Abstract

Targeting the current challenges in decentralized finance, The Force Protocol proposes solutions that include DeFi technical components and tokenized protocols, aiming to provide secure, inclusive, innovative, and transparent decentralized financial services for users worldwide.
# Table of Contents

1. Background ................................................................................................................. 1

   2.1 DeFi Technical Components – “The Force” ......................................................... 1

   2.2 Tokenized Protocols -- ForTube ........................................................................... 2

3.1 Basic Component -- APEC ....................................................................................... 2

   3.1.1 Design Concept ................................................................................................. 2

   3.1.2 Structure Diagram ............................................................................................ 3

   3.1.3 Technical Structure ........................................................................................... 3

   3.1.4 Asset Security .................................................................................................... 5

3.2 Extended Component BEAMS ................................................................................... 6

   3.2.1 The Limit of Blockchain .................................................................................... 6

   3.2.2 Design Concept ................................................................................................. 6

   3.2.3 BEAMS Structure Diagram .............................................................................. 7

   3.2.4 Technical Structure ........................................................................................... 7

3.3 Financial Component ................................................................................................. 8

   3.3.1 Three Principles for DeFi Security .................................................................... 8

   3.3.2 GEL .................................................................................................................... 9

   3.3.3 CALM ............................................................................................................... 9

   3.3.4 MAK .................................................................................................................. 9

4. Tokenized Protocol ....................................................................................................... 10

   4.1 Bond Financing Protocol -- ForTube Bond .......................................................... 10

      4.1.1 Bond Credit Rating ......................................................................................... 10

      4.1.2 BondTokens .................................................................................................. 11

      4.1.3 Bond liquidation ............................................................................................ 12

      4.1.4 Bond Trading Market and Bond Derivatives ................................................. 14

      4.1.5 Community Governance in Bond Module ................................................... 14

   4.2 Cryptocurrency Loan Protocol -- ForTube Bank ................................................... 15

      4.2.1 Design ............................................................................................................. 15
1. Background

Ethereum smart contract is a great invention. It is no longer only a digital cash system, but rather a Turing machine with logical processing power. However, due to the asset security and other requirements, Ethereum smart contract was designed as a mechanism that cannot be modified or upgraded, which imposes great challenges to application development on the smart contract.

First, developers may make mistakes. Unnoticeable errors are more likely to emerge in complicated logic in a contract. It’s impossible to ensure that all codes are correct even after strict and repeated logic checks and code audits. Correction and fix of potential problems and errors are inevitable. Second, the real world is ever-changing, where users’ needs won’t stay the same forever. Despite thorough and detailed consideration and design, problems in existing functions and new function needs will inevitably emerge, which requires smart contracts to be upgradable.

Ever since the launch of the very first Decentralized Application (DApp), data and asset security have always been the key factor affecting or even destroying a DApp. Endless asset security incidents continue to shock the whole industry. How to maximize the system security of blockchain applications and protect assets has become a major challenge faced by every DApp development and operation team.

2. The Definition of The Force Protocol

The Force Protocol, a decentralized finance service protocol built on blockchain systems, is comprised of a set of DeFi technical components and tokenized protocols. The Force Protocol is committed to providing secure, inclusive, innovative, and transparent decentralized financial services for users worldwide.

2.1 DeFi Technical Components – “The Force”

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, which collectively form “The Force”. The force is well known by people through movie series “STAR WARS”, in which “the force” is the most important power to secure love and peace in the universe, drawing on this important concept, we named our product “The Force”. The goal of our project is to realize an internet product level of development and upgrading pace as well as user experience among Ethereum finance DAmps 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).
2.2 Tokenized Protocols -- ForTube

Based on “The Force” DeFi technical components, The Force Protocol integrates the bond financing protocol, crypto loan protocol, and decentralized stablecoin protocol, to form the ForTube decentralized financial services platform. The ForTube will provide individual and enterprise clients with crypto asset investment, financing, and trading services, to meet various crypto financial needs of various clients.

- ForTube Bond: A bond financing protocol with crypto-asset loan service with fixed term and interest rate.
- ForTube Bank: A loan protocol provides token deposit and loan services with algorithm-driven current and variable interest rate.
- QIAN: A decentralized stablecoin protocol committed to becoming the most influential project in crypto field. QIAN stablecoin can be invested in ForTube Bond, deposited in ForTube Bank for interests.

The three protocols mentioned above have high business connectivity with each other and can form aggregation effect to boost their development.


3.1 Basic Component -- APEC

APEC (Assets Protected Elastic Contracts) platform in Solidity is the major basic component in The Force Protocol.

3.1.1 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:

- Asset protected
- Logic upgradable
- Data extensible
3.1.2 Structure Diagram

![APEC Technical Structure Diagram](image)

**Fig1 APEC Technical Structure Diagram**

3.1.3 Technical Structure

APEC is composed of three modules:

- **Data**: Data from the classic contract structure is isolated and made into data contract(s) for data storage. Only necessary read and write interfaces is revealed 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 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 following 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.

For each set 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.

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 issues, 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.

**Expansible 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 expansion. 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.

3.1.4 Asset Security

Following the upgradable logical contracts and expansible 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 current 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 exists in the data contract and only provides two interfaces - incoming and outgoing transactions, and other interface is not allowed to write or update this asset table.

- Incoming transactions will be sent directly to data contract address and call the incoming 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 outgoing transaction, the outgoing 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 the logical contract, calculate the transaction and finally make the transaction.

- 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 that 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”.
3.2 Extended Component BEAMS

BEAMS refers to Blockchain Enquiring, Auditing, and Messaging System.

