Inchain White Paper 2.0

Chongqing Inchain Technology Co., Ltd.

April 2017

Contents

Text Parts

I. The Understanding of Inchain to Blockchain

As Bitcoin comes to the sight of the public, the charm of the Blockchain technology has been gradually discovered and recognized by more and more people. Characterized by decentralized, de-trustful and non-manipulation of data, it will overturn many traditional industries, and at present, the Blockchain technology is in an initial stage with a narrow application, so the Inchain is committed to breaking this situation.

The nature of the Blockchain is a consistent distributed data account book, and during the development of project, the Inchain block has its own deep understandings to Blockchain technology. Combining with the p2p technology and consensus mechanism, and on the basis of the application development of the public Blockchain of Inchain, it is as easy as developing on traditional databases and the result is that the Inchain is able to provide the bottom protocol supports for various applications, especially the business applications. The technology and business of Inchain will bring a breakthrough development for the Blockchain industry.

II. What is Inchain?

The Inchain refers a public Blockchain project serving the bottom platforms of Blockchain business application initiated and led by the Chongqing Inchain Technology Co., Ltd. and one original intention of the Inchain is to combat counterfeit products by applying the Blockchain technology and provide the most credible technology for brand businesses to protect their brand images. The Inchain project was officially launched in December 2016, and it had finished the lower layers's design and development of Blockchain and general security traceability business process by April 2017, therefore the first application platform adopting security traceability based on the public Blockchain of Inchain had released estimation and everyone can experience it!

III. Why Is Inchain More Suitable for Developing Business Applications

Block chain is short in talents, requires highly for bottom technologies and most applications are needed to be established on a certain bottom platform, so the Inchain

offers another choice for these applications.

Needs in general businesses are not taken into consideration by platforms like Bitcoin, Ethereum and lisk, and business needs fit the bottom difficulties, but the applications are as difficult as producing business logic. One important thing is that it does not meet the needs in business regulation.

The Inchain is the first application eco-platform of professional business Blockchain, and certifies and manages grading systems from the bottom architecture identity as well as signs multi-signature registration of dual-key encryption to bind the management. This system, combining with management agencies and advanced arbitration systems developed by Inchain, meets the requirements of decentralized regulation in decentralized network and government-accessible commercial-level regulation.

IV. Innovation of Inchain

(I) Innovation in Consensus

Created by the registered Chongqing Inchain Technology Co., Ltd., the Inchain has uniquely created the POC-Proof of Credit (see more details in next parts).

(II) Innovation in Account Systems

In order to be suitable for business, the Inchain in the bottom applies the exclusive certification of hierarchical management system to equip different roles with different permissions and functions, so that businesses and other role accounts are able to naturally form a combination of patterns to achieve various business models.

(III) System Tokens Credit Dual Value Intermediary

In addition to the token INS, the nodes are able to accumulate and obtain another data flow in the consensus: the credit value. The Inchain, for the first time, introduces a credit value into the Blockchain as a management intermediary creatively, and constitutes double intermediary mechanisms.

(IV) Innovation in Trading Models

Unlike other Blockchain projects which boast of simple transaction types like transferring and double signatures, the Inchain implants many trading models on the basis of bottom creatively and these models independently finish more complex business activities. Such as: verify renters trading model, reward contract model,

credit cash deposit model and auction bidding model.

(V) Innovation in Models

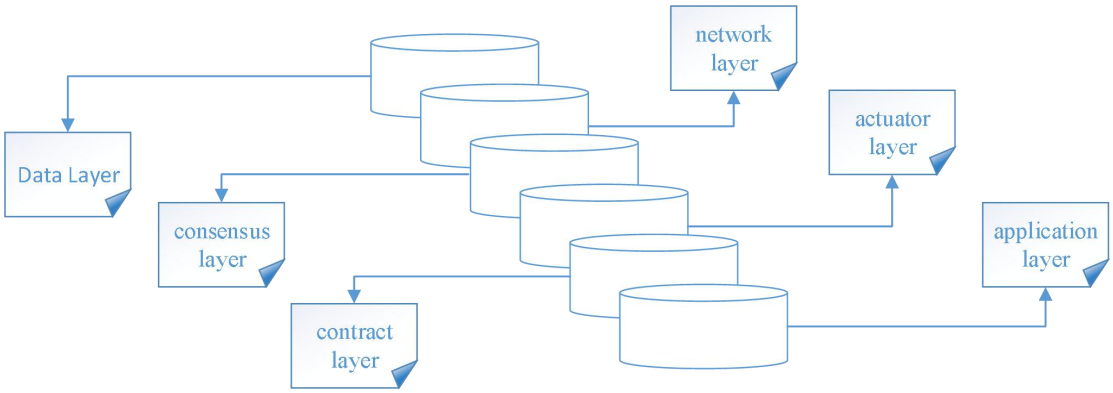
The Inchain will support the architecture by adopting the global assets white list and its application to make the issuance of assets to be fully managed and regulated in multiple levels like protocols, applications and bottom networks. It seems realizing comprehensive functions like issuance, bankruptcy liquidation, and online application of reality enterprises' assets.

(VI)Innovation in Technologies Integration

The Inchain strives to integrate advanced technologies in Blockchain, this industry and other industries, for example, the Chongqing University of Science and Technology cooperates in using small two-dimensional code technology. It will continuously adopt new technologies including virtual machines, advanced intelligence contracts, advanced arbitration, isolation and verification.

V. Technical Frameworks of Inchain

The Inchain includes six basic models like the data layer, the network layer, the consensus layer, the actuator layer, the contract layer and the application layer.



