White Book on Token Guard

June 5, 2018 v1.0

Contents

1. Introduction

According to the latest statistics, the most popular digital currency market on the basis of blockchain technology is now worth more than 100 billion dollars, including BTC, ETH and LTC and Ripple, formed in the context of global application and popularization of blockchain technology. Blockchain means a string of associated data blocks generated by cryptography, gathering all the information for BTC network transaction in a single time. These data blocks based on chain combine such powerful computation that the goal that "once confirmed, it is impossible to be altered" can be realized. Thus, blockchain becomes a new application mode of computer technology such as distributed data storage, point-to-point transmission, decentralized consensus mechanism and encryption algorithm. With the rapid development of blockchain technology, digital currency gradually appears, and a large number of digital currency transactions also lead to the industry engaged in developing digital wallets. According to the networking features of wallet use, we can divide the wallets into two types; hot wallet and cold wallet. The essential function of all digital currency wallets is to help users manage their secret key and address safely. There are many different kinds according to different functions. To facilitate bookkeeping and transactions, the official will often issue full-node wallets, such as Bitcoin Core and Parity Wallet. Third-party teams tend to develop some wallet services including digital currency wallets like Bitpie, imToken, CocoWallet, Bixin and Bibao to improve user experience or operation. These wallets do not synchronize all blockchain data, also known as light wallets. Both are called hot wallets. Besides these strong online wallets, there are some hardware wallets providing cold wallet services. Compared with hot wallets, hardware wallets enjoy a relatively higher security because the secret key is not exposed on the network. Common hardware wallets include Ledger Nano, Trezor wallet, and so on. After analysis of the wallets in the mainstream market, we found that there are various potential safety hazards whether in hot wallets or in other hardware wallets.

From the other aspect, since the birth of BTC nine years ago, thousands of competing coins have been developed successively, all of which have their respective strengths and characteristics including, but not limited to; transaction performance, capacity size, data privacy protection, regulatory compliance considerations, etc. Generally speaking, these coins have decentralized blockchains more or less, but these chains have their own data structures and unique ecological systems. However, the non-compatibility of the blockchains severely constrains the application of these blockchain systems. Cross-chain technology is the key to realizing value compatibility whether for public chains or private chains. It is the core linking scattered blockchains and is also a bridge for blockchains to expand and connect to the outside. The early cross-chain technology is represented by Ripple and BTC Relay, which pay more attention to assets transfer. Ripple proposed an alternative account book deviating from BTC consensus and created its own token, Ripple coin. It set up a differential agreement that is compliant with and able to accomodate all bookkeeping systems , thereby achieving a global payment standard. BTC Relay provided a solution from the angle of side chain, a new type of blockchain based on the principle of anchoring tokens in the original chain. A side chain aims at connecting a variety of chains. Other blockchains can exist independently. However, it is difficult to establish a cross-chain smart contract on a side chain, so the financial functions can not be achieved. This is also the fundamental reason why the existing blockchains have not yet made progress in stocks, bonds and derivatives. Token Wallet protects users' secret key and digital

assets based on proven security, and builds a secure and reliable storage and payment basis with the perfect protocols and architecture design. In addition, based on the extendable architecture of Token Wallet, the transaction and payment processes are not dependent on blockchain underlying technologies. Thus, we propose a set of cross-chain solutions different from traditional cross-chain technologies focusing on assets transfer. We pay more attention to the transfer of chain status and the design of smart contracts based on chain status.

2. Status of wallet apps

2.1 Potential safety hazards of existing wallets

In general conditions, blockchain technology is considered to be based on strict cryptography, so it is very safe. But a series of cases of huge losses in digital currency assets appeared.

On February 28, 2014, Mt. Gox, which ran the world's largest BTC exchange, announced that it suffered network attack on February 7, 2014, and it had to stop all BTC withdrawals for 850 thousand bitcoins on the trading platform (about 50 billion yuan at the current market price) were stolen, which caused a lot of trade chaos and user dissatisfaction.

On the morning of the August 3, 2016, Bitfinex, the largest US dollar bitcoin trading platform, announced that due to the security vulnerability of the website, users' bitcoins had been stolen, approximately 120 thousand bitcoins totally (about 6 billion yuan at the current market price), on its official website. This series of events led us to wonder whether the blockchain was really safe. In fact, all this reflects the most important link of network security in blockchain, that is, the security of digital currency wallet.

According to the recent analysis of some well-known wallets at home and abroad, Token team found that the first time many wallets ran, they would create a new account for users by default and store secret key files directly in the local system without encryption. Theoretically, an attacker could read the secret key files stored in the local system at any time.

We analyzed the current popular nearly 20 wallets and classified them into three types according to running types (according to the order of security from weak to strong); wallet with secret key and transaction trusted, wallet with secret key and transaction signature stored at app terminal, and wallet with secret key and transaction signature isolated from external network. Wherein, the wallet services with secret key and transaction trusted means our control right to the assets is fully trusted to the central server, so the security of the assets depends on the third-party server. Once the server that our secret key is trusted to has any internal management or technical problems, our assets will be in danger.

