MIT Project White Paper

version 1.6

2018-07

Disclaimer

Please read this disclaimer carefully. If you have any questions about the action taken, please consult your legal, financial, tax or other professional adviser.
This is a conceptual document (“White Paper”) that explains and describes our proposed Mundellian Infrastructure Technology platform and MIT tokens. This document may be subject to change or replacement at any time. However, we are under no obligation to update this white paper or to provide readers with any access to additional information. Readers please note the following:
Not open to everyone: the Mundellian Infrastructure Technology platform and MIT tokens are not open to everyone. Participation in the platform and token distribution may require a series of steps, including the provision of specific information and documentation.
No regulated products are available in any jurisdiction: MIT tokens (as described in this white paper) are not intended to constitute securities or any other regulated products in any jurisdiction. This white paper does not constitute a prospectus or any form of offer document, nor is it intended to constitute an offer or solicitation of securities or any regulated product in any jurisdiction. This white paper has not been reviewed by regulatory authorities in any jurisdiction.
No advice provided: This white paper does not constitute a recommendation as to whether you should participate in the Mundellian Infrastructure Technology platform or purchase any MIT tokens, nor should it be used as a basis for any contract or purchase decision.
No representations or warranties: We make no representations or warranties regarding the accuracy or completeness of the information, statements, opinions or other matters described herein, or otherwise convey information about the Program. In the circumstances, we make no representations or warranties regarding the achievement or reasonableness of any forward-looking or conceptual representation. Nothing in this document shall be relied upon as a basis for future commitments or representations. To the fullest extent permitted by applicable law, in the event of any negligence, default or lack of attention, any liability arising out of or relating to any relevant person or aspect of this white paper (whether foreseeable) Can be exempted. However, the scope of liability that cannot be completely waived is limited to the maximum extent permitted by applicable law.
Other companies: Except for MIT Funds Limited ("Foundation") and Mundellian Infrastructure Technology LLC, the use of any company and/or platform name and

trademark does not imply any association or endorsement with any party. References to specific companies and platforms are for illustrative purposes only.

1 Preface

1.1 Overview

In economics, there is a theory called the Mundellian Trilemma, also known as the Impossible Trinity, and the current block chain suffers from the same dilemma, namely, it is impossible to meet the following three conditions at the same time:

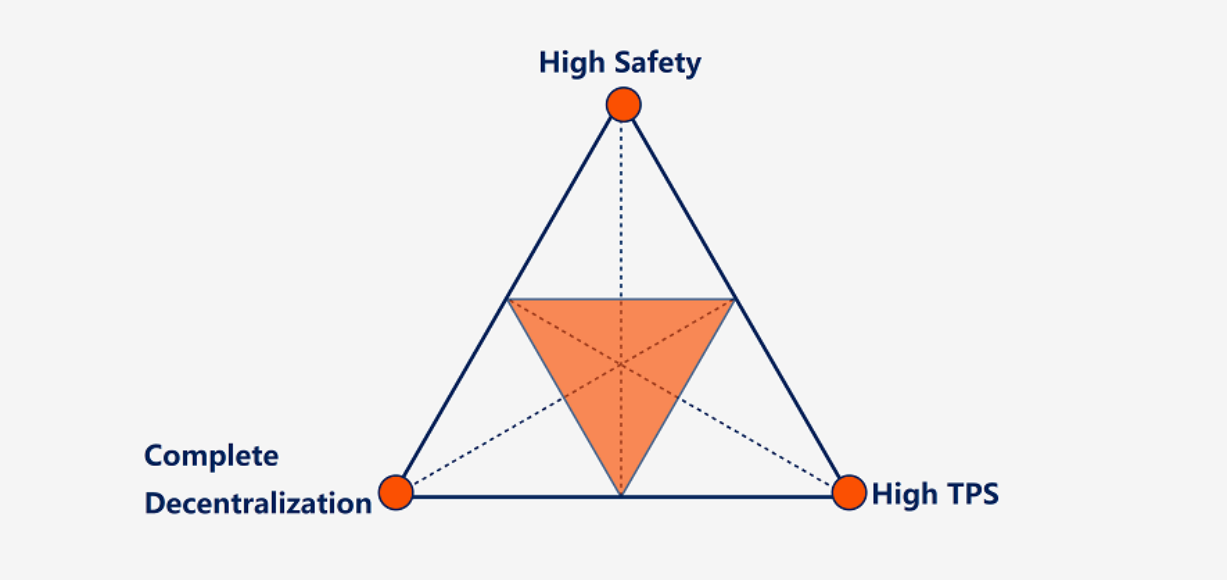


Fig 1 Blockchain Mundellian Trilemma

Bitcoin: completely decentralized, highly secure, but TPS is less than 10;

Ethereum: Highly decentralized, security is normal, there have been DAO security incidents, TPS is only about 20;

EOS: claims to process millions of speeds, but is weakly centralized because 21 centralized super nodes are established;

According to the ternary paradox theory, any new blockchain technology attempts to innovate, either need to limit TPS, or weakly centralize, or reduce the security of the entire system, can you get a reasonable balance, or even both?

Based on the characteristics of blockchain technology, decentralization, traceability, value transfer, etc., MIT will make major innovations and improvements from system architecture, consensus mechanism, distributed protocols and other aspects to create a brand new blockchain system.

1.2 Technical background

Since October 31, 2008, Satoshi Nakamoto announced the bitcoin white paper[1], Bitcoin as the largest application of the first generation of blockchain technology, opened the Bitcoin network as a point-to-point value exchange network. The booming era brought decentralized encrypted digital currency and proposed a solution to establish a peer-to-peer trust relationship that does not require third-party intervention;

Ethereum[2] as the second generation of blockchain technology, including asset digitization and smart contracts, the establishment of a world computer, brings a decentralized application platform, and solves the bitcoin blockchain scripting language is too simple The problem, on behalf of the technology is EVM Ethereum virtual machine technology and contract programming language, accompanied by innovation is the birth of a large number of decentralized applications, this is the DApp stage;

The MIT blockchain proposes a new underlying infrastructure structure for the next generation blockchain, and establishes a high-performance blockchain platform with balanced scalability, security, efficiency, etc., and forms a set of its own cross-chain collaboration technology and Protocol system to achieve point-to-point value transfer and chain-chain cooperation. Through these core

technologies and the decentralization and non-tampering characteristics of the blockchain technology itself, our system will serve the supply chain finance, digital assets, equity bonds, supply chain product sources, financial credits, etc. industry.

2 MIT Overview

2.1 MIT Blockchain Design Motivation

The main problems facing the current mainstream blockchain technology:

1. Unable to perform high frequency trading
2. Lack of a new type of smart contract platform. Currently, the existing smart contract platform is mainly based on Proof of Work (POW), and the consensus mechanism of POW is especially energy-intensive, and the interval between blocks is long, making TPS very low and difficultly applied to a real business environment.
3. Compatibility between different blockchain technologies, such as the bitcoin ecology based on the UTXO model and the Ethereum ecosystem based on the Account model, is difficult to be compatible.
4. The consensus mechanism itself lacks flexibility. Because of the different participants, the requirements for the consensus mechanism are different in the public chain and the alliance chain.
5. Data explosion, the current Ethereum full data has exceeded 200GB, and is still growing rapidly, using compression, expanding block size or using light nodes, cannot completely solve the problem.
6. The existing blockchain system has great closure. At present, most of the smart contract triggering conditions come from the blockchain system itself, and there are few external triggering conditions and lack

of interaction with the real world.

