BIUT

BIT TRUST SYSTEM

Bit Trust System

No Need For Trust, Free To Trade!

Abstract

This paper proposes a trust computing network based on transaction records completely through peer-to-peer technology, which enables C2C transactions (C2C transactions in this white paper specifically refer to decentralized and peer-to-peer transactions of various objects) to be directly initiated and completed by both parties, and do not involve with any centralization institution. Although bitcoin system solves the challenge of using electronic cash, it still cannot address to the trust issues in the decentralized online transactions. Ethereum can solve the trust issues in transactions which involve with issuance of tokens on the main network through smart contracts. However, in the extensive blockchain application scenarios, and P2P transactions involve with digital currency and legal tender, commodities, services, the industry gets none of any effective solution towards trust issues.

CONTENTS

1 Introduction

Synchronizing with emergence and development of Bitcoin, there appearing new Internet economy businesses such as crowdfunding, crowdsourcing, sharing economy, P2P finance and P2P insurance. Get a lift from a stranger, invest in a stranger' s creative product, find a lodging in a stranger's house, outsource design to a stranger, lend money to a stranger, all together manifest C2C business characteristics. At present, these business models evaluate reputation through buyers' reviews and ratings. Buyers make purchase decisions through sellers' open information and these evaluation systems.

These new economy business organizations often have a furious start up, but soon they will encounter obstacles and hesitate to move forward, or even backward to the original beginning. Car-sharing platforms became taxi companies, crowdsourcing transformed into supplier selection, and China' s P2P lending platforms turned to centralized capital pool to defraud public. The underlying reason is the lack of new trust mechanism. Old wine in new bottle, these business models originated from the trust reconstruction, but old Internet technologies cannot provide system-level solutions of trust issues.

In the blockchain industry, there appears decentralized bitcoin and preliminary form of decentralized collaboration, but lacks the decentralized trust mechanism. Therefore, besides currency transaction and fund-raising, blockchain cannot yet be applied in practice that even for the simple operation of transferring legal tenders cannot be achieved. As long as the transaction is combined with legal tenders, off-chain assets, commodities and services, it cannot be decentralized and de-trust. All transactions are subject to the trust mechanism. In the investment market of the blockchain industry, strangers would invest BTC with liquidity value in new projects, this is also a new form of financial crowdfunding which needs new type of cooperative trust. However, because of the lack of trust

mechanism, there are many canceled projects, resulting in “bad money drives out good money”.

There are three phases in the trust development of human society. The agricultural society has a customary trust, the industrial society has a contractual trust, and the information society has a cooperative trust. The corresponding trust establishment is based on interpersonal relationship, secured contract by trust-intermediary and information system. At present, for traditional online transactions, contractual trust mechanism generated from industrial age is widely applied. In Bitcoin White Paper, Satoshi Nakamoto also argued that traditional Internet-based electronic transactions need a centralized organization as a third-party institution to conduct trust evaluation for both parties, which is a model based on the contractual trust mechanism with high-level trust cost of transactions and requires the transaction parties to provide unnecessary private information.

2 Trust issues in decentralized C2C transactions

In the development of e-commerce, eBay, Amazon, Taobao, Meituan and Dianping all adopt centralized evaluation algorithm to compute trust degree. However, the effect of trust mechanism derived from centralized evaluation system is diminishing or even fading, due to increasingly collective online sham transactions conducted by sellers, resulting in higher cost of seller-selection, lower credibility of buyers’ reviews, and opaque algorithms.

In the exploration of P2P application in e-commers, Lightshare has very early used P2P technology to create a C2C mall, and Openbazzar also has attempted to provide C2C transaction services by using blockchain technology, coupling with digital currency payment functions such as BTC, BCH, and ETH. However, due to the lack of trust mechanism, the transaction efficiency has not enhanced.

Logically, the Bitcoin network solves the issue of multiple information transmission that Alice sends electronic information to Bob, which is a game question of one-way information transmission between Alice and Bob. While in the Internet C2C transactions, the game question which needs to be solved is two-way information transmission that Alice sends electronic currency to Bob, and Bob sends back electronic currency (or physical assets, commodities, services) to Alice.

From the perspective of game theory, multiple game transactions can generate direct trust. A single transaction can use mortgage to compensate the default cost, while multiple games use transaction records as references, and use economic incentives to raise the default cost. Under the circumstance in which the benefit of reputation of an account outweighs the default cost, the account is more likely to conduct a transaction without cheating.

Karl et al. first proposed and solved the issue of trust management in P2P network environment. There are increasing people who attempt to address the trust issues by using algorithms in complex networks. There are many trust models, such as Peer Trust model that uses elements of evaluation and reward to compute trust through local reputation value and global reputation value. EigenTrust model uses trusted nodes based on distributed Hash Tables and direct trust to calculate global trust value, to filter out malicious nodes and eliminate the network. PowerTrust model selects trusted nodes and improves the rate of convergence in EigenTrust model, coupling with Power node algorithm it improves the EigenTrust model. Inspired by the characteristics of gossip spread, the Gossip Trust parallel computes the global reputation of nodes.

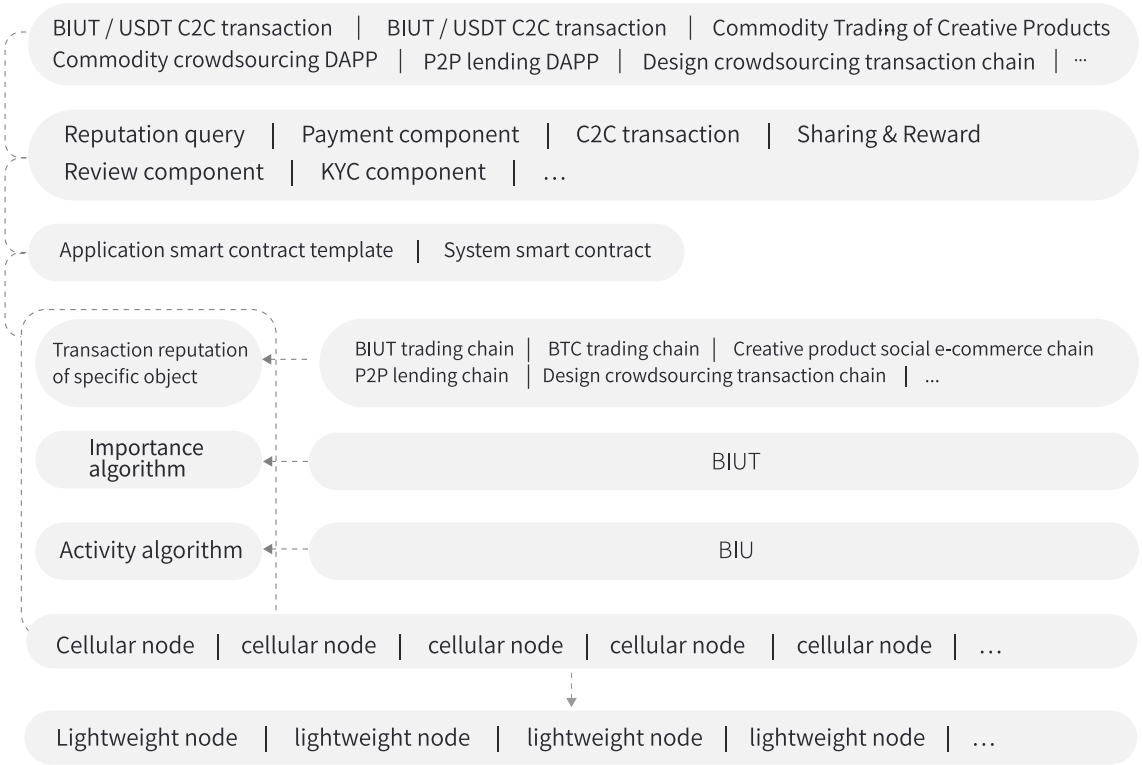
The account activity calculation is based on the Leader Rank and the Trust Rank algorithms, and uses the P2P decentralized trust algorithm to calculate the trust value of accounts, creating a new distributed trust system through the PGPOW and DPOS-like reward models. The two parties bidirectionally complete the transaction, once they recognize that

the transaction is successful that the blockchain will record the transaction. According to the transaction record of certain object between two accounts, the system will dynamically calculate the activity, importance, direct trust value, reputation value and recommendation trust value of the accounts based on the blockchain transaction records. Therefore, users can judge the reliability of the counterparty of the transaction according to the recommendation trust value and the reputation value of the counterparty, which reduces the probability that the malicious account is selected as the counterparty.

