Lightning Bitcoin (LBTC)
Whitepaper

1 Overview

Lightning Bitcoin (LBTC) is a fully decentralized Internet-of-value protocol for global payments. The specific realizations of LBTC cover such fields as peer-to-peer transactions and decentralized digital asset exchanges. Any user who works on the LBTC protocol can be assured to conduct instant and secure transactions almost free of charge.

LBTC aims at addressing related problems such as miner centralization, network congestion, and low efficiency of transaction processing in Bitcoin operation. It comes into being as a blockchain based on DPoS (Delegated Proof of Stake) consensus mechanism after the Lightning team hard-forked the Bitcoin. It has now become an essential part of the Bitcoin experiment as a whole.

By running on DPoS consensus mechanism which is featured by high block generation rate as well as efficient and robust operation performance, LBTC enables extremely fast transaction confirmation. “As fast as lightning” shows how LBTC received its name. LBTC is now the world’s most efficient and promising forked version of Bitcoin protocol. With strong network throughput, LBTC provides quality support for instant peer-to-peer payments, decentralized trading platforms, smart contracts, on-chain Oracle and governance.

2 Fork Methodology

2.1 A Peer-to-Peer Electronic Cash System

In the end of 2008, Nakamoto pointed out in the white paper Bitcoin: A Peer-to-Peer Electronic Cash System that Bitcoin is a peer-to-peer electronic cash system that does not rely on any central financial institutions.

The so-called “electronic cash”, put in the terms of current business, is a way of payment or payment system. But unlike the common third-party payment system, Bitcoin defines payment without going through a center or an intermediary. Besides, Bitcoin is itself also a kind of currency products. Whether we define Bitcoin as currency or not, its property of being so always remains unquestioned, which attributes to Bitcoin embedded values.

Prior to the current version of the Bitcoin, the pioneers of the Cypherpunk Movement had tried several efforts with this regard, but all failed in the end. The essence of Nakamoto’s solution is that he first ensured the technical feasibility of the decentralized P2P network, and then established a robust and long-term sustainable economic system. Numerous precedents have demonstrated that without decentralization, any attempt at establishing an electronic cash system will ultimately be hit back by the challenge of centralization.

Based on the asymmetric encryption system and the hash function, the Bitcoin has built a robust anti-crack system, making the inverse structuring of the data on Bitcoin blockchain computationally impossible. The P2P network of Bitcoin has been applied for a long time, but Nakamoto by creatively using the asymmetric encryption and the trap-door feature of the hash function had established a series of sophisticated mechanisms including a cryptographic structure relying on the private-public-address pattern, the hash pointers between blocks, and the verifiable transaction scripts for digital signature. All these make those efforts in destroying a Bitcoin database far greater than those in building the database.

The wits of the designers are reflected in the miner reward mechanism, that is, relying on the miners to provide the computing power for building a wall that Bitcoin trusts. Then, the fundamental indicator - ‘trust’ for any global electronic cash system is created from scratch by irreversible coagulation of powers. In a sense, building a strong and constantly growing trust is at the heart of the Bitcoin protocol design.

2.2 Fork Methodology of LBTC

LBTC became a branch version of Bitcoin after a hard fork on the original Bitcoin protocol was initiated. Therefore, LBTC can be considered as an interpretation of the Bitcoin protocol and should also be regarded as a landing solution for the peer-to-peer electronic cash system.

Bitcoin fork, broadly speaking refers to the topological splitting of the Bitcoin blockchain, forming a coexistence of two chains in a short period of time. But under the Bitcoin consensus mechanism, the whole blockchain will ultimately return to the consensus state of one unique chain. The narrowly defined Bitcoin fork generally refers to a kind of hard fork caused by the man-made changes on the protocol. The splitting based on the shared consensus causes the Bitcoin network to operate in multiple sets of different groups while forming a number of independent blockchain protocols.

Bitcoin has to date a number of forked protocol versions running successfully. These different versions of the protocol have proposed varied solutions for the defects or limitations of Bitcoin. Among these many forked versions, LBTC first proposed the UTXO-based DPoS consensus mechanism globally and achieved long-term and stable main network operation after having solved a series of technical problems.

LBTC believes that a true peer-to-peer payment system needs to meet the following conditions:

1) The capacity of adequate information throughput and transaction processing speed should be possessed in order to deal with high-frequency small-amount transactions.

2) The cost in supporting the payment system should be sufficiently low, much lower than the overall benefits the system can generate to society.

3) An economic system that enables the payment system to operate steadily in long-tern senses should be designed and appropriate players introduced to support those system functions with expansible potential and to balance their interests.

4) There should be feasible ways to realize self-updating of the protocol, enabling the system to keep developing and adding new features constantly to adapt itself to the might changing environment.

Methodology on LBTC fork:

1) LBTC respects and recognizes the value of the original Bitcoin protocol and has reused the data generated by it and drawn on some of its design ideas.

2) LBTC hopes to realize the original vision of the Bitcoin peer-to-peer cash payment system, and establish a technically feasible, globally shared system by transforming the existing Bitcoin protocol.

3) On the basis of the peer-to-peer cash payment system, the protocol is required to load some economic activities, which is simple, safe and available to everyone.

4) The above improvements and innovations LBTC made in the Bitcoin protocol must not only fundamentally address the technical and economic problems in building a peer-to-peer cash system, but also should introduce as many as possible those proven developed technologies and models to ensure the stability, user acceptability, and long-term sustainability of the system.

In order to strike a balance between ensuring sufficient information throughput and controlling costs in operation, LBTC has introduced an efficient DPoS consensus mechanism and addressed the incompatibility between the underlying UTXO model of Bitcoin and the DPoS account system, making it the only Bitcoin fork protocol that uses DPoS consensus mechanism and has successfully tackled UTXO+DPoS problems technically. The DPoS consensus mechanism enables LBTC to finish block generation within 3 seconds with an irreversible block design, which not only provides technical support for peer-to-peer payments, but also makes fully possible such complex on-chain functions as built-in dApp, on-chain governance, and smart contracts.

Besides, in view of the requirements for the protocol to be infused with maintainability, sustainability as well as constant and creative problem-solving ability, LBTC has built an on-chain governance philosophy with its own characteristics and introduced the SGS on-chain governance system that balances itself between democracy and efficiency. The system has encouraged the community participation and promoted the response of the participants. This mechanism helps the system quickly update and evolve itself upon any changes from outside environments.

With regard to the needs of complex system roles in accordance with the protocol functions in the economic model, the on-chain governance system and DEX system of LBTC have introduced some economic action roles such as nodes, committees for governance sharing, transaction gateways and acceptance gateways. The separation of the two rights, namely accounting rights and governing rights, has been realized in its power structure, marking as a creative step in the democratic on-chain governance.

2.3 The Deviation of Bitcoin from Its Original Design

Although Bitcoin was initially designed to ensure the technical feasibility of a decentralized and peer-to-peer electronic cash system, this does not mean that its actual development is fully in line with this original intention outlined in the white paper. Bitcoin however has exposed many of the ills of the peer-to-peer electronic cash system and positioned itself towards a Store of Value under market influence.

As mentioned earlier, a true peer-to-peer payment system should meet the following requirements:

1) The capacity of adequate information throughput and transaction processing speed should be possessed in order to deal with high frequency small transactions.

2) The cost in supporting the payment system should be sufficiently low, much lower than the overall benefits the system can generate to society.

3) An economic system that enables the payment system to operate steadily in long-tern senses should be designed and appropriate players introduced to support those system functions with expansible potential and to balance their interests.

4) There should be feasible ways to realize self-updating of the protocol, enabling the system to keep developing and adding new features constantly to adapt itself to the might changing environment.

While the first problem faced by Bitcoin is the transaction throughput and transaction confirmation time caused by low information throughput. This problem essentially is brought about by the POW mechanism of Bitcoin, the design of block size (2M) and block time (about 10 minutes). The block size and block time are determined on the basis of ensuring the extent of network decentralization under the POW framework, which cannot be improved by simple parameter adjustments. Lightning network though provides a solution for off-chain scaling, it is still controversial and is not an overhaul solution (causing centralization and intermediation). In addition, any other Bitcoin fork protocol based on the POW mechanism simply split the computing power of POW and further divide the valuable resources needed for trust construction, let alone to solve this problem on a real basis.

The second problem facing Bitcoin is the huge consumption of resources by the POW mechanism. The long-term operation of POW can indeed build a valuable trust moat, but it can never support a peer-to-peer electronic cash system at a low cost. This makes Bitcoin have to reposition itself under the influence of the market by whatever actively or passively embarking on a path to online Store of Value to transform itself into an electronic version of gold. We here don't comment too much on this route of development. But it is at least certain that the Bitcoin has deviated from its original intention of establishing a global peer-to-peer cash system.

The third problem lies in that although Bitcoin has built a mining system that seems to run sustainably, the mining system is but too simple at a low level for peer-to-peer payment system that tends to be more practical and functionally complex. Moreover, it is generally believed that the interests of miners, users and developers cannot be well coordinated under the POW mechanism proven by mathematical and economic principles. The Bitcoin system cannot provide a well-functioned solution that enables complex on-chain roles (such as gateways) to generate incomes while balancing the interests of all parties at the same time. Nor can it separate accounting rights from governing rights, thus hindering the Bitcoin in adapting to complex economic activities.

Further, the governance mechanism of Bitcoin relies on the most primitive off-chain mode which is featured by serious internal consumption and cannot achieve rapid responses. This has become a so well-known problem that once even affected the survival of Bitcoin. Moreover, the way Bitcoin follows has made its development team extremely conservative about the changes and upgrades of the protocol, which makes Bitcoin unsuitable for being a peer-to-peer electronic cash system.

To summarize, all the current features of the Bitcoin (POW, longer block time, smaller block size, unitary mining economic system, and conservation toward protocol changes) make it more suitable for its position at present of a Store of Value and electronic gold. However, this at the same time has deviated it from its original design of the peer-to-peer electronic cash system.

2.4 LBTC Fork Information

- Fork Time：December 18, 2017；
- Fork Block Height：499999；
- Consensus Mechanism: UTXO-based DPoS;
- Block Generation Interval: 3 seconds (fixed), able be adjusted dynamically;
- Irreversible Block Mechanism;
- Block Size: 2M, able be adjusted dynamically;
- Does not support Seg Wit;
- Added Replay Protection;
- Support CPU Mining;
- Able to expand Smart Contracts;

3 Technological Architecture of LBTC

	BTC	LBTC	BCH	BTG	BCD	B2X	SBTC	BCHC	BTX
Fork Time	—	2017.12.18	2017.8.1	2017.10.25	2017. 11 (End)	2017.11.16	2017.12.17(Test)	2017.8.1	2017.4.24 (Non-Forked)
Circulation	21 million	7,265,926	21 million	21 million	21 million	21 million	21.21 million	21 million	21 million
Distribution Mode	Mining	Mining	Mining &. Fork	Mining &. Fork	Mining &. Fork（40 million expected）	Mining &. Fork	Mining &. Fork（210,000 expected）	Mining &. Fork	Mining, Airdrop & Snapshot Claim
Consensus Mechanism	PoW	DPoS	PoW	PoW	PoW	PoW	Unknown	PoW	PoW
Algorithm	SHA256	—	SHA256	Equlhash	Optimized x13	Unknown	Unknown	SHA256	Timetravel 10
Mining Equipment	ASIC	CPU	ASIC	GPU	GPU	GPU	Unknown	ASIC	GPU
Block Size	1M (2-4M)	2M	8M (8M)	1M (2-4M)	8M (8M)	2M (4 - 8M)	8M (8M)	8M (8M)	20M
Block Interval	10 minutes	3 seconds	10 minutes	10 minutes	10 minutes	10 minutes	Unknown	10 minutes	2.5 minutes
Difficulty Adjustment	2 weeks	—	DAA	EDA	2 weeks	DAA	Unknown	EDA	Diff64_J5
SegWit	Support	Not Support	Not Support	Support	Support	Support	Unknown	Not Support	Support
Serious Err Prevention	—	Support	Support	Support	Support	Support	Support	Support	—-
Other Features	—	SGS On-Chain Governance, Decentralized Exchanges	—	Unique Address Format	Transaction Amount Encryption	—	Smart Contract, Lightning Network, Knowledge Proof, Remove Dynamic, Checkpoint Protection	—	—
Team	Bitcoin Core	Lightning Team	BitcoinABC, Bitcoin Unlimited, BitcoinXT, etc.	Bitcoin Gold	Evey Team, 007 Team	BitcoinX Team	Super Bitcoin	Team Unknown, whose introduction on official website was plagiarized from BCH.	Bitcore