3.2.1 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 is 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.

3.2.2 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
3.2.3 BEAMS Structure Diagram

![BEAMS Technical Structure Diagram](image)

3.2.4 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 inquires 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 permission 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**

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 information 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 triggered.

3.3 Financial Component

3.3.1 Three Principles for DeFi Security

“The Force” DeFi Security Philosophy can be concluded as three principles 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 Force DeFi security system is a comprehensive multi-layer 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.

3.3.2 GEL

GEL refers to Global Emergency Lockdown.

In The Force 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.

3.3.3 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 asset loss. Meanwhile, it will notify administrators and the operation team to react quickly and introduce human intervention and investigation.

3.3.4 MAK

MAK refers to Multisig Admin Keys.

“The Force” DeFi components 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 stolen, 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 the assets.

4. Tokenized Protocol

4.1 Bond Financing Protocol — 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.

4.1.1 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 issuance information of bond 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 evaluation of agreement violation risk, which provides reference for users’ investment decision making. ForTube platform adopts the following bond credit rating table.

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-1</td>
<td>The highest level of short-term financing bonds with very low level of risks of paying the principal and interests &amp; high level of security.</td>
</tr>
</tbody>
</table>
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 ecosystem token FOR. After understanding the bond information, a rater locks his FOR tokens in the corresponding ranking, 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.

4.1.2 BondTokens

After the bond credit rating is complete, the crypto digital bond 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 par value is usually 100 USD. Whoever holds BondTokens is the creditor in a debt relationship, which can be exchanged for principal and interests on the ForTube platform.

Table 2 Main Information About BondTokens

<table>
<thead>
<tr>
<th>Bond Information</th>
<th>Example</th>
</tr>
</thead>
</table>

<p>| A-2 | Relatively low level of risks of paying the principal and interests &amp; 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. |</p>
<table>
<thead>
<tr>
<th>Issuer</th>
<th>Ethereum Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bond credit rating</td>
<td>A-3</td>
</tr>
<tr>
<td>Total supply</td>
<td>1,000,000 DAI</td>
</tr>
<tr>
<td>Par value</td>
<td>100 DAI</td>
</tr>
<tr>
<td>Amount of bonds issued</td>
<td>10,000</td>
</tr>
<tr>
<td>Interest rate</td>
<td>15%</td>
</tr>
<tr>
<td>Duration</td>
<td>30 days</td>
</tr>
<tr>
<td>Start date</td>
<td>Feb 1, 2020</td>
</tr>
<tr>
<td>Maturity date</td>
<td>Mar 2, 2020</td>
</tr>
<tr>
<td>Callable bonds?</td>
<td>No</td>
</tr>
<tr>
<td>Puttable bond?</td>
<td>No</td>
</tr>
</tbody>
</table>

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.

4.1.3 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 liquidation discount 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; current collateral rate - CCR; discount rate - Discount; current price of the collateral - Price; remaining amount of the collateral before liquidation - AC. Discount rate (1-Discount) 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

\[ CCR \leq 70\% \times TCR \]

\((X - \text{the amount of the collateral liquidated}; Y - \text{the liquidated debt volume.})\)

\[ Y = X \times \text{Price} \times \text{Discount} \]

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

\[ AC \times \text{Price} \times \text{Discount} < CD \]

When this situation occurs, all the collateral will be liquidated

\[ X = AC \]

If the liquidated collateral assets can cover the debt

\[ AC \times \text{Price} \times \text{Discount} \geq CD \]

The collateral rate after liquidation needs to equal TCR

\[ TCR = \frac{(AC-X) \cdot \text{Price}}{CD-X \cdot \text{Price} \cdot \text{Discount}} \]

Hence,

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

**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:

\[ AC \times \text{Price} \times \text{Discount} < CD \]

all the collateral will be liquidated.
\[ X = AC \]

When the collateral assets can cover the debt:
\[ AC \times \text{Price} \times \text{Discount} \geq CD \]

then
\[ X = \frac{CD}{\text{Price} \cdot \text{Discount}} \]

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

4.1.4 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 secondary bond trading market in the future. Bond holders can set the transfer price and quantity basing on the reference pricing given by the system. Investors can see bond’s 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 (meaning that the bond issuer retains the privilege to redeem the bond prior to its maturity);
- Puttable bonds (meaning that bondholders is allowed to sell the bond back to the issuer, prior to maturity);
- Other bond derivatives that meet business needs.

4.1.5 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 3 ForTube Bond Value Flow

4.2 Cryptocurrency Loan Protocol -- ForTube Bank

ForTube Bank is a crypto digital currency deposit and loan protocol that supports deposit, withdrawal, as well as borrowing and paying 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.

4.2.1 Design

With ForTube Bank, users are able to earn interests by depositing their digital assets in the smart contract. 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 pay 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. Please check the following table for product information.

