# iquant Chain White Paper

## Content

# 1. Iquant Chain Technology Background

With the birth of the block chain, the evolution of and attention to the block chain has never stopped. Block chains of various technical architectures and technological ideas are constantly emerging. From the technical point of view, the characteristics of distributed fault-tolerance, unmodified features and privacy protection are the important aspects of people’ s attention. The discussion of block chain related business application scenarios is also a corresponding hot topic in this industry.

iquant Chain hopes to integrate the existing advantages of block chains as much as possible, and provides an efficient, easy-to-implement, highly extensive block chain solution according to the characteristics of transactions, which can provide good foundation for appropriate distributed

applications and services.

# 2. Iquant Chain Technology Solution

iquant Chain provides distributed assets and application platforms, which allows users to develop digital assets and corresponding distributed applications through the infrastructure and development interface SDK provided by the iquant Chain. At the same time, iquant chain provides a series of industry-standard technical solutions, including smart contracts, asset side chains and so on. We look forward to providing easy, comprehensive and plug-and-play options.

Iquant Technology solutions includes:

1. DPOS+PBFT consensus mechanism algorithm
2. Remote equity design to improve the participation of small equity accounts
3. Confirmation design of Equity asset---IQT
4. Release and rewards of basic asset IQE
5. Design and storage of Block Chain Ledger
6. Expansion of side chain solution
7. Smart contract

## 2.1. Consensus Algorithm

The choice of block chain consensus algorithms affects the development of the platform architecture. When designing the architecture, it is hoped that the existing advantages of the consensus algorithm block chain can be integrated, and the consensus mechanism that is suitable for the iquant chain can

be selected, and then the consensus algorithm can be developed.

Analyzing the existing consensus mechanism in block chain:

1. **POW (Proof of Work)**

   Since the birth of Bitcoin, the consensus mechanism based on POW has been recognized worldwide in its reliability and mistake tolerance ability through the certification of many years. Ethereum adopted a consensus mechanism based on POW and meanwhile introduced smart contracts, which further validated that POW can support more applications. As the demand for computing power continues to increase, energy consumption also increases. At the same time, the competition for computing power is becoming more and more intense. Besides, the trend of centralized computing pools is becoming more and more obvious, and the mining fields that rank top has covered the most mining rewards. So there has been many controversies over the POW consensus mechanism.

2. **POS (Proof of Stake)**

   In order to solve the increasing power consumption of POW, a consensus mechanism based on equity certification emerged. This consensus mechanism can greatly reduce the consumption of computing power. Therefore, a variety of block chains based on POS continue to emerge, and get more and more support from development community. In order to further reduce the time for reaching consensus and speed up the production of blocks, various enhanced POS mechanisms have also emerged, such as DPOS (Delegated Proof of Stake) . Quantum chain that is based on DPOS has also been widely recognized. Ethereum development team also mentioned the implementation plan of POS in its subsequent versions of Casper and considered switching from POW to POS (Reference[1]).

3. **POI (Proof of Importance)**

The new coin NEM has proposed a new consensus mechanism after considering the advantages of POS, that is POI(Reference[2]). Different from POS, it not only give rewards to block producers according to their equity, but also considers the number of transactions of users and the contributions of active users to the entire block chain network. By designing a consensus mechanism according to user's importance to the entire network, NEM's unique community contribution program has given the users enthusiasm for participation and has received more and more recognition. At the same time, NEM provided an asset release platform. Various assets issued on the basis of NEM also continue to emerging, which also verified that they can support more applications.

4. **PBFT (Practical Byzantine Fault Tolerance)**

The consensus of the PBFT mechanism has high consistency, availability, and strong anti-fraud ability, and is a more practical consensus algorithm in the chain alliance. In order to prevent the block chain from reaching consensus due to the abnormal influence of certain nodes, the consensus of the distributed nodes is confirmed according to the Byzantine algorithm without the need of confirming by all the nodes. The Internet giants Tencent and Alibaba Group also proposed a block chain solution based on the PBFT consensus mechanism. Tencent is more open source and based on the PBF block chain solution BCOS (Reference [3]). The alliance chain HyperLedger solution sponsored by IBM based on BFT is also used widely in the industry (References [5]).

**Consensus mechanism of Iquant Chain:**

After taking many things into consideration, iquant chain chooses the consensus mechanism of DPOS + PBFT, expecting to achieve the goals of fast block verification, high fault tolerance, and reliable block ledger.

