Whitecoin Technical Whitepaper

A Decentralized Blockchain For Multi-chain Ecosystem

TABLE OF CONTENTS

1. Content Summary 4

1.1 Explanation of terms 5

1.2 Document Declaration 5

1.3 Disclaimer 5

2. The Project Background 7

2.1 Development trend of blockchain industry 7

2.2 History of Whitecoin 8

3. Properties of Whitecoin 10

3.1 Interconnection of cross-chain 10

3.2 100% reserve ratio 10

3.3 Efficiency 10

3.4 Smart contracts 12

3.5 Flexible transaction fee 13

4. Random Proof of Stake（RPOS） 14

4.1 Participants 14

4.2 Whitecoin mining and assets deposit mechanism 15

4.3 Whitecoin RPOS Competitive Algorithm 16

4.4 Incentives mechanism 18

4.5 Security of the RPOS consensus mechanism 20

5. Community governance 22

5.1 Selection of Wallfacer 22

5.2 Obligations and rights of Wallfacer 22

5.3 Proposal of switching Wallfacer 23

5.4 The penalty mechanism of the Wallfacer 24

5.5 Advantages of community governance 24

6. Cross-Chain 26

6.1 Realization of Cross-chain 26

6.1.1 Multi Tunnel Blockchain Communication Protocol（MTBCP） 26

6.1.2 Whitecoin Axis 27

6.1.3 Whitecoin Wallet 27

6.1.4 Smart contract 27

6.1.5 Lightning network 30

6.2 Cross-chain operation process 31

6.2.1 Initialization process 31

6.2.2 Account creation 32

6.2.3 Cross-chain recharge process 33

6.2.4 Cross-chain withdrawal process 36

6.3 Safety of side chain assets 38

6.3.1 Fund dynamic balance strategy 38

6.3.2 Capital dynamic balance period 39

7. Technical feature and innovation 39

7.1 Contracts and virtual machines 39

7.3 Consensus random number generator 43

7.4 Events and callbacks 44

7.5 Local query interface 45

7.6 Asset block link into model 45

8. Project development plan 47

8.1 Wallfacer Project 47

8.2 Threatening Project 47

8.3 Staircase Project 47

8.4 Black domain Project 48

9. Conclusion 48

10. References 49

1. Content Summary

Whitecoin is a public chain that interconnects inter-block values through the innovative Multi Tunnel Blockchain Communication Protocal (MTBCP). The Whitecoin ecosystem uses the Random Proof of Stake（RPOS）consensus, Whitecoin Axis, Whitecoin Wallet, decentralized pool and smart contract platform to build a cross-chain blockchain ecological system.

High performance features of Whitecoin:

- Blockchain asset management

It realizes the cross-chain circulation between the existing blockchains (BTC, LTC, BCH, ETH, EOS, ERC20, OMNI, etc.) and the multi-asset management of the chain.

- Turing complete smart contract

Supporting complex digital asset business through Turing complete smart contracts, such as OTC on the chain, asset certification, etc.

- The underlying virtual machine

The blockchain underlying virtual machine of Whitecoin ,supports SDK and RPC interfaces of multiple development languages, providing the foundation for constructing a multi-asset distributed business application ecosystem.

Whitecoin's main chain assets is XWC. XWC holders can enjoy services and share ecological benefits by co-constructing the ecology. Other public chains such as BTC, LTC, BCH, ETH, EOS, ERC20, OMNI can also pass The Multi Tunnel Blockchain Communication Protocal（MTBCP）enters the Whitecoin ecosystem, opening up barriers between blockchains and creating a new blockchain world for interoperability.

1.1 Explanation of terms

Whitecoin: Whitecoin (XWC) is a decentralized global blockchain with five years of history.

XWC: XWC refers to the asset token on the Whitecoin chain.

MTBCP (Multi Tunnel Blockchain Communication Protocal) : Whitecoin's innovative peer-to-peer communication protocol for supporting cross-chain information transmission.

WAMP (Whitecoin Anchored Multi-properties): Refers to other asset chain digital assets anchored on Whitecoin. For example: WBTC refers to the anchored bitcoin asset on Whitecoin.

Miner: Refers to the group that Whitecoin is competing for in the billing rights.

1.2 Document Declaration

For the convenience of explanation, the use of Bitcoin BTC and Litecoin LTC for example does not mean that the project only supports the cross-chain of BTC and LTC. This project supports the cross-chain circulation of most digital assets on the market and in the future.

1.3 Disclaimer

This Whitecoin technical white paper is for reference use only. We do not guarantee the accuracy or conclusion of this white paper. This white paper is provided on a factual basis. We make no warranties, express, implied, statutory or otherwise, including but not limited to:

- Marketability, fitness for a particular purpose, suitability, use;
- there is no error in the content of this white paper;

- Such content does not infringe the rights of third parties.

We and its affiliates do not constitute any form of damages for the use, reference or reliance on this white paper or any content contained herein, even if it is told that such damage may occur. In no case shall any person, or its affiliates, be liable for any direct or indirect damages, losses, liabilities, costs or expenses, consequential, compensatory, contingent, practical, exemplary, punitive or specific use, reference or reliance on this white paper or any content contained herein, including but not limited to any business loss, income, profit, data, use, goodwill or other loss of intangible assets.

2. The Project Background

2.1 Development trend of blockchain industry

In 2008, Satoshi Nakamoto published the Bitcoin White Paper "Bitcoin: A Peer-to-Peer Electronic Cash System" that brings the blockchain to the public. Since then, more and more developers have joined the ranks of developing and promoting blockchains, constantly innovating blockchain technology and supporting a wider range of application scenarios. In the 10 years since the birth of Bitcoin, industry practitioners have continuously explored more technical solutions and more application scenarios in the blockchain. The blockchain also experienced a point-to-point payment from the 1.0 era to the 2.0 era of the smart contract and evolved towards the 3.0 era.

In the era of blockchain 2.0, the development of Ethereum enriched blockchain ecology tremendously, and it has produced many public chain projects with different application directions and outstanding value. However, the richness of the public chain ecology has also brought new problems. At present, the information and value between the major blockchains cannot be circulated freely, and objectively form block islands, which greatly limit the application value of the blockchain. Compared with the network effect of the Internet value, the isolation of the blockchain public chain greatly restricts the network value of the blockchain. Therefore, the interoperability of blockchain will be an important solution to the value of blockchain, and cross-chain technology is the key to realize the value interconnection of blockchain.

Large numbers of pioneers are exploring blockchain, and some projects attempt to solve cross-chain problems through different paths such as notary schemes, sidechains (relays), hash-locking, and distributed private key controls. Whitecoin will create a public chain that can connect the value interconnection between different chains in a trusted way, integrate existing blockchain resources, and create a new world of blockchain.

2.2 History of Whitecoin

Whitecoin was born in April 2014 and is a blockchain digital asset with more than 5 years of history. Whitecoin has gone through two historical stages and is about to enter the third stage.

2.2.1 Phase I: April 2014 - April 2017 (POS 1.0 Phase)

In 2014, the Whitecoin Creation Zone was born, an initial POW distributed mechanism was used migrating to POS once the initial distribution period was concluded. The project token XWC also successfully landed on world-renowned exchanges such as Bittrex, Poloniex and Cryptopia, and attracted the attention of global digital currency investors.