3 System function

3.1 System function

Through the Bit Trust System, it enables free transactions which need no third-party intermediary, nor construct interpersonal/contractual trust with the counterparty of the transaction.



▲ System function diagram

The cellular nodes assume the function of the blockchain full nodes, and according to the corresponding algorithms respectively calculate the activity, importance and the reputation value of specific transaction object through the BIU transaction records, BIUT transaction records, and transaction-chain transaction records. When the lightweight node makes a query request to the cellular node, if there is no activity, importance and reputation value of the node, or the block of the node has been updated, then the cellular node stores and responds to the query request result after calculation.

Each transaction chain corresponds to the transaction record of a transaction object, and calculates the direct trust value and reputation value of the account in regard to the transaction object. The value calculation will differ with various transaction objects. A BTC seller with high reputable value does not have to be a qualified logo designer seller.

The activity and importance of a seller' s account has an overall importance throughout the system. In the activity algorithm and the importance algorithm, there are factors such as guarding against sybilattack, the higher value of activity and importance of an account therefore, the less likely it is to default in the transaction, which also applies to buyers.

3.2 Systematic element description

- **Transaction chain:** is used to store information of specific transaction object and corresponding transaction records.
- **BIUT:** Credit
- **BIUT chain:** is used to store the transaction records of the digital currency BIUT in the application layer.
- **BIU:** Credit Order
- **BIU chain:** is used to pay, convert GAS, implement Token transfer and record, support smart contract system.

- **Cellular node:** is used as under normal circumstances for PCs to jointly maintain the entire system operation.
- **Lightweight node:** generally applied in a mobile terminal, it can automatically choose to become a cellular node. Once becomes a cellular node, it will join the node community and complete the round-robin cycle with other cellular nodes, downloading BIU chain information.
- **Miners in the node community:** the cellular nodes in the node community that successfully solve issues will have the right and obligation to generate new blocks and package data, and get rewards for generating new blocks.

3.3 Example of decentralized C2C transaction

The C2C transaction of digital currency can use smart contract through the verification mechanism of lightweight nodes and cellular nodes to ensure the successful transaction. In a wider range of scenarios, such as using banknotes to purchase digital currency (similar to buying commodities or services in digital currency), the transaction may not offer payment information, smart contracts therefore are applied. We will use the following example to describe the process.

For example, in the case of a C2C transaction in which US dollars are used to purchase BIUT, buyer Alice wants to use US dollars to buy BIUT. In DAPP, the cellular node queries the BIUT transaction reputation value and quotation of different sellers. Once Alice selects the seller Bob and initiates the transaction, the BIUT seller issues a request to the smart contract of digital currency transaction and transfers the corresponding amount of BIUT into the address designated by the smart contract. In the case of successful transaction, Bob will receive corresponding payment offline or through a bank account. After Bob informed the smart contract that the payment has been received, then the smart contract triggers the account to transfer BIUT to Alice.

In the case that the transaction arouses disputes that Bob refuses to acknowledge the receipt after Alice completes the payment. The smart contract will temporarily lock the BIUT, and if Alice's account has high-activity, high-importance and high-reputation value, the pledged fee is withheld for dispute resolution and the corresponding materials are submitted. According to the algorithm, it will arbitrarily select three BIUT credit gatekeepers, one of which is the first designated judge. If the judge decides that Bob breaches the contract, and Bob does not appeal, the pledged fee will be returned to Alice, and the smart contract will transfer the BIUT to Alice. If Bob appeals and submits materials and pledged fee, 18 credit gatekeepers will newly join in to vote for the arbitration on infringement. If they decide that Bob breaches the contract, then Bob's pledged fee will be rewarded to the credit gatekeepers. In addition to the submitted materials, the system shall conduct dimensionality reduction on Bob's account activity, importance, reputation value and network-wide transaction records.

With the development of the system, after multiple transactions and games, the credible account active, importance, and reputation value of active accounts will improve, which enables both parties to quickly make decisions, while the default accounts are basically excluded from the active account system. Because the default costs are expansive, the active accounts in the system are credible accounts in the transactions of specific object, realizing the decentralization. Decentralized transactions can be performed quickly without trust intermediaries, which accelerates the market transaction speed.

4 System architecture

4.1 Multi-chain structure

The blockchain is foremost a decentralized system, in which any data will be transparent, traceable and unmodifiable to the public. It does not need a server for storing transaction information. Second, its encryption mechanism ensures the high security for storing the users' private keys and addresses, and selectively encrypts the transaction information, which protects the users' privacy during transaction process.

In the system, a multi-chain parallel structure is adopted, which is divided into transaction chains, BIUT chains and BIU chains. The transaction chains contain autonomous domains that each autonomous domain has its own transaction chain.

4.2 Modular design

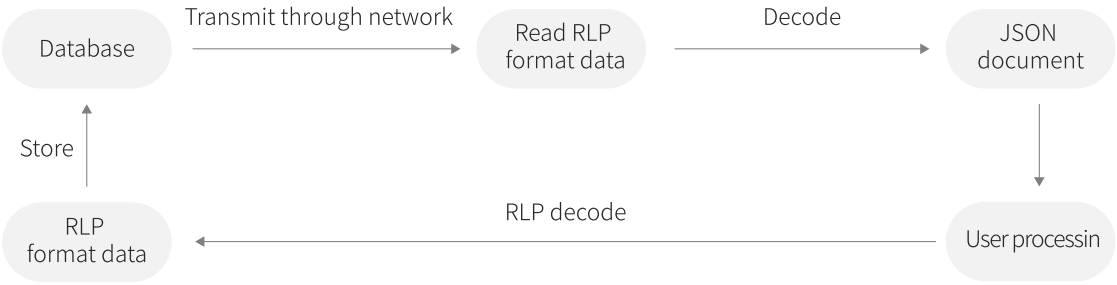
The system adopts modular design that multi-chain structure chain, asymmetric encryption algorithm, trust-related algorithms and functions, system-level and user-level smart contracts, consensus algorithm and data structure all adopt modular decoupling design, which have excellent scalability.

4.3 Data format and storage

The system uses JSON format and RLP encoding method to process and store block information. JSON is a data exchange format with simple and concise structure that is easy to be analyzed and generated by the system, which is beneficial to improve transmission efficiency. The system adopts protogenetic RLP code from Ethereum project that the code format conforms to the system design objective. RLP code can be nested in binary arrays of arbitrary length, specifically for data processing of list structures. It has the following advantages:

- The structure is simple and concise that it can understand data structure by analyzing a prefix of a few bytes.
- It can easily ensure absolute byte expression consistency.
- Provide an explicit sequence of key/value maps.
- It is superior to bencode algorithm in coding length.

Specific flow chart is shown as follow:



