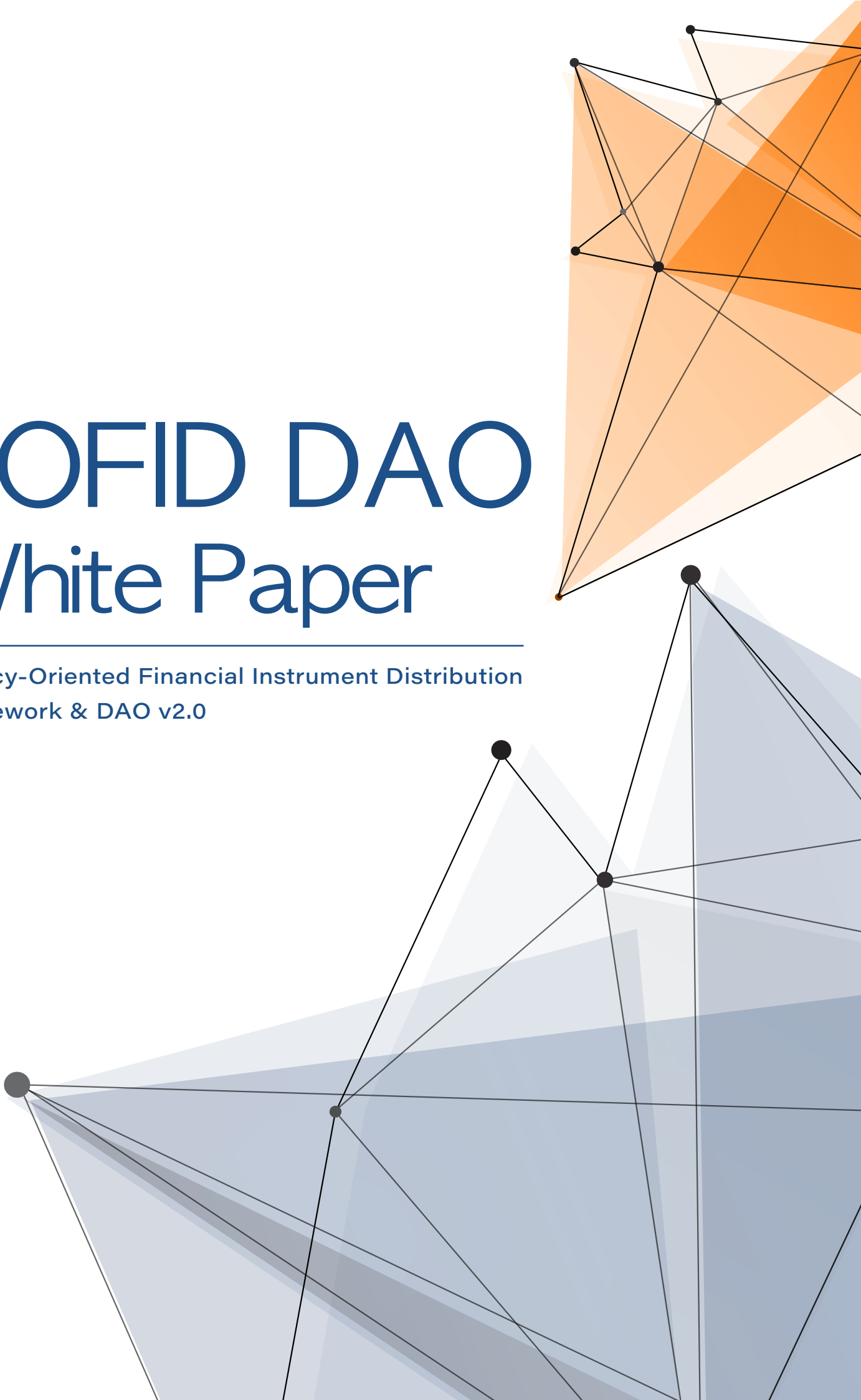
POFID DAO White Paper

Privacy-Oriented Financial Instrument Distribution Framework & DAO v2.0



Summary

The birth of Bitcoin in 2009 brought blockchain technology into people's field of vision. After a few years of rapid growth, the financial sector began to realize the financial properties of Bitcoin and the many other cryptocurrencies that rose alongside it. There was a broad, world-wide consensus that blockchain was the future. However, the value of blockchain technology did not seem to present itself in the way many expected. With the launch of the Ethereum ERC20 standard, it suddenly became possible for anyone to quickly and easily issue cryptocurrencies. The market become a truly mixed bag, with endless empty projects, and even outright scams, able to prosper alongside established and technologically-innovative projects.

Global investors have experienced painful lessons. Not long after came a prolonged period of self-reflection, government supervision and industry self-regulation. It was not until much later that the core value of blockchain technology that was able to withstand the chaos began to gradually surface.

In 2019, some 10 years after the emergence of Bitcoin, Facebook's Libra whitepaper presented an opportunity for change. Libra is a cryptocurrency that seeks not to maintain a stable exchange rate against the US dollar, but rather actual purchasing power. In a world where Facebook reaches billions around the world, Libra is likely to be the world's first cryptocurrency that has broad consensus and protection under the law. It is also a notable example of a stable cryptocurrency (stablecoin) that has entered the public's field of vision. Governments began to entertain the possibility of giving stablecoins the scope of their own laws.

However, even if Libra uses a basket of low-volatility assets as the credit endorsement of its value, it cannot ensure the absolute stability of its purchasing power. In fact, no currency can achieve a completely stable purchasing power, because as long as the corresponding pledge behind a currency's assets are endorsed by a limited collection of assets, it will definitely be affected by the stability of these assets.

At the same time, the change that blockchain brings to the world is by no means only limited to digital currency. Because it gives peer-to-peer networks a consensus mechanism that can be trusted, it will likely change the mode of human interaction and the mechanism of collaboration moving forward. With blockchain technology, information can be transmitted and processed

with complete trust, so the processing efficiency of many interpersonal transactions is greatly improved. Its transparent, direct and efficient mode of transmission seems almost like the high-level communication through brainwaves that you may see in a sci-fi film!