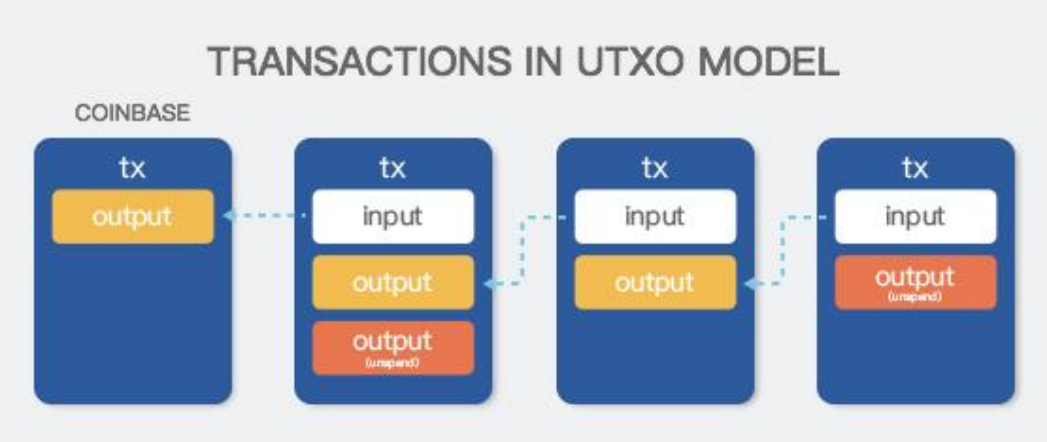
3.1 LBTC as an Internet-of-Value Protocol

LBTC is an Internet of Value Protocol. 'Value' here refers to the value expression, transmission, credit construction, and economic and financial activities based on these. It may include a series of applications with realistic functions and social benefits such as transferring remittance, fiat currency-cryptocurrency exchange, issuing and trading of credit endorsements, decentralized exchanges, as well as trading and acceptance of online gateways.

The core in the design of the LBTC protocol is to ensure that LBTC has sufficient capacity to act as a carrier system for global Internet value transmission by selecting an appropriate technical infrastructure. The LBTC protocol is the basic framework for achieving value transmission, that is, the parent of all on-chain economic actions. Therefore, we set high the requirements for the technical architecture and every internal detail of LBTC, and creatively established the UTXO-based DPoS consensus mechanism.

Further, we designed the such items as irreversible block mode, timestamp consensus and Cache middleware to balance the performance and reliability of this combination, creating a protocol version that is closer to the original intention of the peer-to-peer cash payment system proposed by Bitcoin.

3.2 UTXO Model: The Most Secure Way for Accounting



At the data level, LBTC follows the UTXO model adopted by Bitcoin as the architecture of the blockchain ledger. UTXO is the abbreviation of Unspent Transaction Output. It is the first technical solution suggested by Nakamoto in the design of the data structure of Bitcoin transaction. It is also a highly innovative concept of data structure brought by Bitcoin protocol to the whole world.

Here is how UTXO presented in the database of the Bitcoin protocol: first, it is confirmed that a few transfer transactions flowed to User A on the chain. Plus, A has not spent the assets specified by these transactions. Then all the protocol participants will recognize that A is the holder of these assets.

Compared with the UTXO model, it is easier for the average to understand the Account Model. The Account Model refers to the ID that keeps the account, the marking of the owner and the balance of the assets of the account in the database. When transfer transaction occurs, the balance of these accounts will be adjusted accordingly to form a new account-balance mapping relationship.

In the UTXO model, the balance of an account is not stored as a number but is calculated using the sum of the occupied UTXOs. In other words, UTXO does not carry an account-balance mapping relationship, it is just a faithful record of all historical transactions, simple but very robust.

UTXO is featured by following strengths:

UTXO Reliability

In a block structure, previousblockhash and merkleroot are the two most important fields, both of which prevent the transaction information from being tampered. The core of the UTXO model is to ensure that the data which has been written is immutable. Based on this 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 as well.

UTXO One-time-ness

Each transaction in the UTXO model consists of multiple transaction inputs, which are in nature UTXO + signatures. There are only two states for each Transaction Output, namely those have been spent and not spent yet. This ensures that each UTXO can only be spent only once and is hence highly resistant to double-spend attacks.

UTXO Invisibility

Compared with the Account Model, UTXO is more private. As previously outlined, each UTXO is only “one-time”. If the user changes an address for each transaction, it will be difficult to find the correlation between two addresses, which guarantees the invisibility of the transaction. If there is a need to further improve this invisibility, you can also consider such technical means as ring signature and a mixed use of trading elements.

UTXO Parallelization

The UTXO Model is commonly recognized as potentially scalable since UTXO allows parallelization of transactions. When a transaction sender sends two separate transactions, UTXO which separates each spending will also allow these transactions to be processed in any order. This can actually separate one’s spending and at the same time demonstrate the ability of processing transactions in parallel while ensuring privacy.

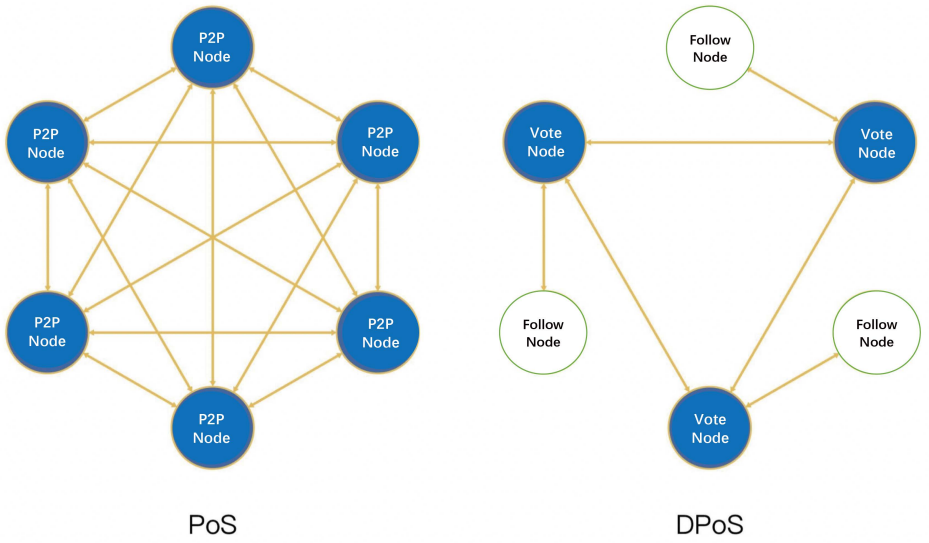
Having been running and tested for many years, the performance and security of Bitcoin UTXO model have both been proven ideal and satisfying. For LBTC, an alternative version to Bitcoin protocol, adopting the UTXO model is also an inheritance of Bitcoin's underlying technology. It is also a more prudent choice for LBTC to develop on the basis of the core code of Bitcoin. The security and parallel trading feasibility of UTXO will also add to LBTC a higher efficiency.

3.3 DPoS Infrastructure: The Most Efficient Consensus Mechanism

In the consensus protocol, LBTC adopted the Delegated Proof of Stake (DPoS). Based on POW and POS, DPoS is a new type of consensus algorithm for ensuring both the security and efficiency for a blockchain network. It can not only solve the problem of serious energy consumption caused by POW in the mining process, but also can avoid the occurrence of 'Trust Imbalance' that may occur under POS distribution of stakes. Therefore, DPoS can become a representative of the Consensus Mechanism 3.0.

Now, we briefly explain the DPoS consensus mechanism. The principle is to first let each token holder vote and select a certain number of holders as representatives, which can be understood as a certain number of representative nodes. Then, these representative nodes will complete transaction verification and block generation in a certain period of time. Token holders can change these representatives at any time by voting to maintain the "long-term purity" of the chain system and ensure that the protocol is fully decentralized.

DPoS is to date the fastest, most effective, most decentralized, and most flexible consensus model among all current consensuses. It runs by the power of stakeholders approving votes to resolve consensus issues in a fair and democratic manner. All network parameters, from relatively simple transaction fee criteria, block time and block parameters to more complex chain governance rules, can be adjusted by designated representatives.



PoS VS. DPos

The DPoS consensus mechanism has the following advantages:

Excellent Performance:

Faster confirmation speed: In the case of LBTC, the block time is fixed at 3 seconds. One transaction (after 6-10 confirmations) takes about 1 minute, and the complete block generation procedure takes only 5 minutes. Irreversible blocks can be then generated every 1-2 procedures. By contrast, taking Bitcoin as an example, it takes about 10 minutes to generate a block in the POW mechanism, and at least 1 hour to confirm a transaction waiting for 6 confirmations.

Low Power-Consumption:

The DPoS mechanism while reducing the number of nodes changes the relationship among nodes from competition to cooperation, avoiding unnecessary loss caused by the competition of computing power and mutual attacks. Under the premise of ensuring network security, the power consumption of the entire network is further reduced and the cost for running network is the set at the lowest.

Efficient Governance:

Developers can implement any changes they deem appropriate as long as they are approved by the stakeholders. This policy not only protects developers, but also protects stakeholders and ensures that no one is unilaterally controlling the blockchain network or getting the blockchain network out of control. The hard forks have replaced 51% of witnesses, so the more stakeholders involved, the more elected witnesses there are, and the higher the robustness of the entire system will be.

Outstanding Robustness:

Throughout the process, anyone can monitor the running of the network by observing the witness participation rate. If the witness participation is below a certain level at some point, all on-chain user can be given more time for transaction confirmation, and they will also be prompted to stay highly vigilant about their network environment. Also, users will be informed that there may be potential problems on the blockchain network within minutes after the problem is detected.The DPoS mechanism was first applied by BM in the BTS project. BM's other star projects STEEM and EOS have also followed this consensus mechanism. Since its inception, DPoS has been always with excellent performance, high efficiency, and outstanding flexibility. The practice of many other projects has also proved these sparkling features of DPoS.

3.4 UTXO+DPoS: An Amazing Combination

Many people may misunderstand that DPoS is only suitable for account models and cannot be used for UTXO ones. In fact, UTXO model is a mechanism where historical transactions get orgainzed and stored on the blockchain. DPoS, on the other hand, is a consensus algorithm that makes network participants reach agreements on transaction data in distributed ledgers. UTXO and DPoS are not mutually exclusive and have no correlation either.

The combination of UTXO and DPoS will in fact show many added advantages.

