use in daily life. (For example, we want to price a 250ml carton of milk at 0.3 δ , but not 0.0000003 δ so too many zeros after the decimal point would be confusing)

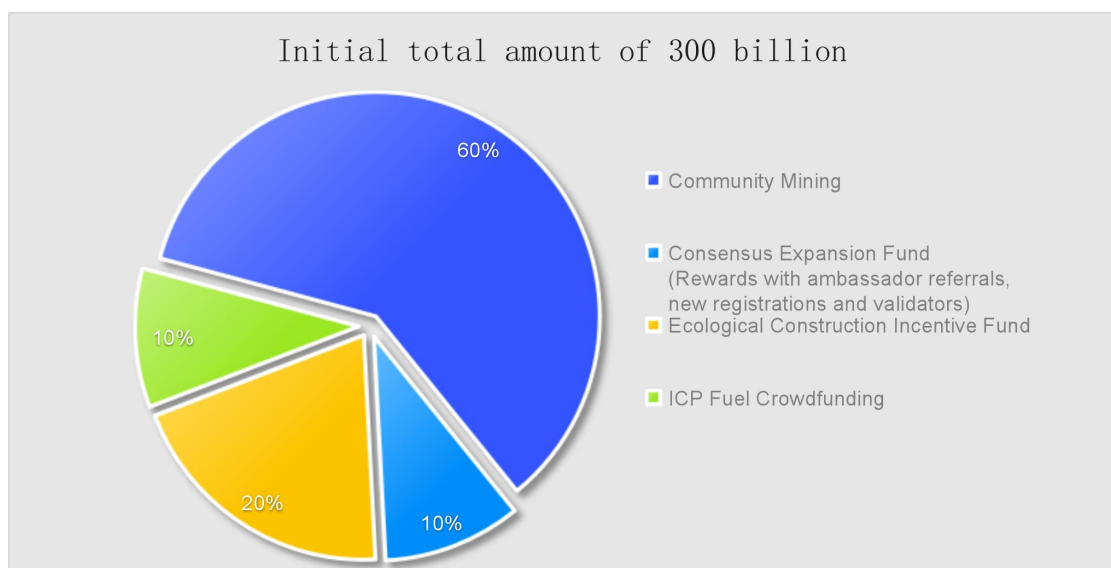
Then, we divide these 300 billion coins into four parts, each part plays a different role:

Part 1: Community Mining - 60%

Part 2: Consensus expansion fund (for ambassador recommendation, new registration and validator rewards) - 10%

Part 3: Ecological Construction Incentive Fund - 20%

Part 4: ICP Fuel Crowdfunding – 10%



The purpose of dividing the currency amount into multiple parts for distribution is to simultaneously promote the development of community consensus and ecological construction, and to stimulate the enthusiasm of the community in the initial

ecological construction and ensure the reliability of long-term system operation.

Some additional notes on the allocation scheme are as follows:

1. The initial total and the current distribution plan are executed under an "[interim governance mode](#)". Obviously these aggregates are not enough to serve as a global consensus currency. Afterwards, under the DAO model, the "Governance Committee", which can be elected by all Delta members, can discuss and propose additional issuance proposals based on development needs.
2. all of them can become tradable DTC later . This 300 billion is the total amount of Delta Credit (DTCT) , which represents the effective amount before activation and release through KYC. After KYC screening, generally speaking , the final number of DTC that can be circulated will usually be smaller than DTCT.
3. Delta is based on the concept of human currency. In theory, all coins should be distributed through community mining and consensus expansion, while other parts should be raised through donations or handling fees. However, in the early stages of the project, the demand and workload for ecological construction were very large. In order to ensure the success of the project and give ecological builders more confidence, we implemented reserved allocation. The fuel crowdfunding part is also to provide a more reliable operating mechanism.

