yearn.deFinance (DeYFI) Protocol

Decentralized Financial Services Protocol White Paper V1.0

Abstract

Targeting the current challenges in decentralized finance, yearn.deFinance 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, distributing cryptocurrency and participating in charity.

Table of Contents

Contents 1

1. Background 3

2. The Definition of yearn.deFinance 3

2.1 DeFi Technical Components – “yearn.deFinance” 3

3. “ yearn.deFinance ” DeFi Technical Components 4

3.1 Basic Component – APEC 4

3.1.1 Design Concept 4

3.1.2 Structure Diagram 5

3.1.3 Technical Structure 5

3.1.4 Asset Security 7

3.2 Extended Component BEAMS 8

3.2.1 The Limit of Blockchain 8

3.2.2 Design Concept 8

3.2.3 BEAMS Structure Diagram 9

3.2.4 Technical Structure 9

3.3 Financial Component 11

3.3.1 Three Principles for DeFi Security 11

3.3.2 GEL 11

3.3.3 CALM 11

3.3.4 MAK 12

4. Ecosystem Expansion 13

4.1 Ethereum 2.0 13

4.2 Binance Chain and Binance Smart Chain 13

4.3 Polkadot 14

5. yearn.deFinance Protocol Ecosystem Token 15

5.1 DeYFI Token's Function 15

5.1.1 Participate in Bond Rating Voting 15

5.2.1 Community Ecosystem Construction 15

5.2.2 yearn.deFinance Protocol Foundation 15

Reference 16

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 yearn.deFinance

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

2.1 DeFi Technical Components – "yearn.deFinance"

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, yearn.deFinance Protocol proposes three DeFi technical components:

- 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).

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 DApps while maintaining their security.

3. “ yearn.deFinance ” DeFi Technical Components

3.1 Basic Component – APEC

APEC (Assets Protected Elastic Contracts) platform in Solidity is the major basic component in the yearn.deFinance.

3.1.1 Design Concept

As the core 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:

