CAICT 中国信通院

可信区块链推进计划
TRUSTED BLOCKCHAIN INITIATIVES

# Blockchain White Paper

## （2018）



China Academy of Information and Communication Technology

Trusted Blockchain Initiatives

December，2018

# COPYRIGHT STATEMENT

## Foreword

Blockchain, with its unique trust-building mechanism, has become an important direction for the deep integration of finance and technology. With the support of policy, technology and market, Blockchain technology is promoting the integration of the real economy, which is providing help for the high-quality development. Therefore, it is of great significance for China to explore a new model of sharing economy, build a digital economy industrial ecology, and improve the quality of governance and public service.

As an integrated innovation of peer-to-peer networks, cryptography, consensus mechanisms, and smart contracts, Blockchain provides a trusted channel for information and value transfer in untrusted networks. At present, the application of Blockchain has been accelerating, and key technologies such as cross-chain, privacy protection, and security supervision are becoming research hot spots. However, while the Blockchain technology is still at the stage of social experiment, there is no consensus on the concept, structure, technical characteristics, development route, governance and supervision of the Blockchain.

To promote the deep integration of Blockchain technology and the real economy, as well as to form development consensus, China Academy of Information and Communications Technology and Trusted Blockchain Initiatives co-organized the "Blockchain White Paper"(2018). This white paper deeply interprets the concept of Blockchain, proposes a Blockchain technology architecture, analyses the key technology development routes, the latest situation and development opportunities of current Blockchain in terms of policies, industries, technologies and standards. In the end, the white paper discusses the challenges with the development of Blockchain and puts forward corresponding policy recommendations.

# catalogue

# 1 The Concept and Characteristics of Blockchain

## 1. 1 Concept of Blockchain

A Blockchain is a decentralized, distributed and public digital ledger, which is jointly maintained by multiple parties, using cryptography to ensure the security of transmission and access, to achieve data storage consistency, data tamper-proof, and prevention of repudiation. It is also known as Distributed Ledger Technology (DLT). A typical blockchain stores data in the units of blocks. Each block includes the cryptographic hash of the prior block in the blockchain for linking the two adjacent blocks. The linkages of blocks are "chains". Blockchain, as the new computing paradigm and collaboration model in an untrusted competitive environment, is changing the application scenarios and operating rules of many industries with its unique trust-building mechanism. It is one of the indispensable technologies for building a new trust system and developing digital economy in the future.

In a typical blockchain system, each party shares information and reaches consensus in accordance with rules agreed in advance. In order to prevent the consensus information from being tampered with, the system stores data in units of blocks which form a cryptographical chain of data structure in chronological order, and the record nodes are selected by the consensus mechanism to determine the data of the latest block and other nodes participate in the verification, storage and maintenance of the latest data block. Once the data is confirmed, it is difficult to delete and modify, and only the authorized query operation can be performed. Depending on whether the system has a node admission mechanism/control, blockchains can be classified into Permissioned Blockchains and Permission-less Blockchains. The joining and exiting of the nodes in the permissioned blockchain require the permission of the blockchain system. Depending on whether the entities with control rights are centralized or not, Permissioned

blockchains can be divided into the Consortium Blockchain[1] and the Private Blockchain[2]. The Permission-less Blockchain, also be called as the Public Blockchain[3], is completely open, which nodes can join and exit at any time.

## 1.2 Characteristics of Blockchain

Compared with the traditional distributed database, the blockchain reflects the following characteristics: First, from double-entry accounting to distributed accounting. In traditional information system, each accountant records separately, and There are multiple different ledgers at each reconciliation. The blockchain breaks the original double-entry accounting and becomes a distributed account book for “whole network to share”, which the parties involved in the bookkeeping prevent data tampering and ensure the consistency of data. Through the synchronous coordination mechanism, avoiding the complicated multi-party reconciliation process. Second, from “insertion, deletion, selection and update” to “insertion and selection”. Traditional databases have four classic operations of insert, delete, update, and select. From the prospective of the whole network book, the blockchain technology is equivalent to the databases of giving up deletion and update options[4], leaving only two manipulation, insertion and selection, through the "block-chain" structure of blocks and linked lists, and corresponding timestamps to consolidate the voucher forming trusted data sets that are interlocking and difficult to tamper with. Third, from unilateral maintenance to multi-lateral maintenance. For each entity, the



[1] Consortium Blockchain: According to a certain feature to select the nodes that can participate in and make transaction, and the consensus process is controlled by the pre-selected node blockchain.

[2] Private Blockchain: Write permissions are in the hands of an organization, and blockchain access permissions may be restricted.

[3] Public Blockchain: Anyone can read the blockchain information, send the transaction for confirmation, participate in the consensus process. It is the actual decentralized blockchain, and the bitcoin blockchain is the best representative of the public blockchain.

[4] Users can delete or update local data, but it does not affect the data consistency after the network consensus.

traditional database is a single-party maintained information system, whether it is a distributed architect or a centralized architect, which has a high degree of control over data records. The blockchain introduces a distributed ledger, which is a distributed information system that is jointly maintained by multiple parties with no a single point of failure. Data writing and synchronization are not limited to one subject and are further required to be verified by multiple parties for reaching consensus to decide which data can be written. Fourth, from a plug-in contract to a built-in contract. Traditionally, financial capital flow and business information flow are two distinct business processes. Contracts signed by business cooperation, after manual review and results verification, can notify the finances to make a payment and form a corresponding capital flow. The emergence of smart contracts, based on arranged rules, is performed independently through code execution, collaborative writing, and a "built-in contract" that integrates information flow and capital flow through algorithmic code.

## 1.3 Scenarios applicable to blockchain

As an emerging technology, blockchain has the potential to be applied in many areas. However, the blockchain is not a panacea. It is technically decentralized and difficult to tamper with, making it with a high applicable value within a limited number of scenarios. The applicable scenarios can be summarized as “new database, multi-service entity, mutual trust, strong business related".

Firstly, application scenario from the needs of the database. The blockchain is essentially a new type of time-stamped database. From the perspective of reaching the organization's requirement of real, effective, unforgeable, and tamper-proof data, they have a new starting point and new demands compared to traditional databases. **Secondly, it needs to be a cross-subject, multi-party application scenario.** The maintenance of the books by multiple entities is often caused by the fact that the data is not shared, and the business logic is not uniform, resulting in the phenomenon of

"Reconciliation Failure". In contrast, each entity in the blockchain can have a complete copy of the book, ensuring data consistency between multiple entities through an instant clearing mode, avoiding complex reconciliation processes. **Again, application scenarios are to build math-based trust in an untrusted environment**. The blockchain guarantees the system's data trust (cryptographic algorithm, digital signature, timestamp), reliable results (smart contract, formula algorithm) and historical trust (chain structure, timestamp) at the technical level, so the blockchain provides an "intermediate machine" that is particularly useful for industry applications where the collaborators are not trusted, have inconsistent benefit, or lack the involvement of a third-party authority. **Finally, scenarios can be classified into the cases of whether the system control rights and transaction information are open or not.** The public blockchain allows the joining of any node, and it does not restrict the dissemination of information, and the information is disclosed to the whole system; the consortium blockchain only allows the accredited institutions to participate in the consensus, and the transaction information and consensus mechanism is limited to a certain extent; in contrast, the private blockchain has the narrowest scope, only applicable to a limited organization.

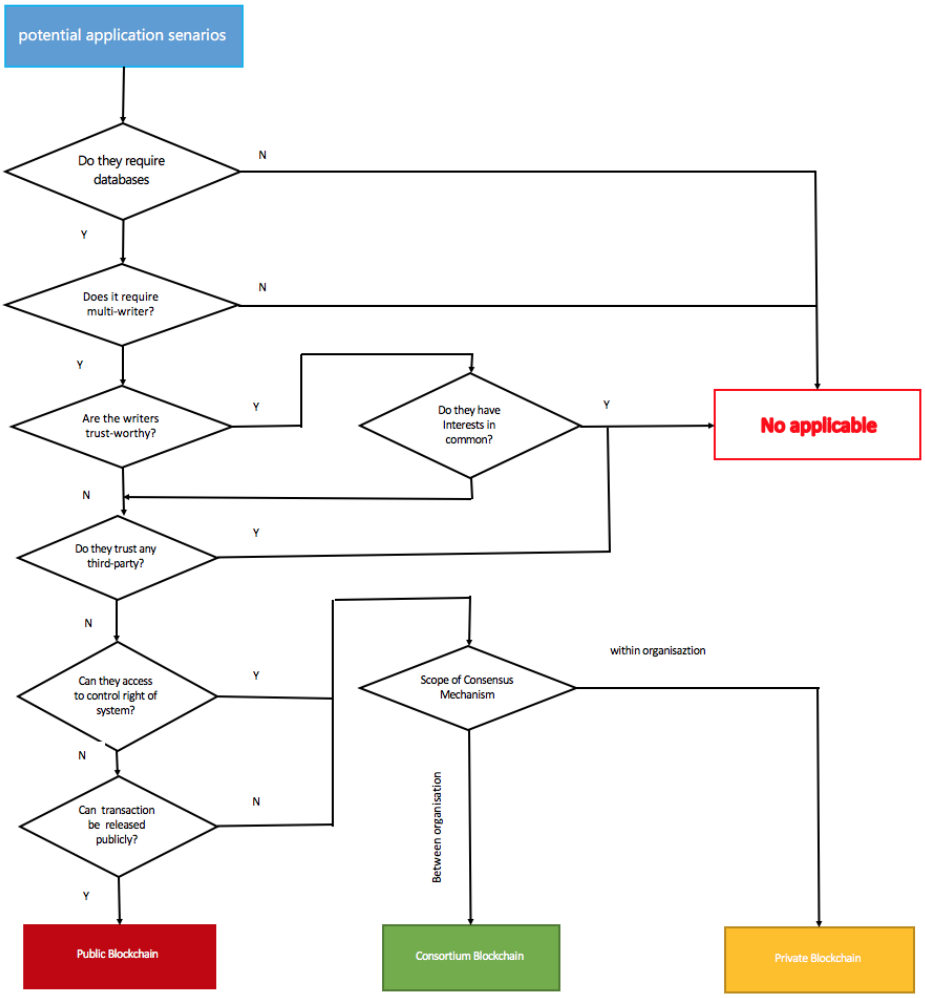


*Figure 1. Scenarios are applicable for blockchain*

# 2 The key technology architecture and development trend of blockchain

## 2.1 Blockchain technical architecture

Different blockchains have different implementations, but there is a general blockchain architecture that is widely acknowledged. This white paper suggests a classification of nine dimensions. They are layers of Infrastructure, Utility, Ledger, Consensus, Smart Contract, System Management, Interface, Application and Operation, and Maintenance.