▲ Data format storage flow chart

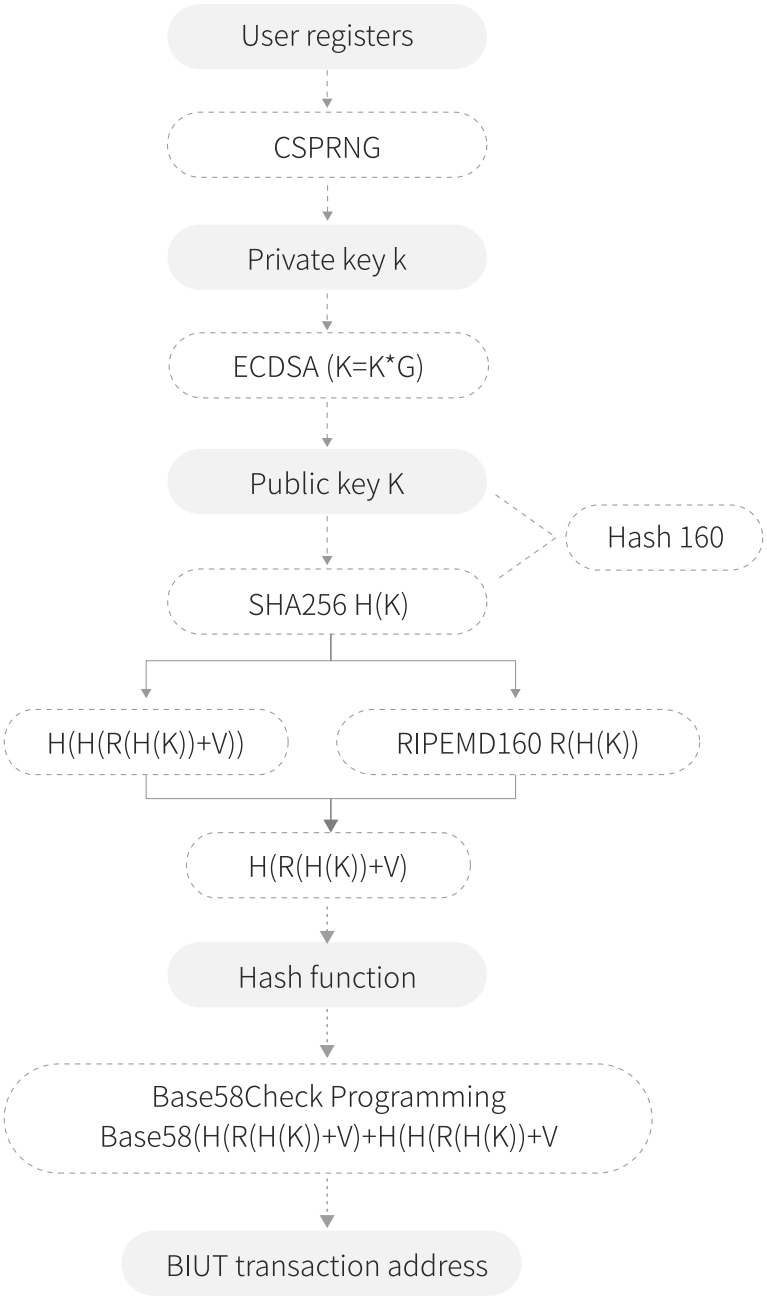
4.4 Encryption algorithm

It adopts elliptic encryption in asymmetric encryption, and the encryption algorithm is secp256k1. The algorithm is also the encryption method used by Bitcoin. Elliptic encryption has a higher efficiency than the asymmetric encryption RSA algorithm that the byte length of RSA algorithm is six times as long as the byte length of elliptic encryption for the same security level. Therefore, elliptic encryption greatly reduces the operational load of the entire system, and this algorithm is irreversible.

When a user registers, the system will generate a random number k as the user's private key, and the private key is encrypted through the one-way encryption function ECDSA(k) to obtain the user’s public key K. At this point, a one-way cryptographic hash function Hash(K) is used to obtain the user’s transaction address. The pseudo-random number generator CSPRNG is used to generate private key, which usually has a length of 256 bits and is a binary number indicated in 64-bit hexadecimal, each hexadecimal occupies 4 bits.

After a user registers and corresponding transaction address is gener-

ated, the system will send user's public key K and transaction address. The public key acts as a bridge between the private key and the transaction address, and it plays an important role of verifying the authenticity of the transaction to check whether transaction address sent by the operation is consistent with the address generated by the public key. The public key can also verify the signature of the private key, which used to verify the private key signature of the transaction.

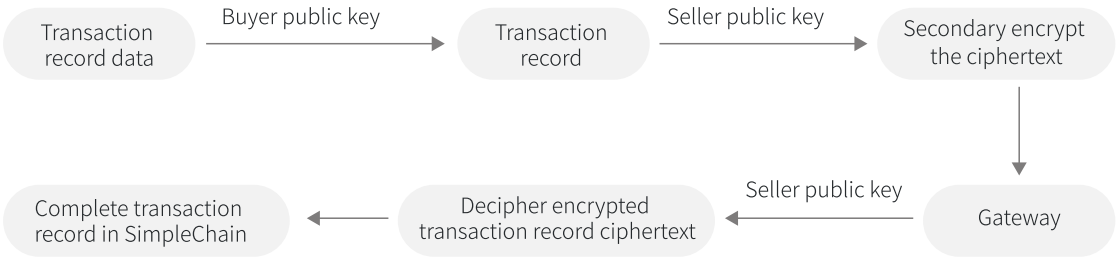


▲ Encrypting process diagram

4.5 Transaction chain

4.5.1 Structure of transaction record data and on-chain process

The main contents of a transaction record data are: seller' s address, buyer' s address, transaction record and transaction status, of which the transaction record needs to be encrypted before stored in chains, and the transaction record content stores the product name and the product price.



▲ Transaction record on-chain diagram

- The transaction record in the transaction record data will first be encrypted with the buyer's public key to generate the transaction record ciphertext, which will be stored in the transaction chains of the autonomous domain.
- The transaction ciphertext generated in the first step is encrypted again by using the seller's private key and sent to the system gateway.
- The system-level smart contract in the system gateway deciphers the secondary encrypted transaction ciphertext by using the seller's public key. If the ciphertext can be deciphered, the authenticity of the transaction record can be confirmed (it is actually generated and sent by the seller), verifying the authenticity of transaction record.
- After the verification, the responsible node in corresponding round-robin packages and stores the transaction record on chains.

The transaction data through this on-chain process can only be deciphered and examined by the seller and buyer involved in the transaction. Other nonrelevant nodes to the transaction have no right to view the specific content of the transaction, but are only aware of the occurrence of the transaction, ensuring the confidentiality and anonymity of the transaction records in chains.

4.6 BIUT chain

The BIUT chain is used to store the transaction records of digital currency BIUT (credit) used by the storage application layer, and the block record of BIUT chain is used for the importance algorithm to calculate account importance degree. The credit currency is the payment currency of the transaction chain and is also a measuring tool for the reputation value algorithm on transaction chain.

There are many participants in the public chains, including users, investor communities and developers. Under the traditional model, the consumption of token is huge, which is not conducive to the ecosystem expansion and reward mechanism. In the design of BIUT, benefits of all participants have been taken into account. Therefore, the setting of BIUT in the model can well balance the benefits of all participants.

4.7 BIU chain

The BIU chain is used to maintain the block generation and security of transaction chain and BIUT chain. When there is bifurcation in the BIU chain, that is, there are two different blocks derived from the same paternal block due to network delay, it can be solved by using method similar to Bitcoin, which is the recognition of longer chains. The solution of the bifurcation is implemented through the network event processing mechanism. The basic logic is as follows:

When node A receives a new block, if the height of the block is less than or equal to node A's own blockchain length, the block is directly

discarded. If the height of the block exactly equals to node A' s blockchain length, the block is directly added into its own blockchain. If the height of the block is greater than node A' s own blockchain length more than 1, node A will directly request all of the excess blocks to the node which sends the block. With the acceptance of the block, the consistency verification is performed that if the verification fails, it will compare the blockchain lengths of node A and the other node and enforce the shorter blockchain update into the longer one.

4.8 Autonomous domain

The autonomous domain is a reserved logical structure of cross-chain technology. Each transaction chain corresponds to an autonomous domain, and the entire transaction chains are also an autonomous domain. Other blockchains outside the system also exchange transaction data with the system in the form of autonomous domains. The existence of autonomous domain has greatly improved the scalability of our system, as well as the parallel processing ability.

4.9 Gateway and Smart Contract Design

4.9.1 BIUT Gateway

Smart contracts contain user-level smart contract and system-level smart contract. The user-level smart contract enables users to customize the behavior of the transaction. System-level smart contract is provided directly by the system. We define a collection of all system-level smart contracts as BIUT gateway.

4.9.2 System-level smart contract

The BIUT system-level smart contracts are stored in transaction chains. BIUT system-level smart contracts are mainly applied in smart contracts across the entire network, such the smart contract for domain name, smart contract for automatic purchase of BIU through BIUT to pay GAS cost, on-chain smart contract of legal tender payment.

4.9.3 User-level smart contract

BIUT user-level smart contracts for specific transaction chains are stored in transaction chains, such as reward on buyer's sharing behavior. When a transaction between the seller and the buyer is completed, the seller node runs the smart contract in the VM environment. Then the smart contract will generate blocks for storing the transaction information and monitor the buyer's sharing behavior.