- Assetprotected
- Logicupgradable
- Dataextensible

3.1.2 Structure Diagram

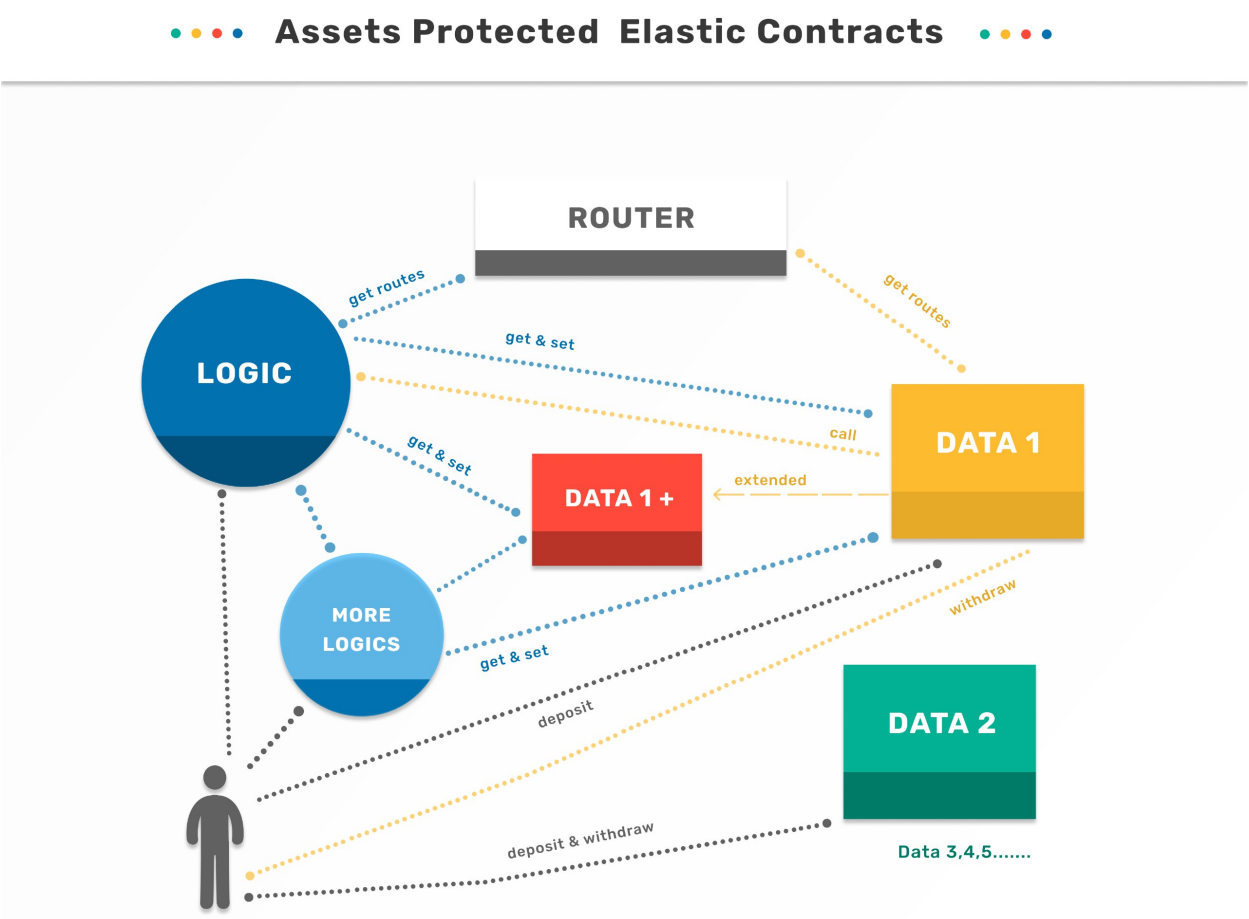

Fig1 APEC Technical Structure Diagram

3.1.3 Technical Structure

Fig1 APEC Technical Structure Diagram

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 sen tdirectly to data contrac taddress 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 out going transaction, the out going 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 out going 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

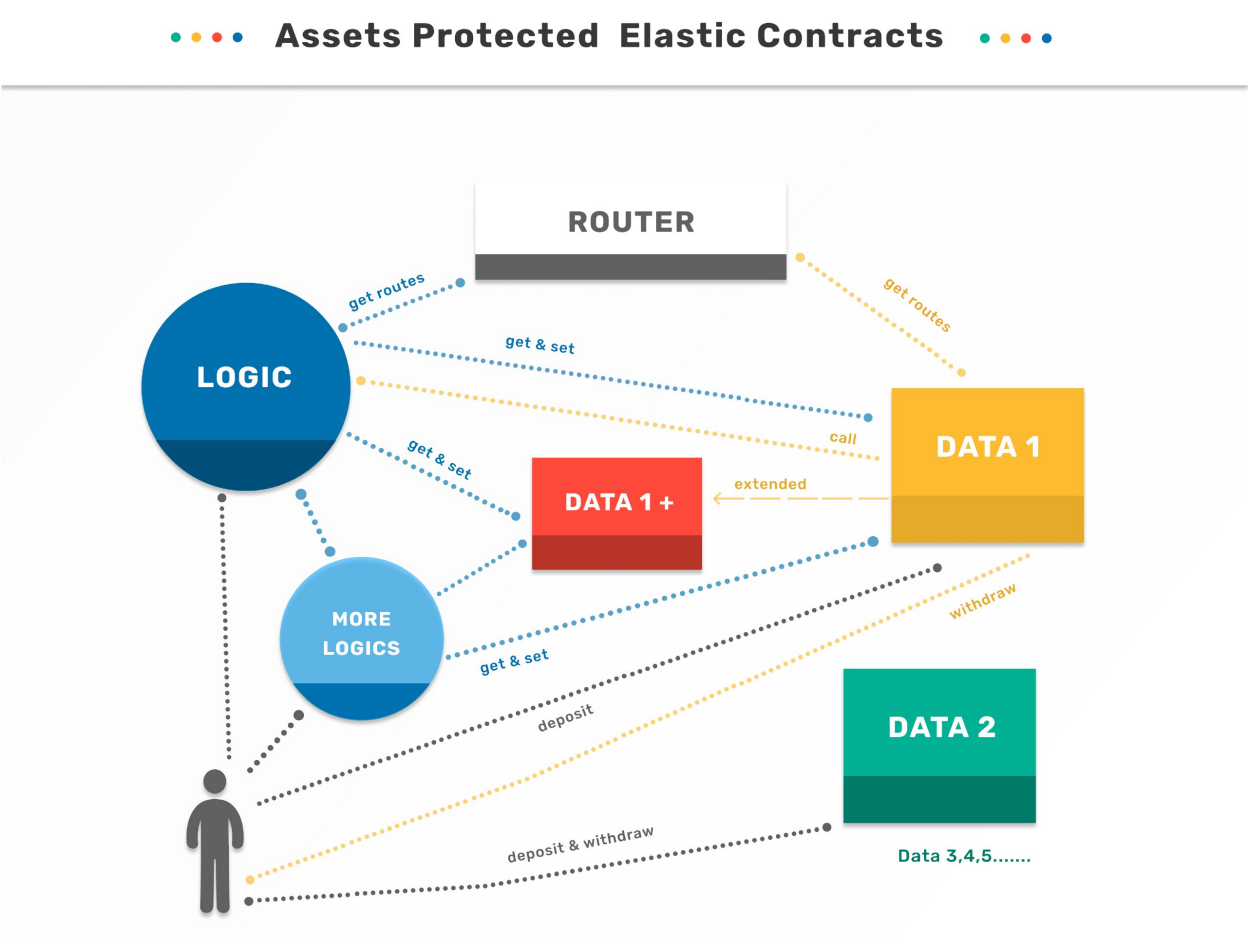

Fig 2 BEAMS Technical Structure Diagram

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 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 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

" yearn.deFinance " 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

3.3.2 GEL

GEL refers to Global Emergency Lockdown.

In yearn.deFinance 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.

3.3.4 MAK

MAK refers to Multisig Admin Keys.

“yearn.deFinance” 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.

runs 24/7. CALM checks the contract state once every 5 seconds and conducts strict bookkeeping with a hot standby configuration, 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.

The multi-signature mechanism of the admin key guarantees that

- If an admin key is stolen,the attacker can not use the key to complet ehigh-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, there maining admin key scan 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. Ecosystem Expansion

4.1 Ethereum 2.0

yearn.deFinance Protocol has completed the development of “yearn.deFinance” 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.

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.

yearn.deFinance 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. yearn.deFinance Protocol will also closely follow the upgrade of Ethereum, and lead the developing trend of the business module and technical upgrade on yearn.deFinance 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.

4.2 Binance Chain and Binance 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 yearn.deFinance 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 yearn.deFinance Protocol on Ethereum can be seamlessly extended to the Binance Chain and Binance Smart Chain ecosystem.

yearn.deFinance Protocol will support BNB as lending collateral in our our game based on blockchain. Since BNB is BEP2 cryptocurrency on Binance Chain, and the our game based on blockchain is developed on Ethereum, we will offer SWAP tool for BEP2 BNB and ERC20 BNB for users. yearn.deFinance Protocol will also deploy game based on blockchain 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, online service will become an important cross- chain DeFi platform through value exchange of mainstream tokens, highly concurrent financial trading, and virtual machines with good compatibility.

4.3 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.

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

5. yearn.deFinance Protocol Ecosystem Token

5.1 DeYFI Token’s Function

5.1.1 Participate in our game based on blockchain Bond Rating Voting

Community raters who hold yearn.deFinance Protocol ecosystem token DeYFI can participate in bond credit rating. After understanding the bond issuance information, the rater locks his DeYFI asset to a certain ranking, and the DeYFI 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 our service operation team (later this authority will be handed over to the game based on blockchain community), providing materials that can prove one’s professional capabilities and qualifications, and stake 3.000 DeYFI tokens in the system. Staked tokens cannot be withdrawn during the rating period and the duration of the rated projects.

5.2.1 Community Ecosystem Construction

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

5.2.2 yearn.deFinance Protocol Foundation

The foundation's main tasks are the construction and operation of the yearn.deFinance ecosystem, the making of development strategy directions, the issuance and management of DeYFI tokens, and transparent management.

Reference

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

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

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

Wikipedia. Federal Reserve. *https://en.wikipedia.org/wiki/Federal_Reserve*

Wikipedia. United States Treasury security. *https://en.wikipedia.org/wiki/United_States_Treasury_security*

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

Wikipedia. Quantitative easing. *https://en.wikipedia.org/wiki/Quantitative_easing*