Better Performance:

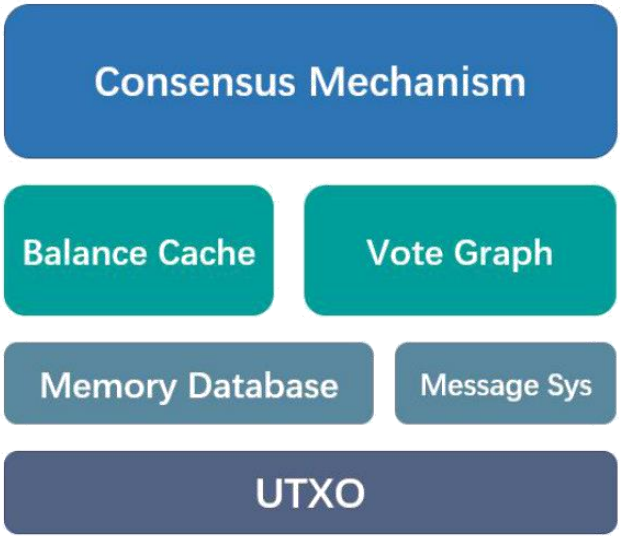
Given the fact that UTXO enables separation as well as potential parallelism, LBTC has been given excellent performance coupled with the support of DPoS. According to actual operation experience, LBTC can meet the 2800TPS operation requirements.

Higher Security:

In DPoS infrastructure, nodes will finish block generation in the given order within short time intervals. If we use the account model, the database will swell very quickly, and there may be many problems when the instant database synchronization is faced with network anomalies. With the UTXO model, however, not only the size of the database can be maintained, but also a forging table can be generated according to a specific algorithm. The forging period table forging table calculated by the whole network nodes according to the shared data is consistent, and it is at this time that the whole network nodes reach a consensus. When cases such as downtime and network partition happen, the whole network will automatically switch to the longest chain as the body chain according to the principle of “transaction submission” to ensure consistency.

Timestamp Consensus:

A big difficulty in combining UTXO with DPoS is the timestamp. The DPoS consensus is based on time and will strictly check the time serial of blocks. The time of the whole node system therefore must be set in line with the standard time, otherwise there will be problems with consensus consistency. Though UTXO itself also records timestamps, the timestamps are not based on standard time. The timestamps are unified into a standard time protocol in the LBTC to ensure the operation of blocks. When blocks that are identified evil or not synchronous appear, they will be treated as abnormal ones and be addressed accordingly.



Data Snapshots and Voting:

In the UTXO model adopted by Bitcoin, address balance querying is not supported. In Bitcoin, address balance is calculated in real time by only thoroughly scanning UTXO data. The efforts put in the calculation are quite huge measured by hour, which is not feasible. However, Bitcoin does not adopt the DPoS consensus and therefore does not require such functions as node registration and voting.

While in the LBTC system, new functions such as address balance calculation, node registration and node voting are added for the needs of the DPoS algorithm. Considering the requirements for high performance of the consensus algorithm and the limited number of registered nodes, information about the address balance, node registration and voting is stored in the memory. When exiting the program, the data will be written back to the disk. The process of how the information of UTXO accounting and DPoS consensus mechanism are linked through database, address balance and the information of voting:

- The information of registration and voting is transmitted by the Bitcoin underlying protocol.
- The information of registration and voting is stored in the memory database.
- The DPoS consensus Model checks the information and completes the consensus.

4 LBTC On-Chain Governance

4.1 The Connotation and Implication

4.1.1 Blockchain: A Living Self-Evolving System

Since a nine-page white paper presented by Nakamoto in 2009 and after the implication of the initial code version, the Bitcoin protocol has been continuously improved and updated over the past 10 years and has formed a huge network of protocols that consume more than 1% of the world's power with market value of more than 300 billion US dollars.

It is worth noting that if we consider that Nakamoto has only provided a design of initial protocol version, then it's safe to say that Bitcoin is but an impact free from any centralized leadership and structure, which brings profound changes to the real world.

The whole blockchain project is widely accepted as a new form of social experiment. It essentially tries to answer the question whether the decentralized social organization model can converge the wisdom and strength of the groups and communities and whether this model can show strong vitality and adaptability in respond to the changing environment. This means that the blockchain projects should not just be seen as sort of loose social organization structure but should be considered a life-like system with vitality, adaptability and self-evolving ability.

In the long run of life evolution, single-cell prokaryotes first formed the extremely rich species after sporadic mutation and natural selection, and finally evolved into the high-level multi-cellular vertebrates.

The miracle of natural evolution fully demonstrates that though the original design of life is important, and that accurate design can solve many problems efficiently, the ability of living entities to continuously evolve and adapt themselves to environmental changes is the key basis for the continued prosperity of life in the long run. The ability of self-evolution to adapt to the environment is actually the one that responds to those never-occurred stimulus or adjusts to a wider range of changes. All these require us to abandon the stereotyped model and design with evolutionary ideas.

4.1.2 Governance as the Institutional Basis for the Self-Evolution of Blockchain

The essence of the blockchain protocol lies in the combination of network protocols, transaction protocols, and consensus protocols.

- Network protocols: discover and disseminate transactions;
- Transaction protocols: define a valid transaction;
- Consensus protocols: define and form a unique chain.

The consensus protocol is the soul of the whole blockchain protocol since it clearly defines how the seemingly loose decentralized organization forms the basis of opinions and that of rights and obligations.

The governance of the blockchain serves as the real basis and institutional guarantee for forming and maintaining consensus protocols. Meanwhile, governance also provides lines of ideas for all parties to reach consensus. Some areas covered by governance may include:

- Changing existing protocols;
- Tracing the records of blockchain changes;
- Distributing benefits and subsidies;
- Any other related matters.

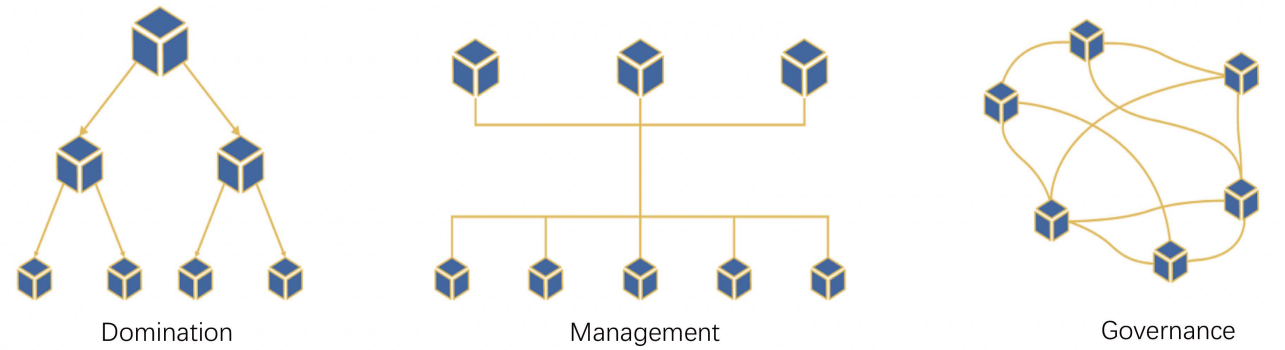
It can be seen that the fundamental purpose of blockchain governance is to ensure the formation, maintenance and continuous evolution of consensus protocols. Therefore, it's safe to say that the blockchain governance provides an institutional basis for the self-evolution of blockchain from the top-level design.

In addition, with the blockchain as a great attempt to decentralize an organization, the governance of the blockchain may also likely to become the exemplar of the most advanced group action in the history of human civilization. A group system can integrate into itself the evolution of individuals. Moreover, given the fact that blockchain governance is a multi-participant system, it is in nature highly robust and can therefore withstand many unforeseen risks.

4.1.3 Management, Domination and Governance

To understand the connotation of blockchain governance, we should distinguish the concepts of management, domination and governance, and make clear that governance is different from both domination and management.

	Management	Domination	Governance
Claims	The manager coordinates the activities of those being managed to gain effects or economic benefits that otherwise cannot be achieved by the individuals.	The upper level of an organization uses its authority to manage the lower-level members in a one-way manner.	By guiding, controlling, and regulating activities within an organization to maximize the all public interests within the organization.
Running Direction	one-way from manager to the managed	one-way and top-down	two-way and interactive
Running Basis and Action	• Emphasis on gaining greater organizational effectiveness, that is, the sum of the individual value becomes larger after management; • Primarily coordinating the relationship between the people and motivate their initiative.	• Developing and implementing policies to form one-way management for public affairs within the organization.	• Cooperation based on market principles and public interests; • Emphasis on the common goals within the organization.



As clearly outlined, what lies behind management, domination and governance is the relationship represented by the requirement of productivity to production, and economic foundation to the superstructure. If we believe that blockchain technology has revolutionized our production relations, then the chain governance is also an innovation of traditional governance.

Blockchain is a decentralized technology model, and chain governance is also a decentralized governance model. The fundamental logic of this concept is that freedom and rights are the source of creativity and the power of order maintenance. Although managers of a centralized system can to some extent help protect the rights of some individuals, they are rather weaker in face of the damage and erosion on individual rights and freedoms caused by such centralized system.

The on-chain governance is also a bottom-up concept. There is no pre-designed direction and mode of operation. Each participant takes actions according to their own choices, and the whole system will move toward as all participants wish. In such an order, every rational individual follows the direction of maximizing his/her own interests. The decision-making of the entire system does not rely on the preferences of any centralized manager but is based on the fundamental requirements of maximizing the interests of the most. Under this circumstance, those public issues concerning the majority are promoted, and those only matter a few people become less focused. That's how individual freedom and rationality are used to promote the development of the whole system.

4.1.4 Governance Defined by LBTC

The core of governance: Roles

Roles may include: users, trustees, delegators, developers, etc.

The basic elements of governance: Incentives and Cooperation Mechanics:

Incentives: determining the structural foundation and operational drivers for the running of organizations or communities;

Cooperation Mechanics: determining the efficiency of running organizations or communities.

Domains of governance: Consensus, Voter, Voting Area, protocol upgrades and changes:

Consensus: deciding rights and obligations in accounting and block generation and determining the distribution of Block reward benefits. It is regarded as the objective basis for on-chain rights and responsibilities;

Voter: deciding who has the right to participate in and influence the governance;

Voting Area: determining the areas involved in governance;

Protocol upgrades and changes: the decision making for upgrades and changes of the protocol and the way it can be updated.

4.1.5 Governance Development: from Off-Chain to On-Chain

The development of blockchain governance has generally experienced a process from the off-chain to on-chain. With the governance moving on chain, the previous internal roles of the blockchain system also gets somewhat blurred.

In the following, combined with the concept of governance proposed by LBTC, an overview and development of a few representative projects will be briefed at the governance level.

1) Bitcoin

The roles in the Bitcoin ecosystem can be divided into: miners, users and developers. Miners receive all economic incentives (from Block Reward and transaction fees) and hold the voting rights for upgrades. There is no direct economic incentive for developers and users.

The setting of this incentive system can explain theoretically the roots of the community conflicts that have appeared in the history of Bitcoin and reveal another hidden danger with lower significance. The incentive system of Bitcoin determines that the following phenomena will inevitably occur: 1. The economic interests and voting rights will be monopolized by miners, which will centralize the system; 2. Developers having no direct economic incentives will tend to be conservative by staying in small groups and are vulnerable to excessive intervention by third-party profit organizations. 3. The absolute advantages of overall miner rights will lead to the splitting of miner- and-user relationship.

From the perspective of incentives, though the mechanism of the Bitcoin protocol is relatively primitive, it is somewhat robust for Bitcoin. The positioning of Bitcoin has shifted from a peer-to-peer payment network to a Store of Value, so the conservative tendency in the development is acceptable or even beneficial. This is a unique feature of Bitcoin and cannot be applied in other projects.

2) Ethereum

Since Ethereum is at present mainly based on POW, its incentive mechanism and roles of system are similar to those of Bitcoin. However, Ethereum has its own unique features in the following two aspects: 1. Ethereum has a community leader (Vitalik Buterin), which leads to better cohesiveness and higher efficiency in the running of the community, but it at the same time is faced with the risk of excessive bundling; 2. Ethereum may in the future turn to POS, which will to some extent alleviate the problem of mining centralization and role confrontation.

