DotKey

DotKey：Blockchain proof-of-interest financial architecture system based on Polkadot

DotKey Team

DotKey

Published by DotKey Founder Team

dotkey.live

First Publish, February 2021

Contents

I Overview

II DotKey: Financialization of Blockchain Infrastructure

III DotKey Technology Implementation and Development

IV DotKey Token Issue

V Appendix

Overview

1. Blockchain Technology

Blockchain is a distributed ledger (database) technology that connects blocks of data in an orderly manner and cryptographically guarantees that they cannot be tampered with or falsified. Generally speaking, blockchain technology can achieve the openness and transparency of all data information in the system without the need for third-party endorsement, which is tamper-proof, unfalsifiable and traceable. As an underlying protocol or technical solution, blockchain can effectively solve the trust problem and realize the free transmission of value, and has a broad prospect in the fields of digital currency, financial asset transaction and settlement, digital government, and anti-counterfeit data services.

1.1 Cryptocurrency

After experiencing physical, precious metal and banknote forms, digital money has become the development direction in the digital economy. Compared with physical money, digital money is easy to carry and store, low cost of circulation, convenient to use, easy to prevent counterfeiting and management, break geographical restrictions, and can be better integrated.

1.2 Financial Asset Transaction Settlement

Blockchain technology has natural financial attributes, and it is creating disruptive changes to the financial industry. In terms of payment and settlement, under the blockchain distributed ledger system, multiple market participants jointly maintain and synchronize a "general ledger" in real time, which can complete payment, clearing and settlement tasks that can only be completed in two to three days now in just a few minutes, reducing the complexity and cost of cross-border transactions. At the same time, the underlying encryption technology of blockchain ensures that participants cannot tamper with the ledger and that transaction records are transparent and secure, so that regulators can easily track transactions on the chain and quickly locate the flow of high-risk funds. Blockchain technology can weaken the role of underwriting institutions and help all parties to establish a fast and accurate information sharing channel. Issuers can handle the issuance by themselves through smart contracts, and regulators can review and verify the issuance in a unified manner, and investors can also bypass intermediaries for direct operation. In terms of digital notes and supply chain finance, blockchain technology can effectively solve the problem of difficult financing for SMEs. The current supply chain finance is difficult to benefit SMEs in the upstream of the industry chain because they often do not have direct trade transactions with the core enterprises and it is difficult for financial institutions to assess their credit qualifications. Based on blockchain technology, we can establish a kind of alliance chain network covering core enterprises, upstream and downstream suppliers, financial institutions, etc. The core enterprises will issue receivable certificates to their suppliers, and the bills will be digitally uploaded on the chain and can be circulated among suppliers, and each level of suppliers can achieve the corresponding amount of financing with the proof of digital bills.

1.3 Digital Government

Blockchain can let the data run and greatly streamline the office process. The distributed technology of blockchain allows government departments to be centralized on a chain, and all office processes are delivered to a smart contract, which can automatically process and flow as long as the clerk passes the identity authentication and electronic signature in one department, and all subsequent approvals and signatures are completed in sequence. Blockchain invoice is the earliest application of blockchain technology in China. The taxation department has launched the blockchain electronic invoice "tax chain" platform, and the taxation department, invoicing party and invoice recipient join the "tax chain" network through their unique digital identities, truly realizing "transaction is invoicing" and "invoicing is reimbursement". "The "invoicing is reimbursement" - invoicing in seconds and reimbursement in minutes - significantly reduces the cost of tax collection and management, and effectively solves the problems of data tampering, multiple reporting, tax evasion and tax evasion. Poverty alleviation is another application of blockchain technology on the ground. Using the open and transparent, traceable and tamper-proof characteristics of blockchain technology, it can realize the transparent use, precise placement and efficient management of poverty alleviation funds.

1.4 Certificate of deposit anti-counterfeiting

Blockchain can prove the existence of a certain document or digital content at a specific time through hash timestamp, and its characteristics of public, immutable and traceable provide perfect solutions for judicial forensics, identity proof, property rights protection and anti-counterfeit traceability. In the field of intellectual property, the digital signature and on-chain storage of blockchain technology can confirm the rights of text, pictures, audio and video, etc., create and execute transactions through smart contracts, allowing creators to regain pricing power, and preserve data in real time to form a chain of evidence, covering three major scenarios: confirmation, transaction and maintenance of rights at the same time. In the field of anti-counterfeiting and traceability, blockchain technology can be widely used in various fields such as food and medicine, agricultural products, alcohol and luxury goods through supply chain tracking.