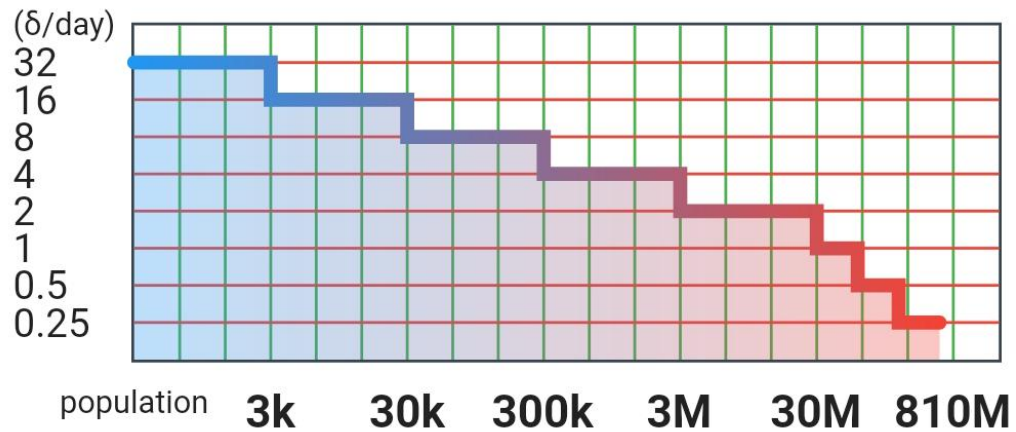
3.6.1 Community Mining

The total amount of community mining is 180 billion, which is equal to 60% of the total amount of 300 billion. We allocate these coins through live users' daily check-in and contribution of attention. In this way, consensus can be formed after a long period of time. The principle is that users convert invisible virtual numbers into currency consensus by contributing attention, and this consensus in turn promotes its value as currency. In terms of the basic mining rate, in order to find a balance between early incentives and long-term fairness, we adopted a two-stage doubling scheme design.

The first stage: When the number of participants is between 1 and 30 million, the rate between 1 and 3,000 people is 32 δ /day, which is used as the starting benchmark. Whenever the number of people increases by 10 times, the rate is halved until the number of participants reaches 30 million, when the rate drops to 2 δ /day and then enters the next stage.

Second stage: When the number of participants reaches 30 million or more, every time the number of participants increases three times, the basic rate will be halved until the final mining is completed and production ceases.

Chart 2 , (Basic rate halving chart analysis)



3.6.2 Registration and recommendation rewards

In order to promote the faster development of Delta Network, we have specially set up a referral reward program. After becoming a miner, anyone can become a promotion ambassador and earn these rewards by recommending others.

- Fixed rewards for referrals: In order to invite friends and family to join Delta, recommenders only need to share their digital DID via a QR code or link. When the other party fills in the recommender's digital DID when registering, both parties will receive a 1δ reward. If the referral registration occurs after community mining has stopped, the reward will be halved, with each receiving 0.5δ . This part of the reward will be distributed from the total amount of 30 billion "Consensus Expansion Fund".
- Direct recommendation reward: Every time an ambassador directly recommends someone, when the recommended person is in mining status, the mining rate will be increased by $1/3$ of the base rate. In addition, when the ambassador's superior recommender is in mining status, this ratio will also be calculated into the direct recommendation reward.

Assuming that the current basic rate is $16\delta/\text{day}$, the number of people recommended by the ambassador is n , and they are in mining status, then the calculation formula for this part of the day's improvement income is as follows: $16 \times \frac{1}{3} \times (n+1) = x (\delta/\text{day})$

- Indirect recommendation rewards: Recommending ambassadors directly recommend everyone in the team and everyone they recommend represents the ambassador's indirect recommended users. When an indirectly recommended user is in mining status, the recommending ambassador's mining rate will be increased by an additional $1/10$ of the base rate.

Assuming that the basic rate is the same as above, and the number of people indirectly

recommended and mining is n_2 , then the calculation formula for this part of the day's improvement income is as follows: $16 \times \frac{1}{10} \times n_2 = x (\delta/\text{day})$. The two parts of rewards, direct recommendation and indirect recommendation, will be calculated superimposed and allocated among the total community mining funds of 180 billion.

3.6.3 Validator Rewards

Chapter [3.4](#) explains the basic principles and processes of three-no verification. In order to implement such a verification process, the system needs some users to apply to become verifiers. At the same time, we also need to design certain rewards to motivate these people who pay for it. The reward method and amount of validators are divided into two situations.

① First, when 10% of the consensus expansion fund has not been used up, the validator's rewards will be paid using this part of the fund. The specific amount of the reward for each completed verification is 1/3 of the current mining base rate.

② In addition, when the consensus expansion fund has been exhausted, the verification fee will be paid by the user who needs to verify, and this fee will be automatically deducted after the verification process is completed. At this time, the verification fee will be calculated as three times the daily transfer fee.

3.6.4 Ecological Construction Incentive Fund

In order to promote the multi-faceted construction and development of Delta Ecology, the fund will be oriented towards multiple incentive programs in ecological construction, including:

1. Ecological dApp developer reward program: designed to encourage early ecological development, contributions to the Delta ecosystem, and high-quality ecological project developers. Please refer to the [dApp Square](#) chapter for more details.
2. Image and visibility promotion award plan: designed to reward individuals or teams that have made special contributions to Delta's image and visibility promotion.
3. Early transaction reward program: used to reward users who participate in various early transactions in the Delta application.

