VGO Public Chain White Paper

2019.05.09

VGO Public Chain White Paper

Table of Contents

Summary....4

1、Background of designing....5

1.1 Business background....6

1.2 Demands and painpoints....7

1.3 VGO Program....11

2、VGO Project introduction....12

2.1 Bitcoin peer-to-peer digital cash system....12

2.2 VGO bifurcation method....14

2.3 Deviation of Bitcoin development from its original design goals....18

2.4 VGO fork information....20

3、The technology behind the VGO public chain....21

3.1 VGO as a value internet protocol....21

3.2 The most effective consensus mechanism DPOS....22

3.3 UTXO, the safest accounting model....24

3.4 Omni protocol....28

3.4 Smart Contract Virtual Machine VVM....28

3.5 InterPlanetary File System IPFS.....29

3.6 VGO public chain overall technical architecture.....31

4、Token and main applications.....33

4.1 Token VGO and USDO.....33

4.2 VDEX(VGO Decentralized Transaction Platform).....34

4.3 BFR(Bitcoin Federal Reserve).....36

5、VGO Ecosystem governance.....38

5.1 Problems to be solved in blockchain governance.....38

5.2 VGO governance definition.....40

5.3 System role definition.....41

5.4 VGO node requirements and election rules.....44

5.5 VGO Council Rules and Regulations.....45

5.6 VGO DAO fund.....48

5.7 Self-evolution of the VGO protocol.....50

6、Vision.....51

7、Route map.....52

8、Legal.....53

9、FAQ.....55

10、Disclaimer.....62

11、References.....68

Summary

Since birth of genesis block, Bitcoin has been in the past ten years. Bitcoin has attracted global attention in a dazzling way, and has gradually formed a blockchain platform integrating functions such as payment, reserve and database. On the other hand, Bitcoin also has serious problems, such as energy-consuming, easy to be manipulated, low efficiency, and unfriendly to smart contract and DAPP development. To this end, this paper proposes Bitcoin-based bifurcation technology VGO (HyperBitcoin), and proposes a new bifurcated coin case attempt for the current problems faced by Bitcoin. Since high-power mining hardware is electricity-based, the proof of work mining is unsustainable in the circumstance. Using energy-efficient DPOS algorithms, VGO can be mining on any computer and never requires any specialized mining machines. Also, based on the DPOS consensus mechanism, generating blocks in short time, high efficiency and robustness, VGO can achieve efficient transaction confirmation. As VGO is a decentralized global value Internet transmission protocol, Satoshi Nakamoto is based on Bitcoin's vision. The VGO protocol provides a simple solution for Bitcoin sustainability issues and provides a faster, more scalable blockchain platform for executing smart contract by HVM(HyperBitcoin VM) smart contract virtual machine. The platform is more suitable for daily trading.

It is a sustainable decentralized peer-to-peer transaction, including peer-to-peer payments and decentralized digital asset transactions. Anyone who accepts the VGO protocol can use VGO almost free of charge to ensure the real-time and security of the transaction. With strong network throughput, VGO provides full performance support for rapid development and any requirements such as point-to-point payment, smart contracts, decentralized trading platforms, VGO (Virtual Goods Offering), and Bitcoin Federal Reserve.

In addition to the VGO currency, the VGO public chain also launched the stable currency USDO based on Ominlay. This white paper will explain these concepts in detail.

1 Background of designing

1.1 Business background

Founded in 2009 by Satoshi Nakamoto, Bitcoin is the world's first implementation of blockchain technology applications. The Bitcoin network is a global computer network connected by the Internet, and each computing device is called a node. When someone sends some BTCs, the transaction will be broadcasted to all nodes, and each node can independently verify the authenticity of the transaction. The Bitcoin system packs all transactions that occur every few minutes into a single block. In order to fully process the transaction block and add it to the blockchain or public ledger of all historically valid transactions. The nodes need to compete to solve difficult math problems, the lucky node that took the lead in completing the correct solution first won the new Bitcoin reward, and the block was added to the blockchain. The process of solving difficult mathematical problems, that is, calculating intensive mathematical problems, is called POW proof of work, and POW is a consensus mechanism for Bitcoin network security.From the angle of currency, Bitcoin is by far the most famous digital currency. It is an important application of the blockchain 1.0 era. It is the first application of the blockchain: Bitcoin realizes the functions of digital currency under the premise of decentralization, such as issuance, payment, circulation, etc.; it is a new means of payment.

From the angle of blockchain, as Bitcoin's attention from people has gradually increased, the blockchain has become more and more widely known as the underlying technology. Blockchain has gradually separated from digital currency and penetrated into many business fields. Many different industries are hoping to apply Bitcoin technology in real life, and let people get a better experience through a variety of application.

Satoshi Nakamoto's vision for Bitcoin is to allow cross-border point-to-point payments and create the world's first truly decentralized value transfer network, which is undoubtedly revolutionary. Also, the underlying blockchain technology of Bitcoin directly leads to the establishment of many decentralized networks, such as ETH, EOS, etc. These networks allow for smart contracts, identity protection, intellectual property management, supply chain management and many other unprecedented innovations.

1.2 Demands and painpoints

As public awareness of Bitcoin and blockchain technology increases, so does the valuation of the cryptocurrency market. As more and more investors and speculators begin to understand the true potential value of blockchain technology, mainstream cryptocurrencies value has steadily increased. Even though blockchain technology has bright future, the question is how it ensures its long-term sustainability, scalability in the development

of the cryptocurrency ecosystem. Blockchain energy-consuming networks such as Bitcoin and other proof of work are not sustainable in the long run. Bitcoin's energy consumption is growing rapidly because it uses a very inefficient POW consensus mechanism to protect its network. The whole purpose of Bitcoin is to allow people to transfer value quickly, cheaply, and anonymously in a de-centralized network that does not require a middleman.Bitcoin makes full use of cryptography to ensure the security of the operation of the Bitcoin system. The main principles of cryptography are: hash algorithm and asym metric en-cryption. Hash algorithm, simple understanding, is to "code" all transaction in-formation, it is one-way, and the transaction information of the entire network will not be found like the trader's personal information. The hash algorithm can be said to run through the entire Bitcoin, no matter which step is inseparable from the hash algorithm. Asymmetric encryption enables information security and asset security for both parties without a centralized organization (bank). Although in theory, these cryptographic principles can guarantee the realization of Bitcoin as a basic function of "decentralized currency", Bitcoin has some problems, which makes the direction of Bitcoin development off its purpose:

1.2.1 Processing transactions is too slow

In the Bitcoin system, up to 7 transactions are processed in one second. Obviously, this speed cannot meet the normal trading needs. To know that Alipay, Taobao, WeChat, which we use now, can process hundreds of thou-sands or even millions of transactions per second. A transaction takes only

1–2 seconds to process successfully. If Bitcoin is used like daily currency, then It is hard to accept that we make a payment on WeChat, which takes at least 1–2 days to process.

1.2.2 Expensive transaction costs

IMiners now set transaction fees to increase in time and use it to extract rents from everyone's rent as a means of exchange. Now the transaction cost of Bitcoin is very high. According to the current cost, if you want to confirm within half an hour, you need to pay 130000 0.0009=117 yuan (the Bitcoin transaction fee has risen to 500 yuan/per transaction on January 7, 2018). This cost is far higher than all other payment methods except for cross–border remittances. If you are not willing to pay so much, then you need to wait three or four days, but it is more likely that your payment will be rejected. This low efficiency is unbearable. What is even more concerning is that this fee is generated by 12.5 Bitcoin reward of per blockchain. This reward is halved every four years. After continuing to halve twice. The income of the miners is mainly the income of the transaction fee, which means that every time you make transaction, you may have to pay $500 each time.

1.2.3 Bitcoin mining is electricity–consuming

Mining requires a professional mining machine. The professional mining machine has a high computing power, but is electricity–consuming. And in the current market, it is difficult to recover the cost after buy a mining machine in

one year. Bitcoin now consumes 290 billion kWh of electricity from mining, exceeding the electricity consumed by 159 countries. Therefore, some people think that consuming such large amount of electricity to maintain a system with such a slow transaction speed is wasteful and unsustainable.

1.2.4 Not friendly to smart contracts and DAPP development

Bitcoin system can only perform simple script programming. Script is a stack-based scripting language for transaction processing in the Bitcoin protocol. The Script programming language is not turing-complete, lacking the functionality of modern programming languages, such as loops, and can only be used for limited application programming. Bitcoin requires to be developed with common scripting languages to support various applications development.

1.2.5 Deflation as a currency

Currency is considered to be more important than real wealth. Bitcoin has deflation as a cryptocurrency. Because Bitcoin has a total of 21 million, the lack of liquidity has limited the development of Bitcoin. We need enough currency to enable us to trade according to our choice.

1.3 VGO program

Bitcoin system that VGO is dedicated on has many limitations, as a transactional daily currency, VGO is designed to provide a scalable and sustainable alternative to Bitcoin. Using energy-saving DPOS algorithms, VGO can be mined on any computer and never requires professional mining equipment. Also, based on the DPOS consensus mechanism of generating block in short time, efficiency and strong functions, VGO can achieve efficient and fast transaction confirmation. And through the VVM(VGO Virtual Machine) smart contract virtual machine to carry out smart contract encoding operation, it provides a faster, more scalable blockchain platform, which is also more suitable for daily trading use. Deal with the deflation through the USDO token.