The wallet with secret key and transaction signature stored at app terminal, compared to the wallet with secret key and transaction trusted, enjoys much higher security, for all the right to use our funds. However, this type of wallet also shows a relatively higher risk. For example, in the case of unsafe operating environment at our app terminal or no corresponding detection of the current system version before some mobile phone wallets are used, an attacker can easily control system permissions, thus

posing a great threat to the secret key or mnemonic words stored on the mobile phones.

With secret key and transaction signature isolated from external network, the safety factor is highest compared with the previous two situations. However, there are still some risks in cases where some technical operations are not handled properly. For example, the improper settings of random number seeds that the secret key generation algorithms of many wallets rely on are extremely possibly exploited by an attacker. In addition, some weak mnemonic words also give an attacker an opportunity to restore the secret key. It's also easy to ignore that the method of counterfeiting signatures may be mastered by an attacker before using the signature function of your wallet, so your signature may be counterfeited ahead of the entry of transaction data into the wallet. At present, a large number of digital currency wallets in the market are uneven, some good and some bad. Wallet security is not well protected by many wallet products under the principle of priority to business. Due to the particularity of digital assets, once a large number of accounts are stolen for security problems, the stolen assets are hardly recoverable. So the security of digital wallets is crucial. Token team will give priority to wallet safety as the first principle to escort your digital assets.

2.2 Market analysis of hardware wallets

In fact, it was not a good choice to make a hardware wallet in the past, because the market was not mature and users did not pay enough attention to the security of digital assets. But with the recent well-jet development of digital currency and many safety events of digital assets, the solutions to asset security of blockchain have been recognized and accepted by the market and more and more users. At present, digital currency and even the blockchain industry are still in the early development stage, showing relatively small scale and immature technology. However, with the improvement of infrastructure and the landing of various apps of many industries, many apps are bound to penetrate every aspect of people's lives like the Internet. Thus, we are looking forward to a wallet that focuses on asset security and user experience, and the corresponding features will certainly be popular among the masses.

3. Technical design of Token Wallet

3.1 Security base of Token Wallet

3.1.1 Security of secret key generation and storage

In the blockchain network, the only proof for your digital assets is your secret key. Once the secret key is lost or disclosed, your digital assets will never be recovered. The above mentioned problem does not necessarily mean that blockchain is not safe, but that users should attach great importance to secret key protection. It is possible to say that the security protection of secret key is the cornerstone of credible blockchain. The secret key is stored in the user's computer with a file as the carrier or is trusted to a central server. The computer on which the secret key file is stored is often equipped with a large number of other apps. Once a computer faults or app vulnerability appears, it is possible that BTW will be lost whether the secret key is stored by the user or central server. Besides, the trusted secret key also faces the riak of the maintenance personnel of the central server. In these cases, there is higher possibility for BTC or ETH loss, and even direct loss of more than ten thousand coins. To realize absolute security of the secret key, we propose five necessary conditions in the

following. Only the hardware wallet we have designed satisfies the five conditions for the management of the secret key. We can thus conclude that our wallet is absolutely safe.

(1) The generating processes of the secret key and address are offline and the generated secret key must be non-reproducible and unpredictable.

(2) The storage of the secret key is independent, that is, the secret key is stored or used in an independent physical unit that does not depend on other hardware or platforms.

(3) The unit storing the secret key does not automatically communicate with other networked devices.

(4) The secret key conducts signature authentication signed for transactions that meet specific conditions, and the entire signature process is equivalent to a black box for the external systems of the outside world.

(5) The secret key can be safely backed up. The secret key can be safely restored once the physical carrier stored in the secret key is lost or unrecoverable physical faults appear. The first condition is the most important, for random number is the security basis of modern cryptography. The security of the whole system (i.e. the security of the secret key) depends entirely on the generation efficiency and quality of random number sequence. The core of high-quality random number is the “unpredictability”.

In our hardware wallet, the generation standard of our random number is four random number generation conditions that satisfy the cryptography security and are proposed by The Federal Office for Information Security: K1; the probability of the same sequence is very low. K2; it is consistent with statistical averages. For example, all numbers should have the same probability of occurrence, the chi-square test can be passed, ultra-long run-length is roughly very small, and the probability of occurrence of other figures with the same number should be equal. K3; the working status of the random number generator or the next random number should not be predicted according to a sequence. K4; the previous working status of the random number generator should not be predicted according to the status of the random number generator.

In our hardware design, we abandon the combination of "time stamp + a special set of IDs" as a seed. We believe that all pre-set random number seeds may give hackers a possibility to guess the seeds. We directly collect various real entropy sources in the hardware as sources of random number seeds. High-quality random number generation algorithms ensure that our secret key can not be predicted and reproduced by malicious means.

The second condition indicates that the secret key can not be stolen by hackers if the carrier for storing the secret key is independent and does not depend on any third-party hardware or platforms.

The third condition guarantees that the unit storing secret key will not automatically connect to the network, which is weaker than the second condition. Under normal circumstances, the external system will have no opportunity to intrude into the unit storing the secret key. When a secret key signature is required, the only channel to communicate with the outside is to enter the transaction information that needs to be

signed, and then the information after signature is output. Based on the security assumption in the present cryptography, the secret key can't be calculated only according to the signature information with limited computing resources.

The fourth condition is that on the one hand, the secret key authenticates signatures only for transaction information that satisfies a particular structure (not for any information constructed by the user), which can effectively resist the chosen plaintext attack, (this is a very harmful attack against ECC algorithm); on the other hand, the entire signature process is not exposed to the outside, that is to say, the direct information related to the secret key is not disclosed at the time of each signature.