In the early "[interim governance model](#)", the fund was hosted and planned by the Delta core team. Its goal is to promote the prosperity and development of all aspects of Delta's ecological construction. Specific uses and rules will be designed and adjusted based on actual needs and clearly stated in the relevant use plans.

Afterwards, once the "[DAO governance mode](#)" is entered, the core team will transfer the remaining funds to the DAO for custody. Subsequent usage decisions will be made by the DAO.

3.6.5 ICP Fuel Crowdfunding

How funds are allocated in this regard will be explained in the Fuel Mechanism chapter.

3.6.6 Handling fee

One of the benefits of generating a certain handling fee during transactions is to prevent malicious small-amount transfers from generating a large amount of junk accounting data to protect the healthy operation of the Delta system. In addition, the handling fees of the Delta system will adopt the burning mode, and the handling fees consumed by transactions will be directly transferred to an empty address.

Under the "[interim governance model](#)", the handling fee burned for each transaction is 1%, while the minimum limit is 0.01 δ and the maximum is 0.3 δ . Under this model, in order to ensure that power is not abused, new coins are not allowed to be issued for any reason, which is equivalent to a deflationary mechanism in this model.

Later, under the "[DAO governance model](#)", DAO can implement an additional issuance mechanism through proposals based on actual needs. The additional currency can make up for the burning part of the handling fee and prevent further deflation. The first part of the additional currency will be used to pay for the fuel "cycles" Delta runs. Other parts can be used for governance participation reward funds and other matters that are conducive to ecologically sound development. In addition, under the long-term DAO governance model, the specific quota or rules of transaction procedures can be re-determined through annual proposals.

3.7 KYC verification

KYC (Know Your Customer/Client) verification is an important process designed to confirm the identity of the user and prevent the creation of fake accounts. In the Delta system, since its mining mechanism is based on social networks and completely decentralized, KYC verification is particularly important. In order to ensure fair distribution and eliminate false identity mining, we plan to use a combination of AI identification and community KYC markets. Users can achieve

anonymous cross-certification of community members through the KYC market, and set up a certain reward and penalty mechanism. These measures will ensure the fairness and ecological healthy development of the Delta system, while increasing users' trust and participation in the system.

First, AI recognition technology can be used in the identity verification process to automatically identify and compare identity documents provided by users through deep learning and image recognition technology. This can greatly improve the efficiency and accuracy of identity verification and reduce human error and fraud.

Secondly, the community KYC market is a market mechanism based on the idea of decentralization. It prevents behaviors such as "human skin masks" and "digital face-changing" through human inspection and judgment, which can effectively prevent the occurrence of fraud and attacks against AI. Users can achieve anonymous cross-authentication and confirmation of community members through this market . In the community KYC market, users can publish their identity certification information, and a certain reward and punishment mechanism is set up to encourage other users to verify and cross-certify. In this way, we can establish a mechanism of mutual supervision and trust to ensure the authenticity and credibility of each account.

At the same time, during the manual inspection and certification process in the KYC market, we adopt a selective disclosure approach. In authentication, selective disclosure refers to the process of verifying the authenticity of an individual by showing only the necessary information required for verification to the verifier while ensuring that personal information is not leaked . The advantage of using this method is that the necessary information can be effectively verified while ensuring that the privacy of the person being verified is not leaked . Delta uses a fragmented distributed storage method when processing personal information, which provides a technical basis for selective disclosure of identity authentication.

In addition, in order to prevent malicious behavior and the creation of false accounts, the Delta system will also establish a strict supervision mechanism. If suspicious behavior or illegal operations are discovered, the system will immediately take corresponding measures, such as suspending or marking relevant accounts to prevent the process from continuing.

Through the above measures, the Delta system can effectively prevent the creation of false accounts and malicious behaviors, ensuring the fairness and reliability of the system. At the same time, KYC verification can also increase users' trust and participation in the Delta system and promote the healthy development of the Delta ecosystem.

Afterwards, when the user obtains KYC certification, the system will immediately release the first DTC for the user. For specific release rules, please refer to [Chapter 3.12 Release Mechanism](#) .

3.8 Non-KYC accounts

In the Delta system, no one has the authority to delete or freeze any account. It should be noted that when writing the Delta program in the early days, no such function or interface was designed, which is more in line with the concepts of decentralization and user autonomy. Therefore, non-KYC accounts are allowed to exist in the system for a long time and can participate in transactions or interactions. However, accounts that pass KYC certification will receive specific marks, and accounts that are not marked with KYC will be restricted from certain rights, such as participating in DTCT fund release actions, becoming a transaction seller, etc. Since unmarked KYC may be considered untrustworthy, it may be rejected by certain system ecosystem sub-applications or counterparties.

3.9 Fuel mechanism

First, all computer programs require electricity and hardware costs to run. For example, for traditional Web2 programs, you need to host the service on a platform such as Amazon AWS and pay for resource usage. Blockchain is no exception. Bitcoin miners need to purchase expensive ASIC mining machines and pay high electricity bills. Their operating costs are fed back to the miners in the form of mining rewards and transfer fees. Therefore, transfer fees for cryptocurrencies like Bitcoin are quite expensive. Other POS model blockchains have reduced the cost of mining (game-like computing power calculation), so the transfer fees have also dropped relatively, but the governance costs of this model are still high, and the final handling fees are still high.

Delta also has running costs. Delta runs entirely within the Internet Computer Cypherspace developed by Dfinity. The architectural design of Internet computers is more advanced than traditional blockchains and has lower operating costs. According to official data, storage costs are approximately US\$5/GB/year, and Internet computers are not billed in sovereign currency. Instead, it requires a fuel called "cycles" to power computational operations and storage^{vi}. Such "cycles" are generated through the conversion of Internet Computer (ICP) utility tokens. Therefore, Delta needs ICP, a utility token, as its operating cost.

Therefore, Delta needs a fuel mechanism to ensure the long-term operation of its program. Based on the development of Delta, we divide the fuel source into 3 stages, namely the startup stage, the consensus building stage and the consensus formation stage.

① Startup phase - in the early stage of Delta deployment to no users, the core developers will inject 30 ICP tokens into the Internet Computer smart tank at one time (the smart tank will be explained in detail in the running environment chapter) to ensure the normal operation of the program, and provide service guarantees for users who are about to join.

② The consensus building stage - refers to the stage from the start of operation to before the circulation value is generated. At this stage, we launch an "ICP fuel crowdfunding" sub-program in Delta's application square to raise the "cycles" of fuel needed for Delta's operation. Any user can raise the ICP tokens needed to convert "cycles" fuel for Delta through this subroutine, and the program will award the corresponding amount of Delta Credit to participants as a bonus for their support based on the set algorithm. These rewardable ICP tokens are the fourth part of the total distribution (ICP fuel crowdfunding), totaling 30 billion δ . Crowdfunding will automatically stop after all distributions are completed. All crowdfunded ICP tokens will be stored in a virtual DID that is not bound to the MSISDN (meaning that no one has the authority to operate this virtual DID). The Delta Fuel Management Program will automatically monitor the "cycles" balance in the smart tank. When "cycles" is less than 3000 billion, 10 of the ICP in the virtual account will be automatically exchanged for cycles. The calculation result of the crowdfunding exchange rate is mainly determined by the two parameters of the total number of users and the amount issued. The specific algorithm formula is as follows:

definition:

R = number of registrations

D = Amount of Delta Credit issued

Ex_rate = current crowdfunding exchange rate

$$a = \log_{10}(R)$$

$$Ex_rate = a \times \log(D, 13 - a) \times 0.0001$$

where 13 and 0.0001 are fixed constants.

Assume that the number of registered people is $R=100,000$, and the amount of crowdfunding rewards distributed is $D=330,000$ pieces.

Then, the current exchange rate is calculated as follows:

$$a = \log(R, 10) = \log(100000, 10) = 5$$

$$Ex_rate = a \times \log(D, 13 - a) \times 0.0001$$

$$= 5 \times \log(330000, 13 - 5) \times 0.0001$$

$$= 0.00305535$$

That is, currently: 1 *ICP* can be exchanged for $1/0.00305535 = 327 \delta$ (the result is approximately rounded)

③ Consensus formation stage - refers to the completion of large-scale KYC verification and entering the "DAO governance mode". DAO can issue a certain amount of Delta Coin according to the additional issuance proposal to make up for the burning of transaction fees, and give priority to part of the additional issuance amount for exchange. Fuel "cycles".

3.10 dApp Square

dApp Square is Delta's decentralized application market, a platform for Delta's online ecological construction, and a future-oriented Web3 application center. Any user with development capabilities can develop Delta applications and settle in. After extensive community discussion and voting, the "Delta Application Ecosystem White Paper" will be drafted and released. The white paper will determine the design and specifications for developer reward policies, ethical behavior, user privacy and user data autonomy policies.

