享云链
LinkChain

TO BE THE WORLD'S FIRST COMMERCIAL BLOCKCHAIN

LinkChain WhitePaper

www.lianxiangcloud.com

CONTENTS

Abstract

The purpose of LinkChain is to provide a high-performance and secure blockchain infrastructure for scenarios with shared computing and high privacy requirements.

In order to fulfill this purpose, LinkChain has designed a high-performance and strong consistency consensus mechanism, and introduced a privacy protection mechanism that can hide the addresses and token amounts of both sides of the transaction. In order to ensure the feasibility of the widespread application scenarios of Commerce and Finance on the chain, LinkChain has introduced innovative designs such as credit scoring mechanism and multi-asset account model from the level of blockchain account, which makes it possible for LinkChain to deliver value and credit from the on-chain scenario to off-chain scenario.

LTK (Link Token), as the native cryptocurrency of LinkChain, in addition to work as the medium in free trading scenario, also carries a large-scale and promising shared computing ecosystem. In order to realize the vision of replacing the traditional cloud computing services represented by Amazon Cloud etc., LinkChain will continue to exist as a proof of contribution to encourage users to share idle bandwidth and storage resources. Meanwhile, the business value of shared computing ecosystem will be continuously invested in LinkToken system to establish a sustainable ecosystem.

1.Background

Since with the emergence of Bitcoin project in 2008, blockchain technology has gradually attracted the attention of scientific researchers, developers, enterprises and government over the past ten years. Blockchain technology has become a trusted value protocol because of its natural characteristics of decentralization, tamper-resistant and non-repudiation. It also has natural advantages in distributed computing and various cloud services.

In august 2018, Tencent cloud servers lost years of data of the startup company Qingbo ShuKong. In April 2019, researchers from UpGuard, a network security company, discovered hundreds of millions of Facebook users' personal information records (stored in AWS database) in publicly accessible places from AWS.

On the other hand, since the development of the Internet, the question that who has the ownership of the user data was never deeply discussed. Between Tencent and ByteDance, the dispute over the scope of application of user data such as WeChat/QQ nicknames and avatars is still prolonging. Disputes over whether user data belongs to operators or developers when replacing service providers for online games, etc. are also growing recently. Enterprises providing centralized services have never realized that these data should belong to users themselves. Because of centralized services, users can not really own their own data, user data has become a huge profit in the hands of centralized service providers, but users cannot get any benefit from it.

The 5G era is approaching, and the bond between human society and the Internet will be more connected. In the next few years, data of hundreds of millions of smart terminals will be of exponential growth, bringing enormous challenge to the cloud computing industry. With the increasing cost and security requirements of data storage in enterprises, the issue of data security and privacy has attracted much public attention. Centralized processing model cannot meet the changing needs, however, the traditional cloud computing business model cannot provide effective solutions to the problems of limited cloud service speed, high equipment cost, high learning cost, low fault tolerance, limited coverage of enterprises, and challenges to data security and privacy. Traditional operation mode is unable to catch up with the pace of the new era, and those problems above have to be settled urgently.

These problems are not unsolvable, but only with huge cost investment. The cost problem in the era of 4G has already been very prominent, and this would only be severer in the era of 5G. Even worse, the failure of Moore' s law leads to the inability of social computing costs to be reduced accordingly, which also leads to the failure of traditional cloud service models and even Internet business because of the dramatically increasing costs.

We believe that blockchain technology will build a new future for the Internet and the whole world. In this future, data will no longer be monopolized by centralized nodes. Privacy protection will be guaranteed from the bottom logic layer, fundamentally avoiding the abuse of data by centralized organization, and returning ownership of user data to users. Shared computing will effectively solve the cost problem, significantly reduce the cost of computing in the whole society, promote the qualitative change of business model, and accelerate the arrival of a new era.

The combination of blockchains and shared computing has brought new vitality to the Internet industry. The core advantages of blockchains, such as system autonomy, data traceability and immutable information, just make up for the deficiencies of pure distributed computing. The combination will enable people to enter the era of value Internet from the information internet, bringing a new social organization structure and business model of de-intermediation, thus changing our life to a new style. Blockchains can effectively solve the pain points of data fraud and high dependence on a single organization in the centralized model, so as to build a decentralized autonomous ecosystem eventually.

However, the existing blockchain technology still has problems hindering the wide application of blockchain technology. These issues include low performance, lack of privacy protection, trust issues between on to off chains, etc. Some blockchain projects have been devoted to solving some of these problems. For example, Ethereum has tried to add sharding feature to improve its performance; Zcash, MONERO and other projects are exploring privacy protection ways for on-chain transactions.

But in fact, only part of the problem has been solved, which cannot fully support the successful application of blockchain technology in a broader business scenario. A more completed solution is being expected.

2.Target

In order to build a highly decentralized, low-cost, privacy-protected and trusted future of the Internet world, as a blockchain infrastructure, LinkChain needs the following characteristics:

Privacy protection

Privacy protection of assets is not only conducive to personal security, but also a necessary condition for the effective operation of the free market. Therefore, both transaction parties on the chain need to be able to hide account addresses and transaction amounts, and ensure that the transaction data are not related and traceable.

Interaction and circulation of multiple assets

In large-scale commercial and financial services, there are many kinds of transactions of different assets, which require that the chain can provide high-speed assets circulation, can quickly introduce new assets and can trade seamlessly with existing assets, and achieve high throughput and efficient asset transactions on the premise of privacy protection.

High performance

Typical business and financial scenarios have a large number of user groups and frequent transaction requests. A technology platform capable of processing large number of requests with low latency and high throughput is essential.

Low cost

A widely distributed and sustainable resource sharing model needs to be constructed through shared computing ecosystem, which provides low-cost and decentralized computing resources by Token incentive policy, serving at least 90% of Internet products, and constitutes a business ecosystem that can replace traditional cloud service providers such as Amazon Cloud and Google Cloud.