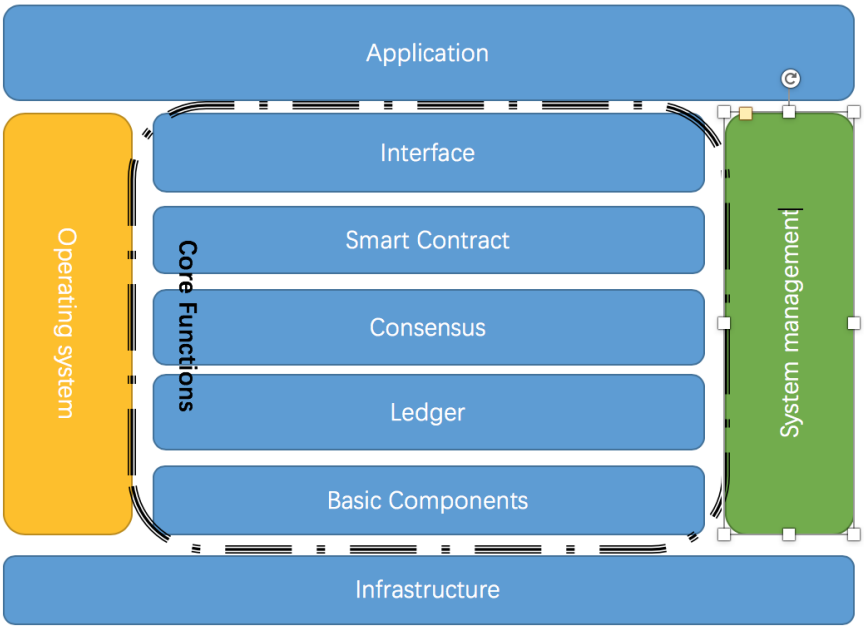


*Figure 2. Blockchain Technical Architecture, Source: CAICT, August 2018*



### 2.1.1 Infrastructure

The infrastructure layer provides physical resources and drivers for the upper layers and is the base support for the blockchain system. The infrastructure layer provides the operating environment and hardware such as Physical Machine, Cloud, etc. required for the blockchain system to function properly. It provides network resources (Network Cards, Switches, Routers, etc.), storage resources (Hard Disks and Cloud Storage, etc.) and computing resources (CPU, GPU, ASIC, etc.) for upper layers.

### 2.1.2 Utility

The utility layer enables the recording, verification and dissemination of information in the network of blockchain systems. In the utility layer, the blockchain is a distributed system based on the transmission mechanism, verification mechanism and storage mechanism. The entire network has no centralized hardware or management organization, and any node has the

opportunity to participate in the records and verification of the general ledger by broadcasting the calculation results to other nodes, and the damage or exit of any node will not affect the operation of the entire system. In particular, it mainly includes five types of modules: network discovery, data transmission and reception, password library, data storage, and message notification.

1) Network discovery

The blockchain system consists of a number of nodes connected by a network. Especially in public blockchain systems, the number of nodes tends to be very large. Each node needs to discover neighbor nodes through the network discovery protocol and establish links with neighbor nodes. For the consortium blockchain, the network discovery protocol also needs to verify the identity of the node to prevent various network attacks.

2) Data transmission and reception

After the node is connected to the neighbor node through the network communication protocol, and the data transceiver module completes data exchange with other nodes. Transaction broadcasts, message consensus, and data synchronization are all performed by this module. According to the architecture of different blockchains, the design of the data transceiver needs to consider factors such as the number of nodes and cryptographic algorithms.

3) Password library

Multiple links in the blockchain use cryptographic algorithms. The cryptographic library provides basic cryptographic algorithm supporting the upper layer components, including commonly used encoding algorithms, hash algorithms, signature algorithms, privacy protection algorithms, etc. Furthermore, the password library also covers functions such as the maintenance and storage of private keys.

4) Data storage

Depending on the data type and system architecture design, the data in the blockchain system uses different data storage modes. Storage modes

include relational databases (such as MySQL) and non-relational databases (such as LevelDB). Usually, the data that needs to be saved includes public data (for example, transaction data, transaction data, status data, etc.) and local private data, etc.

5) Message notification

The message notification module provides a message notification service between different components in the blockchain and between different nodes. After the transaction is successful, the client typically needs to track the records during the execution of the transaction and obtain the results of the execution of the transaction. The message notification module can complete the generation, distribution, storage, and other functions of the message to meet the demand of the blockchain system.

### 2.1.3 Ledger

The ledger layer is responsible for the information storage of the blockchain system, including collecting transaction data and generating data blocks for validity of the local data and passing the checked block to the blockchain. The ledger layer embeds the hash of the previous block into the next block to form a blockchain data structure, which ensures data integrity and authenticity. This is the source of tamper resistance and traceability of blockchain systems. A typical blockchain system design uses a block-chain data structure stored in chronological order.

There are two ways of recording data at the ledger layer, which are based on assets and based on accounts respectively. In the asset-based model, the asset is the core for model establishment, and then the ownership of the asset is recorded, that is, ownership is a field of the asset. In the account-based model, an account is created as an object of assets and transactions, and an asset is a field under the account. In contrast, an account-based data model makes it easier to record and query account-related information, and an asset-based data model can better adapt to the concurrent environment. In order to obtain high concurrent processing performance and timely query status information of the account, multiple

blockchain platforms are developing towards a hybrid mode of the two data models.

Table 1: Two models' comparison in the Ledger Layer

| | **Asset-based** | **Account-based** |
|---|---|---|
| **Modeling Objects** | Asset | Account |
| **Data Record** | Asset Ownership | Account Operation |
| **System Center** | Status（Transaction） | Event （Operation） |
| **Computing Concentration** | Client | Node |
| **Dependency Judgement** | Easy to estimate dependency | Difficult to estimate dependency |
| **Parallel** | Easy | Hard |
| **Account Management** | Hard to manage account metadata | Easy to manage account metadata |
| **Suitable Query Scenarios** | Easy to fetch transaction status | Easy to fetch account balance |
| **Client** | Complex | Easy |
| **Examples** | Bitcoin, R3 Corda | Ethereum, Hyper ledger Fabric |



### 2.1.4 Consensus

The consensus layer is responsible for coordinating and ensuring the

consistency of data records of all nodes in the whole network. The data in the blockchain system is stored independently by all nodes. With the coordination of the consensus mechanism, the consensus layer synchronizes the books of each node, thereby implementing functions such as node election, data consistency verification and data synchronization control. Data synchronization and consistency coordination make the blockchain system with feature of transparent and data-sharing.

Table 2: Two types of Consensus Mechanism Comparison

| | **Type I** | **Type II** |
|---|---|---|
| **Write order** | Write first and consent later | Consent first and write later |
| **Representative algorithms**[5] | PoW、PoS、DPoS | PBFT 、BFT etc. |
| **Consensus Process** | Consensus relies on probability Confirmation guaranteed by engineering structure | Consensus after confirmation |
| **Complexity** | High Computing Complexity | High Networking Complexity |
| **Arbitration Mechanism** | If there are multiple record nodes after making consensus, forks will occur, and the longest chain will be kept. | Quorum vote to reach agreement via P2P broadcast communication between nodes |
| **Fork** | Yes | No |
| **Security Threshold** | No more than half of sum of malicious nodes equity | Number of malicious nodes is not more than one third of total node number |
| **Node Number** | The node number is free to alter, the more node number is, the more stable system is. | The performance decline as node number increase and the number of nodes is not free to alter. |
| **Application** | Mainly used in | Used in Permission Blockchain |

[5] Consensus algorithm representatives include: PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), BFT ( Byzantine Fault Tolerance).

| | | |
|---|---|---|
| **scenarios** | Premissionless Blockchain | |

There are two types of current in operating consensus mechanisms in the blockchain, which are determined according to the order in which the data is written, as shown in the table 2. From the perspective of the requirements of business applications, the implementation of consensus algorithms should consider the application environment, performance and other requests of application. In general, the permissioned blockchain uses a consensus mechanism for node voting to improve system performance at the cost of lowing security level. The Permission-less blockchain adopts a consensus mechanism based on Proof of Workload and Proof of Stake and other evidences, which mainly emphasizes system security, but its performance is poor. In order to encourage the participation of all nodes and maintain the safe operation of the blockchain system, the Permission-less blockchain adopts the method of issuing tokens as the compensation and incentive mechanism of the participants, that is, through the means of economical balance, to prevent tampering with the contents of the general ledger. Therefore, according to the operating environment and trust hierarchy, selecting the applicable consensus mechanism is one of the most important factors that should be considered when the blockchain application landing.



Table 3: Comparison of Consensus Algorithms

| **Characteristic** | **PoW** | **PoS** | **DPoS** | **PBFT** | **VRF** |
|---|---|---|---|---|---|
| **Node Management** | No permission required | No permission required | No permission required | Require permission | Require permission |
| **Transaction Latency** | High (in minutes) | Low (in seconds) | Low (in seconds) | Low (in millisecond) | Low (in millisecond) |
| **Throughput** | Low | High | High | High | High |
| **Energy-saving** | No | Yes | Yes | Yes | Yes |

| | | | | | |
|---|---|---|---|---|---|
| **Security Boundary** | Malicious computing power is no more than 1/2. | Malicious equity is no more than 1/2. | Malicious equity is no more than 1/2. | The number of malicious nodes is no more than 1/3. | The number of malicious nodes is no more than 1/3. |
| **Representative application** | Bitcoin, Ethereum | Peercoin | Bitshare | Fabric（Rev 0.6） | Algorand |
| **Scalability** | Well | Well | Well | Poor | Poor |

### 2.1.5 Smart Contract

The smart contract layer is responsible for compiling, deploying, implementing the business logic of the blockchain system with coding, achieving the conditional triggering and the automated execution of the established rules, to minimize manual intervention. Most of the operating objects of smart contracts are digital assets. The smart contract is hard to modify after data is on the blockchain and its trigger conditions are rigid, therefore, the applications of smart contracts express characteristics of both high value and high risk. How to avoid risks and exert values are obstacles for the wide application of smart contracts.

