# ABSTRACT

Ti-Blockchain, committed to developing the public chain ecology beyond the existing blockchain, will combine the IPFS system to solve the existing financial problems and a large amount of idleness in network storage.

The key feature of Ti-Blockchain is encrypted distributed storage with smart contracts based on graphene technology. Smart contracts can control the level of encryption of stored files and protect the privacy of users in business applications. Distributed storage is called a never-gone hard disk, which uses the space of free hard disk and achieves the purpose of safe storage through reasonable redundant design. Ti-Blockchain will focus on the continuous development of encrypted distributed storage while landing more commercial projects. Its will be used in different levels of encrypted communication system, mainly in the electronic medical record system, electronic education record system and electronic contract system.

Decentralization can significantly reduce the risk of data interruption and its loss, and increase security and confidentiality. Cloud storage relies on third-party large storage providers to transfer and store data, such as 360 cloud disks and cloud storage disks. However, subject to a centralized architecture, it is highly vulnerable to various security threats. Redundant and decentralized distributed storage can effectively improve this situation, effectively preventing tampering and unauthorized access. Files are encrypted prior to uploading the server, protecting the contents of the data, leaving the data owner complete control over the encryption keys and thus limiting others' access to the data.


Traditional Storage and Distributed Encryption Storage

This article mainly introduces the product structure, technical characteristics and advantages of Ti-Blockchain's blockchain. The core value of the blockchain lies in building a trusted, distributed, multicenter system that has the potential to become an infrastructure for building a value internet. Titanium chain project is committed to build enterprise-level blockchain products and provide industry solutions. It has developed a high-performance, highly scalable blockchain finance, business services platform, aimed at enterprise-class operational capabilities. Ti-Blockchain's blockchain has made a number of technological breakthroughs and innovations with respect to the performance, scalability, security and operation and maintenance, forming a series of technical features and advantages. Based on the in-depth exploration of blockchain application scenarios with industry partners, the Ti-Blockchain's blockchain has been applied in the fields of digital assets, trade finance, equity bonds, public notary and data security. Its multi-center trust, as the core, creates ABS + cloud storage network, so that corporate information data become more credible.

**Keywords:** Blockchain, Ti-Blockchain, decentralization

# Contents

# Chapter 1 Cryptography Terminology and Abbreviations

## 1.1 Cryptography Terminology

Key: Divided into encrypt key and decrypt key.

Clear-Text: the information directly representing the original meaning with no encryption.

Cipher-Text: the information after encryption and hide the original meaning.

Encryption: The process of translating clear text into cipher text.

Decryption: The process of translating cipher text into clear text.

Password Algorithm: the encryption and decryption methods that cipher system used. With the development of cryptography based on mathematics, the encryption method is generally called the encryption algorithm, and the decryption method is generally known as the decryption algorithm.

Model of Cipher Communication System: For a given plain-text m and key k, the encryption transform Ek changes the plain-text into a cipher-text c = f (m, k) = Ek (m). At the receiving end, using the decryption key k, To complete the decryption operation, the cipher-text c is restored to the original plain-text m = Dk, (c). A secure cryptosystem should satisfy:

①illegal interceptors find it difficult to deduce plaintext m from cipher-text C.

②encryption and decryption algorithms should be fairly simple and apply to all key spaces;

③the confidentiality of passwords depends only on In the key;

④legitimate recipients can test and verify the integrity and authenticity of the message;

⑤the sender of the message can not deny the message it issued, but also can not fake legal information of others;

⑥if necessary arbitration institutions arbitrarily.

Hash algorithm: A hashing algorithm maps binary values of any length to short, fixed-length binary values. This small binary value is called a hash value. Hash is a piece of data unique and extremely compact numerical representation. If you hash a plaintext and even change only a single letter of the paragraph, subsequent hashes produce different values. To find two different inputs that hash to the same value is

computationally infeasible, the hash of the data can test the integrity of the data. Generally used for quick search and encryption algorithm.

Hash table is based on the set hash function H (key) and conflict handling methods will be a set of keywords mapped to a limited address range, and keywords in the address range of the image as recorded in the table stored Location, this table is called a hash table or hash, the resulting storage location known as the hash address or hash address. As a linear data structure compared with the forms and queues, hash table is undoubtedly the search speed is faster.

Fixed-size results can be obtained by applying unidirectional mathematical functions (sometimes called "hashing algorithms") to any number of data. If there is a change in the input data, then the hash will change. Hash can be used for many operations, including authentication and digital signatures. Also known as a "news feed."

Simple Explanation: The hash algorithm, the hash function. It is a one-way cryptosystem, that is, it is an irreversible mapping from plaintext to ciphertext, with only the encryption process and no decryption process. At the same time, the hash function can be any length of the input to get a fixed length of the output changes. This unidirectional feature of the hash function and the fixed length of the output data make it possible to generate messages or data.

A hash table (also known as a hash table) is a data structure accessed directly based on the key value. That is, it accesses the record by mapping the key value to a location in the table to speed up the lookup. This mapping function is called a hash function, the record array is called a hash table.

For a given table M, there exists a function f (key), and for any given key value key, the table M is called a hash if the address of the record containing the key in the table can be obtained after being substituted into the function, and the function f (key) is a hash function.

## 1.2 Proper Nouns in Digital Currency

**Bitcoin:** An encrypted digital currency, launched in 2009 by open-source software developer Satoshi Nakamoto.

**Ethereum:** A common blockchain platform with intelligent contract capabilities.

**Intelligent Contract:** A time-driven, state-of-the-art program that runs on a

replicated, shared account and that holds the assets in your books.

**Public Chain:** A blockchain where anyone can send a deal anywhere and the transaction can be validly identified and anyone can participate in the consensus process.

**Ethereum Virtual Machine:** Designed to run on a virtual machine on all participant nodes in a peer-to-peer network. It can read and write executable code and data in a blockchain, verify data signatures, and be semi-Turing complete Way to run the code. It executes code only when it receives a data-signed verification message, and the information stored on the blockchain distinguishes between the appropriate behaviors.