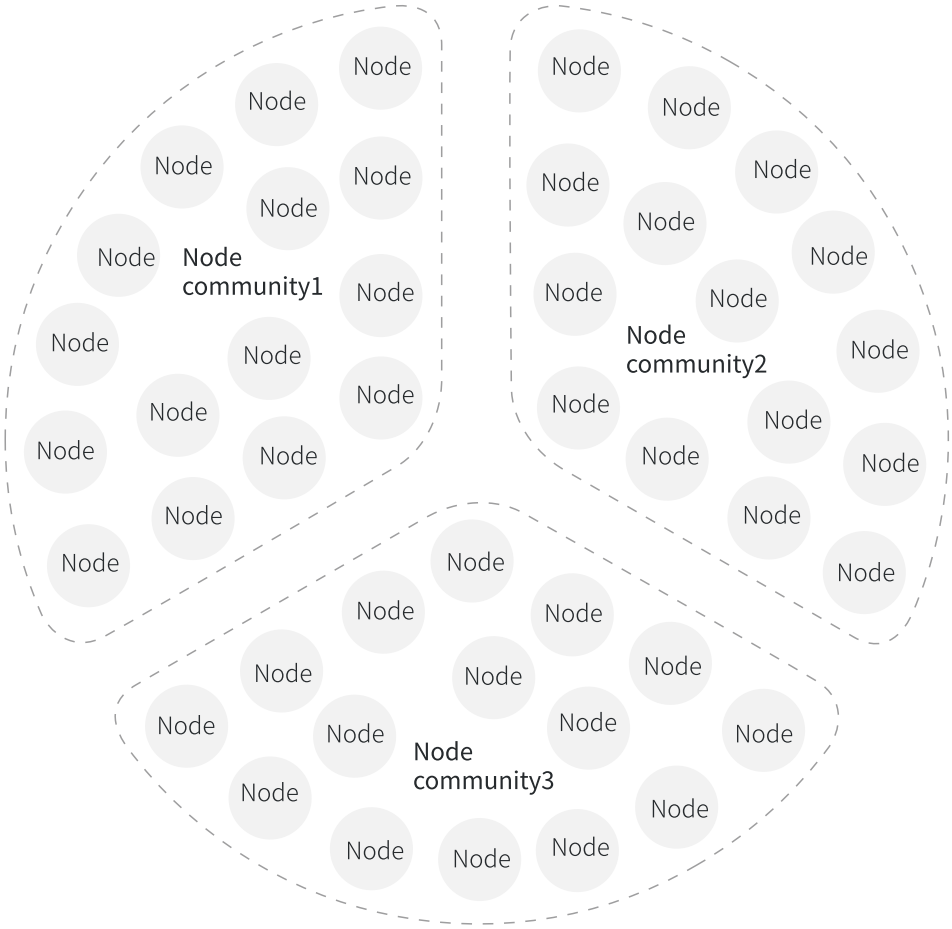
5 PGPoW consensus algorithm

5.1 Node community

At the network level, the system consists only of lightweight nodes and cellular nodes. At the logical level, the system consists of enormous amount of autonomous domains, and each domain contains one and only transaction chain. Each transaction completed in the DAPP will be recorded and stored in the corresponding transaction chain. The autonomous domains are classified according to the category of commodity, which means that each transaction chain corresponds to a specific commodity category.

In order to maintain the enormous amount of transaction chains (such as package validation and on-chain storage for each transaction, the generation of new blocks in each transaction chain), the node community consists of a large quantity of cellular nodes. In essence, the node community solves the calculating force for maintaining large quantity of transaction chains and the generation of new blocks in BIU chain.

The new blocks in BIU chain is generated by the rotation of node communities. If the system is divided into 1 to 10 node communities, these 10 node communities will generate new blocks in sequence, and after a round-robin cycle, they will vote for another round of division of node communities.



▲ Node community diagram

5.2 The generation of node community

Each node community is generated through the voting by cellular nodes. The specific process is as follows:

- If our system consists of 10 node communities which are marked from number 1 to number 10;
- Each cellular node generates a random number x for each adjacent node, and this process is called voting;
- Each cellular node will get the votes from adjacent nodes, and the most votes obtained will be operated. The result is the mark number of the node community in which the node is;
- The cellular nodes that obtain the same node community mark number belong to the same node community.

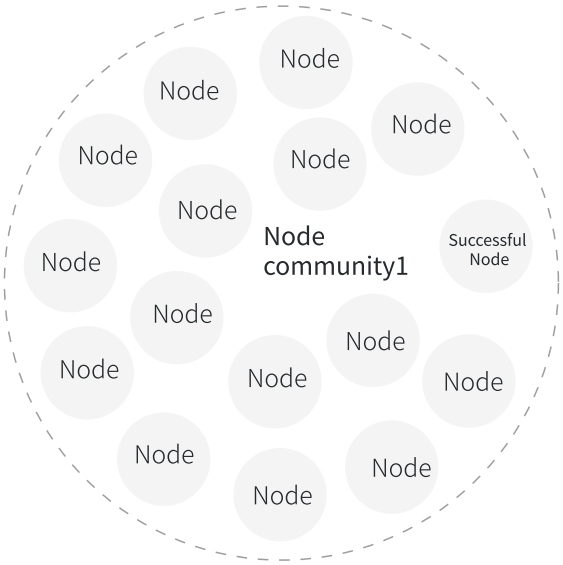
The node communities are divided through the above mechanism to avoid cheating. After each round-robin is completed, the system automatically divides the node communities for another time. In order to prevent attack behavior, we introduce the following formula:

$$S = 5 * \sin x + 5$$

x is a random number, and S is the node community mark number. For example, if the value of S is 0-1, which represents node community 1, and 1-2 represents node community 2. After the node communities are divided, other cellular nodes can selectively check the number of votes obtained by the cellular node and the community it is in. If the result reported by the node does not match the community it is in, which indicates that the node has cheating behavior and it will be punished.

5.3 BIU chain consensus mechanism and maintenance

The BIU chain generates a block every 20 seconds. The 10 node communities rotate to generate a new block on the BIU chain, and they also rotate to maintain the transaction chains. A complete round-robin is a cycle period, and when a cycle is completed, a new round of dividing node community is executed to start the new cycle.



▲ POW mechanism in node community

Inside the rotated node community on duty the PoW mechanism is carried out, and all nodes in the node community compete for an opportunity of generating a Token block, and the node which generates Token block obtains rewards of Token and GAS.

In order to prevent the higher-level PoW energy consumption, we will reduce the setting difficulty. The difficulty of BIU chain changes once through 2016 blocks, ensuring the participation of most node users in the calculation. The calculation difficulty formula is:

$$Calculation\ \ difficulty = \frac{difficulty\_target}{current\_target}$$

The target is a 128-bit long Hash value. The purpose is to determine a cellular node that can generate a Token block. In addition, it can guarantee that the high performance of the cellular node, which ensures the cellular node is competitive for the mission of packaging the data, and can complete the data packaging and storage on BIU chain.

Each of the cellular nodes in the node community maintains the normal operation of the system that even if they did not compete to be a miner node in the node community, they are still rewarded with a small amount of BIU.

Since the node community contains a large quantity of cellular nodes that are most likely include all the transaction chains in the system. These transaction chains are jointly maintained by all the cellular nodes in the round-robin node community. In the case that the node community does not contain all the transaction chains, the newly added cellular nodes in the current node community will broadcast to the entire network, collecting complete messages of the BIU chain.

5.4 Transaction chain consensus mechanism and maintenance

The transaction chain is an autonomous domain blockchain generated according to the category of the transaction object, and all users are not

necessarily engaged in each transaction chain. All transaction chains are also classified through the mechanism same as node communities that a transaction chain generates a block every 8 seconds, ensuring the high efficiency of transaction. For autonomous domain with sluggish activity, it can be adjusted after gone through 2016 blocks.

Suppose node 1, node 2, and node 3 simultaneously have transaction chain A, then node 1, node 2, and node 3 synchronously generates a random number and broadcasts it throughout the node community. After comparing their respective points, the node with the smallest random number will execute the data packaging and storage on chain and the generation of new blocks in transaction chain A. And the node will broadcast throughout the entire network after the data packaging and on-chain, which is verified by other nodes in the local autonomous domain.

The maintenance operation of the transaction chain will not give any reward to the nodes, and it is the obligation of the cellular nodes in the node community. In the autonomous domain, the height of the transaction chain is not high, and the size of packaged data is not large, it will not have high-level requirement on the performance of the node.

Each chain waits for the height of 6 blocks that if there is a bifurcation phenomenon, all node communities will check the height of the chains and vote for the highest chain, chains obtain more than 51% of the votes are legal ones.