(I) Data Layer

The block data of the Inchain conduct storage by applying a chain structure, and all blocks are carried with pointers for reference of the previous blocks to ensure that the data are not tampered. The Inchain conducts the Hash chain to data by applying the sha256 function, verifies the identity by applying ecc asymmetric cryptographic algorithm, encrypts the private keys by applying aes Encryption algorithm, and verifies and stores the transaction by applying Merkle numbers.

(II) Network Layer

The nio socket is used alternatively by Inchain nodes, and load seed nodes by adopting the dns method and program internally installed. All nodes will conduct a self-test after start, and nodes in the public network will automatically report their own ips and ports to the network, and the other nodes will verify the information reported; if the verification is passed, all nodes will store the ip addresses and ports of available nodes to the local places, and it will be directly connected without re-detection the next start; if the verification for many times does not pass (there will be a rule detecting every 10 minutes once, when the number of failures is over 10, a figure for successful numbers, it will be triggered), the node may have been off the assembly line, which will be removed from the storage queues. When the number of connected nodes is too few, it will automatically ask the connected nodes for more available nodes.

The Inchain makes nodes in the intranet connect and communicate with each other by penetrating holes, and makes nodes behind the nat communicate and connect in virtue of nodes passing the verification as a connected bridge.

(III) Consensus Layer

The Inchain does not adopt the existing consensus mechanism, and this is because a business location of Inchain will become the largest public Blockchain with user flow and tps, and meanwhile, the poc will be produced when a link of value is found in the business environment. This also can be called a "hard innovation" of Inchain which gives consideration to the performance and the maintenance efficiency at the same time. A detailed introduction about poc is in the following.

(IV) Actuator Layer

10% of the Inchain tokens are used for the consensus award, this is because the performance of a unique consensus mechanism of Inchain is not affected by the number of nodes, there is no a upper limit set in consensus nodes of the Inchain; they are changed dynamically, and anyone can participate in for obtaining bonus at any time.

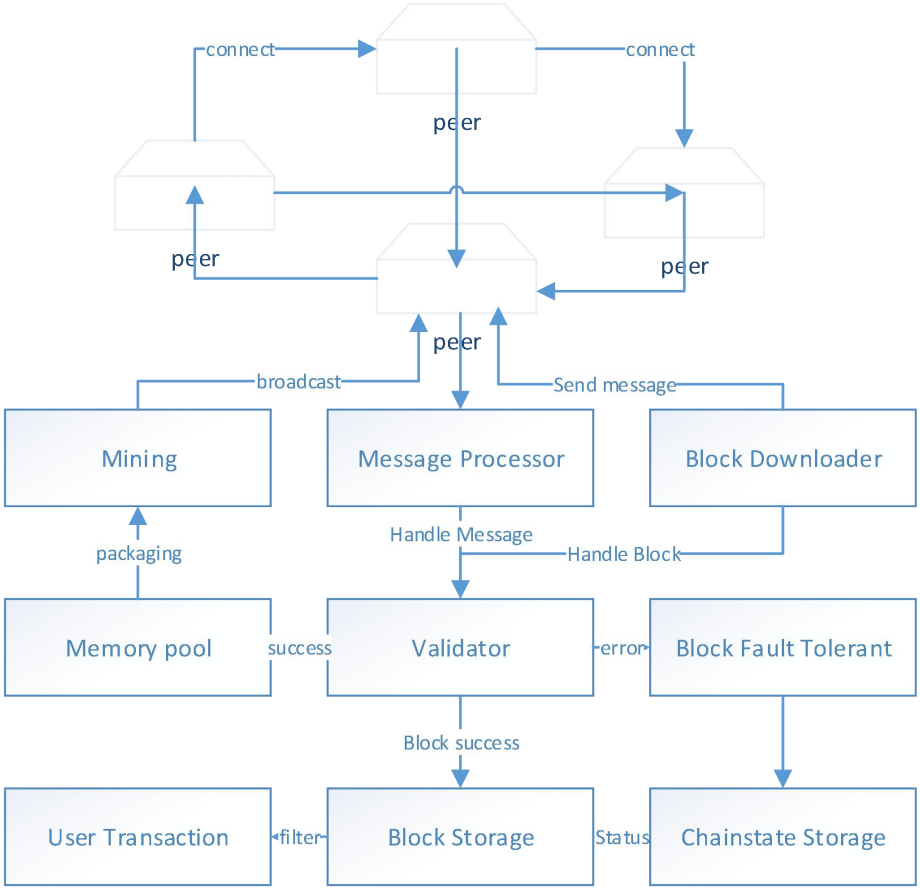
(V) Contract Layer

At present, the contract layer of Inchain is only a simple script code, a verified script in security codes, and a redemption script in the consensus cash deposits, and all of them are small smart contracts. The Inchain positions itself as a business application platform and therefore, it will conduct an ecological integration of public Blockchain and promote formation by adopting ways different from other intelligent contract platforms. The Inchain will recruit a third-party team to create more arrival

application projects down to earth and with practical application; the audience in the front end will be the general public, so it accumulates a large number of users for Inchain. The Inchain plans to develop complete virtual machines in 2018 so as to provide higher flexibility, but there are should be a large number of users for Inchain in advance, and the Inchain is clear about its targets and directions before this.

(VI) Application Layer

In the previous periods, the Inchain will provide general application protocols to the bottom in order to develop different arrival projects, and make the Blockchain benefit the public as soon as possible. Currently, the security traceability protocol is developed and completed and in fact, the application scopes of this set of business protocol are not only security traceability and for more introductions, please refer the later parts.