**Incentives to prove proof of consensus:** In the proof of equity proved to add incentives to estimate nodes online, incentive network nodes can remain online in order to maintain the stability and security of the network.

**Hard Forking:** Permanent disagreement occurs in the blockchain. After the new formula rules are released, some nodes that have not been upgraded can not verify the chunks produced by the upgraded nodes.

**Turing Complete:** A computational system that can calculate each Turing computable function is called Turing Complete. A language is Turing complete, meaning that the language's computing power is comparable to a universal Turing machine, which is also the highest ability that modern computer languages have.

**Oracle:** The input data is screened according to a preset judgment condition, and the most suitable data is selected as the input data.

**Data feeds:** Data feeds provide data link data sources for the blockchain.

**POS:** Equity certification consensus mechanism. According to the proportion and time tokens of each node, the mining difficulty is reduced proportionally to speed up the search for random numbers.

**UTXO:** No spending transaction output. The transaction model is used in Bitcoin networks.

**POW:** Workload proof consensus mechanism. One (often referred to as a prover), submits computations that are known to be difficult to compute but easily verifiable, and anyone else can validate the answer to make sure that the prover has done a significant amount of computational work to get the result.

**DAO:** Distributed autonomous organization. Through a series of fair and open

rules, organizations can operate autonomously without any intervention or management.

# Chapter 2 Theoretical Basics

As the core revolutionary force of financial science and technology, blockchain technology, combined with cloud computing, big data, artificial intelligence and mobile technology, has been organically integrated with many fields such as Internet of Things, insurance, automotive, manufacturing, healthcare, energy and shipping. Internet and other new technologies for the new round of technological and industrial innovation revolution to provide kinetic energy.

## 2.1 The Origin and Development of Blockchain

Blockchain technology has led to people's thinking about abandoning the inefficient and outdated system and opening up entirely new ideas for disrupting multi-industry operations and trade. As a distributed ledger, it has great potential in many fields, especially in the financial industry. Since the data stored in the blockchain can not be tampered with, we believe that blockchain technology can take the data's authenticity and security to a whole new level.

### 2.1.1 Background

In lately 2008, a man named Nakamoto wrote a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" at the Bitcoin Forum. In this paper, the concept of blockchain was proposed for the first time. It can support the mining and trading of bitcoin as the basic technology for constructing the encrypted transmission of bitcoin network and transaction information.

Nakamoto believes that dealing with transaction data with a centralized approach (third-party agencies) not only fails to overcome the problem of mistrust between merchants and customers, but also entails high transaction costs and limited transaction size. To solve such problems, Nakamoto created a blockchain and invented Bitcoin on the basis of it.

### 2.1.2 Definition

The essence of the blockchain is a shared, open, common record of participation in the database. In the absence of a central server, it allows devices such as the computer where it is linked to communicate with each other using "consensus mechanisms," and all networked (peer-to-peer network) devices (nodes) maintain consistent and continual data updates. Because of this model, the blockchain is also known as the "distributed ledger," the distribution of which means decentralization, and the ledger is the vehicle for recording data, so the blockchain can be understood as "decentralized data ecosystem".

### 2.1.3 Development Path

In 2008, Nakamoto made a bitcoin thesis. In 2009, the Bitcoin virtual currency platform was established. In nearly nine years, the Bitcoin system has been operating steadily, enabling Bitcoin distribution, distribution, trading and payment to be automated. As the first application of blockchain technology, its achievements are obvious to all.

In 2015, the concept of blockchain gradually became independent from the virtual currency as a foundation to support technology. It is transformed into a smart contract programmable platform through which various types of assets and contracts can be registered, validated, and transferred, and the concept of a digital asset distribution platform is shaped.

Therefore, bitcoin can be referred to as "blockchain 1.0," a programmable virtual currency. Ethereum open source project can be considered "blockchain 2.0", the smart contract platform. The blockchain 3.0, which is still at the stage of conception, surpasses the economic field and can realize the automated distribution of material assets and human resources all over the world. At the same time, it can promote large-scale government, health, science, culture, arts and other fields Scale collaboration.

## 2.2 The Features and Applications of Blockchain

Blockchain technology has the main features of decentralization, openness, self-control and autonomy, unchangeable information and anonymity, so it has a wide range of application development space in the fields of fund transfer and payment, pan

finance and credit investigation. Can be used with cloud computing, Internet of Things, big data and other innovative technologies.

### 2.2.1 Features

Decentralization: There is a third party (center) organization between the merchant and the client to assist the fund confirmation and settlement in traditional network transaction payment, but using the blockchain technology, under the action of the distributed network consensus mechanism, the transaction data can realize "Automatic" identification and verification that third-party participation can therefore "GET OUT".

Openness: Except that the private information of the parties involved in the transaction is protected by encryption, the data in the blockchain can be disclosed on the entire network and all the connected devices can view the related information at any time.

Self-control and autonomy: Based on the establishment of network rules such as consensus mechanisms, all devices in a blockchain network can automatically and securely record, update, and exchange data that no organization or individual can intervene.

Information can not be tampered with: Once validated data is entered into the blockchain, it is stored permanently. Unless more than 51% of the blockchain network's device data is changed (almost impossible), it can not be partially tampered with.

Anonymity: Each node in the blockchain network can exchange data with each other in a non-public status. In other words, the parties to the transaction can complete the payment, transfer and other transactions without knowing the other party's relevant information.

### 2.2.2 Application Direction

**Transfer and payment:** At present, this is the most mature application of blockchain technology. Blockchain technology avoids complicated systems, saves bank reconciliation and review processes, speeds up the settlement of funds, and at the same time greatly reduces transaction fees.

**Pan-finance business:** Blockchain technology can be used in asset trading, rapid audit and other fields. The two sides of the user to reach the transaction intentions, as transaction information is added to the blockchain, the transaction is declared completed. This eliminates the need to register multi-party data checking with clearing agencies, which not only improves efficiency but also facilitates future audits.

