

Xiaodan Tang
Xiaotie Deng
Rongfang Bie *Editors*

Blockchain Application Guide

Methodology and Practice



中国工信出版集团



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>




Springer

Blockchain Application Guide

Xiaodan Tang · Xiaotie Deng · Rongfang Bie
Editors

Blockchain Application Guide

Methodology and Practice

 中国工信出版集团

 电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

 Springer

Editors

Xiaodan Tang
China Electronics Standardization Institute
Beijing, China

Xiaotie Deng
Peking University
Beijing, China

Rongfang Bie
School of Artificial Intelligence
Beijing Normal University
Beijing, China

ISBN 978-981-19-5259-3

ISBN 978-981-19-5260-9 (eBook)

<https://doi.org/10.1007/978-981-19-5260-9>

Jointly published with Publishing House of Electronics Industry

The print edition is not for sale in China (Mainland). Customers from China (Mainland) please order the print book from: Publishing House of Electronics Industry.

© Publishing House of Electronics Industry 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publishers, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publishers nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publishers remain neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.

The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword

At present, digitalization, networking, and intelligence have become key trends in technological innovation and industrial change. Meanwhile, data is playing an increasingly important role as a critical production factor, and the growth of the digital economy is regarded as a key driver of future economic development as well as an important support for the national governance system. In this context, information technology innovation is becoming a driving force for the rising digital economy, bringing in academia and entrepreneurs together to design a better future for the human kind.

Blockchain is one such technology that combines distributed storage, cryptographic algorithms, consensus mechanisms, and smart contracts into one system. With the characteristics of decentralization, data forgery-proof tampering, and de-trusting, blockchain technology can guarantee credible and governable data and realize programmable contracts and thus can play a significant role in promoting multi-party collaboration, enhancing cyberspace security, and accelerating the inter-connection of value. In recent years, blockchain technology has advanced rapidly, with innovation iterations speeding up, and technological breakthroughs increasing. More groundbreaking applications are emerging in financial services, manufacturing, supply chain management, government services, and people's livelihood, showing a growing value in digital economy model innovation, high-quality real economy development, as well as public services innovation and upgrading.

The window of opportunity to cultivate core competitiveness and take a dominant position in the growth of emerging technology industry is typically quite limited. However, there are still hurdles in the realm of blockchain, such as the technology maturity, application scale, regulatory mechanism, and public knowledge of this technology. How best to address these problems is currently a global challenge.

When considering the future of the blockchain industry, one of the most noteworthy issues is how to cultivate high-quality, practical solutions to industry pain points and form industry-level blockchain applications. It is also a critical step in releasing the effectiveness of blockchain technology. The selection of themes in this book reflects the authors' understanding of these fundamental concerns as well as the actual demands of industrial growth, and the discussion is conducted using a mix

of theory and practice. It presents a comprehensive overview of blockchain applications. This book can be useful for blockchain-related policy-making, as well as for practitioners engaging in technology development, application management, and standard development on blockchain applications. It can also serve as a starting point of learning for blockchain technology enthusiasts. It is hoped that the more experts, scholars, and practitioners will participate in the theoretical and technical research of blockchain applications, the more businesses will focus their efforts on developing high-quality blockchain applications to contribute to an advanced industry chain.



Weimin Zheng

Beijing, China

Weimin Zheng is a professor with the Department of Computer Science and Technology, Tsinghua University. His research covers distributed computing, compiler techniques, and network storage. He is an academician of the Chinese Academy of Engineering.

Preface

In the information age, everyone participates and everything is interconnected. Everyone can contribute to the development of group value by producing, creating, and disseminating information. With its decentralized, distributed, and high trust-worthiness characteristics, blockchain has become a strategic frontier in global technological innovation and industrial change.

Blockchain originated from cryptocurrency, and then as the technology developed rapidly, it broadened the application boundaries in a variety of scenarios. Blockchain technology is now widely used not only in the financial sector, but also in logistics, government services, culture and education, and people's livelihood, propelling the innovation and growth across a wide range of industries. More importantly, the concept and technology of blockchain have promoted the continuous evolution of the mode and mechanism of information interconnection, value recognition and social management, increasing the value of the Internet, innovating the Internet governance mechanism, and forming a new blockchain application ecology, which has become an important way to deepen the integration of information technology and society.

In order to promote the implementation of blockchain and provide theoretical and practical references for associated businesses, this book provides a comprehensive introduction from the perspective of technology, ecology, practice, and governance. Part I focuses on the technological foundations of blockchain, covering an introduction of blockchain technology (Chap. 1), and the integration of blockchain with new generation information technologies such as cloud computing, Internet of Things, 5G, big data, and artificial intelligence (Chap. 2). Part II focuses on the current status and ecology of blockchain applications, proposing a blockchain application ecosystem model and analyzing the technology ecology, based on an investigation on the development of blockchain applications (Chap. 3). Blockchain technology provides an effective way to handle various problems of trust, confirmation, and supervision in production and life, and more and more practical applications favor using blockchain technology as one of the components. Part III examines the implementation route of blockchain applications (Chap. 4) and introduces it in terms of typical application scenarios and practices in a variety of industries, such as financial services (Chap. 5), logistics (Chap. 6), government services (Chap. 7), culture and education

(Chap. 8), and people's livelihood (Chap. 9). It outlines how to combine blockchain with solutions to problems in specific industry, respectively, and exhibits the implementation ways through typical use cases. Part IV delves into governance mechanism (Chap. 10), evaluation system (Chap. 11), and standardization progresses (Chap. 12) for blockchain applications. Part V is on the future prospect. As an emerging technology industry, blockchain has a bright future, but there are still many uncertainties in terms of technology, market, and management, while it will continue to expand its application to more domains, necessitating continuous innovation, practice, and research.

We are grateful for all the authors who contributed to the writing of this book. We also would like to thank Wei Yang, Jianping Zhao, Zilin Chen, Wenting Chang, Xiaofeng Chen, Weiping Deng, Ke Wang, and many other experts for providing valuable information and data on blockchain application cases, open-source communities, infrastructure, standardization, and other aspects.

We hope that the research findings and experiences in this book can provide useful references for users, developers, service providers, and policy-makers. We also welcome any comments and suggestions.

Beijing, China

Xiaodan Tang
Xiaotie Deng
Rongfang Bie

Contents

Part I Technical Foundation

- 1 **Basic Technology** 3
Xiaotie Deng, Wenhan Huang, and Xiaodan Tang
- 2 **Convergence of Blockchain and Next Generation Information Technology** 19
Xiaojun Zhang

Part II Application Ecology

- 3 **Blockchain Application Status and Ecology** 35
Xiaodan Tang, Zijun Jia, and Wei Yang

Part III Application Methods and Practices

- 4 **Blockchain Application Implementation Roadmap** 51
Yaling Liao and Yabo Zhang
- 5 **Blockchain and Financial Service** 61
Xiao Chen and Shubing Shan
- 6 **Blockchain and Logistics** 83
Wenming Zhe, Xiaoqiang Qiao, and Qing Cong
- 7 **Blockchain and Government Services** 105
Xiaojun Zhang
- 8 **Blockchain and Culture Education** 121
Yinfeng Chen, Yaofei Wang, Yu Guo, Haodi Wang, Rongfang Bie, and Peter Thomas
- 9 **Blockchain and People's Livelihood** 149
Boming Yu and Shixiao Zhan

Part IV Governance Norms

10 Governance of Blockchain Application 169
Yukun Cheng and Xiaotie Deng

11 Blockchain Application Evaluation 185
Xiaodan Tang

12 Roadmap of Blockchain Standardization 193
Jianong Li and Xiaodan Tang

Part V Outlook

13 Key Issues of Blockchain 207
Xiaodan Tang

14 Trends of Blockchain 215
Xiaodan Tang

Editors and Contributors

About the Editors

Dr. Xiaodan Tang is currently a senior engineer at China Electronics Standardization Institute (CESI). She received her Ph.D. degree in June 2012 from Institute of Physics, Chinese Academy of Sciences, and BS degree in Nankai University in June 2003. She was an industrial researcher at China Shipbuilding Industry Corporation in 2014–2016. She led and participated in more than ten reports and books. She is the editor of ISO/TR 6277 data flow model for blockchain and DLT use cases. Her current research interests include applications, public policies, and standardization of blockchain technology and post-quantum cryptography.

Prof. Xiaotie Deng got his B.Sc. from Tsinghua University, M.Sc. from Chinese Academy of Sciences, and Ph.D. from Stanford University in 1989. He is currently a chair professor at Peking University. He taught in the past at Shanghai Jiaotong University, University of Liverpool, City University of Hong Kong, and York University. Before that, he was an NSERC international fellow at Simon Fraser University. Deng’s current research focuses on algorithmic game theory, with applications to Internet Economics and Finance including sponsored search auction, p2p network’s economics such as BitTorrent network, sharing economics, and blockchain. He is a foreign member of Academia Europaea, an ACM fellow for his contribution to the interface of algorithms and game theory, and an IEEE fellow for his contributions to computing in partial information and interactive environments. He is the founding director of CSIAM Activity Group on Blockchain.

Prof. Rongfang Bie is currently a professor at the School of Artificial Intelligence of Beijing Normal University, where she received her M.S. degree in June 1993 and Ph.D. degree in June 1996. She was with the Computer Laboratory at the University of Cambridge as a visiting faculty from March 2003 for one year. She is the author or co-author of more than 100 papers. Her current research interests include blockchain technology, knowledge representation and acquisition for the Internet of Things, dynamic spectrum allocation, big data analysis and application, etc.

Contributors

Bie Rongfang Beijing Normal University, Beijing, China

Chen Xiao CFETS Information Technology (Shanghai) Co., Ltd, Shanghai, China

Chen Yinfeng Beijing Normal University, Beijing, China

Cheng Yukun Suzhou University of Science and Technology, Suzhou, Jiangsu, China

Cong Qing JD Logistics, Beijing, China

Deng Xiaotie Peking University, Beijing, China

Guo Yu Beijing Normal University, Beijing, China

Huang Wenhan Shanghai Jiao Tong University, Shanghai, China

Jia Zijun China Center for Information Industry Development, Beijing, China

Li Jianong China Electronics Standardization Institute, Beijing, China

Liao Yaling WanXiang Blockchain Company, Shanghai, China

Qiao Xiaoqiang JD Logistics, Beijing, China

Shan Shubing CFETS Information Technology (Shanghai) Co., Ltd, Shanghai, China

Tang Xiaodan China Electronics Standardization Institute, Beijing, China

Thomas Peter RMIT University, Melbourne, Australia

Wang Haodi Beijing Normal University, Beijing, China

Wang Yaofei Beijing Normal University, Beijing, China

Yang Wei Digital City Company, China Xiongan Group, Xiongan New Area, Hebei, China

Yu Boming Hangzhou Qulian Technology Co., Ltd., Zhejiang Province, People's Republic of China

Zhan Shixiao Hangzhou Qulian Technology Co., Ltd., Zhejiang Province, People's Republic of China

Zhang Xiaojun Huawei Technologies Co., LTD, Beijing, China

Zhang Yabo WanXiang Blockchain Company, Shanghai, China

Zhe Wenming JD Logistics, Beijing, China

Part I

Technical Foundation

Since the concept of Blockchain was proposed in 2008, with rapid developments in recent decades, blockchain technology has been widely used and has become a cutting-edge and strategic technology. From Blockchain 1.0, 2.0, to 3.0, Blockchain technology has gradually broken through the limited application in digital currency. The key technologies, such as consensus mechanisms and smart contracts, have gradually matured. The running efficiency and the energy consumption have been progressively optimized. With these advancements, it becomes possible to develop applications for various scenarios on a Blockchain. Along with the developments of new-generation information technologies, such as cloud computing, the Internet of Things, big data, and artificial intelligence, Blockchain technology increases the synergy and integration with these technologies. Such synergy and integration will stimulate innovations, promote the basic construction of technologies, and broaden the applications.

Chapter 1

Basic Technology



Xiaotie Deng, Wenhan Huang, and Xiaodan Tang

Abstract Blockchain technology and distributed ledger technology have developed rapidly since Bitcoin, the first Blockchain concept, was proposed in 2008. In this chapter, we will introduce the development history and basic concept of the Blockchain. The reader can have a general understanding of the Blockchain so that the reader will comprehend other chapters' content more easily. We will first look back on the development history of the Blockchain and then look to the future of Blockchain technology. Next, we will discuss fundamental technologies for the Blockchain systems. These technologies ensure the efficiency and security of the Blockchain and expand the blockchain's practical scenarios. After introducing fundamental technologies, we will exhibit three classes of blockchain: public chain, private chain, and consortium chain. Finally, we will illustrate the architecture of Blockchain systems.

Keywords Blockchain technology · Blockchain development · Blockchain architecture

1.1 Concept and Development of Blockchain

In 2008, a researcher named Satoshi Nakamoto published a paper, Bitcoin: a peer-to-peer electronic cash system [1], and established a digital currency system without trusted third-party through several technologies, such as the p2p network, cryptographic algorithms, consensus mechanism, and timestamps. Around 2012, people began to realize the virtue of the technical design of Bitcoin, especially the data

X. Deng
Peking University, Beijing, China

W. Huang (✉)
Shanghai Jiao Tong University, Shanghai, China
e-mail: rowdark@sjtu.edu.cn

X. Tang
China Electronics Standardization Institute, Beijing, China

organization with block + chain, named Blockchain. However, after a few companies started to discuss the Blockchain applications for financial services, IoT, and other fields around 2014, the Blockchain gradually attracted widespread attention. In China, such attention lags slightly, but it also starts a wave of upsurge around the second half of 2015 that has continued to this day.

Blockchain is a set of technical solutions extracted from the technical design of Bitcoin. Since such solutions can realize anti-counterfeiting, anti-tampering, and multi-party participation data records, they can be applied to many other fields. Therefore, it is discussed and applied as an independent technology. As the Blockchain is a technical realization for data recording, the prosperity of the Blockchain applications reflects a strong demand for a multi-party shared and synchronized ledger of data records. Later, people find that other solutions besides Bitcoin's one can also achieve such a ledger. As for supplements and extensions to Blockchain, some related concepts have also developed and gradually merged with Blockchain, such as distributed ledger and distributed recording technology.

The International Organization for Standardization (ISO) defines Blockchain [2] as a distributed ledger in which confirmed blocks are organized as incremental, sequential chains with cryptographic techniques. And the distributed ledger is defined as an information store that holds a final, deterministic, immutable record of transactions shared and synchronized among a series of nodes through a consensus mechanism (Fig. 1.1). In traditional business activities, the ledger, as the origin of the records of economic activities, can summarize and verify past activities. With the development of informatization, the informatization ledger has also been "born out" from the traditional ledger to a recording method that supports new types of things such as credit disclosure. However, this approach still brings data consistency, easy forgery, and tampering challenges. For these challenges, the long-term solution is to rely on a third-party institution like a credit endorsement to ensure the authenticity and reliability of the ledger. With the development of the economy and society, people are no longer satisfied with relying on this traditional credit system based on third-party credit guarantees. Instead, they have begun to explore a set of verifiable and reliable trust systems that do not rely on third parties. The continuous development of information technology has gradually made this transformation possible. In particular, the development of modern cryptography has provided important technical means for problems such as impartiality and privacy. The large-scale application of distributed computing has also provided a vast space for the development of new technologies. In this series of backgrounds, the Blockchain, a decentralized distributed ledger, came into being.

Compared with the traditional information ledger, the ledger based on blockchain technology stores the same transaction records on many computers. The cryptography technology ensures the security of the previous transaction records and verification information. When tampering with a particular transaction record in the blockchain, all subsequent transaction records and blocks must be tampered with, which dramatically increases the cost of tampering, so the blockchain is considered immutable. In addition, blockchain technology applies cryptographic technologies

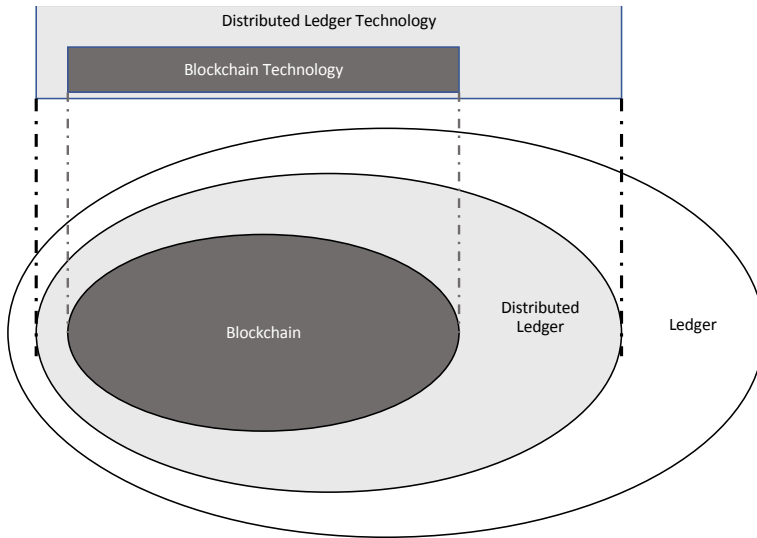


Fig. 1.1 The relationships of blockchain, distributed ledger, and other related terms

such as public-key encryption, which also has good guarantees for privacy and fairness in transactions. In addition, blockchain technology realizes tamper-proof modification, fairness, reciprocity, privacy, etc., in the process of transaction and recording to ensure mutual trust between transaction parties.

Further, through the maintenance of trusted ledgers and the trust relationship established based on them, blockchain technology allows multiple parties to jointly process a transaction, which is regarded as the technical basis for establishing a new multi-party collaborative relationship. Furthermore, smart contracts enable Blockchain to perform agreed actions automatically. Therefore, Blockchain is generally regarded as a new type of trust mechanism. Such a mechanism can optimize social production and cooperation, and it can benefit many fields in efficiency improvement, cost reduction, and intelligence improvement.

Just like a “polyhedron”, Blockchain presents different appearances from different perspectives. The industry’s positioning of Blockchain is also very diversified, giving different understandings and definitions for the word “Blockchain”. For example, the group standard “Blockchain Reference Architecture” [3] defines Blockchain as a mode of realizing and managing transaction processing with a chain block data structure that is anti-counterfeiting, tamper-proof, and traceable through transparent and trusted rules in a peer-to-peer network environment. Yong et al. [4] defined Blockchain from a technical viewpoint: a kind of new decentralized infrastructure and distributed computing paradigm for generating and updating data that uses encrypted chain block structure to verify and store data, uses distributed node consensus algorithm to verify and store data, and uses automated script code (smart contracts) to program and manipulate data. Distributed Ledger Technology: Beyond Blocks,

published by the UK Government Chief Scientific Adviser Chain” [5] believes that: Blockchain is a kind of database, which stores some records in a block, each block is “linked” with the next block using a cryptographic signature, and Blockchain can be used in any Share and collaborate between people with permissions. To a certain extent, Blockchain can be regarded as a ledger maintained by a mutually equal group based on the usage of a series of technical rules to ensure sufficient consensus. From the data point of view, Blockchain can be regarded as a kind of database. Because the records on Blockchain are encrypted, tamper-proof, and maintained by multiple parties, it is a highly trusted database. From the perspective of technology ecology, Blockchain is an autonomous governance method based on information technology, which achieves trust through preset rules and promotes multi-party collaboration.

1.2 Origin of Blockchain Technology

In 1991, Haber and Scott Stornetta [6] proposed the earliest cryptographically secure chain block to design a tamper-proof system. Next year, the two authors and Dave Bayer incorporated Tree [7] into the area. The block structure enables the encryption and verification of many files within one block, which improves the operating efficiency of the entire system. However, a trusted third party is still required to sign for the earliest chain blocks. In 1999, Markus Jakobsson and Ari Juels formally proposed the concept of proof of work (Proof of Work, PoW), using the method of computing consistent hash to reach consensus. Such an idea can be traced back to a paper published in 1993 by Cynthia Dwork and Moni Naor, which reduces spam by computing mathematically complex issues [8, 9]. In 2008, Nakamoto [1] proposed a new data structure of “block + chain” when designing Bitcoin, which improved the original chain block and used the workload proof algorithm to reach a consensus, thereby eliminating the need for Trusted Third Party. At the same time, by adjusting the difficulty of the consistent hash calculation result, the block generation speed can be controlled. However, in a distributed system, the efficiency of solving computational problems is uncontrollable. To solve the fairness problem when different nodes process computational problems simultaneously, Bitcoin adopts the longest chain principle in its design: When computational issues lead to multiple chains existing, only the longest chain is valid.

Since then, Blockchain technology has been widely used in cryptocurrencies. Technological development has focused on expanding the expression of cryptocurrencies, increasing transaction volume, reducing transaction time, and improving computing resource utilization. Therefore, a series of consensus protocols improving transaction efficiency have been proposed to solve the problems of low efficiency of cryptocurrency transactions and eliminate the impact of forks in the chain structure of Blockchain. At the same time, to deal with different application scenarios, the concept of private chain and consortium chain was also proposed during this period by sacrificing some equality and fairness in exchange for efficiency improvement.

At the end of 2013, the Ethereum platform project was launched [10]. Through the technologies such as smart contracts, providing an application development environment and virtual machines, the development of distributed applications (DApp) was pushed to a new development period, and more and more DApps were incubated. Ethereum uniquely adds smart contracts to its Blockchain system, which broadens the boundaries of Blockchain technology applications besides cryptocurrencies. The concept of smart contracts was first proposed by Nick Szabo in 1994, when it was defined as “a set of promises made in digital form, including agreements on which contract participants can execute these promises” [11]. When the smart contract is pre-deployed on Blockchain and the corresponding conditions are satisfied, the system will automatically execute the code in the contract. Therefore, smart contracts can be regarded as program code running on Blockchain. Since the program has no possibility of default and is naturally credible, it can be used for chain-to-chain and chain-to-non-chain interaction.

1.3 Stages of Blockchain Development

Based on the development of blockchain technology, application, standardization, and industrial ecology, the development of Blockchain has gone through three stages since Bitcoin was launched in 2009.

The first stage is Blockchain 1.0 (2008–2013), which is the origin and verification stage of Blockchain technology. The main feature of this stage is the verification of Blockchain technology through the stable operation of Bitcoin. After Satoshi Nakamoto proposed Bitcoin in 2008, it set off a wave of technology research and industrial development around cryptocurrencies. Blockchain was mainly used to store cryptocurrency transaction information during this period, and the consensus mechanism was mostly PoW. And the development of Blockchain was mainly based on the improvement of the Bitcoin framework. The main feature of this period is that public chain technology grew significantly while the exploration for the application of cryptocurrency had just begun. As a result, Blockchain standardization was almost blank, and the typical feature of the industry was the gradual development of the ecology around cryptocurrencies.

The second stage is Blockchain 2.0 (2013–2015), which is the stage for the concept of Blockchain and platform development. At this stage, platforms such as Ethereum and Hyperledger developed rapidly, and the application of technologies such as smart contracts promoted the application of Blockchain in more fields. At the same time, the industry began to discuss the standardization of Blockchain. In 2014, Vitalik Buterin proposed a new type of Blockchain that could run smart contracts. Smart contracts enable deployed Blockchain to complete its mutual trust mechanism. As a result, the development of various applications in Blockchain became possible. During this period, Blockchain and its application development community represented by

Ethereum were not satisfied with simply using Blockchain as a technology for realizing encrypted currency but incubated many prototypes of distributed applications based on smart contracts.

The third stage is Blockchain 3.0 (2015 to present), which is the stage of popularization and application of Blockchain concepts. At this stage, technologies such as cross-chain and privacy protection have gradually developed, and Blockchain has been actively used for finance of supply chain, traceability of food and drug, judicial evidence storage, public services, and other fields. As a result, some kinds of applications have begun to scale. At the same time, with the rapid development of Blockchain standardization at home and abroad, the industry has started to accelerate the exploration for the construction of general-purpose infrastructure.

1.4 Fundamentals of Blockchain Technology

1.4.1 *Technical Design and Advantages*

The core of Blockchain technology design is to implement a tamper-proof, anti-forgery, and traceable maintenance process of a distributed ledger through consensus mechanisms, encryption algorithms, smart contracts, and other technologies in a distributed network. Figure 1.2 shows a Blockchain-based distributed ledger maintenance process. In a distributed Blockchain network, if participant A initiates a transaction, the transaction will be broadcast in the Blockchain network, and then the miner for this transaction will be selected through a consensus mechanism (such as PoW). The miner's task is to package this transaction (possibly together with multiple other transactions) into a block, and then the miner broadcasts the block to all participants in the Blockchain network for verification. The block will be permanently added to the Blockchain ledger after verification. After that, the transaction is completed, and the transaction-related party B in the Blockchain network can view the transaction result.

Compared with the centralized ledger, the distributed ledger implemented by Blockchain stores copies of the ledger in each node of the distributed network, effectively avoiding the ledger damage caused by single-point failure. At the same time, the encrypted data storage, multi-copy storage, and the data structure of "block + chain" make the data extremely difficult to be tampered with or forged. Furthermore, the data on Blockchain is organized in sequence through technologies such as timestamps, which provide good traceability for the on-chain data.

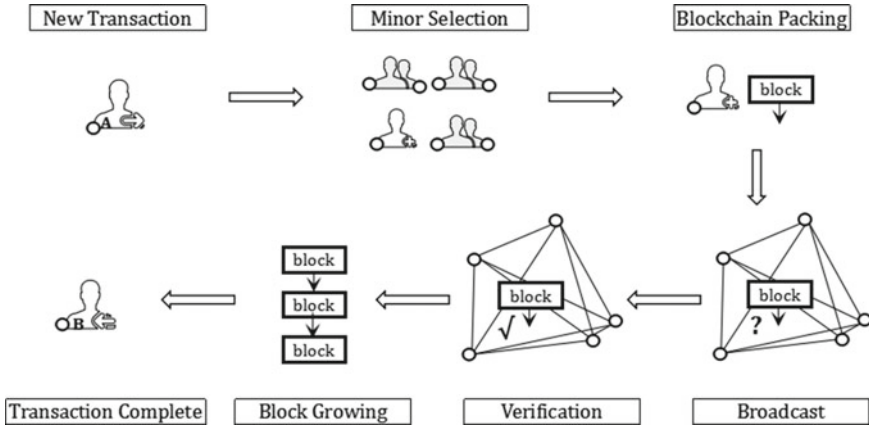


Fig. 1.2 Blockchain-based distributed ledger maintenance process

1.4.2 Core of Key Technology

Blockchain relies on several technologies, including peer-to-peer (P2P) networks (providing infrastructure capabilities for storage, computing, and communication), virtualization, containers, cloud computing, data storage, and other related technologies; encryption algorithms, digital digests, digital signatures, key management, homomorphic encryption, zero-knowledge proof, ring signature, attribute encryption and other security and privacy protection technologies; as well as consensus mechanisms, smart contracts, cross-chain technologies. Many of these technologies are relatively mature, while some are gradually developed or improved in Blockchain, such as consensus mechanisms, data storage, encryption algorithms, smart contracts, and cross-chain technologies.

1. Consensus Mechanism

In Blockchain, the consensus mechanism is the unified transaction verification and confirmation method for distributed nodes. Currently commonly used consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA). Among them, PoW is a consensus mechanism that solves specific computing problems through operations to ensure that all nodes obtain accounting rights reasonably. Because each accounting requires more nodes to operate simultaneously and the enormous computing power of the nodes does not solve the issue, PoW achieves a low efficiency. PoW's fault tolerance allows 50% of the entire network nodes to fail, but there are 25% fault-tolerant attacks for some specific chains [9]. PoS is a consensus mechanism that links the difficulty of a node to obtain mining rights with the stake it holds. The larger the stake, the easier it is to obtain mining rights through a specific hash value. Compared with PoW, PoS reduces much computation, and its fault tolerance allows nodes with 50% stake in the entire

network to make mistakes. PBFT is a consensus mechanism based on the election of leaders, and it conducts miner through voting among committees. PBFT allows Byzantine fault tolerance. Since many calculations are eliminated, the performance efficiency is relatively high, allowing 33% of the entire network nodes to fail. Since the election does not necessarily require all nodes in the network, this mechanism can also be applied to the consortium chain. PoA is similar to PoS, but it replaces equity with authority, and participating nodes need to perform mandatory authentication to obtain the right to participate in book-keeping. Origin PoA has a fault tolerance rate of 50%, but if the mechanism employs Byzantine consensus, the fault tolerance rate drops to 33%.

2. Data Storage

In Blockchain technology, data is generally stored in blocks, and blocks are connected in sequence to form a chain-like linear structure in the generated order. Usually, a block contains a block header (Head) and a block body (Body). The block header stores the connection and encryption information between blocks, and the block body contains all the verified transaction information collected during the block creation process. The data storage structure has improved to enlarge the throughput of Blockchain. There is a technical solution to replace the single chain with the form of a directed acyclic graph (DAG). When each new data unit is published, it must refer to multiple existing parent data units. Over time, all data units containing transactions are connected, forming a graph structure of a directed acyclic graph. This scheme avoids the limitation of serialized writing in a single chain and has excellent improvements in concurrency and scalability.

3. Encryption Algorithm

The commonly used encryption algorithms in Blockchain roughly include hashing (hash) algorithms and asymmetric encryption algorithms. Among these two kinds of algorithms, the hash algorithms mainly convert a piece of information into a fixed-length digest to ensure certainty and randomness. For specific information, the encrypted results are consistent; for approximate information, the encrypted results are random and irrelevant. Currently, the hash algorithm that is used more in Blockchain is SHA256. An asymmetric encryption algorithm employs a pair of keys, a public key and a private key. Anyone who obtains the public key can use the public key to interact securely with the private key holder. But due to the dependency of the public key and the private key, only the private key holder can decrypt the information, and any unauthorized person cannot decrypt it, even the sender of the message. Asymmetric encryption algorithms used in Blockchain include RSA, ECC, and ECDSA.

4. Smart Contract

A smart contract is a program that is fully deployed on Blockchain and can run autonomously, and all the output of the program will be completely recorded on the chain. The program runs in a closed sandbox. The interaction with the outside only depends on the input and output of the program, and the smart contract cannot directly manipulate the information of the external network, file system, or other smart contracts.

The international standard “Blockchain and distributed ledger technologies—Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems” [12] pointed out that smart contracts need to have confidentiality, impartiality, feasibility, and privacy to ensure that smart contracts cannot be misused and abused. Confidentiality means that the execution of the smart contract is visible to all nodes since the smart contract needs to run on the blockchain throughout the whole process. The information needs to be processed using homomorphic encryption or zero-knowledge proof to avoid revealing the current state of the smart contract. Fairness refers to ensuring that smart contracts are executed as initially set. Feasibility means that due to the existence of the halting problem, if the smart contract is Turing complete, the outside world may not be able to judge the running status of the current smart contract program. The standard solution is to either control the running time to ensure that there will be no halting problems; or constrain the smart contract’s language in a smaller language space to avoid halting problems. Privacy means that a specific smart contract can only be called and operated by a particular group to ensure that the state and data of the smart contract will not be leaked.

5. Cross-chain Technology

Cross-chain technology generally refers to the technology of information communication and interaction between two or more relatively independent Blockchains. With the development of Blockchain technology and the rapid increase of different Blockchain projects, multi-chain parallelism and multi-chain interoperability have become the future development trend. As a result, data interaction, data transfer, and information communication between chains are becoming increasingly important.

Cross-chain consists of cross-chain between homogeneous chains and cross-chain between heterogeneous chains. The cross-chain between isomorphic chains mainly occurs in the information interaction between the side chain and the main chain. Transferring their information is relatively easy since the isomorphic chains have the same structure. On the other hand, the cross-chain between heterogeneous chains is much more complicated, requiring both parties to communicate through smart contracts, oracles, or relays from third-party organizations.

The current cross-chain technology is still immature, and the ease of use and scalability of cross-chain needs to be developed. There are also supervision problems in cross-chain, and how to conduct data interaction between chains more safely and faster is still an urgent problem to be solved.

1.4.3 Security and Privacy Protection in Blockchain

1. Security of Blockchain Technology

The security of Blockchain technology includes two aspects: data security and system security. Among them, the data security of Blockchain means that for the

data on the chain, usually, only the private key holder can decrypt it, while others on the chain can only verify the data to prevent the owner from operating data secretly. It guarantees both privacy and security. At the same time, when data need to be stored on the chain, they must pass a consensus mechanism. That is, the data are allowed to be stored when most people in the entire network agree with the correctness of the data record. The system security of Blockchain means that for all participants, the data on the chain are the same, and each participant will have a copy of the information stored on the chain, so Blockchain naturally avoids traditional point-to-point targeted attacks.

2. Security Challenges and Countermeasures Faced by Blockchain Technology

I. Data Openness and Participation Openness

On Blockchain, all data are visible, and everyone (in public chain) or authorized person (in private chain or consortium chain) can participate in Blockchain. Therefore, the prevention of identity forgery or information theft has certain challenges. Current strategies generally prevent the occurrence of such problems computationally through sufficiently difficult cryptographic techniques.

II. Privacy Protection

Since the behavior and changes on the participant chain are visible to everyone, there is a possibility that an attacker can infer relevant information about the participant's behavior on the chain. Zero-knowledge proofs and other technologies currently protect participants' specific behavior and privacy.

III. Attack Prevention

Besides typical double-spend attacks, distributed attacks, and other attack methods, there may be specific attacks where the attacker requires less than 50% of the total resources for particular Blockchains. Therefore, it is a significant challenge for the development of Blockchain to prevent this type of attack on the Blockchain mechanism and the possibility of establishing traditional attack conditions. Furthermore, there is no way to avoid new attacks except for some known attacks. Consequently, the attack and prevention of Blockchain will become a new research hotspot after the development of Blockchain technology matures.

3. Blockchain Security System

I. Physical Security

The network and host running the Blockchain system should be in a protected environment to avoid being attacked and causing the Blockchain network to be destroyed. Depending on the actual situation and security level, the Blockchain system is protected by firewalls, physical isolation, and the establishment of private networks.

II. Data Security and Identity Security

The network and host running the Blockchain system should be in a protected environment to avoid being attacked and causing the Blockchain

network to be destroyed. Depending on the actual situation and security level, the firewalls, physical isolation, and even the establishment of private networks can be used for protection.

III. Private Key Security

Since the private key is the only tool on the Blockchain network that can decrypt the data, the key should be properly kept, such as traditional encryption methods. It is recommended to periodically update the private key or use a one-time private key in transaction transmission to prevent the key from being leaked in multiple transactions.

IV. Supervision and Risk Control

There should be a strict monitoring mechanism for the overall state change on Blockchain. Suspicious operations should be warned and excluded. If there is an illegal operation, the loss should be assessed, the illegal operation should be remedied at both the technical and business levels, and both the source and method of illegal operation should be traced to prevent the recurrence of similar attacks.

1.5 Classification of Blockchain

At present, Blockchain is usually classified as public chains, private chains, and consortium chains from the perspective of the scope of participants.

1. Public Chain

A public chain is a Blockchain in which any group or individual can participate in sending transactions and conducting consensus, typically represented by Bitcoin. The public chain is the earliest Blockchain, and it is currently the most well-known and widely spread Blockchain. The public chain has the characteristics of complete decentralization: all on-chain behaviors are public, no one controls the on-chain operation, and no one owns such Blockchain.

For the public chain, theoretically, there is no situation where a small group can control the overall direction of the public chain unless this small group can control most of the world's resources (computing power, or other resources, depending on the specific consensus protocol). All users can freely participate in and leave the public chain network. Everyone can query all behaviors and all data on the public chain ledger. Therefore, the public chain has a high degree of equality, fairness, and openness.

2. Private Chain

A private chain is a Blockchain owned by an individual or group. The owner exclusively owns the permission to write and modify the blockchain. Therefore, only individuals or groups with the owner's permission can participate in Blockchain activities. Currently, the private chain is mostly used to record the internal behavior of the group.

For the private chain, users with the same permissions still have the nature of the public chain; but for users with different permissions, due to the difference

in their division of labor, they do not have equal status. Furthermore, in some private chains, the owner with the highest authority is allowed to make arbitrary changes to the blockchain.

3. Consortium Chain

The consortium chain is an extension of the private chain. However, unlike the private chain, the authority of the consortium chain is usually managed by a special committee. Thus, the consortium chain is usually used to deal with behavior between groups with common interests.

The consortium chain is between the public chain and the private chain, balancing the advantages of the two types of Blockchain: It is neither as free as the public chain so that it cannot control the identity of the participants nor as close as the private chain. Typical consortium chains include Hyperledger and Diem (formerly Libra). In China, most Blockchain projects belong to the consortium chain.

In addition, Blockchain can also be divided into permissioned and non-permissioned chains from the perspective of whether joining or participating in a Blockchain network requires authorization from specific nodes.

1.6 Blockchain System Architecture

The group standard “Blockchain Reference Architecture” [3] released in 2017 divides the blockchain system architecture into “four horizontal and four vertical” structures, four layers (the user layer, the service layer, the core layer, and the base layer) and four cross-layer functions for development, operations, security, and governance. Among them, the core layer includes the core functional components of Blockchain such as consensus mechanism, ledger record, encryption, digest, digital signature, timing service, and smart contract.

In August 2020, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) released the “Reference Framework for Distributed Accounting Technology” standard [13], in which the architecture of the Blockchain system is divided into six main components: *operation & maintenance*, *application*, *protocol*, *resources*, *external interaction management*, and *extensions*. *Operation & Maintenance* component is about specific behavior of each distributed node in Blockchain. *Application* component covers applications developed on Blockchain. *Protocol* component provides basement for the on-chain behaviour of participants including accounts, consensus, participant managements, and communication. *Resources* component maintains the computing and storage resources to run the Blockchain network more efficiently. *External interaction management* component manages the resources outside Blockchain, such as oracles, off-chain data. *Extensions* component extends Blockchain capabilities so that Blockchains can interact with each other and quickly expand to different practical scenarios. In addition to the six main components above, there are two additional sections: *utils* and *governance*.

Utils section ensures the Blockchain’s privacy and security with modern cryptography methods. *Governance* section monitors the on-chain behavior and provides feedback for each operation.

In February 2022, ISO released “Blockchain and distributed ledger technologies—Reference architecture” [14] and divided the reference architecture of Distributed Ledger Technology (DLT) into six components: *non-DLT systems*, *user layer*, *API layer*, *DLT platform layer*, *infrastructure layer*, and *cross-layer functions*. *non-DLT systems* provides resources or services outside the DLT system. *User layers* provides basic functions to enable participants to interact with the DLT system. *API layer* provides reliable and efficient access to resources inside or outside the DLT system. *DLT platform layer* provides the DLT system’s core functions including consensus mechanisms, communications between nodes and systems, cryptographic services, smart contracts, and on-chain resource management. *Infrastructure layer* provides the storage, the computation, and the communication resources for the operating environment. *Cross-layer functions* support the sections across several layers. These functions are grouped into four categories: *development*, *management and operations*, *security*, and *governance and compliance*.

Based on the ITU-T standard and the ISO standard, the functional architecture of Blockchain system can be summarized as Fig. 1.3. There are five components and one cross-component functions.

- **Operation and maintenance:** This component is mainly about the specific behavior of each distributed node in Blockchain, including the process of publishing transaction information, verifying transaction information, and accounting.

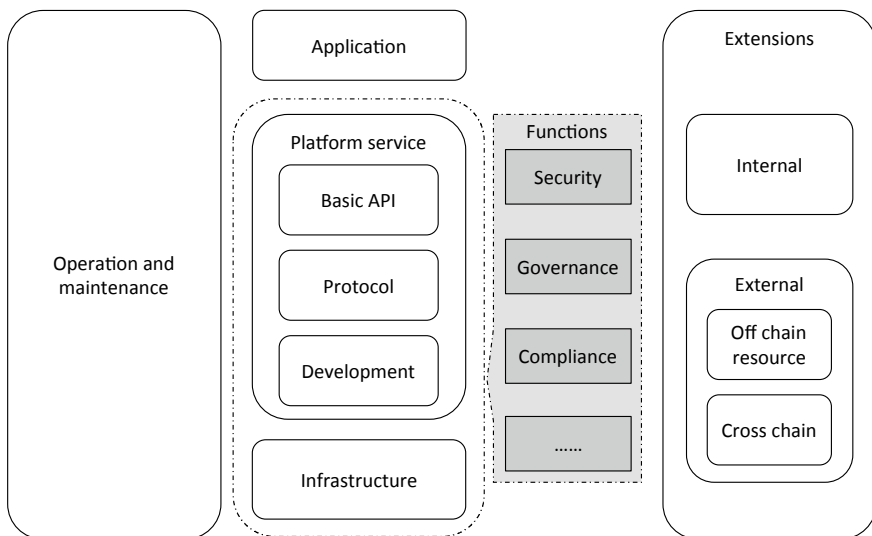


Fig. 1.3 Blockchain system functional architecture

- **Application:** This component covers applications developed on Blockchain, such as DApps. It ensures the maintainability and scalability of applications on Blockchain through the runtime management, the life cycle of applications, and some corresponding development tools.
- **Platform service:** This component helps participants interact with the Blockchain system. The Basic API sector enables participants to access the on-chain resource reliably and efficiently. In protocol sector, participants can deploy some smart contracts as protocols with basic APIs. Some pre-deployed protocols, such as cryptographic services or consensus mechanism, help the Blockchain system run correctly. The development sector supports the developers to develop protocols or applications effectively and efficiently.
- **Infrastructure:** This component provides resources for running the Blockchain system and performs node management, store management, and network management for Blockchain. The management and allocation of computing and storage resources save resources to run the Blockchain network more efficiently.
- **Extensions:** This component extends Blockchain capabilities. Internal extensions mainly expand the capabilities of the modules of Blockchain so that it can quickly expand to different practical scenarios. External extensions provide the off-chain resources and enables Blockchain to operate on the external environment or other chains.
- **Functions:** The cross-component functions support for the sections across components. For example, governance needs to monitor the behavior in platform service component and the corresponding data in infrastructure component. Among these components, security section ensures the Blockchain's privacy and security with modern cryptography methods and the design of the blockchain consensus mechanism. Governance section can prevent some loopholes in Blockchain and monitor the malicious behavior of illegal nodes in the Blockchain network. At the same time governance section can provide feedback about whether some security problems exist.

Through the cooperation between various components, Blockchain can be used independently as a specific application service or as a member of a comprehensive service, which ensures the privacy and security of the overall service, expanding the breadth of the landing for Blockchain applications.

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. (31 Oct 2008). <https://bitcoin.org/bitcoin.pdf>.
2. Blockchain and distributed ledger technologies—vocabulary: ISO 22739:2020. (16 Jul 2021). <https://www.iso.org/standard/73771.html>.
3. China Blockchain Technology and Industry Development Forum. Blockchain Reference Architecture: CBD-Forum-001-2017: 2017. (15 May 2020). <http://www.cbdforum.cn/bcweb/resources/upload/ueditor/jsp/upload/file/20201217/1608188444336059074.pdf>.

4. Yong Y, Feiyue W. Current situation and prospects of blockchain technology development. *J Automation*. 2016;42(4):581–494.
5. Government Office of Science. Distributed Ledger Technology: Beyond Blockchai. (10 Feb 2021). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
6. Haber S, Stornetta WS. How to time-stamp a digital document. In: *Conference on the theory and application of cryptography*. Springer; 1990. p 437–55.
7. Bayer D, Haber S, Stornetta WS. Improving the efficiency and reliability of digital time-stamping. In: *Sequences II: methods in communication, security, and computer science*. Springer; 1993. P. 329–34.
8. Jakobsson M, Juels A. Proofs of work and bread pudding protocols. In: *IFIP TC6/TC11 joint working conference on communications and multimedia security (CMS'99)*. Leuven: Belgium; 1999. P. 258–72.
9. Dwork C, Naor M. Pricing via processing or combating junk mail. In: *CRYPTO'92: proceedings of the 12th annual international cryptology conference on advances in cryptology*; 1992. 139–47.
10. Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. In: *International conference on financial cryptography and data security*. Springer; 2014. 436–54.
11. Yong Y, Feiyue W. *Blockchain theory and method*. Beijing: Tsinghua University Press; 2019.
12. Blockchain and distributed ledger technologies—Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems: ISO/TR 23455:2019. (16 Jul 2021). <https://www.iso.org/standard/75624.html?browse=tc>.
13. Reference framework for distributed ledger technologies: ITU-T F.751.2. (13 Aug 2020). <https://www.itu.int/rec/T-REC-F.751.2/recommendation.asp?lang=en&parent=T-REC-F.751.2-202008-I>.
14. Blockchain and distributed ledger technologies—Reference architecture: ISO 23257:2022(E). <https://www.iso.org/standard/75093.html>.

Chapter 2

Convergence of Blockchain and Next Generation Information Technology



Xiaojun Zhang

Abstract Blockchain technology ensures secure data transmission and use through features such as anti-tampering and traceability. However, blockchain can only ensure of data on the blockchain. To ensure end-to-end security and trustworthiness of data, blockchain needs to cooperate with other technologies. In this way, we can see that blockchain + IOT, blockchain + AI are complementary in technology capabilities and jointly maintain end-to-end secure data transmission.

Keywords BaaS · POC · PaaS · SVN · Sensor · eMBB · mMTC · DT

2.1 Overview

Since it was identified as one of the seven strategic emerging industries in the 12th Five-Year Plan, the new generation of information technology in China has developed rapidly and gradually become the direction of deepening application of information technology in various industries. In addition, the new generation of information technology accelerating the iteration and the in-depth integration with the real economy plays an increasingly critical role in intelligent manufacturing, finance, energy, and healthcare industries. On May 28, 2018, General Secretary Xi Jinping, in his speech at the 19th Academician's Congress of the Chinese Academy of Sciences and the 14th Academician's Congress of the Chinese Academy of Engineering, referred to blockchain technology for the first time and positioned it as a new generation of information technology, noting that "the new generation of information technology, represented by artificial intelligence, quantum information, mobile communications, IoT, and blockchain, is accelerating breakthrough application." During the 18th collective learning of Politburo, General Secretary Xi Jinping stressed the need to build a blockchain industry ecosystem, accelerate the in-depth integration of blockchain with cutting-edge information technologies such as artificial intelligence, big data, and

X. Zhang (✉)
Huawei Technologies Co., LTD, Beijing, China
e-mail: z.x_77@163.com

IoT, and promote integrated innovation and converged application. From the development trend and the evolution path of blockchain technology at home and abroad, the development of blockchain technology and applications requires cloud computing, big data, information physical systems, and artificial intelligence as infrastructure technology support. In contrast, blockchain technology and applications play a vital role in promoting the development of the next generation information technology industry. Blockchain, like cloud computing, Internet of Things, big data, and artificial intelligence, is typical of the new generation of information technologies. Blockchain and other new-generation information technologies are expected to bring a series of changes to people’s production methods and lifestyles through mutual promotion and integration. Especially in the real economy, the combination of blockchain and other new-generation information technologies is needed to jointly guarantee the authenticity and transparency of data. Problems, such as how to ensure the authenticity of blockchain data on the chain, how to guarantee blockchain bandwidth and latency when nodes move down and the number of nodes increases, and how blockchain data collaborate with big data and artificial intelligence, become urgent in blockchain development.

The comprehensive commercial development of blockchain will enhance the collaboration of various new technologies. In the first stage, the data will be collected and transmitted through IoT and the fifth-generation mobile communications technologies (5G), while the data will be accurately analyzed by relying on big data and artificial intelligence in the last stage. The reliability of the middle stage will be guaranteed by blockchain, thus forming the integration of the front, middle, and last three stages, as shown in Fig. 2.1.

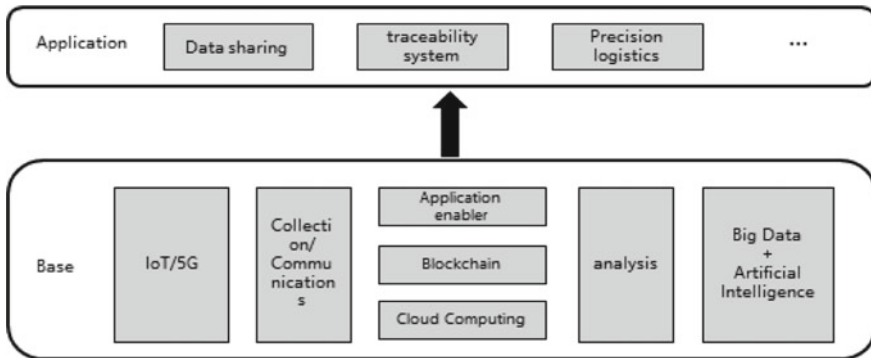


Fig. 2.1 Blockchain and next generation information technology convergence

2.2 Blockchain and Cloud Computing

Cloud computing is an Internet-based computing method that realizes the sharing of software/hardware resources and information and provides computing capabilities for various terminals and other devices as required. Cloud computing is developed from the Client/Server (C/S) mode and is based on the increase, usage and delivery mode of Internet-related services. The National Institute of Standards and Technology (NIST) defines cloud computing as a model that facilitates and improves the availability of computing resources (including networks, servers, storage, applications and services) from a shared and configurable resource pool, which can be acquired and released with minimal effort and no human intervention [1, 2]. At present, cloud computing is not only a kind of distributed computing, but also includes utility computing, load balancing, parallel computing, network storage, hot backup redundancy, and virtualization.

There are still some problems in the development of the cloud computing technology industry. First, the cloud computing market is extremely central, and a few Internet technology giants monopolize the entire cloud computing market by relying on their highly centralized server resources. Second, the over-concentration of cloud computing leads to the high prices of computing services, which become scarce resources, greatly restricting the development requirements of enterprises on the cloud.

Cloud computing is a pay-per-use model, while blockchain is a distributed ledger database and a trust system. By definition, there seems to be no direct correlation between the two, but blockchain exists as a resource, with demand for on-demand supply and an integral part of cloud computing, where technologies can converge.

There are two ways to converge blockchain and cloud computing:

First, Blockchain for Cloud mainly relies on blockchain to implement distributed cloud computing architecture. Blockchain-based distributed cloud computing allows on-demand, secure, and low-cost access to the most competitive computing capabilities. Distributed applications (DApps) can automatically retrieve, search, provide, use, and release all required computing resources through the distributed cloud computing platform, making it easier for data providers and consumers to obtain required computing resources. Using blockchain smart contracts to describe the characteristics of computing resources, on-demand scheduling can be implemented. Blockchain-based distributed cloud computing may be the future development direction of cloud computing, but it is still in the theoretical research stage.

Second, Cloud for Blockchain focuses on the convergence of cloud computing and blockchain technologies, and the cloud platform becomes the carrier of blockchain services, which is the fastest way to combine blockchain and cloud computing. As we all know, blockchain technology development, testing, and proof of credit (PoC) involve multiple systems. Besides, the high cost of the stand-alone mode greatly restricts the promotion of blockchain technology. Therefore, nearly all cloud vendors globally have launched blockchain services based on their own cloud platforms. The integration of cloud computing and blockchain technologies has spawned a new cloud

service market called Blockchain as a Service (Blockchain as a Service, BaaS), which accelerates the application of blockchain technology in multiple domains and brings transformation and development to the cloud service market. The close integration of blockchain and cloud computing has promoted BaaS as a public trust infrastructure and formed a convergence trend of embedding the blockchain technology framework into the cloud computing platform. The blockchain enterprise platform to the business, represented by the consortium chain, needs to improve the blockchain ecosystem with cloud facilities. Meanwhile, blockchain to the client, represented by the public chain, needs to provide a stable and reliable cloud computing platform for decentralized applications. The integration of blockchain and cloud computing can reduce the time and cost of deployment and enhance blockchain security relying on the security of the cloud platform, which meets the requirements of rapid deployment of blockchain technologies in various industries and fields. BaaS is a new type of cloud service designed to provide back-end cloud services for mobile and web applications, including cloud data/file storage, account management, message push, and social media integration. Besides, BaaS is a cloud service in the vertical domain. With the continuous popularity of the mobile Internet, BaaS is also favored by more and more developers. As a new application development model, it can reduce the cost of development and allow developers to focus only on specific development work. BaaS falls between Platform as a Service (PaaS) and Software as a Service (SaaS). BaaS simplifies the application development process, while PaaS simplifies the application deployment process. PaaS is a development platform for executing code and managing application running environments. Users interact with the platform through code version management tools such as the version control system SVN (short for Subversion) or distributed version control system Git. In short, PaaS is like a container whose input is code and configuration files and whose output is a link to an accessible application. The BaaS platform abstracts user requirements, such as user management. Developers want to create user database tables (models) so that clients can directly operate the corresponding models through RESTful interfaces, all of which can be abstracted as CRUD [Create, Retrieve, Update, and Delete]. At the same time, BaaS defines the execution rules and the process of automatic execution of SaaS applications through smart contracts. Therefore, BaaS is somewhere between PaaS and SaaS, is application-oriented rather than just a business middleware.

BaaS services have been valued by major global companies. In April 2013, Facebook acquired Parse. In June 2014, Apple released CloudKit. In October 2014, Google acquired Firebase. Parse, CloudKit and Firebase are all well-known BaaS products abroad using Google Ventures to participate in blockchain projects and company investments and developing their own BaaS platforms with the acquired technology. By contributing to Hyperledger's open-source alliance, IBM provides blockchain services through its BlueMix platform and extends its original industry from finance to healthcare and manufacturing through blockchain. Microsoft provides its own blockchain service through Azure and builds hardware-based blockchain capabilities with Intel's SGX TEE. Besides, cloud platform vendors in China, such as Huawei, Ant Financial Service, Tencent, Inspur, and Jingdong, have

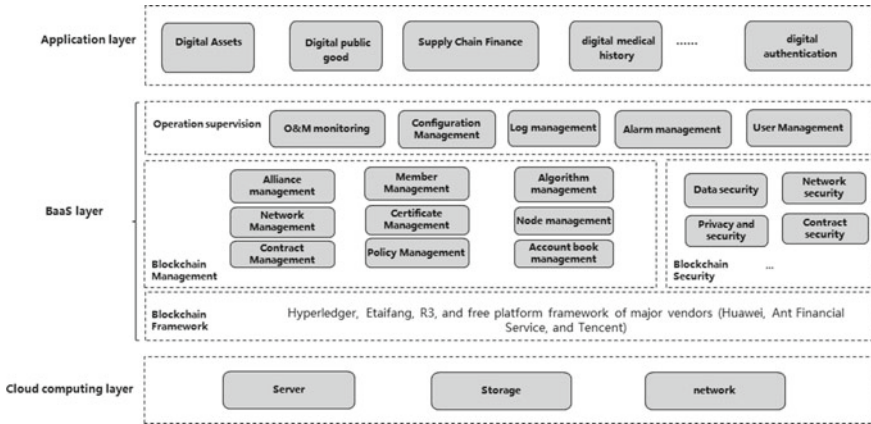


Fig. 2.2 Blockchain + cloud computing framework

developed their own blockchain platform services and built a one-cloud-one-service model. Figure 2.2 shows the blockchain + cloud computing framework.

2.3 Blockchain and IoT

In recent years, the Internet of Things (IoT), as one of the core development areas of the communications industry, is gradually evolving towards a domain-focused and ability-focused IoT ecosystem. The introduction of various emerging technologies has become an important means for the communications industry to cultivate the IoT ecosystem. Digital identity is a unique digital code after the real identity information of users or IoT devices (including objects) is condensed. It is a digital label that can be queried, recognized and authenticated. Digital identity plays an important role in the IoT environment.

Blockchain for IoT refers to the use of blockchain technology, encryption technology and security algorithm to protect the digital identity of IoT, thus building a more secure and convenient digital identity authentication system in the IoT environment. Currently, the most pressing challenges facing the IoT are data privacy, data storage security, data continuity, and data interaction compatibility. Blockchain can solve two of the most critical IoT problems. First, data is encrypted before being sent. During data transmission and authorization, an identity verification link is added. Any operation involving personal data needs to be decrypted and authorized through identity authentication. In addition, information such as operation records is recorded on the chain and synchronized to the blockchain network. Blockchain can protect the security and privacy of user data to a certain extent. Before the IoT digital identity is chained, the IoT digital identity needs to be authenticated

and endorsed by the authentication organization (such as the government and enterprise). Then, the blockchain-based digital identity authentication system ensures the authenticity of the digital identity information and provides trusted authentication services. Each device in IoT has its own blockchain address, which can be registered based on a specific address, protecting its digital identity from other devices. Authentication management of Blockchain-based IoT devices can ensure the security of a large number of original IoT devices. In addition, blockchain technology can prevent hijacked IoT devices from accessing the network, thereby further ensuring IoT network security. Second, the current IoT only connects devices for data collection and device control functions but does not have high intelligence. In the future, IoT requires networked terminal devices to have certain intelligence and cooperate autonomously under a given rule logic to complete a variety of applications with commercial value. The most significant advantage of blockchain technology is that it can provide direct transactions with untrusted intermediaries and make execution terms through smart contracts. When the conditions are met, the transaction is automatically executed.