3) TEZOS

Tezos is a project proposed earlier to practice the on-chain governance. In the coordination mechanics, Bitcoin and Ethereum are both of off-chain type: Bitcoin developers puts forward the BIPs offline, and Ethereum collects protocol upgrading proposals on GitHub, both of which transfer the governance off chain. However, Tezos emphasizes that the governance process should be formulized and that the testing of new developers' proposal and main chain integration be decided through on-chain voting.

The essence of this mechanism is that the governance power is separated from the small groups of developers and miners to be dispersed to each user while guaranteeing the real developers to have economic incentives to promote protocol upgrades. Therefore, it avoids the issue of developers being over conservative.

4.1.6 To-Be-Solved Issues in Blockchain Governance

1) Issue of negative contribution:

The contribution initiative discussed here includes the initiative for both development and voting. Initiative is directly related to incentives, especially to economic and power related ones. In the absence of corresponding incentives, initiative issues are highly probable and very difficult to resolve. Historically, some initiative issues have been overshadowed by the psychological impact of the overall environment the industry hastened. In the future when the competition of blockchain projects are intensifying, this problem is very likely to erupt on a large scale.

The contribution initiative is the key to the survival of the blockchain project. For instance, the issue of Bitcoin developers being over conservative has led to a long-running debate in the Bitcoin community on expansion. The issue of voting initiative has caused the main network of EOS to be delayed. How to 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) Issue of role confrontation:

The issue of role confrontation shares the same roots with the negative contribution in that they can be both attributed to incentive, the important governance element.

In the blockchain ecology, the rights and obligations of ordinary users, developers, miners, and even more complicated trustees as well as delegators show strong asymmetry. For instance, developers and ordinary users often do not enjoy direct economic incentives in a regular ecology and can only gain income from the rise of Token prices, but the responsibility developers take is far greater than that of ordinary users. Rational governance mechanisms cannot rely on developers to complete the development only out of interest or responsibility, so developers may choose to fade out of the community or just 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 role confrontation. If the conflict of interests is considered, it is more likely to lead to direct confrontation. For instance, in the POW ecosystem, miners have the motivation to increase the transaction fee rate and the Token value, while users tend to reduce the transaction fee rate and the Token value (The user may not necessarily be the holder of the coin). The two are completely at opposite position. There have been many cases before in which POW miners maliciously packaged empty transactions and caused network congestion, which confirmed the fact that conflicts of interest will cause confrontation among roles.

3) Issue of fluctuated Token Supply-Demand Matching:

The issue of fluctuated Token matching refers to the fluctuation of Token value and the stakeholders' loss caused by the imbalance of the distribution, locking, and issuance of Token in the blockchain ecosystem. The essence of Token fluctuated matching is actually the imbalance between supply and demand.

For instance, a Token system with excessive issuance may cause inflation in the system and lower the initiative of early users. A system with Token over-locking and mortgaged may cause price distortion and insufficient money supply. In the long run, Token systems with problematic economic model and supply-demand adjustment mechanism, especially those with weak overall balance and extreme policy, are easily to be ruined by their own design.

4.2 The LBTC On-chain Governance System

4.2.1 LBTC Governance: The Separation of Accounting Rights and Governing Rights

As a decentralized system based on DPoS, LBTC adopts the organizational principle of "Delegate" in the maintenance of the main network and the protocol. Delegate refers to the process in which a right holder delegates his or her rights to agents by entrusting or authorizing them to exercise. The DPoS adopted by the LBTC is a kind of consensus mechanism where accounting owner of the main network entrusts and designates the accounting rights to a number of trustees as many as shareholders by voting.

Such agent mechanisms are not uncommon in the governance structures of organizations that have emerged today or in history. In fact, the agency mechanism expands the actions of different right holders in the organization and forms a more efficient model for action governance. For example, voters in a jurisdiction delegate the voting rights to the representatives, and then the representatives vote on behalf of the voters to decide on some important policies that matter the interests of the voters. In a blockchain system, there may also be such delegate action somewhere.

But it is important to note that the rights delegate of the blockchain system can be summarized as follows according to the different rights:

1) Delegate of Accounting Rights;

2) Delegate of Governing Rights.

In the blockchain system, the accounting rights and the governing rights may exist at the same time, and the two rights show certain technological independence. For instance, in the Bitcoin system, the accounting rights are obtained after an open competition on the POW, and the governing rights are decided by the miner voting. The early blockchain project represented by Bitcoin has shown apparent overlap of the two rights, and this is likely to lead the system to centralization and leave it on sidelines, making it difficult for ordinary users and community members to obtain the rights that correspond to their economic interests. In those relatively fully-fledged governance mechanisms, the accounting rights and the governing rights (hereafter referred to as the two rights) have been separated, which improves the efficiency and feasibility for the roles of the system to participate in governance.

LBTC has for the first time proposed the concept of "Two Rights Separation" in governance. The LBTC team believes that:

1) In a more complex blockchain system, an appropriate degree of separation of the two rights is necessary.
2) The rights delegate mechanism should be designed separately in different rights areas to achieve the appropriate degree of right separation.

Separation of rights is an inevitable choice given the complexity of the blockchain system and the variation of roles. The root cause lies in the ability and qualifications required for the negotiation are very different from those required in accounting. The protocol often constrains and prevents the ill manners of accounting right holders by Staking (also mortgage), positive or reverse incentives. In the negotiation, however, the community must fully consider the trustee's public foundation, the willingness and the ability to govern. Therefore, the two are indeed not at the same level. If they are simply mixed, it will inevitably lead to invalid negotiation.

4.2.2 LBTC Governance: Representative Democracy and Direct Democracy

In The Social Contact, Rousseau believes that an ideal society should be based on the contractual relationship between people and an ideal government governance should be based on the fact that the being ruled recognize rights of the ruling class. Therefore, the real social governance should be decided entirely by the will of its members, and these public wills should benefit the whole society.

However, Rousseau did not propose a practical plan to construct the real institutional basis of an ideal social governance, leaving it staying at the mind level. Direct democracy is primitive and idealistic, and its efficiency and fairness are largely influenced by how institutional designers designate the units for achieving democracy. For instance, if the principle of "one person, one vote" is adopted in the extremely primitive direct democracy system, the individual will be defined as the basic unit for achieving democracy. The same goes for the blockchain system of POS that defines Token as the basic unit for democracy realization.

Previous experience has proven that no matter how the unit of democracy realization is defined, direct democracy can hardly overcome its inherent defects of inefficiency. The larger the network of governance, the more obvious this inefficiency will tend to be. Therefore, for blockchain network protocols that require good scalability, direct democracy may become a constraint for efficient on-chain governance.

Representative democracy is a well-developed governance mechanism in modern times, which reflects a good balance between fairness and efficiency. Representative system requires its members to transfer power to those who are capable and able to represent their will, so these members actually excise their ultimate control over the system in an indirect way. Under representative democracy, elections naturally become the key action in system power distributions. This is also the reason why the DPOS-based blockchain system should give enough weight to the design of the election mechanism.

	Direct Democracy	Representative Democracy
Core	Governance is the embodiment of the public will.	The people transfer the rights of governance to those who are capable and able to represent their will, and hence achieve indirect control.
Realization of Democracy	The definition of realization units.	Election and voting rules.
Features	Fair, simple, direct, and universal.	High efficiency and reasonable division of working structure

As a Bitcoin protocol based on DPoS, LBTC needs to really weigh the efficiency of representative democracy as well as the fairness and universality of direct democracy. LBTC adopts a two-layer governance structure combining Council governance and community governance while having a sophisticated communication feedback mechanism between the two governance levels, enabling the Council and the community to focus on matters they are capable of dealing. Under this mixed governance mechanism, the allocation and communication of power becomes more flexible and efficient.

4.2.3 Roles of the System

• Users:

Users can be divided into LBTC users and users for building LBTC ecology. In principle, all users holding LBTC can exercise community governance rights through LBTC.

• Trustees:

The trustee of accounting rights is the node. The trustee of governing rights is the Council.

The node and LBTC Council respectively represent the accounting and governing rights of the system, which is the core of LBTC's efficient governance.

The node and LBTC Council are elected in different ways, and there is no necessary identity correlation between the two.

• Delegators:

The LBTC community is a system controlled and enforced by Token. Therefore, the trustees are the holder of all LBTCs. These LBTC holders are the most fundamental and widespread participants in the LBTC governance system and also the ultimate goal of the governance. The method by which holders participate in the LBTC governance system is quite simple, but when many holders participate in governance, their willingness will become the ultimate guide of the governance.

The holders can delegate their voting rights to the node. The holders choose the nodes they trust and share the same idea with and hand their authority to them. By such, the nodes selected by a large number of holders will exercise users' will. Holders can also choose wallet and mining pool they prefer to directly manage their own tokens and receive their income. They can delegate their governing power to the members of the Council to indirectly participate in the planning of LBTC's future development.

• Developers:

Developers are the cornerstone of the LBTC ecosystem. LBTC will incorporate the rewards for developers into the LBTC chain governance system, directly up to the protocol level. The LBTC system basically is a program supported by codes. The quality of the code determines the performance of the system, and speed of the code update determines how fast it evolves. Because of the technical ability requirements, the development and maintenance of programs should not and cannot be done by all members. Therefore, a developer team is needed to complete the work and get according rewards. This can indeed better motivate the working efficiency of developers.

• On-chain Oracle:

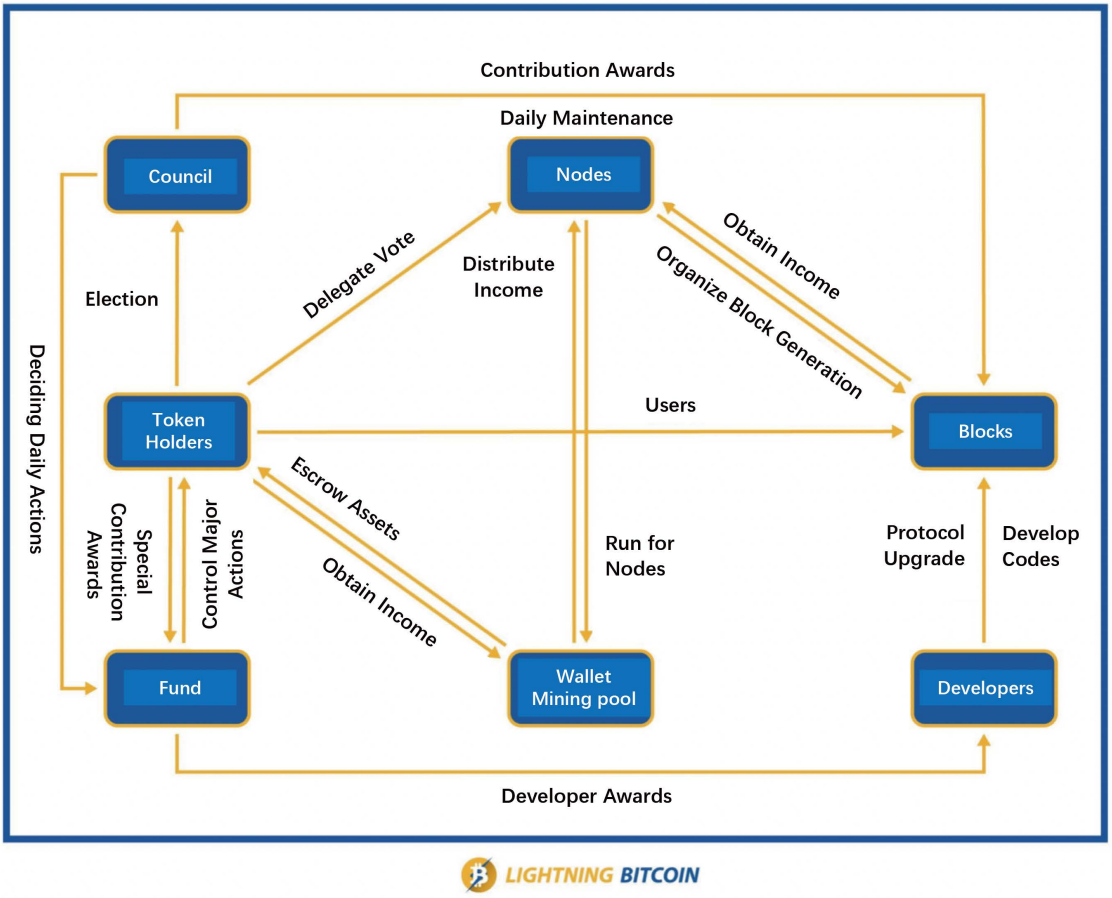
In the LBTC ecosystem, the on-chain Oracle will become an important role in the on-chain gateways and decentralized exchanges. It is also an LBTC user on the chain, but unlike ordinary users, Oracle will exist in the form of functional roles such as service providers and asset acceptors.