**Credit field:** The technical characteristics of blockchains can solve the problem of trust in financial activities at low cost. Trust is the foundation of financial activities, the regulation of financial activities, including product registration, information disclosure, fund management, credit information system construction are all to solve this problem. In the context of the whole society being actively building credit information system, the gradual maturity of blockchain technology has provided excellent conditions for creating a mutual trust and mutual trust financial environment.

**Combination of innovative technologies:** Blockchain technology can also be combined with innovative technologies such as cloud computing, Internet of Things, big data and so on. The application prospect is extremely broad. Relative to traditional technologies, blockchain can help the financial industry effectively improve efficiency and reduce costs and risks. Intermediate costs are effectively reduced without the involvement of third-party agencies. With the improvement of operational automation, the settlement speed is faster and the labor costs are greatly reduced. At the same time, the blockchain can streamline the service process through multiple signatures and other technologies to improve work efficiency, and the recorded information can not be tampered with and can be traced back. This also provides convenience for supervision and auditing work.

In addition, the possible risks are significantly reduced due to the confirmation of transactions, the simultaneous completion of clearing and settlement. Digital trading process can effectively solve the problem of avoiding human input errors. At the same time, due to the characteristics of blockchain such as distributed network and consensus mechanism, system risks such as hacker network attack and server downtime can be effectively avoided. The future, in the energy industry, including residential electricity, electricity purchase, etc. can also be automatically executed through the smart contract. The carbon trading market can also use blockchain technology to improve transparency,

fairness, to avoid double counting and other issues. In addition, the technology can also be used for land ownership and liquidation transactions.

# Chapter 3 Ti-Blockchain Overview

## 3.1 Background of Ti-Blockchain's Birth

The advent of peer-to-peer value transmission networks has its historical inevitability, while Nakamoto Satoshi is a person accelerating this historical process. From the development of the TCP / IP protocol in the 1980s to the application of the Web browser and the application of the server in the 1990s, the Internet technology has changed the mode of data exchange and human life from different aspects and dimensions. The development of Internet technology benefits from the improvement of infrastructures and the popularization of various intelligent terminals from the early information superhighways. These also form the basis of unlimited expansion of the application layer in the Internet OSI seven-layer model.

In the Internet protocol stack, we use TCP / IP, HTTP, HTTPS, FTP, TELNET, SSH, SMTP, POP3 and other network layer, transport layer, application layer protocol, and with these protocols, we have built a wide range of Internet services. But if we think about it, we will find that until the emergence of the Bitcoin network, we have been unable to carry out the transfer and transmission of peer-to-peer values on the Internet without resorting to the help of third parties. In fact, we are not short of a particular method, but we lack Value Super Highway, a value highway based on Information Super Highway, and how to realize the value transmission (VTP) of Value Super Highway, which is exactly running at information speed. The first VTP protocol on the highway.

With the development of interoperability technology (Internet, Internet of Things, VR / AR), people and objects, people and information interact more diversified and more entities are digitized and tokenized or tokens Tokenize and Symbolize. Once the entity is digitized or tokenized, the mapping and segmentation of the entity's assets over the Internet are completed. The immediate question is how to transfer these assets and values point-to-point? Therefore, it can be speculated that with the further deepening of Internet services, the boundary between entities and virtual networks will begin to blur. The demand for point-to-point value transfer will be highlighted. Therefore, the Value Super Highway and Value Transfer Protocol on the Internet are bound to appear, while the bit The currency network has accelerated this historical process.

## 3.2 Development Vision of Ti-Blockchain

Ti-Blockchain will create a trusted business ecosystem for investors, companies and regulators. Investors can view the balance sheet, income statement, cash flow analysis and other financial documents on the Ti-Blockchain; the company can use the Ti-Blockchain to release the company's documents, such as: white paper, budget, code development, management structure, financial statements, etc. Released in the Ti-Blockchain, so interested investors access. In future versions of the Ti-Blockchain, the files can be reviewed through intelligent contacts.

For individual consumers, the Ti-Blockchain can be used as a digital safe, and consumers can upload documents encrypted on the blockchain. No one else can decrypt the document except the person who encrypted the document. Technically, using public and private keys is easy to do. The user uses the public key to encrypt the document. Due to the asymmetric nature of public / private keys, only the person holding the private key can decrypt the document. Therefore, anyone else, including the Ti-Blockchain, can not decrypt the document.

For business users, Ti-Blockchain can be used as a collaborative space for users to work together on a single document. intelligent contracts have access restrictions that allow only users with actual rights to view the file.

Ti-Blockchain also support asset securitization. As a financial innovation, Asset Backed Securitization (ABS), which has enjoyed rapid growth both at home and abroad in recent years, is one of the hot words in both domestic and overseas capital markets. Asset securitization is a form of financing for the issuance of tradable securities backed by a specific portfolio of assets or a specific cash flow. Generally speaking, asset securitization refers to assets that will be liquid but have a steady income (or expected income) To be sold through the issuance of securities in the capital markets to obtain a means of financing development funds. Asset securitization is very common in some countries. More than three-quarters of U.S. mortgages and more than three-quarters of car loans are made by issuing asset-backed securities. The biggest advantage of asset securitization is that, for the issuer, not only reduces the funding threshold, but also provides the liquidity of assets, for investors, can break the investment restrictions, reduce risk and increase revenue.

Ti-Blockchain also has a complete intelligent contract Turing. It can automate the

management of assets on the chain through intelligent contracts and extend business functionality flexibly without changing the chain code. With the distributed storage services provided by Ti-Blockchain, intelligent contracts can play a bigger role, such as: to realize paid files storage and sharing through contracts; to spread confidential documents in a limited scope through contracts; to achieve contract's and document's notarization through contracts; to manage time-sensitive documents such as wills through contracts, etc.

## 3.3 Distribution of Tokens on Ti-Blockchain

The total amount of TV is 210 million, and the specific distribution is as follows:

160 million as a market circulation,

The remaining 50 million is owned by the team and within the next 10 years a tenth, namely 5 million coins will be unfreezed each year on 1, Jan., which will be used as:

Development costs: The development of the platform requires technical research and development, recruitment of personnel, team building. Enough development costs would make sure the project proceed as planned.