In this whitepaper, we will not spend too much space explaining the significance of stablecoins to the global economic market, but rather focus more on the design and implementation of POFID, and how to use these features of the blockchain and thereby improve the liquidity of financial assets.

In short, POFID is a comprehensive DeFi infrastructure based on blockchain technology that provides a decentralized way of managing assets on the chain.

On the premise that real assets that have been confirmed can be put on the chain, POFID can provide the correlation logic between digital assets and real assets, as well as the full set of solutions for on-chain custody, guarantees, auditing, circulation, risk-control and governance.

POFID uses the technical characteristics of the blockchain to give crypto assets a higher credibility. The axiom that "code is law" ensures that the asset management process will not be disturbed by human interference. The difference between POFID and the vast majority of projects on the market is that it provides a privacy protection mechanism for managing assets.

POFID can also be used as a powerful tool for the management of stable cryptocurrencies. In this aspect, POFID supports a system of diversified stable cryptocurrencies, and is not just a tool for issuing a single, more stable cryptocurrency. In addition, POFID also supports a variety of digital assets as stable cryptocurrency guarantee endorsements, and is compatible with a variety of mainstream cryptocurrencies, including Bitcoin.

Background

Blockchain entered the public eye with the birth of Bitcoin in 2009, and it has reached prominence in the more than 10 years since then. This new technology, which is based on existing computing and communication technology, has been reconstructed and become a new, self-contained technology. With their financial attributes, Bitcoin and the various other crypto-

currencies have brought about a paradigm shift and independently developed into a new economic field. In fact, the changes in economic modelling brought about by cryptocurrencies have far exceeded their impressive technological achievements. Ardent believers assert that the revolutionary significance of blockchain far exceeds that of the Internet, and can even trigger a new industrial revolution.

A new industrial revolution must, at least, be marked by the birth of a new kind of productivity. Looking back at history, the First Industrial Revolution was marked by the improvement of steam engines, the second by the widespread application of electricity, and the third by the invention and use computers. Several years ago, Jack Ma famously said that data is a new source of energy. This can be considered a continuation of the industrial revolution triggered by computers.

Put in another way, it can be noted that every industrial revolution is ultimately the liberating of human labor. Computers have replaced much work that was previously the domain of human brains. Data is one of the energy sources that drive this productivity. As the economic dividends brought about by population growth continue to shrink, the need for computers to replace manpower has become more ever more relevant, especially with AI and other technologies showing the promise of completing tasks that humans cannot do.

Therefore, in our opinion, blockchain is still only a continuation of the Third Industrial Revolution. Under the governance model of the blockchain, computers can indeed replace the functions of many people, but this is not because people cannot complete these tasks, but rather because the cost of communication is essentially reduced to zero.

Essentially, most of the meat behind modern economic management theory can be distilled down to the issue of interpersonal collaboration. The cost of collaboration is one of the largest cost components in modern economic activities. This can easily be seen from the large number of executives in large multinational corporations. Why interpersonal collaboration costs so much can be explained by the simple fact that humans have the ability to think logically.

Language and writing enable knowledge to be recorded and passed on, driving the development of human communities. Language and writing are the products of the human mind. Circuit diagrams can simulate the thinking of the human mind as closely as possible (although

there are still some behaviors in the human brain that cannot be explained and therefore expressed with circuit diagrams). Whatever the case, humans "lie", but circuit diagrams do not, and this is something that is easily verifiable.

A 2014 study showed that the prefrontal dorsolateral cortex in the brain may be the "switch" for honesty. Once this brain area is damaged, people tend to lie for self-interest. Research into cases of prefrontal lobe injury have shown that the prefrontal lobe also plays an important inhibitory role in the vocabulary access process of bilingual language production and bilingual language comprehension. Research shows that people with no brain injuries tend to be more willing to tell the truth. People with a damaged dorsolateral prefrontal cortex have different behavior patterns. Once honesty and self-interest contradict with each other, they make more dishonest choices.

However, the activities of the prefrontal lobes are not observable in daily life. The problems of interpersonal collaboration caused by the prefrontal lobes are not all caused by "dishonesty". The essence of interpersonal collaboration is treating each individual as a processor. When information passes through each "processor", it is processed, and then passes onto the next "processor". Regardless of the issue of dishonesty, sometimes people cannot control their own processing logic 100% of the time - the problem lies in the fact the processing of this information is not provable, so there is a cost to collaboration.

The CPU calculation process in computers is closed, so the network formed by the centralized system is very similar to the current form of human collaboration. The transmission of information on each node of the network may be processed without proof, so although the traditional Internet network can transmit the results of information processing at high speed, it cannot solve the problem of credibility of the processed information and therefore cannot reduce the main cost of interpersonal collaboration.

This is the most fundamental role of the blockchain. Information processing in the Bitcoin network has only a single function: that of bookkeeping, while the smart contract of Ethereum is Turing complete. Through contract programming, the blockchain can almost completely imitate the brain' activity in processing all information. Once the smart contract is deployed, it faithfully performs its own information processing obligations, and this process is completely transparent, with all miners able to witness it.

While this was all technologically revolutionary, a new problem was born. Because blockchain networks like Bitcoin/Ethereum all need to verify the processing of information under the premise that the information is completely symmetrical, this information is broadcast and synchronized in an open network. As a result, a lot of private information is leaked. It is for this reason that new public blockchain protocols supporting data privacy have emerged. These chains enable the information to be processed and transmitted faithfully, while ensuring public access to information is limited.

There are immense differences between the characteristics of the blockchain and centralized systems. The blockchain can be said to have three main advantages:

1. The asset records on the chain cannot be tampered with and will not disappear. In contrast, in centralized systems asset data can be modified at will.

2. Assets are on the chain, which means that users have absolute and sole ownership of the assets. In contrast, in centralized systems the administrator has the right to handle all assets like a god.