IoT for Blockchain uses the sensor capability of the IoT to ensure the reliability of data on the chain. One of the reasons why blockchain is questioned is the authenticity of the data on the chain. How to ensure the authenticity of the data on the chain becomes the key. With the help of IoT technology, the data can be automatically chained by sensors instead of human intervention, thus ensuring the authenticity and reliability of the data on the chain. In addition, an end-to-end security defense system is constructed from various aspects of the IoT, such as device chips, terminals, network security, management platforms, and applications, so that the IoT-based security defense system can provide system security assurance for the blockchain platform.

IoT for Blockchain is widely applied. The first category is traceability application. The IoT-based NFC chip can implement traceability of objects, during which the data is chained by NFC scanning to ensure traceability authenticity. The second category is financing applications, such as financing applications based on warehouse receipts. Information scanning of warehouse receipts requires the intervention of the IoT technology to form the IoT-assisted blockchain. Then, the financing of electronic data products, such as warehouse receipts, can be realized. The third category is logistics applications. Currently, logistics applications, especially enterprise-based logistics, are expected to implement precise logistics to reduce logistics gaps and reduce logistics costs. Based on the source tracing of objects, blockchain + IoT linkage can be realized to build credible traceability of information. Figure 2.3 shows the blockchain + IoT architecture.

2.4 Blockchain and 5G

The fifth-generation mobile communication technology (5G) is revolutionary in the mobile communication field with high speed, low latency, massive access, high



Fig. 2.3 Blockchain + IoT architecture

mobility rate, and high security as the main features, which can support new multi-party business models and seamless interaction between services [3]. 5G is no longer limited to serving individuals in the 2G/3G/4G period. It focuses on diversified application scenarios, especially for enterprise applications. The three typical application scenarios supported by 5G are as follows.

First, enhanced Mobile BroadBand (eMBB) is designed to provide the ultimate communication experience under high-speed mobility. It applies to high-traffic mobile broadband services such as three-dimensional (3D), ultra-HD video, and bandwidth guarantee under high-speed mobility.

Second, ultra Reliable Low Latency Communication (uRLLC) can realize real-time information communication for automatic driving, real-time data image transmission for mobile medical care and processing of ultra-high-definition video devices for industrial manufacturing, which have high requirements on latency and reliability.

Third, massive Machine Type Communication (mMTC) is designed to meet the communication requirements of objects-to-objects. It can be applied to application scenarios that aim at sensing and data collection, such as smart cities, smart wearables, smart home devices, and industrial connections.

5G has weaknesses in user privacy protection, trust establishment in online transactions, and virtual intellectual property protection, while blockchain technology can provide transaction and property protection capabilities for 5G through cryptography and other means. In 5G for Blockchain, intelligent terminals and edge computing nodes are responsible for a large amount of computing and storage in the 5G era. As the number of blockchain nodes increases, requirements on bandwidth and latency also increase. 5G network solves local network congestion when the traffic volume increases (such as signaling response, large bandwidth, and low latency), which can be applied to Internet of Vehicles (IoV), remote video, and smart city. In addition, the 5G network can be used to improve the performance and stability of blockchain network interconnection (5G can achieve 10 Gbit/s data transmission), as shown in Fig. 2.4. Blockchain for 5G provides data protection capabilities for 5G application scenarios. Application cryptography, represented by blockchain, reconstructs networks security boundaries, establishes trust domains between devices, and implements secure and trusted interconnection [4]. In addition, blockchain technology realizes the sharing of network resources, such as the 5G spectrum, site location, and

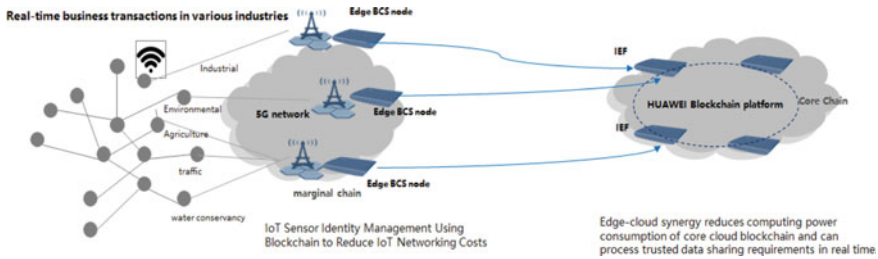


Fig. 2.4 5G for blockchain application networking

bandwidth. Meanwhile, blockchain technology allows users to pay for what they use and they need, with well-defined responsibilities and rights and transparent value allocation.

The convergence of 5G and blockchain technologies provides an efficient, secure, and fast service experience and accelerates the blockchain implementation in 5G application scenarios. 5G technology supports an efficient digital economy, while blockchain technology provides security and trust for the digital economy. The “5G + blockchain” collaboratively promotes the rapid development of applications in financial payment, smart city, IoT, Internet of Vehicles, autonomous driving, and industrial control.

2.5 Blockchain and Big Data

Big data is a data collection that is large enough to exceed the capabilities of traditional database software tools in terms of acquisition, storage, management and analysis, which is characterized by massive scale, rapid flow, diversified types, and low-value density. Big data has been widely used in people’s lives, especially in the outbreak of the COVID-19 epidemic in 2020. For example, big data has played an important role in statistics, analysis, and judgment of the epidemic. In the development process from the information technology (IT) era to the data technology (DT) era, data has become a liquid asset. By analyzing and utilizing big data, huge social and economic values can be mined. The development of big data has made significant achievements, but it also faces great challenges.

- (1) The circulation and sharing among data sources break the security boundary of original data management. Besides, the potential security risks in data flow increase.
- (2) Theft, attack, and abuse of big data resources are becoming more serious, raising higher requirements on the data security protection capabilities of countries and related institutions.

For example, Facebook’s data breach caused the unauthorized use of big data resources to be a problem. The personal data of 50 million users was leaked, which

indirectly affected the outcome of the 2016 US presidential election. Ransomware-related data recovery costs more than doubled in 2019. In 2020, ransomware with data breach mechanisms had brought higher data recovery costs to enterprises. In 2020, LifeLabs, Canada's largest medical laboratory testing services provider, experienced a massive data breach in which nearly 15 million Canadians had their personal and medical information compromised and had to pay ransoms to attackers. Experts believe that attackers use "ransomware + data leakage" to increase the amount of ransom money. Therefore, unauthorized sharing of big data not only affects user's data security, but also poses a severe threat to national security. Realizing safe and controllable circulation and data sharing is the core scientific issue for big data applications and development.

With its advantages of traceability, security, and tamper-proof, blockchain will play a vital role in solving data interconnection and open sharing to ultimately reduce information friction, break through information silos, and achieve the goal of "socialized big data". In the long run, the combination of blockchain and big data could bring great changes in social production and life. In April 2020, the China Internet Network Information Center (CNNIC) released the 45th Statistical Report on China's Internet Development, pointing out that one of the top ten trends in the big data field in 2020 is the gradual enrichment of big data application scenarios of blockchain technology [5]. According to Neimeth, by 2030, the value of blockchain distributed ledgers could reach 20% of the entire big data market, generating up to \$100 billion in annual revenue, more than PayPal, Visa and Mastercard combined [6].

The distributed architecture of blockchain and smart contracts coincide with the requirements of distributed and dynamic access control in the big data environment. Big data access control involves the collection, aggregation, management, and control of big data resources, whose architecture is divided into the basic data layer, resource management layer, infrastructure layer, transaction layer, consensus layer, and contract layer, as shown in Fig. 2.5.

- (1) Basic data layer: Basic data layer contains real big data resources, including structured data, unstructured data, and semi-structured data. Based on blockchain, distributed storage can be realized to ensure the security of the data layer of big data, avoiding the traditional distributed storage and logical centralized of data.
- (2) Resource management layer: Managing big data resources based on blockchain technology realizes the aggregation of big data resources such as File and SQL from different sources.
- (3) Infrastructure layer: The blockchain platform provides the infrastructure for big data access control, which is the foundation of the entire architecture. The infrastructure layer is the carrier of the big data access control platform transactions and smart contracts, which is based on blockchain technology and connects with upper-layer applications.
- (4) Transaction layer: The transaction layer provides transaction access control for data, policies, and contracts. For example, data transactions are used to manage big data resources and meet resource management requirements. Policy

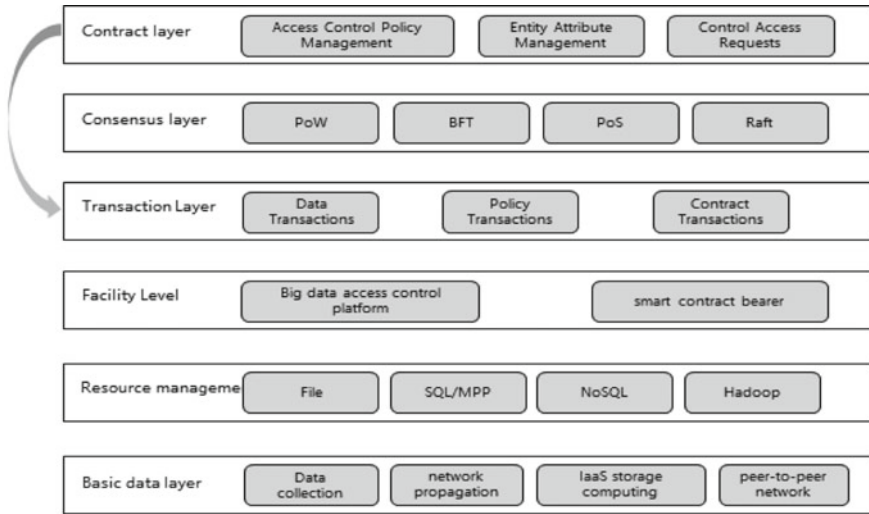


Fig. 2.5 Blockchain + big data visualization analysis platform architecture

transactions provide data support for access control policy management and contract layer. Contract transactions are linked to the smart contract of the blockchain to provide an operating environment for smart contracts.

- (5) Consensus layer: Various consensus algorithm (e.g., PoW, PoS, and BFT of blockchain) can ensure the consistency and authenticity of the access control data between distributed nodes, thus achieving a stable consensus among nodes.
- (6) Contract layer: The contract layer is linked with the transaction layer, providing functions such as access control policy management, control access request and entity attribute management.

2.6 Blockchain and Artificial Intelligence

Artificial intelligence is an intelligent body designed by humans to map perception information to actions, and can take rational actions and make decisions according to the environment [7]. The development of big data, brain-like computing, and deep learning has set off another wave of AI development [8]. Artificial intelligence mainly includes natural language processing, robotics, visual perception, image recognition and expert systems. With the development of the digital industry, blockchain and artificial intelligence can be integrated. Blockchain implements trusted and secure data transmission, while AI realizes the in-depth data analysis, as shown in Fig. 2.6.

Blockchain technology brings the following benefits to AI:

- (1) Helping AI explain the black box. A significant problem facing AI is the uninterpretable and incomprehensible nature of black boxes. Therefore, a clear audit

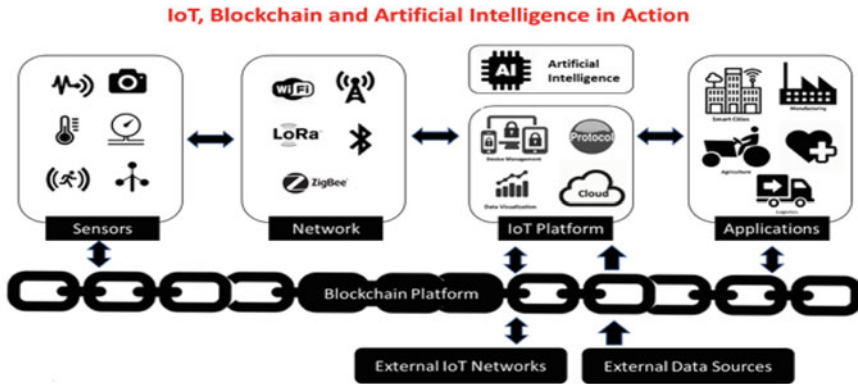


Fig. 2.6 Blockchain + AI build capability collection (Photo Source www.telecomcircle.com)

trail improves the credibility of the data and provides a clear path to trace the machine’s decision-making process. Blockchain’s tamper-proof and unforged time-stamp are undoubtedly the best solution for building audit trails.

- (2) Improving the effectiveness of AI. Secure data sharing means more data, better models, better operations, better results, and better new data. Based on the distributed database nature of blockchain, obtaining more and more authentic data is no longer a challenge.
- (3) Lowering barriers to market entry. First, blockchain will facilitate the creation of cleaner and more organized personal data. Second, blockchain will facilitate the emergence of new markets, such as data markets, model markets, and possibly even artificial intelligence markets. Therefore, data sharing, new markets, and blockchain data verification together can lower SMEs’ barriers to enter the market and narrow the competitive advantage of technology giants, and provide enterprises with more extensive data access and more effective data monetization mechanisms.
- (4) Enhancing credibility. Once part of the work of human society is managed by intelligent machines. The clear audit trail of the blockchain can promote mutual trust among intelligent machines and ultimately win human trust. In addition, blockchain technology can increase machine-to-machine interaction and provide a secure way for transactions to share data and coordinate decisions.
- (5) Reducing the probability of significant risks. Writing AI programs in DAOs with specific smart contracts that can only be executed by themselves will greatly reduce AI catastrophic accidents [9].

AI and blockchain can converge with each other for better results. Based on the traceability of blockchains, AI data sources can be corrected at a fixed point. AI, in turn, also helps blockchain technology. AI brings the following benefits to the blockchain:

- (1) The application of AI helps optimize energy consumption and therefore reduces the investment of blockchain in computing equipment.

- (2) Optimizing and understanding data on the blockchain by using artificial intelligence technologies can make the blockchain more secure and efficient, improve the intelligence of the blockchain service platform, enhance the use of natural language processing technologies on the blockchain, and make the smart contract and autonomous organizations more intelligent.
- (3) Artificial intelligence can enhance the reliability of blockchain in trade applications. In addition, the industry is exploring the use of AI to improve blockchain smart contract security.

The characteristics and pain points of blockchain and artificial intelligence determine the inevitability of combining them. Blockchain will enable isolated and fragmented AI to implement universal intelligence in a shared manner, while AI will solve the challenges of blockchain in terms of autonomy, efficiency, energy-saving, and intelligence. The values brought by the combination of the two technologies are as follows:

- (1) From the perspective of data, blockchain organizes and maintains a large amount of data decentralized based on cryptography technology, thus enabling users to control their own data and breaking the status quo monopoly by technology giants. All data on the blockchain is attached with digital signatures that related persons cannot forge. In addition, the blockchain has many other advantages, such as complete openness, high reliability, and de-trust. It can implement global data sharing and source tracing, making it possible to build a global and decentralized AI data interaction and analysis platform with larger scale, higher quality, controllable permissions, and auditability.
- (2) From the perspective of computing power, blockchain combines distributed computing with artificial intelligence, which uses large GPU or FPGA server clusters, idle GPU servers of SMEs, and idle personal GPUs as computing nodes. By sharing computing power, blockchain technology can provide computing power for AI. The combination of AI and blockchain platforms can effectively improve system performance and reduce computing power consumption.
- (3) From the perspective of the algorithm, based on various deep learning and reinforcement learning task platforms combined with the blockchain technology sharing mechanism, the AI algorithm is further optimized using collective intelligence. Multiple AI experts, instead of one company, can update and maintain one set of algorithms deciding on one set of algorithms [10].

References

1. National Institute of Standards and Technology. NIST Cloud Computing Standards Roadmap. (05 May 2020). https://www.nist.gov/system/files/documents/it/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
2. Zhou HB. Cloud computing: ICT's tower of babel. Beijing: Publishing House of Electronics Industry; 2011.

3. Chaer A, Salah K, Lima C, et al. Blockchain for 5G: opportunities and challenges. 2019 IEEE Globecom Workshops (GC Wkshps). IEEE; 2019.
4. Xu DD, Zhang YY, Zhang DL, et al. Development trend and application analysis of blockchain with 5G. *Telecommun Sci.* 2020;3:117–23.
5. China Internet Network Information Center. Statistical Report on Internet Development in China. (28 April 2020). http://www.cnnic.net.cn/hlwfyj/hlwxzbg/hlwtjbg/202004/t20200428_70974.htm
6. The complementary relationship between blockchain and big data that has to be said. (22 Jan 2019). <https://www.qubi8.com/archives/177710.html>
7. Russell SJ, Norvig P. *Artificial intelligence: a modern approach*. Malaysia: Pearson Education Limited; 2016.
8. Fang JJ, Lei K. Blockchain for edge AI computing: a survey. *J Appl Sci.* 2020;38(1):1–21.
9. What benefits will blockchain technology bring to AI technology?. (01 Sep 2018). <https://blog.csdn.net/lidiya007/article/details/82286961>.
10. What is the potential of combining artificial intelligence and blockchain. (02 Oct 2018). https://www.sohu.com/a/257435926_100217347

Part II

Application Ecology

In order to take up the strategic high ground of blockchain technology, many countries and regions around the world have made great importance to the development of blockchain industry. Several policy documents have been released to give help to the observations and application of blockchain. The role of blockchain is not only at the level of technology, platform or tools, but also in continuous reshaping of the industrial models, operation mechanisms and application environment, thus forming a blockchain application ecosystem that integrates infrastructures, technologies, applications and policies with the participation of multiple parties.

Chapter 3

Blockchain Application Status and Ecology



Xiaodan Tang, Zijun Jia, and Wei Yang

Abstract In order to give a general view of the status of blockchain applications, an application-centered viewpoint is applied to the research of advancement both worldwide and in China. To begin, the policy aspects and application progresses are investigated, with the conclusion that governments are increasingly focusing on blockchain technology and application development. A Blockchain application ecosystem model is proposed, which includes three layers: environmental, organizational and information system. The evolution of blockchain infrastructures, including EBSI, Diem, BSN, and other projects is examined, and an infrastructure ecosystem model is provided based on current trends. In terms of blockchain technology ecology, five prominent blockchain open source communities worldwide and in China are outlined, and the characteristics of global blockchain open source communities are discussed.

Keywords Blockchain · Blockchain application · Ecosystem · Infrastructure · Open source community

3.1 Global Blockchain Application Development

3.1.1 National Policies and Regulations

As one of the most cutting-edge computing paradigms, blockchain technology has attracted a lot of attention and support from governments around the world. In recent years, many governments have begun to turn their focus from observing and monitoring to regulation formulation and strategic deployment of blockchain. China,

X. Tang (✉)
China Electronics Standardization Institute, Beijing, China
e-mail: tangxd@cesi.cn

Z. Jia
China Center for Information Industry Development, Beijing, China

W. Yang
Digital City Company, China Xiongan Group, Xiongan New Area, Hebei, China

Australia, and Germany have invested heavily in the blockchain industry and have proposed comprehensive industrial adoption plans. South Korea, Japan, Singapore, the United Kingdom, and the European Union have given importance to blockchain technology observations and application exploration.

In the United States, the Department of Defense, the Department of Health, the Postal Service and other departments place great emphasis on blockchain's application potential, while state governments such as Delaware and Illinois are exploring blockchain applications in business registration and equity management. Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) have funded a number of projects on blockchain technology. The Department of Defense released its Digital Modernization Strategy in July 2019, which supports blockchain trials on secure data transfer. In April 2022, the Senate introduced a bill to promote development of a national strategy for the research and development of distributed ledger technologies and their applications [1].

In the European Union (EU), the European Blockchain Partnership (EBP) was created in April 2018, and the European Blockchain Services Infrastructure (EBSI) was launched, with the goal of offering cross-border public services utilizing blockchain technology [2]. According to a report released in 2021 by the European Commission, the Horizon 2020 has funded 43 blockchain-related projects for a total grant amount of €172 m [3]. In September 2019, Germany published the world's first national strategic policy document on blockchain, the Blockchain Strategy of the German Federal Government [4]. It defines the strategic positioning, implementation principles, and strategic actions for blockchain industry adoption and proposes 44 concrete measures which are divided among 11 ministries.

In Australia, the Ministry of Industry, Science and Resources released the National Blockchain Roadmap in February 2020 [5], focusing on three key areas of developing regulations and standards, skills, capabilities and innovation, as well as international investment and cooperation. It proposes 12 initiatives to promote the development of Australia's blockchain industry from 2020 to 2025, including the establishment of a National Blockchain Roadmap Steering Committee, promoting relevant application pilots, and supporting blockchain start-ups and investments.

3.1.2 Industry Application Practice

Many businesses have jumped on the blockchain development bandwagon and have steadily boosted their blockchain investment. Global mainstream financial institutions are actively laying the groundwork for research and application of blockchain. American Express, Goldman Sachs, JP Morgan Chase and UBS are among the financial firms that have laid out blockchain by establishing blockchain labs, investing in blockchain startups and developing blockchain applications. More blockchain technology and service providers have entered the market, including IT enterprises and consulting firms, such as IBM, Microsoft, Oracle Intel, Microbank, Deloitte, etc.,

offering a variety of products and services including blockchain underlying platforms, BaaS platforms and blockchain solutions. Technical forces such as universities and institutes are increasing their investment in the blockchain field, hastening the development of the technical ecology. More users are paying attention to, exploring and promoting the application of blockchain in various sectors such as financial services, intelligent manufacturing, supply chain management and cultural entertainment.

The exploration of blockchain applications in the real economy has been accelerated by traditional businesses. Blockchain technology was initially viewed as a technology for cryptocurrencies after its inception. Things did not change until a few years later when the potential value of blockchain-based applications was better understood, and some businesses began to accelerated their exploration of its application in the real economy including the Internet of Things, supply chain, energy management and healthcare. For example, Walmart has asked its leafy green vegetable suppliers to adopt a blockchain-based tracking system to digitally track the flow of products from suppliers to merchandise shelves and finally to consumers, datamining and recording traceability information to a unified storage platform, reducing the process of tracing products from days to 2 s [6]. Maersk and IBM have collaborated to develop TradeLens, a supply chain platform that uses blockchain technology to ensure real-time access to shipping data and documents for multiple related parties, in order to help manage and track shipping paperwork and improve the efficiency and security of shipping. As of January 2022, the platform's alliance has over 300 partners, and has processed over 2.7 billion shipping events and 26 million shipping documents. Its partners includes shipping companies such as Shipper, Maersk, Hamburg Süd and PIL, customs in the Netherlands, Saudi Arabia, Singapore, Australia and Peru, as well as more than 20 ports, and several freight forwarders and logistics firms [7, 8].

3.2 Development of Blockchain Applications in China

3.2.1 Policy Support

In China, blockchain technology is positioned as one of the new-generation information technologies. The central and municipal governments have increased their support for blockchain technology and application innovation. The blockchain industry is listed as one of the emerging digital industries in the 14th Five-Year Plan [9], and it is proposed to develop blockchain service platforms and application solutions in sectors such as financial technology, supply chain finance and government services with a focus on consortium blockchain. The Ministry of Industry and Information Technology and the Office of Central Cyberspace Affairs Commission jointly issued the Guidance on Accelerating the Application and Industrial Development of Blockchain Technology [10] in June 2021, which listed tasks including using blockchain to empower the real economy and improve public services, strengthening

the industrial foundation, consolidating the industrial foundation, building a modern industrial chain and promoting the innovation of integrated technologies. In January 2022, the Office of Central Cyberspace Affairs Commission, along with 17 other ministries, announced a list of 179 national blockchain innovation application pilots [11]. Early in January 2019, the Cyberspace Administration of China issued the Regulations on the Administration of Blockchain Information Services, with the goal of regulating the subjects and activities of providing blockchain-based information services [12]. By the end of March 2022, the Cyberspace Administration of China has issued 7 batches of a total of 1705 blockchain information services.

Meanwhile, municipal governments are actively encouraging blockchain applications and industrial development, as well as executing policies and measures to support local industrial development. As of December 2020, more than 10 provinces/municipali/autonomous regions have adopted blockchain-specific support policies, such as Beijing, Hunan Province, Guizhou Province, and Jiangsu Province.

3.2.2 Industry Application Practices

In China, blockchain applications have expanded into sectors such as financial services, smart manufacturing, culture and entertainment, public services, smart city. The application scenarios include supply chain finance, product traceability, data sharing, evidence deposition and forensics, electronic invoice, etc. Government, enterprises, universities and institutions are all among the types of participants.

Financial services is not only one of the earliest blockchain application sectors, but also with the highest degree of popularity. Financial institutions such as the Industrial and Commercial Bank of China, Bank of China, China Merchants Bank, and Webank have accelerated their exploration of blockchain applications in scenarios including fund asset management, evidence deposition and forensics, and supply chain finance. Blockchain has also become one of the Central Bank Digital Currency (CBDC) enabling technologies. The White Paper on the Progress of China's Digital RMB [13] states that the digital RMB can achieve programmability by loading smart contracts without influencing the currency's functionality.

Another sector where blockchain applications are actively being explored is supply chain management. Core supply chain enterprises, commercial banks, e-commerce platforms and other associated forces have pushed for the adoption of blockchain applications, and a large number of new applications have arisen. Technology companies such as JD Technology and Ant Group, for example, have invested in blockchain-based anti-counterfeiting and traceability applications for food and medicine, and blockchain is proven to be an effective means of ensuring food and medicine safety.

Blockchain applications in public services have also made significant progress. Blockchain-based applications such as government data sharing, judicial depository, electronic invoice, and public resources trading have emerged. Blockchain has played a key role in upgrading public services and improving people's quality of life by

promoting data sharing, optimizing business processes and enhancing synergistic efficiency. The Supreme People's Court has created a unified platform for judicial blockchain, which has established 32 nodes and realized 12.65 million items of data on the Internet as of May 2020 [14]. The Beijing Municipal Bureau of Economic and Information Technology has established a directory blockchain, which has integrated the government data directories of more than 60 departments in the city [15].

3.3 Blockchain Application Ecology

Ecological theory is currently widely applied to various domains, including business ecosystem, industrial ecosystem, innovation ecosystem and information ecosystem [16–18], with a focus on topics such as operation mechanism, development path and development evaluation of these ecosystems. Li et al. [17] divided the industrial ecosystem into three subsystems: innovation ecosystem, production ecosystem and application ecosystem, among which the application ecosystem focuses on the application aspects of products such as users, complementary products, competitive products, distribution channels, after-sales service and user communities.

In the domain of blockchain technology, the ecological theory have been applied in many efforts on blockchain industry, systems and applications. The 2018 White Paper on China's Blockchain Industry [19] provides a blockchain industry ecology map covering three modules: infrastructures and platforms, industry services, and industrial applications. Syed et al. [20] sorted out the main technologies and platforms in the blockchain ecosystem. Riasanow et al. [21] proposed a generic blockchain ecosystem model with 7 categories of stakeholders, as well as elements and services when the stakeholders interact. By examining blockchain application projects, Lopes et al. [22] outlined an application-centric blockchain project ecosystem, focusing on seven typical types of application projects such as fintech and value exchange. Zhang [23] examined the influence of blockchain on e-commerce information ecosystem and studied the information ecosystem model in the e-commerce blockchain application. Cai et al. [24] proposed that the blockchain industry ecology encompasses ecological domains such as the underlying platform, top layer applications, technological research, media and community, and investor. Lin et al. [25] suggested a blockchain entrepreneurial ecosystem model with the enterprises as the core, and the policy, finance, market, technical, service environment, and user organization as the environment. ISO 23257:2022 [26] provides a user view of blockchain systems, dividing parties around blockchain systems into 6 roles: users, administrators, providers, developers, governors, auditors, and detailing the blockchain-system-related activities of these roles.

However, research on the generic blockchain application ecosystems has not yet been reported, and activities such as blockchain applications research, planning, implementation and regulation necessitate a comprehensive understanding of blockchain application ecosystems. This book presents a blockchain application ecosystem model with blockchain application products at its core, as illustrated in

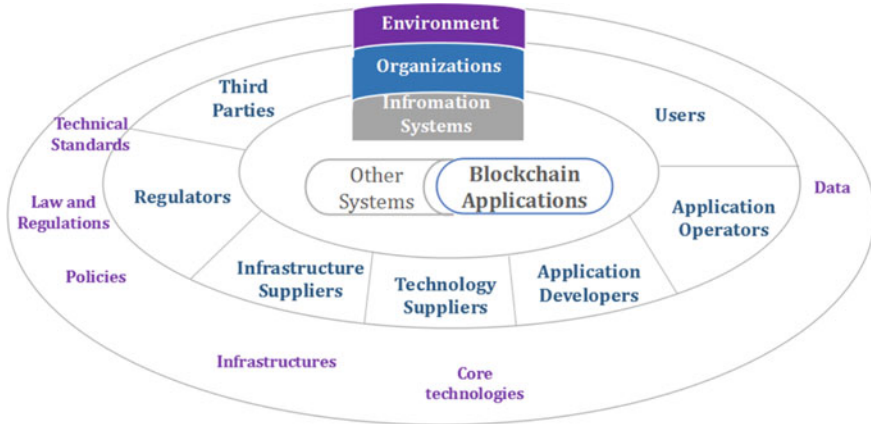


Fig. 3.1 Blockchain application ecosystem model

Fig. 3.1. The model examines a series of activities such as planning, design, development, maintenance, promotion, use, governance, regulation and auditing around blockchain application products and their effects under the current policies, technologies, infrastructures and other environmental conditions by stakeholders such as blockchain users, technology providers, application operators and regulators.

3.4 Blockchain Infrastructure Development Status and Ecology

3.4.1 Overview

Blockchain is positioned as the cornerstone of the future Internet in the Blockchain Strategy of the German Federal Government. Some experts have suggested that blockchain can be regarded as one of the key infrastructures of the Internet of Value. Blockchain infrastructure has become one of the keywords in the global blockchain industry, especially since 2019, indicating that blockchain exploration has reached a critical stage of scaled-up application.

The early Bitcoin and Ethereum networks were both realized by public blockchain, with nodes implemented all over the world, providing the necessary basic services for application developers and users, and already had the attributes of infrastructures. However, the modes and domains of applications based on the two network were limited because of the limit of public blockchain. Many enterprise-level blockchain infrastructures have been built in the industry as the exploration of blockchain-based industrial applications accelerates, with the development of consortium blockchain

technology. For example, a variety of BaaS platforms were built to support the enterprise-level blockchain applications.

Generic blockchain infrastructure needs to facilitate large-scale collaboration and resource integration, which necessitates a certain industry base, especially on application developing level, policy support strength, and technical standardization foundation in the industry. At present, generic blockchain infrastructure is one of the most typical trends in blockchain industry. Generic blockchain infrastructure can support blockchain applications in multiple sectors across a larger regional scope, effectively reduce the costs of blockchain applications, lower the application threshold and promote application cultivation. It's also beneficial for facilitating the supervision of blockchain applications, enhancing standardization of blockchain applications, accelerating the penetration of blockchain technology and accelerating adoption of large-scale applications. The concept of generic blockchain infrastructure has been implied in concepts like "Internet of Value" and "Programmable Society" which were proposed around 2015.

3.4.2 Blockchain Infrastructure Projects

EBSI. The EBSI is aimed to build a network of distributed nodes across EU to facilitate the development of applications in various specific sectors, with the goal of using blockchain technology to provide EU-wide cross-border public services [2]. The EBSI is expected to be a key component of the Connecting European Facility (CEF), providing reusable software, services and technical specifications for EU institutions and European public administrations. The European level nodes will be operated by the European Commission while the national level nodes will be operated by the Member States. In 2019–2020, the EBSI project obtained a €4 million budget, and 4 use cases in identity, diploma, traceability and trusted data sharing were built [2].

Libra. In terms of financial infrastructure, in June 2019, a Facebook subsidiary published the Libra White Paper outlining plans to build a consortium blockchain and issue a low-volatility cryptocurrency tied to a basket of fiat currencies. Libra was described as "a simple global currency and financial infrastructure that empowers billions of people" [27]. In the months following the publishing of the white paper, the Libra project was widely deputed and questioned as it did not fully explore integration with national regulatory frameworks. The Libra Association garnered early engagement from companies in payments, social media and investment industries, with totally 28 initial members. However, payment firms including Visa, Paypal and Mastercard declared their departure from the Libra in the following months. To enhance the compliance, the Libra project released the Libra 2.0 White Paper in April 2020 [28], with a plan to introduce stablecoins anchored in a single currency. Libra was renamed Diem in December 2020, and was positioned to be a complementary stable currency to fiat currencies instead of a standalone digital asset [29]. However, the project was then sold to Silvergate in January 2022. This project has

gone from pursuing complete isolation from regulation to gradually compromising with regulation, which may be said to be a typical practice of investigating the path of constructing blockchain infrastructure.

Infrastructure projects in China. Several institutions in China are attempting to develop blockchain infrastructures. The State Information Center, China Mobile, China UnionPay, and other 6 businesses collaborated to design and build the Blockchain Service Network (BSN) in October 2019, with the goal of providing a blockchain resource environment for developers. The project has developed more than 120 city nodes around the world as of October 2020. The Xinghuo Blockchain Infrastructure and Facility which was established by the China Academy of Information and Communications Technology in collaboration with other businesses, takes the industrial Internet as its main scenario and network identifier as a breakthrough to encourage the development of blockchain applications.

Table 3.1 shows typical blockchain infrastructure projects.

A city-level blockchain infrastructure. As shown in Fig. 3.2, the blockchain infrastructure in a city of China includes platform administration, blockchain management, resource management and other services that enable reliable information sharing among multiple parties and interconnection of multiple blockchain systems. It enables the development of a wide range of upper-layer applications based on multiple blockchain underlying infrastructures. Data in each blockchain is not only protected but also interconnected between systems, so as to horizontally connect various blockchain systems and carry a broader range of applications. The city-level blockchain infrastructure network can provide a convenient public resource environment for various blockchain applications, lowering the repeated construction of multiple isolated local blockchain networks, reducing the cost, technical threshold and supervision difficulties, and solving the problems of cross-chain interconnection of heterogeneous underlying systems.

Table 3.1 Typical blockchain infrastructure projects

No	Name	Initiating parties	Initiating time	Domain
1	The European blockchain services infrastructure (EBSI)	The European Blockchain Partnership (EBP)	April 2018	Cross-border public services
2	Diem (Libra)	More than 20 companies including Facebook	June 2019	Financial services
3	Blockchain-based service network	The State Information Center, China Mobile, China Unionpay, etc	October 2019	Multi-industry application
4	Xinghuo blockchain infrastructure & facility	CAICT, Beijing University of Aeronautics and Astronautics, China Unicom, etc	September 2019	Industrial Internet

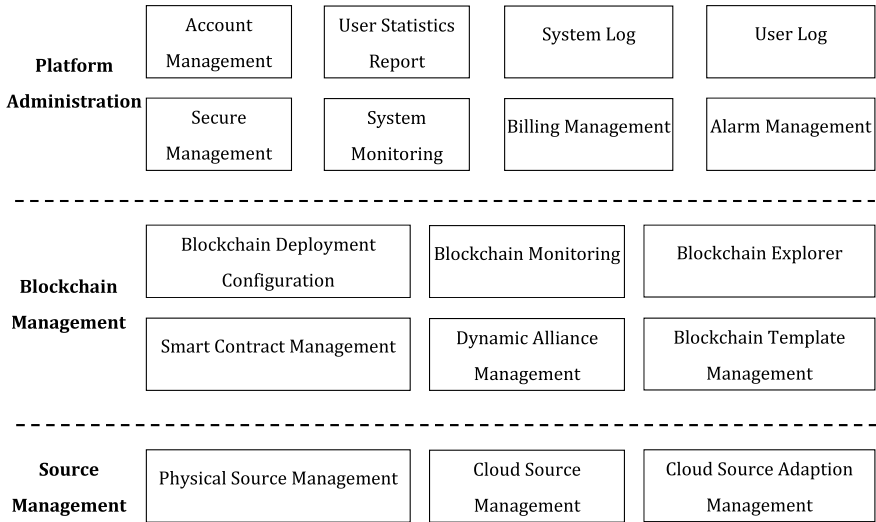


Fig. 3.2 A city-level blockchain underlying infrastructure architecture

3.4.3 Blockchain Infrastructure Ecology

The blockchain infrastructure ecology model is summarized based on the analysis of typical projects, as is shown in Fig. 3.3.

The infrastructure developer is the party that designs, develops and maintains the infrastructure’s hardware and software. The infrastructure operator is the party that manages the infrastructure’s resources and capacity, as well as operates and maintains the entire infrastructure. The application developer is the party that uses the infrastructure to develop various applications based on the needs of customers.

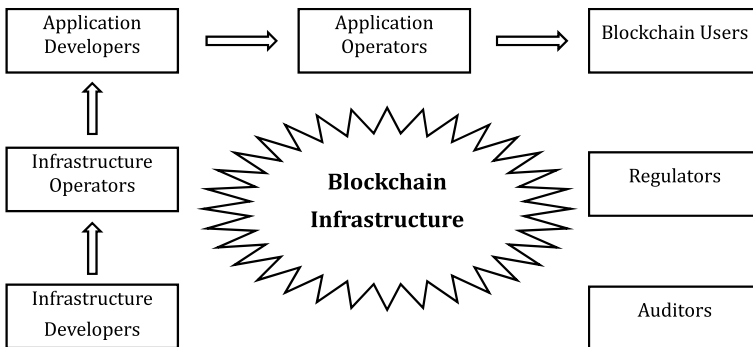


Fig. 3.3 Blockchain infrastructure ecology model [30]

The application operator is responsible for publishing and managing the blockchain-infrastructure-based applications. The blockchain user is the party who uses the applications based on blockchain infrastructures. The regulator is in charge of supervising the entire blockchain infrastructure, and the auditor is in charge of cooperating with other parties to ensure that the blockchain infrastructure and applications are compliant.

3.5 Blockchain Technology Ecology

3.5.1 Overview of the Technology Ecosystem

1. Development of Technology Ecosystem

At present, blockchain technology is still undergoing development and evolution, with innovations in technologies like consensus mechanisms, zero-knowledge proofs, multiple signatures, cross-chain transactions emerging. The development of new technologies is accelerating, as research into the fundamental theories of blockchain become more active. The number of patent applications in blockchain field is increasing rapidly since 2015, from 1540 in 2016 to 21,298 in 2020. China has a fast growing number of blockchain patent applications, accounting for more than half of the total number. Since around 2017, there has seen a significant increase in the number of academic papers published in the blockchain field, indicating that research on the core technologies and fundamental theories of blockchain has progressed.

2. Growth of Technology Ecology Participants

The influence of specific individuals and groups was more visible in the early days of blockchain technology, which was originally born in the technical geek community. Satoshi Nakamoto, the creator of Bitcoin, and Vitalik, the founder of the Ethereum project, both had a significant impact on the development and direction of blockchain technology. At the time, the blockchain technology ecosystem was rather niche, with technological innovation focused on addressing the technical needs of cryptocurrencies, such as certain small-scale industry applications built on top of cryptocurrencies. The number of participants in blockchain theoretical research and technological innovation grew rapidly only after blockchain technology was recognized as a general technology that could be widely used in various industries. A richer and more hierarchical technological ecology pattern emerged then, with universities and institutes focusing on theoretical research and fundamental technology, and enterprises focusing on engineering and application technologies.

3.5.2 Open Source Community

Blockchain open source communities have grown fast in recent years, and has increasingly become an essential source of global blockchain technology innovation. Blockchain open source communities in China have begun to bear fruit, and their influence in the market has gradually increased, providing strong support for blockchain technology innovation and application exploration in China.

1. Global Blockchain Open Source Communities

The creation of blockchain open source community correlated with the emergence of the blockchain concept. Bitcoin, as the first application of blockchain technology, also spawned the first blockchain open source community. After more than a decade, Hyperledger and Ethereum are two of the most influential blockchain open source communities in the international arena.

Hyperledger is an open source community launched by the Linux Foundation in 2015. As of the end of 2019, the Hyperledger open source community had 275 members, 14 active working groups and interest groups [31]. It has promoted 15 open source projects in the form of distributed ledger frameworks, libraries and tools. The most popular project of Hyperledger is Fabric, and many cloud computing platforms, such as Amazon, Google and Microsoft, Alibaba, Tencent, JD, Baidu, support Fabric-based services [31].

The Ethereum project launched by the Ethereum Foundation in 2013 is the first open source blockchain project to support smart contracts, and various DApps are already running on the Ethereum network. Recognizing the growing demand for blockchain technology in the enterprise market, the Enterprise Ethereum Alliance (EEA) was formed in 2017, with more than 500 organizations joining by now. In march 2019. A development report [32] showed Ethereum had an averaged of 99 core protocol developers and 216 application developers per month in the past 10 years, and a total of 9727 core protocol code and nearly 40,000 project-level code submissions. Ethereum is currently the most active public blockchain open source community.

2. Blockchain Open Source Community in China

The blockchain open source communities in China has a fast developing speed despite of late start. In recent years, the industry has paid more attention to the blockchain open source communities. One of the characteristics of blockchain open source communities in China is that they are mainly initiated and promoted by companies with a strong base, with representative projects such as FISCO BCOS, JD Chain, and XuperChain.

FISCO BCOS was developed under the direction of Webank. Its open source ecosystem is gradually taking shape and new applications are arising rapidly. As of December 2020, the FISCO BCOS open source ecosystem has attracted more than 2000 businesses and 40,000 developers, and more than 120 applications running in the

production environment. Applications supported by FISCO BCOS include financial applications in scenarios like payment, reconciliation, transaction clearing, supply chain finance, and credit collection, as well as applications in other industries like judicial arbitration, cultural copyright, entertainment, games, social management and government services. Some of the applications built on FISCO BCOS are beginning the scalization process, such as the inter-institutional reconciliation platform, which has supported over 100 million transactions, and the judicial depository platform, which has over 1 billion certificates.

JD Chain is developed by JD Technology, which was open sourced in March 2019. JD Chain has supported blockchain applications in various sectors including financial services, judicial depository, medical care, supply chain traceability, copyright protection and digital marketing. JD Chain's anti-counterfeiting traceability platform had 1 billion traceability on-chain data, over 1000 partner brands as of September 2020.

XuperChain is a blockchain underlying technology developed by Baidu that was open source in May 2019. It has been used in the fields of justice, copyright, edge computing, data collaboration, traceability, e-government, intelligent healthcare, and other sectors. In 2020, the XuperChain accumulated 660 code commits, 37 contributors, more than 10,000 uses by developers, and a community of 10,000 people. Xinpu Depository Platform, Baidu Library, AIBank, SPD Bank and Beijing Internet Court are among the businesses and platforms that were supported by XuperChain.

3. Characteristics of the Global Blockchain Open Source Community Development

The open source ecology grows and evolves. The number of participants involved in the blockchain open source communities has exploded in recent years, and their roles have been expanded as well. Participants who implement various commercial application scenarios based on platform products have emerged in the open source community, including developers, investors, integrators, application developers and third-party security audit companies, promoting prosperity of the ecology around blockchain applications.

The application support effect has become increasingly significant. While early blockchain open source communities were mainly focused on supporting cryptocurrencies and related applications, the open source communities focused on consortium blockchain, such as Hyperledger, have supported the development and exploration of enterprise-level blockchain applications on a larger scale. At present, blockchain applications based on open source communities have penetrated into a number of sectors such as fintech, judicial deposition, smart healthcare, product traceability, and copyright protection, supporting a number of typical industrial applications.

References

1. National R & D Strategy for Distributed Ledger Technology Act of 2022[EB/OL], 15 June 2022. <https://www.congress.gov/bill/117th-congress/senate-bill/4109>
2. Introducing the European Blockchain Services Infrastructure (EBSI)[EB/OL], 29 April 2020. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi>
3. European Commission. Blockchain in Practice: Promoting blockchain and DLTs in European SMEs. 2021
4. Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen. Blockchain-Strategie der Bundesregierung. 2019
5. Australia government. The National Blockchain Roadmap. 2020
6. Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric [EB/OL]. 15 June 2022. <https://www.hyperledger.org/learn/publications/walmart-case-study>
7. Tradelens Solution Brief (Edition Two) [EB/OL]. 15 April 2020. <https://tradelensweb-assets.s3.us.cloud-object-storage.appdomain.cloud/TradeLens-Solution-Brief-Edition-Two.pdf>
8. Tradelens Network [EB/OL]. 01 July 2021. <https://www.tradelens.com/network>
9. The Outline of the People's Republic of China 14th Five-Year Plan (2021–2025) for National Economic and Social Development and Long-Range Objectives for 2035. 2021.
10. Ministry of Industry and Information Technology, the Office of Central Cyberspace Affairs Commission. The Guidance on Accelerating the Application and Industrial Development of Blockchain Technology. 2021.
11. China selects pilot zones to take part in blockchain trials [EB/OL]. 31 January 2022. <https://www.itpro.co.uk/technology/blockchain/362098/china-launches-blockchain-pilot-projects-across-nation>
12. Cyberspace Administration of China. The Regulations on the Administration of Blockchain Information Services. 2019.
13. The People's Bank of China Digital RMB R&D Working Group. The White Paper on the Progress of China's Digital RMB. 2021.
14. The Supreme People's Court of the People's Republic of China. Opinions of the Supreme People's Court on Strengthening Blockchain Application in the Judicial Field. 2022.
15. Directory blockchain covers 60 departments in Beijing [EB/OL]. 13 January 2020. https://www.sohu.com/a/366539516_99983415
16. Letaifa SB, Gratacap A, Isckia T. Understanding business ecosystems: how firms succeed in the new world of convergence?. De Boeck, 2013.
17. Li XH, Liu F. Industrial ecosystem and strategic emerging industries development. *China Ind Econ.* 2013;3:20–32.
18. Soniecky S. Ecosystems knowledge: modeling and analysis method for information and communication. Wiley-ISTE, 2018.
19. Information Center of Ministry of Industry and Information Technology of the People's Republic of China. China Blockchain Industry White Paper 2018[EB/OL]. 20 May 2018. <https://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf>
20. Syed TA, Alzahrani A, Jan S, et al. A comparative analysis of blockchain architecture and its applications: problems and recommendations. *IEEE Access.* 2019;7:1–32.
21. Riasanow T, Burckhardt F, Setzke D S, et al. The generic blockchain ecosystem and its strategic implications. In: 24th Americas conference on information systems (AMCIS); 2018. p. 1–10.
22. Lopes J, Pereira JLM. Blockchain projects ecosystem: a review of current technical and legal challenges. In: World conference on information systems and technologies 2019 (WorldCIST'19). Berlin: Springer; 2019. p. 83–92.
23. Zhang YB. A model of E-commerce information ecosystem based on blockchain. *Res Library Sci.* 2018;(6):33–44.
24. Cai L, Li QL, Liang XB. Blockchain technology advanced and actual combat. Beijing: The People's Posts and Telecommunications Press; 2018.

25. Lin Y, Zhang QQ, Wang SS. Evaluation on operation effect of blockchain entrepreneurial ecosystem. *Stat Decision* 2019;35(22):37–41.
26. ISO/TC 307. Blockchain and distributed ledger technologies—Reference architecture: ISO 23257:2022.
27. The Libra Association. *An Introduction to Libra*. 2019.
28. The Libra Association. *Cover Letter: White Paper 2.0*. 2020.
29. Diem White Paper[EB/OL]. 21 February 2021. <https://www.diem.com/en-us/white-paper/#cover-letter>
30. Tang XD. Trends of blockchain infrastructure. In: *Annual Report on China's Mobile Internet Development (2020)*. Beijing: Social Sciences Academic Press. 2020. p. 296–307.
31. Hyperledger website. <https://www.hyperledger.org/>
32. Electric Capital. *Developer Report 2020*. https://github.com/electric-capital/developer-reports/blob/master/dev_report_2020.pdf

Part III

Application Methods and Practices

The development of blockchain technology and its integration with other technologies have led to the expansion of blockchain applications both vertically and horizontally. In the vertical domain, this is reflected in the in-depth application of blockchain infrastructure, general technology, core technology, privacy and security. In the horizontal field, besides the applications in the fields of digital currency and finance, blockchain has also made valuable integration with logistics, government services, culture and education, and people's livelihood, and has accumulated rich practical experience in application, forming the "blockchain+" model in the digital economy era.

Chapter 4

Blockchain Application Implementation Roadmap



Yaling Liao and Yabo Zhang

Abstract Other than cryptocurrencies, blockchain applications have landed in multiple industries after 2019, such as finance, government affairs, energy and agriculture. Blockchain application implementation roadmap is the most helpful toolkit for any organization that wants to enter the blockchain field. Check the core application value framework of blockchain to figure out the needs, follow the blockchain application implementation path and use the blockchain application scenario selection methods, then a final conclusion of the suitability of applying blockchain will be drawn.

Keywords Core value framework · Implementation path · Scenario selection methods

4.1 A Panoramic Overview of Blockchain Applications

In the early stage, blockchain technology was mainly applied in the field of cryptocurrency based on public chain, but with the rise of consortium chain in 2015, the application of blockchain technology gradually shifted to many fields of social economy and began to try large-scale applications [1]. In the process of blockchain technology development, public chains are still unable to meet the requirements of large-scale commercialization in terms of performance, privacy and security, etc. In contrast, consortium chains are more mature in terms of technology and more practical in application implementation. Nowadays, blockchain technology is combined with other technologies to utilize the powerful productivity and intrinsic value of data to build the infrastructure of digital information system, which more effectively promotes the development of digital economy and digital society [2].

After 2019, international blockchain applications mainly include blockchain infrastructure, privacy and security, scientific research, computing and data storage, identity identification, financial industry, supply chain and logistics, business and

Y. Liao (✉) · Y. Zhang
WanXiang Blockchain Company, Shanghai, China
e-mail: milu_yaya@163.com

retail, social networking and communication, information technology industry, business services and consulting, real estate industry, asset management, medicine and health industry, entertainment and education, energy and facilities, transportation, tourism, etc. Chinese blockchain applications have landed in multiple industries such as finance, supply chain, government affairs, agriculture, and energy.

Blockchain technology makes it possible to enhance the trust and traceability of data in the digital world, which has greatly promoted the development of the digital world and has combined with industrial applications to build numerous application models.

- (1) Underlying technology and infrastructure: Blockchain-based basic protocols and blockchain technology combined with hardware development.
- (2) General application and technology expansion: Based on blockchain technology, we develop general application and based on blockchain technology, including but not limited to joint computing, cross-chain applications, smart contracts, information security, privacy protection, blockchain-as-a-service (BaaS), deposition, etc.
- (3) Blockchain industry applications: At the current stage, blockchain technology has been combined with many industries to provide technical support to various industries to overcome the pain points of various industries, which include finance, logistics, energy, public welfare, agriculture, medical, entertainment, intellectual property, tourism, real estate, manufacturing, government, audit, law, etc.
- (4) Peripheral services: Blockchain technology is combined with peripheral services to build community services and developer tools.

4.2 Blockchain Core Application Value

Blockchain has great application value in various industries because it can better realize multi-party collaboration and quickly establish trust relationships at low cost. Since it can effectively solve the trust issues such as data trustworthiness, asset trustworthiness, and cooperation trustworthiness, it is important for the security and control of data and transactions in many fields such as finance, government, industry, and agriculture [3, 4].

Data trustworthiness mainly refers to the secure storage and computation of data. The technical features of blockchain, such as distributed ledger, data traceability, tamper-proof, and automatic execution of smart contracts, ensure trustworthy data storage and computation, which makes it a natural fit for applications in the fields of data storage and traceability, audit and supervision.

A smart contract is a tamper-proof and automatically executed computer program that is triggered by a predetermined event. Therefore, by supporting the automatic execution of transaction rules between subjects through smart contracts, the trust problem in the collaboration of multiple subjects can be well solved, and the collaboration between subjects can be trusted.

Blockchain can solve the trust problem between enterprises and promote the interconnection of upstream and downstream ecology and cross-industry ecology; smart contracts support the digitization of business, build digital assets, and make digital assets circulate in the ecology, thus creating digital ecological value.

Blockchain is a tool to build trust, with its tamper-proof, easily traceable, decentralized or polycentric characteristics, it ensures the authenticity and traceability of data, reduces the audit process, and lowers the cost of external supervision. Based on this, we propose the core application value framework of blockchain, as shown in Fig. 4.1.

From the blockchain data level, the blockchain data storage structure ensures that the data can be verified, the consensus mechanism ensures the consistency of multi-node data, the cryptography ensures the security of data transmission and access between nodes [5]. The smart contract composed of code automates the operation of rules and data, which effectively prevents data tampering and allows complete traceability of data-based application processes. From the blockchain IT architecture level, multiple nodes jointly maintain the same ledger and can maintain data consistency based on the consensus of multiple parties, which realizes the characteristics of polycentric or decentralized, open and transparent, tamper-proof, and traceable; from the blockchain application level, blockchain can verify and tamper-proof the data by multiple parties, which ensures data trustworthiness, transaction trustworthiness, and asset trustworthiness, and can make the service trustworthy through the

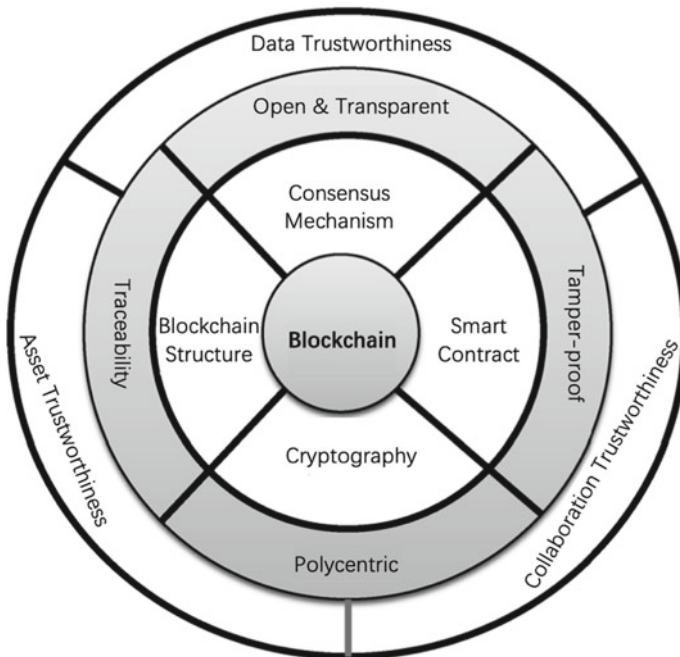


Fig. 4.1 Blockchain core application value framework

smart contract executed automatically. The trustworthy digital social credit system established based on blockchain has a low-cost trust foundation, which makes the collaboration and cooperation of multiple parties in business more credible.

4.3 Blockchain Application Concerns

For blockchain applications to play their strategic value, they must be able to fully recognize the core application value of blockchain and provide commercially viable solutions that can be applied on a large scale. In recent years, blockchain technology has been combined with industrial applications to produce many innovative application models in three areas: government, people's livelihood and business.

In the financial industry, the requirements for authenticity, security and efficiency are very high, and the core application values of blockchain, namely data trustworthiness, asset trustworthiness and collaboration trustworthiness, naturally fit the requirements of the financial industry [6]. In the various business processes provided by the financial industry, there are business pain points such as trust problems, efficiency problems, and default risks, etc. Blockchain is a good match for these pain points and can systematically solve them. For example, in the banking industry, cross-border payment has long been a pain point for the banking industry. Blockchain's features of disintermediation, tamper-proof, traceable and transparent transactions can eliminate the need for third-party intermediaries, shorten the cycle of cross-border payment, reduce costs, and improve the transparency of transactions.