2.2.2 Phase II: April 2017-2019 September (POS 3.0 Phase)

With the continuous innovation of blockchain technology, the Whitecoin development team prepared for a comprehensive upgrade of the project in 2016. In April 2017, Whitecoin completed a new upgrade from the outdated POS 1.0 mechanism to POS3.0. The upgraded Whitecoin team successfully launched the Whitenode mining machine,

Whitecoin hardware wallet, Whitecoin blockchain mobile phone, XWCdice, XWCpoker, XWCmall and other ecological applications based on the decentralized community governance mechanism. The project token was successfully launched on more than 20 industry head exchanges such as ZB.COM and XT.COM. At the same time, XWC also became one of the first 78 currencies in the Weiss Ratings.

2.2.3 Phase III: August 2019 - Future (RPOS Phase)

With the rapid development of the blockchain industry, Whitecoin's original technical architecture and community development organization were unable to keep up with the development of the blockchain. In the second half of 2018, the community began to upgrade Whitecoin.

After nearly a year of preparation, Whitecoin chose to solve the industry's pain points from the basic level, and the crosschain became the final direction of the project. At the same time, in order to create the value of the Whitecoin public chain, the community core developers will also change from the original part-time mode to the full-time development mode.

The new Whitecoin project will integrate the community's original development advantages, ecological advantages, community advantages, and partner advantages to launch a new era of projects.

3. Properties of Whitecoin

3.1 Interconnection of cross-chain

Multi Tunnel Blockchain Communication Protocal(MTBCP) achieved interconnection of different block chains. With the existence of cross-chains，the following improvements which hugely effects the ecosystem were made ：

- Realize Interconnection in cross-chain.
- Establish a cross-chain ecosystem by breaking the barrier between different block chains.
- Provide better extensions and value sharing of block chain.
- Improve the implementation of block chain for internet facilities.

3.2 100% reserve ratio

To ensure the safety and stability of the Whitecoin ecosystem，the reserve ratio of Whitecoin has been kept at 100%. Each WAMP possesses a real original chain asset (such as BTC, ETH, etc). All assets are placed into hot or cold mutli-signature address which are managed by RPOS consensus mechanism. Increasing or decreasing of each asset corresponds to user's each deposit or withdraw, which guarantees no asset will be added or removed without reason on the Whitecoin network.

3.3 Efficiency

According to the RPOS consensus mechanism, the parent chain of Withecoin produces a block every 6 seconds，while it takes BTC 10 minutes and LTC 2.5 minutes to produce one block. When compared to the performance of BTC and LTC, Whitecoin's transaction speed is significantly improved. Transaction of BTC or LTC using parent chain of

Whitecoin are supposed to be 100 times faster than on which of BTC and 25 times faster than which of LTC。

Theoretical TPS (transaction per second) of Whitecoin reaches 10,000, which is enough to carry high-load transactions on multiple chains.

$$\text{tps} = \min\left(\frac{\text{blocksize}}{transaction_{maxsize} * block_{interval}} . \frac{\text{networkspeed}}{\text{transaction_max_size}}\right)$$
$$= \min\left(\frac{2457600000}{2048 * 6} . \frac{100 * 1024 * 1024}{2048}\right) = 51200$$

The performance of Whitecoin and several other block chain

Blockchain	Block time	Size of block	Theoretical TPS
Whitecoin	6s	20M	10,000
BTC	10min	4M	28
ETH	17s	No upper limit (800 million gas)	22
EOS	1.5s	No upper limit	Millions
NEO	20s	No upper limit	1000

Whitecoin has a significant improvement in production rate, block size and theoretical TPS when comparing to BTC, ETH and EOS. With the block time of 6 seconds and theoretical TPS of 10,000, high-frequency and high capacity services can be achieved.

The super nodes of EOS require high stability of internet connection. The block producing mechanism of EOS uses 21 super nodes to produce blocks in order. This could be traceable which puts it under the risk of DNS fraud and DDOS attacks.

However Whitecoin does not require such stable internet connection or high-performance servers. It has better adaption and compatibility when compared to EOS. The producer of Whitecoin blocks are selected from all existing Miners randomly. In this

way, there is high uncertainty for selecting the nodes, which makes it almost invisible on internet and not as easily to be attacked as EOS.

3.4 Smart contracts

With Turing Complete smart contracts, Whitecoin users are able to process flexible and complex services and such as financial contracts.

Without editing the original code of block chain, developers can use limited and controllable dynamic extensible applications such as building Token contracts, trading contracts, lock contracts and all kinds of DAPP contracts

- Limited Controllable

In according to smart contract standard, users can develop programs with pre-defined functions.

- Dynamic Extension

Dynamic extension means these is no modification to the original chain or hard fork needed. When the service environment is changed, users can easily adapt to new service situation by modifying the smart contract. For example; for logic changed to a limit order, to apply other limit order logic, to set the minimum order size to 100 tokens, or to set up limit time trading only need to modify code in the start of contracts.

- Native API

Each time a smart contract is executed on the Whitecoin block chain, a standalone lightweight execution environment is initialized by executing the corresponding contract byte code on the chain. When accessing data on the chain, the native API can also be utilized.

- Standalone storage

Each smart contract has its own independent state stored as 'storage'. When an exaction on smart contract leading to change in storage data, it won't backup the whole historical storage data, but backup part of data which related to current stage and change value of the "storage".

For example, a package includes an array which consisted of 1, 2, 3. It is changed to "1, 2, 3, 4", and then to '1, 2'. "Storage" only records previous array "1, 2" and the change values of 2 times (add 4 into array and remove "3, 4").

With such settings, users are able to obtain expected result of smart contract easily by invoking the previous value of "storage" without reading the historical data which greatly reduce the workload and data storage required by a node. Beside, it saves system resources and improves working efficiency of system. User can also restore or roll back the historical change value of the "storage".

3.5 Flexible transaction fee

Whitecoin block chain can charge transaction fee in both XWC and WAMP payment, which allow user who hold either XWC or WAMP is able to trade without concern about transaction fee.

Transaction fee of Whitecoin is not always at the same ratio, but fluctuations related to market price. When price of Whitecoin changes, the amount of WAMP for transaction fee will also changes.

4. Random Proof of Stake（RPOS）

Whitecoin uses a RPOS (Random Proof of Stake) as decentralized consensus algorithm. RPOS is a stochastic multi-asset equity deposit consensus algorithm, which defines participants, incentive structure and community operation system.

4.1 Participants

4.1.1 Roles in community

Decentralized consensus algorithm defines there are four roles of participants:

- Citizen
- Miner
- Wallfacer
- Swordholder

4.1.2 Relationships among different roles

Flowing Whitecoin community level, participants of Whitecoin has relations below：

- Citizen: Citizens can upgrade to Candidate when they possess a certain amount of XWC
- Miner: A Miner can become Wallfacer by providing an assets deposit which could also be assisted by other users.
- Wallfacer: To become a Wallfacer must provide a responsible reserve deposit and Node votes.
- Swordholder: It's part of Wallfacer, responsible for price feed at whitecoin chain.