### 2.1.1. DPOS + PBFT Consensus Mechanism

When iquant Chain deploys the Mainnet, the entire network will generate 101 nodes (herein referred to as "consensus nodes") that can produce blocks periodically through account equity voting according to the DPOS mechanism. The 101 consensus nodes will take turns to be responsible for the generation of the blocks in order to prevent unpredictable events such as the network problem, which will lead to node crashes, disconnections, etc., and affect the generation of blocks. After introducing fault-tolerance mechanism of PBFT, all the 101 consensus nodes will be verified at the same time when a block is generated. Only when 2/3 nodes agree with the hash value of the next block, the new block will be generated.

All nodes that have equity accounts have the right to become consensus nodes. The 101 consensus nodes will change according to a certain period of time. The voting process will be started on a regular basis to select consensus nodes among candidate nodes and produce the consensus nodes in the next time cycle. At the time of voting, consensus nodes that cannot support the mainnet operation of iquant chain will also be excluded, ensuring the stability and robustness of the entire network.

On the whole, 101 consensus nodes will remain unchanged within a short period of time, and consensus can be reached quickly. Over a longer period of time, the consensus nodes are continuously rotated to prevent the problem of over centralization because of unchanged nodes.

After considering that the network may have less than 101 nodes because of various abnormal factors, the minimum requirement of consensus nodes will be 13 in order to balance the stability and operational efficiency of the network.

## 2.1.2. IQT

"IQT" will be used as equity asset of iquant chain

IQT is the POS in the DPOS consensus mechanism algorithm. Before the main chain of iquant is released, it will be a ERC20 token, whose total supply is 100000000. After the main chain development, ERC20assets will be transferred to the main chain.

## 2.1.3. Calculating method of DPOS voting equity

DPOS is to reach consensus according to the equity in the account. When the account has the corresponding equity, it can become a candidate node, and it may become one of the 101 consensus nodes that generate the block after voting.

The account equity of iquant chain will be calculated on the basis of basic asset IQT. Trough the equity granting mechanism, the effective equity in the account will be calculated according to the IQT number and their existing time in the account:

1. When an IQT is deposited in the account, the account will not be immediately granted equity;

2. After going through a certain number of blocks N (estimated time is 1 day), 1/10 IQT in the account will be converted to effective equity;

3. After 10N blocks, all the equity in the account will be converted into effective equity.

Voting equity will be calculated according to the time length of IQT assets in the account.

## 2.1.4. Remote equity agent

The owner of IQT effective equity needs to deploy the full nodes of iquant chain before he becomes a consensus node candidates. The deployment of all iquant chain entire nodes has certain

requirements for the network, server, storage, etc. So not all equity account owners can have the condition to deploy all nodes.

The remote equity agent mechanism allows the owner of the equity to authorize the voting rights to other trusted full nodes. After the authorized full nodes becomes a consensus node by the proxy user, the obtained block awards will be returned to the remote equity agent in proportion.

Remote Agent Authorizes Voting Rights Process

1. The user account has valid IQT and starts the equity voting authorization process.
2. The account initiates a block chain transaction. The transaction type is: Equity authorization. Grant the voting rights in the account to the remote agent node.
    a) The remote agent node must be a valid block chain full node;
    b) The equity authorization has a certain period of validity and cannot be withdrawn within the validity period.
    c) Equity authorization transaction will apply to create user agent account at remote node.
3. After a certain period of time, the transaction will be confirmed. After the user agent account of the remote node is successfully created, the remote agent node can participate in the DPOS consensus voting and block confirmation process on behalf of the user.
    a) The user does not need to deploy real time running full node.s The server at user end can be shut down, and the remote full nodes will be responsible for running
    b) The user's private key and other information will not be uploaded to the remote full nodes. All the obtained block rewards will only be returned to the user's original equity account. The agent account cannot store assets and can only be authorized to participate in the block confirmation and production.

c) The aim of the agent account is to provide convenience, meanwhile ensure that the user's private key and other personal privacy information will not to be uploaded to the remote full nodes and protect the user’s equity.

