Version： V1.0.0

# SimpleChain

## Whitepaper Beta

SimpleChain Foundation©

2018.12.24

# Copyright Notice

# Abstract

Through years of development of blockchain technology, the industrial effects has gradually formed. User cases and applications are growing with further acknowledgement of the distributed digital economy as a trend. On practical side, however, technical issue along with business mode issue are continuity exposing across different aspects. The SimpleChain, therefore is designed to initiate a revolutionary way to propel the development of blockchain technology and application. With goals of construct a flexible, scalable, stable technical infrastructure and an inclusive, healthy ecosystem, the SimpleChain innovates this architecture.

Proof of Work, the first blockchain consensus conducted by Bitcoin has since be operated for years and verified as the most stable algorithms. Hence, the underlying structure of the SimpleChain has been set as the similar Proof of Work with innovative algorithm. For encouraging the computing power to be distributed, SimpleChain Node Client is published for any computing devices to run as the computing power source easily.

The Proof of Work blockchain layered as the bottom of SimpleChain architecture, which is called the Main Chain. The primary goal for the Main Chain is to secure the unification and finality of distributed ledger data. However, the flexibility could be provided by a second layer on top of the Main Chain, which is called Sub Chain. The Sub Chain periodically interchanges data with the Main Chain to make sure the network stability and ledger security is in line with the whole network, meanwhile, the Sub Chain is customisable for any specific consensus algorithm for applications. As a Sub Chain, apart from the blockchain head, transaction data structure is also flexible in different cases to maximise the compatibility of the SimpleChain.

Within the realm of Sub Chain, sharding mechanism is applied to satisfy Sub Chain developers for enhancing the efficiency of transaction verification on the blockchain. The scalability issue, therefore, is resolving under this design.

In addition to the technical architecture, for a healthy ecosystem, the digital asset on the blockchain will play a key role to bind the community developers, application users and other end clients together. The production of original digital asset SIPC is mined from the Main Chain Proof of Work algorithm with periodical total supply limit for a cryptoeconomy stability. At the same time, an inflation will occur along with the need from any Sub Chain system to escrow or circulate the SIPC within the Sub Chain cases. A circulation system therefore will be healthy for a growing number of Sub Chain system that no value appreciation of SIPC could stagnate the expansion of the ecosystem.

In order to form an open, transparent and consistent distributed community, an inclusive policy is proposed and embedded in the genesis block as a part of the SimpleChain running mechanism. The creator and initial operator of the SimpleChain is the SimpleChain Foundation – a non-profit organisation whose mission is to promoting and supervising the growth of the SimpleChain open source community. The foundation has neither pre-distributed nor pre-mined SIPC at the very beginning of the SimpleChain. Every block along with the incentive reward need to be mined through the contribution of computing power, and only a 5 percent of the computing power rewards will be donated to the predetermined foundation address in the first year. Annually, that donation percentage will be halved, so that the community become fully distributed gradually.

The SimpleChain is a cornerstone for compatible and practical distributed digital economy.

# Contents

# Figure Contents

# 1 Blockchain Current Situation and Problems

## 1.1 Multi-style Development & Relatively Stable PoW

Since the Bitcoin Whitepaper first introduced the blockchain as an underlying technology concept of a peer-to-peer electronic cash system [1]，the blockchain has derived as a comprehensive technical architecture with various types of technical structures，from the degree of openness, it is divided into Public Blockchain and Permissioned Blockchain. According to the diversity of participants，the Permissioned Blockchain can be divided into Consortium Blockchain and Private Blockchain [2][3].

From the consensus mechanism of the blockchain core, it has evolved into different types of algorithm forms such as proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), and Byzantine-Fault-Tolerant (BFT). The arms race and centralized computing power caused by the PoW mechanism in the Bitcoin “mining” process lead to a large consumption of energy. At present, the power consumption of Bitcoin “mining” has exceeded 64 TWh for the whole year [4], approximately $3.3 billion in costs, which means the cost of miners’ verification for each transaction in Bitcoin is at around RMB 100.This large amount of resource consumption makes the PoS mechanism come into being. PoS uses an algorithm to calculate the equity owned by each node and allocates the probability of obtaining the accounting rights according to the equity ratio[5].

The DPoS mechanism was first proposed by BitShares, which can be understood as the representative democracy in reality, that is, agent node exists before each consensus, holds responsible for signature verification of the entire network transaction. Since the number of nodes that require signature verification is relatively small, the efficiency of transaction confirmation will increase a lot. [6]

Tracing back to the source, the earlier consensus mechanism can be traced back to the problem of Byzantine General proposed by Leslie Lamport, Robert Shostak, Marshall Pease (1982)[7]. That is to say, in the untrustworthy environment of all parties, when the cost of instant communication is zero, it is difficult for participants to reach a final consistency. The paper also suggests that when the untrustworthy participants are below 1/3, the entire network can achieve Byzantine fault tolerance（BFT）. In the development process, Byzantine fault tolerance further reduced the complexity of the algorithm from exponential to polynomial, forming a practical Byzantine Fault Tolerance (PBFT), improving efficiency, and being able to process thousands of requests per second, thus applying in practical systems becomes feasible [8].

The way to use PoS as consensus mechanism in the main chain is increasing day by day. For example, PeerCoin and NextCoin add parameters such as currency holding time and currency holding amount to the consensus algorithm, which realizes block creation that does not need to consume a large amount of computing resources to some extent as well as reward and extension mechanism. However, there are still few large-scale main chain based on PoS mechanism that have been running continuously. The Casper consensus of Ethereum has not yet been switched, so its stability remains to be verified. PoS requires users to be online all the time. Otherwise, when some nodes are offline, other nodes may conspire maliciously to forge blockchain history records and form long-range attacks [9]. In addition, the open PoS consensus is also unstable at the convergence rate. Although the blockchain of DPoS mechanism improves the convergence rate but does not support the expansion of the verification node, the performance efficiency decreases when the number of nodes increases. Therefore, EOS based on the historical development of Bitshares proposes Consortium Blockchain structure that supports only 21 super nodes. As a consensus mechanism system applicable to the Consortium Blockchain, PBFT needs to confirm the number of nodes before starting the blockchain, and does not support node increase or decrease in the process of consensus, and it also has the problem of node expansibility limitation. At present, the chain consensus practice of more than 100 nodes has not been completed [10].

Although PoW consumes a lot of energy, it is still a relatively mature consensus technology in various blockchains. After long-term stability practice of large-scale blockchains such as Bitcoin, Ethereum, and Litecoin. Fault tolerance and incentive mechanism are also better reflected. The dynamic joining and exiting of users have become the basis for the true opening of the blockchain under the PoW consensus mechanism [11].

## 1.2 Overpowered Computing & Inefficient Performance

As a relatively mature and stable consensus algorithm in the emerging technology of blockchain, PoW still has the problem of computing power competition and monopoly in the application. Taking the Bitcoin blockchain as an example, the current whole network has formed a hash computing power scale of more than 30000P per second (BTC.com, 2018)[12]. While the world's most advanced super-calculation system Summit's second computing power is 122P (Top500, 2018)[13]. Although the supercomputer performs floating-point operations, in the Bitcoin blockchain network, it means that even if the world's top 500 supercomputer systems are powered on to hash at the same time, it is also difficult to reach half of the 30000P computing power, which means that it is difficult to complete a 51% attack on the Bitcoin blockchain from the outside. Therefore, the continuous expansion of Bitcoin mining machine computing power and the continued consumption of energy has actually lost its meaning. The mining method of calculating the hash value alone also makes the expansion of the computing power become a pure consumption.

However, within the Bitcoin blockchain network, there is a monopoly trend in the pattern of computing power distribution. Since the birth of the first Bitcoin mining machine in 2012, the continuously upgraded ASIC chip has surpassed the computing power of any other devices. The mining pool consisted by mining machines has become the “big node” of the Bitcoin network, and the power tends to concentrate. Fortune magazine disclosed that a mining machine producer has centralized control of Bitcoin computing power by operating a mining pool, selling AISC mining machines, which dominated Bitcoin hard fork and made BCH (Bitcoin cash) come into being. Not only that, the birth of the forked coin directly competes with Bitcoin for computing power. According to the “Tai Media” report, in the beginning of 2018, a mining machine producing company's market share of bitcoin mining special ASIC chips was nearly 80%, occupying an absolute monopoly position, which directly control about 30% of the total Bitcoin network computing power. As long as the Bitcoin price is profitable, the computing power is still expanding and competing.

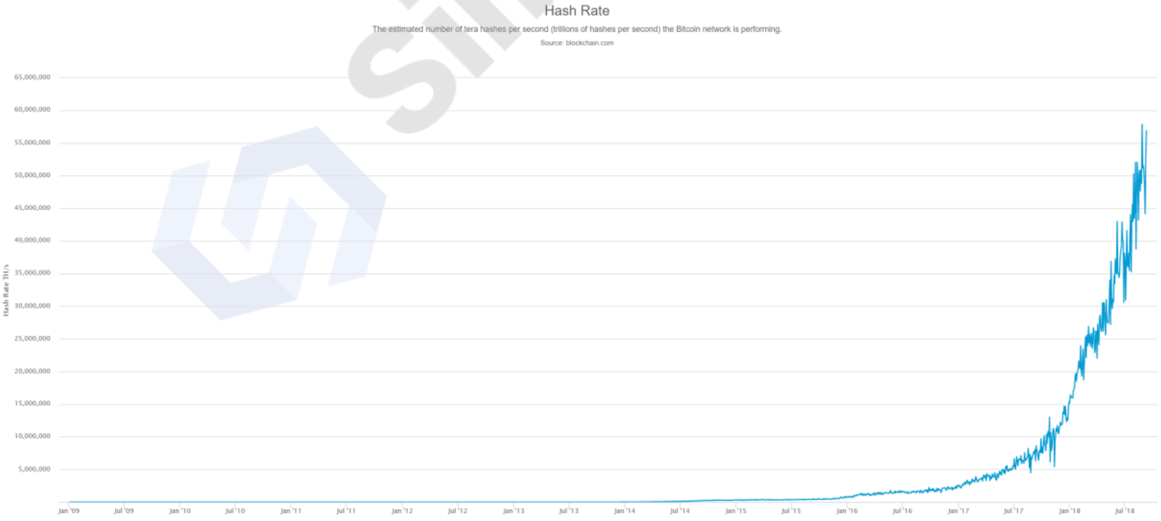

**Figure 1 Bitcoin blockchain computing power**

The industry has gradually formed a consensus that excessive computing power output will eventually result in waste, rather than an effective proof of workload. We know that Bitcoin mining is doing a series of hash algorithm, and outputting a lot of computing power to figure out a series of meaningless answers, so it is denounced as a waste of energy. But not all computational activities that consume a lot of computing power are wasted, such as artificial intelligence (AI). The computing power provided by the blockchain and the computing power required for AI are essentially the set of computing power that the computing device provides to support the logical operation, but the results are significantly different. After training and simulation, AI consumes a lot of computing power to form the result of a logical event. Therefore, we hope to combine the blockchain and AI to match the large-scale computing power output with the demand to form an effective proof of work (EPoW).

## 1.3 Expansion and Contradiction of Economic/Social Incentives

With the scale expansion of the application and the deepening of the scene of blockchain technology, some contradictions are gradually exposed, which has become an urgent problem to be considered and solved in the development of the industry. The contradiction is mainly reflected in four aspects:

### 1.3.1 Internal Development Direction Contradiction

In the past few years since the birth of the blockchain, there have been many cases in which the blockchain has been forked due to disagreement in community opinions or interest disputes. In addition, various blockchains for vertical industries have their own characteristics, and there are only few of public blockchains that can fully meet the needs of various applications.

The first influential hard fork in the blockchain should be the forked event of Ethereum. A well-known project in the Ethereum, The DAO, due to its own loopholes, caused hackers to steal the ETH, which was worth about $60 million at the time. In July 2016, the Ethereum development team revised the code of the Ethereum software, in the 1920000th block, all funds of The DAO and its sub-DAOs are forcibly transferred to a specific refund contract address, thereby "recapture" the DAO contract currency controlled by the hacker. Since some miners did not agree with this modification, which formed two chains, one for Ethereum (ETH) and another one for Ethereum Classic (ETC), each representing different community consensus and values. When this hard fork occurred in Ethereum, two blockchains were created.

BitMEX Research (2018)[14] counts historical events of Bitcoin consensus forks and finds that at least three of these events caused a clearly identifiable blockchain fork. The most influential hard forks divides the Bitcoin blockchain into two, and Bitcoin Cash (BCH) becomes a new chain. The reason for this fork is the difference in the way the Bitcoin community expands its capacity.

## 1.3.2 The Existence of Impossible Triangle

From bitcoin, Ethereum to the now-popular public chain projects, practitioners want to find a blockchain that can adapt to large-scale commercial use. However, the immature blockchain technology is still a realistic problem facing the industry at this stage. The article named <*Impossible triangle: safety, environmental protection, decentralization*>[15] publised in 2014 proposed that the blockchain technology has the "impossible triangle" of performance, that is, the three aspects of decentralization, safety and environmental protection cannot be satisfied at the same time. In April 2018, the " Chain Intelligence Core of Blockchain" forum combined with the current popular consensus mechanism to discuss the "impossible triangle" viewpoint again [16], that is, security, efficiency (non-computational), decentralization (computational) can not coexist, and the existing sidechain or sharding technology is between decentralization and efficiency.

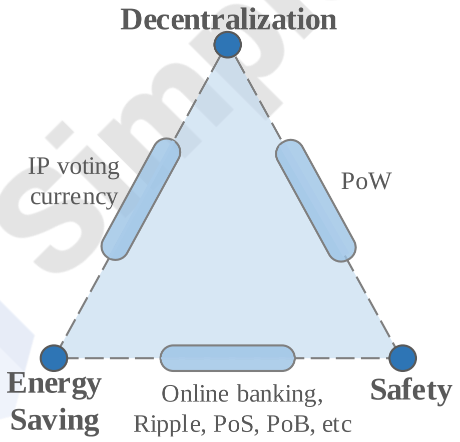

**Figure 2 Impossible triangle of blockchain**

The Bitcoin blockchain has chosen decentralization and safety, but the computing power mining has led to criticism of energy waste. The problem at the same time is the sacrifice of scalability. If you design a cryptographic currency that is both environmentally friendly and secure, either it is a centralized architecture or its decentralized architecture cannot be maintained. For example, Ripple and PPcoin essentially do not break through the centralized verification mechanism such as PayPal and online banking. The "representative democracy" such as POS and DPOS is only to meet part requirements of decentralized centers. In order to achieve a million-level TPS, EOS only completes the consensus by campaigning for 21 super nodes, sacrificing decentralization, but in fact, security also cannot be fully guaranteed.

However, there is no point to sacrifice safety for decentralization and environmental protection. It can be seen that the result of trying to balance three factors on one chain is unsatisfactory.

### 1.3.3 The Contradiction between Demand and Cost

One of the characteristics of the public chain is that anyone can read and write data. Any node on the network can participate in mining to help witness and complete transactions. Mining requires miners to provide computing power, storage and other resources as well as electricity costs. Therefore, the transaction initiator needs to compensate to the miners. This fee is called formalities fee (miner fee). From another perspective, thresholds therefore has seen set to prevent spam from flooding into the public chain, affecting performance or user experience.

Bitcoin has created a mechanism for blockchain accounting rewards. The tokens are distributed through the chain to stimulate nodes to complete transaction and jointly maintain the blockchain network. The combined cost of collaboration is still much lower , more secure and more reliable than a centralized system. However, due to the small amount of transactions supported per second, the concentration of demand on the chain has caused network congestion, and the miner fee has risen. As it can be seen from the figure, the handling fee for each transaction of Bitcoin has experienced several skyrocketing, and the increase in 2017 is about 15 times. The cost of completing a transaction at the peak period is nearly 150 US dollars.