Consultation costs: We will set aside a part of the funds to consult the professionals and institutions in related fields, to ensure adequate market research.

Legal fees: For certain unexpected legal events that may arise in the future, we need to retain a portion of emergency funds. Thus guarantee projects can get long-term development on the right path.

Marketing Costs: As TV is a very broad project that can be vertically involved in many fields, TV needs to maintain good relationships with multiple agencies and users in many fields, also we will give some token back to the community supporters.

Other costs: various expenses other than the above mentioned.

# Chapter 4 Technology of Ti-Blockchain

## 4.1 Technical Characteristics of Ti-Blockchain

### 4.11 Data Storage

Ti-Blockchain will provide a DPOS mode token to support the operation of the titanium chain. Ti-Blockchain will provide intelligent contracts + multi-scene application + online cloud storage capabilities. Ti-Blockchain will provide storage space on the basis of smart contracts, and save basic company information such as business license, tax, personnel and monthly financial statements during the company's operation.

Files and data can be stored in a series of segments framed by the shard technology, and the data owner can separately determine how the file is sharded and where the shards are in the network. Without the prior knowledge of the location of shards, as the network proliferates, the difficulty of finding any given shard increases exponentially. This means that the file's security is proportional to the square of the network size. Fragment size is negotiable contract parameters. The normalized size discourages the sidelines from trying to determine the content of a given slice and can mask the slice flow across the network. Split large files such as video content and distribute fragmented nodes to reduce the impact of content delivery on any node. All devices in a cloud storage system are completely transparent to the user and any authorized user anywhere can connect to the cloud storage via an access cable for data access to the cloud storage. Through a variety of data backup and disaster recovery technologies and measures can ensure that the data in the cloud storage will not be lost, to ensure cloud storage its own security and stability.

Ti-Blockchain utilize Kademlia (Kad) for data indexing and rapid routing support for distributed storage. The Kademlia agreement is a study published by PetarP. Maymounkov and David Mazieres of the University of New York, "Kademlia: A peerto-peer information system based on the XOR metric." It is a distributed hash table (DHT) technology, but compared with other DHT implementation technologies, such as Chord, CAN, Pastry and so on, Kad through a unique XOR (XOR) for distance measurement based on the establishment of a The new DHT topology, compared to other algorithms, greatly improves the routing query speed. Kademlia belongs to a

typical Structured P2P Overlay Network. It is the main problem that Kademlia attempts to solve by storing and retrieving information in distributed application-layer and whole network. In the Kademlia network, all information is stored as hash table entries, which are scattered across nodes to form a huge, distributed hash table across the network. We can vividly consider this hash table as a dictionary: as long as we know the key of the information index, we can query its corresponding value information through Kademlia protocol, regardless of whether the value information is stored in Which node is above? In eMule, BitTorrent and other P2P file exchange system, Kademlia mainly acts as the key role of file information retrieval protocol, but Kad network application is not limited to file exchange.

In the Kad network, all nodes are treated as leaves of a binary tree, and the location of each node is uniquely identified by the shortest prefix of its ID value. For any node, this binary tree can be decomposed into a series of contiguous subtrees that do not contain their own. The topmost subtree consists of the other half of the entire tree that does not contain its own tree; the next subtree consists of the rest without its own half; and so on until the entire tree is split. The figure shows how node 0011 divides the subtree.

### 4.1.2 Consensus Mechanism

The consensus of the current mainstream mechanisms are: POW, POS, DPOS.

①POW workload proof (that is, mining), by AND OR to calculate a random number to meet the rules, that is, to obtain the right to this account, issued the current round of data needs to be recorded, the other nodes of the network verified together stored;

Advantages: completely decentralized, free access to nodes;

Disadvantages: Currently bitcoin has attracted most of the world's computing power, and other re-use of Pow consensus blockchain applications is difficult to obtain the same computational power to ensure their own safety; mining caused a lot of waste of resources; consensus reached a cycle of more Long, not suitable for commercial applications.

②POS Proof of ownership, which is an upgrade consensus mechanism of Pow; according to the proportion of each node and the proportion of tokens time; reduce mining difficulty equal to speed up the search for random numbers.

Advantages: to a certain extent, shorten the time reached by the consensus;
Disadvantages: still need mining, essentially no solution to the pain of commercial applications.

③DPOS shares authorized certification mechanism, similar to the voting board, holding a number of nodes voted cast their proxy for verification and accounting.
Advantages: Dramatically reduce the number of participating verification and accounting nodes to achieve second-level consensus verification;
Disadvantages: The whole consensus mechanism is still dependent on tokens, many commercial applications do not need the existence of tokens.

Ti-Blockchain decided to use DPOS consensus mechanism. The POW algorithm requires high computational power, and due to the benefit driven, computational power will eventually be concentrated in a small number of mineral pools, and therefore can not achieve the purpose of completely decentralization. DPOS does not need to consume a large amount of computing resources, providing a quick consensus. Voting to elect the proxy out of the block ensures that the network will not be dominated by the minority (in the case of a large scatter of post tokens). This is very similar to the actual electoral mechanism and it is even fairer. Naturally, as long as the agent can provide sufficient stability, it is natural for everyone to vote for him.

### 4.1.3 Multiple Signatures

Multiple signatures are a way of managing multiple accounts with multiple private key holders.

Unlike the traditional cryptocurrency, the transaction is mainly verified with a definite signature, and the multiple signatures use multiple private key signatures to operate on an account. Multi-signatures manage accounts using $n/m(m \geq n > 0)$. In creating m private keys of the account, as long as there are n private key signatures, operations such as fund transfer can be performed on the account. This can be applied in many scenarios. E.g:

① Preventing the loss of the private key of an individual user causes the account to become unusable;

② The collective assets of companies and other organizations can be jointly managed to prevent unauthorized use by individuals or minorities;

③ It can be applied to the voting / election scene.