Trust Transfer from On-Chain to Off-Chain

Business entities need to be able to deliver their credit of service or products from on-chain to off-chain (vice versa). In the financial scenario off the chain, there are a large number of service scenarios based on credit scoring, which need corresponding infrastructure support on the chain.

Long-term Credit System

Healthy, positive and fair competition environment can make human society develop and prosper. LinkChain is committed to building a fair competitive environment in the autonomous ecosystem, reducing risks as much as possible from various false information and malicious acts. Therefore, in the ecosystem of LinkChain, another measure of value: trust value, will be gradually added and improved in community development. Through trust value system, LinkChain will build a reliable and significant reference value to all data, information and user behavior on the chain, and solve the problem that the credibility of massive Internet information is difficult to verify and trust among Internet users, thus greatly reducing the operation cost of social affairs.

In this white paper, we will introduce the key technical solutions of LinkChain:
In Chapter 5, we will introduce the consensus mechanism.
In Chapter 6, we will introduce the account model and asset management model of LinkChain, and show the capability of multi-asset management of LinkChain.
In Chapter 7, we will introduce the privacy protection method and show the technical advantages of LinkChain in the high-speed and flexible anonymous transactions.
In Chapter 8, we will introduce a dual virtual machine solution for smart contracts to support a variety of smart contract programming languages.
In Chapter 9, we will introduce the mechanism of node election and community governance in detail.
In Chapter 11, we will introduce the vision of long-term development of LinkChain.

3.Link-Token

TLK (Link Token) is a utility token issued globally by Chinese company. It has been launched for nearly two years and has been firm developing steadily and firmly. OneThing Cloud, in which LTK works as the incentive component, is one of the best-selling smart hardware products in China. At one time, there was a 5-10 times price premium for purchasing machines in the market because of the demand was too high. OneThing Cloud has been followed and welcomed by more than 35 million users.

Since its launch in October, 2017, as a proof of contribution, LTK is to incent users to share idle bandwidth and storage resources, which has accumulated a large number of users for the shared computing ecosystem. At present, more than 1.5 million OneThing Cloud have been involved in this mode, constituting a 30T bandwidth, 1500PB storage space, serving the robust ecosystem for dozens of Internet enterprises.

LTK ecosystem is positively correlated with the rapid growth of social value

In 2015, the upload bandwidth of a single device was 2M at the beginning of the year of shared computing, and 15M at the time of the release of the OneThing Cloud in 2017. In 2019, the number increases to 25-30M, which means that the value that a single OneThing Cloud can produce, and also the value reflected by LTK, has increased 20 times within 3-4 years. In 5G era, the bandwidth will exceed 100M, even into the 1000M, and the value of a single device will continue to exponentially increase. In line with this, the scale of idle resources saved by chain-based shared computing for the whole society will be also scaled up. Such low-cost and high-quality resources will also foster greater commercial value through participating enterprises.

In the 5G era, besides OneThing Cloud, there will also be a large number of innovative hardware devices to join the shared computing ecosystem built by LTK. In 2019, OneThing Cloud mini, who connects idle mobile phones, won the CES Two Picks Award, while long-term online devices such as smart TV, boxes and speakers will gradually be incorporated into the LTK ecosystem. It can be seen that LTK users will be the largest users and beneficiaries of edge computing.

LTK will keep the total amount of 1.5 billion unchanged after its migration to LinkChain. At the same time, LTK will continue to undertake the function of proof of contribution under the shared computing ecosystem, and continue to play its value in resource sharing, energy saving and reducing the cost of the whole society. In the development of LinkChain autonomy community, LTK will also support by its value and incentive feature in multiple facts such as developer incentives, block producing incentives, management members incentives, voting qualifications and so on.

LTK Value in 100 Billion Dollars Cloud Computing Market

In 2018, the global cloud computing industry was 272 billion US dollars. Authorities forecast that this number will grow to 623.3 billion US dollars in 2023. Cloud computing is undoubtedly one of the fastest growing areas in the next few years, and the value of LTK and its Shared Computing Ecosystem will be maximized in this area.

We believe that the essence of shared computing is that the cost of Internet operation is greatly reduced, data privacy is fully guaranteed, and data reliability can be directly trusted. All of these will be realized through the shared computing ecosystem constructed by LTK based on this idea. After two years of practice, LTK has accumulated a large number of users and business scenarios, and has won the support of many tier one internet enterprises. Practice has proved that shared computing prevails traditional cloud computing mode when there are many problems to be solved.

In the future, based on the shared computing ecosystem of LTK, we will build the comprehensive business model through cloud storage, edge computing, network acceleration, content distribution etc., and eventually realize the vision of replacing traditional cloud services. At that moment, whether it is computing capacity, storage space, privacy protection, or other functions, will be able to work synergistically based on LTK, the benefit of shared computing will be delivered to all participants. Ultimately, the commercial profit from various demand sides will be put back into the chain system.

As one of the most well-accepted Token in China, we believe that the ecosystem will be developed on a larger scale and unleash unprecedented tremendous energy when LTK immigrates into the LinkChain.

LTK Current Ecosystem

1. Online Exchange Platform

The LTK Mall established by the foundation has nearly 400 companies enrolled, covering more than ten categories of commodities, such as groceries, kitchen products, mobile phone digital, household appliances, educational reading, video membership, etc., and nearly 2000 SKU, and the merchants and commodities are still expanding. LTK Mall will remain strict assessment policy to keep an outstanding user experience from the continuous applications from merchants.

On the other hand, online exchange platform/campaigns are also a channel to boost growth of shared computing ecosystem, where commercial value from participant enterprises will be re-invested into the ecosystem.

2. New Retailing Projects

In the project named ChaoYouHui built upon LinkChain, the user may deduct the payment directly by credit (Chao Credit) accumulated in the purchase activity, which is exchanged via LTK and the transaction will charge 10% of the LTK as the transaction fee, which increases the demand for LTK. At present, that new business model has been verified. There are more than 600 franchised stores, and the Business side and Consumer side will be continuously expanded throughout China.