Blockchain has also been applied in many other fields. For example, in the field of supply chain and intellectual property, the use of blockchain for digitization of assets has solved the problem of data ownership rights and the problem of data ownership certainty, thus enabling digital assets to be managed, traded, and transferred [7]. Therefore, blockchain has become the infrastructure of digital economy, and with the construction and development of digital society, blockchain applications are gradually being implemented in various fields.

Of course, there are still many difficulties in the commercial implementation of blockchain, such as performance bottlenecks, security issues, regulatory issues, and conflicts between the decentralized or polycentric operation mechanism and the existing social structure, regulatory system, and commercial operation, which need to be solved in the process of development [8].

Based on the above discussion, the current concerns of blockchain applications are mainly on the strategic path of planning to enter the blockchain field and the business models of blockchain applications.

1. Strategic Path of Planning to Enter the Blockchain Field

Based on the research and the perceptions established, if you plan to enter the blockchain field, there are two main choices to think about and pay attention to: First, which application model to choose as the competitive track in this field. Only by finding the real business pain points or innovative business models can you break

through the perception barriers and precisely analyze the feasibility, commercial benefits, and social benefits of blockchain applications from the level of commercial and social values. Secondly, they should optimize their blockchain strategy according to their own market and social positioning to strengthen the competitive track they have chosen.

2. Business Models of Blockchain Applications

One is the native blockchain application model: it is directly based on decentralized blockchain technology to realize value transfer and transaction, such as digital currency; the other is the “blockchain +” model: based on the attributes of blockchain, such as “tamper-proof, traceable, open and transparent”, blockchain is integrated with traditional business scenarios to improve efficiency, reduce costs and solve business pain points. These features of blockchain make it possible to verify information and exchange values without going through a third party. The basic functions of blockchain technology are traceability and asset trading. Blockchain cannot meet the needs of all application scenarios. For how to judge whether the selected application scenario and business needs are suitable for applying blockchain in a specific situation, please refer to Sect. 4.5 “Blockchain Application Scenario Selection Method”.

4.4 Blockchain Application Implementation Path

Blockchain application implementation path mainly includes blockchain application scenario selection principle, blockchain technology selection principle, blockchain application implementation key process and blockchain application system evaluation.

1. Blockchain Application Scenario Selection Principles

Blockchain applications have their own specific application scenarios and business needs for which they are applicable, and these application scenarios are generally driven by the following 5 requirements.

- (1) Social Governance: Through the application of blockchain technology, we can provide transparent and efficient government functions for the society.
- (2) User-driven: The increasing demand of users for privacy protection and social value has urged enterprises to use blockchain technology to improve user satisfaction.
- (3) Innovation-driven: Using blockchain to build innovative applications for business and establish a reliable ecosystem to gain competitive advantage.
- (4) Management-driven: Enterprises, for reasons of efficiency and cost reduction, are applying blockchain technology to bring business process optimization and reduce business friction.

- (5) Research-driven: Scientific research and application experiments on blockchain based on the exploration of new technologies, new business models, social benefits, etc.

2. Blockchain Technology Selection Principles

The principles of blockchain technology selection mainly consider whether the following aspects of blockchain technology meet the requirements of the respective applicable business.

- (1) Consensus Mechanism: It affects transaction performance, Byzantine fault tolerance, etc., which is the cornerstone of blockchain composition trust.
- (2) Performance Requirements: To meet the expectations of business development.
- (3) Security Requirements: The main concern is whether the data is protected, whether the authority control is sound, and whether the blockchain network is stable.
- (4) The Applicability of Smart Contracts: Smart contracts support a wide range of languages, powerful, and will be easier to promote and maintain.
- (5) Whether Open Source: Open source blockchain is easier to maintain, apply and can facilitate the inspection of third parties.
- (6) Node Selection: It is necessary to consider how many nodes the blockchain network is prepared to frame and who will endorse the nodes.

3. Blockchain Application Implementation Key Process

The key process of blockchain application implementation is shown in Fig. 4.2.

- (1) Define Blockchain Network and Consensus Mechanism: Different interest entities manage different blockchain network nodes, forming a federated organization to jointly govern the blockchain network and business cooperation based on a specific consensus mechanism.
- (2) Data Collection: Each collaborating party provides data for the blockchain network through application systems or terminal devices according to their respective identities and privileges.
- (3) Multi-party Data Verification or Endorsement by an Authoritative Party: When a transaction is initiated, the authenticity of the data can be ensured through multi-party data cross-validation or endorsement by an authoritative party according to the verification rules.
- (4) Smart Contract Execution: The smart contract is invoked, and the smart contract processes the business logic and performs data computation according to the commonly agreed rules or consensus.
- (5) Data Storage on the Chain: Data is written to the ledger, generating digital assets or data deposition.
- (6) Data Application: Call the data on the blockchain application chain.
- (7) Third-party inspection of blockchain applications.

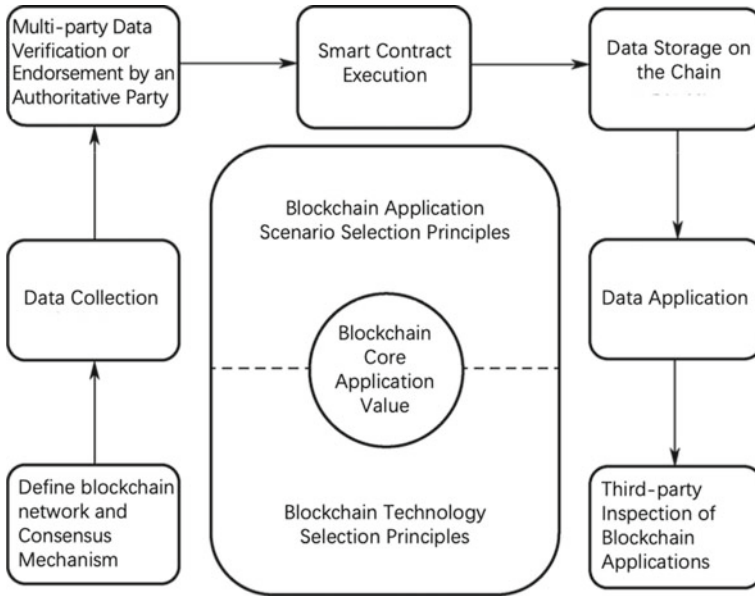


Fig. 4.2 Blockchain application implementation key process

4. Blockchain Application System Evaluation

From an application implementation perspective, the key points of blockchain application system evaluation include:

- (1) The assessment of the degree of compliance of the system is concerned with the fact that the system should comply with the existing legal framework requirements of the country.
- (2) The assessment of the system's regulatory is concerned with the fact that the system should comply with the state requirements for regulation.
- (3) The assessment of the completeness of the system services is concerned with the completeness and correctness of the services that the system should have.
- (4) Evaluation of system availability is concerned with system and technology maturity, fault tolerance and resilience.
- (5) Evaluation of the ease of use of the system is concerned with the ease of development of the system interface and smart contracts.
- (6) The assessment of system portability is concerned with the replaceability of the system and the operability of data migration.
- (7) The assessment of system security is concerned with the network security and data security of the system, especially the network security and the security of the data on the chain when multiple subjects are involved, and the system deployment is complex.

4.5 Blockchain Application Scenario Selection Method

Blockchain cannot meet the needs of all application scenarios, so it is necessary to rationally identify the real application needs of blockchain and avoid blockchain application implementation for the sake of blockchain application. How to select the real application requirements among so many application scenarios and business demands, and how to judge whether the selected application scenarios and business requirements are suitable and are the key issues in blockchain application development and implementation. The selection of blockchain application scenarios requires accurate recognition of the technical features and core application values of blockchain, and the analysis of the business pain points that can be solved or the business demands that will be realized by applying blockchain, in order to judge whether to adopt blockchain and which application scenarios to choose [9].

Based on the research on the core application value of blockchain and comprehensive analysis of industry development, the *Chinese Blockchain Technology and Application Development Research Report (2018)* puts forward the “Blockchain Application Scenario Selection Methodology”, which takes business pain points or innovative needs as the starting point and judges the feasibility and necessity of applying blockchain to solve specific business needs in 4 steps. Specifically, it includes: identification and analysis (identification and analysis of reasons for business pain points or innovative needs), inductive summary (analysis and summary of reasons for application needs), match mapping (analysis of matching mapping of attribution and blockchain value) and decision summary (decision summary of blockchain applicability). The process of blockchain application scenario selection methodology is illustrated in Fig. 4.3.

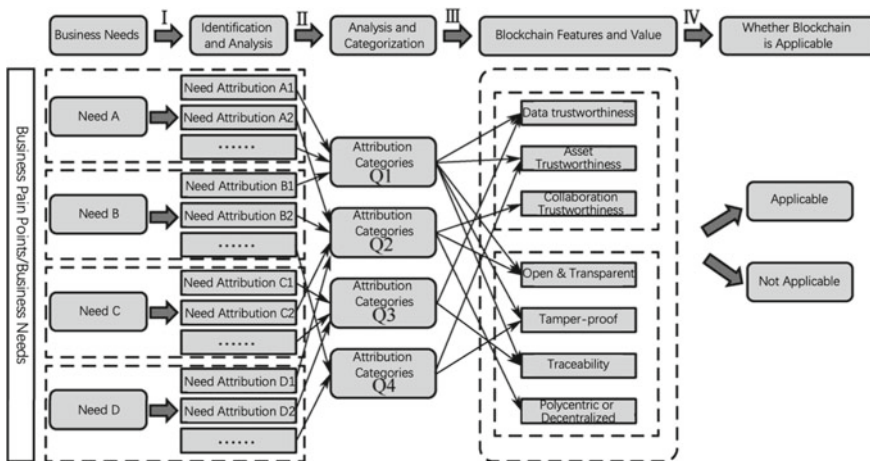


Fig. 4.3 Blockchain application scenario selection methodology process schematic. The above linkage are only examples

Step 1: Identification and Analysis—Identification and Analysis of Reasons for Business Pain Points or Innovative Needs.

Blockchain application scenario selection requires a clear understanding of application requirements (e.g., solving business pain points or application innovation needs), which can be decomposed through knowledge map. This can help to clearly perceive the application requirements, clearly analyze, and judge what values blockchain technology can bring and how these values are realized.

Step 2: Inductive Summary—Analysis and Summary of Reasons for Application Needs.

In the actual application scenarios, different application requirements may be extended by common internal causes, so step 2 needs to summarize the attribution analysis results of the application requirements output in step 1 to get the internal causes of these application requirements. The internal factors are the real reasons for the business pain points that need to be solved or the driving force behind the innovation needs.

Step 3: Match Mapping—Analysis of Match Mapping of Attribution and Blockchain Value.

Step 2 outputs the real causes of business pain points or the motivation driven by innovation needs, and the match mappings correspond the internal causes that summarized with the application value of blockchain, so as to analyze whether blockchain can help solve the internal causes. The mapping is to match the internal causes that can be solved or partially solved by blockchain technology with the application values of blockchain architecture and applications.

Step 4: Decision Summary—Decision Summary of Blockchain Applicability.

Based on the match mapping obtained in step 3, a decision on the suitability of applying blockchain is summarized, then a final conclusion is drawn on whether to adopt blockchain technology.

References

1. Wang Q, Xu YL. Research on the development and application of blockchain technology in China. *Rural Econ Sci Technol*. 2020;31(11):357–8.
2. China Blockchain Technology and Industrial Development Forum. China blockchain technology and application development white paper. (18 Oct 2016). https://www.sohu.com/a/224430559_680938.
3. Xie K, Zhang X, Zhang SL, et al. Application and prospect of blockchain technology in electricity trading. *Autom Electric Power Syst*. 2020;44(19):19–28.
4. Yang YQ, Wang C. Design and application value analysis of blockchain digital copyright protection system. *J Libr Inf Sci*. 2019;4(9):27–32.
5. Gentry C. A fully homomorphic encryption scheme. Stanford University; 2009.
6. Hu J. Blockchain technology's transformation of the accounting industry and its application challenges. *J Hubei Univer Econ*. 2020;17(8):70–3.
7. Yuan Z. Blockchain application analysis of copyright in broadcasting industry. *Radio Television Netw*. 2020;27(7):86–9.

8. Wang W. The Value of blockchain and difficulties in its application of digital currency. *Times Fortune*. 2019;11:10–1.
9. Blockchain Institute of People's Daily Online. Annual report on china's blockchain application and development. *Enterp Observer*. 2019;11:124–5.

Chapter 5

Blockchain and Financial Service



Xiao Chen and Shubing Shan

Abstract First, this chapter analyzes the application scope and application value of blockchain in six financial fields, including cross-border payment, cross-border trade, supply chain, financing, insurance, and credit reporting, and emphasizes that blockchain has security, Query A credible and efficient advantage. Then, this chapter introduces and analyzes the application trends of blockchain in the financial field of 5 continents including America, Europe, Asia, Oceania and Africa, and focuses on the detailed description of the application of blockchain in China's financial field by the broad and deep trend. Finally, as an application example, this chapter describes in detail the business pain points, application progress and implementation cases in the fields of digital currency, financial trading market, and supply chain finance.

Keywords Financial application · Blockchain · Case analysis

5.1 Value

In the financial field, blockchain can promote data sharing, optimize business processes, reduce operating costs, improve collaboration efficiency, and build credible systems [1]. Through merging of blockchain and the real economy, it can effectively solve the problems of small and medium-sized enterprises' loan financing, risk control, and departmental supervision, and effectively improve the ability of the financial sector to serve the real economy.

5.1.1 Upgrade Financial Model

From the perspective of the overall development trend of the financial service industry, financial service capabilities can no longer meet the needs of high-standard

X. Chen (✉) · S. Shan
CFETS Information Technology (Shanghai) Co., Ltd, Shanghai, China
e-mail: chenxiao_zh@chinamoney.com.cn

industries. The financial industry urgently needs technological upgrading to enhance the service capabilities of the real economy, and blockchain can play a key role in it. On the one hand, through the integration of blockchain and multi-party secure computing, Internet of Things, artificial intelligence and other technologies, data sharing can be better promoted, and the algorithm model can be strengthened to accelerate the implementation of intelligent finance. On the other hand, through the multi-party network alliance chain, the problem of high cost and low efficiency of traditional financial collaboration can be improved. Whether it is the upgrading and construction of financial infrastructure, or the innovation and transformation at the business level, blockchain can be used as a key or core technology to participate in it.

Blockchain has a natural and close relationship with finance, especially for digital asset. Through the distributed consensus mechanism to form a credible shared public ledger, the blockchain can not only realize that it does not rely on a single centralized organization for management and maintenance, but also ensure that the data recorded and stored is in a secure and tamper-resistant manner.

In recent years, financial institutions, financial technology companies, and technology service providers have been converging in the blockchain field. Among them, technology service providers are working hard to make up for the shortcomings of financial business capabilities and provide financial institutions with upgrade services from a single technology to an overall business plan. Financial technology companies are strengthening the research and development of blockchain core technologies and actively applying for financial licenses. Efforts are made in both financial business and technology; while financial institutions are increasing their investment in blockchain technology, and a few leading financial institutions have launched technology export services for the same industry. In addition, for business platforms such as supply chain finance and ABS that require business collaboration and resource integration through multiple participants, in-depth integration of business ecology has been achieved.

5.1.2 Innovating Financial Formats

The traditional financial model has many efficiency problems, and it is easy to form data islands, which will not only restrict the development of the industry itself, but also have a certain impact on other related industries [2]. Blockchain technology has tremendous transformative power in the financial field, prominently in cross-border payment, supply chain finance, insurance and credit investigation and other fields.

1. Financial industry pain points

At present, all branches of the financial industry are facing pain points that need to be solved urgently. The cross-border payment industry is facing the core challenges brought about by the need to improve payment efficiency and security. At the same time, the electronic construction of electronic bills in cross-border trade activities also

has problems such as inconvenience and intermediary risks; information in the supply chain industry is not transparent and non-circulating. Each participant in the supply chain only knows about the upstream and downstream companies that they have direct contact with. The financing process is time-consuming and labor-intensive, causing a lot of unnecessary waste of resources; the problem of data islands in the insurance industry is more serious, and insurance data is facing a lack of comprehensiveness. Many problems such as low level of refinement and low update timeliness make it difficult for insurance to innovate through data mining, and it is not conducive to comprehensive supervision and management. The credit information industry has some problems, such as fragmentation of the source of credit information data, lack of strong relevant data, and privacy protection Insufficiency, imperfect legal protection system, and serious data islands, and so on.

2. The power of blockchain transformation

In terms of cross-border payments, based on the “transaction is settled” feature of the blockchain, the payment and settlement system will achieve higher operational efficiency and better supervisory effectiveness. On the one hand, the use of blockchain to establish an efficient digital asset circulation system can improve the operational efficiency and liquidity of bills, and achieve transparent operation, thereby combating fraudulent behaviors of gray intermediaries and solving the problem of “one ticket, more sales” of invoice paper. On the other hand, with the strong consistency, real-time synchronization, tamper-proof and other characteristics, the electronic transmission system of trade documents shortens the transit time of bills and letters of credit, and speeds up capital turnover.

In terms of supply chain finance, blockchain technology can solve the problems of asymmetric information of multiple parties in the supply chain, complex execution processes and low efficiency. Utilizing the transparent and difficult-to-tamper characteristics of blockchain, data can be credible stored as while as the cost of financial institutions’ investigation of trade authenticity can be reduced. Automated settlement of smart contracts can also ease the operational risks in supply chain finance. Based on the block chain efficient rights and interests transfer system, it is possible to create a “credit certificate” based on the core enterprise credit that can be transferred between multi-level suppliers and distributors in the supply chain system, which improves the efficiency of capital transfer and reduces the financing of a single enterprise cost.

In terms of insurance, a blockchain-based trusted certificate deposit system and automatic execution of smart contracts can enhance users’ trust, create a shared and transparent account book maintained by multiple parties, strengthen the integration and analysis of insurance data, and improve the relationship between insurance institutions, especially direct insurance companies and direct insurance companies. The efficiency of collaboration between reinsurance companies [3]. What’s more, the fusion scheme of blockchain + trusted computing can realize the calculation and verification of data without obtaining private data, providing new ideas and possibilities for data sharing between direct insurance companies. Blockchain can also

provide credible records and traceability capabilities for dynamic growth information of animals and plants, climate and geography and other dynamic changes in the fields of agricultural insurance and natural disaster insurance.

In terms of credit reporting, the transformational power of the combination of blockchain and credit reporting is mainly reflected in the ability to Chain technology builds a truly independent and reliable third-party data transaction platform to solve the problem of data islands [4]. Credit reporting agencies exchange or share information such as credit reporting data and credit reporting results through the blockchain platform, which can improve the credibility of data transactions to a certain extent.

5.2 Application Situation

5.2.1 *China Application Trend*

In recent years, Industrial and Commercial Bank of China, Bank of China, Bank of Communications, Postal Savings Bank of China, China Merchants Bank, China CITIC Bank, WeBank, Ping An Bank, Minsheng Bank, Industrial Bank, etc. have carried out explorations of blockchain technology in financial applications. Substantial application results have been achieved in financial fraud, asset custody, transaction financial auditing, cross-border payments, reconciliation and settlement, supply chain finance, and insurance claims, which have promoted the resolution of previous credit checks in financial services to a certain extent Complexity, high cost, long process, large data transmission error and other problems.

At present, there are some typical cases in the financial service field, and the blockchain-based digital bill trading platform promoted by the People's Bank of China has been successfully tested. The Digital Currency Research Institute under the People's Bank of China was officially listed in July 2017. On September 23, 2016, IBM and China UnionPay previewed the "Inter-bank Points Exchange System Using Blockchain Technology", which allows cross-bank and cross-platform exchange of reward points. Consumers' points in one bank can be exchanged for points from other banks Rewards, and even redeem for multiple airline miles and supermarket rewards, greatly improve the efficiency of the use of bank points [5].

5.2.2 *Application Trends in Other Countries*

1. America

There are more than 5900 banks and 5800 credit cooperatives in US financial institutions. These large financial institutions are committed to research and product development in the blockchain field. JPMorgan Chase Bank's participation in the blockchain mainly involves developing technology platforms, cooperating with

blockchain startups, and investing in blockchain companies. JPMorgan Chase built a blockchain platform based on Ethereum, Named Quorum, and on this basis, it launched the Interbank Information Network (INN) [6], which aims to use blockchain technology to solve global payment problems. 75 banks including Royal Bank of Canada, ANZ Bank of Australia, Bank of New Zealand, and Societe Generale have participated in the test.

The blockchain global payment solution developed by Citibank and Nasdaq is regarded as a milestone in the commercial application of blockchain [7]. Citibank and Barclays Bank announced their participation in the trial operation of IBM's blockchain application LedgerConnect [8]. The application aims to provide a platform for banks to deal with AML/KYC compliance and loan collateral management issues. Among them, the full name of AML in English is Anti-Money Laundering, which refers to anti-money laundering; the full name of KYC in English is Know Your Customer, which refers to the process by which the trading platform obtains customer-related identification information. Citibank has also developed a tool called Digital Asset Receipt (DAP), which works similarly to American Depository Receipts (ADR).

Bank of America is the second largest bank in the United States and is currently the largest holder of blockchain-related patents among all banks in the United States [9]. As of the end of 2020, Bank of America has applied for 2,668 patents in the blockchain field. Bank of America hopes to use a proprietary chain to store various types of records that are sent to service providers. This means that all records will be stored in a single ledger, companies and service providers will access these records as needed, and the system will record the information of each data visitor.

Nasdaq has launched the Nasdaq Linq platform for private equity transactions through cooperation with blockchain startup Chain.com [10]. Previously, equity financing and transfer transactions of unlisted companies required a lot of manual work and paper-based work, required manual processing of paper stock certificates, option issuance and convertible notes, and required lawyers to manually verify electronic forms, etc., which may cause a lot of trouble Human error makes it difficult to leave audit trails. Share issuers through private placement of Nasdaq Linq enjoy digital ownership, and Nasdaq Linq can greatly reduce settlement time. Chain.com pointed out: The current standard settlement time of the equity trading market is 3 days, and the application of blockchain technology can increase the efficiency to 10 min, which can reduce the settlement risk by 99%, thereby effectively reducing the capital cost and systemic risk. Moreover, the online completion of the issuance and subscription materials by both parties to the transaction can also effectively simplify the redundant writing work, and the administrative risks and burdens faced by the issuer due to the tedious approval process will also be greatly reduced.

Overstock has created the T0 blockchain trading platform, and securities can be traded directly on the blockchain without passing through traditional trading platforms such as Nasdaq. In the traditional stock trading market, the settlement mechanism T + 1 in the market is to buy on the same day and sell for cash after one day, and it takes a whole day for payment and securities transactions to be resolved. With blockchain, settlement can be completed instantaneously. T0 is commented

as settlement and transaction occur at the same time. In December 2015, the U.S. Securities and Exchange Commission (SEC) approved Overstock to issue shares on the TO platform built through blockchain technology.

2. Europe

As early as 2016, the British government issued a blockchain report “Distributed Ledger Technology: Beyond the Blockchain”, this is the world’s first blockchain research report released by the government, and it also confirms the importance of the British government on blockchain technology. In the financial field, the UK has made a series of attempts using blockchain technology [11]: the Bank of England has launched a PoC plan to test the potential of blockchain technology in the real-time settlement (Real Time Gross Settlement, RTGS) function; the five largest fund operators in the UK Use blockchain technology to save operating costs generated by the transaction system; the employment and pension department of the British government develops a welfare payment system based on blockchain technology. France also has certain research on blockchain financial applications. BNP Paribas and Ernst & Young completed an experiment to explore whether private blockchain technology can help to improve the bank’s global internal treasury business. The test proves that private blockchain helps improve operational efficiency and not only provides more comprehensive cash. Management methods have also enhanced the flexibility and service capabilities of financial services. Spain [12].

The Spanish banking giant Bilbao Biscay Bank (BBVA) has completed a pilot, using two different blockchain technologies to issue 75 million euros (approximately US\$91 million) in corporate loans. Switzerland is actively carrying out digital wallet payment projects based on blockchain technology, instant settlement and transaction technology development projects based on blockchain technology [13]. The Riksbank and IOTA plan to launch the national digital currency E-Krona, which is mainly used for small transactions between consumers, enterprises and government agencies [14].

3. Asia

Singapore’s blockchain has a wide variety of financial applications, including payment, asset exchange, personal finance and other fields. The Monetary Authority of Singapore introduced the Ubin project in 2016 to use blockchain technology for inter-bank payments. It has now successfully connected with the Jasper project of the Bank of Canada and completed cross-border and cross-currency payments using legal digital currencies [15]. Singapore’s banking industry is launching a blockchain-based digital trade finance registration project aimed at achieving greater transparency and reducing the risk of trade fraud. The project was led by DBS Bank and Standard Chartered Bank that was supported by 12 other banks including ABN AMRO Bank, ANZ Bank, Deutsche Bank, Indian Industrial Credit Investment Bank, OCBC Bank and United Overseas Bank [16].

Japan’s blockchain financial applications are also very diverse. Japan’s Mizuho Financial Group, Mitsui Sumitomo Financial Group, Mitsubishi UFJ Financial Group, and Fujitsu have experimented with a cloud-based blockchain platform for sending funds between individuals. In terms of supply chain finance, Mizuho Bank, a

subsidiary of Japan's Mizuho Financial Group, and IBM Japan have jointly developed a blockchain trade finance platform to improve the efficiency of the trade process [17].

In the banking industry, the Indian government uses blockchain technology to establish the online identity of individuals and family alliances, allowing individuals to operate bank accounts, transfer funds, apply for loans, etc., thereby raising financial inclusion to a whole new level [18].

The National Bank of Dubai (NBD) in the UAE is the first bank in the UAE to successfully implement blockchain technology in the cheque insurance system to prevent fraud. In the first month of using blockchain technology to prevent fraud, the bank has received nearly 1 million cheque registrations on Cheque Chain [19].

4. Oceania

Oceania has a number of blockchain financial applications in digital currency, and has also issued a series of articles Incorporating blockchain into the national digital strategy, aiming to become a global financial technology center with the help of emerging technologies such as digital currency and blockchain [20]. The "National Block Link Map" issued by the Australian Department of Industry, Science and Technology in February 2020 pointed out that the most widely used industries in Australia are financial and insurance services, and 3 of Australia's "big four banks" cooperate with IBM Create an enterprise and use blockchain technology to characterize bank guarantee functions.

5. Africa

Kenya has made a certain exploration of blockchain. In terms of insurance, StanChat Banking Group and American Insurance Group (AIG) jointly launched a global blockchain technology pilot. Seychelles mainly uses blockchain technology for exchanges. Tunisia decided to use blockchain technology to promote the national digital currency in 2015 and named it as eDinar. Senegal also launched its own digital currency eCFA [21].

5.3 Application Scenarios and Practices

5.3.1 Digital Currency

1. Application scenario analysis

At present, the commodity economy is highly developed, and people hope that economic and financial activities can be carried out in a more efficient manner. For example, using mobile banking makes consumption, savings, and wealth management easier and more convenient; highly merging of finance and trade, logistics, and other scenarios to make currency functions more customized and ubiquitous; international trade, cross-border investment, and cross-border consumption. When formulating monetary policy, the central bank hopes to conduct in-depth analysis of

currency issuance, circulation, and storage, and provide data support for intervention needs such as monetary policy, macro-prudential supervision, and financial stability analysis in order to better implement macro-control. These new demands posed new challenges for electronic money, prompting people to explore new forms of money.

At present, many governments and their central banks have expressed positive views on blockchain technology. With the goal of reducing the operating cost of the currency system, expanding the field of electronic applications, and consolidating the leading position in the global economy and finance, many central banks try to use or learn from blockchain technology to build legal digital currency prototype systems, such as the United Kingdom, Singapore, the United States, Canada, Germany and China etc. [22]. Legal digital currency is “a digital form of central bank currency that is different from traditional reserves or settlement balances” [23]. It is a digital payment tool that is priced in national accounting units and is a direct liability of the central bank. The legal digital currency needs an information system to support its normal operation, so as to facilitate the provision of services to the public. In a narrow sense, the system includes central banks, operators and banks participating in payment services. More broadly, the system can also include data service providers, companies that provide and maintain applications, and point-of-sale equipment providers that initiate and accept payments [24].

1. Case

(1) British digital currency RSCoin

In December 2015, the Bank of England and the University of London proposed and developed the world’s first legal digital currency prototype system—a “hybrid” legal digital currency RSCoin prototype system. In order to realize the central monetary policy with quantifiable control, the system draws on and absorbs technical means such as centralized currency management methods, blockchain and virtual token models [25] to realize a digital currency prototype system controlled by the central bank and expandable.

The participants of the RSCoin prototype system are composed of central banks, commercial banks and end users, as follows:

As shown in Fig. 5.1. In order to achieve scalable collaborative records, the system adopts a dual hierarchical system structure of “central bank-commercial bank”. A number of credit-granting commercial banks store part of the transaction data separately, and realizes hierarchical management based on blockchain technology. Distributed ledger. The main division of labor of each participant is as follows:

The central bank fully controls the generation of currency, has complete control over the general ledger, and releases final transaction data to the entire system by managing and summarizing transaction information obtained from commercial banks. In addition, the central bank also fully controls the authorization and authentication power of commercial banks, and regularly publishes a list of authorized commercial banks to the entire system. Commercial banks are responsible for collecting and verifying transaction information submitted by users, writing the verified transaction information into the primary ledger, and submitting it to the central

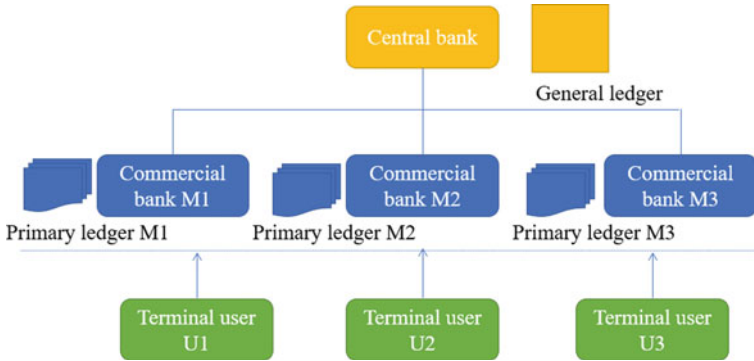


Fig. 5.1 Structure diagram of RSCoin

bank. The end user is associated with the commercial bank and transfers transaction information through the commercial bank. The RSCoin prototype system uses a two-stage consensus mechanism to record and manage transaction information.

In the first stage-the voting stage, commercial banks verify the legitimacy and correctness of end-user transactions. In the second stage, the submission stage, the commercial bank first records the transaction information in the primary account book maintained by itself, and then submits the primary account book to the central bank. This design scheme adopts the design idea of sharding, divides the commercial bank into several groups, and each group is responsible for part of the general ledger; and according to certain rules, the transaction information is distributed to different commercial bank groups for processing, thereby improving the overall System throughput and scalability.

(2) Singapore

In November 2016, the Monetary Authority of Singapore (MAS) launched the Ubin project to explore the practicality of blockchain in the financial ecosystem to reduce the risks and costs of cross-border payment settlement and securities settlement. The project adopts a phased research model, and the first two phases of exploration have been completed. In the first stage, the project developed a digital new currency prototype system based on the Ethereum blockchain platform and continuous depository receipt currency model, and integrated it into the existing MAS payment and settlement infrastructure to realize the use of digital SGD is the goal of real-time payment and settlement between banks [26]. In the second stage, the project focused on exploring the ability of the blockchain-based Real Time Gross Settlement (RTGS) system to achieve multilateral net settlement under the premise of protecting transaction privacy [27]. The digital new currency prototype system is jointly operated by MAS and interbank institutions. It consists of an electronic payment system (MAS Electronic Payment System, MEPS +) and a blockchain system based on Ethereum.

MEPS + : MEPS + , operated and managed by MAS, supports the transfer of large amounts of domestic currency inter-bank funds and the settlement of Singapore government securities. In MEPS + , participating institutions have 3 types of accounts, namely Cash Account (CA), RTGS Account and Blockchain Cash Account (BCA). Among them, the CA account is used to store the cash of the institution, the RTGS account is used for real-time payment and settlement between banks, and the BCA account is used to store the mortgage cash for issuing depository receipts in the blockchain system.

Blockchain system: The blockchain system is jointly operated by MAS and the banking industry. In this system, Depository receipts, as a form of value, can be transferred between digital wallets between institutions.

Blockchain connector: MEPS + and the blockchain system pass through the Blockchain connector (Blockchain Connector) to connect with each other, and realize the interaction between systems through depository receipts and FAST (Fast and Secure Transfers) netting documents.

In the digital new currency prototype system, interbank institutions first use cash deposited in the central bank as collateral to obtain equivalent digital new currency; secondly, use digital new currency to achieve interbank payment and remittance settlement; finally, the bank will convert the digital SGD into an equivalent amount of cash. The main process of the Ubin project is shown in Fig. 5.2.

- In MEPS + , the funds in the CA account that exceed the deposit reserve are transferred to the RTGS account.
- Cash mortgage. Take Institution A as an example: Institution A sends transfer funds to MEPS + to BCA Account request; funds will be transferred from Institution A’s RTGS account to Institution A’s BCA.

Account, this fund will be used as cash collateral for the issuance of depository receipts.

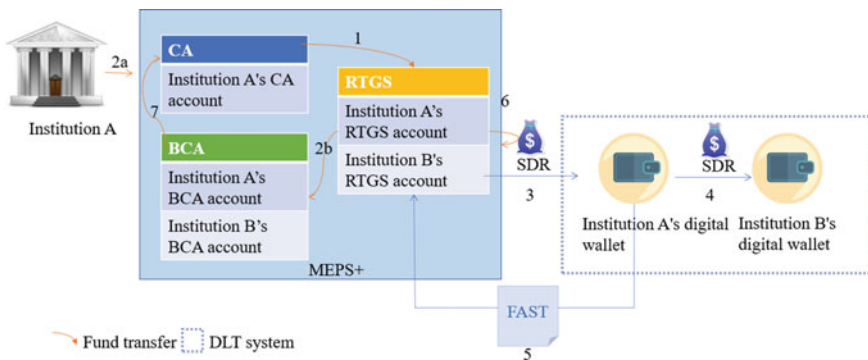


Fig. 5.2 Basic flows of Ubin [26]

- MAS issues depository receipts to institutions' digital wallets through smart contracts. Take organization A as an example: If there are 300 SGD in the BCA account of Institution A, there is a price in the digital wallet of Institution A depository receipt worth 300 SGD. At this point, the processing flow will be transferred to the blockchain system.
- In the blockchain system, institutions conduct transactions with other participants.
- When the above transaction is completed, the blockchain system will send a FAST net amount to the RTGS account Settlement documents. At this point, the process will again be transferred to the MEPS + system.
- If the institution's RTGS account has sufficient funds, the corresponding funds will be deducted from it, and It is credited to the RTGS account of the funded institution.
- Transfer funds from the institution's BCA account to its CA account.

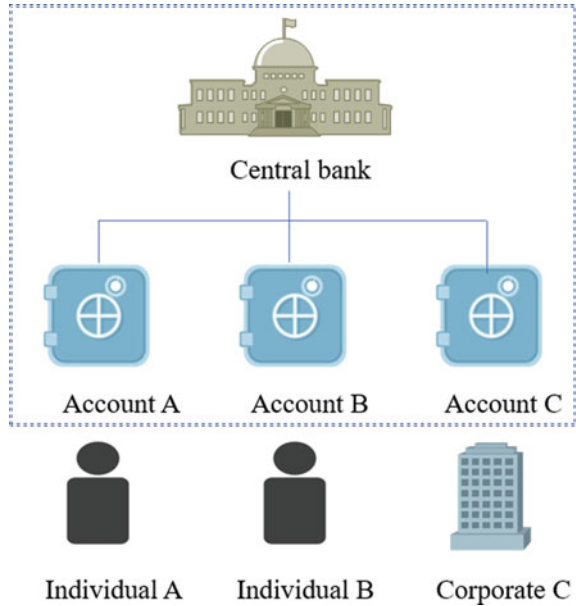
(3) US FEDCoin

On April 13, 2013, JP Koning first proposed a distributed-ledger-based FEDCoin model in a blog to reduce the payment system's reliance on centralized processing [28]. In 2015, David Andolfatto, Vice President of the Federal Reserve Bank of St. Louis, publicly supported the FEDCoin model at the International Symposium on P2P Financial Systems, so that anyone in the world can access through digital wallets and the Internet and use FEDCoin for low-cost peer-to-peer transactions [29]. Although the design is still in the theoretical stage, monetary expert Doug Casey [30] believes that only the Federal Reserve issuing legal digital currency can maximize the consolidation of the US economic center.

The FEDCoin model cancels the dual hierarchical structure of "central bank-commercial bank", allowing many individuals or companies directly open accounts with the central bank, thereby enhancing the Fed's ability to control the total amount of broad money [31]. The overall structure is shown in Fig. 5.3. There are two ways to control the supply of FEDCoin. On one hand, the Federal Reserve has the ability to create and destroy digital currencies, or the Federal Reserve pre-allocates the entire supply of digital currencies. On the other hand, when the supply of digital currencies exceeds demand, the Federal Reserve uses reserves to buy back digital currencies from the public. In the FEDCoin model, companies or individuals can directly purchase digital currencies through the Internet portal of the Federal Reserve, download digital wallet applications to manage FEDCoin, and can exchange FEDCoin and U.S. dollars at a ratio of 1:1 through banks or ATMs.

JP Koning recommends that the Federal Reserve weigh the pros and cons of each technology when choosing the underlying blockchain type to implement FEDCoin to maximize the realization of its design goals. For example, the consortium chain has faster processing speed, stronger supervision capabilities and stricter transaction finality, while the public chain can better reflect the unique qualities of cash, such as anonymity. Aiming at the privacy of digital currency, the plan introduces two design ideas: one is to unbind the account address from the real user to realize the anonymity

Fig. 5.3 FEDCoin overall structure



of the current cash; the other is to use homomorphic encryption or zero-knowledge proof, etc. Cryptographic algorithms reduce the transparency of transactions.

(4) Digital currency of the People’s Bank of China

The People’s Bank of China has been studying legal digital currencies since 2014. In 2017, the Digital Currency Research Institute was formally established, and it has jointly developed digital renminbi research and development with some commercial banks and related institutions. At present, the top-level design, standard formulation, function research and development, joint debugging and testing of digital renminbi have been basically completed, and the pilot work of digital renminbi has been gradually promoted. At the beginning of October 2020, Fan Yifei, vice governor of the People’s Bank of China, stated in a meeting that positive progress has been made in the digital RMB pilot work, a series of innovative application scenarios have been created, and a variety of safe and convenient payment functions have been realized. The pilot application has received national support. The “Opinions on Supporting Shenzhen’s Construction of a Pilot Demonstration Zone of Socialism with Chinese Characteristics” [32] released in August 2019 proposed “supporting Shenzhen to carry out innovative exploration projects such as digital currency research and mobile payment”. According to Fan Yifei, Vice Governor of the People’s Bank of my country, on the choice of China’s legal digital currency (Central Bank Digital Currencies, CBDC) operating framework, my country’s legal digital currency.

The word currency will adopt a two-tier system of “central bank-commercial bank”. Different from the blockchain currency issued by the private sector, CBDC

uses centralized or partially centralized technology, uses a hierarchical consortium chain, and allows supervisory nodes to participate in the distributed ledger for cooperative accounting. At present, my country's legal digital currency CBDC is designed to be in the M0 category. In order to ensure that the second-tier institutions do not exceed the issuance of digital currency, the agency issuing agency needs to pay the full amount of reserves to the People's Bank of China. The current payment system mainly deals with the current deposit part (M1 ~ M0) in broad currency. The convenient payment and settlement speed of digital currency will make the transition from deposits (M2 ~ M0) to cash (M0) more rapid. In order to avoid liquidity risks, restrictive measures need to be set under certain conditions to prevent the crowding-out effect on deposits. It should be noted that the research and development of my country's digital currency does not have a preset technical route. In the research and development process, it only draws on some design ideas of the blockchain, such as peer-to-peer payment, anonymous payment, and easy traceability.

5.3.2 Trading Market

1. Scene analysis

In the current traditional centralized fields, systems such as clearing registration systems and transnational exchange and settlement systems are often the basic systems of a financial industry, and the application of blockchain technology will bring optimization and upgrading of the original financial system. For example, in the field of securities settlement and clearing, after the owner of the securities issues a transaction instruction, the instruction needs to be coordinated by securities brokers, asset custodians, central banks, and central registries in order to complete the transaction. If blockchain technology is used, buyers and sellers can directly realize automatic matching through smart contracts, and automatically realize settlement and clearing through a distributed digital registration system. Compared with the "T + 3" days required for transaction confirmation in the past, after applying blockchain technology, settlement and clearing may only take 10 min to complete. At present, the blockchain technology alliance R3 CEV is testing the clearing and settlement network between banks, and is proposing some brand-new clearing and settlement standards, and trying to develop interactive clearing and settlement standards. Currently, the centralized trading market consists of member institutions (buyer, seller) trading center and clearing institution, as shown in Fig. 5.4. Among them, the transaction center provides transaction matching and transaction confirmation, and the clearing agency is responsible for the clearing of both buyers and sellers. Both the transaction center and the clearing agency are trusted third-party institutions. Such a transaction structure is a reasonable solution based on institutional trust.

At present, the transaction structure of almost all financial institutions is similar to this, and it is common for a certain institution to dominate transactions or clearing and settlement. Although so far, people have not found any major flaws in such

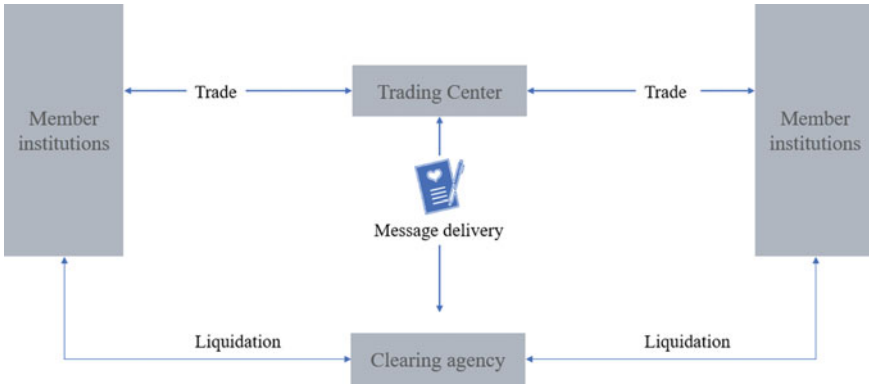


Fig. 5.4 Traditional trading model

a transaction structure, such centralized transaction or clearing institutions may experience downtime, data loss, etc. This is also the case in the financial community actively looking for more decentralized transactions, while the emergence of blockchain is meeting this demand, as shown in Fig. 5.5. In this structure, the trading center only provides matching services, and real transactions and clearing occur on the blockchain-based trading platform. This structure takes full advantage of the “transaction-as-settlement” feature of the blockchain. Blockchain technology can greatly accelerate the payment and clearing process in transactions, making payment and clearing almost real-time.

2. Applications

(1) X-Swap credit matching trading system

The X-Swap credit matching trading system is a comprehensive system launched by China Foreign Exchange Trading Center for market members.

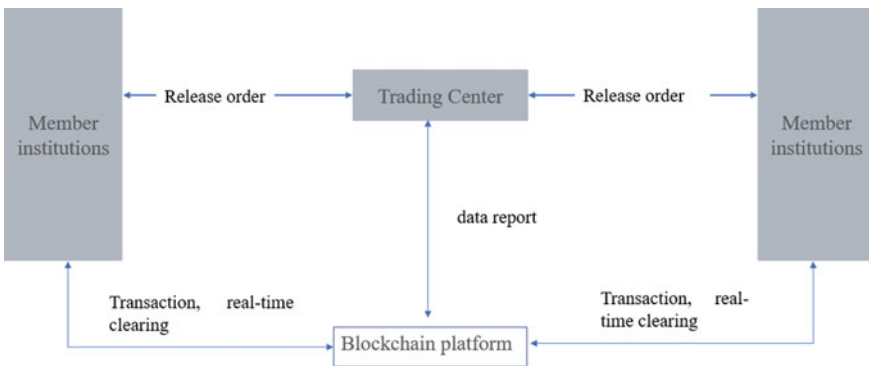


Fig. 5.5 Blockchain-based transaction mode

The self-developed order-driven matching trading system provides market members with convenient trading services for RMB interest rate derivatives such as interest rate swaps and bond forwards. In 2016, Zhonghui Information Technology (Shanghai) Co., Ltd., a wholly-owned subsidiary of China Foreign Exchange Trading Center, launched a blockchain prototype system exploration for the X-Swap system.

In the existing business scenario model, the transaction records generated by the member institution in the system will be stored in the data center of the transaction center, and the member institution also needs to confirm the transaction in the transaction center and perform subsequent clearing work. The member institution conducts matching transactions in the X-Swap system, then downloads the transaction slip in the straight-through processing system service program, and finally completes bilateral self-clearing with the transaction slip, or completes the centralized clearing agency such as the Shanghai Clearing House or the Central Bond Registration Company Liquidation is shown in Fig. 5.6.

The whole process contains multiple links, and a large amount of work needs to be done manually. If one link fails, the entire transaction process will be blocked. Based on blockchain technology, transaction records can be stored in the blockchain network in real time. The transaction center can greatly reduce operation and maintenance costs, and the process of post-transaction operations by market members will be easier. The completed transactions can be checked in real time in the blockchain network, and even bilateral settlement or centralized settlement can be automatically completed, as shown in Fig. 5.7.

- (2) The infrastructure framework of the capital market derived from the underlying design of Bitcoin

The Japan Stock Exchange Group established an internal research team at the end of 2015 to explore distributed records the use of accounting technology in capital

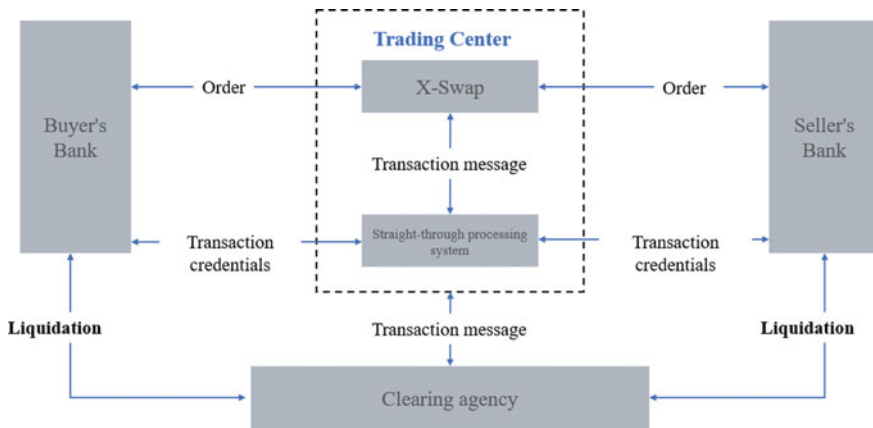


Fig. 5.6 Current X-Swap system transaction and clearing model

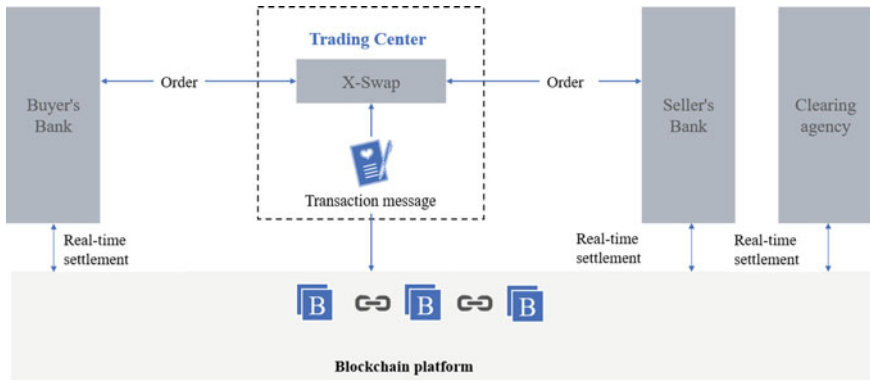


Fig. 5.7 X-Swap system transaction and clearing mode based on blockchain

market infrastructure [33]. Afterwards, the Japan Stock Exchange Group cooperated with six other domestic financial institutions to jointly test whether the process of securities issuance, trading, settlement, clearing and ownership registration can be streamlined in the blockchain environment. The research team pointed out that blockchain can reshape the existing capital market infrastructure by encouraging new business development, improving operational efficiency and reducing costs. Financial products are much more complex than virtual tokens, and their business processing is relatively complex, so it is necessary to use smart contracts, as shown in Fig. 5.8.

The research conclusions are as follows: Firstly, multi-level data privacy control should be introduced, so that ordinary users can only see their own transaction details, and the supervisory authority can understand all transaction details and prove the user’s transaction or ownership. Secondly, it is recommended not to apply distributed accounting technology in the pre-transaction process. The most important thing for the trading link is to design an effective pre-trade order matching mechanism. In order

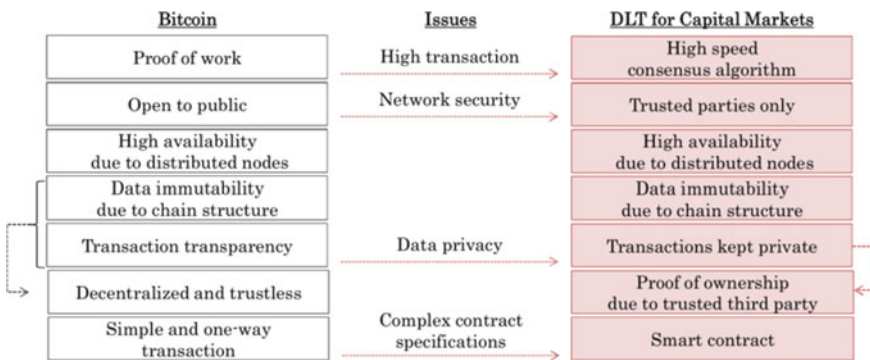


Fig. 5.8 The infrastructure framework of the capital market derived from the underlying design of Bitcoin [33]

to improve the efficiency of order matching, market operators will try to collect as many quotations as possible, that is, use centralized quotations, and the concept of centralized quotations does not match the decentralized processing method of the blockchain. In addition, due to the immutability of distributed accounting technology, it is difficult to apply distributed accounting technology to securities transactions that require frequent cancellation or modification of orders. However, over-the-counter bilateral transactions do not require fierce price competition, and the cancellation or modification of orders rarely occurs. You can experiment with distributed accounting technology. Thirdly, the operators of financial market infrastructure (trading centers, clearing institutions, custodians, etc.) should play the role of certification agencies and be responsible for issuing corresponding financial institutions to financial institutions. Authority certificate. The most suitable node management candidate will be the operator of the existing infrastructure. Of course, the regulatory authority or IT service provider can also serve as the third-party trusted subject. Fourthly, in the long run, the use of blockchain will bring a certain degree of cost savings, which is mainly manifested in the reduction of operating costs after changing the existing business model and the reduction of emergency handling costs brought about by the sharing of nodes in the whole industry.

5.3.3 Supply Chain Finance

1. Scene Analysis

(1) Application requirements

Supply chain finance refers to the core enterprises in the supply chain and their related upstream and downstream enterprises can be treated as a whole. Relying on core enterprises, based on real trade, using self-compensated trade financing to provide comprehensive financial products and services to upstream and downstream enterprises in the supply chain. According to data released by the National Bureau of Statistics, as of March 2020, the accounts receivable of industrial enterprises in my country are 14.04 trillion yuan.

At the end of May 2020, the accounts receivable of small and medium-sized industrial enterprises above designated size increased by 17.5% year-on-year, 11.5 percentage points higher than the same period last year, and 10.8 percentage points higher than the growth rate of large industrial enterprises in the same period. The average payback period for accounts receivable of small and medium industrial enterprises was 62.8 days, an increase of 13.2 days over the same period of the previous year, and 9.2 days longer than that of large industrial enterprises in the same period; overdue accounts receivable of small and medium industrial enterprises accounted for 29.5% of all accounts receivable. An increase of 3.3 percentage points over the same period last year. The reduction in operating cash flow has had a serious impact on the operation of the company. The continuous increase in the balance of

accounts receivable brings about the continuous increase of liquidity risk, and the effective management of accounts receivable is also particularly important [34].

Suppliers or suppliers that have direct first-hand transactions with core enterprises can only use the credit of core enterprises to finance accounts receivables. Some small and medium-sized enterprises in the upstream cannot use their own supply chains for financing. The use of blockchain technology to manage a complete supply chain transaction on the chain can introduce financial institutions to solve the problem of difficult and expensive financing for small and medium-sized suppliers.

(2) Application mode

As shown in Fig. 5.9, after the first-tier supplier S1 has a transaction with the core enterprise, the core enterprise Payment in the form of a voucher. The first-tier supplier S1 will cash this voucher through a financial institution or pay to its own supplier. After the second-tier supplier S2 and the first-tier supplier S1 have a transaction, the first-tier supplier S1 can pay the second-tier supplier S2 with a blockchain certificate. The second-tier supplier can continue to pay the third-tier supplier S3 with the blockchain vouchers, and so on to form the circulation of the blockchain vouchers on the platform. At the same time, each transaction entity can apply for the corresponding amount of financing from the bank with the blockchain vouchers service. At the end of the period, the supplier or financial institution holding the certificate collects from the core company, and the collection bank of the core company automatically transfers the funds to the bank. The system can effectively promote the circulation of digital vouchers based on accounts receivable, meet the financing needs of small and medium-sized suppliers, and increase the participation of financial institutions and the number of customers.

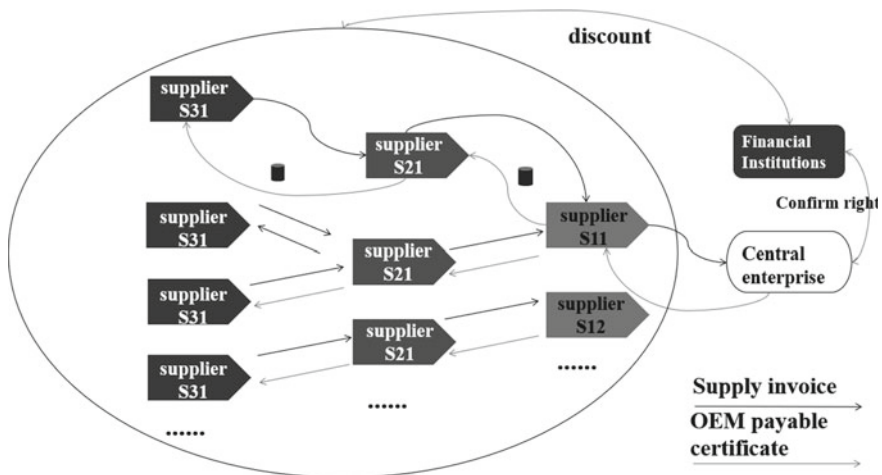


Fig. 5.9 Supply chain finance business model based on blockchain

The issuance and operation of digital bills on the blockchain can be split and transferred at will under the circumstances of openness, transparency and multi-party witness. This model is equivalent to making the credit of the core enterprise transmittable and traceable, so that it can be communicated to secondary and tertiary suppliers that cannot be reached under the traditional business model, and provide services for a large number of small and medium-sized enterprises that cannot obtain financial service, that greatly improves the efficiency and flexibility of the circulation of bills, and reduces the financing costs. At the same time, as a “trusted machine”, the blockchain has the characteristics of traceability, consensus and decentralization. Even if the data of a certain node is modified, the consensus of other nodes cannot be obtained, so that the tampering fails. In addition, the data on the blockchain is time-stamped to trace the entire process of each transaction. Therefore, the blockchain can provide a highly credible environment, reduce the cost of risk control at the capital end, and dispel the bank’s doubts about the tampering of trade information.