4.1.3 Rights and responsibility for roles

Citizen： All users on Whitecoin block chain or other chain interconnected with white coin.

Miner: A Miner, producer and manager of the community, is responsible for validating transactions and block generation. A Wallfacer is also a miner in a decentralized pool.

Wallfacer: Wallfacer is an asset manager and community administrator in the ecosystem. Wallfacer is responsible for managing deposit assets.

Swordholder: A Swordholder is the core role of Whitecoin community. Swordholder have all functions same as Wallfacer, and also for price feeding.

4.2 Whitecoin mining and assets deposit mechanism

Whitecoin community provides different models for bonus sharing for miners in community. Either as citizen or as Miner, a user has possibility to gain bonus for a standalone block from after deposit assets on the Whitecoin network.

RPOS(Random Proof of Stake) provide advanced protection to make sure miners' profits and stabilizing of participants of the community.

Miner can get mining bonus through asset deposit.

Wallfacer and Swordholder can get bonus through block generation, meanwhile distribute interests following predefined diposit asset weightiness of other participants. RPOS realize the distribution of interests.

Advantage of deposit mechanism:

- Deposit mining and its rewards is verified by the all nodes on network. In this mechanism, rewards are distributed in real time. Miners who accepted assets deposit will get the get bonus automatically after a block is generated. This is different from centralized pools which have many unstable factors.
- POS pools demand users transmit digital assets to mining nodes, while for whitecoin

blockchain only deposit the assets, but keep the private key is held by the user. Without asset transferring to Miners, there will be no security problem and users can recall their asset anytime.

4.3 Whitecoin RPOS Competitive Algorithm

The algorithm and mechanism of whitecoin Block chain generation and rightness distribution is defined by RPOS.

- **Basic requirements for Node ledger:**

The basic condition for Miners to compete for accounting rights is the assets deposit, which includes XWC and all WAMPs. The more they deposit, the higher weight they get.

- **Mechanism for block generation:**

RPOS relies on chain random numbers to randomly select Miners based on the weight of assets deposit at the beginning of each round of consensus reached.

- **Rules of selection of Miner for block generation:**

Whenever the number of blocks is an integer multiple of 25, flowing process will be entered: Price Feeding, Election, Block Generation, Confirmation:

1. **Price Feed:**

Price feed refers to the Swordholder calculating price ratio of all WAMP: XWC based on the real-time price in the exchange, and then feed price separately. The role of the feed price is to provide competitive block generation weight of Miners by all Swordholders' participation.

The final result of the feeding processes the highest and lowest values of all Swordholders' feeds are excluded, the return the remaining averages.

2. Block Generation

The RPOS consensus algorithm accurately generates on block every 6 seconds。At any point in time there is only one authorized producer to generate the block. If a block is not generate within the specified time, the producer of this block will be skipped who will be replaced by the next Miner. There will be a delay more than 10 seconds if one or more Miner failed to generate a block.

3. Confirmation

Usually the Whitecoin blockchain has 100% Miner account participation, and a whitecoin original transaction is considered to be confirmed by an average of 3 seconds from the start of the broadcast.

To avoid special situations, such as software bugs, network congestion, and a malicious Wallfacer account which creates two or more forks, and to ensure a transaction is absolutely irreversible, a Miner needs to wait for confirmations from 17 blocks. Based on software configuration of whitecoin, it takes an average of 85 seconds.

In each round all Miners will assume that this block is irreversible after 17 out of 25 producers' confirmation by default. No matter how long the block is, the block generation will not switch to another fork to this without this block. Under circumstance of 100% participation rate，It is usually recommended to delay the block for users.

The advantages of the RPOS competition mechanism:

- Significantly saves system resources and reduces energy waste.

Compared with the POW algorithm, Withecoin chain blocks are generated in order by Miners who are selected randomly. Therefore, Miners on Withecoin chain only need to

keep accounts without wasting energy to find the hash value.

- Avoid forks

The Miners on the Whitecoin chain generates blocks in cooperation rather than competition.

- The randomness of node selection increases the security of the Whitecoin ecosystem

Miners on Withecoin chain are selected randomly, and constantly replaced. Even with the same Miner for different round, the order for block generation will be different. In this way, Miners are hard to find by attacker, which guarantees the security of the Whitecoin ecosystem.

- Increased the security of assets of Withecoin users

Compared with the POS and DPOS mechanisms, whitecoin is more safe. The private key is held by user and could be retrieved anytime which guarantees the security of assets and the flexibility of mining. Users can deposit assets to Miners to share mining rewards, and they can also withdraw the asset at any time.

4.4 Incentives mechanism

- Citizen

A Whitecoin Citizen obtains rewards from contract withdrawal transaction fee (side chain asset). Usually each reward occurs every 100,000 blocks. Rewards are allocated according to the amount of XWCs user held .

Citizens can also get a block reward by becoming a Miner or by deposit assets. After 24 hours price publicity period, they will become a Miner.

- Miner

In the RPOS consensus mechanism, users get a block reward by becoming a Miner or by deposit assets. Citizens spend a certain amount of XWC to register to become Miner, and put assets into deposit. Then they could attract other users to participate in their deposit from the community, and ultimately rely on the RPOS consensus competition billing rights, becoming a Miner to participant in block generation and receive the reward. Miner (with support Citizens) share block rewards and a proportional bonus of contract withdrawal transaction fees.

Miners supporters share deposit reward which is equally divided by the weight of the deposit assets.

To ensure Miner can always be able to package online, not only incentives needed but also punitive measures. When a Miner missed more than 5 blocks in a row, the consensus of block chain will decrease the chance of Miner's participation. Thereby, the possibility the node is selected to generate block will be reduced.

- Wallfacer & Swordholders

All Wallfacer and Swordholders split 20% of the block rewards and 20% of the contract withdrawal transaction fees.

- Foundation

Foundation gets 30% block reward.

Three kinds of incentives of whitecoin:

- Block Reward
- Block transaction fee (including normal transaction fee and contract transaction fee), the fee is charged and rewarded in XWC) 。

- Contract withdrawal fee in the block could be different kind of assets, XWC and WAMP (such as WBTC, WLTC). The transaction fee charges 1/10000 which determined and modified by consensus of Wallfacer. 20% of contract withdraw fee is received by Wallfacer., and the rest is divided equally by all users based on the amount of XWC they hold.

User rights comparison table:

	Citizen	Miner	Wallfacer	Swordholder	Remark
Wallfacer Registration fee	None	None	None	None	Destructed directly on the chain
Normal transaction fee	None	Yes	Yes	None	Type of fee is XWC
Block reward	None	Yes	Yes	Yes	Regular XWC reward
Contract transaction fee	None	Yes	Yes	None	Type of fee is XWC
Contract withdrawal transaction fee (sidechain assets)	Yes	Yes	Yes	Yes	Types of fee are XWC and WAMP (XWC/WLTC/WBTC)

4.5 Security of the RPOS consensus mechanism

RPOS possess a very high level security system to guard against various malicious attacks and emergencies, to ensure safety of network and assets.