3. Other applications

At present, there are many games including pet cultivation, chess and cards, as well as cloud service management software running on the LinkChain. In the future, the foundation will vigorously support many kinds of applications on LinkChain.

Looking back, it is the functionality and scarcity of LTK that have consolidated the base for LinkChain ecosystem. Looking forward, LTK will play more roles in the ecosystem, and this autonomous co-construction ecosystem will also give LTK greater value.

4.Technical Architecture

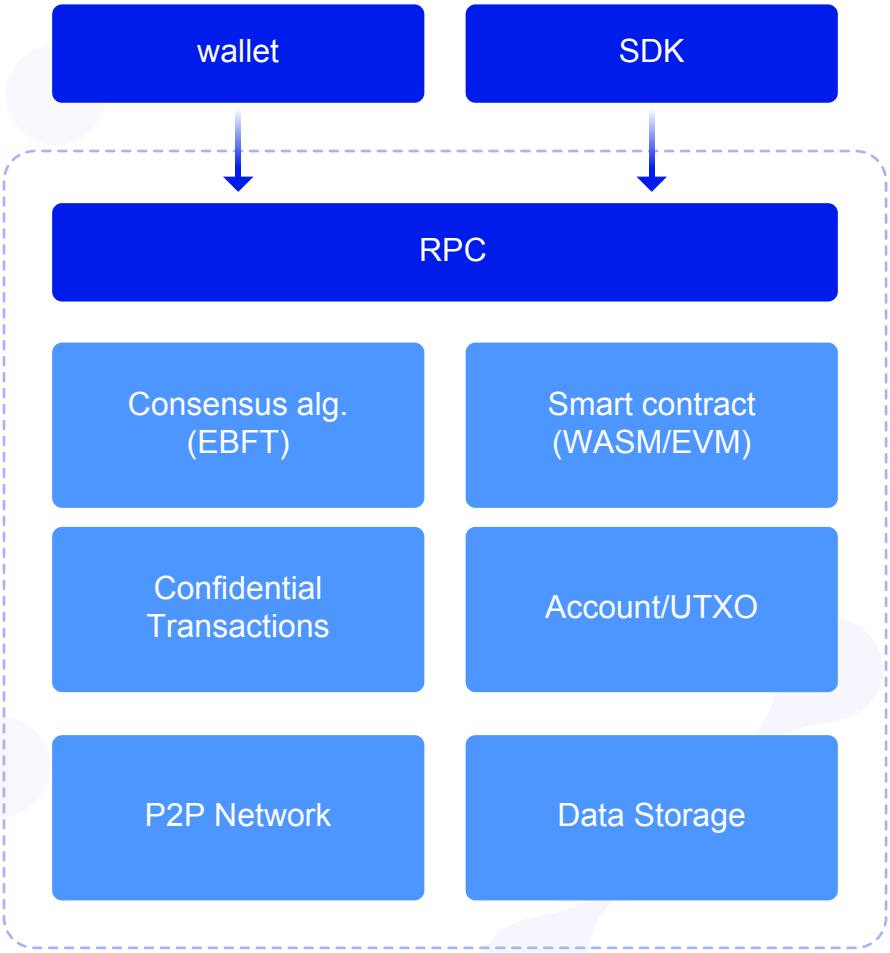


Fig.1. Technical Architecture Diagram of LinkChain

The LinkChain includes wallet application, DApps SDK, RPC interface layer, smart contract, privacy protection, consensus algorithm, P2P network, account and asset management, data storage and other modules.

5.EBFT Consensus

EBFT is a kind of Byzantine consensus algorithm designed to automatically replace validator nodes periodically adopted in LinkChain, featured in high throughput, low latency and strong consistency. E(Elective) indicates that the appointment of the validator node is achieved through regular elections, and the performance of the validator node during its term of office will affect the results of its next election.

Qualification of Validator nodes

n the EBFT consensus, the nodes that can participate in the consensus algorithm are called validator nodes. All the eligible nodes will form a validator pool. The consensus algorithm will select validator nodes periodically from the pool. To enter the validator pool, a node needs to meet the following conditions:

1.Provide IT resources that meet certain standards (server specification, bandwidth, security specifications, operation and maintenance, etc.);
2.Submit a certain amount of LTKs as deposit, in order to obtain a higher probability of producing block, can provide excess deposit;
3.Open elections are needed to enable the top-ranking nodes to enter the validator pool and gain the opportunity to participate in consensus.

In principle, the number of nodes in the validator pool is unlimited and the scale of the pool can be very large. However, there is not a positive correlation among consensus efficiency, the benefits of a single node and the number of nodes, so the number of nodes will be adjusted according to the development of LinkChain. Validator pools will be firstly operated on a scale of 15-35 nodes in the initial stage.

Validator Node Replacement

LinkChain automatically and periodically (usually after 1321 blocks) runs a validator campaign algorithm, A certain number of nodes (usually 22 nodes) are selected from the validator pool to replace the incumbent validator nodes in this round. The campaign algorithm will evaluate comprehensively according to the three conditions: node service quality, deposited LTK amount and random factors to ensure the following characteristics:

1. Blocking malicious nodes; reduce the probability of unstable nodes (such as nodes that often time out and do not produce block) being selected.
2. In honest nodes, the higher the deposit amount, the greater the probability that the node will be selected as the validator.
3. The random factor guarantees that honest nodes with lower deposit amount can also be selected as validator nodes with lower probability.
4. Every validator change requires more than 2/3 nodes of consensus, which will be recorded in the block.

After the validator nodes are elected, the block proposal request will be confirmed by EBFT consensus algorithm among the validator nodes during the term.