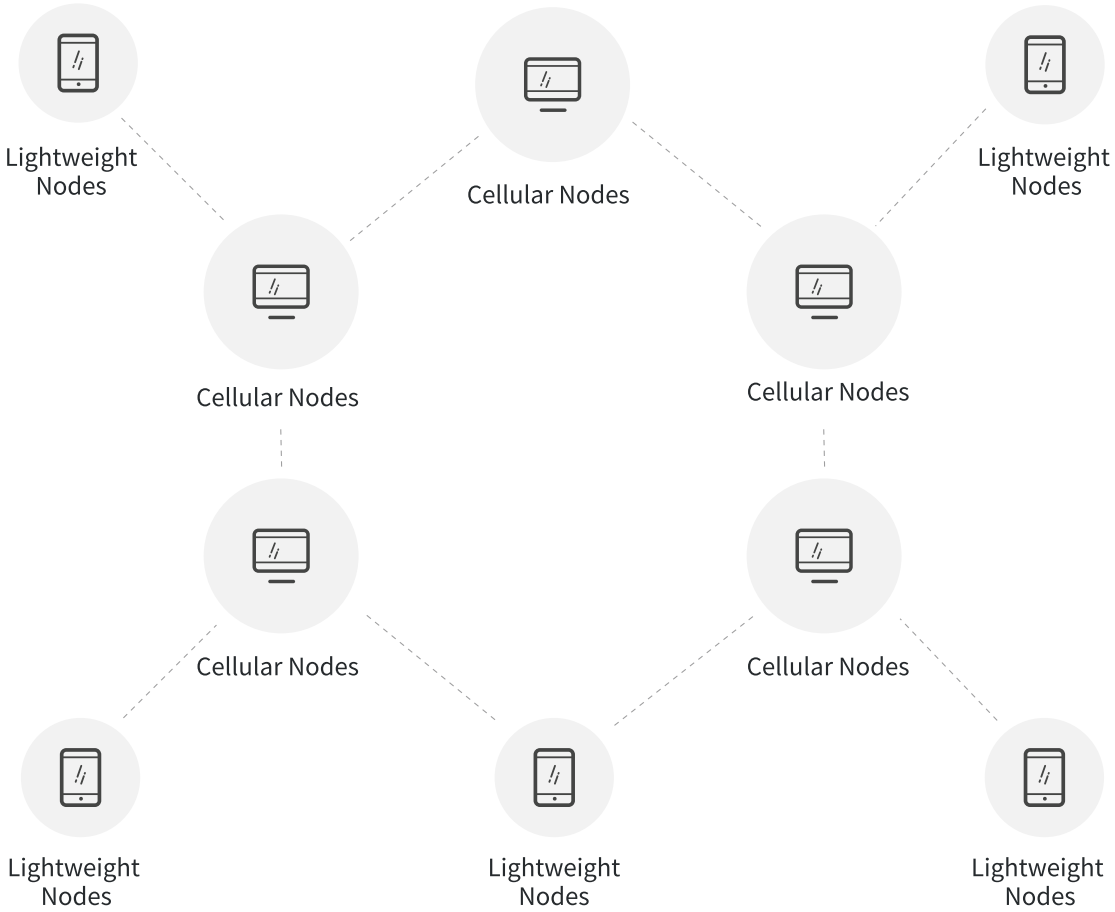
6 Network

The BIUT blockchain network is a structured distributed network similar to KaZaA and is a typical third-generation P2P network. All the node information in the network is aggregated into a distributed Hash Table which contains information with keywords and the address of the node where it is located. Then the distributed Hash Table is divided and its segments are stored in the nodes of the network. Through Hash Table

it can find the specific node that stores content of Hash Table corresponding to the keywords. The network is highly flexible, highly structured and greatly scalable.

The BIUT network consists of lightweight nodes and cellular nodes.

- **Lightweight nodes:** Generally, they are for the mobile terminal, and only connect to the cellular nodes from which data would be pulled.
- **Cellular nodes:** Generally, they are for the PC terminal, ect to othe cellular nodes, the data stored in the domain where a cellular node is in synchronizes with other cellular nodes.



▲ P2P Network Framework

7 Trust algorithm

7.1 Implementation of the trust mechanism

In the C2C transaction scenario, when the default cost is greater than the default revenue, then the user is inclined to complete the transaction. In the C2C transaction system, the safest choice for users is to have transactions with users with high-level credit. An account' s historical transaction records of an object represent the importance rank of the account in the transaction market for the object, and obtain higher evaluation through algorithms. We use the reputation algorithm and recommendation trust value to address the evaluation on transaction ability of the account, and reveal it to users, implementing system-level trust through transaction records and algorithms.

In the system, when a transaction is completed, a cellular node stores the transaction evaluation locally. When a lightweight node needs to calculate the reputation value of an account, it will extract information from the cellular node. The cellular node queries whether there is a new transaction and whether need to update the reputation value based on the transaction record of the block.

- If there is no new transaction record, it will return to the original reputation value;
- If there is a need to update, it will first extract information of activity, importance, direct trust value, full-region reputation value and recommendation trust value from the block. If there is no direct transaction record between the two accounts, it will rely on the recommendation trust by the system, and algorithms to calculate recommendation trust value of the counterparty of the transaction.

7.2 Definitions

- **Definition 1.** Activity Rank is the calculation of activity ranking

of different accounts in the network based on the relation of BIU account transactions.

- **Definition 2.** Importance Rank is the calculation of account importance ranking based on the account transaction relation, transaction volume, coinage and balance of BIUT.
- **Definition 3.** Direct Trust is the calculation of the trust value of the counterparty of the transaction based on the historical record of direct transactions between accounts.
- **Definition 4.** Recommendation trust refers to that there is no transaction relation between account A and account B, and it is the system which calculates the trust value.
- **Definition 5.** Reputation is a global trust, which refers to the network-wide trust value towards an account.

7.3 Activity Rank calculation based on BIU chain transaction records

According to the transaction relation in the BIU chain, the BIU activity rank of each account is calculated by using the leader rank algorithm.

Algorithm meaning:

- If an account has transactions with many other accounts, which indicates that this account has greater importance and also has a higher activity rank.
- If an account with a higher activity rank value generates a GAS fee due to a transfer or a transaction, the activity rank of the passive account involved in the transaction will rise accordingly.
- Activity rank is only related to the account transaction relation, and has nothing to do with the transaction volume, it is defined as a vector matrix.

Take account of factors such as resist whitewishing and sybilattack, and the setting is as follows:

- Calculate all accounts that have a transfer record with the system black-hole account 0000000000000000, and other accounts have an activity of 0. The function of black-hole account in the system: The service fees of all accounts are transferred to the black-hole account, and the GAS fees are awarded to the miners through the black-hole account.

- PGPoW miners need to provide computing force, and ordinary PCs can execute the mining. According to the algorithm, the activity rank of the miners' accounts is larger than other accounts, and the miner accounts are set as trusted accounts. The matrix information of the trusted accounts can be used for evaluation to calculate recommendation trust for the transaction chains, diminishing sybilattacks effectively.

According to the mutual transfer relations, the accounts in the system can be organized into a web map G_w=<V,R>, wherein V is a collection of accounts, that is, a vertex set in the web map, and R is a collection of transfer relations between accounts. In the G_w of the Web map, define the transfer relations between accounts as R_i, j∈R represents the transfer from account i to account j.

Then calculate the activity by activity in split, which refers to that if the activity of an account is 1 and connects with n accounts, then each account it transfers to will get a trust value of 1/N. Therefore, the trust value of an account is the total activity obtained from all accounts which transferred into it. Through is way, it avoids the inability to converge due to isolated points in the matrix and balances the rights of new entrants at the application level.

AR_i is defined as the activity of account i. AR_i(k) is the first-order activity of the steady account i in the system after k-step calculation. The

black-hole account then distributes its activity evenly to other accounts to obtain the global activity of the account *i*. The final global activity AR_i value of the account i is calculated as follows:

If there is no transaction record between the account *i* and black-hole account:

$$\mathrm{ARi}=0$$

If there is a transaction record between the account i and black-hole account:

$$\begin{cases} \mathrm{ARi}(0)=1/\mathrm{n} \\ \mathrm{ARi}(\mathrm{k})=\sum_{\mathrm{j}=1}^{\mathrm{n}+1}\bar{\mathrm{a}}\mathrm{ji}\mathrm{ARj}(\mathrm{k}-1),\mathrm{k}=1,2,\cdots \\ \mathrm{ARi}=\mathrm{ARi}(\mathrm{k})+\mathrm{ARg}(\mathrm{k})/\mathrm{n} \end{cases}$$

Where n is the number of network accounts (excluding black-hole account and accounts which have no transaction record with black-hole account); $AR_g(k)$ is the activity of background account v_g at step k; $\bar{a}ij$ is the matrix element in web map:

$$\bar{a}ij=\begin{cases} 1/\mathrm{k}_{\mathrm{i}}^{\mathrm{out}}, & \text{there exists transfer relation from account i to account j} \\ 0 \end{cases}$$

In the formula, ki^{out} is the out-degree of account *vi*.