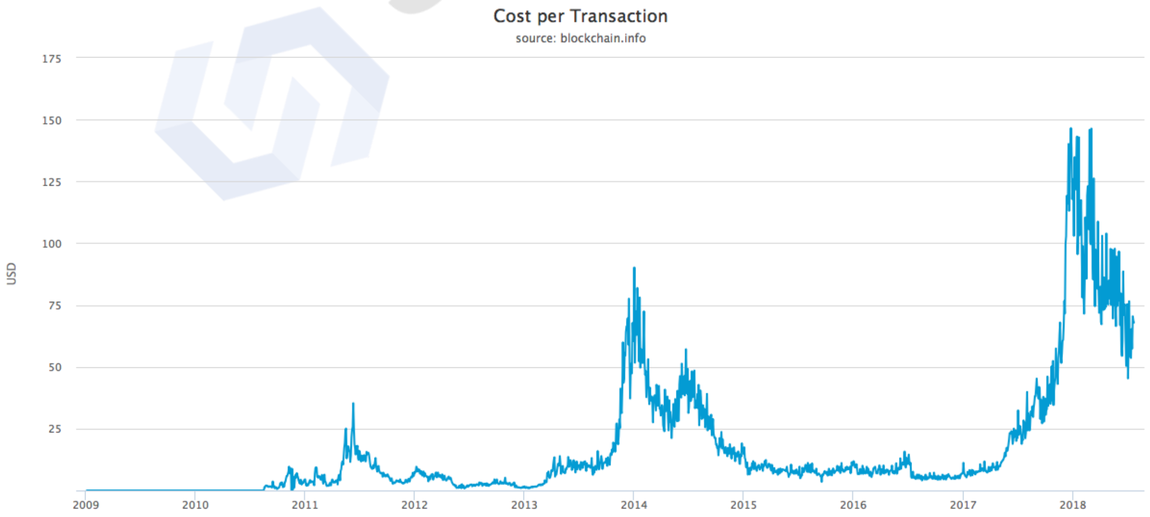

**Figure 3 Fee for each transaction**

The concept of Gas was introduced in the formality fee of Ethereum. Gas consists of two parts: Gas Price and Gas Limit. Gas Price (unit：Wei, 1ETH=$10^{18}$wei) refers to the cost that the user is willing to pay for performing an operation or confirming a transaction. Gas Limit is the maximum amount of Gas the user is willing to pay. The Ethereum official website records the Gas Price for each transaction in history. We convert it to US dollar units. It can be observed that the formality fee experienced two skyrocketing at the end of 2017 and June 2018.The reason may be related to the hot application of the two periods.

At the end of 2017, due to a sudden popularity of the blockchain game CryptoKitties based on Ethereum, it occupied a lot of Ethereum network resources, which caused the Ethereum network to be paralysed. In order to reach the transaction, users continuously pushed Gas Price higher, and at that time ETH was in the bull market, the ETH price surged to new highs again and again which made the transaction fee reach a historical peak. In June 2018, Fcoin exchange based on the Ethereum proposed the concept of “transaction is mining”[17]. By attracting users through the money-burning subsidy and the profit repurchase model, the crazy trading volume once again caused the Ethereum network congestion. Because the ETH price was almost drop 50% compared with the time of the 2018 New Year, the transaction fee for the dollar unit was relatively low, but it was still 2-3 times the transaction cost as much as the non-congestion period.

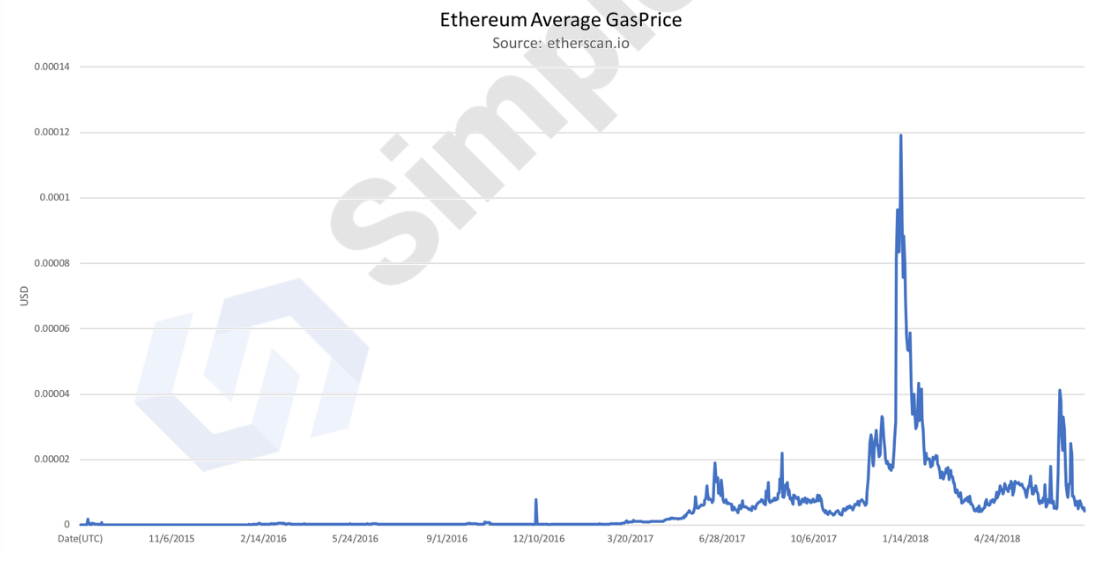

**Figure 4 Transaction cost**

A similar situation also occurred on the EOS blockchain. RAM (Random Access Memory) is a storage resource required for application development on EOS. At first, RAM was allocated based on the number of EOS tokens held, but those who held a large number of EOS tokens were not developers, which may result in a waste of limited RAM resources, especially when facing the public chain expansion and performance challenges at present. Thus, EOS created a RAM trading market based on the Bancor algorithm to improve RAM circulation. Market speculation caused the price of RAM to soar in a short period of time - 54 times in 13 days [18]. For developers, there is no doubt that the development and operating costs of applications will increase dramatically, and network development progress may slow down. This may not be beneficial for a public-chain network that has not yet produced sufficient quality applications.

At the time when blockchain was just born, this technology was acclaimed for its low cost advantage. However, we have seen in the development of the industry that due to performance limitations, it is unable to quickly meet a large number of transaction demands, and the cost of transactions is continuously pushed up. Instead, the cost advantage of the blockchain is gradually disappeared, and the enthusiasm of application expansion is suppressed. For public chain and application developers, how to create a “blockchain network that is both popular (creating greater economic value) and smooth (avoiding excessive cost expansion)” is a major issue.

### 1.3.4 The Contradiction between Innovation and Order

As early as April 2017, The DAO became the largest crowd-funding project in global history with an ETH value of approximately $150 million. However, due to the vulnerabilities in the writing of smart contracts, the ETH stored in the contract was stolen by “hackers”, and the funds of a large number of investors were damaged. According to the official of The DAO project, The DAO should be a free token that is completely dominated by unforged, non-stopping, and non-tampered code. As a result, the DAO’s theft case has risen from technical issues to social discussions. Is it “legal” to seek private gains for vulnerabilities in irreversible blockchain smart contract codes? Is it reasonable? And, the Ethereum main network hard-forked the blockchain that once claimed to be irreversible, helping investors to find the stolen tokens, is it in line with the original logic of the blockchain? As a result, the controversy led to the fork of Ethereum, and it also made people aware of the incompatibility between the declaration of “code is law” and real world law and ethics.

Currently main countries already have article in law to provide reference for data nad virtual property protection[19]. However, the anonymity in the current mainstream public blockchain makes the asset identification become unsolvable, and the protection of rights is even more difficult to talk about. Therefore, how the new characteristics of the blockchain adapt to existing social rules and laws, or promote its progress, has become the cornerstone of the real success of the blockchain[20]. However, for blockchain data notary application in judicial system, question as how to prove the blockchain is online during data attestation process, and to prove that it is impossible to be polluted in the process of data transmission need to be answered. Therefore, it can also be seen that the gap between rapid development of technology and the lag of the judiciary are still the urgent issue.

# 2 SimpleChain：Simplified & Distributed Chain-Network

## 2.1 The Design of SimpleChain

SimpleChain is a framework for secure blockchain protocols, a platform that is easy to use, and a trusted network based on machine consensus. SimpleChain absorbs the advantages of the existing blockchain projects, solves the current defects and problems, develops innovative technical solutions, and aims to build the distributed chain-network with simplicity and usability, in order to form a prosperous application ecosystem.

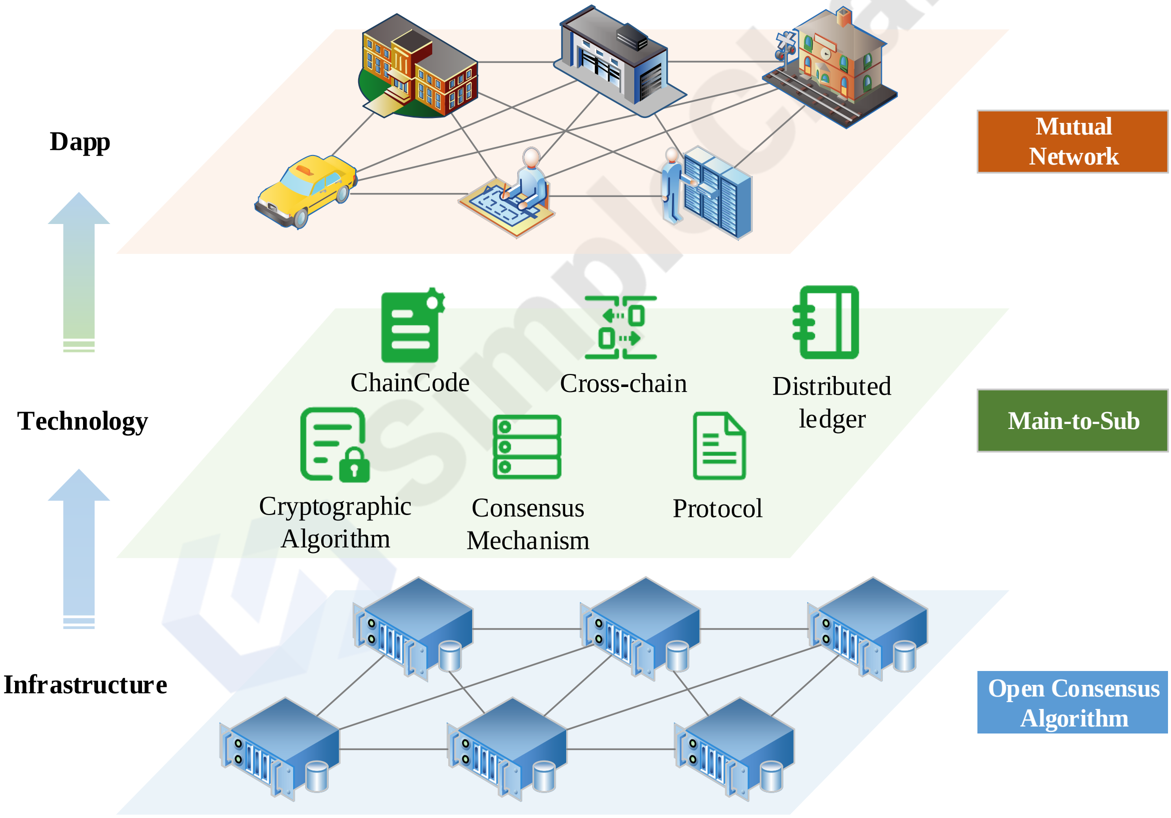

**Figure 5 Distributed chain-network of SimpleChain**

SimpleChain is the public blockchain that has the design concept of one main-chain with multiple sub-chain, applying PoW which is the only distributed consensus mechanism practiced through time and scale combining open consensus algorithm and publicly available consensus algorithm to guarantee the security of ledger as well as persistent excitation. By designing the multi-layer distributed value network, SimpleChain can support the deployment and extension of public blockchain in multiple business scenarios. Sub-chain can choose their own consensus algorithm which is suitable for their scenarios according to business requirement, and the two-way anchoring between the cross-chain node and the main chain further forms the cross-chain transactions with other sub-chain. It can satisfy the performance of thousands of TPS, and obtain the eventual consistency provided by the main chain at the same time.

## 2.2 Application Ecosystem of SimpleChain

One main-chain with multiple sub-chain is adopted in the design of SimpleChain structure, which can support for various business scenarios. For sub-chain project, it can choose their own consensus algorithm, and the two-way anchoring between the cross-chain node and the main chain further to form the cross-chain transactions with other sub-chain.

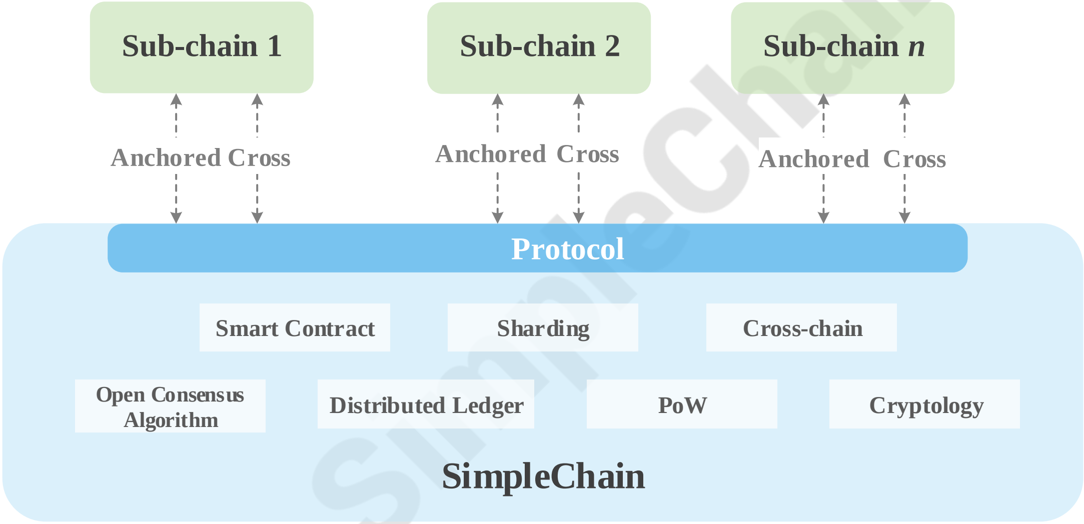

**Figure 6 Chain structure of main-to-sub**

### 2.2.1 Sub-chain Fields of Applications

SimpleChain has a single main-chain with multiple sub-chain network ecosystem that provides extension of high degrees of freedom for different application scenarios based on the final certainty. Supporting multiple applications also increases the integrity and diversity of SimpleChain ecosystem since the supported sub-chain projects involving the fields of digital entertainment, luxury goods, real estates, stable-coins, copyright protection and so on. Linking to the judicial consortium blockchain provides the legal effect for the whole network. SimpleChain forms a good and stable ecosystem through distributed data exchange in multiple industries and value exchange under compliance framework.

#### 2.2.1.1 Data Trading

In the past few years, the Internet industry, the financial industry, government agencies and so on have been in different degrees involved and implemented in big data related areas. But these big data enterprises are facing with a variety of problems, including data security risks, data silos, low data quality, inadequate circulation methods and other issues. Moreover, most of the government's big data is not well used hence not fully utilized.

Use blockchain that has distributed, transparent, traceable characteristics, can eliminate the concerns of data providers, while meeting the demand for compliance and legal data. The data owner’s privacy and legitimacy of data flow therefore could be protected. Combining blockchain and big data will complete efficient liquidation settlement and accounting of data asset, stimulate the enthusiasm of data trading, promote market prosperity, solve the data island problem, and truly establish a cross-broad connection.

#### 2.2.1.2 Digital Entertainment

Traditionally, the game will be released on the game store and in that mode, both game projects developers and players are both vulnerable groups. The game platform monopolize the market and determines what the game players can see and how many players the game can obtain in a centralized way, which makes the life-cycle of the game become shorter and shorter. The persistent problem that game and the players cannot be matched limits the healthy development of the current game industry.

Game World Chain, a peer-to-peer value network between game projects providers and game players, has therefore built a blockchain distributed game-release platform. The game projects developers can make a game crowd-funding based on GWC that the potential players will invest in specific game products and earn preferential rewards for in-game assets with GWC in advance. In-game assets are managed as on-line assets and can set a period of lock-up. When the locked up period ends, there is a period of hesitation. It is a period after the game is online when the player can exchange the in-game assets back to GWC in a certain percentage. Other game players can judge the popularity of game according to the volume of exchange between in-game assets and GWC, so that the game product provider can be ranked transparently. Driven by the digital value, a healthy distributed game industry ecology is formed.

### 2.2.1.3 Diamond

Unlike other commodities, it is difficult for diamonds to reach uniform price. Diamond industry is a monopoly market that price of diamonds is nontransparent. At the same time, the diamond market lacks liquidity and is often difficult to exchange them at their real market price because it is often stranded in a unilateral market. Although there are diamond exchanges, most of them are limited to B2B transactions, and buyers are hardly to distinguish their quality and authenticity of diamonds traded on the market because the flow of diamonds involves too many processes.

Digitizing warehouse receipt by combining diamonds with blockchain can create a convenient and efficient way to trade digital diamonds and link traditional diamond industry to the innovative financial markets. This innovative and secure way to trade diamonds will attract participants including traditional diamond trading chains, diamonds holders, investment traders who need to hedge their position and so on, thereby bringing together more diamond traders to make the diamond exchange and investment in a safe, stable and transparent manner. The use of digital warehouse receipt trading also reduces the cost of diamond circulation and the possibility of fraud, allowing digital diamond holders to get back diamonds at any time.

### 2.2.1.4 Real Estate

Real estate refer to property that cannot be moved according to natural property or by law, such as land, houses and other land fixed objects. At present, a large number of people are investing in real estate, and some want to invest in oversea real estate, However, the vouge and complicated polices for the investment process is the hurdle of that. As in the process of finding a third party, there are cases where the fee is too high and the information is unclear.