EBFT Algorithm

The EBFT algorithm of LinkChain is an improvement of PBFT (Practical Byzantine Fault Tolerance) algorithm. These improvements include:

1. Simplified state machines (such as removing View Changed and other states, and going directly to the next block proposal process after a timeout) to reduce message types and make them more suitable for consensus scenarios in blockchains.
2. Nodes use their digital signatures to propose or vote so that the algorithm can trace malicious nodes through their public keys.
3. The algorithm punishes malicious nodes and unstable nodes: the deposited LTK of maliciousnodes will be eliminated and the validator node will be disqualified, which will greatly increase the cost of improper behavior. The node with timeout in proposing a block will be reduced the probability of being selected as the validator node in the future, while the long-term stable block node will increase the probability of being selected as the validator node. By such the stability of the system will be greatly increased.

EBFT algorithm is a consensus algorithm with strong consistency, which requires two rounds of voting with more than 2/3 nodes for each block, and can tolerate up to f=(N-1)/3 Byzantine nodes (N is the number of validator nodes); honest nodes will not repeat proposing block in the same height, nor will they vote for two blocks in the same height, thus is to avoid soft forking. LinkChain will be able to have high transaction throughput, and confirm a block every 1-3 seconds, in a word, the transaction in LinkChain can be confirmed within 1-3 seconds.

Extensibility

When the data volume or transaction concurrency exceeds the limit that a singular chain can support, LinkChain is able to achieve unlimited scalability by its homogenous-chain architecture and/or layer 2 extension technologies.

Recovery Mechanism

If more than a third of the incumbent validator nodes crash or confront Byzantine errors, the block producing process will be stalled. Then the recovery mechanism would be activated.

After the system has been in a standstill for a period of time (for example, 10 minutes), all nodes on the network can sense it, because all nodes cannot receive new block confirmation during the standstill. At this time, a special block, called recovery block, is constructed by the proposer in the currently available validator. The recovery block contains a list of new validators obtained by executing the campaign algorithm, and then broadcasts the block to other candidate nodes in the network. When the other nodes receive the recovery block, they verify the validity of the block and check whether the blockchain is really stuck in a standstill. After 2/3 confirmation of all online nodes, all nodes update their own list of validators. The selected validators can form a new set of validators and restore the block producing process. If more than one third of the validation nodes in the new list are unresponsive and unable to produce block, then the unresponsive nodes will be delisted and the corresponding number of validators will be re-elected until the system returns to normal.

The recovery mechanism, confirmed by two rounds of voting, each round requires over 2/3 of the candidate nodes' voting, is feasible because it can be proved to be still in Byzantine security. Although it may be slow and expensive to reach consensus in a large set of nodes (a large number of message broadcasts), automated recovery mechanisms are very important and the incurring expense is acceptable for system pause that actually rarely occurs in decentralized systems.

In order to avoid stalling as much as possible, after a validator node had been continuous found to timed out for three times without proposing block, the node will be removed from incumbent validators and system will select a new one from the validator pool to join the incumbent validator set after reaching a consensus.

6.Account Model and UTXO Model

So far, there are two account models in blockchain: UTXO from Bitcoin and Account model represented by Ethereum. These two account models have their own advantages: UTXO is stateless, easier for concurrent processing and privacy protection; Account model has a global state, transaction execution efficient, lower cost, and more conducive to the implementation Turing-complete scripting language for smart contract.

The LinkChain supports both UTXO and Account models; moreover, users can manage a variety of digital assets by UTXO and Account accounts; each asset is differentiated by asset type. Token assets are issued by smart contracts, or received through smart contracts from other public blockchains (such as bitcoins or eth), Hence, the type of assets in LinkChain is actually a smart contract address.

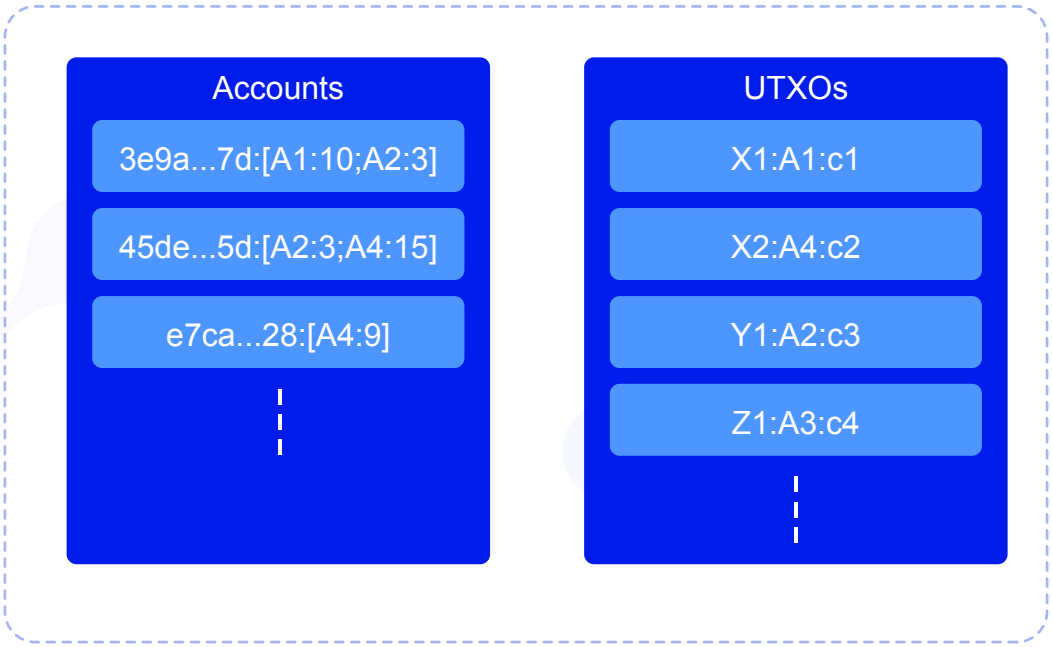


Fig.2. Multi-asset Account & UTXO model

For instance, Figure 2 depicts the multi-asset Account & UTXO model in LinkChain. There are two types of accounts, Account and UTXO:

1.Each Account maintain a list of assets to keep track of the balance of each asset. Take account record “45de…5a: [A2:3; A4:15]” as an example, “45de…5a” is the account address，this account has two types of assets, “A2” and “A4” , the balance of A2 is 3, and the balance of A4 is 15.