Inchain Framework Figure

VI. Credit System

(I) What Is Credit System

The credit system of the Inchain refers a feedback process of systems to participating systems. The Inchain team thinks that people with vested interests who obtain the approval of systems the system should not be those who reap without sowing (pos) or the strong in the law of jungle (pow), but the friends of systems should be the labor people active in systems friends, and contribute to the system with heart and soul. Therefore, the introduction of credit system in Inchain realizes this concept.

(II) Why Do Inchain Need Credit System?

Here one important reason will be analyzed that the Inchain is a business Blockchain bottom platform. Because its business, there are will be more behavior types of nodes than the previous other Blockchain and public Blockchain. Therefore, it is necessary to regulate behaviors of nodes with effective ways, to form a stable order, to be suitable for business and to avoid upper limit abuse by others at the same time in case of garbage data expansion.

The tokens of Inchain need a circulation, so it is not suitable for them play as intermediaries. Therefore the Inchain proposes a dual intermediary system of tokens and credit. Conforming to the business arrival of the Inchain and users' flow lines, it is necessary to design the credit system as a management and value link standardizing user behaviors.

(III) The Credit System of Inchain

Based on the credit system of Blockchain, there may be a big wave. The credit system of Inchain has been in a management and value link after combining nature of business. Credit, as a norm to regulate the behaviors of the clients, cannot be a reality and in circulation, and it is a good behavior of the users.

The purposes of credit includes but not are limited to participating consensus, transfer fees discount, modify aliases, transfer of goods, application for senior arbitration and participating in business targeted activities. Currently, the Inchain has realized participating consensus via credit, credit penalties for consensus violation, modifying the alias and consuming credit and credit consumption via transferring second-hand goods. As one value intermediary in the whole system, the credit will develop more user codes of conduct gradually in virtue of its link role.

Credit acquisition: as a value intermediary paralleled to the tokens, the credit does not a price with actual interests, but just complies with system rules and maintains good user habits. The obtained credit acquisition realized currently is transfer within

24 hours, and much reasonable credit will be added in the latter to obtain the sources.

VII. POC Consensus Mechanism

Any Blockchain project requires a consensus mechanism to reach a consensus among the opposite nodes distributed the globe and states of the data. The Inchain aims to develop a set of consensus system with efficiency and self-maintenance to adapt to the business orientation of the Inchain, so the POC consensus comes out.

The full name of POC is Proof of Credit in Chinese, referred to as POC.

The POC consensus mechanism of the Inchain solves the performance problem of POW, the problem of uneven equity of POS, and the problem of illegal processing efficiency of DPOS.

So what is the POC on earth?

POC refers a system based on the Inchain credit system, adopting uniqueness and certainty of existing Blockchain account book, coordinates nodes to determine single point broadcast permissions and verification.

(I) Consensus Admission

As a public Blockchain, the consensus nodes cover the clients, and whole network will not run with stability and security in accordance with protocols until the behaviors of users are regulated. POW regulates nodes in virtue of competition indexes; POS regulates node behaviors in virtue of number of holding tokens and tokens ages, DPOS elects the trustees in view of votes; these currently popular consensus, in addition to POW in terms of principles, (in fact, the difficulty regulation of pow also uses existing account books), the others select nodes boasting of single-point broadcast permissions by adopting the certainty of account books. Therefore, the consensus set orders will be gotten according to the certainty of data account books on chains.

The consensus threshold of Inchain refers participation when the credit reaches a certain value. It is difficult for this way for the credit is needed to be accumulated and because it is a as an open source public Blockchain, the attacker may attack a network consensus after preparing for a long time.

The introduction of economic sanctions mechanisms in Inchain prevents this situation, because the benefits obtained by attackers will not be less the loss, which refers increasing the cash deposit mechanism as a supplement on the basis of the credit.

Some people say: it is fine to cash deposit the cash deposit directly and credit is redundant! This is because the consensus situations are extremely complicated, and some are not suitable for economic sanctions, such as the consensus nodes computer crash, network dropping lines; if there is no credit admission, systems cannot identify and exclude such nodes; if the unified economic sanctions are adopted, a large

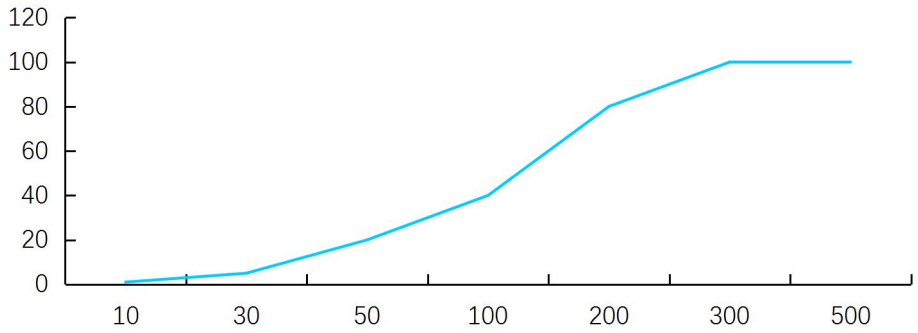
number of users will be shut out. Besides, the rights of credit guarantee systems shall not be monopolized by a large number of money-holders. As one value intermediary in the bottom, the credit is bound to usher in a more extensive prospect and crucial purposes.

(II) Floating Cash Deposit Mechanism

Because the consensus of the Inchain will reach a consensus without needing a frequent communication among nodes (described below), the performance of the Inchain is not affected by the number of consensus nodes, and the performance of the 100 nodes and 1000 nodes is almost same. Therefore the Inchain adopts innovative floating cash deposit mechanisms to balance the income of consensus nodes.