7.4 Calculation of Importance Rank based on BIUT chain

The Importance Rank value is calculated according to the Trust Rank (TR) value which is calculated by using the transaction record of the BIUT chain and the trust rank core algorithm.

Trust Rank algorithm setting: Trusted accounts are little likely to participate in fraud attacks. First, the trusted accounts can be identified by AR (that is, the "seed" accounts), then the accounts which are pointed

by the trusted accounts may also be the trusted accounts, which indicates the accounts have high-level TrustRank. The farther away from the "seed" account, the lower the TrustRank of the account. This algorithm contains the effect of the path factor.

The TrustRank algorithm first sets a subset of good accounts SP_g, that is, the accounts in the set are trusted accounts. The default activity of these accounts is 1. Then set the activity of attack accounts as 0, and the activity of the other accounts is 0.5. If all paths from an account in the trusted account set to another account do not contain a spam account, set the activity of the trusted account as 1.

Calculate the TR value of the account.

$$\mathrm{TR(i)=(1-d)+}\sum_{j=1}^{k_i^{in}}\left(\bar{c}\,ij * TR(j)\right)d$$

Where TP(i) is the Trust Rank value of the account V_i, d is the damping coefficient; k_i^{in} is the in-degree of the account V_i.

$$\bar{c}ij=\begin{cases}1/\mathrm{k}_i^{\mathrm{out}} & \text{account i points to account j}\\ 0\end{cases}$$

In the formula, k_i^{out} is the out-degree of account Vi.

Calculate the transaction importance rank (IR) of each account:

$$\mathrm{IR}=\mathrm{TR}\times\mathrm{AR}^{\mathrm{T}}\times\frac{\mathrm{In}(\mathrm{CA}_i^{\sum_i \mathrm{t}_i})}{1-e^{\partial \mathrm{C}}}$$

In terms of account importance, it is necessary to consider the overlapping effects of all factors. First, in the calculation of coinage (CA) and activity rank, factors such as systemic features and authenticity of all accounts are taken into account. Second, at coinage level, the coinage status of all holdings of an accouns is considered in the calculation, and the absolute value is obtained through accumulated weighted algorithm, finally converted by using logarithmic coefficient; finally, CA is

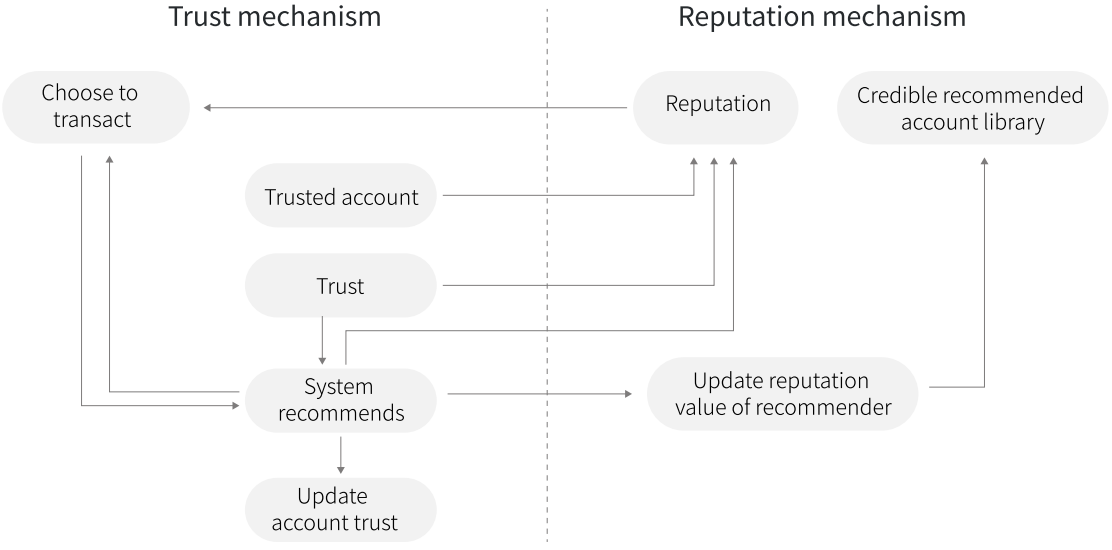
the weighted sum of the coinage of the balance, and δC is the proportion of the balance in the total pledge. In the overall position, each account has a low proportion and is normalized, enabling the total value to be multiplier processed within a single order, and avoiding the multiplier amplification caused by more open position accounts and smaller position accounts.

In the formula, at BIU and BIUT levels, the comprehensive consideration of the characteristics of the transaction records is necessary, that is, the higher the activity, the higher the coinage, the higher the balance, the larger the value for the function, and the higher-level the importance is.

7.5 Calculation of reputation and trust value based on the transaction chain

For the C2C transaction of an object, the transaction record is included in the transaction chain. In the C2C transaction application layer, according to the Reputation algorithm, the Reputation value of two parties in the transaction is calculated, recommending C2C transaction counterparty according to the recommendation trust value.

The relation between trust value and reputation is as follows:



▲ Trust-reputation relation diagram

7.5.1 Direct trust value

The direct trust value represents the reliability of the account which provids transaction services. In the transaction performed by two accounts, account i purchases the transaction object from account j, which uses the Beta probability density function to calculate the direct trust value of account i to account j:

$$dij = \begin{cases} 0, g(i,j) = u(i,j) \\ \dfrac{Max(g(i,j) - u(i,j), 0)}{\sum_j Max(g(i,j) - u(i,j), 0) \times N_p}, otherwise \end{cases}$$

Where gij is the number of successful transactions between i an j, uij is the number of unsuccessful transactions between i and j, and Np is the penalty coefficient (when Np>1, take the actual value of Np; when Np<=1, take the value of Np equals to 1). The more times of successful transactions between account i and account j, the greater the mutual direct trust value Dij; with the penalty coefficient Np, if the malicious account conducts attack, the direct trust value Dij will drop rapidly.

Np is related to the chain-relative ratio of network-wide unsuccessful transactions of adjacent cycles, and the importance (IR). The initial state is set as 1, and this parameter is adaptively adjusted as the system robustness increases, but the minimum value is 1. With Np, the rate of descent of direct trust value will be faster than the rate of ascent.

7.5.2 Reputation value

The set of trusted accounts is filtrated by using activity rank, and the reputation value is calculated by using direct trust value through Eigen Trust algorithm. Assuming that after multiple transactions between account i and account j, dij is the normalized direct trust value; define $\vec{t_i}$ as the vector contains , t_{ik} where t_{ik} is the trust value of account i towards account k based on the query account:

$$t_{ik} = \sum_j d_{ij} d_{jk}$$

Matrix [dij] is D, get:

$$\vec{t}_i = D^T \vec{d}_i$$

In order to obtain more comprehensive information, account i will calculate reputation value of many accounts that have transaction relations with account i. the final formula is: $\vec{t}_i = D^T \vec{d}_i$,and when n is large, $\vec{t}_i$ will converge to the same vector of each peer account, that is, $\vec{t}$ is the global trust vector in the model, and the elements in the vector quantify the trust degree of account i towards to other accounts; $\vec{t}_i = [t_{i1}, t_{i2}, \ldots, t_{im}]^T$, w here m is the total number of trusted accounts in the global data.

- Reputation calculation of trusted accounts

  According to AR algorithm, the set of trusted accounts P is filtrated, and the reputation value of account i is pi:

$$p_i = \begin{cases} 1/|P|, V_i \in P \\ 0, otherwise \end{cases}$$

- The iterative computation formula of reputation value of account i is:

$$\vec{t}_i^{(k+1)} = (1-a)\mathrm{D}^T \vec{t}^{(k)} + a\mathrm{P}$$

The formula will continue the iterative computation until

$$\left\| \vec{t}_i^{(k+1)} - \vec{t}^{(k)} \right\| < \varepsilon$$

Where $\vec{t}^{(k)}$ is the reputation value after the kth iteration; P is the initial reputation cardinal matrix of account i ; the exponent T is the vector trans-

pose; ε is a small number; initial $\bar{t}_i^{(0)} = \frac{1}{n}$ $\alpha \in [0,1]$ is the trust degree of an account towards to the hypothesis trusted account.