2.Each UTXO has an “AssetType” field. Take a UTXO record “X2: A4: c1” as an example, the owner of this UTXO is X2(X2 is a one-time privacy address in LinkChain), and AssetType of this UTXO is A4, and the amount of A4 is c1, which c1 is a ciphertext which is referred to as “amount commitment” in the privacy protection technology of LinkChain，only the owner of this UTXO can see the actual amount after decrypting it with the corresponding private key.

If Alice’ s Account address is 45de…5a, her privacy address is X, and the one-time privacy address of X is X1 and X2, then Alice’ s wallet will show the assets list as blow:

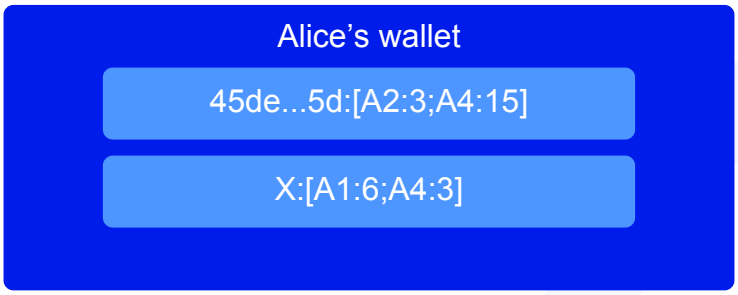


Fig.3. Alice’s wallet

In Figure 3, Alice’ s wallet shows she has asset A2 with balance 3 and asset A4 with balance 15 in account address 45de … 5a, and in addition, there are asset A1 with balance 6 and asset A4 with balance 3 in her privacy address X.

The multi-asset account model of LinkChain endows ordinary token assets with the ability of the first kind of assets, which enables Token assets to circulate freely like native crypto currency and to interact more complexly with any smart contract. Users ’ crypto wallets can display all assets balances under the two account models, and can transfer assets between the two account models by sending transactions.

Thanks to the support of two types of accounts and multi-asset models, LinkChain can provide a complete privacy protection solution and a decentralized exchange.

7.Privacy Protection

In traditional banking and business, privacy protection is the most important aspect, because privacy protection is not only to protect personal security, but also a necessary condition for free competition in the market.

However, in the blockchain system represented by Bitcoin and Ethereum, all transaction data and account data on the chain are open and traceable to all nodes or users. Anyone can view the balance of any account and trace all historical transaction data. As long as a user discloses his account address (in order to trade with others, it is inevitable), others can see all his account information and transaction records happened on the chain, which actually belong to personal privacy or business secrets. In order to protect personal security or competitive advantage, this information is not expected to be leaked in the real world. This weakness of the blockchain is greatly different from the traditional banking and business standards, which results in that most of the financial and business activities cannot be carried out on the blockchain.

Bitcoin developers have developed a mixed currency solution to avoid this disadvantage, but this solution has the disadvantage that it relies on a centralized third party; Zcash project uses zero-knowledge proof to achieve privacy protection, but this knowledge proof requires about 30 KB of additional data per transaction, which makes the solution difficult to be accepted by users; Monero project uses ring signature and Bulletproofs, it is an excellent solution to realize address hiding and amount hiding meanwhile reduces the volume of transaction data, however, Monroe coin cannot support smart contracts, and the throughput and transaction verification speed are still low, so it is difficult to use on a large scale.

The preliminary version of the privacy protection solution of LinkChain is based on ring signature solution and Bulletproofs technology to realize address hiding and money hiding for both sides of the transaction. It also improves transaction verification performance and user experience from consensus algorithm, homogeneous-chain architecture, parallelization, hardware acceleration and so on. Considering that there are a large number of application scenarios in open transactions, the privacy protection feature of LinkChain is an optional function for users. When users initiate transactions, they can decide whether they need privacy protection or not.

The Principle of Address Hiding

LinkChain Ring Signature Solution is used to hide the address of private transactions.
For each user U_i There is a set of public and private key pairs (x_i, x_iG) ,
x_i is private key, $P_i = x_iG$ is public keys, in addition, each public key has a bound label Tag_i .
When User U_0 is to sign, he finds out $n-1$ other users from the network,
say, $U_1, U_2, \cdots, U_{n-1}$. That user will implement the ring signing and show the Tag in the UTXO public key set $L = \{P_0, P_1, \cdots, P_{n-1}\}$ which also includes his own public key.
Validator can verify the validity of ring signatures, but cannot verify the mapping relationship between the private key ownership and public key in the group $L = \{P_0, P_1, \cdots, P_{n-1}\}$,in that way the signer' s information has been hidden, and whether the signature Tag has been used, so as to stop the double spend.

The Principle of Hiding Transaction Amount

The amount of private transactions in the LinkChain is hidden by using the Bulletproofs solution. Through non-interactive zero-knowledge proof protocol, the solution becomes to solve below mathematical problem:
Given the value (bound with a specific token amount) $\mathrm{Com} = xG + aH$, to prove $a \in [0,2^d - 1]$.
The proof system of Bulletproofs is mainly based on Perdesen Commitment $C(x,a) = g^x h^a$
in discrete logarithm. The establishment of proof system can be divided into the following steps:

1.Compute a new inner product argument in logarithmic size.
2.Construct a zero-knowledge range proof based on the new inner product argument.
3.Provide the aggregation method of the range proof.
4.Construct a zero-knowledge proof system based on arbitrary arithmetic circuit.

UTXO Structure of Privacy Transactions

All privacy transactions are implemented through UTXO model. If a user who wants to initiate a privacy transaction has only a balance in his Account model, he can first convert the amount in his Account model into UTXO model, and then initiate a privacy transaction.