3. The path from birth of each asset on the chain is clearly traceable. When you see the existence of a bitcoin, you exactly the computing power paid for it by a miner. If the digital asset is a contract-issued asset (for example, a debt asset on the chain), you know exactly what triggered the contract to issue the asset. In contrast, in centralized systems there is no such transparent auditing mechanism, so it is difficult to say whether or not data on such a centralized system can be understood as a real asset.

From the perspective of commercial applications, at present, real assets are confirmed on the chain through an interface to digital assets with associated legal significance. This is already a technological reality and most of the commercial work is achieved through the processing of logic on the contract level. If the problem of data and asset privacy can be solved, then the last piece of the puzzle in technology will be put into place for widespread adoption in the commercial world to be possible.

So, what kind of economic activities have assets that can be optimized through blockchain technology? How can we distinguish real digital assets from other digital information? And how do we define the standards of these digital assets?

The value logic behind many so-called “digital assets” in the market is questionable. Nowadays, most crypto exchanges have rejected the listing of tokens with the nature of securities. There is an essential difference between assets and securitized assets. Crucially, the latter has a clear investment value. If digital assets cannot support securitized assets, the significance of the blockchain will shrink by more than half. However, if the anchoring relationship between real assets and securitized digital assets on the chain cannot be established, it will be difficult for the securitized digital assets to become a reality.

In summary, we are seeing an opportunity for the blockchain to usher in a paradigm shift in finance and commerce, and governments of various countries have entered into substantive consultation and legislation on the compliance of assets on the chain. With positive policy changes rapidly approaching, the market urgently needs a tool to provide solutions for the securitization of digital assets.

Stablecoins

Blockchain and Stablecoins

Cryptocurrency started as an appendage of blockchain technology, but it gave the theory of free money without borders a practical opportunity never before seen in history. Blockchain technology provides a diversified trust mechanism for the issuance and circulation of crypto-currencies. Due to the transparency of their operating mechanisms, these assets have gained a broad consensus in a relatively short period of time. This emerging technology of blockchain has received widespread attention and exploration for application. Whether Bitcoin has made the blockchain or the blockchain has made Bitcoin is difficult to determine, but there is no doubt that it is the characteristics of this technology that has enabled Bitcoin to reach such heights in such a short period.

Among the many cryptocurrencies, stablecoins seem to special place at the moment. Signifi-cant stablecoins account for only a very small proportion of all cryptocurrencies, but in fact they provide a crucial role for traders as a hedging mechanism and trading medium.

Regardless of whether or not the Libra project will come to fruition, more national governments

have begun to explore digital currencies anchored to their domestic fiat currencies. From the perspective of these governments, such stablecoins have the potential to provide completely new and revolutionary payment systems and inter-institutional settlement technologies that help to strengthen the “voice” of the domestic currency in the global market.

From another point of view, a single fiat currency has proved to be a considerable risk in the face of a severe economic crisis, causing its stability to be greatly challenged. In the economic crisis that broke out in Asia in 1997, the fiat currencies of countries such as Thailand, the Philippines, Indonesia, South Korea, and Japan were hit hard, and they all experienced large devaluations. One of the major reasons for this was that the value of a country’s currency largely depends its foreign exchange reserves. There are often risks associated with fast-growing economies: banks issue more loans, and foreign exchange reserves are often not large enough to withstand potential risks and guarantee the stability of the domestic currency. In order to attract more investment, countries often have loose foreign exchange controls and relatively simple economic diversification, leading to the situation where centralized capital can quite easily exert a great influence over domestic currency.

Given that significant market interference by governments can be problematic in the best of situations, stablecoins have the potential to lessen the risk of having only one single legal currency circulating in the market by providing a diversified currency system and allowing for credit endorsements issued from a greater selection of currencies.

Diversified Currency System

History has shown that a currency issuance mechanism with market competition will have a more reliable and credible durability. Although fiat currency minting rights are protected by laws issued by governments, currency substitutes with applications in specific scenarios (for example, customer loyalty points) have a value that is endorsed by the credibility of the institution and the endorsing of the substitute by an anchored basket of commodities. Once Bitcoin is accepted in many countries, this method will very likely receive significant attention and gain popularity.

Controlling value stability through competition is an important part of Friedrich August von

Hayek's theory of free money (emphasized in his book The Denationalization of Currency). If a currency-issuing institution cannot maintain the stability of its issued currency, its currency issuance rights will be revoked by the market since the currency it issues will no longer be accepted and circulated in the market. Such an institution cannot force its currency onto the market like a government. If their currency-backed endorsements or credits have the ability to be fully trusted by the market, and assuming the entire market environment does not undergo major changes, institutions will surely be able to ensure the stability of their currencies, which will therefore achieve even further acceptance and circulation on the market. Furthermore, during times when there are major changes in the entire market environment, this kind of competitive currency issuance mechanism can effectively prevent the total and systematic collapse in market value of a currency. This principle can be analogized to the storing of grains and rice during peacetime. During wartime, these basic commodities became hard currency and such investment ensured the stability of assets. Viewing currencies as a commodity, which they undoubtedly are, the logic remains the same.

The more stable the purchasing power of a universal currency, the more it tends toward the inflation level of a barter system economy. In fact, the inflation level in the barter system era can be understood as basically zero, because even when individual commodities suddenly increased in price due to market demands or supply costs, the influence on the price of other commodities was still very limited since everything could be exchanged.

In fact, the stability of a currency is not equivalent to the fixing of its value. The law does not require the anchoring of value of a certain currency with commodities, but it can determine the anchoring relationship between the currency's value and commodities when a certain currency value is disputed. The latter enables the currency to maintain its stability for a longer period of time in a competitive environment. The law allows for such a competitive environment, but at the same time it can exercise the right of value anchoring. This mechanism itself guarantees the stability of the currency in the market.