The above processing mainly rests on that the global trust is derived from the accumulation of all direct trust value, but in the case whether the account is trustworthy has not been determined, the increment in the assignment value of direct trust in each account is in the consideration of the fairness to the new entrants in the algorithm.

7.5.3 Recommendation trust value

The direct trust value and reputation value of the account are in a positive correlation with the corresponding recommendation trust. When the time element approaches to the present time, the behavior is more meaningful, the time decay therefore is applied on the formula factors to make the recent time more meaningful and more weighted.

The time decay factor $\tau_j$represents the decay ratio of the direct trust value and the reputation value at present time generated by the transaction conducted by the account i and the account j, s_j is the time when the transaction happens.

$$\tau_j = e^{-(s-s_j)}$$

The recommendation trust value of account i is TTi, and its calculation formula is:

$$TT_i = \sum_j^k \tau_j \times (1-\rho^k)\ d_{ij} + \sum_j^k \tau_j \rho^k t_i^{s_j}$$

$t_i^{s_j}$ is the reputation value of account i at the transaction time s_j, in order to reduce a large amount of calculation, according to the calculation process of reputation value, $t_i^{s_j}$ tends to be stable, then:

$$t_i^{s_j} \approx t_i$$

Where dij is the direct trust value of account i towards account j; $(1-\rho^k)$ is the weight of direct trust, and $(0 < \rho < 1)$, k represents the number of successful transactions between account i and other accounts, the more direct trans-

actions between account i and account j, the more inclined recommendation trust is to the direct trust value.

7.6 Summary of PoW TRUST mechanism algorithm

We named the above algorithms and the trust mechanism based on the reward model as the PoW TRUST mechanism, which contains a set of PGPoW-based reward mechanism, distributed accounting system, and distributed trust algorithm functions.

The algorithms include: BIU-chain system black-hole account and Leader Rank algorithm, Trust Rank algorithm, IR importance algorithm, and activity and importance ranking algorithms based on the BIU and BIUT transaction records. The activity and importance algorithm solve the issue of the dynamic selection of trusted accounts, and calculate direct trust value, reputation value and recommendation trust value based on factors such as importance.

7.6.1 Trust mechanism algorithm and malicious transaction behavior

The system often has malicious accounts that use various strategies to bypass the trust mechanism and conduct transaction attacks on the credible accounts in the system. The resistance methods included in the PoW TRUST mechanism that against common attacks are as follows:

- Problem 1: Inconsistent behaviors. For example, an account was the credible account, but conduct default transactions after its trust value increases;

  Solution 1: In PoW TRUST mechanism, the contradict attack in a single transaction is solved through mortgage. In importance rank algorithm and reputation value algorithm, although the positive growth is slow, when a fraudulent behavior emerges, due to the existence of penalty factor, the reputation value can drop quickly.

- Problem 2: Cooperative attack. For example, multiple malicious ac-

counts cooperate to conduct sham transactions in order to augment reputation value;

Solution 2: In PoW TRUST mechanism, the activity algorithm and importance algorithm are related to the transaction relations, due to the existence of trusted accounts, malicious accounts cannot augment their reputation values through cooperation on sham transactions.

- Problem 3: Wash-sale reputation, frequent malicious transactions with high-reputation accounts. For example, in order to obtain high value in activity and importance, malicious accounts will frequently conduct from/to transfer of funds with accounts in large-scale centralized exchange;

  Solution 3: In PoW TRUST mechanism, in the activity rank algorithm and contribution rank algorithm, due to large in/out-degree of authoritative accounts and existence of trusted accounts, such behaviors cannot significantly improve the reputation ranking;

- Problem 4: Multiple account attacks. Such attacks include sybilattack and whitewishing.

  Solution 4: In PoW TRUST mechanism, the trusted accounts are the miner accounts of the BIU chain and other miner accounts, and the system can mine through ordinary PCs, through miner accounts in PGPoW therefore, can effectively resist the sybilattack. In the Activity Rank algorithm, the activity rank of accounts that have no transfer-out behaviors is zero, due to t the PoW TRUST mechanism, the speed of reputation accumulation is slow, coupling with high default costs, which can effectively prevent the whitewishing.

- Problem 5: Disintegration attack. Such attack refers to the disintegration of a credible account due to the loss or off-chain of the account into a malicious account and conduct attacks. For example, mobilizing friends to conduct sham transactions for the seller,

or the seller buys a large number of honest accounts to conduct attacks.

Solution 5: In PoW TRUST mechanism, for individual wash-sale behavior, it is difficult to identify the attack behaviors through transaction records or behaviors. And at present, the current PoW TRUST mechanism cannot effectively identify such attacks, even through collaborative filtering algorithms. For the bribery acts to a large quantity of credible accounts, due to high-level attack costs and uncertain attack earnings, such attacks can be avoided.

7.6.2. Fine-grained trust mechanism algorithm

The PoW TRUST algorithm implemented in the BIT TURST SYSTEM uses transaction records as a medium to form a transaction mechanism to facilitate the successful transactions. With the development of the system, there will emerge more types of transaction chains, and there will be more suitable transaction algorithms for different transaction objects. For example, the trust algorithm based on evaluation is the mainstream trust algorithm for traditional e-commerce and social media websites. Indeed the algorithm has defects, but through optimization in BIT TRUST SYSTEM, new transaction chains and trust algorithm can provide more data and dimensions to the system in account transaction, which is more conducive to the fine-grained trust mechanism, facilitating the whole system to run effectively.

8 Reward

As a public chain used for transactions, the system reward mechanism has three layers. The application layer of DAPP is set by each DAPP autonomously. The total fixed amount of credit (BIUT) is 1.5 billion, and the reversion and distribution mechanism is implemented through the role of gatekeeper and smart contract. The total fixed amount of credit

order (BIU) is 1.5 billion, which is mined by PGPoW. The first half output of the BIU is related to the number of network-wide transactions every three months, and the total output of BIU is related to the application demand. After the network and ecological development are mature, the latter 50% of the BIU will be halved mined over four years, ensuring the user reward, ecological development and network security.

8.1 Economic Model of BIUT

8.1.1 Usage and total quantity of BIUT

BIUT application: application layer payment, mining Proof-of-Stake (PoS), transaction mortgage, transaction market opening fee, transaction dispute arbitration fee, etc.

BIUT distribution scheme

Type	Tokens quantity	Proportion	Ratio	Description
Credit gatekeeper rewards	600,000,000	40%	0.40	With applied ecology, produced in a mechanism similar to POS
Community	600,000,000	40%	0.40	
Foundation (Operation and business)	150,000,000	10%	0.10	Three years of maturation period
Technology team	150,000,000	10%	0.10	Three years of maturation period
	1,500,000,000	100%		Total quantity

8.1.2 Proof-of-stake (PoS) in mining

For BIUT within interval of [0, upper limit] in cellular nodes, the more BIUT the more BIU mined from single block. The mortgage algorithm is written into the main network program. The initial BIUT proof of stake interval is [0, 100,000].

Considering the fairness factor, the upper limit of BIUT proof of stake in mining is 10<=the upper limit of proof of stake <=100,000, and the

position is not locked. Taking 365 days as a cycle, and make adjustment. If the number of transactions increases significantly, which indicates a rapid development of system, the upper limit of Proof-of-Stake in mining will be lowered. Calculate the current Proof-of-Stake PQi+1:

$$PQ_{i+1}=\begin{cases} PQ_i/(TQ_{i+1}/TQ_i), \mathrm{TQ}_{i+1}\le TQ_i \\ \dfrac{PQ_i}{\log_{10}(10+(TQ_{i+1}/TQ_i))\times\log_{10}(10\times(TQ_{i+1}/TQ_i))}, \mathrm{TQ}_{i+1}>TQ_i, TQ_i\le 100000 \\ \dfrac{PQ_i}{\log_{10}(10+(TQ_{i+1}/TQ_i))\times\log_{10}(10\times(TQ_{i+1}/TQ_i))\times\sqrt{\mathrm{TQ}_i/100000}}, \mathrm{TQ}_{i+1}>TQ_i, TQ_i>100000 \end{cases}$$

Where PQi is the upper limit of Proof-of-Stake from the previous period, and TQi is the number of network-wide transactions from the previous period. TQi+1=the number of network-wide transactions in current period.