• Wallets and Mining pools:

Wallets and mining pools are the applications designed by the community or other third parties that allow users to use or hold their tokens in escrow. They can utilize users' tokens to vie for nodes and gain income, but these rights themselves belong to the original users. Thus, the wallets and the mining pools must return these rights to the users and distribute part of the income to the them as well. They have to conduct voting as users wish. Wallets and mining pools hence just help users achieve their right to vote.

• LBTC DAO Fund:

The fund is an organization organized by the LBTC community leaders and managed by the Council to maintain the LBTC system development.



4.2.4 Node Requirements and Election Rules

The node is the most crucial part of the LBTC governance system and is the agent directly involved in the governance. The main tasks of the node include to generate, confirm, and record block information. Those loyal nodes will get according block rewards while those evil ones will lose the rewards. But to become a node not only requires a device with good supporting performance to ensure the accuracy of the block generation, but also needs to gain support from the majority of token holders.

Nodes are elected by users and represent them. Nodes can cast an important vote when participating in the LBTC governance, but if they violate the opinions of most users, they will gradually lose votes and eventually become not qualified.

Each node can display the information on its own technology, team and ideas on its own home page to attract token holders to vote for it. The ubiquitous token holders have the right to choose nodes that they think are qualified and meet their demands, and then vote for them. Each token holder can vote for up to 51 trusted nodes, each of which will receive all votes from the token holder. The system automatically counts the number of votes periodically and selects first 101 ranking votes to become the nodes elected.

4.2.5 Rules and Regulations of LBTC Council

1) Definition of the Council and its Members

The LBTC Council (hereafter Council) is a designated institute responsible for the negotiation of LBTC community. The Council is responsible for the maintenance and update of the parameters of the main network protocol and the management of daily community affairs.

The members of the Council are the personnel performing the negotiation and handling related affairs on behalf of the LBTC community. They are also the functional roles on the chain officially formularized by the LBTC protocol.

2) The Separation of Two Powers

The Council is independent of the DPoS accounting nodes and is not responsible for the accounting and node elections.

3) Member Qualifications

Any LBTC address holder can become a node.

Candidates need to get certified by KYC as a natural person or organization group with full capacity.

The LBTC Council initially set five places for its members. As the community expands, the number of the places can be appropriately increased, but not less than five. Because of the special importance and contribution of the Council, members are not only required to have sufficient technical background, but also certain community support to understand the status quo and public opinion of the community. Therefore, three of the five members of the Council are recommended by the given LBTC developer community, and the rest two are elected within ordinary communities. The members are required to hold at least 20,000 LBTCs, and they can also serve as nodes at the same time.

4) Way of Election

The membership is decided through an on-chain election. The election is independent and different from DPoS node election and is held quarterly.

Any LBTC holder can entrust a ballot to candidates in the wallet. After the election, the top five ballot-wining candidates will officially become members.

Before the election, the candidates for the council supported by the community should officially publicize their information and governance proposal on the community platform.

5) The Functions and Powers of the Members

1) Determining the variable parameters of the LBTC main network;
2) Reviewing and discussing proposals from community opinions and developers;
3) Discussing matters related to the update of the main network protocol;
4) Discussing and organizing community affairs;
5) Discussing and deciding on the current DAO Fund allocations and other public funds;
6) Discussing changes to the rules and regulations involved in the LBTC governance system.

6) Economic Incentives

The LBTC will allocate a specific sum of funds to the Council as a bonus for the Council members.
(Developer Reward Mechanism, Rewards for Promotion and Operation)

7) Council Decision-Making Mechanism

The decisions of the Council are compiled into units of resolutions organized and managed by the Council.

The unanimously approved issues by the Council, after being voted by the members, will be formally recognized as Council resolutions, and be publicly displayed as the title No.* LBTC Council Resolution together with resolution time to the community.

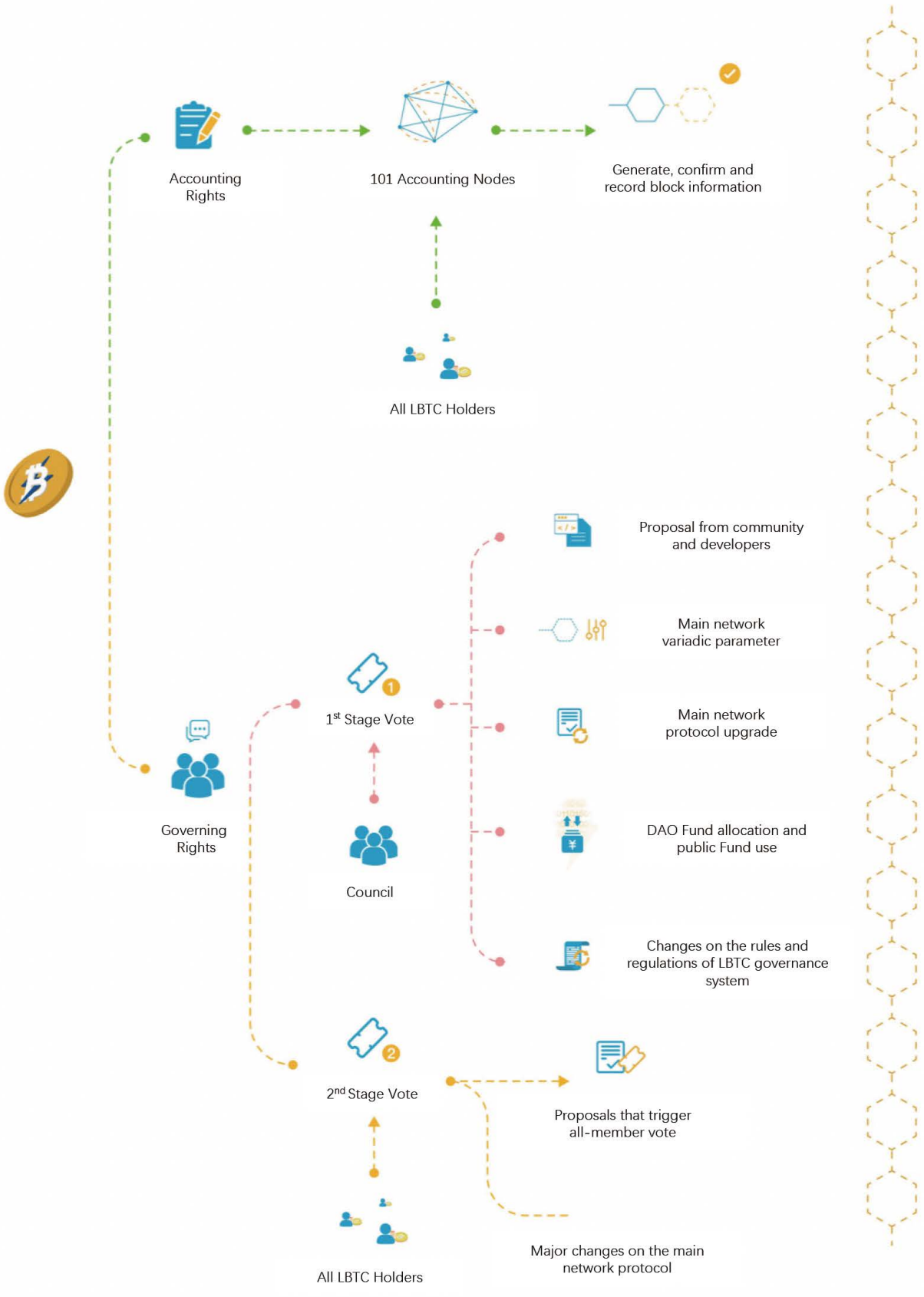
After the adoption of the resolution by the Council, principally it will take effect in three days after the display, unless the it triggers a full vote of within the community.

The internal resolution vote of the Council is decided according to the number of LBTCs the members are entrusted. But the weight of an individual member must not exceed 40% and not less than 10%.

8) All-Member Voting Mechanism of Community

The all-member community vote refers to all members of a community being required to vote on the resolutions approved by the Council through LBTCs, and the final resolution will be decided on the results of the vote.

The all-member community 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 LBTC wallet or project homepage (They can also vote against it using their own LBTC). If a resolution is opposed by more than 1/5 votes of the total LBTC circulation, it will automatically trigger the community to vote. Moreover, the all-member community vote is supposed to be supported by more than 67% of the LBTCs participating in the vote. The Council resolution that triggered the all-member community vote and has not been passed will automatically become invalid.


Accounting Rights
101 Accounting Nodes
Generate, confirm and record block information
All LBTC Holders
Governing Rights
1st Stage Vote
Council
Proposal from community and developers
Main network variadic parameter
Main network protocol upgrade
DAO Fund allocation and public Fund use
Changes on the rules and regulations of LBTC governance system
2nd Stage Vote
Proposals that trigger all-member vote
All LBTC Holders
Major changes on the main network protocol

4.2.6 LBTC DAO Fund

This fund is organized by the LBTC community leaders and managed by the Council to maintain the development of the LBTC system. Since the development of the entire LBTC is more like a public utility, the system upgrades can therefore benefit every participant. But each individual is reluctant to pay for it - if some other users can take free-rides. This requires an organization that charges all participants (not directly, but a portion from other tokens) to support the upgrade and maintenance of the system. The role of the fund is extremely crucial in the overall governance, which is however not dominant. The fund is also but a delegate of user rights, helping the entire system to maintain evolution.

We will take some of the long-term unrecognized rights from the LBTC pool and release them to the Fund in portions. The Fund is responsible for rewarding those who contribute to the LBTC ecosystem, increasing the contribution of all system participants and making the entire ecosystem a closed loop. The Fund belongs to the entire LBTC community, and its daily tasks are managed by the LBTC Council. The major issues related to the Fund are determined by all participants. The Fund will be responsible for the following awards issuing:

- Council Awards: awards for the day-to-day management by the Council;
- Developer Awards: awards for recognizing developers' efforts in upgrade and production of protocols;
- Community Contribution Awards: awards for recognizing proposals, resources or other contributions from community members;
- Other rewards.

Before each release is conducted, the Fund will first launch a proposal to determine the amount and time of the token release. The Council will vote on it and implement the program after being approved.