1.5 Data Services

Blockchain technology will greatly optimize the existing big data applications and play a huge role in data circulation and sharing. In the future, the Internet, artificial intelligence, and the Internet of Things will generate massive data, and the existing centralized data storage (computing mode) will face great challenges, and edge storage (computing) based on blockchain technology is expected to be the future solution. Moreover, the tamper-proof and traceable mechanism of blockchain ensures the authenticity and high quality of data, which becomes the basis of all data applications such as big data, deep learning and artificial intelligence. Finally, blockchain can realize data computing in collaboration with multiple parties while protecting data privacy, which is expected to solve the problem of "data monopoly" and "data silo" and realize the value of data circulation. For the current blockchain development stage, many traditional cloud service providers have started to deploy their BaaS ("Blockchain as a Service") solutions to meet the blockchain development and application needs of general business users. The combination of blockchain and cloud computing will effectively reduce the cost of enterprise blockchain deployment and promote the implementation of blockchain application scenarios. In the future, blockchain technology will also play an important role in charity, insurance, energy, logistics, Internet of Things and many other fields.

2. Market Pain Points

Since the birth of Bitcoin, there have been countless public chains, including Omni, ETH, EOS, etc., and countless smaller vertical application public chains. DotKey is based on the polkadot ecology, providing liquidity for the cross-chain tool polkadot ecology and financializing the cross-chain infrastructure so that the infrastructure and service providers can gain revenue, thus becoming a lubricant for the cross-chain.

II DotKey: Financialization of Blockchain Infrastructure

3. DotKey Platform

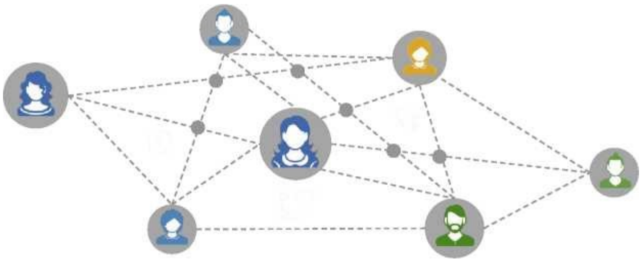
DotKey propose a blockchain solution to financialize infrastructural assets for maximiz- ing efficiency of consensus and boosting onchain application usage. DotKey build a financial channel to turn on chain assets into flexible and tradable financial products. This paper compares the traditional financial product issues and the implications of staking assets in blockchain, examines the financial influence of staked assets on application usage. Through our financial channel, individuals can get mutual benefits from both staking rewards and the surplus generated from participation of onchain applications. Node operators can issue derivatives to sell staking assets with a time threshold. Thereby, this financial protocol allows users for the first time to earn significant premiums on staking and application at the same time. The issuance of underlying assets derivatives bring flexibility and finan- cialization to the blockchain infrastructure.

3.1 DotKey Background

All blockchains aim to create a database system that parties can jointly maintain and edit in a decentralized manner, with no individual party exercising central control. The decentral- ization of the operating system on blockchain affects agents’ incentives and business practices in the economy. In a standard proof-of-stake system, the more people stake, the more tokens are taken out of circulation. This may seem good for the price of the token, but in many cases insufficient liquidity can get in the way of network growth.

Sufficient liquidity is necessary for capital to flow efficiently through a financial network. Illiquidity can act against demand because a relatively small increase in demand could cause a sharp increase in price, potentially to a point that exceeds the application utility buyer’s maximum price preference. It can also affect the economics of the supply side by making it more expensive to exit the system if selling has too negative an effect on price. Movements in price due to buys and sells are called slippage, and too much of it is undesirable. We intend to build a financial channel between protocol layer and application layer. Proof of stake token holders can deposit a native network coin into a staking contract and obtain a synthetic token which has equivalent value to the original network coin. With the synthetic token, a holder can trade in the secondary market and participate in onchain applications such as defi. While using the token freely, the holder essentially is claiming the staking reward from the underlying collateralized coin in the staking pool on the proof of stake chain. Conversely, for a node operator who is running a staking node with a large amount of staking assets, He can issue derivatives backed by his staked assets through staking auctions in our financial channel. The derivative is in the form of tokens and auction bidders can freely use the derivative tokens in applications or tradings.

