Technology Development and Application of Blockchain: Current Status and Challenges

Article · January 2018

DOI: 10.15302/J-SSCAE-2018.02.005

3 authors, including:

Lingjun Fan
Chinese Academy of Sciences
13 PUBLICATIONS **17** CITATIONS

DOI 10.15302/J-SSCAE-2018.02.005

Technology Development and Application of Blockchain: Current Status and Challenges

Sun Yi[1,2], Fan Lingjun[1], Xuehai Hong[1]

1. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
2. University of Chinese Academy of Sciences, Beijing 101407, China

Abstract: Blockchain, as the backbone of the future "Internet of Value," is considered to have the potential to considerably alter the economy and society that we have today. This paper focuses on explaining the state-of-the-art of blockchain technology and its applications, especially presenting the challenges of using blockchain widely in different domains and from the perspective of technology. We conclude this paper by providing suggestions for enforcing the further development of blockchain technologies in China.

Keywords: high-throughput blockchain; consensus protocol; smart contract; cross-chain communication

1 Introduction

A blockchain is a data structure in which blocks are grouped together in a chain. Each block is connected to a previous block by a hash, thus enabling traceability; meanwhile, cryptography is used to guarantee that the block data cannot be tampered with and cannot be forged. The creation of each block is dependent on the consensus of participants in the sequence of events and the current state of the entire system's transaction records. Each participant can record and store data, and can have backups of the entire blockchain data. Thus, without a central control node, a distributed peer-to-peer network has been built. Therefore, blockchain technology has many advantages such as decentralization, trustlessness, tamper resistance, and traceability.

Blockchain technology originated from the groundbreaking paper "Bitcoin: A Peer-to-Peer Electronic Cash System" published in 2008 by a scholar named Satoshi Nakamoto. As the underlying implementation technology of Bitcoin, blockchain is a distributed ledger technology (DLT). Owing to its advantages of decentralization, trustlessness, and tamper resistance, this technology is considered to be the future of the "Trusted Internet" and "Value Internet." The supporting technology is becoming the most popular topic in the global innovation field and is highly sought after by the investment community, academia, industry, and government. Although governments have different attitudes toward Bitcoin and various virtual currencies, they have a positive attitude toward blockchain technology.

In recent years, organizations such as the United Nations, the International Monetary Fund, and several developed countries have issued a series of reports on blockchain, exploring blockchain technology and its applications. At present, the application field of blockchain technology has extended beyond the financial field to include the fields of supply chain, credit information, identity authentication, charity, and the Internet of Things. Start-ups have sprung up, and a white paper on the development of blockchain industry released by the Wuzhen Think Tank in 2017 pointed out that, since 2012, the number of global blockchain companies has grown rapidly with a compound growth rate of more than 65.2%. An optimistic forecast is that by 2025, 10% of the global GDP will be stored using blockchain technology. Ac-

Received date: March 22, 2018; **Revised date:** March 30, 2018
Corresponding author: Sun Yi, Institute of Computing Technology, Chinese Academy of Sciences, Researcher. Major research fields include blockchain and Internet service. E-mail: sunyi@ict.ac.cn
Funding program: CAE Advisory Project "Research on Development Strategy of 'Internet Plus' Action Plan"(2016-ZD-03); Project of National Natural Science Foundation of China (61772502, 61672499)
Chinese version: Strategic Study of CAE 2018, 20 (2): 027–032
Cited item: Sun Yi et al. Technology Development and Application of Blockchain: Current Status and Challenges. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2018.02.005

cording to Digital Marketing Ramblings (DMR), the blockchain industry is expected to reach 20 billion US dollars by 2024.

2 Industrial application status

As the birthplace of Internet technology, the United States has invested heavily in blockchain technology and applications. In 2017, at least eight states in the United States proposed and studied bills that promote the application of blockchain technology. In February 2018, the US House of Representatives held two blockchain hearings in succession to explore new applications of blockchain technology. The US State Department emphasizes transparency through blockchain technology to address corruption, fraud, or misappropriation of public procurement funds. The US Treasury is conducting a pilot program to determine whether blockchain technology can be used for supply chain management, and has also taken measures to improve the "Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)" law against blockchain-based cryptocurrencies and to form public-private partnerships (PPPs) with financial institutions to share information. South Burlington, Vermont, will try blockchain technology to record real estate transactions. California lawmakers have filed a bill that, if passed, the state's electronic record law will approve blockchain signatures and smart contracts. New York State Power Company TransActive Grid proposed a new energy concept based on a blockchain-based P2P distributed microgrid network, establishing a microgrid network through blockchain and improving clean energy utilization. Remaining power could be recorded on the blockchain and sold to neighboring users via smart contracts.