2 VGO project introduction

2.1 Bitcoin peer-to-peer digital cash system

Bitcoin is a digital cash system that is fully implemented through peer-to-peer technology. It enables online payments to be initiated directly by one party paying to the other without the need to go through any financial institution. Although digital signatures partially solves this problem, if third-party support is still needed to prevent double-spending, then the system loses its value. The Bitcoin White Paper proposes a solution that allows the cash system to operate in a peer-to-peer environment and prevents double-spending issue. The network adds timestamps to all transactions by random hashing, and merges them into a continuous, random-hash-based proof of work chain as transaction records. The transaction records that have been done will not be changed unless re-complete all proof of work. The longest chain will not only serve as proof of the sequence of events observed, but also as a chain containing the maximum computational effort of the CPU. As long as the majority of CPU computing power is not intended to cooperate together to attack the entire network, honest nodes will generate the longest chain that exceeds the attacker's. The system itself requires very little infrastructure. Information can be spreaded throughout the network with the utmost effort, nodes can leave and rejoin the network at any time, and the longest proof of work chain is used as proof of the transactions that occurred during the offline of the node.

The subtext behind Nakamoto's "decentralization" is "most people's integrity", and the consensus mechanism is the core concept of Bitcoin. Establish a “decentralized P2P payment system” without centralized (intermediary) payment system. In order to avoid double-spending, how to check the ledger? The answer is through a consensus mechanism: replace the centralized authority credit with the cryptographic principle and the proof of work (Pow). There will always be a sequence of new transactions, even if it is a double spending, there is always a sequence, the same user can not create two transactions at the same time. Bitcoin first introduced a timestamp-based random hash, which was formed into a sequence before and after. Bitcoin transaction record is a time series chain. This is why it is called a blockchain. To avoid double spending, just prove that one of the chains is valid and record it on the trading chain, then other transactions are invalid. To prove that one of them is valid and does not allow centralization to exist, there is only one way: to mobilize everyone to participate in this activity and to carry out "majority people witness".

The POW consensus algorithm is for solving the problem of who are the majority, and the "majority" decision is expressed as the longest chain. The new block performs node broadcast; once a node receives the broadcast of the block, it will follow the rule of "if and only if all the transactions contained in the block are valid and have not existed before, other nodes will recognize the validity of the block." After the verification is passed, the node will no

longer accept the same block of other nodes. At the same time, this node will terminate its own block calculation containing the same transaction. The node starts a new transaction block calculation based on this block, and so on, forming a chain. Due to the network delay, if several nodes receive the transaction block from each other and record the same chain (fork), the break of the deadlock will wait until the next proof of work. Through a period of operation, there is always a blockchain with the longest time series as the final approved chain. The Bitcoin blockchain is a process of bifurcation, abandonment, bifurcation, and merging (the forks here are temporary soft forks). The consensus mechanism replaces the intermediary trust, and the designer intelligently introduces the miner's reward mechanism, which relies on the miners' power to build a wall of Bitcoin trust, and then creates a global digital cash system from scratch by irreversible coagulation calculation. The key element of the cash system is trust. Bitcoin cash system is a technology for transforming Internet communication protocols that will create new trust networks that will form a huge economic ecosystem and produce lasting long-term value. In a sense, building a strong and cumulatively growing trust is at the heart of the core of the Bitcoin protocol design philosophy.

2.2 VGO bifurcation method

Bitcoin bifurcation, in a broad sense, refers to the splitting of the Bitcoin blockchain in the topological structure, which forms the coexistence of two

tchains in a short period of time; but under the role of the Bitcoin consensus mechanism, blockchain will eventually recover to the consensus state to the unique chain. The narrowly defined bifurcation generally refers to the hard fork caused by the change of the protocol. The splitting of the consensus causes he Bitcoin network to operate in multiple sets of different consensus groups, forming several independent blockchain protocols. Bitcoin has numbers of forked protocol versions that are still running successfully. Different versions of the protocol have different solutions for the defects or limitations of Bitcoin. VGO is an implementation version of Bitcoin by initiating a hard fork of the original Bitcoin protocol. VGO can be considered as an interpretation of the Bitcoin protocol and should be considered as a landing solution for the peer-to-peer electronic cash system. VGO adopts UTXO-based DPOS consensus mechanism, which is designed to be a long-term stable operation of the main network.

VGO believes that a true point-to-point payment system needs to meet the following conditions:

1) The necessary information throughput and transaction processing speed should be sufficient to deal with high-frequency micropayment transactions;

2) The operating cost of supporting the payment system is low, which is much lower than the total social utility of the system's effectiveness;

3) Design an economic system that enables the system to operate stably over the long term, introducing appropriate roles to support system functions with expanded potential and balancing their interests;

4) There are some ways to self-update the protocol, enabling the system to evolve and introduce new features to adapt to the environment.

VGO's bifurcation methodology: 1) VGO recognizes the value and status of the original Bitcoin protocol, reuses and draws on the data generated by the original Bitcoin protocol and most of the important design ideas; 2) VGO hopes to realize the Bitcoin point-to-point cash system, the original intention of the design. Establishes a technically feasible and globally shared peer-to-peer cash system by transforming the Bitcoin protocol; 3) On the basis of the point-to-point cash system, the protocol is required to carry certain economic activity functions, which is simple, safe and available to everyone. 4) VGO's above modifications and innovations in the Bitcoin protocol not only fundamentally solve the technical and economic problems that must be faced in building a peer-to-peer cash system, but also introduce technologies and models that have been proven mature as much as possible. Ensure system stability, user acceptability and long-term sustainability.1

In order to ensure sufficient information throughput and control of operating costs, VGO introduces an efficient DPOS consensus mechanism to ensure stable 3 seconds of block generating and irreversible block design, which not only makes point-to-point payment technical support, but also allows the built-in dApp, on-chain management, smart contracts and other complex on-chains functions to be fully feasible. Secondly, in view of the maintainability and sustainability of the agreement and the ability to solve problems in a long-term creative way, VGO has built its own characteristics of on-chain governance philosophy, introducing an on-chain governance system that combines democracy and efficiency. The system greatly encourages the community's participation on the chain and promotes the response of the participating groups to environmental changes. Therefore, the agreement can quickly update iterations and become a Bitcoin protocol that can self-operate and self-renew and evolve. In view of the need of protocol functions for complex system roles in the economic model, VGO's on-chain management system and VDEX system introduce economic behavior roles such as nodes, sharing governance committees, transaction gateways, and acceptance gateways, and the power structure realizes the separation of the two powers of accounting and governance, which has taken a creative step in the democratic practice of governance on the chain.

2.3 Deviation of Bitcoin development from its original design goals

The original intention of Nakamoto to design Bitcoin was originally to pursue a relative fairness and pursue an unmanipulated monetary system. The original intention of Nakamoto to create Bitcoin: to establish an digital monetary system that does not rely on government; it’s decentralized. Bitcoin, as a cryptocurrency, is gradually deviated from his original intention. Although Bitcoin has most of the characteristics of the legal currency, it is indeed a big pit for the wide circulation in terms of stability. Although the exchange rate between national currency is often fluctuating, it does not affect the daily use of people. The price fluctuation of Bitcoin can only appeared on the K-line chart. Bitcoin does have some attributes of currency in some respects, but as far as the current situation is concerned, stability and liquidity are the two flaws, and these two flaws are also the main reason hindering the civilianization of Bitcoin. Although Bitcoin is designed to guarantee the technical feasibility of the decentralized, peer-to-peer digital cash system, this does not mean that the development path of Bitcoin fully conforms to the original intention of its white paper.

Bitcoin has serious energy-consuming problem, and its computing power is easily manipulated. Low efficiency, and is not friendly to smart contracts and DAPP development. Bitcoin has exposed many shortcomings as a

peer–to–peer cash system, and has chosen to prefer stored value asset under market influence as self–positioning. As mentioned earlier, a true peer–to–peer payment system requires: 1) The necessary information throughput and transaction processing speed should be sufficient to deal with high–frequency micropayment transactions; 2) The operating cost of supporting the payment system is low, which is much lower than the total social utility of the system's effectiveness; 3) Design an economic system that enables the system to operate stably over the long term, introducing appropriate roles to support system functions with expanded potential and balancing their interests; 4) There are some ways to self–update the protocol, enabling the system to evolve and introduce new features to adapt to the environment.t

In addition, the governance mechanism of Bitcoin relies on the most primitive off–chain governance. The internal cost of governance is extremely serious and cannot achieve rapid response. This should be a well–known problem that once affected the survival of Bitcoin. Due to the choice of the Bitcoin route, the Bitcoin development team is extremely conservative about the changes and upgrades of the protocol, which makes Bitcoin unsuitable as a system for point–to–point cash systems that favors payment applications. Although Bitcoin has built a miner system that can be operated continuously, the miner system is too simple and low for a point–to–point payment system that is more practical and has a more complex function design. Moreover, the current mainstream arguments generally is that it is possible to prove from the mathematical and economic principles that the interests of miners and users and de

velopers are inconsistent under the POW mechanism. The Bitcoin system cannot give a good solution that can produce revenue and balance the interests of all parties in complex chain system economics (such as gateways), nor can they separate the two rights of accounting and governance, greatly hindering Bitcoin to adapt to complex economic activities.