2. Application case: Yunlian League

Transport Chain Alliance is based on blockchain technology, integrating the three major functions of automobile logistics, settlement and supply chain finance. The integrated service platform for energy modules is jointly built by Zhongdu Logistics, Wanxiang Blockchain, and DBS Bank. Transport Chain Alliance uses blockchain technology to manage the entire business process on the chain, which effectively solves the problems of waybill circulation, settlement and reconciliation, and capital pressure, and brings together automobile OEMs, logistics general contractors, carriers, 4S shops, etc. To address the financing difficulties of carriers, the platform introduces financial institutions. On the platform, automobile OEMs and logistics general contractors can publish order and waybill information online; carriers at all levels can record online business data such as job handover vouchers, settlement vouchers, invoices, and realize online reconciliation of upstream and downstream enterprises. What’s more, finance institutions can provide carriers with financial services based on business data recorded on the chain.

In the traditional vehicle logistics process, due to paper-based documents, supply chain information fragmentation, etc., logistic process documents are cumbersome and reconciliation is complicated, especially the long payment cycle causes the pressure enterprises’ capital problems in downstream. Through the electronic orders and waybills in the logistics and transportation process, as well as the online reconciliation mode of upstream and downstream enterprises, the logistics alliance can effectively reduce the cost of document management. At the same time, the business process is managed on the chain, and upstream and downstream enterprises can realize data sharing and improve overall operational efficiency. In addition, the blockchain can ensure the authenticity and reliability of data records, and provide all business parties with traceable, penetrating asset confirmation and verification channels for all business parties, reducing the possibility of fraud. Financial institutions can provide carriers with financial services based on online accounts receivable and invoice records, and small and medium carriers can also obtain more financing opportunities at a lower cost.

The transport chain alliance platform uses blockchain technology to broadcast and publish public information streams such as order information, vehicle information, transportation plan information, and logistics process information. The information publisher and the information confirmer reach a consensus through their respective digital signatures. Information is added, modified, and invalidated, and all the processes will be recorded in the blockchain. Confidential data is kept by the companies on the chain and transmitted through encryption when necessary. On the basis of consensus reached on the blockchain, the upstream and downstream reconciliation functions are realized by screening and filtering data and using unified calculation rules. After the reconciliation results are confirmed by both parties, the conditions for commercial invoicing are met. Finally, use the basic attributes of blockchain to deliver value to realize supply chain financial services, and introduce financial institutions to provide bond financing for suppliers at all levels. The WinChain Alliance platform makes full use of the characteristics of blockchain credit transmission, value transmission, and provides credit endorsements for supply chain financial services through authentic, credible business data, and promotes the formation of a benign closed loop of the entire supply chain.

References

1. Yi T. Jingtong technology: using blockchain technology to empower financial technology. *Int Finan.* 2020;7:40–2.
2. Minfeng L, Yangyang X. Research on the strategy of building China's internet financial center. *Southwest Finan.* 2017;2:3–11.
3. Peng W. The application of science and technology in the insurance cross-border service platform of the greater bay area in the digital age-based on the blockchain in the cross-border practical exploration of the integrated development of the international insurance industry. *Finan Technol Era.* 2020;7:19–22.
4. Ge X. Exploration of taxation credit management based on sovereign blockchain technology. *Hunan Taxation College News.* 2020;33(3):3–9.
5. Xiaoya R. Research on financial issues of supply chain finance model based on blockchain technology embedded-with ant financial shuangliantong as an example[J]. *Shanxi Agricultural Economics*, 2020(10): 162-163
6. Hunter JC, Patel P S, Sant'Anna L, et al. System and method for implementing an interbank information network: U.S. Patent Application 16/279,137[P]. 2019-6-20.
7. Nasdaq and Citi Announce Pioneering Blockchain and Global Banking Integration. [EB/OL]. [2017-05-22]. <https://www.citigroup.com/citi/news/2017/170522a.html>.
8. Banking Giants Including Citigroup and Barclays Sign Up for a Trial Blockchain Project. [EB/OL]. [2018-07-30]. <https://fortune.com/2018/07/30/blockchain-barclays-citi-app-store-ledgerconnect/>.
9. Titans of Technology: Blockchain/The Top Companies in Blockchain Patents 2021. [EB/OL]. [2018-07-30]. <https://harrityllp.com/titans-of-technology-blockchain-the-top-companies-in-blockchain-patents-2021/>.
10. NASDAQ linq enables first-ever private securities issuance documented with blockchain technology. [EB/OL]. [2015-12-30]. <https://ir.nasdaq.com/news-releases/news-release-details/nasdaq-linq-enables-first-ever-private-securities-issuance>.

11. Distributed Ledger Technology: beyond block chain. [2016]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
12. BNP Paribas and EY explore private blockchain to optimize the bank's global internal treasury operations. [EB/OL]. [2017-10-17]. <https://group.bnpparibas/en/press-release/bnp-paribas-ey-explore-private-blockchain-optimize-bank-s-global-internal-treasury-operations>.
13. BBVA issues corporate loan using blockchain. [2018-04-26]. <https://www.ft.com/content/8c5a44e8-4878-11e8-8ae9-4b5ddcca99b3>.
14. IOTA-based 'E-KRONA' cryptocurrency to be launched by sweden. [EB/OL]. [2018-04-01]. <https://ethereumworldnews.com/iota-based-e-krona-cryptocurrency-to-be-launched-by-sweden/>.
15. Project Ubin: Central Bank Digital Money using Distributed Ledger Technology. [EB/OL]. [2020-12-08]. <https://www.mas.gov.sg/schemes-and-initiatives/project-ubin>.
16. Trade Finance Registry: Singapore launches the world's first blockchain-based solution aimed at preventing double financing fraud. [2020-10-08]. <https://www.tradefinanceglobal.com/posts/singapore-launches-the-worlds-first-blockchain-based-solution-aimed-at-preventing-double-financing-fraud/>.
17. Fujitsu to Conduct Blockchain Field Trial of Money Transfer Service with Three Major Japanese Banks. [EB/OL]. [2017-10-10]. <https://www.fujitsu.com/global/about/resources/news/press-releases/2017/1010-03.html>.
18. Blockchain technology in India. [EB/OL]. [2017-04]. <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf>.
19. Major UAE bank implements blockchain tech to prevent check fraud. [EB/OL]. [2018-04-23]. <https://cointelegraph.com/news/major-uae-bank-implements-blockchain-tech-to-prevent-check-fraud>.
20. These countries are creating their own digital currencies. [EB/OL]. [2017-09-27]. <https://www.verdict.co.uk/bitcoin-countries-digital-currency/>.
21. Move over bitcoin, these countries are creating their own digital currencies. [EB/OL]. [2017-09-27]. <https://www.verdict.co.uk/bitcoin-countries-digital-currency/>.
22. Wang Qiao. The impact of the rise of digital currency on my country's financial industry[J]. Modern Business, 2018(5): 136-137.
23. Committee on Payments and Market Infrastructures and Markets Committee, Central bank digital currencies. [EB/OL]. [2018-03-12]. <https://www.bis.org/cpmi/publ/d174.pdf>.
24. Bank of Canada, European Central Bank, Bank of Japan, et al. Central bank digital currencies: foundational principles and core features. [EB/OL]. [2020-10-09]. <https://www.bis.org/publ/othp33.pdf>.
25. Cai Weide, Zhao Zihao, Zhang Chi, et al. Discussion on the British legal digital currency RSCoin [J]. Financial digitization, 2016(10): 78-81.
26. Darshini D.,Stanley Y.,A. Lewis. The future is here project Ubin: SGD on distributed ledger[R]. deloitte.
27. Accenture. Project ubin phase 2[R], The Association of Banks in Singapore, 2017.11.
28. JP K. Why-fed-is-more-likely-to-adopt-bitcoin. [EB/OL]. <http://jpkoning.blogspot.ca/2013/04/why-fed-is-more-likely-to-adopt-bitcoin>. <http://jpkoning.blogspot.ca/2013/04/why-fed-is-more-likely-to-adopt-bitcoin.html>.2013.4.2013.4.
29. Rod G. Fedcoin CAD-coin versus[R], R3 reports, 2016.11.15.
30. Wendy M. Fedcoin: the U.S. will issue e-currency that you will Use. [EB/OL]. <https://news.bitcoin.com/FEDCoin-u-s-issue-e-currency/2017.1.12>.
31. JP K. FEDCoin: A central bank-issued cryptocurrency[R], R3 report, 2016.11.
32. The Central Committee of the Communist Party of China and the State Council. Opinions on supporting Shenzhen to build a pilot demonstration zone for socialism with Chinese characteristics. [EB/OL]. [2019-08-18]. http://www.gov.cn/zhengce/2019-08/18/content_5422183.htm.

33. Atsushi Santo, etl. Applicability of distributed ledger technology to capital market infrastructure. JPX exchange group. 2016.
34. Analysis of accounts receivable of industrial enterprises above designated size in 2020Q1 [EB/OL]. 2020-06-23. https://www.sohu.com/a/403615440_818225.

Chapter 6

Blockchain and Logistics



Wenming Zhe, Xiaoqiang Qiao, and Qing Cong

Abstract The participants in the logistics process are different entities from different areas of the logistics. When they work together to establish productive relationships, a massive cost is needed to solve the trust issues, such as operational costs of service quality, billing reconciliation costs, and audit management costs for logistics documents, etc. Blockchain technology can effectively solve the trust problem in large logistics, and can facilitate the realization of large-scale, low-cost and high-trust logistics platforms. This chapter introduces the trust problems in the logistics industry, as well as the solutions based on the blockchain. It also presents the application scenarios and practices to help better understand the application of the blockchain technology in the logistics industry.

Keywords Blockchain · Internet of things · Logistics traceability · Logistics documents

6.1 Overview of Application Areas

As an industry connecting the primary, secondary and tertiary industries, and linking production and consumption, logistics involves a wide range of fields, has great development potential and a strong driving effect. Logistics provides an important guarantee for international trade and an essential support for commodity circulation in China. According to the estimation of the World Economic Forum, reducing trade barriers in the supply chain can increase global GDP by nearly 5% and global trade by 15%. At the same time, logistics is also an important foundation for building the Internet economy. With the progress of globalization of the Internet, the logistics industry is increasing in both scale and complexity, and the requirements for

W. Zhe · X. Qiao · Q. Cong (✉)
JD Logistics, Beijing, China
e-mail: congqing@jd.com

logistics enterprises are becoming increasingly diversified. In this background, logistics enterprises adjust strategical layout, utilize social logistics resources and accelerate innovation with various techniques to provide more comprehensive services for customers.

According to data released by the National Development and Reform Commission of China, in 2019, the national total value of social logistics goods amounted to 298.0 trillion yuan, a year-on-year growth of 5.9%; the total revenue of the logistics industry reached 10.3 trillion yuan, a year-on-year growth of 9.0%. In May 2020, the General Office of the State Council has forwarded the “Implementation Opinions on Further Reducing Logistics Costs”, issued by the National Development and Reform Commission and the Ministry of Transportation, which emphasized the acceleration of the development of smart logistics, and proposed “promoting the application of emerging technologies and intelligent equipment to improve the level of automation and intelligence in logistics including warehousing, transportation, and distribution”. In August 2020, thirteen departments including the National Development and Reform Commission, and the Ministry of Industry and Information Technology issued the “Implementation Plan for Promoting the Deep Integration and Innovative Development of the Logistics Industry and Manufacturing Industry” ([2020] No. 1315), which proposed to actively explore and promote the application of emerging technologies such as blockchain and fifth-generation mobile communication technology (5G) in information sharing and credit system construction of logistics. According to a survey of 202 transportation and logistics industry respondents from 16 countries or regions released by IBM in May 2018, 14% of the logistics industry executives surveyed are using and investing in blockchain, and 77% of logistics industry executives expect to have a blockchain network in production within the next 1–3 years [1]. It can be said that blockchain has become an important technical choice for developing smart logistics, improving the level of logistics information sharing and the ability to build a credit system.

In August 2020, Maersk published the report “Digital transformation in logistics: revolution of data and technology in supply chain logistics” [2], which mentioned that the logistics industry is currently relatively behind other industries in terms of digital reform and that fundamental changes are needed in order to gain the advantages offered by new technologies. The main reason for this situation is that there are a number of barriers in data standardization, sharing and collaboration. In summary, the general problems in the logistics industry including information asymmetry, poor information compatibility, and impeded data flow, lead to higher and higher trust costs in the production relationship in logistics..

Firstly, the centralization of information systems causes high interaction costs. Due to the centralization of enterprise logistics system, the data sharing and data flow between upstream and downstream enterprises in supply chain usually requires data connection through the corresponding interfaces. Moreover, because there are many credit handover links in the information flow of the entire supply chain, the connection of the system will be very cumbersome. In addition, even if the data intercommunication is realized through the existing technology, the authenticity and reliability of the data cannot be guaranteed.

Secondly, the authenticity of commodities cannot be fully guaranteed, especially for food and medicine. It can be said that the biggest challenge in commodity traceability and anti-counterfeiting lies in that authenticity and reliability of the information provided by any party in the supply chain can not be ensured. There are many stakeholders are involved in the whole logistics process and the sources of commodity information are diversified, resulting in high risks of forgery and data tampering, and difficulty in tracking when problems occur. Consumers are lacking of credible basis to judge the authenticity of commodities, which makes it difficult to produce evidence and deal with disputes.

Thirdly, the logistics credit mechanism is imperfect. There are a large number of credit subjects in the logistics ecology, including individuals, enterprises, logistics equipment, etc.. How to safely and effectively establish a high-trust collaborative relationship between multiple parties is the key to ensuring that front-line logistics practitioners provide high-quality services, enterprises undertake the social responsibility, and smart electronic equipment operates safely. However, the logistics industry is currently lacking of industry-recognized credit evaluation standards and credit guarantee mechanisms, and the logistics credit ecology needs to be established. At the same time, the lack or low credit rating of small and medium-sized enterprises in the logistics supply chain also cause difficulties in investment and financing.proof.

As a distributed database system jointly maintained by distributed computer network nodes, blockchain has the characteristics of decentralization, openness, transparency, and tamper-proof, which can help solve the problems of information asymmetry and information fraud in social logistics. At the same time the system paralysis caused by network attacks can be effectively avoided. The consensus mechanism based on blockchain can build a decentralized trust system, which can help all participants to build an open network that is both open and transparent while fully protecting the privacy of all parties, and establish a highly trusted social logistics environment, which can effectively solve the above-mentioned problems.

6.2 Blockchain-Based Solution Ideas

The participants in the logistics process are different entities from different areas of logistics, and when they work together to establish productive relationships a massive cost is needed to solve the trust issues, such as operational costs of service quality, billing reconciliation costs, and audit management costs for logistics documents, etc. Data exchange between organizations through traditional electronic data interchange (EDI) can cause data inconsistencies between organizations due to network problems, system failures, or human modification, etc., thus reducing data credibility. In addition, EDI is also premised on the establishment of a cooperative relationship between two parties, which increases the threshold for the use of the system. Blockchain technology is able to achieve security, reliability and integrity of data in the exchange process. At the same time, blockchain network is more open which can

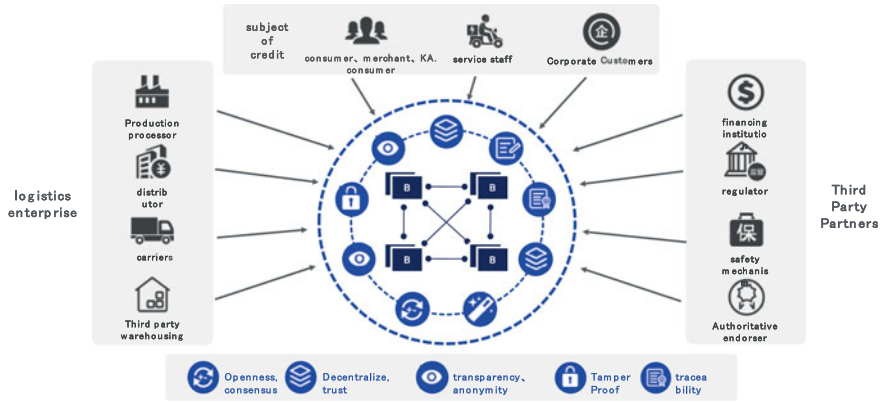


Fig. 6.1 Blockchain-based technology to solve the trust problem of big logistics

effectively solve the trust problem in large logistics, and can facilitate the realization of large-scale, low-cost and high-trust logistics platforms [3], as shown in Fig. 6.1.

In the logistics industry, from the initial “business flow” to “goods flow”, and the corresponding “capital flow” and “information flow”, a key issue behind the various “flows” is the transfer of ownership of goods. Many of the problems solved by blockchain technology are related to the friction of trust in the transfer process of goods ownership. From this perspective, the logistics industry involving the convergence of multiple streams is very suitable for applying blockchain technology.

The use of blockchain technology can promote the convergence of business flow, goods flow, information flow and capital flow in logistics, which can rapidly aggregate high-quality resources on the basis of mutual trust of multiple parties, create three-dimensional ecological supply chain services, and ensure the authenticity and credibility of the data collection through Internet of Things technology. At the same time, the distributed ledger based on blockchain can effectively break the information island, ensure the authenticity and reliability of data storage, greatly improve the speed, breadth and depth of the mapping from goods flow to information flow, further strengthen the credible information flow, and reduce the distance between capital flow and goods flow. In addition, blockchain technology can ensure the authenticity and real-timeness of enterprise financial data, which can significantly enhance the convenience of financing for entity enterprises, shorten the settlement cycle and realize quasi-real-time settlement.

Therefore, logistics enterprises can use blockchain technology to provide integrated logistics services based on the existing logistics network for manufacturers, distributors, retailers and other merchants, to offer monitoring, traceability and standard logistics service operation for each commodity in the whole process of manufacturing, transportation, warehousing and circulation, to achieve the traceability and quality assurance of goods in the process of omni-channel inventory sharing, to reduce the number of times of goods handling and realize the “short chain”, thus reducing the logistics cost of the whole society.

6.3 Application Development Trends

In terms of applied research, a study, jointly published by DHL and Accenture in 2018, concludes that blockchain can play a role in facilitating faster and leaner logistics in global trade, improving supply chain transparency and traceability, and automating logistics business processes through smart contracts, thereby further unlocking the value of logistics [4]. A report published by PricewaterhouseCoopers (PwC) in 2020 believes that blockchain has high application potential in the logistics industry to address key challenges through creating encrypted digital records that tracks goods at every stage in the supply chain, which makes the shipment clearly visible, solves the dispute quickly, and automates operations, reduces paper-based operations, and supports end-to-end traceability [5].

In terms of application implementation, the application of blockchain in logistics involves process optimization, logistics tracking, logistics finance and logistics credit, covering settlement and reconciliation, commodity traceability, cold chain transportation, electronic invoicing, ABS asset securitization. Especially in the fields of shipping, food traceability, logistics finance, there are already some mature projects. TradeLens, a blockchain-based supply chain platform jointly built by Maersk and IBM, uses blockchain technology to help manage and track shipping document records, thereby improving shipping efficiency and security. Oracle's smart supply chain tracking application uses blockchain technology to help trading partners manage the complexity of the global network, improve supply chain efficiency and visibility, and enable the use of smart contracts to send alerts and even take actions. IBM launched Food Trust, a blockchain-based food supply chain ecosystem in 2018, aiming to improve the transparency and traceability of the food supply chain by creating an end-to-end history of each product. It has already achieved some application success with Walmart and Nestle. In 2019, UPS with Inception, a company in the e-commerce space, launched the Zippy Logistics blockchain platform, which enables merchants to monitor the entire supply chain process from product launch to shipment, and ensures that sensitive data such as specific contract pricing and rates are only available to specific buyers and sellers, thus helping companies improve their supply chain management.

In addition, companies in the logistics field have collaborated to explore the application of blockchain in logistics by establishing alliances. For example, the Global Blockchain Freight Alliance (BiTA), established in August 2017, aims to promote the application of blockchain and other emerging technologies in logistics and freight through industry standards, application and solution training, etc.. The members are mainly from freight, transportation, logistics and affiliated industries, and it currently has nearly 500 members in 25 countries. The "Logistics + Blockchain Technology Application Alliance" led by JD Logistics in May 2018, aims to build an international interaction platform for blockchain technology, which promotes the establishment of a unified application technology standard for blockchain in the logistics industry, and helps the innovative development of blockchain technology in the logistics industry.

6.4 Application Scenarios and Application Practices

6.4.1 Logistics Documents

1. Overview of applications

Logistics documents are the general term for all documents, bills and vouchers used in the logistics process, including transportation documents, storage documents, distribution documents, packaging documents, etc. [6, 7]. In the field of supply chain, most of the credit documents between enterprises and enterprises, between enterprises and individuals still use paper documents and handwritten signatures. These documents are used not only as operational documents but also as settlement documents, bringing a series of obstacles to logistics operations and supervision, and restricting the development of intelligent logistics and logistics finance.

(1) Costs caused by paper-based documents

The existence of paper-based reconciliations, caused by the requirements of traditional internal and external audits, creates waste in terms of material and management costs. The costs can be significantly reduced by going paperless.

(2) Operational problems caused by paper-based documents

Paper documents are usually delivered offline, which easily leads to inconsistencies between information flow and document flow, generating more operational abnormalities, resulting in large reconciliation discrepancies and long settlement cycles. As a result, the cash flow of carriers as well as payback are seriously affected, and more time is spent on specific matters such as account exception, resulting in a negative user experience.

(3) Regulatory issues arising from paper-based documents

Currently, the network freight is entering in the era of digital supervision. In terms of the requirements that the network freight operators are not allowed to fabricate transactions, transportation, settlement information etc., it is difficult to ensure the the authenticity and real-time nature of document content by paper documents and reporting supervision data through the system interface.

In recent years, the rapid development of electronic technology makes social production and life more and more dependent on electronic technology products, digital communication networks and computers, etc., so that the storage, transmission, statistics, release of information gradually realize paperless. The “Contract Law” promulgated in 1999 and the “Electronic Signature Law” promulgated in 2005 established the legal effect of electronic signatures. The “Electronic Signature Law” proposed reliable electronic signatures have the same legal effect as handwritten signatures or seals, while the “Contract Law” also states that data messages, like paper contracts, are a type of of writing form and have the same legal effect.

As an emerging technology, blockchain has also been gradually recognized by the judiciary, The Supreme People’s Court Of The People’s Republic Of China issued

the “The Provisions of the Supreme People’s Court on Several Issues Concerning the Trial of Cases by Internet Courts”, which clearly states in Article 11 that if the authenticity of the electronic data submitted by the parties, through electronic signatures, trusted timestamps, hash value verification, blockchain based evidence collection, fixation and anti-tampering, or certification through electronic evidence collection and storage platforms can be proved, the Internet Court shall confirm it.

JD Logistics uses blockchain and electronic signature technology to create the “E-Signature chain” product, which solves the problems of untimely receipt, easy loss, easy tampering, and high management costs introduced by traditional paper documents. It also uses digital signature technology to solve the problems in processing abnormalitie of traditional paper documents, and to realize timely correction in the logistics distribution process, and to put the modified data on the chain in real time. Therefore, the operation and settlement personnel of both sides can obtain accurate data in time. At the same time, a blockchain-based trusted document signing platform, backed by the supply chain advantages of JD Logistics and the existing logistics network and technology, can achieve the integration of document flow and information flow.

2. Application of technology

Digital signature technology is a kind of electronic signature, the signature mentioned in the current electronic signature law, generally refers to the digital signature. Simply, the digital signature is a string of unique electronic passwords generated by a certain cryptographic operation. Instead of written signatures or seals, it can be used to identify the signer and the recognition of the content of an electronic data, to verify whether the original document has changed during the transmission process, to ensure the integrity, authenticity and non-repudiation of the transmitted electronic documents.

The document information is stored on the chain through blockchain technology, and the document uses asymmetric encryption technology for electronic signature and signature data verification. During the electronic document signing process, the logistics participants store the signature data into the blockchain, which can achieve data fidelity by verifying the authenticity of the data. Figure 6.2 shows the electronic document signing process of the carrier agreement between the cargo owner and the carrier driver.

The digital signature service uses the private key to sign, and the users use the public key to confirm. The private key can be the main identity or a role identity that needs to be legalized through platform registration and authentication by an authority. Having different role identities, the users can use digital signature services for different scenarios, such as file signature Decentralized application (Dapp) certification, etc.

First of all, it is necessary to pre-define the agreement template, the signatories and the signing process of the Power of Attorney Agreement. The trusted document service platform needs to provide the ability to define different signing processes according to the needs of different scenarios.

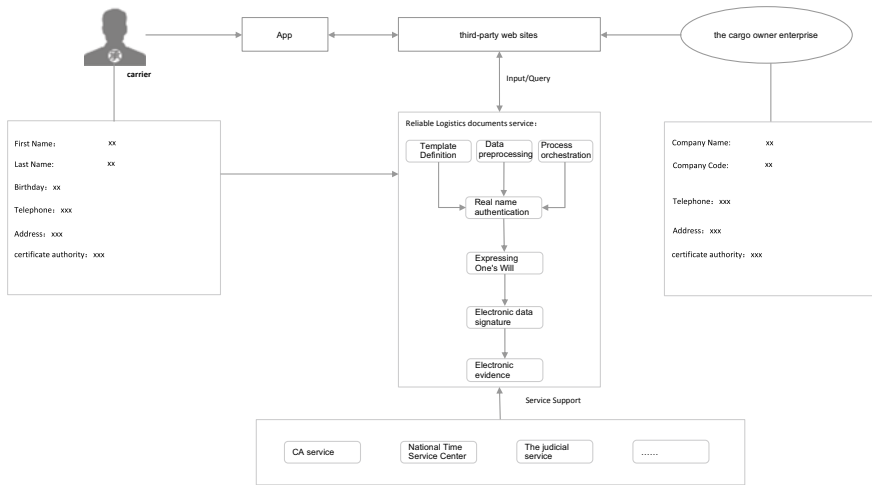


Fig. 6.2 Example of a file signing service

Before the document is signed, the owner enterprise and the driver as the signer of the document need to complete the real-name authentication in advance, and digital certificates to authenticate their identities can be issued by the CA. authentication technology to check the. The legitimacy of the identity of the certificate holder could be verified through CA technology, ensuring that all transactions signed by the private key on the blockchain are real-named. The real-name authentication and digital certificate issuance information are also stored on the chain for evidence.

When signing a document, it is necessary to complete the expression of willingness to sign through biometric identification and SMS verification to ensure the validity of the signing subject and behavior. The confirmation of willingness information will be uploaded to the chain for evidence.

Finally, the signed electronic power of attorney agreement and related logs are stored as certificates. Each participant can view, extract, and verify the stored certificate information on the chain through publicity tools such as exclusive blockchain browsers.

Blockchain certificate deposition is a service based on blockchain technology, which can use a multi-node consensus method to unite the electronic data storage services provided by courts, notary offices, judicial appraisal centers, time service agencies, audit institutions, and digital identity authentication centers, etc. Blockchain and related distributed ledger technologies can guarantee the integrity and authenticity of the storage information [8] (Fig. 6.3).

It can also build a credible document inspection platform through the blockchain to provide stakeholders with a unified view of document inspection and download, and complete the evidence chain connection with authoritative organizations based on standard cross-chain protocols, such as the Beijing Internet Court “Tianping Chain”,

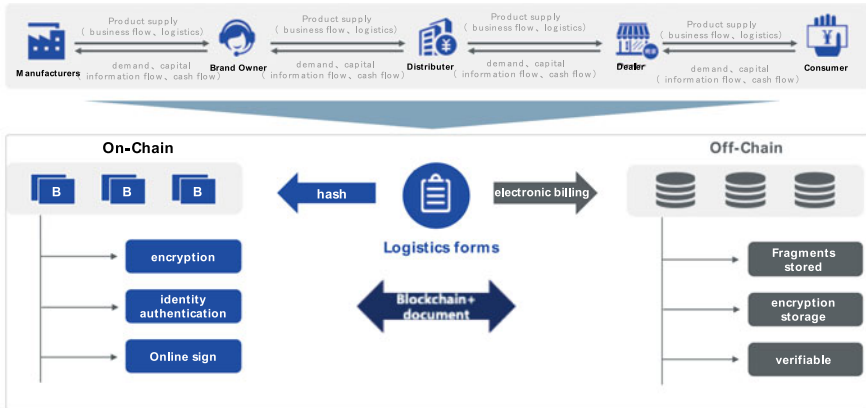


Fig. 6.3 Blockchain-based unification of document flow and information flow

thereby Improve the efficiency of evidence collection and reduce the cost of judicial evidence collection.

It can also build a trusted document checking platform through blockchain to provide stakeholders with a unified view of document checking and downloading, and to complete evidence chain docking with authoritative institutions based on standard cross-chain protocols, such as the “The Libra Chain” of the Beijing Internet Court, thereby improving the efficiency of evidence collection and reducing the cost of judicial evidence collection.

3. Application governance

The credible document service platform can adopt the governance method of the consortium blockchain. In this network, JD Logistics, carriers, CAs and other business stakeholders can join as nodes on the chain to form a reliable consortium chain network. In the business setting, a governance method that conforms to the characteristics of supply chain logistics is adopted to ensure the credible sharing of supply chain data, and to have good security features and privacy protection capabilities. The blockchain platform used is based on JD Chain, a basic blockchain platform, which strengthens the application of the blockchain in customer real-name, as well as contract signing, management, maintenance and guarantee, It lays a good foundation for the application scenarios of logistics documents.

6.4.2 Express Reconciliation

1. Overview of applications

At present, the logistics express transport business can be divided into Full Truck Load and Less Truck Load transport of main and branch lines, TC (rapid distribution

center) transfer business, city distribution, door-to-door collection, etc. The business development is very fast, which puts high demands on the reconciliation ability of transport carriers. However, due to the limited degree of informatization and other reasons for express reconciliation, there are still the following development pain points.

(1) Poor carrier experience due to long reconciliation cycles

According to incomplete statistics, the reconciliation cycle of carriers is often as long as 90 days, which greatly affects the cash flow and the payback. Both sides need to spend some time on specific matters such as approved account abnormalities, resulting in a negative user experience. and with the increase in the volume of JD. Logistics express business, these problems are more prominent.

(2) Passive reconciliation and uncontrollable bill recovery rate

Due to the imperfect mechanism for sending and collecting paper statements, there are frequent cases of non-collection of paper statements, which makes reconciliation management difficult and makes it difficult to control the collection and reconciliation rate of statements.

(3) Low reconciliation coverage and difficult in ensuring accuracy caused by manual reconciliation.

Manual reconciliation has large data differences, such as asymmetrical information. It takes a lot of time and manpower to verify these difference in the reconciliation, and the accuracy is difficult to guarantee.

(4) High costs caused by paper-based office

The existence of paper-based reconciliations due to traditional internal and external audit requirements creates waste in terms of material and administrative costs, which can be substantially avoided by going paperless.

In the case of manual reconciliation, a series of follow-up work such as bill collection, reconciliation results verification and statistics are handled manually, which brings about problems such as greater labor intensity of employees and lower efficiency of reconciliation. It also makes it difficult to provide timely feedback on reconciliation results, and reconciliation costs and management costs will continue to rise with the increase of the number of customers (Fig. 6.4).

The general logistics carrier process has several stages including order placement, inquiry, transportation and sign-off. The enterprises on both sides of the settlement need to complete the sharing and circulation of data at different stages with system interface. Through traditional technical means, only information flow interoperability can be achieved and the trust problem can not be really solved. Credit signing still relies on paper waybill, and Both parties have a set of clearing and settlement data. During each settlement cycle, both parties have to reconcile, requiring manual review of a large number of paper documents, which is costly, inefficient and has a long settlement cycle. The use of blockchain technology to achieve trusted sharing of multi-party data can help enterprises and carriers to establish a trust relationship, so

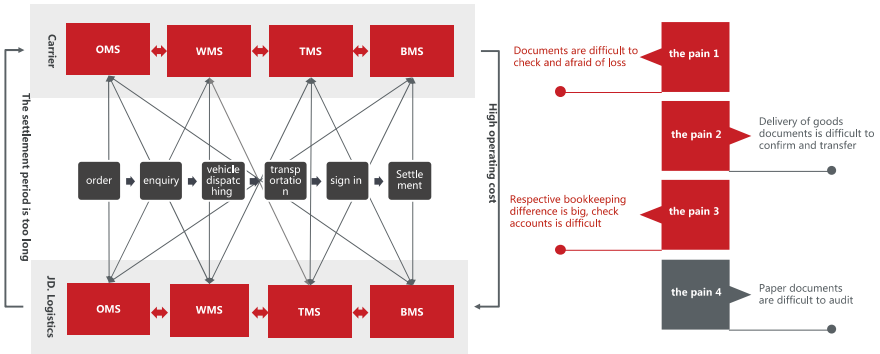


Fig. 6.4 Traditional reconciliation process: inefficient and costly

as to solve pain points of the logistics reconciliation, the problems of the document handover and operational reconciliation, and to meet the settlement requirements between enterprises and carriers.

2. Application of technology

Blockchain-based distributed ledger and smart contract technologies improve existing business processes to achieve shorter reconciliation and payment cycles, thereby helping logistics companies increase the discount space for carriers. The overall process is shown in Fig. 6.5.

(1) Paperless offline document handover

By integrating the mobile app application, the quantity, weight, volume, receiving time, handover time, delivery time, and the upstream and downstream cost data of

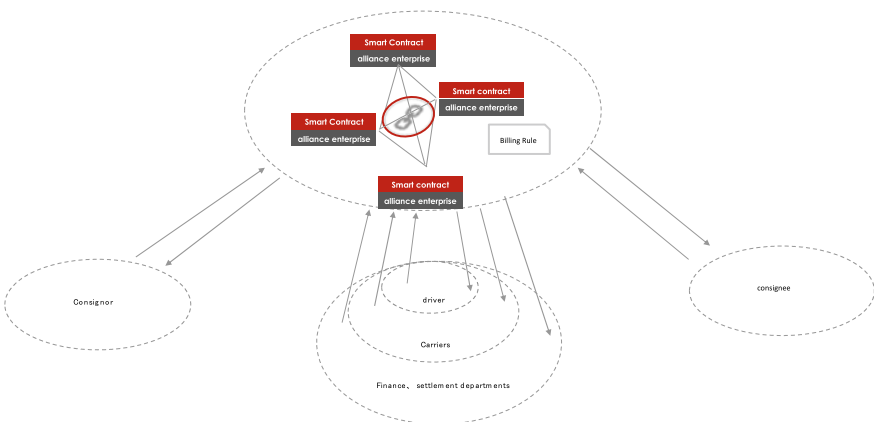


Fig. 6.5 Smart contract-based express reconciliation process

the entire process can be used to generate electronic statements in a unified way, and the credit handover of goods can be realized based on electronic signatures.

(2) Paperless reconciliation in the settlement department

Through the regular push of ledger data from the blockchain smart contract platform and support for exportable statements with electronic signatures, the multi-party coordinated reconciliation between the sender, the receiver, the carrier, and JD Logistics can be realized. The automated reminders of the specific difference can be realized, so the account difference can be located and checked timely.

As shown in Fig. 6.6, the blockchain-based express transportation reconciliation process starts to be chained from the order generation to inquiry, quotation, distribution, and delivery. The blockchain-based electronic transportation settlement vouchers is generated through paperless sign-off by credit entity. During the transportation process, RFID and other IoT technologies are used to ensure the authenticity of data collection in the logistics process, In order to achieve the consistency of vehicle mounted information flow and GPS physical data flow. With vehicle GPS system to collect location data, the consistency of information flow and physical flow could be achieved.

The real-time, realness, reliability and hard-to-tamper characteristics of the data on the chain can realize realtime transaction clearing. At the same time, the electronic contract containing the freight rate rules can be written into the blockchain, and both parties of the settlement can share the same mutually recognized transaction data and freight rate rules, so that the reconciliations are fully consistent. Moreover, if there are abnormal bills in the reconciliation process, it can also be handled by adjustment. While the audit process of adjustment and information of settlement, payment and invoice will be written into the blockchain as a deposit evidence.

3. Summary

By standardizing the existing business process, JD. Logistics, with carrier enterprises, have shortened the supplier reconciliation period from the original 90 day to

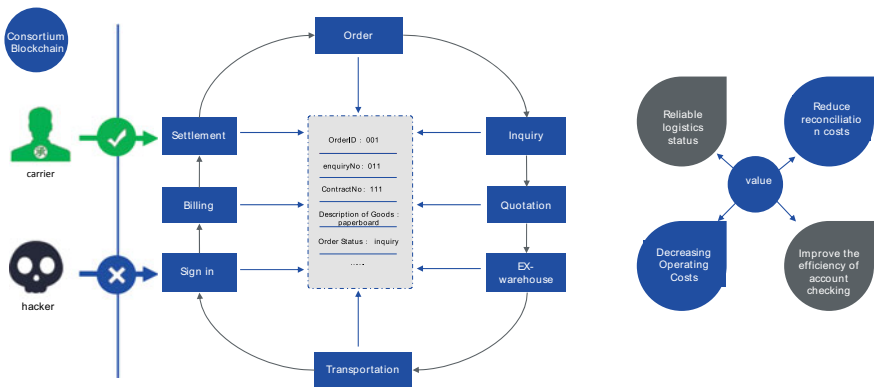


Fig. 6.6 Blockchain-based reconciliation process: quasi-real time and low cost

30 days, thus achieving a significant reduction in operation and management costs. If the national annual express transport expenditure is 2 billion yuan, the application of blockchain technology can achieve cost savings of 200~300 million a year. With the rapid development of express transport business in the future, there will be even more room for cost savings. Meanwhile, more application scenarios can be derived by applying the consortium chain technology and taking the advantages of the core logistics enterprises in the supply chain. For example, trusted documents and transaction data on the blockchain can be used to provide factoring services for supply chain finance to deal with the difficulty and high costs of financing for small and medium-sized enterprises.

6.4.3 Agriculture-Logistics Traceability

1. Overview of applications

At present, most of China's logistics traceability systems for agricultural products are based on centralized database and bar codes, which can usually only trace back to the production enterprise, but less to the quality and safety of the whole process, especially rarely to the information on production environment, the key concern of consumers. The main agricultural products traceability systems in China are still in the pilot stage, and there exist problems such as inconsistent standards, making it very difficult to promote their application.

As a decentralized distributed accounting technology, blockchain, with its characteristics of consensus mechanism, open and transparent records and tamper-proof data storage, can provide good data security and trustworthiness guarantee for logistics traceability of agricultural products. It can also be combined with IoT technology to ensure the real-time and authenticity of traceability information collection, unify the quality and traceability information standards of agricultural products, provide proof of the safety and reliability of producer's agricultural products, and provide consumers with a highly credible consumption ecology of agricultural products (Fig. 6.7).

2. Application of technology

Based on blockchain and IoT, one-thing-one-code of information flow can be realized. By assigning unique anti-counterfeit code for small packaged agricultural products, the offline one-thing-one-code can be implemented by means of laser marking irreversible QR code, chip and laser marking. Therefore, the collection process of key data generated by agricultural products in production, storage, logistics and trading is authentic and credible, and the authenticity and reliability of data storage can be guaranteed. Finally, the whole life cycle data of agricultural products can be provided to the regulatory authorities or consumers for traceability and authenticity checking.

As shown in Fig. 6.8, the overall architecture of the logistics traceability platform for agricultural products based on blockchain technology can be divided into three

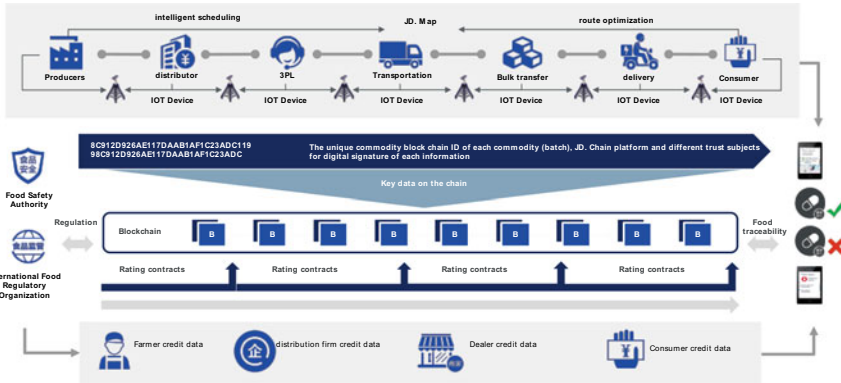


Fig. 6.7 Blockchain-based traceability process for agricultural logistics

layers: user application layer, data service layer, and data access layer. The data access layer and data service layer are in charge of the data recording and storage for agricultural products. The IoT devices in the perception layer can be used to realize data collection and upload based on the front-end network. The data uploading into the blockchain ledger is ensured by intelligent terminal devices used in the production process and the communication of the blockchain platform.

Sensors and intelligent collection terminals are used to collect data of traceability information to replace the traditional manual input manner, which can effectively avoid artificial fraud and errors. The way of data interaction based on the direct connection between devices and blockchain ensure the diversity and uniformity of data sources. Moreover, with a unified traceability system standard based on determined requirements of data types and communication protocols, and signing and uploading of data on the chain through digital certificates in IoT nodes, the credibility of the data collection process of IoT nodes can be further enhanced.

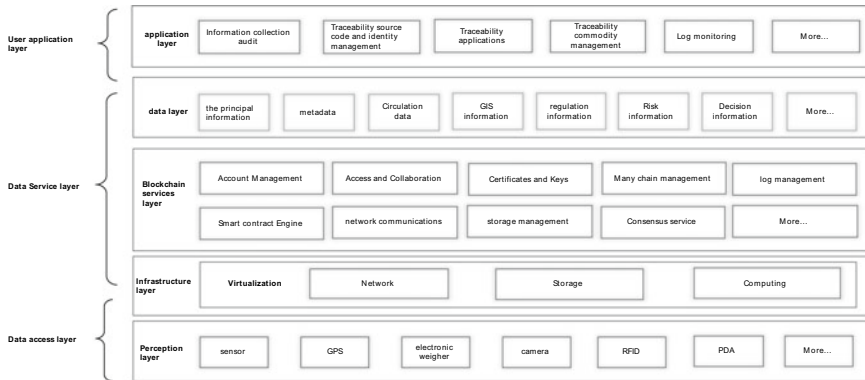


Fig. 6.8 Overall architecture of the agricultural product logistics traceability platform

Transmitted through decentralized blockchain network, the original information of goods in different supply chain nodes can be transmitted through peer-to-peer network, combined with asymmetric encryption technology to ensure the privacy and authenticity of data. The all involved parties maintain the same ledger, which can effectively solve the problems of data island, untraceable commodity information Inaccurate logistics tracking information.

The data storage is designed using a combination of blockchain and database, as shown in Fig. 6.9. The chain storage structure only supports queries through transaction addresses or block addresses, while the traceability data of goods are stored in the local storage of their respective organizational nodes, interacting with multiple subsystems. The data generated in the production, processing, circulation and distribution of goods are encrypted and written into the blockchain ledger through blockchain transactions, and the transaction address is bound to the unique code of goods and then mapped to the database storage system, which can be associated with more non-chain information of goods. When querying the goods traceability data, the blockchain address can be queried from the database of the traceability system, and the data could be obtained and displayed from the corresponding block.

When using the data, consumers only need to identify the unique code through the APP to obtain information on the production and processing of goods, logistics, inspection and testing results, commodity transactions, and so on. The unique goods code combines the “clear code + secret code” method to ensure one-thing-one-code.

3. Application governance

The logistics traceability platform of agricultural products is developed based on consortium chain technology. The organization nodes can be created according to the actual situation of business participants including production and processing parties, logistics parties, brand owners, etc. All participants under different organizations, including producers, IoT devices, packers, warehousemen, distributors, consignees

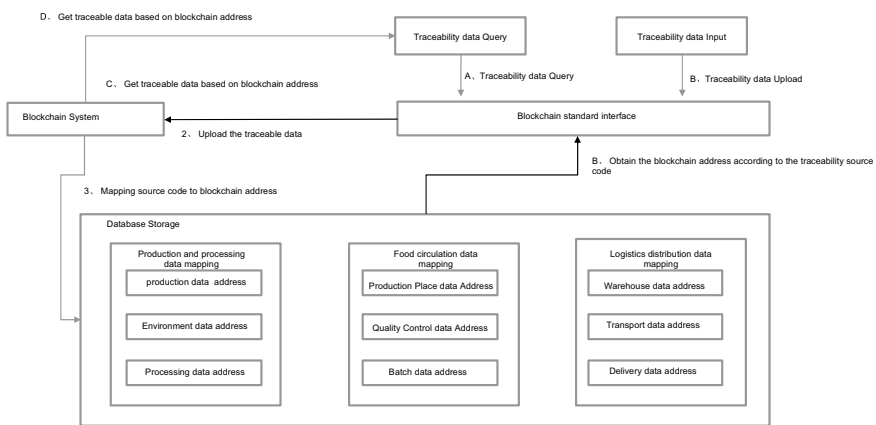


Fig. 6.9 Agro-product logistics traceability information storage and query process

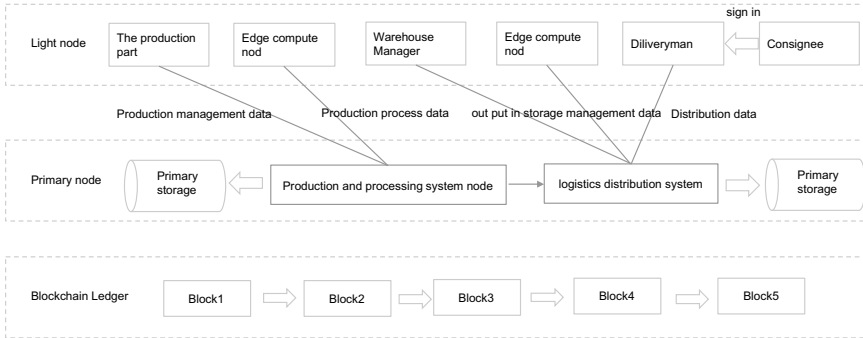


Fig. 6.10 Agri-logistics traceability participation node interaction process

can register their identities as slave nodes. The master node has the right to participate in consensus and accounting, while the slave nodes realize the interaction with the blockchain ledger through the authentication of the master node. All participants are required to pass the authentication of the business system to ensure that the whole agricultural traceability blockchain network is formed based on the trusted identity registration and authentication services. As shown in Fig. 6.10, the authentication request sent by a slave node carries the identity information of itself. After authentication the master node generates a digital fingerprint based on the traceability information uploaded by the slave node, writes it into the blockchain along with the corresponding timestamp, and broadcasts the transaction among all slave nodes. Each node, according to the transmission path of the agricultural products in the physical space, in turn generates a package status information based on the digital fingerprint and the node information of itself and the next one and writes it to the blockchain by the master node. The package signing and receipt information of the user receiving node is formed and uploaded to the master node to be written in the blockchain ledger.

The project applies blockchain technology to agricultural traceability scenarios. The tamper-proof characteristics of blockchain to ensure the authenticity and state traceability of agricultural traceability information, which enables timely and efficient preservation and update of traceability information and meets the requirements of real-time supply chain logistics.

4. Summary

The core of the logistics traceability service platform for agricultural products is to establish a low-cost, high-trust supply chain collaboration environment and to create a new synergy effect. Compared with the traditional closed and linear supply chain logistics management system, the logistics traceability service platform for agricultural products uses a multi-role, large-scale, real-time social collaboration approach to create new value based on a trusted agricultural product supply chain logistics collaboration network. It realizes the upgrade from information transmission to credit transmission and then to value transmission, thus achieving a wider range of

social collaboration. In other words, it brings more participants in the industry chain into this high-trust network at a low cost, and increases the breadth, depth and density of interaction to gradually enhance the synergy effect and promote the innovation of the application mode of the agricultural supply chain logistics.

6.4.4 Logistics Credit Rating

1. Overview of applications

In recent years, the social credit system has played an increasingly important role in improving government management and services, maintaining market economic order, and preventing financial risks. In 2014, the State Council of the People's Republic of China issued the Planning Outline for the Construction of a Social Credit System (2014–2020), which specifies the requirements for credit information sharing. At present, the construction of credit platforms and mechanisms for social organizations including enterprises has achieved positive results. Comparatively, credit of natural persons, especially professional credit, has not yet been realized on a large scale due to scattered information sources and difficulty in collection. The Planning Outline for the Construction of a Social Credit System (2014–2020) proposes to “Give prominence to the fundamental role of natural persons’ credit construction in the construction of a social credit system Strengthen professional credit construction among focus groups.....Broaden the use of professional credit reports, and guide toe construction of professional ethics and behavioral norms.”. Professional credit information, including identity information, education and certificate information, and work experience information, is the foundation of professional credit construction and a key basis for enterprises and institutions in recruiting and employing workers. Many enterprises and institutions have realized the informatization of employee’s professional credit information. However, because professional credit information cannot be interconnected, the fake education and work experience is still a common phenomenon. Even the information of some employee’s illegal behavior cannot be effectively exposed, which brings great challenges to the optimization of the industry environment. These problems are especially prominent for some industries with high staff mobility, such as logistics, catering and housekeeping. In the logistics industry, its upstream and downstream stages involve carrier drivers, appliance technicians, security and maintenance workers, etc. These practitioners usually need to be trained and pass the examination before they can be employed. However, currently the logistics industry is relatively decentralized in terms of career management and credit information, with problems such as incomplete endorsement content, restricted use of credit data and inaccurate credit data, etc. At the same time, as the rating rules and rating results for practitioners are only used within specific enterprises, there is no uniform rating standards in the industry.

Blockchain, as an anti-forgery, anti-tampering and traceable database technology based on multi-party consensus, ensures limited and controllable credit data sharing

and verification on the basis of effective data privacy protection from the technical perspective. A blockchain credit alliance could be established by uniting logistics ecological enterprises, forming a consortium chain of multiple parties such as digital identity management agencies, universities and employers. It can accumulate credible transaction data and provides effective means for sharing and circulation of professional credit information. At the same time, it can be combined with technologies such as electronic signature and privacy calculation to protect the personal privacy of practitioners to achieve a high degree of sharing and effective use of professional credit information. It can also be combined with the construction of credit rating standards for logistics practitioners to truly form the entire logistics credit ecology with data credit as the main body.

As shown in Fig. 6.11, the participants join the network as blockchain nodes, both as data providers and data users. The original data of each party are stored in their respective central databases, from which only a small amount of non-sensitive summary information is extracted and stored in the blockchain. When a party has a credit data query for another one, it first queries the public and transparent summary information in its own node and forwards the query request to the data provider through the blockchain. The data provider extracts the detailed plaintext information from its own local database to the querying party after obtaining authorization from the engineer and receiving payment from the data querying party.

In addition, the autonomy of blockchain technology can be used to facilitate the establishment of credit rating standards in the logistics industry. The prerequisite for data credit establishment is a set of industry credit rating standards, and logistics industry credit rating standards require the joint participation of enterprises in the industry. The rating algorithm can be implemented through smart contracts and published to the consortium chain. The rating results can be calculated using real transaction data on the ledger, so that the system can automatically execute

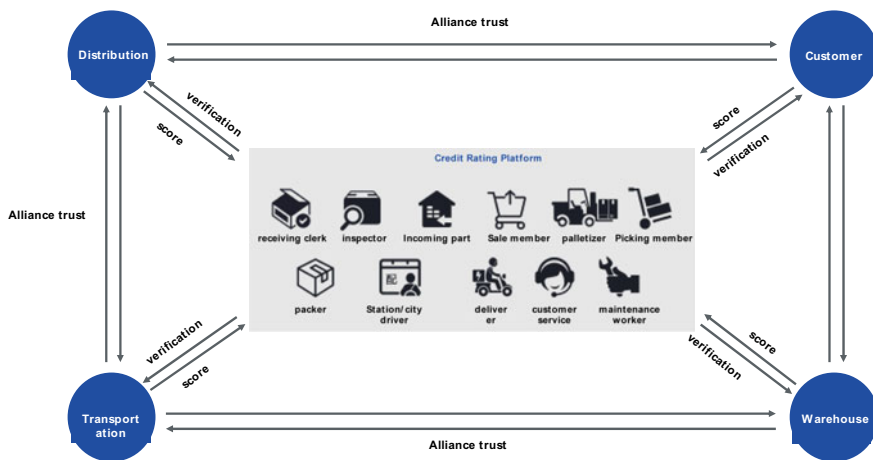


Fig. 6.11 Logistics credit rating service platform based on block chain

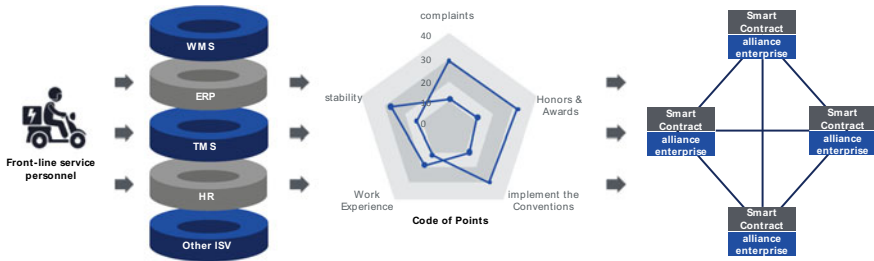


Fig. 6.12 Logistic credit rating standardization

the rating procedure without human intervention. Based on coordinated specifications and protocols among the consortium nodes, all nodes in the whole system can exchange data freely and securely in a trusted environment, as shown in Fig. 6.12.

2. Application of technology

As a legal and authoritative third-party electronic authentication service provider, CA can authenticate, issue and manage digital certificates for individuals, enterprises, institutions and government agencies, confirm the identity of each subject in e-commerce activities, and implement secure information exchange and secure transactions online through encryption and decryption strategies. The role of CA is to check the legitimacy of the certificate holder's identity, and issue certificates, and perform certificate and key The role of CA is to check the legitimacy of the certificate holder's identity, issue the certificate, manage the certificate and key, and ensure that the certificate is not forged or tampered with. The digital certificate is actually a record stored on a computer. It is a statement issued by the CA to prove the unique correspondence between the certificate subject and the public key contained in the certificate. The certificate includes the name and other related information of the certificate applicant, the applicant's public key, the digital signature of the CA and the validity period of the certificate, etc. The role of the digital certificate is to ensure the security of electronic commerce and to mutually verify the identity of both parties in the online transaction [9].

A digital identity for each participating built with blockchain technology can be associated with CA, so that the digital identity has a legal effect when participating in social activities. At the same time the attributes associated with the digital identity can be defined. For example, Zhang San defines an ID card. After being authenticated by an authoritative organization, the authentication information is encrypted and written into the blockchain for evidence. When a third party needs to verify Zhang San identity, it can be verified by means of authorization. Likewise, a professional qualification certificate can be created in the same way.

Blockchain has the features of decentralization, credibility, timestamping, asymmetric encryption, and smart contracts, which ensures limited and controllable credit data sharing and verification on the basis of effective data privacy protection from the technical perspective. The original data of detailed service records are stored in

its own central database. When the data is uploaded to the chain, a small amount of summary information, mainly including engineer number, overall rating and evaluation, is extracted from the central database and saved in the blockchain through broadcast. For detailed service records and engineer contact information, only the HASH value of the content is extracted and uploaded on the chain, which can fully protect the core data assets of the service provider and the personal privacy of service engineers.

3. Application governance

Blockchain can only guarantee that the data on the chain is not tampered with. If the source data is artificially manipulated and falsified because of the interest, it will destroy the trust of all participants in the consortium chain. How to ensure the authenticity of the data from the source is crucial to the establishment of the entire consortium chain ecology. To address this problem, when inviting logistics service providers and appliance installation and maintenance service providers in the industry, it is necessary to sign an alliance agreement to ensure that they will provide true and objective information after receiving the authorized and paid inquiry requests from other service providers. The blockchain will also permanently record the evaluation information of all data transactions to promote the healthy development of the alliance ecology. At the same time, by inviting some financial institutions and government agencies, after obtaining the engineer's authorization, it is convenient to query the third-party credible data of practitioners, such as financial rating credit data and whether there is a criminal record. After comprehensive verification, these data from different participants can reflect the credit status of the engineer as objectively as possible. The status of the initiator and all participants of the consortium chain is also equal, and there is no problem of using the platform to collect data from other service providers, which also fully reflects the decentralization and openness of the blockchain.

4. Summary

Blockchain-based logistics credit information platform can provide multi-role distributed trusted identity services for supply chain participants (individuals, organizations, and smart devices). Based on the credit rating standards of national/industry/group alliances, a logistics express credit rating system could be built and personal credit-like data assets could be constructed. They can be confirmed and circulated in the blockchain network to realize the value chain of the digital economy transcends the boundaries of individual enterprises and evolve into a value network. Through the application of blockchain, the credit system of the logistics industry is built, allowing customers to independently choose service personnel with confidence, allowing enterprises to employ staff with higher competence and professional ethics, allowing service personnel with better overall quality to have more opportunities, and allowing the quality of service to be improved. In the future, industry standards could be built through uniting credit association, application alliance of logistics and blockchain technology, and a decentralized and credible

service system could be developed based on blockchain technology, and an honest and sunny logistics supply chain collaboration environment could be established.

References

1. Ma ST, Ding W. The development trend of blockchain in logistics industry and IBM's layout. *Logistics Technol Appl.* 2018;09:158–61.
2. Maersk. Logistic's Digital Revolution: The Transformation of Data and Technology in Supply Chain Logistics. https://www.maersk.com/~media_sc9/maersk/solutions/technology-and-electronics/files/maersk-logistics-digital-revolution.pdf
3. Bohui S. Research on logistics system based on the theory of large logistics elements. Beijing Jiaotong University; 2013.
4. DHL, Accenture. blockchain in logistics: perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry. <https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf>
5. PwC. Blockchain in Logistics. <https://www.pwc.de/de/strategie-organisation-prozesse-systeme/blockchain-in-logistics.pdf>
6. National Logistics Standardization Technical Committee. Basic requirements for logistics documents, GB/T 33449–2016. Beijing: China Standard Publishing House; 2017.
7. National Logistics Standardization Technical Committee. Classification and coding of logistics documents, GB/T 29184–2012. Beijing: China Standard Publishing House; 2012.
8. Xiao D. Research on the authentication of blockchain deposition evidence. Huaqiao University; 2019.
9. Hong C, Xianhua X. A multidimensional review of authenticity of electronic signature evidence: fidelity, authentication and proof. *Hunan Soc Sci.* 2019;05:61–70.

Chapter 7

Blockchain and Government Services



Xiaojun Zhang

Abstract Government services require trusted data, data sharing between government, and data sharing between governments and enterprises. Based on the advantages of blockchain technology, government data can be shared and exchanged in a trusted manner based on blockchain, implement a data ownership separation mechanism, promote cross-department and cross-efficient, and low-cost administrative supervision system, and build an intelligent mechanism for pre-event evidence storage, data sharing, and linkage collaboration to optimize administrative supervision, city management, and emergency assurance processor and improve governance efficiency. Implemented in market surveillance, administrative law enforcement, and audit scenarios to provide high-quality, efficient, and convenient mobile government services for enterprises and people.

Keywords EI · PBFT · ROMA · Sandbox

7.1 Application Area Overview

In recent years, the digital economy industry has grown steadily. With the development of digital industrialization and industrial digitization gradually stepping into the fast track of development, the proportion of the scale of digital economy in the gross domestic product is increasing in all parts of the country, and the establishment of new technological industrial agglomeration zones is being accelerated in all parts of the country [1]. For example, the Kunpeng Eco-aggregation Zone in Tianfu New District of Chengdu plans to achieve an industrial scale of over 50 billion yuan by 2025. At the same time, the three AI industry clustering areas are mainly Beijing, Yangtze River Delta and Guangdong. At the same time, digital government construction has been accelerated. The integration and sharing of data resources is accelerating. Since the second half of 2018, China has accelerated the promotion and use of electronic license and license to solve the industry problem of license and license separation.

X. Zhang (✉)
Huawei Technologies Co., LTD, Beijing, China
e-mail: z.x_77@163.com

Digital reform and integration of government services through electronic certificates have become the development direction of digital government [2], and the comprehensive upgrade of digital social services is being accelerated. Improvements in the experience of digital social security services are being strengthened. Government service is one of the fundamentals of the application of convenience service, with “zero leg-run” public service as a typical representative, covering employment and entrepreneurship, social insurance, talent service, labor rights protection, etc.

Blockchain applications in the government domain can be classified into four types: data sharing. With blockchain technology, government departments can safely authorize relevant parties to access data and record data invoking behaviors. In this way, data breaches can be effectively and accurately investigated, providing a trusted environment for cross-level and cross-department data interconnection and improving government service efficiency. The application of blockchain technology in digital government will ensure the openness and transparency of government information and facilitate the open sharing of government data. By querying the record information of each node and block in the blockchain, the open and transparent government work can be greatly promoted, and the government supervision mechanism can be improved. Trusted sharing of government data can be applied to land registration and transaction. Anyone can directly query information such as land location, size, ownership, and transaction records recorded on the blockchain. This facilitates open sharing of land transaction information and effectively avoids the rent-seeking phenomenon of public officials. The digital bill trading platform can also be constructed by using blockchain technology, so that the clearing scheme on the chain can realize the registration, circulation and settlement of the digital bill throughout its life cycle. The second is the application of the proof of government information. The original information storage mechanism of enterprises and citizens based on blockchain technology cannot modify the information records, but can only add new records. Therefore, the original information of enterprises and citizens can not be changed, which greatly protects the information security of enterprises and citizens. At the same time, blockchain technology ensures that data cannot be changed or deleted once established, which ensures the validity of judicial evidence, the uniqueness of identity information and the difficulty of tampering with contracts. In addition, individual participants can directly verify personal and corporate information stored in the digital government system through blockchain, avoiding the need for third-party trust agencies, which will significantly improve government efficiency. For example, the application of electronic identity card to prove digital identity [3] and electronic license can accelerate the separation of license and license through blockchain to solve the problem of having business license but not operating license. Application of traceability of certificates, such as marriage certificate, degree certificate, graduation certificate, real estate certificate, etc., from the issuance of certificates to any time of use tracking management. The third is the application of administrative examination and approval and management. Such applications, such as the examination and approval of electronic data evidence, and the one-stop management and review of electronic data evidence, ensure that such applications are managed in a secure and credible process based on the blockchain. Improve

the efficiency of government services, simplify costs, and enhance the credibility of government services. Fourthly, the government supervision responsibility class application. The traceability advantage of blockchain is of great significance for innovation of regulatory model and improving government credibility. The application of blockchain technology in the supervision platform of “digital government” can record all the information of the supervised object, and can monitor and trace the real-time status of the supervised object accurately and efficiently. Once a problem occurs on a regulated object, the blockchain technology can be used to trace the problem source, which greatly improves the effectiveness and efficiency of regulation, and reduces the cost of regulation. For example, a blockchain technology is applied to a food safety platform of the government, and information about each link such as food production, transportation, and sale is recorded in the blockchain, so that consumers can query and verify food quality problems and perform problem tracing at any time, thereby greatly improving the source tracing effect of problematic food. The quality of life of residents is improved.

Information sharing is the premise of digital government service. However, the digital government service in China has long existed such problems as “doing their own administration, partitioning of pieces, numerous chimneys and information island”. Due to the consideration of data security, information silos among government departments in the digital government system are very serious, and data sharing is difficult to promote. Meanwhile, the digital government also faces the problem that electronic data is easy to be tampered with and has no time mark. The integrity and authenticity of the electronic data are in urgent need of reliable technical verification means. In addition, the cost of electronic data replication is almost zero, which makes electronic data vulnerable to leakage. Compared with traditional carriers, the Internet indirectly increases the risk of electronic data leakage. Meanwhile, the rapid development of informationization makes digital government not only satisfy the traditional private network environment, but how to ensure the trustworthy transmission of government data in the Internet environment becomes a key issue for government services.

The blockchain technology features de-intermediation, anti-tampering, traceability, and strong encryption capabilities, which meet the requirements of government services for data circulation security and trustworthiness. consensus mechanism is used to build a trust network with multiple parties to further integrate the Internet and government services. Optimize government business processes to make government affairs transparent, and trustworthy. Blockchain helps to establish trust mechanisms for the flow of data. In a traditional centralized database, an entity department is usually responsible for collecting, protecting, and sharing information, while distributed blockchain nodes can help departments verify the authenticity and originality of data during data transmission without relying on a third party, thereby ensuring the trustworthy relationship of data transmission. At the same time, blockchain can create a trusted audit trail of information that records in real time the location, usage, and visitors of the data, greatly increasing the transparency of data processing and processes, and preventing misuse or falsification of information in government environments for effective oversight. Blockchain improves service

efficiency and lowers information system operating costs. Blockchain uses smart contract to pre-determine data processing processes, which helps improve work efficiency in network data interaction. Its automated distributed structure can save data processing costs and reduce the operating burden, and improve the robustness of the system. Service data of each department does not need to be replicated to the central data exchange system in full redundancy mode. This reduces the workload of each department, protects data privacy between departments before a specific cross-department service occurs, and reduces the maintenance burden of the information service center on the central system. Blockchain enables information sharing and data privacy protection simultaneously. The blockchain is used to build a coalition of relevant departments. The trustworthiness of blockchain data is used to implement data sharing, and the privacy security is ensured by blockchain encryption, thereby implementing comprehensive data collection and separation of rights and duties. According to the system design mode, the administrator can develop a complex permission scheme to control who can access which types of information and which information can be shared by the multi-party system. That is, the government can authorize the access party and the access data independently to implement data encryption and controllability and real-time sharing.

Based on the advantages of blockchain technology, government data is shared and exchanged in a trusted manner based on the blockchain, implementing data ownership separation, promoting cross-department and cross-region sharing of government data, facilitating collaborative service processing, breaking up information barriers between different industries and regional regulatory agencies, and optimizing the service level of “maximum one run”. Use the data storage, consensus mechanism, and smart contract in the blockchain to build a transparent, reliable, efficient, and low-cost administrative supervision system, and build an intelligent mechanism for pre-emergency storage, data sharing, and linkage collaboration, thereby optimizing the administrative supervision, city management, and emergency assurance processes and improving governance efficiency. Blockchain is implemented in market supervision, administrative law enforcement, and audit scenarios to provide high-quality, efficient, and convenient mobile government services for enterprises and people.

7.2 Application Development

Currently, blockchain’s government services in countries around the world are mainly reflected in the realization of completely paperless digital government and the minimization of corruption. Blockchain in Digital Government, published by the European Commission Joint Research Center (JRC) in 2019 [5], argues that blockchain technology is not yet disruptive or transformative for the public sector, nor is it seeing new business models or new services. It mainly plays an efficiency improvement role based on the upgrade of record keeping technology, and will play a role in policy design, supervision, and interaction with the public. With the exception of Antarctica, government and public sectors on six continents on the planet have started blockchain

pilot projects. For example, the United States Department of Homeland Security, the United States Department of Health and Human Services and the United States Food and Drug Administration have applied blockchain technology to anti-counterfeiting. Georgia's application of blockchain technology to land title registration; Switzerland Applying blockchain technology to decentralised identity management; Estonia and Dubai apply blockchain technology to digital government construction; India applies blockchain technology to payments and land registration; Denmark applies blockchain technology to voting; Gibraltar applies blockchain technology to stock exchanges, etc.

Figure 7.1 shows the blockchain practice map in the government and public service fields. Currently, blockchain applications in the government service field focus on the following four directions:

1. Identification and Identity Management

Most government documents are easily forged. For example, many high school students in the United States have forged driver's licenses, which can be tampered with by age and bar access to places where minors are not allowed to enter. In many spy movies, there are often forged passports and impersonated people. Blockchain technology can help solve the problem of identity authentication errors. For example, ID2020 serves as a coalition of governments, NGOs and private institutions to help people identify themselves to access basic services such as health care and education. Both the Finnish government and the UN World Food Programme (UNWFP) have launched a blockchain program to provide digital status to refugees. In the United States, Austin, Texas, and the Bronx, New York, have also used blockchain to address the identity of homeless people, making it easier for them to access food pantry, shelters and banks.

2. Government Information Records

Other important information in government records is susceptible to tampering and falsification. For example, personal information (marriage, divorce marriage, death, passport, visa), land registration, deeds, property ownership, vehicle ownership, vehicle registration and company registration information. According to statistics, more than 50 million travel documents have been lost or stolen worldwide and are being sold to various countries or regions. Blockchain technology enables lost, tamper-prone paper documents to be replaced by digital documents on immutable books. For example, in Andhra Pradesh in India, blockchain systems are being used for land registration records and vehicle registrations to ensure authenticity and security of information and to promote operational efficiency across government departments.

3. Citizenship Services Management

The traditional government's "data island" and "data right" problem greatly reduces the efficiency of government service and citizens' satisfaction. The blockchain-based e-government system has been implemented from theory to solution, which can solve the current public concerns. Estonia, for example, has

























Blockchain Practice Map in Government and Public Services	
 <p>U.S. Department of State Moves Labor Contracts Up</p>	 <p>Illinois Establish Distributed ID DID</p>
 <p>Ernst & Young Assists the Vienna Government in Safely Disclosing Government Documents</p>	 <p>Estonian government initiates e-residency</p>
 <p>Foshan Chancheng Notary Office Store and Verify Notary Certificate</p> <ul style="list-style-type: none"> The Electronic Evidence Cloud of the Chinese Economic Balance Blockchain of the Crowdchain and the Alliance Chain Policy and Public Credit Chains Ordered by Guangzhou Development Zone 	 <p>Guizhou Municipal Government Performs Fingerprint Recording and Confirmation of Poverty Alleviation Objects</p> <ul style="list-style-type: none"> ID-Hub Assists Foshan Chancheng District to Realize IMI Identity
 <p>Ghana has digitally registered its land</p>	 <p>Trial Blockchain Registration of Land in Andhra Pradesh, India</p>
 <p>Georgia Chains Land Titles</p>	 <p>UK asks citizens to take advantage of GOVCOIN System Use Benefits</p>
 <p>Denmark chained data for all cars</p>	 <p>Vehicle Registration</p> <p>All information on the whole process of second-hand vehicle transaction is linked to facilitate tax collection by the tax department.</p>
 <p>Shenzhen Tax Bureau issues electronic invoice</p>	 <p>Electronic Invoice</p> <p>The invoice cannot be tampered with after being issued. The authenticity of the invoice can be confirmed by multiple parties.</p>
 <p>Voting in Russia</p>	 <p>West Virginia Citizens Vote in Mobile Voatz System</p>
 <p>The United Nations and the World Identity Network (WIN) register child information to prevent child trafficking and detect cases of trafficking.</p>	 <p>Prevention of human trafficking</p> <p>The child identity information and the status of being abducted are updated in real time on the blockchain, and the information is transparent and public.</p>
 <p>Evidence preventing and authorizing</p> <p>Files are not easily lost and file information is not tampered with.</p>	 <p>Land management</p> <p>Land information is chained, information cannot be tampered with and updated in real time, and government departments are informed in time.</p>
 <p>Resident Identity authorization</p> <p>Distributed storage of resident identity cards ensures identity information security, and multi-party verification ensures smooth subsequent business handling.</p>	 <p>Welfare Management</p> <p>The information is open and transparent, and cannot be changed to improve the credibility of the government.</p>
 <p>Voting and election</p> <p>Blockchain technology makes voting information transparent and unchangeable, preventing cheating.</p>	 <p>Wellness Management</p> <p>The information is open and transparent, and cannot be changed to improve the credibility of the government.</p>

Fig. 7.1 Blockchain practice map in government and public service

a portal that allows anyone to become an e-resident in about half an hour for 100 euros. Dubai will store all its government files on the blockchain by 2020, and 50% of its services will run on blockchain platform in 2021. These systems will simplify all government activities and are expected to save hundreds of millions of hours of work time.

4. Government Services

The government usually needs to carry out a series of activities, such as voting, taxation and so on. Given the security requirements of data storage and the devastating impact of hacking, few of these activities can be conducted online in most countries. Relevant government departments at home and abroad have carried out a series of blockchain application practices in the public service field. For example, Russia has started a pilot of blockchain technology in the electronic voting system, Estonia has launched an electronic residency pilot, and the United States has chained labor contracts to ensure the authenticity of contracts and timely dispute settlement.

7.3 Application Scenarios and Practices

As a new technology, blockchain creates new development opportunities for government service reform and innovation. Relying on technical forces, we can explore the application scenarios of systems and departments between governments, explore the existing industry issues, and help government services to increase the quality and efficiency of government services through blockchain.

7.3.1 Government Data Sharing

1. Solutions from Blockchain

By utilizing the technical features of the blockchain technology, such as multi-party consensus, anti-forgery, anti-tampering, and automatic execution, the level of government data sharing can be effectively improved, and information such as government data sharing, exchange, and use processes can be chained. Establish a secure sharing mechanism for encrypted transmission, authorized use, full-process traceability, and dynamic update of government data to form a trust system for government data sharing, eliminate data barriers between departments, and promote accurate data invocation and on-demand sharing between departments. Implements data scheduling across layers, regions, systems, departments, and services.

Government data sharing is an integrated solution based on blockchain technology and concepts, consisting of software and corresponding management

methods. The distributed storage ensures that the permission management directories viewed by government bureaus are reliable and reliable. Data can be shared and tracked. Modifications on any node can be synchronized to all nodes. The e-Government data permission management system is protected from tampering to ensure that the shared scope and interconnected systems cannot be independently modified. The e-Government data permission management system is controlled by consensus and smart contract, and services are changed under the coordination of multiple parties. This ensures that the data permission management directory is comprehensive and reliable. Smart contracts are used to solidify traditional big data exchange behaviors into software logic that runs automatically, and blockchains are used to share government data and drive shared exchange. All operation behaviors and access behaviors are recorded in the blockchain. Provide authentic and reliable data sources for subsequent business appraisal and data source tracing. On this basis, the e-Government data permission management chain drives probes for database detection, extraction, and interface encapsulation, which evolves the original large-scale data exchange to on-demand data extraction, and drives trusted data exchange (sandbox) on this basis. "Available or not available" for large-scale data modeling.

(1) Application value

There are some problems in government data sharing, such as data not being implemented, data exchange and data permission management system are disconnected, data sharing and openness are incomplete. To further improve data management efficiency, the blockchain concept is introduced to build an e-Government data sharing system, and the data permission management requirements of each department and key data are locked in the chain, implementing logical management and control of e-Government data.

- In data permission management, such as the "two skins" between the permission list and data, the change of the permission list, and the random authorization of data sharing are solved, and a set of "home base" of data and system is formed.
- From the level of city-level management, we reconstruct and upgrade the technical architecture of the shared exchange system through blockchain, solve the relationship between "agglomeration" and "pass" and realize the dynamic adjustment of "agglomeration" and "pass" in different historical periods.
- By means of directional opening, special zones opening, and full opening, the system will integrate with the expansion of the urban service industry to play the leading role of Big Data in promoting industry driving and improving service people's livelihood, thereby improving social benefits of Big Data.
- Through the technical system transformation, it is clear that the information systems that have not been deployed in the municipal government departments are not allowed to apply for O&M or upgrade and upgrade expenses, and promote the change of the new mode of government data.

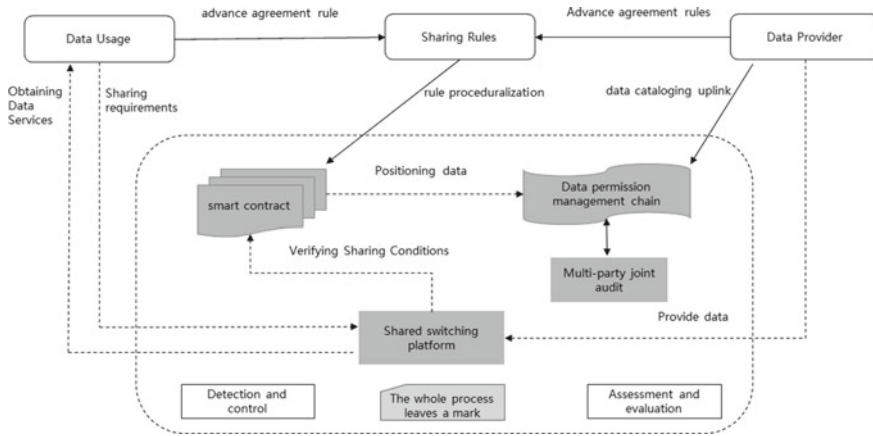


Fig. 7.2 Data permission management chain and data exchange architecture based on data sharing

(2) Application Idea

The application idea of the data permission management blockchain based on data sharing is as follows: The government department forms a complete and unique department data permission management platform, and the government agency platform provides a unified data permission management interface (registration, query, etc.) and management tool. Applications in government data sharing need to be based on the data permission management platform of the blockchain to ensure compatibility with the original system and facilitate quick deployment and application in new applications. Therefore, seamless connection between traditional systems and new systems can be effectively realized. Figure 7.2 shows the data permission management chain and data exchange architecture based on data sharing.

(3) Technical Concerns

First, focus on building end-to-end capabilities of blockchain with security as the core. To build alliance chains based on blockchains and centering on government services, performance requirements must be considered while security is first. Government data is the basis of all government service applications and the core of government resources. Therefore, data security must be fully ensured from the chain to application, and end-to-end security must be ensured. Byzantine Fault Tolerance(PBFT) algorithm can ensure the efficiency of the blockchain and the stability of the system in case of partial node failure. blockchain platform must ensure the security of smart contract, transaction, identity management and data encryption. On the network, optimize the P2P algorithm and transaction process to solve the requirements and impact on the network when a large number of nodes go online. In terms of hardware, a trusted blockchain environment combining software and hardware is built around Chinese hardware chips (such as Huawei Kunpeng) to support efficient consensus and secure data access, and

enhance the independent controllability of software and hardware as a technical guarantee for blockchain.

The other is to collect data through probe technology. Blockchain cannot implement large data transmission capabilities of the Internet. Therefore, a data exchange platform needs to be established for public cloud or hybrid cloud, and a data probe technology needs to be applied to the platform, so that applications and data integration can be completed by using the data probe. The data exchange platform implements service integration, data integration, device integration, and message integration, supports data, service, and resource collaboration, and implements data communication between government departments and between government departments and enterprises. By adding a probe platform to the data permission management chain, the data permission management chain triggers and manages probe operations. In this way, data can be opened in real time on the premise of data permission confirmation.

Third, the trusted data exchange (sandbox) technology can be used to streamline government data and enterprise data, helping more data and fewer personnel. The probe platform and sandbox technologies are added to the data permission management chain to implement the “available and unavailable” and “burning after reading” of data usage, and record operators, calculation forces, and data flow in real time to facilitate data source tracing.

2. Application Case: Beijing Government Data Management Catalog Blockchain Project

Beijing uses Huawei’s blockchain technology to link the responsibilities, directories, and data of 53 departments in Beijing to form a directory blockchain system, providing support for the aggregation and sharing of big data and optimizing the business environment in Beijing. The system went live nationwide in October 2019 and started the data sharing process based on directory blockchain.

By using directory blockchain to lock the sharing relationship between departments and the process chain, a new rule of data sharing is constructed, and the problems of random data flow and unordered business collaboration are solved. All data sharing and business collaboration activities are co-managed on the chain. Responsibility directories without data will be adjusted, and systems that are not linked will be shut down. A new closed loop of department business, data, and job fulfillment will be established.

Beijing uses the directory blockchain to explore “data zones” to promote socialized use of government data for data hotspots such as finance, healthcare, transportation, and education. For example, the sharing of the “construction land planning permit” and “construction project planning permit” by the Beijing Municipal Bureau of Water Affairs and Natural Resources Commission is automatically implemented under the control of the “directory blockchain”. The whole process can be completed in 10 min. In addition, by using the orderly data operation capability of each department in the city under the directory blockchain scheduling, the data on the chain can be trusted and shared, so that standard data interfaces such as household registration, population, and social

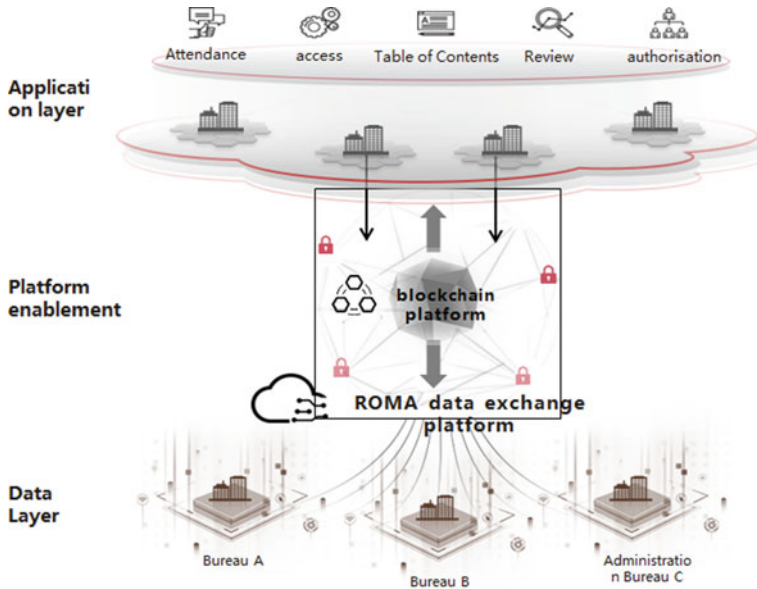


Fig. 7.3 Blockchain solutions

organizations of multiple departments such as public security and civil affairs can be invoked in real time, reducing materials, processes, and time.

The Beijing directory blockchain solution is shown in Fig. 7.3.

Advantages and innovations of the system include:

- Information resource cataloging system based on blockchain. Blockchain technology is used to build alliance chain solutions to solve a series of problems such as performance, resource consumption, and deployment in the information resource cataloging system. In addition, Chinese national cryptographic algorithm is added to ensure the security and effectiveness of data encryption based on government security requirements.
- Data probe technology based on ROMA platform. In the overall solution, the data probe is based on Huawei ROMA platform to integrate applications and data.
- Through trusted data exchange (sandbox) technology, data cleaning is realized, which not only ensures the privacy of original data, but also enlarges the data sharing and use scope of government and enterprise.

In the construction scheme, each unit shall update and improve according to the five-level catalog structure on the basis of the existing “home base” to form a complete and unique set of department catalogs. The municipal platform provides unified catalog management interfaces (registration, query, etc.) and cataloging tools. In this way, most units can directly use the existing basis such as catalog sorting, system integration, planning and archiving, and cloud migration. Some units that

have no basis (or have changed greatly) can use the new cataloging tool to directly extract the original catalog from the database as a preliminary “home base”.

In terms of promoting the application of information sharing, data that can be obtained through sharing cannot be collected by itself based on the requirements of relevant documents in Beijing. The directory blockchain system performs internal comparison and “blood relationship” analysis by collecting and sorting data structures from each business department, while the information management department needs to give prompts to users and information management departments to establish electronic protocols through the directory blockchain system. Business departments can sign agreements based on the sharing requirements on the directory to ensure the full utilization of the directory.

To ensure that the catalog is alive and well, technical capture methods and business sorting methods are used. The directory blockchain system automatically captures information such as user database or service system data structure, and provides users with an intuitive display through the system, helping users edit key elements such as Chinese names of information resource structures. The directory blockchain system also supports the import and export of standardized data dictionaries, which further provides a convenient technical means for users. Based on Beijing requirements, the catalog information is updated during the project approval and acceptance phases of the information system to ensure the real-time data.

In addition, Beijing has also established a big data catalog assessment and evaluation system to study and formulate assessment and evaluation quantitative indicators, so as to guide all departments in the city to carry out catalog sorting. At the same time, the appraisal results are incorporated into the city’s performance appraisal system.

7.3.2 *Electronic Certificate*

1. Solutions Provided by Blockchain

The process of preparing and issuing electronic certificates is that each commission bureau shall be responsible for the processing of the business within the scope of responsibility of the department and issue the electronic certificates at the same time [6]. As the manager and monitor, the large data center can read the electronic certificate data of each business department, but does not generate data. If a large data center synchronizes electronic certificates from other business departments in the centralized mode, data inconsistency may occur between the business department and the centralized department (large data center). In addition, the electronic certificate data collected by the large data center has no legal effect and can only be consulted for reference. It cannot support the functional certificate requirements for cross-department coordination of government affairs.

Through the blockchain technology, electronic license management is implemented, multiple electronic license registration is promoted, and high-frequency

government service matters are handled in combination with abundant authorization and license usage modes. This can help deepen the reform of “simplification” of government service matters, promote the electronic approval of application service matters, parallel approval of engineering projects, and online processing of tax matters. Speed up the realization of the goal of “one-network operation”. As shown in Fig. 7.4, the application of blockchain technology to electronic certificate data sharing provides the possibility for cross-region, cross-department, and cross-level data exchange and information sharing, which is conducive to establishing trust and consensus among the commissions and bureaus, and promoting cross-border sharing of government data while ensuring data security. In addition, the integration of government services has been improved, and the “data running” has been implemented instead of the “person running” service, thereby improving the people’s sense of access and satisfaction.

The difference between the blockchain electronic license and the traditional mode of sharing and exchanging electronic license of each government department lies in that: the blockchain electronic license is driven by transaction, while the shared photos or data are electronic license data of departments related to the event, not full data. The electronic certificate data shared in the blockchain mode is the most vivid and accurate data. It is the data generated by business departments during business processing. Data is shared immediately after being generated. Large data centers can build electronic certificate libraries based on the most “live” data on blockchain nodes [7], and the data in the electronic certificate libraries created in this way is real data that can be used by various commissions. Instead of collecting a bunch of unuseable data. For example, the e-Centres

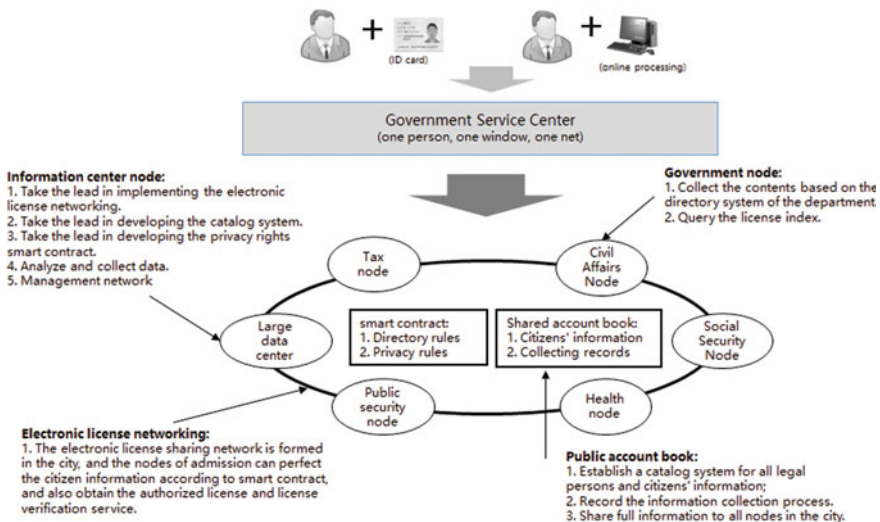


Fig. 7.4 Blockchain technology allows licenses to start, use, and finally

collected by the large data center can effectively support the handling of government affairs and the construction of the comprehensive population database and integrated legal entity database.

2. Application Case: X Digital Government Trusted Certificates Based on Blockchain

At present, the domestic electronic license management platform mainly relies on the third-party certification organization to set up a central database to store data, and uses a centralized database to complete the production, storage, information query, exchange and sharing of license. Data access and update rights belong to state organs, although the departments can share the rights. However, the information barrier and information exchange between different documents can not be effectively solved.

The Notice of the General Office of the State Council on Forwarding the Implementation Plan of the Pilot Implementation Plan of “Internet + Government Affairs Service” by the National Development and Reform Commission and other Departments (Guo Office F [2016] No. 23) [8] points out that the number of the resident ID card should be used as the unique identifier. The electronic certificate library is established. The electronic certificate is beneficial to realize the electronic closed-loop management and application of the whole network and the whole process, to prevent the proliferation of false certificate, to solve the difficult problem of identification, and to reduce the social cost and resource consumption. But in practice, the realization of electronic certificate needs to solve the following problems: First, ensure the authenticity of the source of electronic certificate; Second, ensure the confidentiality and integrity of electronic certificate data; Third, the issuing department of electronic license must be authoritative and reliable, so as to improve the legal effect of electronic license. Fourth, ensure the validity of the electronic license [9].

As shown in Fig. 7.5, the objective of the blockchain-based electronic license platform is to achieve unified storage, sharing, and management of electronic license by government departments through the blockchain technology, and to realize mutual recognition and interworking between different systems. At the same time, it can realize the unified supervision of civil electronic license, and realize the mutual recognition and communication between civil and government license. In terms of user experience, users can upload authentication information at one time and use it across regions and across departments for multiple times, allowing the public to check, verify, make, and use the authentication information anytime and anywhere. In addition, with the anti-tampering and traceability of blockchain account books, the risk of electronic certificate counterfeiting and information modification can be effectively avoided.

In the process of platform construction, according to the power list and responsibility list of government departments at all levels, the electronic certificate catalogue, standardization and electronic, forms the electronic certificate catalogue, thus establishing the electronic certificate. On this basis, the electronic license platform is

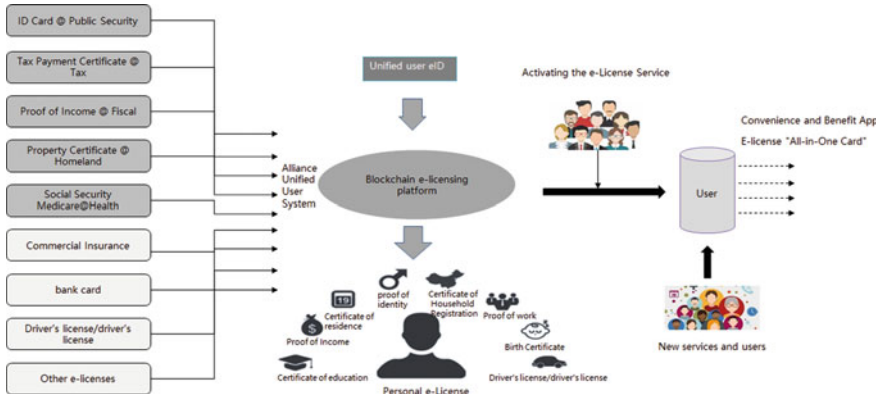


Fig. 7.5 Blockchain-based e-Crisure platform management

constructed according to the principle of combination of decentralized and centralized, so as to realize the multi-collection, sharing and multi-use of basic license information. In addition, it supports access and supervision of civil electronic certificates, mutual access of government electronic certificates and civil electronic certificates, and develops the application ecosystem of electronic certificates.

Through the construction of the platform, the entity registration and license chain will be realized finally [10]. The electronic certificate issued by the enterprise is reviewed by the issuing organization to generate the electronic certificate. On the basis of not affecting the original issuing business processing system of each department, the blockchain business node is superimposed, and the blockchain business node is deployed in each office equipment room and large data management center. The index data of electronic certificate is chained in real time, but the original data is not chained. It ensures the security of the original data and realizes the trusted sharing of certificate and photograph. You can check the photos on the mobile phone or PC App client. The check operation records are stored in the unified management center. For example, the app can be used to query device licenses, and the public security certificates of the public security department and the social security certificate of the people's social security department, and the big data center blockchain service node can be used to query open data of the public security department and the people's social security department. The person who inquires should provide the true identity card, and the public security department shall verify the identity card.

References

1. Hu C. A Breakthrough in promoting the integration of E-government in the Yangtze River Delta. Learning Times, 22 June 2020 (007).

2. He L. The framework of the national integrated government service platform is initially formed. *China Credit*. 2020;6:49.
3. Cui J, Lv Y, Wang H. The development of digital identity based on blockchain. *Cyberspace Secur*. 2020;11(6):25–9.
4. Liu L. Continuously improve the level of digital governance. *China Electronic News*, 24 July 2020 (004).
5. Joint Research Centre of European Commission. *Blockchain for digital government: An assessment of pioneering implementations in public services*. Luxembourg: Publications Office of the European Union, 2019.
6. Haoliang W, Yuzhong L, Lili W. Research and implementation of blockchain technology for electronic certificate sharing. *Comput Eng*. 2020;46(8):277–83.
7. Hongbo Z. Blockchain-based E-government big data security sharing analysis. *Inform Technol Inform*. 2020;6:234–6.
8. Notice of the General Office of the State Council on Transmitting the Implementation Plan for the Pilot Implementation of “Internet + Government Services” by the National Development and Reform Commission [EB/OL]. 23 April 2016. http://www.gov.cn/zhengce/content/2016-04/26/content_5068058.htm
9. Xiaole C. *Electronic data storage system based on blockchain technology*. Nanjing: Nanjing University of Posts and Telecommunications; 2019.
10. Dingfang J. Application of blockchain technology in “Digital Government.” *China Econ Trade Guide* (Chinese). 2020;3:6–7.

Chapter 8

Blockchain and Culture Education



Yinfeng Chen, Yaofei Wang, Yu Guo, Haodi Wang, Rongfang Bie, and Peter Thomas

Abstract With the rapid development of Internet technology, the content of cultural education is rapidly transferred from offline to online. The transformation solves the problem of time and space limitation, yet brings new challenges such as digital copyright protection, quality certification of curriculum resources, education evaluation and certification, personalized learning services, and education quality supervision. The emergence of blockchain technology provides strong support to solve the above challenges in cultural education. This chapter focuses on the solutions based on blockchain for copyright deposit, transaction, and value evaluation, as well as education certification, learning incentive and credit cashing modes, and the subject-object evaluation model for online education and learning. Three application scenarios and application cases are tackled, including educational authentication and certificate management, multiple evaluations for online learning, copyright certificate storage and trading, and knowledge securitization. The discussion and research in this chapter could be referenced for further development of blockchain in cultural education.

Keywords Culture education · Evaluation and certification · Copyright protection · Knowledge securitization

With the development of the Internet, especially the mobile Internet, digital publishing in the field of culture has formed a complete industrial chain through which writers can obtain income. However, at present, digital copyright is not well protected. The emergence of blockchain technology brings an opportunity to protect digital copyright.

Education is essential to social development and the cradle of young talents and scientific productivity. In the era of network information and big data, the field of education is constantly applying advanced technologies while inheriting advanced

Y. Chen · Y. Wang · Y. Guo · H. Wang · R. Bie (✉)
Beijing Normal University, Beijing, China
e-mail: rfbie@bnu.edu.cn

P. Thomas
RMIT University, Melbourne, Australia

knowledge and ideas. Information reform has happened in educational equipment, model, system, environment and resources, setting off a wave of educational digitalization. At the same time, it provides an opportunity for the application and development of blockchain technology in education. Although the application of blockchain technology in the field of culture and education is still in its infancy, it has great potential.

8.1 Overview

People's consumption has gradually changed from focusing on material consumption to spiritual and cultural consumption. Over the past decade, China's cultural industry has maintained steady and rapid growth, the structure of the cultural industry has been continuously optimized, and the development momentum of new cultural formats has been strong.

In August 2019, the Ministry of Science and Technology and other six departments jointly issued *The Guiding Opinions on Promoting The Deep Integration of Culture and Science and Technology* [1], which puts forward key development goals such as "strengthening the research and development of key technologies with cultural commonality, improving the construction of cultural science and technology innovation system, accelerating the industrialization and promotion of cultural scientific and technological achievements, promoting the modernization of content production and communication means, and strengthening the construction of cultural big data system". These goals are inseparable from the participation of blockchain technology.

In the field of education, the development of online education has promoted the development and reform of the education system. The online education model represented by MOOCs and micro-courses has fundamentally changed the form of education, curriculum resources, teaching interaction, learning evaluation, and quality certification. Online education has begun to profoundly change teaching and is recognized by colleges and universities so that hybrid learning mode has become one of the development trends in the future.

In the light of the impact of the COVID-19 epidemic on normal school opening and classroom teaching, the Office of the Leading Group of the Ministry of Education for Dealing with the Pneumonia Epidemic in novel coronavirus issued *The Guiding Opinions on Doing a Good Job in Online Teaching Organization and Management in Colleges and Universities during The Epidemic Prevention and Control Period* on February 5th, 2020 [2], that proposed to actively carry out online teaching activities, relying on online course platforms to ensure the progress and quality of teaching during epidemic prevention and control, and realizes "classes suspended but learning continues".

In May 2020, the Ministry of Education issued *The Action Plan for Blockchain TechnolInnovationtion in Colleges and Universities* [3], which put forward the action goal of building several blockchain technology innovation bases in colleges and universities by 2025 and cultivating and gathering several blockchain technology

breakthrough teams. The document defines the construction direction of the following two industry application platforms.

- *Blockchain and education governance.* Educational innovation and development, such as crowdfunding and crowd creation and sharing of digital education resources, digitalization of teaching behavior, and refinement of educational management decisions, have brought a series of challenges such as confirmation of copyright and guaranteeing privacy. The document aims to build an educational governance and application innovation platform based on blockchain, support the research and development and application of innovative technologies in the field of education, such as the construction of intelligent digital resource sharing platforms, the protection and traceability of innovative intellectual property rights, authentic and reliable digital archive storage and tracking, sensitive information flow control and privacy protection, lifelong learning based on credit bank and other innovative technologies in the field of education, research on the application of blockchain key technologies facing the needs of the field of education, and improvements to independent, open and controllable Chinese educational governance.
- *Blockchain and intellectual property.* Facing the needs and problems of blockchain application in the field of intellectual property, the document aims to build a technological innovation application platform for blockchain-based intellectual property management and services, support the research on the innovative application of blockchain in the fields of intellectual property service, management, protection, transaction and justice, and support the research on the application of blockchain key technologies facing the needs of intellectual property right confirmation, traceability, and transaction, and improve the level of intellectual property protection and market transformation in China. In addition, the document also points out that it is necessary to support colleges and universities to strengthen regional cooperation, promote the transfer and transformation of blockchain technology breakthroughs to education, intellectual property, and other fields, and strengthen the application research of blockchain in the field of digital rights management and the research and application of education management and service collaboration platform based on blockchain in the demonstration and application of blockchain technology.

Since the reform and opening up, the network has brought a lot of convenience to people's lives. Cultural education in China is being rapidly transferred from offline to online, and people are constantly adapting to the production and dissemination of online knowledge content, which brings new challenges.

8.1.1 Digital Copyright Protection

Digital cultural and educational content such as movies, literature, music, animations, and video tutorials means that production, reproduction, circulation, and dissemination of these contents are all completed through the Internet. While the Internet has improved the transmission efficiency in the field of culture and education, it also faces the challenges of developing various piracy technologies and rampant piracy. The replicability of digital cultural content directly leads to the shrinkage of copyright value, which means that much excellent work is unable to maximize its value through copyright trading, which in turn affects the healthy development of cultural and creative industries. At the same time, a large amount of pirated content can harbor false advertisements and viruses, which means a poor experience for consumers and creates a vicious circle in the copyright market. The infringement of intellectual property rights is a serious problem, copyright disputes are frequent, and there are problems in the fight against piracy, such as the difficulty of proof and the high cost of rights protection, which has become a pain point for culture and education.

8.1.2 Dynamic Quality Certification of Curriculum Resources

In the era of ‘Internet plus,’ knowledge is no longer static but constantly evolving and developing, allowing dynamic co-construction and sharing. Therefore, knowledge production is a collaboration process characterized by networking, personalization, fragmentation, and multi-modality [4]. Educational resources should not stay at the level of simple knowledge but promote the occurrence of deep learning, and resources generated by groups are valuable sources of online curriculum resources. Regarding curriculum quality certification, the US QM has formulated six editions of online curriculum evaluation standards for higher education [5]. China has also made some recommendations for the selection of national online courses. Still, so, for, there is no unified and authoritative quality assurance mechanism or third-party organization evaluation in online education to guarantee the quality of educational resources and services [6]. How to ensure the effectiveness, high quality, shareability, and protection of all kinds of resources, and establish the quality certification mechanism of resources’ access, release, audit, certification, sharing, aggregation, copyright, and transaction, are all problems that must be considered in the field of education.

8.1.3 Educational Evaluation and Certification Issues

1. The Plurality of Online Learning Evaluation

The educational evaluation system is based on formal learning in schools, and the evaluation is based on the examination results. The evaluation of learning

is one-sided. For online learning, a free and informal learning method, it is necessary to comprehensively evaluate students by combining multiple factors of formal learning (online viewing of course videos, tests, exams, etc.) and informal learning (online information searching and reading, discussion and communication, posting and sharing, etc.). However, considering multiple factors also imposes an administrative burden on educators. Managing and evaluating learners' academic performance fairly and intelligently is a key issue for online education management.

2. *The Nonconformity of Evaluation Standards*

On the one hand, there is a lack of standards between informal learning outcomes of online education platforms and formal learning outcomes of school education. On the other hand, there is a lack of uniformity in the evaluation methods of learning outcomes among various online education platforms. All of these lead to the fact that the learning achievements obtained through online education can't be substantially recognized, and it is difficult to get recognized credits, academic qualifications, or other educational achievements.

3. *The Risks of e-Certs for Online Courses*

The storage of certificates is not sufficiently safe, which leads to the proliferation of electronic certificate fraud and reduces the credibility of electronic certificates. For e-certificates of online courses, third-party organizations lack credible public verification channels, so the verification of certificates depends on license issuing agencies, which leads to high verification costs and low efficiency.

8.1.4 Individualized Learning Service and Support

In addition to high-quality online course resources and effective evaluation and certification system, how to assist learners in completing online learning is an important issue in online education. Setting up a special teaching and learning service support department is a common strategy that can help teachers and students solve problems in the online teaching process. How to provide personalized support services according to learning characteristics and learning behaviors is also a research hotspot in education.

8.1.5 Multi-subject Participation in Educational Management and Supervision

Inside a school, online education is no longer the management responsibility of a single department but involves many departments and institutions. Outside of school, through cooperation with other schools, educational institutions, and online education service providers, the scope of online education management subjects from

outside the school has also been expanded. Therefore, the campus has become a community of online education management and supervision, and how to ensure effective management and supervision with multi-participation is a challenge for online education.

8.2 Solutions Based on Blockchain

Given the above problems in cultural education, blockchain technology can provide a solution with lower costs and higher efficiency.

8.2.1 Blockchain Solution of Copyright Deposit, Transaction, and Value Evaluation

Piracy in the field of cultural education can be solved through the supply chain approach based on blockchain technology, which can be applied to various fields such as content production, content dissemination, content trading, and content rights protection in the field of cultural education, as shown in Fig. 8.1.

Blockchain technology can enable creators to effectively confirm the content in the process of content creation, especially for tracking, confirming, and auditing the data of co-created works. In content dissemination, the credible dissemination of content can be ensured through the research on incentive mechanisms to avoid data tampering caused by a centralized system. In content trading, creators can realize the openness and transparency of licensing, trading, and other processes through the blockchain platform and get paid directly by publishing, promoting, or trading works based on the blockchain platform. For content rights protection, using blockchain distributed data storage, cryptography, and other technologies to sign the transaction data and then upload it digitally, means that it can provide an evidence chain through smart contracts so that the data can be directly used as notarized, authentic and legal evidence.

1. Copyright Deposit Certificates

Applying blockchain technology to intellectual property rights will contribute to the protection and trading of intellectual property rights. Blockchain technology

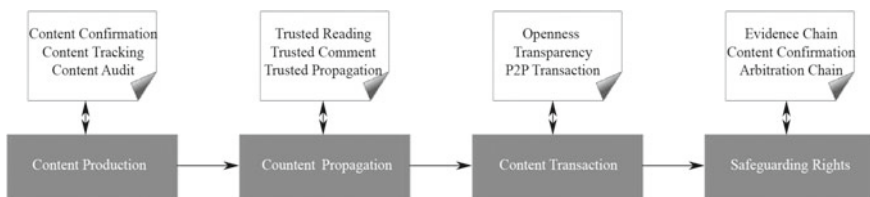


Fig. 8.1 Blockchain application in copyright protection

time stamps every data record, and data records are highly reliable and not easy to be tampered with. Therefore, we can build a “distributed account book of knowledge achievements” that is authentic in time and content, traceable and anti-counterfeit, and provides evidence for intellectual property rights determination and legal rights protection, so that blockchain technology can play an important role in the generation and confirmation of intellectual property rights.

In the application of intellectual property protection, an asymmetric encryption algorithm can be used to sign the knowledge results in the blockchain digitally, and the certified blocks of knowledge results can be generated and recorded in the blockchain to achieve the goals of secure storage of knowledge results, tamper-proof and disintermediation and independent verification. When implementing this function, the following three requirements should be met in setting user rights for different roles.

- **Owner privileges of knowledge achievements:** The owner of knowledge achievements has the right to upload his knowledge achievements to initiate certification applications, digitally sign his own certified knowledge achievements blocks using private keys, and share the address of his certified knowledge achievements blocks and personal public keys with other nodes. The owner should not be able to certify knowledge achievements and the accounting rights of his knowledge achievements block.
- **Permissions of the Certification Authority for Knowledge Achievements:** The Certification Authority for Knowledge Achievements has the right to use the private key to authenticate any knowledge achievement that applies for certification by digital signature (or directly issue the certificate for the knowledge achievement that the private key of the institution has digitally signed). It may have the right to account for the blocks of knowledge achievements signed and certified by the Institute (of course, the request can also be determined by competition through different consensus mechanisms). To ensure the owner’s ownership of the knowledge achievements, the certification authority should not have the authority to transfer any block information. The public key of the knowledge achievement certification authority is publicly available throughout the system.
- **Third-party user/institution privileges:** Third-party users/institutions (such as employers, other node users or institutions in the system, etc.) that are not part of the first two categories of users should not have the privilege to write chain and transfer block information. They only have the rights to receive the block information sent by the owner of the knowledge achievement, access the blockchain, and use the public key of the owner of the knowledge achievement and the corresponding certification authority public key to verify the ownership of the knowledge achievement and the authenticity of the knowledge achievement.

The process of storage and validation of knowledge achievement certification based on the blockchain is shown in Fig. 8.2.

The specific solutions are as follows.

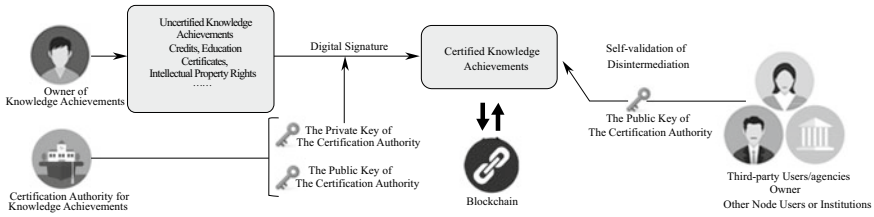


Fig. 8.2 Authentication, storage, and verification process of knowledge achievements based on blockchain

- **Upload or generate the knowledge achievements:** The owner of knowledge achievements uploads his achievements not certified by the institution in the blockchain system and sends the certification authority for knowledge achievements to request the certification. If the certification authority issues the certificate of knowledge achievements, the owner of the knowledge achievements sends the certification request directly to the certification authority. After the certification authority receives the request and confirms the applicant's qualification, the certification of knowledge achievements is generated instantly.
- **Certificate Authority Digital Signature:** A certificate authority has a fixed pair of public and private keys that are public to the public. Use the private key to encrypt and complete the certification of digital signatures for checking the correct knowledge achievements or the certificates of knowledge achievements generated by this institution.
- **Certified Knowledge Achievements Up-Chain Storage:** The blocks generated by the accredited knowledge achievements are recorded in the blockchain by the authority with signature certification. Before a block is directly recorded in the blockchain, the owner of the knowledge achievement can double-sign it using his private key to ensure that others cannot steal the knowledge achievements.
- **Third-party autonomous validation of knowledge achievements:** According to the block address sent by the owner of the knowledge achievements, third-party users or institutions can access the corresponding knowledge achievements blocks in the blockchain and use the public key of the publicly obtained certification authority to decrypt the knowledge achievements to complete the independent validation of the authenticity of the knowledge achievements. If a block has been double signed by the owner of the knowledge achievement, the owner of the knowledge achievement needs to send the address of the block to a third-party user or institution and a personal public key at the same time so that the third party can verify whether the owner of the knowledge achievement is himself first by using the decryption of the personal public key.

2. Solutions to Copyright Transactions

Figure 8.3 shows that two categories of copyright transactions are recorded using blockchain technology.

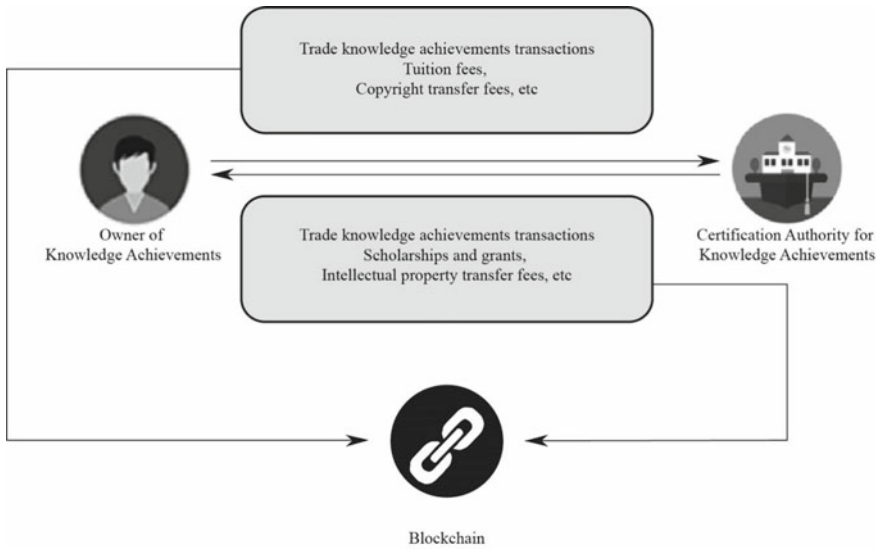


Fig. 8.3 Blockchain-based copyright trading of knowledge achievements

- Actual transaction records of knowledge achievements: In the process of actual transaction of knowledge achievements, the owner of knowledge achievements may pay tuition fees, copyright transfer fees, and other fees to the knowledge achievements certification institution, while the knowledge achievements certification institution may also issue grants to the owners of knowledge achievements, prices for the transfer of intellectual property rights, transaction income of copyright certificated works, etc. In this process, the actual transaction data between the two parties can be recorded using blockchains as safe and reliable transaction vouchers.
- Reward records in the form of knowledge assets: Certificate institutions can independently grant users rewards in the form of knowledge content coupons, knowledge achievements transaction vouchers, etc. by deploying smart contracts on the blockchain and writing a set of reward rules in the form of knowledge assets, and also recording the reward distribution as transaction information. Take the online original literary community based on blockchains as an example. After the academic creators upload their original literary works, such as novels and collections, to the blockchain system of literary works in the community and complete the copyright confirmation, the authors can collect the reader’s purchase fees for the e-books in the community platform. In this process, profit records of copyright transactions of works can be stored openly and transparently in the blockchain system of literary works to prevent third parties such as community platforms from using their intermediary identities to fake profit data and embezzle rebates. Readers can get e-book coupons for their use through reading, learning, benign discussions, and even publishing literary creations in the community. The

voucher is not redeemable or transferable, and its issuance will also be recorded as transaction information in the literary works blockchain system.

3. Solutions for the Digital Copyright Value Evaluation

Digital copyright is the right to disseminate content through emerging digital media, including producing and distributing all sorts of copyrights such as e-books, e-magazines, and mobile publications [7]. With the advancement of global information technology and the continuous extension of information technology to various fields, the digital publishing industry has a substantial development momentum. It has increasingly become the frontier of the publishing industry reform in China.

Copyright is an essential intangible asset of an enterprise. Evaluation of the copyright owned by an enterprise can significantly promote the development of the copyright industry and the asset evaluation industry. However, in our country's intangible assets value evaluation field, the copyright value evaluation is a blank state [8]. Using blockchain technology, we can realize the independent value evaluation of digital copyright, eliminate the unfair influence caused by human intervention in valuation, make the evaluation process open and transparent, and provide new ideas for evaluating digital works and copyright value.

In the above scenarios, whether it is to use blockchain technology to complete online learning evaluation and credit accumulation or evaluate the value of digital works or copyright, it can be summarized as blockchain to assess specific knowledge content. Smart contracts are the primary reliance on the blockchain to achieve an independent evaluation of the value of knowledge content.