In January 2016, the British government issued a report entitled "Distributed Ledger Technology: Beyond the Blockchain." The report points out that blockchain technology has great potential to transform public and private services. In addition to creating a public platform based on blockchain to serve the entire population and society, the UK government plans to develop an application system that can be used between government and public agencies. The Japanese government has strongly supported the blockchain and digital currency industries and established the first blockchain industry organization, the Japan Blockchain Association (JBA), and the Blockchain Cooperation Alliance. Russia is vigorously promoting the construction of a blockchain infrastructure. Sberbank, Russia's largest bank, has cooperated with the government to transfer and save documents with blockchains, becoming a real application case for blockchains. Canada has a large blockchain entrepreneurial community that brings together a large number of top block talent including Ethereum founder Vitalik Buterin. The Canadian Securities Regulatory Commission (CSA) has proactively launched a new "Fintech Sandbox" program to promote the development of the Canadian blockchain industry.

Blockchain technology originated in the open-source community and grew stronger afterward. It has gradually attracted the attention of financial institutions, IT giants, and other institutions. For example, the open-source projects represented by Bitcoin and Ethereum focus mainly on the public chain and creating a blockchain public platform. The Linux Foundation's Hyperledger project, launched in 2015, focuses on the research of consortium chain technology. At the same time, IBM, Microsoft Azure, Amazon Web Services (AWS), and other Internet international giants are struggling to build infrastructures that support blockchain applications and blockchain as a service (BaaS).

Since 2016, the Chinese government has also paid attention to and supported the development of blockchain technology and industry. In October 2016, the Ministry of Industry and Information Technology released the "White Paper on China's Blockchain Technology and Application Development (2016)" [1]. In December of the same year, the blockchain was first used as both a strategic frontier technology and a subversive technology in the State Council's "13th Five-Year Plan" national informationization plan. The plan clearly states that it is necessary to strengthen the innovation, experimentation, and application of new technologies such as blockchains in order to achieve the preemption of the new generation of information technology.

The People's Bank of China established the Digital Currency Institute in 2017 to study the digital currency issuance and the commercial operation framework that supports blockchain technology. The blockchain-based digital bill trading platform of People's Bank of China entered the trial operation phase in early 2017, and the test was successful. In addition, Tencent, Alibaba, and other well-known domestic Internet companies are also actively deploying blockchain technology. There are more than 100 blockchain startups in China, mainly aiming at the development of blockchain infrastructure technology and its applications to credit, supply chain, asset management, Internet of Things, and other industries. From 2008 to 2017, the number of patent applications in China's blockchain technology field ranked first in the world with a total of 550 patent applications filed, surpassing the second-ranked US (284).

3 Technical challenges

Bitcoin is the first successful application of blockchain technology. As of now, the Bitcoin blockchain system has been in operation for more than eight years. Except for a limited number of forks, there have been no major security incidents, which fully demonstrates its strong stability and security. Most of the current applications of blockchain technology are still concentrated in the financial field, such as digital currency, cross-border payments, securities trading, property registration, and certification. However, in the future, large-scale promotion and application in the financial field will also need to overcome problems such as performance issues and regulatory issues.

In the supply-chain field, through blockchain, all parties in a

supply chain can use a transparent and reliable unified information platform to view the status of the supply chain in real time and trace the entire process of production and delivery of goods, thereby improving the efficiency of supply chain management and reducing logistics costs. Tracing and proofing becomes easier when disputes arise. However, supply chain management often involves many entities, including logistics, capital flow, and information flow. There are many complex collaboration and communication issues between these entities. There are also many technical problems that need to be tackled with regard to applying the blockchain to effective off-chain coordination.

In the manufacturing fields, Industry 4.0 applications can use blockchains to record every step of the production process. For different participants in the production process, different permissions are used to access the blockchain in a more reliable and secure manner. Participants extract relevant information and confirm the steps in the production process. However, different terminals and sensors should participate in the blockchain network for coordination and verification. The computing power and storage of current IoT terminals and sensors are difficult to support, and the real-time coordination of blockchain networks needs to be improved and optimized.