2.4 VGO fork information

- Forking date: The plan is on August 8th, 2019 Beijing time;
- Fork block height: 555555;
- Consensus mechanism: DPOS based on UTXO;
- The total amount of VGO tokens will be issued: 84 million;
- Generating block interval: fixed for 3 seconds, can be adjusted dynamically;
- Set an irreversible block;
- Block volume: up to 128M, can be adjusted dynamically;
- Issue stable currency USDO (1 : 1 USD)
- Add VVM virtual machine function;
- Add replay protection;
- Support CPU mining;
- Have the ability to expand smart contracts;
- Integrate with IPFS.

3 The technology behind the VGO public chain

3.1 VGO as a value internet protocol

n a large model such as the Internet, a blockchain is a value point-to-point transmission protocol in the application layer, and its value is the same as the value of the HTTP protocol in the information Internet. Without the HTTP protocol, websites can't find each other; without blockchain protocol and help of the intermediary, it is impossible to complete the value transmission on the Internet peer-to-peer. The blockchain itself is an Internet protocol, which is where the blockchain is in the overall Internet model. VGO is an Internet value transfer protocol. The so-called value transfer refers to the value expression, delivery and credit construction that can be realized under a specific protocol framework, and all economic and financial activities based on this, which may include transfer remittance, digital asset transaction, legal currency transaction, and other series of applications with real-world functions and social utility, such as digital asset exchange, credit endorsement of digital asset issuance and trading, decentralized exchanges, and transaction and acceptance gateways. The core design of the VGO protocol is: by selecting the appropriate technical architecture to ensure that VGO has sufficient capacity to act as a carrier system for global Internet value transmission. The VGO protocol is the basic framework for achieving value transmission, that is, the carrier of economic behavior in all chains. The VGO protocol is based on the UTSO-based DPOS consensus mechanism. It balances the per

formance and reliability of UTXO and DPOS with irreversible blocks, timestamp consensus, and Cache middleware. It achieves a protocol that is closer to the point-to-point cash system design than the original Bitcoin. The VGO value Internet protocol network transcends the level of social networks and realizes the value connection between people. From the nature of the connection, the network forms a relationship between the distributed entities of the subsystem through the protocol, thereby realizing the interaction of the subsystem or node with other subsystems or nodes. Connection are ubiquitous, it makes elements interaction possible and forms the economy.

3.2 The most effective consensus mechanism DPOS

DPOS (Delegated Proof of Stake) Features: The time of generating block is extremely short, the efficiency is high, and it is hardly forked. These features make DPOS have unique advantages for a long period of time in the future, and it is a relatively advanced consensus model. VGO adopts the DPOS mechanism. DPOS guarantees that voting rights are in the hands of the token holders, so the token holders will be able to vote whether or not to pass the case, thus determining the direction of the project. This also means that the direction of the project depends on the people who care about the project, and the power of the public will drive the project to develop better. Also, the advantages of the DPOS mechanism are that there is no computing power attack, strict observance of time, and resource conservation.

3.2.1 DPOS consensus mechanism advantages

(1) Low power consumption

The DPOS mechanism reduces the number of nodes, and changes the relation between nodes from competition to cooperation, avoiding unnecessary loss of unnecessary computing power and mutual attacks. Before ensuring network security, the entire network energy consumption is further reduced and the network operating cost is the lowest.

(2) High efficiency

Faster confirmation speed: Take VGO as an example, the time per block is fixed at 3 seconds, a transaction (after getting 6–10 confirmations) takes about 1 minute, and the completed block production cycle takes only 5 minutes. An irreversible block can be generated as a confirmation point every 1–2 cycles. In the PoW mechanism, taking Bitcoin as an example, it takes about 10 minutes to produce a block, and it takes at least 1 hour to confirm a transaction (get 6 confirmations).

(3) Robustness

Throughout the process, anyone can monitor the health of the network by observing the witness's participation rate. If at some point the witness's participation level is below a certain level, the entire blockchain trading network user can be allowed to use more time for transaction confirmation, and

also remind users to be highly vigilant about their network conditions. It can remind users that there may be potential problems on the blockchain network within 1 minute of the problem. The DPOS mechanism was first applied by BM in the BTS project. BM's other famous projects STEEM and EOS have also followed this consensus mechanism. Since DPOS has appeared, DPOS has been synonymous with high performance, efficiency, and flexibility. The long-term practice of many projects has proven these excellent features of the DPOS mechanism.

(4) Efficient governance

Developers can implement any changes they deem appropriate as long as it is approved by stakeholders. This policy not only protects developers, it also protects stakeholders and ensures that no one is unilaterally controlling the blockchain network or getting the blockchain network out of control. Hard forks replace 51% of witnesses, so the more stakeholders involved, the more election witnesses they have, and the higher the security of the entire system.

3.3 UTXO, the safest accounting model

UTXO stands for Unspent Transaction Output, which is a core concept of Bitcoin transaction generation and verification. The transaction constitutes a chain structure, and all legal Bitcoin transactions can be traced back to the output of one or more transactions backward. The source of these chains is

the mining reward, and the end is the current unspent transaction output. In the UTXO model, transactions simply represent changes to the UTXO collection. The concept of accounts and balances is more abstract on the UTXO collection, and the concept of accounts and balances only exists in the wallet. Based on UTXO (BTC) trading rules: 1) In addition to the coinbase transaction, all sources of funds must come from UTXO of one or several transactions before, just like water pipes, one after the other, and money flows between transactions. 2) A transaction can have multiple inputs or multiple outputs, but the total transaction input for any transaction must equal the total transaction output (plus the total transaction fee incurred during the process), and the equation must be balanced on both sides.

Bitcoin was originally designed to be a peer-to-peer digital cash system. In Bitcoin, each transaction consumes the UTXO generated by the previous transaction and then generates a new UTXO. The balance of the account is the unspent UTXO set belonging to the address. The status of Bitcoin is the current unspent UTXO collections. In the past 10 years, the UTXO data model used in Bitcoin has proven to be a reliable way to create stable and reliable digital currency. The most important function of currency is to become a medium of exchange, and the UTXO model does this very well. The core idea of the UTXO model is to ensure that the data that has been written is immutable. Based on this core idea, the chained UTXO connects the input and output of different transactions through a hash pointer to ensure the legitimacy of all transactions and realize the traceability of UTXO. Inheriting this

through forks is critical to VGO. UTXO is currency-centric, not human-centric, and assets are easy to be monitored and counted. UTXO's asset-centric design model is well suited for asset management on VGO.

3.3.1 UTXO model advantages

(1) One time

Each transaction in the UTXO model consists of multiple transaction inputs, which are actually UTXO + signatures. There are only two statuses for each transaction output, one is spent and the other is unspent. This ensures that each UTXO can only be spent once and is highly resistant to double-spend attacks.

(2) Secrecy

Compared to the account model, UTXO is more private. As previously known, each UTXO is "one time". If the user changes an address for each transaction, it is difficult to find the correlation between the two addresses, which guarantees the concealment of the transaction. If there is a need to further increase this concealment, it is also possible to consider the use of circular transaction signature pairs, trading elements and other technical means.

(3) Reliability

In a block structure, previousblockhash and merkleroot are the two most important fields, both of which prevent the transaction information from being tampered with. The core idea of the UTXO model is to ensure that the data that has been written is immutable. Based on this core idea, the chained UTXO connects the input and output of different transactions through a hash pointer to ensure the legitimacy of all transactions and realize the traceability of UTXO.

(4) Parallelization

The UTXO model is recognized of being potential scalablity because UTXO allows parallelization of transactions. When a transaction initiator sends two separate transactions, spending an independent UTXO also allows the transaction to be processed in random order. This allows a person to separate funds and have the ability to process transactions in parallel while maintaining privacy. Bitcoin's UTXO model has been running and testing for many years, with great performance and security advantages. VGO, as a forked currency for Bitcoin, uses the UTXO model, which is an inheritance for its underlying technology. VGO is based on the development of the Bitcoin core code and is a more cautious option. UTXO's features of security and parallel trading will also enhance VGO’s efficiency.

3.4 Omni protocol

The Omni protocol is a very complete protocol implementation that takes full advantage of the features of the UTXO model and enables Token management without changing the consensus and protocol. Also, Omni Layer is also adhering to the spirit of the open source movement, using the MIT license, is an important basis for us to achieve unlicensed innovation. VGO distributes USDO stable currency through the Omni protocol.