The fifth condition is independent of the previous four conditions. It mainly solves the problem of how to recover the secret key (i.e. hardware storing the secret key is lost or a non-repairable failure appears). Token Wallet backs up the secret key mainly by specially adapted mnemonic words.

In the earliest mnemonic word design, since the secret key is 64-bit and completely unreadable, 64-bit secret key is converted into more than 10 common English words by some algorithms. These words are derived from a fixed word library, and then the secret key can be restored according to a certain algorithm. So the mnemonic word becomes another embodiment of your secret key. In the design of Token Wallet, our mnemonic word is not derived from any fixed word library, the structure of the word is entirely determined by the user. Theoretically, there should be words in infinite combinations.

3.1.2 Security of signature process

In 3.1.1, we introduce the security assurance of Token Wallet in generating and storing the secret key. However, the security risk of hardware wallet also appears when sending out information, i.e.ouputting the signature information at the time of signature calculation, because all input transaction information and output signature information are plain text at the time of signature and can be read by any two-dimensional code scanning software. If the secret key is read directly in memory at the time of signature calculation, the secret key will no longer be secure once the memory data is copied (the operation is extremely difficult). Thus, when designing relevant signature calculation, we replace the signature calculation method in which the secret key is directly used with a generated obfuscated order set. Specifically, when a secret key file is generated in Section 3.1.1, a static digital secret key expression is not generated directly but an order set of fully obfuscated codes. In the case of the secret key signature operation for a transaction hash the obfuscated order set is directly ran. The whole process is complete in the hardware chip. In theory, there is no possibility of disclosing the secret key, because even if an attacker gets the obfuscated order set, there is no way to find out what the specific secret key is.

3.2 Product workflow of Token Wallet

In this section, we briefly introduce the basic workflow of Token Wallet.

3.2.1 Account establishment of Token Wallet

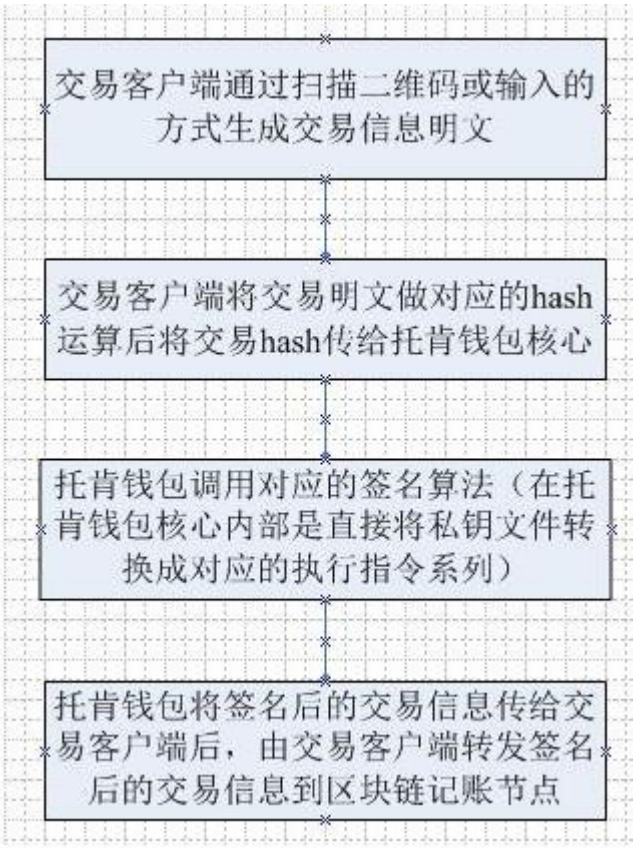
First, the account of Token Wallet is off-line. The corresponding button can be directly operated under the prompt of the hardware screen when establishing a new

account. Users can select the secret keys and addresses corresponding to the digital currency types they are using (such as BTC and ETH).

It is important to note that when the account is being established, users need to manually enter a 16-word mnemonic word. Although the system provides the way to quickly establish an account (in theory, the account is also in line with the security standard), it is highly recommended that the users should enter the mnemonic words by themselves, because the users can enter non-standard English words as their mnemonic words. Thus, theoretically, the users have unlimited choices for inputting mnemonic words, which can greatly improve the security of the secret key. Whether the address is quickly generated by the system or by users manually, it requires the users to replicate the corresponding mnemonic words on paper (in a securer environment), because the only way to restore the secret key and address is mnemonic words, once the hardware wallet is lost.

3.2.2 Transaction (Payment) initiating process of Token Wallet

Token Wallet mainly serves as a tool for secure storage and signature of the secret key and thus needs to be used in conjunction with PC-terminal software or mobile-terminal apps to complete the normal payment and transaction functions of digital currency. Here, we use the PC-terminal software to describe the whole transaction process. The whole transaction process in the mobile terminal is similar.



交易客户端通过扫描二维码或输入的方式生成交易信息明文	Transaction client generates transaction information plaintext by scanning two-dimensional code or inputting
交易客户端将交易明文做对应的 hash	Transaction client transfers the

运算后交交易 hash 传给托肯钱包核心	transaction hash to Token Wallet center after the corresponding hash operation for the plaintext.
托肯钱包调用对应的签名算法（在托肯钱包核心内部是直接将私钥文件转换成对应的执行指令系列）	Token Wallet invokes the corresponding signature algorithm (in Token Wallet center, directly converting the secret key file into the corresponding execution order series)
托肯钱包将签名后的交易信息传给交易客户端后，由交易客户端转发签名后的交易信息到区块链记账节点	After Token Wallet sends the transaction information with signature to the transaction client, the transaction client forwards the information to the blockchain bookkeeping node.

In the whole process, the transaction client software transfers data with Token Wallet through USB interface. After the transaction is complete, it is recommended that the USB connection between PC terminal with Token Wallet be suspended.

4. Cross-chain transaction based on Token Wallet

Token Wallet is designed to create a universal digital currency wallet and a universal digital currency trading system. The digital currency is now at the stage of a hundred battles. Each digital currency has its own trading model and ledger structure, and there is no direct compatibility mechanism for these digital currencies. Based on Token Wallet, we have developed a cross-chain technology called Token Chain. Token Chain is a cross-chain technology based on status transfer.

4.1 Communication protocol models for cross-chain transactions

The communication protocol between blockchains is similar to the traditional TCP/ IP protocols, which aim at establishing a reliable connection to transfer messages. A message is generally divided into header and data. The header records the source, destination, length and category of the message. During the message transfer, the header is peeled off layer by layer, and the corresponding modification will be made according to the requirements of the protocol. The message will eventually be sent to the destination according to the information indicated by the header. In the entire transfer process, the message shows its status. The sender can also know the status of the current communication and make the correct response according to the receiver's feedback.

Based on the analysis of the principles of TCP/ IP protocols, we have constructed a complete cross-chain communication protocol. It mainly consists of two parts; communication address and communication data. Communication address includes Chain ID of source chain or destination chain, and height of the current chain. Communication data includes srcChainID, dstChainID, Status and Data. Wherein, the data will not be unfolded during transfer.

跨链通信	Cross-chain communication
通信地址	Communication address
来源链	Source chain
链高度	Height
通信数据	Communication data
源链标识	srcChainID
目的链标识	dstChainID
数据状态	Status
数据	Data

The status of cross-chain communication data corresponds to the current communication status. When a cross-chain transaction is initiated, the communication status is “to be received”. When the receiver receives the message, the sender will be sent “successful sending”, and the receiver then sends back the status of successful receipt. This is the whole process of a successful cross-chain communication. In addition to the above status, we also provide some error status such as connection timeout. For example, when a transaction is made from the first chain to the second chain, a life cycle subject to the chain height shall be specified. Before reaching the life cycle, the link will send back the status of the communication result to the first subchain. If it exceeds the life cycle, the link will send back the status of connection timeout directly to the first subchain.

Similar to normal network communication, cross-chain communication may also be subject to cyber attacks, especially DDoS attacks. Therefore, a verification mechanism is neccessary to prevent attacks on the link through designing a complex communication verification mechanism. As mentioned earlier, the subchain is ready to send up-to-date block and up-to-date block voting to the link. When a transaction is sent from the subchain to the link, the height of the block in which the transaction is located is reflected in the communication address. We only need to find out if there is this transaction in the block height because it is possible to prove the authenticity of a block by submitting the up-to-date block and its voting. A block alone can not prove

the legality. According to an existing block, it is possible to forge a fake block that is illegal but is in line with the block structure, such as modifying part of the transaction information of block data and modifying the transaction hash value in the header. In the common blockchain consensus structure, it is often expected to go through two or more rounds of voting after a block is proposed, and will be temporarily stored in the last round as part of the block of the next round. Based on this, if the subchain submits a certain block and the voting information at once, we can prove that this block is credible in one round of block generating cycle. As a bridge between different subchains, our link also needs to be responsible for maintaining public status on the subchains.

Firstly, if the subchains wish to communicate with Token Link, registeration must be completed on Token Chain, which includes chainID, the information on the verification node, the asset category and the verification mechanism of the subchains, etc., in order to assist Token Chain in communication forwarding and verification operation.

Secondly, Token Chain needs to collect the latest information on the blocks from subchains in real time so as to maintain the basic status of each subchain and help light clients to verify transactions from subchains.

As a cross-chain technology, Token Chain has designed an independent consensus mechanism to realize basic inter-chain communication and verify the legality of the independent blocks on the subchains and the legality of inter-chain transactions.

4.2 Cross-chain consensus mechanism

4.2.1 Brief introduction of consensus mechanism in blockchains

Before determining the consensus mechanism for Token Chain, we briefly review some of the other consensus mechanisms used in the field of blockchain. Proof of Work (POW) consensus is one of the earliest consensus algorithms used in BTC and Ethereum. Since the issuance of BTC, POW algorithm has proved its reliability, but its waste of resources is also alarming. Proof of Stake (POS) mechanism is proposed to address the serious waste of resources in POW, in which the proportion of stake of voters in the voting pool replaces the computing power consumed during miners' mining and the corresponding punishment mechanism is adopted to ensure the integrity of voters. However, there is a very big difference between computing power and stake. By computing power, a miner is unlikely to mine on the two chains at the same time, but a voter with a certain stake may vote for every possible block. As long as any block becomes a future winner, it is possible to ensure that his stake is not damaged. But there is a significant potential safety hazard, as this can greatly reduce the cost of doing evil. Delegated Proof-of-Stake (DPOS) consensus mechanism is based on decoupling voting rights and bookkeeping rights. Its principle is to allow each person holding tokens to vote for several representatives, and we can understand these representatives as super-nodes. These super-nodes have totally the same rights. From a point of view, DPOS is a bit like a parliamentary system or the System of People's Congress. If a representative fails to perform his duties, he will be removed and a new super-node will be selected to replace him. But by DPOS, in which bookkeeping rights are generated by simulating human voting rights and behavior, there is a centralized tendency, and compared to POW, it is impossible to prevent cheating under DPOS in advance.