If anyone of Miner works properly, block generation on XWC network will not be effected. As long as there is a Miner online, it can continuously produce 25 blocks. Even in such extreme anomaly, relying on incentives of the block, it can get through to the next round. Under normal circumstances if a Miner failed to generate block 5 times continuously, RPOS consensus algorithm will decrease participation rate of the Miner. Participation rate will reduce Miner's deposit assets by coefficient, which calculates Miner’s final deposit:

XWC Amount = XWC amount deposit by user * participation rate (0-100%)

Therefore, with the operation of the XWC network, eventually all Miner will be qualified nodes.

- Two different blocks generated at the same time by malicious Miner

At the end of a block generation round, to avoid double spend attack, whitecoin will be switched to a longer chain when 2 different chains were generated by a malicious Miner. In this situation, 17 confirmations are need to avoid double spend attack.

- Double spend attack when mining pool possess assets less than 51%

Even if a mining pool possesses large amount of assets on blockchain, there is no guarantee that more than 50% of nodes will be occupied in each round. Therefore, based on confirmations from 17 blocks required, it is difficult to commit a double spend attack.

- Double spend attack when mining pool possess assets more than 51%

In extreme cases, when mining pool possesses more than 51% assets, the mining pool is likely to cause data rollback problems on the chain. Since assets on block chain consists of not only XWC but also lots of WAMP whose cross-chain controlled by Wallfacer. If mining pool lunched a joint attack, it will take risk of being punished by community votes. The risk it takes will be greater than benefit.

5. Community governance

For long-term development and ecological construction of the main chain, the blockchain must have a set of governance mechanisms

Bitcoin relies on the bitcoin developer community and miners to coordinate updates. However the process is quite slow and the contradiction between the community and miners on the scalability problem directly led to the fork of bitcoin. After solving the problem hacker the DAO caused, ETH were divided into two forks, ETH and ETC.

Given the community experience of mainstream digital currencies in history, a better design of community governance has always been a topic of the blockchain world. Whitecoin owns a well-designed community governance mechanism. The governors of whitecoin consist of Miners, Wallfacers and Swordholders. They collaborate to manage cross-chain assets and participate in the establishing and revising community rules.

5.1 Selection of Wallfacer

To become a Wallfacer, user must deposit a minimum liability deposit which set by the Foundation. The minimum asset threshold at start is 10,000,000 XWC. The number of Wallfacer on block chain is fixed to 15.

15 initial Wallfacer will be selected by foundation from users who are in standard safe environment and hold most amount of coins.

5.2 Obligations and rights of Wallfacer

- Wallfacers are involved in management of block chain, including revising Whitecoin consensus of basic parameters, consensus of transaction fees, and consensus of Wallfacers' basic deposition amount and consensus of additional deposition amount

for newly introduced asset chain.

- Cross-chain assets are managed by Wallfacers. Wallfacer manages cross-chain assets by creating a cold and hot multi-signature wallet on the asset chain. Withdraw of cross-chain assets can only be achieved when more than 2/3 Wallfacer reach consensus.
- Wallfacers shares corresponding proportional income of withdrawal transaction fee of contract and 5% mining reward.
- If assets are lost on the chain in accident, such as loss in hot wallet, Wallfacers will pay for the loss.

5.3 Proposal of switching Wallfacer

- **Wallfacer addition proposal:**

Wallfacer addition proposal can be put forward by anyone of previous Swordholder. After confirmed by more than 2/3 Wallfacer, the proposal for this candidate to be Wallfacer will be officially raised.

The official proposal is voted by Miner who's voting weight decided by the assets they deposit in proportion. The proposal will be approved after receiving more than 2/3 Miner consensus votes.

- **Wallfacer resignation proposal**

The Wallfacer resignation proposal is raised by a previous Wallfacer. After receiving confirmations from more than 2/3 Wallfacer, the proposal will be approved.

- **Request to switch Wallfacer**

Each Wallfacer switching request requires a minimum interval of 25,000 blocks. Each

request will unconditionally reset the interval.

The number of Wallfacer to be switched must less than 1/5 of the number of current Wallfacers.

Any change of Wallfacer must take effect after 10,000 blocks.

Changes related to switch Wallfacer must be completed within 10,000 blocks

After proposals to add or discarded a Wallfacer taking effects, the corresponding multi-signature wallet must be rebuilt. Besides, the consensus must be broadcasted on Whitecoin chain. The assets in the original wallet need to be transferred to the new multi-signature wallet with the consensus of the original Wallfacers. The old address will be discarded after 20,000 blocks. Before the old address is discarded, any deposition to the address will still reach the account. After assets in the old cold and hot multi-signature wallet are changed the entry for new wallet will be triggered.

5.4 The penalty mechanism of the Wallfacer

In extreme cases, when there is a loss of assets in the system, the Wallfacers liability deposit will be used as compensation.

5.5 Advantages of community governance

Wallfacer manages assets and communities through consensus. Miners voted for the replacement of Wallfacer through consensus. The interests of both are the same however restrained mutually, which guarantees the security and stability of entire Whitecoin network

The entire Whitecoin network is governed by 15 Wallfacer who are qualified nodes through consensus, which greatly ensures the efficiency of decision-making.

Wallfacers' interests are closely related to the community interests. Wallfacers can achieve stable rewards consistently from the Whitecoin ecosystem. Besides there is a high threshold for becoming a Wallfacer on the Whitecoin chain (a considerable amount of asset deposit), Wallfacers' liability deposit will be used as compensation in the event of an asset loss.

6. Cross-Chain

6.1 Realization of Cross-chain

Whitecoin takes the lead in innovative Multi Tunnel Blockchain Communication Protocal(MTBCP), Whitecoin Axis, Wallet, smart contracts and other blockchain technology and realized the interconnection among blockchains, which is laying the foundation for complex distributed commercial applications.

6.1.1 Multi Tunnel Blockchain Communication Protocol （MTBCP)

Multi Tunnel Blockchain Communication Protocal is whitecoin's original communication protocol for point-to-point information transmission among blockchains.

When a user creates an account in Whitecoin, Whitecoin generates a corresponding tunnel account based on the Multi Tunnel Blockchain Communication Protocal and binds it to the whitecoin account. When a cross-chain transaction occurs, the corresponding data is encapsulated and packaged securely through the Blockchain Multi Tunnel Protocol.

The tunnel account generated by the Multi Tunnel Blockchain Communication Protocal is used to help whitecoin confirm the unique correspondence of the transferred assets.

Multi Tunnel Blockchain Communication Protocol only recognizes assets which commit cross-chained transaction through tunnel account, and issues or destroys the corresponding WAMP asset tokens based on consensus, and issue or destroy corresponding WAMP asset tokens according to the consensus.

6.1.2 Whitecoin Axis

Whitecoin Axis is an essential part of Withecoin to realize cross chain. As a multi-asset decentralized ledger, Whitecoin Axis is responsible for recording, verifying, broadcasting cross-chain data, generating and destroying corresponding WIOU tokens, and completing the transfer of cross-chain assets. In Whitecoin Axis, network security is ensured through Wallfacers' consensus. The binding relationship between the Whitecoin accounts and the corresponding tunnel accounts is verified by Wallfacers. Cross-chain transactions for each asset are also verified by Wallfacers to ensure that each asset chain is consistent with Whitecoin Axis.