Table 3 Bank Information Table

<table>
<thead>
<tr>
<th>Key element</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tokens</td>
<td>USDT(ERC-20), USDC, DAI, ETH, WETH, HBTC, IMBTC, QIAN</td>
</tr>
<tr>
<td>Collateral rate</td>
<td>150%</td>
</tr>
<tr>
<td>Liquidation discount</td>
<td>95%</td>
</tr>
<tr>
<td>Margin closeout</td>
<td>When the total deposited asset volume is less than the value of borrowed volume multiplied by the sum of staking rate, a margin closeout will be made</td>
</tr>
<tr>
<td>Annual lending interest rate</td>
<td>1.5% to 20%</td>
</tr>
<tr>
<td>Annual deposit interest rate</td>
<td>0 to 18%, the annual deposit interest rate is decided by the annual lending interest rate and usage rate. Formula: annual deposit interest rate = annual lending interest rate * usage rate * 0.9</td>
</tr>
<tr>
<td>The maximum amount of one token that can be lent in the contract</td>
<td>= [(Sum of all deposit - sum of all borrowed assets*corresponding collateral rate) ÷ the minimum collateral rate of the corresponding token] ÷ the price of the corresponding token</td>
</tr>
<tr>
<td>The maximum amount of one token that can be lent in the page</td>
<td>= the maximum amount of each token that users can borrow in the contract × (1 - token liquidation discount)</td>
</tr>
</tbody>
</table>

4.2.2 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 $a$:

$$x = \frac{\text{Total amount of lent stablecoin } a}{\text{Remaining amount of lendable stablecoin } a + \text{Total amount of lent stablecoin } a}$$

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

$$y = \begin{cases} 
  x^e + 0.015; & \text{if } 0 \leq x < \frac{3 - \sqrt{5}}{2} \\
  \left(\frac{3 - \sqrt{5}}{2}\right)^{e-1} x + 0.015; & \text{if } \frac{3 - \sqrt{5}}{2} \leq x < \frac{\sqrt{5} - 1}{2} \\
  \left(\frac{3 - \sqrt{5}}{2}\right)^{e-1} - (1 - x)^e + 0.015; & \text{if } \frac{\sqrt{5} - 1}{2} \leq x \leq 1 
\end{cases}$$

As shown in the formula, ForTube Bank divides the change of interest rate into three stages:

- **First** stage. In order to stimulate the increase in loan amount in the initial stage, the interest rate growth model approximates an exponential curve, which also conforms to the law of natural growth.
- **Second** stage. By accumulating a certain amount of borrowings, the growth of interest rate becomes stable, represented as a line with a certain slope in graph.
- **Third** stage. As the amount of lent assets becomes significant, the loan interest rate grows faster, in order to properly control the pace of lending funds and boost the amount of deposits. The pace of the increase in interest rates will gradually approach an extreme value, which is demonstrated as a modified exponential curve.

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 0.1)

4.2.3 Interest Rate Calculation

The annual deposit interest rate and the annual loan interest rate will be converted into interest rate per second, while adopting the continuous compounding formula. Assuming that “R” is the annual loan 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:

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

\( \Delta t \) 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 to the above.

Fig 4 ForTube Bank Value Flow
4.3 Decentralized Stablecoin Protocol -- QIAN

In Chinese, sky and money are both pronounced as QIAN. In the Book of Changes, QIAN represents the sky and the law of the universe’s movement, symbolizing the most noble spirit and positive energy. We name the decentralized stablecoin protocol "QIAN" due to its important connotation. QIAN is committed to creating a stablecoin system where everyone can equally, freely and conveniently participate and enjoy non-discriminatory financial services.

4.3.1 The Design Concept of QIAN

Cryptocurrency holders can lock their assets to QIAN’s smart contract to obtain the amount of QIAN stablecoin that is equivalent to fiat currency without having to pay any interest. The stablecoin QIAN is regarded as the currency exchange proof issued by the smart contract to the holders of the cryptocurrency. We name the smart contract under this mechanism as CSA (i.e. Currency Swap Agreement).

No interest cost for holding CSA

As a liquidity provider, QIAN CSA’s holders do not have to pay any interest. On the contrary, they could gain interest from the smart contract as additional income, which will encourage the creditors to hold QIAN’s CSA for a long time, and is likely to enable QIAN’s various financial functions, such as overseas payments, consumer payments, asset transactions, and loan. Only by eliminating the costs of holding assets can QIAN really participate in the development of the decentralized financial ecosystem, and grow shoulder by shoulder with fiat-backed stablecoins which do not require holding cost neither, to serve users with different needs.

Support Flash Loan

It is known that Flash Loan is a safe technology. Any smart contract with assets is able to provide external Flash Loan service. By charging a certain amount of loan interest, holders can obtain more revenue from his assets. Currently, there are Flash Loan aggregation tools in the Ethereum DeFi ecosystem, which provide more powerful loan services by aggregating the traffic of smart contracts that support Flash Loan. QIAN’s smart contract will support Flash Loan, and the crypto assets locked in the QIAN smart contract can generate additional rewards. QIAN’s administrator will regularly use the rewards to buy FOR tokens in the market. FOR, as the value storage container for the revenue of QIAN smart contract, will be locked into a smart contract that preserves the revenue of the QIAN system.

Risk Control

In the design of QIAN, we followed the following risk management rules:
First, QIAN 2.0 adheres to the principle of excess reserves. When users use crypto assets such as ETH to generate QIAN, they need to meet a certain start adequacy rate. The ratio of the value of locked crypto assets to the value of generated QIAN must be at least 120%.

Second, in order to enhance the security of locked assets in CSA, and avoid the occurrence of account blow ups in extreme market conditions, while taking into consideration the usage rate of crypto assets, QIAN will introduce a volatility factor according to the changing pace of the market price of crypto assets, to control the asset lock multiplier of CSA. When the price rises or falls unilaterally, the volatility rises and the system will increase the CSA’s start adequacy ratio. In a stable market, the volatility rate will decrease and the system will lower the CSA’s start adequacy ratio. This design will effectively reduce the impact of market volatility on locked CSA assets, encourage users to lock CSA under stable market conditions, and enhance the security of the locked assets.