In the energy field, blockchain-based microgrid networks have scalability issues and energy consumption issues for verifying transactions. In addition, owing to the limited storage capacity of the blockchain itself, when it is applied to social, e-commerce, and other fields, it is necessary to consider the storage problem of a large amount of data, transaction efficiency issues, and the like.

The current blockchain industry is developing at a high speed, and blockchain technology has been applied more and more. However, in the field of basic research, relevant research work is still in its infancy, and the technical challenges of blockchain architecture, consensus algorithms, privacy protection, smart contracts, cross-chain transactions, etc., are increasingly restricting the development of blockchain technology and its industry. Finding effective solutions as soon as possible, realizing key technological breakthroughs, and strengthening the theoretical foundation and key technologies are the key points in the current wave of blockchain development.

3.1 Research on blockchain architecture

The blockchain architecture is the basis of the operation of the blockchain system. However, as the number of users and the system scale increase, problems such as low throughput, long transaction confirmation time, the slow access speed of consensus nodes, and waste of storage resources worsens, seriously affecting the blockchain's utilization and industry expansion. In recent years, industry and academia have carried out preliminary research work in designing blockchain architecture, albeit on a small scale.

Parallelization architecture: Blockchain sharding technology (Sharding) adopts the parallelization idea to divide users into different network shards and process disjoint transaction sets in parallel to improve overall performance. However, when dealing with transactions involving different shards, it is necessary to go through complicated cross-shard communication, which is very expensive. Plasma uses a sidechain hierarchy tree to divide the entire network, and uses "divide and conquer" to expand the transaction scale.

On-chain and off-chain collaborative architecture: Based on a Bitcoin-like blockchain, the Lightning Network proposes to place the transaction process as much as possible off-chain for fast transactions, while on-chain transactions will be used only for guarantees and settlements. In essence, the Lightning Network does not improve the performance of on-chain trading, and off-chain trading is not stored in the blockchain, which will affect the traceability of the transaction. As the "Ethereum version" of the Lightning Network, the Raiden Network can be combined with Sharding and Plasma to further enhance transaction processing capabilities.

New architectures such as parallelization and on-chain off-chain collaboration provide new research directions for solving the problem of blockchain performance and resource occupation. However, this research work is still in a relatively early stage. Many specific problems such as the rational fragmentation of parallel architecture, cross-chip communication, decentralization, and traceability of on-chain off-chain collaboration lack efficient algorithms and mechanisms.

3.2 Research on blockchain consensus algorithm

The blockchain consensus algorithm ensures that each node in the blockchain system can maintain the same transaction content and order, which is the core mechanism of the blockchain system. Currently, widely used consensus algorithms include Proof of Work (PoW), Proof of Stake(PoS), Delegated Proof of Stake(DPoS), and the Byzantine Fault Tolerant Algorithm (PBFT) [2], each of which has advantages and problems (Table 1).

In recent years, in order to meet the needs of practical applications, some new consensus algorithms have been proposed. Algorand randomly selects a set of verifiers to use the optimized Byzantine protocol for consensus to improve consensus efficiency through a password-draw mechanism [3]. Bitcoin-NG released a transaction block by the selected leader of the workload, which improved the performance of the Bitcoin blockchain PoW consensus to some extent [4]. Casper raised the security and decentralization of the PoS algorithm by locking the margin certifier's bet consensus.

However, both the classic consensus algorithms such as PoW and PBFT and the new algorithms such as Algorand and Bitcoin-NG are facing a trilemma. That is to say, the blockchain

Table 1. Comparison of popular consensus algorithms.

Consensus algorithms	Security	Network scale	Resource consumption	Transaction confirmation time	Transaction throughput	Fork	Decentralization
PoW	High	Large	High	long	Small	Easy	A little high
PoS	A little high	Large	Medium	Medium	Small	Easy	A little high
DPoS	General	Large	Low	Short	General	Not Easy	Low
PBFT	General	Small	Low	Short	General	Not Easy	General

system can only optimize two of the three objectives of decentralization, high performance, and security at the same time. The optimal solution for the trilemma will be the main research direction and technical challenge in the future.

3.3 Research on blockchain privacy protection

Blockchain privacy protection solves the problem of account privacy leakage caused by open transaction information. At present, it mainly realizes the direct or indirect hiding of user key information. Typical privacy protection technologies include CoinJoin, Stealth Address, Ring Signature [5], and the zk-SNARKs zero-knowledge proof algorithm [6].