In response to the challenges of these current blockchain industries, the MIT chain has carried out a series of innovations in blockchain technology and concepts: multi-side chain multi-sub-chain node group architecture, modular replaceable adaptive consensus mechanism, based on fragmentation Dynamic weight consensus algorithm, independent DAG distributed file system, distributed cross-chain communication protocol, etc., make MIT chain become a real-world business world to provide a new generation of artificial intelligence and blockchain technology that can support large-scale commercial applications. Combined ecological world.

2.2 Core Objectives

1. Propose a solution to the data explosion that solves one of the biggest problems in the blockchain

A new frame structure multi-side chain multi-sub-chain node group is used to isolate the application logic, transaction data and production data in three layers. The main chain is responsible for token flow, side chain creation, and application logic running on the side chain. The HASH value of production data and business data is stored in the sub-chain for verification, production data and business data are saved in the cloud or other. Traditional databases such as DB2, MySQL, MongoDB, etc.

2. Support more than one million user groups

Currently, there are massively concurrent applications like Taobao, Facebook, Twitter, and eBay, which need blockchain technology that can handle tens of millions or even millions of daily active users, such as the shopping spree of Double Eleven, which is produced in a very

short time. With a huge transaction volume, the system may not work properly or even, so it is important to provide a platform that can handle many concurrent requests from users.

3. Support complex business logic and user-friendly smart contracts

The current mainstream Ethereum smart contract supports Turing's complete contract programming language Solidity and provides GAS consumption mechanism to prevent infinite loops, but the support for complex business logic is not satisfactory, and it is not very useful for use, deployment and implementation. Convenient, so MIT will achieve the goal of supporting complete business functions, clear contract results, reasonable security checks, complete debug deployment upgrades, customer-friendly, developer-friendly and enterprise-friendly new smart contract platforms.

4. AI-based smart contracts

The MIT blockchain combines a series of AI rule knowledge bases, transaction model identification, semantic analysis and other algorithms that have been successfully used in combination with Hoare logic form validation for smart contract design to ensure the security of smart contracts. Reliability and ease of use.

5. New smart contract token consumption mechanism

Unlike the complex computer system that consumes GAS in the Ethereum smart contract, the MIT blockchain uses a completely new solution, anchoring a basically stable reference object such as USDT to calculate the code execution cost in a smart contract. That is, the execution cost of each instruction is defined in French currency, the number of tokens consumed = the cost of instruction × the number of instructions × the market price of the token, and the complicated scheme of designing two sets of ETH and GAS mechanisms by

Ethereum is avoided.

3 MIT Blockchain System Architecture

The architecture of the MIT blockchain is based on layered, modular, and microservice groups. The system is divided into five layers:

The first layer is the application layer

Various application scenarios and cases that encapsulate the blockchain, such as building various blockchain applications, wallets, block browsers, Dapp, etc. are all based on Json RPC's interactive API library. Based on Json RPC, we can also create When Dapp or system sub-chain sidechains, the system is built using weakly coupled componentized pluggable replaceable microservice groups.

The second layer is the middle layer

Provide API, SDK, CLI, allowing external systems or artificial intelligence agents to access and operate. Blockchain's various business contracts (contract processes, contract services) information, various transaction results of blockchains, current process status, asset status, or blockchain transactions, proof of asset existence, chain governance interface , can also be provided to the external system in the form of API. Through the API interface, it is also possible to perform various business contract operations, such as manual processing submission, contract action transaction submission, and the like.

The third layer is the blockchain core layer

The AI service group and the most important logical parts including the MIT blockchain, such as the consensus module, the encryption security module, the storage management module, the smart

contract service including virtual machine, contract registration, lifecycle management, node registration, account management, Token management module, etc.;

The fourth layer is the network layer.

The bottom layer of the P2P network protocol is some common basic modules, such as basic encryption algorithm, network communication library, stream processing, thread encapsulation, message encapsulation and decoding, system time, etc.

The fifth layer is the hardware infrastructure layer.

The hardware infrastructure that contains the stored data can be the traditional database SQL SERVER, DB2, etc. It can also be a storage cloud or the latest interstellar file system IPFS. The chain structure of the underlying data block is encapsulated and stored in it, which is the lowest data structure in the entire blockchain technology.

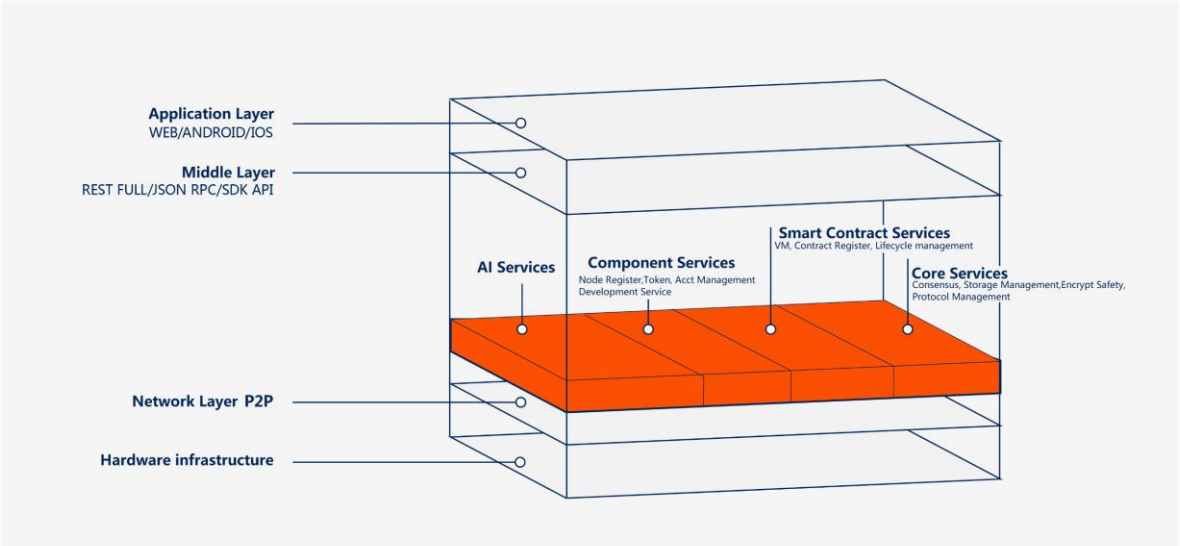


Fig 2: MIT Blockchain System architecture

4 Blockchain – Technology Solution

4.1 Multiple-Sidechain and multiple-subchain

MIT blockchain improves TPS processing speed through multi-side chain multi-sub-chain group, which can achieve more than 100,000 transaction processing per second. The same node can participate in multiple chains, and can simultaneously execute multiple transactions, parallel execution and asynchronous communication. It can support multiple business-level applications at the same time, while isolating different business processes to ensure business security and data security.