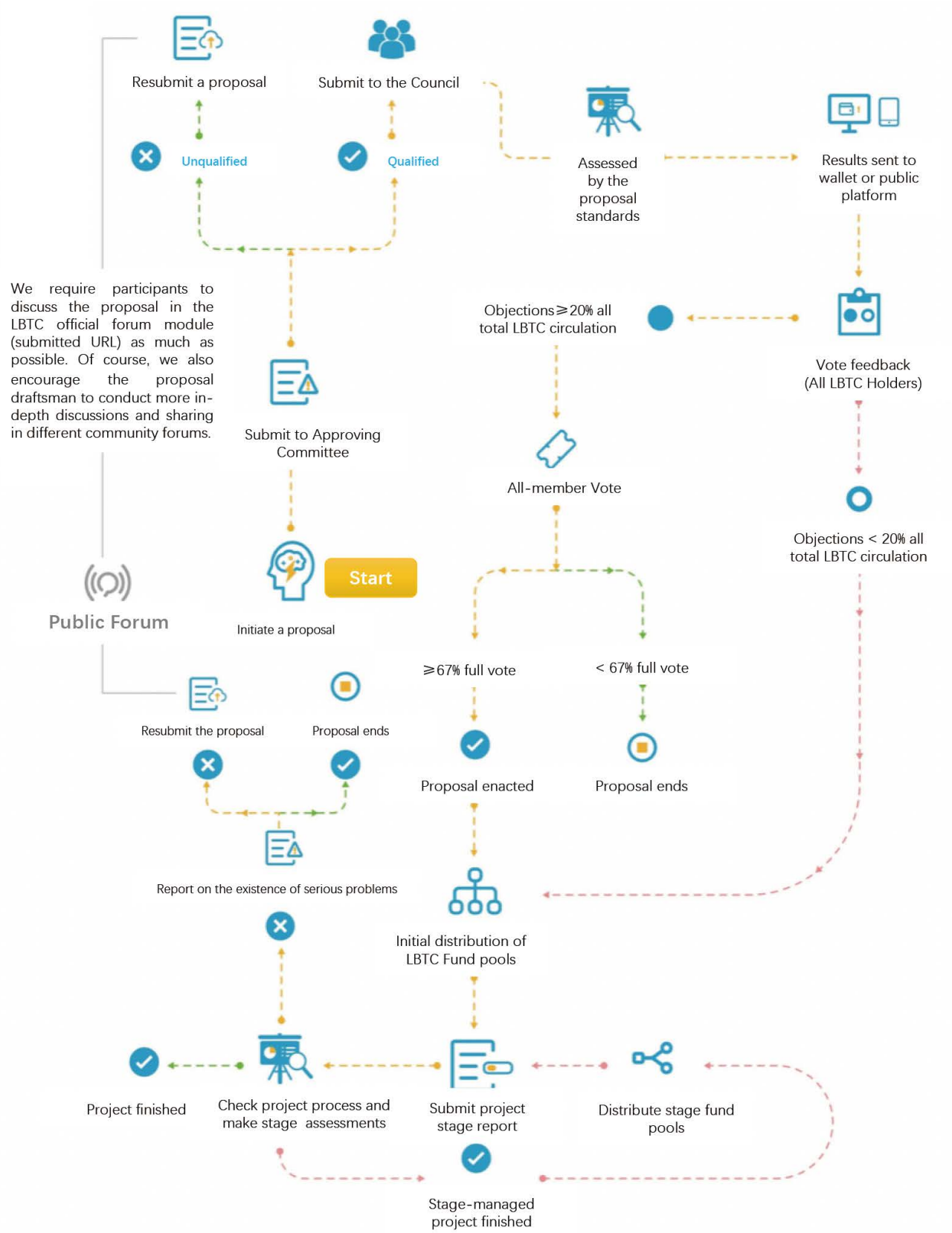
4.2.7 Self-Evolution of the LBTC Protocol

The LBTC is a self-evolving protocol. Based on the current version, all participants jointly make decisions to further the upgrade. Members of the community can submit their ideas to the Council, which can be on the changes to the management system, on paths for future development, or even a simple suggestion. As long as the idea is presented, the Council will consider whether it is a good one, whether it is worth upgrading, and then return feedbacks to the developer community.

The developer community will form a Lightning Bitcoin improvement proposals (LBIP) based on the suggestions from the Council or ideas directly from the developer community, and the LBIP will then be evaluated by the Council.

If the Council approves the LBIP, the protocol upgrade will be directly implemented with the code, details and changes of the upgrade announced in the official website and wallet. All token holders are free to express their opinions or objections. When the number of objections exceeds the set threshold, an all-member vote will be initiated. If the upgraded LBIP is considered extremely important, fundamental and revolutionary, then it will skip the previous steps and go directly to the all-member vote.

SGS Chain Governance System:



5 LBTC Decentralized Transaction Platform

5.1 The Future of DEX and Tokenization

5.1.1 DEX as the Future of Exchanges

DEX, the Decentralized Exchange, refers to a token exchange controlled by smart contracts or built-in functions on the blockchain. Corresponding to DEX is a company-operated exchange with centralized model management.

DEX will become an important part of future exchange ecology, responsible for a clear division of work with traditional centralized exchanges. The irreplaceability of DEX lies in:

1) In DEX, users can completely control the assets on the chain, and there is no trust risk related to the traditional centralized exchanges. Moreover, there will be no such cases as illegal freezing, misappropriation, or stealing of user funds in DEX.

2) DEX does not require KYC and AML processes, users will not provide additional information to the exchange. However, centralized exchanges hold a large amount of user information, and may use this information illegally.

3) DEX can keep running with the main chain, and there will not be such problems as rollback, downtime or shutdown caused by human factors of exchanges.

4) DEX relies entirely on the chain, so it is in nature global and unrestricted. Thus, the flow of assets on the chain embodies a strong degree of freedom.

But we also realize clearly that there are currently some problems with DEX that hinder large-scale applications:

1) The performance of DEX is limited by that of the main chain, and the transaction confirmation is relatively slow, so it is not suitable for high frequency operation and operations that require fast feedback.

2) Most of the DEX in market does not have a clear product positioning, and repeated competitions rather than misplaced competitions exist between DEX and centralized exchanges. With this regard, DEX should not conduct blind competitions denying the inherent advantages of centralized exchanges.

3) DEX does not show much advantage in the trading of those super-class and more standardized assets, such as BTC, ETH and ERC 20 Token. Centralized exchanges can provide excellent and in-depth trading experience, as well as flexible and diversified derivative trading, which however is DEX's weakness.

5.1.2 The Inevitability of Tokenization

In the past few years, digital assets have become more of a purely on-chain asset, namely blockchain-based Tokens and Token-derived tokens. But in the foreseeable future, digital assets will have a big role to play to become more versatile and ubiquitous, and be connected to real-world assets and credit systems, which will bring about the issuance, trading, custody, acceptance and other needs related to digital assets.

We can foresee that Tokenization is an important path for blockchain technology to go to a bigger stage. A chain-based system that is completely isolated from the real world can hardly be called an architecture that supports extensive tokenization. More notably, Tokenization can be further interpreted as Asset Tokenization and Security Tokenization, though it is widely believed that Security Tokenization is the nature of tokenization in a broad sense. For instance, we can tokenize equity, creditor's rights, non-standard income rights, and derivative securities, confirming them and transferring them in the form of tokens on the chain. This understanding in fact does not break awayfrom the scope of traditional finance. We believe that the tokenization may trigger a more comprehensive realization rather than be narrowly confined to the scope of traditional securities.

Therefore, we need to further distinguish the concept of assets from securities and explain why LBTC hopes to support the large-scale asset tokenization that will occur in the future by constructing a decentralized trading platform and introducing the Oracle to the chain. By definition, securities are certificates of economic rights featuring as a certificate collection of property rights, circulation rights and income rights. While assets are resources in a broader sense, and they may in the future bring about some other benefits or privileges not confined to economic interests. The revolution blockchain triggers will never be limited to simply transforming the traditional form of securities from the off-chain to the on-chain, but will create a variety of new, non-traditional and non-standard asset types. Technically, with the help of the blockchain accounting system and the introduction of Oracle on the chain, we can build a platform for the issuance, circulation, custody and acceptance of all forms of assets. These assets can further represent any form of rights, which is much more meaningful than financial securities.

5.1.3 Non-Standard and Non-Traditional Assets

Non-traditional assets refer to assets that have not been or cannot be securitized or even rights that cannot be classified into assets in traditional sense. Non-standard assets are the assets that may be personalized and differentiated at any stage including but are not limited to innovative assets that differ from traditional assets in terms of underlying rights, distribution methods, rights and responsibilities and forms of realization. The LBTC decentralized exchange ecosystem will place great emphasis on these non-standard and non-traditional assets (Double Non-Assets) that have huge market demand but not yet been developed on a large scale.

Thus, the LBTC decentralized exchange will redefine the connotation of the Double Non-Assets tokenization. The tokenization of such assets can cover those types of assets that have recently emerged or are still in their infancy, such as:

- STO (Security Token Offering);
- FOF (Fund-of-Funds);
- Small-scale crypto secondary market funds;
- The share of the mining pool;
- Second distribution of specific stake shares;
- Issuing acceptable IOUs.

For instance, when a key opinion leader (KOL) of a community wants to recommend and pre-sell a project he/she favors to the community members, even if the project is not yet put online and has not been officially issued for token sales, the KOL still can issue this digital asset on the LBTC, make them available to all members of the community, and enable free transactions among members. After the token is issued, all holders of this asset can redeem tokens via the asset issuer.

It should be noted that in this example, the token issuer actually acts as a gateway or Oracle on the chain and sells the token on the basis of his/her own credit or collateral. This model is a new on-chain economic model LBTC believes will be promising in the future. The nature of the gateway is an on-chain Oracle that provides intermediary services. It is decentralized in the technical sense and is credited in the economic sense. In a purely decentralized economy, real-world assets are isolated from the on-chain assets, which is the result of the logical isolation of the atomic world from the digital world. The LBTC has consistently defined itself as the intermediary in connecting atomic world and the digital world, whose role will serve the going-on-chain movement of real-world assets and nurture a soil suitable for Oracle growth on the chain.

Of course, users can also issue customized non-standardized products in the DEX supported by LBTC, such as an insurance for Bitcoin price, a quantified fund share and a computing power of mining pools. Anyone is entitled to participate in such transactions of rights and interests and get paid at the issuer. Even securities in the traditional sense can be transacted in DEX in the form of digital assets via Oracle's acceptance and offering on the chain. Theoretically, as long as it is a definable, quantifiable, and divisible right or interest, it can be customized and transacted in the DEX supported by LBTC.

5.2 Building DEX and Oracle Ecology on LBTC

5.2.1 Ideal Adaptability of LBTC to DEX

LBTC is a decentralized Internet-of-value protocol for global payments. But the cases where peer-to-peer payment can be used are rather limited in the world of vast digital assets. Therefore, the support for the transmission of decentralization and functions in digital asset transactions is a must-have requirement by LBTC users. LBTC is in its nature suitable for DEX, on-chain Oracle and the construction of Double Non-Assets ecosystem.

LBTC uses the UTXO-based DPoS consensus mechanism, which is featured by short block time, large network throughput, as well as stable and robust network operation. It is therefore highly suitable for decentralized digital asset transactions. LBTC itself is a mature peer-to-peer payment network. The DPoS mechanism makes the time needed for transaction confirmation at about 3s, which is even fast enough to meet the requirements of enterprise applications. In addition, when building DEX on the LBTC, a modular architecture can be adopted with functional components and APIs opening to the public, which will provide high terminal flexibility to third-party transaction platforms and on-chain Oracle.

As we all know, the circulation of digital assets and real assets has always been a thorny issue. As the regulations of each country gets more stringent, it is becoming increasingly difficult to undertake the legal tender passage open and legally, but the construction of DEX on the LBTC can help solve this problem. The DEX can also decentralize the legal tender channel, enabling anyone who participates in the network on the platform to be a gateway to undertake the exchange of legal tender and digital assets, or just issue digital assets that represent national currencies. Besides, The gateway can start the exchange without having to obtain a license for the legal tender passage, and there is no need to consider the risk of policy changes in the future. Under the current market supervision system, the acceptors act as a gateway to provide transaction and exchange services, and both the two sides are compliant with regulations. Therefore, LBTC connects the real world and the virtual one in a simple and legal way.