Third, when the price plummets, users’ CSA adequacy rate will decline. During the decline, CSA will have two states: warning and frozen. If a user holds the CSA of ETH, and his reserve asset adequacy ratio drops to around 150% (ETH’s warning line), the QIAN system will demand a margin call from the user. However, if the market continues to plunge quickly and the user is not able to cover the margin call, his adequacy ratio will continue to decline. When it is less than 120%, the smart contract will freeze the user's CSA until the user brings the locked assets back to the safe level, before which the user is not be able to redeem the locked assets through his own address.

Fourth, the frozen CSA may be liquidated. The smart contract allows non-CSA holders to use the same amount of QIAN that is generated by the frozen CSA to redeem the frozen asset. This part will be explained in details later in the chapter of Smooth Arbitrage Mechanism.

Under extreme market conditions, the adequacy ratio of some or all assets in the QIAN system may be less than 100%, resulting in insufficient support for QIAN's intrinsic value. If none of the CSA holders has the intention to cover the margin call, and the market price of the underlying reserve assets does not recover for a while, a reserve gap (i.e. debt) will be created in the QIAN system. In this case, the system will start a global debt auction after a certain observation period, if the overall reserve adequacy ratio continues to stay below a certain level.

In the global debt auction, the system will unfreeze the governance token FOR provided by The Force Protocol Foundation and auction it. The auction proceeds will be used to make up the reserve asset adequacy ratio of the entire system.

In summary, the design advantages of QIAN are as follows:

<table>
<thead>
<tr>
<th>Subject</th>
<th>QIAN 2.0</th>
<th>DAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuance mechanism</td>
<td>Tokens swap</td>
<td>Collateral and loan</td>
</tr>
<tr>
<td></td>
<td>CDP holding cost</td>
<td>Medium to high cost</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CDP holding risk</td>
<td>Medium to low risk</td>
<td>Medium to high risk</td>
</tr>
<tr>
<td>Extreme condition resistant capacity</td>
<td>Strong, to be examined</td>
<td>Weak, has been shown</td>
</tr>
<tr>
<td>Is there interest on collateral?</td>
<td>Positive gains</td>
<td>Negative gains</td>
</tr>
<tr>
<td>Support for new technologies</td>
<td>Strong</td>
<td>To be examined</td>
</tr>
<tr>
<td>Ecosystem support</td>
<td>In progress</td>
<td>Relatively complete</td>
</tr>
<tr>
<td>Is there any final buyer?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Target market</td>
<td>DeFi; Cross-border payments; Customer payments; Asset trading; Loan; etc.</td>
<td>Limited to DeFi</td>
</tr>
<tr>
<td>Pegged fiat money</td>
<td>CNY</td>
<td>USD</td>
</tr>
</tbody>
</table>

4.3.2 Locked Assets Management

QIAN is generated by users locking their crypto assets in the smart contract. In the initial stage, underlying assets will mainly be crypto digital currencies such as ETH and ERC-20 version of BTC. After a certain period of stable operation of the system, offline asset tokens with consensus will be considered to be included as an issuance collateral.

For each crypto asset, the core parameters of the system configuration include:

- **Market price volatility** $\text{Vol}_i$: Since crypto trading is highly frequent, the QIAN system will draw on RV (Realized Volatility) indicator, a common one on the international market currently, to define the volatility of crypto asset $i$ ($\text{Vol}_i$). In the initial stage, $\text{Vol}_i$ will be updated according to the quoting interval of the oracle. Unlike options, the risk of the underlying assets for stablecoins can be effectively regulated through the recent RV, so $\text{Vol}_i$ does not involve the prediction of future volatility.
• **Start adequacy ratio** $Q_{i,0}$: Affected by the market price fluctuations of each crypto asset, $Q_{i,0}$ is in a dynamic change. In the initial stage of QIAN, $Q_{i,0}$ will be updated according to the oracle’s quoting cycle.

• **Current adequacy ratio** $Q_{i,t}$: $Q_{i,t} = \frac{Pledged(i,t)}{QIAN_i}$

• **Minimum adequacy ratio** $Q_{i,\text{min}}$: When the CSA of cryptocurrency $i$ is lower than $Q_{i,\text{min}}$, asset freezing will be triggered.

• **Alarming adequacy ratio** $Q_{i,\text{alarm}}$: $Q_{i,\text{alarm}} = \frac{Q_{i,0} + Q_{i,\text{min}}}{2}$, When CSA is lower than $Q_{i,\text{alarm}}$, an alarm will be triggered and the user will be suggested to cover a margin call; however, if the user does take the suggestion, he can still withdraw his CSA.

• **Maximum mining volume**: refers to the maximum amount of QIAN that one cryptocurrency can generate in the system;

  $Pledged(i)$ is the total value of locked crypto asset $i$. Its quote comes from the oracle and is updated regularly.

  For a specific crypto asset $i$, if its amount available for mining is $H$, then

  $$0 < H \leq \frac{Pledged(i) \times Price(i)}{2}$$

  $Price(i)$ is the current market price of the cryptocurrency (from the oracle).

For the overall system, core parameters include:

• **Total Adequacy ratio** $Q_{\text{total}}$: $Q_{\text{total}} = \sum_{i=1}^{N} Q_i \times \frac{QIAN_i}{QIAN_{\text{total}}}$

• **Minimum Adequacy Ratio** $Q_{\text{min}}$: In the initial stage, $Q_{\text{min}} \geq 90\%$ is required, and it will be adjusted according to community governance procedures.

• **Observation Time Before Auction** $T_{\text{auction}}$ refers to the interval before the auction starts and after the adequacy hits $Q_{\text{min}}$.