3.4 Smart Contract Virtual Machine VVM

Through independent virtual machine architecture (VGO Virtual Machine, VVM for short), VGO is able to implement smart contracts. The benefit of implementing smart contracts with VVM is that you can add new functions as needed to run virtual machines with multiple different blockchains. VVM smart contract system supports more programming languages. For now, VGO's development of VVM mainly has two phases of planning. The first phase is compatible with the Ethereum Virtual Machine (EVM). Because EVM is the initial implementation platform for smart contracts, VVM needs to be able to run smart contracts on existing EVMs with code fine-tuning. In the second phase, VGO plans to dynamically adjust the EVM code to bring VGO code closer to native code and support more programming languages.

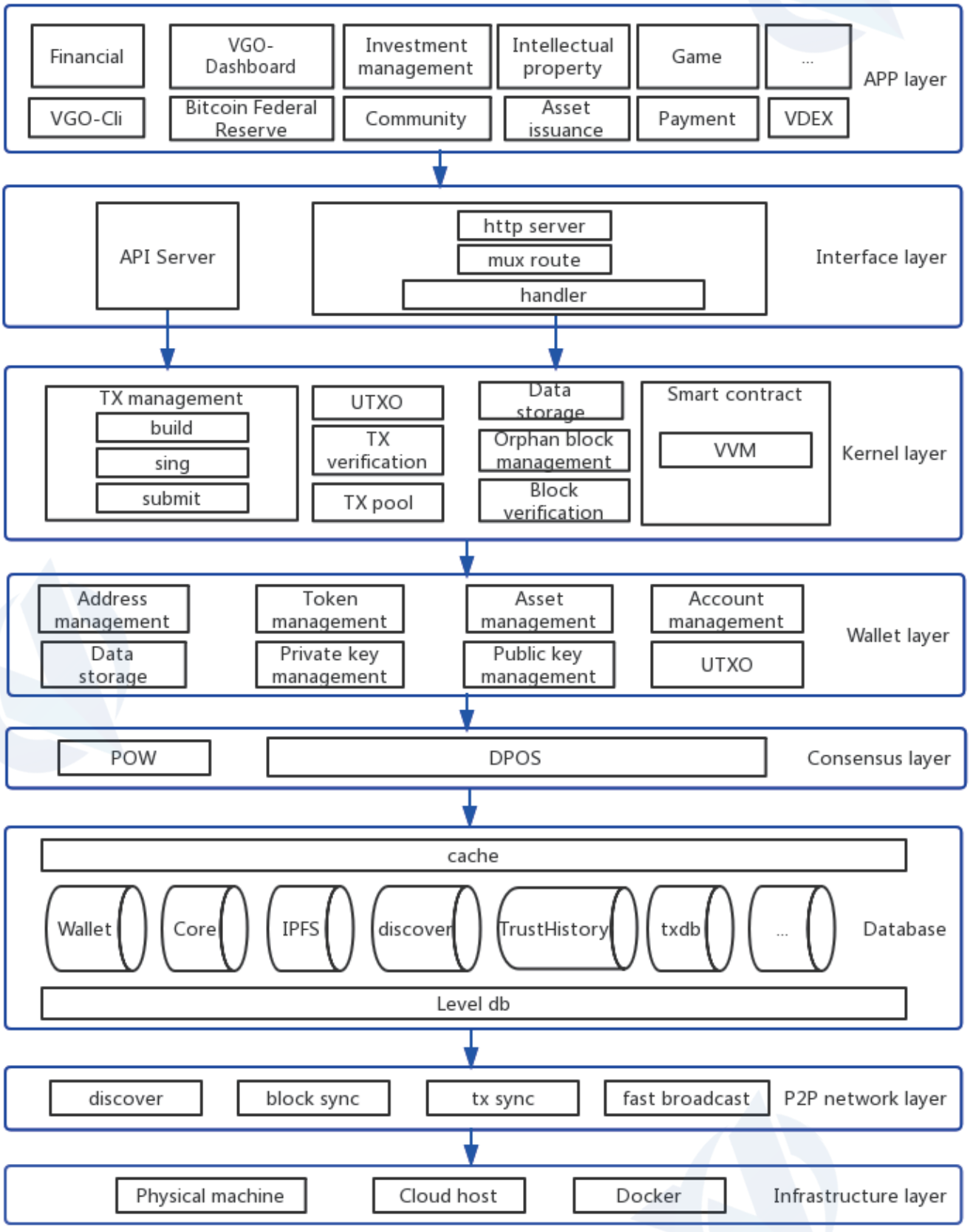
3.5 InterPlanetary File System IPFS

IPFS is based on the principles of Merkle DAG and introduces the concept of "content-based addressing." Use content-based addressing when requesting specific resources, users do not need to specify a location, just specify the requested content, each file has a unique hash value, which can be considered as a fingerprint or identification of the file. If you want to access a specific file, simply request the network for a copy of the file with the specified hash value. After the request is completed, someone on the IPFS network will provide the resources requested by the user. The user will download the resource and save the copy to the user's IPFS cache. When another person comes and requests the same file, the user will be able to provide them via a hash link. IPFS is a peer-to-peer hypermedia protocol that makes the network faster, safer, and more open. It is a global, peer-to-peer distributed file system that attempts to connect all computing devices with the same file together.

The integration of IPFS and blockchain technology seems to be a perfect option. Using IPFS in blockchain transactions, you can place immutable permalinks. Timestamps protect user-uploaded data without actually storing the data content on the chain, reducing blockchain bloat and providing a convenient way to help blockchain extensions for secure off-chain solutions.

VGO will increase support for IPFS. The file sharing platform allows anyone to upload media files supported by the IPFS protocol and the VGO blockchain. Due to IPFS integration, VGO file users can upload files larger than the previous 128m or more, enabling the platform to support various DAPP applications. You can upload a 200MB file to IPFS and save the file's IPFS hash link on VGO. The VGO platform will add file preview support for the uploaded file, such as MP3, WAV, text and image files.

3.6 VGO public chain overall technical architecture



(VGO technical architecture)

The VGO public chain technical architecture is as shown above, from bottom to top, sub-infrastructure, P2P network, database, consensus, wallet, kernel, interface and application. The infrastructure can be physical machines, virtual machines (clouds) and containers; the main functions of the P2P network layer are node discovery, block and transaction synchronization, transaction broadcasting, etc.; the database layer contains a variety of databases for different purposes, the most important one is Core, used to store all the main block information and transaction information; IPFS, IPFS is mainly used for file sharing platform support; wallet database is also included; the consensus layer mainly refers to the DPOS consensus algorithm used by VGO for Bitcoin hard fork; It is efficient and stable. The function of the wallet layer is mainly for public and private key and address management, as well as for account, token management and UTXO maintenance. At the core of the whole VGO, kernel, the most important functions are transaction management, transaction construction, transaction signature and transaction submission, including smart contract and its operating environment VVM; interface layer includes API Server service, which mainly receives requests form application layer. This layer mainly for the developers of the VGO public chain ecosystem; finally we talk about the application layer, the application layer contains two user interaction tools VGO-Cli and VGO-Dashboard, and various DAPP applications.

VGO ecological applications mainly include Bitcoin Federal Reserve, VDEX (decentralized exchange), and other such as investment and wealth management, finance, payment, games, community, asset issuance and intellectual property.

4 Token and main applications

4.1 Token VGO and USDO

4.1.1 VGO token

VGO is the original currency of the VGO public chain. It is a hard forked currency of Bitcoin. The total c irculation of VGO is 2.1 billion, which is exactly 100 times the total amount of Bitcoin. Among them, 17.7 million VGO are provided to Bitcoin holders, distributed by airdrops, 28 million for operating and technical reserves, 75 million for exchanges, the remaining 1.98 billion will be automatically transferred to the community reward pool as a mining reward. Like BTC, VGO is characterized by decentralization, anonymity, used only in the digital world, not belonging to any country or financial institution, and is not restricted by areas, and can be exchanged anywhere in the world. Users can use VGO to purchase some virtual items, such as items in online games. If anyone accepts VGO, users can also use VGO to purchase real-life items. VGO is inherited from BTC. The purpose of VGO is not to replace BTC, but to enhance the credit of BTC, improve the shortcomings of Bitcoin system, and dedicate to realize the practical application of blockchain technology. This includes its revolutionary features that support both real-life uses, also it's global financial and payment systems complement, as well as a programmable economy through smart contracts to create a programmable business community. The VGO economy uses a distributed database of nodes in the entire P2P

network to identify and record all trading behaviors, and uses cryptographic design to ensure the security of all aspects of currency circulation. The decentralization of P2P and the algorithm itself ensure that the currency cannot be manipulated by mass-produced Bitcoins. Cryptographic-based design allows Bitcoin to be transferred or paid only by the real owner, while ensuring the anonymity of currency ownership and circulation transactions.

4.1.2 USDO stable curren-

In order to stabilize and prosper the ecosystem, VGO also launched the USDO (USD Offering) stable currency, the ratio of USDO and USD is 1:1 for the stabilization of the deflation. The distribution mechanism is based on Bitcoin as a credit endorsement. How many Bitcoins there are stored in the platform, will be issued a corresponding proportion of USDO. The platform Bitcoin storage address is disclosed, and anyone can query the address on the platform. The stored Bitcoin value is greater than the issued USDO, and there is no over-issue. The exchange rate without having risk makes it understandable as a variant of the currency, with price fluctuations being almost zero relative to the digital currency.