The data body of each UTXO with privacy protection in the LinkChain is composed of the following parts:

- UTXO public key: UTXO public key is open to whole net, the private key is managed by this UTXO owner.
- Amount binding commitment: The Amount will be either shown as a explicitly (No privacy) or commit $\mathrm{Com} = xG + aH$ (Privacy, x is the confusion parameter).
- Amount legality proof: The range proof π that the UTXO commit $\mathrm{Com} = xG + aH$ applies to $a \in [0,2^d - 1]$
- UTXO index information: Including ring-signature information and block information.

Privacy transaction execution process

When Alice initiates a privacy transaction to Bob, her crypto wallet works in the following process:

1.Look for confusion UTXO;
2.Calculate the new UTXO amount commitment and the legality proof of the amount;
3.Encrypt the new UTXO amount with confusion parament by her public key;
4.Negotiate the new UTXO public key (only the recipient can calculate the private key);
5.Sign a transaction with a linkable ring-signature.

Transaction requests are broadcast to the chain. When the validator node packages the transaction, the following process will be performed:

1.Verify the validity of the old UTXO;
2.Check if it is double-spending;
3.Verify the validity of ring signature;
4.Verify the validity of the range proof of the new UTXO.

Once the block is confirmed, Bob’ s wallet will work in the following steps to receive the new UTXO:

1.According to the new UTXO public key, the new UTXO private key is calculated;
2.Decrypt the amount and confusion parameter of the new UTXO;
3.Verify the correctness of the new UTXO commitment;
4.Use his wallet to save the new UTXO.

8.Smart Contracts and Virtual Machines

LinkChain supports two Turing-complete virtual machines, WASM and EVM. Users can use common programming languages such as C/C++, solidity to develop smart contracts.

The smart contract of LinkChain has a global state, and its address is Account address; users can send a specified amount of private assets from Account or UTXO address to contract address; similarly, smart contracts can also send a specified amount of token assets to Account address or UTXO private address.

On the LinkChain, Token assets issued through smart contracts can be sent to UTXO or Account addresses through a common transaction. The Token assets sent will be converted to the equivalent unspent UTXO or balance increment in Account. The type of Token assets will be set to the address of Token issuance contracts.

9.Node Election

The stable transaction and block producing are very important to the operation on blockchain. A validator nodes pool and candidate nodes synergistically work together in the LinkChain.
The stability of the nodes and the quality of produced blocks have a direct impact on the whole ecosystem. Nodes entering the validator pool, whether in the status of producing block or not, need to keep the server online to ensure the stability and high speed.

In return, the corresponding transaction fees are all owned by the node when it produces the block. At the same time, LinkChain foundation will also guarantee the minimum reward that all the validator nodes in the validator pool (excluding evil nodes) can get. The mechanism of burning LTK may lead to insufficient circulation of LTK in the future, therefore LinkChain may require more LTK to participate in the circulation, if more LTK is issued, the validator pool will also get the corresponding LTK to reward the validator nodes, so as to ensure the block producing speed and stability.

In addition to the rights and interests as community members, nodes also have the right to propose to important events and vote on them. However, if the node fails to produce block within the maximum time window, or has cheating, collusion and selective non-participation behavior, it will be eliminated immediately, and the replacement will be selected from the validator nodes that do not participate the block producing in this round. Those nodes that do not commit their duty like increase the latency or not be online many times will lead to be removed from current block producing round.

For those nodes who commit crimes, the punishment is not only will they be immediately delisted from the validator nodes, but also their deposited LTK will be destroyed and they will be put to the blacklist. Incentive and punishment mechanism are designed to protect the interests of all members in the system and to maintain the healthy development of the entire ecosystem.

Node Election and Voting Rules

Nodes who meet the sever configure standard and deposit more than required LTK can be candidate nodes.

All LTK holders have the right to vote the node candidates. The voting weight is related to the amount of LTKs held by voters, and eventually the nodes with the highest votes will be selected. In the voting rules, the members who own the OneThing Cloud can vote not only by LTK, but also with the OneThing Cloud, please refer to the details of voting campaign rule.
As the LinkChain is a dynamic developing ecosystem, the election rule may vary according to current situation. Please refer to the relevant contents about election and voting rules published on the official web site.

In the first election campaign, in order to ensure the smooth switch to the node election mode, several rounds of nodes recruitment will be carried out, a small number of nodes will be recruited in each round, and the validator pool will be formed together with the nodes from the foundation for a period.

After the debut validator pool runs for a period till it has been deemed as stable enough, secured enough and in high-speed, the next new election campaign will start, the nodes from the foundation will apply for it equally with other nodes and will no longer have the privilege of directly entering the validator pool.

Nodes entering the validator pool will be assessed in terms of the deposited LTK amount, the quality of produced blocks and random seeds, and the block producing nodes will be selected from the pool in a fixed term. Among them, the more deposited LTK the node puts, the higher chance it will be selected, and random seeds can ensure that the nodes with lower deposited LTK also have chance to produce new blocks.

Please refer to the first election campaign details on the official website.