Although we cannot determine the number of universal stable currencies that would need to exist in the market for optimal economic development, in light of the historical problems caused by the single currency system, if it happens that a diversified currency system can alleviate the financial situation, then such an attempt would certainly be worthy of consideration.

Diversified Asset Endorsements

In its initial introduction to the world, Libra chose a combination of several major currencies (including the US dollar, euro, Japanese yen, British pound and Singapore dollar) for its currency-backed endorsement, with regulation under a specific governance structure.

If Libra can achieve the implementation of such an asset endorsement and Facebook can carry out some form of banking business, then in essence it will be a multinational bank with a broad user base and the ability to issue currencies. Institutions that are able join its alliance will gain access to Libra's vast payment network and cross-border users. There is no doubt that the ultimate goal is a much improved, super-sovereign world currency. But once Libra has grown in size, whether or not the Libra Association can at all times guarantee the stability of the system and an appropriate level of inflation is still difficult to say.

At the same time, even if Libra is able to increase its diversity of fiat currency asset pledge types, its asset endorsements will likely still not be flexible enough to accommodate other assets. It is difficult to imagine a situation where Libra can one day support asset endorsement backed by Bitcoin. If such a situation occurred, it would undoubtedly bring a huge crisis to Bitcoin, because Libra would then control a large enough amount of Bitcoin to control its price.

Cryptocurrency Characteristics

The blockchain technology underlying cryptocurrencies has many natural advantages, including reliability brought about by a multi-node consensus, immutability of block data, security of peer-to-peer payment, the ability to execute code through smart contracts that cannot be tampered with (ensuring for example that the code executed before payment will not be modified during payment), and support for processing smart contracts of different digital asset types, including on-chain assets. These advantages are precisely the shortcomings of the current centralized currency system.

Since blockchain technology has already become widely popularized and its characteristics are

widely known, I will not elaborate further.

On-chain Assets

Confirmation of real assets has always been a relatively centralized behavior, which as a result has led to a bottleneck in asset liquidity. Public governance-based Blockchain networks have the potential to greatly improve the efficiency of such a system and reduce related costs. In fact, in recent years large financial institutions have initiated an alliance of blockchain networks to this end. However, a blockchain system of this type is still unable to break through the huge monopoly of large financial institutions, and cannot achieve the complete freeing of liquidity. POFID works with the existing systems rather than reinventing the wheel: with POFID public networks with privacy protection functionality can be utilized to achieve the same purpose.

After the outbreak of the subprime mortgage crisis in 2008 wreaked havoc on global financial systems, governments around the world started initiating strict supervision of financial institutions with the aim of reining in bad actors, tightening balance sheets and preventing similar calamities from occurring again in the future. Although this measure restricted banks' impulse to uncontrollably expand risky businesses, it also brought about two major negative side effects.

First, it created a liquidity trap. Central banks around the world expanded their financial statements and printed money to create large amounts of liquidity within the financial system. However, strong supervision prevented this liquidity from flowing into the real economy, forcing financial institutions that obtained such liquidity to import it into secondary asset markets with ultra-high transaction liquidity. This led institutions to artificially increase the value of such assets, causing their actual rate of return to continue to decline. The aftermath of all of this was evident in the zero or negative interest rates of assets seen in many developed economies. What resulted was the destruction in profitability of savings of ordinary citizens.

Second, operators of small and medium-sized enterprises could not benefit from all this superficial liquidity. On the one hand, their capital savings were trapped and had nowhere to go. On the other hand, the institutional arbitrage of major financial institutions was under strong supervision. Except for the so-called "risk-free" and "low-risk" assets that continued to absorb excessive liquidity and accumulate risks, a large number of small and medium-sized business opera-

tors who were truly creators of value did not have a reliable, efficient and reasonable cost channel to obtain funds.

It is a fact that a large number, if not a majority, of major financial incidents are in part due to an excessive reliance on the credit rating evaluation system of centralized institutions. Therefore, one core element in solving the liquidity problem of the real economy lies in breaking down internal barriers within finance. Blockchain technology allows for the realization of unique assets on the chain and the construction of a decentralized credit system where assets can be entrusted based on the credit rating of actual financial business data rather than institution ratings.

In POFID, we call on-chain assets OCA and they include stablecoins.

POFID Overview

POFID (short for Privacy-Oriented Financial Instrument Distribution Framework & DAO) is currently one of the most comprehensive and powerful options among all open-source solutions. Completely transcending the limits of a simple "stable currency tool", POFID was is a trusted digital asset conversion channel that maps real assets into quantifiable digital asset on the chain through smart contract technology and strong privacy protection controls. POFID supports both homogenized assets and heterogeneous assets, and uses such assets as a guarantee to generate other digital assets with various financial attributes, thereby providing better liquidity for these assets.

POFID also provides an oracle interface for evaluating real asset value behind digital assets, reliably obtaining real-time asset value fluctuations and thus providing data support for underlying risk control. POFID also serves the functional role of an on-chain autonomous trust asset management system, providing custody and investment channels for digital assets. It can be said that the emergence of this tool has the opportunity to break down barriers within financial institutions and disrupt the industry as a whole.

1) POFID Composition

The core framework of POFID is composed of several parts, including asset custody, asset risk control and POFID platform governance based on the platform currency PFID.

PSC (POFID Standardization Contract)

A series of smart contracts form the basis POFID's OCA On-chain Assets issuance and management tools. These contracts allow for asset pledges, OCA chain issuance and management, pledge repurchases, cross-chain compatibility (to support assets such as Bitcoin being used as collateral), as well as payment and clearing.

POFID's on-chain asset management smart contract functionality, although containing the basic elements of custody assets anchoring, does not define specific parameters. Any OCA can be constructed using these contracts, and parameters, such as pledge asset type or details of liquidation conditions, can be freely defined. All the characteristics of the OCAs contained in the new contracts built by inheriting these contracts are queried and displayed in a very transparent manner.