Lunabay is a retirement community maintained by the whole members of all ages with transparent, dynamic and precise management of community members' personal real estate and community supporting services (products). The community will enhance the quality of life of community members at all ages and further form the world's most professional aged care community. Given that real estate remains the most important fixed asset for most individuals throughout their lifecycle worldwide, Lunabay is able to determine, authenticate and allocate the ownership and access to the real estate based on blockchain technology and maximize the balance of combined needs the members have for consumption, investment and pension at different ages of its communities.

### 2.2.1.5 Backed Token

A convenient, secure and reliable trading method has not been found since the birth of the digital asset trading market. On the one hand, most cryptocurrencies price are too volatile to use them for payment or settlement. Therefore, participants have constructed a “Backed Token” that anchors the fiat currency for valuation and payment. However, there are still some problems in the stable tokens market. For example, the mortgaged US dollar assets are issued with a stable token but there is no assets hosting and auditing leading to risks such as credit over-issuing, misappropriation of funds, and black-box operation. On the other hand, the centralized exchanges are suspicious of security, and theft of assets and malicious outbursts have caused investors to lose confidence.

Based on the experience of foreign exchange investment services, MintEx closely combines foreign exchange transactions with digital asset transactions to create a secure and credible digital asset trading platform. MintEx introduces the backed token Mint to anchor foreign exchange assets with the corresponding assets deposited in the bank. The number of Mint in circulation increases or decreases according to the total amount of assets, thus forming a connector for foreign exchange assets and digital asset transactions.

### 2.2.1.6 Distributed Computing Power

With the development of technology, computers are everywhere, offering great convenience to people. However, in practice, the user needs to purchase servers or storage space in order to compute or store a large amount of data, which can be complicated and trivial.

In the distributed computing power sub-chain projects, users can obtain corresponding distributed computing power according to their own rights. For the distributed computing power acquired by users, it can be operated according to its own needs, such as data training in artificial intelligence. Through the tokenization of distributed computing power, the distribution of computing power can be more reasonable and transparent, thereby meeting the needs of users.

### 2.2.1.7 Copyright Protection

Though people's awareness of copyright protection has increased, the development of

Internet technology makes it easier to copy and spread works. Digital piracy is rampant and many works are spread without authorization. At the same time, digital copyright trade has become more frequent, and the demand for copyright authorization has soared. However, the traditional copyright transaction method is complicated in processes, high in transaction cost, and low in transaction efficiency, which cannot meet the needs of the digital copyright trade in the Internet era.

The blockchain copyright protection platform provides an effective way for online copyright protection and transact the ownership online. The platform records all the actions of users purchasing, citing, and spreading the works on the blockchain, effectively protecting the copyright for original author to obtain legal rights. In addition to the copyright of works, the personal branding can be digitalized as well, and the benefits of the personal branding can be automatically allocated according to the settings, thus protect the copyright of works, portraits, etc. related to the brand. The blockchain digitalization could increase the value of online personal branding and promote the circulation of the copyright trading market.

### 2.2.1.8 Digital Forensic & Validation

The facts of the case must be based on evidence, and only by obtaining true and sufficient evidence the accurate identification of the case can be revealed. In the traditional process of evidence collection, there are problems in evidence acquiring and also time consuming. At the same time, many evidences in digital form is easy copying, delete, and modify leading to more difficulties on collecting evidence. That is one of the reasons which made the judicial work process slow and inefficient.

Through the effective combination of blockchain and big data, it provides stable support and implementation assistance for the improvement of the existing judicial system. The use of blockchain, which is distributed and transparent, can acquire and verify evidences rapidly synchronize the judicial information, improve efficiency of case handling, avoid data silos, reduce constraints on time and space, adapt to changes in the Internet era, and promote judicial innovation.

As the innovative combination of peer to peer network, decentralized storage, cryptographic algorithm, and consensus mechanism the fundamental characteristic of blockchain is the integration of currency, bill, receipt and accounting. Different application scenarios have different requirements for the verification and confirmation frequency of chain transactions, data format and capacity, performance and openness of the chain. In order to ensure the maximum compatibility of the public chain platform and the effective isolation among transactions of different chains that applications on, SimpleChain, a single-chain with multiple sub-chains, will become an easy-to-use, secure development platform for distributed application developers.

## 2.2.2 SimpleChain Access

### 2.2.2.1 SimpleChain Explorer

SimpleChain provides users with the blockchain viewer and the network dashboard.

The blockchain viewer is the main window for browsing the information on the SimpleChain. The content recorded in each block can be viewed from blockchain viewer, including the ledger data of both the original digital asset SIPC and various on chain tokens. Digital asset user of SimpleChain could use the blockchain viewer to query the transaction information recorded within the block. The blockchain viewer also allows user to search the contents of both the main chain and each sub-chain network. The information includes block height, block hash, mining difficulty, received time, transaction price, transaction address etc.

The network dashboard is a visual administration panel developed for the users and operator of the SimpleChain node. It provides information such as the number of active nodes, block time, gas price, mining difficulty, last blocks miners. It helps node user to understand the network status of its own nodes and other nodes across the network. The delay and connection information shown on the SimpleChain network dashboard is useful for node operator to optimize the net connection. For miner nodes it is also key for them to supervise the timing of transaction validation.

Blockchain Explorer is the most direct entrance for developer and user to understand the SimpleChain through a visualized way. The open source explorer are open to accept any community developer to further enhance the function and accessibility of the blockchain.

### 2.2.2.2 Node Client

SimpleChain provides users with easy-to-use client software. Users can create and manage accounts, synchronize account books and query related information through the client to open the blockchain tour. Once becomes a node, the user can send and verify transactions. Users can also visually deploy smart contracts through the client to easily create their own blockchain applications. Miners can participate in mining and management mining activities through the client.

### 2.2.2.3 Mobile Wallet

Blockchain wallets are tools for users to manage their digital assets. In order to facilitate users to manage all kinds of SimpleChain certificates, we have developed a multi-currency mobile wallet “ChainBox”, which has the functions of query, storage, transfer, transaction, etc., and is suitable for iOS phones and Android phones. In the future, it will continue to optimize and upgrade ChainBox to support more functions and more kinds of devices

### 2.2.2.4 Blockchain Attestation Platform

BAOQUAN.COM, a sub-chain of SimpleChain, has developed a blockchain-based data service platform to provide users with data stored service, online forensics services and copyright protection platform.

The advantage of this application is that user data is permanently stored on the blockchain. No reliance of the company operator that provides the service, which might went off. Moreover, the Chinese judicial system has recognized the legitimacy of data stored and transacted on blockchain, which makes this product effectively reduces the legal cost and saves users time.

By providing a simple RESTful API to read, write, and search BAOQUAN blockchain entries, you are able to have everything you need to get started. BAOQUAN.COM includes APIs, SDKs, documentation, and a blockchain explorer to verify and debug entries.

The BAOQUAN.COM is a sub-chain service open to any other sub-chain application on the SimpleChain network, therefore, the transaction on the SimpleChain could not only get public verification from the on chain nodes but also get validation from judicial institutions with law enforcement. The BAOQUAN.COM as the genesis sub-chain application would be the easy access for conventional centralized data to be blockhained.

# 3 Economic Model & Token Mechanism

This part first introduces the design principle of economic model of SimpleChain, and analyzes the relationship between token of main chain and sub-chain. Finally, the economic model and token mechanism of SimpleChain will be introduced in detail.

## 3.1 Token Issuance & Circulation

### 3.1.1 Economic Model Design

#### 3.1.1.1 Token Interpretation

**1、Token Attributes**

Currency is defined as a medium consensus that improves the efficiency of transactions [21]. It has four functions: the medium of transaction, the unit of account, the value of storage and the standard of deferred payment [22].Moreover, the property of currency evolves with the rise and fall of economic system: the rise of commodity economy gives rise to metallic currency; the rise of plutocracy economy [23] gives rise to representative currency [24]and credit currency; the sharing economy gives rise to super-sovereign reserve currency [25]So far, the world is still in the market system of plutocracy economy-based, and credit currency achieves the maximum of efficiency [19].

Based on the market system of plutocracy economy, token should be regarded as a digital commodity or security that has the right to use, but it is not money. As is known to all, token generated by SimpleChain originates from mining, and comes from the algorithm. For those token that generated by algorithm, their circulation process is shown in the following figure.

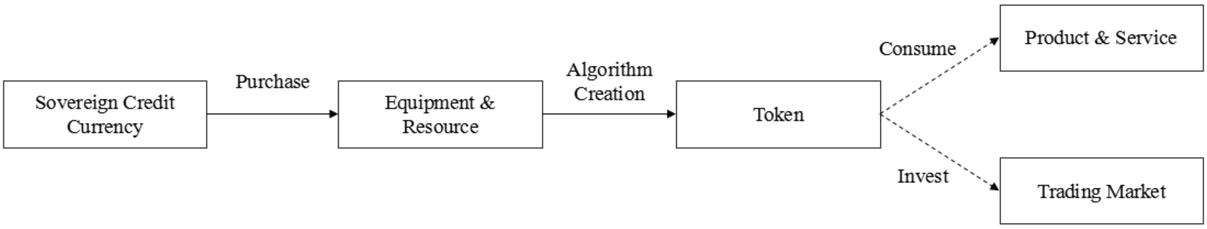

**Figure 7 Process of token-algorithm**

From the perspective of digital economy, sovereign credit currency has become an external input source of the lately-appeared token. Token issue channel of smart contract which is the same as certificate issuance by central bank, and token can be used for consumption and investment. And there are three main states of token: 1) held in digital form; 2) destroyed by consumption; 3) destroyed in currency exchange.

### 2、Token Interpretation for Main-chain & Sub-chain

#### （1）SIPC token of main-chain

As a medium of the entire ecosystem, SIPC can be obtained by mining, used in chain-transaction or contract calls, and burned during computing process. The performance of SIPC is well correlated with backed-token and common-token, in other words, the value of SIPC is determined by these two kinds of token.

#### （2）Backed-token of sub-chain

Backed-token, which has the stable value in a certain period. In the whole ecosystem of the main-chain, we can pay the required charging by converting backed-token into SIPC as well as invest by exchanging common-token. Backed-token is issued by their own group, and fully backed by fixed value for flat currency, mainly for payment. The issuer should have an equal amount of flat currency (i.e. a one-to-one ratio reserves in commercial bank) or other assets (i.e. diamond, gold) held in reserve. The backed-asset held in our reserves which means the system is fully reserved when the sum of all tokens in existence is exactly equal to the balance of asset held in our reserve. According to the ecosystem, the digital assets on the main-chain or sub-chain can be reserved by smart contract, others (i.e. BTC, ETC) can be hosted on the third-party platform. With the high stability of backed-token, it plays an important role in main-chain’s verification, which also has a higher value-to-weight ratio to the main-chain.

#### （3）Common-token of sub-chain

The price of common-token fluctuates freely, and it has various types, including function token, commodity token, security token and so on. Common-token is issued by their own group, giving full support to our ecosystem, which has both circulation attributes and storage functions. With continuous project access, more and more application scenarios are open to users, which not only increase the number of users, but also attracts the computing power of main-chain transfer to the application of sub-chain. For those projects, they also connect with the commodity market in the real world, and the virtualized commodity will enter into the ecosystem in a digital way, thus breaks through the circulation barrier between the industries to perfect the main ecosystem.

#### （4）Circulation relationship of tokens

Under the system of SimpleChain, there are three main tokens: SIPC token of main-chain, backed-token of sub-chain and common-token of sub-chain. For those token that associated with asset-backed (such as credit currency, physical assets and digital assets), we called them backed-token. Thus, there exists the convertible and negotiable relationship between currency, backed-token and common-token, circular economy of tokens is shown in the following figure.

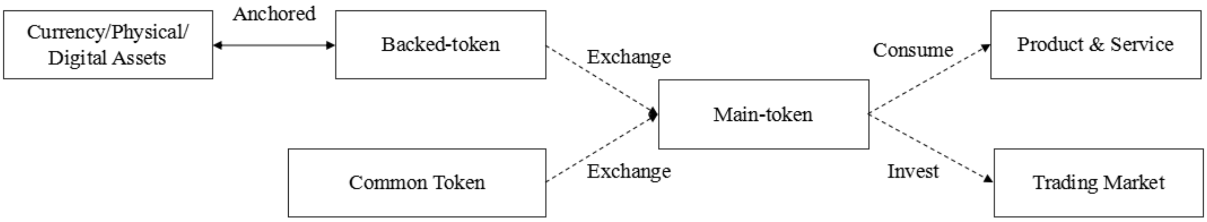

**Figure** 8 **Circular economy of tokens**

We can find that backed-token conforms to the definition and function of fiat currency, and common-token comes from the trust-creation of blockchain projects. Under the circulation system of P2P, loan relations and credit support become clearer without the intermediary (i.e. Bank). Monetary theory is still worthy of our token issuance for reference.

## 3.1.1.2 Token Model

### 1、Quantity Theory of Token

In general, the liquidity characteristics of tokens is similar to currency in the blockchain economic system, so we can choose “Monetary Model”. From the transaction scale and velocity of circulation, Fisher Equation [26] can be obtained as follows.

$$MV_t = P_tT$$

Where $M$ represents the quantity of currency, $V_t$ represents the velocity of circulation, $P_t$ represents price, $T$ represents the scale of transaction, and $P_tT$ represents the value of transaction. Furthermore, assume that the scale of transaction $T$ is equal to the total output (SIPC output of main-chain, which is determined by backed-token and common-token), which is represented as $Y$. We also assume that the velocity of circulation $V_t$ is stable (users have formed a certain trading habit), so $V_t$ can be regarded as a constant $\bar{V}$. From the view of assets, we can get quantity theory of Cambridge school as follows:

$$M_d = kP_tY\ （k = \frac{1}{\bar{V}}）$$

Hence, mapping to the blockchain, the demand of tokens $M_d$ is proportional to the actual transaction volume $Y$ and price $P_t$ (i.e. the price of sub-chain that SIPC-marked or other digital assets on chain). If the variables are further refined, we can get the quantity model of tokens [27] as follows:

$$\frac{M_d}{P_t} = f\left\{Y_p, e_t, t_c, s, v_t, \frac{1}{P}\times\frac{dP}{dt}, i_t, u\right\}$$

Where $M_d$ represents the demand of tokens, $P_t$ represents the price which has positive correlation with $M_d$; $Y_p$ represents the user's income level (including all the assets that can be invest in token), which has positive correlation with $M_d$ . $e_t$ represents the expected nominal yield of backed-token or pledged financial asset (the return of assets in finance system), which has positive correlation with $M_d$; $t_c$ represents the cost of transaction (including transaction commission and exchange fee); $s$ represents average turnover rate of tokens; $v_t$ represents velocity of token circulation; $(1/P)\cdot dP/dt$ represents expected rate of price volatility (the expected rate of inflation, including the growth rate of main-chain according to the growing demand of sub-chain ), which has negative correlation with $M_d$; $i_t$ represents the function of pledge rate (hereinafter referred to as ratio, higher ratio means the higher issue cost), which has negative correlation with $M_d$; $u$ represents some other variables (i.e. investment preference of users), which has uncertain correlation.

Furthermore, extract the key variables: income, cost of transaction and ratio, according to Baumol-Tobin Model, minimize the cost of held tokens, we can get the square root function [28] as follows:

$$M^* = \sqrt{\frac{Y_p}{2}\cdot\frac{t_c}{i}}$$

Where $M^*$ represents optimal token holdings; $Y_p$ represents income level of token holders, which has positive correlation with $M^*$; $i$ represents ratio, which has negative correlation with $M^*$; $t_c$ represents the cost of transaction (the consumption of SIPC); Assume the average monthly holdings of tokens is equal to half of monthly income $Y_p/2$. Therefore, the transaction demand of tokens changes with the income level in codirectional way, and with the ratio in negative direction.