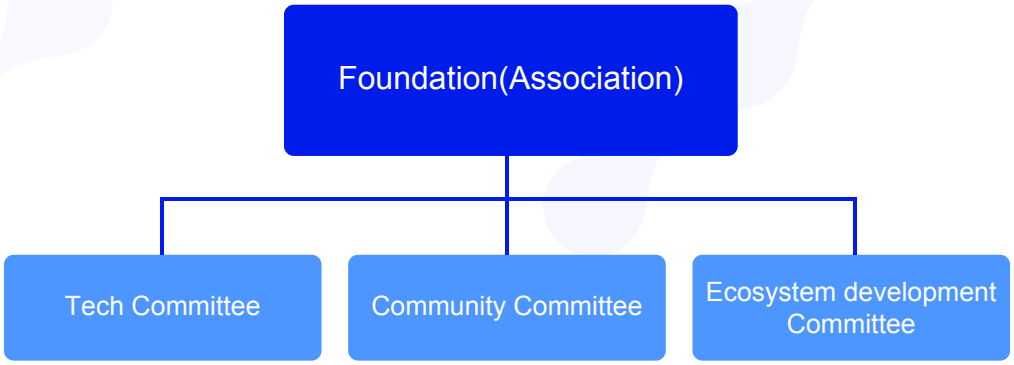
10.Community Governance

In blockchain world, we need not only the technology, the corresponding value method, but also the management system to make it self-evolving. In the autonomous system of LinkChain, the foundation/association (as the representative of LinkChain issuer) will undertake the construction of main network, technology upgrading and community incentive policy. DAPP developers and validator nodes will work as a special role in the LinkChain development in technological development and ecological prosperity, the vast number of LTK holders can also become a member of the community, or even as a member of the community management team to contribute to community governance and the construction of the LinkChain ecosystem.

Community management organizations will perform their duties and coordinate all resources, strive to the guide ecosystem development and community operation. LTK will work as the incentive function under the consensus mechanism of LinkChain, and become the bond between productivity and production relationship.

Assignment and Responsibility of management team

In order to maintain the ecosystem development and the stability of community order, and ensure the transparency in operation of the project and the token assets, the following organizational structures have been established in the system:



Foundation (Association): As the representative of project issuer, it undertakes the function of long-term scheduling and arbitration of major events, and provides incentives to nodes, developers and others who contribute to the ecosystem of the LinkChain.

Technology Committee: mainly to assist in technology optimization, technology construction and technological interation of LinkChain and DApps;

Community Committee: responsible for the daily management and operation of the community, to ensure the activity and regular operation of the community;

Ecosystem Development Committee: Responsible for proposals and actions related to ecosystem development, and guide its robust development.

Community Management and Development

Community management and development requires the participation of all members. In the autonomous system, different community membership reflects the participation rights in their own different community. Voting will be an important part of community management, which can be divided into three categories: community governance voting, election voting and evaluation voting. Different voting items will be controlled by different decision makers, so that the whole community can flourish in a game-filled environment.

In the design of the management system, the management members will obtain LTK incentives through their daily work. Each qualified member of the committee will receive a certain proportion of the LTK assets allocated by the Foundation. People or groups contributing to the LinkChain, whether they are developing, publicizing or investing, will be assessed by the community and matched with reasonable rewards.

We believe that there is no a complete system to deal with all the problems in the development of LinkChain. The community of LinkChain will develop continuously and needs self-evolving. Therefore, we believe that the community of LinkChain, which is composed of foundations, validator nodes and three committees, is similar to the legislature in the physical world and can continuously improve itself.

Due to the different functions among the three committees, the way in which the first members are selected, the change in members composition, the expansion and reduction of the size of the committee are also different. Rules of governing the committees and management details, as well as regulations of the community, will be published before the opening of the first community elections.

Thereafter, in the process of continuous development of the community, the scope of initiating events, the functions and so on will be discussed continuously with the nodes, developers and foundation through the three committees, constantly launching new proposals and constantly improving the rules. Foundations(associations) will also join in as voters. The LTK ecosystem will become more and more democratic, reasonable and practical.

11.Future – Trust Credit for All Information on Blockchain

Based on the high-performance consensus algorithm, privacy protection solution and multi-asset account model, a comprehensive index, trust credit, will be introduced in the future to measure the value and behavior credibility of users' contribution, which will help LinkChain become more practical in the decentralized organization, business, finance and public welfare scenarios, and make all behaviors, information and data based on blockchain credible then to enable a broad accepted indicators in all business.

Each user (The crypto address in LinkChain), including the validator node will be given a certain credit (Credit Value), which is used to measure the credibility of a user (whether the crypto address is attached to an ordinary person, a node or an enterprise), in the system, the higher the credit value, the higher the credibility.

The credit value of LinkChain is generated by the combination of on-chain and off-chain. It is a machine trust system with a higher form of institutional design. Such a system has higher productivity and economic vitality.

For example, in the future as LinkChain consensus algorithm improves, trust is defined as a mechanism that can significantly reduce the system' s entropy. Trusting a node is an optimistic way to reduce the uncertainty impact of the node in the system. The higher the credit value of the node, the lower its uncertainty, so the system composed of high credit value nodes will be more orderly and efficient.

When the credit value mechanism starts to run in the future, LinkChain will design a consensus algorithm based on credit value, which integrates credit accumulation mechanism, economic factors, cryptography and BFT fault-tolerant algorithm in on and off-chain scenarios, realizes a consensus mechanism with low latency, high throughput and strong consistency, and can identify and eliminate malicious or unsustainable nodes. That can improve the stability of the system, and encourage users to provide stable and reliable validator nodes. We call this algorithm PoCredit-EBFT.

In decentralized communities, as long as there are clear objectives, we still need an organization to undertake coordination: to organize personnel and implement plans in order to achieve a goal, in this process, we need to establish certain norms and evaluation and arbitration mechanisms for ownership, structure, operation, incentives and penalties. In the future, the decentralized community of LinkChain will also be included in the trust credit system. Through an effective credit system, the reputation or credibility of community members will be measured, thus greatly improving the credibility of the community operation process. Based on this, we can build a decentralized community that can develop and evolve healthily.

Economics research considers that the cost of trust is the biggest cost of economic activities, and the reason why enterprise organizations appear is that they can achieve a lot of and long-term trust relationship, reduce the cost of internal transactions to achieve profit. The scale of an enterprise will continue to expand until the cost of executing a transaction within the enterprise is greater than the cost of executing the transaction outside the company. The introduction of credit value system will help protect privacy and greatly reduce the cost of online transactions, so decentralized organizational, commercial and financial applications will become more feasible.