### 4.3.3 Price Fluctuation Buffer Mechanism

**Design Concept**

The current mainstream cryptocurrency-backed stablecoins for staking lack a mechanism to adjust close out and collateral operations according to volatility indicators. As a result, when extreme market conditions come, the stablecoin system cannot effectively buffer the impact of market fluctuations on the staked assets. In face of price plummeting as what happened on March 12, 2014, staked assets are likely to suffer losses, which will affect the balance of the entire stablecoin system.
Therefore, when designing the QIAN system, we comprehensively considered the impact of price, volatility, time, etc. on the underlying reserve assets. The introduction of volatility ratio index to the QIAN stablecoin system aims to reduce the disturbance of asset prices to the stability of the stablecoin, so as to maximize the overall balance of the system.

**Volatility Ratio Index**

QIAN will introduce the volatility index $V_i$ as a key indicator to measure the volatility of the underlying reserve assets. Every cryptocurrency changes in price, and when the price rises or falls faster, the $V_i$ of the underlying reserve asset of the stablecoin increases, so does the risk of staking, as the rate of return accelerates to go up or down. Now, by increasing the start adequacy ratio $Q_{i,0}$ and postponing liquidating, the impact of price fluctuations on the security of the underlying reserve assets can be effectively buffered. When the price of the underlying reserve assets becomes stable, $V$ drops and the risk to stake is released. By reducing $Q_{i,0}$ and resuming the liquidating, the deviated price of QIAN can go back to normal.

**Daily RealVol**

In the traditional derivatives market, the rate of return, or Realized Volatility (RealVol), especially the daily RealVol, has been widely accepted and used as the basic calculation parameter for option volatility indexes (such as RVOL and RVOV, etc.). Due to the particularity of cryptocurrency trading, the daily RealVol formula for the traditional market needs to be redesigned to serve as a basic parameter to calculate the volatility of the stablecoin’s reserve asset $i$.

The daily RealVol formula starts with the traditional standard deviation formula and has been modified in several key aspects:

- **Annual coefficient:** RealVol sets the annual coefficient to a constant. Since the crypto market has trading conducted 24/7, the actual number of trading days should be changed to the day number of a natural year. Because of changes in the day number in the month, it is better to have an approximate constant, rather than several exact but different values, so we set the annual coefficient to 360 at the beginning of the system.

- **A simpler representation:** The result of RealVol is usually a value less than 1.00. So we choose to multiply the RealVol result by 100 to achieve a simpler representation. For example, the annual RealVol for a cryptocurrency may be 0.20. Normally, we would multiply this value by 100 and represent it as 20.00.

**Daily RealVol Formula**

$$R_t = \ln \frac{P_t}{P_{t-1}}$$

$R_t$ = Continuously Compounded Return from $t-1$ to $t$

$\ln$ = Natural logarithm
\[ P_t = \text{The benchmark price at } t \text{ (time) on the current day ("closing price", the specific time is determined by the oracle’s quote source)} \]
\[ P_{t-1} = \text{The benchmark price on the day before } t \text{ ("closing price", the specific time is determined by the oracle’s quote source)} \]

\[
Vol = 100 \times \sqrt{\frac{360}{n} \sum_{t=1}^{n} R_t^2}
\]

\( Vol = \text{Daily Realized Volatility} \)

\( 360 = \text{a constant representing the approximate number of trading days in a year.} \)

\( t = \text{the count for each trading day} \)

\( n = \text{number of trading days in a time frame} \)

\( R_t = \text{Rate of continuously compounded return calculated by the formula.} \)

**RealVol Formular**

Cryptocurrencies are traded constantly, we need to calculate the real-time RealVol based on the daily RealVol. We will calculate the real-time RealVol on a 30-day cycle.

All factors involved in the daily RealVol formula are the same as the real-time RealVol formula. To convert daily values to real-time values, we need to start with the daily RealVol formula and take the current base price and weighting plan into consideration. This can provide continuous updates throughout the trading day and provide useful real-time instructions to CSA holders to understand the daily RealVol in the next 30 days. Essentially, the 30-day constant RealVol can be measured when we are at any moment of the day (today).

For example, if the trading hour percentage on day \( n+1 \) has passed 80%, we will use the latest underlying real-time price (URP) and yesterday’s corresponding URP (80%), to get the return for today \( (n + 1) \). Then, we will take the first day of the calculation period and weigh the rate of return on that day by 20% (100%-80% = 20%). In this way, we can still get the weight of the RealVol achieved at any point within 30 days, even if there are actually 31 returns. The weight of the 1st day and 31st day are 20% and 80% respectively, and that of the remaining days is 100%.

Note: Although the partial return for the day is self-weighted, hence no additional synergy factor is required, it is still necessary to calculate the self-weighted part of the day in order to apply an appropriate residual weight to the full-day return on the 1st day. In order to calculate the weight of the day, the nearest minute of the day should be taken. Since there are 1,440 minutes in a day, the current and the second counts in a day will be applied to the weight of the 1st day in real-time RealVol formula.
When the time of n+1 day is the closing time, the weight of the n+1 day is 100%, and the weight of the 1st day is 0%. Therefore, since its weight is 0, the rate of return on day 1 is deleted from the calculation. The original day 2 is now day 1, and all other days are renumbered. The real-time RealVol formula is simplified to the daily RealVol formula at this point (in our example, the market closes at 0 o’clock, China Standard Time every day). The moment after the market closes, a new trading day begins, and the rate of return is renumbered, so that there are only 30 rates of return, and the new weighted rate of return starts from the 31st day.

$$\text{Vol}_R = 100 \times \sqrt{\frac{360}{n} \left[ \frac{1,440 - m}{1,440} R_1^2 + \sum_{t=2}^{n} R_t^2 + R_{n+1}^2 \right]}$$

1,440 = minute count in a day

n+1 = today

m = the minute count from the nearest closing time on Day n to the nearest minute on Day n+1

$R_1$ = the rate of return on the 1st day in a calculation circle

$R_{n+1}$ = partial returns (the return of the current related price and the related reference price on the day before)

Note: For clarification, the flower body "R" means partial returns, and all other returns are full-day returns.

The Relationship between Start Adequacy Ratio $Q_{i,0}$ and $\text{Vol}_{i,R}$

If there is no adjustment factor and $Q_{i,0}$ is always kept at a fixed value (for example, 150%), users who open new positions will be exposed to great risks when the price is fluctuating. With real-time volatility, we can establish the following relationship between the real-time volatility change value and the start adequacy ratio:

$$Q_{i,0,n} = 120\% + e^{(\text{Vol}_{i,n,\text{in}} - \text{Vol}_{i,n,\text{in-1}})}$$

n = the current moment

i = a certain cryptocurrency, like Ethereum

$\text{Vol}_{i,n,\text{in}}$ = the real-time realized volatility of asset i at the current sampling point

$\text{Vol}_{i,n,\text{in-1}}$ = the real-time realized volatility of asset i at the last sampling point

The above relationship reflects the change value of volatility itself and its adjustment effect on $Q_{i,0}$. We will continue to test this formula based on the operation of the QIAN system. If the above formula is found to be inadequate, The Force Protocol team reserves the right to modify it through community governance procedures.
4.3.4 Smooth Arbitrage Liquidation Mechanism for Cryptocurrency

The QIAN system will decide whether to switch on the arbitrage mechanism based on the value of Vol\(R\). The system encourages liquidation under low market volatility to mitigate the impact of short-term panic sentiment on the stability of the QIAN system.

At \(t(i)\) moment, \(Q_{i,t}\) may have the following several CSA states in the QIAN system:

- **Normal contract**, \(Q_{i,t} > Q_{i,alarm}\)
- **Alarming contract**, \(Q_{i,min} < Q_{i,t} \leq Q_{i,alarm}\)
- **Frozen contract**, \(Q_{i,t} \leq Q_{i,min}\)

For arbitrageurs who do not hold CSA, their redemption may cause a reduction in the locked assets of CSA holders. For fairness and efficiency, the source of the callable assets for participants in smooth arbitrage liquidation at \(t(i)\) moment will be limited to CSA (frozen).

During the arbitrage, arbitrageurs will do arbitrage from all frozen assets of reserve asset \(i\). Assuming that at moment \(t\), there are 100 frozen CSA in the QIAN system, which generate a total of 100,000 QIAN. Now, arbitrageurs can use less than 100,000 QIAN of liquidation funds, to obtain all or partial frozen assets from the liquidation contract, stating from high investment offers to low. During the liquidation, all CSA (frozen) holders will share the loss proportionally to the percentage of their frozen assets in the total frozen CSA.

All reserve assets in CSA (frozen) are available for redemption by arbitrageurs. In order to prevent losses, CSA (frozen) holders must cover the margin call first to remove their assets from being frozen. Both the operations of arbitrageurs’ redemption and CSA (frozen) holders’ covering the margin call, will efficiently improve the adequacy ratio of QIAN, making the value of QIAN return to normal as soon as possible when the reserve asset is insufficient.

The design of this liquidation mechanism is not only able to encourage CSA (frozen) holders to cover the margin call, but also smooth the liquidation speed and quantity, while slowing down and reducing the losses suffered by individual users as much as possible. Therefore, this mechanism is named as smooth arbitrage liquidation.

The smooth arbitrage liquidation mechanism becomes complicated when the QIAN system supports multiple cryptocurrencies. In theory, arbitrageurs can redeem any asset that meets the liquidation conditions in the system, and there is no liquidating sequence among the reserve assets. The system displays the callable amount of each asset in a dynamic and real time manner. Arbitrageurs will conduct redemption within the limits, and the distribution of crypto assets throughout the system will not be significantly changed.

The callable amount of various assets is always in dynamic change. When the staked asset \(i\) reaches the maximum callable ratio \(R_i\), the overall reserve adequacy ratio of the system is objectively improved, and the arbitrage will be paused due to the limit. QIAN is a multi-collateral system and arbitrage on other assets will not be affected.
4.3.5 Debt Auction

Under extreme conditions, the system's global asset adequacy ratio $Q_{\text{total}}$ may drop below 100%. If the market continues to be sluggish, the liquidation arbitrage may not develop well due to the lack of intention to arbitrage. Now, the value of the reserve assets in the system is insufficient, hence overall debt will be generated. In order to maintain the intrinsic value of the QIAN system, the governance token FOR will be unlocked to make up the gap of the various reserve assets through auctions, so that the overall adequacy ratio will be brought back to the safety line and the intrinsic value of QIAN will be restored under extreme conditions.

The reason why auction participants are attracted is that the unlocked FOR will be auctioned at a price that is below the market price. The maximum discount $\Delta r$ will be introduced to QIAN’s debt auction. The initial value of $\Delta r$ is set to 70%, and this value will be modified by the community through voting after detailed discussions. The total amount of FOR in the debt auction is:

$$\text{FOR total value in debt auction} = \frac{\text{Debt balance}}{\Delta r}$$

In the auction, the start price of FOR is

$$p(\text{start}) = \frac{\text{market price(FOR)}}{\text{market price(i)}} \times \Delta r$$

If the auction participants use asset $i$ as the underlying asset for quotation and settlement, the final price falls in the following range:

$$i(\text{start}) \leq i(\text{final}) \leq i(\text{market})$$

The asset $i$ obtained from the auction will be used to pay the system debt. If there is any surplus, it will be locked in the auction surplus contract for future use.