6.1.3 Whitecoin Wallet

Whitecoin wallet is the client-side of Whitecoin. Whitecoin Wallet is responsible for generating the corresponding data within the whitecoin ecosystem. By registering Whitecoin account through Whitecoin Wallet, users are able to become a role in the ecological system and participate in ecological construction; for example, mining, cross-chain trading etc, to obtain the ecological benefits.

6.1.4 Smart contract

With smart contracts, Whitecoin users are able to achieve complex cross-chain transactions, asset certification, etc, which lays the foundation for building cross-chain distributed business applications in the whitecoin ecosystem.

Trading behaviors such as multi-asset pending orders are achieved through smart contracts on Whitecoin chain. Following points are included:

- Pending purchase order functionality rules

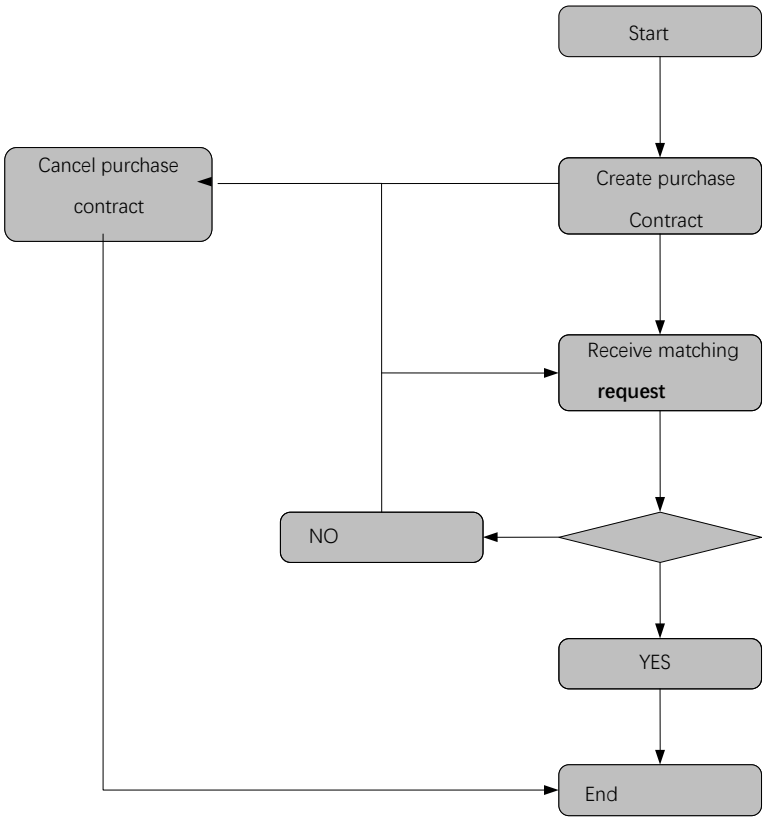
When creating a pending purchase order by implementing a smart contract, a pending purchase order is a new smart contract.

Pending orders are able to be partially filled.

Pending purchase orders are able to be cancelled.

The matching and cancelling of pending purchase order are contract transactions of smart contract.

Transaction fees are needed for buying pending orders, matching pending orders, and cancelling purchases.



- Smart contract template

The pending order is executed by smart contract, and the user can flexibly formulate the pending order logic. Each new pending order is a new smart contract.

Use smart contracts to make pending orders and matching instead of directly implementing in bottom layer which is more scalable for complex pending orders, for example, discount for one-time transactions or limitation of minimum transaction unit.

Since most of the pending order logic is basically the same normally, to avoid keep sending smart contract bytecode, it is allowed to pre-register the contract bytecode as contract template. Each contract template has a unique address on the chain. Contract template address and creator address can be used instead of send contract bytecode which is user-friendly and also saves storage space on the chain.

Fully abstract template, which significantly reduce the threshold for contract

Multi-asset trading on the chain will not be matched on the chain. If a user sends a buy or sell pending order on the chain, other users will actively match the corresponding order to complete the transaction.

- Transaction fee rules

Transaction fees are needed for activities including Transfer of assets, creating contract, calling contract, creating contract template, Initiate a pending order purchase transaction, cancelling a pending order purchase transaction and matching purchase transaction

Users can initiate a fee acceptance pending order to purchase WIOU with XWC which can be used to matching transaction fee exchange with arrayed price.

When a user initiates a transaction, XWC and also other assets can be paid as transaction fee, corresponding transaction fee acceptance pending orders will be matched.

Transaction fee acceptance pending orders cannot be cancelled anytime. After a cancel request is initiated, if the order is not matched with any other user through a round of block generation, the order can be cancelled. Otherwise the request of cancelling order will turn to invalid and user must choose whether to cancel the order again or not.

- Transaction fee type

The minimum charge for all kind of fees is 0.00001 system tokens (0.00001 may be modified by consensus).

Type	amount	Address
Transfer Transaction Fee	Basic Transaction Fee（XWC）	System Transaction Fee Address
Contract Creating Fee	Basic Transaction Fee（XWC）	System Transaction Fee Address
Contract Template Creating Fee	Basic Transaction Fee（XWC）	System Transaction Fee Address
Basic Contract Creating Fee	Basic Transaction Fee（XWC）	System Transaction Fee Address
Contract Assets Deposition Fee	Contract Calling Fee（XWC）	System Transaction Fee Address
Contract Assets Withdraw Fee	A certain percentage of the assets withdrawn (multiple assets) (not collected by the contract creator) + contract calling fee (XWC)	A certain percentage of contract withdrawals enters the asset reward pool, Contract calling fee to enter system Transaction fee address
Others	Basic Transaction Fee（XWC）	System Transaction Fee Address

6.1.5 Lightning network

Lightning Network is a decentralized system that supports instant, large-scale micropayments and removes the risks caused by transferring funds to a trusted third party.

Whitecoin Lightning Network greatly expands network scalability. Through the innovative technologies through MTBCP, Whitecoin Axis, Wallet, Smart Contract, Whitecoin has opened up barriers between different blockchains, realized the value interconnection between blockchains, and laid the foundation for the realization of complex distributed commercial applications between the block chains.

The funds of the Whitecoin Lightning Network are placed in a both sides multi-signature address called the "channel". In order to spend money from the channel, both parties must reach a consensus on the balance. The current balance is stored as the latest transaction indicated by the two parties from the channel address. The current balance is stored as the latest transaction signed by the two parties from the channel address. When payment is required, both parties sign a new exit transaction from the channel address. All the old exit transactions will do the same.

Lightning network does not require permission from the other party when exiting the channel. Any party can choose to unilaterally close the channel to end their relationship. Since each party has multiple multi-signature channels on the XWC network, each party can send payment operations to any other party through the network.

6.2 Cross-chain operation process

6.2.1 Initialization process

- Initialize Whitecoin for initial asset allocation and basic parameter configuration.

- Wallfacer on Whitecoin creates a multi-signature account on the BTC, LTC and other asset chains through consensus, and the address of the multi-signature account is signed by all Wallfacer and broadcasted to Whitecoin.
- The liability deposit required by each Wallfacer Recharge Foundation is used to maintain the stability of the chain.

6.2.2 Account creation

To complete the cross-chain transfer, Citizens need to create a Whitecoin account on Wallet. Wallet will provide a tunnel account creation option and bind to the Whitecoin account.