Built on Polkadot, our financial channel lives on parachain and is developed by substrate and connected to parallel chains. The financial layer is an improved smart contract layer that integrates financial models. Running on polkadot blockchain, smart contracts can increase contractibility and facilitate the exchange of money and ownership of valuable things in a pro- grammable and algorithmically automated way. Even in some situations where smart contracts require the execution to be conducted by centralized parties, a decentralized consensus record reduces contracting and execution frictions. Smart contracts can improve contractibility and enforceability on certain contingencies.



4. DotKey Architecture

4.1 Staking derivative issuance

DotKey propose a staking auction mechanism where stakers can auction the staked assets and auction buyers can bid for a portion of the auction, which represents a portion of staked assets. Auction buyers can also participate in trenches to form staking backed derivatives. The governance will firstly verify the validity of staking parties and the amount of staked assets that are proposed to issue derivatives. The pricing of the derivative contracts are determined by issuers, but DotKey have a framework to provide guidelines for issuers to set ask price. DotKey first define features of staking contracts as follows:

Standard notations for each staking contract:

- Annual return rate in the staking: $k\%$；
- Staking term: T；
- Staking term: τ；
- Contract Size: C；
- Current Token Price: S；
- Current value of the staking contract: $V = S*(1+k\%)^{\tau/T}$ 。

If there are n contracts traded in the market, with all notations sub-labelled with i. Suppose $0=\tau 0<\tau 1<\cdots<\tau n$, then the (continuous-compounding) return rate of the token should be a piecewise constant ri over time $([\tau i-1],\tau i)$. These return rates should satisfies

$$\begin{cases} e^{r_1*\tau_1} = \frac{(1+k_1\%)^{\tau_1}}{V_1/S} \\ e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)} = \frac{(1+k_2\%)^{\tau_2}}{V_1/S} \\ \vdots \\ e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)}\dots e^{r_n(\tau_n-\tau_{n-1})} = \frac{(1+k_n\%)^{\tau_n}}{V_n/S}. \end{cases}$$

So we have

$$\begin{cases} r_1 = \frac{1}{\tau_1}\left[\tau_1 \ln\left(1+k_1\%\right) - \ln\left(V_1/S\right)\right] = \ln\left(1+k_1\%\right) - \frac{\ln(V_1/S)}{\tau_1} \\ r_2 = \frac{1}{\tau_2-\tau_1}\left[\tau_2 * \ln\left(1+k_2\%\right) - \tau_1 * \ln\left(1+k_1\%\right) - \ln\left(V_2/V_1\right)\right] \\ \vdots \\ r_n = \frac{1}{\tau_n-\tau_{n-1}}\left[\tau_n * \ln\left(1+k_n\%\right) - \tau_{n-1} * \ln\left(1+k_{n-1}\%\right) - \ln\left(V_n/V_{n-1}\right)\right] \end{cases}$$

Now if we want to evaluate an staking contract with time to maturity and return rate $k\%$ then its value should be:

$$\begin{aligned} V &= e^{r_1 * \tau_1} e^{r_2(\tau_2-\tau_1)} \ldots e^{r_i(\tau_i-\tau_{i-1})} e^{r_{i+1}(\tau-\tau_i)} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(e^{r_{i+1}(\tau_{i+1}-\tau_i)} \tau_{i+1}^{\tau-\tau_i} \tau_i\right. \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{V_{i+1}/S} \Big/ \frac{(1+k_i)^{\tau_i}}{V_i/S_i}\right)^{\frac{\tau-\tau_i}{\tau_{i+1}-\tau_i}} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{(1+k_i)^{\tau_i}} \frac{V_i}{V_{i+1}}\right)^{\frac{\tau-\tau_i}{\tau_{i+1}\tau_i}} \end{aligned}$$

With this pricing guidance, the issuer can evaluate the present price of their derivatives and open auction sale of staked assets.

4.2 Staking ETFs

DotKey also create a basket construction for staking rewards and it provides the easiest way to go long on the best proof of stake protocols. By holding one token, a holder can get exposure to the best return staking assets. The universal of potential PoS assets considered for inclusion into the basket are filtered based on market cap and daily volume. Assets are then ranked through factors such as staking ratio and reward ratio. Then our token basket consists of the top three tokens, market cap DotKeyighted and rebalanced monthly.