There are three advantages to using smart contracts to evaluate the value of knowledge content.

- *De-intermediation and autonomous operation.* Managers write smart contract contents and set evaluation rules in the blockchain system initially. The system runs autonomously after the completion of the writing, without the need for managers to continue the artificial intervention in the evaluation process, which will save the workforce needed for system management. At the same time, the evaluation process without human intervention further ensures the fairness of knowledge content value evaluation.
- *User privacy protection.* Users do not need accurate identity information such as real names when they receive knowledge or create knowledge content in the blockchain system. They only need to log on to their accounts anonymously for learning or authoring activities, which will protect their privacies. Relevant data of knowledge content will be recorded in a personal history, periodically packaged and triggered to evaluate the value of the smart contract, settled into the corresponding value of the knowledge results, and the resulting knowledge results block will be digitally signed by the account to determine the ownership of the results.

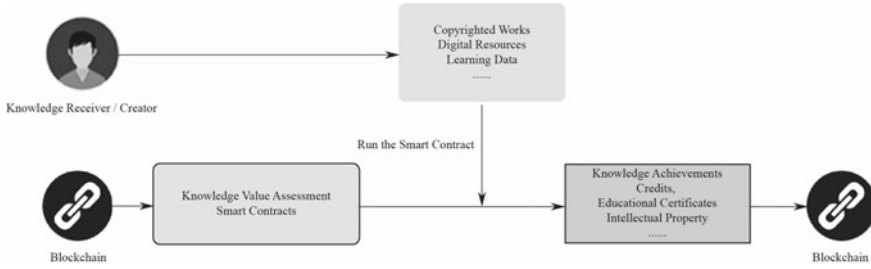


Fig. 8.4 Value evaluation of knowledge content based on blockchain

- *Secure storage of knowledge achievements throughout the life cycle.* After the smart contract generates the blocks of knowledge achievements, they are permanently stored through the network consensus chain. The consensus and encryption mechanism of the blockchain will ensure that the knowledge achievements cannot be tampered with and ensure authenticity and security.

The value assessment of knowledge content based on blockchains is shown in Fig. 8.4.

8.2.2 Educational Certification, Learning Incentive, and Credit Exchange Model

1. Digital Badge Electronic Certification Issuance and Verification Mode

Electronic certificates are gradually replacing the traditional paper certificate system because of their easy storage and forwarding. They are becoming an emerging mode of education certification, one of which is the digital badge.

A digital badge is an electronic badge that has evolved with the development of information technology [9]. It can also be translated as an open badge. The Mozilla Open Emblem website [10] defines the Open Emblem as a “new standard for identifying and validating learning (results) online.” Liu Dongying et al. [11] believe that the digital badge is a digital evaluation tool used to evaluate and characterize learners’ knowledge, skills, abilities, and interests and show their achievements to the public through the network.

A digital badge is an image [12] that uses metadata to accomplish a pre-specified goal and acquire a digital symbol. As a graphical indicator of learning activities and a way to certify learning results, digital badges are primarily used in informal learning situations. They can certify learners’ achievement skills online or provide proof of quality work and learning. They can provide corresponding solutions for Distributed Learning Certification in education [13].

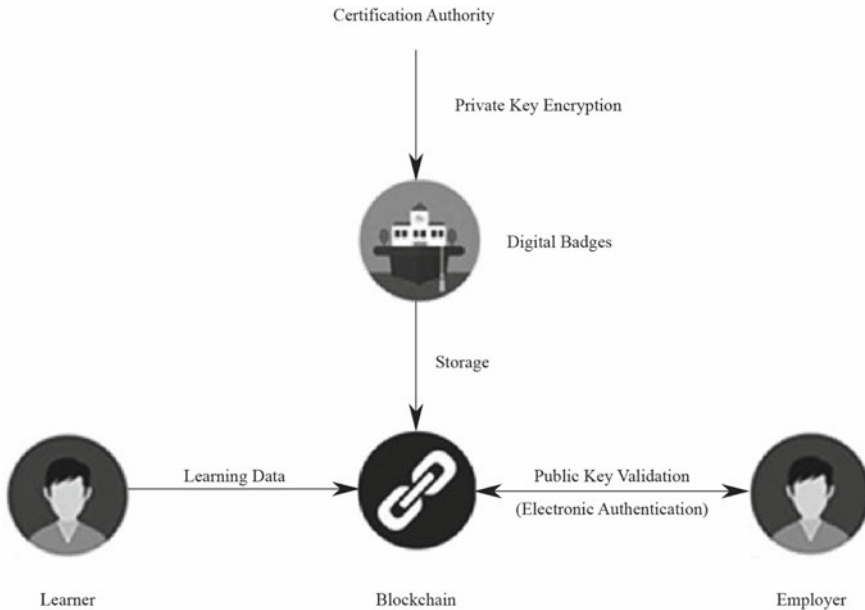


Fig. 8.5 Education authentication based on blockchain

As shown in Fig. 8.5, the combination of the blockchain system and the digital badge can help the badge avoid verifying the work of third-party organizations, establish time-saving and effort-saving peer-to-peer operations, and make up for the security vulnerability of the digital badge by tampering-proof based on maintaining its openness and distributed storage.

Applying the features of blockchain technology, public key and private key to digital badges makes the display of digital badges both public and confidential. Learners use the public key function when presenting their learning results and skills to employers. When an employer is interested in the learner's skills, they will establish a connection with the learner. By opening the learner's learning profile with a private key, the employer can obtain information about the learner's learning trajectory and learning process, verifying the learner's results' authenticity without a third-party entity's intervention.

2. Tuition Payment and Grant Distribution

Blockchain technology plays a role in encrypting currency by securely recording transaction information. It can also be migrated to record educational-related transactions such as tuition payments, grants, etc., to make the flow of educational funds more open and transparent. The University of Nicosia allows students to use the Bitcoin system to pay for their tuition and record their tuition transactions using the Bitcoin blockchain.

Figure 8.6 shows that educational aid can be allocated and distributed to students or educational institutions through blockchains as incentives to award grants and “knowledge credits.” In this scenario, the government (or sponsor) distributes educational funds fairly and autonomously to students or educational institutions based on specific performance criteria, such as performance, in the form of “knowledge credits” in the blockchain system. Many countries (as well as private sponsors) provide tuition support to students in poor areas by providing “knowledge credits” to “top achievers” in educational institutions or pre-approved lists of educational organizations. This *knowledge integral* system is an increasingly popular method of educational aid because it provides free education for students but still allows institutions to compete with each other to provide better support for students.

3. Credit Exchange Mode

Online learning is also an effective way to encourage non-school students to learn independently, promote lifelong learning and build a learning society. However, for this kind of free and informal learning method, managing and evaluating learners’ academic performance is a key issue for education managers.

Taking from the early western credit system, the management concept of a “school credit bank” was put forward. School credit bank [14] draws lessons from how banks work so students can freely choose learning content, time, and place. Learners can accumulate credits through online free learning. A bank is a credit institution

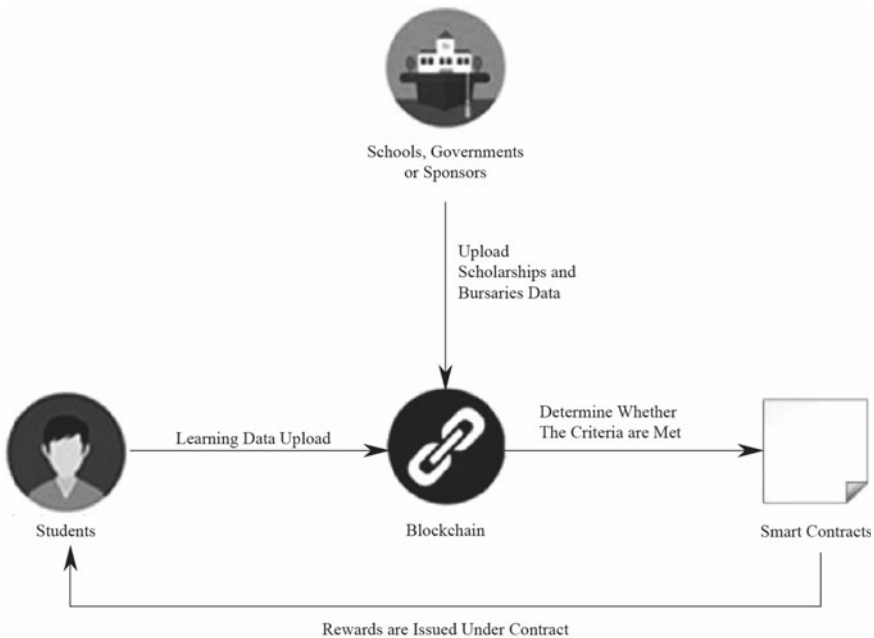


Fig. 8.6 Blockchain-based learning incentive

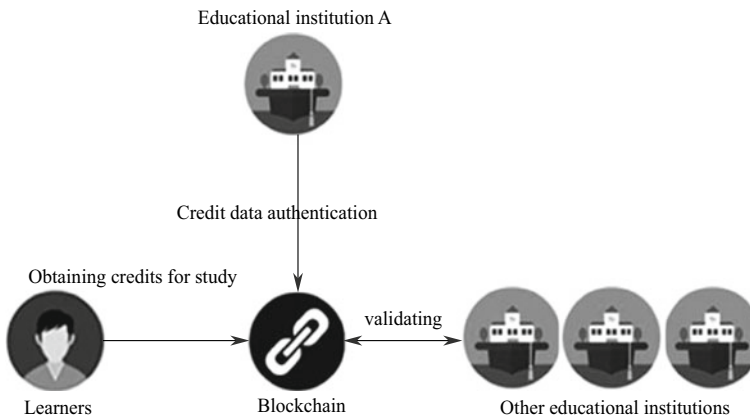


Fig. 8.7 Credit exchange based on blockchain

that undertakes the function of a credit intermediary. It usually has the functions of deposit, loan, exchange, and so on. From the definition, a school credit bank has the basic functions of the bank, such as storage function and exchange function. However, the difference between the school credit bank and the actual bank is that the school credit bank replaces the storage currency with the store credit and replaces the currency exchange with the credit exchange degree or qualification certificate.

As shown in Fig. 8.7, the school credit bank can allow sharing of teaching resources and credit exchanging among educational institutions and become a unified credit certification platform for academic education and non-academic education, formal learning, and informal learning.

Similar to the cryptocurrency based on blockchain technology, which can be issued and operated without the bank as a credit intermediary, blockchain technology can also be used in the disintermediation evaluation and storage of online learning credits, build a distrusted blockchain system, replace the intermediary management function of credit bank and retain the original management advantages of credit bank. It can make online learning evaluation more open, transparent, efficient, and credible.

8.2.3 Subject and Object Evaluation Model of Online Education Learning

From a subjective and objective point of view, the online education management system based on blockchain integrates the qualitative and quantitative evaluation of multiple evaluation subjects and objects and automatically realizes the evaluation of students' learning performance and teachers' teaching performance, as shown in Fig. 8.8.

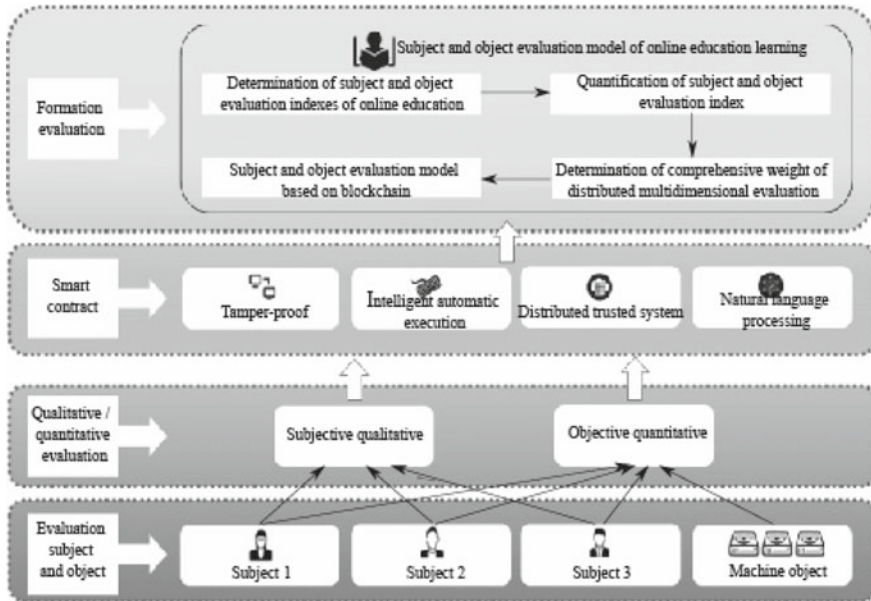


Fig. 8.8 Subject and object evaluation model based on blockchain

The subject and object evaluation model of online education learning is based on smart contracts. It constructs a distributed evaluation model and forms a trusted evaluation system.

Specifically, the subject and object evaluation process of online education learning includes four parts: determination of subject and object evaluation indicators of online education, quantification of subject and object evaluation indicators, determination of the comprehensive weight of distributed multi-dimensional evaluation, and subject and object evaluation model based on blockchain.

8.3 Application Scenarios and Practices

8.3.1 Educational Certification and Certificate Management

The falsification of educational certificates means that the current learning certification system has been criticized. Therefore, the creation of an educational certification system and educational certificate management system based on blockchain technology will help learners or other talents in different educational institutions, different workplaces, and different countries can safely, truly, conveniently, and efficiently store and use their blockchain learning certification to facilitate cross-institutional and cross-regional learning and employment [15].

An education certificate management system based on blockchain technology has high security and reliability. In such a system, a digital education certificate containing the basic information of relevant students can be created, and the certificate can be digitally signed with the private key of relevant students to ensure the consistency of user information and certificate content. Schools and other educational institutions use their private keys to sign a digital certificate with complete information records and store its hash value in the blockchain. The smart contract triggers the multi-signature verification during each issuance and query. The created hash value and the corresponding public key decryption can verify whether the certificate content has been tampered with.

In addition, learners often verify the authenticity of educational qualification information such as academic information and reward and punishment information in the process of entering a higher school and applying for a job. In practice, there are some problems, such as complex verification procedures of academic certificates, difficulties in proving the authenticity of award-winning certificates, and difficulty verifying relevant educational qualifications. Confirming these records costs a lot of manpower and resources and certification fees. The application of blockchain technology in degree certificates can completely change the verification and sharing mechanism for educational qualification information.

Using blockchain technology-based education certification and digital certificate management systems, employers and schools can verify educational qualifications more efficiently and at a lower cost. In addition, blockchain technology allows users to directly verify the validity of certificates using the blockchain verification tool without contacting the organization that initially issued the certificates. Therefore, learners no longer need to pay fees to the certification authority to identify achievements and prepare for employment. Employers can verify the authenticity of certificates without relying on the certification authority. This will greatly reduce the cost of further education, job hunting, and talent employment.

2. Application Cases

(1) *University of Nicosia and the Open University.*

University of Nicosia (UNIC) is committed to maximizing the potential of blockchain in education. It is reported that UNIC is the first university to realize the following four blockchain technology-related activities:

- In October 2013, bitcoin could be used to pay the tuition of any degree course at the University of Nicosia.
- In January 2014, the university course on cryptocurrency entitled “Introduction to digital currency” was first released in MOOC.
- In March 2014, the publicly recognized master of Science degree was provided for the digital currency course taught in online English (the first batch of students graduated in June 2016).
- In September 2014, students were awarded degree certificates using their internal software platform based on bitcoin blockchain technology.

The knowledge Media Institute (KMI) of the Open University (OU) has also participated in research projects on the blockchain. In the context of blockchain research and certification, KMI hopes to improve the security standards of digital badges, certificates and honors issued online by using blockchain as a trusted distributed account book.

(2) *Sony Global Education* [15]

Sony Global Education announced the construction of a global learning and certification platform based on blockchain technology to encourage learners, schools, and employers to share data on the learning process and learning certification. Its founder, Isozu, believes blockchain technology can give learners greater autonomy in managing their scores. For example, after a learner obtains an examination score, he can ask the examination provider to share his score with a third-party organization. Then third-party organizations can apply blockchain technology to evaluate the learner's score. To determine whether their knowledge and skills meet the needs of the organization. In addition, based on the potential and value judgment of blockchain technology in education and teaching, Sony Global Education is committed to promoting universities and other educational institutions worldwide to explore and use its blockchain technology platform.

The platform provides various applications and integrates various learning elements, breaking through some of the limitations of the existing curriculum. It brings a new educational experience to people of all ages and different social backgrounds worldwide and provides certifiable educational experiences and learning certificates. It allows learners' transcripts to be safely stored in the cloud server forever. Learners, teachers, or educational institutions can safely share these data with third parties. Isozu explained this application case: for example, a student who studied in an educational institution in China, participated in the online examination of an institution in the United States, finally graduated from a university in Japan, and now wants to apply for a graduate student in Spain. How should the school confirm the results from different educational institutions and process the student's application? Different assessment agencies may use students' test results in different ways. As the field of education becomes more and more international, it will be convenient for students and schools to share learning data and learning certification conveniently and safely for learners, educational institutions, and employers.

(3) *MIT Media Lab* [15, 16]

MIT Media Lab has developed a learning certificate platform using blockchain technology. The working principle of certificate issuance is as follows. Firstly, use blockchain and strong encryption to create a certification infrastructure that can control complete reward and achievement records, including digital files containing basic information of certificates, such as recipient name, issuer name, issuance date, etc. Secondly, the private key is used to encrypt and sign the certificate. Thirdly, create a hash value to verify whether the certificate content has been tampered with. Finally, use the private key again to create a record on the bitcoin blockchain to prove

who the certificate was issued at a certain time. In practical application, although the above work can be completed by one key operation, the platform is still improving due to a series of privacy problems caused by the transparency of the blockchain itself.

(4) *Holberton School of Software Engineering* [17, 18]

Founded in March 2015, Holberton School of Software Engineering is the first school worldwide to use blockchain technology to record academic information. It has shared academic certificate information on the blockchain since 2017, which has been appreciated by many recruitment companies. Sylvain kalache, co-founder of Hoberton School, believes that using the blockchain decentralized, verifiable, and tamper-proof storage system to store academic certificates in the blockchain database can ensure the authenticity of academic certificates and diplomas make academic verification more effective, safe, and straightforward. At the same time, it can save the time and labor cost of manually issuing certificates and reviewing academic materials, as well as the cost of building an operation database, which will become a perfect solution to the fraud of academic diplomas and certificates. In addition, some countries have also begun to take action. For example, the Kenyan government is strongly aware of the serious impact of academic fraud on national education and even the social economy. To severely crack down on the illegal act of counterfeiting diplomas, it is currently working closely with IBM to establish a blockchain-based academic certificate network publishing and management platform. For all schools and training institutions, it can publish academic certificates on the blockchain network to realize the transparent production, transmission, and inspection of academic certificates.

8.3.2 Multiple Evaluations of Online Learning

1. Multiple Evaluation Scenarios for Online Learning

Learning certification is an effective means to evaluate learning results. However, due to the complexity of learning itself and the conservatism of the education system, learning certification has adhered to simplified and test score-oriented standards for a long time and only certifies the results of formal learning. With the advancement of quality education, talent evaluation requirements can include informal learning.

A student learning information recording platform based on blockchain technology ensures students' privacy in the system and makes tamper-proof records of students' online informal learning data such as browsing web pages, using learning apps, and using smart contracts to convert learning data into learning results for permanent storage. It will facilitate the optimization of the learning certification and evaluation system and further promote the construction of a "lifelong learning passport."

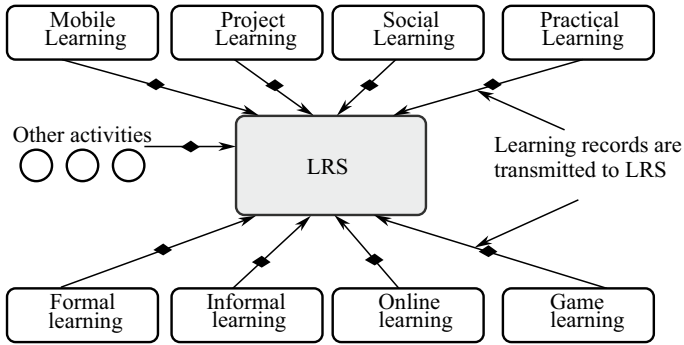


Fig. 8.9 Blockchain-based learning storage platform

2. Application Cases

(1) Learning Storage Platform Based on Blockchain Technology [18]

A learning storage platform based on blockchain technology is shown in Fig. 8.9.

Blockchain can be used to record and store formal or informal online or offline learning experiences and processes and can promote the wide and in-depth application of xAPI (Experience API). xAPI is a technical specifications used to store and access learning experiences. It is considered to improve and surpass the SCORM technical specification. xAPI can track and record learners’ online learning experience more carefully than SCORM. These records help teachers and researchers design teaching models and contents according to learning needs and analyze learners’ habits, styles, and behavior patterns, to realize personalized learning. xAPI can describe any ongoing activity stream, including learning activities and social media such as Microblog, Facebook, and Twitter use activity stream. xAPI also has the function of recording a learning database, that is, Learning Recording Store (LRS).

People’s learning time and place are increasingly decentralized and autonomous, and mobile, fragmented, and informal learning has become the primary mode of learning. A learning storage platform based on blockchain technology can track and record learners’ learning experiences and processes at different times and places through the application of xAPI, including formal learning and various informal learning contents such as computer games, simulations, or social media activities. Moreover, the learning data stored in LRS can flow between different LRSs, and LRS can exist anywhere, such as on mobile phones, computers, and other devices. When learners use new tools or content, take new courses and change jobs, all accumulated learning records can be taken with them. It can be seen that freeing learning data from learning systems, tools, and content is a subversive concept and practice mode of blockchain technology applied to education and teaching.

(2) Online Education Multiple Learning Evaluation Model [19, 20]

The Research Center of Knowledge BlockChain at BNU proposes an online education system framework based on blockchain [19]. It gives a smart contract solution to the problem of online education multiple evaluations.

As shown in the system framework in Fig. 8.10, article [20] describes in detail the model of online education multiple learning education. All educational institution users can create and deploy a Course Credit Generation Contract (CCGC) on the LA private chain, which can automatically score based on the user's online learning multiple data (such as learning time, test scores, and online discussion activities) according to online learning multiple rules written in CCGC, and calculate a specific course credit of a learning user, and constitute the online learning evaluation mechanism (Fig. 8.11).

Moreover, based on the program above, the Research Center of Knowledge Blockchain of BNU is exploring how to apply blockchain for online education management. There is always a many-to-many relationship in a class, which means

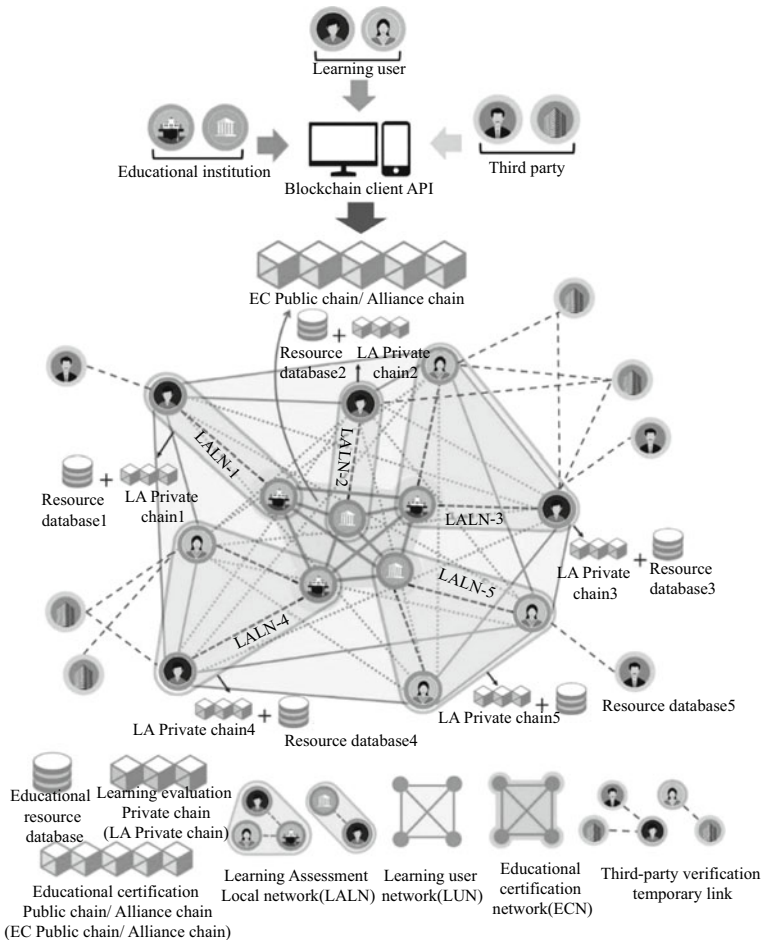


Fig. 8.10 An online education system frame based on blockchain

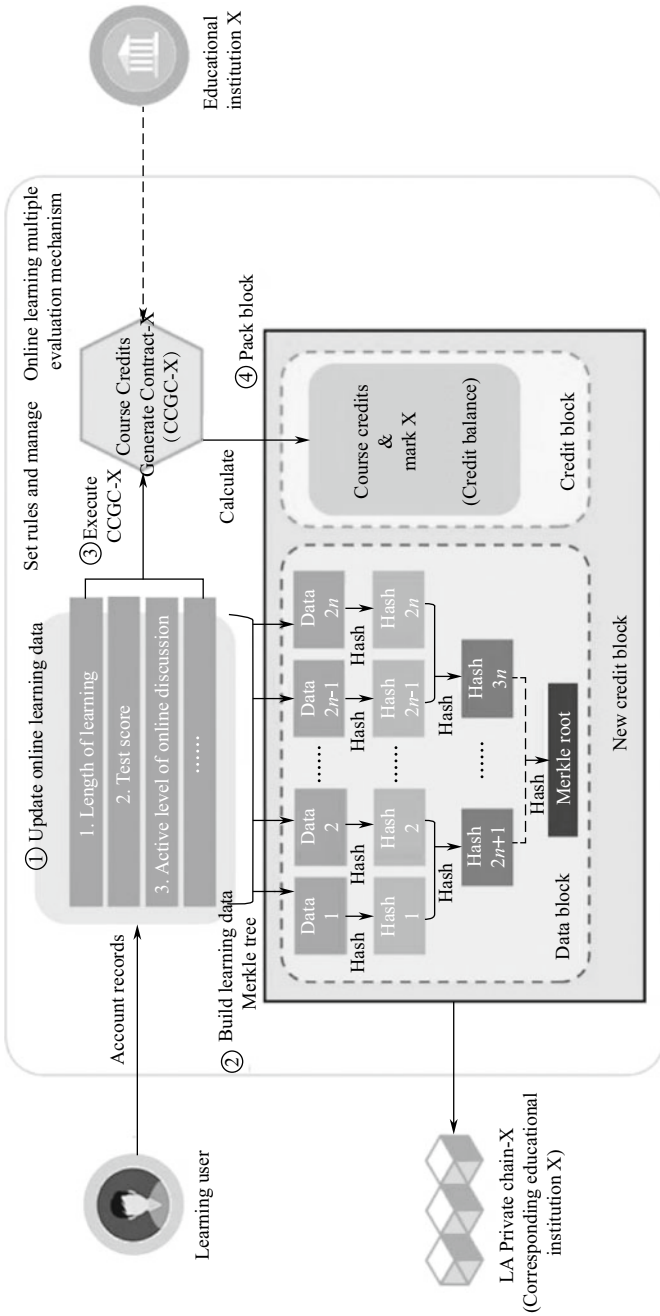


Fig. 8.11 The online learning evaluation mechanism based on blockchain

that a teacher may teach many students and all students evaluate the teacher. At the same time, a student's comprehensive score is given by all teachers.

In this process, the evaluation index between subject and object is multiple and distributed, which means in the process of the evaluation system, evaluation of students and teachers must be generated at the same time, and the result should be consistent in every node. Traditional evaluation methods cause data transmission redundancy, and the results created before can be tampered with by a third party. The safety and tamper resistance of blockchain can avoid these problems. Fully considering the evaluation of multiple quantitative indicators between subject and object in the education evaluation process, they allow the creation of an objective and accurate online education distributed subject-object evaluation model, implement an online education subject-object evaluation system based on blockchain and smart contract, and realize the quantitative assessment of students and teachers automatically. Organically combining automatic quantitative assessment of blockchain and evaluation of multiple evaluation subjects can achieve the harmonization of structured and unstructured evaluation, the harmonization of depth and breadth, the harmonization of effectiveness and quantity, and resolves the problem of dynamic evaluation and authentication in online education quality management system.

8.3.3 Copyright Deposits and Transactions

1. Copyright Deposits and Trading Scenarios

When using blockchain technology to register the copyright, after holders upload the work materials, the blockchain system will add a timestamp to each work by timestamp technology and, at the same time, generate a string of hash values and finally store all related data in the blockchain and accomplish the copyright registration [21]. This method doesn't require a submission to the Copyright Center; it can complete the copyright registration and issue a copyright registration certificate.

In the book publishing industry, blockchain can effectively protect a book's copyright. Before publishing, a publisher can register copyright in the blockchain copyright system to determine the attribution of works, which registers a digital ID card for original works. This method can protect original copyright and provides a good foundation for rights protection and copyright monetization.

Blockchain also has potential for rights protection in the digital music market. Blockchain technology can make charges and usage transparent and authenticate music ownership to the benefit of musicians. In addition, musicians can publish and promote their works through the blockchain, not through the publishers and distributors, so they don't need to worry about infringement.

2. Applications

- (1) Proof of Existence Copyright Registration Service and Xiaoxi Copyright Chain [22]

Proof of Existence blockchain in America can prove the work's ownership without leaking information and provide proof at a specific time. After a user uploads a work and pays for encryption fees, Proof of Existence can create a hash value for the work, representing the unique ID for the work, and store it in the blockchain. By comparing the hash value in the blockchain and the hash value of the work and timestamp, it is easy to prove the existence of the work at that time. Moreover, the Poet program based on Proof of Existence, can conveniently calculate the hash value of pictures, words, and voices, and store the hash value and content in the blockchain. The whole registration process can finish on our computers without going to the copyright agency.

Xiaoxi copyright chain is a copyright comprehensive service platform built by Copyright Protection Center, Notary office, and Industry Fund, and its core function is copyright confirmation in electronic works. After real-name certification, the holder uploads an original work, Xiaoxi copyright chain will generate a unique timestamp combined with the working name, the holder information, and registration time and store the timestamp in the anti-tampering blockchain. Finally, it can generate a unique and anti-tampering proof of work existence. The proof will receive endorsement from the blockchain and become the proof of ownership. The advantage of the Xiaoxi copyright chain is that it can naturally adapt to all kinds of digital production tools. Once a creator generates a work, it is easy to upload the work to the blockchain and so speed up the confirmation process. Taking films as an example, a creator can not only upload the video to the blockchain immediately to get proof protection but also upload the non-splittable text content which is in production and belongs to the film so that it can prevent the danger of infringement in a film's production stage.

(2) PaiPian Blockchain, a Film and Television Copyright Trading Platform [23]

PaiPian is a video content production platform in a 'didi-director' mode and offers deep video content production service for SME customers. In 2018, the CEO of PaiPian announced "All in Blockchain," and the company transformed from commercial shooting video to film and television copyright transactions based on blockchain. PaiPian uses blockchain technology to add a digital certificate for each video. Every transaction record will be stored in blockchain for deposit evidence, so it becomes easy to identify piracy by traceability of blockchain. Furthermore, PaiPian is establishing a worldwide copyright transaction network, allowing all film, media, and publishing practitioners to upload film and television works to finish copyright certification and transact in the world. The uploading content includes but is not limited to creative ideas, drama, video material, 3D models, films, TV shows, documentaries, and art short films. The process includes:

- Create a digital identity for digital media content, such as film, in a distributed network.
- Make a smart contract with clear income distribution and publish it to the blockchain. The contract cannot be tampered with because of the consensus mechanism of the blockchain.

- Due to decentralized features, transactions can happen point-to-point, meaning the video can be traded directly between creators and users.

(3) Mediachain System and Monegraph Digital Artwork Trading Platform [24]

Mediachain is a blockchain company in New York that obtained seed round financing from Andreessen Horowitz and Union Square Ventures in 2016. According to co-founder Jesse Walden, Mediachain provides a digital image copyright protection service. Its goal is to realize a 100% seamless connection between the owners and their works by sharing pictures and information using the decentralized operation platform. Spotify is optimistic about the prospects of Mediachain and acquired Mediachain. Mediachain uses IPFS (Interplanetary File System) to protect the copyright of digital works. The main working principle is that blockchain technology provides open-source point-to-point database and protocols used in registration, identification, and tracking on the Internet. Based on the metadata protocols above, Mediachain provides copyright recognition for innovative works.

Monegraph Digital artwork trading platform (referred to as the Monegraph platform) is a project developed by Kevin Mc Coy, a professor at New York University, and Anil Dash, a technical expert. It is based on using blockchain to protect artists' digital assets. They aim to build a system to perfectly resolve the problems of digital resource certification and royalty distribution through blockchain. The Monegraph platform aims to make digital resource monetization by blockchain and achieve the goal of verifying resource ownership. On the platform, the owners can create options such as sale, resale, and license certification and can price free at the time of settlement. Users can log in to the Monegraph platform using a Twitter account, choose a digital resource URL, and record Twitter account details and digital resource links on the blockchain. For the content buyers, the Monegraph platform can show the titles and everyone's attributes obviously, and the buyers can get ownership directly and pay for usage, which means there is no need for a third-party intermediary.

8.3.4 Knowledge Securitization

1. Knowledge Securitization Scenario

Knowledge securitization is knowledge shareholding - the process of treating knowledge as a factor of production, quantitating knowledge into intangible capital, and combining it with financial capital and physical capital. In the process of knowledge securitization, the body of knowledge is not general knowledge but knowledge about high-tech, management, or behavioral science. The securitization process is the evaluation, certification, and transaction of knowledge capital. Blockchain technology can be used in building a securitization platform for credible knowledge dissemination, management, and transaction, thereby promoting knowledge securitization realization, a promising and potential application direction for blockchain.

2. Application

(1) Knowledge Blockchain and Knowledge Securitization Platform

The Research Center for Knowledge BlockChain at BNU proposed the concept of *Knowledge Blockchain* in 2019. Knowledge Blockchain is a system using technology in blockchains, such as a distributed ledger, decentralization, and tamper-proof smart contracts to share, spread, and evaluate knowledge and education resources in education and intellectual property. Compared with a traditional blockchain system, Knowledge Blockchain has characteristics such as diverse user groups, storing knowledge achievement, and replacing economic profit with knowledge assets. Moreover, the research center proposed a plan to build a more systematic and comprehensive knowledge securitization platform based on blockchain (Fig. 8.12). This plan helps to promote project implementation, improves the welfare of all intellectual property owners, reduces the financing risk of high-tech enterprises, and stimulates technology innovation.

Blockchain is promoting the development of credibility and the circulation of data value. Applying blockchain in the cultural education field, especially copyright and educational certification, will positively impact the long-term development of cultural and creative industries and education industries.

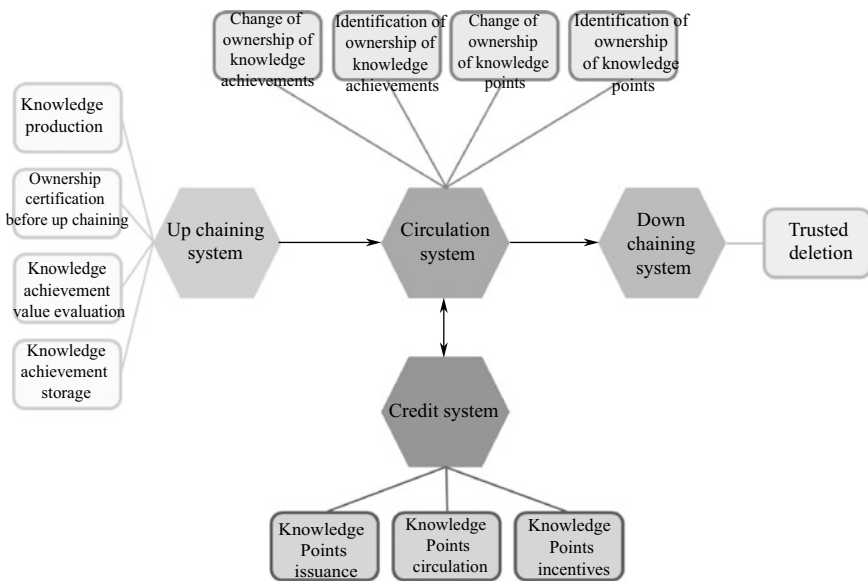


Fig. 8.12 The model of knowledge securitization platform based on blockchain

References

1. Ministry of Science and Technology, Central Propaganda Department, Central Cyberspace Administration, etc. Guiding Opinions on Promoting the Deep Integration of Culture and Technology [EB/OL]. 13 August 2019. http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2019/201908/t20190826_148424.htm
2. Ministry of Education. Guiding Opinions on Doing a Good Job in the Organization and Management of Online Teaching in Ordinary Colleges and Universities during the Period of Epidemic Prevention and Control [EB/OL]. 05 February 2020. http://www.moe.gov.cn/jyb_xwfb/gzdt_gzdt/s5987/202002/t20200205_418131.html
3. Ministry of Education. Action Plan for Blockchain Technology Innovation in Colleges and Universities [EB/OL]. 06 May 2020. <https://aimg8.dlssyht.cn/u/1765035/ueditor/file/883/1765035/1589785203649119.pdf>
4. Li C, Xing L, Qinhuo Z. Conceptualizing knowledge in “Internet + education Internet education”: the nature of knowledge and knowledge evolution. *Distance Educ China* 2019;(7): 9–18.
5. Ling Q, Huifu X, Wei G. Practice, impact and trends of online education in the United States: analysis and reflection of CHLOE 3 Report. *Open Educ Res* 2019;(3):10–21.
6. Yuwei S, Li C. Two-sided analysis of the development of “grassroots service grassroots” model under the era of internet plus: analysis of the development of the model in the field of online education. *Open Educ Res*. 2018;23(5):26–33.
7. Liangxu L. Research and application of block chain technology in digital rights. Beijing: North China University of Technology, 2018.
8. Xiaoyu C. Research on the construction of copyright value evaluation mechanism. *China Publishing J*. 2015;22:44–9.
9. Shoudi J, Hongliang M, Yang Y et al. The value and its use of open badge for online learning—based on case analysis of Moodle course. *Modern Educ Technol* 2014;(8):78–79.
10. What is a badge? [EB/OL]. 04 May 2020. <http://openbadges.org/about/>
11. Dongying L, Xiaohan H. Online learning assessment accreditation study supported by digital badges. *Software Guide*. 2017;16(3):189–92.
12. Muilenburg LY, Berge ZL. Digital badges in education: trends, issues, and cases. New York: Routledge; 2016.
13. Tao X. The application and challenges of blockchain technology in educational practice. *Modern Educ Technol* 2017;27(1):108–14.
14. Shuangzhi Z. “Blockchain + Credit Bank”: empowering lifelong learning. *E-education Re* 2020;41(7):62–8, 107.
15. Grech A, Camilleri AF, Andreia IDS. Blockchain in education. Publications Office of the European Union, 2017.
16. Qing L, Xin Z. Blockchain: a technology to win open and trust in education. *J Distance Educ* 2017;35(1):36–44.
17. Xianmin Y, Xin L, Huanqing W et al. The application model and challenges of blockchain technology in education. *Modern Distance Educ Res* 2017(2):34–45.
18. Tao X. Research on the development and significance of “Blockchain+” Education. *J Distance Educ* 2017;35(2):19–28.
19. Li C, Guo J, Zhang G, et al. A blockchain system for E-learning assessment and certification. In: 2019 IEEE International Conference on Smart Internet of Things (SmartIoT). New York: IEEE, 2019. p. 212–9.
20. Chuyang L. Research on smart contracts for multivariate evaluation mechanism in online education. Beijing: Beijing Normal University, 2020.
21. Bingqing Z, Lin L. The balance of digital copyright interests based on blockchain technology. *China Publishing J* 2019(11):22–5.
22. Baoyong H, Yizheng S. Analysis on the innovative application of blockchain technology in copyright registration. *J Chongqing Univ (Soc Sci Edition)*. 2020;26(6):117–26.

23. “Paipian.com” makes movies and enters the blockchain, and what changes can this technology bring to the film and television industry? [EB/OL]. 09 May 2020. https://www.sohu.com/a/223136518_104421
24. Weiluo C. Research on the construction of streaming music copyright management application system driven by blockchain technology. Beijing: China Conservatory of Music, 2019.

Chapter 9

Blockchain and People's Livelihood



Boming Yu and Shixiao Zhan

Abstract Livelihood issues and people's lives are closely related, which have always been an important focus in the process of social construction. In this paper, the first part describes the value of blockchain applications in people's livelihood, especially analyze the significance of providing reliable and credible business collaboration and value transmission platforms. The second part discusses the typical application scenarios and practices, including Healthcare data sharing, Traceability of drugs, Donation management, Crowd-sourcing compensation, Targeted poverty alleviation and Land requisition and demolishing management.

Keywords Blockchain · People's livelihood · Trust

9.1 Overview of Application Fields

9.1.1 Value of Application

Livelihood issues and people's lives are closely related, which have always been an important focus in the process of social construction. At present, difficult problems still exist in supervisory institutions of people's livelihood, including the lack of trust, opaque management, low credibility of information and information asymmetry, etc. These problems lead to the low efficiency of business collaboration between institutions, more difficulty in conducting government supervision and some measures failing to achieve the expected performance. Based on the unique mechanism of trust establishment, blockchain is changing the application scenarios and operational rules of multiple industries. It will become one of the indispensable technologies in developing the digital economy and forming the new trust system in the future [1]. In the field of people's livelihood, blockchain can provide reliable and credible business collaboration and value transmission platforms, to share information transmission

B. Yu · S. Zhan (✉)
Hangzhou Qulian Technology Co., Ltd., Zhejiang Province, People's Republic of China
e-mail: zhanshixiao@hyperchain.cn

and trusted sharing between organizations, resolve the issue of information asymmetry and break information barriers. In doing so, it is likely to resolve trust issues and improve the efficiency of business handling and offer firm support for government regulation, thus enabling the government and enterprises to provide more efficient, convenient, and reasonable services for people's livelihood.

Theoretically, services for people's livelihood, which require trust support, value transmission and multiple collaboration, can provide solutions through blockchain technologies [2].

1. Based on the unique distribution, establish the collaboration platform, and improve business efficiency

Based on the unique trait of distributed ledger, blockchain allows the business data to be rapidly shared and synchronized in upstream and downstream parts of platforms. Serial processing, which was previously required by some businesses, is now converted to parallel processing. Moreover, costs of data flow and interflow decrease to provide reliable and credible platforms of business collaboration and value transmission for relevant parties. In addition, blockchain technologies can be utilized to set up channels for information transmission and sharing, to resolve issues like information asymmetry and improve the quality of service for people's livelihood. For example:

In terms of "blockchain + medical treatment and health", the traditional storage and management of medical data are administered by the systems built by medical institutions. Due to requirements on data privacy and safety, medical data can hardly be shared and utilized across different institutions. If collaboration platforms are built with blockchain technologies to record and trace medical data, they can effectively help hospitals to achieve efficient cooperation and facilitate the development of medical treatment and health in terms of coordinating diagnosis and joint scientific research.

In terms of "blockchain + pension service", blockchain technologies can be used to connect civil affairs departments at different levels and nursing institutions for the aged in different regions, to provide home-based care service and institutions for the aged. Besides, relevant data can be fed back to their children and regulatory organizations, aiming to achieve positive progress in the quality evaluation, stimulation, and improvement for pension services.

2. Reliable certification of business data. Enhance transparency of the business process

Compared with conventional databases, blockchain technologies can ensure the reliability and authenticity of data. They can also significantly increase the efficiency and reduce the cost of taking and obtaining certification. In the meantime, blockchain-based data structures endow time sequence with data information. In doing so, it provides reliable base support for data tracing. This process complies with the requirement of transparency on data in food safety and public benefit. Besides, it can also enhance the credibility of improving people's livelihood, which serves as a useful approach to information auditing and social supervision. For example:

In terms of “blockchain + merchandise anti-counterfeiting”, blockchain-based supply chain source tracing can get through links such as production, circulation, and sales, etc. By attaching supervision codes to merchandise, information on specific products, which are dispersed among different institutions, can be managed systematically, to manage the information of merchandise during full-life circles and maintain the uniqueness, thus reducing counterfeit products and low-quality products.

As for “blockchain + public charity”, based on the transparency and credible traceability of blockchain, it is feasible to set up a new system of charitable donation. Through integrating the capabilities of blockchain certification, logistics tracing, cross-validation, public supervision, and regulatory organizations, it is likely to establish the informatization platform for charitable institutions with reliable certification and charitable data. In this way, data about donations, goods and materials received and sent by charitable institutions can be uploaded to the chains, to offer reliable and transparent means of inquiry and monitoring for society.

As for “blockchain + social assistance”, blockchain has quite apparent traceability. It can upload all the information on those in need of assistance, directly link donors, receivers and projects being donated. Besides, the entire process of social assistance can be uploaded to ensure that each sum of donation money is explicit and not tampered. By engaging multiple parties in the supervision of social assistance, projects receiving donations are open and transparent to the public. Through real-time tracking of those who are assisted and the process of assistance, it is feasible to offer true help to the people in need rather than viciously obtaining social assistance through defrauding.

3. Build the distributed system of digital identity. Challenges caused by blockchain performance and functional features

Identity verification is the basis of service for people's livelihood. When it comes to the application of blockchain in the field of people's livelihood, it is essential to build the mapping mechanism of real identities and on-chain digital identities for the people. Therefore, a distributed system of digital identity should be set up to realize on-chain identity verification and help people to verify their own identities, declare wills and manage their own assets and information in the blockchain network. With the assistance of a distributed system of digital identity, governments can rapidly arrange and manage the public information that disperses among different institutions, thus providing accurate and high-quality service for people's livelihood.

In terms of “blockchain + employment service”, blockchain can establish the digital identity system for the public. Identity Information about education and past work status, which dispersed among different institutions, is connected through digital identities to form electronic records, to help people better demonstrate their skills and achieve more efficient and accurate matching in employment. In the meantime, based on the digital identity system, it is feasible to set up the most flexible platform of employment and form the model of “online crowd-sourcing of work”. In doing so, people can apply for jobs online through digital identity and calculate compensation by using intelligent contracts of blockchain. Moreover, the income is

distributed to corresponding accounts of people's digital identities, to realize efficient and flexible model of employment.

As for "blockchain + medical service", collaborative diagnoses among different institutions are concerned with information on plenty of doctors and patients. As a result, issues like privacy and compliance may exist in the process of information exchange. Digital identities of blockchain can be used to gain data access control, enabling patients to authorize private information and doctors to sign diagnoses. Moreover, data with when processing data with encryption levels and critical information, the alliance should be required to conduct strict authority checking [3], to clearly divide rights and liabilities, as well as trace the process of authorization.

9.1.2 Issues and Challenges of Application Implementation

Due to such reasons as traditional business models and unique technical features of blockchain, some challenges still exist in the present application of blockchain in people's livelihood, which specifically includes the following three aspects:

1. Business model changes and conflicts with existing models due to blockchain technologies

Blockchain technology places emphasis on collaboration among multiple parties. Only in this way is it possible to give full play to the value of blockchain. Currently, mature forms and business centers have come into being in most fields of people's livelihood. In addition, business centers have powerful discourses the over the business process and management modes. With multiple centers and disintermediation, blockchain equalizes all aspects of business to form new models. Because of the changes in business ownership division and benefit distribution, the transition from business models to new ones tends to suffer resistance, which is also the most significant challenge as to the application of blockchain in people's livelihood.

2. Issues of blockchain system construction and system docking

Blockchain is a distributed system. What makes it different from the centralized system is that the blockchain system will surely induce disputes in the division of administration authority among business participants and the rights of utilization among main bodies of construction. Concerning such imperfections in the development and management of the systems, the implementation process of blockchain applications may suffer more resistance than traditional applications. Meanwhile, the docking between the blockchain system and existing business systems will also become an issue about project implementation.

3. Challenges caused by blockchain performance and functional features

Technical points like consensus algorithms, smart contracts and data storage models enable blockchain to conduct tamper resistance and reduce costs of trust. However,

they also bring about relevant problems as to data privacy, data volume and system performance, etc.

- (a) Issues of data privacy: traditional blockchain systems require all data to maintain consistency at all nodes, which means all on-chain data are open to organizations involved. It has a major influence on many scenarios of people's livelihood, especially in the medical field. Some domestic blockchain service providers provided different solutions as to the protection of data privacy. However, different due to varying demands for privacy protection in different scenarios, no universal solution has been proposed yet.
- (b) Issue of data volume the feature of blockchain storage is that multiple nodes store multiple copies, which is not friendly to the application of large data volume. Take the medical scenario for instance. A medical institution must store terabytes of data on images and medical records. With existing hardware conditions, all the data can hardly be uploaded and stored using traditional blockchain modes.
- (c) Issues of system performance: the expanding scope of blockchain applications and the increasing number of users pose more requirements on the performance of the blockchain platform. high-frequency user demands, such as how to conduct merchandise anti-counterfeiting and work crowdsourcing, are another big challenge facing blockchain systems.

9.2 Application Scenarios and Practices

9.2.1 Healthcare Data Sharing

1. Blockchain solutions

Medical data sharing means the efficient and safe sharing of information on patients' records, images, and medical records in hospitals at all levels. Medical treatment alliance is a typical model of sharing medical data. It is a service system that integrates medical resources in a certain region to engage big hospitals and communities, as well as connect medical care, rehabilitation, and nursing. The purpose is to promote labor division and collaboration, reasonable use of resources and resolve the difficulty of getting medical service for the people. For instance, in 2018, in Jiading District, Shanghai, five district-level hospitals and 13 community healthcare centers formed the medical treatment alliance [4]. Community hospitals send the medical images to the central hospital of Jiading District, so that they can be analyzed by the doctors in the Division of Medical Images. In this way, patients in nearby community hospitals can gain access to the diagnostic services in second-class hospitals.

Despite a series of explorations and innovations in terms of medical data sharing, the following problems still exist in the current model of sharing medical data: (1) The enormous quantity of medical image data makes it difficult to be stored in the cloud for long periods of time. The data are stored respectively by medical institutions, which can hardly be jointly shared among hospitals. (2) Medical data of the same patient

are dispersed in various hospitals; thus, it is difficult to be effectively coordinated and identified. As a result, patients must go through similar examinations repeatedly in different hospitals. Third, medical data sharing is achieved through interactions among hospitals, but patients are not authorized, thus causing threats to their privacy security.

Due to unique features of security, transparency, joint accounts and anti-tempering, blockchain has changed the traditional forms of data storage and sharing. It can effectively safeguard private data, clarify the rights and liabilities of data, reduce costs of sharing. Hence, blockchain is an important technology to resolve the difficulties in the current sharing of medical data. Take the alliance of medical treatment, blockchain technology can be used to establish the platform of diagnosis and treatment information based upon electronic health records and electronic medical records of residents. By setting up the smart regulatory model, patients' information seeking for medical care and medical institutions are accurately matched, to monitor and control the process, as well as record and transfer the entire process of information. In addition, it can also provide comprehensive and one-stop services for patients to authorize image data collection, expert diagnosis, post-treatment rehabilitation and delivering medicare to serious diseases.

Through the application of the blockchain technology, the following objectives can be achieved.

- (a) Establish the system of sharing medical image data. Health Commissions and hospitals at various levels deploy blockchain nodes. This measure aims to break through the medical data of hospitals within the medical treatment alliance and promote the reliable and efficient sharing of medical image data.
- (b) Forge the model of on-chain and off-chain coordinated data storage. In order to resolve the difficulty of large storage quantity and long term of medical data, the blockchain technology makes it possible to store the dispersed medical image data within the hospitals' PACS (Picture Archiving and Communication System). In this way, the data and metainformation are stored on-chain, to form on-chain and off-chain data anchoring, allowing other medical institutions to check and gain access to utilizing the authorized data.
- (c) In addition to fully safeguarding the privacy of patients, form the medical data sets centered on patients as the main body. Medical data relate to patients' digital identities. Through the blockchain digital identities, patients can manage and examine their diagnosis data. The medical data among hospitals should also be authorized by patients. Meanwhile, diagnosis and treatment information should be uploaded on-chain to ensure the traceability of medical records, thus providing convenient and reliable services for patients to receive treatment.

Based on the blockchain sharing of medical data, it is feasible to promote medical data sharing among hospitals, enhance the efficiency and value of medical image data and promote technological interaction among them as well. Doctors can gain access to patients' past medical records and come up with more effective diagnoses and treatments according to patients' medical conditions. Meanwhile, blockchain

digital identities can fully safeguard the privacy of patients' data, to offer reliable medical services for them.

2. Application cases: blockchain-based platform of medical big data and scientific research

The big data research platform of the National Clinical Medical Research Center for Infectious Diseases is jointly set up by Hangzhou Shuniu Technologies Co., Ltd together with 49 national core units. The first batch was implemented by four hospitals, including The First Affiliated Hospital, College of Medicine, Zhejiang University and Hangzhou Xixi Hospital. They are committed to the research and studies about COVID-19 prevention and cure. Based on technical features of blockchain, the big data research platform of National Clinical Medical Research Center for Infectious Diseases can provide manageable, auditable, and traceable sharing of medical science and research data. Meanwhile, it places emphasis on privacy and security, and aims to form an effective mechanism in terms of data masking and safe transmission, etc. This platform plays multiple roles, including user verification, organization management and system management, etc. For this reason, it can supervise the full life cycle of medical data generation, transmission, and application. Moreover, user rights, data logs and operation logs are stored through blockchain to ensure secure data sharing and increase sample sizes to facilitate the cause of scientific research and studies in medicine. The blockchain based big data medical research platform is shown in Fig. 9.1.

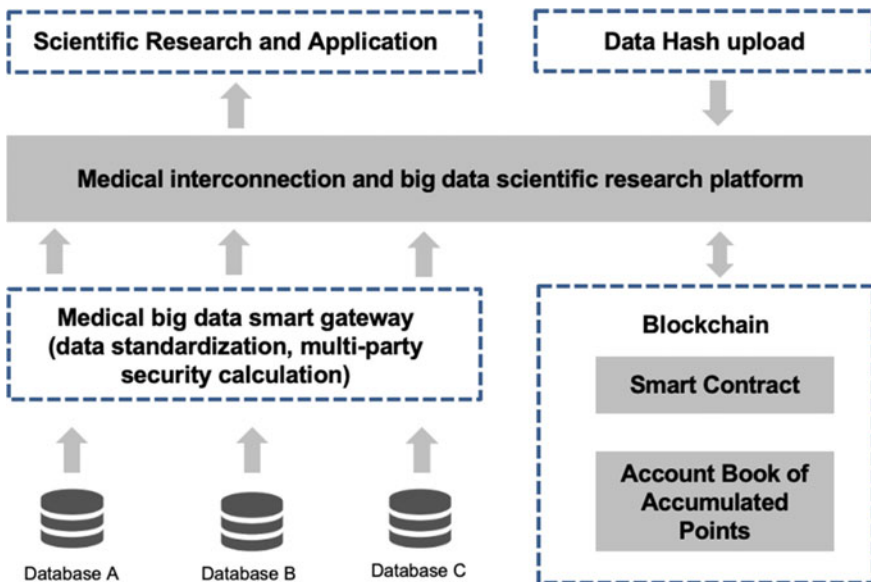


Fig. 9.1 Blockchain based medical big data platform of scientific research

9.2.2 *Healthcare Data Sharing Traceability of Drugs*

1. Blockchain solutions

Issues and problems that occurred during the process of drug circulation, such as inappropriate storage and selling fake medicine, have severely negative impacts on the safety of consumers. In recent years, drug administration departments have also tightened supervision on the circulation of drugs in terms of combating fake medicine, controlling the quality, and protecting the safety of patients. In the meantime, pharmaceutical enterprises also expect to conduct full-process and automatic drug supervision, to reduce human errors, optimize the supply chain and enhance circulation efficiency, etc. The pharmaceutical industry is in urgent need of regulating and processing mechanisms to standardize the management and risk control of the whole industry.

The difficulty in discerning fake medicine from the genuine, lack and hysteresis of traceable data have led to tremendous challenges in supervision, which mainly include the following problems:

- (a) Risk events cannot be prevented, and supervision lacks forceful implementation. Production and circulation enterprises can't gain access to the data of overall drug whereabouts. As a result, overstock and stockout frequently occur in the sales of medicine. Pharmaceutical companies have difficulty in marketing and management as well. Hence, it is not only difficult to safeguard the security of consumers, but also hinder the development of pharmaceutical enterprises and disrupts the environment of drug markets.
- (b) Low efficiency of inspection. Difficulty in Law enforcement and examination.

After going through factories bulk pharmaceutical chemicals, pharmaceutical factories, multiple levels of wholesalers, dealers and transport links, medicine eventually reaches the hands of consumers. Various participants seek to defend their own business data. Regulatory organizations can only gain relevant information through multiple levels of statistics and reporting, which makes it difficult to obtain comprehensive information on drug quality and circulation. In cases of quality problems, it is also difficult to determine the specific links of problems.

1. Non-transparency of drug data. Difficulties of consumers in distinguishing the fake from the genuine. For consumers, the chains of drug traceability data are incomplete. And the drugs are hard to be verified as well. In case of discovering quality issues, the public does not have proper ways to make complaints. Therefore, there is no reliable guarantee as to safe medication.

Traceability and tampering resistance of blockchain technology can be applied to source tracing. Furthermore, the pharmaceutical industry poses more rigorous requirements for authenticity verification and source tracing than other industries. The application of blockchain in source tracing of drugs include the following advantages:

- (a) Build the overall blockchain management system. Enhance control and monitoring of drug quality. Blockchain can gather comprehensive information on all links of pharmaceutical production, circulation, and sales. Moreover, it is also able to conduct checks of drug samples, display the results of samples, attach supervision codes to drug sources and sales identifications, to ensure testing for drugs, traceability of the process and reliability of authentication.
 - (b) Provide strong evidence for legitimate reviews and accountability. Based on the information on links of drug storage, production, circulation, and consumption, it is feasible to trace sources, determine whereabouts of drugs and claim responsibilities for personnel involved, thus offering valid data support for behavior accountability.
 - (c) Form penetrative supervision. Promote the development of the pharmaceutical industry. By deploying nodes of blockchain networks, drug administration sectors can check all the blockchain data. With the grasp of critical information about links from production to consumption, drug administration sectors can free themselves from the complicated process of information collection. They are also able to achieve truly penetrative supervision through smart contracts and setting granularity of monitoring. In addition, consumers can scan QR codes to check the overall data of the overall medicine circulation, so that they can report quality issues promptly. Based on the transparency of production and circulation information, as well as tampering resistance and traceability of blockchain, regulatory sectors can detect disqualified enterprises, which is conducive to optimizing the atmosphere of the industry and facilitating its healthy development.
2. Application cases: the drug tracing comprehensive service platform based on blockchain

In 2019, the Shandong Branch of China Construction Bank and Medical Products Administration of Shandong jointly developed the comprehensive service platform based upon blockchain drug tracing [5]. Oriented by “Exclusive codes for specific items. Common Tracing for items and codes”, the two organizations aimed to set up a comprehensive service platform based upon blockchain to “trace sources and examine accountability” for all types and procedures of drugs and medicine. This platform consists of three sections, including the platforms of drug source tracing and monitoring, drug tracing and public inquiring. The platform of drug source tracing mainly strives to collect the all-procedural drug tracing data to achieve supervision from drug production to drug circulation within Shandong Province, enhance the level of drug administration and management in the “province, cities and counties”. Besides, it also aims to check information on drug selling, outputting, and inputting of warehouses through code scanning for retail drug stores and medical institutions, as well as enable consumers to trace drug sources according to the “exclusive code for specific item”.

9.2.3 *Donation Management*

1. Blockchain solutions

In traditional public charity projects, regardless of donors or platforms, it is hard for them to promptly supervise and track donations. This task is mostly completed by public interest organizations providing image and text feedback to society and monitoring sectors. Due to low levels of transparency, this form of donation and contribution leads to a lack of public trust. As a result, donations cannot be provided accurately, which also demotivates donors to participate in charity. During the COVID pandemic, issues and problems of existing charity and donations have become prominent. Money donors put more rigorous requirements on the transparency of charity platforms. The public account, fund flow, project procedure and result of implementation of each donation should be explicitly and tightly related, thus ensuring the outcome and efficiency of charitable donation.

The current charity industry reveals the following acute problems:

- (a) Counterfeiting and cheating can hardly be monitored. Due to the lack of supervision authentication and the imperfect mechanism of information disclosure, information about assistance acceptance is difficult to be verified. Besides, because of the absence of restriction, it is difficult to monitor if charity organizations fake information or embezzle the money of donations, which is also a direct reason for the issues of trust crisis. The industry of charity and public interest should urgently enhance the level of social trust.
- (b) Low the efficiency of allocating donation funds. In conventional cases, charity organizations need to submit application materials to administrative authorities for review and approval. The process is rather complicated, which usually takes approximately 20 workdays. As a result, assistance recipients cannot receive donations promptly, thus lowering the level of urgency.
- (c) Non-explicit flows of donation. Non-prompt information disclosure. Inaccurate donation appropriating. If the information about donation is not revealed promptly and there is no effective way to track and audit funds, it may lead to repeated donations, appropriations, and inaccurate donations, as well as the absence of tracking methods.

Blockchain has technical advantages in terms of data consensus, information synchronization and authentication tracking. It is feasible to establish platforms of sharing information and business collaboration based up blockchain, as well as incorporate different nodes in the alliance to form new models of donation management, thus resolving the issues and problems effectively.

- (a) By breaking through the business systems for parties involves, it is possible to achieve transparent data records across all chains. Demanders release the information of demand on the platforms, which should be approved and verified by authorities. Donors release the information of donations. Logistics and banks publish information about the circulation of goods, materials, and funds. Relevant information and data of the donation process can be recorded and connected

for the verification of smart contracts, thus effectively preventing counterfeiting in the donation process.

- (b) Information on donations can be tracked to facilitate accountability and examination. Because of tampering resistance of blockchain, once the information is uploaded and stored, it cannot be altered. When fund auditing or judicial accountability is necessary, blockchain can offer authoritative data proofs, so that donations have evidence to be examined and reviewed.
 - (c) Transparent information disclosure. Penetrative ways of fund monitoring. Critical data should be stored, authenticated, and jointly shared based on blockchain. Information on donations should be open to various parties involved. In doing so, charity organizations can release the information for social supervision to enhance the public credibility. Meanwhile, regulating sectors are also able to review all the on-chain data, comprehensively monitor donations and fund appropriations, thus ensuring the public and transparent process of donating.
2. Application cases: charitable donation tracking platform based on blockchain

On February 10th, 2020, Hangzhou Qulian Technology Co.,Ltd developed and provided relevant techniques, and worked with China Xiongan Digitalcity Corp to officially release the “Shanzong” platform for tracking sources of donations. By making the best use of alliance-oriented blockchain networks, this platform provides reliable and efficient solutions for charitable donations during the COVID pandemic [6] (Fig. 9.2). In addition to on-chain traceability of donation data, it also serves as a convenient and handy entrance to browse on-chain information, and provide information check services for all people, to ensure the right to learn about the interior information of the platform for all sectors of society. Moreover, this platform strives to break through all procedures of charitable donations, including “seeking donation-connecting donation-sending donation-tracking logistics-confirming donation”. Finally, this platform offers legal safeguards. The notarization service is provided by Hangzhou Internet Notary Public Office, aiming to prevent dishonest acts like false donations through legal means. Up till February 27,2020, more than 200 enterprises registered on this platform. Many of them made charitable donations to hospitals and charity organizations in Hubei to fight against the COVID pandemic. There were nearly 600 entries of data about donations on the platform.

9.2.4 Crowd-Sourcing Compensation

With the nationwide advocacy of “dual entrepreneurship and innovation among the masses”, the service crowd-sourcing industry has embraced great opportunities for development. Crowd-sourcing platforms recruit idle human resources and undertake tasks from contract-issuing parties. In doing so, they can acquire crowd-sourcing service capacities of online member recruitment and training, project releasing, production implementing and the integration of management and controlling.

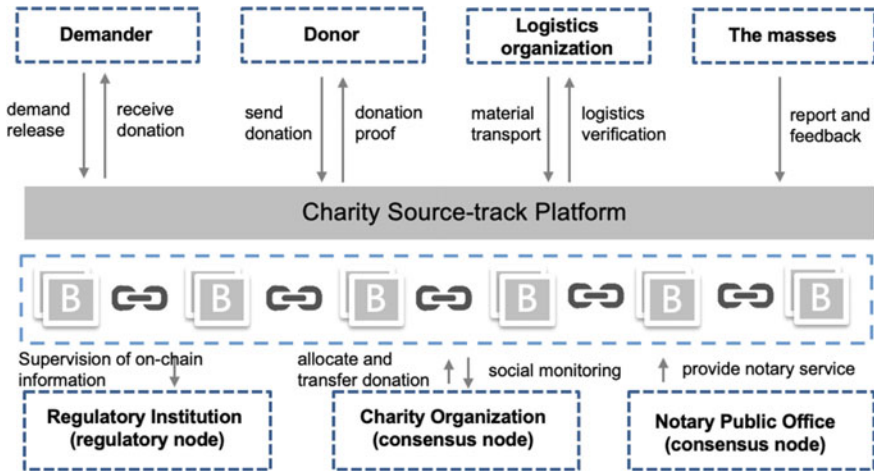


Fig. 9.2 Basic model of blockchain donation management

Traditional procedures of crowdsourcing include outsourcers distributing task packages and members getting the packages to engage in call-out services of various sorts. After production is completed, platforms will rate and examine the subsequent status and quality testing of production for the members, to calculate specific workload and give remuneration to them on a regular basis. Generally speaking, business platforms will pay attention to expanding the scope of crowdsourcing, extending the quality service, enhancing information connection, resource sharing, mutual trust and exchange among various parties. Moreover, unified, and credible data and information management for the members and relevant parties involved. In this regard, crowd-sourcing compensation service should improve in two aspects:

1. Other than safeguarding users' privacy, give full play to mutual sharing of data.
2. Accurately assess production work and establish the consistent crowd-sourcing model of compensation and labor.

Blockchain technologies can energize and reform crowd-sourcing platforms, which effectively improves crowd-sourcing services in the following aspects:

- (a) Establish the ecological alliance. Forge credible and quality brands. Unit platforms, supporters, BPO enterprises and other willing organizations to set up multi-node blockchain alliances, achieve mutual connection and trust among them, establish crowd-sourcing service alliance platforms with authentic rights and data authentication, as well as information source sharing. In this way, it is likely to give full play to the potential and value of data and create the new value of crowd-sourcing brands.
- (b) Set up reasonable compensation systems and harmonious labor relations. It is feasible to set up new mechanisms of remuneration calculating and distributing through blockchain technologies. Payable wages for contract-issuing parties and due remunerations for members are calculated by platforms. Remunerations are

directly paid to members through banks. Based on blockchain, transparent flows of funds and data can be achieved to regulate employment and form harmonious labor relations.

- (c) Crack data islets and jointly form credible chains of value authentication. The difficult problem of data islets can be overcome by opening crowd-sourcing platforms to supporters and BPO contract-issuing parties. The comprehensive information of production by members is comprehensively uploaded and stored to achieve authentication, traceability, and tampering resistance through all procedures. In addition, data consulting and credit authentication can be completed with blockchain to facilitate corporate governance enhancement and equity process of crowd-sourcing services.
- (d) Confirm authentic rights of data and safeguard user privacy. Blockchain technologies can be applied in big data sharing and transaction. Based on the authority of smart contract, business processes, such as authentic rights, sharing and authority control of data, can be realized to ensure the effectiveness, authenticity, instantaneity, and safety of shared data. For private information of individual members, it should be approved by members themselves before information recipients (contract-issuing parties, crowd-sourcing platforms, and supporters, etc.) acquire it, thus fully guaranteeing the privacy security for users.

As for crowd-sourcing platforms, authenticating members' information through blockchain platforms can ensure tampering resistance, integrity, and traceability of data, thus forging credibility and reducing costs of information communication. Salary administration services can enhance the transparency of processes and results of salary calculation. In the meantime, platform responsibilities are detailed to reduce risks of operation. For crowd-sourcing personnel, blockchain offers effective guarantees for workload rating, salary distribution and legitimate safeguarding rights. For BPO enterprises, blockchain can select superior crowd-sourcing personnel, conduct reasonable and efficient salary administration, to improve the quality of crowd-sourcing services.

9.2.5 Targeted Poverty Alleviation

1. Blockchain solutions

Poverty alleviation is an important strategic deployment of the Party Central Committee and State Council. Fixed-point poverty alleviation by Party and government offices constitutes a key component in the strategic deployment of poverty relief and development, which plays an important and positive role in facilitating the growth of economy and society in poverty-stricken areas. Targeted poverty alleviation also serves as a critical requirement for poverty relief. According to different environments of poverty-stricken areas and specific situations of rural poor households, it is necessary to apply scientific and effective procedures to accurately identify, assist

and administer objectives of poverty alleviation, which is also the focus and difficulty of the existing anti-poverty project [6].

A tremendous amount of information records and fund flows are involved in the process of poverty alleviation, which cannot be completed without the information-based system. However, some issues and problems still exist, including the excessively long term of project application, difficult monitoring of project scheduling and implicit utilization of poverty alleviation funds, etc. They cannot be resolved simply by information engineering construction. Blockchain is conducive to data sharing, publicity, and transparency. Poverty alleviation management platforms, established on blockchain, can implement information monitoring throughout all procedures, as well as tampering resistance, dependability, and traceability of poverty alleviation data. According to Fig. 9.3, these systems can relate to institutions through blockchain, such as government examination and approval, government supervision, financial departments, poverty alleviation enterprises and commercial banks. Moreover, information about the application and approval of poverty alleviation projects, fund granting, and project supervision can be stored through blockchain as well, to guarantee tampering resistance, auditability, and source tracking of poverty alleviation data. Finally, information stored by blockchain can also provide related services, such as information statistics, real-time monitoring, and effectiveness evaluation of loaning process, for the parties who apply for loans in poverty alleviation.

In targeted poverty-relief work, blockchain can mainly provide the following services:

- (a) Identify poverty information and confirm objectives of poverty alleviation. Targeted poverty alleviation should accurately grasp the status of the poor. By utilizing the blockchain, information systems of relevant organizations, including industry and commerce, taxation, and banks, can be comprehensively connected to learn about the assets and credibility of people living below the

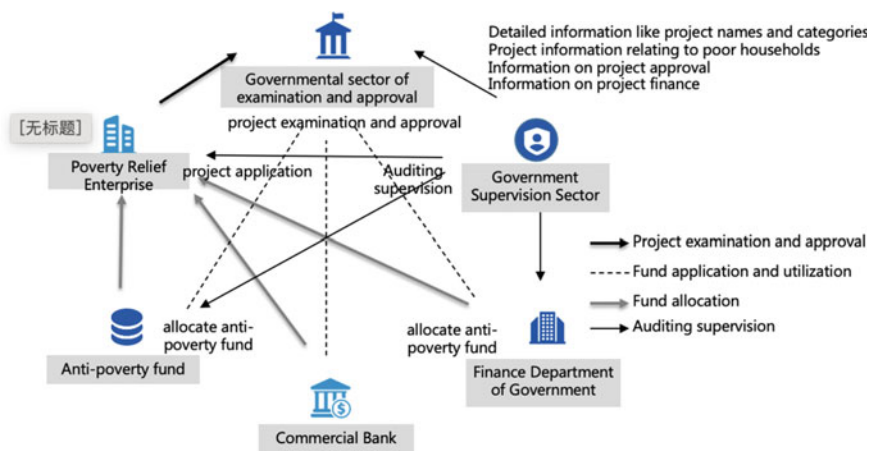


Fig. 9.3 Basic form of blockchain targeted poverty alleviation

poverty line, in order to prevent cheating in applications for subsidies. Meanwhile, poverty alleviation information is reported through various levels of blockchain to implement on-chain reviewing and examining, thus preventing corruption of poverty alleviation personnel. In addition, key information on poverty alleviation can be connected to regulatory sectors and government agencies through blockchain to ensure the transparency of application and approval of the anti-poverty process.

- (b) Record the process of fund circulation through blockchain. government sectors release lists and time periods of poverty alleviation. On this basis, banks confirm and release related information like the amount of discount on blockchain. According to such information, poverty relief offices and other government sectors can track and monitor the overall flow of anti-poverty funds. During the process of government reviewing and approval, the status of anti-poverty fund auditing and distributing can be referenced from any node. Corresponding information of initiating, auditing, confirming, and allocating is all publicly released on blockchain.
 - (c) Information during critical stages of poverty relief is recorded through blockchain. Moreover, with the help of biological pattern recognition, application for poverty alleviation funds and acceptance of funds can be confirmed by the poor in person. It can prevent any form of false poverty alleviation, which lays the foundation for subsequent examination and accountability.
2. Application cases: The blockchain-based platform of financial targeted poverty alleviation

As for the issues and problems, such as difficulty in accessing the information of poverty alleviation, financing for anti-poverty projects, affirming the loans and managing the funds, China Construction Bank developed the block-clock based platform of financial targeted poverty alleviation. The purpose of this platform is to release anti-poverty policies, apply for funds and supervise the funds and enhance the credibility of governments, enterprises, and bonding companies. Since the block-clock based platform of financial targeted poverty alleviation was released online on Sept 29, 2018, the Guizhou Branch of China Construction Bank contacted the municipal government of Bijie to log on the platform to publish anti-poverty policies and projects. corporate clients are notified to submit applications for anti-poverty project financing online and promptly procedures of finance handling, applying, and approving, etc. Through the block-clock based platform of financial targeted poverty alleviation, the Guizhou Branch of China Construction Bank released the first loan of 10 million RMB for targeted poverty alleviation, thus greatly helping the poverty-stricken areas to overcome poverty and other difficulties [7].

9.2.6 *Land Requisition and Demolishing Management*

1. Blockchain solutions

Land requisition and demolishing is related to the immediate interests of people. It is necessary to adhere to principles of justice, openness, and fairness. The multiple-party consensus feature of blockchain can minimize the chance of corruption and rent seeking in previous stages, aiming to guarantee the transparent and just process of fund appropriation, as well as innovate the model of governmental administration.

Based on the features of tampering resistance and traceability of blockchain technologies, land requisition and demolishing management can be improved in the following ways: 1. Transparent information disclosure can administer relevant information on projects and contracts, fund appropriations and the reference of fund payment results through the blockchain, to reduce risks of manual operation and proofreading, as well as improve the efficiency of fund appropriation. 2. Through connectivity between data and overcoming data barriers, it is feasible to break through the channels of system data between governmental agencies, financing institutions and relevant partners. 3. integration of financial service. By accurately connecting with financial products of banks, innovative products, including payment settlements, supply chain financing, loans on credit and personal financing, can be customized, to meet the varying demands for payment and financing.

2. Application case: The blockchain platform of displacement and resettlement funds management in a new district

In May 2019, the blockchain platform of displacement and resettlement funds management was initiated in a new district. The platform was jointly developed management committee of the district, Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, and China Construction Bank, etc. The blockchain technology was used to conduct the overall on-chain management of original archives and fund appropriations and keep track of the flow of funds in materials, equipment, labor service and salary. The blockchain platform of displacement and resettlement fund management enabled governmental administration to innovate. In doing so, financial data and government affairs related to financing institutions to integrate resources and services. Till the end of 2019, 3.9 billion RMB of displacement and resettlement was allocated through this platform to benefit more than 5700 households. In addition, this model can be applied in engineering construction and house renting to constantly expand and improve the 1 + 2 + N application scenarios in the new district. Lastly, the platform incorporates governments, companies with financing institutions to optimize government administration and people's livelihood services, which is conducive to forging the new ecology of open and shared smart cities.

References

1. China Academy of Information and Communication Technology. White Book of Blockchain. (8 Nov 2019).
2. Hongcan Z, Xinbo W. "Blockchain + people's livelihood": connotation, situation and task. *J Guangxi Normal Univer.* 2020;1:76–86.
3. Jieyong W. Difficulties and countermeasures of targeted poverty alleviation practice in China. *Sci Technol Dev.* 2017;6:412–7.
4. Medical Alliances were Set Up in Four Regions in Jiading. Shanghai to Comprehensive Enhance the Medical Service Capacity.
5. Trace Sources of Medicine. Hatch big healthy ecosystem—construction and promotion of drug traceability system in shandong branch of China Construction Bank. (29 Apr 2019). http://www.ccb.com/cn/ccbtoday/newsv3/20190429_1556524628.html.
6. Yaqiong S. "Pandemic Combating": tech companies are on the move. 2020. (12 Feb 2020). <https://36kr.com/p/1725095346177>.
7. With financial, scientific and technological strategy, CCB adopted various measures in targeted poverty alleviation. (10 Apr 2019). http://www.ccb.com/cn/ccbtoday/newsv3/20190410_1554863762.html.

Part IV

Governance Norms

The wide application and benign development of blockchain technology are closely related to governance and norms. For the evolution of blockchain basic technology and its large-scale multi-category applications, an orderly, coordinated, and sustainable governance, which combines on-chain and off-chain, is needed. At the same time, a systematic, reasonable and effective application evaluation system is required. In addition, it is more necessary to form standards in research and practice, enhance the right to speak, and promote and lead the technological progress and application of the whole industry.

Chapter 10

Governance of Blockchain Application



Yukun Cheng and Xiaotie Deng

Abstract The governance of blockchain is crucial for the stability and correctness of the blockchain system. With the continuous development of blockchain technology, the governance on blockchain extends to online and offline transaction contracts under the environment of smart contracts. Especially in recent years, the rapid development of blockchain applications in China and the increasing cross-chain transactions of information and assets between different blockchains also make cross-chain governance be put on the agenda. Therefore, this chapter will introduce the governance of blockchain from the perspectives of the off-chain and on-chain design. In particular, we focus on the economic incentive governance and IT technology governance for the permissioned blockchain systems, as well as the cross-chain design for the blockchain eco-environmental governance.

Keywords Blockchain · Governance · Consensus mechanism · Smart contract · Economic incentive mechanism

In the blockchain system, the generation of a new block needs verifications and confirmations from all distributed nodes. The stability and correctness of the blockchain system partly depend on the governance of blockchain. With the continuous development of blockchain technology, the governance on blockchain extends to online and offline transaction contracts under the environment of smart contract. In recent years, the rapid development of blockchain applications in China and the increasing cross-chain transactions of information and assets between different blockchains also make cross-chain governance be put on the agenda.

Therefore, for different blockchain systems such as public blockchain, consortium blockchain and private blockchain, the blockchain governance should decide whether to suspend, delay, modify or upgrade the system when the normal operation of the

Y. Cheng
Suzhou University of Science and Technology, Suzhou, Jiangsu, China
e-mail: ykcheng@amss.ac.cn

X. Deng (✉)
Peking University, Beijing, China
e-mail: xiaotie@pku.edu.cn

system fails. Online or offline governance can be adopted to introduce relevant system processing procedures to change the abnormal state of the system.

According to the difference of governance process, governance on applying blockchain can be categorized as on-chain and off-chain. The on-chain governance can be fully automated and efficient to complete the entire governance procedure, realizing the greatest transparency; while the off-chain governance can slow down governance decisions appropriately, pool wisdom, and complete governance decisions more reliably.

In recent years, blockchain technology has been widely used in all walks of life, including public service, justice, intellectual property, scarce resources, finance, logistics, education, health care, public welfare and philanthropy. Different industrial applications of blockchain have different advantages and governance needs. When the collaborative application is needed, the problem of cross-chain data integration and collaboration between different blockchains comes, and the cross-chain governance challenges of different blockchain architectures need to be solved.

The current blockchain ecosystem, in the process of evolution, is marked by decentralized blockchain and gradually expanded to a variety of multi-center or weakly centralized consortium blockchains and private blockchains. In such large-scale and multi-category application scenarios, it is extremely urgent to carry out effective, orderly, equitable and sustainable governance, including stable governance of system economics and IT technology governance of authority management.

10.1 Introduction

In the early stage of development, the management and control procedures upon which blockchain systems operated were largely determined by the automated consensus mechanism. The consensus mechanism could automate a stable operating world of digital token exchange without human intervention. This automatic and stable operating system has brought a subversive change to the economic and financial system management. Its simple governance system has become a typical example of digital economy transactions.

The main function of blockchain is to maintain a history of digital transactions that is hard to tamper with. The realization process of this function, mainly uses the one-way hash function in the calculation theory. The hash function is used to calculate the summary of the history record which would be put into the new block of digital transactions by the bookkeeper. By applying the hash function, an attacker's modification on any block will result in the modifications of all subsequent transactions data. This approach can be applied across different types of blockchains, so that it becomes the foundation of tamper-proof digital transaction history data for public, consortium and private blockchains. In particular, Wang Xiaoyun pointed out that "hash function is the original technology of blockchain, and the signature technology under hash function is blockchain technology" [1].

With the development of information science and technology, a number of distributed system algorithms have emerged, which effectively combine the basic concepts of blockchain with the actual social organization structure, becoming the technical basis for promoting the progress of social governance. It also provides the guiding principles of blockchain technology implementation and the fundamental framework supported by IT technology.

In such an automated system as blockchain, public key cryptography is also widely used in protocol design to discriminate the identity of each transaction trader and her corresponding rights and responsibilities of the bookkeeper. Blockchain technology can achieve anonymity, which can separate the identity of the “natural person” in human society from that of the “digital trader” in the blockchain system, and ensure the consistency of the identity of each “digital trader” in the system. At the same time, the incentive mechanism of blockchain technology for individuals or small groups can still play its part in economics. It plays a key role in the design of decentralized consensus mechanism.

Consensus mechanism is the key protocol in distributed system both in public blockchain and consortium blockchain. From the perspective of governance, consensus mechanisms can help to reach a mutually agreed decision when there are different opinions. In distributed systems, the consensus can be reached by simply broadcasting all new transactions which are collected by a fixed correct bookkeeper and validating all these transactions. However, when there are malicious bookkeepers in the system, or when the transaction information collected by multiple bookkeepers is inconsistent, it is too difficult to reach a consensus. The Proof-of-Work (PoW) mechanism in blockchain technology uses an economic solution to effectively achieve the consensus.

PoW consensus mechanism requires each bookkeeper to collect unrecorded digital transaction information and package it into a new block. The bookkeeper is required to input [accounting data | random data] into a one-way hash function. If the output of the hash function satisfies some conditions, then it is called that the bookkeeper solves out the hash function. Hence, in order to obtain the output results meeting the preset conditions, bookkeepers need to consume a lot of computing power to find a suitable nonce. In a blockchain system, multiple bookkeepers simultaneously look for the nonce to be a hash function solution. PoW consensus mechanism stipulates that the first one to solve the hash function wins the right to add his/her new block to the chain and broadcast it to others in the system. When the other bookkeepers receive the new block, they will check whether the winner’s new block is compliance, and if so, they will record the block in their local accounts. It can be seen that the more computing power the bookkeeper has, the faster the speed of finding a suitable nonce is, and the probability of winning the right to account, which is proportional to the amount of computing power, will also be greater.

We can also understand how PoW consensus mechanism works from the perspective of economics, where the behavior that the bookkeepers spend computing power to look for the nonce can be seen as they participate in an auction that requires some entry fee. When the entry fee meets certain requirements, the auction is completed. And

the winner of this auction will be randomly selected from bookkeepers participating in the auction in proportion to the fee paid by them.

This computation-cost design method is the economic basis for ensuring the correctness of blockchain and is the core of designing and implementing blockchain consensus mechanism, which greatly simplifies the implementation of distributed consensus mechanism.

Ethereum, Vitalik's pioneering design for the second generation of blockchain, directly extends the simple history of digital exchanges into Turing-complete computing for any possible digital processing, collectively known as smart contract. This expansion has greatly expanded the application of blockchain. In particular, applications in different environments, such as digital finance, Internet of Things, intelligent manufacturing, supply chain management and digital asset transaction, need to integrate the requirements of various laws and regulations into smart contracts to make them be a part of blockchain design. It poses new challenges to the formulation of corresponding governance rules. Smart contract not only expands the available scenarios of blockchain technology, but also puts forward new challenges and new ideas for the governance on applying blockchain. It also greatly increases the difficulty of correctness analysis of blockchain, putting blockchain application governance on the agenda of blockchain technology development.

Blockchain 3.0 is defined as the core of the Internet of Value, which is used to confirm, measure and store the property rights of the information and bytes representing value in Internet. Therefore, the Internet value assets can be tracked, controlled and traded on the blockchain. Zheng Zhiming evaluated blockchain 3.0 as the Internet of distributed value, believing that it will gradually grow into a mature digital economic infrastructure and provide the overall framework of a rules-based credible intelligent social governance system [2]. Many scholars also believe that blockchain 3.0 will become the most basic integrity protocol for the future construction of smart society, and blockchain application governance will provide the most important foundation for the successful realization of this goal. Difficulties that could not be effectively solved in the blockchain 2.0 era will be solved under the new framework of blockchain 3.0. At the same time, however, blockchain 3.0 has to face the challenges of effective governance across different economies, especially across different blockchains in the digital and physical worlds.

According to the development process of blockchain technology, the governance of blockchain application has gone through three stages. Each stage of governance expands the application capabilities of blockchain technology on the one hand, and also puts forward a richer set of tasks of governance that it needs to deal with on the other hand. To achieve the govern goal, we need to constantly innovate on-chain and off-chain technology design to achieve effective governance of blockchain applications.

10.2 The Off-Chain and On-Chain Design of Blockchain Application Governance

In sharp contrast to the traditional economy and even the digital economy, the emerging blockchain economy has changed the concept of traditional institutional governance in many ways. Since participants and decision makers in the public blockchain system can join and leave the system without permission, the correct elements of blockchain system governance must be based on the condition of the consistency of individual behavior. This feature changes our past understanding of institutional governance of economic activities, so that the blockchain application governance is needed to be designed and analyzed from different perspectives correspondingly.

10.2.1 *Blockchain Governance Scheme Different from that of Electronic Currency*

In the era of blockchain 1.0, Bitcoin continued the basic governance system of electronic currency, but its most unique and successful innovation is PoW consensus mechanism and the design of incentive mechanism for rewarding new bitcoin block. So it can achieve the governance of overall consistency of the blockchain system by the incentive scheme of individual interests.

Firstly, PoW consensus mechanism ensures time consistency through the use of cryptographic hash functions, and meanwhile ensures that the historical transaction data is difficult to tamper with. After each period of consensus, the system efficiently preserves the transaction data. In the governance of blockchain 1.0, modern cryptography technology has played a huge role in the successful implementation of consensus mechanism. Various cryptography technologies, such as hash function, one-way function, asymmetric cryptography system and zero-knowledge proof homomorphic encryption, have repeatedly appeared in the development process of blockchain at different stages. The one-way function method of cryptography enables PoW consensus mechanism to fairly and impartially select bookkeepers of blockchain distributed ledger. We can say that there would be no blockchain today without modern cryptography.

Secondly, how to achieve the common goal that all participants want to achieve through the efforts of each individual in the distributed system is one of the most important governance issues for the realization of the distributed concept of blockchain, namely the mechanism design problem. Blockchain 1.0 applies the design of incentive mechanism to the realization of consensus mechanism, which is a major innovation in mechanism design. An effective reward mechanism can promote each participant to take active efforts to achieve the common goal of the system. Meanwhile, it also solves the long-standing distributed computing problem to greatly improve the efficiency of consensus computing among large-scale distributed nodes.

The design and implementation of consensus mechanism and incentive mechanism endow the public blockchains with the super power to correctly execute instructions in a completely unfriendly environment. In the open execution environment required by public blockchains, it has a high requirement on consensus, which makes some more efficient consensus mechanism unable to be used. However, in consortium blockchains, the application of efficient consensus mechanism can meet the needs of consortium blockchains, which leaves a broader development space for the mechanism design of consortium blockchains.

10.2.2 On-Line Execution and Off-Line Improvement of Blockchain Governance

Due to the wide application of blockchain technology, the automatic operation system called “procedure as law” can be realized. In the era of blockchain 2.0, the implementation of the system depends on the consistent execution of the same program by all nodes, so as to ensure the complete execution of system instructions in a distributed environment. Online governance of the blockchain system entirely relies on “enforcement” programs, as well as the realization of incentive mechanism for all nodes and bookkeepers. To ensure the proper design and execution of “enforcement” programs, Ethereum has established a set of off-line procedures to determine modifications, updates and replacements of programs, which are promoted and executed by the bookkeepers and users, meanwhile trying to ensure that these nodes work and make decisions together, as well as accept their jointly determined future.

The DAO (Decentralized Autonomous Organization) mechanism on Ethereum is a good representation of this governance principle. Due to a minor error in the DAO master program, a large number of stolen assets were transferred to a separate account and isolated. Following the principle of “procedure as law”, some members of the community think the asset can belong to the account, while the other members think the system should roll back to the state before the asset was transferred. Both sides stuck to their own stand, resulting in the largest fork in the history of blockchain due to different governance concepts.

The current governance process of blockchain is implemented through modifying procedures. In the case of Ethereum, the off-line ecosystem of the blockchain is maintained by a founding team who is supported by bookkeepers, users and foundations. The Protocol ERC (Ethereum Request Comments) proposes that each open source community needs a system to handle the requests made by its members and adopt the requests. EIP (Ethereum Improvement Proposals) proposes the core protocol and rule to improve Ethereum, requiring that the final implementation depends on the consensus of the system participants on the Ethereum concept and the influence of proposals and leaders.

Another common type of blockchain governance scheme is a decision made by multiple votes of users and stakeholders. Such schemes accommodate the wishes

of the majority of members or assets and ensure the stability of the system. Online governance ensures the fast and automated operation of blockchain systems, while the necessity of offline governance can be attributed to the rule of impossibility of full automation. How to determine the boundary between online and offline governance can be one of the most basic issues in blockchain design theory. This issue is essentially related to Arrow's impossibility theorem [3] and is one of the urgent research issues in blockchain technology.

10.3 Economic Incentive Governance and IT Technology Governance for Permissioned Blockchain

The governance of permissioned blockchain has a long history, and it usually consists of private blockchains and consortium blockchains. Generally speaking, the blockchains established within enterprise groups or treaty organizations are mostly consortium blockchains. David Yermack [4] believed that "the use of blockchain technology within an organization to achieve corporate governance is a huge progress, which can be comparable to any significant corporate governance scheme since 1933 to 1934".

The governance of permissioned blockchains is closely related to the business logic of its application system. In the process of in-depth study about the application fields, the specific governance goals will generate from the influence of the business logic, ethical principles and politically correct regulations in the application. The governance of private blockchains can be carried out for enterprises funds, resources, orders and other relevant data.

The govern principles of consortium blockchains formed by enterprises in the same industry, especially those based on the Internet of Things in the upstream and downstream of commercial activities, are often determined by the established alliance relationship of business logic. In addition, the characteristics of blockchain itself, such as the property that is difficult to be tampered and the one to be consistent, can also be realized by various consensus mechanisms applicable to different alliances, including Proof of work (PoW), Proof of Stake (PoS), Proof of Authority (PoA) and so on. The differences of various consensus mechanisms are often hidden behind the consensus of smart contracts accepted by the system, and their functions can be replaced by the abstract models of smart contracts.

The permissioned blockchain system needs to confirm the online identities of participants and observe and analyze their on-chain behaviors for a long time. Therefore, responsibilities, penalties, and system regulations can all play a greater role in permissioned blockchains to meet the requirements of the system design and ensure the safety of the system.

10.3.1 IT Technology Governance of Blockchain Application System

Based on the design of proof-of-work (PoW) and incentive mechanism, blockchain adopts the incentive of individual interests to achieve the overall consistency of the system governance. The hash function method of cryptography technology is used to ensure that the historical transaction data of blockchain is not tampered with, and efficient data storage is realized through the consensus mechanism of each time period. Data-based governance in blockchain applications also draws extensively from a series of important methods in modern cryptography, including asymmetric public key system, zero-knowledge proof, multi-party computing for identity establishment and verification, authorization and supervision, decision making of consensus voting, supervision and audit and other governance technologies. These cryptographic techniques play important roles in the process of governance on digital individuals and alliances.

Blockchain technology provides a new methodology and technical means based on cryptographic information science in distributed system governance, in which the system governance scheme designed by incentive mechanism plays an important role. In the blockchain alliance composed of different enterprises in the same business circle, cryptography and incentive mechanism can be used to most common governance issues, such as the access rules of members in the private blockchains, as well as the supervision, coordination, audit, ruling and other permission assignments among members of consortium blockchains.

When the traditional distributed system governance scheme is digitalized, on the one hand, the use of information science and technology can promote the progress of business and technology together with the industry; On the other hand, using incentive mechanism and market design method can make enterprises mutual benefit, creating the atmosphere of cooperation and competition between enterprises, and realizing the safe and effective operation of consortium blockchains.

Integrity and transparency are the key elements to ensure fairness of permissioned blockchains. The widespread use of smart contracts provides the infrastructure for secure, immutable, and auditable application of permissioned blockchains, and ensures the authenticity of permissioned blockchain applications during implementation. In addition, from the perspective of application, smart contracts can be used to describe cryptography applications provided by IT technology, including confidentiality, integrity, transparency and security in the implementation of various applications [5].

In the era of blockchain 1.0 represented by Bitcoin, the theoretical design of PoW mechanism could have been completely realized by online governance in its logical structure. But in the early days of the bitcoin system, several IT missteps led to a fork in the main chain that needed to be artificially corrected. Tezos [6], developed by Arthur Breitma, is the real attempt to fully realize governance on the chain. Tezos aims to build a complete set of functions to prevent blockchain from splitting [7]. In recent years, this effort has also led to complete COQ validation of smart contracts

on Tezos [8], while various governance solutions on other blockchains have matured to some extent.

10.3.2 Governance of Permissioned Blockchain Economy System

The governance of permissioned blockchain is different from that of permissionless blockchain, it has more choices in consensus rules. In several permissionless blockchains, there also exist permissioned members participating in the implementation of the consensus mechanism. At the same time, the quality certification of the participants in permissioned blockchain is also a favorable factor to simplify the consensus mechanism and ensures the correct operation of the blockchain system. Even in the permissionless blockchain, there are elements of permissioned blockchain showing up in the governance, such as the core developers in Ethereum, who play a key role in offline governance, as in many permissionless blockchains. The consensus in permissioned blockchain is greatly accelerated by the quality certification of participants, making the consensus decision of the permissioned blockchain more efficient and reducing the waste of resources. Meanwhile, there are differences in governance among different permissioned blockchains, including differences between the roles of members in the decision-making process of enterprises, and differences in the final decision rights of all members in the decision-making process of functional committees, etc.

Hence, within relevant enterprises of specific institutions and industries, constructing the permissioned blockchain system by using private blockchain or consortium blockchain can greatly simplify the tasks of system governance through limiting the rights of participants in the system. The construction of digital currency item DCEP (Digital Currency Electronic Payment) [9] in China is such a prominent example. The design of DCEP is divided into upper and lower layers. The upper layer guarantees the production of digital currency through the People's Bank of China based on traditional currency, issuing and managing the data processing and ownership of DCEP at the national level and providing technical support. The lower commercial banks issue digital currency to commercial customers in the form of B2C according to traditional economic principles to provide digital currency to currency users in real economic activities. The transactions of real economic activities protect the privacy of users through IT cryptography technology, and can also combat economic crimes such as money laundering and fraud through traceability.

In the design process of DCEP system, the governance of its business logic directly connects with the traditional financial system, without any new financial and economic risks. In the realization, the primary problem that urgently needs to be solved in the design of this kind of digital currency is eliminated, thus reducing the design difficulty. In addition, the DCEP system is implemented using a mature

blockchain technology architecture without introducing new economic security assurance technologies.

Roughly speaking, blockchain technology can guarantee historical consistency and uniqueness of distributed ledger, but to apply it to national digital currency, it is urgent to establish and develop new technology to realize online and cross-border security governance of blockchain. For DCEP, commercial banks are not responsible for the operation of the digital currency system, but the technical team of the People's Bank of China is in charge of the system design and operation, which greatly reduces the safety risk of malicious attacks on commercial banks due to the use and management of digital currency transactions. From this point of view, DCEP has far more advantages over the public blockchain ecology than Bitcoin and Ethereum whose volumes and dynamic characteristics are constrained by the public blockchain ecology at the current.

Another kind of important digital currency is Libra, developed by Facebook, which also adopts architectures of consortium blockchain and private blockchain. In addition to the B2C advantage of its 2.6 billion user base, Libra's financial system governance design is built on three infrastructures: ① Ledger security and system scalability are ensured with blockchain technology; ② Provide traditional financial assets matching the level of real economic activities as the offline currency (mainly USD) support (similar to DCEP); ③ Governance is vested in the Libra Association coalition.

Libra's implementation of the technology system is divided into three main parts: ① Libra designed MOVE programming language (similar to blockchain general programming language GO) as the open source Libra core for smart contract design; ② Provide a system with its own library and establish a controllable permissioned blockchain economy system; ③ Establish the allied offline governance mechanism of Libra Association based on founding members in the early stage (plan to convert to public blockchain system in the later stage).

At the same time, Libra uses three steps to design a governance scheme from simple to deep for the initial stage of blockchain: ① A community of blockchain security verifiers is formed by the founding members to ensure their loyalty; ② With the maturity of the market and the reduction of speculators, Libra gradually turns to the PoS consensus mechanism, and uses the governance scheme that stable investors decide its development direction; ③ In the long-term competition, establish a governance mechanism represented by reputation right and mortgage right. We can use the above governance schemes to conduct equilibrium analysis and incentive design for the governance of Libra, a virtual cryptocurrency, and we can find that Libra's governance mechanism is consistent with the final theoretical results of the "economic scheme of all participants paying for the auction" of PoW consensus mechanism in Bitcoin.

So far, no other virtual currency has been successfully implemented like Libra's move from consortium blockchain to public blockchain. The theoretical basis of this transfer process is that there should be more and more dispersed rights and interests, which is the natural conclusion of the development of systematic dynamics in reality.

Whether it can turn the early design ideal into reality remains a difficult problem to be solved.

10.4 Cross-Chain Design for Blockchain Eco-environmental Governance

China's rapidly developing blockchain economy has brought about a variety of different needs, from underlying technologies, industry platforms to various practical scenarios of the Internet of Things, prompting the emergence of blockchains in different application fields. Before a global blockchain system is created, blockchains with different targets are constantly formed and developed to meet the personalized needs of different application scenarios. These individual blockchains with different objectives are integrated to form a large blockchain ecosystem. The advantages of individual blockchains applied to specific scenarios ensure the efficiency and success of the ecosystem. At the same time, the development of cross-chain technology can realize the complementary advantages between different blockchains. Before the emergence of cross-chain technology, data exchange and mutual transactions between different blockchains were very difficult, mainly due to the different choice of consensus mechanisms of different blockchains, the differences in their technical implementation, and accordingly, the differences in the design of governance schemes. Cross-chain technology has become one of the important methods to solve the data communication among multiple blockchains, which can help us link the scattered blockchains together and give full play to the advantages of each independent blockchain. However, whether cross-chain governance and single-chain governance synergistic development is still a difficult problem.

10.4.1 Cross-Chain Requirements for the Wide Application of Blockchain

In terms of the field of data governance and data development application governance, the blockchain approach presents a set of basic theories and analytical tools, and develops a route map for fundamental technical solutions. However, the emergence of various professional application blockchain has led to more and more isolated islands between the blockchains. Therefore, it is urgent to develop cross-chain technology for opening up the data of isolated blockchains.

Data market: In today's rapid development of data property rights, data circulation, data sharing, data economy and digital economy, the voice of guaranteeing the rights of data subjects is growing louder, including the right of informed consent, right of access, right of refusal, right of being forgotten, right of correction and other rights that should be enjoyed by the data subjects in the right of privacy of data

subject. The development of blockchain's transparent disclosure features, data security management and data privacy protection technology has become the foundation of a major challenge to protect the rights of data subjects.

Government blockchain: In the process of government services and corporate governance, data sharing is the key to data management. Traditional management systems need to balance the relationship between the distribution and privacy protection of data, and need to choose between solutions and restricted execution permissions. The introduction of blockchain technology into government services and corporate governance can better guarantee the correct and standardized use of data.

Social governance: The formation of the digital society enables the comprehensive application of data to quickly accomplish tasks that were difficult to achieve in the past. However, the accuracy of social data can be affected by various factors, resulting in data loss, artificial destruction or falsification into false information. How to eliminate fake data is one of the most important challenges in current social governance, and the tamper-proof blockchain technology can provide strong support to solve this challenge.

Stock trading blockchain: Aiming at the governance issues of enterprises and institutions, the introduction of blockchain technology into stock trading can increase the transparency of equity ownership, achieving low-cost management, more accurate recording and the preservation of transaction data.

The advantages of blockchain technology mentioned above can bring greater development opportunities for all kinds of practical applications, but also lead to more scattered data. The theory and technology of cross-chain unified governance can solve the problem of decentralized data well. However, it is a big challenge to unify the use of massive scattered data according to the consensus mechanism and incentive mechanism on the blockchain, so we should constantly update and develop cross-chain technology to solve this problem.

10.4.2 Cross-Chain Technology

The first application of cross-chain technology is asset transfer payment between different blockchains [10], which is a solution implemented through side chain. Back et al. transfer Party A's assets on the main chain A of one blockchain to Party B's account on the side chain B of another blockchain through side chain locking. The design of the algorithm is based on the double payment authentications scheme. Firstly, Party A's assets on the A chain are locked and the proof is sent to Party B on the side chain B. After the side chain B realizes the asset transfer, the proof of the assets payment is returned to the chain A, and then the chain A transfers the assets back to the side chain. There needs to be a buffer period in the above transfer process to avoid double spending problems. This basic framework of bidirectional embedding has reappeared as a basic module in other cross-chain designs since then and appeared in many similar cross-chain transactions.

The side chains used by the asset transfer payments between the blockchains mentioned above are usually private blockchains or consortium blockchains. At present, cross-chain data interaction is also realized through SPV (Simplified Payment Verification), which is mainly used for drive chain and hybrid blockchain [11].

Solutions of cross-chain technology for different blockchains make differences, but some cross-chain technologies aim to connect all blockchains. Service providers of DAPP (Decentralized Application) are often entrusted with many key technology research and development work to realize cross-chain connection transactions, including the challenges of serving for trustless and permissionless work. The continuous development of cross-chain technology can extend the single blockchain to multi-purpose application scenarios.

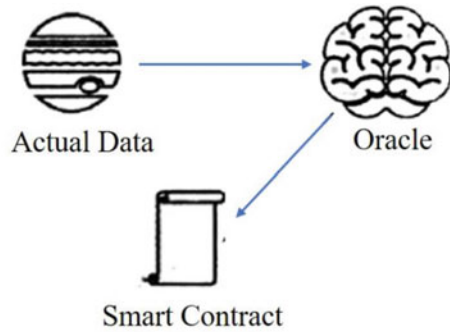
Permissioned blockchains are typically applied to specific scenarios, each of which has its own featured services and governance rules. However, a single blockchain system may lack some previously unknown blockchain resources in the application process. So, such a single blockchain system needs the assistance of other blockchains. Considering resources and cost, it needs to obtain resources from other blockchains through cross-chain collaboration. Therefore, the new governance requirements of blockchain ecosystem are proposed to realize through cross-chain technology.

Permissioned blockchains are particularly useful in application scenarios where decision objectives are clear, but when facing social application problems they as solutions are not necessarily able to predict all governance problems. At this time, the choice of cross-chain technology governance becomes one of the most convenient solutions. Different blockchains can focus on their strengths and perfectly implement them in specific domains. Cross-chain technology can connect blockchain with different resources, integrating their advantages to complete tasks that cannot be completed individually.

10.4.3 Oracle: A Kind of Blockchain Cross-Chain Technology

As mentioned above, the proliferation of blockchains in different application scenarios makes the on-chain and off-chain exchange of information and value between blockchains the norm. As a deterministic and closed system environment, blockchain has strict requirements on the historical consistency of internal data. Currently, blockchain design only focuses on the acquisition of data within the chain, for two main reasons. On the one hand, blockchain is separated from the real world. Blockchain cannot guarantee the authenticity of data in the outside world, and smart contracts executed by virtual machines have no network callers. On the other hand, the access to off-chain data is also unstable, and it is impossible to redesign the

Fig. 10.1 The execution process of oracle



blockchain's interface with external data every time. Thus, when the trigger condition of a smart contract is external information (off-chain), the oracle is a solution that can be used to provide data services. The on-chain and off-chain governance solution is beginning to become widely used through the input of real-world data into the blockchain by the oracle.

The Oracle is categorized into many types like software, hardware, human, computing, input/output, specific contracts and consensus, etc. But from a data point of view, each oracle is an interface to provide external data to smart contract. Such an interface, through the smart contracts with which the data is exchanged, can be widely used in the blockchain data interaction process under most existing architectures, which is also determined by the Turing completeness of smart contract. Figure 10.1 shows the execution process of oracle.

Oraclize, which was designed and implemented in 2015, began offering “service of proof”, an oracle service for smart contracts that provides proof of the authenticity of data off the chain. Ensuring that the provided data is not tampered with through the encryption algorithm has realized the required authenticity function for some data to a certain extent. The services include: access the API of Web site directly to provide the secure link of data transmission and realize the data authenticity of transmission process; improve overall system security through verification of authenticity through multiple technologies (and references); the proven data above is used for on-chain smart contracts to provide real data of nodes under public available distributed architectures; provide blockchain oracle services to reduce surface attacks. Oraclize focuses on building blockchain real data infrastructures, using consensus oracle to complete the whole process management of external data up-link. Among them, the incentive mechanism is combined with the oracle effectively, and the efficient operation of the oracle is realized through economic incentive. At present, in the competitive market environment, there have been a lot of oracles. When they are used in DEFI (Decentralized Finance), incorrect oracles will be exposed to the risk of arbitrage in the competition, so they are eliminated. While the oracles that can provide correct information will be encouraged by the positive incentivize to provide the correct data.

According to the different number of nodes, the oracles can be divided into centralized and decentralized ones. The centralized oracle can control the information provided to the smart contracts is unique; while the decentralized one can reduce risks and ensure the validity and accuracy of data. A decentralized oracle can also include multiple centralized oracles, on which market model-based oracles are generated. Just like a market maker in the Chicago futures market, the oracle needs to provide sufficient liquidity to the market through bilateral quotations, that is, when establishing the market price p , the oracle provides one unit of goods in the market and simultaneously p units of currency. In this way, both the buyers and the sellers who trust the oracle can participate in the transaction through it, thus ensuring the correctness of the quotation of the oracle. NEST, the decentralized price oracle network, has successfully built such a market on DEFI, with a unified oracle solution that can be implemented in a variety of trading markets.

10.5 Selection, Evolution and Prospect of Blockchain Governance Ecology

Blockchain application governance is mainly to solve the following problems: ① How to govern blockchain, and how to transform from the traditional sociological theory governance to be applicable to the automatic operation of blockchain application governance; ② How to make the implementation of blockchain technology in practical application scenarios take advantages to promote progress in social governance; ③ In a large number of blockchains (especially including many private blockchains and consortium blockchains), how to design cross-chain technology to connect different blockchain applications, using their high-quality digital resources to strengthen the social utility of blockchain.

We see that the governance ecology of blockchain is changing at different stages of its development. When various common consensus mechanisms and incentive mechanisms fail, the disposal process of blockchain application governance protocol on blockchain system in the abnormal state including decision-making team identification, selection and implementation of decision plan these three processes. Additionally, for different applications of blockchain, different risk control and regulatory measures need to be established.

What calls for special attention is that the governance of blockchain ecosystem is a key direction of blockchain application governance. In the prospect of the emergence and development of a large number of blockchain applications, especially in the ecosystem where consortium blockchains and private blockchains are widely used in social production and life, the design and implementation of side chain, cross-chain and oracle can maximize the expansion of blockchain application scenarios, but also bring new challenges to blockchain application governance. According to the current development direction of blockchain technology, blockchain application governance will focus on the interaction between designers, government [12] and

society, which will then become a key technical issue faced by the next generation of blockchain application governance.

References

1. Xiaoyun W. Hash function and blockchain technology. In: Blockchain technology and application science and technology frontier Forum, Shenzhen, China, 2019.
2. Zhi Z. Blockchain technology and development. In: Blockchain technology and application science and technology frontier forum, Shenzhen, China, 2019.
3. Arrow KJ. A difficulty in the concept of social welfare. *J Polit Econ.* 1950;58(4):328–846.
4. Yermack D. Corporate governance and blockchains. *Rev Finan.* 2017;21(1):7–31.
5. Mustafa MK, Waheed S. A governance framework with permissioned blockchain for the transparency in e-tendering process. *Int J Adv Technol Eng Explor.* 2019;6(61):274–80.
6. Goodman LM. Tezos---a self-amending crypto-ledger white paper. (02 Sep 2014). https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf
7. Gidcon LK. Inside the crypto world's biggest scandal. (19 June 2018). <https://www.wired.com/story/tezos-blockchain-love-story-horror-story/>
8. Bernardo B, Cauderlier R, Hu Z, et al. Mi-Cho-Coq, a framework for certifying Tezos smart contracts. (18 Sep 2019). <https://arxiv.org/abs/1909.08671>
9. Jie M. Opportunities, challenges and prospects of the central bank to implement the legal digital currency DCEP. *Economist.* 2020;3:95–105.
10. Back A, Corallo M, Dashjr L, et al. Enabling blockchain innovations with pegged side chains. (22 Oct 2014). <https://www.blockstream.com/sidechains.pdf>
11. Kyle. Five ways bitcoin can transfer between main and side chains. (20 Feb 2017). <https://www.jianshu.com/p/65b04ddb9f6>
12. Su Y. Government responsibility for blockchain governance. *Stud Law and Business.* 2020;37(4):59–72.

Chapter 11

Blockchain Application Evaluation



Xiaodan Tang

Abstract As blockchain applications spread across a wide range of industries, the evaluation of blockchain applications is playing an increasingly important role in deciding which projects to invest in, develop, or cultivate. In this chapter, a comprehensive hierarchy evaluation model for blockchain applications is proposed based on the ecosystem model presented in Chap. 3. Totally 16 factors respectively in technical, business and social aspects are examined and the blockchain-specific characteristics and suggestions for the evaluation are analyzed. Finally, a method on design and implementation of blockchain application evaluation based on the evaluation model are discussed for the reference of stakeholders such as investors, government sectors, blockchain supplier and users.

Keywords Blockchain · Blockchain application · Evaluation · Evaluation model

11.1 Overview

Blockchain has vast application prospects in financial services, supply chain management, intelligent manufacturing, and social services due to its characteristics of being distributed, anti-counterfeiting, tamper-resistant, transparent, trustworthy, and high reliability. Many enterprises and organizations have entered the blockchain industry and developed products, services, and solutions in domains ranging from infrastructures to industrial applications. In the market, a variety of distributed application services and products are emerging. The importance of blockchain applications in social production and life is growing, and some industrial applications are beginning to scale up. However, the blockchain industry is still in its infancy, and its applications may be immature and non-compliant. Exaggerating the functions of blockchain and speculating are common occurrences. Meanwhile, the planning and development of blockchain applications frequently lack systematic methodological guidelines, resulting in a lot of waste, uneven application quality, and risks.

X. Tang (✉)
China Electronics Standardization Institute, Beijing, China
e-mail: tangxd@cesi.cn

The Blockchain Strategy of German listed conducting technology assessments for new blockchain-based applications as one of its actions [1]. Since January 2019, The Cyberspace Administration of China implemented a recordation policy for blockchain information services including blockchain applications [2]. A systematic methodology for evaluating blockchain applications is significant support for the industry's sustainable development, both in terms of market cultivation and government oversight. It can be used to assess the capabilities that a blockchain application should possess, to facilitate the acquisition and use of a specific blockchain application product or service, and to provide reference information for assessing the level of blockchain applications.