In this way, when the asset chain (such as BTC) recharges to the multi-signature account, Whitecoin will issue the same amount of WAMP to the bound Whitecoin account after confirmation.

When the entire Whitecoin is initialized or a new Wallfacer joins the Whitecoin network, a multi-signature account needs to be created or updated in the asset chain (BTC, LTC, etc.).

Account types include:

- Whitecoin account

Users first need to create a Whitecoin account to store and trade multiple assets on Whitecoin, including WAMP, XWC, and more.

- Tunnel account

When a user creates an account in Whitecoin, Whitecoin generates a corresponding tunnel account based on the tunneling protocol and binds it to the Whitecoin account.

The daily free quota of the Whitecoin account for the tunnel account is 10,000 (approximately 10,000 can be revised with Consensus), and the Wallfacer is required to exceed the limit.

- Hot and cold multi-signature account

Cross-chain assets will be stored in hot and cold multi-signature accounts on various asset chains created and managed by Wallfacer consensus.

6.2.3 Cross-chain recharge process

Besides the Whitecoin account, Whitecoin Citizen also has several bonded tunnel accounts. Through the light wallet component of other asset chains included in Whitecoin, users can recharge from other asset chain addresses or from centralized exchanges to Whitecoin accounts. Bind the tunnel account address.

The Miner on Whitecoin detects the recharge address of the associated multi-signature. After receiving the transfer, after waiting for the number of blocks to reach a certain confirmed height, find the associated Whitecoin account according to the source address of the recharge, and agree to this account on Whitecoin. The corresponding WAMP of the address (for example, WBTC/WLTC, etc.). Whitecoin WAMP (such as WBTC/WLTC, etc.) defaults to frozen assets (m blocks), waiting for the number of Whitecoin blocks to reach a certain height (such as m+6 Block), the new consensus generated WAMP (WBTC/WLTC, etc.) assets are changed from frozen to Available status.

Deposit on Whitecoin is divided into the following sections:

- The user deposit to the tunnel account bound to the Whitecoin account.

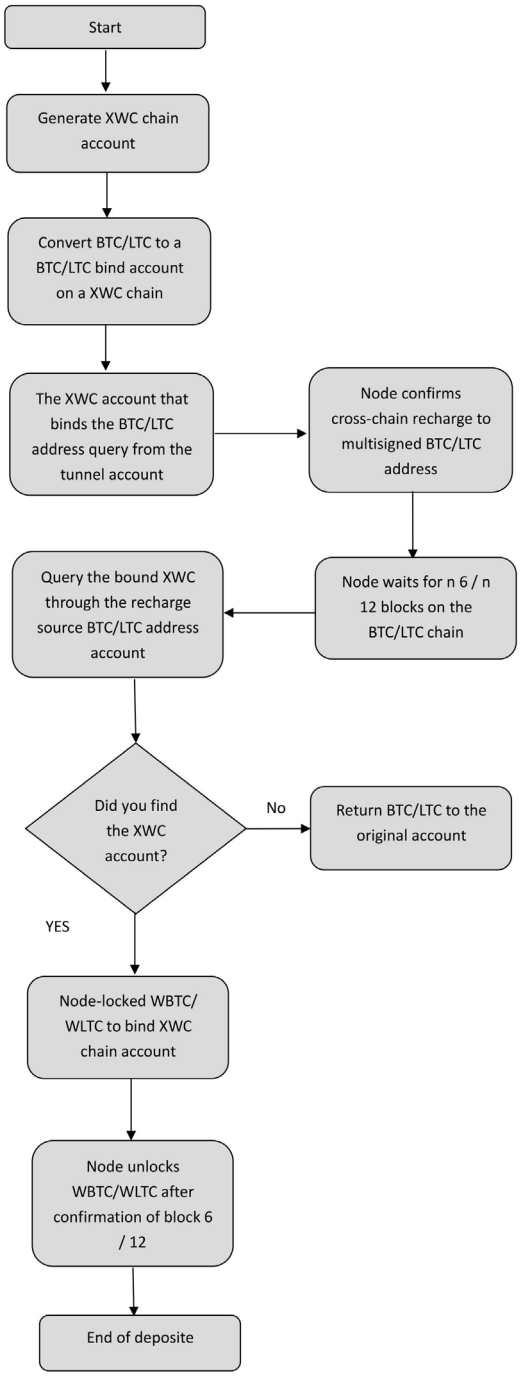
This transaction confirmation depends on the confirmation time on the original asset chain. For example, the BTC delays 6 blocks for confirmation, the LTC delays 12 blocks for confirmation.

- Transfer from the tunnel account to the multi-signature address managed by the Wallfacer consensus.

This transaction confirmation also depends on the confirmation time on the original asset chain, such as BTC delay 6 block confirmation, LTC delay 12 block confirmation.

- The Miner on Whitecoin generates a corresponding WAMP for the user on Whitecoin through consensus, and waits for the block on Whitecoin to delay 17 blocks and confirm.

The Underlying operation flow chart for cross-chain deposit is as follows:



In practice, XWC Wallet will simplify the majority of the process in human-computer interaction, and users only need simple steps to complete cross-chain recharge.

6.2.4 Cross-chain withdrawal process

- The user initiates a withdrawal transaction, which includes the withdrawal address of other asset chains.
- After the Wallfacer receives the withdrawal transaction request, they need signature verification, and broadcasts it on the network, and collects the signature of other Wallfacers on the transaction.
- When it is the turn of a Miner to block out, it is judged whether the signature of Wallfacer is less than 2/3 currently collected. If the condition is met, the transaction and all collected signatures are packaged into the block, otherwise the transaction will not be packed into the block, handled by the latter Miner
- After the transaction is packaged into blocks, the corresponding WAMP (such as WBTC, WLTC, etc.) owned by the user will destroyed.
- After the Wallfacer is verified, judge whether the balance of the multi-signature hot wallet is sufficient, and then perform the withdrawal process.

If the balance is sufficient, the signature of the hot and cold multi-signature wallet managed by Wallfacer to the withdrawal of the address will be issued on this asset chain, and the withdrawal will be completed after the multiple signature conditions are met.

If the balance is insufficient, the assets are extracted from the multi-signature cold wallet to the multi-signature hot wallet. After the assets in the hot wallet are sufficient, the Miner maker initiates the transfer process.

After the user request a withdrawal on Whitecoin chain, Cross-chain withdrawal is divided into two steps:

Step 1: waiting for the Miner account to be packaged (average 3 seconds).