Users do not need to consider any technical issues when releasing customized digital assets on LBTC, including server construction, technical team, code writing, code maintenance and upgrade. All necessary technical solutions for the construction of DEX on LBTC can be provided. Users only need to open the LBTC client or web page and customize the parameters of the token according to their needs (It may be possible in the future that users can only create an inflation or deflationary token economy without setting the total amount of tokens). Users can also distribute the tokens certificated by the assets to clients according to the rules and allow them to make transactions freely on LBTC. The entire process does not require the asset issuer to participate in any technical operation in person.

5.2.2 An Overview of Building DEX Services on LBTC

The main purpose of building a DEX platform on LBTC is to serve the on-chain Oracle or simply gateways of traditional sense. Besides, it concerns the issuance, escrow, transfer and acceptance of various digital assets, especially focusing on supporting non-standard and non-traditional digital assets. The non-standard and non-traditional digital assets are asset classes that are difficult to be recognized and held in escrow on a large-scale basis before blockchain technology emerges. The combination of decentralized architecture and on-chain Oracle has fully liberated the productivity and sent the Double Non-Assets to large-scale applications. This will be the most promising and groundbreaking innovation of the blockchain revolution.

Building a DEX platform on LBTC will provide complete and customizable technical solutions for various roles (asset issuers, acceptors, guarantors, traders, self-built exchanges, etc.) to facilitate the customization, distribution, custody, transfer and acceptance of digital assets. Users can participate in the LBTC DEX platform in a variety of roles or identities.

Asset Issuers:

The asset issuer can customize the asset type and parameters and sell the Token of their own. For instance: 1) The KOL of a community issued the pre-sale volume of an investment project and packaged it as Token issued in DEX. And the KOL himself/herself is influential enough to directly bring users to DEX; 2) A mining pool can issue mining shares, define the selling token as the shares of the mining pool, and is responsible for accepting the token. Non-mining pool users can also purchase shares in DEX without a registration or certification of the mining pool.

Acceptors:

The acceptor provides acceptance services by getting its obligations recognized by the market. In general, the acceptor can also be the issuer of the customized assets. For instance, an acceptor issues a stable token anchoring the BTC in DEX and assumes responsibility for exchange of the token to BTC.

Guarantors:

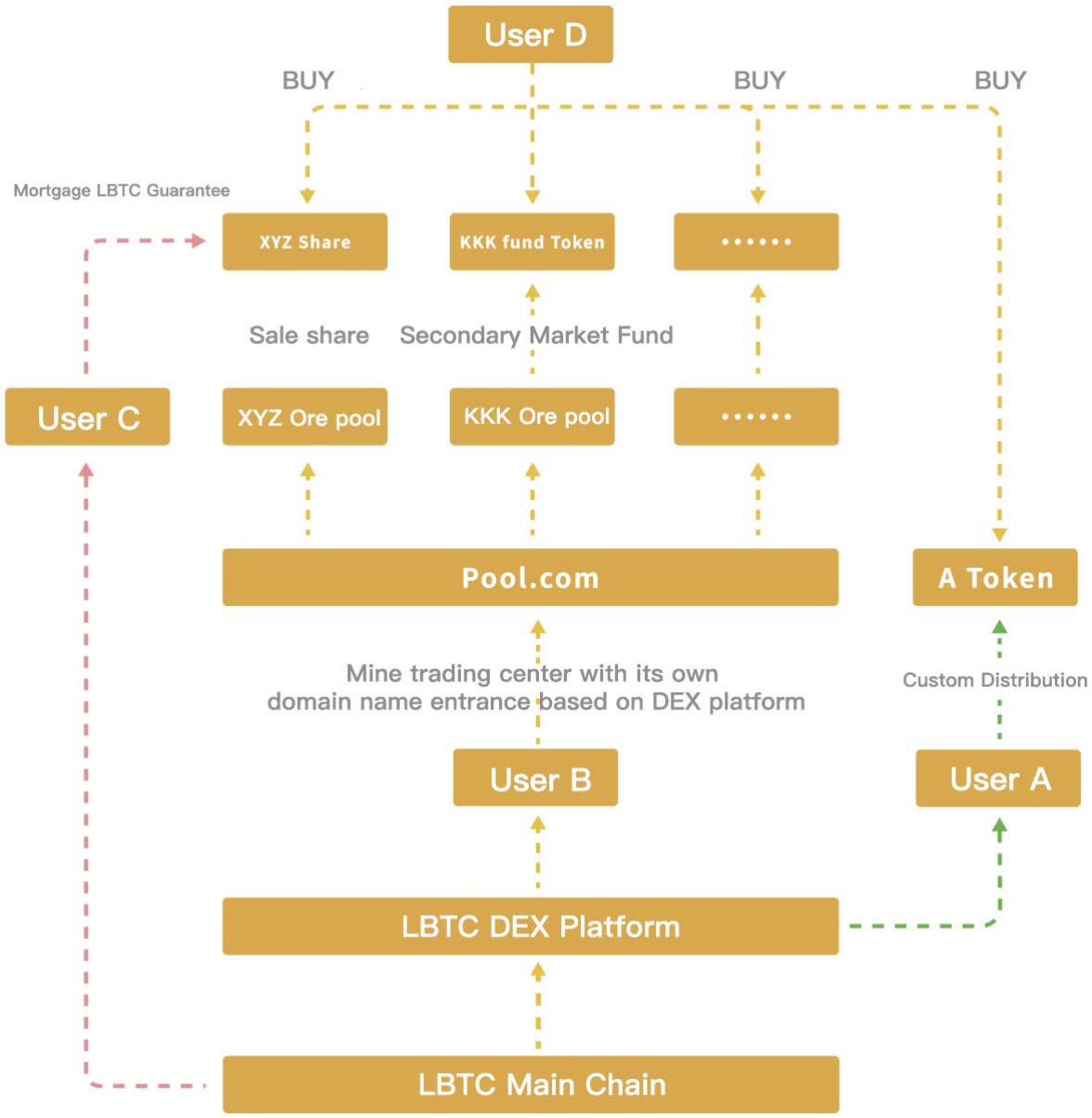
DEX allows for the guarantee assumed for customized assets for sale, and the collateral can be LBTC or other DEX registered digital assets.

Traders:

Traders refers to participants engaged in simple trading activities. Since LBTC is built on the DPoS consensus mechanism, traders only need to provide a very low sum of transaction fee to enjoy a high frequency and in-depth transaction model.

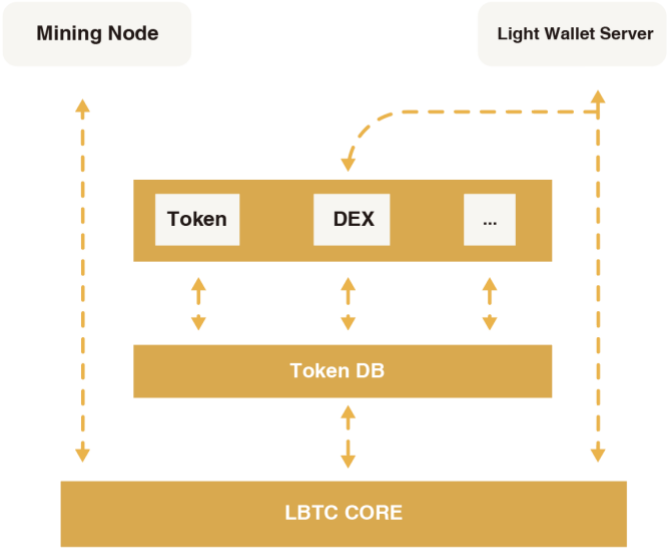
Self-built Exchanges:

The user can establish a decentralized personalized exchange based on the LBTC DEX architecture in its own name (including providing its own domain name and exchange UI interface). For instance, a senior operator of a mining pool can establish a platform for mining-pool share trading with an independent domain name and customize the standards for issuance and auditing of online assets. The user can even sell tokens representing the exchange based on the cash flow asset on LBTC DEX.


User D
BUY
BUY
BUY
Mortgage LBTC Guarantee
XYZ Share
KKK fund Token
••••••
Sale share
Secondary Market Fund
User C
XYZ Ore pool
KKK Ore pool
••••••
Pool.com
A Token
Mine trading center with its own
domain name entrance based on DEX platform
Custom Distribution
User B
User A
LBTC DEX Platform
LBTC Main Chain

5.3 Technology Implementation

5.3.1 An Overview of System Architecture



The construction of DEX architecture on LBTC can be divided into four levels.

• LBTC Core (LBTC main chain protocol layer):

The main chain is responsible for the verification of DEX on-chain transactions, package and block generation, as well as the process of consensus reaching. Meanwhile, the main chain is also the carrier of the assets traded by DEX. The transaction data is chained to ensure the decentralization of DEX, which is safer, more transparent and more reliable than traditional centralized exchanges.

• Token DB (Token Database):

Token DB is an abstract storage medium. Token is an on-chain asset different from the primary assets on the LBTC main chain and can be customized by the user. Token DB is an individual on-chain storage system that organizes and manages the Token balances and overall information.

• Application Module Layer (Token module, DEX module, etc.):

This layer contains AppModules with different functions, such as the issuance and transfer of Token, and Token transactions. The AppModule is built on the top of the Token DB and can initiate transactions to directly operate the Token DB and control the balance information of users.

• Other Supporting Roles:

Other supporting roles include mining nodes, light wallet servers and so forth. These auxiliary roles can participate in the running of DEX, but not in a direct way. For instance, a full-node wallet can choose whether or not to support the DEX module. If a full-node wallet supports access to DEX, the user can directly invoke the Token issuing and transaction in the wallet, at which point the wallet can be considered a DEX client.

5.3.2 Token DB

- Token DB is a storage medium abstracted from the architecture. The Token DB is used to store the information of Token definition, user token balance, address, and ID Mapping.

- Token DB is a memory database that is highly efficient. The app will load data from disk at startup and writes back on exit for the persistence of the data.

- Token DB is a KV database that is easy to use and user-friendly.

- Token DB realizes a memory-based rollback operation that allows for state rollback in extreme cases, protecting user assets and transaction records. In the state rollback, the corresponding AppModule only processes the logic of businesses and is separated from the state, which is hence simple and efficient. The following code illustrates the logic of a state rollback based on memory:

```
OP(blockheight, key, value)
        Undo(key) = Balance(key)
        Undos(blockheight).push_back(Undo(key))
        Balance(key) = value

Rollback(blockheight)
         For item : Undos(blockheight)
                Balance(key) = Undo(key)
                Delete Undos(blockheight)

Commit(blockheight)
        Delete Undos(blockheight)
```

5.3.3 Token Module

- The Token module is of the application type, which is loaded on the top of the DEX architecture in the form of the AppModule that keeps updating.

- The Token module enables the user to create Tokens, define token parameters, issue, transfer and lock or unlock tokens. DEX will develop and refine the Token standards through iteration (similar to the ERC20 and ERC721 standards of Ethereum) to implement all mainstream Token templates such as interchangeable Tokens and Non-Interchangeable Tokens.