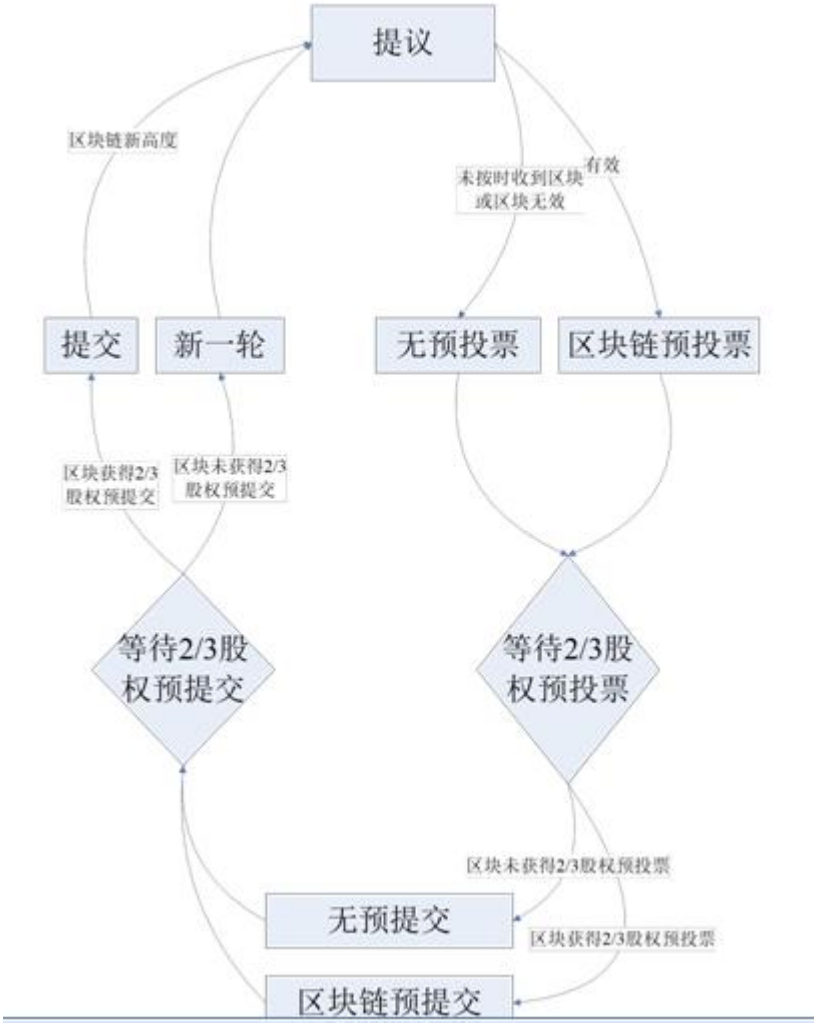
Raft, a consensus mechanism adopted by Ripple, is also a common high-efficient consensus algorithm in distributed field, but its biggest drawback is that the Byzantine fault node can not be prevented. A Byzantine leader node with powerful network configuration can bring destructive blows to the raft algorithm. In addition, the consensus mechanism widely used in the league chain is Practical Byzantine Fault Tolerance (PBFT) consensus, for example the IBM-based HyperLedger Fabric project adopts PBFT consensus. PBFT is an algorithm in which the back-up copy of a state machine is reproduced, that is, the service is modeled by a state machine and the state machine performs back-up copy replication on different nodes in the distributed system. The back-up copy of each state machine saves the service status and implements the service operation. The set of all back-up copies is represented by the capital letter R, and each back-up copy is represented by an integer from 0 to | R | 1. Assuming that there are f back-up copies that may become invalid in the system and | R | 3f1 is satisfied, the system can satisfy the eventual consistency.

4.2.2 Byzantine Fault Tolerance Mechanism for the agency stake of Token Chain

In Token Chain, our purpose is to carry out cross-chain transactions. The model is similar to that of league chain. The consensus mechanism based on PBFT is very popular in league chain, mainly because the network topology structure between nodes in league chain is relatively stable, with relatively low frequency of node entry and exit. It is undeniable that the Byzantine Node Fault Tolerance algorithm used in PBFT can guarantee the cyber security of less than 1/ 3 Byzantine nodes. However, in practice, especially when cross-chain transactions are relevant to economic benefits, even if the verifier is a selected reliable node, we can not simply rely on 1/ 3 of the security under the non-punishment mechanism. The reward and punishment must be directly linked to economic interests. Here, we have amended the original PBFT consensus mechanism so that the weight of the verifier's vote corresponds to that of his tokens on Token Chain.

As a result, the mechanism in which more than two-thirds of the voters are required in the original PBFT consensus algorithm to confirm the block generation has been modified to more than two-thirds of the total stake. In addition, in the PBFT consensus algorithm, ordinary nodes are only synchronized with new blocks from the leader nodes and are not involved in consensus. The security of PBFT depends solely on the number of verification nodes, so the increase in the number of ordinary nodes can not increase the security of Byzantine fault tolerance. As a result, we involve non-verified nodes in Token Chain's consensus mechanism. A verification node corresponds to a verifier's account, and a non-verifier can delegate his stake to the verifier, thereby authorizing the verifier to vote on behalf of his stake. Due to the introduction of interest-based relationship in Token Chain, non-verifiers will select their agents very carefully so that everyone can be involved in the consensus, but that does not result in any efficiency loss due to the involvement of all nodes.

Token Chain's consensus mechanism can be briefly represented by the following diagram



提议	Proposal
区块链新高度	New height of blockchain
未按时收到区块或区块无效	Failure to receive blocks on time or ineffective blocks.
有效	Effective
提交	Submit
新一轮	A new round
无预投票	No pre-voting
区块链预投票	Blockchain pre-voting
区块获得 2/3 股权预提交	Pre-submission with block obtaining 2/3 of the stake
区块未获得 2/3 股权预提交	Pre-submission with block not obtaining 2/3 of the stake
等待 2/3 股权预提交	Pre-submission waiting for 2/3 of the stake
等待 2/3 股权预投票	Pre-voting waiting for 2/3 of the stake
区块未获得 2/3 股权预投票	Pre-voting with block not obtaining 2/3 of the stake
区块获得 2/3 股权预投票	Pre-voting with block obtaining 2/3 of the

	stake
无预提交	Without pre-submission
区块链预提交	Blockchain pre-submission

In the consensus protocol of Token Chain, if the leader is an honest person, it can continuously promote consensus nodes to reach consensus on new transactions. However, if the leader is a malicious node, it may deliberately delay or discard messages from other honest nodes and slow down the protocol. In order to punish these malicious leader nodes, Token Chain will periodically change leader nodes through voting of Stake Commission. This can also prevent malicious nodes from delaying consensus in an indefinite period. In addition, based on PBFT consensus mechanism adopted by Token Chain, we can easily create light wallet nodes. In ordinary blockchain clients, transaction verification requires synchronization of all the block data in the blockchains. Such clients are powerful, but too many data to be stored lead to a great deal of redundancy. As Token Chain adopts a PBFT algorithm based on verifiers' voting, our client only needs real-time synchronization of the latest verification members on a blockchain and then verifies the information on the blockchain. In order to follow up and verify the latest block height and world status on the blockchain, the light client only needs continuous synchronization of the header on a blockchain and to update verifiers' information.

4.3 Privacy Protection of Token Chain

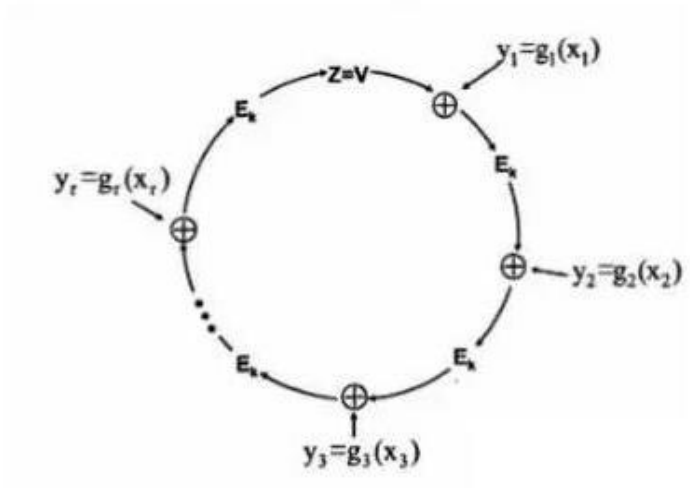
There has always been a strong demand for Privacy in blockchain systems. Especially for cross-chain structures, privacy protection is particularly important. If we only secure blockchain transactions but avoid talking about privacy, it provides no significance for security protection. How can privacy be protected under the premise of security protection?

At present, privacy solutions in the field of blockchain mainly include the following;

Coin Shuffle Scheme; This is also originated from Coin Shuffle services based on early BTC or ETH, and later used in Monero. Its purpose is to allow each address to be mixed with other addresses in a blender. In the transactions that come out of the coin mixer, no one except the mixer knows whom the coin is transferred to. It is a scheme for direct storage and processing of encrypted data. It is used in some league chains more widely. Only the participants of a transaction can decrypt the data. The scheme is relatively reliable and privacy can be rigorously proved by cryptography, but the drawback is that verification nodes can not be verified.

Zero-knowledge proof; It is a very powerful tool in modern cryptography. In the zero-knowledge proof algorithm, the party with private information can let the verifier confirm the proof party's information without revealing its private information. But the non-interactive zero-knowledge proof technique based on ZK-Snark has demonstrated efficiency problems in the industry. At present, it takes about 90 seconds to create a zero-knowledge proof based on ZK-Snark on an ordinary computer. In addition, it is difficult for ZK-Snark-based algorithm to dynamically create security verification parameters because of its poor ductility. Some security parameters must be set in advance. This may also cause some problems in practice.