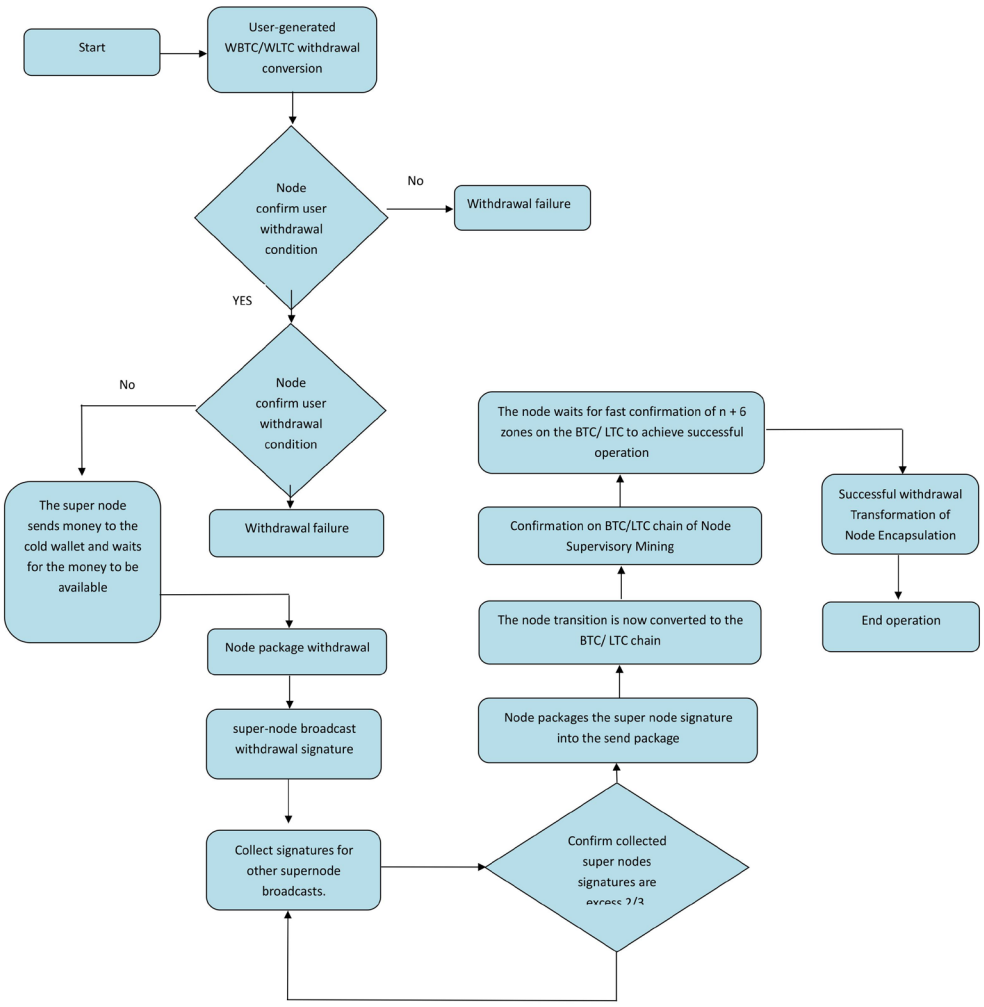
Step 2: waiting for with no less than 2/3 Wallfacer account signature for the withdrawal request.

If more than one-third of the Wallfacer accounts do not approve the request, the transaction is void.

If received the signature of Wallfacer is no less than 2/3, Wallfacer will generate a corresponding asset chain transaction, which will be confirmed by the corresponding asset chain (wait for the corresponding block Number), Whitecoin's Miner Packer completes the transaction and completes the transaction when the transaction is approved by Whitecoin.

The specific technical implementation process is as follows: after the user initiates the withdrawal request, the Miner maker initiates the corresponding original transaction from the multi-signature address transfer to the user target address, and the original transaction is packaged into src_trx and broadcasted to Whitecoin. After Wallfacer synchronizes to src_trx and then verifies, the signature of src_trx is wrapped into sig_trx broadcast and billed to Whitecoin. When the entire network collects enough Wallfacer signatures, Miners package the collected signatures to generate a complete withdrawal transaction, and then call the corresponding asset chain in the corresponding asset chain light wallet component built into Whitecoin Wallet transaction broadcast interface, broadcast to the network of the corresponding asset chain.

The underlying operation flow chart for cross-chain cash withdrawal is as follows:



6.3 Safety of side chain assets

6.3.1 Fund dynamic balance strategy

Whitecoin supports multi-signature hot and cold wallet fund dynamic balance

If the hot wallet multi-signature account asset exceeds 3 times the limit, a fund dynamic balancing process is initiated to transfer the assets in the multi-signature hot wallet address to the multi-signature cold wallet address.

Implementation plan:

- A Wallfacer initiates a fund dynamic balancing process, and the other Wallfacers are notified after packaging on the chain.
- Other Wallfacer will verify, after the verification is successful, the signature transaction will be broadcast, and then packaged by Miner to Whitecoin.
- When Miner Collector collects the signature of Wallfacer who is not less than 2/3, package the transaction and confirm the transaction of the original chain corresponding to WAMP.
- Finally broadcast to the original chain to complete the fund dynamic balance process.

6.3.2 Capital dynamic balance period

The Whitecoin chain will perform a fund dynamic balancing process for every 10,000 blocks, and adjust the total assets of the multi-signature hot wallet to the set range according to the assets of the multi-signature hot wallet.

The above-mentioned fund dynamic balance transaction is additionally signed by the Wallfacer with no less than 2/3 signature comfirmation after the basic transaction broadcast is created by the block's Miner.

7. Technical feature and innovation

7.1 Contracts and virtual machines

A bytecode specification that is well-formed and custom designed for blockchain smart contracts is used as an implementation specification for smart contract virtual machines. A compiler implementation that provides static-type high-level programming languages such as C#, Java, TypeScript, etc., generates smart contract bytecode from a high-level language.

- Smart Contract Virtual Machine:

The smart contract virtual machine is implemented as a Turing-complete bytecode virtual machine, which is deterministic at runtime, performs logic controllability, and can be monitored for state changes.

- Smart Contract Language:

A subset of the main features of popular programming languages, such as C#, Java, and TypeScript, are used as high-level programming languages for smart contracts, compiled into bytecodes that conforms to the smart contract bytecode specification, and used as smart contracts.

- Built-in library of smart contracts:

Smart contracts provide basic libraries for common numerical operations, string manipulation, and some built-in libraries for queries such as chain queries, transactions, etc., and can be called in smart contracts.

- Mutual call of smart contracts:

After the smart contract deployed on the chain, in addition to being directly invoked or accessed by the user, other smart contracts/built-in native contracts can be called or invoked by other smart contracts.

Part of the functional logic can be implemented in a smart contract and deployed on the chain, as a third-party library used by other smart contracts in the chain to function as an extended blockchain.

- The function limits of smart contracts:

Smart contracts can be written in Turing's complete programming language. They can query the data on the chain, can deterministically access the state of the contract, can call other smart contracts/native contracts, and can output return information to the caller. Restriction: Unable to read out-of-chain data; cannot generate logic that is inconsistent for each node; the number of execution instructions and the amount of memory used are controlled by the blockchain; the blockchain can terminate the execution of smart contracts at any time, such as in contract execution. When the cost is over budget.

- State storage of smart contracts:

Each smart contract has a separate state storage space called Storage. Storage's format is an unstructured data structure. The storage of smart contracts in the chain stores changes, rather than storing the latest storage to the chain each time. For example, in a contract call, change the contract storage from {"name": "chain" } to { "name": "chain", "count": 123 }, only the changed part of the chain { "count": 123 }, and even if the contract calls the fee, the storage part charge only calculates the size of the changed part rather than the size of the full storage. Therefore, even if the state storage space of a smart contract is large, as long as the amount of change generated by each contract is small, the data increment and gas fee on the chain are not high.