CoinJoin, Stealth Address, and Ring Signature technology are only indirect hidden key information involved in the transaction, and there are deficiencies in their reliability. Although the zk-SNARKs zero-knowledge proof algorithm is directly hidden information, it has "trustworthy public parameters" and inefficiencies. At the same time, the continuous development of quantum computing puts forward new requirements for privacy protection research, and these typical privacy protection technologies are not resistant to quantum attacks. The newly proposed zk-STARKs completely rely on hash and information theory, thus solving the "trustworthy setup" problem of zk-SNARK, and have the ability to resist quantum attacks. However, this research is in its early stage, and the technology is still immature and has drawbacks such as too-large evidence. Therefore, the design of technical solutions that can ensure high efficiency and security, as well as guarantee concealing of key transaction information and validity verification of transactions, is still the main technical challenge facing future blockchain research.

3.4 Research on blockchain smart contract

Nick Szabo first proposed the concept of smart contracts in 1996. A smart contract is a set of conventions defined in digital form, including agreements on which contract participants can enforce these conventions. The blockchain provides a decentralized, non-tamperable, and transparent operating environment for smart contracts so that smart contracts can be automatically executed according to a default contractual agreement without trusting a third party. At present, the research on smart contracts mainly focuses on smart contract virtual machines, smart contract upgrades, and credible feeding of off-chain data.

Smart-contract virtual machines can be divided into two categories: autonomously controllable virtual machines, such as the Ethereum Virtual Machine (EVM), and virtual machines that use existing mature compiling and running environments, such as the Java Virtual Machine (JVM). A virtual machine using an existing mature compiling and running environment has higher efficiency, but there are more uncontrollable factors, and current self-controllable virtual machines such as EVM still have significant operating efficiency problems. The current research work mainly includes optimization of the Solidity compiler, the WebAssembly (WASM) execution environment development for smart contracts, etc., all of which are in the early stages of research.

Smart contracts are computerized trading protocols for real-world contracts. In the development of smart contracts, developers cannot take all circumstances into consideration. When the smart contracts on the chain do not work as expected, they need to upgrade the smart contracts, and the behavior of smart contracts needs to be explained. Corda proposes combining the legal text of the contract with the code and storing it on the chain. When the contract code has an unexpected behavior, the legal text will prevail, but there is still a lack of flexibility for code upgradeability. Thus, a scalable and interpretable smart-contract complete solution is the key to the large-scale application of smart contracts.

Smart contracts are stored and run on blockchains, and their association with real-world activities off-chain is a prerequisite for their large-scale application. Oraclize links smart contracts with Web APIs through cryptographic proofs, enabling smart contracts to obtain real-world activity data without additional trust; IC3 proposes the Trusted Data Feeding System Town Crier (TC), which provides authentic, credible, and confidential data to smart contracts through Intel's latest trusted hardware SGX. However, existing trusted data feeding solutions are less flexible. For example, Oraclize needs to return the entire https request responses and relies on a centralized off-chain server. TC cannot support updates to the code. We need to study new, flexible, and reliable data feeding programs to meet the smart contract's feeding needs for off-chain data.

3.5 Research on cross-chain communication

As blockchain technology is widely used in the fields of encrypted digital currency, asset tracking, identity management,

etc., many discrete blockchain systems have emerged. These independent blockchains need to trade with each other to maximize value, and it is necessary to study cross-chain communication technology. Solving the problems of validity, scalability, and atomicity in cross-chain transactions is the research focus of current blockchain cross-chain communication technology.

At present, the representative programs of blockchain cross-chain communication technology research include Paired Communication, Interledger, Cosmos, and Polkadot. Paired Communication proves the validity of cross-chain transactions without external participation by obtaining the block headers of the other blockchains and the simplified payment verification (SPV) proofs of the specific transaction. Interledger builds a connector to find a way to transfer money to the recipient, and funds are transferred between the connectors to achieve cross-chaining. Cosmos utilizes Hub and Zone. When the source Zone and the destination Zone perform cross-chain transactions, the Hub forwards the packets formed by the Zones across the chain. Polkadot's vision is to achieve cross-chains between heterogeneous blockchains, while transactions can be performed in parallel on different blockchains, thus increasing system throughput.