Ring signature scheme; This scheme meets an unconditionally anonymous requirement. The signer can freely specify its anonymous range. An external attacker may not be able to determine the real signer, even if he illegally obtains all possible secret keys of the signer. It is obvious that the ring signature scheme realizes privacy protection through anonymity. Based on the analysis of the above mainstream privacy solutions, as well as the actual demand of cross-chain, Token Chain adopts ring signature scheme to protect the privacy of transactions. Ring signature is a signature scheme characterized by a fuzzy signature of a signer. You don't need to create a ring in the ring signature, nor do you need to assign a specified key. You can not override the anonymity of the signer, unless the signer wants himself to be exposed. In the ring signature scheme, the signer selects a temporary signer set first, which includes the signer himself. Then the signer uses his secret key and the public key of other persons in the signer set to independently generate a signature without others' help. A ring signature does not have a trusted center. For the verifier, the signer is entirely anonymous. The ring signature provides an ingenious way of anonymous disclosure. The unconditional anonymity of the ring signature is very useful in some special circumstances that require long-term protection of information.



The ring signature consists of the following parts:

(1) Key generation. Create a key pair (public key PKi and secret key SKi) for each member of the ring.

(2) Signature. Th signer uses his secret key and the public key of any n ring members (including himself) to generate signature a for message m.

(3) Signature verification. The verifier validates whether the signature is signed by the ring member according to the ring signature a and message m. If it is valid, it will be received. Otherwise, it will be discarded.

At the same time, the ring signature must meet the following features:

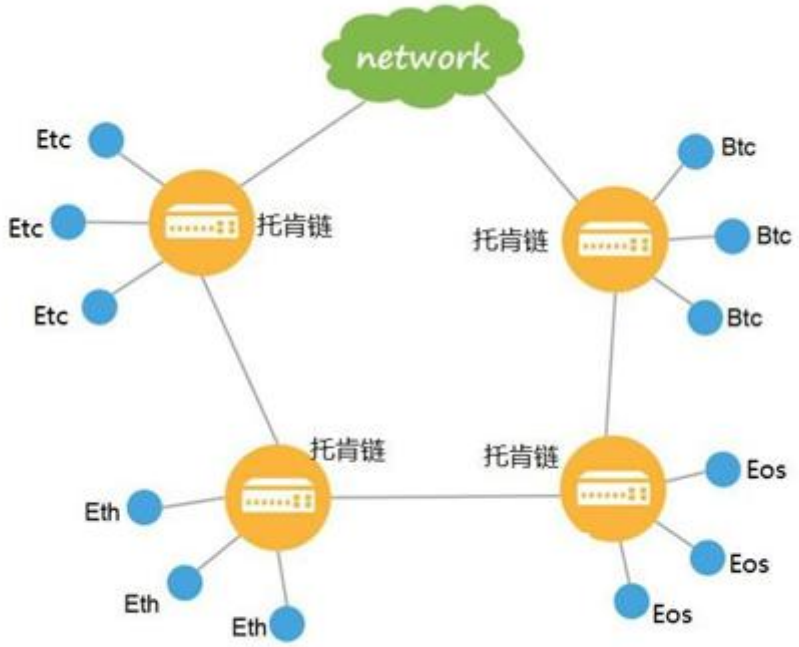
(1) Unconditional anonymity. An attacker can not determine which member of the ring generates the signature. Even if the secret key of a ring member is stolen, the probability is no greater than 1/ n.

(2) Correctness: Signature must be verified by all others.

(3) Unforgeability: Other members of the ring can't forge a signature of the real signer. An external attacker can't forge a signature for message m even if he obtains a valid ring signature.

4.4 Smart contracts based on Token Chain

We believe that with the rise of digital currency, the process of payment contracts is greatly accelerated. With blockchain as the infrastructure of the internet, smart contracts help enhance the perfect unity of credit guarantee, payment settlement and incentive mechanism. The asset owners and workers in Token Chain, or members of Token Chain, collaborate with each other based on P2P. They participate in the construction of secure payment channels of the entire system based on the standard no-difference smart contracts. In addition, each member obtains the corresponding reward on the basis of its contribution to constructing secure payment channels in the entire system. The biggest feature and advantage of smart contracts are that the trust problem is solved by technology. Before a traditional contract is reached, participants must know the credit background of the parties and select proper guarantee contracts in advance of the payment. The resources on Token Chain are real and transparent. The contract will not be changed once it is determined, and its execution is not dependent on any additional operation. The smart contract based on Token Chain has one more aspect of meaning than that of regular blockchains, that is, cross-asset property. Since Token Chain itself realizes the universal digital currency transactions and payment system based on cross-chain technology, more application properties appear in the cross-chain transaction. For example, we can allow users to verify BTC transaction in Ethereum, so as to make purchases in multiple currencies.