4.3 Consensus and protocols

We use Polkadot based Proof of Stake consensus algorithm, which is a hybrid consensus model that separates block production from the final determination of the block. Our network has multiple types of nodes: diligence nodes, mining nodes, and Stake proxy nodes. Diligence nodes have the right to vote and recharge channels in addition to block generation. Also they will become block generation nodes when they meet the threshold of votes. The mining node generates blocks and are more appealing to votes. The Stake agent node is elected by the block generating node. Diligence nodes, mining nodes, and Stake proxy nodes must have the same network access environment and computing capabilities. Although Diligence nodes do not need to produce blocks, it is necessary to build real nodes to send heartbeat transactions. Nodes’ block production, missing blocks, dropped or other malicious behaviors will be punished. At the same time, the node’ s self-mortgage and the user’ s waiting for reward will be deducted. Stake agent nodes will get additional Stake revenue and violate the terms of the revenue contract and will be punished accordingly. The punishment funds will be transferred to the parliamentary fund, and a subsequent referendum will decide how to deal with it.

Node registration and application are open to all users. After the node server is set up, you can start running. We use a one-vote, one-vote model to prevent node conspiracy. All users can use BNC for node voting elections. The synchronization node and the block producer node need to pay the same cost to ensure the stable operation of the network, so the synchronization node and the block producer node will get the same benefits. The Stake agent node will be an important part of our multi-chain ecosystem, responsible for the production of the Stake income of our ecosystem. In addition to the block node’ s income, the Stake agent node will also receive the dividends generated by our Stake. As an important part of our chain, the runtime environment is more low-level than smart contracts. The runtime environment consists of various runtime modules. The runtime mod- ules include modules such as accounts, balances, staking, smart contracts, transition bridges, governance, and consensus. Modules can be independent of each other, while allowing modules to call each other. Most of the code logic of the chain runs in the runtime environment.

The runtime environment allows each runtime module to be upgraded independently, while an important feature of it is that there is no hard fork upgrade. When the existing blockchain system is upgraded, due to the inconsistent running versions of each node, there is a risk of causing a hard fork of the entire chain, which seriously affects the healthy development of the entire ecosystem and the interests of nodes and users. We generate two versions each time the module is upgraded: Native and WASM. When the runtime environment determines that the version of the updated module is consistent with the current Native version, run the Native version code directly to get the fastest operating efficiency.

The assets locked by the user in the main chain through the cross-chain are multi-signed by the escrow contract, and the escrow contract is jointly managed by multiple witness nodes. Through the decentralized governance mechanism, the witness nodes are elected by the partic- ipants according to the voting share, and are rotated regularly. At the same time, when the assets held by the main chain escrow contract are too large, they can be split into multiple escrow contracts, and more trust node groups are introduced for custody to improve overall security.

4.4 Insurance and security

By depositing our platform tokens, and specifying certain key parameters (e.g. underlying asset, strike price, expiry date, etc.), options writers are able to mint arbitrary fungible option tokens called DTokens. Selling those minted Tokens allows writers to earn premiums, thereby generating revenue on their collateral. Buyers can then purchase these DTokens, which trade on exchanges such as 0x or Uniswap, ensuring market liquidity. Beyond the primitive of fungible, freely tradable ERC20 option contracts enabled by this framework, in particular focusing on protective put strategies for deposit insurance (e.g. protecting users of tokenized money markets like Compound against hacks and liquidity crises), as well as protection against stablecoins like DAI crashing in value. We also consider cases wherein option sellers wishing to offer protection can do so using a collateral type (such as ETH) which is different than the asset (such as USD) in which the strike price is denominated.