**2、Short-term Ratio Model**

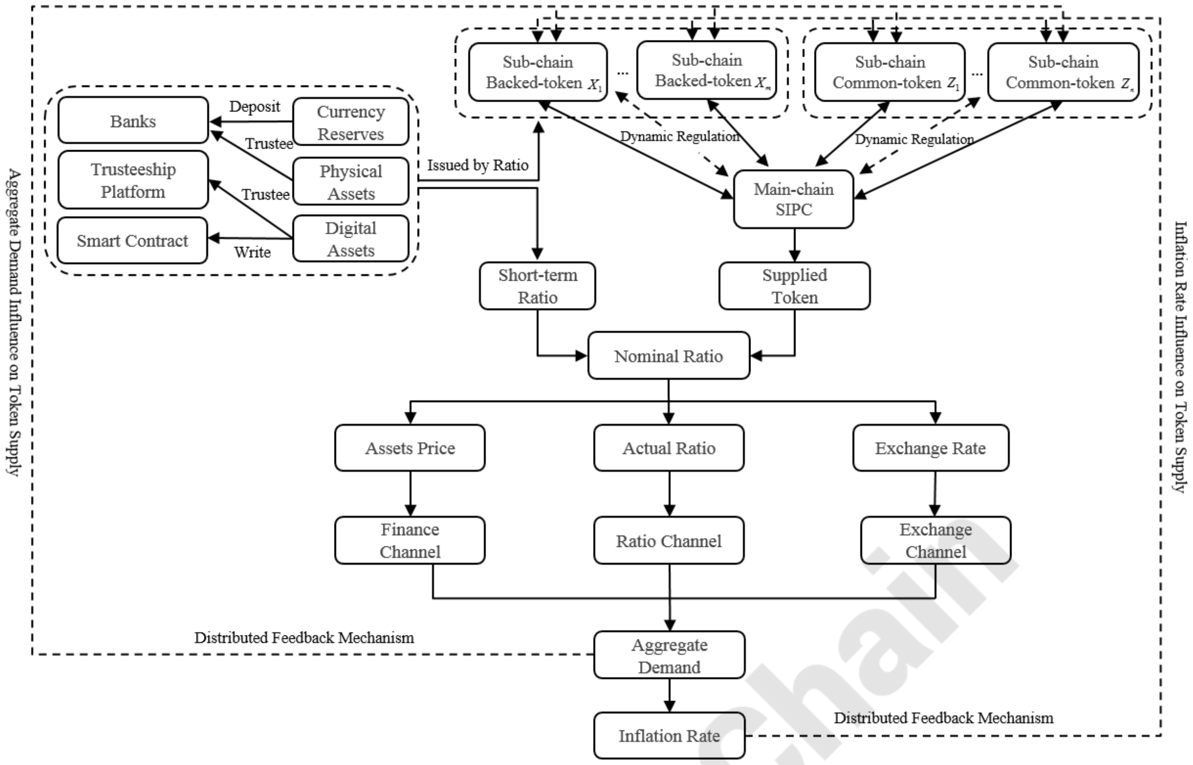

**Figure 9 Dynamic regulation of token supply**

The demand and value of SIPC is determined by backed-token and common-token, in other words, the dynamic regulation of SIPC supply is according to the demand of sub-chain. As shown in the above chart, for the issue of backed-token, ratio plays an important role in the supply regulation of SIPC. There are three main channels influence the aggregate demand: finance, ratio and exchange rate. And then the exuberance of aggregate demand forms the pressure of inflation. However, based on the distributed feedback mechanism of main-ecosystem, the aggregate demand and inflation pressure would be transmitted to those sub-chain synchronously, and then the supply of SIPC will be adjusted by the dynamic communication. So the inflation to some extent acts on the fluctuation of the ratio. Thus the supply regulation formula for ratio-based can be written as follows:

$$i_t = f\left(i_{t-1}, R, \pi_t^*, X_t^*, Z_t^*\right)$$

Where $f(\cdot)$ represents supply regulation function of SIPC, $R$ represents average short-term ratio, including the return of asset-pledge, $\pi_t^*$ represents the difference of inflation rate between the real and the target, $X_t^*$ represents the output gap of backed-token (the difference between actual output and potential demand), $Z_t^*$ represents the output gap of common-token (the difference between actual output and potential demand), $i_{t-1}$ represents the smoothing characteristic of dynamic regulation for SIPC supply.

According to Taylor’s Rule, short-term ratio model can be written as:

$$n_t - \pi_t = R + \alpha(\pi_t - \pi^*) + \beta(\frac{X_t - X^*}{X^*}) + \gamma(\frac{Z_t - Z^*}{Z^*})$$

Where $n_t$ represents nominal ratio, $\pi_t$ represents inflation rate, $n_t - \pi_t$ represents actual short-term ratio, $\pi^*$ represents the target of inflation rate, $\pi_t - \pi^*$ represents the shift-value of inflation target, $R$ represents average short-term ratio, $X_t$ represents the actual output of backed-token, $X^*$ represents the potential demand of backed-token, （$X_t$ - $X^*)/X^*$ represents the output gap rate of backed-token (ratio between the actual output and potential output), $Z_t$ represents the actual output of backed-token, $Z^*$ represents the potential demand of common-token, $(Z_t$ - $Z^*)/Z^*$ represents the output gap rate of common-token (ratio between the actual output and potential output), $\alpha$、$\beta$、$\gamma$ respectively represents the weight for the shift-value of inflation target and the output gap of backed-token and common-token. Therefore, when the output gap rate and the shift-value of inflation are both positive (the inflation rate exceeds the target), the short-term ratio should be at a premium, and vice versa.

### 3、Supply Model of Main-token

Quantity supplied of SIPC generally fluctuates in different periods according to the circulation situation of the sub-chain (backed-token and common-token). In addition, together with the short-term ratio model, we can obtain the supply model of main-chain as follows:

$$M_s(t) = f\{ \ (X(t), Z(t), i(t) \ \}$$

Where $M(t)$ represents the supply function of main-chain (quantity supplied in $t$ period), $X(t)$ represents the output function of backed-token, $Z(t)$ represents the output function of common-token, $i(t)$ represents the supply regulation function for ratio-based （the response function of main-chain according to inflation rate）.

Furthermore, supply function[29] can be written as:

$$M_s(t) = X(t)Z(t)(P_{t-1}PP_{t-2})^{-q}$$

Where $M_s(t)$ represents the quantity supplied of main-chain in $t$ period, $X(t)$ represents the output function of backed-token, $Z(t)$ represents the output function of common-token, $P_{t-1}$，$P_{t-2}$ respectively represents the price of $t$-1 and $t$-2 period, represents the response ratio of inflation. And then take the logarithm on both sides of the above function, we can get the following formula:

$$m_{s_t} = x_t + z_t - q(p_{t-1} - p_{t-2})$$

Where $m_{s_t}$ represents the growth rate for main-token in $t$ period, $x_t$ represents the growth rate for backed-token in $t$ period, $z_t$ represents the growth rate for common-token in $t$ period, $p_{t-1}$, $p_{t-2}$ represents the inflation rate of $t$-1 and $t$-2 period. With the high weight of backed-token, we can find that $x_t - q(p_{t-1} - p_{t-2}) > z_t$, which means the growth rate of main-chain ($m_{s_t}$) is mainly affected by backed-token. For the backed-token, it has the stable value with currency-backed. For the consumption demand of SIPC, it can meet with the stable development of ecosystem in long-term by adding more backed-token projects.

### 3.1.1.3 Node Balance Theory

So far (until September 3, 2018), Bitcoin network hashrate reaches to 52.29 EH/s, that is, if each equipment of hashrate achieved 13.5T, the probability of block generation is extremely low, which means it only has one in a million chance of being bookkeeper. Therefore, with the exponential growth of network hashrate, the block generation probability of solo mining is becoming lower and lower, and users are gradually moving to the mining pool. As Satoshi Nakamoto argues, when the network grows to a large scale, each node will be a large cluster of servers [30]. So the transformation from solo mining to pool mining is the result of natural development.

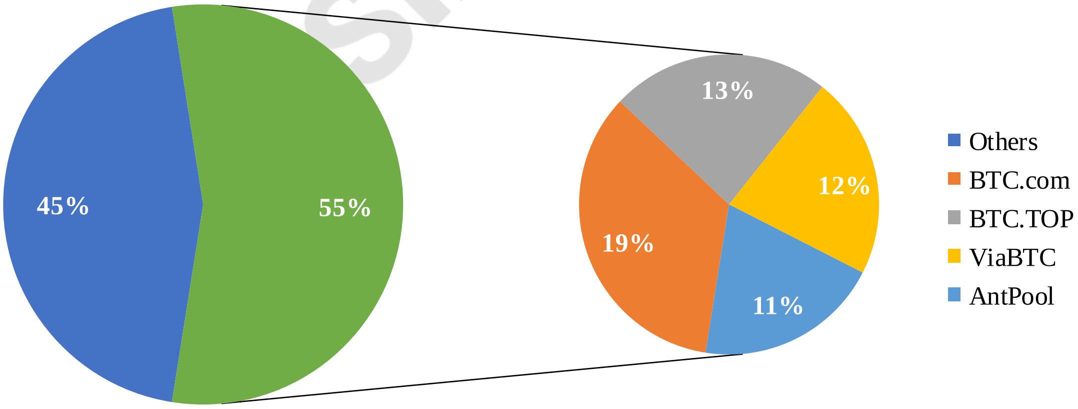

**Figure 10 Pool distribution of BTC**

The present stage, as shown above (Pool Distribution of BTC), more than half of network hashrate is being concentrated in the top four pools. Although the hashrate tends to be centralized, it is still scattered among the nodes, and there has no one exceeded 25%. In other words, BTC has formed a considerable number of efficient nodes against another, and these specialized server farms keep running full network nodes which processing blocks [31].

There is no denying that the result of hashrate concentration can be predicted, and the efficient nodes will be form a relationship of node balance to promote the healthy development of ecosystem.

Taking Bitcoin pool as an example, node balance theory makes evidence in the trend of hashrate concentration. According to the analysis of the scattered graph in the following figure, in the past year, the fluctuation value of hashrate in the top four mining pools (compared with the previous month) basically remained under 2%, and the highest value also did not exceed 6%. That is to say, the hashrate of these efficient pool nodes has formed a certain scale, and they can maintain their holding share to achieve the effect of node balance.

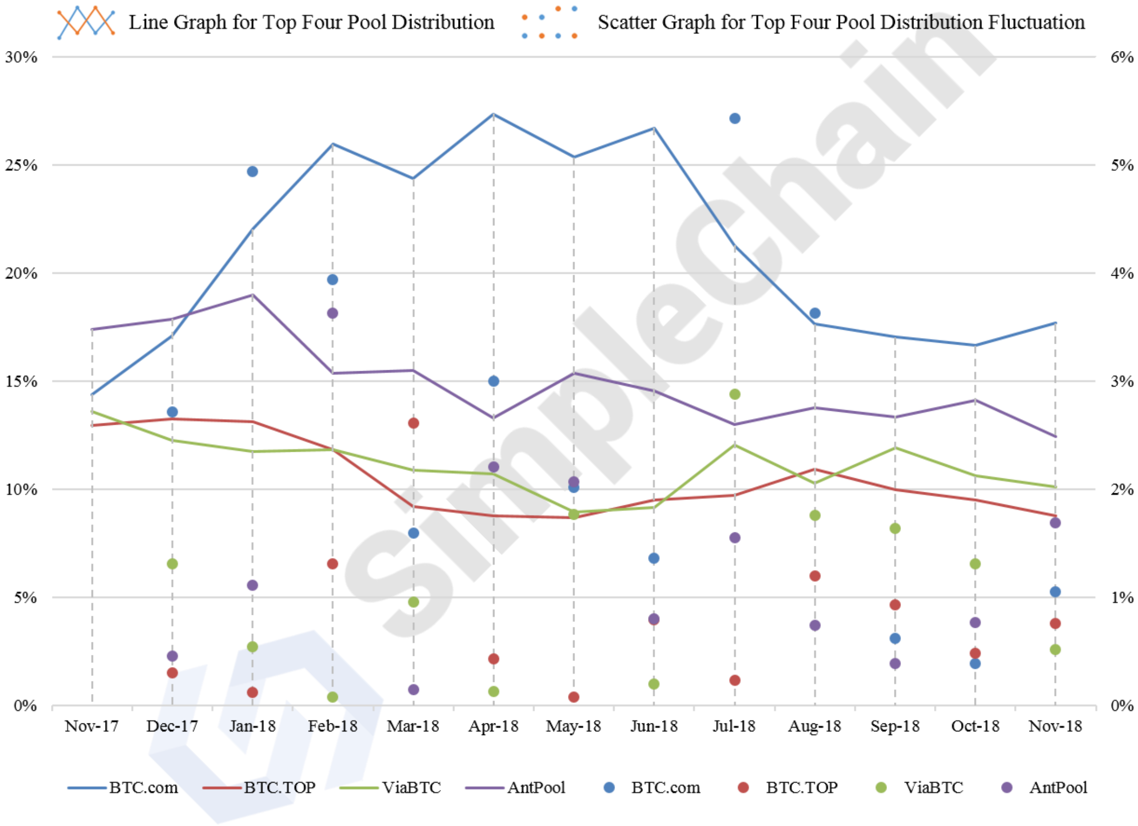

**Figure 11 Top four pool distribution/fluctuation（monthly）graph**

Assuming that the full hashrate has formed a specific market scale, during the stable stage of development, we can ignore its small volatility, then the hashrate proportion of pool/solo mining can be regarded as fixed value in a short period of time. That is, the probability of generating block remains unchanged. For the statistical point of view, assuming that the probability of success ( $X=1$) is $p\,(0\le p\le 1)$, and failure ( $X=0$ ) is $1-p$, then the random variable is obtained from Bernoulli distribution, its variance can be written as $p(1-p)$. According to the default time of block generation of SimpleChain (12s), we can learn that there are 5 blocks to be generated per minute on average. In addition, for statistical analysis of hourly mining, we can obtain the variance of mining return is $60\times5\times p(1-p)$, the expected return is $60\times5\times p$, and the relative standard deviation is shown as follows:

$$s=\frac{\sqrt{60\times5\times p(1-p)}}{60\times5\times p}\quad \text{(Simplified as } \frac{1}{\sqrt{60\times5}}\times\sqrt{\frac{1}{p}-1}\text{)}$$

As we know from the above, the higher proportion of network hashrate that user owns, the smaller relative standard deviation as well as the risk. For the investment psychology, compared with solo mining, users only need to run lightweight SPV nodes when they join the mining pool, on the one hand, they avoid the trouble of running the full network nodes, and on the other hand, they can reduce the variance of mining return further reducing risk [32]. When considering risk, the return rate of mining pools also should be considered by users. According to the analysis of the top four pool distribution curve in the above figure, the hashrate proportion of BTC.com in each period is superior to the other three mining pool, but it also has the maximal variation and its advantage is no longer obvious in the later stage. The fundamental cause of the intensity fluctuation lies on its trust level. When the mining pool node owns a large proportion of hashrate, its centralization degree will be higher, and the mining return will be more uncontrollable, then the mining pool may loss its credibility that users starting to leave. So it will cause the hashrate proportion to obvious fluctuations as well as the uncertain return. However, it also can keep the balance between the mining pool nodes and solve the problem of over-concentration of hashrate. Furthermore, after entering the cooperative period of mining pools, node balance needs to be maintained by a large number of users. Then, users can choose the optimal mining node according to the ratio of return to risk, that is, the ratio of mining return to the relative standard deviation, it can be written as:

$$\frac{F(h)}{S(p)}=f(p,h,w)$$

Where $p$ represents hashrate proportion, $h$ represents trust degree of mining pool, $w$ represents some other variables that influence on the ratio of return to risk. $F(h)$ represents return function with the main variable $h$, that is, the mining return depends largely on the trust degree of pool nodes, and when the hashrate proportion reaches to a certain level, the trust degree will decrease. $S(p)$ represents relative standard deviation function with the main variable $p$, that is, the mining risk depends largely on hashrate proportion, which has negative correlation with $p$. Therefore, for the selection of mining pool nodes, users can choose the optimal mining node based on the ratio of return to risk, the higher ratio means the better investment. Of course, users also can adjust the investment proportion of hashrate corresponding to the investment portfolio, that is, choosing the different node to maximize the profit. In this way, users can spread the risk to increase revenues. For the mining nodes, the diversity of users' selection also stabilizes their competitiveness, finally to maintain the balance between nodes.

Similarly, for SimpleChain, all issued SIPC are generated by mining, and all mining nodes are running based on the original algorithm, then using the uniformity of the whole network to ensure fair competition among nodes, further helping nodes in the balance of mining. Initially, SimpleChain sets the original algorithms include block generation awards of SIPC, difficulty adjustment, etc. As SIPC is gradually worked out, its output function $f_1(x)$ is shown in the following figure. For the joined sub-chain, the block awards function $f_3(x)$ will be compared with the reference function of block awards $f_4(x)$, and then to activate the block awards to meet the needs of sub-chain by dynamic regulation. At the same time, in order to prevent the sudden increase of users and the exponential growth of network hashrate, we will raise the degree of difficulty according to the difficulty adjustment function $f_2(x)$, then the network will enter into the difficulty raising period to ensure the stable growth of SIPC. In general, using the unified algorithm and dynamic regulation to guarantee the fair competition between nodes, and introducing the healthy competition mining method to ensure the dynamic equilibrium of the whole network, finally promoting to form a healthy ecosystem based on these efficient nodes.

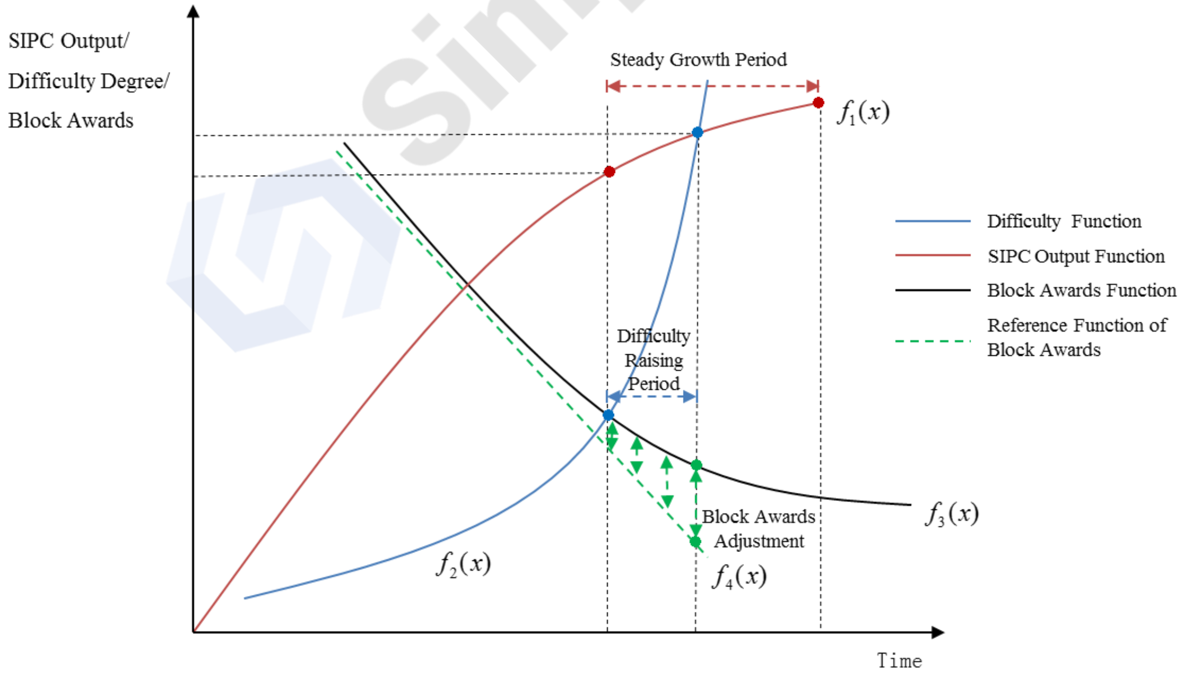

**Figure 12 SIPC functions**

## 3.1.2 Analysis of Multiple Sub-chain Token Mechanism

### 3.1.2.1 SIPC: SimpleChain Token

SIPC is SimpleChain (main-chain) token which will be consumed in the formation, development, positive cycle of sub-chains ecological community.

### 3.1.2.2 SIPC Total Supply Dynamic Adjustment

Total value of SIPC is equals to the sum of all sub-chains value.

Set the total value of SIPC as $W$，Assume that there are $n$ sub-chains $A_1, A_2, \cdots, A_n$ join main-chain, and the weight of each sub-chain contributes to main-chain is $C_1, C_2, \cdots, C_n$. Thus the SIPC total value $W$ is calculated as follows,

$$W_{SIPC} = \sum_{i=1}^{n} W_{A_i} * C_i$$

Where $W_{A_i}$ represents the value of main-chain $A_i$, $W_{A_i} > 0, i = 1, 2, \cdots, n$, $C_i > 0, i = 1, 2, \cdots, n$.

SIPC total supply dynamic inflation is designed for two purposes.

Firstly, SIPC total supply is adjusted to the growing number of sub-chains. When new projects join SimpleChain network, the demand for SIPC will increase, as well as the SIPC total value. The SIPC supply needs to be dynamically adjusted to meet transactions needs.

The SimpleChain dynamic system mechanism is similar to the equation of exchange

$$MV = PY$$

Where $P$ represents price level, $Y$ represents real GDP, $M$ represents money supply, $V$ represents velocity of money. In the SimpleChain dynamic system, where $Y$ represents the total volume of data that needs to be confirmed, $P$ represents the SIPC consumption per unit volume of data that needs to be confirmed (transaction fee), $M$ represents SIPC total supply, $V$ represents velocity of SIPC.

When there are $n$ sub-chains join SimpleChain network, the total volume of data that needs to be confirmed is $Y_n$ with price $P_n$ per unit of data volume while $V_n$ represents the velocity of SIPC. When there are $n+1$ sub-chains join SimpleChain network, the total volume of data that needs to be confirmed is $Y_{n+1}$ with price $P_{n+1}$ per unit of data volume while $V_{n+1}$ represents the velocity of SIPC. The total value of main-chain will rise when new sub-chains add to it, as well as the total volume of data that needs to be confirmed. So the corollary of this is:

1. The total volume of data that needs to be confirmed will go up, which means $Y_{n+1} > Y_n$.

2. While we can rewrite the equation of exchange $MV = PY$ as：

$$M = \frac{PY}{V}$$

3. Try to ensure that the transaction fee $P$ and velocity of SIPC will not fluctuate too much, then $P_{n+1} \approx P_n$ and $V_{n+1} \approx V_n$. Under the condition $Y_{n+1} > Y_n$, it can be concluded that $M_{n+1} > M_n$.

As above, it can be seen that the actual token demand will increase, so SIPC needs a little inflation.

Secondly, from the perspective of SIPC holders, they prefer to purchase the products and services on sub-chains since there is only a little inflation of SIPC, thus stimulate the development of the sub-chain and make the sub-chain develop healthily.

### 3.1.2.3 SIPC Consumption Mechanism

SIPC Price is decided by the capacity per transaction（kb/tx）that needs to be confirmed by main-chain. SIPC Price is then ordered and confirmed by miners on main-chain, and its order is decided by two factors.

The first factor is the capacity of each transaction.

It is clear that the larger the capacity of transactions need to be confirmed, the more the computing resources have to be consumed. Thus the price need to be paid will increase as well, since it is the product of abstract, undifferentiated computing power. It can be written in the formula:

$$y_1 = kx$$

Where $y_1$ represents the price of transaction capacity, $k$ represents constant, $x$ represents the capacity of transactions that need to be confirmed.

The second factor is the actual time consumption that a miner complete a transaction.

For the same type of transactions, the more time the current transaction consumes, the higher the price of the next transaction needs to be adjusted. Miners on main-chain made choices freely which results the changing transaction price. Say one transaction is not grouped into a package for a long time, it indicates that there is a deviation between the transaction fee it consumes and the estimated transaction fee, thus miners are unwillingly to accept this transaction. At this time, increasing the transaction price can stimulate miners to accept the transaction. Vice versa, when one transaction is grouped into a package and confirmed instantly, it means that the transaction price is higher than market price. Actual consumed computing power is lower than the current transaction price, so miners can get high profit. Market price can be calculated from the following formula:

$$y_{n+1} = y_n * \frac{t}{t_e}$$

Where $y_{n+1}$ represents the expected price set by the market next time, $y_n$ represents the current price, $t$ represents the actual trading time, $t_e$ represents constant.

In summary, transaction price is in direct proportion both to $y_1$ (the price of transaction capacity) and $t$ (time consumption for the last transaction), while transaction price and $t_e$ (expected trading time) are inversely proportion.

Transactions are sorted according to the bidding order, ensuring top-ranked bidders who have urgent command can be prioritized while users who are less urgent get a favorable transaction price.

The initial transaction price is decided by the transaction capacity price, and the following price of transactions (from 2 to $n$) can be calculated from the formula. In conjunction with the bidding mechanism, these three elements decide the pricing and ordering of transaction verification.

### 3.1.2.4 Backed-token Mechanism

Miners on main-chain will prioritize the transactions from sub-chain with backed-token, ensuring SIPC converted to backed-token of sub-chain first.

There will be a great number of sub-chains to join SimpleChain after the ecosystem is built. A stable SIPC, as the main-chain token, is needed to support and benefit a healthy ecosystem.

Some sub-chains are stable but others are not due to their natural property, thus they can be divided into two categories, the sub-chain with backed-token and the sub-chain with common-token.

Both the value of main-chain and sub-chains should be recalculated. Assume that category A is the sub-chain with backed-token and there are $m$ of them, $A_1, A_2, \cdots A_m$ and the weight of each sub-chain contributes to main-chain is $C_{A_1}, C_{A_2}, \cdots, C_{A_m}$. Assume B is the sub-chain with common-token and there are $n$ of them, $B_1, B_2, \cdots B_n$, and the weight of each sub-chain contributes to main-chain is $C_{B_1}, C_{B_2}, \cdots C_{B_n}$.

Then

$$W_{SIPC} = \sum_{i=1}^{m} W_{A_i} * C_{A_i} + \sum_{j=1}^{n} W_{B_j} * C_{B_j}$$

Giving priority to the sub-chain with backed-token, the SIPC price will be positive related to the backed-token price, and the trend of SIPC price is consistent with the trend of the backed-token price. The backed-token of sub-chain comes with stable attributes, such as diamond-backed-token, gold-backed-token and petro-backed-token. Therefore, SIPC price will keep stable by preferentially confirming the transactions from sub-chain with backed-token.

The specific implementation is as follows:

Three parameters count in forming the transaction confirmation price.

$i$ is the price parameter depending on the capacity of transaction.

$j$ is the parameter of price order set by SIPC platform for backed-token and common-token.

$k$ is the parameter of additional price that users are willing to pay for additional capacity of transactions per kb.

Set the capacity of one transaction that need to confirm is $x$, then the ordered transaction price is

$$y_M = x * i * j * (1+k)$$

and the profit of miners on main-chain is calculated as follow

$$y_N = x * i * (1+k)$$

For example, say transaction A of the backed-token and transaction B of the common token both need to be confirmed by SimpleChain.

Capacity of transaction A is $x_1$=5 kb and capacity of transaction B is $x_2$=5 kb.

Assume $i$=10, set the price order of transaction A and B is $j_1$=1.2 and $j_2$=1.1 separately. Users for transaction A pay extra $k_1$=10%, and users for transaction B pay extra $k_2$=10% as well.

Then the ordered transaction price $y_{M_1}$ for transaction A on SimpleChain can be calculated as follow,

$$y_{M_1} = x_1 * i_1 * j_1 *(1+k_1)$$

=5*10*1.2*（1+10%）

=66

and the ordered transaction price $y_{M_2}$ for transaction B on SimpleChain is

$$y_{M_2} = x_2 * i_2 * j_2 *(1+k_2)$$

=5*10*1.1*（1+10%）

=60.5

Confirming transaction A is prior to confirming transaction B, because $y_{M_1} > y_{M_2}$.

The mining reward $y_{N_1}$ on main-chain for transaction A is calculated as follow,

$$y_{N_1} = x_1 * i_1 * （1+k_1）$$
$$=5*10*（1+10\%）$$
$$=55$$

And the mining reward $y_{N_2}$ on main-chain for transaction B is calculated as follow,

$$y_{N_2} = x_2 * i_2 * （1+k_2）$$
$$=5*10*(1+10\%）$$
$$=55$$

When the transaction costs provided by the sub-chain with backed-token and the sub-chain with common-token are the same, the transaction of the backed-token is prioritized. That is, the main-chain miners prioritize the verification of the sub-chain with backed-token to ensure that the SIPC are firstly converted to the backed-token.

### 3.1.3 SimpleChain Total Token Supply & Adjustment Mechanism

SIPC, the token of SimpleChain, generated by mining, will be produced when the main-chain starts to operate.

The total volume of SIPC will keep the same when there is no sub-chain join the network but it will increase when new sub-chains add to the main-chain. Set the assumption that the total volume of SIPC is $C$, the block generation time is $t$ (second), initial mining reward is $m$ SIPC, and reward halved every $T_s$ (seconds) with reduction ratio $\mu$. We can write the total volume of SIPC when there is no sub-chain as formula,

$$C = \frac{T_s \cdot m}{t \cdot \mu}$$

Taking the improvement of blockchain technology and the following up ecologically development into account, the quantitative parameter of SimpleChain is set and showed in table 1.

**Table 1 SimpleChain Quantitative Parameters**

| SIPC Total Volume | Block Generation Time | Initial Mining Reward | SIPC Halving | Reduction Ratio |
|---|---|---|---|---|
| $1.0512 \times 10^8$ | 12 seconds | 20 | Once a year | 50% |

According to the quantitative parameters showed above, block generation time is 12 seconds with 20 SIPC initial mining reward, and the block reward will halve for each year (every 365 days). In the condition of no sub-chain, the total volume of SIPC is $1.0512 \times 10^8$, so mining block reward and total volume of SIPC that will be mined for every year is illustrated in figure 13.

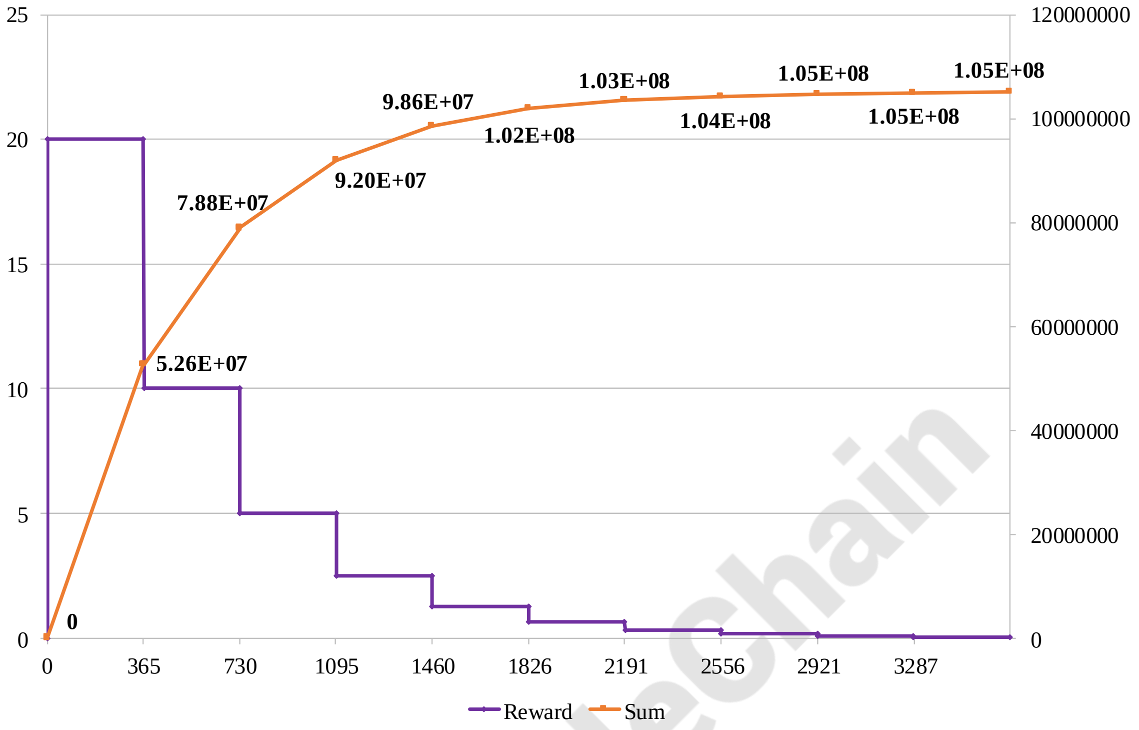

**Figure 13 Mining reward and total volume of SIPC**

The supply of SIPC will increase when new sub-chain join the SimpleChain network. It is adjusted according to some features of the sub-chain, such as type, tokens supply and price of sub-chains. Type of the sub-chain considers the existence of tokens in sub-chain. In some cases, consortium or private blockchain do not have tokens. Tokens supply is the sum of total tokens in the sub-chain. The value of the sub-chain refers to the price of token at the time when it join the SimpleChain network.

Assume that $n$ sub-chain join the SimpleChain and $\xi$ indicates whether one sub-chain has tokens or not ($\xi$=0 means sub-chain has no tokens, $\xi$=1 means just the reverse). The total volume of token on the sub-chain $i$ is $c_i$, while the token price is $u_i$ and SIPC price is $U_i$ at the begining. So the increment of SIPC with $n$ sub-chains calculated as：

$$C_{add} = \sum_{i=1}^{n}\left( (1-\xi_i)\cdot c_i \cdot \alpha + \xi_i \cdot c_i \cdot (\beta + \frac{u_i}{U_i}\cdot \gamma) \right)$$

Where $\alpha$ represents the impact factor of the sub-chain on main-chain when the sub-chain does not have tokens, $\beta$ represents the impact factor of the total volume of token on the sub-chain when the sub-chain has tokens, $\gamma$ represents the impact factor of the sub-chain value on main-chain when the sub-chain has tokens.