### 4.1.4 Contract and Consensus Mechanism

**Contract Languages:** We use a class Lua language as the default programming language for intelligent contracts on titanium chains, support for static compilation into bytecode and then bytecode execution on blockchain networks as needed.

Lua is a Turing complete programming language, compiler and bytecode virtual machine targeted design and optimization in the blockchain.

**Contract Interpreter:** The Contract Interpreter is an interpreter of Lua's bytecode. In operations or block synchronization verifications that involve smart contracts in a blockchain network, the blockchain node takes the contract word out of the blockchain if needed Section code, loading the bytecode with the Lua bytecode interpreter, and then invoking the required API with the appropriate parameters, the resulting run-time results and context-state changes are used by the blockchain.

An operation on a smart contract may call an indefinite number of times at many different nodes at different times, but the result of each invocation of the same operation at different times and at different times is the same as that of the context status.

Intelligent contracts operate because of the need for different nodes of computer resources for execution and take up blockchain capacity and network traffic, so the operation of smart contracts need to deduct a certain amount of execution costs.

## 4.2 Safety of Ti-Blockchain

**DPOS model:** Safety is the main focus of our Ti-Blockchain’s design. Ti-Blockchains use so-called "provably secure DPOS blockchain protocols." The algorithm has the following five features, making it a very safe DPOS model.

First, the model focuses on persistence and activity, which are two of the formal attributes of a healthy trading ledger. Persistence means that once a system node announces that a transaction is "stable," the remaining nodes (if queried and truthfully responded) will also report it as stable. Here, stability is to be understood as a predicate, which is parameterized by some safety parameter k and affects the certainty of property holdings. (For example, "Too deep than k blocks.") Activity guarantees that once a real-generated transaction has been offered to a sufficiently large number of network nodes, say u time steps, it will become stable. The combination of activity and permanence guarantees a healthy transaction ledger, meaning the use of real-life

transactions and making it constant.

Second, we describe a new DPOS-based blockchain protocol. Our agreement assumes that participants are free to create accounts, receive and pay, and these rights vary over time. We use a very simple, secure, multi-part voting protocol to achieve the randomness of the first election. This prevents the so-called grind attack, which distinguishes our approach from other previous solutions (the previous scenario either defined this value to introduce entropy based on the current blockchain or the use of collective tossing) [4] . In addition, the uniqueness of our approach lies in the fact that the system ignores round after round of changes to the rights. Instead, the current group of interest holders is regularly recorded, called epochs; at each such interval, a secure multi-party calculation takes place using the blockchain itself as a broadcast channel. Specifically, in each era, a randomly chosen group of stakeholders forms a committee and is then responsible for executing the tossing agreement. The outcome of the agreement determines the set of next-time rights holders for the next era of implementation and the outcome of all the first elections to that era.

Third, we provide a formal argument that no opponent can break the persistence and activity. Based on some hypothetical assumptions, our agreement is safe:

① highly synchronized network;

② Most of the selected proprietors may participate in each epoch as needed;

③ Interests will not be off-line for a long time;

④ Adaptive damage is subordinate to a small delay, and the safety parameters are linear. Or, participants can access an anonymous broadcast channel from the sender.

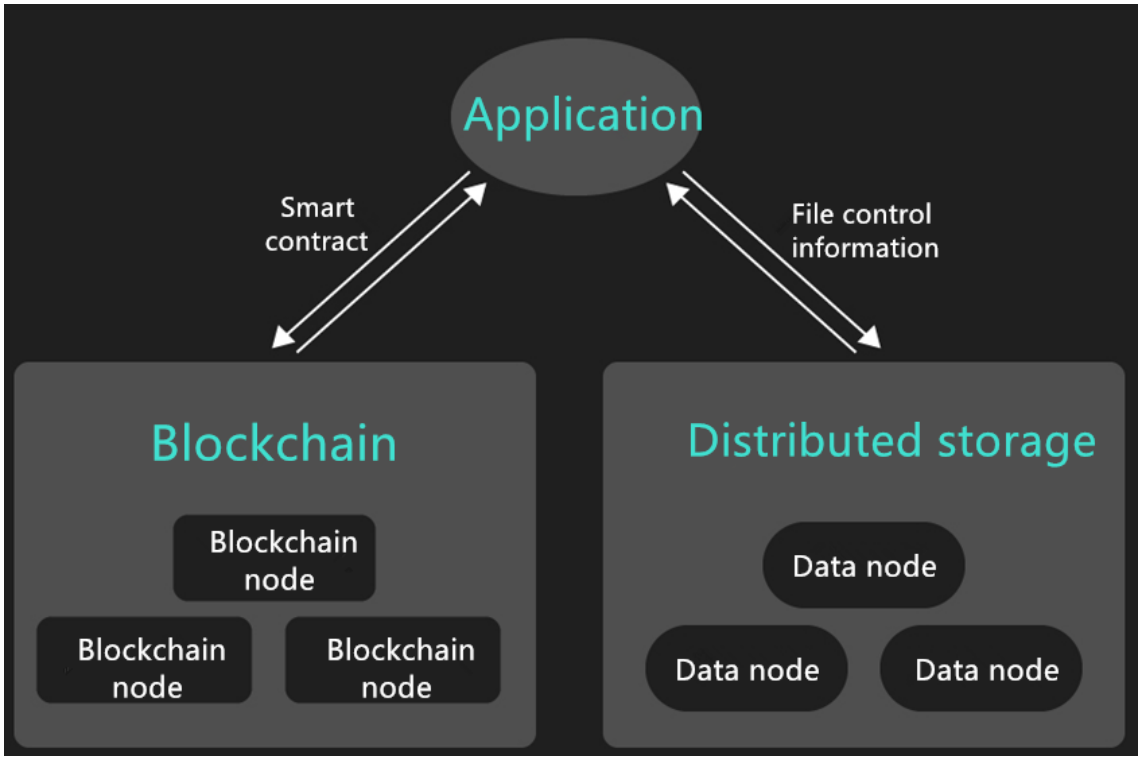
Fourth, we turn our attention to the incentive framework for the protocol. We propose a new incentive mechanism that motivates participants to join our system, which is proved to be roughly a Nash equilibrium. In this way, our design alleviates such attacks as block seizures and private mining. The core idea behind the incentive scheme is to provide a positive return for those who agree with the agreement. In this way, we can prove that under reasonable assumptions, the implementation costs of some agreements are small, and when all the participants are rational, faithfully follow the agreement to strike a balance.

