DeFi Ecology Protocol
Decentralized financial ecological agreement

White Paper V3.0

Abstract: in view of the problems existing in the field of encryption and open finance, the defi ecology protocol (its token DFC, hereinafter referred to as DFC protocol) has proposed a solution including the technology components of defi and multiple token based protocols to provide secure, inclusive, innovative and transparent encrypted open financial services to global users.

1 Background

Ethereum smart contract is a great invention. It makes blockchain not only an electronic cash system, but also a Turing machine with logical processing ability. However, based on various considerations such as asset security, Ethereum smart contract has been designed as a mechanism that can not be modified and upgraded from the beginning, which poses a severe challenge to the application development based on smart contract.

First of all, programmers are likely to make mistakes, especially for the complex logic in the contract. Even after strict and repeated logic check and code audit, they still can't ensure that all the codes are correct. The correction of potential problems and the repair of error codes are inevitable. Second, the real world is changing rapidly, and user needs can't be the same. No matter how careful and detailed a product is in advance, after operation, especially after large-scale operation, there will always be problems in the realized requirements and new requirements to be realized. This requires the smart contract to be continuously iterative and upgraded.

Since the first decentralized DAPP was launched, data and asset security issues have always been one of the most critical factors affecting or even destroying DAPP. Asset security incidents emerge in endlessly, which continue to shake the entire industry. How to maximize the system security of blockchain applications and protect user assets has become the primary problem in front of each DAPP development and operation team.

2 DFCA Greement definition

DFC protocol is an encrypted open financial service protocol based on the mainstream blockchain system, which is composed of a set of difi technology components and multiple token protocols. DFC is committed to providing secure, inclusive, innovative and transparent encrypted open financial services to global users.

2.1 DeFi Technical components—— “The DeFi”

In view of the problems existing in the development of Ethereum DAPP, such as the contract is not easy to be upgraded and iterated, the data structure is solidified, the interaction speed on the chain is slow, the user experience is poor, the lack of necessary infrastructure,

and the security problems are prominent. The DFC protocol proposes three major difi technology components, namely basic component, extension component and financial component, collectively known as "DFC". The ultimate goal is to make Ethereum financial services DAPP close to the development iteration speed and user experience of traditional Internet products, and retain its security features.

Ÿ Basic component: APEC (assets protected elastic contracts), flexible smart contract for asset security.

Ÿ Extended components: beams, namely blockchain inquiry, auditing & messaging system, blockchain query, audit and messaging system.

Ÿ Financial components: gel, namely global emergency lockdown; calm, cooperative automatic lockdown mechanism; Mak, multisig admin keys, the administrator key of multi signature.

2.2 Token agreement—— “DFC-Tube”

Based on the difi technology components, DFC protocol integrates bond financing protocol, currency lending agreement and decentralized stable currency protocol to form DFC tube encryption open financial service platform. DFC tube will provide investment, financing and transaction services of encrypted digital assets for individual and enterprise users to meet the needs of different users for encrypted digital finance.

Ÿ DFC-Tube Bond： Bond financing agreement, fixed term, fixed rate digital currency lending services;

Ÿ DFC-Tube Bank： Currency lending agreement, algorithm driven current and variable interest rate card deposit and loan service;

Ÿ QIAN： The decentralized stable currency protocol is committed to becoming an influential stable currency project in the field of encryption and digital technology. Qian

stable currency can be used to invest in DFC tube bond or deposit in DFC tube bank for interest.

The above three protocols promote each other and have a high correlation among services, which can form a aggregation effect and is conducive to the collaborative development of business.

3 DeFi Technical components

3.1 Basic components APEC

The APEC platform based on the solidness language is the main basic component of the defi protocol. APEC is assets protected elastic contracts, an elastic smart contract for asset security.

3.1.1 Design concept

As the core architecture of on chain, APEC is based on the solid smart contract and adheres to the decentralization and asset ownership, and adjusts and optimizes the inconveniences in contract development.

The core concepts of APEC are asset security and component resilience, which mainly include the following three aspects of characteristics:

- Assets Protected

- Logic Upgradable

- Data Extensible

3.1.2 Data scalability

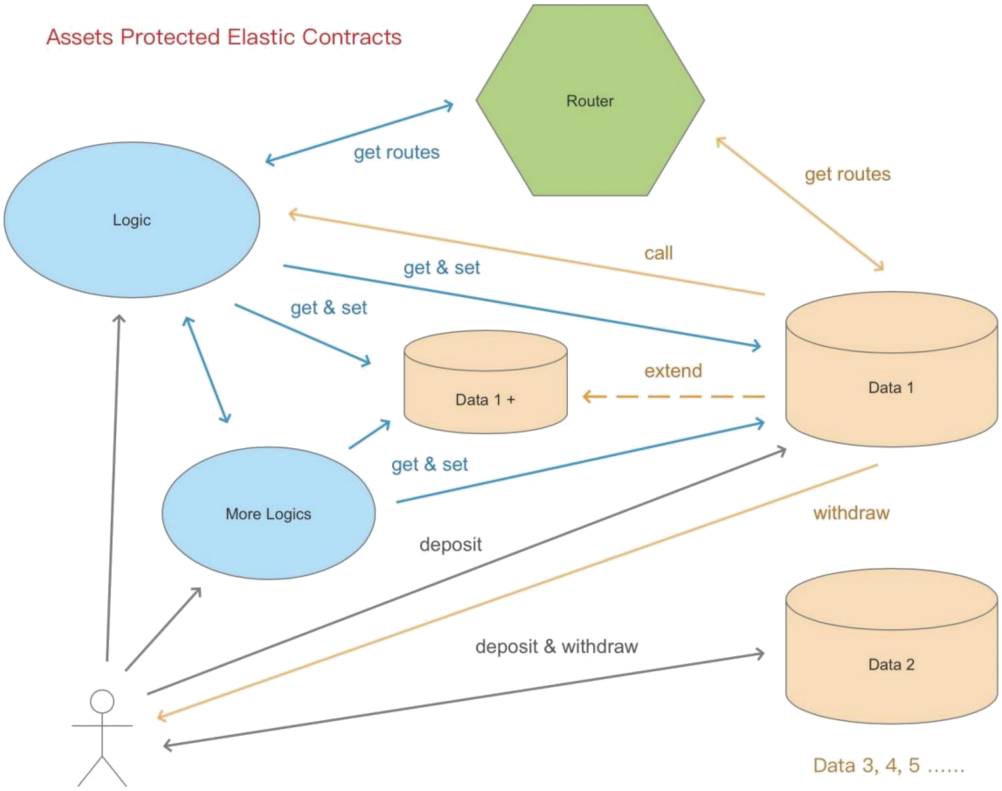

Figure 1 APEC technical architecture

3.1.3 Technical framework

APEC can be divided into three modules：

Ÿ Data: the data part of the classic contract structure is separated and made into a data contract or a group of data contracts, which is used to store data, and only the necessary read-write interfaces are exposed.

Ÿ Logic: the logical contract is responsible for pure business logic without business data.

Ÿ Router: the field data that needs to be read and written by the business logic can be queried from the routing table according to the data module and field name, and then accessed according to the positioning results.

Routing table

The routing table is an independent contract, including a routing comparison table, which stores the routing mapping of logical contract and data contract address, and can be updated continuously with system upgrade.

After the contract system is deployed, the address of each logical contract will be stored in the routing table. External requests can access the routing table, obtain the address mapping of the logical contract and call its interface. The data contract can also obtain the logical contract address by querying the routing table for business logic call or callback.

For each group of data, there will be an independent data contract of its own, and the address of the data contract will be automatically stored in the routing table when it is created. Before accessing the specified data, the logical contract will first obtain the data contract address from the routing table, and then read and write the data contract through the address.

Logic can be upgraded

Logical contract does not store assets and does not contain business data, so there are no problems such as asset security and data migration, so it is scalable and pluggable. After testing and auditing, the new version of logical contract can be deployed to the chain.

When a new contract is deployed, the mapping table data in the routing table contract will be updated at the same time, and the address mapping point of the logical contract in the routing table will be changed for query and call by other contracts or application front-end.

Data scalability

As an application that can be iterated and upgraded, its data structure is often required to be iterative. However, due to the consideration of data ownership and asset security, the data contract cannot be upgraded. The solution we've adopted is expansion. If the business needs to add new fields, these fields will be stored in a new data contract. At the same time, the address and field name of the new data contract will be added and updated to the routing table. The business logic obtains the address route of the new field by querying the routing table for reading and writing.

The expansion of data contract should be restrained and limited. Blindly adding new data contracts will improve the complexity and efficiency of the whole system. The data extension mechanism only makes the requirement of data structure iteration impossible to possible, and it is not encouraged to use this mechanism frequently and arbitrarily.

When we design and use data structures, we still need to follow the classic design principles and best practices of contracts to design adequate and flexible data structures. For data expansion, we should always keep a restrained attitude, and do not use data expansion mechanism when it is not necessary.

3.1.4 Asset security

If the logical contract can be upgraded and the data contract can be extended, then the following question is whether the user's data ownership and asset security can be guaranteed.

As we all know, for traditional defi applications, all of the user's assets are locked into the contract. Smart contracts, especially open source contracts, guarantee users that no one or program can touch the assets locked in the contract except users themselves. Furthermore, the immutability of the contract makes it impossible to change the code once the contract is deployed.

APEC adopts the method of separation of responsibilities to solve the security problem of contract assets under the scalable architecture.

Business contract can be modified and upgraded, while data contract adheres to the concept of classic contract and cannot be modified and upgraded. During initialization, an initial data contract is automatically generated for each data set. Once the contract is deployed to the chain, its code logic cannot be modified.

Ÿ Data contracts maintain a mapping table of user addresses and asset details internally. In the data contract, the mapping table only provides two interfaces of user asset entry and accounting, and no other interface has the right to write and update the asset table.

Ÿ The user records the transaction directly to the data contract address and calls its entry interface. After the user's assets are locked into the contract, the user's address and asset details are recorded in the asset mapping table. Then the logic contract is called to process and record the business logic.

Ÿ When the user enters the account transaction, it still calls the interface of the data contract directly. The contract will verify whether the user's address exists in the asset mapping table, then call the logical contract, calculate the amount of the account, and transfer the assets directly to the user's request address.

Ÿ For any address that is not in the asset mapping table, the billing interface will not respond to its asset request. In logic, it ensures that any asset out of the account belongs to the original address of the original investment entry, which ensures the ownership of the investment asset and the security of the user's asset. Even the operation team itself can not tamper with and falsely claim any locked assets of users.

Through strict ownership constraints of data contracts, the ownership and security of user assets are guaranteed, which makes APEC's security philosophy adhere to the consistent concept of smart contracts: it goes beyond "don't be evil" and realizes "can't be evil".

3.2 Extension components BEAMS

BEAMS is Blockchain Enquiring, Auditing & Messaging System， Blockchain query audit and message system.

3.2.1 Limitations of blockchain

Blockchain is almost completely separated from the real world. It cannot actively push messages down the chain. If the logic of the smart contract fails or is attacked, the real world cannot be passively perceived. Therefore, we need to continuously monitor the operation of the contract, strictly audit the data and assets in the contract, and give an alarm at the first time when there is a problem, so as to ensure the security of the application as much as possible.

For users, the interactive experience of blockchain is naturally unfriendly. Asynchronous feedback caused by block delay, frequent and large amount of on chain data reading and business model reconstruction, and message fragmentation on and off the chain all cause slow experience and even confusion in interaction.

3.2.2 Design concept

The existence of the above problems urges us to build a system connecting the chain and the chain, continuously monitor the operation of contracts, audit data and assets, accelerate the response speed of products, smooth the fluctuation curve of response speed, and make the inevitable asynchronous feedback more smooth and smooth. Various status reminders and message push triggered by conditions can enable users to obtain a more user-friendly product experience in addition to solving financial needs by using the defi application.

Beams is an off chain system which closely cooperates with contracts

3 features

- Enquiring
- Auditing
- Messaging

3.2.3 BEAMS Architecture diagram

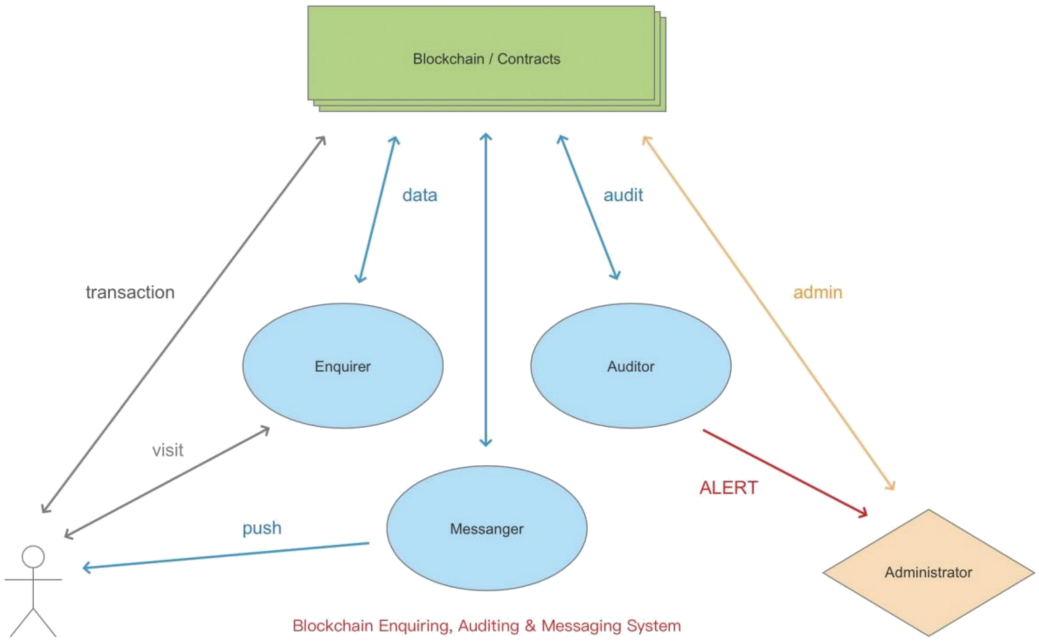

Figure 2 technical architecture of beams

3.2.4 Technical architecture

Beams consists of three modules: Enquirer, auditor and messenger.

Beams adopts the round robin mechanism based on the event on the chain to monitor the change of contract status and data on the chain. The basic data will be stored in the database and provided to the front-end interface through the interface. The change of contract data will be audited in real time, and the abnormal situation will be reported to the system administrator. At the same time, the change of collateral value and liquidation status are continuously calculated, and various forms of notification and alarm are actively pushed to relevant users when necessary.

Data query

Core transactions involving asset changes will trigger custom chain events. The query system continuously monitors the generation of new events and queries the corresponding contract data according to the event content. The data contract provides a read-only interface for exposing data to the outside, and the query system reads the relevant data from the contract according to the requirements of the data model.

The read data will be collated and aggregated to the data warehouse of beams, and the data changes will be recorded. As the data core of the whole system, the data warehouse will

provide quasi real-time data cache to the front end through the back-end API interface, and provide the required data for calculation and trigger to the message module. The audit module will also use these data to review and audit the status transition and data changes of the contract on the chain.

Audit risk control

The audit risk control module will continuously monitor the status and data changes of each contract. For the asset changes involved, the audit risk control module will use independent and parallel logic to review the asset changes. If there is any abnormality, the system administrator will be informed in real time for processing.

The audit risk control module will use different review methods such as total assets, change logic and status verification to audit the contract data in real time from all directions, so as to improve the accuracy of the audit. The audit module can grade and alarm the abnormal situation, and the risk control module will even have the right to intervene and manage the operation of the contract on the chain in the scenario of extremely high risk.

The audit risk control module will also be responsible for the statistical analysis of the user's order record, historical income, asset change curve, platform real-time income index, historical income curve and other system operation data, predict and control risk points, and provide data reference for product operation direction.

Message push

In order to improve the user experience of asynchronous feedback due to the characteristics of blockchain, message push module will play an important role in all aspects of the user use process. Especially in the aspect of reminding notice and warning message related to user's own interests, the blockchain which lacks infrastructure needs message push system to cooperate.

On the side of the page, the message push module will give priority to the websocket long connection mode, establish a two-way real-time link with the user through the front-end page, monitor the execution of the transaction on the chain at each link that needs to execute the transaction on the chain, and push the transaction result and the status on the chain to the user after the transaction.

For the information of asset liquidation, income release, redemption reminder, etc., the message push module continuously monitors and analyzes the contract data. After reaching the trigger conditions, various methods including email and SMS can be used to push the reminder notice and warning information to users in real time.

3.3 Financial components

3.3.1 DeFi Three laws of financial security

The security philosophy of defi can be summarized as the three laws of financial security in the concept of hierarchical defense

Ÿ Protect the platform from attack and intrusion

Ÿ Protect assets in case of intrusion

Ÿ If the asset is no longer safe, minimize the loss

Defi financial security system is a multi-level and all-round system. Decentralization is the core and the foundation, but it is not the only and the whole. An open financial application with good scalability, able to cope with tens of millions of users that may exist in the future, is safe and reliable with complete risk control capability. If only relying on decentralized infrastructure, it is impossible to build a successful financial application.

3.3.2 GEL

Gel means global emergency lockdown.

In the defi system, all smart contract interfaces involving asset changes have global emergency locking switch. If there is a problem with the contract, the emergency locking can be triggered manually or automatically to prohibit all the transfer of accounts in and out, so as to protect the security of the assets locked in the contract.

3.3.3 CALM

Calm (cooperative automatic lockdown mechanism)System.

Calm is an off chain risk control mechanism, which adopts financial level risk control standard, uses independent high availability master-slave hot standby cluster, and operates continuously for 7x24 hours. Calm checks the contract status every 5 seconds, strictly bookkeeping and reconciliation of all financial assets in the contract. Once possible asset risk is found, it will automatically trigger the global emergency locking, prohibit all the entry and exit interfaces of the affected assets, and minimize the asset loss. At the same time, inform the management personnel, start the rapid response mechanism of the operation team, and manually intervene and check the problems.

3.3.4 MAK

The administrator key mechanism is adopted in defi. The administrator can use the key to set all levels of permissions, such as updating the contract route, feeding authority of Oracle machine, setting permission of global blocking flag bit, etc. The administrator key can add, delete and update the subordinate authority. When the subordinate authority key is leaked, the key can be changed quickly.

In order to avoid the risk of the key being stolen and lost, we adopt the multi signature mechanism. At present, 3-2 multi signings are used. With the increase of platform locked assets, we will gradually upgrade to 5-3 or even 7-5 mechanism.

Taking 3-2 multi signature as an example, three administrator keys are saved in the contract. When performing operations with the highest security level, such as changing the administrator key, at least two administrator keys must be used and multi signature must be performed at the same time.

The multi signature mechanism of the administrator key ensures that:

If an administrator's key is leaked, the attacker can't complete the operation of high privilege level with this key. The platform administrator can use the multi signature mechanism to delete the leaked key and make it invalid.

If an administrator key is lost, you can use the remaining administrator key to add a new administrator key and delete the missing key.

The mechanism of multi signature of administrator key makes every high-level authority operation depend on collective decision-making and execution, effectively preventing internal control risk and further protecting asset security.

4 Token agreement

4.1 Bond financing agreement——DFC-Tube Bond

Crypto bond is a new type of bond issued and recorded in the form of token. It can not only provide financing services for teams or individuals holding encrypted assets, but also supplement fixed income products to crypto money market to meet the needs of some investors. DFC tube bond will provide a complete set of solutions for encrypted digital bonds, including credit rating, bond issuance, bond clearing, bond trading, etc.

4.1.1 Bond credit rating

Limited by the fact that the current crypto financial services are still immature and not suitable for the issuance of medium and long-term bonds, the current crypto digital bond products will be mainly short-term bonds. The issuance of encrypted digital bonds adopts the registration system, which does not need to be reviewed and approved by any centralized organization. The basic information of bond issuance submitted by bond issuers will be automatically verified by the DFC tube platform. After the credit rating of the bond issuance information is determined by the DFC tube community, the bonds can be officially issued.

Bond credit rating is to evaluate the default risk of bonds and provide reference for users' investment decisions. The DFC tube platform adopts the following bond credit rating table.

The bond credit rating of DFC tube platform consists of community rating and professional rating. The community rating is carried out by the holder of DFC agreement ecological token. The rater will lock the DFC to the corresponding level after knowing the bond information, and then the DFC token can be retrieved after the rating. Professional rating is performed by professional credit rating agencies or professionals. To become a professional rater, an application should be submitted to the DFC tube operation team to provide materials that can prove their professional ability and qualification. The final rating results will be jointly determined by community rating and professional rating, with

community rating weight of 60% and professional rating of 40%. Participating in rating will receive rating service fee, which will be distributed in equal proportion.

4.1.2 BondTokens

After the bond credit rating is completed, the encrypted digital bond can be issued. Each bond is issued in erc-20 format, which is called bondtokens. Bondtokens are investment certificates obtained after investment in bonds. Each type of bondtokens has its own erc-20 contract, which contains all the necessary information and related operations of the bond. Bondtokens can be transferred freely, but they are indivisible, and their face value is usually 100 USD. The creditor who owns bondtokens is the creditor in the creditor debt relationship. The principal and income can be cashed on the DFC tube platform if the bondtokens are owned.

Bondtokens is a new type of encrypted digital assets. Bondtokens with different pledge assets, different maturity dates, different interest rates and different credit ratings can meet the diversified needs of the encrypted digital asset market and become the cornerstone of other innovative financial applications.

4.1.3 Bond liquidation

If the underlying pledged assets of bonds have a significant depreciation or the issuer fails to repay on time, the liquidation of the pledged assets will be involved. DFC tube platform currently adopts the discount clearing mode, that is, the liquidator can exchange the pledge at a discount price.

To facilitate calculation, the following parameters are set: set target pledge rate as TCR, total current debt CD, current pledge rate CCR, discount rate, current price of pledge, and remaining quantity of pledge before liquidation AC. The discount rate (1-dicount) is the liquidation reward to the liquidator.

Liquidation within the duration of bonds

During the duration of the bond, when the value of the pledged property decreases by 20%, the system will send a replenishment reminder to the debtor. When the value of the pledge drops by 30%, the system will trigger the disposal of the pledge, and the system will liquidate some of the collateral to make the pledge rate return to the initial value.

Liquidation of overdue repayment

After the maturity of the bonds, if the debtor fails to repay, the system will trigger the disposal of the pledge. The system will clear part of the pledge to repay all debts and service charges, and the remaining pledge will be returned to the debtor.

4.1.4 Bond trading market and bond derivatives

In order to facilitate bondholders to withdraw from investment ahead of time and recover the principal and interest, the DFC tube platform will launch a secondary bond trading market in the future. Bondholders can freely set the transfer price and transfer quantity on the reference price given by the system. Investors can view the basic information of bonds, credit rating information, expected income, etc. After paying the investment funds, the investors can obtain the bond tokens of the corresponding bonds, and can cash the principal and interest on the platform after maturity. With the popularity of bondtokens, DFC tube platform will continue to launch more functions to support various bond derivatives, including:

Ÿ Bond repo (including reverse repurchase); and;

Ÿ Callable bonds (i.e. the bond issuer can redeem the issued bonds before the maturity date of the bonds);

Ÿ Callable bonds (i.e. bondholders can sell back the bonds to the issuer before the maturity date); and;

Ÿ Other bond derivatives meeting the business needs.

4.1.5 Bond module community governance

DFC tube is committed to promoting decentralized (or polycentric) bond issuance and settlement. System permissions and core parameters will be managed by the community in the future. However, in the early stage of the project, in order to quickly promote the development of the project and the platform, the system permissions and parameters will be maintained by the DFC tube developers. DFC tube developers will adhere to the principles of fairness and transparency, and inform the community of any changes to the system. Currently, the system parameters maintained by DFC tube developers include but are not limited to:

Ÿ Supported encrypted digital assets and their pledge rate, maximum number of bonds to be issued, clearing discount, etc;

Ÿ The basic parameters of bond issuance, such as coupon rate, bond maturity, issuance cost, rating service fee, etc;

Ÿ Credit rating, repayment period, etc;

Ÿ Bond credit rating setting;

Ÿ Bond credit rating setting;

4.2 Cryptocurrency lending protocol——DFC-Tube Bank

DFC tube bank is an encrypted digital currency deposit and loan protocol, which supports deposit and withdrawal, and loan and return. Through the automatic program (smart contract) deployed on the blockchain system, investors can quickly obtain capital gains without friction, and borrowers with capital needs can quickly and conveniently obtain financial support after providing appropriate collateral.

4.2.1 Design ideas

DFC tube bank supports users to deposit their digital assets into smart contracts to earn interest income and obtain loan line. Users can borrow other digital assets within the loan limit. Whether it is a deposit or a loan, the user does not need to pay attention to the term of the loan and withdraw or repay at any time.

When the borrower's outstanding loan exceeds the limited proportion of its collateral, the system will seize the user's assets and enter the liquidation process. At this time, arbitrage is allowed to call the liquidation contract to replace the seized assets according to a certain discount ratio. Due to the differences in market scale, liquidity and price stability of different digital assets, there will be differences in pledge rate and liquidation discount.

4.2.2 Interest rate model

DFC tube bank adopts a set of algorithm controlled interest rate model. Based on the change of supply and demand, the interest rate is adjusted automatically, so as to adjust the total scale of loan and the amount of capital supply.

For the regulation of loan funds, bank The following principles should be followed: when the amount of money lent in the loan pool is low, the lending interest rate will rise at a lower rate, so as to promote the borrower to borrow from the fund pool; when the loan amount of the loan fund pool is high, or even close to saturation, the loan interest rate will rise rapidly, driving the increase of deposit interest rate, so as to promote depositors to deposit more assets into the fund pool. Through the algorithm adjustment, the development and growth of the whole loan fund pool is in a healthy range.

DFC tube bank divides the change of interest rate into three stages:

Ÿ In the first stage, in order to stimulate the increase of loan volume in the initial stage, the interest rate growth model approximates the exponential curve, which also conforms to the natural growth law;

Ÿ In the second stage, by accumulating a certain amount of loans, the growth rate of interest rate has entered a stable period, and its graph is a straight line with a certain slope;

Ÿ In the third stage, the increase rate of lending interest rate will accelerate due to the large amount of funds lent. With proper control of the lending rate, the deposit volume will increase, and the rate of interest rate increase will gradually approach an extreme value. The change of interest rate in this stage is close to the modified index curve.

4.2.3 Interest rate calculation

4.3 Decentralized stable currency agreement——QIAN

Qian is the same as Qian and Qian. In the book of changes, qiangua represents the heaven, represents the law of the universe, and is the most noble spirit and positive energy. Following

this important implication, we named the decentralized stable currency agreement Qian. Qian is committed to creating a stable currency system in which everyone can participate equally, freely and conveniently, so that everyone can enjoy financial services without discrimination and discrimination.

4.3.1Design concept of Qian

Users who hold encrypted assets only need to lock the excess encrypted assets to Qian's smart contract, then they can obtain Qian stable currency equivalent to legal currency without paying any interest. Stable currency Qian is regarded as the proof of currency exchange between smart contract and crypto asset holder. We named the smart contract under this mechanism as CSA (currency swap agreement).

No interest cost of holding CSA

As a liquidity provider, the CSA holding qian does not need to pay any interest, on the contrary, it may obtain interest from smart contracts as additional income, which will stimulate creditors to hold the CSA of Qian for a long time, making it possible for Qian to be used in cross-border payment, consumption payment, asset trading, lending and other economic activities. Without holding cost, qian can really participate in the development process of encryption and open financial ecology, develop together with the stable currency guaranteed by French currency without holding cost, and serve users with different needs.

Support flash loan

At present, it is known that flash loan is a safe technology. Any smart contract with assets can choose to provide flash loan service externally. By charging a certain amount of loan interest, it can use its own assets to increase more income. At present, the aggregation tools of flash loan have appeared in Ethereum defi ecology. By aggregating the traffic of smart contracts supporting flash loan, more powerful lightning loan service can be provided. Qian's smart contract will support flash lending. The encrypted assets locked in the Qian smart contract can obtain additional income. The operator of Qian system will regularly use the income to buy DFC token in the market. As the value storage carrier of Qian's smart contract income, DFC will be locked into the smart contract that keeps the revenue of Qian system.

Risk Management

In the design of Qian, we follow the following risk management rules:

First of all, the proportion of Qian to the value of assets generated by Qian should be greater than 120.0% of Qian's asset value. When the Qian is used to generate the asset value, the ratio should be at least 120.0%.

Secondly, in order to increase the security of the locked assets in the CSA, avoid the explosion in the extreme market, and take into account the utilization rate of the encrypted assets, Qian will introduce the volatility factor according to the change speed of the market price of the encrypted assets to regulate the asset lock-in multiple of the CSA. When the price rises or falls unilaterally, the volatility will rise, and the system will increase the start-up adequacy ratio of CSA. When the market is relatively stable, the volatility decreases, and the system will lower the start-up adequacy ratio of CSA. This design will effectively reduce the impact of market fluctuations on the CSA lock up assets, encourage users to lock positions in a stable state of the market, and increase the security of locked assets.

Third, when the market price falls sharply, the user's CSA adequacy ratio will decrease. In the process of decline, CSA has two changes: warning state and freezing state. For example, if a user holds the CSA of eth, when its reserve asset adequacy ratio drops to 150% (the warning line of ETH), the Qian system will prompt the user to make up the position. At this time, if the market continues to plummet and users have no time to make up positions, the adequacy ratio of CSA will continue to decline. When it is lower than 120%, the smart contract will freeze the user's CSA until the user replenishes the locked assets above the safety level. The user will not be able to initiate the redemption of the locked object through his own address before replenishing the locked asset.

Fourth, the frozen CSA may be liquidated, allowing non CSA holders to redeem the assets in the frozen contract with Qian according to the value of Qian generated by all frozen CSAs. This part will be elaborated in the following chapter on smooth arbitrage mechanism.

Under the extreme market conditions, the adequacy ratio of some or all reserve assets in Qian system may be less than 100%, which leads to insufficient support of internal value of Qian. If CSA holders generally have no intention to replenish the lock-in, and the market price of the underlying reserve assets has not recovered for a period of time, this will form a reserve gap (debt) in the Qian system. In this case, the system will start the global debt auction after the overall reserve adequacy ratio continues to be lower than a certain level and after a certain observation period.

In the global debt auction, the system will unfreeze the governance token DFC provided by DFC foundation and conduct external auction. The proceeds from the auction will be used to make up for the reserve asset adequacy ratio of the whole system.

4.3.2 Lock in management

Qian is generated by users locking encrypted assets to smart contracts. At the initial stage, the underlying assets will be mainly encrypted digital currencies such as Eth and erc-20 version BTC. After the system operates stably for a certain period of time, it will be considered to include crypto assets such as token, which have a consensus, as collateral for issuance.

4.3.3 Price fluctuation buffer mechanism

Design concept

At present, the mainstream crypto asset pledged stable currency lacks the mechanism to adjust the closing position and mortgage operation based on the volatility index, which results in that the stable currency system can not effectively buffer the impact of market fluctuation on the pledged assets in the face of extreme market conditions When the market falls sharply, it is easy to cause the loss of pledged assets, which will affect the balance of the whole stable currency system.

Therefore, in the design of Qian system, we consider the influence of price, volatility and time on the underlying reserve assets. The purpose of introducing volatility parameter into Qian stable currency system is to reduce the disturbance of asset price on the equilibrium of stable currency, so as to maximize the overall equilibrium of the system.

Volatility index

Qian will introduce the volatility index VI as an important indicator to measure the volatility of underlying reserve assets. The price of any asset will rise or fall. When the price rises or falls rapidly, the underlying reserve assets VI of the stable currency will increase and the pledge risk will gradually increase with the acceleration of the return rate. At this time, by increasing the starting adequacy ratio Qi, 0 and suspending the liquidation operation, the impact of price fluctuation on the security of underlying reserve assets can be effectively buffered. When the price of the underlying reserve assets of the stable currency gradually tends to be stable, VI decreases and the risk of pledge is released. By reducing Qi, 0 and restoring the liquidation operation, the deviated Qian price can be returned.

Daily realvol

In the traditional derivatives market, the yield, or realized volatility, especially the daily real volume, has been widely accepted as the basic calculation parameter of option volatility index (such as rvol and rvov). Due to the particularity of cryptocurrency transaction, it is necessary to redesign the daily real Vol formula of traditional market as the basic parameter for calculating the volatility of reserve asset I of stable currency.

4.3.6 Global liquidation

Although we are optimistic about the development of encryption assets for a long time, we must also face up to such a situation: the encryption assets are still in the early stage of the overall development, and the market explosion and fall often occur. In the past market records, there has been a bear market for several years.

Although Qian stable currency has a series of stabilization mechanisms, it is still possible that even through debt auction, the reserve asset adequacy ratio of the whole system can not be compensated even in the case of extreme market conditions and long-term market downturn. If this happens and lasts for a while, it will mean the whole Qian

The stable currency system has lost the support of its intrinsic value. In this case, we will discuss whether to carry out global liquidation and close the Qian stable currency system through the process of community governance. Once the community governance has passed the closure of the Qian stable currency system, the global liquidation will be started.

In the global clearing state, Qian stable currency system will first freeze all the CSAs, turn off the generation function of the CSA, and then turn off the Oracle machine feeding price, and take the price of the last Oracle machine feeding price as the reference quotation for the global clearing of the system. At this time, the system state changes again. Based on the last Oracle quotation, users holding CSA (normal) will be able to redeem their locked assets from the contract first, and the system will process the asset redemption operations of these users. After the completion of the redemption of assets by the holding users of CSA (normal), if there is still a surplus of reserve assets in the system, the holding users of CSA (alarm) will be allowed to redeem.

In the global clearing state, it is uncertain whether the user can take back all the locked assets without loss. The probability of full redemption of locked assets is CSA (normal) > CSA (alarm). Different factors such as the number of underlying reserve assets, market price and other factors will have a comprehensive impact on the probability of successful redemption

4.3.7 QIAN System governance

The main participants of Qian system include Qian foundry, Qian holder and DFC holder. The purpose of system governance is to balance the interests of all participants and maintain the stability and sustainable development of the system on the basis of certain trade-offs and trade-offs.

The main risk of Qian foundry in the system is the redemption risk caused by the fall of reserve asset price and the lock-in of the system. The benefits of Qian foundry include obtaining liquidity, value storage, risk hedging and other functions. Based on the study of similar schemes in the industry, we believe that the casting of Qian should be encouraged within a reasonable risk range, which is conducive to the development of Qian system, so we design an adjustable interest mechanism. The core demand of Qian holders lies in the stability of their exchange rate. Therefore, we have designed the exchange rate stability adjustment mechanism.

The DFC holder will be the bearer of the final profit or risk of the whole system. The management of the platform is determined by the DFC holder's vote. The proposal selected by the vote can modify the internal management variables of the Qian platform. These variables include but are not limited to:

- Add new reserve assets
- Choose a trusted Oracle
- Adjustment of interest
- Adjust the interest rate of flash loan
- Risk parameters: debt ceiling, initial lock-in ratio, redeemable upper limit and warning line of each reserve asset.

5 Ecological expansion

At present, DFC protocol has basically completed the development of profi technology components on Ethereum, as well as the development of token based protocols such as bond financing, currency lending and decentralized stable currency. In the future, we will extend these token based protocols to other blockchain systems, including eth2.0, coin security chain and Boca.

5.1 Ethereum 2.0

Eth 2.0 is a new generation of Ethereum. It's totally different from the blockchain architecture. The goal of eth 2.0 is to improve the scalability, security and programmability of Ethereum. Unlike eth 1.0, which can only achieve a throughput of 15 TPS, ETH 2.0 can process thousands to thousands of transactions per second without reducing the degree of decentralization.

Eth 2.0 is a great leap forward. Its fragmentation technology will make it possible for the mainstream chain to anchor currency. In fact, it will become a cross chain system connecting all blockchains. If eth 2.0 achieves this, combined with its high concurrent transaction execution capability and POS features, it will become a model of cross chain platform.

DFC protocol will make full use of the huge technical advantages of eth 2.0. As soon as the main chain is upgraded, the current application will be smoothly migrated to the latest stable version, closely following the pace of Ethereum upgrading, leading the development trend of business model and technology upgrading of the difi financial platform.

In addition, based on the POS characteristics of Ethereum 2.0, users who lock their eth assets into Qian, bank and other smart contracts will still be able to obtain eth mining rewards. Qian, bank and other contracts can form a similar function to the mine pool in the future, while continuing to provide the original financial services to maximize the use of users' eth assets and create more value.

5.2 Currency security chain and currency security intelligent chain

Binance chain is a community driven blockchain software system composed of developers and contributors from all over the world. It is a public chain focusing on transferring and trading blockchain assets, focusing on performance, ease of use and liquidity. It is a public trading chain tailored for DEX. Coin security chain has launched bep2 token standard, which can issue user-defined token on it. In particular, the coin security chain has

supported the mainstream token anchored currencies, such as BTC, ETH, XRP, BCH, LTC and TRX. These anchor coins, combined with cosmos based cross chain characteristics of coin security chain, provide unlimited imagination space for DFC protocol cross chain difi financial application.

In 2020, the development team of coin security chain released a solution to expand the function of currency security chain through parallel chain: coin security intelligent chain. The scheme keeps the high-performance matching of coin security DEX, and realizes the function of smart contract friendly to developers.

Combined with the second level transaction and high TPS characteristics of coin security chain, bep2 mainstream anchor currency, and EVM compatibility of coin security intelligent chain, the application of DFC protocol on Ethereum can be extended to coin security chain and coin security intelligent chain ecosystem seamlessly. At that time, based on the currency security chain ecology, through the value swap of mainstream token, highly concurrent financial transactions and good compatibility with virtual machines, DFC tube will become an important cross chain difi financial platform.

