

Ti-Blockchain

16 Aug, 2017

Summary 4

Special Terms and Abbreviations in Cryptology 5

Special Terms 5

Proper Nouns for Digital Currencies 7

Overview of Blockchain 10

1.1 Origin and Development of Blockchain 10

1.1.1 Background 10

1.1.2 Definition 11

1.1.3 Development history 11

1.2 Features and Application of Blockchain 12

1.2.1 Features 12

1.2.2 Application direction 13

1.3 Introduction to Main Applications of Blockchain 15

1.3.1 Ethereum 15

1.3.2 Qtum 16

1.3.3 The DAO 17

1.3.4 Stroj 17

Overview of Ti-Blockchain 20

2.1 Background of Ti-Blockchain’s Coming into Being 20

2.2 Development Vision of Ti-Blockchain 21

Ti-Blockchain Technology 24

3.1 Technical Features of Ti-Blockchain 24

3.1.1 Data storage 24

3.1.2 Consensus mechanism 25

3.1.3 Multi-signature 25

3.1.4 Contract and virtual machine 26

3.2 Safety of Ti-Blockchain 26

DPOS model 27

3.3 Technical Scheme of Ti-Blockchain 29

3.3.1 Overall architecture 29

3.3.2 Main process 30

3.3.3 Smart contract 31

Application of Ti-Blockchain 33

4.1 Transfer of Private Equity Registration 33

4.2 Free Circulation of Assets 33

4.3 Blockchain Cloud Storage 34

4.4 Smart Storage 36

Team Members 38

5.1 Technical Advisers 38

5.2 Technical Team 40

5.3 Marketing Team 43

References 46

# Summary

Ti-Blockchain is devoted to developing the public chain ecology beyond the existing blockchain and solving the existing financial problems and a lot of idle network storage problems, in combination with the advantages of Ethereum ecology and storj.

Although the charm of blockchain is everywhere, actually not all transactions, smart contracts, credit collection, business and other systems can be completely replaced with today’s so-called distributed new technology, for such replacement is completely unrealistic. No boss of a financial institution would make such a decision. Therefore, we plan to call the so-called distributed technology as services, i.e. gradually adding distributed functionalities and properties in existing systems, which is feasible in existing systems.

Decentralization can significantly mitigate the risk and loss of data interruption and increase security and confidentiality. Cloud storage relies on third-party large storage providers to transmit and store data, such as 360 Cloud Disk and Baidu Cloud Disk. However, the data thus stored are very vulnerable to all kinds of security threats due to a centralized architecture. Redundant and decentralized distributed storage can effectively improve such condition and resist tampering and unauthorized access. Files can be encrypted before transferring to a server, which can protect the contents of data. The data owner completely controls the encryption key to limit others’ access to the data.

This article mainly introduces the product architecture, technical features and advantages, industrial application cases and other aspects of Ti-Blockchain. The core value of blockchain lies in the construction of the reliable distributed multi-center system. Blockchain has the potential to be the infrastructure for building value Internet. Ti-Blockchain Company is devoted to creating enterprise-level blockchain products and providing industry solutions and has developed highly expandable blockchain finance and enterprise service platform with high performance for enterprise-level product operation capacity. Ti-Blockchain has obtained multiple technological breakthroughs and innovations and formed a series of technical features and advantages in performance, expansibility, safety, operation, maintenance and other aspects. On the basis of the joint exploration of the application scenarios of blockchain with industrial partners, Ti-Blockchain has been applied to such fields as digital assets, trade finance, equity bonds, public notarization and data security. With multi-centralized trust as the core, Ti-Blockchain creates ABS + cloud storage network to make enterprise information & data more reliable.

# Special Terms and Abbreviations in Cryptology

## Special Terms

**Key**: Keys are divided into encryption key and decryption key.

**Plaintext**: the unencrypted information that can directly represent the original meaning.

**Ciphertext**: the encrypted information that hides the original meaning.

**Encryption**: the process which converts plaintext into ciphertext.

**Decryption**: the process which coverts ciphertext into plaintext.

**Cryptographic algorithm**: the encryption and decryption methods applied by the cryptosystem: with the development of ciphergraph based on mathematics, encryption methods are generally called “encryption algorithm” and decryption methods “decryption algorithm”.

**Model of cryptographic communication system**

For given plaintext m and key k, encryption transformation Ek changes plaintext into ciphertext c = f (m, k) = Ek (m). On the receiving end, decryption key (sometimes k = k) is used for decryption to restore the ciphertext c to the original plaintext m = Dk, (c). A safe cryptosystem should meet the following requirements: ① It is difficult for illegal interceptor to infer the plaintext m from the ciphertext C; ② The encryption and decryption algorithms should be quite simple and suitable for all key spaces; ③The encryption strength of cipher only relies on keys; ④ Legitimate receiver can inspect and verify the integrity and authenticity of the message; ⑤ The sender of the message cannot deny the message sent, nor forge others’ legitimate messages; ⑥ It may be arbitrated by an arbitration institution if necessary.

**Hash algorithm**

Hash algorithm maps a binary value with an arbitrary length into a shorter binary value with a fixed length. The smaller binary value is called hash value. Hash value is the unique compact numerical representation of a piece of data. If hashing a piece of plaintext even with only one letter of the paragraph changed, the subsequent hash will generate a different value. It is computationally impossible to find two different inputs hashed as the same value, thus the hash value of data can check the integrity of data. It is generally used in quick search and encryption algorithm.

Hash table maps a set of key words into a limited address range according to the hash function H (key) set and the conflict-handling approach, with the image of such key words in the address range as the storage location for recording in the table. Such table is called hash table or hash and the corresponding storage location is called hash address. Compared with the queue as a linear data structure, hash table definitely realizes a faster search.

The fixed results from applying a one-way mathematical function (sometimes called “hash algorithm”) to any number of data; Hash changes with the data input. Hash can be used in many operations, including authentication and digital signatures, also called “message digest”.

Put it in a simple way, hash algorithm is a hash function. It is a one-way cryptosystem, i.e. an irreversible mapping from plaintext to ciphertext, with only encryption process, no decryption process. Meanwhile, a hash function can obtain an output with a fixed length by changing the input with arbitrary length. This one-way feature and the feature of the fixed length of output data of hash function enables it to generate message or data.

Hash table is a data structure with direct access according to the key value. That is, it has access to records by mapping key value into a location in the table to accelerate the search. This mapping function is called hash function and the array where records are held is called hash table.

For given table M, there is a function f (key). For any given key value “key”, if the address of the record containing the keyword in the table can be obtained by substituting into the function, table M is called hash table and the function f (key) hash function.

## Proper Nouns for Digital Currencies

**Bitcoin**: a special encrypted digital currency launched by pseudonym developer Satoshi Nakamoto in the form of open source software in 2009.

**Ethereum**: a public blockchain platform with smart contract function.

**Value transfer protocol**: applied to Internet-based value transfer.

**Internet of Things:** the network with which the Internet, traditional telecommunication network and other information carrier can all be interconnected, linking such ordinary objects capable of performing an independent function as physical equipment, cars and buildings.

**Smart contract**: a program which is driven by time, has a state, runs on a duplicated and shared ledger and can keep the assets on the ledger.

**Public chain**: the blockchain where everyone can send transactions and such transactions can be effectively confirmed and everyone can participate in the consensus process.

**Ethereum virtual machine**: a virtual machine designed to run on all participant nodes in point-to-point network. It can read and write the executable codes and data in a blockchain, verify digital signature and can run the codes in a perfect semi-Turing way. It only executes codes when receives the message verified by digital signature; and the information stored on the blockchain will distinguish appropriate behaviors.

**Incentive proof of stake consensus**: incentive measures added to proof of stake consensus. It estimates the online nodes and stimulate nodes to remain online to maintain the stability and safety of the network.

**Hard division**: the permanent division of the blockchain: after the release of new formula rules, some unupgraded nodes cannot verify the blocks generated by upgraded nodes. In such case, hard division occurs.

**Turing-complete**: a calculating system capable of calculating the functions that can be calculated by each Turing. If a language is Turing-complete, the computing power of this language is equivalent to a universal Turing machine. This is the highest capacity a modern computer language can possess.

**Oracle**: to screen the input data according to the preset judgement conditions to select the most appropriate data as input data.

**Data feeds**: data feeds provide data source under the data link for the blockchain.

**POS**: proof of stake consensus mechanism. The mining difficulty is reduced proportionately according to the token holding proportion and time of each node, thus it speeds up the search for random numbers.

**UTXO**: unspent transaction output. The transaction model used in Bitcoin network.

**POW**: proof of work (POW) consensus mechanism. A party (often called reference) submits the computing results which are known to be difficult to calculate but easy to verify, while anyone else can firmly believe, by verifying the results, that the reference has completed a lot of computation to obtain the results.

**DAO**: distributed autonomous organizations. The organization structure that can run independently without intervention and management via a series of fair and open rules.

# Overview of Blockchain

As the core revolutionary force in financial technology, with the organic combination with such fields as the Internet of things, insurance, automobile, manufacturing, medical, energy and shipping and such new technologies as cloud computing, big data, artificial intelligence and mobile Internet, blockchain provides kinetic energy for a new round of technological and industrial innovation.

## 1.1 Origin and Development of Blockchain

Blockchain technology aroused people’s thinking of abandoning inefficient old systems and opening up new ideas that overturn multi-industry operation and trade. As a distributed ledger, blockchain can play a great potential in many fields, especially in financial industry. Since the data stored in blockchain cannot be tampered, we believe that blockchain technology can bring the authenticity and security of data to a new level.

### 1.1.1 Background

A so far unidentified person named Satoshi Nakamoto published a paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System* in the Bitcoin forum at the end of 2008. The concept of blockchain was first proposed in this paper. As the basic technology for building Bitcoin network and the encrypted transmission of exchange information, blockchain can support the mining and transaction of Bitcoin.

Satoshi Nakamoto held that the problem of distrust between merchant and customer cannot be overcome if processing transaction data by centralized means (third party organizations). Moreover, the transaction cost is high and the transaction scale will be limited. In order to solve such problems, Satoshi Nakamoto created blockchain and invented Bitcoin on this basis.

### 1.1.2 Definition

The nature of blockchain is a shared and open database with co-participating records. In the absence of a central server, blockchain allows the link to the computer and other equipment to apply “consensus mechanism” intercommunication. All networking (point-to-point network) equipment will keep data consistent and updated. Due to such mode, blockchain is also called “distributed ledger”. Distribution means decentralization. The ledger is the carrier for recording data. Therefore, blockchain can be interpreted as “decentralized data ecosystem”.

### 1.1.3 Development history

Satoshi Nakamoto published a paper about Bitcoin in 2008. Bitcoin virtual currency platform was established in 2009. The Bitcoin system has run steadily for nearly nine years and could automatically realize the issuance, circulation, trading and payment of Bitcoin. As the first application of blockchain technology, the achievements of Bitcoin are obvious to all.

As a basic support technology, the concept of blockchain was gradually independent from virtual currencies in 2015. It was converted to smart contract programmable platform, via which different kinds of assets and contracts can be registered, confirmed and transfered. The concept of digital assets issuance and circulation platform was thus formed.

Therefore, Bitcoin can be called “blockchain 1.0”, i.e. programmable virtual currency. Ethereum open source project can be deemed as “blockchain 2.0”, i.e. smart contract platform. Blockchain 3.0 is still in envisioning phase. It is beyond economic field and can realize the automatic distribution of material assets and human resources and can promote the large-scale collaboration in such field as government, health, science, culture and art.

## 1.2 Features and Application of Blockchain

Blockchain technology is mainly featured with decentralization, openness, autonomy, information untampering and anonymity, thus it has extensive application and development space in transfer and payment, pan-financial business and credit field and can be applied in combination with cloud computing, Internet of things, big data and other innovative technologies.

### 1.2.1 Features

**Decentralization**

Third party (central) organization assisted in the confirmation and settlement of funds in traditional online transaction payments between merchant and customer. When blockchain technology is applied and under the action of distributed network consensus mechanism, the transaction data can get “automatic” discrimination and verification, thus there will be no need of third party participation any longer.

**Openness**

In addition to the encipherment protection of the private information of the parties of the transaction, the data in blockchain can achieve openness throughout the network. All networking equipment can check relevant information at any time.

**Autonomy**

Based on the establishment of consensus mechanism and other network rules, all equipment in blockchain network can record, update and exchange data in an automatic and safe manner without intervention by any organization or individual.

**Information untampering**

Once verified data are entered to the blockchain, such data will be stored permanently. Unless more than 51% of the equipment data in the blockchain network are simultaneously changed (almost impossible), such data cannot be locally tampered.

**Anonymity**

The nodes in blockchain network can conduct data exchange in the case of mutual non-disclosure. That is, the two sides of transaction can complete payment, transfer and other transactions without knowing each other’s information.

### 1.2.2 Application direction

**Transfer and payment**

Currently, this is the maturest application of blockchain technology. Blockchain technology can avoid the multifarious system, save interbank reconciliation and review process, accelerate the settlement of funds and greatly reduce transaction fees.

**Pan-financial business**

Blockchain technology can be applied in such fields as asset transaction and quick audit. When users reach a transaction intention and the transaction information is added to the blockchain, the transaction is completed. Multi-party data verification by registration and settlement institutions is not required, which not only improves the efficiency, but also is convenient to future audits.

**Credit field**

The features of blockchain technology can solve the problem of trust in financial activities at a low cost. Trust is the foundation of financial activities, the supervision of which, including product registration, information disclosure, funds trusteeship and credit system construction, is to solve this problem. Under the background of active construction of credit system in the whole society, the gradual maturity of blockchain provides perfect conditions for creating a financial environment of mutual trust.

**Combination with innovative technologies**

Blockchain technology can also combine with cloud computing, Internet of things, big data and other innovative technologies. Its application prospect is very extensive.

Compared with traditional technologies, blockchain can help the financial industry to effectively improve efficiency and lower cost and risk. Since third-party participation is not required, the intermediate cost is effectively lowered. With the improvement of operational automation level, the settlement speed has been faster and human costs have been greatly reduced. Meanwhile, blockchain can simplify service process by means of multi-signature and other techniques and improve work efficiency, while the information recorded cannot be tampered and can be traced back, which provides convenience for supervision, audit and other work.

In addition, since transaction confirmation, clearing and settlement are completed synchronously, the possible risks are greatly reduced. Digital transaction process can also effectively avoid manual input error and other problems. Meanwhile, since blockchain has such features as distributed network and consensus mechanism, hacker cyberattack, server downtime and other system problems can be effectively avoided. In the future, in the energy industry, including residential electricity consumption and payment of electric charge can also be automatically executed by smart contract. Carbon trading market can also adopt blockchain technology to improve transparency and fairness to avoid repetitive computation and other problems. In addition, this technology can also be applied to land right confirmation and transfer transactions.

## 1.3 Introduction to Main Applications of Blockchain

Blockchain is a technology system which is maintained by multi-parties, applying cryptology to ensure transmission and access security, thus it can achieve the consistent storage of data and cannot be tampered or denied. Blockchain can pursue the consistency and correctness of the system and solve the most fundamental problem of trust in human society from the mechanism level.

### 1.3.1 Ethereum

The core idea of Ethereum is a blockchain of the computational programming language for built-in Turing machine. The creation of any application is allowed. Ethereum is different from original Bitcoin technology: first, Ethereum realized the smart contract based on Solidity language and regarded smart contract as a special account to make it possible to realize specific methods on smart contract; second, Ethereum realized the EVM (Ethereum virtual machine) which can be implemented by smart contract and change such js code as Solidity into the cipher codes that can be executed on blockchain.

Different from Bitcoin technology, the Transaction in Ethereum requires gas. The gas for a contract or a transaction is fixed (dependent on code size and complexity), while the price of gas is determined by the oracle in Ethereum.

In addition, Ethereum has built complete and open source ecosystem, which has Geth at the bottom, Solidity for programming, contract online browser, Browser-solidity, contract wallet Mist/wallet, the front-end development framework for Ethereum Truffle, various open source DAPP, etc. These elements make it easy to get started quickly and develop blockchain applications suitable for implementing.

Disadvantage: The fact is that the cost of the current GAS design of Ethereum is too high for small transactions and that the acknowledging time of about 12s is also too long.

### 1.3.2 Qtum

This is a third blockchain ecosystem other than Bitcoin and Ethereum developed by Qtum open source community to extend the application boundaries and technical boundaries of blockchain technology.

In Qtum system, information can realize point-to-point value transfer via Value Transfer Protocol and establish an application development platform (DAPP Platform) which supports decentralization.

Qtum has made a series of innovations in blockchain technology and idea: including the privacy protection smart contract model based on UTXO, the consensus mechanism for public chain and union chain, the separation of transaction ledger and smart contract ledger, which are convenient for entry of external supervision and other data source into the design and realization of Oracle and Data Feed of the main contract.

Qtum established its consensus by modifying proof-of-state and other underlying algorithm and applying the POS with incentive mechanism.

### 1.3.3 The DAO

The DAO is decentralized autonomous VC developed on the basis of Ethereum blockchain platform. Each participant of crowd funding obtains corresponding DAO token according to the amount invested (Bitcoin) and has the right to review the project and vote. The voting weight is relevant to the amount of contribution.

In traditional VC funds, the investment strategy is developed by experienced fund managers and other professionals, while The DAO is based on the collective intelligence of the participant of The DAO crowd funding project.

Relation between Ethereum and The DAO: Ethereum can be regarded as a global computer, while The DAO is a DAPP (decentralized application) established on Ethereum platform; or Ethereum is the platform layer, while The DAO is application layer.

### 1.3.4 Stroj

Storj laboratory can let software developers apply push and pull data to their own application software on a distributed network platform. Such data are generally stored in a community formed by “farmers”, who can rent their free disk space to distributed network system users.

As the compensation for renting free disk, “farmers” can obtain a kind of network currency called Storjcoin. Storj laboratory originates from the open source project Storj project, which has a large community formed by software developer. The community aims to create a most efficient distributed cloud storage platform with blockchain service as the background.

Storj can create a decentralized market with blockchain technology and free disk space and conduct transactions with built-in digital currency SJCX. Storjcoin X (SJCX) is a token in Storj network system. It allows users to use in an APP named “DirveShare” and rent or purchase storage space like MetaDisk via SJCX.

SJCX has issued the first version of the graphical interface on November 28, 2015. This version allows ordinary computer users to use it to test software system before the issuance of the final version. Since Storj objects are untrusted individuals in distributed network, “farmers” should not rely on safety precautions to ensure data security as traditional cloud storage companies.

Indeed, farmers can close nodes at any time. Therefore, Storj strongly advises data owners to implement redundant schemes to ensure the security of their archives. Since protocols only deal with personal contract, this shows that cheating client attack is a big problem to be solved by any system which cares about reputation. Hostage-byte attack is a specific storage attack. Malicious farmers refuse to transfer fragment or a part of fragment to charge additional charges for the payments of data owners.

Data owners should protect themselves to realize hostage-byte attack by redundantly storing fragment via multiple nodes. As long the client maintains a secret of its erasure coding, malicious farmers cannot know the last byte. Redundant storage is not the complete solution to such attack, but most of the actual applications of such attack. To beat redundant storage requires linking and spanning multiple malicious nodes, this is difficult to execute in practice.

There certainly are other blockchain platforms. Hypherledger alliance already has such project code open sources as Fabric, Elements and SawTooth Lake. Fabric is more suitable for financial industry. Privacy protection, consensus algorithms, identity authentication and modular design are very flexible. Nevertheless, Fabric is in rapid development and code changes very quickly, for example: the application developed in last month cannot be used next month.

Besides, the stability and performance of Fabric itself is not enough. R3 organization announced the source code of blockchain Corda on November 30, 2016. Corda is written in a niche language. The development is in early stage. Its design idea is distributed ledger, not blockchain, and is suitable for interbank international payment and clearing settlement, such as Bitshares, Openchain and Chain, all of which have applicability and desirability.

Numerous blockchain underlying technology platforms make financial institutions have to learn one by one and understand the technology so as to adopt certain blockchain in combination with application scenarios. In view of the numerous standards and structure of Central Bank, Ministry of Industry and Information Technology of the People's Republic of China, China Financial Standardization Technical Committee, some industries, such as financial industry, may change the platform, thus the time cost and manpower cost are high.

# Overview of Ti-Blockchain

Satoshi Nakamoto publicized the white paper of Bitcoin (*Bitcoin: A Peer to Peer Electronic Cash System*) and proposed some features of Bitcoin network for the first time on October 31, 2008:

1. Double-spending is prevented with a peer-to-peer network.

2. No mint or other trusted parties.

3. Participates can be anonymous.

4. New coins are made from Hashcash style Proof-of-work.

5. The proof-of-work for new coin generation also powers the network to prevent double-spending.

The founding blocks of Bitcoin were dug out and the first Bitcoin transfer transaction occurred in the 170th block on January 3, 2009. Since then, the Bitcoin network has been developing as a point-to-point value exchange network. Although there were a variety of crises, Bitcoin network has changed from an unvalued network to a point-to-point payment network with a value exceeding USD 100 billion.

## 2.1 Background of Ti-Blockchain’s Coming into Being

The appearance of point-to-point value transmission network was historically inevitable, and Satoshi Nakamoto was the person who had sped up this historical process. Since 1980s, the development of TCP/IP protocol and the application of web browser and server in 1990s until today, Internet technology have changed the mode of data exchange and human’s life in different ways and dimensions. The development of Internet technology benefited from infrastructure improvements from the popularization of early information super highway to various intelligent terminals. All these also formed the foundation for the infinite expansion of application layer in Internet OSI seven layer model.

In various protocol stacks of Internet, such protocols for network layer, transport layer and application layer as TCP/IP, HTTP, HTTPS, FTP, TELNET, SSH, SMTP and POP3 are widely used. With these protocols, we have established various Internet services in a perfect manner. However, if we think about it, we’ll find out that we could not realize point-to-point value transfer and transmission on Internet without a third party before the appearance of Bitcoin network. Actually, we do not lack a specific method, but the Value Super Highway of Information Super Highway and how to realize the value transmission (VTP protocol) of Value Super Highway, and Bitcoin network was the first VTP protocol running on Information Super Highway.

With the development of interconnectivity technologies (Internet, Internet of things, VR/AR), the interactive mode between human beings and object and human beings and information has been more diversified. More entities have been digitalized, tokenized or symbolized. Once entities are digitalized or tokenized, the mapping and sharding of real assets on Internet have been completed. The problem immediately faced with is that how to transmit such assets and value in a point-to-point value. Therefore, it can be speculated that with the further deepening of Internet service, the physical and virtual boundaries will begin to blur and the demand of point-to-point value transfer will be highlighted, thus the Value Super Highway and Value Transfer Protocol on Internet will inevitably appear. Bitcoin network has accelerated this historic process.

## 2.2 Development Vision of Ti-Blockchain

Ti Blockchain will build a trusted business ecosystem for investors, companies and regulators. The investor can review the financial documents such as balance sheet, income statements, cash flow analysis etc. posted on the Ti Blockchain. Companies can leverage the Ti Blockchain to post documents such as white paper, budget, and milestones of code development, coin distributions, governance structure and financial statements, for interested investors to review. In future version of Ti Blockchain, the documents will be checked and reviewed by a smart contract program for compliance.

In addition to provide on chain storage for immutable documents to protect investors, Ti Blockchain can also provide the decentralized storage space for consumers and for business users as well.

For individual consumers, Ti Blockchain can be used as a digital safe; the consumer can upload the document encrypted on the blockchain. No one else can decrypt the document except for the person who uploaded the document to the blockchain. Technically, this is easy to implement leveraging public and private key pairs. The user encrypts the document using public key. Due to asymmetric property of the public/private key pairs, only the person who holds the private key can decrypt the document. As such, no one else, including Ti Blockchain can decrypt the document.

For business users, Ti Blockchain can be used as collaborative space for user to work together on a single document. The access control smart contract can be deployed to allow only users who have the actual privileges to see the documents.

Ti Blockchain also supports Asset Backed Securitization (ABS). As a financial innovation, asset securitization has developed rapidly both at home and abroad in recent years and has been one of the hot search words in capital markets at home and abroad. Asset securitization is a financing form issuing negotiable securities with specific portfolio or specific cash flow as supports. Generally speaking, asset securitization refers to a financing form which sells the illiquid assets with stable income (or expected revenue) by issuing securities in capital markets to obtain development fund. Asset securitization is very commonly applied in some countries. At present, more than half of home mortgage and three quarters of car loan in America are provided by issuing asset securities. The greatest strength of asset securitization is as follows: for issuer, it not only lowered the financing threshold, but also provided asset liquidity; for investor, it can breakthrough investment restrictions, reduce risks and increase revenue.

Ti-Blockchain has Turing-complete smart contract, to automatically manage the assets on the chain via smart contract and flexibly expand business function. Smart contract can play a greater role in combination with the distributed storage service provided by Ti-Blockchain. For example:

1. To realize paid file storage and sharing via contract.

2. To realize the transmission of confidential documents within limited scope.

3. To realize the notarization of contracts and documents via contract.

4. To realize the management of such time-efficient documents as wills via contract.

# Ti-Blockchain Technology

## 3.1 Technical Features of Ti-Blockchain

### 3.1.1 Data storage

Ti-Blockchain will provide a token of DPOS mode to support its operation. It will provide smart contract + multi-scenario application + online cloud storage function. Also, it will provide storage space on the basis of smart contract and save the company’s such basic information as business license, tax, personnel and monthly financial statements in the process of company operation.

The files or data can be stored using small fragments using sharding technology; data owners can separately determine how to fragment files and the location of such fragments in the network. If the location of fragments is not learnt about in advance, with the spread of the network, the difficulty in finding any given fragment shows exponential growth. This means that the safety of the document is in proportion to the square of network size. Fragment size is a negotiable contract parameter. Normalized size discourage side line tries to determine the contents of fragment and can block the fragment flow passing through the network. Splitting large files, such as videos, and distributing fragment nodes can reduce the impact of content transfer on any node. All equipment in cloud storage system is completely transparent for users. Any authorized user in anyplace can have data access to cloud storage by connecting with cloud storage via an access cable. The data will not be lost by various data backup and disaster recovery technology and measures to ensure the safety and stability of cloud storage itself. Ti-Blockchain is established in a distributed hash table, which can be used to store data location information or other information.

### 3.1.2 Consensus mechanism

Ti-Blockchain decides to apply DPOS consensus mechanism. POW algorithm has high requirements for calculation capacity. Driven by interests, the calculation capacity will finally concentrate on a small amount of mine pool, thus decentralization cannot be realized. However, DPOS can provide quick consensus way without consuming large amounts of computational resources. Selection of agent block by vote ensures that the network will not be controlled by the minority (when tokens are greatly distributed in later period). This is quite similar to the electoral mechanism in reality and is fairer. As long as the agent can provide sufficient stability, people will certainly select him.

### 3.1.3 Multi-signature

Multi-signature is a way to manage an account by multiple holders of private key.

Different from traditional encrypted currency, which mainly uses clear signature to verify transaction, multi-signature applies multiple private key signatures to operate a certain account. Multi-signature manages account in the way of n/m(m >= n > 0). For the m private keys of the account created, only n private key signatures are required to realize transfer and other operations of the account. This can be applied in many scenarios. For example:

1. To avoid the unavailability of the account due to lost private keys of single user;

2. To jointly manage the assets of company and other organization collectives to avoid unauthorized use by individuals or the minority;

3. To be applied to vote/selection and other scenarios.

### 3.1.4 Contract and virtual machine

Contract language: we use class java language as the default programming language used by the smart contract on Ti-Blockchain. This language supports static compilation to bytecode and executes such bytecode in blockchain network as required.

Java is a Turing-complete programming language, compilers and bytecode virtual machines are specifically designed and optimized for blockchain.

Contract interpreter: Contract interpreter is the interpreter of the bytecode of Java. In case of the operation of smart contract or block concurrent validation in blockchain network, blockchain nodes will take contract bytecode from blockchain, load bytecode with Java bytecode interpreter and use appropriate parameter to call the required API. The operating results obtained and context changes will be used by blockchain.

An operation of smart contract may call different times at different nodes and times, but the results called by each operation at each time at different nodes and times are the same for the changes in context state.

The operation of smart contract needs to deduct certain executive cost for requiring computer resources at different nodes to executive and occupies blockchain capacity and network low.

## 3.2 Safety of Ti-Blockchain

The basic problem of establishing blockchain protocol on POS is the simulation of the first election process. In order to realize the random election among right holders, entropy must be introduced into the system. The introduction mechanism may be manipulated by an opponent. For example, independent of the solution, the opponent controlling a group of right holders can select to simulate protocol implementation and try different right holder sequence to find out the favorable chain extension for first election. In order to avoid such operation, honest right holders must be able to add enough entropy and resist any prospective operation executed by opponent.

### DPOS model

Safety is the main focus of the design of Ti-Blockchain. Ti-Blockchain uses the so-called “DPOS blockchain protocol which can be proved safe”. The algorithm has the following five features to make it a very safe DPOS model.

First, the model focuses on persistence and activity, which is two formal attributes of a healthy transaction ledger. Persistence refers to the fact that once a certain node of the system declares a transaction as “stable”, other nodes (if queried and answered truthfully) will also reported to be stable. In such case, stability will be understood as a predicate and will be parameterized by some safety parameters k, and will influence the certainty of property holding. (for example, “deeper than k blocks”.) Activity ensures that once an actually generated transaction is provided to network nodes with sufficient time, such as u time step, it will be stabilized. The combination of activity and persistence ensures a healthy transaction ledger, the significance of which is the application of actually generated transaction and making it constant.

Second, we described a new blockchain protocol based on DPOS. Our protocol assumes that the participant is free to create accounts, receive and make payments and such rights change with time. We use a very simple and safe voting protocol implemented by multi-party to realize the randomness in first election process. This can prevent the so-called abrasive attack and distinguish our method from the former other solutions (former solution defines this value on the basis of current blockchain or introduces entropy by collectively throwing coins [4]). In addition, our method is unique in that the system has ignored one round after another right modification. Instead, the current group of right holders is regularly recorded and is called era; in each such interval, a safe multi-party calculation will occur by using the blockchain itself as a broadcasting channel. Specifically, in each era, a group of randomly selected right holders form a committee, which will be liable for executing the coin tossing agreement. The results of this agreement decide the next set of right holders to execute the agreement in the next era and the results of all the first elections in that era.

Third, we provided a set of formal argument to prove that is no opponent can break persistence and activity. Our protocol is safe according to some reasonable assumptions:

(1) The network is highly synchronized;

(2) Most of the right holders selected can participate each era as required;

(3) Rights will not be offline all the time within a long time;

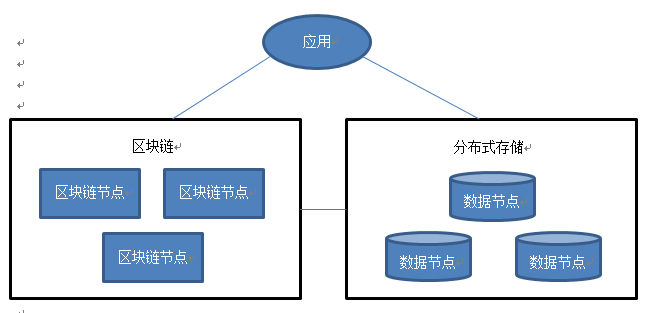
(4) The damage of adaptivity is subject to a small delay and the safety parameters are linear, or participant can have access to the anonymous radio channel of a sender.

Fourth, we transferred our attention to the incentive structure of the protocol. We proposed a new reward mechanism to stimulate participants to join in the system proved by us to be a Nash equilibrium system. In this way, our design reduced such attacks as block detention and unauthorized mining. The core idea behind the reward mechanism is to provide active return to the participants with behaviors in line with the protocol behaviors. We can prove in this way that under reasonable assumption, the execution cost of some protocols is low and that the faithful compliance with the protocol reaches a balance when all participant are rational.

Fifth, we introduced a share entrustment mechanism which can be added to our blockchain protocol seamlessly. Share entrustment is particularly useful in our context for we hope that our protocol can be scaled up in the environment with highly dispersed right holders. In such case, the entrustment mechanism can let right holders to delegate their “voting power”, i.e. the right to participate in the committee of the first election agreement in each era.

## 3.3 Technical Scheme of Ti-Blockchain

### 3.3.1 Overall architecture



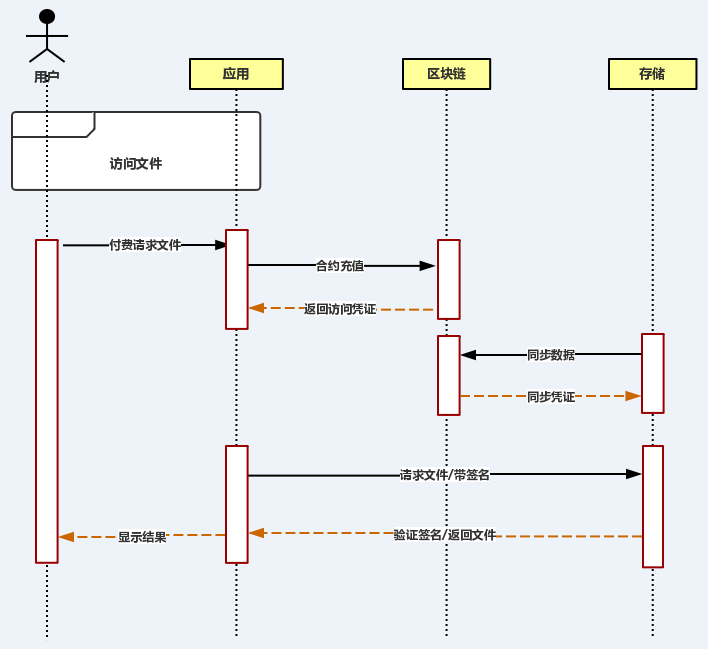
First, there should be two independent distributed networks:

1. The blockchain constitute a control and business network, which is mainly responsible for the maintenance of accounting data, including blocking out, transfer and contract function.

2. The nodes of distributed storage form a storage network, which is mainly responsible for storing actual data, right control and synchronization of block data.

### 3.3.2 Main process

There is simple consensus among the nodes of distributed storage, i.e. receiving blockchain data and execute right control according to the data on the blockchain. Since the data are stored by blocks, even a few nodes do not follow the consensus, the complete data cannot be accessed. User should issue a request on the blockchain for any access to documents (specifically call contract, such as charging the contract). Then the blockchain will generate access credentials for users’ request and record on the blockchain. When users get such credentials, they can sign with their own private keys and issue a request for data node with such credentials. Data node can verify such credentials via the data on the blockchain and verify that this request belongs to corresponding users. The data will be send to the corresponding user.



### 3.3.3 Smart contract

Smart contract is an extensibility features provided by the blockchain. However, for safety reasons, contract will not be registered arbitrarily. Some contract templates will be provided on the blockchain to provide basic management functions for uploading and downloading documents. Clients may have access to documents via contract.

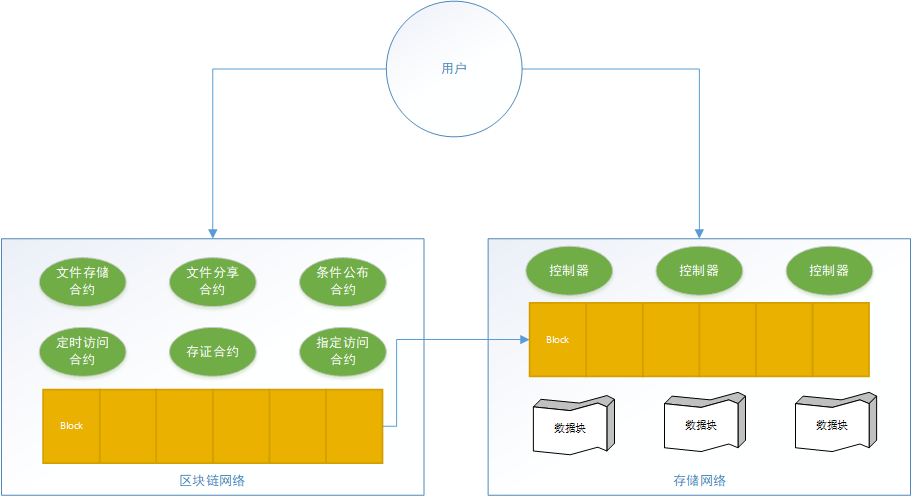
There will be more needs after the improvement of the whole ecology and more contract templates can be provided on the blockchain. Such functions do not require the modification of bottom chain, only require the registration of new contract.

**Virtual machine**

The smart contracts on the chain are developed in Turing-complete language. The grammar may support Lua, C# and other language through adaptation. The results of the execution by the virtual machine are recorded on the chain. Not all nodes are required to operate the virtual machine, reducing the load of the whole blockchain network.

**Contract**

In systems similar to Ethereum, contracts can be registered and called arbitrarily. This is greatly favorable for expansibility and test. However, in our storage system, we support any contract, but the registration on cochain requires certain rights. The category of contracts is limited to a certain extent and is controlled for the stability of the whole network and the development direction in the future. Meanwhile, for contracts to be added for future development, its scalability and flexibility are not influenced at all.



# Application of Ti-Blockchain

## 4.1 Transfer of Private Equity Registration

The application of such securitized assets as encrypted stake and bonds of blockchain technology helps to perfect registration and circulation service, especially the multi-center system established on the blockchain, which can significantly improve the efficiency of cross-domain circulation of assets, lower transaction costs and make the management safer, more efficient, reliable, inexpensive and compliant. Currently, equity registration requires manual handling; the maintenance of the register of shareholders tedious; the maintenance and tracking of historical transactions are very difficult.

Traditional equity transaction is based on the credit of two sides and can be made when bilateral credit extension is established. The credit risk is borne by respective side, and the transaction platform is liable for the credit risk of market participants in a centralized manner. The unique real digital credential is application to the registration of such securitized assets as equity and bonds; cross-domain multi-centralized trust is convenient for the transfer and transaction of encrypted securitized assets; the enhanced information disclosure records are easy to meet the regulatory compliance requirements.

Ti-Blockchain can be applied to crowdfunding platform, regional equity transaction center, regional financial asset transaction center and private placement management platform, etc.

4.2 **Free Circulation of Assets**

Compared with traditional centralized system, the application of the blockchain to digital asset field has the following advantage: once the assets are issued on the blockchain, the subsequent circulation link can be no longer dependent on the issuer’s system. In the process of circulation, the assets are changed from single center control to socialized transmission. Any channel with sources may be the catalyst of asset circulation. Therefore, the blockchain can greatly improve the circulation efficiency of digital assets to actually realize “issuance by multi-party and free circulation”. Traditional asset services require corresponding middlemen, for example, the proof of asset owner and authenticity notarization can be completed only with the intervention of a third party. The whole asset circulation process may be completed only with the intervention of asset issuer, asset receiver and circulation platform. There are the following pain points in the current three-party model:

（1）When asset circulation begins, the use and transfer of asset will still rely on the asset issuer’s system, which limits the scope of asset circulation to the user group of the issuer’s system; and

（2）Traditional asset circulation has limited channels and almost relies on large channels, which increases the cost due to the monopoly position and causes the significant increase of circulation cost. In such case, small channels and individuals cannot play a role in circulation link.

## 4.3 Blockchain Cloud Storage

Cloud storage relies on third-party large storage providers to transmit and store device, such as 360 Cloud Disk and Baidu Cloud Disk. However, due to the limit of non-standard client encryption system, such data thus stored are very vulnerable to all kinds of security threats. The distributed storage based on data center can effectively improve such condition and resist review, tampering and unauthorized access. Files should be fragmented before being encrypted on a client, which can protect the contents of data. The data owner completely controls the encryption key to limit others’ access to the data.

Data owners can separately determine how to fragment files and the location of such fragments in the network. If the location of fragments is not learnt about in advance, with the spread of the network, the difficulty in finding any given fragment shows exponential growth. This means that the safety of the document is in proportion to the square of network size. Fragment size is a negotiable contract parameter. Normalized size discourage side line tries to determine the contents of fragment and can block the fragment flow passing through the network. Splitting large files, such as videos, the system will distribute fragment nodes to reduce the impact of content transfer on any node. All equipment in cloud storage system is completely transparent for users. Any authorized user in anyplace can have data access to cloud storage by connecting with cloud storage via an access cable. The data will not be lost by various data backup and disaster recovery technology and measures to ensure the safety and stability of cloud storage itself.

The basic principle of CDN is the wide application of various cache servers, which are distributed in the region or network where user access is relatively centralized. When users access a website, global load technique is applied to direct users’ access to the nearest cache server in normal operation. Such cache server will directly respond to user request. CDN content distribution system and data encryption technique ensures that the data in cloud storage will not be accessed by unauthorized user. Meanwhile, various data backup and disaster tolerance technologies are applied to ensure that the data in cloud storage will not be lost and ensure the security and stability of cloud storage itself. Ti-Blockchain is established in a distributed hash table, which can be used to store data location information or other information.

## 4.4 Smart Storage

As mentioned before, we can do a lot of things in combination with smart contracts and distributed storage.

First is basic distributed file storage function, traditional distributed storage requires centralized companies to provide service or can be used for free as p2p networks. The former is a strong control system. Once centralized service cannot provide service any more for some reason, all users will suffer great losses. It is difficult for the latter to stimulate participants to continue to share their storage or file due to being free. Storage/file providers can be awarded with token via smart contract. Both providing storage and sharing file can obtain certain benefit to encourage sharing (including storage space and data source).

Complex commercial logic can be realized with basic guarantee of file storage and in combination with smart contract. For example, users can uplink their own wills and periodically pay certain fees to the contract to ensure that the contents of the contract will not be disclosed. Once the user passes away, since the initiator cannot make further payments, the contract contents can be accessed by anyone.

Users can upload the documents to be stored as evidence to Ti-Blockchain and periodically make payments to ensure the contents are always valid. Such documents can be used as evidence at any time if necessary.

Users can specify some documents to be shared among a few users via contract. Or such documents can be shared to other users after a certain time.

Users can buy some necessary data by issuing some purchase contracts and making payments. The persons who have such important data can select free transaction. This is also a simple value transaction market.

There is more imaginary space. The current blockchain is distributed database based on ledger and it is difficult for it to store large amount of data. For example, the chains for notarization services only store the hash of source file to a small field and the source file cannot be stored. The combination effects brought by the blockchain with unlimited storage space can greatly improve the application scenarios of the blockchain and speed up the implementation of blockchain in various industries.

# Team Members

## 5.1 Technical Advisers

****

**Xu Wei,** Technical expert and entrepreneur in blockchain. Early participant and preacher of digital currency

Acted as the special assistant of the President of China Binary, a listed company of the Hong Kong Stock Exchange, and the founder of ThinkYoung.

Mr. Xu participated in the R&D of the world’s first multimedia smart card, as a core member of American start-up companies in 2007.

He joined China Binary in 2009, responsible for the R&D of new technologies and new modes and especially devoted to the mode exploration of electronic currency. He established the first online mall in electronic currency at the end of 2014, realizing the direct exchange of digital currency and virtual currency, and started ThinkYoung in 2015.

****

**Shentuqch**, Founder of BankLedger.com

CEO of BankLedger.com, Executive Vice Secretary-General of Financial Blockchain Shenzhen Consortium (FISCO), Member of Shenzhen Finance Standardization Technical Committee, Doctor of Shenzhen University; he began to study blockchain in 2013 and published more than 20 technical articles relevant to blockchain.

****

**Zhao Wei,** OracleChain CEO

He started to contact Bitcoin in 2011, participated in several blockchain community projects (Peercoin, Factom and BitShares) and maintained 1/23 of global blocking out nodes as a core member BitShares Chinese Community. He studied and worked for 8 years in Singapore, after which he returned to China to start business in 2016 and won the second place of “Shanghai Wanxiang and Deloitte Blockchain Programming Marathon” and the second place of “Mercedes-Benz Technology Marathon” the same year.

## 5.2 Technical Team

****

**Liu Shuaicheng**

Doctor in Electronics and Computer Engineering of National University of Singapore; now works in University of Electronic Science and Technology of China (UESTC) and mainly studies computer vision and algorithm theory; and has published several research articles on internationally known journals and conferences.



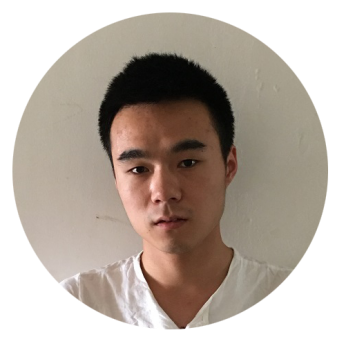
**Dong Tiansheng**

Senior C++ development engineer, worked in several software and Internet companies, is proficient in C/C++ and several other languages, has years of experience in software development and system architecture and is good at analyzing and solving various difficult problems in complex software environment.



**Dai Peng**

Graduate of UESTC, graduated as an undergraduate in School of Electronic Engineering of UESTC and was honored as excellent graduate in undergraduate school; is skillful in blockchain bottom technology development and algorithm theory.



**Deng Xuan**

Graduate of UESTC; graduated as an undergraduate in Chongqing University of Posts and Telecommunications; research interests include computational algorithm theory and data mining.

  
**He Zhiwei**

Graduate of UESTC; graduated as an undergraduate in School of Electronic Engineering of UESTC; research directions include computer vision, machine learning and Ai intelligence.



**Liao Han**

Senior network engineer; participated in the development of various software and the development and design of the basic data system of Bitcoin.

## 5.3 Marketing Team

****

**Zhang Songhao (Ricardo Zhang)**

Engaged in advanced studies in Wudaokou School of Finance of Tsinghua University; a dark horse in entrepreneurship among the generation after 90s; 8 years of working experience in the Internet; 5 years in-depth cultivation in digital currency and blockchain.



**Caizi**

Several years of working experience in Bitcoin industry; studies and takes root in digital currency and blockchain market; has rich industrial experience and keen market judgment.



**Ye Xiangyang**

Worked in domestic top-level domain name service provider new network; 8 years of working experience in the Internet; ethusiastic fan of digital currency.



**Cai Xin**

Has years of working experience in marketing and strong market perception; can keenly grasp market dynamics and the direction of development.



**Essen Zhang**

Master of Arts in Southwest Jiaotong University (SWJTU). Worked in universities and training institutions as Japanese teacher & Chinese teacher for foreigners; once worked as editor in Japanese enterprise.

# References

1. *Data Structures and Algorithm Analysis*, Yan Weimin, Tsinghua University Press, 2011.

2. *Blockchain: How to Redefine the World*, Tang Jianwen, Lu Wen, China Machine Press.

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

4. *White Paper on China Blockchain Technology and Application Development 2016.*

5. Qtum Whitepaper

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

7. https://panteracapital.com/wp-content/uploads/The-Final-Piece­of-the­Protocol­Puzzle.pdf

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

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

10. S. Nakamoto, *Bitcoin: A peer-to-peer 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/