The following code briefly explains how to define a TokenTransfer function:

```
TransferToken(blockheight, data, fee)
        CheckFee(fee)
        (fromAddress, dstAddress, tokenId, amount) = Analysis(data)
        CheckBalance(fromAddress, tokenId, amount)
        fromAddressId = GetAddressID(fromAddress)
        dstAddressId = GetAddressID(dstAddress)
        OP(blockheight, fromAddressId ,Balance(key) - amount)
        OP(blockheight, dstAddressId ,Balance(key) + amount)
```

5.3.4 An Overview of DEX Module

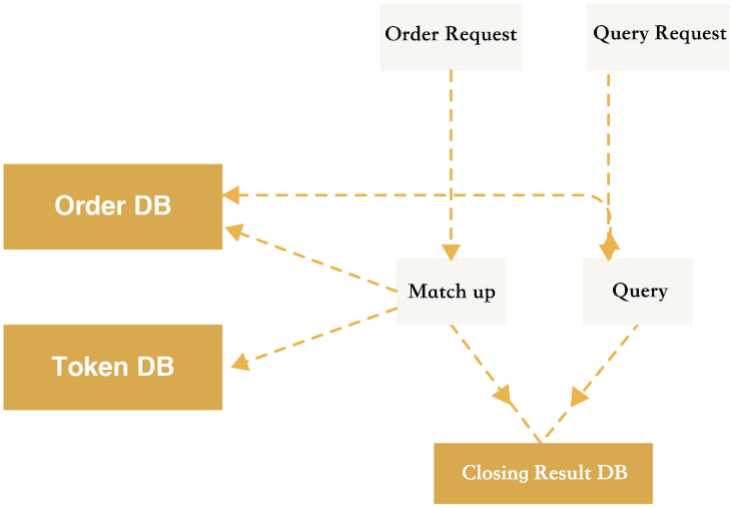
- The DEX module is also of application type which is loaded on the top of the DEX architecture in the form of the AppModule that can keep updating. The DEX module needs to rely on the Token module and adapt to corresponding Token standards.

- The DEX module when invoking basic functions such as TokenTransfer implements a combination of a shared depth order pool, a Skylark matching engine, and a customizable UI interface.

- Theoretically, any LBTC user can create its own DEX based on the DEX module. Users can define the DEX processing fee, the Token category of the transaction, the user interface, and the web portal. This feature will greatly facilitate the external expansion based on the building of DEX ecosystem on LBTC.

- All LBTC-based DEX can share the order pool, and further share the transaction depth provided by the order pool. The order pool can also treat orders with different DEXs the same way and enables access to them fast and accurately. Moreover, DEX can also reserve the right to only use the individual order depth.

5.3.5 Technological Architecture of DEX



- **OrderDB:** used for saving the information of users' unfilled purchases/sales.
- **TransactionDB:** a transaction database used to save the information of finished purchases/sales, also the transaction history of the user in DEX.
- **TokenDB:** used for saving the information of users' token balance, which is represented as a mapping relationship for maintaining Virtual Account-Token Balance.
- **OrderHistroyDB:** used for saving the order history of buying and selling transactions.
- **Matching:** used for checking whether there is a price matching order in OrderDB after receiving a users' new purchase order, and if there is any, then the transaction will be completed, and the balance information of the user will be updated in TokenDB, and the information of the transaction result will be saved in OrderHistroyDB.
- **Query:** responsible for querying the current order queue and transaction records.

It should also be mentioned that both OrderDB and TokenDB belong to a memory-based database, and OrderHistroyDB is stored on disk due to its large amount of data. Since the DEX built on the LBTC is an on-chain data system, combined with the time feature of LBTC block generation, the OrderHistoryDB will complete the writing in batches when each block is generated.

5.3.6 Issues on DEX performance

As a user-oriented on-chain product of application type, users must be very concerned about the performance of the DEX system since it directly affects the users' using experience and the significance in facilitating transactions. The building of DEX on LBTC has taken system performance issues and corresponding performance improvement solutions into serious consideration from different perspectives.

1) Consider the relationship between DEX performance and the performance of LBTC main chain:

DEX is in essence an application developed on the basis of the blockchain database. The performance of DEX will therefore be directly affected by the blockchain data throughput and processing speed. In fact, the bottleneck of DEX processing lies in the capacity of data throughput which relies actually on the data throughput ability of blockchain database. Therefore, the underlying blockchain with high TPS will help the DEX with the processing of orders and transactions. LBTC uses UTXO-based DPoS consensus mechanism with an average of 3 seconds in block generation, which provides DEX with excellent underlying technical guarantee. At this point, the building of DEX on LBTC is much more desirable than that on Ethereum, which will provide users with more powerful transaction performance and smoother experience.

2) LBTC uses a self-developed and optimized Skylark transaction matching engine.

The Skylark transaction matching engine is based on a series of operations in memory database with an I/O performance far superior to both that of a disk database and the TPS bottleneck of the LBTC blockchain.

The Skylark transaction matching engine does not handle those computationally complicated operations such as the user signature verification. It mainly queries the transaction order in memory databases. It realizes the ~log(n) complexity in the query of orders, thus achieving extreme high matching efficiency. In contrast, DEX based on Ethereum can only settle for something that is second-best, taking the off-chain server matching, in order to compete with the Skylark transaction matching engine with regard to the matching ability.

3) The performance of DEX query:

DEX queries are divided into the query of Order and Order History:

Order query is realized through OrderDB, the memory database, which is faster;

Order History query is realized through OrderHistoryDB. Since this database is not based on memory and given the complexity of query logic, the speed is obviously lower to the Order query.

It also should be noticed that in the actual using, the number of queries a user initiates may be not less than, or even higher than that of specific order operations (such as placing an order or withdrawing an order), so we must solve the efficiency-related issues of queries not based on memory database. If Skylark implements the above-mentioned queries only according to its standard processing logic, it may fail to break the TPS bottleneck of the data processing by the LBTC itself with this regard. This will lead to the DEX not being able to utilize the advantages of the LBTC main chain and weakening the ecological advantage of building DEX on LBTC.

For these reasons, the DEX technology development team considered the following potential solutions:

Solution 1: Expanding it to a distributed query

The necessary foundation of distributed queries is the nodes that support large-scale DEX running. When the number of queries initiated by users reaches a certain threshold, the system will automatically distribute query tasks and send requests to different nodes. This means that nodes are able to process query tasks in DEX in a distributed manner (The query itself does not change the on-chain state, so the distributed way of handling is entirely feasible and trustworthy).

The difficulty of this solution is that there is a need for nodes that support large-scale DEX running, otherwise it is technically impossible to implement distributed queries. A mature technology solution never solves a real-world problem simply by proposing a theoretical framework. Therefore, we must consider another feasible solution if this option (nodes that support large-scale DEX running) is not available.

Solution 2: Separating the query server or establishing a query server group

As we have already discussed in the previous part that since the query operation in DEX does not necessarily change the state of the chain, the implementation of the query action can therefore be completely changed in terms of its methods. In addition to distributed queries, we can also separate the function module of the query server and supplant it with an entity-centralized server, or even set up a separate server cluster to provide query support for users with high query demands.

This solution is like using etherscan to query the on-chain data and status of the Ethereum. Although etherscan.io itself is a web page run by a centralized server, this does not affect the decentralization of Ethereum. This is because etherscan provides services of the query type, and the query does not rewrite the blockchain. The DEX built on LBTC can support the two schemes discussed above according to the actual needs of users.

4) The issues of DEX data throughput:

As mentioned above, the construction of order information for DEX is realized through a series of databases based on memory operations, and memory resources are often limited and cannot be expanded easily within a certain period of time.

We can calculate the memory consumed by a single order, and then calculate the data throughput limit for processing order information like this:
MaxOrderNumber = MaxMemory / MemoryPerOrder

This means that high requirements are necessary for the nodes running DEX, and we also need to determine the maximum order quantity that the current system can support according to the actual memory size to realize a Dynamic Order System Management. See the description below.

When the number of order processing reaches the system maximum, we discuss the following situations:

First, when the total number of orders is greater than the maximum number of orders set by the system, the fixed number (or fixed ratio) of unreasonable orders should be revoked. The unreasonable order is defined as a transaction that is away from the price at which the transaction may be successfully made in a transaction pair, which can be adjusted by a dynamic parameter.

Second, when the number of trade pairs is greater than the maximum, all orders in the transaction pair with latest trade volume are revoked.

Third, an adjustable mandatory processing limit should be set (similar to a Hard Cap) to ensure that it can support the operation of DEX and the control of orders even if extreme conditions or high fluctuations of demands occur in a short term, thus effectively avoiding the server crash caused by the pressure of orders.

6 Prospects

In the cryptocurrency arena, many users often experience catastrophic losses, usually in exchanges that are dedicated to depositing and holding user assets. Cross-chain atomic swaps were therefore born. From a technical point of view, it enables direct peer-to-peer transfers of cryptocurrencies on different blockchains, replacing the vulnerable exchanges currently used by investors. As a technological pioneer in the blockchain industry, LBTC will of course not let go of the emerging cross-chain atomic swaps. DEX combined with the use of cross-chain atomic swaps will enable the transfer and trading of various types of currencies. In the future, many large money pools of clients will be eliminated by codes. The implementation of cross-chain technology requires a scalable blockchain for the cross-chain platforms. The LBTC based on the DPoS consensus mechanism meets the need for scalability of cross-chain technology and also has enough space to build the architecture for developing atomic swaps.

In the future, lbtc will support cross-chain technology to achieve value exchanges among chains. We believe that the blockchain of the future will become an architecture of multi-ecosystems and multi-chains. Bitcoin is positioned as a decentralized Internet-of-value protocol for global payments and it is necessary to further expand the cross-chain function and address the issues related to the interaction between chains. The first problem that needs to be solved is the transfer of cross-chain assets. The method currently adopted is to transfer cross-chain assets through centralized exchanges. We have already mentioned in many places above the various drawbacks of centralization. After adopting the cross-chain technology in the LBTC decentralized exchange, we can directly achieve the transfer of assets on the chain through the LBTC decentralized exchange. The next domain we will explore may be a cross-chain oracle. It refers to automatically triggering a specific event on another chain to perform the specified operation when we are performing an action on one chain, which can be possibly applied to the handling of cross-chain contracts. For instance, when an asset transfer occurs between chain A and chain B, some functions in the cross-chain contracts will be used such as interest and assets pay.

The smart contract is also a technology that has gradually emerged and matured in the blockchain industry in recent years, which has also been included in LBTC development plan. The smart contract system according to the trigger condition in the event description automatically issues pre-set data resources and an event including the trigger condition when the trigger is considered valid. The smart contract is just a system formed by transaction processing modules and state machines, which does not generate and modify smart contracts. Smart contracts allow a complex set of digital commitments with trigger conditions to be executed correctly in accordance with the will of the participants, thus achieving the maximum decentralization of the blockchain. After the smart contract is launched, the scalability of LBTC can be greatly improved, and many LBTC-based Dapps can be released. With high TPS, support for popular apps will not cause network congestion. Besides, the privacy algorithm has been included in the planning, so it is predictable that a mature LBTC will have the features of anonymity and compatibility with multiple applications. With the advancement of technology development and ecological construction, LBTC will have more powerful and complex functions in the future.

LBTC has almost created an empire of its own in its vision. The support of safe and reliable technology has laid a solid foundation for the construction of the empire. The planning of the on-chain management has set up the framework of the empire, while the gateway protocol, the decentralized exchanges, and the smart contracts are the flesh and blood of its superstructure. From the development to date, it can be seen that LBTC is never willing to take a “mediocre” route. DPoS+UTXO mechanism, on-chain management SGS as well as decentralized exchanges all are offbeat practices in the blockchain industry. The LBTC is steadily moving forward step by step, at which point the forked coin is no longer its one and only label. The combination of LBTC’s “UTXO-based DPoS+Internet-of-value Protocol” is a brand-new experiment ever. What will it bring to us and the world? Let’s wait and see.

7 References

[1]Satoshi Nakamoto,Bitcoin:A Peer-to-Peer Electronic Cash System[M],2009.

[2]Ethereum:A Next-Generation Smart Contract and Decentralized Application Platform[M],2017.

[3]Ripple Labs,The Ripple Protocol Consensus Algorithm[M],2014.

[4]Bitshares,A PeertoPeer Polymorphic Digital Asset Exchange[M],2013.

[5]Steem,An incentivized,blockchain-based,public content platform[M],2017.

[6]Kevin Kelly,Out of Control: The New Biology of Machines, Social Systems, and the Economic World,2010.

[7]Jean-Jacques Rousseau, Du Contrat Socia, 1762.