Via the credit value system, the business of on-chain and off-chain will be combined seamlessly as a complete system: users can improve their credit value and gain reputation and trust through the actions of goods supply, services, community contributions and public donations under the chain, ranking based on credit value will increase the chance of good users to be found, thus is to optimize the high-quality services from all users on the chain, thus is to promote users to improve the goods or services off the chain, or more contribute to the community, or avoid improper behavior, in order to obtain higher credit value.

The function of trust credit mainly includes the following aspects:

1. Establish a credit value system to make the business model in the ecosystem operate with low cost and high efficiency, promote anonymous transactions, and protect privacy on the basis of security and credibility.

2. The use of credit system can reduce the cost of search, contract signing and coordination, and practically support decentralized autonomous organizations or community service.

3. To develop decentralized financial services, community members can do credit verification, loan, investment and financing and risk management through the credit value system.

4. To evaluate the reliability of organizations and individuals, as well as projects initiated by them and information released by them.

From the micro point of view, credit system can reduce business costs and improve business efficiency; from the macro point of view, credit system can provide a reliable reference for all acts, data and information based on blockchain, thus reducing the cost of verifying the reliability of Internet information, so that everyone can simply, directly and accurately judge whether a piece of information in the massive network data is trustworthy or not.

12.Conclusion

With high-performance consensus mechanism and privacy protection solution, LinkChain supports multi-asset account model. Through credit value system, LinkChain system has implanted trust into software protocols and deployed it to the whole network, bringing a new public facility for innovative organizations, business and financial services industries.

On the LinkChain, any user can construct all kinds of services, maintain trust and privacy, and form an effective free competitive market. Hence, LinkChain has the ability to be applied in a wide range of scenarios, including decentralized autonomous organizations, exchanges, finance, business services and public welfare projects.

Thanks to LTK and the shared computing ecosystem behind it, the foundation will continue to invest the LTK from companies who acquires computing resources by LTK, and together with other application scenarios, continuously enhance the ecological value of LinkChain.

13.Roadmap

We believe that blockchain technology and LinkChain will bring the world with unprecedented possibilities and create a new era. To achieve this goal, we will make at least five major upgrades. With the expectation of exploring the infinite possibilities of the future, we name these five upgrades with five great navigators' names.

ZhengHe Upgrade

The test will be started at Sep. 2019, and the upgrade is to be officially launched within the month. It will Support UTXO account model and Account model, the first blockchain which supports both UTXO and Account model. Private LTK will be released, supporting private UTXO transactions, EVM and WASM dual virtual machine.

In this version, developers can issue non-privacy tokens, can develop decentralized crypto exchange built upon smart contracts which supports non-privacy to be exchanged with privacy LTK. Even though privacy LTK in this version will be the only privacy anchor token, the technology behind this has consolidate the basis that more privacy tokens can be created, and enable the capability of decentralized exchange.

On the other hand, when this upgrade is finished, EBFT consensus algorithm, validator nodes and candidate pool will be activated as well.

The consensus process will be handed over to validator nodes and candidate pool, and LinkChain will officially come in the stage of development by committees.

Christopher Columbus Upgrade

At the end of 2019, this upgrade will natively support multi-token in single account, which will support issuing privacy tokens by smart contracts. Each token issued on LinkChain can be changed to privacy UTXO format.

LinkChain will offer the fundamental service for private exchange, which empowers other tokens other than just LTK with privacy features. Developers will be able to create their own privacy tokens and also conduct the transactions between Privacy tokens and privacy token to privacy LTK via decentralized exchange.

Da Gama Upgrade

Will be released at Q1, 2020, which will realize cross-chain communication. Foundation/Association will select 1-2 Token from other projects like BTC, Eth, EOS etc. to have them fulfilled the cross-chain communication with LinkChain. That will be the samples in the ecosystem, and foundation will encourage other developers to finalize the cross-chain communication with other tokens, so as to support the private transaction for all tokens in the decentralized exchange.

Fernando de Magallanes Upgrade

It is expected to be released at Q2, 2020. It is to finalize the extensionality of LinkChain via homogenous chain structure or multi-layer structure, which will be a solid base for a massive concurrency from DApps.

James Cook Upgrade

It is expected to be released at Q4, 2020. This upgrade will build up the credit value system, where the community autonomous management and ecosystem development will be based on this credit value system, so as to open a credit era in internet industry.

Reference

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf

[2] BitcoinWiki. Proof of stake. https://en.bitcoin.it/wiki/Proof_of_Stake

[3] Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper

[4] Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. 1982, 4 (3): 382–401. doi:10.1145/357172.357176

[5] Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance and Proactive Recovery. ACM Transactions on Computer Systems (Association for Computing Machinery). 2002, 20 (4): 398–461. doi:10.1145/571637.571640: http://pmg.csail.mit.edu/papers/osdi99.pdf

[6] MONERO RESEARCH LABS: RING CONFIDENTIAL TRANSACTIONS: https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2015/1098&version=20151217:200440&file=1098.pdf

[7] Zerocoin Electric Coin Company. ZCash: All coins arecreated equal, 2017. https://z.cash.

[8] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich: Algorand: Scaling Byzantine Agreements for Cryptocurrencies: https://people.csail.mit.edu/nickolai/papers/gilad-algorand.pdf

[9] Ethan Buchman, Jae Kwon and Zarko Milosevic: The latest gossip on BFT consensus: https://arxiv.org/pdf/1807.04938

[10] Ethan Buchman: Tendermint: Byzantine Fault Tolerance in the Age of Blockchains: https://allquantor.at/blockchainbib/pdf/buchman2016tendermint.pdf

[11] Nicolas van Saberhagen: CryptoNote v2.0: https://cryptonote.org/whitepaper.pdf

[12] bulletproofs: https://crypto.stanford.edu/bulletproofs/

[13] Benedikt Bunz, Jonathan Bootle, Dan Boneh Andrew Poelstra, Pieter Wuille, and Greg Maxwell: Bulletproofs: Short Proofs for Confidential Transactions and More: https://eprint.iacr.org/2017/1066.pdf