## 3.2 Ecology Incentive Settings

### 3.2.1 Basic Distributed Ledger Incentive

The traditional double entry system of accounting is based on the view of the business entity. With double entry system, financial accountant can effectively check and manage the entry, exit of receipt and payment of multiple internal accounts. However, its lagged and single viewed feature limits the flow of accounts in macroeconomic activities, which is happening more frequently with smaller scale. The asynchronous accounting and reporting mechanism makes accounting and auditing an high cost activity. At the same time, there have been cheating behaviors such as “book cooking” to avoid taxation trying to maintain such accounting mechanism.

The responsibility to look after SimpleChain is distributed to the entire network by different devices on the network through sharing the transaction states and the confirmations, which originally belongs to the business entity itself, and thus reduces the cost. With distributed workload and distributed rewards, the cost of ledger maintenance is kept within the ledger network instead of spread externally. In addition, blockchain data structure can be viewed as a time-series ledger database as a chain of blocks. At a macro level, the blockchain has become an globally traceable account. This penetrating, comprehensive bookkeeping system constructed a complete economic growth path.

With the consensus of PoW, SimpleChain rewards tokens to the nodes that contribute to the distributed ledger according to their working hours and computing resources. The basic incentives provided by SimpleChain will promote nodes to record, verify, and superimpose the data state of the entire distributed system during the accounting process.

### 3.2.2 Developer Community and Incentive

We have set up an incentive protocol for developers to propel the development of blockchain and the construction of the application ecosystem. We reward and encourage the developers who support and help SimpleChain with SIPC.

Rewards for code contributions are primarily focused on the development of smart contracts. The incentive protocol determines the reward $R$ based on the quality $Q$ of the smart contracts. The quality of a smart contract is determined by the addresses at which they are called and used. The influencing factors include the address influence ranking $I$, the impact factor $\alpha$, and the activity degree $A$. The higher the influence and activity of the address, the greater the value of the impact factor.

Assume in a time period of the incentive protocol is $T$, and the reward is $M$. In order to ensure the fairness of the incentive mechanism as much as possible, the address needs to satisfy the condition to be considered as a valid address. The condition is that $\alpha > 0$ and $A \ge \lambda$, where $\lambda$ is the limitation value of the address activity, and is set according to the actual situation. In a certain incentive cycle, it is assumed that there are a total number of $T$ smart contracts, and $S$ effective address calls the smart contracts. The smart contract C has a value of quality $Q_C$, and there are $N$ effective addresses in the cycle to call the smart contract C. Then, the rewards $R_C$ that can be obtained by smart contracts are calculated as follows.

$$R_C = \frac{Q_C}{Q} \cdot M = \frac{Q_C}{\sum_{t=1}^{T} Q_t} \cdot M = \frac{\sum_{i=1}^{N} (S - I_i) \cdot \alpha_i \cdot A_i}{\sum_{t=1}^{T} Q_t} \cdot M$$

In the process of implementation, the incentive protocol will be adjusted and optimized according to the actual situation for maximize the development of SimpleChain.

In addition to the above incentives for smart contract developers, technicians who make reasonable suggestions, find problems and propose solutions for SimpleChain technology will also be rewarded after evaluating their contribution value.

In addition to the above incentives for smart contract developers, engineers who make reasonable suggestions, find problems and propose solutions to SimpleChain technology will also be rewarded after evaluating their contribution value.

### 3.2.3 Nodes Extension Incentive

The node excitation of SimpleChain will be calculated according to the type of node on the chain. There is a normal verification node on the main-chain, the sub-chain has a sub-chain verification node, and a cross-chain node is set to cause cross-chain transactions. The normal verification node on the main-chain will complete the accounting on the main chain. According to the PoW mechanism adopted on the main-chain, the transaction fee for the block reward and accounting transaction will be obtained. The reward of the sub-chain verification node is calculated according to the consensus mechanism adopted by the specific sub-chain and the set economic model. The cross-chain trading nodes whose synchronized data includes the main-chain information and the sub-chain information provide a safe and correct cross-chain transaction in order to obtain the block mining rewards and the cross-chain transaction fees.

In order to ensure the correct execution of cross-chain transactions by the chain nodes, the number of cross-chain nodes and the selection of nodes must be stricter, and a deposit will be imposed. If a false transaction is provided, the deposit will be deducted and the node will be disqualified.

# 4 Architecture and Development of SimpleChain Main-chain and Sub-chain Technology

Sub-chain on SimpleChain can choose appropriate consensus mechanism according to the scene demand, and in order to ensure the stable development of the entire chain ecosystem, main-chain and sub-chain adopt a multi-layered sharding mechanism and fraud authentication to punish the miner’s evil behaviors. This chapter briefly describes the structure of main-chain and sub-chain and outlines the R&D content and plan.

## 4.1 Main-chain & Sub-chain Structure

### 4.1.1 Alternative Consensus of Sub-chain

In order to meet the application needs of various industries, SimpleChain’s sub-chain adopts a multi-consensus mechanism, that is, the sub-chain can select a suitable consensus mechanism according to actual needs. The main-chain adopts the mature PoW mechanism. The internal nodes of the sub-chain are only responsible for the internal consensus to realize the effective use of various consensus mechanism through the verification node of the main-chain as a connection. Since many of the consensus mechanisms currently proposed are still in the exploration stage, there may be unpredictable problems. The alternative consensus method of sub-chain can not only meet the needs of different scenarios, but also limit the boundary of some immature consensus algorithms of sub-chains. The main-chain proceeds security maintenance on the sub-chain while avoiding the influence of the sub-chain on the main-chain.

### 4.1.2 Main-chain & Sub-chain Multi-layer Sharding Mechanism

#### 4.1.2.1 Structure of Main-chain & Sub-chain

The main-chain and sub-chain of SimpleChain have the same structure that each block has several shards. Sharding on main-chain includes transaction sharding on main-chain and anchoring sharding for sub-chain. Sharding on sub-chain includes transaction sharding on this sub-chain and anchoring sharding related to this sub-chain. The block on the chain contains several shard slots. The miner selects the shard slot inserting into block's shard slot according to the QoS algorithm, and reaches the maximum TPS under the condition of ensuring the availability of the chain service and the anchor service.

In order to keep light and simple, the main-chain does not do a lot of data synchronization, only as a global ledger maintenance mechanism. Therefore, the main-chain and sub-chain adopt DAG-like structure, and use consensus sharding (network sharding, transaction sharding, state sharding). In the sub-chain sharding, in order to ensure a smooth and secure information flow, reasonable segmentation management and distribution of storage shard will be carried out according to actual needs and conditions. The sharding technology of the SimpleChain will continue to be promoted and developed. The sub-chain transactions being packaged through sharding will be achieved firstly and the function of sub-chain sharding will be fully implemented to enhance the TPS based on it.

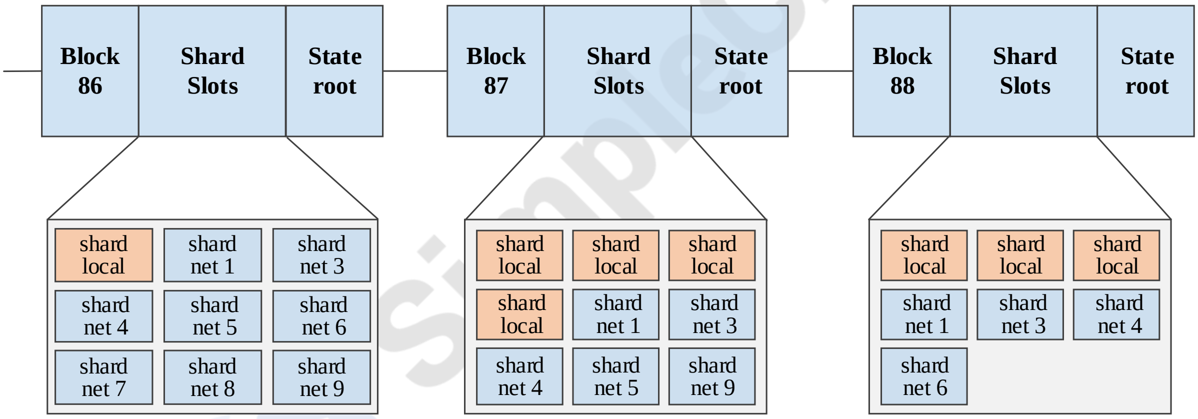

**Figure 14 Structure of main-chain and sub-chain**

### 4.1.2.2 Cross-chain Transactions

Cross-chain trade shardings are generated by anchor miners when make SimpleChain cross-chain transactions. The transaction processes between main-chain and sub-chain have five steps and they are shown in figure 15.

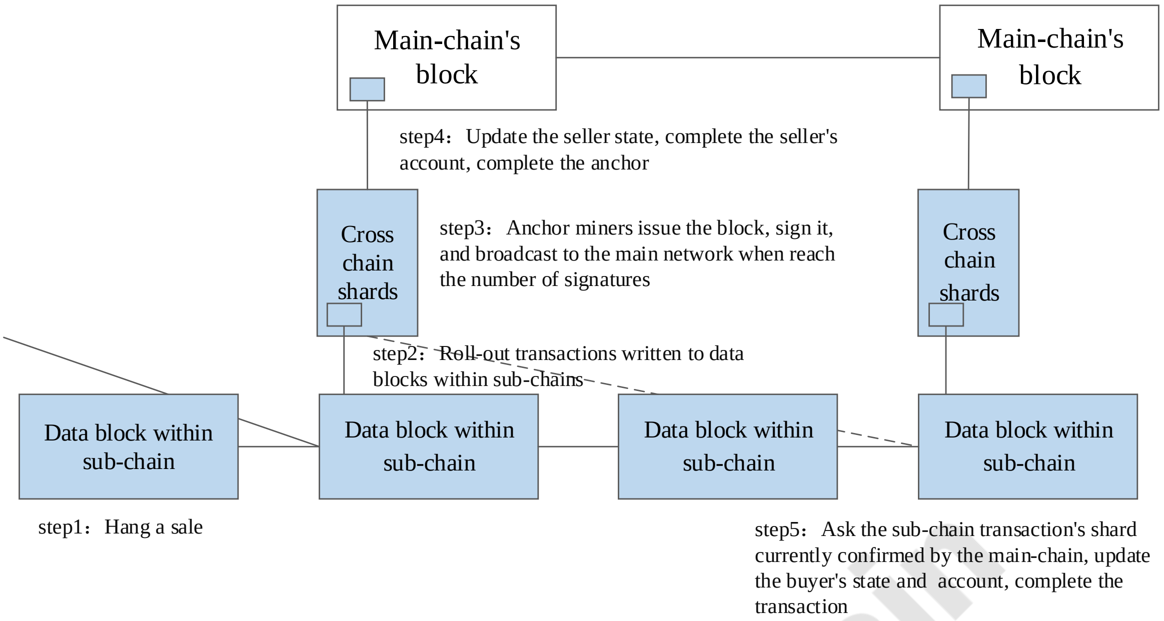
Main-chain's block
Main-chain's block
step4：Update the seller state, complete the seller's account, complete the anchor
Cross chain shards
step3：Anchor miners issue the block, sign it, and broadcast to the main network when reach the number of signatures
Cross chain shards
step2：Roll-out transactions written to data blocks within sub-chains
Data block within sub-chain
Data block within sub-chain
Data block within sub-chain
Data block within sub-chain
step1：Hang a sale
step5：Ask the sub-chain transaction's shard currently confirmed by the main-chain, update the buyer's state and account, complete the transaction

**Figure 15 Cross-chain transaction process**

In the process of cross-chain transactions, both the operation of main-chain and sub-chain have two phases which is introduced as follow,

(1) Sub-chain users submit cross-chain transactions on the chain, and then, the token is locked (the first phase of sub-chain two submitting phases);

(2) Other users submit purchase transactions (the first phase of main-chain two submitting phases);

(3) The cross-chain transaction anchoring shard, which generated by anchor miners matching cross-chain transactions, is verified by the main-chain miners and inserted into the main-chain block, and then update the status of the cross chain transaction on the main-chain (submitted the second phase of main-chain's two-phase);

(4) The sub-chain node as the light node of the main-chain, confirms the anchor information through Merkle tree and unconditionally updates the status of the cross-chain transaction on sub-chain (submitted the second phase of sub-chain's two-phase);

Cross-chain transactions satisfy the final certainty, if the sub-chain does not update the status of the cross-chain transaction on sub-chain as agreed, the anchor node does not generate anchor sharding for the corresponding fork. Therefore, all cross-chain transactions anchored on the main-chain will eventually be confirmed. At the same time, main-chain and sub-chain of SimpleChain are in a master-slave relationship. Even in the case of a temporary fork of the main-chain, the cross-chain transaction on any one of the forked main-chain and its anchored sub-chain satisfies the atomicity, and the transaction on the fork that is confirmed by the majority node is finally verified.

### 4.1.2.3 Selection of Anchor Miners

Set every *n* blocks as one period, before each period, the anchor miner $u$ with the public key address $PK_u$ pays a certain deposit to join the mining pool. Suppose each sub-chain select a fixed parameter *K* and the Merkle hash of all blocks in period *x* is $H(x)$. Before the end of a certain period *x*, the anchor miners of their respective sub-chain for the *x+2* period are selected by the way of $H_1\left(H(x), K, PK_u\right) < \mu$, where $H_1()$ is hash algorithm, $\mu$ is set threshold.

In order to avoid and inhibit fraud, SimpleChain has a fraud authentication mechanism that everyone can prove evil behaviors of anchor miners through it. Suppose the challenger finds a fraudulent account *X*, the corresponding anchor and miners' signatures are hash1 and hash2, the proof process is as follows:

(1) The challenger pledges a certain deposit, and asks the anchor miner who signed for hash2 to give the Merkle tree of hash1→hash2, the data change of account X and the signature of corresponding transaction.

(2) If the anchor miner fails to give the corresponding proof within a certain period of time, the miner will be delisted while the challenger will get a part of the miner's deposit, and the corresponding anchor block is set as an error block.

(3) If the anchor miner gives proof of the need, the challenger will lose the deposit.

### 4.1.2.4 The Security of Main-Chain & Sub-Chain's Value

1）The security of sub-chain's value

The tampering of the sub-chain data occurs only in the case of the joint evil between the sub-chain miners and the anchor miners. Anchor miners protect data and value of sub-chains that are vulnerable and have fewer nodes.

2）The security of main-chain's value

The value conversion between the main-chain and sub-chain is determined by the market. The joint evil between the sub-chain miners and the anchor miners will inevitably affect the value of the sub-chain, resulting in a change in the value exchange rate between the main-chain and sub-chain. The value of the main-chain depends on the value of the main-chain itself and the flow value between each sub-chain. Anchor miners who do evil will lose the pledged token, and the sub-chains with higher value will be joined in due to the miners' profit seeking nature. Therefore, the cost of doing so increases with the value of the sub-chains rise. For the main-chain, single sub-chain doing evil is less risky to the value of the main chain.

### 4.1.2.5 Anchor Miners Signatures Minimization

In order to improve the anchoring efficiency and solve the scalability problem, in later development phase, Schnorr-type multi-signature technology will be used to minimize the signature.

The so-called digital signature [33]is a method similar to ordinary physical signature on paper for identifying digital information. A digital signature is a string of digits that only the message sender can generate while others cannot falsify, thus not only verifying the integrity and authenticity of the information, but also verifying the source of the information. Because there are multiple signers who sign messages in real life, Itakura and Nakamura first proposed the concept of multi-signature in 1983 [34]. Subsequent researchers have proposed various multi-signature schemes based on different mathematical problems, but correspondingly there will be a problem that the signature length linearly increases with the increasing number of signatures, and the scheme has security problems. In 2006, Bellare and Neven proposed a more practical and safety multi-signature scheme based on the Schnorr's signature scheme [35].

The Schnorr signature was described by Schnorr in a paper entitled *Efficient Signature Generation for Smart Cards* in 1991 [36], which is based on the problem of discrete logarithmic DLP and is relatively safe. Schnorr signature system mainly includes *setup*, *sign*, *verify*, and etc. The specific process is as follows:

- *Setup*： System global parameters are *p*, *q* and *g*, that *p* and *q* are both large prime numbers, $g \in Z_p^*$ and $g^q = 1 \bmod p$. The local parameters of the system are *x* and *y*, where $x \in [1, p-2]$ is user's private key and $y = g^x \bmod p$ is user's public key.
- *Sign*： Suppose the message that needs to be signed is *m*, the user first randomly selects an integer $k \in [0, p-1]$, calculates $r = g^k \bmod p$, and calculates the sign $e = H(r, m)$, $s = (xe + k) \bmod q$, where $H(\ )$ is a safety hash function. After the calculation complete, $(e, s)$ as the signature of the message m is sent to the signature verifier.
- *Verify*： After receiving the message signature $(e, s)$, the verifier first calculates $r' = g^s y^{-e} \bmod p$, then calculates $H(r', m)$, and finally verifies whether the equation $H(r', m) = e$ is true. If it does, then the signature is valid, otherwise it is invalid.