- Status inquiry of smart contracts:

The smart contract can directly query part of the value of the Storage of this contract, or can extract part of the data in the nested data structure through the SQL-like programming language. When the storage of the smart contract is large, the data load

can be reduced in this way to improve the query speed, avoid the full table scan, and improve the performance limit of the data access part of the smart contract.

For example: the storage structure of a smart contract like

```
{
 "name": "blockchain",
 "userBalances": [
   { "userAddress": "a", "amount": 10000, "freeze": false },
   { "userAddress": "b", "amount": 20000, "freeze": true },
   { "userAddress": "c", "amount": 30000, "freeze": false },
   ..... ]
}
```

You can use the SQL-like syntax like var freezedUsers = storage.query("select userBalance.userAddress from userBalances as userBalance where freeze=true") to query out all the user addresses of the frozen account in this smart contract, and the amount of data read and write is greatly reduced. And avoid the full table scan, which can meet the business scenarios of storing more data in smart contracts but not much reading each time, such as implementing simple push exchanges in smart contracts, realizing smart contract assets, realizing contract insurance, etc..

- The life cycle of smart contracts:

1. Generate smart contract bytecode files by high-level programming language or by manually constructing bytecodes

2. Deploy smart contract bytecode to the blockchain, you can create it as a smart contract, or you can create it as a smart contract template for the next time you create a contract.

3. Call the smart contract API or transfer money to the smart contract address

4. Each time the blockchain calls a smart contract, it first initializes an independent lightweight smart contract sandbox execution environment, loads the smart contract and executes it.

5. After executing the smart contract, save the execution result and the contract storage change according to whether the execution exit status is abnormal or not.

7.3 Consensus random number generator

Smart contracts have the need to obtain consensus-aware random numbers. To generate consensus-aware random numbers, the inputs must be chain-related data.

Here are two methods for obtaining random numbers:

Simple random number: The contract directly calls an interface to get a random number, providing a random number based on the current random seed.

Complex random number: The user specifies a set of consecutive blocks in the contract, and the system uses the prev_secret of the block as input to generate a random number. The user can specify that a set of block records that are not generated are set in the contract, and after the chunk is generated, the random number is determined.

The user can call the interface directly in the contract to get a simple random number.

In this way, for a contract call, when the execution result stakeholder happens to be the current producer, there is a possibility that the producer will choose not to package the call according to the random number result and the self-interest. Complex random

numbers can be employed when it is desired to avoid this possibility. The complex random number takes the prev_secret of the continuous block as the input. If the blocker wants to generate a random number that is advantageous to itself, the prev_secret of the current block needs to be adjusted according to the prev_secret of other blocks in the group, but the prev_secret is in the previous round of production. It has been determined that it cannot be modified, that is, the producer cannot control the generation of random numbers.

7.4 Events and callbacks

An event is specific data that is thrown within the contract code and is recorded on the blockchain. Once the event occurs, all blockchain nodes can observe this data.

The callback is for the event binding processing method in the contract. When receiving the event of the specified type, the binding method is executed.

The official wallet provides a default script callback, which can also be customized by the user based on his or her own situation. The Node executes the contract, triggers an event, and pushes it into the block together and broadcasts it to the network.

Advantages of the event mechanism:

Since a smart contract is called at different points in time or under different external conditions, it may go into different branches of the contract code and execute different code logic. For the caller, it is not very good to understand the status of contract execution. With the event mechanism, the user has the ability to understand the status of the contract execution and the results of the contract execution.

With this ability, the user can make relevant feedback actions based on receiving the corresponding event, such as launching a transaction again, or initiating a contract call, or some local action, such as logging, or recording. Database, or make an HTTP request for these. Users can create a decision-making program to connect to our blockchain, make some practical decisions, and implement different feedback operations based on the decision results.

7.5 Local query interface

The data in the smart contract storage area can be queried through the contract interface, but this will consume the fee and need to be packaged in order to get the result. For some simple query functions that do not involve consensus, the contract supports a local query interface (offline). By querying the blockchain data in the region, the current data status of the contract is obtained, which is not only fast, but also does not require a gas fee.

7.6 Asset block link into model

Each new asset block is linked in, all in plug-in mode. Ordinary nodes can choose whether to mount cross-chain plug-ins, Miner and Wallfacer are forced to mount all cross-chain plugins.

The new cross-chain plugin process is as follows:

- Miner and Wallfacer agree on downtime;
- Miner / Wallfacer completes the restart and load the plugin in batches within the agreed time;
- All Wallfacer complete the operation of the supplementary margin;

- After the agreed time arrives, initiate the initialization operation of the new currency (create a multi-signature address, broadcast the relevant parameters of the new currency, and carry out the new currency feed price);
- Complete the blockchain upgrade;
- Select the normal node that mounts the cross-chain plugin to select a new plugin and then mount it. (Ordinary nodes can choose which chain of cross-chain plug-ins to mount, so it does not affect the consensus).

8. Project development plan

Whitecoin cross-chain project will divide into four stages, which are Wallfacer Project, Threatening Project, Staircase Project) ,Blackdomain Project.

8.1 Wallfacer Project

This phase will be upgraded from Whitecoin POS 3.0 to cross-chain program preparation to the end of the old XWC and the new XWC interchange, which lasts for one year. This phase will focus on Whitecoin technology path selection and preparation. This phase will also be completed successfully when the old XWC completes the switch at the scheduled time.

8.2 Threatening Project

This phase will be from the Genesis Block of the Whitecoin blockchain to the end of 5,256,000 blocks. This phase is for one year. At this stage, the Whitecoin blockchain will open cross-chain operation, attracting more people to participate in the development by providing higher mining revenue. The ecological value of Whitecoin is achieved through the establishment and improvement of the Whitecoin ecosystem.

This phase will focus on the establishment of Whitecoin Eco Project, Whitecoin blockchain Tools, Whitecoin Wallet System, Whitecoin related infrastructure and more.

8.3 Staircase Project

The Staircase phase will start from block 5,256,001 to 26,280,000, which will last for about four years. At this stage, the block reward will decline in a stepwise manner. The blockchain network will also enter a stable operation phase. At the same time, cross-chain asset classes will cover all major digital assets, and blockchain applications will cover

more application scenarios. The Whitecoin blockchain will be in a stepped upgrade state.

8.4 Black domain Project

After entering block 26,280,001, Whitecoin officially entered the black domain project. The opening of the Black domain Program also marks Whitecoin's entry into the future of the blockchain chain. After entering this phase, Whitecoin will truly become the infrastructure of the blockchain.

9. Conclusion

The Whitecoin blockchain system will be the basic tool for breaking blockchain islands and realizing blockchain value transfer and value reengineering. With the advancement of Whitecoin's four development stages, the network structure of blockchain interconnection is finally realized, and the network effect of the blockchain is realized.

10. References

1 Bitcoin: https://bitcoin.org/bitcoin.pdf

2 Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper

3 TheDAO: https://download.slock.it/public/DAO/WhitePaper.pdf

4 BitShares: http://docs.bitshares.org/bitshares/history.html, 2013

5 https://en.wikipedia.org/wiki/The_Three-Body_Problem

6 https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md