### 2.1.5. PBFT Consensus Algorithm

Of the 101 consensus nodes, only one is the primary node when generating a block, and the rest of the nodes are backups nodes. The primary node is responsible for sorting the transaction requests from the clients and sending them sequentially to the backup nodes. However, the primary node may be subject to abnormal errors or fraudulent actions: it may generate the same serial number for different transactions, or may not assign the number value, or make the adjacent number values not continuous. The backup nodes have the responsibility to proactively check the legitimacy of these number values, and it can detect whether the primary node has gone down through the timeout mechanism. When these abnormal conditions occur, these backup nodes will trigger the condition update protocol to elect the new primary node.

The BFT algorithm guarantees that all normal nodes perform the operations of the same sequence. Because all nodes have consensus algorithm determinism and their initial state is the same, these nodes will produce the same result state based on state machine replication.

After the transaction result is confirmed, when the block is generated, all 101 consensus nodes will verify simultaneously. Only when 2/3 nodes agree with the hash value of the next block, the new block will be generated.

## 2.2. Basic Asset IQE and Block Reward

As the equity asset of iquant chain, IQT will serve as equity object in DPOS+PBFT consensus

algorithm to select 101 consensus nodes according to effective equity and remote equity from all the candidate nodes. The main function of IQT is for equity confirmation.

Meanwhile, iquant chain will release basic asset IQE. The functions are as follows:

1. Rewards of block generation
2. Trading fee payment
3. Fee payment of releasing a cryptocurrency
4. Confirmation of interaction and transaction with side chain
5. Fee payment of releasing and operating smart contract

Before the release of the iquant chain’ s main chain, 100 million IQT have been generated via ERC20 Tokens and IQEs have not yet been generated. IQE will be generated with the creation of each new block. The initial IQE total supply is zero. When a new block is created, a certain number of IQEs are created and rewarded to the consensus node that generated the block. At the same time, 95% of the IQE transaction fee in the block is rewarded to the consensus node responsible for the production block (while 5% of the transaction fee is reserved for the Foundation's account for the Foundation's community rewards and operations). If a user grants the equity to the consensus node through the remote equity authorization, then the IQE will be distributed to the corresponding user account in proportion.

## 2.3. Block Chain Ledger

## 2.3.1. Content in Block Chain Ledger

The content stored in Block chain ledger determine the basic structure of the block chain. When Bitcoin appeared, the Block chain ledger was designed to save the transaction records in the block chain. After a long period, it gained more and more recognition and became another viable option for global digital asset payment.

Ethereum also stores the compiled smart contract code in the block chain ledger. The extended functionality allows Ethereum to run smart contracts and complete relatively complex processes.

When designing the block chain ledger layer of iquant chain, it is considered to store block transaction records, and other related extended information such as side chains:

1. block version
2. Block time line
3. Public key of creating block address
4. Block signature
5. Hash value of the last block
6. Block height
7. Block transaction information list
8. Extended information of block

## 2.3.2. Block Production Period

The time period of block generation is 5seconds. Every new block will be generated in 5 seconds.

### 2.3.3. Storage Method of Block Chain Ledger

Bitcoin and Ethereum use text storage methods (such as BerkelyDB, LevelDB, etc.). Text storage is simple to implement, and it provides B-tree, hash and other structures, and can support the storage of a large amount of data. There are also other block chains that use relational databases to store block chain data. Because of the advantage that the relational database is easy to build and it is a mature application, it makes block chain application development more convenient and conducive to expansion.

Because the block chain data is stored in a distributed way, and all the nodes data is synchronized, the storage capacity of the block chain ledger becomes more and more challenging as the blocks increase. How to store block data has also become a challenge. At the same time, data migration has also become a time-consuming task.

Iquant chain considers the introduction of the data abstraction layer when storing data, which will decouple the logical structure of the data and the underlying storage method, and interact with the underlying data storage layer through the adaptation layer. It will allow each block chain node to choose the storage method (text or relational database, etc.) through configuration to improve the flexibility of data migration and deployment, and also to provide upgrade conditions for subsequent data storage compression and optimization.

## 2.4. Account Layer Design

Bitcoin is based on the UXTO (unspent transaction outputs) account layer, which is highly secretive. The user can generate a new address for each transaction. The user's private key is used to identify the user's wallet. The user can use the UXTO digital assets of multiple addresses in the same wallet. The wallet and the account address are in a one-to-many relationship. It is highly private, and also the third

party verification can be avoid through decentralized consensus mechanism.

Each Ethereum account is only associated with a single address. In addition to the user account address, there is also the smart contract address. Smart contracts can be written in advance to define several logical relationships and execute them automatically. The user account and the smart contract account are placed in the same position. The smart contract address and the user account address will interact with each other, and various relations between person and object, person and person, object and object can be established, which makes DAO (Democratic Autonomous Organization) possible. This account system has strong extension ability.

Iquant chain considers the use of the UXTO underlying mechanism in the account layer design. The same wallet is corresponding to multiple account addresses. High privacy features will be retained, and smart contract addresses will be introduced. Smart contracts is associated with logical relationships, which will provide a base for extending DAO applications. The architecture provides possibilities for future expansion.

## 2.5. Side Chain Plan

iquant chain’ s main chain is designed as efficient as possible, and the operation efficiency is high. In order to achieve the balance between efficiency and function, iquant chain adds most of the extended functions to the side chain.

Through the common interface between the main chain and the strategy, the side chain can interact with the main chain, and the related assets of the side chain can be further integrated with the main

chain, and the related assets in the side chain can be integrated into the unified account in the main chain.

## 2.6. RPC Interface

Based on JSON-RPC protocol and RESTful json technology, a main chain remote interface is provided. At the same time, for the interaction between the main chain and the side chain, a corresponding remote interface is provided. Through the universal interface, the development of the distributed application based on the main chain and the adaptive development of the side chain can be simple and convenient while securing the security.

Remote interface includes:

1. Management of main chain assets
2. Management of main chain account
3. Management of the strategy stored in main chain
4. Interaction between main chain and side chain
5. Management of IQT equity
6. Management of IQE equity
7. Establishment and management of smart contract

## 2.7. Smart Contract

The block chain smart contract can be pre-written to define logical relationship and automatically executed. It can complete the fixed processing flow of several existing tasks in the entire block chain network, providing very great flexibility for the expansion of blockchain network. Multiple smart

contracts can be used to complete more complex functions. It provides scalable block chain ledgers to make smart contracts more efficient and stable.

The function of the smart contract provided by Ethereum has been more and more widely recognized. From digital asset issuance, to decentralized autonomous organization, ID authentication, and distributed game applications, many related applications have emerged.

Iquant chain introduces the extension of smart contracts and further integration with side chains to provide more extension.

# 3. Application Scenarios

Iquant chain cryptocurreny issuing and application platform can be used in many scenarios.

1. Creating Token

   Iquant chain can create token, something similar with ERC token. The created token is the virtual asset or real product of the issue party. All these tokens can be traded with IQS through side chain, and they can also be traded in exchanges.

2. Inter Block chain connection across assets and application

   With the development of block chain technology, various block chains have received more and more recognition. At the same time, connection across block chains has become a hot topic. By extending the side chain of iquant and the interaction between the side chain and the main chain, inter-connectivity across assets can be realized and various applications can be realized.

3. Decentralized exchange

   Through the infrastructure provided by the side chains of iqaunt chain, other assets can transfer a certain amount of assets to the side chains, and a certain number of main chain assets will be locked through the sub-operations collection of the cross-chain trading API. The abstract ledger

data storage layer, data storage extensions (such as database integration, etc.) can achieve a more efficient trading experience.

4. DAO organization and application based on smart contract

   Iquant chain provides smart contract. It can make the relationship between person and object, person and person, object and object abstract, and provides DAO organization and application.

5. Distributed automatic trading checking and audit

   Trading platforms and exchanges require a large amount of manual checking. Even within a single trading platform or exchange, there is a large amount of manual trading checking and audit between various departments and regions. Through the deployment of consensus nodes, automatic checking and audit can be achieved, which reduces the need of manual work.

6. Other decentralized applications

   The iquant chain based on the DPOS+PBFT consensus algorithm has the characteristics of achieving consensus very fast. It also considers the benefits of small accounts and provides a mechanism for expanding the ledger storage. Side chains and smart contracts provide further extension. These characteristics can be used to develop communities to further realize more decentralized applications and create value for the community.

# Reference


[1] https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide

[2] https://nem.io/investors/harvesting-and-poi/#proof-of-importance

[3] https://github.com/bcosorg/whitepaper/blob/master/BCOS_Whitepaper.md

[4] https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[5] https://www.hyperledger.org/industries/finance