Most of the abovementioned cross-chain communication schemes are oriented to a specific scenario across the chain and have low scalability. For example, paired communication is limited to transaction presence verification, and Interledger and Cosmos are only used for the single function of cross-chain transfer. Although Polkadot supports a richer cross-chain type, it is still in a very early stage of design. As the demand for cross-chain transactions continues to increase, it is extremely imperative to implement a safe, efficient, and versatile cross-chain technology solution.

4 High-throughput blockchain

Performance issues are one of the important bottlenecks that limit the future large-scale application of blockchain technology. The current widely used public chains (such as Bitcoin and Ethereum) and consortium chains (e.g., HyperLedger) are not able to support high-frequency trading scenarios. There are several orders of magnitude differences in throughput and the actual demand for high-frequency transactions (such as payments and a large-scale Internet of Things). In order to make up for this gap, the Institute of Computing Technology at the Chinese Academy of Sciences (ICT, CAS) has carried out research on high-throughput blockchain technology.

Different from the existing performance optimization work that mainly focuses on the protocol and algorithm levels [2–4], the research on high-throughput blockchain technology being conducted by ICT, CAS focuses on technical breakthroughs at the underlying architecture level, including the blockchain infrastructure and the supporting hardware architecture of the blockchain system. First, with regard to the blockchain infrastructure, by constructing a transaction graph, the original blockchain is divided into many slices, and the transaction records of different slices are processed in parallel. The on-slice consensus uses pipeline technology and random rotation to optimize the consensus efficiency. The accounting node aggregation mechanism ensures security while improving efficiency. For cross-slice transactions, the InterChain cross-slice communication architecture (Fig. 1) was designed to enable cross-slice communication of transactions through the collaboration of the slice gateway nodes and the Interchain nodes. Second, in the hardware architecture, as the efficiency of the existing general-purpose computing architecture is insufficient, and the dedicated chip is only for the limited application of a specific algorithm, we propose a dedicated chip architecture that supports custom algorithms (Fig. 2). By abstracting the computing kernels of various consensus and verification algorithms, a chip architecture based on a loosely coupled computing kernel is designed, and the fault tolerance of the blockchain algorithm itself is used to simplify the functional unit design, thereby improving the computational throughput.

5 Policy suggestions

At present, China's investors, industry, academia, and government have paid significant attention to blockchain technology. However, just like at the beginning of the development of the Internet in the past, there are bad and good blockchain projects. The Hype Cycle, published by Gartner, a well-known information technology research and consultancy firm, believes that the development of any technology must go through five stages: an initial period, an expansion period of hot speculation, a period with a trough of disillusionment, a steady climb period, and a mature real industry period. Technologies such as cloud computing, big data, and virtual reality all developed in this way, and blockchain technology will not be an exception. After two years of hot selling, blockchain technology must undergo solid technical

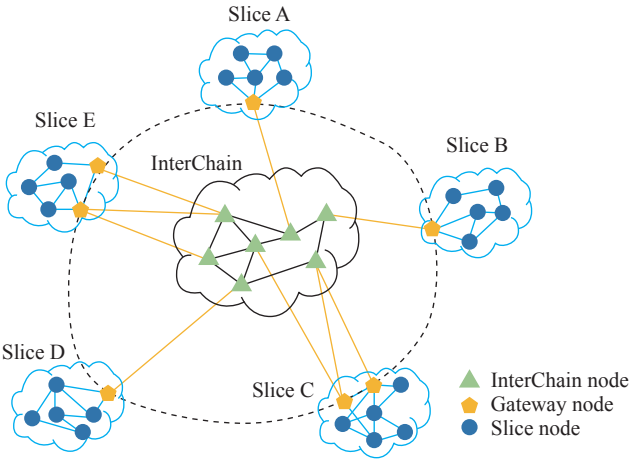

Fig. 1. InterChain cross-slice communication architecture.

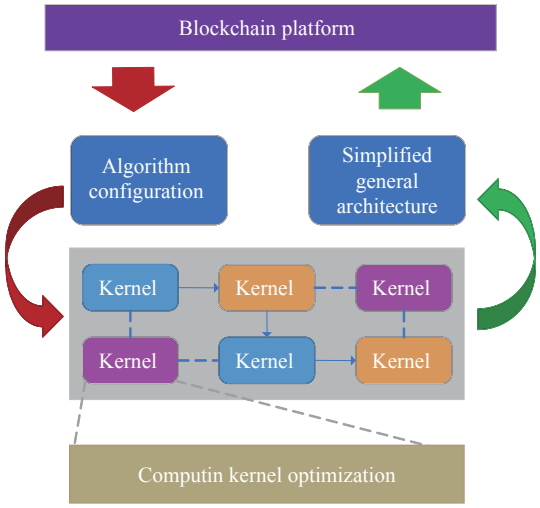

Fig. 2. Optimization of high-throughput blockchain chip architecture.

research and development. It is then possible to form an industry on a large scale that can affect social progress, economic development, and people's daily lives.