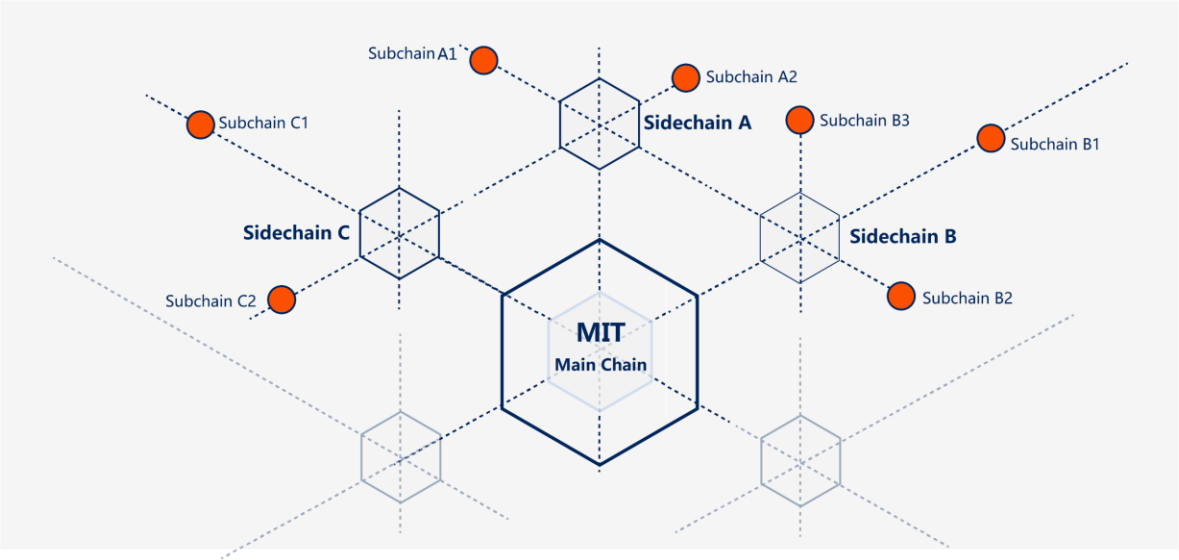


Fig 3： MIT 区块链网络结构 Fig

Sidechain

In the MIT blockchain design, each application development DAPP corresponds to a sidechain (Sidechain), and the system provides APIs to create sidechains. The side chain itself is technically a completely independent blockchain. You can choose your own consensus

mechanism, database, transaction type and account system. According to its business logic, decide whether to issue your own token and carry all the business logic of the application, but not Save production data, transaction data.

Subchain

The subchain is a subchain. Different from the sidechain, the subchain can be used as a repository for storing various data, or it can be a public service provider. For example, an IPFS subchain, a timestamp subchain, a true random number subchain, and the like can be deployed.

If the amount of data applied is huge, such as many source systems, you need to query the source report of the product, but many products are time-sensitive, such as seafood, imported fruits, red wine, etc., and one of the characteristics of the blockchain is that it cannot be modified. And delete data, so for this type of application, the MIT blockchain uses a combination of blockchain plus cloud or other traditional database, that is, the complete source report of the commodity is stored in the traditional data warehouse, but it is HASH calculated. The HASH value is stored in the blockchain of the sub-chain. When verification is required, the process is divided into three steps. One is to obtain the complete resource report from the external traditional data warehouse and calculate the HASH value; the second step is to obtain the sub-chain from the sub-chain. The HASH value of the product; the third step is to compare and return the verification result.

Inter-link routing

There are two kinds of inter-link routes in the MIT block system, one

is the network route between the sidechains, and the other is the route between the subchains. The communication rules are:

• Direct communication between side chains;

• Subchains based on the same side chain can communicate with each other;

• Inter-chain communication across sidechains is currently not supported as it greatly reduces processing speed and security risks.

4.2 Token Consume Mechanism

In addition to supporting the value transmission of one of the important features of the blockchain, MIT is different from Ethereum's complex GAS mechanism. The MIT blockchain provides a new solution, that is, the cost of code execution is a basically stable reference. USDT coins are priced so that even if the price of the MIT token market fluctuates drastically, the execution cost of each smart contract is constant, but the number of tokens to be paid goes with the market, avoiding Ethereum designing and maintaining two sets of tokens in one system. practice.

	GAS PRICE	
PARAM	Computed	Actual
DUP	3	3
SWAP	3	3
PUSH	3	3
ADD	3	3
MUL	3	5

Table 1: Ethereum smart contract instruct GAS price

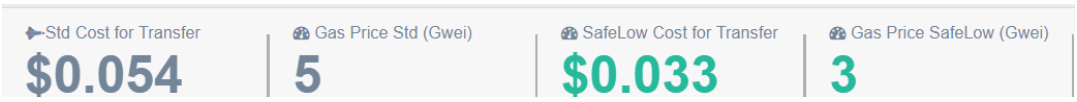


Fig 4: Price exchange rate between Ethereum GAS and ETH

For example, the execution cost of an instruction is defined as 0.00001 USDT, the smart contract contains 1000 instructions, and the current market MIT exchange rate is 1 MIT to 10 USDT, then the entire smart contract execution requires: 0.00001×1000×10=0.1USDT, Approximately 0.01 MIT, if the market volatility becomes 1 MIT to 0.001 USDT, the USDT currency cost corresponding to the same smart contract is unchanged, but the number of MITs to be paid becomes 100 MIT.

	Instruction	Price(USDT)
1	ADD	2×10^{-8}
2	MUL	6×10^{-8}
3	MOD	5×10^{-8}
4	SHA3BASE	25×10^{-8}

Table 2: MIT Blockchain smart contract instruction price

4.3 Replaceable modular adaptive consensus mechanism

The side chain and sub-chain of the MIT blockchain system are modular and replaceable. Most blockchain systems currently cure the consensus algorithm in the underlying code base, while the mainstream consensus algorithms are Each has its own advantages and disadvantages. Adaptive is a pointer to nodes with different credit ranks, and the system automatically chooses a consensus mechanism for it to achieve optimal configuration.

For example, different consensus algorithms are used for different subgroups, for example, in highly trusted sub-chains, such as financial institutions, banks, etc., PAXOS or RAFT can be used; in general trust sub-chains, such as enterprise organizations or bank alliances, SDWBFT can be used. , PBFT; in the public chain, you can use SDWBFT, POS, DPOS, Ripple consensus, etc.; within the development sub-chain, you can choose not to use any consensus algorithm, focus on business development.

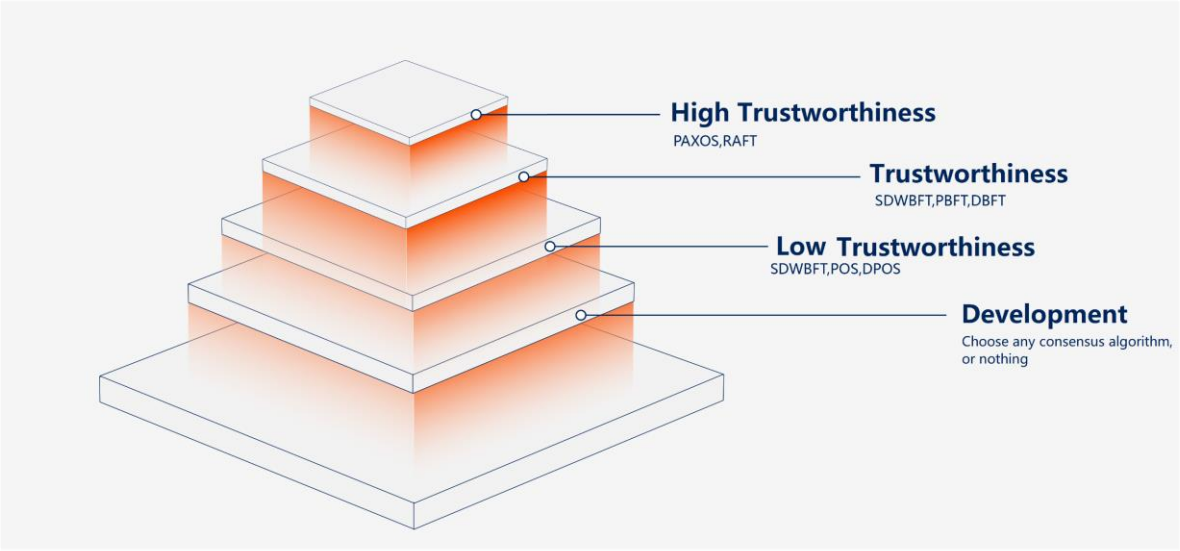


Fig 5: Replaceable modular adaptive consensus mechanism

5 MIT Blockchain Technology Introduction

5.1 Public consensus algorithm

In the consensus algorithm of the Bitcoin network, due to the excessive consumption of PoW resources and the increasing concentration of computing power, Dan Larimer proposed a fast, secure and relatively low energy consumption authorization in 2014 as the lead developer of the bit stock. Equity Proof (DPoS) Consensus Mechanism. DPoS gives each shareholder a certain amount of voting rights while minimizing the cost of the network, and they vote to generate a "super node" representative. Finally, a certain number of super nodes that obtain the most votes take turns to generate blocks equally. In the bit stock, Dan Larimer chose 101 super nodes, but selected 21 super nodes in EOS, mainly for two reasons: First, because users are difficult to fully understand a large number of super nodes, so too much Super nodes reduce the activity of user voting; second, the number of nodes with a size of 20 can achieve an efficient consensus in the Byzantine problem with lower resource costs. However, the proof of shares is very easy to generate large shareholders to commit to evil and the use of super nodes violates the principle of decentralization of blockchain. MIT blockchain adopts a new consensus algorithm based on three-dimensional weight calculation: Sharding dynamic weight Dynamic Consensus (SDWC):

• node load; • network quality; • node credit;

Weight calculation formula。

$$W_{1,\ 2,\ 3} = w_1x_1 + w_2x_2 + w_3x_3;$$

W = Relative Weight (%)

X = Normalized Value

Factor Name	Weight	Data Range	Notes
Node Credit	80%	0-100000	Bigger is better
Node Load	10%	0-1000	Smaller is better
Netword quality	10%	0-1500	Smaller is better

Table 3: Weight example table

Credit value normalization formula

$$x' = \frac{(x+1) - min}{max - min}$$

*X: Data original value

Load and network quality normalization formula

$$x' = \frac{1}{Log\,(x+1) + 1}$$

*X: Data original value

Node selection assignment principle:

• 80% of nodes choose from the highest weighted score node

• 20% nodes randomly choose from low-weight nodes

• Percentage dynamic adjustable

Credit score principle:

• Increase the credit each time the selected node releases the block by time

• Nodes make bad credits clear

• Nodes are not out of time, credit is reduced

Advantages of the SDWC algorithm:

• Balance the entire network computing power to avoid high-load nodes, giving priority to nodes with low load to verify and pop out

• Encourage new nodes to join, using better hardware and a high-speed, stable network

• The 20% new nodes were chosen to reward and encourage first-time registration nodes, thus preventing old nodes from monopolizing coins.

• Prevent malicious nodes, prevent 51% attacks, and prevent major shareholders from doing evil.

Under the premise of ensuring fairness in the consensus process, balance processing speed, security, and decentralization to provide an efficient, high-availability consensus mechanism. The reason why MIT blockchain does not adopt super nodes is because the establishment of super nodes itself has the original intention of decentralization of blockchains. If more than 10 super nodes are spoofed or invaded, the system will be completely paralysed or hijacked.

5.2 AI-based smart contract

5.2.1 Current smart contract technical defects

The intelligent contract represented by Ethereum is a state machine with unattended, program execution and automatic guarantee from the user's point of view. It can automatically release and transfer funds when certain conditions are met. A smart contract is a network service in terms of technology. It implements specific contract procedures through blockchain consensus. Because of the consensus, any intelligent contract code and state on the blockchain must be made public and subject to open testing. In the software development industry, every 1000 lines contains a security hole, and the new and new things represented by Turing's complete Ethereum smart contract, although complete and flexible, the reliability and security of the code become Big problems, such as the addition overflow vulnerability in SMT and the multiplication overflow of BEC, have led hackers to exploit smart contract vulnerabilities to steal huge amounts of digital currency.

The main shortcomings of current Ethereum smart contracts:

• Code is vulnerable to loopholes and lacks security

• Smart contracts are not smart enough to be very difficult to use

• Cannot obtain external information and cannot communicate safely and effectively with the outside world.

5.2.2 MIT Blockchain Smart Contract Design Principles - Artificial Intelligence Limitations

At present, AI technology is still in the era of weak artificial intelligence. At present, various artificial intelligence projects are emerging in the market, but various exaggerations have made the public somewhat detached from the actual expectations of AI.

However, the MIT blockchain project is aimed at achievable, providing a basic framework structure for blockchain technology that can be used for large-scale commercial applications. Through extensive research and in-depth exploration, we believe that at the current level of AI technology, we try to generate a similar "automatic" language for a Turing-complete programming language, whether based on "machine learning" or "neural network semantic analysis". The "programming" feature is fully automatic smart contract verification, which is currently not possible.

So, at this stage, we try to formally verify the Ethereum's intelligent contract language (Solidity), claiming to use the rigorous mathematical logic method to fully verify the correctness, effectiveness and security of the Ethereum smart contract. Practical.

Based on the above judgments, the MIT blockchain provides a solution to create a new non-Turing complete Contract Semantic Processing Language (CLP) that exposes artificial intelligence systems to a variety of different contracts. Once the system has mastered a

contract term, the trainer will point out other concepts that need to be identified. CLP technology makes algorithmic recognition concepts possible, even if they appear in a way that has never been seen before. For this reason, the MIT blockchain uses a concept + assertion (keyword) approach. Artificial intelligence can identify a concept, no matter how it is expressed or where it appears, so the artificial intelligence system of the MIT blockchain can run in a more mature way than keyword search.

5.2.3 MIT Blockchain Smart Contract Design Principle-Hoare Logic Formal Validation

Based on the non-Turing-complete CLP (Contract Semantic Processing Language) unique to the MIT blockchain, the MIT blockchain system will use Hoare Logic, also known as Floyd-Hoare Logic is a method of formal verification. The purpose of this system is to provide a set of logic rules for the correctness of computer programs using strict mathematical logic inference. The central feature of Hoare logic is the Hoare triple, which provides the following axioms and inference rules:

Partial Correctness

- Empty Statement Axiom

  $$\frac{}{\{P\}\ \mathbf{skip}\ \{P\}}$$

  If P is established before an empty statement, it is also true after executing this empty statement. "skip" here means an empty statement.

- Assignment Axiom Mode

  $$\frac{}{\{P[E/x]\}\ x := E\ \{P\}}$$

  Any proposition that was previously true for a variable assigned to the right hand side is still true after assignment.

- Order Rule

$$\frac{\{P\}\ S\ \{Q\}\ ,\ \{Q\}\ T\ \{R\}}{\{P\}\ S;T\ \{R\}}$$

- Conditional Rules

$$\frac{\{B \wedge P\}\ S\ \{Q\}\ ,\ \{\neg B \wedge P\}\ T\ \{Q\}}{\{P\}\ \textbf{if}\ B\ \textbf{then}\ S\ \textbf{else}\ T\ \textbf{endif}\ \{Q\}}$$

- Inference Rules

$$\frac{P' \rightarrow\ P\ ,\ \{P\}\ S\ \{Q\}\ ,\ Q \rightarrow\ Q'}{\{P'\ \}\ S\ \{Q'\}}$$

Total Correctness

- All correctness Rules

$$\frac{\{P \wedge B \wedge t = z\}\ S\ \{P \wedge t < z\}\ ,\ P \rightarrow t \geq 0}{\{P\}\ \textbf{while}\ B\ \textbf{do}\ S\ \textbf{done}\ \{\neg B \wedge P\}}$$

In order to solve the problem of the security and validity of smart contracts, combined with the formal verification of Hall logic, a three-step solution step is given:

- Pre-Condition: Standardization during contract writing and vulnerability analysis of contract releases;
- Execution and verification: completion of contract commands and dynamic security and validity verification in the MIT Smart Contract Virtual Machine;
- Post Post-Condition: Post-analysis and audit of the results of smart contract execution to ensure that the execution results must fall within the range of results specified by the smart contract without bias.

5.2.4 MIT Blockchain Smart Contract Implementation

The MIT blockchain applies a variety of techniques in artificial intelligence to the design of smart contracts, and provides

countermeasures to address various shortcomings of current smart contracts, including:

• Rule-based knowledge base syntax checking

The contract text file, through the built-in compilation tool, will construct an abstract syntax tree (AST) based on the BNF paradigm for the contract. Through the syntax abstract tree, the contract content can be grammatically recognized for simple contract security identification. . At present, it is recommended to perform a check based on the knowledge rule base on the grammar abstract tree according to the method of recursive descent analysis to determine whether there is a security risk.

• Transaction model identification and security check based on semantic analysis NLP

The grammar-based security check rules can only identify contract defects statically, while the transaction model identification and security check based on semantic analysis mainly determines the unsatisfied rules or unsafe operations in the smart contract through context-related review. Currently supported security checks include: type checking, control flow checking, and consistency checking.

Through the above static semantic analysis, it is possible to basically eliminate the various logical defects of the surface layer caused by the artificial writing smart contract but cannot solve various logical problems occurring in the dynamic execution process.

• AI-assisted formal verification and dynamic constraints

In the contract verification, the AI-assisted formal verification and dynamic constraint checking methods are used to solve the above security problems. The core ideas include: using pattern matching to obtain the user's real demand constraints, and the abstract tree formed by static semantic analysis. The Bayesian classifier is used to classify the models, and the branches in the tree are determined to belong to the corresponding generics. And the artificial intelligence classification results, obtain all the static and dynamic constraints of the current contract, based on the constraint can generate the assertion of the contract code, and based on the result for formal verification and dynamic verification.

• Smart contract security check based on AI form verification

The MIT blockchain uses formal verification techniques to automate the inspection of the security of smart contracts. Among them, the formal verification model is built using the F* Functional Programming Language, which integrates the Z3 solving tool. The

input format is SMT-LIB2.0 standard, which has rich type and condition checking functions.

The artificial intelligence method is used to automatically identify the program semantics and discover the typical patterns therein, thereby generating the attributes needed to meet the security requirements according to the pattern. When the user provides the smart contract and the translated execution code, MIT's AI engine will automatically complete the local similarity matching and global similarity matching of the code to speculate the behavior model of the code. According to the AI, the behavior model is obtained, and the corresponding formal verification constraint is generated, thereby performing deep-level behavior verification and realizing code security.

5.2.5 Virtual Machine and Sandbox

Sandbox is an execution environment that limits program behavior in accordance with security policies. Early used to test suspicious software, etc., such as hackers in order to try a virus or unsafe products, they can often run them in a sandbox environment. The classic sandbox system is generally implemented by intercepting system calls, monitoring program behavior, and then controlling and restricting the use of computer resources by the program according to user-defined policies, such as network calls, IO read and write, and so on.

The MIT blockchain system has designed a new MVM (MIT Victual Machine) to implement the sandbox mechanism. MVM includes an analysis module that invokes AI microservices, and a text semantic smart contract translation module, as well as an engine that executes the translated smart contract, which can be used to execute post-translation bytecodes, using system-level APIs such as network transport-related Modules, but not allow third-party libraries, which requires DAPP developers to use the SDK package provided by MIT to obtain information from secure sidechains through a network protocol, thus taking into account the completeness of security and functionality.

5.3 Distributed Cross-chain Protocol

The cross blockchain protocol of the MIT blockchain mainly includes two parts: a message address and a message packet. The protocol address includes the chain identifier (srcChainID) of the message source chain and the current chain height (Height). A message packet consists of two parts: a message header (MessageHeader)

and a message body (MessageBody). The message header includes a start chain identifier (srcChainID), a target chain identifier (destChainID), a message status (MessageStatus), a message validity time (MessageValidDuration), a trigger transaction, and the like.
The message status corresponds to the message status mechanism in the network message protocol. When a message packet is sent, the message status is "receive pending". When the receiver receives the message, it will return a message packet to the sender, in which the message status is "successful transmission". If the sender receives the message packet containing the "send successfully" identifier, the sender will reply to the other party with a " Received successfully "identified message packet. The above is a success message. If there is a message packet reception failure during the process, for example, if the receiver does not reply "send successfully", the sender will resend the transaction after a certain time, trying to establish communication again.
In addition to the above status, we also specify the "connection timeout" status. When a transaction is sent from sidechain A to sidechain B, it indicates the message lifetime of the specified link based on the height of the block. Before the arrival time of the message, the link returns the status of the message result to the side chain. If the message lifetime is exceeded, the link is directly returned to the sender "connection timeout" status. The sender side chain logs the message as a message failure.

6 MIT Blockchain Application Area

At present, the MIT blockchain is divided into two parts. The first is the blockchain underlying infrastructure. The second is the upper layer for multiple industries. The MIT blockchain will be developed in cooperation with multiple companies and organizations in many industries around the world. And put together several actual projects based on MIT technology, and will carry out in-depth mining and expansion of related industries, providing a solid blockchain infrastructure for all industries to improve efficiency and reduce costs. Here are a few examples of applications that will be available on the MIT blockchain.

6.1 Supply Chain Finance

Supply chain finance is a huge market with a scale of 10 trillion yuan. According to the public data of the National Bureau of Statistics, the balance of accounts receivable of industrial enterprises in China at the end of 2017 was 13.48 trillion CNY. At the end of 2016, China's industry the balance of accounts receivable of enterprises was 12.58 trillion yuan, a year-on-year increase of 8.5%. From the year-end balance of accounts receivable of industrial enterprises in the past five years in the coming year, the annual ending balances are increasing, and both the prospect and the growth space are high enough. The current industry pain points are mainly:

- SMEs have difficulty financing and have high costs;
- Difficulties in the circulation of financial bills;
- The risk of trust is always the

re and the cost of risk control is high;

• The core corporate role is too heavy and the bargaining power is too high.

Supply chain finance is typical of multi-party participation and cooperation, but it is subject to the low transparency of the entire supply chain industry, as well as information asymmetry, imperfect credit mechanism, etc., and there is no traditional centralized organization in governance, so with the help of MIT The development of next-generation information technology such as blockchain, big data, artificial intelligence, and Internet of Things promotes the transformation of traditional supply chain finance into digital and intelligent, better integrates information flow, capital flow, and logistics, and establishes dynamic credit evaluation. System to achieve high efficiency and high quality of funds. Supply chain finance will move toward a digital form, an intelligent way, and rely on the paradigm of blockchain to help shape the future industrial ecology.

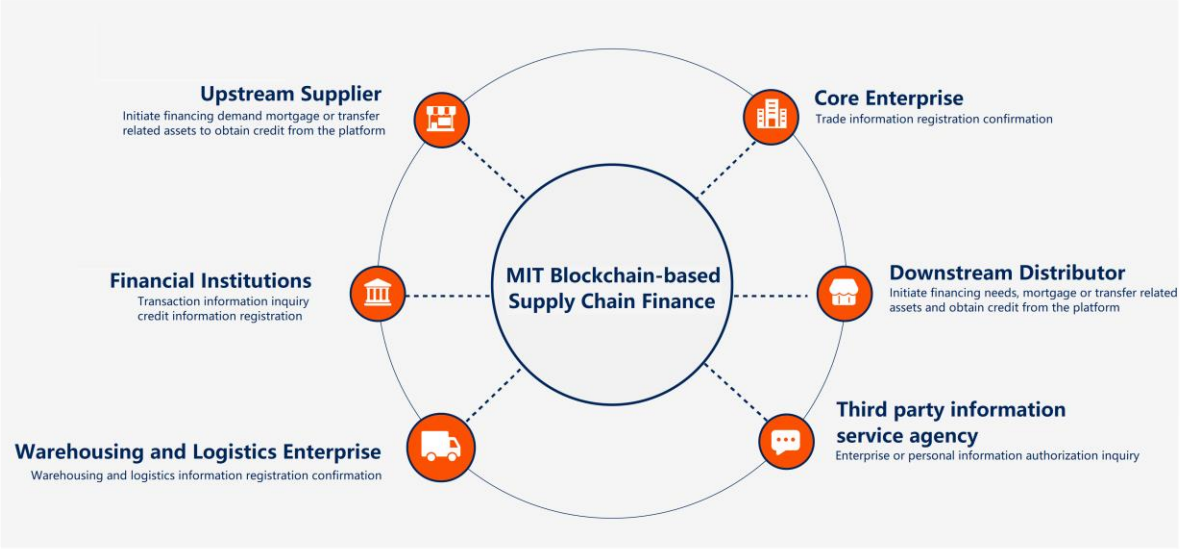


Fig 6: Supply Chain Finance Process Architecture

6.2 Asset Digitization

Compared with the traditional centralized system, the advantage of the blockchain in the field of digital assets is that once the assets are issued on the blockchain, the subsequent circulation links can no longer rely on the issuer system. In circulation, the assets are controlled by a single center. As a social communication, any channel with resources may become a catalyst for asset circulation. Therefore, the blockchain can greatly enhance the efficiency of digital asset circulation and truly achieve “multi-party issuance and free circulation”.

For traditional asset services, the corresponding intermediary, such as the asset owner's certificate, authenticity notarization, etc., requires the intervention of a third party to complete the entire circulation process. There are several pain points in the current model:

(1) After the assets enter circulation, they must still rely on the asset issuer system to complete the use and transfer, which limits the circulation of assets to the user system of the issuer system;

(2) Traditional asset distribution channels are limited, and almost all rely on large channels. The large channels of the industry have increased their expenses due to the monopoly position, resulting in circulation and significant cost increase. It is difficult for small channels and individuals to play a role in circulation.

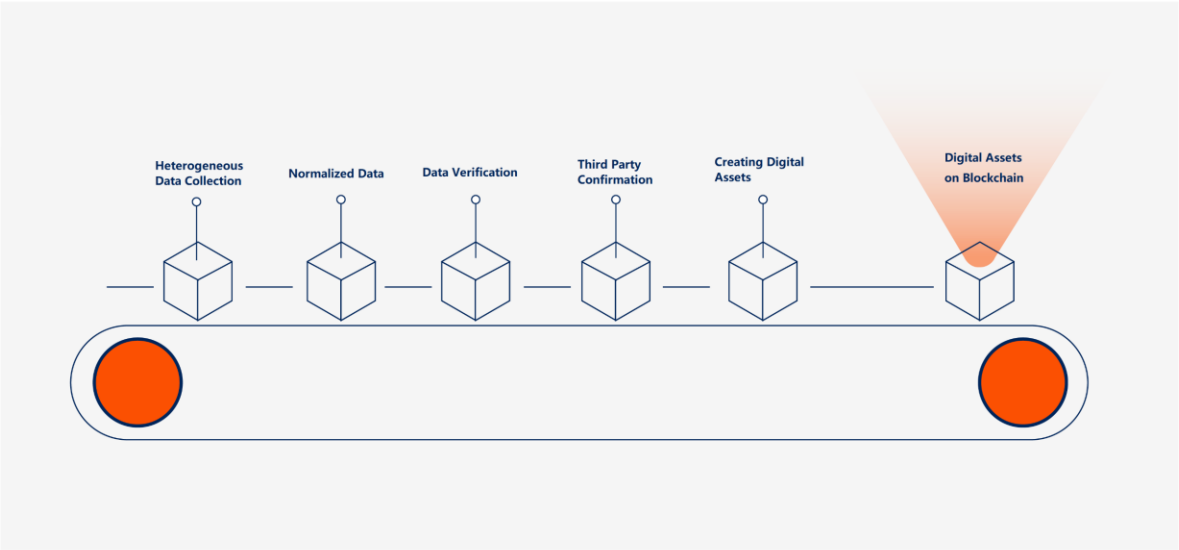


Fig 7: Assets digitalizing Process

6.3 Product Provenance

At present, there are more and more counterfeit and shoddy products on the market, such as waste oil, poisonous bean sprouts, fake milk powder, and XX superior products of major e-commerce companies also frequently send counterfeit goods. The nature that suffers the most is consumers, especially the purchase of fake and shoddy food and medicine, which will cause harm to our human body. At the same time, the reputation of the company will also be harmful, and the brand will be drastically reduced. Therefore, traceability plays an important role in social life. It can realize the traceability function of the whole supply chain from raw materials, processing and processing to logistics and sales. Once the relevant accidents occur, the supervisors can judge whether the company is at fault through the system. The system can also use the system to find out which link and steps have occurred, so that the problem can be solved faster. The MIT blockchain organically combines technologies such as the Internet of Things, blockchain, and intelligent anti-counterfeiting. It

utilizes the technical characteristics of blockchains that are open and transparent, unable to cheat, non-tamperable, and information security, and solves the problem of opaque information in various supply chains. Solve the problem of consumer goods trust from the source, protect the interests of consumers and achieve the brand value growth of target customers.

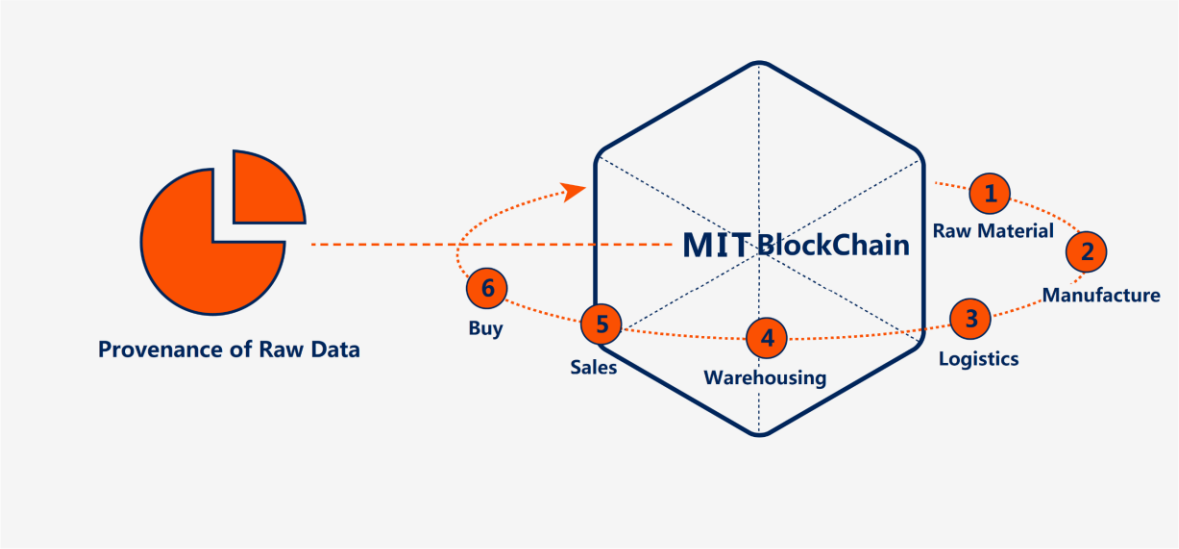


Fig 8: Product Provenance Process

7 MIT Core Team and Advisors

Jason Huang

CEO

Ph.D. in Computer Software, Tsinghua University

He has worked for well-known technology companies such as Lucent, CA, and Microsoft.

Excellent technical experts in the field of blockchain, more than ten years engaged in the design and development of distributed systems, cloud computing and communication standards. In 2006, the world record of the PennySort World Sorting Competition was created by the BSIS algorithm and was awarded by American Engineering Fellow Jim Gray and Chinese Academy of Engineering Academician Sun Jiaguang.

Adam Mallet

CTO

Master of Computer Science

University of Queensland, Australia

Worked at IBM and HP as Senior Architecture Engineer.

Technical expert in the field of blockchain. Joined the BTC community in 2010.

Si Wei

CIO

Doctor of Artificial Intelligence

Australian National University

NASA Senior Technical Specialist

NASA leads the world's top data traceability standard PROV3.0 and leads the development of the PROV4.0 standard.

Richard Fang

COO

Master of Finance, University of Queensland, Master of Banking Finance;

Several supply chains, founders and operators of fresh cold chain companies, senior investors; engaged in the supply chain industry for more than ten years, with rich industry experience, profound insights into the operational details of the entire industry。

Alexander Kristensen

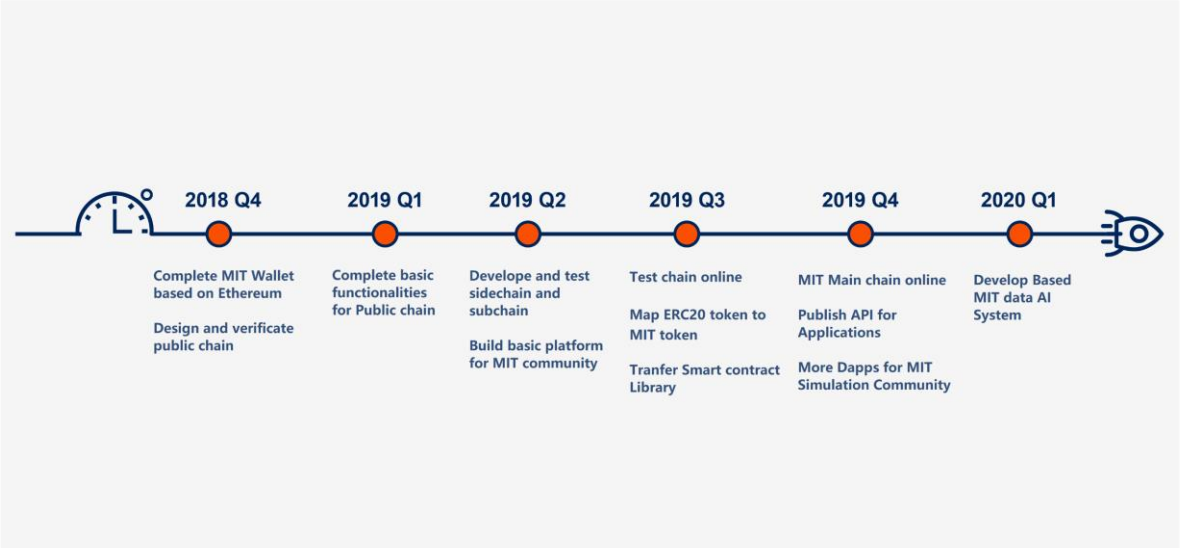
Chief Adviser

Master of Business Administration

Edinburgh Business School

Computer Science and MBA, Senior Risk Control Consultant, Scandinavian Bank, Hedge Fund Model Design Specialist

8 Road Map



2018 Q1	2018 Q2	2018 Q3	2018 Q4	2019 Q1	2019 Q2	2019 Q3	2019 Q4
Start MIT Project	Select and design the technical path of public blockchain for MIT project	Completed the MIT white paper	PC wallet based on CLI	Mobile wallet based on IOS	Launch pre-α version of MIT main chain	Launch α version of MIT main chain	Launch β version of MIT main chain
Research and analyze the advantages and disadvantages of the existing public chains	Start writing technical white paper	Completed project website v1.0	MIT blockchain browser	Mobile wallet based on Android	将共识引擎结合共识算法进行联调	Include verification and implementation of CBP distributed cross-chain protocol	Implementing sharding functionality for main chain and light nodes
	Confirm strategic partners	Create and execute solidity scripts based on ERC 20 for project token	Verification and implementation of sharding dynamic weighted consensus	Develop kernel of MIT blockchain	MIT network file system	Verification and implementation of cross-sidechain routing protocol	Realize transaction model identification and security check based on semantic analysis NLP
			Release open source code on Github and keep updating	Develop P2P network protocol	MIT main chain deployment, debugging and rollback mechanism	Verification and implementation of cross-subchain routing protocols	The formal verification of Hoare Logic is realized through Z3 and using F* function
				Develop block storage for ledger	Verification and development of MIT sidechain	Verification and implementation of Non-Turing complete CLP (contract language	Dapp integrated development environment
				Runtime environment development	Multi-sidechain support	Implement the abstract syntax tree (AST) based on the BNF paradigm	A pluggable and modularized mechanism for Various consensus algorithms
				Test network development	Verification and development of MIT subchain		
				Consensus algorithm test	Multi-subchain support		
				Consensus engine design and validation			
				Consensus engine implementation			

9 TOKEN Distribution Plan

The total number of MIT is fixed at 10 billion，distribution plan as the below:

%	Recipient	Purpose	Condition
40%	Public Offering	For project development	No feezing or limitations
10%	Initial Investors	For investors and investment institutions	Frozen for one year and a maximum of 2% can be sold monthly from the second year
10%	Founding and Developmer	For development team	Frozen for one year and a maximum of 1% can be sold monthly from the second year
		Administration Committee	
10%	Project protection	Rewards to ensure the benefits of investors and supportors of the project.	Token are rewarded and not for sale
10%	Cooperative institutio	Encourage cooperative business organizations and communities	Token are rewarded and not for sale
20%	Marketing	Business development, marketing, publication and others	Token are rewarded and not for sale

10 Risk Disclosure

Currency supervision risk

Governments are still designing public policies on the regulation of cryptocurrencies as a form of trade settlement. Governments that use encrypted currency for local businesses may issue laws and regulations that use password currency as a regulated activity. In recent weeks, countries such as China and South Korea have issued regulations or statements prohibiting the sale of tokens, while other countries have attempted to regulate token sales as a securities issue. This may result in MIT token holders not being able to use their MIT

tokens in the future without the MIT tokens further advancing compliance.

Risks associated with token/crowdfunding sales

MIT tokens are not investment products. Specifically, MIT tokens can provide specific functionality in the MIT system. Without MIT tokens, the public may not be able to access the MIT system. There is no future profit or benefit from the MIT token. For these and other reasons, we believe that the sale of MIT tokens does not constitute securities that meet the registration requirements of the public offering prospectus. However, the public policy of token sales is changing, and it is conceivable that regulators may expand the scope of regulation of token sales in the future. This may result in token sales being subject to registration requirements in the United States and similar jurisdictions. If MIT token sales are subject to registration requirements, this may delay or delay the sale of the proposed MIT token indefinitely.

Tax risk

The use of MIT tokens as a settlement currency may be subject to local income tax, capital gains tax, value added tax or other forms of taxation. This uncertainty in tax legislation may expose merchants and customers to unforeseen future tax issues related to the use of MIT tokens as settlement currency and/or token transactions or Well token capital gains.

Capital control risk

Many jurisdictions, such as China, impose strict controls on the flow of cross-border capital. MIT token holders may be subject to these regulations and/or enforced by such regulations at any time. This would make the transfer of MIT tokens from certain jurisdictions to

overseas exchanges an illegal activity that would subject users of MIT tokens to government penalties or other regulatory sanctions.

CTF and Anti-Money Laundering Regulations

The United States has introduced a series of regulations to combat terrorist financing and money laundering. Many other countries have enacted similar laws to control the flow of capital for these illegal activities. In this case, the illegal use of any MIT token (such as money laundering activities by criminals) can seriously affect the international reputation of the MIT network. This may lead to censorship by CTFs and anti-money laundering regulators and may have a significant negative impact on the distribution and circulation of tokens and MIT tokens in the MIT ecosystem.

Blockchain risk

In the Ethereum network, since the block time is determined by the workload proof, the block time is random. The buyer confirms and understands that the Ethereum Smart Contract may not package the buyer's transaction at the buyer's expected time, and the buyer will not receive the MIT token on the same day that the buyer sent the ETH. The Ethereum blockchain may experience periodic blockages, in which case the transaction may be delayed or lost. Individuals may also deliberately confuse the Ethereum network to make a profit on the purchase of MIT tokens. The buyer acknowledges and understands that the Ethereum miners may not package the buyer's transaction when the buyer wants it, or may not package the buyer's transaction at all. MIT tokens may be lost and/or stolen. Hackers or other malicious groups or organizations may attempt to interfere with the distribution and circulation of MIT networks or MIT tokens in a variety of ways, including but not limited to malware attacks,

denial of service attacks, consensus-based attacks, Sybil attacks, smurf attacks, and electronics. Fraud. In addition, because the Ethereum platform relies on open source software and the MIT network is based on open source software, Ethereum smart contracts may contain intentional or unintentional vulnerabilities or weaknesses that may negatively impact MIT tokens or lead to buyers. The token is lost, the buyer loses access to or controls the tokens it purchases, or the ETH in the buyer's account is lost. In the event of such a software error or defect, the company may not be able to provide any remedy, and the company cannot guarantee that the MIT token holder will receive any remedy, refund or compensation. Everything raised in this white paper is new and untested. Therefore, the project may not be completed, implemented or launched. Even if the project has been completed, implemented and enabled, it may not function as expected, and any tokens associated with the blockchain that uses the project may not have the expected functionality or value. Moreover, due to rapid technological development, MIT networks or tokens may be outdated. The regulatory status of cryptocurrency, digital assets and blockchain technology is unclear or unclear in many jurisdictions. It is therefore difficult to predict how the government will regulate these technologies and whether the government will make any changes to existing laws, regulations and/or rules affecting cryptocurrency, digital assets, blockchain technology and its applications. Such changes may have a negative impact on the MIT network and tokens in a variety of ways, including, for example, determining that tokens are regulated financial instruments that require registration. If government actions make it illegal or continue to operate projects

that are not commercially viable, the company may stop issuing MIT tokens and project development or stop projects in a jurisdiction.

Business risk

The company plans to stop the sale of tokens after receiving sufficient funds. If the company raises less than a certain amount from the sale of MIT tokens, the company may not have sufficient funds to implement its business plan, and buyers who purchase tokens will face higher investment risks.

The ability of the company to remain competitive may depend in part on its ability to develop new products and/or enhance existing products or services and to deliver these products or services in a cost-effective manner. In addition, the introduction of our competitors' products and services, enhancements or the use of other technologies may result in a decline in the sales or market acceptance of our existing products and services. We cannot guarantee that a company will succeed in selecting, developing and promoting new products and services, or enhancing existing products or services. Failure to do so may adversely affect the company's business, financial condition and operating results.

The company's ability to achieve its goals depends on its ability to attract and retain more quality talent. The competition for these talents is fierce, and we cannot guarantee that the company's performance will not be adversely affected by the inability to attract and/or retain qualified personnel.

The industry in which the company is located is a completely new industry and may be subject to high levels of government oversight and review, including investigations or enforcement actions. We cannot guarantee that government agencies will not review the

company's operations and/or take enforcement actions against the company. Such government activities may or may not be specific to the company's results, but all of these activities may result in the company being judged or punished, or the company reorganizing its business and activities, or discontinuing the provision of certain products or services, all of which may harm The company's reputation may increase the company's operating costs and may have a significant adverse impact on the development of MIT tokens and/or projects.

12. Contact Us

You can contact us in the following ways to get up-to-date information about the MIT platform and its tokens.

Official website： MIT.club

E-Mail： info@MIT.club

Wechat： MITclub

Telegram： Blockchain MIT@mitblockchain

Facebook： MIT Club

Twitter： Mitclub

Github: MITFC

13. References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.
[2] Buterin, V. (2014). A next-generation smart contract and decentralized application platform.
[3] T. Stein, Supply chain with blockchain — showcase RFID, Faizod, 2017
4． R. Hackett, The financial tech revolution will be tokenized, Fortune, 2017.
[5] D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.
[6] A. Back, Hashcash — a denial of service counter-measure, Hashcash.org, 2002.
[7] B. Dickson, Blockchain has the potential to revolutionize the supply chain, Aol Tech, 2016.
[8] KCDSA Task Force Team, The Korean certificate-based digital signature algorithm, IEEE Standard Specifications for Public-Key Cryptography, 1998.
[9] R. T. Clemen, Incentive contracts and strictly proper scoring rules. Test, 2002.
[10] J.-Y. Jaffray, E. Karni, Elicitation of subjective probabilities when the initial endowment is unobservable, Journal of Risk and Uncertainty, 1999.
[11] Blockchain Luxembourg S.A., https://blockchain.info.
[12] J. Gong, Blockchain society — decoding global blockchain application and investment cases, CITIC Press Group, 2016.
[13] D. Johnston et al., The general theory of decentralized applications, Dapps, 2015.
[14] P. Sztorc, Peer-to-peer oracle system and prediction marketplace, 2015.
[15] R. Hanson, Logarithmic market scoring rules for modular combinatorial information aggregation, Journal of Prediction Markets, 2002.
[16] Goldman Sachs report Blockchain Putting Theory into Practice, EQUITY RESEARCH | May 24, 2016.
[17] IBM 区块链技术（Blockchain）简介---z Systems China Client Council, for ICBC, Mar. 2016