In order to propose a more secure and practical multi-signature scheme, various multi-signature schemes based on Schnorr signature have been proposed. There are also some cases in which the Schnorr class signature technology is used to overcome the technical difficulities of the blockchain technology. In March 2018, blockchain developers published the Schnorr multi-signatures research paper named *Simple Schnorr Multi-Signatures with Application to Bitcoin*, which describes how to apply Schnorr-like multi-signatures to bitcoin blockchain. By multiple signatures, multiple signatures are combined into one signature, which not only saves space in the blockchain, but also enables the blockchain to handle more signatures and increase security. However, this scheme has proved to be unsafe. At present, more and more researchers are dedicated in multi-signature schemes, hoping to propose a more secure and efficient multi-signature scheme for blockchain. As the basis for securing blockchain, digital signature has always been the major research for cryptography researchers and as well as SimpleChain's.

## 4.2 Simple Contract

As the key feature for distributed applications, smart contract running on the blockchain transforms the business logic from entity controlled centric to community monitored distributed. However, due to the immutable feature of the blockchain, any smart contract running is irrevocable, therefore, any bugs or flaws for programming the smart contract could be a threat for not only the contract itself but also the whole blockchain. The DAO on the Ethereum which triggered the hard fork, is the typical but not only one of this example.

For most of the common developers however, a clean and simple way to accomplish their requirements through a straightforward way is the key need rather than a new programming language with newly defined syntax. For achieving the goal of providing a simple blockchain environment SimpleChain with its SimpleContract, will provides the modular development tools to satisfy the need of most applications. Common smart contract developers could easily find and match the right module to fit in their business logic, and with customisable parameters.

All module would be provided and audited by community developers as well as the Technical Steering Committee of the SimpleChain foundation to enhance the robustness of them. A GUI platform could further optimise the user experience of smart contract developing on the SimpleChain and hence, reduce the hurdle of developing DApps.

## 4.3 Simple IDE

For advanced developer on both the smart contract and the updating of the main-chain, an IDE will also be encapsulated into the node clients. By installing the node clients, developer cloud conduct coding and test on the offline local node. After fully testified on the local node or on the private blockchain network, it can be pushed onto the publish environment.

Once it published, the SimpleIDE will automatically list the newly pushed code on to the verification process on the SimpleChian open source community. The auditing from community developers and Technical Steering Committee will occur, and a recognised code bits with full function which passed the robustness test will be acknowledged as the new module of the SimpleContract for common developers to call.

## 4.4 Easily Deployment

Different node tools are used depending on the node type. For lightweight user nodes, the convenient and efficient mobile terminal is used. For the high demanding verification nodes, simple deployment tools are provided, including the one-click services from deployment verification to template selection to binding, and provide rich tutorial videos and deployment documents to offer tutorials help to operate. In addition, SimpleChain has a visual node management system and cloud deployment services to facilitate node's join in and manage nodes.

## 4.5 Support & Update of Security

### 4.5.1 Periodic Adjustment of Underlying Algorithm

If there are too many malicious nodes and monopoly of computing power, the main-chain will become unstable since SimpleChain adopts PoW. It is a risk to cause a hard fork similar to what Ethereum experienced in 2017. In order to guarantee the security of main -chain, the underlying of SimpleChain adopts open computing power and periodically adjusts the algorithm to prevent large-scale computing arms race, thus effectively maintaining the final certainty of block extension.

### 4.5.2 Controllable Sub-chain Openness

To ensure the security of the sub-chain, SimpleChain can control the sub-chain's development and support authorization management. A CA certificate management system based on the PKI system (supporting third-party of CA) can be used for node deployment and IDE/API access control. Only authorized nodes can be set to have permission to join the sub-chain network or use sub-chain services, that is, the extension of the license within the sub-chain.

### 4.5.3 Support for Multiple Cryptographic Algorithms

In order to adapt to different industries and diverse applications, SimpleChain uses multiple cryptographic algorithms. The supported cryptographic algorithms include international cryptographic algorithms and national cryptographic algorithms.

The cryptographic algorithm is a mathematical function used for encryption, decryption and other operations. Currently, cryptographic algorithm includes public key cryptography (asymmetric cryptography), message summary algorithms, and etc. However, the security of a crypto-system focuses on the confidentiality of the key, not algorithm. Therefore, the most of the international cryptographic algorithm and the national cryptographic algorithm are public, which is convenient for users to use these algorithms. In order to meet the needs of different scenarios, sub-chain can support for different types of cryptographic algorithms, such as RSA, AES, SHA256 in international cryptographic algorithms, asymmetric cryptographic algorithm SM2, symmetric cryptographic algorithm SM4 and message summary algorithm SM3 in national cryptographic algorithm.

### 4.5.4 Algorithm Update & Iteration

With the development of technology, quantum computers have had a huge impact on the current cryptography system. Because quantum computing has natural parallelism that makes some difficult problems in the electronic computer environment can be easily solved by using quantum computers. Existing public key cryptography is based on computational complexity, so the quantum computer with super computing power has threatened the existing public key cryptography .

At present, Shor algorithm and Grover algorithm are the main procedure can be used to decipher. Shor algorithm is a quantum algorithm for integer decomposition, and Grover algorithm is a quantum database search algorithm. Therefore, in the quantum computing environment, RSA, ECC public key cryptography, EIGamal, and etc., which are widely used now, are no longer secure.

Although quantum computers threaten many existing cryptographic algorithms, there are still some problems that quantum computers are not good at. The passwords constructed by these problems can resist the attacks of quantum computing. These cryptographic algorithms are called anti-quantum computing passwords, such as lattice ciphers.

Besides the threat of quantum computers, cryptographic algorithms need to consider the resistance from traditional attacks. Therefore, in the subsequent development process of

SimpleChain, the cryptographic algorithm will be updated and iterated to the optimal cryptographic algorithm according to the development and application requirements.

## 4.6 Main-chain’s Effective Proof of Work（EPoW）

In order to ensure the safety and finality of the main-chain, and to provid e a fair and open consensus model, SimpleChain will adopt the technical route of proof-of-work and set the goal to build an effective proof-of-work.

The so-called effective proof of work (EPoW) is based on the blockchain with distributed incentives, uses the effective computing power output as the distributed computing power type, and carries out the verification of PoW, thus will change the current status of the existing proof of work which is only for the operation hash. SimpleChain introduces the algorithm verification of matrix operation in the consensus algorithm, so that the computing power of the consensus algorithm not only can be used to the PoW, but also can be used as the required matrix multiplication operation computing power for the artificial intelligence in each layer of the deep neural network.

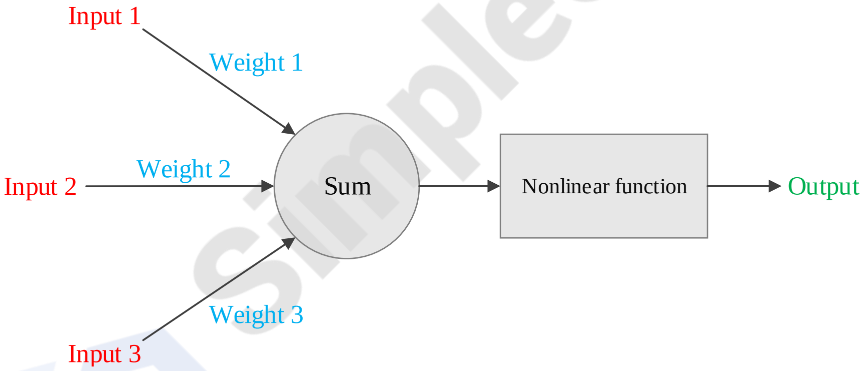

**Figure 16 Neuron model**

Deep neural networks are developed from artificial neural networks. The most basic neuron structure in artificial neural networks is an MP model. According to the typical neuron model shown above, there are three inputs, one output, and two computational functions, while the connected part is an important component of the neuron model, which is the weight. The purpose of the neural network training algorithm is the predictive effect of the entire network can be adjusted to the best by adjusting the weights [37]。

If inputs are $a_1$, $a_2$, $a_3$, and weights are $w_1$, $w_2$, $w_3$, the output $b$ of the neuron model is as follow:

$$b = f(a_1 \times w_1 + a_2 \times w_2 + a_3 \times w_3)$$

The function $f(x)$ contains the expression of summation and nonlinear functions.

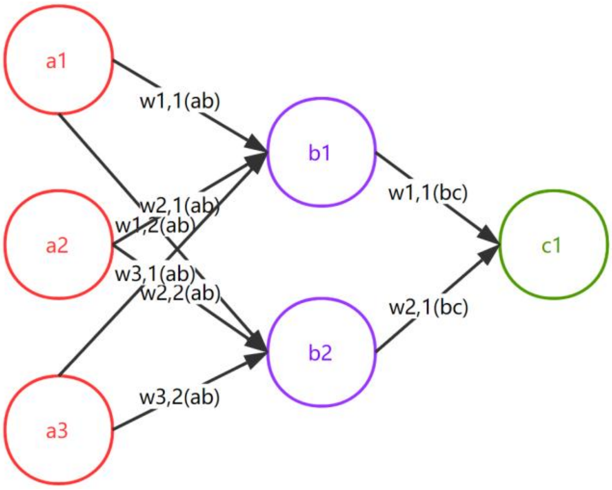

**Figure 17 Model**

When it comes to the perceptron model in the deep neural network, we add a neuron node at the input position in the original MP model and mark it as an "input unit" (red circle). The "input unit" is only responsible for transferring data, and the "output unit" (purple circle) is required to calculate the input of the previous layer.

The multi-layer network model in the above figure is represented by formulas:

$$b_1 = f(a_1 \times w_{1,1}^{(ab)} + a_2 \times w_{2,1}^{(ab)} + a_3 \times w_{3,1}^{(ab)})$$

$$b_2 = f(a_1 \times w_{1,2}^{(ab)} + a_2 \times w_{2,2}^{(ab)} + a_3 \times w_{3,2}^{(ab)})$$

$$c_1 = f(b_1 \times w_{1,1}^{(bc)} + b_2 \times w_{2,1}^{(bc)})$$

Through the above inference, it can be abstractly expressed that a large number of calculations of each layer is the matrix multiplication of the output of the previous layer and its weight value [38].

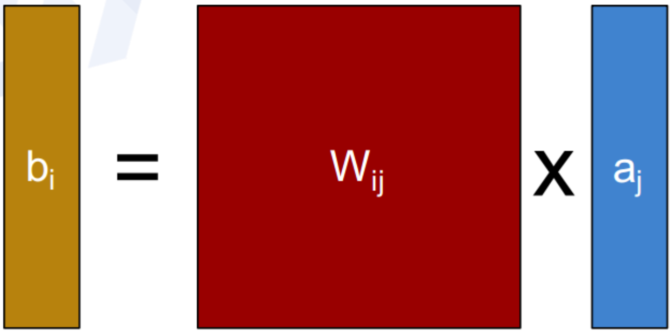

**Figure 18 Abstractive expression**

The logic of this calculation is similar to the chained application formed between the block header hashing in the blockchain. Therefore, by adding the matrix calculation to the blockchain consensus algorithm, the computing power consumed by PoW can be transformed into an effective PoW in the deep neural network algorithm as well, which serves the calculation of artificial intelligence.

Bitcoin, Ethereum and other use PoW consensus algorithm blockchains have capitalize the distributed computing power, and the EPoW will further capitalize the effective distributed computing power, promote the circulation and distribution of computing power resources, improve the efficiency of resource utilization and promote the effective solution of the impossible triangle problem of centralization, safety and environmental protection existing in the blockchain.

# 5 Team Background & Members

## 5.1 Core Team Members

### Hansen Gao

Hansen Gao is a financial technology expert and technical geek who is one of the earliest blockchain entrepreneur. Hansen was once the CTO of ibite.com, the CEO of zjmax.com, the CEO of Baoquan.com. He is also a member of the National Internet Finance Security Technical Expert Committee of China Internet association, as well as the executive director of China Blockchain Application and Research Centre.

### Leo Yu

Leo Yu is the professional of Zhejiang Blockchain Technology Association Think-tank. Leo has worked in several financial institutes with a Master's Degrees in Risk Management in UK. He was once the project manager of Government Blockchain project, Banking Blockchain project, and Industrial Securities Blockchain project, as well as the co-founder of Suanlibao.com. he also published papers on provincial and country level journals and selected as a high-yield author of the blockchain research of the Chinese Association of Science and Technology Top10. Leo Yu co-authored “Blockhain and the new-economy”, “Blockchain and Artificial Intelligence” and some other books.

### Jean

Jean is an expert both in cryptography and blockchain with a master's degree in computer science. She has rich experience in blockchain research and has long been engaged in blockchain, big data, artificial intelligence and other related industries and technology research. She has published academic papers in international academic conferences and list journals in SCI, as well as applied for a number of invention patents. She has published many blockchain industry reports and participated in the compilation and publication of the blockchain book “Blockchain and Artificial Intelligence” as well.

### Moro Zhang

Moro Zhang is the SimpleChain technical director and senior technical expert, with more than 10 years development experience in game area. He was once the technical director for multiple projects such as Baoquan.com, Bank of Hangzhou, Industrial Securities and so on. Moro has also participated in construction of many industrial consortium blockchain and development for blockchain related applications.

### Billy Qin

Billy Qin is a senior Dapp development engineer with many years of experience on different projects including Baoqun.com, eQianxin.com, blockchain-in-taxation, Suanli.com and Calforce International Station, and etc. He currently mainly focuses on the development of ChainBox and clients in the SimpleChain team.

### David Yang

David Yang is a senior R&D engineer and has worked in different companies as a software engineer with 8 years of working in the field of game and payment. Hearing about the work of the SimpleChain team, he was quick to jump to the opportunity to play a role in its development of underlying technology.

### Benett Qu

Benett Qu is the core developer of SimpleChain, as well as a senior R&D engineer. Benett is skilled with many programming languages and worked as a Java software engineer for 7 years. He has participated in the R&D development of blockchain application in multiple fields such as big data, finance and forensic. Benett engaged in the development of underlying technology and smart contract in SimpleChain team.

## 5.2 Project Consultants

### Chadwick Lee

Chadwick Lee is a well-known investor with more than two decades of experience in venture capital and investment management. He has unique insights and successful investment experience in the field of private equity investment and capital markets regionally and internationally. He has participated in dozens of investments portfolios and many companies have successfully listed. Chadwick Lee is currently focusing on investments in areas such as TMT, blockchain, advanced technology and smart hardware.

### Krzysztof Piech

Krzysztof Piech is the professor at the Department of International Economic Relations and Director of Blockchain Technology Centre at Lazarski University (Warsaw, Poland).

About 20 years of lecturing at the Warsaw School of Economics (SGH). CEO of the Blockchain Technologies sp. z o.o. & the leader of Polish Accelerator of Blockchain Technology.Professor Piech is also member of the board of directors of the International Decentralized Association of Cryptocurrency and Blockchain (Moscow), research fellow at University College London Centre for Blockchain Technologies, external associate at Iran Blockchain Labs in Sharif University of Technology.And he is the scientific editor of over 30 books. He combines science with business. He is both a startuper and a mentor of startups; he is also a consultant to dozens of businesses, and inventors.

## Zhaolin Yip

Zhaolin Yip is the Chairman of the Board of Sum V King Energy. Over the past 30 years, he has hosted several M&A and IPO projects in Singapore and has extensive experience in the capital market.

# 6 SimpleChain Foundation

## 6.1 Mission and Vision Statement

The SimpleChain Foundation is a non-profit organisation act as the supporter and promoter of the SimpleChain open source blockchain community. By spreading the idea of distributed Neo-digital economy around the world, the foundation aims to form an active developer community which would empower the development of the public blockchain infrastructure as well as a business implementation on top on that. Its mission is to make SimpleChain thrive into a comprehensive trustworthy ecosystem which will benefit a new global business world with lower cost and less asymmetric.

## 6.2 Standing Bodies of Foundation

The standing bodies of this foundation are Council, who is responsible for a comprehensive community governing as a whole for healthy development, and Technical Steering Committee, who is focusing on the technological development of the SimpleChain and technical community. Two standing bodies make decision by members voting for their own responsibilities respectively. The operational funds comes from donation of the SimpleChain community.

### 6.2.1 Foundation Council

SimpleChain Foundation council performs as the idea leader, community promoter and strategic guider at the early stage of the foundation. The members are obligated to provide resources including knowledge, skill, funding and other tangible or intangible assets to make the foundation fully functional.

The council’s membership is open to any participants in the SimpleChian open source community. The Foundation Council is responsible for operational decision making through general annual meetings and amendments could be made by voting process of the existing council members. The council’s membership will be reelected every three years.

The initial council is a composition of sophisticated industrial practitioners, academic researchers and business leaders. The total number of the initial council member is 7, and will be expanding to the total number of 14 after the first year through blockchain voting mechanism. Every member of the council has one vote for the council decision making excepting the chairman who elected thorough blockchain voting mechanism has two votes.