5.3 Polkadot

Boca is a platform that allows different blockchains to transmit messages, data and values in a way without trust cost. They can share their unique features and security at the same time. Simply put, poca is a scalable heterogeneous multi chain technology. Boca is the leader of independent cross chain technology. Its concepts of relay chain, parallel chain and transfer bridge may become the de facto standard of general cross chain technology. Through the cross chain system of Boca, the mainstream chain will carry out good token value exchange and transaction coordination through cross chain mechanism.

DFC protocol will continue to conduct in-depth research and Practice on poca, and carry out prototype verification and adaptive development of DFC protocol application based on poca system. With the improvement and gradual launch of Boca system, DFC protocol will consider gradually expanding DFC tube system into Boca ecology, and ensure the continuous competitive leading position on the cross chain financial application track.

6 DFC Agreement ecological token

6.1 DFC Usage of pass

6.1.1 Participate in DFC tube bond rating vote

Community raters can participate in bond credit rating if they hold DFC agreement Eco circular. After knowing the bond issuance information, the voter will lock the DFC to the voting grade, and the DFC lock can be released after the rating is finished.

Professional rating is conducted by professional credit rating agencies or professionals. To become a professional rating agency or individual, it is necessary to submit an application to the DFC tube operator (the approval authority in the later stage will be handed over to the DFC tube community), provide materials that can prove professional ability and qualification, and lock a million DFC certificates to the system. The lockdown pass cannot be retrieved during the rating period and the duration of the rated project.

6.1.2 The stability of Qian participation

Through the flash loan, the encrypted assets locked in the Qian smart contract can obtain additional income. The Management Committee of the Qian system will buy the DFC token in the market with the income obtained from the regular use. As the value storage carrier of the revenue of Qian smart contract, DFC will be locked into the smart contract that keeps the revenue of Qian system. When the Qian system thinks that it is necessary to motivate the mints to improve the circulation of Qian, the system will pay interest to the newly created CSA users. The interest paid is calculated by the value of the DFC token, and the interest paid is also DFC.

6.1.3 Participate in global debt auction of Qian

In extreme cases, the global asset adequacy ratio of Qian system may be less than 100%. If the market environment continues to be depressed, the arbitrage intention of arbitrage will be insufficient, and the value of reserve assets in the system will be insufficient, which will lead to the overall debt. In order to maintain the intrinsic value of Qian system, the system will unlock the governance token DFC and make up the balance of the overall reserve assets through auction, so as to make the overall adequacy ratio return to the safety line.

6.1.4 Participate in the governance of DFC tube

The governance of DFC tube platform is carried out through the voting of DFC holder. The proposal selected by voting can modify and adjust the system key variables of DFC tube bond, DFC tube bank and Qian.

6.2 DFC Pass distribution plan

The total amount of DFC circular is 1 billion, and it will never be issued again. Under the leadership of the DFC agreement initiation team, 85% of the token will be used for community construction and community donation programs, of which 30% are for community ecological construction and DFC agreement

Foundations account for 25%, and strategic investors and community donations account for 30%. The remaining 15% of the token will be reserved for the DFC agreement founding team and the DFC tube development team as a reward for their contribution at the beginning of the project and as an incentive for subsequent new team members. The token allocated to the team was locked for 3 years and was publicly traded for the first time

30% was released after 12 months, 30% after 24 months and 40% after 36 months.

6.2.1 Community ecological construction

Community ecological construction includes but is not limited to: DFC tube ecological governance and incentive, developer community construction, business cooperation and industrial cooperation, marketing promotion, academic research, education investment, laws and regulations, etc.

6.2.2 DFC Agreement Foundation

We have registered a non-profit DFC agreement foundation in Singapore. The main task of the foundation is to be responsible for the construction and operation of DFC ecology, the formulation of development strategic direction, the issuance and management of DFC token, etc., and openly and transparently manage the funds obtained from the donation of the token.

6.2.3 Strategic investors and community donations

According to the needs of project initiation and operation, we will reserve 30% of the pass to give back to strategic investors and community members. The cornerstone round

investment is completed by the founding members of the team. Due to the long-term optimism and self motivation of the project, the team decided that the DFC token corresponding to the capital invested in the cornerstone round will never be unlocked.

7. R & D Roadmap

In April 2020, the project was launched, the white paper was designed and the official website was launched;

In August 2020, it will launch a centralized point-to-point lending product currency loan;

In December 2020, DAPP, an experimental loan based on EOS, will be launched;

In February 2021, DFC of the project will be open for trading in the open market;

In March 2021, DAPP pawn, a peer-to-peer lending based on Ethereum, was launched;

In May 2021, the bank lending function will be launched in pawn;

In August 2021, Qian, a decentralized stable currency, was launched to support Ethereum network;

In September 2021, DAPP DFC tube bond was launched;

In December 2021, loans, stable currencies and bonds will be integrated into DFC tube to form a one-stop defi flat

Taiwan;

In April 2022, the stable currency Qian 2.0 was launched;

In July 2022, it launched the security protocol component of the defi application;

In September 2022, it cooperated with other public chains in DFC tube business, such as binance chain and Polkadot

Etc;

In October 2022, promote the use of Qian among users in Southeast Asia who cannot obtain banking services;

In December 2022, it launched the pilot business of encryption bonds for physical enterprises;

In March 2023, the Qian stable currency open technology alliance was established to develop the global cooperation partner of Qian stable currency

Companion.