Fifth, we have introduced a share-based delegation mechanism that can be seamlessly added to our blockchain agreement. The commission of shares is particularly useful in our context because we want our agreement to scale up in a cluster of

high-profile fragmented environments. In such cases, the delegation mechanism allows the rights holders to delegate their "voting rights," that is, the rights of the committees participating in the first electoral agreement for each era.

## 4.3 Technical Programs of Ti-Blockchain

### 4.3.1 Overall Architecture




overall technology framework of Ti-Blockchain

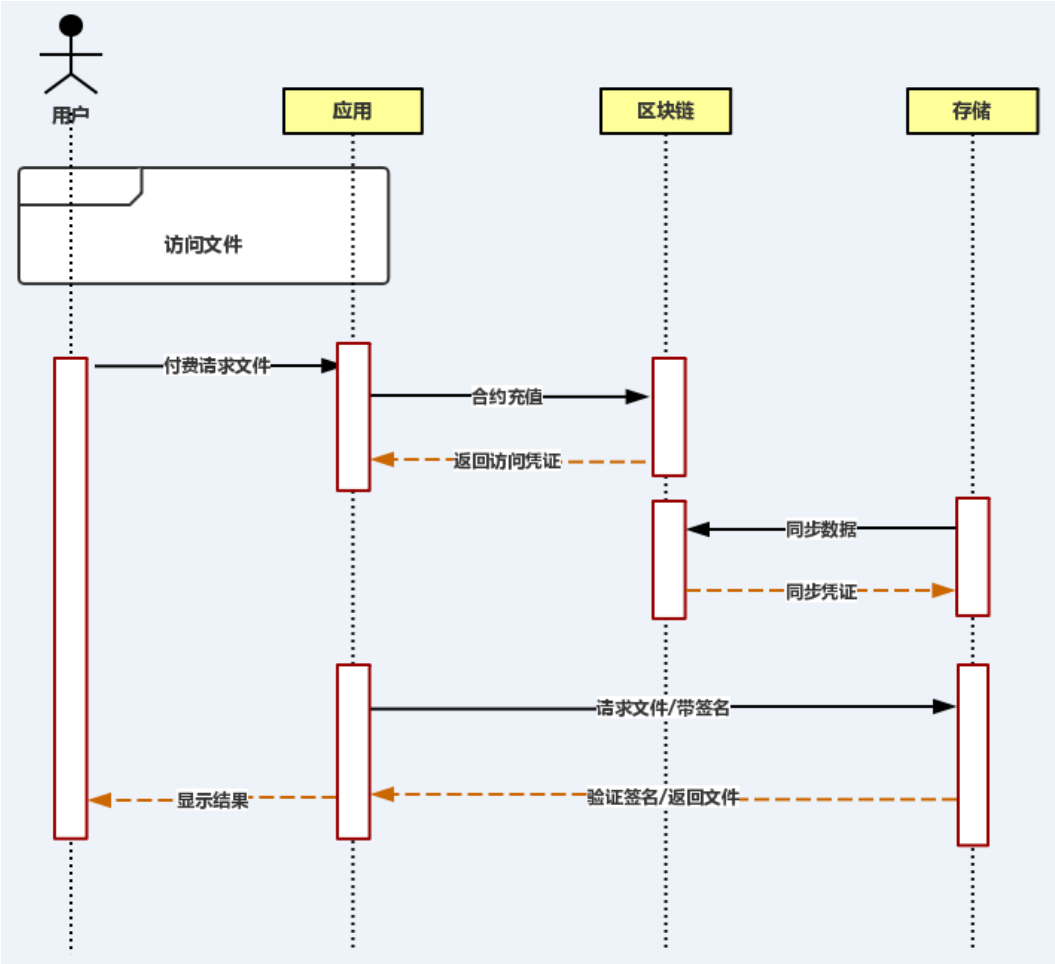
At first there are two separate distributed networks:

① blockchain constitutes a control and business network, is mainly responsible for the maintenance of the book data, including the block, transfer and contract functions.

② distributed storage of each node constitutes a storage network, is mainly responsible for storing the actual data, as well as access control, at the same time block data can be synchronized.

### 4.3.2 The Main Process

There is a simple consensus among distributed storage nodes that blockchain data is received, and permission control is performed based on the data in the chain. Because the data is stored in chunks, even if a small number of nodes do not follow the consensus, they can not access the complete data. All user access to the file requires initiating a request on the blockchain (specifically calling the contract, such as charging the contract). The blockchain then generates access credentials for the user's request and records it in the chain. After the user gets this voucher, he can sign it with his own private key and send a request to the data node with this voucher. The data node can verify this credential by synchronizing the data on the chain, and at the same time, it can verify that the request belongs to the corresponding user through the front. Then the data will be sent to the corresponding user.




the main technical processes of Ti-Blockchain

### 4.3.3 Intelligent Contract

Intelligent contracts are scalability features provided by the chain, but for security reasons, there is no arbitrary registration of the contract. The chain will provide some contract templates for the file upload, download to provide basic management functions. The client must have access to the file through the contract.

After the entire ecosystem is complete, there will be more demand, and more contract templates can be provided on the chain. These functions do not need to change the underlying chain, only need to register a new contract.

**Virtual Machine:** Intelligent contracts on the chain are developed using Turing's complete language. Grammar can be supported through adaptation Lua, C # language. The result of the virtual machine execution is recorded on the chain, eliminating the need for all nodes to run virtual machines, reducing the load on the entire blockchain network.

