ForTube

DeFi Lending Market

White Paper V1.0

Abstract

ForTube is a DeFi platform developed based on the DeFi technology component of The Force Protocol. It is committed to providing decentralized lending services for cryptocurrency enthusiasts around the world, supporting most of the world's popular assets. ForTube allows users to deposit and withdraw anytime, borrow and repay anytime, globally.

Table of Contents

1. Introduction to ForTube

ForTube is a decentralized financial service platform developed by The Force Protocol, including two modules: ForTube Bank and ForTube Bond. ForTube Bank is an algorithm-driven crypto digital bank that allows users to deposit and withdraw anytime, borrow and repay anytime. ForTube Bond is a one-stop crypto digital bond issuance and investment platform.

ForTube is developed based on The Force Protocol. The Force Protocol is a decentralized finance service protocol built on blockchain systems comprised of a set of DeFi technical components and tokenized protocols.

1.1 DeFi Technical Components

In response to the challenges in Ethereum DApp development like difficulty in contract upgrade, fixed data structure, slow on-chain interaction, poor user experience, lack of necessary infrastructure, and security issues, The Force Protocol proposes three DeFi technical components: Fundamental component, Extended component, and Financial component. The ultimate goal is to realize an internet product level of development and upgrading pace as well as user experience among Ethereum finance DApps while maintaining their security.

- Fundamental component: Assets Protected Elastic Contracts (APEC).
- Extended component: Blockchain Enquiring, Auditing & Messaging System (BEAMS).
- Financial component: Global Emergency Lockdown (GEL); Cooperative Automatic Lockdown Mechanism (CALM); Multisig Admin Keys (MAK).

1.2 Tokenized Protocols

Based on DeFi technical components, the bond financing protocol, crypto lending protocol, and decentralized stablecoin protocol can be further developed.

- Bond financing protocol: crypto-asset lending service with fixed term and interest rate.
- Crypto lending protocol: token deposit and loaning services of current and variable interest rate driven by algorithms.
- Decentralized stablecoin: cryptoassets reserve-type decentralized stablecoin protocol.

2. DeFi Technical Components of ForTube

2.1 Fundamental Component - APEC

APEC (Assets Protected Elastic Contracts) in Solidity is the major fundamental component in DeFi protocols of ForTube.

2.1.1 Design Concept

As the core on-chain structure, APEC is written in Solidity and ensures decentralization and asset ownership while making adjustment and improvement in contract development.

The core concept of APEC lies in asset security and component elasticity. It has three characteristics:

- Assets Protected
- Logic Upgradable
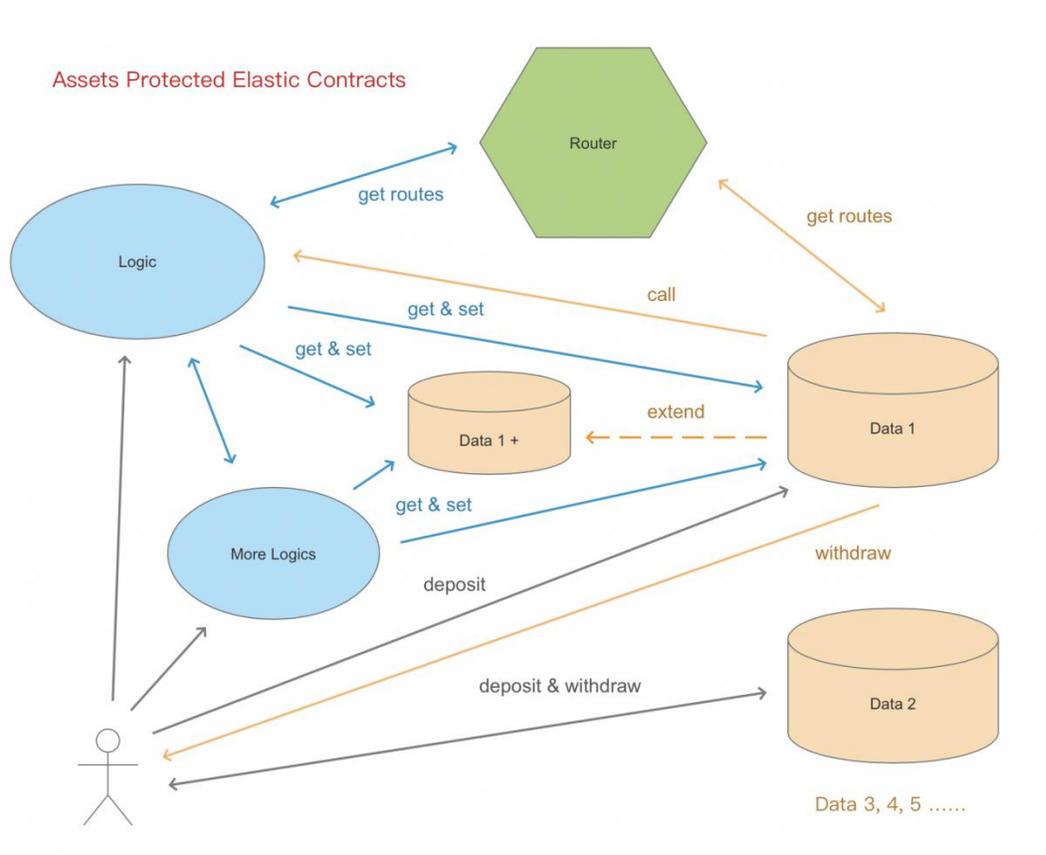- Data Extensible

2.1.2 Structure Diagram

Fig1 APEC Technical Structure Diagram

2.1.3 Technical Structure

APEC is composed of three modules:

- Data: Isolate the data from the classic contract structure and make it into data contract(s) for data storage, and only reveal necessary read and write interface to the public.