Blockchain technology integrates distributed technology, consensus mechanism, encryption algorithm, smart contract and many other technologies, and its evaluation differs much from that of traditional information systems. Meanwhile, due to its broad application area, industry needs, business requirements, regulatory requirements, and technical requirements of applications in different sectors may vary significantly. Therefore, the evaluation of blockchain applications is complex, requiring consideration of not only related parties and technologies, but also external factors such as policies, administration systems, and technical standards.

There are a lot efforts related to the evaluation of blockchain applications. The "Rules for Evaluating Blockchain Systems" [3, 4] published by the Ministry of Economy, Trade and Industry (METI) of Japan covers 32 evaluation items in 13 categories divided into three main areas: quality, maintainability, and cost. The "Blockchain Technology Overview" report [5] from the National Institute of Standards and Technology examines a number of considerations when adopting blockchain applications, including data visibility and transaction per second (TPS), as well as the suitability of adopting blockchain solutions. In the China Blockchain Technology and Industry Development Research Report [6], 14 evaluation indicators under 3 dimensions of business, technology, and social effects are used to comprehensively evaluate blockchain applications. Fridgen et al. [7] proposed an 18-category evaluation framework for refugee management blockchain applications in Germany, including three domains: technology, functionality, and legality. Saito et al. [8] gave 21 criteria covering functional, performance, administrative and compliance dimensions. There are also a number of articles on the evaluation of certain indicators related to blockchain application systems, such as performance, information security and technical applicability [9–13]. However, comprehensive and universal evaluation methods for blockchain applications are still lacking.

11.2 A Hierarchy Evaluation Model for Blockchain Applications

Existing evaluation models for blockchain applications, including decision model, applicability criteria, maturity model, quality model, etc. [3, 4, 14], mostly focus on

the evaluation activities of one stage or one stakeholder. The concerns of a specific blockchain application can be different for different stakeholders, and the emphases may change as the stage of the application changes. In this respect, it's necessary to have an evaluation model which considers the evaluation requirements of all the stakeholders and ranging of all the stages of the blockchain applications.

Based on the application ecosystem model in 3.3, a hierarchic evaluation model for blockchain applications is proposed in this chapter, to provide comprehensive references for evaluation activities of all the stakeholders and throughout the whole life-cycle of the blockchain applications. The evaluation model is basically deduced through the mapping relationships between the application ecosystem and the evaluation factors which are connected by a set of application concerns. The product quality model and quality in use model for system/software in ISO/IEC 25010:2011 [15] are applied to blockchain applications to check the detailed technical and business factors.

As shown in Fig. 11.1, the blockchain application evaluation framework has a 3-layer hierarchic structure, with each level corresponding to one layer of the ecology model. The fundamental layer is the technical layer, which focuses on the requirements of blockchain applications and other information systems, and mainly refers to the quality of application system. The medium layer is the business layer, which focuses on the concerns of organizations related to the blockchain applications, and it's partly associated to the quality in use model. The top layer is the social layer, which reflects the environmental requirements of the blockchain application. The factors displayed in this model is not exhaustive, and the model is expected to be practical for identifying more detailed evaluation factors of blockchain applications in various sectors.

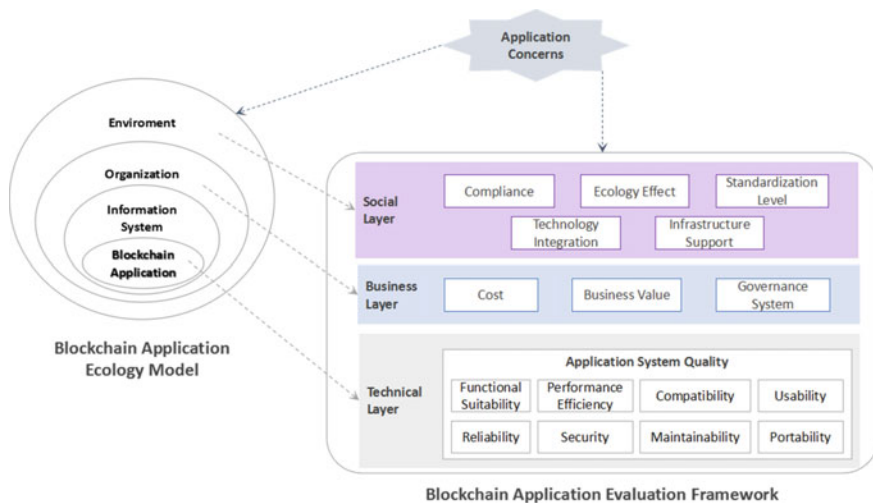


Fig. 11.1 Evaluation model for blockchain applications

11.3 Evaluation Factors

11.3.1 Technical Evaluation Factors

In the technical layer of the evaluation framework, the quality model in ISO/IEC 25010:2011[15] is applied in the context of blockchain applications. Some of the factors have no big difference from any other IT systems, while others need to involve blockchain-specific measures.

Functional suitability. One of the basic characteristics of a blockchain application is to include the blockchain-specific functional components completely and correctly, such as consensus algorithm, smart contract, crypto services, transaction system, ledger, etc. It's also a critical criteria to verify whether an application is really based on blockchain technology. The user and administration functional components, which are usually varied for applications in different industries or scenarios, should also be emphasized in the functional evaluation.

Performance efficiency. This factor relates to the amount of resources used under stated conditions, and includes time behavior, resource utilization, and capacity [15]. The performance efficiency is a bottleneck of blockchain, especially blockchain applications in scenarios requiring high-frequency transaction or storage of large amounts of data. Blockchain applications usually occupy more bandwidth and storage spaces due to its distributed architecture. And blockchain applications which use consensus mechanism like Proof of Work (POW), also need to consume large amounts of computing power. The most crucial metric of time behavior is the transaction throughput which can be represented by the TPS. Other metrics, such as network latency, scalability, storage resources and energy consuming, are also critical to the evaluation of blockchain application.

Compatibility. In terms of interoperability, a blockchain application may need to exchange information with other non-blockchain systems or other blockchain systems. In some blockchain applications, interoperability can also involve assets transfer. Oracle and cross-chain mechanism are among the technologies that can enhance the interoperability of blockchain applications.

Usability. A blockchain application should enable users to recognize the appropriateness of the application, support the conditions and resources for the user to learn how to use it [15]. This capacity is especially significant for those users who are not familiar with blockchain technology. Tutorials, documentations or a website which provide information on the applications are all useful for these requirements. Furthermore, it should also provide a friendly using environments like user interfaces, as well as be easy to access, operate and control.

Reliability. The elimination of single point of failure is a well-known advantage of blockchain technology, and the consensus mechanism can provide a relatively high fault tolerance. Blockchain applications are required to have a low frequency

of failure, with high availability when facing unforeseen events, such as node failure/cheating occurs, or network unstabilization. Another crucial metric is the length of time it takes to recover and update the ledger, as well as re-establish the application's state after the failure.

Security. Blockchain applications in many industries are associated with business data which should be confidential except for certain stakeholders. Access control is one critical approach to ensure the confidentiality of the blockchain application. Many early blockchain applications based on permissionless blockchain, such as Bitcoin, utilize an absolute anonymization design to enhance the confidentiality, and now a partial anonymization mechanism combined with authorization management is more common in applications based on permissioned blockchain. Blockchain technology is well recognized with benefits on data integrity, data consistency, and non-repudiation of ledger records, which is attributed to its designs on data structure and consensus mechanism. However, there are still security risks on various aspects, such as smart contract security, network security, cryptographic key storage, as well as threats to the traditional cryptographic algorithms from quantum computing, which should also be examined in the evaluation.

Maintainability. It's a common practice to use platforms such as underlying blockchain platform, application infrastructure and BaaS (Blockchain as a Service), as foundations when building blockchain applications. Also there are a lot of blockchain open source communities which provide underlying platforms, tools, and smart contract libraries. Pluggable technologies on consensus mechanism, cross-chain protocol, smart contract and cryptographic algorithm modular are increasingly mature. These are all ways to improve the modularity and reusability of the application systems. In terms of modifiability, a blockchain application should ensure smooth operation with modifications including system upgrade, fork, and smart contract changes.

Portability. The extension of blockchain applications often coexists with the growth of user size, and may bring business evolving. It's beneficial for a blockchain application to have the ability of adapting to environment evolving, as well as installability such as fast implementing. Meanwhile, the replaceability of various traditional business systems which may belong to different stakeholders should also be emphasized during the design and evaluation of blockchain applications.

11.3.2 Business Evaluation Factors

The business layer focuses on the achieving of business goals, as well as business model innovations. It includes cost, business value and governance system, which are usually more tightly bonded to various stakeholders around the blockchain applications. The business factors are supported by the technical factors, e.g., the security aspects of the technical layer should be emphasized to ensure the governance system.

Cost. The cost of a blockchain application includes but not limited to development cost, implementation and maintenance cost. The complexity of distributed applications and the scarcity of blockchain developers both lead to higher cost of blockchain applications comparing to traditional applications. Developing or implementing a blockchain application based on an existing mature underlying platform, such as an open source one, or a blockchain application infrastructure, is a common way to reduce the cost of blockchain application development.

Business value. Blockchain technology is well regarded to have the value of optimizing business processes, reducing transaction and interaction time, realizing automation, as well as enhancing trust and cooperation between organizations. However, all these benefits require the suitability of using blockchain technology. Therefore, it's significant to measure the business value while considering the necessity of using blockchain technology. The methods for measuring of business value vary for different industries or scenarios. In terms of necessity, there are many decision making models [16, 17] reported on judging whether the application of blockchain technology is recommended or not.

Governance system. Blockchain applications usually involve rich collaborative activities of many interested parties around the application systems, so the design and implement of governance systems is particular important for development of the consortium as well as operation and continuity of business. The governance of a blockchain application involves dimensions like data, protocol, and organization [18], and the solutions may cover on-chain, off-chain, and cross-chain aspects.

11.3.3 Social Evaluation Factors

The social layer of the evaluation framework focuses on the influence of the blockchain applications to the environment, which can summarize the realization of social responsibility and benefits.

Compliance. Early blockchain applications were often vague in terms of compliance, even utilized as a criminal tool in some situations, thus their compliance are more emphasized today by many governments. Meanwhile, the laws and regulations on blockchain applications are still under development in most countries, which makes the issues on compliance more complicated and gives more reasons to cautiously treat the compliance.

Industrial ecology effect. The industrial blockchain applications can serve as a trust foundation of the industry, and have the potential to enhance cooperation among businesses, as well as improve the supply chain. The industrial ecology effect factor is about the degree of improvement on industry collaboration relationships by using blockchain technology. It's strongly associated with the scale of the application, as well as the number and scale of the participated enterprises.

Standardization level. On the industrial level, standardization can promote the practical experience propagation and reuse, ensure the protection of the stakeholders' interests and rights, enhance interconnectivity between products, strengthen trust in the market, and hence increase the industrialization degree. From this perspective, a high standardization level is a strong plus point of a blockchain application. Furthermore, standardization is also required for the achievement of the long range prospect of blockchain technology, such as Internet of Value.

Technology integration. The integration of blockchain and other emerging information technology, such as cloud computing, big data, Internet of Thing (IoT), and Artificial Intelligence (AI) can realize functional complimentation, and is beneficial for fostering comprehensive industrial solutions and facilitating technology upgrade. The degree of technology integration can be evaluated especially in application scenarios with clear business requirements beyond capabilities of blockchain technology.

Infrastructure support. Infrastructures represent social overhead capital and sharing cost, and can support the economic and social development in many ways. Blockchain technology can play a role in infrastructures in many industries due to its data sharing and social trust mechanism, thus the infrastructure support is an important factor for evaluation the social effect of blockchain applications.

11.4 Application Evaluation Methods

The evaluation activities can be sponsored either by businesses who are planning to develop or purchase a blockchain application, or by government sectors or investors who are choosing the promising projects to invest or foster. The general evaluation framework given above is applicable to applications based on public blockchain, consortium blockchain and private blockchain in various industries. For the evaluation of a specific blockchain application, an indicator system is suggested to be deduced based on the evaluation framework combining with the characteristics and requirements of the industry. The measuring methods of the indicators can be automatic tools, experts assessment, and system test, etc. The output of the evaluation, which can be scores or rating systems, can be designed by the organizers in accordance with their goals on blockchain applications.

References

1. Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen. Blockchain-Strategie der Bundesregierung. 2019.
2. Cyberspace Administration of China. The Regulations on the Administration of Blockchain Information Services. 2019.

3. Information Economy Division, Commerce and Information Policy Bureau. Evaluation Forms for Blockchain-Based System. (12 Apr 2017). https://www.meti.go.jp/english/press/2017/pdf/0329_004a.pdf
4. Information Economy Division, Commerce and Information Policy Bureau & Ministry of Economy, Trade and Industry. Report on the Survey on Technology and Institutes Related to Distributed System. (23 July 2018). https://www.meti.go.jp/english/press/2018/0723_003.html
5. Yaga D, Mell P, Roby N, et al. Blockchain Technology Overview. (25 Oct 2020). <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>
6. China Blockchain Technology and Industry Development Forum. China Blockchain Technology and Application Development Study Report (2018). (18 Dec 2018). <http://www.cesi.cn/images/editor/20181218/20181218113202358.pdf>
7. Fridgen G, Guggenmoos F, Lockl J, et al. Developing an evaluation framework for blockchain in the public sector: the example of the german asylum process. In: Proceedings of 1st ERCIM blockchain workshop, 2018.
8. Kenji S, Akimitsu S, Mitsuyasu T, et al. Requirement analyses and evaluations of blockchain platforms per possible use cases. <https://arxiv.org/abs/2103.03209>
9. Wang S. Performance evaluation of hyperledger fabric with malicious behavior. In: International conference on blockchain (ICBC 2019). Springer; pp. 211–219. 2019.
10. Ismail L, Hameed H, Aishamsi M, et al. Towards a blockchain deployment at UAE university: performance evaluation and blockchain taxonomy. In: 2019 international conference on blockchain technology, 2019. pp. 30–38.
11. Fu Y, Zhu J, Gao S. CPS information security risk evaluation based on blockchain and big data. Tehnički vjesnik. 2018;25(6):1843–50.
12. Ye C, Li G, Cai H, et al. Security detection model of blockchain. J Softw. 2018;29(5):1348–59.
13. Lo S, Xu X, Chiam Y, et al. Evaluating suitability of applying blockchain. In: 2017 international conference on engineering of complex computer systems, 2017. pp. 158–61
14. Ricardo C, Mary S, Daniel A. A critical review on blockchain assessment initiatives: a technology evolution viewpoint. J Softw Evol Proc. 2020;32: e2272.
15. Systems and software engineering—Systems and software quality requirements and evaluation (SQuARE)—system and software quality models. ISO/IEC 25010:2011
16. Wüst K, Gervais A. Do you need a blockchain?. In: 2018 crypto valley conference on blockchain technology (CVCBT). IEEE; 2018.
17. Lo SK, Xu X, Chiam YK, et al. Evaluating suitability of applying blockchain. In: 2017 International conference on engineering of complex computer systems. IEEE; 2018.
18. Blockchain and distributed ledger technologies—Guidelines for governance. ISO/TS 23635:2022.

Chapter 12

Roadmap of Blockchain Standardization



Jianong Li and Xiaodan Tang

Abstract Economic globalization has further strengthened the strategic position of standards. Mastering the formulation of standards means mastering the discourse power of industrial development. As an emerging field, blockchain has been developing rapidly in recent years. From a worldwide perspective, blockchain standardization is still in its infancy. This chapter analyzes the requirements and value of blockchain standardization, introduces the development process of international and national standardization in China in the field of blockchain and distributed ledger technology, the latest trends of ISO, ITU and other international standardization organizations, the key direction of blockchain standardization work in China, as well as the implementation suggestions of blockchain standardization.

Keywords Blockchain · Distributed ledger technology · International standard · National standard · Group standard

At present, standardization organizations around the world have carried out a series of work in the area of blockchain standardization, such as organization construction and standard development, etc. In the next stage, the construction of a reasonable and coordinated standard system for the actual needs of the industry will become the focus of development.

J. Li · X. Tang (✉)
China Electronics Standardization Institute, Beijing, China
e-mail: tangxd@cesi.cn

12.1 Analysis of Blockchain Standardization Demand and Value

12.1.1 Analysis of Blockchain Standardization Demand

As a disruptive and innovative application model, the widespread application of blockchain has brought challenges while creating value, especially at this stage, the lack of core concepts and basic technical consensus in various industries has fragmented the industry development. The development of blockchain industry faces some practical problems, such as poor compatibility and interoperability of blockchain applications in the market, lack of standardized reference for blockchain application development and deployment, and lack of evaluation methods for security, reliability and interoperability.

1. Disorder of the industry

The technical design of blockchain was first proposed in 2008 by a scholar pseudonymously named Satoshi Nakamoto [1], and Bitcoin is the earliest practice of blockchain. In the process of blockchain development, due to the lack of popularization of concept and standardization guidance, people often equate blockchain with various cryptocurrencies represented by Bitcoin, and the blockchain industry is inevitably questioned. In addition, there is also a phenomenon of excessive hype and exaggeration of blockchain functions. Due to the lack of understanding of blockchain technology, it happens a lot that investors mistakenly trust some project parties about blockchain, and thus bearing unnecessary economic losses. Therefore, there is an urgent need to carry out standardization work in terms of terminology and classification to provide the necessary support for reaching basic consensus and regulating the development of the industry.

2. Characteristics of blockchain technology

Blockchain is conducive to the establishment of an open, transparent and reciprocal trust mechanism, a new type of business collaboration mechanism in different industries, and can be well applied in abundant fields. As a new technology field involving multiple fields, multiple types of technologies and multiple added values, the development of blockchain needs to be supported by high-quality standards, such as consensus mechanisms, distributed computing and storage, cryptographic algorithms, smart contracts, cross-chain and other key blockchain technologies whose innovation and implementation urgently need the guidance of standardization. Therefore, it is necessary to accelerate the development and release of key and urgent standards for blockchain technology research and development, system construction and interconnection, privacy protection, etc., to meet the actual demand of the technology industry and provide standard support for cultivating the blockchain industrial ecology.

3. Status of industry development

Blockchain has a wide application space in the real economy, public services and other fields, helps the model innovation of digital economy, and can provide effective support for accelerating the successive conversion of old and new dynamics and promoting high-quality economic development, with broad development prospects. However, the lack of standards to guide the implementation and landing of applications has resulted in insufficient openness to applications in various industries, which limits the technical and application innovation of blockchain. In addition, it should also focus on the role of blockchain in promoting data sharing, optimizing business processes, reducing operational costs, enhancing collaborative efficiency and building a credible system, and increase efforts to develop standards for convergence applications in digital finance, intelligent transportation, energy and electricity, intelligent manufacturing and other fields to support the creation of a blockchain application ecosystem.

12.1.2 Value of Blockchain Standardization

1. To unify the understanding of blockchain

At present, the industry and the general public have inconsistent understanding of the concept, characteristics and key technologies of blockchain, and there are even cases of misinterpretation and abuse of blockchain, which bring obstacles to industrial development. As the ISO terminology international standard defines the relevant terms [2], the standardization can promote the formation of a consensus on blockchain in the whole society, thus guiding the healthy and orderly development of the blockchain industry.

2. To promote the development of industry applications

The application scope of blockchain is very broad, and it has to meet the traditional industry habits and development requirements such as financial services and supply chain management, and especially needs to adapt to the existing rules and development direction of these industries. Standardization is conducive to regulating and guiding the application of blockchain in various industries and achieving integrated development.

3. To promote the resolution of key technical issues of blockchain and helps build a new ecology of technology development

For example, standardization can guarantee blockchain privacy and security and promote the development of safe, reliable and high-quality blockchain products and services by, for example, unifying and standardizing identity identification.

12.2 Development History of Blockchain Standardization

12.2.1 Development History of Blockchain Standard System

As a fast-developing emerging technology, the construction of early blockchain standard system adopted a market-oriented decentralized autonomous route.

Starting from the origin of blockchain technology in 2008, blockchain experienced the technical origin, validation stage and concept introduction and platform development stage within seven years until 2015 [3], but the standardization of blockchain was basically in a blank state, and there was a lack of basic consensus in the industry, and blockchain applications were chaotic, while the status quo of multi-platform development side by side brought serious interoperability problems, and blockchain system development, deployment, operation and security are lacking the necessary standardized guidelines [4].

In response to these problems, discussions on blockchain standardization have been hotly debated at home and abroad since 2016. Internationally, in July 2016, the World Wide Web Consortium (W3C), in a thematic meeting for blockchain, argued that blockchain needs standards to eliminate redundancy while promoting competition, while proposing that the key directions for blockchain standards are interface and data format standards, identification and authorization, and software licensing and sourcing, etc. In late August 2016, the advisory group meeting of ISO/IEC JTC1 in Ireland Dublin, made recommendations to JTC1 for the standardization of blockchain that included the establishment of a new subtechnical committee for this area. Subsequently, in September 2016, ISO established ISO/TC 307 (Blockchain and Distributed Ledger Technologies) to focus on the development of standards for blockchain and distributed ledger technologies to support interoperability and data exchange between users, applications and systems. International Telecommunication Union (ITU) initiated standardization work in the field of blockchain around 2017. SG16, SG17 and SG20 initiated standardization studies on the general requirements, security and other aspects of distributed ledgers, respectively. In addition, 3 blockchain-related focus groups were established for distributed ledger, data processing and management, and legal digital currency. The development history of blockchain standardization is shown in Fig. 12.1.

Meanwhile, major countries and regions are highly concerned about blockchain standardization. National Institute of Standards and Technology (NIST) released the research report “Blockchain Technology Overview” [6] to clarify the core features, limitations and common misunderstandings of blockchain technology in the context of standardization perspectives. The Institute of Electrical and Electronics Engineers (IEEE) initiated blockchain standards and project exploration in 2017, and has now established several blockchain standards. The European Union has focused on blockchain standards earlier, with the European branch of International Securities Association for Institutional Trade Communication (ISITC) and Organization for the Advancement of Structured Information Standards (Oasis) proposing 10

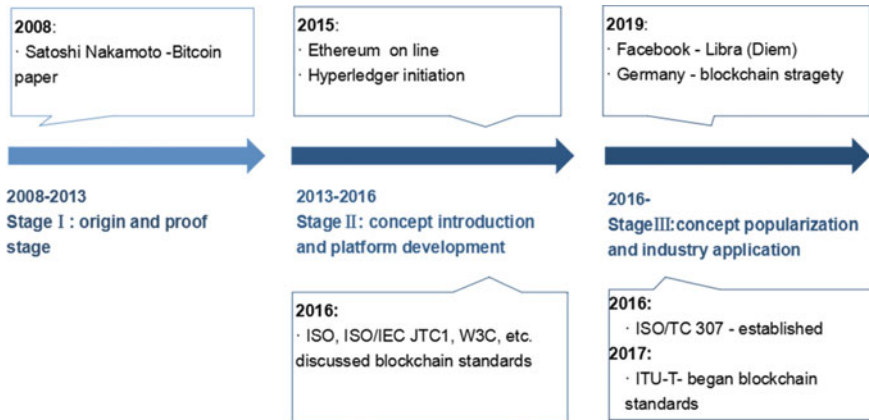


Fig. 12.1 Development history of blockchain standardization [5]

blockchain standards back in 2016. The European Telecommunications Standardization Association established the Permissioned Distributed Ledger Industry Specification Group in January 2019 to provide an analytical basis for managing the deployment of permissioned distributed ledgers across different industries and government agencies. The European Commission attaches great importance to blockchain standards and follows the activities of standard organizations such as ISO, ITU-T, IEEE, and W3C, and plans to translate the results of relevant international standards into EU standards. In 2019, the European Blockchain Observatory and Forum, established by the European Commission in cooperation with the European Parliament, published “Blockchain Scalability, Interoperability and Sustainability” [7], calling for the development of blockchain standards in directions such as interoperability. Germany emphasizes the role of standardization in the “Blockchain Strategy of the German Federal Government” [8], proposing the development of standards for data protection, product sustainability, etc., emphasizing the application and promotion of standards, while stressing that Germany will actively participate in the development of international standards and adopt open interfaces. Australia has paid high attention to blockchain standardization. Standards Australia released the Blockchain Standardization Roadmap in March 2017, in which several blockchain standardization priority topics were proposed; the Australian Department of Industry, Science and Resources in February 2020 published the National Blockchain Roadmap [9], which focuses on the areas of setting regulations and standards.

12.2.2 Standardization Institutions and Development Path in China

The standardization technical committee plays a key role in the development of standards. In September 2016, China Electronics Standardization Institute and other enterprises and institutions proposed a framework for China blockchain standards system in the “White Paper on the Development of Blockchain Technology and Applications in China (2016)”, which divides blockchain standards into five major categories, including foundation standards, procedure and methodology standards, credibility and interoperability standards, business and application standards, and information security standards, in consideration of process and method, trustworthiness and interoperability, and information security standards.

In order to strengthen the coordination of blockchain standardization work, China has established a national blockchain and distributed ledger technology standardization technical committee (SAC/TC 590), which is mainly responsible for the construction, management and maintenance of blockchain and distributed ledger technology standard system. SAC/TC 590 will further clarify the direction and development line of standardization work through the study of proposed policies and measures for standardization work in the blockchain area; strengthen the systemic and coordinated development of national standards in the blockchain area through the construction of the blockchain national standard system and the unified management of the standard plan.

Social groups such as academies, associations, chambers of commerce, federations and industrial technology alliances have been the main force in blockchain standards development for a long time. since 2016, various types of blockchain alliance organizations have been established in China, and several of them have made blockchain group standards development as their work content, and some of them have also set up standards working groups. since 2017, relevant social groups have cumulatively released dozens of blockchain group standards have been published, and system testing and other work have been carried out based on the group standards, so that the standard achievements can be implemented and promoted rapidly. At the same time, based on the research results of group standards, they have promoted the development of relevant national standards and industry standards, and even international standards.

12.3 Development of Blockchain Standardization

12.3.1 Development of Blockchain International Standardization

At present, two of the three major international standardization organizations - International Standardization Organization (ISO) and International Telecommunication Union (ITU) have been involved in development of blockchain standards.

1. Blockchain standards in ISO

As of February 2021, ISO/TC 307 has 46 participating members (P members) and 14 observing members (O members), and has established seven working groups in the direction of foundation, security and privacy, smart contracts, governance, use cases, interoperability, and one task force in the direction of auditing. Since 2017, ISO/TC 307 has accelerated the promotion of reference architecture, smart contracts, security and privacy, interoperability and other key standards development. As of February 2021, 14 ISO standard projects have been established, including terminology, reference architecture, taxonomy and ontology, use cases, data flow, etc., of which four standards have been published, including terminology and overview of smart contract interaction. In addition to ISO/TC 307, technical committees such as ISO/IEC JTC1 (Information Technology Committee), ISO/TC 68, and ISO/TC 46 (Information and Documentation Technical Committee) are also working on blockchain-related standards.

2. Blockchain standards in ITU-T

ITU-T launched blockchain standardization research work in 2017, established the Distributed Ledger Technology Focus Group, and started research in terminology, use cases, architecture, evaluation, security, and regulation, etc. Eight research results were completed and released in August 2019. In addition, ITU-T has also set up special subject groups in the 16th and 17th research groups, and the 13th and 20th research groups have also started international standardization work related to blockchain, and several projects are about to enter the submission stage.

12.3.2 Blockchain Standards in China

In China, the Standardization Law defines five types of standards with have descending implementation scopes, which are respectively national standards, industrial standards, local standards, group standards and enterprise standards.

As of June 2021, four national standards have been established, namely, reference architecture, smart contract implementation specification, depository application guide and terminology.

In terms of industry standards, a number of industry standards have been established in financial, judicial, communications, civil affairs, and cryptographic industries. The State Administration of Radio and Television released the “Blockchain-based Content Audit Standard System (2021 Edition)” in April 2021, in which 13 standards are proposed to be established.

China Electronics Industry Standardization Technology Association, China Software Industry Association and other blockchain-related organizations have developed and released a number of group standards. As of August 2020, there are 32 blockchain group standards publicly released on the national group standards information platform.

12.4 Key Directions of Blockchain Standardization

With the gradual attention to the development of blockchain industry in China, the standardization work will also step into a new level. Combining the work content and development direction of blockchain standardization-related organizations at home and abroad, the standardization work in the field of blockchain is recommended to focus on the following aspects.

12.4.1 Foundation

Foundation standards are the core of supporting the development of blockchain industry, mainly used to unify blockchain terminology, related concepts and models, provide support for the development of various other parts of standards, and ensure common knowledge and understanding of the main concepts in a particular standard. The main role of such standards is to recognize what blockchain is, how to define blockchain, and to distinguish blockchain technology from other related information technologies. The foundation category includes standards mainly for terminology, reference architecture, taxonomy and ontology. Currently, the international standard ISO 22739 [2] defines a total of 84 terms in the field of blockchain, reflecting the new understanding and new focus of blockchain technology from different countries, and providing a basic consensus for other international standardization projects to be carried out.

12.4.2 Smart Contracts

Smart contracts have long been widely regarded as the main feature of blockchain stage 2.0, and the gradual maturity of smart contract technology has enabled blockchain to integrate from a single digital currency application into various fields.

Blockchain applications in the fields of finance, supply chain, public welfare, government affairs, etc. are all run in the form of smart contracts in the platform. Compared to traditional contracts, smart contracts are more likely to generate logical loopholes due to irregular writing while guaranteeing non-repudiation, thus causing internal disagreements and affecting the consistency of the system. With the rapid development of blockchain technology, there is a need to develop relevant standards to guide developers in designing and building smart contract-related components, to provide a systematic description of the smart contract life cycle, and to standardize the process of writing, publishing, deploying and managing smart contracts, so as to enhance the application of the technology.

12.4.3 Use Case Development

As the industry continues to deepen its knowledge and understanding of blockchain, from the initial cryptocurrency to financial applications, as well as the current widespread use in scenarios such as government services, copyright depository, supply chain traceability, smart cities and smart medical care, the application situation of blockchain is developing from the small-scale verification to the wide-scale popularization stage, and its unique value gradually brings changes to various aspects of social and economic life. Therefore, it is necessary to develop application case-related specifications to integrate typical application cases of blockchain in various fields, i.e., to define the general framework, role model, typical business process, technical requirements and security requirements based on blockchain technology in specific application scenarios, to guide the development and implementation of applications and realize the sharing of experience.

12.4.4 Data and Asset Management

As a comprehensive and integrated innovation of distributed data storage, P2P network, consensus mechanism, cryptographic algorithm and other technologies, blockchain technology is naturally applicable to data and asset management because of its features such as multi-party consensus maintenance, traceable use and tamper-proof flow, which can build a credible value transfer network. By formulating relevant standards, it can clarify the security risks and threats of data and asset management based on blockchain technology, thus helping to avoid risks and at the same time guiding the establishment of a secure management system to safeguard data security and prevent privacy leakage through standardization.

12.4.5 Industrial Blockchain

In recent years, digital transformation in industry has become the main development direction. The distributed ledger, tamper-proof and traceable features of blockchain technology have been gradually applied to the intelligent evaluation of industrial equipment assets and asset securitization, etc., which have achieved certain economic and social benefits. The significance of formulating industrial blockchain standards is to create a sustainable application ecology in the industrial field, provide normative guidance and basic basis in government support and industrial services, and guide the integration and development of blockchain technology with the industrial field.

12.4.6 Cross-Chain Interoperability

As blockchain technology is increasingly applied in various industry sectors, a large number of independent blockchain systems are generated, and these independent blockchain systems need to exchange data with each other to maximize their value. With the increasing demand for interoperability between chains, it is necessary to accelerate the development of cross-chain interoperability-related standards for guiding the construction of blockchain development platforms, regulating and guiding the development of blockchain-related software, and realizing the interoperability of different blockchains. Cross-chain interoperability-related standards mainly include standards for development platforms, application programming interfaces (APIs), data formats, hybrid message protocols, and interoperability.

12.4.7 Governance

Compared with other information technologies, blockchain is still in the early stage of development, and it is particularly important to guide the standardization of its business model and organizational structure, etc. The significance of developing governance-related standards is to help organizations maximize the value of blockchain technology using a governance approach, regulate the duties and responsibilities of relevant roles, and reduce potential security and compliance risks of the system, etc. By providing a set of blockchain governance frameworks, it can assist managers in understanding and fulfilling their established responsibilities and improve the effectiveness and usability of blockchain governance.

12.5 Implementation Plan of Blockchain Standardization

It is foreseeable that blockchain standardization will enter a critical development period in the coming period, and the process of standard development and other work will be accelerated. Carrying out the standard development in the blockchain field is conducive to improving the technology level and promoting the technical progress and application landing of the whole industry. The standard implementation builds a bridge between the standard developers and users, which is a prerequisite for the users to understand the standard, master the standard and accurately implement the standard, and is an effective means to stimulate the vitality of the standard. Here are some suggestions for the implementation of standards in the field of blockchain.

Standard dissemination. The publicity and implementation of published standards is the basic link to ensure that the standards give full play to their functions. Blockchain is still in the early stage of development, and many related enterprises haven't invested enough resources in standardization, resulting in a lack of understanding of the published standards and lagging execution of the content of standards, which may affect business standardization and market share. Therefore, through timely, in-depth and thorough propagation, the published standards can be well implemented so as to regulate production, ensure safety and reliability and promote the orderly development of blockchain industry.

Application verification. Application verification is a key part of the implementation of standards, to verify the correctness and feasibility of standards. In the field of blockchain, develop measurement program and test cases about system security, reliability, compliance and other aspects based in reference architecture, system construction guidelines and other related standards, to promote the formation of standards- led industrial form.

Evaluation and improvement. Evaluate and improve the standard after application verification to ensure that the content of the standard can fully adapt to the actual development demand of blockchain. Summarize the application effect of the standard, draw on the demand for continuous improvement of the standard from different related parties such as government, enterprises and society, and improve, optimize and perfect the content and scope of use of the standard.

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 31 Oct 2008. <https://bitcoin.org/bitcoin.pdf>.
2. Blockchain and distributed ledger technologies—Vocabulary: ISO 22739:2020. 16 Jul 2021. <https://www.iso.org/standard/73771.html>.
3. Tang WH, Tang SH, Liu ZH. China Mobile internet development report. Beijing: Social Science Literature Press; 2020. p. 296–307.
4. China Blockchain Technology and Industrial Development Forum. China blockchain technology and application development white paper. (18 Oct 2016). https://www.sohu.com/a/224430559_680938.

5. Tang XD. Towards an aligned blockchain standard system: challenges and trends. In: Blockchain and Trustworthy Systems-3rd International Conference; 2021. P. 574–84.
6. Yaga D, Mell P, Roby N, et al. Blockchain technology overview. (25 Oct 2020). <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>.
7. Lyons T, Courgelas L, Timsit K. Scalability, interoperability and sustainability of blockchains. (6 Mar 2019). https://cdn.crowdfundinsider.com/wp-content/uploads/2019/04/European-Union-Blockchain-Observatory-and-Forumreport_scalability_06_03_2019.pdf.
8. Bundesministerium für Wirtschaft und Energie, Bundesministerium der Finanzen. Blockchain-Strategie der Bundesregierung. (18 Mar 2020). https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=12.
9. Australia government. The National Blockchain Roadmap. (1 Feb 2020). <https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf>.

Part V

Outlook

From a global perspective, blockchain has risen to a significant position in many countries' technology strategy. A solid basis of blockchain industry has been established and a broad prospect has been observed. However, blockchain is still in its early stages, with many unknowns in terms of technology, market and policies, as well as the need for more time for technical verification and experience accumulation.

Chapter 13

Key Issues of Blockchain



Xiaodan Tang

Abstract Blockchain has sparked passionate debates and even controversies. The “double-edged sword” aspect of technology is especially prominent in blockchain, and its uncertainty is extremely apparent. In this chapter, a few open questions about the nature and value of blockchain are discussed, with the aim of providing some ideas for understanding and grasping this technology.

Keywords Blockchain · Distributed ledger technology · Disruptive technology · Internet of value

13.1 Is It a Disruptive Technology?

Since Satoshi Nakamoto proposed the design of blockchain in 2008 [1], the technology has been developing rapidly, exhibiting disruptive characteristics, particularly in the application of cryptocurrency, also extending to more areas of the social economy, such as financial services, Internet of Things, supply chain.

Distributed Ledger Technology: Beyond Blockchain [2], a report released by the UK Government Chief Scientific Adviser, argues that “Distributed Ledger Technologies have the potential to be radically disruptive”. The Blockchain Strategy of the German Federal Government proposes that Blockchain technology is “a building block for the internet of the future”.

Disruptive technology is a term introduced by Clayton M. Christensen in 1997, referring to technologies that replace existing mainstream technologies in unanticipated ways [3, 4]. Disruptive technologies frequently begin in low-end or marginal markets, and are often initially characterized by simplicity, convenience, and low cost. They eventually replace old technologies, open up new markets, and create a new value system through constant improvement and perfection of performance and functionalities. For a long time, blockchain technology was only regarded as a supporting technology for cryptocurrency, but with the development of concepts like

X. Tang (✉)
China Electronics Standardization Institute, Beijing, China
e-mail: tangxd@cesi.cn

smart contract and consortium blockchain, it has progressively expanded its market and also created a new value system.

In terms of technology, blockchain has broken through the previous technology development track and opened up new technology domains, potentially altering the existing power structure, impacting the market patterns, and destroying and reconstructing the existing industrial ecology. In terms of application, blockchain has embodied significant permeability in its application and increasingly replaced traditional products in many industries as an alternative, exhibiting great development potential in many fields of social economy such as financial services, intelligent manufacturing, supply chain, public services, etc.

13.2 Blockchain and the Internet of Value [5]

The Internet of Value (IoV) is an emerging concept, an improved form of Internet that evolved from the Internet of Information (IoI) matured, particularly following the rise of the Mobile Internet. The interconnection of values such as money, contracts, and digital assets is a key component of the IoV. People will be able to transmit value on the Internet as easily, rapidly, reliably and securely as they do with information in the IoI era. The value attribute is added to the IoI eventually developing a new type of Internet that realizes both information and value transfer.

Broadly speaking, the IoV prototype can be traced back to the 1990s, when many financial institutions began to use Internet technology to expand their payment business, and models such as third-party payment, big data finance and online financial portals arose, and IoV-related industries represented by Internet finance continued to develop. The scope and degree of value interconnection has continuously risen, and the scale and functions of the IoV have had early development, particularly since 2010, with the rapid growth of Internet finance.

The emergence of blockchain has given the IoV a new development area and initiated a new stage. Before the introduction of blockchain, the IoV was in a very early stage, with a fragmented development model centered on a few intermediary institutions. Blockchain technology has the potential to facilitate the formation of a large-scale and universal IoV, and thus make it easier for the IoV to proliferate globally and injecting a new connotation.

The use of blockchain in various industries has derived a new type of value storage and delivery mechanism based on the IoI, which has accelerated the growth of the IoV. The use cases and models of blockchain in a variety of industries show that it can effectively boost the construction of IoV in terms of infrastructure, expand the user scale and reduce social transaction costs, and therefore is a critical technology for IoV's future development.

Through the development of a new type of social trust mechanism and the promotion of the application mode with highly generic value storage and value transfer mechanisms, blockchain is gradually triggering a fundamental change in the way value is transferred, as well as the way of social collaboration, which is critical to

the development of the IoV. Firstly, blockchain can serve as the infrastructure for IoV. Blockchain-based identity authentication can authorize value carriers, determine the safe and reliable transmission of value through encryption and privacy protection mechanisms, provide basic value transmission protocols in combination with consensus mechanism and other technologies, and thus offer a trust foundation and value transmission mechanism for IoV. Second, the deployment of blockchain lowers the threshold of IoV. More users in a variety of sectors, such as financial services, supply chain management and IoT, are incorporated into the IoV system as a result of the ability to realize assets digitization. This effectively expands the scale of users of IoV and increases its value. For example, blockchain has the ability to accelerate the process of financial inclusion by bringing more citizens from underdeveloped areas into the financial system, hence enhancing the value of IoV. Third, by realizing intermediation and other ways, blockchain can optimize the assets-related business collaboration mechanism and process, which can help to improve social transaction efficiency, lower social transaction costs and hasten the construction of IoV. For example, blockchain can save a significant amount of transaction costs in cross-border remittance on a worldwide scale. With the advancement of blockchain technology and applications, and the transition from blockchain 2.0 to blockchain 3.0, it's expected that the IoV's scale will gradually grow, its operation mode will innovate, and its impact on social production and life will gradually deepen.

13.3 Blockchain and Digital Economy [6]

According to G20's definition, the digital economy is a broad range of economic activities that include using digitized information and knowledge as the key factor of production, modern information networks as an important activity space, and the effective use of information and communication technology (ICT) as an important driver of productivity growth and economic structural optimization [7]. The trust mechanism provided by blockchain can promote more efficient and convenient collaboration among enterprises, push social division of labor and collaboration to a higher level, enable more effective sharing and allocation of social resources, lower social division of labor and transaction costs, and improve digital economy benefits. Furthermore, blockchain technology has the potential to profoundly transform numerous industries and assist in improving their digitalization levels, stimulating the development of new business models, and is expected to generate more social value through industry innovation.

Blockchain can facilitate the marketing of data elements. In view of data quality issues and a lack of guarantee of data asset rights and interests, blockchain can improve the quality and security of data by ensuring the trustworthiness, anti-forgery, anti-tampering and traceability of data through consensus mechanism, blockchain data structure and encryption algorithm. It can provide effective solutions for scenarios such as open government data sharing, data asset identification

and trading, as well as strong technical support for the data flow and effective data usage.

Blockchain can facilitate the improvement of the digital economy's ecology. With the growth of the digital economy, virtual space has gradually become one of the most importance places for people to engage in social production and life. However, obstacles related to trust issues exist almost everywhere, such as the difficulties in defining the identity of subjects in virtual space and tracking the behavior trajectory, online illegal criminal activities and dishonest phenomena Blockchain provides an technology-based trust mechanism that can serve as a solid technical foundation for the establishment and maintenance of multi-party collaborative relationships. Blockchain can also be used to track network behavior and collect credit. It also provides the required trust backing for numerous economic activities in virtual space, making it extremely valuable in the creation of a healthy digital economy ecology.

Blockchain can promote the innovation of digital economy models. The interaction between individuals, enterprises and other subjects, flows of factors, resource allocation, are increasingly frequent. The trend of real-time information interaction and accurate supply–demand matching has grown crucial, spawning a number of new business models such as platform economy, sharing economy and new retail. Blockchain technology can provide effective trust support for these new business models, and smart contracts can help to enhance the intelligence of related applications. Combing with another characteristics of blockchain technology which emphasizes a peer-to-peer cooperative production relationship, new models such as distributed commerce are emerging.

13.4 Blockchain and the Real Economy

The integration of blockchain with the real economy has become an important trend in many industries' development. The implementation of blockchain in the real economy has attracted the interest of many countries all over the world. In China, the Guidance on Accelerating the Application and Industrial Development of Blockchain Technology [8] highlighted blockchain applications in real economy. In the areas such as product tracking, healthcare, transportation and logistics, supply chain management, energy management, there are a number of blockchain application projects. The impact of blockchain on the real economy has begun to appear.

Blockchain technology has become an important grip for the deep integration of the digital economy and the real economy. The innovation in the integration of blockchain and the real economy is particularly active, and there are more use cases in product traceability, supply chain management and copyright protection, and other fields. Blockchain applications have also been explored in manufacturing, healthcare, transportation and logistics, commercial circulation and other industries.

Blockchain can serve as a foundation for credible industrial data sharing, a link for division of labor and collaboration within the industrial ecology, and an important carrier for industrial value circulation. It also plays a significant role in product and

service quality improvement, supply chain optimization and industrial model innovation. The application of blockchain in the real economy can be combined with the Internet of Things (IoT), edge computing, artificial intelligence and other technologies, which can improve industrial digitization and facilitate the cultivation of smart industries. In agriculture, blockchain-based anti-counterfeit traceability of agricultural products can connect farmers, sellers, consumers and other related parties, ensuring the safe supply of agricultural products and the safe use of consumers through sharing data on production, circulation and testing of agricultural products that can be traced throughout the process. In forestry, blockchain technology can be used to realize the entire life cycle management of forestry resources such as seedlings, as well as to strengthen the management of afforestation funds, etc. In manufacturing, blockchain can be used in industrial collaborative manufacturing, supply chain, information sharing, industrial security and supervision, and collaboration of internal resources involving the integration and flow of various industrial production factors such as data, capital, technology, as well as interconnection between industrial equipment, production and data between enterprises. In Industrial finance, blockchain provides effective solutions for management and transaction of physical assets and supply chain finance, which can effectively reduce the financing cost of small and medium-sized enterprises in the real economy and assist the innovative development of industrial finance.

However, blockchain has yet to establish large-scale commercial applications in the real economy. The applications are rarely related to core business, and most enterprises are still waiting to see the effect of blockchain technology. First, the level of informationization in some real economy industries is insufficient to allow large-scale blockchain applications. For example, in many regions of the world, there are few information infrastructure and information system applications that can realize data collection, transmission, storage and sharing in agriculture, and blockchain applications typically require linking multiple enterprises' information systems, making them more difficult to implement. Second, the threshold of application transformation is high in manufacturing, commerce and other real economy industries, due to the long industry chain, complicated infrastructure and business systems, and the application scenarios are yet to be clarified. For example, in manufacturing, the differences in equipment, processes, protocols and networks are significant, and the application of blockchain may necessitate a large transformation of the original system. Additionally, the scenarios in manufacturing are mostly large-scale scenarios with difficulty in data collection and high data storage and transmission requirements, while the current support of blockchain technology for large-scale applications is still limited. Finally, the key to a blockchain application is multiple related parties' willingness to share their data and resources, while current organizational forms still fail to keep up with the needs of application development, and the lack of mature privacy protect solutions for on-chain data causes related enterprises to be more cautious in promoting blockchain applications.

13.5 Blockchain and Social Governance

Blockchain can help promote new mechanisms for social cooperation, address equality through social empowerment, and improve governance efficiency while also lower governance costs and risks [9, 10]. The value of blockchain in helping modernize the national governance system and governance capacity has been further highlighted in recent years, with the accelerated application of blockchain in the fields of government data sharing, judicial deposition, people's livelihood, environmental protection and international trade. In China, many government departments in cities such as Beijing, Chongqing, and Tianjin have implemented cross-departmental government data sharing exchange based on blockchain, which has proven to be effective in streamlining public workflow and improving administrative efficiency. The Supreme People's Court and the Internet Courts have developed blockchain-based blockchain platforms to enable electronic evidence data sharing and administration among courts, as well as between courts and judicial expertise centers, notary public offices and other institutions. The Supreme People's Court has clarified the legal validity of data on the blockchain as electronic evidence in documents such as "Provisions on Several Issues Concerning the Hearing of Cases in Internet Courts", "Provisions on Several Issues Concerning the Online Handling of Cases in People's Courts", "Rules for Online Litigation in People's Courts" and "Opinions of the Supreme People's Court on Strengthening Blockchain Application in the Judicial Field". The application of blockchain in the field of people's livelihood is highly active in food traceability, social welfare, precise poverty reduction, social security, education and medical care, etc. The advent of blockchain enabled multiparty governance, sharing and win-win situation, all of which have helped to protect and improve people's livelihood.

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. 31 October 2008. <https://bitcoin.org/bitcoin.pdf>
2. UK Government Chief Scientific Adviser. Distributed Ledger Technology: beyond block chain. 2016.
3. Christensen CM. The innovators dilemma: when new technologies cause great firms to fail. Boston: Harvard Business School Press; 1997.
4. Jing XX, Suo XW, Geng YF. Review and revelation on disruptive technology development. Natl Def Sci Tech. 2015;36(3):11–3.
5. Zhou P, Tang XD. Blockchain and construction of internet of value. Inform Secur Commun Privacy. 2017;7:53–9.
6. Tang XD. Opportunities and challenges of blockchain to facilitate the development of digital economy. Sci-Tech Fin. 2020;6:34–7.
7. G20. Digital Economy Development and Cooperation Initiative. 2016.
8. Ministry of Industry and Information Technology, the Office of Central Cyberspace Affairs Commission. The Guidance on Accelerating the Application and Industrial Development of Blockchain Technology. 2021.

9. Gao QQ. A preliminary study of the intelligence revolution and national governance modernization. *Soc Sci China*. 2020;7:81–102.
10. Yu YX, Zhang YG. Blockchain provides technical support for the modernization of national governance system and governance capacity. *Shanghai J Econ*. 2020;1:86–94.

Chapter 14

Trends of Blockchain



Xiaodan Tang

Abstract As an emerging technology, blockchain is developing rapidly, and has gained much achievements. However, it's still full of uncertainty. In this chapter, the characteristics and trends in industrialization, technology, application and industrial ecology aspects of blockchain are analyzed, to provide some insights for foreseeing blockchain development in the future.

Keywords Blockchain · Industrialization · Industrial ecology · Technology system

Currently, the global markets are experiencing a serious economic recession. Global trade is slowing down, and investment, consumption and exports are being greatly affected. The global economic situation may cause a contraction of blockchain technology investment and application market. The limited market resources will probably flow to more powerful large enterprises, posing greater challenges to small and medium-sized blockchain enterprises. At the same time, the economic downturn has made many businesses more hesitant about the layout of new technology, potentially affecting the industry' driving force.

In the long run, blockchain technology is expected to provide a solution to cyberspace's trust and security challenges, as well as an optional technology for Central Bank Digital Currency (CBDC) [1], and allowing the Internet to shift from sending information to transmitting value. Its importance for economic and social development has been realized by many governments and businesses, and it could become one of the most competitive technology tracks in the next years. China issued the Guidance on Accelerating the Application and Industrial Development of Blockchain Technology in June 2021. The US Senator introduced the "National R & D Strategy for Distributed Ledger Technology Act of 2022" in April 2022, aiming to promote the development of a national blockchain strategy. The concentration on blockchain technology by the governments of the two major economies is anticipated to be a substantial stimulant for the development of blockchain technology in the coming period.

X. Tang (✉)
China Electronics Standardization Institute, Beijing, China
e-mail: tangxd@cesi.cn

14.1 Blockchain Industrialization

From the standpoint of industrial evolution, blockchain is experiencing a process of breeding and gradually industrializing from the original software industry. A series of blockchain products have been gradually developed based on the initial technological innovation, including application solutions in the fields of product traceability, data sharing, supply chain management, evidence deposition and public services, as well as platform products like the blockchain underlying platform and BaaS. A great number of blockchain businesses, including traditional IT enterprises, Internet enterprises and blockchain startups, have been incubated. Many traditional industrial businesses have also increased their blockchain R&D and application. Meanwhile, industrial support, such as related talents, infrastructure, technical standards and industrial services has been accelerated.

From the standpoint of market incubation, the blockchain market has expanded significantly in recent years and has enormous potential for future market growth. According to a report released by Grand View Research in February 2022, the global blockchain technology market size was valued at USD 5.92 billion in 2021 and is expected to grow at a compound annual growth rate of 85.9% from 2022 to 2030 [2]. In China, the consortium blockchain market is developing rapidly. According to the blockchain filing data from the Office of Central Cyberspace Affairs Commission, more than 1000 blockchain projects have passed the filing procedure. Furthermore, several blockchain applications are steadily expanding in scale, and their effectiveness in terms of social and economic benefits has been highlighted.

From the standpoint of government direction, there is a global tendency to promote the growth of blockchain as a strategic emerging industry. With the innovative exploration and application of blockchain technology in many industries, governments all over the world are becoming increasingly interested in blockchain technology, and supporting it through policies, funds and pilots to capture the opportunity of blockchain technology and industrial development. The number of countries who have national blockchain industry policies is increasing. At the same time, governments are gradually distinguishing between prudent regulation of cryptocurrencies and encouragement of blockchain technology development. With the continued expansion of the industry, various nation's policies are expected to reinforce the layout, support the integration of blockchain with the real economy on a larger scale, and accelerate the growth of blockchain industry scale.

14.2 Technology Moves Towards Systematization

The technologies supporting blockchain are getting more systematic and diverse, however the core technologies still require improvement. The understanding of technologies such as blockchain and distributed ledger technology are gradually reaching consensus, and the advancement of these technologies continues to push past previous

boundaries. The evolution of related concepts also represents the future development direction and characteristics. Meanwhile, the underlying technologies of blockchain are continually evolving. While the fundamental technologies of consensus mechanism, data storage, privacy protection and smart contract are constantly developing, technologies like partitioning and cross-chain are also speeding innovation and development to assist blockchain technology to adapt to wider range of application scenarios. On the flip side, blockchain is still not mature enough in terms of performance, privacy protection, governance, and cross-chain interoperability. It's not yet advanced enough to carry enterprise-level applications in many sectors, especially in terms of performance and privacy protection, and the existing technology level is insufficient to enable large-scale applications in many domains. Due to storage volume and throughput limitations, blockchain requires more technical transformation and breakthrough when dealing with specific business applications, while the legal basis of smart contract technology, as well as security and privacy protection technology, are currently among the bottlenecks limiting the development of blockchain applications. The optimization and iteration of core technologies will continue to be a priority in the future years.

14.3 Applications Begin to Scale

The discovery of blockchain applications in many industries has intensified in recent years, with application fields expanding and the integration with the real economy strengthening. The application of blockchain technology aids in the digitalization of several industries, the cultivation of new business models, and even the realization of industry innovation. Blockchain is gradually becoming a significant support for the development of digital economy due to its increasingly important role in social-economic development and social governance enhancement. It's expected to be widely used for the scale coordination of human activities, especially with the arrival of blockchain 3.0 era, and is predicted to progressively evolve into the infrastructures of the digital economy. In China, many blockchain application infrastructures has been encouraged by municipal governments, and a large number of applications such as “blockchain + government” and “blockchain + people's livelihood” supported have been implemented, which will promote the growth and interconnection of blockchain applications.

However, blockchain applications as a whole are still in their infancy, with few large-scale industrial applications. In many scenarios, the business collaboration model between related parties cannot be well established, limiting the development of applications. Furthermore, due to complex scenarios and high replacement costs, there are still limited blockchain applications in several critical areas, such as industrial blockchain. The key to future blockchain industry rivalry from a global perspective, will be to achieve scale and effective applications in critical areas of economy. The introduction of supportive industrial policies and the establishment of regulatory system have established a favorable environment for the development of blockchain

applications. It is foreseeable that blockchain applications will enter an unparalleled period of development chances, and more large-scale applications will be cultivated to realize further release of the value of blockchain technology.

14.4 Further Development of Industrial Ecology

Blockchain innovation and entrepreneurship are thriving, and the industry's development ecology is improving. Mainstream financial institutions, IT enterprises and technology start-ups are currently exploring and promoting the development of blockchain technology and applications, driving a new wave of technology innovation and entrepreneurship. The future industrial development ecology will help to improve the level of collaborative innovation, reduce technical and market risks, strengthen the rationality of industrial layout, and promote the benign development of blockchain applications. In terms of standardization, the demand for standardization in terms of basic terminology and architecture, security and privacy protection, interoperability and governance has become prominent. Standard development organizations around the world are actively promoting the development of blockchain standards, and the quality of products and industrial services is continually improving. Relevant businesses have launched industrial services such as blockchain planning and consulting, testing, evaluation and talent training, as well as accelerated the construction of relevant industrial service platforms to provide the necessary industrial resources for blockchain enterprises. However, the present blockchain standard system and the blockchain industrial service system are still in the early stage of development. Providing strong development support via the creation of standardization and industrial service system, as well as continuously increasing overall competitiveness, will become an essential avenue to promote blockchain industry growth in the future.

References

1. PWC. Global CBDC Index and Stablecoin Overview 2022, 2022.
2. Grand View Research. Blockchain Technology Market Size, Share & Trends Analysis Report By Type (Private Cloud, Public Cloud), By Application (Digital Identity, Payments), By Enterprise Size, By Component, By End Use, And Segment Forecasts, 2022–2030. (16 June 2022). <https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market>.