Therefore, in order to develop blockchain technology, we cannot blindly follow the trends, and we need to be rational. It is necessary to see both the advantages and possible changes in blockchain technology, as well as the shortcomings and challenges of current blockchain technology. From a technical perspective, the R&D and optimization of the underlying blockchain and basic technologies must be increased. From the governance perspective, laws and regulations must be followed up with, and the regulatory model should be innovated. From the talent perspective, interdisciplinary talent training should be strengthened, and talent vacancies should be supplemented.

5.1 Pay attention to the research and development of the underlying technology of blockchain

It should be soberly realized that, behind the rapid development of the blockchain industry, there is a hidden reality of insufficient investment in the R&D of the underlying blockchain technology. At present, most blockchain projects and blockchain teams in China are in secondary development or are directly exploring applications in specific areas and specific industries based on Bitcoin, Ethereum, HyperLedger, and other foreign blockchain platforms.

In order to cope with the abovementioned challenges of blockchain technology development and large-scale applications such as performance and security, innovation of the underlying technology of blockchain is the top priority. R&D investment in architecture, consensus algorithms, verification mechanisms, (cross-chain) communication protocols, and proprietary hardware should be increased. We should patiently start from the bottom of the research and development in order to achieve technological autonomy and control, and strive to lead the development of the global blockchain technology.

5.2 Develop innovative regulatory models

Different from traditional Internet applications, there are special operating units that can be used as specific regulatory objects. Once a decentralized application (DAPP), which is designed with distributed and decentralized ideas, is deployed on a blockchain, all free access nodes and participants are jointly responsible. There is no centralized node and storage, and no specific organization is responsible for it. This poses a considerable challenge to the regulation of blockchain applications.

Therefore, on the one hand, while encouraging the development of blockchain technology and applications, the state should actively follow up from the legislative level, guide the application direction of the blockchain, and standardize the review and deployment of blockchain applications. On the other hand, from the level of information technology tools, we must increase R&D investment and the intensity of information technology tools such as monitoring, analysis, discrimination, and early warning for blockchain platforms and applications, and introduce and apply advanced technologies such as artificial intelligence, big data, and information security, thereby achieving better regulation of blockchain platforms and applications.

5.3 Strengthen interdisciplinary talent training

A smart contract is a computer program that runs on a blockchain. Blockchain technology allows people to reach consensus on decentralization, while smart contracts determine what kind of consensus can be reached. In other words, the blockchain is just a public ledger formed by a distributed accounting method. The smart contract further determines with whom, under what circumstances, and what kind of ledgers are formed in thousands of different application scenarios and economic activities.

In the future, after the blockchain system infrastructure has been built successfully, the so-called extensive application of blockchain technology in the commercial application scenario will largely use the blockchain to write and run smart contracts. Participating parties negotiate, form contract terms, and then write computer programs to implement smart contracts, and ensure that they are accurate and correct before they can be deployed. Writing and reviewing smart contracts requires a large number of cross-border talent who are proficient in computer technology, laws and regulations, and other professional fields. It is necessary to strengthen the training of such talent.

References

[1] Ministry of Industry and Information Technology of the PRC. White paper on the development and application of blockchain

technology in China (2016) [R]. Beijing: Ministry of Industry and Information Technology of the PRC, 2016. Chinese.

[2] Castro M, Liskov B. Practical byzantine fault tolerance [C]. New Orleans: USENIX OSDI, 1999.

[3] Yossi G, Rotem H, Silvio M, et al. Algorand: Scaling byzantine agreements for cryptocurrencies [C]. Shanghai: ACM SOSP, 2017.

[4] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: A scalable block-chain protocol [C]. Santa Clara: USENIX NSDI, 2016.

[5] Bender A, Katz J, Morselli R. Ring signatures: Stronger definitions, and constructions without random oracles [C]. New York: Springer TCC, 2006.

[6] Ben-Sasson E, Chiesa A, Tromer E, et al. Succinct non-interactive zero knowledge for a von Neumann architecture [C]. San Diego: USENIX Security Symposium, 2014.