4.3.6 Global Liquidation

Although we are optimistic about the long-term development of the crypto market, we must recognize the current situation: crypto assets are still in the early developmental stage, where extreme price changes often occur, and the records show that a bear market could last several years.

Despite the involvement of a series of stabilization mechanisms in QIAN stablecoin, there is still a possibility that the debt auction gains cannot make up for the overall reserve asset adequacy ratio, when the market suffers from extreme conditions and long-term sluggishness. Under this circumstance, the entire QIAN stablecoin system will lose the support of its intrinsic value. In this case, we will discuss whether to launch global liquidation and shut down the QIAN stablecoin through community governance. Once the community agrees to close the QIAN stablecoin system, a global liquidation will be initiated.

In the global liquidation, the QIAN stablecoin system will first freeze all CSA, stop generating CSA, and then close oracle feed price. The last oracle feed price will be used as the quotation for the global liquidation. Now, the system state changes again. Based on the last quotation
from the oracle, CSA (normal) holders will have the priority to first redeem their locked assets in the contract, and the system will manage the asset redemption operations. After the redemption of assets by CSA (normal) holders, if there is still a surplus of reserve assets in the system, CSA (alarm) holders will be allowed to redeem.

In the global liquidation, it is uncertain whether users can redeem all locked assets without losses. The probability of being able to redeem all locked assets follows CSA(normal)> CSA(alarm). Amounts of different underlying reserve assets, market price and other factors will have a comprehensive impact on the probability of a successful redemption.

4.3.7 QIAN System Governance

The main participants of the QIAN system include QIAN miners, QIAN holders and holders of the governance token FOR. The purpose of system governance is to balance the interests of all participants, and to maintain a stable, sustainable and healthy development of the system on the basis of a certain level of trade-offs.

For QIAN miners, the main risks are the fall in reserve asset prices and the potential redemption difficulty after the assets are locked by the system. Main benefits include gaining liquidity, value storage, and risk hedging. Based on research on similar projects in the industry, we believe that within a reasonable risk range, the mining of QIAN should be encouraged, which is beneficial to the development of the QIAN system. So we designed an adjustable interest mechanism. The core demand of QIAN holders is the stability of its exchange rate, so we designed a mechanism to maintain exchange rate stability.

FOR holders are the ultimate beneficiaries or risk takers of the entire system. FOR holders decide the management of the system through voting and the approved proposals 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
- Adjust interest
- Adjust the interest rate for Flash Loan
- Risk parameters: debt ceiling, initial lock ratio, redemption ceiling, warning line, etc. for each reserve asset
The Force Protocol has completed the development of “The Force” DeFi technical components on Ethereum and the construction of tokenized protocols such as bond financing, crypto loan, and decentralized stablecoins. In the future, we will expand these tokenized protocols to other blockchain systems, including ETH2.0, Binance, and Polkadot.

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 aim 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.

ETH 2.0 itself is a major breakthrough. Its sharding technology has made tokens pegged to mainstream chains a possibility, which in essence makes ETH 2.0 into a cross-chain system connecting all blockchains. If this can be realized, ETH 2.0 will become a model for cross-chain platforms, given its high throughout, high execution capacity, and its PoS characteristics.

The Force Protocol 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. The Force
Protocol will also closely follow the upgrade of Ethereum, and lead the developing trend of the business module and technical upgrade on DeFi platforms.

Moreover, thanks to the PoS characteristics of ETH 2.0, locked ETH in smart contracts such as QIAN and Bank will generate staking rewards. In the future, smart contracts like QIAN and 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 Chain and Binance ETH Smart Chain

Binance Chain is a community-driven blockchain software system composed of developers and contributors around the world. Focused on transaction and crypto trading, the public chain attaches great importance to performance, ease of use, and liquidity. It is a trading public chain tailored for DEX. Binance Chain has launched the BEP2 token standard, on which customized tokens can be issued. In particular, Binance Chain has supported several mainstream token-pegged coins, such as BTC, ETH, XRP, BCH, LTC, TRX. These pegged coins together with the cross-chain feature of Binance Chain based on Cosmos provide unlimited possibility for The Force Protocol’s cross-chain DeFi applications.

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. Thanks to the high TPS features of Binance Chain, BEP2 mainstream pegged coins, and EVM compatibility of Binance Smart Chain, DeFi applications of The Force Protocol on Ethereum can be seamlessly extended to the Binance Chain and Binance Smart Chain ecosystem.

The Force Protocol will support BNB as lending collateral in ForTube Bond and ForTube Bank. Since BNB is BEP2 cryptocurrency on Binance Chain, and the ForTube is developed on Ethereum, we will offer SWAP tool for BEP2 BNB and ERC20 BNB for users. The Force Protocol will also deploy ForTube Bond, Bank and QIAN service on Binance Chain, provides decentralized finance service to Binance Chain users, who can directly use their BEP2 asset as collateral and liquidity. Then, based on the Binance Chain ecosystem, ForTube will become an important cross-chain DeFi platform through value exchange of mainstream tokens, highly concurrent financial trading, and virtual machines with good compatibility.

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.

The Force Protocol will continue to conduct research on Polkadot, and carry out prototype verification and adaptive development of The Force Protocol based on the Polkadot system. With the improvement and launch of the Polkadot system, The Force Protocol will consider the
expansion of the ForTube system into the Polka ecosystem to ensure its leadership in the cross-chain financial application industry.

6. The Force Protocol Ecosystem Token

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 ranking, 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 this 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 Stability Adjustment of QIAN

Through Flash Loan, the crypto assets locked in the QIAN smart contract can generate additional income. The management committee of the QIAN system will use the additional income obtained to buy FOR tokens in the market regularly. As the value container of the QIAN smart contract revenue, FOR will be locked in the smart contract that preserves the revenue of the QIAN system. When the QIAN system believes that it is necessary to incentivize miners to increase the circulation of QIAN, it will pay interest to the new CSA users. The interest is calculated based on the value of FOR, and will be paid in FOR as well.

6.1.3 Participate in QIAN’s Global Debt Auction

Under extreme conditions, the system’s global asset adequacy ratio may drop below 100%. If the market continues to be sluggish, the liquidation arbitrage may not develop well due to the lack of intention to arbitrage. This will be followed by insufficient value of the reserve assets in the system, hence overall debt will be generated. In order to maintain the intrinsic value of the QIAN system, the governance token FOR will be unlocked to make up the gap of the various reserve assets through auctions, so that the overall adequacy ratio will be brought back to the safety line.

6.1.4 Participate in the Governance of ForTube

FOR holders govern the ForTube platform through voting, and the key system variables in ForTube Bond, ForTube Bank, and QIAN can be modified and adjusted according to selected proposals.
6.2 FOR Token Distribution Plan

The total supply of FOR tokens is 1 billion and there will never 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.
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 The Force Protocol 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 of 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 by the project founders. Due to the confidence and to motivate themselves, the team decided that the FOR tokens corresponding to the cornerstone investment stay locked forever.

7. Research and Development Roadmap

June 2018, Project Launch; White Paper Design, Official Website Release;
February 2019, EOS-based Experimental Lending Dapp Launch;
April 2019, The Project Token FOR Open for Trading;
June 2019, Pawn, a P2P Lending DApp based on Ethereum Release;
November 2019, Bank Loan Function launched in Pawn;
December 2019, QIAN, a Decentralized Stable Coin Release Supporting Ethereum and RSK Network;
March 2020, ForTube Bond Launch;
June 2020, Integrated Loan, Stablecoin, and Bond into ForTube;
July 2020, Stablecoin QIAN 2.0 Launch;
September 2020, DeFi Application Security Protocol Component Launch;
December 2020, Collaboration with Binance Chain, Polkadot, etc. in ForTube Business;
March 2021, Promote QIAN Among Users in Southeast Asia Without Access to Banking Services;
June 2021, Launch Pilot Business of Crypto Bonds for Real Enterprises;
March 2022, Establish QIAN Stablecoin Open Technology Alliance.

8. Team Members

**David Lei**  Founder
Master of Tsinghua University; Learned the Bitcoin and crypto ecosystem since 2011; studied crypto economy and open finance since 2016; pioneer of open finance.

**Ben Yorke**  Co-Founder
Former research analyst and content writer; entrepreneur with experience both in international markets and China, Business Administration degree from San Diego State University.

**Seamon Liu**  Co-Founder
CTO of Yunbi Exchange in 2017; CTO of Chaince Exchange from 2018 to 2019; senior blockchain technologist; deep research in blockchain, Networking security, and encryption protocol.

**Fabian K**  Blockchain Developer
Experienced and enthusiastic developer and project manager with 15 years of knowledge in high traffic web services; with experience and focus on blockchain analytics and insights.
Louis Xu  Chinese Marketing Director
Former cloud computing architect of ZTE; blockchain technology enthusiast and early community project participant.

Arpit Kamath  Full Stack Developer
Software Engineer on the Software Defined Security team at Salesforce; BS from UC Berkeley specializing in EECS with sound in-depth experience in designing and implementing reliable, large-scale software services.

Aaron Liu  Product Director
Former product director in multiple fintech companies responsible for products with transaction volume exceeding 100 billion, and the number of users reaching tens of millions; expert in product management, growth hacking and financial risk management.

Janet Weng  Community Manager
Former operations and business analyst at CERNET Corporation; former head of overseas marketing and user growth at DOS Network; MSIS from University of Maryland Robert H. Smith School of Business.
Reference


Wikipedia. 香港外匯基金 [EB/OL]. https://zh.wikipedia.org/wiki/香港外匯基金

MBA 智库·百科. 货币发行制度 [EB/OL]. https://wiki.mbalib.com/wiki/货币发行制度


潘攀（北京大学金融法研究中心）. 港币的发行及其稳定机制 [J]. 金融法苑, 1999, 14（总第二十六期）: 52 页

朱孟楠. 香港外汇基金的发展及投资策略的选择 [J]. 国际经济合作, 1997, No.6: 39~42 页

瞿新荣. 美联储重启扩表，美元发行的逻辑与油价 [EB/OL]. https://www.guancha.cn/QuXinRong/2019_10_13_521093_s.shtml


DAppTotal. 稳定币 [EB/OL]. https://dapptotal.com/stablecoins

CEIC. 中国香港特别行政区 外汇储备 [EB/OL]. https://www.ceicdata.com/zh-hans/indicator/hong-kong/foreign-exchange-reserves

CEIC. 中国香港特别行政区 货币供应 M1 [EB/OL]. https://www.ceicdata.com/zh-hans/indicator/hong-kong/money-supply-m1


RealVol Indices and Instruments. RealVol Real-Time Formula (Realized Volatility Formulas) [EB/OL]. https://www.realvol.com/VolatilityFormula2.html