4.2 VDEX(VGO Decentralized Transaction Platform)

In terms of centralized exchange, all the funds that users use to conduct in the transaction are kept in the same place. Users' funds are stored directly in

the exchange, which is not only responsible for matching the order, but also keeping the current order book and depositor's funds in the correct state. Since all users' private keys are kept together, the exchange system can be hacked and all users lose all funds. The use of decentralization by exchanges can prevent many users' assets from being involved in problems caused by hackers. To this end, VGO launched the VDEEX (VGO Decentralized Transaction Platform), which manages individual token assets and conducts point-to-point token exchanges. When conducting an order under VDEX, the user can specify the transaction object and only allow the specified account to pay for the order. This function is very suitable for the two parties to directly exchange different tokens, to ensure that both parties to the transaction "pay the money in one hand, delivery in one hand."

The USDO can be used as a currency token for VDEX. It can be used as a trading medium to pay the corresponding fee as the digital asset is traded on VDEX, it can be used as a corresponding discount or reward. The VDEX application supports transactions for various digital assets, such as transactions between USDO and VGO, transactions between USDO and BTC, and exchange of various virtual currencies. In the future, the public chain plan supports the exchange between USDO and legal virtual currency, as well as the exchange of many commodities and other physical assets or their corresponding digital assets. We plan to develop an ultra-high performance platform based on the basic technology supported by VDEX for the highest performance and stable P4P technology, supporting high-speed switching and clearing operations.

4.3 BFR(Bitcoin Federal Reserve)

Bitcoin is one of the most successful digital assets based on blockchain technology. With its characteristics of non-tampering and decentralization, Bitcoin achieves high security and is not easily stolen. But because Bitcoin has only a specific key to keep it, it can be said that whoever has this key is equivalent to owning all the Bitcoin assets in the wallet. The stolen events of Bitcoin are also countless. Bitcoin was stolen as early as November 2013 and lost about 4,100 Bitcoins, which was worth about $1.1 million. Later, the sudden disappearance of Bitcoin on the OKcoin exchange in December, the loss reached 640,000 yuan. In February of 2014, the famous "Moutougou" incident broke out. At that time, the world's largest Bitcoin exchange was stolen, and nearly 850,000 Bitcoins were stolen. Some people claimed that this was self-stealing. In March, the US Poloniex Exchange issued a statement that lost about 12.3% of Bitcoin. In May of 2016 years, the Hong Kong digital currency exchange Gatecoin was also attacked by hackers, with losses of up to 2 million US dollars. Besides these stolen Bitcoins, according to Chainalysis, 30% of Bitcoin may have been lost, and this lost Bitcoin cannot be retrieved back anyway. The outbreak of this series of incidents shows that there are huge loopholes in the security of digital assets. How to find a low-cost and efficient solution has become a top priority, and digital asset custody has become a high-demand choice for all parties.

Asset custody services are an indispensable part of modern finance. With the increase of asset and the complexity of asset portfolio, it is increasingly necessary for professionals or organizations to provide services in the frame-work of reducing the operational burden associated with owning assets, there-by keeping the value of the trustee’s assets of the trillions dollar safe. With the rise of digital asset investment, as well as the frequent occurrence of inci-dents such as scam and hack, the demand for digital asset custody services is becoming more and more urgent. With regard to this situation, VGO launched the Bitcoin Federal Reserve (BFR) application, in which users can store their Bitcoin in the Bitcoin Fed by digital asset custody, and the platform will safely store and reward the corresponding proportion of VGO to the users. The digi-tal asset security of the Bitcoin Fed is guaranteed. First, the platform itself will store certain proportion of the Bitcoin. If the user's Bitcoin is lost in the Bitcoin Fed, the platform will compensate with the USDO of the corresponding value.

5 VGO Ecosystem governance

5.1 Problems to be solved in blockchain governance

(1) Problem of negative attitude toward contribution

The attitude for contribution discussed here includes the attitude for development and voting. The attitude is directly related to incentives, especially economic incentives and rights incentives; in the absence of corresponding incentives, attitude issue is difficult to to be resolved. Historically, certain attitude issues have been hidden by the impact of the overall environment in which the industry breaks out; and in the future when blockchain projects are intensifying, this problem is more likely to be broken out on a large scale. The attitude toward contribution is related to the survival of the blockchain project. For example, the issue of conservatization in Bitcoin developers has led to a long-running debate in the Bitcoin community (about expansion, etc.); The attitude toward EOS's voting has caused the EOS main network to be delayed. How reconstruct the incentive mechanism of the blockchain and balance the rights and obligations of the key roles of the system is a crucial issue facing the blockchain project.

(2) Role problem

The problem of role opposition is homologous to the problem of negative attitude toward contribution in a certain sense, and can be attributed to the incentive category.

In the blockchain ecosystem, regular users, developers, miners, and even more complex entrusted rights holders, entrustee rights holders, etc., have strong inequalities in their rights and obligations. For example, in the ecosystem, developers and regular users are often not directly incentivized with reward, and can only obtain income from the rise of token price, but the responsibility on developers' shoulder is far greater than regular users' ; rational governance mechanism cannot be expected that developers only complete their work by interest or responsibility, so developers may choose to fade out of the community or become a regular user.

The above example is a situation in which the powers and responsibilities are not equal, and often does not lead to serious confrontation; if the situation of conflict of interest is taken into account, it is more likely to lead to direct confrontation. For example, in the common POW ecosystem, miners have high transaction fee rates and high token value motives, and users have motives to reduce transaction fee rates and reduce token value (note: users are not necessarily holders of token), two parties will be completely opposite. Historically, there have been many cases in which POW miners maliciously packaged empty transactions and caused network congestion, confirming the logic of conflicts of interest caused by conflicts of roles.

(3)Token liquidity matching problem

The token liquidity matching problem refers to the imbalance in the distribution, locking, and issuance of token in the blockchain ecosystem, which leads to the imbalance of the token value and the lose of the stakeholders. The

The token liquidity matching problem refers to the imbalance in the distribution, locking, and issuance of token in the blockchain ecosystem, which leads to the imbalance of the token value and the lose of the stakeholders. The essence of token's liquidity matching problem is the imbalance between supply and demand. For example, an excessively large number of token issuance system may cause itself inflation and detract from the enthusiasm of early users; the token system with over-locking and mortgage may cause price distortion and insufficient money supply. In the long run, the token system of economic model design and supply-demand relationship adjustment mechanism, especially the system with weak overall balance and extreme policy, is easily countered by its own design.

5.2 VGO governance definition

(1) The core of governance activities: roles

Roles may include: users, entrusted rights holders, entrustee rights holders, developers, etc.

(2) Basic elements of governance: incentives and collaboration mechanisms

·Incentives: Determine the structural foundation and operational drivers that organizations (communities) form.

·Collaboration mechanism: Determine the efficiency of the organization (community) operations.

(3) Specific areas of governance: Consensus, Voter, Voting Area, protocol upgrades and changes

·Consensus: Determining the rights and obligations of participating in bookkeeping and generating block, and determining the distribution of benefits of Block reward are the objective basis for the formation of chain rights and responsibilities.

·Voter: Decide who has the right to participate in and affect governance activities

·Voting Area: Determine the areas involved in governance on the chain, and which matters can be voted on.

·Protocol upgrades and changes: It is how decide the upgrade and change of the protocol, and how the agreement is updated.

5.3 System role definition

(1) Users

Divided into VGO users, VGO built ecological users. In principle, all users with VGO can exercise community governance rights through the VGO platform.

(2) Entrusted right holder

The VGO community is a system controlled and enforced by Token; therefore, the VGO's entrusted rights holder is all VGO holders. VGO holders are the most basic participants in the VGO governance system and the ultimate goal of VGO governance. The way in which holders participate in the VGO governance system is simple, but when many holders participate in governance, their will becomes the ultimate guide to action. The holder can delegate their voting rights to nodes. The holders choose the nodes they trust and have the same concept, and give out their own authority to them. The nodes selected by a large number of holders execute the user's will. Holders can also choose their favorite wallet and mine pool to directly manage their own tokens and get their own income. Holders can delegate their parliamentary authority to the board of directors to participate in the planning of VGO's future development.

(3) Entrustee right holder

The entrustee right holder of the bookkeeping right is the block node; the trustee of the right to discuss is the director. VGO's nodes and directors represent the system's bookkeeping rights and deliberation rights, which are the core of VGO's efficient governance. VGO's nodes and directors conduct elections in different ways, and there is no necessary identity connection between the two.

(4) Developers

Developers are the cornerstone of the VGO ecosystem; VGO will get the rewards of developers into the governance system of the VGO chain, getting it on the protocol level. The VGO system is a code-maintained program in its form. The quality of the code determines the performance of the system. The progress of the code updating determines the speed at which it evolves. Developers are the most important force in maintaining system programs. Program development and maintenance are not required and cannot be done by all members because of the unique technical threshold. So a specific developer team is needed to complete the development and maintenance work, and therefore rewarded — so that the developer's productivity is better motivated.