托肯链	Token Chain

5. Payment data model based on Token Wallet

5.1 Payment data model

By creating a universal digital currency payment ecology, Token Chain will accumulate a large number of data related to digital currency payment and consumption over the long run. From the perspective of future data currency payment, Token Chain will change the payment habits of consumers by big data on payment. In general, digital currency payment based on blockchain technology is quite different from traditional payment in many respects; the basis for blockchain payment is decentralized technology. It is no longer necessary for both transaction parties to rely on a central system for capital clearing and all transaction information storage, but rely on a consensus mechanism that does not require trust coordination directly for the value transfer. With the development of blockchain payment, the blockchain distributed ledger technology connects the digital asset flow on the blockchain with the real payment. The blockchain payment is very similar to Alipay's wallet functionally, but because of its establishment on the decentralized p2p network infrastructure, beyond the limits of the country and region, it possibly plays an irreplaceable role in the high-efficiency and low-cost value transfer in the global internet market compared with traditional financial institutions. Based on Token Wallet, we developed a self-financing platform that can be used for P2P payment, deposit, transfer, exchange, loan and so on.

6. Issuance and incentive

6.1 TKGN Token

As a typical project based on blockchain, Token Chain is a new distributed autonomous economic organization. The return of investment is not allocated according to the corporate equity investment mode. Investing in Token Wallet does not mean buying the company's equity but buying a universal security tool for digital currency. Token Chain builds a distributed, credible asset trading and payment platform based on cross-chain technology, and it also has a local token, called TKGN.

TKGN is the only stake token of Token Ecology, and TKGN is a permit for holders to vote, verify or delegate to other verifiers like ETH of Ethereum. In addition, TKGN can also be used to pay transaction fees to reduce data redundancy. Additional inflation TKGN and block transaction fees are awarded as a reward for verifiers and clients. Any person or group can obtain TKGN in accordance with the same rules. TKGN can be obtained by purchase or by completion of system tasks. The Price of TKGN is determined by market.

6.2 Issuance quantity

At the preliminary stage of the project, 590 million TKGN tokens will be issued, 220 million of which are issued for circulation and the rest of which is shown in the following table in details:

Issuance quantity (100 million)	Description of issuance purpose
0.455	Investment in institutions with certain resources
0.59	Community node rewards and subsidies (divided into three years)
0.885	Community and promotional incentives
0.295	Public charity (divided into five years)

0.885	Team awards (divided into three years)
0.59	Security technology and investment reserve, and income fed back to token holders.

Token Chain has imposed strict restrictions on the additional issuance of TKGN. Only if the following conditions are met, will additional issuance be conducted according to certain rules. After the project has more than 50000 users of hardware wallet and accesses to decentralized wallet exchange for development, no more than 0.08 billion TKGN tokens will be issued additionally in order to support the ecology and application. After the project completes the hardware wallet exchange project and enters the digital assets payment system ecology and application, no more than 0.08 billion TKGN tokens will be issued additionally according to the project progress in each of the two years. After the project completes the asset payment system and enters the application fields of big data and consumption, no more than 0.08 billion TKGN tokens will be issued additionally according to the project progress in each of the two years.

The total issuance of TKGN shall not exceed 990 million.

6.3 Upper limit of verifiers

Different from POW blockchain like BTC, Token Chain may have slower speed because of increased communication complexity and verifiers. Fortunately, we can support enough verifiers to realize a globally robust distributed blockchain, making it possible to have shorter transaction verification time. In addition, more verifiers will be involved in the future with enhanced bandwidth, memory and parallel computing power. On the day of the creation of the foundation block, the number of verifiers was set to 100 at most and the growth rate for the later decade would be 13% and the number of verifiers will eventually reach 300.

6.4 Punishment against verifiers

Certain punishment mechanism should be set up against verifiers to prevent them from intentionally or accidentally deviating from the approved protocol. Some evidence may be immediately adopted, such as double signature at the same height and in the same round, and violation of "pre-voting lock-up", which will result in losses of good reputation of the verifiers and their TKGN tokens as well as their proportion of tokens in the reserve pool. Sometimes due to regional network interruption, power failure or other reasons, the verifiers are unable to connect. If the number of votes submitted by the verifiers in the blockchain does not exceed the limit in the block at past time points, the verifiers' activities will be terminated and they will suffer from certain punishment in terms of their rights and interests for their overtime.

7. Founding team and consultants

Token Chain's founding members all are senior experts in global chip, security and blockchain finance and are experienced engineers in software engineering.

Name or nickname	Post	Experience

Robert	CEO	Founder of Token Guard. Core patent holder of Token Guard Chip, senior security expert, security consultant of several international banks, and investor of early BTC. Participated in the design and guidance of key security projects of several international banks on many ocassions.
Cao Yunbo	CTO	PhD from University of Washington, Chinese-American expert. Research direction; distributed computing, blockchain finance, big data and artificial intelligence. Presided over in person and participated in several national projects and research projects at the University of Washington.
Jason	CPO	Senior software development engineer. Master in Software Engineering of the Ivy League. Has worked in many well-known international software enterprises with rich experience in software products development, and keen on blockchain technology.
Fusion	Architect	Senior system architect, with a Masters from the University of Electronic Science and Technology of China. Served as a senior architect in a well-known internet company. Rich experience in highly concurrent services and reliable service architecture. Keen on research on open source technology. Has an in-depth research and a unique insight into the technology of blockchain projects such as BTC and Ethereum.

8. Remarks

This white paper only provides an overview of the core parts of Token Wallet and Token Chain technologies. Technology is endless. Token Chain will create a collaborative, open and innovative technical ecosystem. Token team also welcomes the world's outstanding developers to join the Token family and promote the technical progress of Token Ecology.