The Inchain network dynamically calculates the cash deposit required for the participation in consensus currently through the number of current consensus nodes and a linear growth algorithm.

```
recognizance = maxRecognizance * ((Math.log(size/Math.log(2)) * size) / Math.log(maxSize/Math.log(2))
```



It can be seen from the above cash deposit calculation formula that the cash deposit required to participate in the consensus increases linearly with the increase of the number of consensus nodes; when the number of consensus nodes reaches a maximum number, the cash deposit also reaches a maximum value.

(III) Verification to the Whole Network

The whole network will strictly verify the applications and exits of any node consensus.

1. The Verification of Credit

When any node requests to become a consensus node, other nodes will firstly verify credit value of the nodes; if the credit value is lower than the admission threshold, then the request from this node will be discarded.

2. The Verification of the Cash Deposit

The corresponding cash deposit should be submitted for any request of consensus application. Unlike the transfer, the cash deposit recipient submitted is an intelligent contract script which has strictly imposed a mandatory specification for the

redemption of the cash deposit. The whole network not only verifies the credit and cash deposit applied for a consensus request, but also the intelligent contract script of redeem of cash deposit, and highly defines the security of the cash deposit.

3. Cash deposit Redemption Verification

The consensus protocols of Inchain include economic sanctions system, so the cash deposit submitted by nodes does not use a traditional way of freezing; in the operation of systems, once nodes severely illegal are found, any integrity node is able to fine the node cash deposit. As a matter of fact, the node cash deposit is submitted to an intelligent contract script, and in an aimless state, so in order to keep this fund secure, verification will be strictly conducted to requests for any consensus withdrawal or punishment; the verification rules include a strict protocol that it is impossible for any person o take away the cash deposits of others, and it is impossible for anyone to arbitrarily fine them of others.

4. Sanctions Verification

There are signatures at each block heads of Inchain, so the evidence of cryptography will be left when someone tries to do evil things.

When the consensus nodes are overtime and out of the block, or fail to get out blocks as a result of computers crash and other non-human factors, the whole network is bale to monitor the perception, and degrades the nodes as ordinary nodes the first time. Although there is no evidence of cryptography for this situation, verification evidences are still needed to be provided of the whole network and its nodes.

Any node will impose sanctions on other nodes, and must provide a reasonable or evidence of cryptography, so it will be verified and accepted by other nodes in the whole network.

(IV) Determination of Single Point Broadcast Permissions

Combining the theoretical knowledge mentioned in the previous sections, this section will provide a more comprehensive POC operating principle and details.

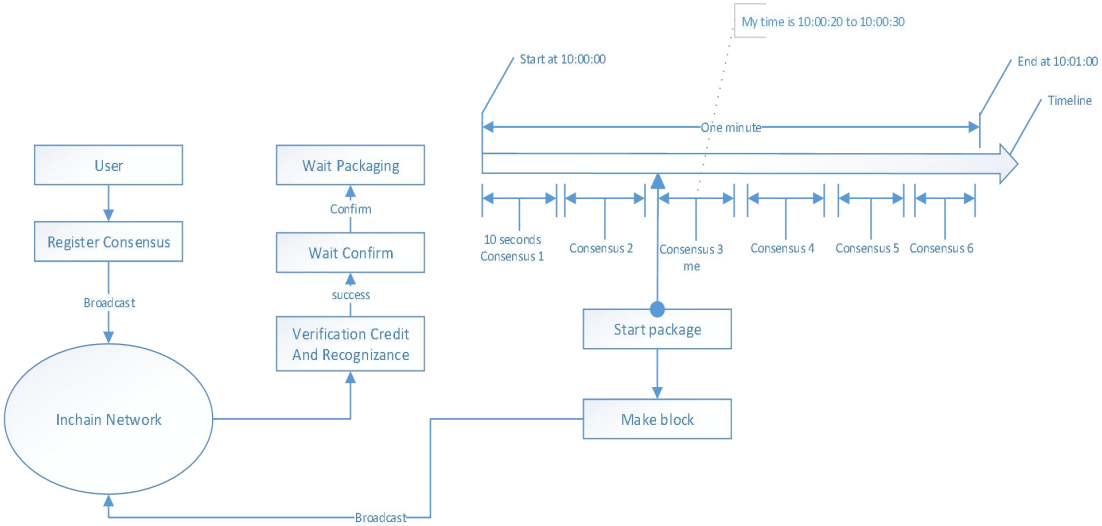
Some explanations of terms:

- **Consensus node:** meet the credit admission threshold and successfully apply for a consensus node
- **Consensus rounds:** a consensus round refers a full time period when all consensus nodes take turns out of blocks. Each consensus round has a start timestamp and an end timestamp, and the end time of last round is the start time of the current round, so the nodes must follow this time rules, otherwise any changes will be rejected by the whole network. In each consensus round, all consensus nodes have and only have one right for broadcast blocks.
- **Consensus order:** in a consensus round, the consensus order refers the orders of each consensus node. In the consensus of the Inchain, the order of each round is randomly changed, and according to the start timestamp of current one round (that is, the end timestamp of last round) and the consensus node accounts, calculate the orders. All nodes (including non-consensus nodes) must comply with this rule in order to realize a normal operation, and any even minor changes,

will lead to changed node to be rejected by the whole network.

- **Consensus period:** after determining a consensus order, each node is mapped to a time period, so the single point broadcast permissions are naturally determined; during this time period, there are also a start time and end time, the interval is the block time, known as a consensus period.
- **Block permission verification:** each block head is marked with the start time, time information of consensus nodes and their signatures in the current round and the legitimacy of blocks are verified through information.

A Complete Operation Flow of POC



1. Application consensus
2. Verification credit and cash deposit
3. Application includes entering blocks with determination
4. Wait for the end of current consensus round
5. The next consensus round begins after the end of last round, and the next round becomes the current round
6. Determine the number of people in current consensus round
7. Initialize the current consensus round orders and each node calculates its own consensus time period
8. Receive new blocks, verify and monitor the block rights and wait for personal own time period coming
9. Pack blocks after reaching its own consensus time periods
10. The package program obtains new trading and verification in memory pools
11. Stop package when it is estimated in personal consensus time periods
12. Ask whether there are violations to be dealt with of the fault-tolerant monitor unit and release credit
13. Verification of block trading data
14. Broadcast blocks to the whole network
15. Continue to receive new blocks, verify and monitor the block rights and wait for next round coming

(V) Mechanisms of Fault-tolerant Monitoring and Punishment

The Blockchain system is a very complicated, not only because of the complexity of the bottom technology, but also the extremely complicated operation environment, especially the public Blockchain. A normal operation of the system will be affected by using habits, network environment and man-made damages. The consensus mechanism of Blockchain will effectively solve the impacts brought by these factors.

As for the POC consensus mechanism of the Inchain, any action of the nodes will be supervised by other nodes in the whole network. The innovative consensus of Inchain will punish the following circumstances, and the entire system will adjust itself and maintain stability.

1. Within blocks, deduct a certain credit value, and downgrade to ordinary nodes.
2. Non-human factors like without blocking on time or network synchronization delay, make decisions cording to selections of other nodes in the whole network; it is fine if the next block cites this block; the block will be lonely if it is discarded by the next block and what it will face is a credit penalty and downgraded to a ordinary node.
3. Random broadcast block non-consensus nodes, and discard directly if the verification is not passed.
4. A number of broadcast blocks in the same time period seriously violate types, and will be confiscated security and blacklist credit.
5. Package double flower transactions seriously violate types, and will be confiscated security and blacklist credit.
6. Attempt bifurcation systems from old blocks in chains, and the so-called double flower attack is a serious violation of types, and will be confiscated and blacklist credit.

Type 4, 5 and 6 are in a serious violation, and can be monitored through the whole network with the evidence of cryptography; any integrity node is able to exercise punishment as long as only any integrity node submits one or more block header information including signature; confiscate the cash deposit in this node to community finance accounts and deduct the credit value of node 999999, and the punished node will never commit bad things again permanently.

(VI) Advantages and Shortcomings POC Consensus Mechanism

Advantages:

1. Energy saving: take up few the system CPU and memory resources.
2. High efficiency: reach a consensus without extra network communication among nodes.
3. Stability: system can adjust the operating states and maintain high degree self-maintenance.
4. Safety: over 50% of fault tolerance
5. Innovation: introduce the dual value intermediary mechanism for the first time

(credit and tokens).

Shortcomings:

Like all public Blockchains which allow bifurcation but points are needed to be checked. But the POC is a short-term bifurcation, and the fault-tolerant detectors will solve problems generally in about two blocks of time.

(VII) POC Conclusions

The biggest highlight of POC is to deal with bad conditions timely, and although the system's self efficient maintenance is difficult in the realization of technology, the Inchain team had done this.

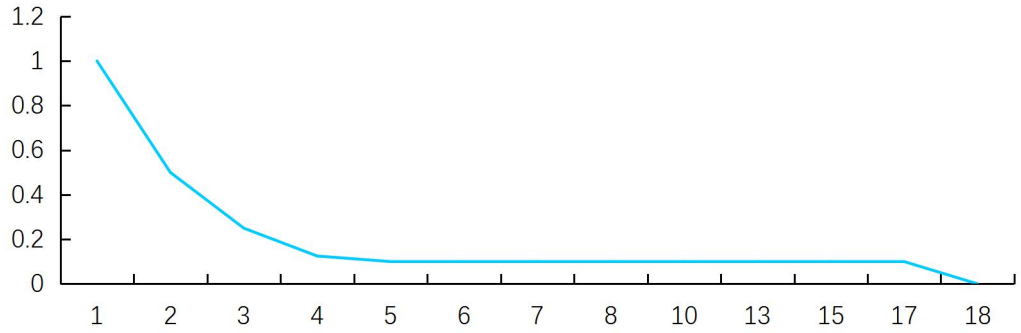
The team has a continuously optimized program to make POC gradually perfect to meet the growing business needs.

1. Introduce advanced compression technology in nodes communication.
2. Optimize new blocks to synchronize to flows of the whole network.
3. Realize isolation witness technology reduce the sizes of the new block broadcast.

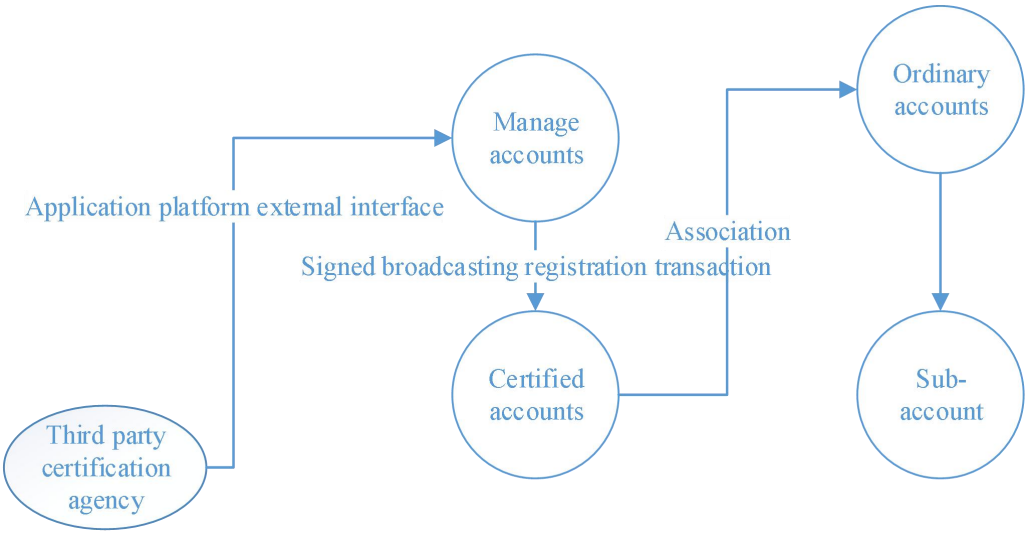
The TPS in the whole network will be greatly improved through the optimization of three aspects above.