3.11 USDT dual currency mining

USDT^{vii} dual-currency mining means the simultaneous mining of two digital currencies, DTC and USDT.

Its purpose is to provide miners with a certain amount of effective income in the early stages when the Delta ecosystem has not yet formed and prospered; at the same time, it also provides developers with certain financial support to ensure that developers can continue to provide development services in the long term, and ultimately realize Delta Planning and vision; it also provides an effective promotion channel for advertisers to promote the positive development of consensus.

The principle is to use the large user base of the Delta community to monetize traffic and provide multiple benefits to advertisers, Delta core developers and miners.

The method is to connect to the existing mature advertising platform. Users can display incentive advertisements and obtain monetization benefits through a "play button" of the USCT mining module.

Details such as the allocation mechanism and settlement cycle can be found on the Delta App "USCT Mining Module" page.

3.12 Activation and release mechanism

After the emergence of Ethereum smart contracts, a variety of tokens have been issued in the market. Most of the issuances of these tokens have release activation mechanisms. Their method generally requires users to promise (or stipulate) to use the tokens in a certain proportion and a certain amount. The tokens are pledged according to the time period, and then released one or more times according to the pledge period. The released tokens can obtain the right to flow freely.

The purpose of this design is to ensure the stability and upward price of tokens and prevent the value of tokens from collapsing due to large-scale selling. The

principle is to obtain the development of ecology and consensus through the extension of time. This is indeed helpful to early consensus building and price stabilization, but its effect is not strong. Because doing so will form a large number of zombie users in the system. These zombie users do nothing but wait for the time to come and the price to skyrocket. This situation will not be helpful to the long-term construction of the consensus ecosystem.

To this end, Delta has redefined the release mechanism. We combine the cycle with community behavior, that is, within a set cycle and meeting certain behavioral conditions, DTC will be released. We call this release mechanism behavioral cycle release.

Our specific design plan is as follows: Set the release of account DTC to 100 cycles, each cycle is at least 7 days, and each cycle is released in equal amounts, with a total of 100 releases completed. After the account completes the corresponding barter behavior within a cycle, it can obtain the right to release.

Specifically, first, before large-scale KYC, we will build a "flea market" application in the dApp square. The application allows any Delta user to post and buy and sell idle items on it. Trading activities on this application will be organically integrated with the DTC release program. When a user purchases or sells on the "Flea Market" application, the behavior will be automatically transmitted to the DTC release program. Buying and selling behavior that complies with the rules will immediately trigger the release mechanism and complete the due DTC release within the cycle.

The first DTC release will be performed immediately after the user completes KYC, and 1/100 of the total amount will be released. After that, every 7 days, if the user has a valid transaction on the "Flea Market" application, the release of DTC will be triggered. The release amount in each cycle is 1/99, 1/98, and 1/97 of the total amount, until the last 1/1 is released.

At the same time, the condition that effective behavior needs to meet is that one-way buying or selling cannot be carried out for a long time. In the program design, there is a maximum of 3 consecutive one-way behaviors. After exceeding the limit, the amount of the current period will not be released until the transaction direction is changed and restored.

In terms of periodicity, in the actual program design, we judge that a maximum of two times within 14 consecutive days are effective release actions. Doing so helps users schedule their transactions flexibly. In addition to releasable transaction behaviors, users can participate in more transaction behaviors, which is completely free and contributes to better consensus building.

3.13 DID digital identity

When a user enters the Delta application through three-no verification, the system will generate a globally unique 13-digit string for the user as a digital identity DID (decentralized identifier). As a digital identity DID not only carries personal information and credit value, and can manage, receive and send assets. Combined with the implementation of KYC, a unique, authentic and trustworthy binding relationship is formed between the user and the DID digital identity.

In the future, it will be possible for users to authorize and manage other third-party applications or digital twins in the metaverse through Delta digital identity DID.

3.14 Privacy protection and traceability

If an individual's financial status is fully disclosed in the transaction ledger, it may cause anxiety, discomfort, embarrassment or shame. Regardless of whether the property is large or small, exposure to property conditions can have adverse consequences for individuals. Therefore, the right to protect personal privacy cannot be ignored.

At the same time, traceability plays an active role in improving data security and trust. The openness, transparency and traceability of transaction data increase people's trust and security in assets, so that people do not have to worry about data being tampered with or operating in secret.