Smart contracts can be divided into two categories of whether Turing Complete[6] is fulfilled, that is, Turing complete and Turing incomplete. Typical reasons for affecting Turing completeness achievement are including: loop or recursion being constrained, incapable arrays implementation or containing complex data structures. Smart contracts

[6] Turing completeness: In computability theory, a system of data-manipulation rules (such as a computer's instruction set, a programming language, or a cellular automation) is said to be Turing complete or computationally universal if it can be used to simulate any Turing machine. (Gannon, Paul, Colossus: Bletchley Park's Greatest Secret, London: Atlantic Books, 2006-01-10 [2006], ISBN 978-184-354-330-5)

with Turing complete have considerable adaptability and can program for more complex business operations than ones not, but it is possible to run into an infinite loop. However, Smart contracts with Turing incomplete are simple, more efficient, and secure despite of incapable of operating complex business logic.

Table 4: Smart Contract Characteristics of some Blockchain System

| Blockchain platform | Turing Completeness | Developing language |
|---|---|---|
| **Bitcoin** | Incompleteness | Bitcoin Script |
| **Ethereum** | Completeness | Solidity |
| **EOS** | Completeness | C++ |
| **Hyperledger Fabric** | Completeness | Go |
| **Hyperledger Sawtooth** | Completeness | Python |
| **R3 Corda** | Completeness | Kotlin/Java |



Currently, the progress of smart contracts landing is still at its early stage, and smart contracts have become the “hardest hit area” for blockchain security issue. from the security incidents caused by previous smart contract vulnerabilities, there are many security vulnerabilities in contracts writing, which poses great challenges to maintain security. There are several approaches operated currently for improving the security of smart contracts: One is the Formal Verification. The rigorous mathematical proof is used to ensure that the logic expressed by the contract code conforms to the intent. This law is rigorously logical, but it is difficult to operate. Generally, it is necessary to entrust a third-party professional organization to conduct audits. Another method is the smart contract encryption. Smart contracts cannot be read in plain text by third parties, thereby reducing smart contracts from being attacked due to logical security breaches. This method is low-cost but not available for open source applications. Another method is to strictly regulate the syntax of the contract language. The

standardization of smart contract coding, such as the summaries of excellent smart contracts model and the smart contract templates standard development, are aiming to improve the quality and security of smart contracts.

### 2.1.6 System Management

The system management layer is responsible for managing other parts from the blockchain architecture. It includes two types of functions: rights management and node management. Rights management is a key part of blockchain technology, especially for Permissioned chains that have more requests from data access. Rights management can be achieved in the following ways: 1) submitting the permission list to the ledger layer and implementing distributed permission control; 2) using access control list to implement access control; 3) Using permission controls, such as ratings/sub-regions. With rights management, you can render certain data and function calls by corresponding operator.

The core of node management is the node identification, which are usually implemented using the following technologies: 1) CA[7] authentication: Centralized issuing of CA certificates to applications in the system, and identity and authority management are authenticated and confirmed by these certificates. 2) PKI[8] authentication: The identity is confirmed by the PKI address. 3) Third-party authentication: The identity is confirmed by the authentication information provided by the third party. Node management is variated due to the different application scenarios of the blockchains. Business extensions can interact with authentication and rights management.



[7] CA: Certificate Authority, also known as the E-Commerce Certification Authority, is the authority responsible for issuing and managing digital certificates. As a trusted third party in e-commerce transactions, it assumes the public key in the public key system. The responsibility for the legality test.

[8] PKI: Public Key Infrastructure is a key management platform that adheres to established standards. It provides cryptographic services such as encryption and digital signatures and the necessary key and certificate management systems for all network applications.

### 2.1.7 Interface

The interface layer is mainly used to complete the encapsulation of function modules and provide a simple call for the application layer. The application layer communicates with other nodes by calling the RPC interface, and accesses and writes the local ledger data by calling the SDK toolkit. At the same time, RPC and SDK should abide by the following rules: First, it is fully functional and can make complete transactions and maintain distributed ledgers. It has a comprehensive intervention strategy and authority management mechanism. Second, it is portable and can be used in many applications in a variety of environments, not just designed for certain software or hardware platforms. The third is it has scalability and compatibility. The design should at most forward and backward compatible and consider its scalability. Fourth, it is easy to use. The structured design and good naming methods are developers-friendly. Common implementation techniques include calling control and objects serialization.

### 2.1.8 Application

The application layer is the part that is finally presented to the user. The main function is to call the smart contract layer. The interface adapts to various application scenarios of blockchain to provide various services and applications for users. Since blockchains have data validation attribute and characteristics of value network, now, much of the work from applications can be resolved by the underlying blockchain platform. In the process of developing blockchain applications, the preliminary work must be very cautious. Proper selection from the decentralized public blockchain, efficient consortium blockchain, and secure private blockchain as the underlying architecture ensure the core algorithm has no fatal errors during the design phase. Therefore, proper packaging of the underlying blockchain technology and providing a one-stop blockchain development platform will be an inevitable trend in the development of the application layer. At the same time, the maturity of inter-chain technology allows the

application layer to add flexibility when choosing a system architecture.

Depending on the implementation and the purpose of the application, the current application based on blockchain technology can be divided into three types of scenarios, as shown in Table 5: First, the value transfer. Digital assets transfer between different accounts, such as cross-border payment. Second, deposit certificate, i.e., information records on the blockchain with no asset transfer, such as electronic contracts. Third, authorization management. It uses smart contracts to control data access, such as data sharing. In addition, there are mixed-typed of scenarios as application requirements continue to escalate.

Table 5: Blockchain Application Scenarios Classification

| **Type** | **Governance** | **Finance** | **Industry** | **Healthcare** | **Law** | **Copyright** |
|---|---|---|---|---|---|---|
| **Value transfer** | | Digital bill; Cross-border settlements; Account receivable; Supply Chain Finance | Energy deal | Health insurance | | |
| **Receipt** | Electronic invoices; Digital license; Targeted poverty alleviation | Cash serial number; Traceability; Supply Chain Finance | Security traceability | Electronic Medical Record; Medicine Trackability | Notary; Digital Receipt; Online Arbitration | Copyright verification; |
| **Authorization Manage** | Government data sharing | Credit Investigation | | Health data sharing | | Copyright Managem |

| | | | | | | |
|---|---|---|---|---|---|---|
| **ment** | | | | | | ent; |

### 2.1.9 Operation and Maintenance

The operation and maintenance layer are responsible for the daily operation and maintenance of the blockchain system, including the log library, monitoring library, management library, and extension library. In the unified architecture, the mainstream platforms are different according to their own demand and positioning. The choices of storage modules, data models, data structures, coding languages, and sandbox environments in the blockchain system are also different (see Table 6). These variations bring great challenges to operation and maintenance of blockchain platforms.

Table 6: Blockchain technology system architectures comparison

| **Layer** | **Platform difference** | **Bitcoin** | **Ethereum** | **Hyperledger Fabric** | **R3 Corda** |
|---|---|---|---|---|---|
| **Application** | | Bitcoin | Dapp/ Ether | Enterprise Class Distributed Ledger | CorDapp |
| **Smart Contract** | Development Language | Script | Solidity/ Serpent | Go/Java | Java/Kotlin |
| | Sandbox environment | | EVM | Docker | JVM |
| **Consensus（Data Access）** | | PoW | PoW/ PoS | PBFT/SBFT/Kafka | Raft |
| **Ledger** | Data Structure | Merkle Tree/Block-chain list | Merkle Patricia Tree/ Block-chain list | Merkle Bucket Tree/ Block-chain list | No Block connection Transaction |

| | | | | | |
|---|---|---|---|---|---|
| | Data Modeling | Asset-based | Account-based | Account-based | Asset-based |
| | Block storage | Document storage | LevelDB | LevelDB/CouchDB | Relational Database |
| **Utility Layer** | | TCP，P2P | TCP，P2P | HTTP2 P2P | AMQP(TLS) P2P |

## 2.2 Blockchain technology development trend

### 2.2.1 From prospective of architecture, the integration of Public Blockchain and Consortium Blockchain evolution is continuing

The consortium blockchain is an important application to land blockchain technology at the current stage, but the consortium blockchain does not have the scalability, anonymity and community incentives that the public blockchain has. As the application scenarios increase their complexity, the architectural models of the public blockchain and the consortium blockchain begin to merge, and the hybrid architecture model in which the public blockchain is offered to the public at the bottom level and the consortium blockchain is offered to the enterprise at the upper level to form a technology ecosystem with integration of wallets and exchange markets. For example, when selecting a verification node in the public blockchain, there are problems such as high uncertainty under PoS, significant resource consumption under PoW, and incapability of supporting a large number of nodes to make consensus under PBFT. The Algorand algorithm[9] selects a small number of nodes from a large number of nodes by cryptography, and then use the PBFT algorithm to reach a consensus among a small number of nodes, provides a possibility for a hybrid architecture of the public blockchain and consortium blockchain.

[9] The Algorand consensus algorithm was proposed by the Turing Award winner, Professor Silvio Micali.

### 2.2.2 From prospective of deployment, blockchain-as-a-service are accelerating applications to land

The combination of blockchain and cloud computing will effectively reduce the cost of blockchain deployment. On the one hand, pre-configured networks, common distributed ledger architecture, similar identity management, distributed bottom business monitoring system logic, similar node connection logic, etc. are modularized and abstracted as the blockchain services to support the upper application layer with different clients. Quick construction of blockchain services with cloud computing can conduct quick verification of concepts and model feasibility. On the other hand, cloud computing charged by usage make use of fundamental infrastructure services or adjust to meet the actual requirement to accelerate application development process, reduce deployment costs, and meet the service request of start-ups, academic institutions, open source communities, alliances and financial institutions in the future blockchain ecosystem.