On-chain Asset Governance

As mentioned earlier, the issuance and management of all types of OCA includes a complete set of PSCs. During the construction of these PSCs, not only are the important indicators and parameters of the OCA system defined, but also a complete OCA governance structure.

These governance structures are divided into three levels: the command level, contract level and decision level.

Command-level governance means that OCA governance is implemented through PSC configuration. When the PSC is constructed, its preset parameters can be defined to achieve governance including access authorization for PSC issuance, liquidation permits and PSC-related internal variables Users can adjust supported asset types, quantity limits, risk control parame-

ters, pledge rates, repurchase anchor values, etc.

The contract level includes the deployment, execution and modification permissions of each contract that constitutes the OCA system.

The decision-making level refers to a set of decision-making systems provided by POFID for OCA managers to make decisions during governance.

Importantly, all three levels of governance modules can call each other.

PFID (Platform Coin Incentive Mechanism)

The PFID token can be understood as the role of each member on the POFID platform participating in the POFID ecosystem, governance and reward points system.

Holding PFID is a necessary condition for using some of the core functions of the POFID platform. At the same time, it is also an important incentive to participate in the POFID ecosystem and acts as an equity certificate of the overall income distribution of the POFID platform. The overall governance structure of the POFID will be described later.

2) Advantages of POFID

Cross-chain Network

POFID is by no means just a financial application based on a public chain. With regards to future design concepts of the blockchain, cross-chain connectivity is perhaps the most important type of infrastructure.

Digital assets are distributed amongst various public chains, alliance chains, and centralized systems. Digitization, settlement and confirmation of rights are not a generalized task, but one of decentralized governance. For POFID, assets provided by other systems need to be screened and processed separately, and these assets must be opened up in a cross-chain fashion.

POFID has a complete phased plan and set of solutions, based on Layer 2, for the better decentralized governance and implementation of a borderless Layer 1 network that connects digital assets from different networks. This plan can be split into three major steps:

1. Achieve the implementation of the repeater method by Layer 2. Priority will be given to ETH and similar ledger structures/public chains that support similar contract script compilation/EVM technical standards. Focus will be put on deployment on and compatibility with BSC.

2. Open up the cross-chain connectivity of major digital assets with important consensuses, for example BTC and DOT.

3. Realize POFID's own Layer 1 infinite cross-chain network within a fully decentralized governance structure, as a general standard for asset mapping, accepting the circulation and securitization of these assets on POFID.

Privacy Protection Mechanism

The public blockchain technology underlying OCAs is based on zero-knowledge proof-based privacy protection, supporting Turing complete smart contracts, and data privacy protection in the following situations:

Account asset privacy: the assets in the encrypted account, i.e. the account in the POFID system, cannot be accessed through the block browser and cannot be queried in a public manner. Rather, the account’s private key or query key must be used to obtain account asset information.

Transaction privacy: the transaction or payment information sent between two accounts cannot be publicly queried. Again, the private key or query key is necessary to obtain the content of the transaction.

Input and output privacy of smart contracts: smart contracts, including PSCs, can selectively implement privacy protection for input/output assets or other conditional data.

One would suspect that the above privacy protection mechanisms would be available for most currency systems, since very few users are willing to expose their assets to public scrutiny, but

in fact most major public blockchain platforms and stablecoins (including Ethereum and DAI) have no such protection. Their only form of privacy protection is the lack of a link between a blockchain account and the identity of its holder. But in fact, it is often possible to trace a holder and his/her associated transaction history through the account's associated KYC information. POFID has no such problem.

Multi-Currency Systems

POFID is a system with a complete framework for the management of stable cryptocurrencies. Based on POFID, OCAs can be realized through the on-chain issuance of real assets after confirmation. POFID is not only compatible with the technology and governance systems of existing stable cryptocurrencies, but can also support a diverse set of cryptocurrencies with differing standard systems.

Powerful On-chain Risk Control

PSCs provide diversified risk control strategies. In issuing contracts, transparent audits of assets are fully supported. The period and price of pledged assets can be clearly seen, and the pledge rate, early warning threshold, return purchase parameters, etc., can all be made public. There is a more detailed introduction to risk control governance below.

Endorsement of Non-homogeneous Assets

In the POFID framework, the following asset types are supported:

1) Native cryptocurrency assets

As long as the issuing organization is willing, digital assets like Bitcoin and Ethereum can be used, regardless of whether or not the endorsed cryptocurrency itself has sufficient stability. While this is an issue that issuers and users who are willing to hold this OCA need to consider,

the corresponding risk control contract mechanisms and clearing system will ensure the stability of the value of the OCA.

2) Digitized fiat currency assets (fiat stable cryptocurrencies)

Similar to the asset endorsement behind Libra, after digitizing one or more legal currency assets, 1:1 digital assets can be issued. The physical legal currency assets behind these assets can be supervised by institutions such as banks. In contrast to Libra, with POFID these corresponding legal currency assets can be arbitrarily combined, and as an asset endorsement of any OCA. Since these legal currencies are digitized, the pledge process and their status on the chain can be displayed and trusted in a more transparent way.

3) Non-homogeneous digital assets

This is perhaps the most powerful part of POFID. This is not an innovation from the perspective of monetary economics - assets behind the issuance of legal currencies in many countries are often structured in the form of national debt. However, the currency itself cerainly does not have a deadline. Assets such as creditor's rights actually have a time limit. When the creditor's rights expire, the corresponding currency needs to be recovered and destroyed. In reality, this often does not occur, leading to a risk of inflation.

The smart contract technology adopted by POFID supports rich and structured underlying data that can support the use of non-homogeneous assets such as debt, commercial bills, etc., allowing for the issuance of OCAs structured from extremely diversified assets.

Portfolio Endorsement

All the asset types mentioned above can be combined in any combination as one or more OCA pledge combinations. Moreover, an OCA itself can also be used as a pledge of another OCA's assets, as long as it has market holding requirements.

Asset endorsements of stablecoins are compatible with existing mainstream cryptocurrencies. The difference between POFID and most other encrypted stable currencies is that its underlying cross-chain technology and powerful oracle functionality can enable mainstream assets on

other chains to lock asset pledges across chains as an endorsement of an OCA's issuance.

3) Digital Asset Pledge Contracts

PV (Pledge Vault) refers to the vault of pledged decentralized assets. After an asset is digitized onto the chain, it can be pledged into the PV through a PV contract, and the OCA corresponding to the PV will be generated. It should be noted that each PV only accepts one type of asset portfolio.

The customer injects assets into the PV and issues the OCA, freezing control of only this part of the assets in the PV. The OCA issued by the user can be freely controlled, but the pledged assets can only be taken back once the user repays the OCA. Effective PVs are over-collateralized, which means that the value of the collateral is higher than the value of the debt.

POFID provides technical components for building PVs, with each PV accepting only one asset structure.

A complete PV container definition must include at least the following elements:

Supported asset types: each asset must have an independent and uniquely marked name, such as ETH for Ethereum and BSC for BSC. The PV used to construct an OCA must specify the type and combination of asset pledges supported by the OCA

Pledge upper limit: the maximum amount of pledged assets. When this amount is exceeded, new OCAs will not be issued. This mechanism is mainly used to control the issuance threshold and avoid the risk of inflation caused by excessive issuance.

Licenses that are allowed to accept repurchase: A repurchase license can be generated through the system, with the license containing a set quota. When the account holding this license initiates a repurchase from the PV and OCA1 assets are placed into the PV, then after the PV is destroyed, the corresponding OCA1 assets are released to the account that initiated the repurchase. By default, no repurchase license will be generated, so that only the account that pledges assets to the PV can initiate the repurchase.

Access permission: When the PV is constructed, it is necessary to define a list of accounts that have the right to participate in the governance of the PV and their corresponding permissions, including permissions for modification, the viewing of assets, storage and liquidation.

Contract invocation whitelist: POFID allows the contract to define a list of all addresses allowed to be invoked by the contract when the contract is constructed. This list can be adjusted by a predefined governance mechanism.

LGC mark: When a PV is constructed, the user can select the decentralized organization LGC (POFID Liquidation Governance Committee) to decide whether or not to guarantee the disposal of part of the assets. That is, when PV liquidation is triggered, and the auction mechanism still cannot obtain an asset quotation that is at least higher than that required to meet the repurchase requirements, LGC will dispose of the marked PV assets and complete the repurchase action. LGC's specific operating mechanism will be introduced later.

Case 1: PV life cycle example

1) Construct a PV1 container for an OCA, and define a digital asset (OCA1) of 1 million euros due in 1 month as the only supported asset type in a cross-border procurement trade. The smallest unit of the asset is 1, and the degree of accuracy is 0, which represents 1 euro's expired equity. The upper limit is set to 1 million. No additional issuance is allowed. When the circulation is 0, PV1 will be automatically destroyed.

2) Generate 1 million new encrypted stablecoins OCA1 for OCA1 holders and chose to generate a repurchase license.

3) The holder sells the 1 million OCA1 for 990,000 euros and provides the buyer with a repurchase license of the corresponding amount.

4) The buyer pays OCA1 to PV1 and obtains control of the pledged OCA1. PV1 initiates an instruction to destroy all OCA1 and completes self-destruction.

4) Value Stabilization Mechanism

Although the competitive currency market itself has contributed to currency stability, in order to prevent systemic market risks, it is still necessary to ensure the stability of the value of issued currencies through some pre-agreed mechanisms. There are two core issues that need to be resolved, namely currency issuance and demand constraints on holding currencies, as well as pledge asset value fluctuations and buyback strategies.

What needs to be reiterated many times over in this white paper is the point that, since POFID is a technical framework for creating a complete stablecoin system, our work will not go deep into the specific parameter definitions that define these two mechanisms, but rather just define the product modules corresponding to the mechanisms themselves, providing convenience for institutions that recognize and need these mechanisms to ensure that their stablecoins achieve improved market competitiveness.

The relationship between the demand for holding a currency and its issuance

Existing stablecoin systems generally focus on the price stability of pledged assets and rarely consider supply and demand relationships in the market of issued stablecoins. This is especially true with partial credit currencies with low value pledge rates, where these systems often pay attention to only the relationship between demand growth, repurchase trends and issuance in different historical cycles. This in itself violates the original intent of using cryptocurrencies as stable currencies, making traditional currencies more "principled" and thus more trusted by the market.

POFID provides multi-dimensional monitoring of factors and values that may affect the stability of the currency value (risk of inflation), and allows the values obtained by these monitoring modules to be connected to a PSC so that the PSC preset strategies can take effect. The changes in these values trigger various actions, such as the control of additional currency issuance, early warnings, liquidation, etc.

Strategies for the purchasing and price fluctuations of pledged asset value are influenced by:

1) Possible factors of price fluctuation

This includes the stability of pledged assets mentioned above and the relationship between supply and demand. Under the premise of guaranteeing payment and asset privacy, governance institutions can obtain global currency circulation data to observe trend changes, model supply and demand relationships, and predict future fluctuations, thereby making governance decisions that are most beneficial to achieving currency stability.

2) The way in which price fluctuations are monitored

When building an OCA PSC, you can conduct value monitoring of all asset types supported by the corresponding PV. The PSC contains customized oracles (so that the blockchain system can be governed in a decentralized way while interacting with data of centralized systems), and provide modules to integrate the data obtained by these oracles to build a flexible risk control system.

3) An intervention mechanism before passive liquidation

All PSCs must include a clearing mechanism, including active clearing and passive clearing. As in the first case, the result is a sort of active settlement request. The passive liquidation mechanism is mainly used to ensure that when assets pledged by a PV experience severe market fluctuations, the issuer is allowed to increase the asset pledge amount, or actively repurchase OCAs and destroy it. In this way, the commitment to the stability of the currency of users who are willing to hold a stable currency at the time of issue is achieved. But when the monitored value fluctuations of a pledged asset triggers an early warning (according to the liquidation rate set in the PV), the intervention mechanism will be activated.

4) Passive liquidation – an auction control mechanism

When the value of pledged assets falls below the liquidation rate, POFID DAO's liquidation governance module will come into effect. In order to ensure the stability of OCAs, when the assets of a PV depreciate below the risk control line and the requirement of an increase in pledged assets is not met, the corresponding PV assets will be auctioned off.

This method is an auctioning of PV rights - the bidder gains control of the PV by supplementing a set amount of assets (the “bid premium”) so that the PV reaches the initial margin rate. In this way, users can buy out PVs at constant prices to create significant risk-free profit.

In this mechanism, smart contracts calculate the PV's actual asset allocation quota. The assets obtained by the auction winner are equivalent to the return value of the asset redemption obtained when he immediately repays the OCA and his total investment (exercise bidding price plus repaid OCA). For users who complete the bidding, this is equivalent to obtaining a future option for this PV asset. The bid is actually a competitive acquisition of control options for all PVs, with extremely strong controllable risk and a high return space, thus providing a competitive guarantee for the stability of OCAs.

If the auction mechanism still fails to obtain a quotation, then the PV assets marked as disposable by the LGC Clearing Management Committee will be disposed of by the LGC in accordance with the guarantee mechanism set by the PV. Therefore, the LGC mark has the last guarantee in stability of the value of OCAs.

5) POFID Overall Governance Structure

5.1 Underlying technical governance

The core POFID team will complete all the work of the V1.0 version, while later versions will be open to technical contributions from developers from around the world. The decision-making work of technical governance will be completed by 12 technical "knights of the round table". There will be an election every six months, with knight commanders who rank first in the election having the right to two votes when making decisions.

5.2 PV Governance

The digitalization of assets through blockchain technology is an irreversible trend. It can be foreseen that new asset types will continue to appear in the POFID platform as collateral in the PV. The compatibility of assets is another very important feature of the POFID platform.

Some standard PV containers are preset in the POFID platform, with support for BTC, BSC and other assets. You can easily inherit the characteristics of these PVs to build your own containers that support these assets as well. When new asset types are added to the POFID system, the PV manager will observe and actively add the demos of these asset types to the PV library.

PV managers do not only exist to observe new digital assets around the world and maintain the PV library. Rather, PV managers need to make their own assessments of these assets, inform the risk control managers of the sources of these assets, and help them build up these assets' value supervision system. The members of the PV Governance Committee vote to make decisions about PV asset management in the community.

At the same time, PV managers need to use technical means and knowledge of monetary economics to evaluate the operation of all PVs currently in operation on the platform. In addition, they should conduct preliminary asset risk assessments, remind the risk control managers of the risks, as well as make economic reports on the overall PV status of the POFID platform in different periods.

5.3 Supervision and Risk Control Governance

Value Guard (VG) is constructed by risk control managers. In the POFID platform, it is

a smart contract library for value monitoring and early warning of asset types pledged in PVs.

The risk control governor of the POFID platform is not responsible for the value of the assets in specific PVs, but rather monitors value fluctuations and evaluates risk by constructing value guard contracts over different asset types.

The PSC contract triggers the liquidation intervention and operation mechanism of the liquidation repurchase mechanism. To a large extent, the evaluation basis behind it comes from the VGs on the platform. Therefore, the main responsibility of risk control managers is to design the fairest way to evaluate fluctuations in the value of assets.

5.4 LGC Liquidation Governance

The PV will set the pre-liquidation intervention mechanism condition parameters. When this occurs, the liquidation governance committee (LGC) will not play a role right away, but will need to pay close attention and be prepared to intervene at any time. If the pre-liquidation intervention fails, the liquidation auction is automatically initiated. With this said, the liquidation governance committee needs to ensure the fairness of each community bidding process,

because each liquidation involves the reallocation of assets.

A clearing distribution mechanism is defined in each PV. When users purchase an OCA, it means they already know the following information:

1. The OCA's asset endorsement composition

2. The OCA's PV liquidation method: whether or not there is mark indicating final disposal by the LGC

3. How the value of each asset in the OCA in the PV is evaluated

4. When liquidation occurs what percentage of the asset value after disposal exceeding the value of the stablecoin will be used to compensate the holders of the OCA that is liquidated and repurchased

Therefore, the LGC needs to supervise the liquidation auction process in an open and fair manner, with the possibility of eventually intervene in the execution of the liquidation.

5.5 Seigniorage

In the fiat currency system, seigniorage originally meant the difference between the cost of minting and circulating a currency and its true purchasing power. In the era of the credit currency, the composition of fiat currencies has become diversified. For example, the US dollar includes coins, paper money, bank reserves and demand deposits. In any case, seigniorage essentially derives from interest rate differentials.

More than 97% of currency in circulation is created by commercial banks through loans, and this figure is 95% in the United States. Similarly, when OCAs are issued and circulated, the assets of the loan should be added to the asset side of the balance sheet. That is, the borrower should repay the principal and interest according to the agreed upon timetable. At the same time, new assets should be added to the liability side. Adding current deposits of the same amount on the liability side (issued to borrowers), the seigniorage is calculated as the difference between these two parts, excluding other coinage and circulation costs.

From the perspective of demand, platforms like POFID have created completely new possibili-

ties. In reality, almost all mainstream monetary and financial textbooks describe banks as "financial intermediaries, which absorb savings on the one hand and grant loans on the other." Most of the currency in circulation was created, so a large part of the proceeds from seigniorage belongs to banks, at least in the United States.

If the minting entity is defined as an institution or individual that endorses the ownership of the asset, then the unprecedented undertaking of POFID allows for a a more diversified minting entity and reasonable distribution of seigniorage. In POFID, the minting entity is defined as the currency issuer. Distribution rights go to the issuer by default, but can also be set to one or more digital accounts.

One point is particularly important: on POFID seigniorage tax is processed through OCAs or PFID (the POFID platform currency). POFID collects OCAs as seigniorage tax, and distributes part of the proceeds to PFID holders, with the other part bought back from the market and burned.

The method of seigniorage taxation is mainly based on the annualized target defined by each governance DAO of POFID. According to the seigniorage tax payment methods set by the mint at the time of issuance, the figures that need to be paid in different periods are automatically calculated and the PV is only released once the seigniorage payment has been paid. The following abstracts the minting action to illustrate how the minting cost and seigniorage are expressed during the minting process.

Case 2: seigniorage payment

Here we will add the seigniorage mechanism to Case 1 to see how it works.

Assume that POFID's current seigniorage rate benchmark is set at 8% per annum.

1. PV1 container, containing an on-chain asset (OCA1) of 1 million euros receivable due in 1 year in a cross-border procurement trade, representing 1 euro due equity, with a set upper limit of 1 million. No additional issuance is allowed.

The options for OCA1 holders include (the following figures are just examples):

a) A one-time seigniorage payment at the time of issuance. The system gives a one-time payment valuation of 5%, so the holder needs to pay 50,000 OCA1 units.

b) After the issuance, seigniorage is paid every month, 0.5% each time, which is 5000OCA1 units.

c) Choose to pay seigniorage in a lump sum before the final repayment due in 1 year, and pay 8% OCA1 units (which will be higher than the interest rate paid at the time of issuance).

d) All OCAs will have a public evaluation consideration price with respect to PFID, and the PFID of the same value can be selected as the seigniorage based on this consideration.

It should be emphasized that all seigniorage late fees need to be paid with PFID. The use of PFID will be explained in more detail later.

6) POFID and the Market

POFID's underlying layer uses blockchain technology, with the core project goal being the sort of currency circulation that is indispensable for financial and daily business activities.

The POFID system can achieve optimization in at least two important aspects within the field of everyday currency systems. One is making available to the market more competitive currencies and the other the convenience of payment and settlement provided by POFID's stablecoins. These are two significant advantages given that foreign exchange settlement is currently a constraint on the efficiency of world currency circulation, something that can be considered a factor contributing to slower economic development.

POFID can quickly complete peer-to-peer payments without geographical restrictions, using any currency recognized by both parties. This is especially pertinent for multinational companies, such as Samsung, Facebook, Wal-Mart, etc., which are fully equipped to issue "borderless" stable currencies endorsed by their own commodities or other assets. The use of POFID-issued stablecoins is not only suited for these multinationals, but also institutions in the prediction market and gaming economy.

Although POFID is an open source framework for currency management, it is in fact a set of

asset securitization tools. Therefore, the following scenarios in the financial field may be used with POFID:

Lending: for supply chain finance, leverage trading, hedge funds, etc.; includes other financial derivatives such as options, speculative contracts, etc.

Cross-border transactions and remittance: can effectively improve currency stability and improve efficiency while reducing transaction costs.

The traceability of assets: charity, non-profit organizations, and government departments can use POFID to develop a transparent and traceable asset-management system and improve credibility.

Loyalty points: using the POFID system can help large enterprises develop a loyalty point-based system that puts consumers' minds to rest.

7) PFID Platform Token

Core Functionality

POFID's platform token, PFID, plays a vital role in the governance of the POFID platform. It can be understood as a decentralized platform equity, but with the additional characteristic of matching its holding with the participation and governance of the POFID platform in both a flexible and accurate manner.

Governance Authority

It should be noted that PFID is not only a form of income certificate, but also a right to governance. Governance roles are explained in succession above, including governance of the underlying technology, PVs, risk control, the liquidation governance committee (LGC), as well as the governance of institutions and individual members. It must be emphasized that with POFID, these governance roles are uniquely identified by each blockchain account on the platform.

Governors make decisions through the governance voting system included in the POFID platform on issues involving the overall decision-making of the POFID platform (for example, the way that seigniorage is collected). The election of governance roles itself is done in a similar way. Decision-making needs to be completed by designated governors with specific roles. For example, the LGC liquidation committee mentioned before will carry out bottom-up liquidation repurchases for a certain PV assets. This is all modularly integrated in the POFID governance framework.

Users need to hold a certain amount of PFID to maintain different governance roles. During the tenure of governors, these PFIDs will be entrusted to be managed by smart contracts in a sort of credit guarantee that ensures governors are fair their decisions. When problems of trust arise, these PFIDs may be deducted and destroyed as part of the punishment mechanism.

Output Incentives

Alongside its crucial role in the development of the POFID ecosystem and governance, PFID tokens are also given as a reward to governors that maintain governance duties and to encourage other capable users to participate in platform governance.

Global Assets

PFID is the default global asset on the POFID platform. In some cases, when a global asset needs to be used for consideration between all OCAs in circulation, PFID will play this role, for example in the case of the default penalty mechanism mentioned earlier.

Dividend Certificate

The last but arguably most important value of PFID tokens lies in the share of seigniorage income that they produce. Based on their PFID holdings, token holders are able to receive seigniorage income when tokens are locked up for a period of time.

Issuance Mechanism

A total of 10 million PFIDs will be produced, which is set for an entire production cycle of 10 years. Some of these tokens are fixed in proportion to governors' quotas, and are also gradually produced over 10 years. The specific distribution mechanism is as follows:

	Amount	Allocation	Duration
Underlying Technology	600,000	6%	10 years
PV	300,000	3%	10 years
Risk Control	1,500,000	15%	10 years
LGC	1,000,000	10%	10 years
Institutional Investors	1,500,000	15%	2 years
Token Holder Staking	5,100,000	51%	10 years

8) How to Follow POFID

POFID Website: https://pofid.com

Facebook: https://www.facebook.com/pg/pofiddao

Twitter: https://twitter.com/pofiddao

GitHub: https://github.com/pofid-dao

Tech Docs: https://pofid.com/Tech_guide.html

Telegram: https://t.me/pofid

Medium: https://medium.com/@pofiddao