Therefore, privacy protection and traceability are equally important. We need a reasonable approach to resolve these two seemingly conflicting issues. Delta adopts the design of separation of accounting address and DID digital identity, and the one-way association of DID digital identity and accounting address to solve this problem. The accounting address uses an 18 to 19-bits cryptographic address based on Base58 encoding, which is a variant of the Bitcoin address algorithm. Its purpose is to make it easier for people to distinguish it from Bitcoin addresses and to save storage resources. In this way, all funds and transactions are recorded at the accounting address. Anyone can view and track transactions through the Delta browser, but they cannot find the DID digital identity corresponding to the accounting address. Multiple accounting addresses can be created under one DID digital identity (in order to prevent abuse, when more than one address is created under one DID digital identity, a transaction fee will be incurred for each address created), and a default payment can be set. address. Users can use any address to collect money, and they can also directly use DID digital identity or mobile phone number to collect money. The amount received using DID or mobile phone number will be automatically transferred to the default address. In this way, users can choose between privacy and convenience based on usage scenarios.

3.15 Decentralized multi-chain wallet

The decentralized multi-chain wallet is one of the core features built into the Delta system. Delta multi-chain wallet makes it possible for users to transfer assets, communicate information and collaborate with other blockchains. It can easily receive and send other public chain assets. When users manage these assets, they do not require any private keys, mnemonic words or passwords at all. This convenient, easy-to-use and secure feature is mainly due to Delta's three-no verification protocol and Internet Computer-based ECDSA threshold signatures (Threshold ECDSA signatures) technology. ECDSA threshold signature technology allows people to create addresses on third-party blockchains and perform transfers without possessing private keys. This makes assets hosted in the Delta multi-chain wallet extremely safe and trustworthy.

The Internet Computer implements a novel threshold ECDSA protocol as part of its chain-key signatures toolbox. In this protocol, the private ECDSA key exists only as secret shares held by designated parties, namely the replicas of a threshold-ECDSA-enabled subnet on the IC, and signatures are computed using those secret shares without the private key ever being reconstructed. Each replica of such subnet holds a key share that provides no information on its own (in fact, any set of shares up to a threshold of one third cannot be distinguished from a set of random strings). At least one third of the replicas are required to generate a threshold signature using their respective key shares. Besides the actual threshold signing protocol, chain-key ECDSA also comprises protocols for secure key distributed key generation and periodic key resharing, which are crucial parts of the protocol. This makes chain-key ECDSA signatures much more powerful than any off-the-shelf threshold ECDSA protocol.

Each canister on any subnet of the Internet Computer has control over a unique ECDSA public key and can request signatures for this public key to be computed. A signature is only issued to the eligible canister, i.e., the legitimate holder of this ECDSA key. Each canister can obtain signatures only for its own ECDSA keys. Note that canisters do not hold any private ECDSA keys or key shares themselves. Threshold cryptography can help enable functionality in the trust model of a blockchain that would be impossible to achieve with conventional cryptography alone.^{viii}

3.16 Technical solutions and implementation

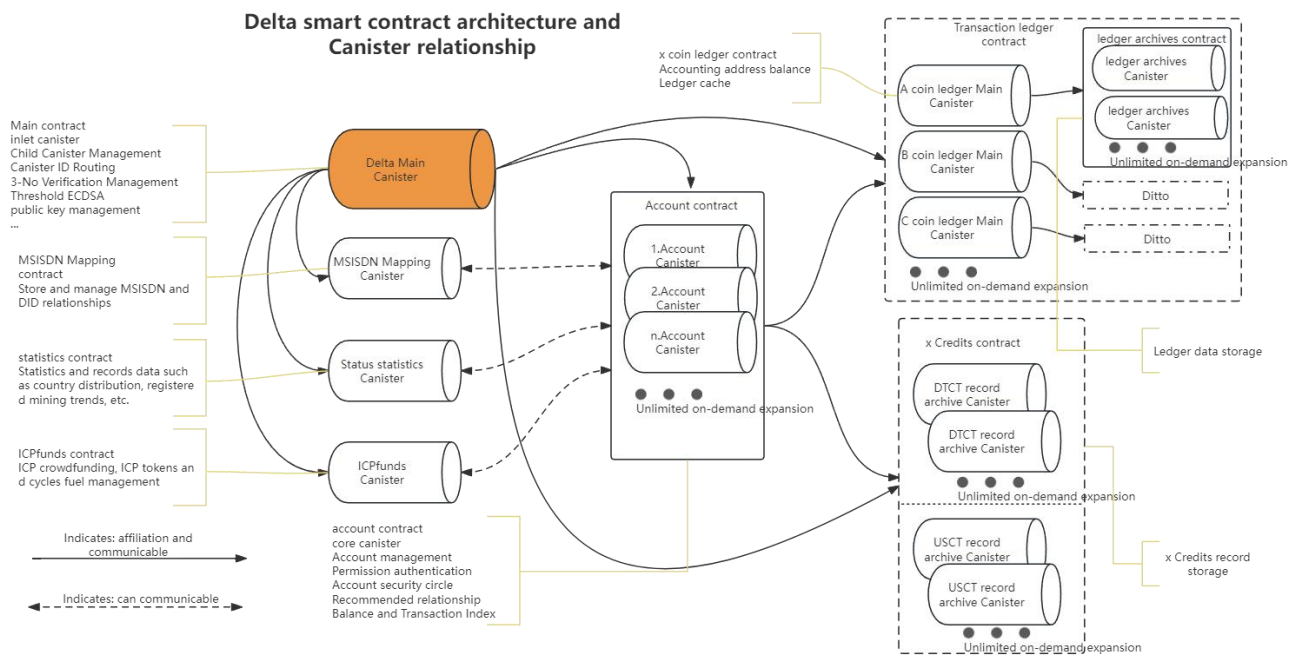
Delta chose Internet Computer (IC) as the basic operating environment and used the Motoko programming language to implement its server-side coding. The complete and complex functions of the Delta system are realized thanks to the powerful programmability and high-speed, low-cost operating environment provided by the IC.

Internet Computer (IC) is currently the world's most advanced smart contract container running platform. This achievement is attributed to Dominic Williams, the founder and chief scientist of the DFINITY Foundation. He led a group of top computer and cryptography experts to conduct years of research, providing a strong and reliable foundation for the implementation of Delta.

Internet Computer (hereinafter referred to as IC) realizes the vision of a world computer - an open and secure blockchain-based network that can host programs and data in the form of smart contracts, and perform calculations on smart contracts in a safe and reliable manner. and infinitely expandable. IC smart contracts are composable and autonomous software components that run on a decentralized blockchain, which makes them unable to be tampered with and stopped. IC gets rid of the speed, storage cost and computing power limitations of smart contracts on traditional blockchains , allowing the full potential of smart contracts to be unleashed. IC allows smart contracts to achieve complete decentralization for the first time.

About the Motoko programming language, it is a new, modern, type-safe language suitable for building smart contracts for next-generation distributed applications to run on the Internet Computer blockchain network. Motoko is specifically designed to support the unique features of Internet Computer and provide a powerful programming environment and capabilities that are familiar to users.

Delta system architecture diagram: (This architecture will be adjusted as functions increase and change)



Note: canister is the running container and basic unit in the IC

3.17 Flags and Currency Symbols

- Symbol: δ , such as 10δ , 100δ , 1000δ .
- Currency code: DTC, derived from "Delta Coin"
- Logo icon: a golden Lello triangle outline with a green bud abstracted from the delta symbol in the center. This sign symbolizes wealth, stability, smoothness, security, reliability and hope.
- Festival: In order to enrich spiritual life and promote communication and development of Delta, we need to define a festival. Starting from 2023, March 3rd every year will be defined as Delta's Day. At the same time, all Delta transactions generated on the day will be completely exempt from handling fees. This transaction fee-free mechanism will be set in the program from the beginning of development.

4. future

4.1 Stablecoin

There is no doubt that sovereign currency is the most popular currency at present, and we look forward to Delta becoming the mainstream super- sovereign digital currency in the world in the future. A stablecoin^{ix} is a cryptocurrency that always aligns with the price of a sovereign currency. This means that, from a value perspective, it can be directly replaced in the current legal currency transaction scenario. Reliable stablecoins are the bridge between non-sovereign currencies and sovereign currencies. We plan to design an inclusive stablecoin that allows every ordinary person to participate in the casting and operation. This will completely trigger the prevalence of non-sovereign digital currencies in the future. We will strive to establish such a stable currency based on Delta during subsequent community discussions and opinion collection processes.

4.2 open source approach

In order to ensure the transparency, fairness and openness of the system, and to gain support from the wider community and become a common currency system for all mankind, Delta's open source will be imperative. The entire Delta system needs to be composed of multiple parts and multiple software projects. These parts need to run in different environments, such as running on the Internet Computer in the form of a server, running on an Android or IOS device in the form of a client, or running in the form of a client. WEB form. In order to protect the Delta ecosystem and prevent source code from being abused, we will gradually open source some software projects

based on development needs. It is expected that when the total number of users reaches 1/30 of the world's total population, we will be completely open source.