(VIII) Incentive Mechanisms

Like other public Blockchains, the Inchain conducts an incentive policy to consensus nodes. The reward section is 10% of the total, and is gradually distributed through the new block of coinbase transactions. The block interval of Inchain is 10 seconds, and in the first year, each block outputs 1INS, and reduces by a half each year later and until 0.1INS for each block, and maintain this value. The consensus reward of Inchain will be distributed out about 17 years and the business will be forced to establish nodes maintenance network in the
future.



IX. Account Classification Certification System



The Inchain system account is divided into an administrator account, a certified account, a general account and a subaccount.

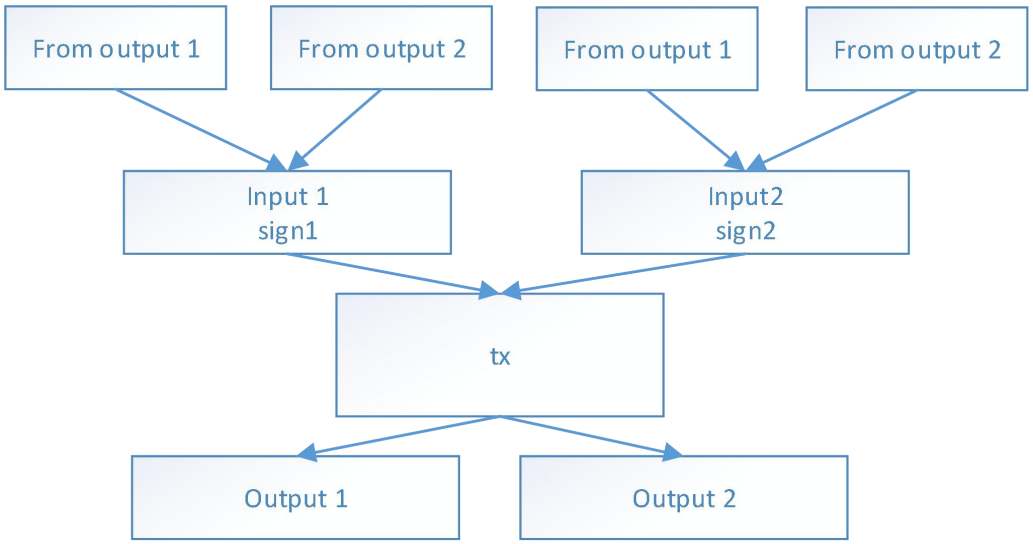
Administrator account: it is just one more registered business authority, and is similar with authentication account in other aspects.

Certification account: nothing can be accomplished without norms or standards. The Inchain will serve as a business and reviewer in the future; cooperate with third-party professional certification agency to submit the rights through the interfaces. All certified accounts must be signed by the administrator account before they will be accepted by the Inchain network.

Ordinary account: the accounts used by majority of user groups of Inchain include the basic functions of the Inchain clients, goods verification and goods transferring.

Sub-account: the authentication account can be associated with the general account as its sub-account. After the association, the sub-account is able to add traceability information to the goods produced by the authentication account.

X. Improved UTXO Trading Model

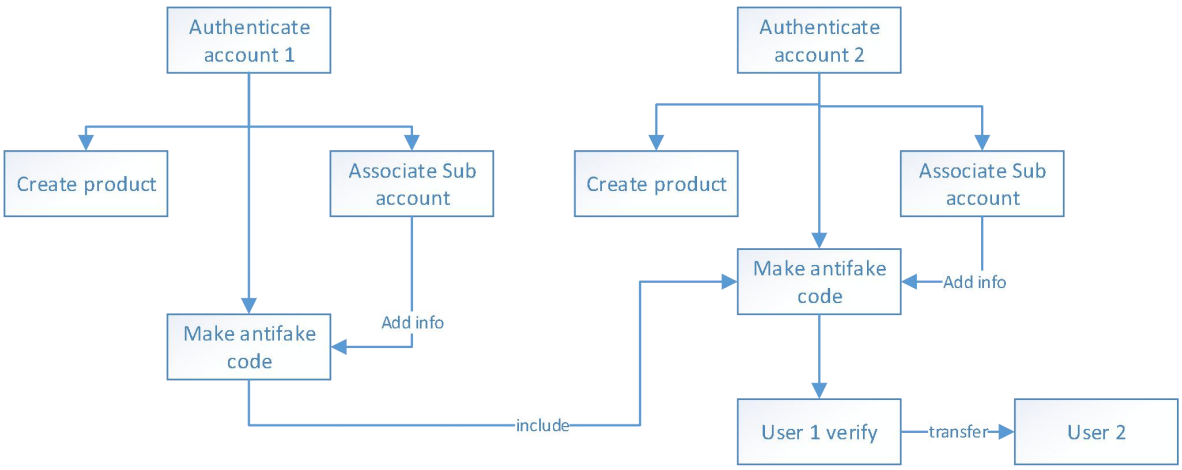


The trading models of Inchain mostly adopt UTXO model. Combining the account systems of Inchain, the improved UTXO model has improved efficiency and reduced transaction sizes.