(5) On-chain Oracle

In the VGO ecosystem, Oracle will be an important role on the chain of gateways and decentralized exchanges. On-chain Oracle belongs to VGO users, but unlike regular users, On-chain Oracle exists in the form of functional roles such as service providers and asset acceptors.

(6) Wallet and mining pool

Wallet and mining pool are applications made by communities or other third parties that allow users to host and use their token. They can use the user's token to campaign for nodes and gain revenue, but the rights itself belongs to the original user. Wallet and the mining pool must return these rights to the

users, and distribute the proceeds to the users and conduct voting according to the user's wishes. Wallet and mining pool helps users achieve their right to vote, and that's it.

(7) VGO DAO fund

The fund is organized by the VGO community leaders and managed by the board of directors to maintain the organization of the VGO system.

5.4 VGO node requirements and election rules

Node is the most important part of the VGO governance system and is a representative who directly participate in VGO governance. The main task of the node is to generate, confirm, and record block information. The loyal node will get the block reward, and the evil node will lose the reward. But to become a node, not only do devices with sufficient performance need to support a node service in order to ensure the accuracy of the block, and also need the support of the majority of token holders.

Nodes are elected by users and represent the users who elect them. Each vote held by node is important when node participating in the VGO chain gov–ernance, but if they violate the purpose of most users, the node will gradually lose his votes and eventually lose the qualification to become a node.

Each node can display its own technology, team, ideas and other information on its own home page to attract token holders to vote. As the most ubiquitous token holders, they have the right to choose the nodes that are qualified in their minds and meet their own demands, and then vote for them. Each token holder can vote for a trusted node, up to 51 nodes, each of which will receive all votes from the token holder. During each cycle, system automatically counts the number of votes and selects the node candidate who obtained the first 101 votes to become the node.

5.5 VGO Council Rules and Regulations

(1) Director and Council

The VGO Council (the Council) institution of the VGO making execution. The Council is responsible for the maintenance and update of the main network protocol parameters and daily community affairs management. The VGO Board of Directors (referred to as the directors) is the personnel who performs the parliamentary functions and handles affairs on behalf of the VGO community, and is also the on-chain role of the VGO protocol in a functional form.t

(2) Principle of separating rights of two definition

The Board of Director is independent of the DPOS bookkeeping node and is not responsible for the accounting and node elections.

(3) Qualification of council

Any VGO address holder can become a node. The Council needs to be certified by KYC as a natural person or organization group with full capacity. The VGO Council initially established with seven; as the community expands, the size of the Council can be appropriately increased, but not less than seven. Because of the special importance and contribution of the Council, the Council not only needs to have sufficient technical standards, but also needs certain community support to understand the status quo and public opinion of the community. So the tentative four of the seven members of the board are selected by the VGO developer community and the other three are elected by the community. The Council are required to hold at least 20,000 VGOs, and the Council can also serve as nodes at the same time.

(4) Election method

The Council selects decision through on-chain. The election is an independent, different DPOS node election activity, held quarterly. Any VGO holder can entrust vote to the Council candidate in the wallet. After the election, the top seven candidates will be officially elected as directors according to the number of entrusted votes. Before the election, the candidates for the Council should officially disclose their information and governance plans on the community platform, and have obtained public support from the community.

(5) Director's functions and powers

1) Determine the variable parameters of the VGO main network;

2) Review and discuss community opinions and developers' cases;

3) Discuss matters related to the update of the main network protocol;

4) Discuss and organize community affairs;

5) Discuss and decide on the current DAO fund allocations and other public funding arrangements;

6) Discuss changes to the terms of the rules involved in the VGO gover-nance system.

(6) Economic incentive

VGO will allocate a specific amount of funds to the Council incentive fund as a financial compensation for directors. (developer reward mechanism, pro-motion of operational activities rewards)

(7) Council decision-making mechanism

The decision of the Council is organized and managed by the directors. In response to the issues discussed by the Council, after all the members voted, the matters passed are formally recognized as Council resolutions, and the VGO Council Resolution No.* with the time of the resolution is disclosed to the community. After the adoption of the resolution of the Council, it will take effect three days after the announcement, unless the resolution triggers a full

vote ofthe community. The internal resolution of the council votes and the voting weight is determined according to the number of VGOs the director is entrusted; however, the weight of a single director must not exceed 40% and must not be less than 10%.

(8) Community full member voting mechanism

The so-called community vote means the Council resolution, requiring all members of the community to vote with VGO, and final democratic resolution based on the results of the vote.

Community full member vote is triggered by a specific situation, not by law. After the Council's resolution is open to the community, members of the community can vote on the resolution in the VGO wallet or project home page as feedback(ie, they can vote for their own to express opposition); if a resolution is approved by VGO's total circulation of more than 1/5 votes against it , it will automatically trigger the community full member vote. The community full member vote is required to exceed more than 67% of the VGOs participating in the voting; the Council resolution that triggered the community full member vote and has not been approved will automatically become invalid.

5.6 VGO DAO fund

The fund is organized by the VGO community leaders and managed by the Council to maintain the organization of the VGO system. Since the development of the entire VGO is more like a public utility, the system upgrade can benefit every participant, but each individual is not willing to pay for it — if

other users can get a free hitchhike, it requires an organization that charges all participants (not directly, but take a portion of the other tokens) to support the upgrade and maintenance of the system. The role of the fund is extremely important throughout governance, but it is not dominant. The fund is just a executor for user rights, helping the system to be maintained evolution.

We will take a portion of the long-term unrecognized VGO pool and release it to the fund in batches. The fund is responsible for rewarding those who contribute to the VGO ecosystem, increasing the contribution of all system participants and making the entire ecosystem a closed loop. The fund belongs to the entire VGO community, with daily tasks managed by the VGO Council and major events being decided by all participants. The fund will be responsible for the following awards for specific reasons:

·Council Awards: Awards for the day-to-day management of the Council.

·Developer rewards: reward developers for all code development or development of new protocols.

·Community Contribution: Reward community member for provided proposal, resource, or other contribution.

·Other rewards.

Before each release to the fund, the foundation will make pre-proposal to determine the number and timing of the release of the token, and the Council will vote and obtain approval to implement the program.

5.7 Self-evolution of the VGO protocol

The VGO protocol is a self-evolving protocol. Based on the current version, all participants jointly make decisions to promote the upgrade. Members of the community can give the Council suggestions, which can be changes to the management system, can be a future development path, or even a simple suggestion. As long as there is an idea, the Council will consider whether it is a good suggestion, whether it is worth upgrading, and then give feedback about the suggestion to the developer community.

6 Vision

Our vision is to create a peer-to-peer digital cash system advocated by Bitcoin White Paper to provide users with convenient, fast and secure services.

Our goals:

Build a strong and responsible community;

Create a high-end currency with a bright future;

Establish a bright prospect for the Bitcoin Federal Reserve to enhance the credit of the BTC;

Create a stable decentralized encrypted digital asset exchange;

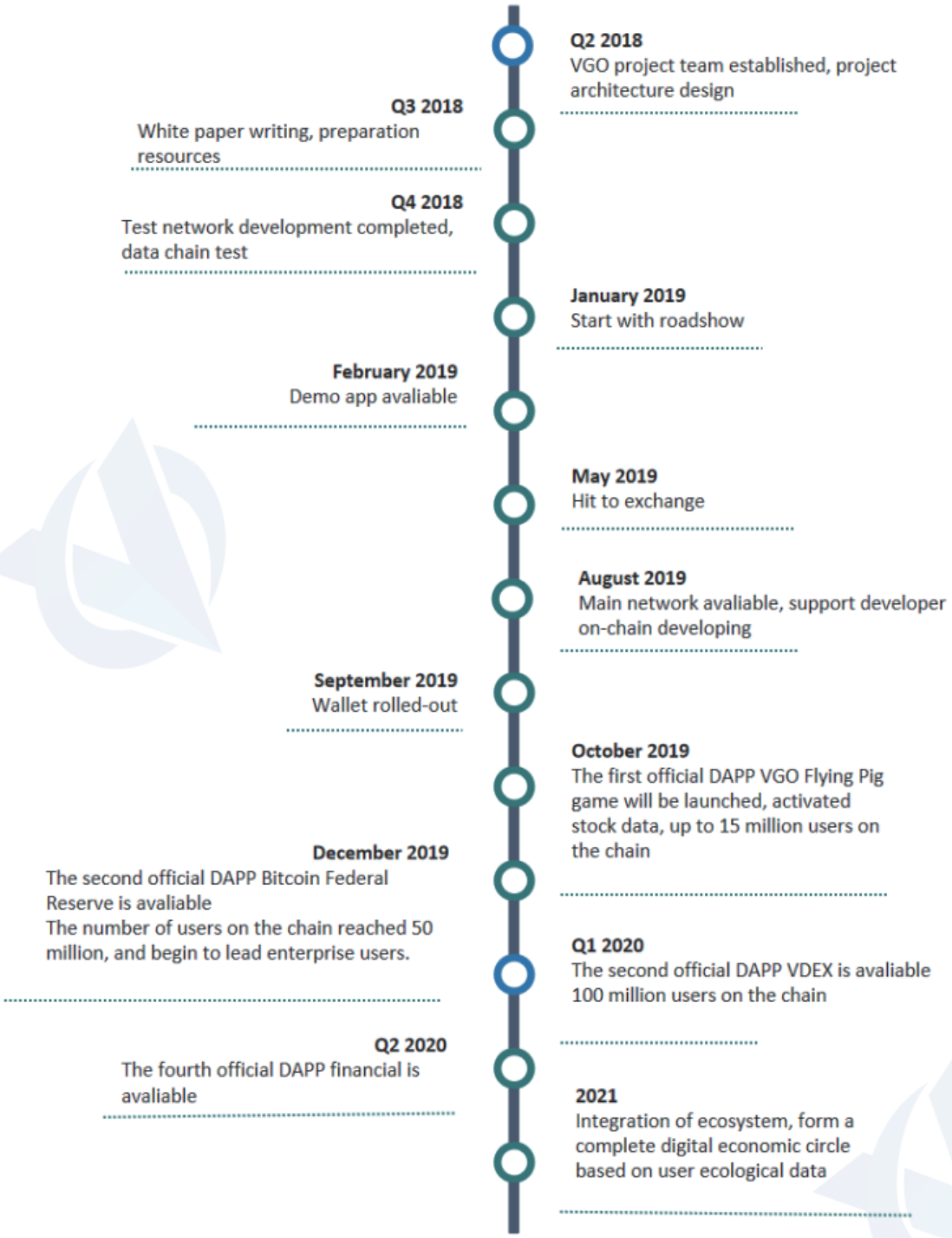
Create an environment that supports cryptocurrencies to avoid future disputes;

Make it widely adopted for open source and decentralization;

Users can be completely anonymous, without having to share their identity for their transactions or holding VGO.

7 Route map

The VGO team has provided clear support for future visions and paths to ensure the network and the users in community. We have planned and developed our road map as a digital currency and a decentralized future.



8 Legal

In the past year, financial authorities in the United States, Singapore, China, Switzerland and Germany have tightened their Encrypted token sales policy and warned because the tokens are increasingly classified as securities. VGO Token Sales recognizes and will comply with safety regulations in several major jurisdictions, and will follow KYC and AML regulations. In detail, this means:

8.1 Securities regulations

Please read this section carefully. If you have any questions about the action you should take, we recommend that you consult your legal, financial, tax or other professional adviser.

The information listed in this document may not be comprehensive and does not represent any element of the contractual relationship. This document does not represent investment, tax, legal, regulatory, financial, accounting or other advice, neither is it the sole reason to participate in the support and development of the VGO ecosystem. Before making a decision, potential buyers must consult their legal, investment, tax accounting, and other advisors to determine the potential benefits, limitations, and other consequences of such transactions.

No part of this document is issued a prospectus or offer that is not intended to be a securities offer or a requirement to invest in securities in any type of jurisdiction. This document has not been prepared in accordance with the laws or regulations of any jurisdiction, which prohibits or in any way restricts transactions relating to digital tokens or any form of their use.

8.2 KYC and AML

Understanding your customer (KYC) and anti-money laundering (AML) regulations are different in different nations, but they all require to check and verify a list of customers based on terrorism, embargoes, and political exposures (PEPs). VGO is now in this process with a professional service provider. In the financing process for the crowd, the category of investor will be checked after the authentication and AML check. If there is still a question, a manual investigation will be conducted. The exchange from encryption to fiat currency will be conducted by a regulated broker/exchange, and the bank will receive KYC and AML reports.

8.3 Company management

Under corporate governance, VGO is being prepared to hire an international accounting firm to evaluate the VGO token module and its processes, audit its accounting, and provide reports on how it follows its guidelines.after the authentication and AML check. If there is still a question, a manual investigation will be conducted. The exchange from encryption to fiat currency will be conducted by a regulated broker/exchange, and the bank will receive KYC and AML reports.

9 FAQ

What is the Blockchain?cy

Blockchain is the simplest form, is also an independent, transparent, secure, and permanent database that coexists in multiple locations and is shared by the community.

The magic of blockchains is that databases are not stored in one place or managed by anyone. Instead, it is called distributed; it exists on multiple computers or nodes, and in the same way that any interested person can maintain a copy of it.

In addition, the verification system provides security to ensure that no one can change the records in the database. Old transactions are permanently retained and new transactions are irreversibly added to the ledger. Anyone on the network can check the ledger and view the same transaction history as everyone else.

What areas does the blockchain involve?

The blockchain involves many fields, including distribution, storage, cryptography, psychology, economics, game theory, and network protocols. From a technical angle, the core technologies in blockchain include: distribution, consensus mechanisms, cryptography, Merkle Tree, smart contracts, and more.

The development of the blockchain?

The development of blockchain is in full swing. Governments, companies and startups all over the world have laid out their plans, lest losing this technology that can change the world economic structure. The World Economic Forum said in a report that technological innovation has drastically transformed the financial services industry over the past 50 years. The blockchain can be regarded as one of the leading technologies to open the next technological revolution. However, no one can predict the future of the blockchain, just as we could not predict the future of the Internet in the early 1990s. But what is certain is that this technology will make a huge impact on the development of the world economy. The blockchain is like the Internet of the year and is at the breaking point of widespread acceptance and application. Blockchain provides a mechanism for information and value transfer in an untrusted environment and is foundation for building a future Internet.

What is cryptocurrency?

Cryptocurrency is a transaction medium that uses cryptography to ensure transaction security and control the creation of trading units. The cryptocurrency is a new type of digital currency and virtual currency that is cryptographically and numerically hashed and tied to a smart contract. Bitcoin became the first decentralized cryptocurrency in 2009, after which the term cryptocurrency refers to this type of design.

What is Bitcoin?

Bitcoin is a consensus network that has led to a new payment system and a fully digital currency. It is the first decentralized peer-to-peer payment network that is controlled by its users without the need for a central authority or intermediary. From the user's point of view, Bitcoin is much like the cash of the Internet. Bitcoin can also be seen as the most outstanding three-entry bookkeeping system.

Who created Bitcoin?

Bitcoin is the first currency to realize the concept of "secret currency". In 1998, Wei Dai first explained the concept of "secret currency" on the cypherpunks mailing list: a cryptographic principle to control the issuance and trading of currency, rather than relying on the new monetary form of the central authority. In 2009, Satoshi Nakamoto (Satoshi Nakamoto alias) published the first Bitcoin specification and proof of concept on the cryptography mailing list. At the end of 2010, Nakamoto took the project and did not reveal much about his identity. Since then, many developers have worked on Bitcoin projects, and the Bitcoin community has grown rapidly. Nakamoto's anonymous identity often causes unfounded concerns, many of which are related to the misunderstanding of Bitcoin's open source features. Bitcoin's protocols and software are publicly open, and any developer around the world can view the code or develop their own modified Bitcoin software version. Like current developers, Nakamoto's influence is limited to the changes he has made that others have ad

opted. Therefore, Nakamoto does not control Bitcoin. Well, today, the identity issue of the inventor of Bitcoin may be the same as the identity of the paper inventor.

Who is controlling the Bitcoin network?

No one owns the Bitcoin network, just like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin holders around the world. Developers can improve the software, but they can't force changes to the rules of the Bitcoin protocol because all users are free to choose the software they want to use. In order to maintain compatibility with each other, all users also need to choose software that follows the same rules. Bitcoin can only work properly if all users reach a consensus. Therefore, all users and developers are very motivated to accept and protect this consensus.

How does Bitcoin work?

From the user's point of view, Bitcoin is a mobile phone application or computer program that provides a personal Bitcoin wallet that users can use to pay for and receive Bitcoin. This is how Bitcoin works for most users. Behind the scenes, the entire Bitcoin network shares a common ledger called a "blockchain." This general ledger contains every transaction processed so that the user's computer can verify the validity of each transaction. The authenticity of each transaction is protected by the digital signature corresponding to the sending address, which gives the user full control over the Bitcoin that is

transferred from their own Bitcoin address. In addition, anyone can take advantage of the computing power of specialized hardware to process transactions and receive Bitcoin rewards for this purpose. This service is often referred to as "mining." You can check out the dedicated pages and original papers to learn more about Bitcoin.

Is anyone really using Bitcoin?

Yes, more and more businesses and individuals are using bitcoin. This includes both traditional businesses like restaurant, accommodation and law firm, as well as popular online services like Namecheap, Overstock.com, and Reddit. Although Bitcoin is still a relatively new concept, it is growing rapidly. At the end of August 2013, the total value of Bitcoin in circulation exceeded $1.5 billion, and millions of dollars worth of Bitcoin were exchanged every day.

Are there other cryptocurrencies?

Bitcoin is the largest and most frequently used cryptocurrency. As of January 7, 2020, there were 1,384 cryptocurrencies on the Internet.

What is the government’s attitude towards cryptocurrency?