4.5 Financial Auditing

The auditors' technology adoption exhibits strategic complementarity because the cost of auditing cross-auditor transactions decreases when more auditors adopt. When clients strongly value the benefit of misreporting even after taking into consideration the possibility of being detected, they would prefer to work with auditors not using blockchain, notwith- standing that the auditor using blockchain can offer a lower auditing fee. Consequently, when other auditors are not adopting, an auditor would not find it profitable to adopt because adoption would not only fail to attract more clients, but also could result in losing clients that the auditor would get with traditional auditing. Overall, three technological features of blockchain are conducive to the auditing process:

- decentralization: the peer-to-peer design of blockchain eliminates the requirement of a trusted central party;
- encryption: the zero-knowledge proof method allows encrypted communication that preserves data privacy;
- immutability: once auditors request infor- mation through the federated blockchain, it is difficult for any auditors or outside hackers to intentionally revise or delete the information, unless they can revise information on a majority of nodes on the federated blockchain. We will build a decentralized financial auditing system to monitor the after auction activity of stakers who participate in the staking auction.

5. Economics

We have a native token for our financial channel. It serves to capture onchain value for our channel. The main functionalities of our tokens are as follows:

Services: We propose a token-locking reward model, which enables users to reward our protocol contributors by locking tokens, without needing to sacrifice their tokens. This process is similar to locking tokens: the principle is locked in a pool by a franchisee based on terms signed. Derivative issuers must negotiate a term, in terms of tokens needed and time length, allowing our financial channel to service as a public record of their agreement. Once terms have been established, the derivative issuer writes a transaction to the blockchain with the terms of their agreement. We refer to this transaction as the agreement transaction. Derivative issuers need to stake a certain amount of platform tokens to get permission for doing an auction.

ETF Issuance: we will allocate a pool of platform tokens to issue staking ETFs. Our newly issued token tracks a transparent, algorithmically managed basket of proof of stake assets. Rewards generated by the underlying assets tracked by our newly issued tokens are used to repurchase and burn.

Insurance: The concept of insurance comes from communities in the past who pooled their resources to protect each other from the risks they all faced. We realised we could build a mutual on a platform where individuals only need to trust the system, not everyone in it. The aim is to provide our members with more simple, transparent, accessible and cheaper financial protection against their risks. Our platform token will have a pool of insurance funds which secure the onchain activities. We have staking derivative cover and it provides stakers and bidders against hacks in the value storing.

Buy back and burn: We will generate fee revenues from transactions and services in the operation of financial channels. All the revenue will be used to purchase back tokens and we will burn them as the benefit to all token holders.

III

DotKey Technology Implementation and Development

6. DotKey Project Technology Implementation and

The initial version of DotKey is a token system developed based on ERC20. Tokens (tokens) are the way to define value in the blockchain and are used to calibrate financial or digital assets. On the ETH chain, tokens use the same standard so that exchange between tokens and DAPP support will be easy.

7. Blockchain technology applications

Blockchain is in essence a distributed database of transactions where all nodes in the network share data. This is the technological innovation of Bitcoin, which acts as a public ledger in this transaction process. Each node in the system has a copy of a block on the existing chain, which contains data about all the transactions that have taken place, and each block is linked to the previous block by a hash value, and these linked blocks form a blockchain. Each blockchain contains four dimensions, three horizontal dimensions of data layer, consensus layer, application layer and a vertical dimension of governance.

7.0.1 Data Layer

As the underlying horizontal dimension, the recorded transactions are broadcasted between nodes, and the complete nodes generate blocks. As the foundation of the blockchain, the transmission of digital assets and their accompanying values occurs in the blockchain, and account security is achieved through cryptographic means such as elliptic curve ciphers, hash functions, and Merkle tree algorithms.

7.0.2 Consensual Level

The consensus layer is the intermediate horizontal dimension of the blockchain and reflects the peer-to-peer style of the blockchain. In this layer, all nodes in the network reach consensus on the internal state of the chain through techniques such as proof-of-work algorithm (PoW), proof-of-stake algorithm (PoS) or its variants, Byzantine fault-tolerant algorithm (BFT) or its variants. The scalability of a blockchain is mainly influenced by the consensus layer. PoW (proof-of-work algorithm) is generally considered to be less scalable than PoS (proof-of-stake algorithm). In addition, the double payment problem and the possible state tampering attacks on the blockchain can also directly affect the security of the consensus layer.