Improve details: introduce multiple transactions merged into the same account, and share one signature.

XI. A General Bottom Protocol Specially Designed for Business Applications

The bottom of the Inchain is designed for business applications and a set of application protocols completed currently are able to accommodate many business scenarios.



1. Certify account information and flexibility of product information, use common key values to type -in any form of data information.
2. Certify accounts and create goods
3. Certify the only one ID in the whole network of appointed goods produced by accounts. (It is called security code in systems)
4. Certify accounts associating sub-accounts
5. Certify the unique ID associated information of sub-accounts associated by accounts (flow trace information).
6. Certify that when accounts produce the unique goods ID, it can introduce the unique ID of other goods in the whole network. (Form sources traceability)
7. Verify unique ID of goods by ordinary accounts.
8. Transfer of the ownership after verifying goods by ordinary accounts.

The above business process protocols have been realistic in the Inchain clients (purse) and open to all third parties through the PRC.

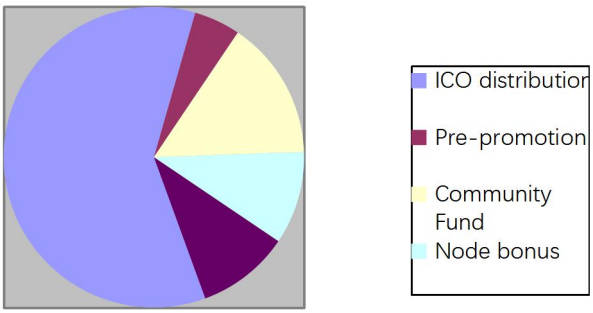
At present, the Inchain team has developed the first application based on the Inchain network-- a core function of security traceability application platform.

This set of bottom application protocol of Inchain is not only suitable for the security traceability of goods and based on this protocol, it is possible to develop systems like *Small and Medium - sized Employee Picking System Based on Blockchain* and *An Interior Management System Based on Blockchain.*

XII. The Business Applications and Arrival Plans of Inchain

For business applications and arrival plans, please refer to the *White Book Second Edition - Business Applications.*

XIII. Token Parameters and Assignments of Inchain



The Inchain has its own system tokens: INS, with a total amount of 100 million.
ICO distribution: 60%;

Pre-promotion: 5%;

Community Fund: 15%;

Node bonus: 10%;

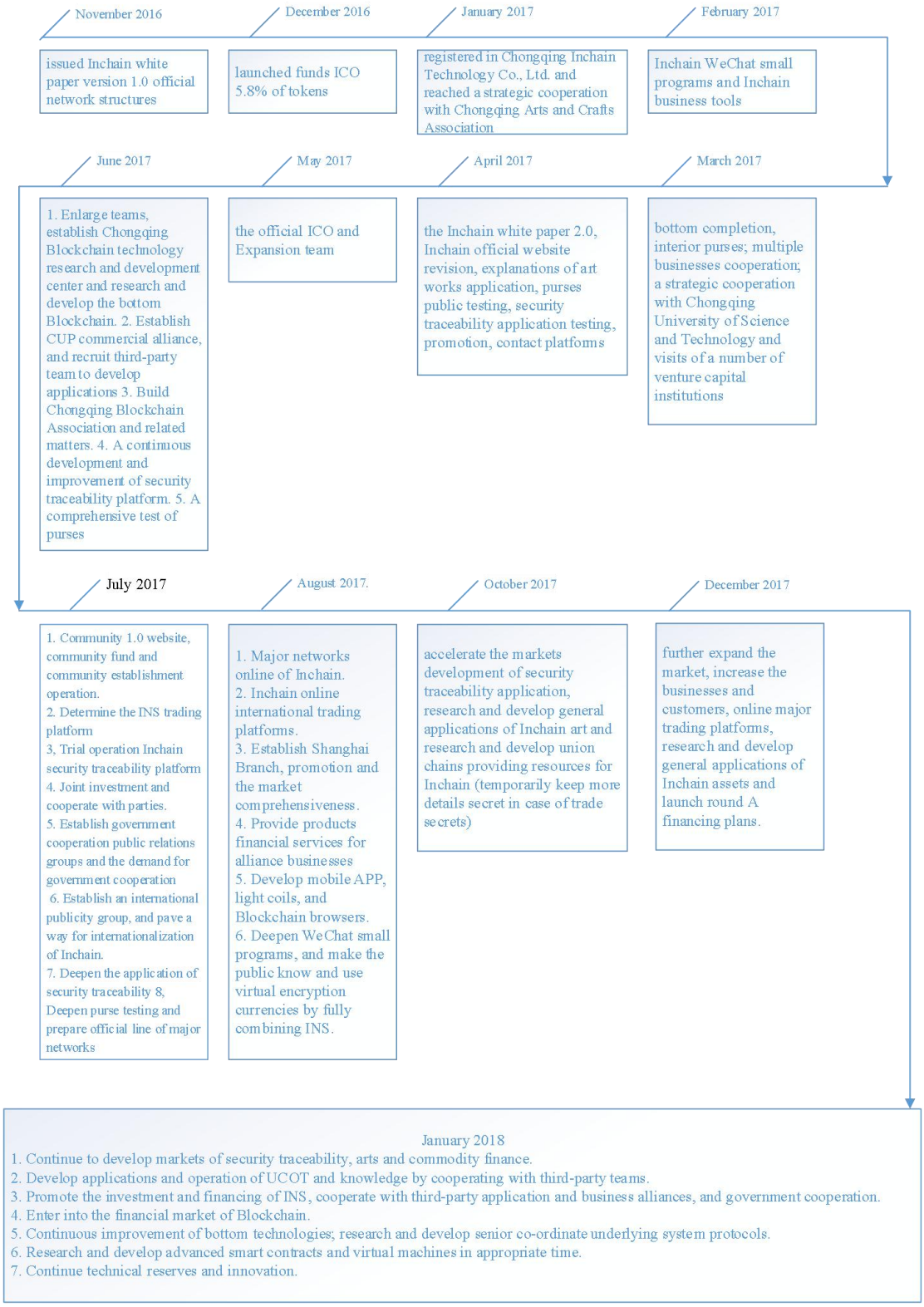
Team: 10%;

Statement: if here is the remaining for previous promotion, it will be transferred into communities (if the remaining is 1%, the community funds will be 16%), and in the charge of communities; for management methods, please refer *Inchain Community White Paper*;

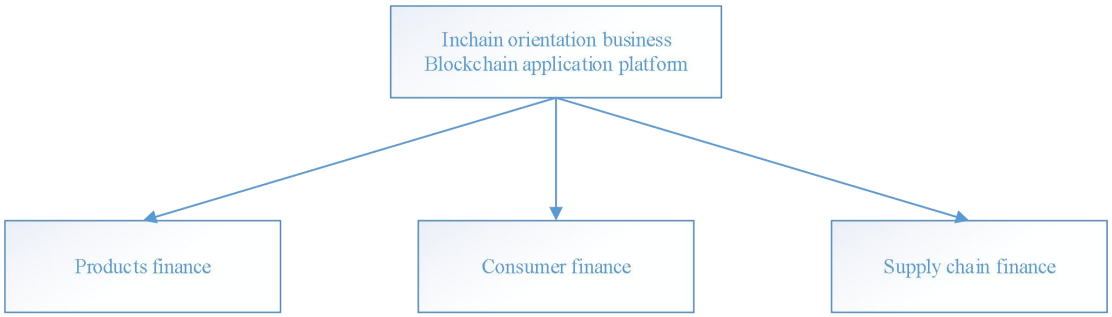
The team has held partial official on-line technologies with two years;

For node reward distribution, please see the specific *Node Reward Rules.*

XIV. The Development Routes of Inchain



XV. The Ultimate Goals of Inchain



One goal for Inchain is to reach a minimum of $ 3 billion of tokens in the market for three years.

Launch over 10 arrival applications in three years, accumulate millions of users, and thousands of businesses.

Profits achieved of security traceability in four years.

The company will be listed after seven years.

Conclusions

Big environment:

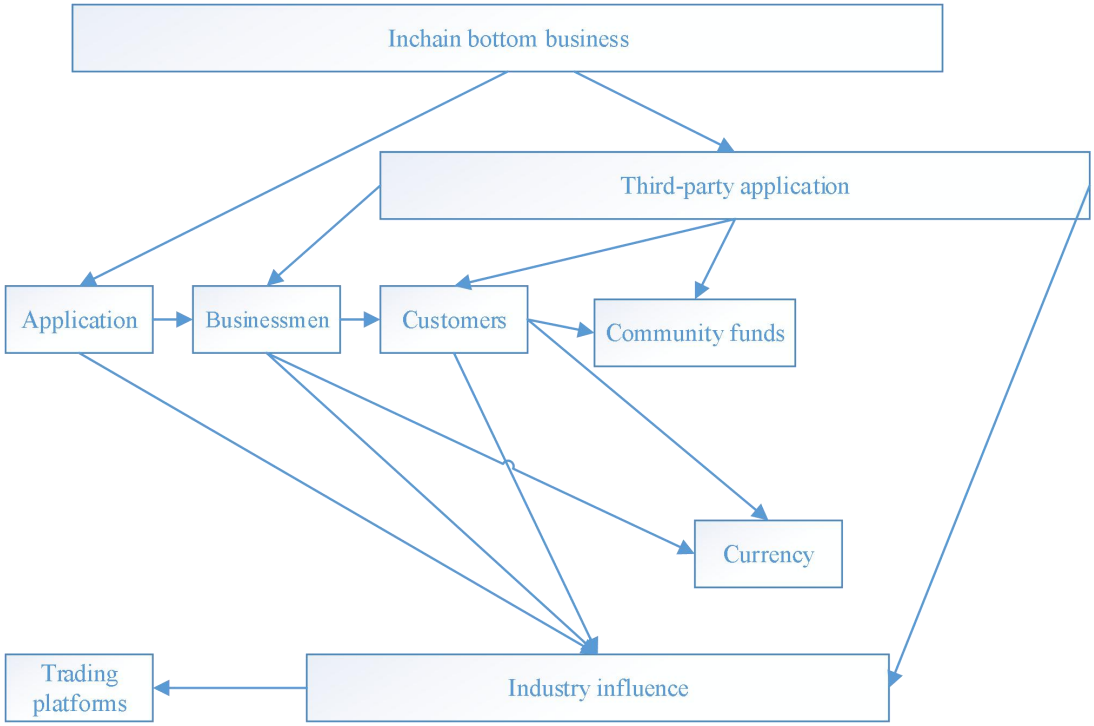
Blockchain outlet, the nature of public welfare, international supports, the Chinese market, the popular of Internet economy, and great pressure for enterprises restructuring.

Team:

Legitimacy, self-discipline, integrity, earnestness, practice, long-term vision, clear strategies, the orderly development, advanced technologies and concepts.

Direction:

Ecosystem construction



Ecosystem Map

The Inchain is equipped with clear understanding of industries, complete strategic plans, high efficient implementation team and an opening and developing attitude. We welcome businessmen in all walks of life to join us, and far-sighted personages to build this ecological cause together.