- Logic: logical contracts only cover business logic, not business data.

- Router: The field data that the business logic needs to read and write, which can be queried from the routing table according to the data module and field name, and then accessed based on the positioning result.

Routing Table

Routing table is an independent contract, which contains a routing comparison table that stores the routing swap of logical contract and data contract addresses. The routing table can be updated along with the system upgrade.

After the deployment of the entire contract system, the address of each logical contract will be stored in the routing table. External requests can be granted and access to the routing table to obtain the address swapping of the logical contract and call its interface. Data contracts can perform business logic call or callback through inquiring the routing table and obtaining the logical contract address.

Every group of data has its own independent data contract, whose address will be stored in the routing table upon creation. Before accessing certain data, the logical contract will first obtain the data contract address from the routing table, and then read and write the data contract via the address.

Upgradable Logic

Logical contracts do not store assets nor business data. Hence, they do not involve asset security and data migration, and they are upgradable and pluggable. After testing and audit, the new version of the logical contract can be deployed on-chain.

Data in swap tables of the routing table contract will be updated when deploying new contracts. The address swapping direction for the logical contract will also be modified for other contracts and application front-end to inquire and call.

Scalable Data

As an upgradable application, its data structure is also required to be upgradable. However, due to data ownership and asset security requirements, data contracts cannot be upgraded. The method we adopt here is scalability. If new fields are required in a new business, the new fields will be stored in a brand new data contract. Meanwhile, the address and field name in this new data contract will be added into the routing table. Business logic can be read and written through the new field's address obtained from the routing table.

The expansion of data contracts should be limited, as adding new data contracts without a limit will increase the complication of the whole system and hence adversely affect its operating efficiency. Data expansion mechanism only makes it possible to upgrade the data structure. However, overuse of this mechanism is not encouraged.

When designing and using the data structure, we need to follow the classic contract design principles and the best practice to come up with a sufficient and elastic data structure. In terms of data expansion, we need to exercise restraint to avoid the overuse data expansion mechanism.

2.1.4 Assets Protected

Following the upgradable logical contracts and scalable data contracts comes the issue of whether data ownership and asset security can be ensured.

It's widely known that users' assets are locked in contracts in traditional DeFi DApps. Smart contracts, especially those with open-source codes, guarantee that a third party is not able to touch the assets locked in contracts. Moreover, the non-tamperability of contracts make it impossible to change the codes once the contract is deployed.

APEC adopts the method of the separation of duties to solve the asset security issue in an upgradable structure.

Business contracts can be modified and upgraded, while data contracts cannot as in classic contracts. During initialization, each data set automatically generates an initial data contract. Once this contract is deployed on the chain, its code logic cannot be modified anymore.

- **The data contract will maintain a swapping table of user addresses and asset details internally.** This swapping table is inside the data contract and only provides two interfaces - inward and outward transactions, and other interface is not allowed to write or update this asset table.

- Inward transactions will be sent directly to data contract address and call the inward transaction interface. After the users' assets are locked into the contract, **the user's address and asset details will be recorded on the asset swapping table**. And the logical contract will be called, then the business logic will be processed and recorded.

- When making an outward transaction, the outward transaction interface on the data contract will be called directly and **the contract will verify whether the user's address exists in the asset swapping table** and then call logical contract, calculate the transaction and finally make the transaction to the requested address.

- **For any address that does not exist in the asset swapping table, the outgoing transaction interface will not answer its request.** This ensures that any asset that is going out belongs to the original address it went into from the logic level, hence guarantees the ownership and security of assets. And even the operation team itself will not be able to tamper with or steal any locked asset.

It ensures users' asset ownership and security through the strict ownership constraints of data contracts, making APEC's security philosophy adhere to the consistent concept of smart contracts, which has already exceeded "don't be evil" and realized "can't be evil".

2.2 Extended Component BEAMS

BEAMS refers to Blockchain Enquiring, Auditing and Messaging System.

2.2.1 The Limit of Blockchain

Blockchain is almost entirely isolated from the real world as it cannot send messages to off-chain proactively. If a smart contract encounters a problem in its logic or being attacked, the real world will not sense it passively. Hence, it requires continuous monitoring of the operation of the contract and strict audit of the data and assets in the contract. It also requires immediate alert when a problem is found to best ensure the security of the application.

For users, the experience of interacting with blockchain is naturally unfriendly. Asynchronous feedback caused by delays, frequent and large amounts of on-chain data reading and business model reconstruction, and the fragmentation between on-chain and off-chain messages have all led to slow and even chaotic interaction.

2.2.2 Design Concept

The issues mentioned above urge us to build a system that connects the on-chain and off-chain worlds, which can constantly monitor the operation of the contract, audit the data and assets, and accelerate the response speed of a product, making the response speed more stable, and the inevitably asynchronous feedback more smooth and fluent. All reminders and messages triggered by conditions can not only meet users' financial needs but also give them better product experience when using DeFi applications.

BEAMS is an off-chain system that works closely with contracts. Its core concept contains the following three characteristics:

- Enquiring
- Auditing
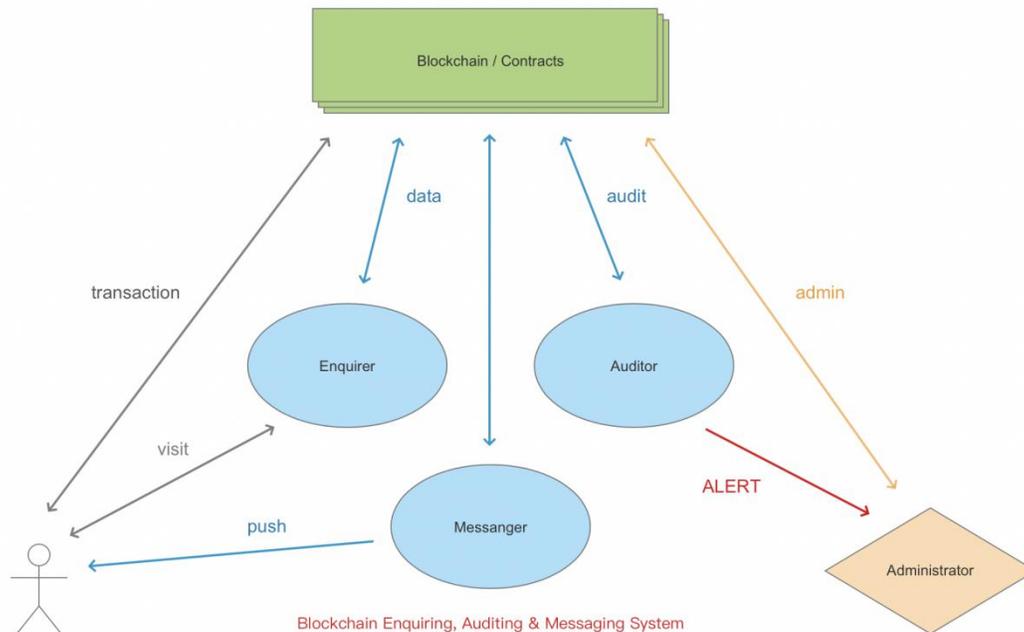- Messaging

2.2.3 BEAMS Structure Diagram

Fig 2 BEAMS Technical Structure Diagram

2.2.4 Technical Structure

BEAMS is composed of three modules: enquirer, auditor, and messanger.

BEAMS adopts a rotating mechanism that is based on on-chain events, to monitor contract state and data change. Basic data will be stored in the database and given to the front-end through the interface. Changes in contract data will be audited and abnormalities will be reported to the system administrators in real-time. Meanwhile, the changes of collateral value and the liquidation state will be continuously calculated, and various forms of notifications and warnings will be pushed to users when necessary.

Data Enquiry

All major transactions that involve asset changes will trigger customized on-chain events. The enquiring system constantly monitors for the emergence of new events and inquiries the corresponding data contracts of the event content. Data contracts provide the read-only interface that exposes data for the external, and the enquiring system reads the relevant data from the contract according to the data model's requirements.

All the data read will be sorted and aggregated into the BEAMS data warehouse, and changes in the data will be recorded. As the 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 data required for calculation and triggering to the message module. The audit module will use this data to review and audit the state transformation and data changes.

Audit Risk Control

The audit risk control module will constantly monitor the state and data change in every contract. It will use an independent and parallel logic to conduct a secondary review of the asset changes, and notify the system administrators to take action in real-time once an abnormality occurs.

The audit risk control module will use different review methods such as total assets, dynamic logic, and status verification to conduct real-time audit of contract data from all directions to improve the accuracy of the audit. The audit module can rate and alert on abnormalities, and the risk control module will have the authority to interfere and manage the operation of the on-chain contract when it is evaluated as highly risky.

The audit risk control module is also in charge of statistical analysis. It will count and analyze system operation data including user order records, historical returns, asset change curves, real-time return indicators of the platform, and historical return curves. The audit risk control will also predict and control risks, and provide data reference for product operation direction.

Message Push

In order to improve the user experience of asynchronous feedback caused by blockchain's characteristics, the message push module will play an important role in all aspects of the use process. A blockchain that lacks infrastructure needs a message push system to coordinate, especially when it comes to reminder notifications and warning messages that may affect users' interests.

On one side of the page, the message push module will preferentially use the Websocket long connection mode, and establish a two-way real-time link with users through the front-end page. It will monitor the execution of the transaction on-chain in each link and push transaction results and on-chain state to users when a transaction is finished.

In terms of messages regarding asset liquidation, returns distribution, and withdrawal reminder, the message push module will conduct constant monitoring and analysis on the contract date and push reminders and warnings to users in various forms including emailing and text messaging in real-time when the action is trigger.

2.3 Financial Component

2.3.1 Three Principles of DeFi Financial Security

DeFi Security Philosophy can be concluded as **three principles of DeFi financial security of layer defense concept.**

- Protect the platform from attack and invasion

- Protect the assets once the platform is invaded

- Minimize the loss when the assets are no longer secure

The DeFi financial security system is a multi-layer and comprehensive system. Decentralization is the core and the foundation, but it is not the only and everything. A secure and reliable open finance application with good scalability, capacity to serve tens of millions of users in the future, and complete risk control ability, is impossible to build by merely relying on decentralized infrastructure.

2.3.2 GEL

GEL refers to Global Emergency Lockdown.

In the DeFi system, all smart contract interfaces that involve asset changes have a GEL switch. Once a problem occurs to the contract, the switch can be manually or automatically triggered and all incoming and outgoing transaction interfaces will be banned, to protect the assets locked in the contract.

2.3.3 CALM

CALM refers to Cooperative Automatic Lockdown Mechanism.

CALM is an off-chain risk control mechanism. It adopts finance-level risk control standards, utilizes an independent high availability master-slave cluster with a hot standby configuration, and runs 24/7. CALM checks the contract state once every 5 seconds and conducts strict bookkeeping and reconciliation for all financial assets in the contract. Once a potential asset risk is discovered, the GEL will be immediately and automatically triggered to stop all interfaces related to the involved assets, to minimize the asset loss. Meanwhile, it will notify administrators and the operation team to react quickly and introduce human intervention and investigation.

2.3.4 MAK

MAK refers to Multisig Admin Keys.

DeFi adopts the admin key mechanism, where the administrator can use the key to set various permissions, like contract router update permission, oracle price feed permission, global lock flag setting permission, etc. The administrator key can add, delete and update subordinate permissions. When the subordinate permission key is leaked, it can be replaced quickly.

In order to avoid the loss of the admin key, we have adopted a multi-signature mechanism. Currently we use 3-2 multi-signature, and with the volume increase of locked assets on the platform, we will gradually upgrade to 5-3 or even 7-5 mechanism.

Taking 3-2 multi-signature as an example, three admin keys are stored in the contract. When performing actions with the highest security level, such as replacing the admin key, at least two admin keys must be used to perform multi-signature at the same time, to make the action happen.

The multi-signature mechanism of the admin key guarantees that

- If an admin key is leaked, the attacker cannot use the key to complete high-level permissions. And the platform administrator can use the multi-signature mechanism to delete the leaked key and make it invalid.

- If an admin key is lost, the remaining admin keys can be used to add a new admin key and delete the lost one.

- The admin key multi-signature mechanism makes every high-level authority operation depend on collective decision-making and execution, which has effectively prevented internal control risks and further protected assets.

3. ForTube Bank

ForTube Bank is a crypto digital currency deposit and lending protocol that supports deposit and withdrawal at any time, as well as borrowing and returning at any time. Through automatic procedures (smart contracts) deployed on the blockchain system, investors can quickly obtain returns without any obstacle, and borrowers can quickly and easily obtain financial support after providing appropriate collateral.

3.1 Design

With ForTube Bank, users are able to earn interests by depositing their digital assets in smart contracts. Meanwhile, they will obtain loan quotas, and are allowed to lend an amount of their cryptocurrency that is within the quota. Users no longer need to pay attention to the duration and can withdraw or repay anytime, regardless of whether it is a deposit or a loan.

When the borrower's outstanding loan exceeds the limited ratio of its collateral, the system will seize the user's assets and start the liquidation process. Now, arbitrageurs are allowed to call the liquidation contract and replace the seized assets at a certain discount. Since various digital assets differ in market size, liquidity, price stability, etc., their collateral rates, liquidation discounts, etc. will not be the same.

Several core concepts of ForTube Bank:

Deposit tokens: Users transfer the crypto-assets supported by the platform to the smart contract through the Bank's deposit function to obtain deposit interests. When users deposit their tokens, the deposited asset will first repay the loan (if any) of that asset, and the net assets will begin accruing interest.

Withdraw tokens: The user's withdrawable amount of a certain token includes the deposited amount of the token and the borrowable amount by depositing other crypto-assets as collateral. If debts are generated after withdrawal, borrowing interests will be generated.

Maximum LTV (loan-to-value ratio): The maximum Loan-to-Value ratio represents the maximum borrowing capacity of particular collateral. For example, if the maximum LTV of a token is 75%, it means a deposit worth $100 allows the user to borrow at most $75 using it as collateral.

Maximum secure borrowable amount: Assuming that the deposit value of the user's asset i is V_i, then V_i=the quantity of i * the price of i. Assuming that the maximum LTV of the asset is F_i, the user's maximum borrowing capacity is $\sum(V_i \times F_i)$. If the user borrows according to the maximum borrowing capacity, he would face the risk of being liquidated. Therefore, the system of the ForTube platform would multiply the user's maximum borrowing capacity by a coefficient MAX of less than 1 (currently is 0.8), that is, the maximum secure borrowable amount of the user = $\sum(V_i \times F_i) \times MAX$.

3.2 Interest Rate Module

ForTube Bank adopts an algorithm-driven interest rate model where the interest rate is automatically adjusted according to changes in the relationship between supply and demand, so as to adjust factors such as the total size of loans and the amount of fund supply.

In terms of the adjustment and control of loans, the Bank follows the following principles When the lending amount in the loan pool is low: loan interest rate increases slowly to encourage borrowers to borrow from the loan pool; And when the lending amount in the loan pool is high, or even close to saturation, loan interest rate increases quickly to boost deposit interest rate and encourage lenders to deposit more funds to the loan pool. The adjustment by algorithm can ensure that the loan pool develops and increases healthily.

To quantify the amount of the lent asset, we introduce parameter x to represent the lent proportion

of stablecoin a:

$$x \ (Utilization \ rate) = \frac{Total \ amount \ of \ lent \ stablecoin_a}{Remaining \ amount \ of \ lendable \ stablecoin_a + Total \ amount \ of \ lent \ stablecoin_a}$$

Let the borrowing interest rate be y, and the relationship between y and x can be demonstrated as follows:

$$y = Minimum \ borrowing \ rate + Slope \times Utilization \ rate$$

Accordingly, the formula for SIR (Savings Interest Rate) is:

$$SIR_a = x \times y \times (1 - s)$$

x = The lending proportion of stablecoin a

y = The lending interest rate for stablecoin a

s = Adjustment ratio (0 ≤ s < 1, normally 0.2)

3.3 Interest Rate Calculation

The annual deposit interest rate and the annual borrowing interest rate will be converted into interest rates per second, while adopting the continuous compounding formula. Assuming that R is the annual borrowing interest rate, the formula for the interest rate per second "r" is:

$$r = \frac{R}{365 \times 24 \times 60 \times 60}$$

Therefore, the interest rate at time "t" is:

$$r_t = r_{t-1} \times e^{r \times \Delta t}$$

Δt refers to the time interval from time t-1 to t.

Assuming that a user borrows "BA" amount of asset at time "t0", and pays the debt at time "t1", the amount that this user should pay, including the principal and interests, is

$$BA \times \frac{r_{t1}}{r_{t0}}$$

Deposit interest rate and interest calculation formulas are similar.

3.4 Health index

Different from general lending platforms, ForTube support pledging various assets as collateral to borrow other assets, so a simple pledge rate and liquidation line of a single asset are no longer applicable. Therefore, ForTube introduces the concept of health index. The health index is a value used to reflect the health of the user's debt. The higher the value, the lower the possibility of liquidation and the higher the security status of the user's funds.

The health index H is defined as follows:

$$H = \sum (Vi \times Fi) \div Debt$$

When the user borrows according to the maximum borrowing capacity, H=1; if the price fluctuation makes H<1, the user's assets will be liquidated.

When the user can borrow according to the maximum secure borrowable amount, H = 1.25. Therefore:

When H>1.25, it indicates that the user debt is relatively safe;

When 1≤H < 1.25, it indicates that the user's debt is in an early warning state and the user should increase the pledge or repay part of the debt;

When H<1, the user's assets are in a liquidated state.

3.5 Asset sections

Currently, ForTube Bank includes the Ethereum asset section and the Binance smart chain asset section. The Ethereum Asset section not only supports mainstream assets such as ETH, HBTC, WBTC, USDT, USDC, DAI, but also popular DeFi assets such as YFI, UNI, and LINK. The Binance Smart Chain Asset section also supports traditional classic assets such as LTC, EOS, and BCH, and innovative assets such as YFI, YFII, DOT, and FIL. In the future. ForTube Bank will open a stable asset section (only supports BTC, ETH, USDT, USDC and other stable assets) and a global burgeoning asset section (global popular potential assets) according to asset types.
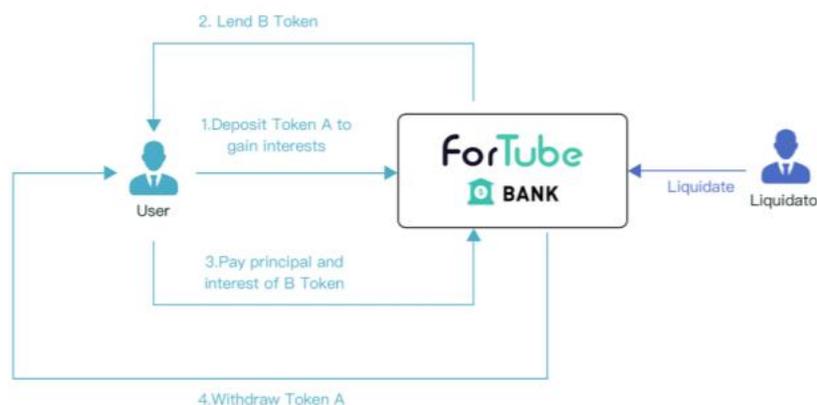

Fig 3 ForTube Bank Value Flow

4 ForTube Bond

Crypto Bond is a new type of bond that is issued and bookkept in the form of tokens. It can provide financing services for teams or individuals who hold crypto assets; it is also another

product with fixed returns in the cryptocurrency market to meet the needs of some investors' demand. ForTube Bond will provide a complete set of solutions for the crypto digital bonds, including credit rating, bond issuance, bond liquidation, bond trading, etc.

4.1 Bond Credit Rating

Restricted by the fact that the current crypto financial services are still immature and unsuitable for medium and long-term bond issuance, the current type of crypto digital bond products are mainly short-term. The issuance of crypto digital bonds adopts a registration mechanism and does not require any centralized agency to review or approve. The ForTube platform will conduct a formalized and automatic check on the basic information of bond issuance submitted by the bond issuer. After the ForTube community determines the credit rating for the bond, it can be officially issued.

Bond Credit Rating is an evaluation of agreement violation risk, which provides reference for users' investment decision making. ForTube platform adopts the following bond credit rating table.