8.1.3 Credit gatekeeper campaign and obligation

Training 101 credit gatekeepers' accounts in rotation that the accounts with importance level above certain value can campaign for the credit gatekeeper, candidate accounts must have 100 votes from other accounts. The credit gatekeeper needs to pledge the BIUT, and the pledge ratio is adjusted by a cycle of 365 days. If the number of transactions increases significantly, which indicates the rapid development of system, and the upper limit of proof of stake in mining will indicating that the system is developing rapidly, the upper limit of the rights be lowered. The initial pledge is 1000 BIUT, and the pledge adjustment is similar to the upper limit adjustment for proof of stake in mining.

8.1.4 Credit Gatekeeper Benefits

- Initiate a new trading market unit to charge market naming fees through the opening of smart contract in the market. The opening of trading market needs to be voted and approved by the credit gatekeeper.

The market domain naming fee is locked in the smart contract account. When the consecutive active transaction volume in the trading market unit reaches 10,000, the market naming fee will be returned to the initiator 1.2 times the original value, and the smart contract will reward BIUT to the credit gatekeeper at the value of 0.8 times market naming fee. If the active transaction volume within 720 consecutive days does not reach the standard, the market naming fee of the trading market will be deposited in the ecosystem account.

- Primary arbitration of transaction disputes, a new gatekeeper will be randomly designated to arbitrate, and the security deposit of the responsible party of the transaction dispute is rewarded to the credit gatekeeper.

- Algorithm store

  The ecosystem developer provides a trust algorithm on the transaction object, a consensus algorithm for the application chain, a data structure, etc., and 0.1% of the transaction earnings is deposited in the reserve account of credit gatekeeper.

8.2 Economic model of BIU

BIU is used for payment such as the consumption of all network layers, network-wide transfer fees, smart contract execution fees, and network charges for the launch of new parallel chains.

8.2.1 BIU total amount and output

Use PGPOW consensus algorithm Proof-of-Work is used in mining, and the total amount of 1.5 billion BIUs will be mined in two stages. The first 50% of BIUs are mined that the output each cycle will be according to the network-wide transaction volume in the previous cycle. The latter 50% of the BIUs will be halved mined over four years.

8.2.1.1 First stage output

The output at the first stage is related to network-wide transaction volume in two cycles, and the period of each cycle is three months.

Calculate the output of the next cycle PQi+1:

$$PQ_{i+1}=\begin{cases}PQ_i/100, TQ_{i+1}\geq TQ_i\times 100\\ \dfrac{PQ_i}{\sqrt{TQ_{i+1}/TQ_i}}, TQ_{i+1}<TQ_i\times 100\end{cases}$$

Where PQi is the output of the previous period, TQi is the network-wide transaction volume in the previous period, and TQi-1 is the network-wide transaction volume in the number of transactions in the whole network in the period before the previous cycle.

In the formula: if TQi, TQi-1 are 0, add 1.

8.2.1.2 Second stage output

The remaining 50% of BIUs are halved mined over four years that since the beginning of the second stage:

The output of first four years: 375 million, the output of second four years: 187.5 million · · · · · ·

8.2.2 GAS costs

8.2.2.1 GAS transfer fees

The basis for GAS cost of each cycle is adjusted according to the network-wide transaction volume in the previous cycle. Theoretically, it will maintain a reasonable price for each transfer fee, and the period of each cycle is 365 days.

Calculate the next cycle GAS cost basis GQi+1:

$$GQ_{i+1}=\begin{cases}GQ_i/\left(TQ_i/TQ_{i-1}\right), TQ_i\leq TQ_{i-1}\\ \dfrac{GQ_i}{\log_{10}(10+\left(TQ_i/TQ_{i-1}\right))\times\log_{10}(10\times TQ_i/TQ_{i-1})}, TQ_i>TQ_{i-1}\end{cases}$$

Where GQi is the previous period GAS cost basis, TQi is the network-wide transaction volume, and TQi-1 is the network-wide transaction volume in the period before the previous cycle.

8.2.2.2 Smart contract and transaction fees for new parallel chains

If the smart contract can get space, the GAS cost will be calculated in byte space.

The GAS cost of a new transaction chain is adjusted according to the number of bytes occupied by the data structure relative to the original transaction volume.

9 Public chain store

Considering the complexity of the development of blockchain applications and the development of the developer community, we plan to launch a public chain store. The public chain store provides various modules for public chain development, and application components required by DApp development.

9.1 Code framework for public chain store

The Bit Trust System modular design and multi-chain structure provide excellent scalability. The transaction chain can autonomously customize the transaction object, and also self-define the main chain data structure and consensus algorithm as well. Coupling with smart contract and DAPP, it effectively reduces the development difficulty and cost to use for the development of blockchain applications.

The code modular optimization provids basic functions such as the main code framework of the public chain store, token issuance, graphical custom transaction chain data structure, POS, DPOS and other custom consensus algorithms.

9.2 Components

The public chain store provides a variety of development components, as well as modules required for public chain development, which have full-function algorithms and functions, and components provided by developers can open free source by using MIT Lesser General Public License, or charge to users for rewards.

10 Conclusion

Bit Trust System is the first blockchain network established based on system-level trust between accounts, which used blockchain transaction records and trust algorithms to evaluate the reputation value of specific transaction object of an account, recommend and make a match, and eastablish reward mechanism through PGPoW+ and PoS consensus algorithms, increasing default costs to transaction accounts. The network uses JavaScript language, modular design, and applies the blockchain system of multi-chain architecture, realizing high performance, high security, high decentralization degree of the whole network. The network has features such strong scalability and friendly to developers that it is comprehensive network of the implementation of decentralization.

Bit Trust System is based on the decentralized C2C transaction application and extends to peer-to-peer businesses such as crowdfunding, crowdsourcing, social e-commerce, sharing economy and P2P finance. We believe that Bit Trust System is the basic platform for the implementation of decentralized trust, helping Internet users to conduct decentralized transactions and collaboration safely. Bit Trust System can solve key issues of trust reconstruction in the new economy and new finance, which is a key to open the door of digital economy for developers, merchants and Internet users.

Bit Trust System, no need for trust, free to trade!

11 Code address

Github

https://github.com/BIUT-Block

NPM

https://www.npmjs.com/org/sec-block

https://www.npmjs.com/org/BIUT-Block

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

[2] Ethereum White Paper. [EB/OL]. https://github.com/ethereum/wiki/wiki/White-paper

[3] Kamvar S D, Schlosser M T, Garcia-Molina H. The eigentrust algorithm for reputation management in p2p networks[C]//Proceedings of the 12th international conference on World Wide Web. ACM, 2003: 640-651.

[4] Page L, Brin S, Motwani R, et al. The PageRank citation ranking: Bringing order to the web[R]. Stanford InfoLab, 1999.

[5] Li Q, Zhou T, Lü L, et al. Identifying influential spreaders by weighted LeaderRank[J]. Physica A: Statistical Mechanics and its Applications, 2014, 404: 47-55.

[6] Liu C, Zheng X L, Xu A W, et al. C2C trust evaluation model based on social network and reputation[J]. Computer Engineering, 2010, 2010(24): 41.

[7] MA Xiaoxue, LIU Yuling, TIAN Junfeng.Trust model based on extended subjective logic for P2P environment.Computer Engineering and Applications, 2011, 47(7):74-77.

[8] XU Junming, ZHU Fuxi, LIU Shichao, et al. Identifying opinion leaders by improved algorithm based on LeaderRank. Computer Engineering and Applications, 2015, 51(1):110-114.

[9] Peng DS, Lin C, Liu WD. A distributed trust mechanism directly evaluating reputation of nodes. Journal of Software, 2008,19(4):946−955. http://www.jos.org.cn/1000-9825/19/946.htm

[10] LI Fengqi, LI Guangming, YANG Nanhai, et al. TWIT:two-way algorithm for local trust inferring in social networks. Computer Engineering and Applications, 2016, 52(4):66-73.

[11] Gyöngyi Z, Garcia-Molina H, Pedersen J. Combating web spam with trustrank[C]//Proceedings of the Thirtieth international conference on Very large data bases-Volume 30. VLDB Endowment, 2004: 576-587.

[12] Zhou R, Hwang K. Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Transactions on parallel and distributed systems, 2007, 18(4): 460-473.