4.3 Governance and upgrades

In order to build a lasting governance model and find a balance between efficiency and fairness, Delta will adopt a two-phase plan.

4.3.1 Interim governance model

Before the system is open sourced, a "interim governance model" will be adopted, similar to the current mainstream "off-chain" governance model. In this model, core developers play a very important role in system development and direction. Delta will first launch a "roadmap" subroutine, and developers will first publish the completed parts, ongoing parts, and planned development parts in the "roadmap". In addition, the "Roadmap" subroutine will also have suggestions and voting functions, through which any member of the Delta community can provide feedback and make suggestions. Finally, core developers will further update the roadmap based on these comments and suggestions. This model ensures efficiency and openness, but relies heavily on core developers for impartiality and durability.

4.3.2 DAO mode

After the system is fully open source, it will adopt the "Decentralized Autonomous Organization (DAO) model". Under the DAO model, Delta will establish a "governance committee" and a "developer committee" based on voting by all users, and rely on a service nervous system (SNS). Members of the governance committee will publish and vote on proposals through this SNS system, and the proposals that are finally voted on will be taken over by members of the "Developer Committee" and develop the proposal. After the implementation is completed, it will be submitted to the "Developer Committee" for review and voting. After the vote is passed, SNS will execute the release of the new version of the program. The execution flow of this process will be controlled by SNS. In addition, a "Governance and Developer Reward Fund" will be established to reward governors and developers who invest time and energy into Delta. The cost of the "Governance and Developer Reward Fund" mainly comes from part of the newly issued quota after the transaction fees are burned and the remaining part of the original "Ecological Construction Reward Fund".

Formally, in order to increase people's attention to each upgrade and express the importance of each upgrade, Delta will adopt a naming method related to global

rivers to name each major version upgrade. Specifically, Delta will use the names of the top 100 rivers in the world in terms of river length, in order, as the version names of each major upgrade. This plan was adopted from the geographical term "Delta", which happens to refer to the triangular plain area impacting the mouth of a large river downstream of the sea.

According to "Wikipedia" data, the current top^x 100 river lengths are the Nile River, Amazon River, Yangtze River... Tocantins River.

4.3.3 Proposal Type

In the DAO mode, the operating parameters and upgrades of the system are mainly improved through proposals. We divide the main types of proposals into annual proposals and daily proposals.

Annual Proposal: Represents a proposal that can only be revised and implemented once a year. In order to give this process a more ceremonial feel, we decided to carry out the annual proposal on Delta's Day (March 3rd). Typically, annual proposals involve modifications to wide-ranging system parameters, such as changes to transaction fees.

Daily proposals: All other proposals can be daily proposals.

at last:

The design and creation of Delta did not come out of nowhere. Delta is the result of standing on the shoulders of countless currency revolutionaries and shouters, drawing on their wisdom and summarizing their experiences. Delta's inspiration mainly comes from "Denationalization of Currency", "Bitcoin", "Ethereum", "Internet Computer", "Pi White Paper" and other related books, documents, and projects. Here are some comments on "Friedrich Hayek", "Satoshi Nakamoto", "Vitalik Buterin", "Dominic Williams", "Nicolas Kokalis" and Fan Enlightenment Couple" and other authors expressed their thanks. At the same time, I would also like to thank everyone who has acted and contributed in the field of blockchain and non-sovereign currency. Thank you all.

Haida in 2023

references:

- ⁱ Triffin Dilemma : https://en.wikipedia.org/wiki/Triffin_dilemma
- ⁱⁱ Cambridge Center for Alternative Finance : <https://ccaf.io/cbnsi/cbeci>
- ⁱⁱⁱ Pi Network: <https://github.com/pi-apps>
- ^{iv} Decentralized SMS Verification:
https://github.com/delta-kim/document/blob/main/DecentralizedSMSVerification%20protocol_en.md
- ^v E.164 : <https://en.wikipedia.org/wiki/E.164>
- ^{vi} Gas and cycles cost of IC: <https://internetcomputer.org/docs/current/developer-docs/gas-cost/>
- ^{vii} USDT: [https://en.wikipedia.org/wiki/Tether_\(cryptocurrency\)](https://en.wikipedia.org/wiki/Tether_(cryptocurrency))
- ^{viii} Threshold ECDSA signatures:
<https://internetcomputer.org/docs/current/developer-docs/integrations/t-ecdsa/>
- ^{ix} Stablecoin : <https://en.wikipedia.org/wiki/Stablecoin>
- ^x List of global river length rankings: https://en.wikipedia.org/wiki/List_of_river_systems_by_length