Based on the three types of services currently provided by cloud computing (IaaS, PaaS, SaaS), blockchain combined with cloud computing to develop BaaS (Blockchain as a Service). BaaS service providers aim to provide users with better blockchain services, so BaaS service providers pay more attention to the vertical industries connection than the blockchain infrastructure technology providers to deliver reasonable smart contract templates, suitable account system management and resource management tools and customized data analysis and reporting systems.

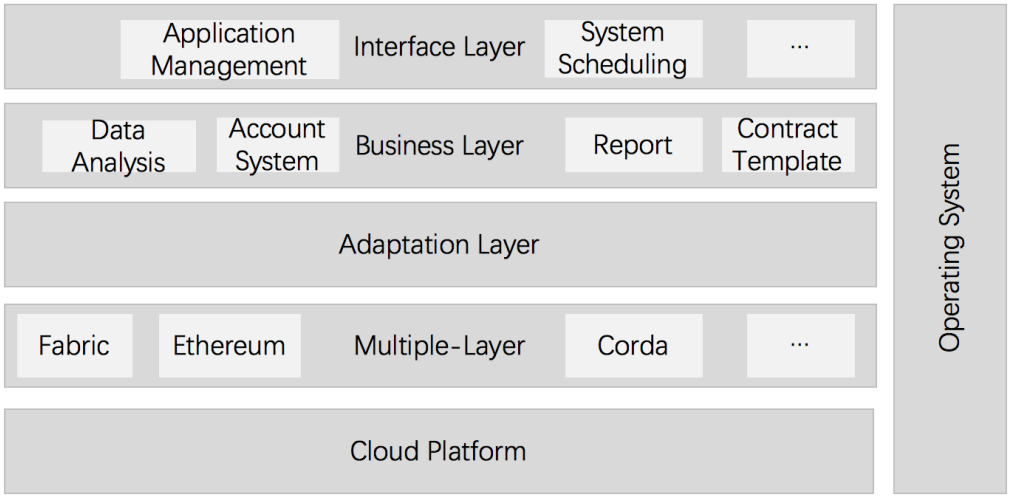


*Figure 3. BaaS Architecture, Source: CAICT, August 2018*

At this stage, BaaS service providers support the background data storage, application data analysis, mobile terminals, application launching, and information identification. Relying on the cloud computing platform, blockchain developers can focus on applying blockchain technology to different business scenarios, helping users build blockchain services with low entry barriers and high efficiency, while promoting the transformation and upgrading of their own industries to create new products, business and business models for our customers.

### 2.2.3 From performance prospective, the demand for Cross-chain and high performance is highlighted

One of the growing demands of blockchain is to conduct direct circulation of values across blockchains. Inter-chain technology constructs the connection of blockchains in different industries with complex scenarios to achieve digital asset transfer between multiple blockchains, such as financial pledge and asset securitization. Current mainstream Inter-chain technologies include Notary schemes, Sidechains/relays, and Hash-locking.

Table 7: Inter-chain Technology Comparison

| Classification | Notary | Sidechain/relays | Hash-Locking |
|---|---|---|---|
| **Inter-Blockchain** | Bi-directional | Bi-directional/Uni-directional | Bi-directional |
| **Asset Exchange** | Support | Support | Support |
| **Asset Transfer** | Support | Support | No Support |
| **Trust** | Require the third-party | No require | No require |
| **Type** | Protocol | Technology Architecture | Algorithm |
| **Difficulty** | Average | Hard | Easy |
| **Use Case** | Ripple | BTC relay<br>Poldadot<br>COSMOS | Lightning network |

In order to improve the throughput of the blockchain system, blockchain technology and academic experts have proposed a variety of high-performance solutions, as shown in Table 8 below.

Table 8: High performance Schemes comparison

| Type | DAG | Parallel | Reduction of node number |
|---|---|---|---|
| **Optimizing Layer** | Topology | Framework | Consensus |
| **Security** | High | High | May reduce |
| **Resource consumption** | Low | Low | Low |
| **Scalability** | Well | Well | Average |
| **Difficulty** | Relatively Hard | Average | Security Assurance Scheme is relatively hard |

| | | | |
|---|---|---|---|
| **Performance** | High | High | Average |
| **Examples** | IOTA<br>Byteball<br>Hashgraph | Ethereum（Sharding）<br>TrustSQL（Subchain）<br>Fabric（Multichannel） | Algorand<br>BitcoinNG<br>PoS |



The first type of high-performance solution is to change the blockchain topology to a transaction-based Directed Acyclic Graph (DAG). Under this topology, after the transaction request is initiated, the entire network is confirmed by the broadcast to form a transaction network. There is no packaging process, and the transaction can be stripped from the network or be merged back. DAG-based designs have no block concept, and expansion is not limited by block size. The scalability depends on network bandwidth, CPU processing speed, and storage capacity limitations[10]. This topology addresses security issues, high concurrency issues, scalability issues, and data growth issues and adapting to micropayment scenarios.

The second type of high-performance solution is to change the consensus strategy to increase throughput by reducing the number of nodes participating in the consensus. In this type of scheme, in order to improve performance, the number of nodes participating in the consensus is reduced as much as possible without affecting security, and the algorithm to control a node participating in the consensus is not predicted in advance. Although this solution can improve performance, the strategy to ensure security is difficult to achieve now.

[10] For the first time in the IOTA white paper, the Tangle blockchain is a directed acyclic graph (DAG), but its architecture is not only a double-spending risk, but also a risk of forging digital signatures. In order to solve the double-spending problem, Byteball proposed the concept of the Mainchain based on the DAG of IOTA and realized the mainchain selection algorithm through the witness method, effectively solving the DAG double-spending problem.

The third type of high-performance solution is to improve the overall throughput of the system by improving the horizontal expansion capability of the system, representing technologies such as fragmentation, sub-blockchain, and multi-channel. For this type of technology, data synchronization is required within the intra-slice, sub-blockchain, and channel, and the slice interval, sub-blockchain, and channel are asynchronous. Sharding is to divide the nodes in the entire P2P network into several relatively independent areas to achieve system level expansion. In the case of sharding, by directing the transaction to different nodes, multiple network segments share the work of verifying the transaction in parallel. Current fragmentation strategies include Network Sharding, Transaction Sharding, and Computational Sharding. The sub-chain technology is a blockchain with independent functions derived from the mainchain. The sub-chains depend on the mainchain and can define their own consensus mode and execution module. By defining different sub-chains, the system's scalability, availability, and performance are improved. Multi-channel technology is a system in which multiple nodes form a channel. Each node can also be added to different channels. The channels are isolated from each other and communicate with each other through anchor nodes. Multi-channel technology eliminates network bottlenecks and increases system scalability.

### 2.2.4 From the consensus prospective, the consensus mechanism evolved from a single to a mixed approach

The consensus mechanism plays an important role in the blockchain, which determines who has the right to book, and the selection process and reasons for the bookkeeping rights. Therefore, it has always been the focus of blockchain technology research. Common consensus mechanisms include PoW, PoS, DPoS, Byzantine fault tolerance, etc., depending on the applicable scenario, also present different advantages and disadvantages. The single consensus mechanism has its own drawbacks. For example, PoS

relies on tokens and its security is fragile, while PoW is non-final and energy consumption is high. In order to improve efficiency, trade-offs should be made among safety, reliability, and openness. The blockchain is showing the trend of switching the consensus mechanism according to the scenario and will evolve from a single consensus mechanism to a multi-class hybrid consensus mechanism. The support consensus mechanism is dynamically configurable during the running process, or the system automatically selects the consistent consensus according to the current situation.

Table 9: Consensus Mechanism of Scenarios

| **Scenarios** | **Consensus** | **Algorithm Examples** |
|---|---|---|
| **Untrusted environment, unknown number of nodes** | Equity | PoW，PoS，DPoS |
| **Untrusted environment, certain number of nodes** | Byzantine | PBFT |
| **Trusted environment, unknown number of nodes** | Non-Byzantine | Raft |
| **Trusted environment, certain number of nodes** | Message distributed Mechanism | Kafka |



### 2.2.5 From smart contracts prospective, pluggability, usability and security have become the focus of blockchain development.

Richness of smart contracts applications depends on the ability of the smart contract itself and the blockchain to support the smart contract application, and the development and execution efficiency of the smart contract depends on the programming language and execution of the virtual machine. In the current ecosystem, the programming language of smart contracts is not standardized. In order to adapt to smart contracts, new languages for contract need to be created with more formal specifications

and verification. Smart contracts will enable quick start time and high execution efficiency in a lightweight execution environment.

The development direction of smart contracts includes the following points: 1) Pluggable execution environment architecture: The default execution environment should not provide persistent storage, so that the contract default is a stateless function similar to microservices to conduct concurrent processing. 2) Explicit call relationship: that is, only the function of static call is provided, so that the call relationship of the program can be clarified before running it. 3) Contract code that can be stored off-blockchain: the storage space is expanded by storing hash values in the blockchain and storing the contract code outside the blockchain. 4) Low coupling design: reduce the contract language, execution environment, coupling between blockchains, and improve the versatility of smart contract systems; 5) secure protection system improvement in fields of: Verification and inspection of code shaping and release, dynamic verification of nodes in execution contracts, rationality judgment of contract execution completion, complaint mechanism of relevant stakeholders and automatic judgment technology.

# 3 The Current Situation of Blockchain

## 3.1 Various countries are competing to lay out Blockchain and occupy the commanding height in industry.

Blockchain is being recognized by many countries which are exploring technology popularization and application in many fields. On January 22, 2018, a staff in Innovate UK said that the UK would invest 19 million to support new products or services in nascent technology fields such as Blockchain. On February14, 2018, U.S. House of Representatives held the second Blockchain hearing and reached a consensus on the idea “These Innovations Should be Fostered Not Smothered”. The Bank of Korea encourages Blockchain technology, and Korea Exchange (KRX), South Korea's only stock exchange, has announced the development of a trading

platform based on Blockchain technology as well. Australia is actively exploring Blockchain technology in various fields. And Australian Post has already applied Blockchain technology to identity recognition. Dubai has established the Global Blockchain Committee and a coalition of more than 30 members, including Cisco, Blockchain Start-ups and the Dubai government.