At the most extreme level, both China and South Korea ban the financing of cyptocurrency in their own markets. As far as China is concerned, the first round of cryptocurrency financing and the nature of decentralized cryptocurrency undermines the degree of regulation to the domestic economy in all as

pects from central government and the relatively high proportion of fraudulent activities in China. On the other hand, in Russia, the Moscow Stock Exchange is developing infrastructure to allow legitimate transactions in cryptocurrency, while in Estonia, the government is considering the construction of cryptocurrency economy for its own currency.

During this period, many other regulators have taken a more wait-and-see attitude:

●In Singapore, MAS makes cryptocurrency as assets. Although transactions are not regulated, both KYC and anti-money laundering are monitored.

●The Swiss Financial Market Regulatory Authority has classified cryptocurrency as an asset, but the company does not require specific licenses or approvals to operate.

●In the United States, the US Securities and Exchange Commission has decided that cryptocurrency financing should be subject to federal and state laws if token-sell is considered as securities-sell, although they are considering more flexible legislation.

What are the positive factors of cryptocurrency?

●Provide opportunities for promising projects with no other ready–made funds or any widely accessible platform.

●As a decentralized currency, cryptocurrency avoids the intermediary of controlling the flow of money and the costs associated with transactions within that currency.

●Avoid unnecessary paperwork over time through other, most of which have no real value.

10 Disclaimer

Please read the full content of this Notice and Disclaimer section carefully. No legal, financial, commercial or tax advice is required here, and you should consult with your own legal, financial, tax or other professional adviser before participating in any activity related to this.

The white paper is for general information purposes only and does not constitute a prospectus, an offer document, a securities offer, an investment invitation or an offer for any product, item or asset (whether digital or other). The information herein may not be exhaustive and does not imply any element of the contractual relationship. The accuracy or completeness of this information cannot be guaranteed and the accuracy or completeness of this information is not guaranteed or claimed. If the white paper contains information obtained from third-party sources; the foundation, the distributor, and/or the VGO team have not independently verified the accuracy or completion of this information. In addition, the white paper may be updated with the development of the project or a text file related to it.

Nothing in this white paper shall constitute a foundation, distributor or team selling any offer of USDO or VGO (as defined herein), nor shall it form a basis on or any part of it or its stated facts, or rely on any contract or investment decisions. Nothing contained in this white paper or on this website may or may be a commitment, representation or commitment to the future perfor

1mance of the VGO Platform. For any sale or purchase of VGO or USDO, the agreement between the distributor and you is only subject to the separate terms and conditions of the agreement.

By reading the white paper or the website (or any part thereof), you represent and warrant to the foundation, distributors, its affiliates and the VGO team as follows:

(a) In any decision to purchase any VGO or USDO, you are not relying on the white paper or any statement on this website;

(b) You will, at your own expense, ensure that you comply with all applicable laws, regulatory requirements and restrictions (as the case may be);

(c) You acknowledge that understanding and agreeing that VGO and USDO may have no value, VGO or USDO does not guarantee or represent value or liquidity, VGO and USDO are not used for speculative investments;

(d) Foundations, distributors, affiliates and/or VGO team members are not responsible or liable for the value of VGO or USDO, the transferability and/or liquidity and/or availability of VGO or USDO, through third parties or other means in any market of VGO or USDO; and

(e) If you are a citizen, national, resident (tax or other), household registration and/or green card holder of any regions or countries, you acknowledge, understand and agree that you are not eligible to purchase any VGO or USDO (i)VGO or USDO sale may be interpreted as selling securities (no matter how

named), financial services or investment products and/or (ii) applicable laws, laws prohibiting participation in token sales, regulations, treaties or administrative law (including but not limited to the United States of America, Canada) , New Zealand, the People's Republic of China (but not including the special administrative regions of Hong Kong and Macao, as well as the territory of Taiwan), the Republic of Korea and the Socialist Republic of Vietnam).

Distributors that issue and sell VGO or USDO should be affiliates of the foundation. All contributions will be used to promote, facilitate research, design and develop the blockchain-based platform that will connect global gold buyers/holders and industry users to create reliable and limited supply of gold tokens. Those digital assets represent the right to acquire physical gold, thereby creating a reliable and transparent universal value exchange platform for all users based on the oldest physical products (gold) and cutting-edge future technologies (blockchain technology). Foundations, distributors and their affiliates will develop, manage and operate the VGO and USDO platform.

The foundation, distributors and VGO team do not and will not make any representations, warranties or promises to any entity or individual and will make no statements (including but not limited to their accuracy, completeness, timeliness or reliability). The content of the white paper or website, or any other material published by the foundation or distributor). To the fullest extent permitted by law, foundation, distributors, affiliates and service providers are not liable for any indirect, special, incidental, consequential or other damages of any type of infringement, contract or otherwise (including but not limited on

any liability, loss of income, income or loss of profits, use or loss of data, etc. resulting from the use of the white paper or this website or any other published material. Or its content (including but not limited to any errors or omissions) or other generated content. Potential purchasers of VGO or USDO should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with VGO or USDO token sales, foundations, distributors and VGO teams.

The information listed in the white papers and on the website is for community discussion only and is not legally binding. No person should draw up any contractual or binding legal commitment to acquire VGO or USDO and must not accept any virtual currency or other payment method on the basis of a white paper or website. The VGO or USDO sale and purchase agreement and/or an agreement to continue to hold a VGO or USDO must be governed by a separate set of terms and conditions or a token purchase agreement (as the case may be) and must provide for such purchase terms and / or continue hold VGO or USDO (Terms and Conditions) and these terms should be provided separately or on the website. If there are any inconsistencies between the terms and conditions and the white paper or the website, the terms and conditions will prevail.

No regulatory institution reviews or approves any information listed in the white paper or website. Such actions will not or will be taken in accordance with the law, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of a white paper or website does not imply compliance with applicable laws, regulatory requirements or rules.

The information presented here is conceptual only and describes the future development goals of the VGO platform to be developed. White papers or websites may be modified or replaced from time to time. There is no obligation to update the white paper or website, or to provide recipients with access to any information provided here.

All statements contained herein, statements in press releases or any place accessible to the public and any oral representations made by foundations, distributors and/or VGO teams may constitute forward-looking statements (including statements regarding intentions, beliefs or current expectations of market conditions, business strategies and plans, financial conditions, specific regulations and risk management practices. Please do not rely too much on these forward-looking statements as they involve known and unknown risks, uncertainties and other future actual results are materially different from those described in such forward-looking statements, and the reasonableness of not reviewing any such statements or assumptions by an independent third party. These forward-looking statements are only for the dates set forth in the white paper, and the Foundation, the Distributor, and the VGO Team expressly disclaim any liability (whether express or implied) for any revisions to these forward-looking statements that reflect events after that date.

The use of any company and/or platform name or trademark (other than those relating to foundations, distributors or their affiliates) herein does not imply any association or endorsement with any third party. References to specific companies and platforms in white papers or websites are for illustrative purposes only.

The white paper and this website may be translated into languages other than Chinese. If there is a conflict or ambiguity between the Chinese version and the translated version of the white paper, the Chinese version shall prevail. You acknowledge that you have read and understood the white and Chinese versions.

The white paper or any part of this website must not be reproduced, copied, distributed or transmitted in any way without the prior written consent of the foundation or the distributor.

11 References

[1] Maymounkov, P. and Mazieres, D. (2002). Kademlia：a peer-to-peer information system based on the XOR metric, International Workshop on Peer-to-Peer Systems, 53-65.

[2] Naor, M. and Rothblum, G. N. (2009). The Complexity of Online Memory Checking. Journal of the ACM (JACM), 56(1).

[3] Back, Adam, et al. "Enabling blockchain innovations with pegged side-chains." URL：http：//www.opensciencereview.com/papers/123/enabling-blockchain-innovations-with-pegged- sidechains (2014).

[4] Bentov, I., Gabizon, A. and Mizrahi, A. (2016). Crytocurrencies without Proof of Work. International Conference on Financial Cryptography and Data Security.142-157.

[5] Kshemkalyani A D, Singhal M. Distributed computing：principles, algorithms, and systems[M]. Cambridge University Press, 2011.

[6] 朱立，《详解最近大热的闪电网络、雷电网络和 CORDA》，2016 年 6 月 12 日，http：//www.8btc.com/ln-rn-corda

[7] 马龙，《柔支付：基于 2-of-2 多重签名实现的类闪电支付》，2016 年 11 月 6 日，http：//idgui.com/RouPay.com

[8] Vitalik Buterin，翻译 He1l_Q，《中本聪的天才：比特币以意想不到的方式躲开了一些密码学子弹》，2013 年 10 月 28 日，http：//www.8btc.com/satosh-is-genius-unexpected-ways-in-which-Bitcoin-dodged-some-cryptographic-bullet

[9] Bandara, H. M. N. D. and Jayasumana, A. P. (2012). Collaborative Applications over Peer-to-Peer Systems Challenges and Solutions. Peer-to-Peer Networking and Applications. arXiv：1207.0790.

[10] 中本聪，《比特币：一种点对点的电子现金系统》，2008 年 11 月 1 日，http：//www.8btc.com/wiki/Bitcoin-a-peer-to-peer-electronic-cash-system

[11] LBTC White Paper (English Version)，2019 年 4 月 17，https：//lbtc.io/web/viewer.html