### 6.2.2 Technical Steering Committee

Technical Steering Committee acts as the director of the technical development of SimpleChain public blockchain infrastructure. By a majority approval through quarterly committee, the Technical Steering Committee could conduct decisions include the qualifying and disqualifying of the member of committee, the acceptance of upgrade proposal for SimpleChain infrastructure coding version control and implementation, the acknowledgement or advices for newly developed module or tool for SimpleChain application from the open source community.

The composition of the committee is the researchers, scientists and engineers who have sophisticated blockchain experience, as well as the top contributors on the successfully merged code of SimpleChain open source community, the excellent creator of Sub-chain or smart contract on SimpleChain. Each member of the Technical Steering Committee has one vote for any proposal on the quarterly committee meeting.

The initial Technical Steering Committee member is the combination of 2 researchers, scientists and engineers who have at least 3 years blockchain experience. And for any decision making of the TSC, the Foundation Council Committee has one vote as a whole to make no tie situation. After 2 years, the TSC will be expanded into 7 members group. In addition to the 2 initial members of TSC, the other 5 are the top 2 contributors on the successfully merged code of SimpleChain open source community, and top 3 excellent creators of Sub-chain or smart contract on SimpleChain.

## 6.3 Source of Fundation Funds

The operational funds of SIPC comes from the SimpleChain’s community members’ donation and the foundation serves as a non-profit organization for SimpleChain. SimpleChain foundation will have designated digital asset wallet address and smart contract account to receive either direct-digital asset or computing power donation.

For the digital asset donation, community members can transfer their SIPC, Ethereum, Litecoin,,and Bitcoin to the designated wallet.

For the computing power donation, based on the pre-determined rules of Proof of Work of SimpleChain, 5% of the total block rewards will automatically transfer to the smart contract account of SimpleChain foundation. The percentage of donation will be decreased by 50% annually. 10% of the total donation will be transferred to SimpleChain Foundation

Council address and TSC address as member’s salary. The rest 90% of donation will be used for the expansion of foundation, the promotion of SimpleChain technology and some other operations. All these decision are pre-determined by the SimpleChain Foundation Council.

The intention of donation is to provide the basic financial support to these members in Foundation Council and TSC. And it aims to weaken the foundation's influence in the community meanwhile, it also can prevent the single node from monopolizing the full computing power.

# 7 Legal Compliance & Risk Control

## 7.1 Definition of Open Source Technology Platform

Blockchain is a technology that is characterized by multi-participation, distributed structure, and the open, transparent, and verifiable principles of data on the chain. Since the blockchain proposed from Bitcoin, it has adhered to the idea of open source and community-based operation.

As a public blockchain, SimpleChain will promote participants to develop the community as much as possible and facilitate the formation of application sub-chain network based on SimpleChain. Its positioning is an open source blockchain technology platform. After launched the official version of main-chain, SimpleChain will open source the core code and tool code contributed by the initial team to support the continuous development and participation of community developers.

Of course, open source does not mean unrestricted and random use or freely and arbitrary changes. Open source technology needs to maintain the spirit of open sharing and regulatory use at the same time according to the requirements of various open source license. At present, hundreds of different types of open source licenses have occurred, each of them has different requirements. In order to promote the formation of a broad developer community with depth, SimpleChain will limit the closed source of source code modifications from open source rules, and require developers to add new code to follow this rule to maintain the continuity and coherence of the developer community. Based on the above considerations, combined with initial team's experience in the Linux open source community, SimpleChain's core code and tool component code will use the GNU General Public License (GNU GPL).

The GNU GPL [39]is proposed by the Free Software Foundation and provides HTML, text, ODF, Docbook v4\v5, Texinfo, LaTeX, Markdown, and RTF formats for embedding in other documents. GNU GPL v3 is currently the latest version, which protects new developers' copyrights on their own creative parts while further providing legal permission for copying, distribution and modification (Free Software Foundation, 2007). SimpleChain will follow this license and continue to advocate for the community to maintain the GNU GPL v3 rules.

## 7.2 Digital Asset Definition & Filing Requirements

In the economic system of SimpleChain, SIPC is the only native digital asset. As a consumable digital asset, SIPC can only be obtained by becoming a verification node of SimpleChain and running the PoW consensus algorithm to verify the blockchain transaction. According to the algorithm, generating new blocks will provide the verification nodes participating in the consensus with SIPCand verification fee as rewards .

A node holding SIPCs can create main-chain code or sub-chain code. The operation of these code requires SIPC to pay for the verification fee in order to obtain confirmation from other verification nodes. The verification fee as the feed back for the blockchain network stimulates the verification node. This is the complete SIPC supply and demand cycle.

According to the current US SEC, Singapore MAS, Swiss FINMA and other worldwide financial regulators, SIPC as a consumable digital asset or Utility Token, there is no filing application requested. The SimpleChain Foundation, as the initiator and open source community manager, ensures projects' legality with local business laws and regulations and continuously updates the constraints and recommendations for compliance and risk control in the SimpleChain community in accordance with new regulatory requirements.

## 7.3 Community Governance and Risk Warning

SimpleChain is an innovative technology architecture in blockchain. The SimpleChain Foundation is the initiator of the SimpleChain blockchain technology and community, undertaking the responsibility of early technology research and development, and community building and promotion. As a non-profit organization, the Foundation accept appropriate donations to maintain the healthy development of the community, but it does not undertake any specific obligations and does not participate in any commercial operation. The business value of the sub-chain and chain code applications in the SimpleChain community has no relationship with the Foundation.

As a continuous R&D blockchain technology and a newly established technology community, due to the technical complexity of SimpleChain's development, unpredictable or insurmountable technical difficulties, it may face delays or feature reductions. The SimpleChain Foundation will try its best to promote the technology update and iteration with the initial team and the community. The code may have a security problem due to flaws, bugs, and vulnerabilities. Through opening source, SimpleChain accepts the verification from community and any form of update suggestions.

SimpleChain’s native digital asset, as one of the functional elements in blockchain, is not any type of physical, financial or monetary assets, and has no association with any type of physical, financial, and monetary assets. SimpleChain Foundation does not guarantee the value in any form.

# Appendix: Glossary

**1、EPoW**

Short for Effective Proof-of-Work, which is proof of effective workload. Using the characteristics of blockchain distributed incentives, the effective computing power output is used as the distributed computing power type, and the workload verification is performed to change the phenomenon that only the hash operation is performed in the current workload proof.

**2、SIPC**

SimpleCoin, the token of SimpleChain, can be used for SimpleChain internal data verification (transaction).

**3、Verified transaction capacity and actual time to complete the transaction**

When it needs to be verified by the main chain, the transaction fee is determined according to the transaction capacity and completion time. The transaction capacity is the size of the data in the transaction, and the transaction time is the time when the SimpleChain blockchain network verifies the transaction.

**4、Multiple consensus mechanism**

A variety of consensus mechanisms, including PoW, PoS, PoC, etc., SimpleChain is set to meet and adapt to the needs of various industry scenarios.

**5、Node**

The nodes in the SimpleChain blockchain network include a main chain normal verification node, a sub-chain normal verification node, and a cross-chain node.

**6、International cryptographic algorithm and national cryptographic algorithm**

The international cryptographic algorithm is a cryptographic algorithm issued by the US Security Agency, and the national cryptographic algorithm is a domestic cryptographic algorithm identified by the National Cryptographic Bureau of China.

**7、Access control**

To ensure the security of the sub-chain, open-end control is performed on the nodes that join the sub-chain network or use the sub-chain service, and only the authorized nodes can join the network or use the service.

# Proper Nouns

| English | Chinese |
|---|---|
| Average turnover rate | 平均换手率 |
| Actual ratio | 实际比率 |
| Aggregate demand | 总需求 |
| Average short-term ratio | 平均短期比率 |
| Anchor miners | 锚定矿工 |
| Anchor node | 锚定节点 |
| Anchor sharding | 锚定分片 |
| Alternative consensus | 可选共识 |
| Blockchain | 区块链 |
| BFT | 拜占庭容错 |
| Bitcoin/BTC | 比特币 |
| Bitcoin cash/BCH | 比特现金 |
| Block generation rate | 出块时间 |
| Backed-token | 稳定通证 |
| Baumol-tobin model | 鲍莫尔-托宾模型 |
| Bitcoin hashrate | 比特币算力 |
| Block generation awards algorithm | 出块奖励算法 |
| Block awards function | 区块奖励函数 |
| Block /mining awards | 区块奖励/挖矿奖励 |
| Block awards adjustment | 区块奖励微调 |
| Consortium blockchain | 联盟链 |
| Consensus mechanism | 共识机制 |
| Computing power | 算力 |
| Cryptographic currency | 密码学货币 |
| Cryptocurrency | 加密货币 |

| English | Chinese |
|---|---|
| Cross-chain compatible | 跨链兼容 |
| Chain-network | 链网 |
| Common-token | 非稳定通证 |
| Commodity economy | 商品经济 |
| Credit currency | 信用货币 |
| Currency reserves | 准备金 |
| Cluster of servers | 服务器集群 |
| Capacity per transaction | 交易容量 |
| Cross chain transaction | 跨链转账交易 |
| Distributed | 分布式 |
| DPoS | 代理权益证明 |
| Digital assets | 数字资产 |
| Distributed feedback mechanism | 分布式反馈机制 |
| Difficulty adjustment algorithm | 难度调整算法 |
| Difficulty function | 难度调整函数 |
| Difficulty degree | 难度系数 |
| Difficulty raising period | 难度快速提升期 |
| Double entry system of accounting | 复式记账 |
| Ethereum Classic / ETC | 以太经典 |
| Effective proof of work / EPoW | 有效工作量证明 |
| Expected nominal yield | 预期名义收益率 |
| Exchange rate | 汇率 |
| Expected return | 期望回报 |
| Eventual consistency | 最终一致性 |
| Ethereum/ETH | 以太坊 |

| | |
|---|---|
| Fisher equation | 费雪交易方程式 |
| Full network nodes | 全节点 |
| False accounting | 假账 |
| Fraud authentication | 欺诈认证 |
| Formality fee/miner fee | 手续费/矿工费 |
| Gas | 以太坊手续费 |
| Hard fork | 硬分叉 |
| Inflation rate | 通胀率 |
| Joint evil | 联合作恶 |
| Litecoin/LTC | 莱特币 |
| Lightweight node | 轻节点 |
| Main-chain | 主链 |
| Multi-layer | 多层级 |
| Metallic currency | 金属货币 |
| Monetary theory | 货币理论 |
| Multiple sub-chain | 多子链 |
| Mining machine producer | 矿机生产商 |
| Multi-layer sharding mechanism | 分片多层机制 |
| Negative correlation | 负相关 |
| Nominal ratio | 市场名义比率 |
| Optimal token holdings | 最优通证平均持有量 |
| Proof of work/PoW | 工作量证明 |
| Peer-to-peer electronic cash system | 点对点电子现金系统 |
| Public blockchain | 公有链 |
| Permissioned blockchain | 许可链 |
| Private blockchain | 私有链 |
| Power monopoly | 算力垄断 |

| | |
|---|---|
| Plutocracy economy | 金权经济 |
| PoS | 权益证明 |
| Practical Byzantine Fault Tolerance/ (PBFT) | 实用性拜占庭容错 |
| Positive correlation | 正相关 |
| Physical assets | 实物资产 |
| Pool mining | 矿池挖矿 |
| Quantity theory of Cambridge school | 剑桥派的货币数量论 |
| Quantity model of tokens | 通证数量论模型 |
| Representative currency | 金属代用货币 |
| Ratio | 比率 |
| Relative standard deviation | 相对标准偏差 |
| Reference function of block awards | 区块奖励参照函数 |
| Reduction ratio | 衰减因子 |
| Social incentives | 社区激励 |
| Smart contract | 智能合约 |
| Sub-chain | 子链 |
| Sharing economy | 共享经济 |
| Super-sovereign reserve currency | 超主权货币 |
| Sovereign credit currency | 主权信用货币 |
| Short-term ratio | 短期比率 |
| Solo mining | Solo 挖矿 |
| SIPC output | SIPC 产量函数 |
| Steady growth period | 平稳增长期 |
| Sharding | 分片 |
| Two-way anchoring | 双向锚定 |
| Trusteeship platform | 第三方托管平台 |
| Variance of mining return | 挖矿回报方差 |

# Reference Material

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System [Z]. bitcoin.org, 2008.

[2] Buterin, V. On Public and Private Blockchains [Z]. Ethererum Blog, 2015-08-07.

[3] Prusty, N. Building Blockchain Projects [M]. *Berminghan: Packt Publishing*, 2017.

[4] Digiconomist. Bitcoin Mining is more Polluting than Gold Mining [Z]. Digiconomist.net, 2018-01-16.

[5] Bentov, I. & A.Gabizon & A.Mizrahi. Cryptocurrencies without Proof of Work [J]. *Computer Science*, 2014:142-157.

[6] Snider, M. & K.Samani & T.Jain. Delegated Proof of Stake: Features & Tradeoffs [Z]. Multicoin Capital, 2018-03-02.

[7] Lamport, L. & R.Shostak & M.Pease. The Byzantine Generals Problem [J]. *ACM Transactions on Programming Languages and Systems*, 1982, 4 (3): 382–401.

[8] Castro, M. & B.Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery [J]. *ACM Transactions on Computer Systems (Association for Computing Machinery)*, 2002, 20 (4): 398–461.

[9] Buterin, V. Long-Range Attacks: The Serious Problem With Adaptive Proof of Work [Z]. Ethererum Blog, 2014-05-15.

[10] 邵奇峰, 金澈清, 张召, 钱卫宁, 周傲英. 区块链技术：架构及进展[J]. 计算机学报, 2017:1-20.

[11] 姚前. 分布式账本技术研究进展综述[J], 武汉金融, 2018, (3):5-9.

[12] BTC.com. Network Status. btc.com, 2018.

[13] Top 500. TOP500 List – June 2018. www.top500.org, 2018.

[14] BitMEX Research. 比特币共识分叉的完整历史[Z]. blog.bitmex, 2018.

[15] 长铗. 不可能三角：安全，环保，去中心化[Z]. 8btc.com, 2014-02-04.

[16] 长铗. 计算即权力[Z]. 区块之链智能之芯, 2018-04-28.

[17] Bianews. 独家深度：BES内部报告「FCoin模式」详解[Z]. baijiahao.baidu, 2018.

[18] Odaily星球日报. EOS RAM价格暴涨会带来哪些负面影响？[Z]. 36kr.com, 2018.

[19] 中华人民共和国第十二届全国人民代表大会. 民法总则. 2017年3月15日,第127条.

[20] 潘建萍，钱塘江畔崛起“中国区块链创新城市”：互联网法院成功维权，每日商报.

[21] 维基百科.“货币”词条.
https://zh.wikipedia.org/wiki/%E8%B2%A8%E5%B9%A3#cite_note-3.

[22] William Stanley Jevons. Money and the Mechanism of Exchange, 1875.

[23] 维基百科.“金权政治”词条.
https://zh.wikipedia.org/wiki/%E9%87%91%E6%AC%8A%E6%94%BF%E6%B2%BB

[24] 任碧云，姚莉. 货币金融学. 北京：中国财政经济出版社, 2009.

[25] The exploration of the path of super-sovereign currency. ResearchGate, 2017.

[26] 刘卫平. 美国货币政策调整及其影响研究[M]. 北京：清华大学出版社, 2017: 51-54.

[27] 苗龙文. 现代货币数量论与中国“高货币化”成因[J]. 数量经济技术经济研究, 2007(12): 109-110.

[28] 曹家和. 宏观经济学[M]. 北京：清华大学出版社,北京交通大学出版社, 2006:158-162.
[29]万解秋，徐涛. 货币供给的内生性与货币政策的效率[J]，经济研究, 2001(3): 41-42.

[30] Topic: Scalability and transaction rate [Z]. bitcointalk.org, 2010.

[31] Topic: dasg [Z]. https://bitcointalk.org/index.php?topic=125.msg1149#msg1149.

[32] Why mining variance matters? [Z].
https://medium.com/@lmgoodman/why-mining-variance-matters-80ef0ff4b183.

[33] 数字签名，百度百科.
https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D/212550?fr=aladdin.

[34] K. Itakura and K. Nakamura. A public-key cryptosystem suitable for digital multisignatures [J]. *NEC Research and Development*, 1983, 71:1–8.

[35] Mihir Bellare and Gregory Neven. Multi-Signatures in the Plain Public Key Model and a General Forking Lemma [J]. In Ari Juels, Rebecca N.Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security - CCS* 2006, pages 390–399.ACM, 2006.

[36] Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *J.Cryptology*, 1991, 4(3):161–174.

[37] 史忠植. 神经网络[M]，高等教育出版社, 2009.

[38] 王玉伟. 深入理解CPU和异构计算芯片GPU/FPGA/ASIC（上篇）[Z]. 云加社区, 2017.

[39] Free Software Foundation. GNU General Public License, 2007.