China laid out the frontier of the Blockchain industry and explored the various applications in advance. In 2016, the Blockchain was first put into "13th Five-Year" National Informatization Plan which issued by the State Council of China. In June 2018, the Ministry of Industry and Information Technology issued Action Plans for Industrial Internet Development (2018-2020). It encouraged to promote the application and research of edge computing, Deep learning, Blockchain and other nascent but cutting-edge technologies in the industrial Internet. On May 28, 2018, President Xi Jinping pointed out in his speech at the Congress of the Chinese Academy of Sciences (CAS) and the Congress of the Chinese Academy of Engineering (CAE) that, “The new generation of information technology represented by artificial intelligence, quantum information, mobile communication, internet of things, and Blockchain accelerate the breakthrough in application”.

Hence, various regions have launched incentive policies and Blockchain projects. By the end of May 2018, 24 provinces, cities or regions, including Beijing, Shanghai, Guangdong, Hebei (Xiong'an), Jiangsu, Shandong, Guizhou, Gansu and Hainan, had issued policies and guidance on Blockchain. Besides, several provinces listed Blockchain in the 13th Five-Year Plan of the province, and carried out the industrial chain layout of the Blockchain. With the continuous expansion of Blockchain technology in the application layer, regions have introduced incentive policies of Blockchain, and more and more Blockchain technology enterprises choose to settle in preferential areas for development.

## 3.2 The Integration of Blockchain and Real Economy Proves to Be the Theme.

From the respective of the industry development, the Blockchain technology is moving towards integration, which make the Blockchain industry subdivided gradually. According to the upstream and downstream structure of the Blockchain industry, it can be divided into four categories from bottom to top: development of underlying infrastructure and platform, technology expansion and general services, industry applications, and industry services. The corresponding product can be further divided into different types, such as Blockchain itself, client and application. Following Blockchain 1.0 represented by Digital Currency, Blockchain 2.0 with smart contract and other related technical foundations has the ability to support applications and general application development in some vertical industries.

With the innovation and upgrade of Blockchain, its deep integration and innovation with cloud computing, big data and other cutting-edge technologies will promote the commercial exploration and application of Blockchain technology in medical, judicial, industrial, media, games and other sub-areas. It’s obvious that it will transform Blockchain from fictitious to real. So far. the eco-industrial chain has taken shape initially, which is providing help for the high-quality development of the real economy in many fields.

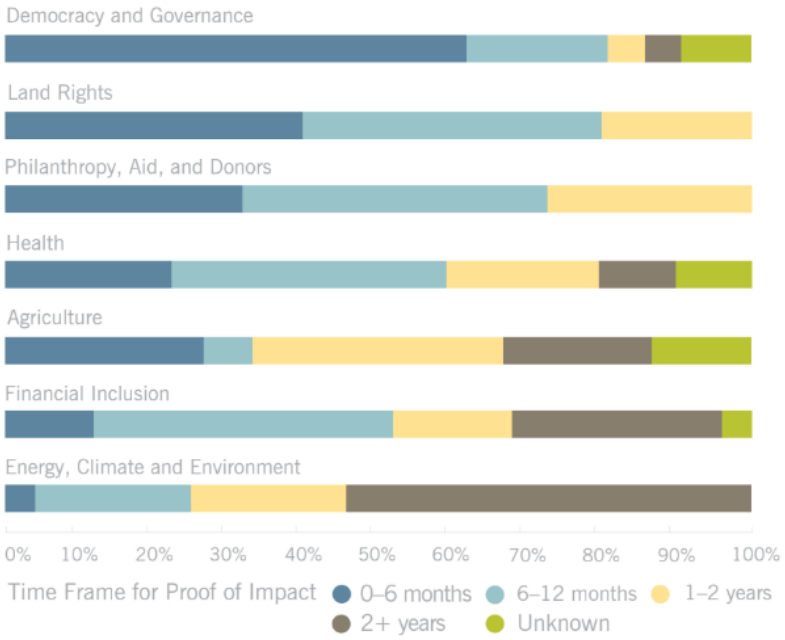


*Figure 4. Blockchain Applications Development Time, Source: Blockchain for Social Impact: Moving Beyond the Hype, J Stanford Graduate School of Business, July 2018*

From the perspective of Blockchain enterprises, we have the second largest number after the US. According to the survey conducted by China Academy of Information and Communications Technology, 1242 companies have been actively involved in the Blockchain industry all over the world, as shown in Figure 5. The number of Blockchain enterprises in the US, China and the UK is in the top three. In terms of industry classification, the number of companies which are engaged in Cryptocurrency-related technology and services (467, 37.60%) is the largest, followed by Blockchain technology companies and companies that researches and develops software platform (201, 16.18%), as shown in Figure7. According to public information, As of June 2018, the top five cities in China have the number of blockchain enterprises: Beijing, Shanghai, Shenzhen, Hangzhou, Guangzhou, of which Beijing ranks first with 175 blockchain companies, See Figure 6 for details. It is noteworthy that, a number of new forces in Southeast Asia (Singapore, Vietnam, Thailand, etc.) have emerged in the era of Blockchain 2.0 by the support

of governments and community collaboration. Under the innovation model of regulatory sandbox, a series of interoperability systems of Blockchain, which are mainly based on crosschain and multichain-subchain technologies, have been incubated, which may occupy the blockchain ' s commanding point in the future.

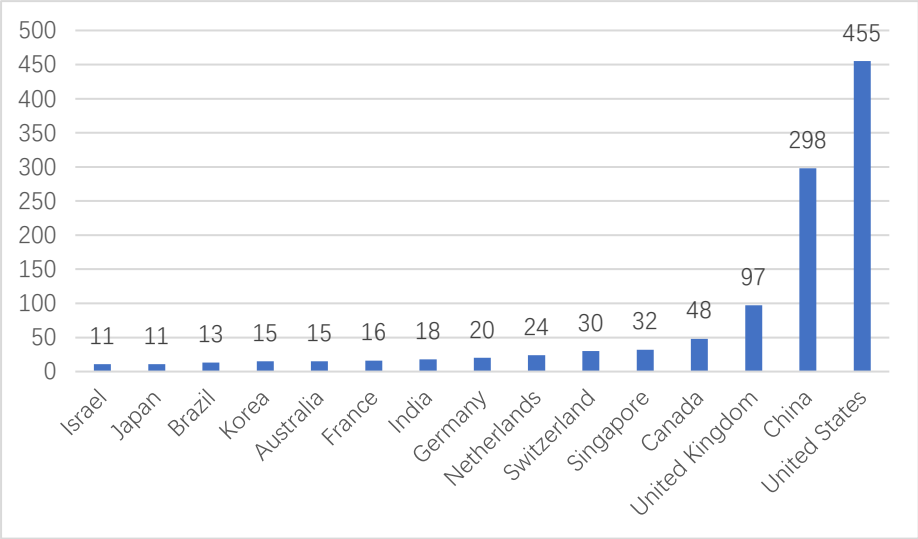


*Figure 5. Number of blockchain companies in countries around the world Data sorted by CAICT, June 2018*

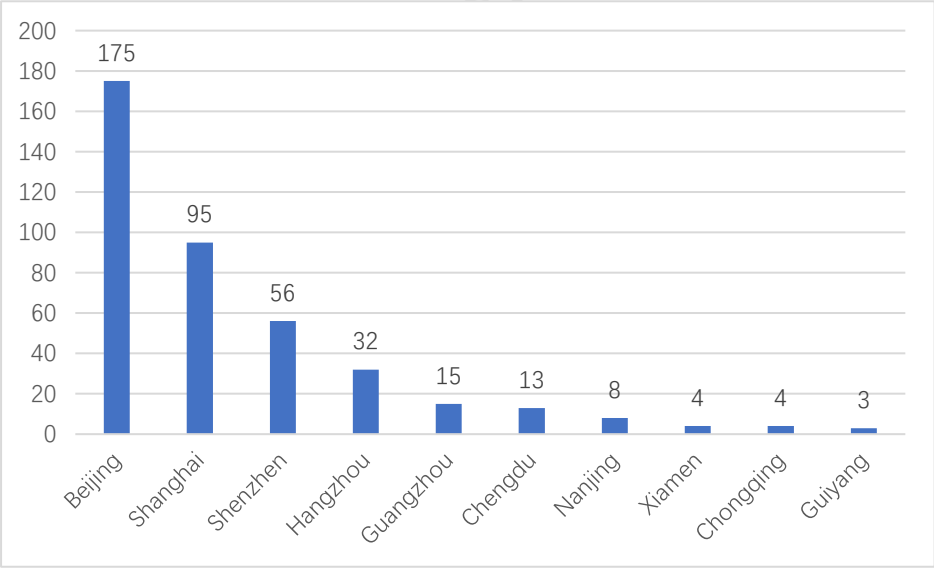


*Figure 6. China's blockchain enterprise distribution, Data sorted by CAICT, July 2018*

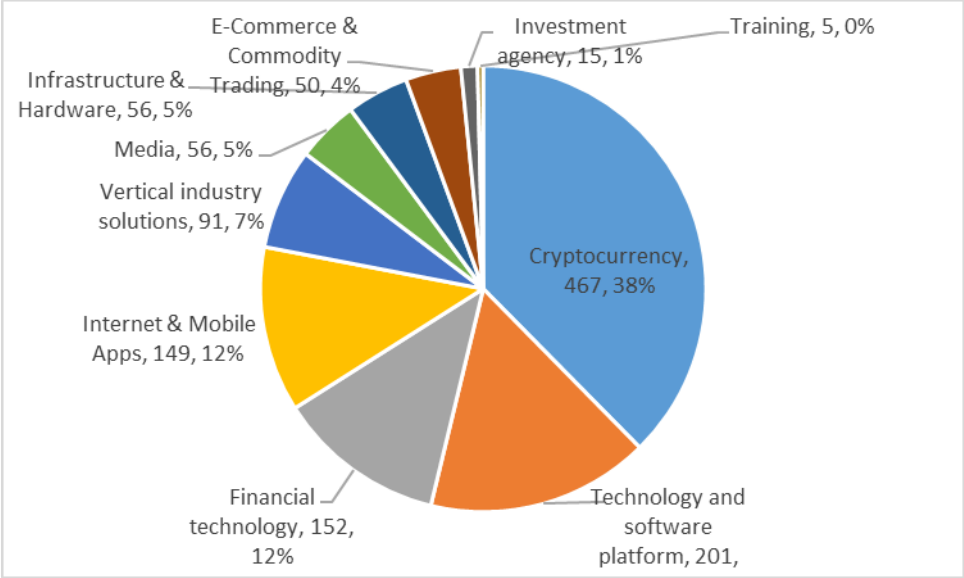


*Figure 7. Number of blockchain companies in various industries,*

*Source：Cbinsight & CrunchBase, July 2018*

From the perspective of investment and financing, financing in global Blockchain industry has accelerated, and the domestic regulatory policy is stricter. On the one hand, financing in Blockchain start-ups (non-ICO financing) reached $4.81 billion in total from 2009 to 2018, as shown in Figure 8. In terms of areal distribution, the United States has a total of $2.542 billion in financing, China ranks the second with $602 million and Canada ranks the third with $247 million. On the other hand, ICO has become a new financing channel, and the rising trend in 2018 remains. From 2014 to 2018, ICO's cumulative financing amounted to $18.09 billion, far exceeding the amount of traditional financing in the same period. Among them, Blockchain start-up EOS financed $4.2 billion on June 1, 2018, making it the largest ICO financing as yet. A few months after China's regulators banned ICO and closed the domestic virtual currency exchange on September 4, 2017, ICO went back in the way of "Exportable goods put on the domestic market" or other patterns in early 2018. And it organized relevant fund-raising activities through agents and middlemen. In this case, People's Bank of China, National Internet Finance Association of China and other institutions prohibited frequently, and more domestic regulatory

measures were introduced. On August 24, 2018, China Bank Insurance Regulatory Commission and the Ministry of Public Security and other five ministries and commissions issued ‘Warnings Regarding Prevention of Illegal Fundraising in the Name of “virtual currency” and “blockchain “‘.” Regulate cryptocurrency and encourage Blockchain technology" is the theme of the development of China's Blockchain.

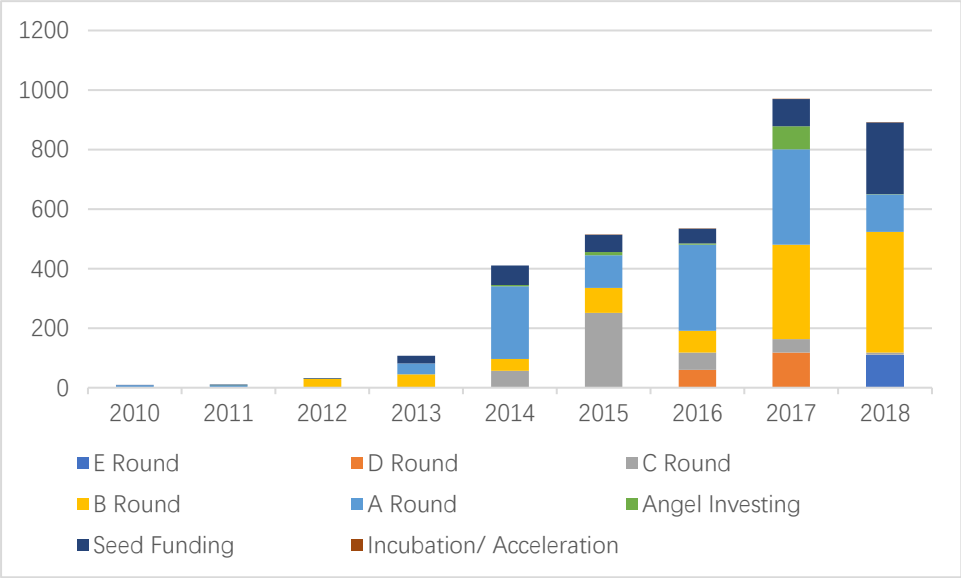


*Figure 8. Distribution of financing rounds in each stage of the blockchain*

*Source：Cbinsigh t& CrunchBase, July 2018*

From the perspective of talent supply, the growth rate of talents in Blockchain cannot meet the market demand. According to the data shown by business networking site LinkedIn in February 2018, the global demand for talents in Blockchain has been increasing since 2015, and experienced explosive growths during 2016 and 2017. However, it still takes a low proportion of the total demand of the global talent market now. In recent years, the fastest growing demand for Blockchain talent came from computer and software industry, followed by the financial services and insurance sector. From 2015 to 2017, candidates who had listed Blockchain skills as a talent on the LinkedIn platform rose by nearly 19 times. However, the total supply of Blockchain talents still remained small, equivalent to

just 2 percent of the total number of global artificial intelligence talents on the LinkedIn platform. According to the current global distribution of talents in Blockchain, the United States accounts for 25%, followed by India with 7% and Britain with 6%. And most talents in the US are in Greater New York (24%), San Francisco Bay (21%) and Greater Los Angeles (10%). Now China's talents in Blockchain are relatively less, They're mainly in Beijing, Shanghai, Shenzhen and Hangzhou.

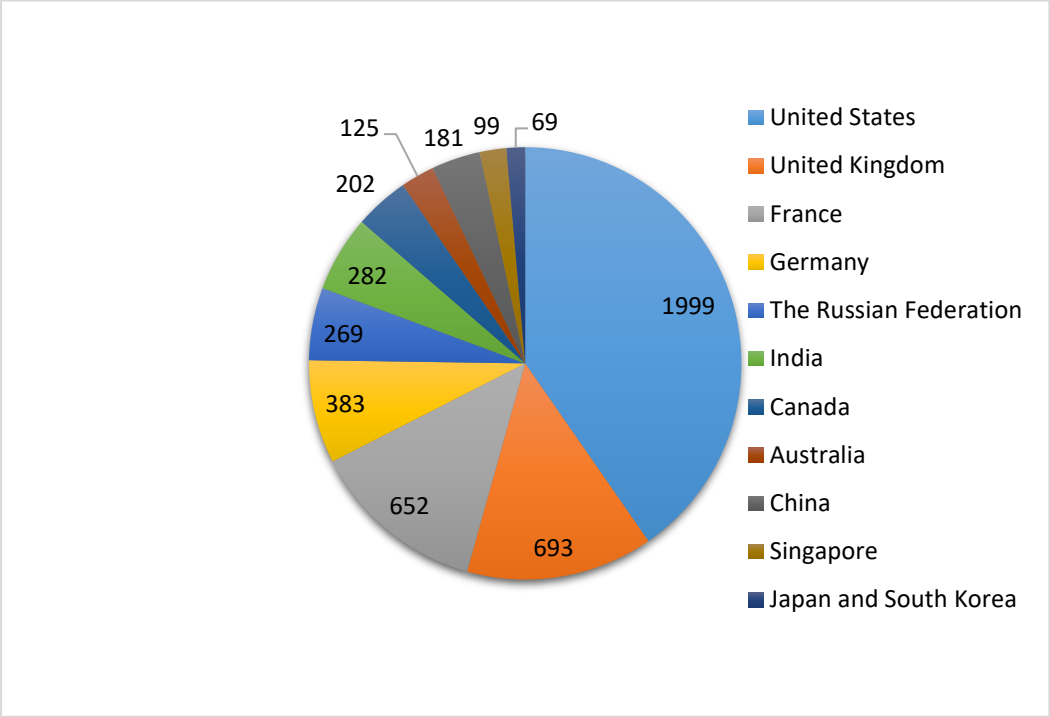


*Figure 9. Proportion of demand for blockchain talent in major countries around the world, Source: LinkedIn, February 2018*

## 3.3 The Innovation of Blockchain Technology Is Becoming More and More Dynamic.

More and more foreign companies have been involved in the development and contribution of Blockchain source code. According to the data on GitHub, the proportion of Blockchain projects in 2010 was less than 1%, but it ran up to 11% in 2017. And there were lots of open source platforms or individual collaboration ecosystem coming into being, such as Bitcoin, Ethereum, Hyperledger and Ripple. At the same time, a number of international Blockchain industry alliances have emerged, such as the R3

Blockchain Alliance (Corda), Hyperledger Blockchain Alliance which supported by the Linux Foundation, the Enterprise-level Ethernet Alliance (EEA) and so on.

In terms of open source code, China's code contribution is only 1/3 of that in the US. As a traditional technological highland, the United States is leading the technology trend in the global open source community by cross-chain technology, multi-party trusted computing, trusted oracle, digital identity, privacy protection, smart contract language and other fields. There are not many independent technology platforms in China, and over 90% of the Blockchain technology platforms use products or fork version made by open source technology abroad, such as Hyperledger or Ethereum.

Unlike the growth in the number of patents, China's contribution to open source declined significantly in 2017 compared with 2016, as shown in Table 9. There were 2,538 open source projects in the United States in 2016 and 1,728 in 2017; while there were only 834 in China in 2016 and 527 in 2017, which were less than 1/3 of those in the United States. It can be seen that the development of Blockchain in China pays more attention to the application level, and there is still a significant gap in the open source and core algorithm between the international leading level and ours.

*Table 10. Comparison of the number of China-US blockchain projects*

| **Country / Region** | | **2014** | **2015** | **2016** | **2017** |
|---|---|---|---|---|---|
| **China** | **National** | 263 | 274 | 834 | 527 |
| | **Beijing** | 67 | 76 | 225 | 137 |
| | **Shanghai** | 62 | 35 | 134 | 119 |
| **USA.** | **National** | 1906 | 1920 | 2538 | 1728 |
| | **San Francisco** | 389 | 318 | 227 | 150 |
| | **New York** | 150 | 161 | 208 | 147 |

In terms of patent application, the number of patent applications in the field of Blockchain has ranked first in the world. According to the analysis data of the platform Incopat, by July 2018, the number of global patents related to Blockchain reached 3731, and it increased by 87% in 2017 compared with 2016. As shown in Figure 10, China is currently the country with the largest number of patent applications for Blockchain with the cumulative number of 2002, and the US has 1076. At present, there are 376 patent applications related to cryptocurrency and 286 patent applications for smart contracts in global Blockchain patent applications. In several consensus algorithms, the PoW algorithm is the earliest and the patent applications are more than other algorithms. From the perspective of areal distribution, the US has a large number of patent applications in the fields of cryptocurrency, smart contracts and PoW algorithm. And China has the highest number of patent applications in the field of smart contracts.

In terms of patent application, the number of patent applications in the field of Blockchain has ranked first in the world. According to the analysis data of the platform Incopat, by July 2018, the number of global patents related to Blockchain reached 3731, and it increased by 87% in 2017 compared with 2016. As shown in Figure 10, China is currently the country with the largest number of patent applications for Blockchain with the cumulative number of 2002, and the US has 1076. At present, there are 376 patent applications related to cryptocurrency and 286 patent applications for smart contracts in global Blockchain patent applications. In several consensus algorithms, the PoW algorithm is the earliest and the patent applications are more than other algorithms. From the perspective of areal distribution, the US has a large number of patent applications in the fields of cryptocurrency, smart contracts and PoW algorithm. And China has the highest number of patent applications in the field of smart contracts.

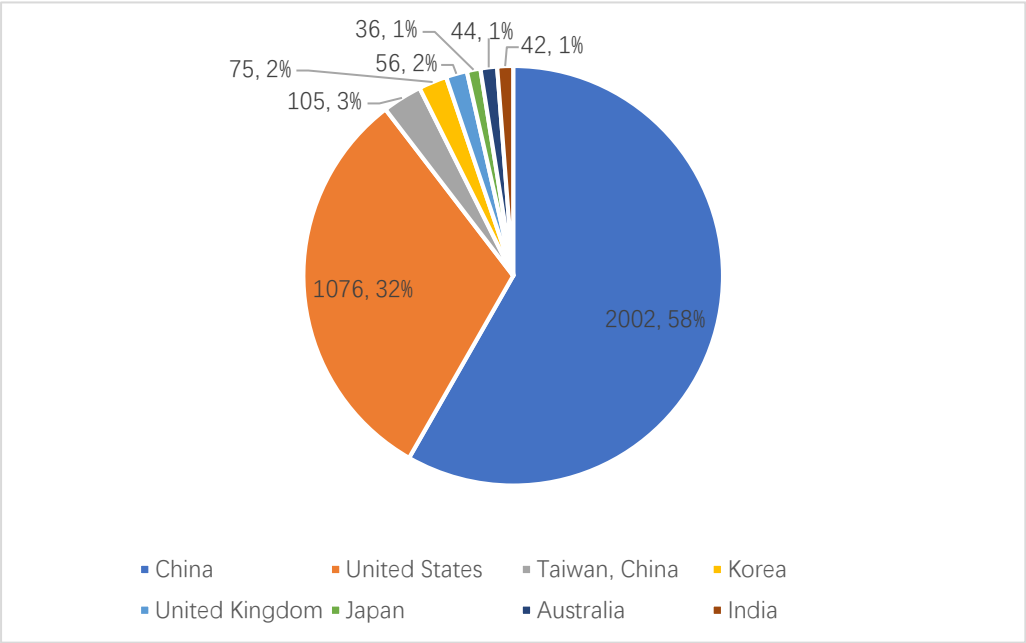


*Figure 10. Blockchain distribution in various countries. Source: Incopat, July 2018*

In scientific research, foreign research attaches more importance to technological breakthroughs of core issues, while domestic research pays more attention to the business scenarios of Blockchain applications. According to the survey data of China Academy of Information and Communications Technology in July 2008, global research institutes began to pay more attention to the Blockchain from 2015. In 2017, the number of SCI papers on the Blockchain collected by Web of Science reached 445, it was an increase of 181.6% compared with 2016, as shown in Figure 11. Institutes in France, Denmark, Portugal, Australia and the United Kingdom are also actively engaged in research. By April 2018, 27 universities worldwide, including the Massachusetts Institute of Technology (MIT), the University of California, Berkeley and Imperial College of Technology, have explicitly set up courses related to Blockchain or offered relevant training courses to study Blockchain, as shown in Figure 12. A number of academic institutions and project teams have sprung up in the mainstream foreign universities from various perspectives, such as performance, technology and application. The form of Industry-University-Research Collaboration could cultivate talents in a positive way. Domestically, some industry organizations carry out the Blockchain training camps,

Blockchain president classes with the theme of popularization and application. Besides, colleges and universities are also making progress gradually in the area of Blockchain. In July 2016, the Central University of Finance and Economics established the first Blockchain laboratory in China and offered relevant courses on Blockchain. In April 2018, Xi'an University of Electronic Science and Technology offered the course of "Block Chain Technology Principle and Development Practice", while the School of Computer Science of Zhejiang University offered the Blockchain Research Center. At present, there is still a lack of systematic research on key technologies and core issues in China, and the Industry-University-Research Collaboration has not yet formed.

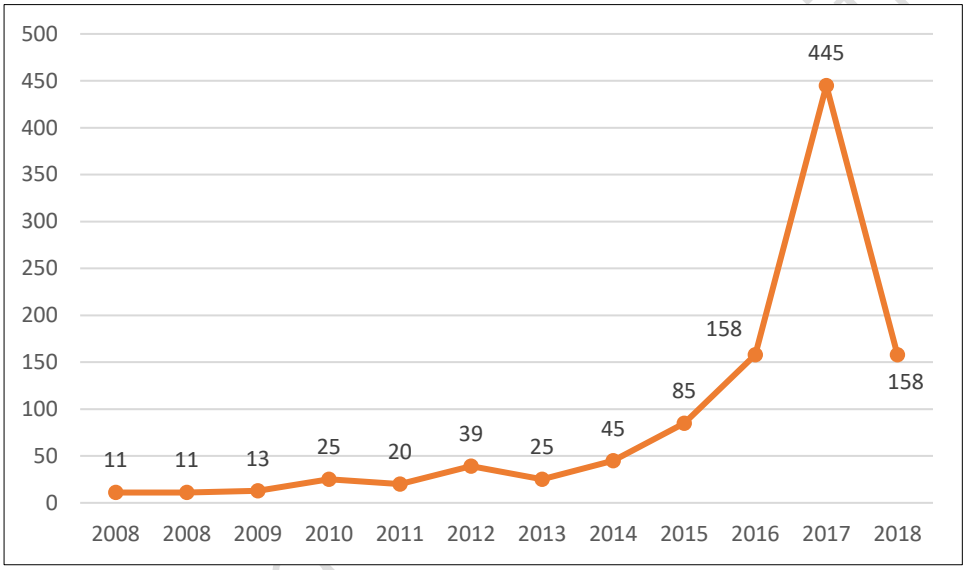


*Figure 11. Number of Blockchain SCI papers published in each year. Source: Web of Science, July 2018*

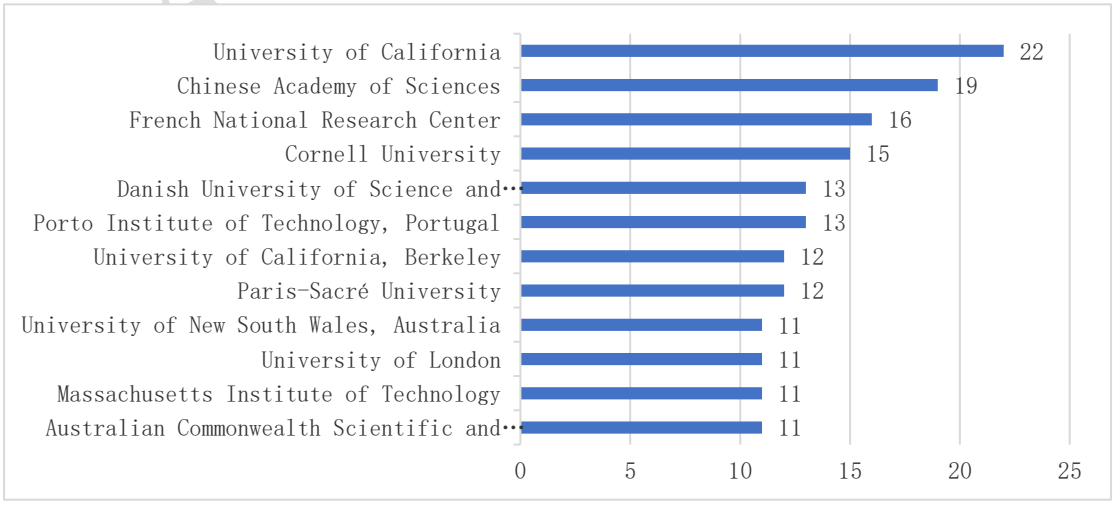


*Figure 12. The charts of Blockchain SCI papers publishing agency. Source:*

*Web of Science, July 2018*

## 3.4 Speeding Up to Establish Blockchain Standard System

The World Economic Forum survey predicts that 10% of global GDP over the next seven years will be preserve based on the Blockchain technology. In order to promote the benign development of Blockchain industry, many international organizations have actively explored the construction of Blockchain standard system. The ITU-T Standardization Unit (ITU-T) decided to launch the standard study of F.DLS (Distributed Accounts Service Requirements) in February 2017. ITU-T FG DLT Focus Group was established in May 2017, and a new research topic Q22（Distributed ledger technologies and e-services) was set up at the ITU-T SG16 Plenary Meeting in July 2018. China is the main contributor to the research of ITU-T Blockchain Standards. Four international standards including Blockchain Requirements, Reference Framework, Evaluation Benchmarks have been set up by the Institute of Information and Communications of China, and have received active support from all over the world. The International Organization for Standardization (ISO) also established the Blockchain and Distributed ledger Technical Committee (ISO/TC 307) in September 2016.The main work is the development of international standards in the field of Blockchain and Distributed ledger Technology, and the study of problems related to the standardization of Blockchain and Distributed ledger Technology in cooperation with other international organizations. In addition, organizations such as the World Wide Web Consortium (W3C), the Association of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Task Force (IETF) are also actively focusing on the standardization of Blockchain.

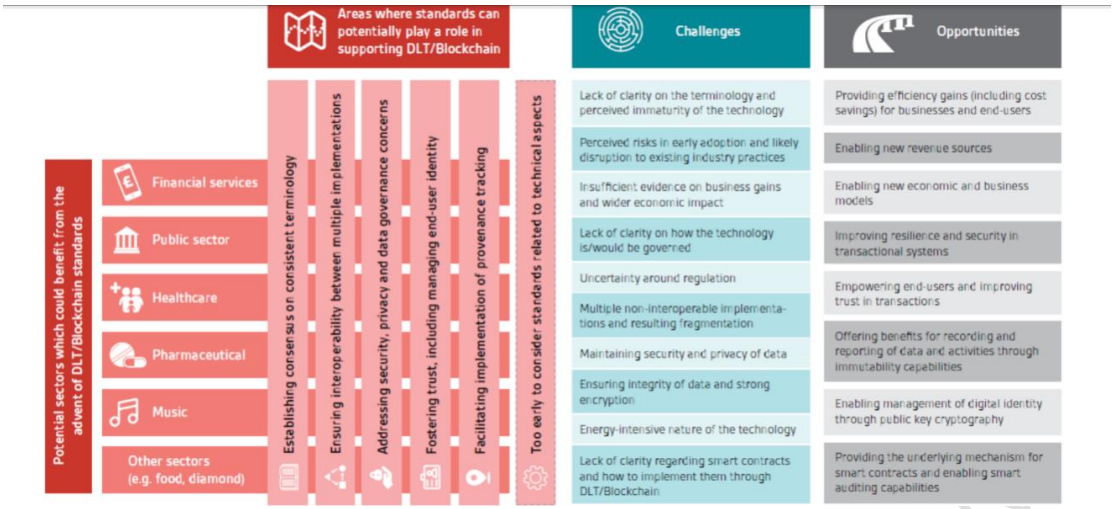


*Figure13. Blockchain standard SWOT analysis. Source: BSI & RAND Europe, May 2017*

Blockchain technical standards will be a breakthrough to accelerate the development of the whole Blockchain industry. However, there is no consensus on the Blockchain standard system as yet. Trusted security has become a key element in the future development of Blockchain technology standards, as described in the report *"Distributed Ledger Technologies/Blockchain：Challenges, opportunities and the prospects for standards"* published jointly by the British Standards Association and Rand in 2017. Details are shown in Figure 13. At present, China is actively promoting the transparency of Blockchain industry, and building a standardization system including trusted Blockchain standards. After a long-term tracking study, combined with ideas of the existing standardization in cloud computing, big data and so on, the China Academy of Information and Communication has proposed the first series of trusted Blockchain standards in China. The China Communications Standardization Association (CCSA) has launched two industry standards. Three Trusted Blockchain evaluation criteria have been released and a Trusted Bench Blockchain Benchmark tool is being developed. Trusted Blockchain evaluation criteria includes 19 targets and 95 evaluation points, covering functions, performance, security and other aspects. In April 2018,

the China Academy of Information and Communication jointly launched the "Trusted Blockchain Promotion Plan" with 158 units to promote the development and application of Blockchain technology and the benign development of the industry.

# 4 Challenges Blockchain are facing

## 4.1 Hidden dangers at the mature level of Blockchain technology

At present, the Blockchain technology is not mature in terms of system stability, application security, business model and so on. There are five main problems: the performance cannot meet the three requirements of "high efficiency with low energy", "decentralization" and "security" simultaneously. The transaction throughput that can be performed on the Blockchain is not high, and it's difficult to meet the needs of the high-frequency service; From the perspective of energy consumption, the consensus algorithm such as Proof of work have high energy consumption and high cost, which makes the Blockchain waste a lot of network computing power and resources; From ecological point of view, the current Blockchain products are immature, it lacks of relevant development, integration, operation and maintenance system, and it's short of standards as well. China doesn't have too much right and influence on Blockchain open source platform; As for the security , Blockchain is facing a grim situation of platform security and application security which including privacy protection, harmful information, smart contract vulnerabilities, consensus mechanism and private key protection, 51% computational attack, cryptographic algorithm security and so on; From the perspective of the supervision · encryption technology has posed great challenges to legal monitoring, customer identification, anti-money laundering and other regulatory means. At the same time, multi-party collaborative governance of Blockchain also puts higher requirements on supervision.

## 4.2 The application scenario model is unclear.

Along with the "Blockchain" turmoil, not only industrial technology giants such as BAT have focused more on it, but more and more traditional companies have also officially entered the Blockchain industry. At the same time, because of the low cost and low investment threshold of starting a business, a large number of start-ups are rushing to enter the market. However, on the one hand, the immaturity of technology restricts the commercial application. At present, although there are many kinds of Blockchain core technologies such as privacy protection algorithm, consensus mechanism, etc., they are not commercially available. On the other hand, the application mode of Blockchain is still being explored, and no real "killer" application has been found. The "irreplaceable" advantage of Blockchain has not been reflected. Blockchain is not required and cannot be applied to all fields. Its outstanding features make it more valuable for risk-free, high-value and easy-to-implement scenarios.

## 4.3 Industry professionals are relatively scarce.

Blockchain technology is a multidisciplinary and cross-disciplinary technology that includes operating system, network communication, cryptography, mathematics, finance, production and so on. At present, China still has some shortcomings in cross-disciplinary and interdisciplinary fields. The research and development of Blockchain technology mainly concentrated in programming languages like Go, JavaScript, C and C++. The new smart contracts use Haskell, Ocaml, Rholang and other new functional programming languages, so there is a very big gap about technical talents who has relevant language and senior R&D experience in the global talent market. Compared with R&D technical talents, Blockchain underlying system architecture designers have to master a number of interdisciplinary professional skills and have an in-depth understanding of the underlying design principles of

Blockchain. Besides, they should have experience in system architecture design, and understand the specific business logic of the application scenario, which can be described as "it`s hard to find a general". Although some colleges and universities have set up interdisciplinary education and special skills disciplines of Blockchain, professional talents are still scarce in the market.

## 4.4 Relevant laws and regulations need to be improved

Although Bitcoin and Ethereum have become hot topics, there are still no clear laws and regulations in this field. The governance, supervision and standards of Blockchain technology are still not perfect, which mainly reflects in two aspects: first, the legal subject is not clear. The body of system maintenance and governance in the Blockchain is not clear. There is no central organization responsible for the whole system in the Blockchain system. The lack of centralized legal entities also makes it difficult for the traditional legal rules to post-accumulate the distributed ledger system. To carry out supervision, effective supervision must be promoted with the technical rules in advance. Second, the rules on the chain are not clear. In the context of Blockchain participants, code is "law", but law is not code. Unlike the legal rights and obligations, the technical rules of Blockchain directly determine the security and stability of Blockchain system, and directly affect the rights and obligations of each participant. Due to the ambiguity of the rules on the chain, a series of problems will arise about smart contract vulnerabilities, token issuance compliance, personal information protection and so on.

# 5 Some Measures and Suggestions for Development

## 5.1 Guide the public to learn Blockchain objectively and rationally

We should actively guide the society and the public to view the value of Blockchain objectively and rationally. On the one hand, we should fully recognize the importance of Blockchain technology in building trust mechanisms, transmit information and value. On the other hand, we should avoid exaggerating the subversive influence of Blockchain technology on traditional industries, and be aware of the expansion of bubbles. Attention should be paid to the impact caused by Blockchain application to traditional institutional management, business operations and other modes, as well as operational pitfalls, technology monopoly and other potential risks. And we should promote the related medias to radically reform their statements and create a clean and positive atmosphere for the industry to make an excellent communication environment for subversive technologies like Blockchain.

## 5.2 Strengthen the research on core technology

We will accelerate the research and development of key technologies on Blockchain, including consensus mechanism, cryptography algorithm, cross-chain technology and privacy protection, and conduct product development and integration testing. And we should support and foster open source software, build an independent open source community, and build an ecological system for the co-development of software and hardware. We also need to comply with the actual needs of the technology industry and appropriately promote the formulation of standards. Besides, it’s also necessary to build innovative platforms for basic research and interdisciplinary research and to train composite talents with

interdisciplinary, knowledge fusion and technology integration. What's more, we need to establish and improve the coordinated promotion mechanism of universities, research institutions, industry associations and think tanks, and strengthen the coordination and cooperation in tackling key technical problems, breaking through bottlenecks and setting standards.

## 5.3 Promote deep integration with the real economy

To promote the deep integration of Blockchain technology and real economy, first, we should explore and highlight the irreplaceable role of Blockchain technology in building trust relationships, improving collaboration efficiency, promoting data sharing and enhancing the government's penetrating supervisory capacity. Second, we should explore the innovation mode of digital economy, realize the supply and demand docking, and serve the transformation and upgrading of the real economy. Next, we have to select key areas, organize and carry out the concept verification, test platform, pilot application demonstrations and assessments of Blockchain applications to cultivate industry leaders who will lead enterprises and industry ecosystems. Finally, combined with good application case demonstrations, we should conduct Blockchain technology and application training for industry organizations and enterprises to popularize and apply landing experience, and avoid potential application risks.



## 5.4 Improve the policy environment of Blockchain development

Following the routine of technological development, we should make systematic arrangements from the policy level. The impact of Blockchain on personal information protection and cross-border data flow will be studied in depth, and the regulatory issues of Blockchain in the underlying core technology, middle-level application logic and upper-level

information management and control are discussed. And we will actively promote the information disclosure of the participants in the Blockchain system, build a compliance review and audit mechanism for smart contracts, and promote industry self-discipline. At the same time, relevant policies and laws and regulations of the Blockchain should be studied, and the supervision mechanisms and certification systems for the technology and application of the Blockchain should be explored to create a good environment for the healthy development of the industry.