**Contract:** In systems like Ethereum, contracts can be arbitrarily registered and invoked. This has great benefits for scalability and experimentation. But within our storage system, we support any contract, but we need some permission to register it. To some extent, the type of contract is limited, but it is controlled for the stability of the entire network and the future direction of development. At the same time, its scalability and flexibility have not been affected by the need for new contracts for future growth.

# Chapter 5 Application of Ti-Blockchain

## 5.1 Registration and Transfer of Private Equity

The application of blockchain technology, such as the encryption of equities and bonds and other securitized assets, will help improve the registration and transfer services, in particular the multi-center system of blockchain construction, which will greatly enhance the efficiency of cross-border circulation of assets and reduce the transaction costs. Manage safer, more efficient, credible, less expensive, more compliant. At present, the equity registration needs to be handled manually, the maintenance of the roster of shareholders is complicated and the maintenance and tracking of historical transactions is very difficult. Traditional equity transactions, based on the credit of both parties, require the establishment of bilateral credit transactions before they can be traded. The credit risk is borne by both parties and the trading platform focuses on the credit risk of market participants. The only true digital voucher for registration of securitized assets such as equity bonds; cross-domain, multisignificant trust to facilitate the transfer and trading of securitized assets; and enhanced disclosure records that easily meet regulatory compliance requirements.

Ti-Blockchain can be used in crowdfunding platform, regional equity trading center, the regional financial assets trading center and private equity management platform.

## 5.2 Free Circulation of Assets

Compared with the traditional centralized system, the advantage of using blockchain in the field of digital assets lies in that once the assets are issued on the blockchain, the subsequent circulation can no longer depend on the issuer system. In the circulation, the assets are controlled by the single center As a social communication, any channel with resources may become a catalyst for the circulation of assets. Therefore, the blockchain can greatly enhance the efficiency of the circulation of digital assets and truly achieve "multi-issue and free circulation." Traditional asset services require corresponding intermediaries, such as the proof of the owner of the assets and the notarization of authenticity, which can only be completed by the intervention of a third party. Only through the intervention of the

three parties of the asset issuer, the asset receiver and the circulating platform, can the asset Complete the entire circulation process. In the current tripartite model, there are several pain points:

① After assets enter the circulation, they still have to rely on the system of assets issuer to finish the use and transfer, which limits the circulation of assets to the system users of the issuer;

② The traditional channel for asset circulation is limited and almost all depend on large channels. As the monopoly position of the industry greatly increases the costs, the circulation costs are significantly increased. Small channels and individuals can hardly play a role in circulation.

## 5.3 Cloud Storage of Blockchain

Cloud storage relies on third-party large storage providers to transport and store devices, such as 360 cloud disks and cloud storage disks. However, subject to non-standard client-side encryption systems, they are highly vulnerable to various security threats. Decentralized storage based on the data center can effectively improve this situation and effectively resist censorship, tampering and unauthorized access. The file should be fragmented before the client encrypts, which protects the content of the data, leaving the data owner full control over the encryption keys and thus limiting others' access to the data.

Data owners can separately determine how files are sharded and where fragments are located on the network. Without the prior knowledge of the location of shards, as the network proliferates, the difficulty of finding any given shard increases exponentially. This means that the file's security is proportional to the square of the network size. Fragment size as negotiable contract parameters. The normalized size discourages the sidelines from trying to determine the content of a given slice and can mask the slice flow across the network. Segmentation of large files, such as video content, distributes fragmented nodes to reduce the impact of content delivery on all nodes. All devices in the cloud storage system are completely transparent to the user and any authorized user anywhere can connect to the cloud storage via an access cable for data access to the cloud storage. Through a variety of data backup and disaster recovery technologies and measures can ensure that the data in the cloud storage will not be lost, to ensure cloud storage its own security and stability.

The basic principle of CDN is to widely adopt various cache servers. These

cache servers are distributed to areas or networks where user visits are relatively concentrated. When users visit websites, global load technology is used to point the user's visit to the nearest working cache On the server, the cache server responds directly to the user's request. CDN content distribution system and data encryption technology ensure that the data in the cloud storage will not be accessed by unauthorized users. Meanwhile, various data backup and disaster recovery technologies ensure that the data in the cloud storage will not be lost and the cloud storage itself Safe and stable. Ti-Blockchain is based on a distributed hash table, which can be used to store data location information or other information.

## 5.4 Intelligent Storage

As mentioned earlier, there are many things we can do with intelligent contracts and distributed storage.

The first is basic distributed file storage. Traditional distributed storage either requires a centralized company to provide services or is free to use as a p2p network. The former is a strong control system, once the centralized service for no reason to provide services, then all users will suffer huge losses. The latter is hard to motivate participants to share his storage or files continuously for free. Through intelligent contracts, you can give incentives to store provider / document provider tokens. Whether it's providing storage or sharing files, you get some money to encourage everyone to share (including storage space and data resources).

With basic document storage security, re-use of intelligent contracts, you can achieve complex business logic. For example, users can put their own wills on the chain, pay a contract to pay a certain fee, to ensure that the contract is not open. Once the user does pass away, the contract content can be accessed by anyone because the sponsor can no longer pay for it.

The user can upload some documents that need to be saved to the Ti-Blockchain, and pay the fees on a regular basis to ensure the content is always valid. Remove at any time as evidence when needed.

Users can contract, specify a few documents to share among a small number of users. Or after a certain period of time to share with other users.

Users can post some buy contracts, paid to buy some of the information they need. Those who hold these important information are free to trade. This is also a simple value trading market.

There are other more imagination. The current blockchain is based on a distributed account database, it is difficult to store large amounts of data. Such as some notary business chain, only the source of the hash stored in a relatively small field, the source file can not be restored. The block chain coupled with unlimited storage space, bringing the combined effect is sufficient to greatly enhance the block chain application scenarios, accelerate the application of blockchain in various industries.

# Chapter 6 Team Members

## 6.1 Technical Adviser

**Wei Xu**

A blockchain technology expert and entrepreneur; early participant and preacher in digital currency. Served as a special assistant to the chairman of Digital China, a company listed on the Hong Kong Stock Exchange; THINKYOUNG's founder.