Table 1 Bond Credit Rating Table

Ranking	Meaning
A-1	The highest level of short-term financing bonds with very low level of risks of paying the principal and interests & high level of security.
A-2	Relatively low level of risks of paying the principal and interests & high level of security.
A-3	Normal level of risks of paying the principal and interests with the security level prone to the influence of a disadvantageous environment.
B	High level of risks of paying the principal and interests with a certain level of risk of agreement violation.
C	Very high level of risks of paying the principal and interests with a high level of risk of agreement violation.
D	Incapable of paying the principal and interests on time.

ForTube's bond credit rating consists of community rating and professional rating. The community rating is carried out by the holders of the Force Protocol ecological token FOR. After understanding the bond information, a rater locks his FOR tokens in the corresponding level, and then he is able to withdraw the tokens after the rating is finished. Professional ratings are performed by professional credit rating agencies or professionals. A professional rater needs to

submit an application to the ForTube operations team and provide materials that can demonstrate his professional capabilities and qualifications. The final rating result will be determined jointly by the community rating and the professional rating, with 60% and 40% of weights respectively. Participating in the rating will generate a rating service fee, which will be distributed in equal proportions.

4.2 BondTokens

After the bond credit rating is completed, the crypto digital bonds can be issued. Each bond is issued in ERC-20 format, which is called BondTokens. BondTokens are investment proofs obtained after investing 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 are indivisible and can be transferred at one's will. Their nominal value is usually 100 USD. Whoever holds BondTokens is the creditor in a debt relationship and can be exchanged for principal and interests on the ForTube platform.

Table 2 Main Information About BondTokens

Bond Information	Example
Issuer	Ethereum Address
Bond credit rating	A-3
Total supply	1,000,000 DAI
Par value	100 DAI
Amount of bonds issued	10,000
Interest rate	15%
Duration	30 days
Start date	Feb 1, 2020
Maturity date	Mar 2, 2020
Callable bonds?	No

Puttable bond?	No

BondTokens is a new kind of crypto digital asset. Various BondTokens of different collateral, maturity dates, interest rates, and credit ratings can meet the diverse needs of the crypto digital asset market and become the cornerstone of other innovative financial applications.

4.3 Bond liquidation

The liquidation of the collateral assets will be involved if the underlying collateral depreciate significantly or the issuer fails to pay on time. The ForTube platform currently uses a discounted liquidation model, which means that the liquidators can trade collateral at discounted prices.

To facilitate calculations, we set the following parameters. Target collateral rate - TCR; current debt - CD; the current collateral rate - CCR; the discount rate - Discount; the current price of the collateral - Price; and the remaining amount of the collateral before liquidation - AC; The discount rate (1-Dicount) is a reward for liquidators.

Liquidation Within the Bond Duration

If the collateral depreciates by 20% in the duration of the bond, the system will send a margin call to the debtor. When the value of the collateral falls by 30%, the system triggers the disposal of the collateral, and will liquidate part of the collateral until the collateral rate returns to the initial value.

When

$$CCR \leq 70\% \times TCR$$

X - the amount of the collateral liquidated; Y - the liquidated debt volume.

$$Y = X \times Price \times Discount$$

The following shows how X is calculated. If the collateral assets cannot cover the debt, then

$$AC \times Price \times Discount < CD$$

When this situation occurs, all the collateral will be liquidated

$$X = AC$$

If the liquidated collateral assets can cover the debt

$$AC \times Price \times Discount \geq CD$$

The collateral rate after liquidation needs to equal TCR

$$TCR = \frac{(AC-X) \cdot Price}{PD - X \cdot Price \cdot Discount}$$

Hence,

$$X = \frac{AC \cdot Price - TCR \cdot CD}{Price \cdot (1 - TCR \cdot Discount)}$$

Liquidation of the Overdue Debt

If the debtor is unable to pay when the bond is due, the system will trigger collateral disposal and liquidate part of the collateral to pay all debts and fees. The remaining part will be returned to the debtor if there is any.

If the collateral assets cannot cover the debt

$$AC \times Price \times Discount < CD$$

all the collateral will be liquidated

$$X = AC$$

When the collateral assets can cover the debt

$$AC \times Price \times Discount \geq CD$$

then

$$X = \frac{CD}{Price \cdot Discount}$$

The remaining amount of collateral (AC - X) will be returned to the bond issuer.

4.4 Bond Trading Market and Bond Derivatives

To make it easier for bond holders to withdraw their investment earlier to recover their principal and interests, the ForTube platform will launch a bond secondary trading market in the future. Bondholders can set the transfer price and quantity based on the reference pricing given by the system. Investors can see bond basic information, credit rating information, expected earnings,

etc. Investors can obtain the BondTokens of the corresponding bonds after making the investment, and can redeem the principal and interest on the platform after maturity. With the increasing popularity of BondTokens, the ForTube platform will continue to introduce more features to support various bond derivatives, including:

- Bond repurchase (including reverse-repurchase);

- Callable bonds (means that the bond issuer is allowed to retain the privilege of redeeming the bond at some point before the bond reaches its date of maturity);

- Puttable bonds (means that bondholders is allowed to sell the bond back to the issuer, prior to maturity);

- Other bond derivatives that meet business needs.

4.5 Community Governance in Bond Module

ForTube is committed to promoting the issuance and settlement of decentralized (or multi-centralized) bonds. System permissions and core parameters will be handed over to the community in the future. However, in the early stage of the project, in order to best promote the development of the platform and project, the system permissions and parameters will be maintained by ForTube developers. They will uphold the principles of fairness and transparency, and promptly notify any changes in the system to the community. Currently, system parameters maintained by ForTube developers include but are not limited to:

- Supported crypto digital assets and their collateral rate, maximum number of bonds that can be issued, liquidation discounts, etc.

- The basic parameters of bond issuance, such as interest rate, bond maturity, issuance fee, rating service fee, etc.

- Time parameters, such as credit rating period, bond issuance period, payment grace period, etc.

- Bond credit rating setting
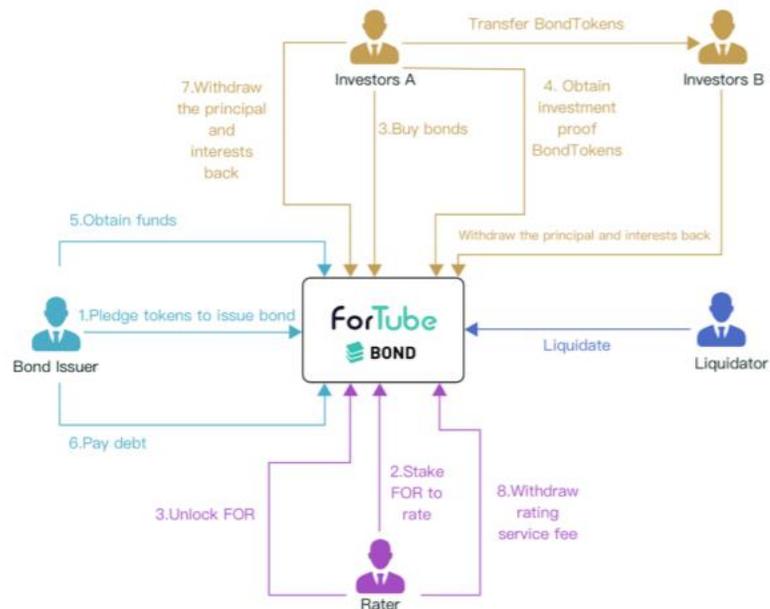
- Credible oracle price feed program

Fig 4 ForTube Bond Value Flow

5 Public Chains Ecosystem Construction

Currently, ForTube has launched ForTube Bank and ForTube Bond on Ethereum, and ForTube Bank on Binance Smart Chain. The market size is among the top global lending platforms.

5.1 Ethereum 2.0

ETH 2.0 is the new generation of Ethereum. As a brand new project, it adopts a completely different idea on blockchain structure. The aims of ETH 2.0 is to improve the scalability, security, and programmability of Ethereum. Without having to downgrade its decentralization, ETH 2.0 can process tens of thousands of transactions per second, demonstrating a great contrast with a throughput of 15 TPS for ETH 1.0.

ForTube will take full advantage of the great technical advantages of ETH 2.0, and smoothly migrate the application to the latest stable version as the mainchain update. ForTube will also closely follow the upgrade of Ethereum, and lead the developing trend of the business module and technical upgrade on DeFi finance platforms. Moreover, thanks to the PoS characteristics of ETH 2.0, locked ETH in smart contracts such as Bank will generate staking rewards. In the future, smart contracts like Bank can have functions similar to a staking pool, while continuing its original financial services. This will maximize the use of users' ETH assets and create more values.

5.2 Binance Smart Chain

In 2020, the development team of Binance Chain launched the function expansion solution through a parallel chain - the Binance Smart Chain. While preserving Binance DEX's high performance, it is friendly to developers. ForTube will continue to contribute to the Binance smart chain ecosystem and become an important cross-chain DeFi financial platform.

5.3 Polkadot

Polkadot is a platform that allows different blockchains to transmit messages, data, and value in a trustless way, while sharing their unique features and security at the same time. In simple terms, Polkadot is a scalable heterogeneous multi-chain technology. As a leader in independent cross-chain technology, Polkadot's concepts of relay chain, parallel chain, and bridge may become the standard for cross-chain technology. Through the Polkadot cross-chain system, mainstream chains will conduct good token value swap and business coordination. With the improvement and launch of the Polkadot system, ForTube will expand Polka ecosystem to ensure its leadership in the cross-chain financial application industry.

5.4 Other Public Chains

As DeFi is recognized by the crypto world, all major public chains have announced their own DeFi ecosystem development plans. ForTube will cooperate with more public chains in the future to support their DeFi ecosystem development and meet the different requirements from users of ForTube platform.

6. ForTube's Governance Token

FOR is ForTube's governance token which means users can participate in ForTube's governance through FOR tokens. The ForTube team will pursue the complete decentralization of ForTube governance and hopes to build ForTube into an excellent DeFi infrastructure through the efforts of all FOR holders.

6.1 FOR Token's Function

6.1.1 Participate in ForTube Bond Rating Voting

Community raters who hold the Force Protocol ecosystem token FOR can participate in bond credit rating. After understanding the bond issuance information, the rater locks his FOR asset to a certain rating level, and the FOR will be released when the rating is over.

Professional rating is conducted by professional credit rating agencies or professionals. To become a professional rating agency or individual, one needs to submit an application to the ForTube operation team (later the authority will be handed over to the ForTube community), providing materials that can prove one's professional capabilities and qualifications, and stake 1

million FOR tokens in the system. Staked tokens cannot be withdrawn during the rating period and the duration of the rated projects.

6.1.2 Participate in The Governance Of ForTube

Long-term supporters of FOR can participate in the governance of ForTube platform. Participating in governance will be rewarded with service fees. Locking FOR to the ForTube Staking contract can obtain governance voting token GFOR, which is issued according to a certain proportion of the locked amount of FOR. GFOR can only be used for governance voting and will be destroyed when users redeem FOR. The voted proposal can modify and adjust the key system variables of ForTube Bond and ForTube Bank.

Yield farming of FOR
lender and borrower

ForTube user

FOR as collateral

ForTube

Rate Bond

Governance voting

FOR holder

Fig 5 FOR Token Function

6.2 FOR Token Distribution Plan

The total supply of FOR tokens is 1 billion and there will be additional issuance. Under the guidance of the Force Protocol team, 85% of the tokens will be used for community construction and donation programs. The community ecosystem construction, the Force Protocol Foundation, and strategic investors and community donation take up 30%, 25%, and 30% respectively. The remaining 15% will be saved to reward the Force Protocol founder team and ForTube development team for their contribution, and incentivize new team members. The tokens for the team will be locked for 3 years, then the contract will release 30% of the tokens 12 months after the initial public trading, a further 30% after 24 months, and 40% after 36 months. The distribution of FOR is shown in the figure below.
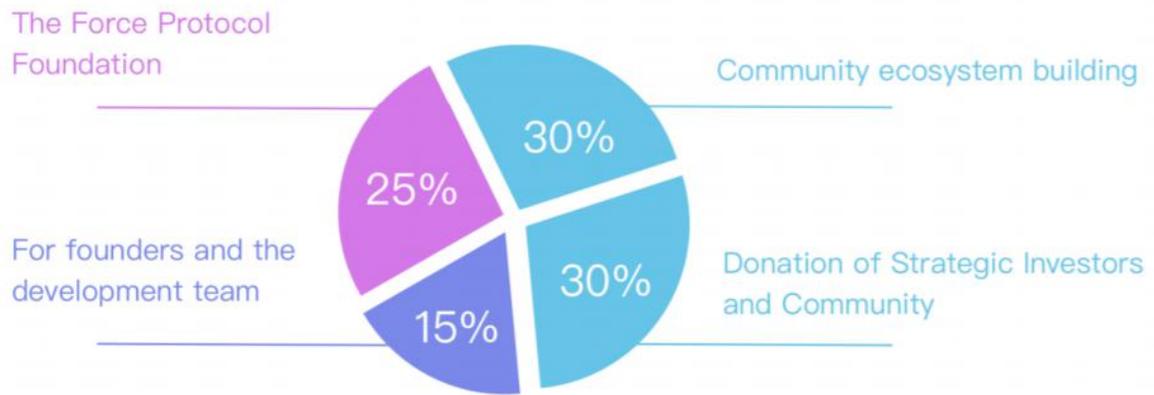
Fig 6 FOR Token Distribution

6.2.1 Community Ecosystem Construction

Community ecosystem construction includes, but is not limited to ForTube ecosystem governance and incentives, developer community construction, business and industrial cooperation, marketing promotion, academic research, education investment, laws and regulations, etc.

6.2.2 Foundation

The Force Protocol is registered as a non-profit foundation in Singapore. The foundation's main tasks are the construction and operation of the Force ecosystem, the making of development strategy directions, the issuance and management of FOR tokens, and transparent management of the funds obtained by token donation.

6.2.3 Donation for Strategic Investors and Community

According to project launch and operation needs, we will reserve 30% of the tokens to return to strategic investors and community members. The cornerstone investment is completed by the self-raised funds from the project founders. Due to the confidence and to motivate themselves, the team decided that the FOR tokens corresponding to the cornerstone investment stay unlocked forever.

7. Research and Development Roadmap

March 2020, launched crypto digital bond DApp — ForTube Bond;

June 2020, integrated lending, stablecoin, and bond into ForTube and formed a one-stop DeFi platform;

September 2020, launched ForTube Bank V2.0 on both Ethereum and Binance Smart Chain;

June 2021, cooperate with other public chains for ForTube business, such as Polkadot, Cosmos, etc.

December 2021, launch the pilot business of crypto bonds for entities.

Reference

An Introduction to Smart Contracts and Their Potential and Inherent Limitations [EB/OL].https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Implementation of Smart Contracts Using Hybrid Architectures with On- and Off-Blockchain Components [EB/OL].https://arxiv.org/pdf/1808.00093.pdf

Robert Leshner and Geoffrey Hayes. Compound: The Money Market Protocol [EB/OL]. *https://compound.finance/documents/Compound.Whitepaper.pdf*

MakerDAO. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System [EB/OL].*https://makerdao.com/en/whitepaper*

Wikipedia. United States Treasury security [EB/OL].*https://en.wikipedia.org/wiki/United_States_Treasury_security*

Fedreal Reserve Bank of New York. How Currency Gets into Circulation [EB/OL].*https://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html*

Wikipedia. Quantitative easing [EB/OL].*https://en.wikipedia.org/wiki/Quantitative_easing*

中信期货研究员 姜沁. 美国国债的规模管理体制、发行体制以及流通管理体制 [EB/OL].*https://finance.sina.com.cn/money/forex/forexroll/2018-10-19/doc-ifxeuwws5814324.shtml*

中国金融期货交易所. 美国国债期现货市场研究报告 [EB/OL].*http://yjs.dwfutures.com/uploadfiles/2013/8/20130806142789838983.pdf*