While the above two horizontal dimensions build the basic architecture of the blockchain, the application layer is critical to the actual application of the blockchain, affecting issues including blockchain scalability and usability. For example, the programmability of smart contracts used by wavefields allows individuals to rely on a distributed "global computer" to execute the terms of the contract. Sidechain technology and merge mining have also greatly advanced programmability. The development of stateful channel technology for secondary protocols, represented by the Lightning Network, further enhances the scalability of blockchains at this level. In addition, application tools, software development kits, framework structures, and graphical user interfaces are particularly important for the usability of blockchains. The application layer provides developers with a platform to develop decentralized applications (DApps), which is an important part of the blockchain to realize its usability and value.

7.0.3 Governance Layer

Like any organism, a successful blockchain will be the best adaptor of its environment. With the premise that blockchain systems can only survive through evolution, while the initial design is important, the mechanism that is changeable over a long enough period of time is undoubtedly the most important, and this mechanism is what we call vertical-level governance.

7.1 Consensus mechanism

7.1.1 PoW

PoW (Proof of Work), or Proof of Work, is known as Bitcoin, commonly known as "mining".

PoW is a metric set by the system to achieve a certain goal. It is simply understood as a proof that you have done a certain amount of work. The whole process of monitoring work is usually extremely inefficient, and certifying the results of work to prove that a certain amount of work was done is a very efficient way to do so.

POW has the advantages of decentralization and high security, but it wastes arithmetic power, consumes a lot of resources, has low network performance, and has obvious disadvantages such as centralization of arithmetic power.

7.1.2 PoS

PoS (Proof-of-Stake), or Proof of Interest, can be seen as a replacement for PoW, which solves some of the problems in PoW, but also presents new problems. The design concept is that the choice of block-keeping rights is randomly chosen based on the shares and possession time of different nodes. It solves the problem of Bitcoin's possible crippling of the entire network as miners' motivation decreases and thus the number of miners decreases, and also increases security because the cost of breaking the ring is not only 51% of the arithmetic power, but also 51% of the holdings.

PoS is more energy efficient, decentralized, and inflation-proof. the basic idea of PoS is to randomly select a group of nodes to vote on the next block and weight their votes according to the size of their funds (i.e., equity). If some nodes misbehave, the system may confiscate the funds on their chain. In this way, the blockchain can still operate more efficiently without going through the high computational cost of PoW, in addition to achieving economic stability on the chain: the more equity participants have, the greater their incentive to maintain the ledger consensus mechanism, and the lower the likelihood of their nodes misbehaving.

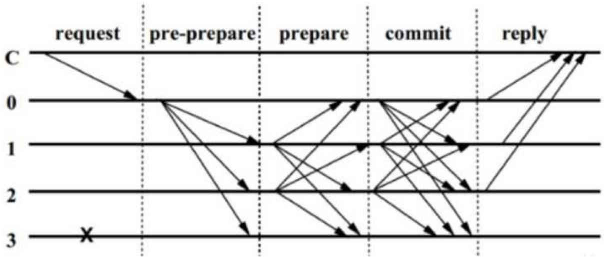
7.2 Practical Byzantine Fault Tolerance Algorithm

Practical Byzantine Fault Tolerance (PBFT) is an effective attack-resistant algorithm proposed by Castro and Liskov in 1999 for reaching agreements in distributed asynchronous networks. We plan to use PBFT as the base voting algorithm for our DPoS consensus mechanism because it is a concise and well-researched algorithm that provides fast settlement, which is essential for building efficient and scalable blockchains. As demonstrated in Castro and Liskov's original paper, PBFT can provide availability and security to the chain as long as less than one-third of the network nodes fail or act maliciously; at the same time, the network cost of PBFT is very low, only 3% of the cost of an unreplicated network system.

PBFT is a state machine copy replication algorithm, i.e., the service is modeled as a state machine, and the state machine is replicated in different nodes of the distributed system. Each copy of the state machine preserves the state of the service and also implements the operations of the service. The set of all replicas is represented using the capital letter R. An integer from 0 to $|R|-1$ is used to represent each replica. For descriptive convenience, it is usually assumed that the number of failed nodes is f and the number of nodes of the entire service is $|R| = 3f+1$. f is the maximum number of replicas that are likely to fail. Although more than $3f+1$ replicas can exist, additional replicas cannot improve reliability except for degrading performance.

All replicas operate in a rotation process called view (*view*). In a given view, one replica acts as the primary node (*primary*) and the other replica nodes act as backup nodes (*backup*). Views are consecutively numbered integers. The master node is calculated by the formula $p = vmod|R|$, v is the view number, p is the replica number, and $|R|$ is the number of replica sets. The view rotation process needs to be started when the master node fails.

The PBFT algorithm is implemented as follows:



IV

DotKey Token Issue

8. Token Issue

8.1 Project Roles

- Direct builder: the foundation and founding team responsible for developing the underlying technology of Dotkey public chain and the "fund" supporting the operation of the founding team;
- System maintainer: the "miner node" that maintains the operation and security of the Dotkey system;
- Eco-builder: "Community users" who continue to create value for the Dotkey ecosystem.

From the perspective of these eco-members, Dotkey's economic model will adopt different incentive models according to different stages, so that the whole Dotkey eco-system can make a smooth transition from initial operation to mature development

8.2 Project operation phase

- Initial phase: Solve the cold start problem of the system by motivating direct builders and eco-builders
- Operation phase: Promote continuous upgrading of the system by continuously motivating system maintainers; promote adaptive allocation of Dotkey's system resources through market-based system resources

8.3 Token Allocation

To effectively incentivize community building and achieve the growth and prosperity of DotKey ecology, DotKey issuing platform issues pass token - DotK. The total issue volume is 100 million, which will never be increased and deflation mechanism will be implemented to ensure the effective rise of the coin price. DotKey is allocated for the following purposes.

- 10%: First round investors: the first round investors receive 10% of the Genesis pass incentive, which circulates in a timely manner.
- 36%: Foundation Team and Founding Team: The Foundation Team and Founding Team will receive 36% of the Genesis pass incentive, which will be distributed as a pool of funds on an

ongoing basis. This portion of the pass will be unlocked in 4 years.

- 12%: Community Fund: 12% of the Genesis pass will be used to incentivize general community users and encourage early community input into the building and maintenance of the Conflux ecosystem. This portion of the pass will be unlocked within 4 years.
- 42%：Eco Fund: 42% of the Genesis pass will be used to incentivize community developers and incubate DApp projects that support the Dotkey ecosystem. This portion of the pass will be unlocked in 4 years.
- Public Funds: No additional credits will be allocated to the DOTKEY Public Funds account during the initial phase

V

Appendix

9. Appendix

9.1 Legal Statement

The sale of DotKey is intended solely as a medium of exchange for a specific target audience or participant and is not a prospectus or offering document in any form, nor is it intended to constitute an offer of any form of securities, units in a business trust, units in a collective investment scheme or any other form of investment, or an offer of any form of investment in any jurisdiction. No regulatory authority has reviewed or approved any of the information set forth in this White Paper. This White Paper has not been registered with any regulatory authority in any jurisdiction. By accessing and/or accepting possession of any information in this White Paper or part thereof, as the case may be, it is implied that you meet the following conditions.

1. You are not in the People's Republic of China, nor are you a citizen or resident (for tax purposes or otherwise) of, or residing in, the People's Republic of China.
2. You are not in the United States of America, nor are you a citizen, resident (for tax purposes or otherwise) of, or residing in, the United States of America.
3. You are not in a jurisdiction where the sale of a token in any form or manner, in whole or in part, is prohibited, restricted or unauthorized, in accordance with the laws, regulatory requirements or rules of your jurisdiction.
4. You agree to be bound by the above restrictions and limitations on the letting of ownership.

9.2 Risk Warning

This white paper does not constitute investment advice, or a license to sell, and does not induce or attract any purchase. Any such offer or solicitation will be made on trustworthy terms and as permitted by applicable securities and other relevant laws, and the above information or analysis does not constitute an investment decision or specific recommendation. This white paper does not constitute any investment advice, investment intention or solicitation of investment in the form of securities. DotKey expressly states that the prospective user expressly understands the risks of DotKey and that by participating in the program, the investor understands and accepts the risks of the program and is willing to personally assume all consequences or consequences thereof. DotKey expressly disclaims any liability for any direct or indirect losses resulting from participation in a cryptocurrency market project, including:

- Economic losses due to the user's trading operations.
- Any errors, omissions or inaccurate information arising from personal understanding.
- Losses arising from personal trading of all types of blockchain assets and any actions resulting therefrom.

DotKey is not an investment, and there is no guarantee that DotK will increase in value, and in some cases there is a possibility that the value will decrease, and that those who do not use DotK properly may lose the corresponding rights to use it.