In 2007, Mr. Xu participated in the research and development of the world's first multimedia smart card as the core member of US-funded start-up company.

Mr. Xu joined Shenzhou Digital Group in 2009 and is responsible for the research and development of new digital technologies and models for Digital China. In particular, he devoted himself to exploring the mode of electronic money. Mr. Xu founded the first online shopping mall in the field of electronic money by the end of 2014 to realize the direct exchange of digital money and virtual currency. In 2015, THINKYOUNG was founded.


**Qingchun Shentu**

Bankledger's founder and Bankledger's CEO; deputy Secretary General of FISCO; member of Shenzhen Gold Standard Committee; doctor of Shenzhen University; started research on blockchain in 2013 and published more than 20 technical articles about blockchain.

**Wei Zhao**

OracleChain’s CEO

Starting with Bitcoin in 2011, Mr. Zhao has participated in various blockchain community projects (Peercoin, Factom, BitShares) as the core BitShares community in China to maintain a global 1/23 block-out node. After studying in Singapore for 8 years, he returned to China in 2016 to start his own business. In that year, he won the second place in "Shanghai Wanxiang Deloitte Blockchain Programming Marathon" and the second place in "Mercedes-Benz Technology Marathon".

**Shuaicheng Liu**

Ph.D. Electrical Engineering and Computer Engineering, National University of Singapore. Dr. Liu currently works at the University of Electronic Science and Technology of China. His research interests include computer vision and algorithm theory. He has published numerous research articles in internationally renowned periodicals and conferences.

## 6.2 Technical Team

Huihui Tang

Senior Software Engineer, experienced in software development and project management. Used to be leader for developing products that have millions of users.

**Tiansheng Dong**

Senior C + + development engineer, worked in a number of software and Internet companies, proficient in C / C + +, proficient in multiple languages, with many years of experience in software development and system architecture, good at analyzing and solving various difficult problems under the software complex environment.

**Yangyu Li**

Graduated from Southwest University of Nationalities with computer specialty, former NOKIA senior engineer, has participated in information security, cloud computing and other innovative projects, blockchain technology enthusiast.

**Han Liao**

Telecommunications Senior Software Engineer, once participated in the design and research & development of customer service system, contributors of open source community, blockchain technology enthusiasts.

**Siqi Chen**

Used to be senior algorithmic engineer of a well-known data recovery company in China. In-depth study of encryption decryption data recovery and consensus algorithm. Open source community contributor, block chain technology enthusiast.

**Nicko**

Ph.D. in Information Technology Management in Universitas Surabaya; Indonesian entrepreneur; blockchain enthusiast; chairman of the association PT EMRIC ASIA (Asia Educational Multimedia Information Center).

**Haykel (German)**

Software architect specialist in many Internet giants. Worked as a technology development expert in Germany, Egypt and Tunisia. Has in-depth study on Ethereum, bitcoin and other open source systems software, good at multi-language computer programming and has extensive experience in system design, responsible for the overall technical work of Ti-Blockchain project.

## 6.3 Marketing Team

**Brother. Shangbi**

Doctor of Engineering in Dalian University of Technology; a famous angel investor; a blockchain industry veteran expert, with many years of marketing and management experience.

**Songhao Zhang**

Further studied in Tsinghua University Wudaokou Finance Institute; a post-90 dark horse in business, having 8 years' experience of Internet, 5 years' of digital currency and blockchain.

**Xianglecaizi**

Years of working experience in Bitcoin industry, researched and rooted in the digital currency and blockchain market, with rich industry experience and keen market judgments.

**Jingxi Lei**

In 2013, Mr. Lei was involved in the Bitcoin industry, introduced the concept of technology in the blockchain and preached in universities across the country. He joined the founding of the China Currency Exchange in 2014 and has keen insight into the technical application of blockchain projects. From 2015 to 2017, he served as the assitent president in Fangsiling and has extensive practical experience in project management and team management. He has promoted and preached in more than 20 universities and colleges in more than 10 countries including the United States, Australia, Japan and other countries and promoted the application of blockchain technology.

**Xiangyang Ye**

Served in the domestic top-level domain name service provider New Network, having 8 years experience of internet, a senior digital currency lover.

**Xin Cai**

Years of marketing experience, with strong market perception, able to grasp the market dynamics and its development direction.

**Shuai Zhang**

Master of Arts in Southwest Jiaotong University. Worked in universities, training institutions as Japanese/Chinese teacher, once worked in a Japanese enterprises as Japanese editor.

# References

[1] "Data Structure and Algorithm Analysis": Yan Weimin, Tsinghua University Press, 2011.

[2] "Blockchain: How to redefine the world": Tang Jianwen, Lu Wen, Mechanical Industry Press.

[3] Blockchain Revolution, [Canada] Don Tapscott / [Canada] Alex Tapscott, CITIC Publishing Group, September 2016.

[4] "China-Blockchain Technology and Application Development White Paper 2016"

[5] "Qtum White Paper".

[6] https://en.bitcoin.it/wiki/Category: History

[7] https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.pdf

[8] https://github.com/bitcoinbook/bitcoinbook

[9] https://github.com/ethereum/wiki/wiki/White-Paper

[10] S.Nakamoto, Bitcoin: A p-2-p electronic cash system, https://www.bitcoin.org/bitcoin.pdf/

[11] N. Szabo, Smart contracts, 1994, http://szabo.best.vwh.net/smart.contracts.html

[12] N. Szabo, The idea of smart contracts, 1997, http://szabo.best.vwh.net/idea.html/

[13] Bruce Schneier, Applied Cryptography (digital cash objectives are on pg. 123)

[14] Crypto and Eurocrypt conference proceedings, 1982-1994

[15] David Johnston et al., The General Theory of Decentralized Applications, Dapps, 2015, https://github.com/DavidJohnstonCEO/DecentralizedApplications/

[16] Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, http://ethereum.org/ethereum.html

[17] Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf/