JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 223-235 (2023)
DOI: 10.6688/JISE.202301_39(1).0013

Research on Secrecy Law Based on Blockchain Encrypted Traceability Technology

XIAFEI YAN+ AND XU ZHENG
School of Fujain Police University
Fuzhou, Fujian, 350000 P.R. China

With the large-scale application of blockchain technology, especially the deep integration of blockchain technology into the administrative and judicial systems, many legislative provisions re-enter into force in the form of codes, and its technical logic and market logic are preset. The company's values pose a series of unconventional risks and challenges to the existing legal system, which determines the inheritance and breakthrough of blockchain legislation to the existing legal framework. In this paper, the existing part based on encryption traceability technologies, such as blockchain, are analyzed and studied from a technical point of view, and the traceability technology is simulated and experimentally analyzed, which can better reflect the importance of corresponding laws.

Keywords: blockchain, data traceability, secrecy law, smart contract, homomorphic encryption technology

1. INTRODUCTION

In recent years, the rapid development of exports in various countries has brought many problems. Including intellectual property rights, counterfeit goods, logistics and transportation, information security, *etc.*, it is difficult to solve the traceability problem of cross-border e-commerce products with existing technical capabilities. All countries have formulated corresponding laws and regulations to regulate safety issues. An important part of this technology is to solve the traceability problem of cross-border products by the emergence of blockchain technology. The traceability system of products in cross-border electronic commerce can be established from the industrial chain of production, processing, transportation and consumption.

Blockchain and other new technologies follow a three-stage rule: the first stage is driven by interest. The leading creators and audiences are laboratory technicians, and seldom involve business values, laws and regulations. The second stage is business-driven. After the new technology shows its commercial potential, investors and speculators have followed suit. The lagging supervision leads to a lack of supervision in the emerging market. The third stage is rule-driven. After the market is stable, both enterprises and governments standardize relevant technical standards and social applications [8, 9].

In modern cryptographic systems, cryptographic algorithms, cryptographic protocols and key management are three indispensable parts, and among these three, cryptographic algorithm is undoubtedly the core. Although the practice has proved that most security vulnerabilities are generated during the process of implementation and deployment, the security of the algorithm directly determines whether the foundation of a remote system is secure [10, 11]. For example, using unsafe algorithms such as SHA-1, MD 4,

Received May 29, 2021; revised November 22, 2021; accepted May 6, 2022.
Communicated by Carlos E. Montenegro.
+ Corresponding author: yanfei010156@163.com

MD 5, RC 4, RSA, *etc.*, and the critical length is less than 2048 bits, it is impossible to realize a secure cryptosystem. Thus, the secrecy laws and password laws promulgated by various countries have their implementation effects.

Passwords are divided into core passwords, common passwords and business passwords. Core passwords and conventional passwords are state secrets, while retail passwords protect information that is not a state secret. Therefore, in common applications, business passwords have been widely promoted. Therefore, in practice, when "state secrets" are mentioned, each country's own domestic business password algorithms are often used as the default.

Fig. 1. The cloud pipe end of industrial internet security.

Industrial Internet security is an indispensable part of industrial information security, and the development of the industrial Internet urgently needs the synchronous application and development of passwords. Passwords can avoid the back door. By using cryptographic technology, people, software and hardware, process and so on Can be trusted to ensure that there is no back door. The identity of the future needs to be authenticated when it is connected, and the identity of the sender needs to be shown when the end executes important instructions; "pipeline" can be understood as a communication channel. The data collected by the end is sent out, the platform transmission needs to be encrypted, and the platform also needs to be encrypted when sending data to specific actuator; "cloud" can be understood as a platform, and the security policy of the platform needs a password protection.

In this paper, the existing part based on encryption traceability technologies, such as blockchain, are analyzed and studied from a technical point of view, and the traceability technology is simulated and experimentally analyzed, which can better reflect the importance of corresponding laws.

2. RELATED WORK

Blockchain refers to a series of data records with time stamps managed by a computer cluster that does not belong to any single entity. The whole data network has no central authority, because it is a shared network and its information is open to all. The problem of cross-border logistics can be solved through blockchain technology. The logistics of cross-

border electronic commerce products mainly passes through postal parcels, cross-border logistics and memorial lines, while the construction of international express delivery and overseas warehouses is relatively slow. There are many difficulties in the traceability of cross- border logistics [16]. With an efficient and safe operating system, the whole blockchain is a data storage point, which can optimize the whole cross-border logistics and find a more suitable path. It can solve the problems of high cost and slow speed of cross-border logistics at present, and then determine which link has the problem and track the responsible person.

Cross-border product quality problems can be solved through blockchain technology. After many years of export development of cross-border electronic commerce, the quantity and value of products have increased rapidly, but the quality problem of product have also been exposed. The main reason is that most cross-border e-commerce export companies have no brand awareness, and foreign trade companies that have grown up with OEM orders cannot form competitive international brands by competing at low prices. Some cross-border export companies have grown up on the Taobao platform, over-pursuing sales, and product quality cannot be guaranteed. It is difficult to unify the standards because the product quality of cross-border commodity export companies is not uniform. Cross-border product are difficult to return and exchange, enterprises consume a lot, and products they sell cannot be traced back. The most fundamental reason is that foreign consumers can not accurately grasp the product information, and it is also difficult for domestic merchants to recourse, and the responsible person cannot be confirmed. Therefore, by using the time stamp technology of the blockchain, cross-border export companies can verify each links with problems and find out the responsibility of each node according to the records of different times and the transparency and invariance of the blockchain technology. Man. From the raw materials to semi-finished products and finally to finished products, every link can be traced back. Whether government regulatory agencies or cross-border export companies can obtain product quality composition information, they can find the nodes of product quality problems.

3. RESEARCH ON SECRECY LAW BASED ON BLOCKCHAIN ENCRYPTED TRACEABILITY TECHNOLOGY

3.1 Classification of Blockchain

Blockchain anti-counterfeiting technology makes it less and less possible to tamper with various types of data of products [1-3]. By recording the whole product data and transaction data from the source, it is possible to build a product traceability and anti-counterfeiting system by using blockchain technology. The transaction process style can also be verified through various intermediate institutions, especially the traceability tracking of logistics information, forming a traceability and anti-counterfeiting system for the whole process of production, sales, and consumption.

The regulation of blockchain can be divided into two parts: blockchain-related law and blockchain-specific law. On the one hand, this regulation continues the existing network law system, which is reflected in the individual legal norms of each sectoral law in the existing legal framework that regulates blockchain through individual cases, and the

new blockchain-specific legislation is bound by the higher norms and legislative principles of the existing network law. On the other hand [4], blockchain can guarantee the efficient flow of production factors and assist in the implementation of laws, and the potential multiple risks and challenges in its application determine that the relevant legislation and regulation must break through the established legal framework.

Blockchain technology has developed rapidly and gradually materialized from the concept, and the actual blockchain technology has become more and more mature, showing diversity, specifically divided into three frameworks: public blockchain [5, 6], private blockchain, and federated blockchain. The following table shows the comparison of the three blockchains in terms of participants, trust consensus, centralization, and carrying capacity, and it can be found that the advantages of the coalition chain in terms of throughput rate are obvious.

Table 1. Blockchain classification.

	Private chain	Alliance chain,	Public chain
participants	Individual or company	Business or organization	Free for anyone to go in and out
consensus mechanism	Self-endorsement	Collective endorsement	Proof of work
bookkeeper	Up to you	Participants decide together	All participants
incentive mechanism	Not needed	Optional	Needed
degree of centralization	Centralization	Multi-centralization	Decentralization
advantages	Transparent and traceable	Efficiency, cost optimization	Credit self-establishment
TPS		1000-10000 Times per second	3-29 Times per second

Public blockchain uses complex algorithms to achieve consensus among network participants, but because public blockchain lacks protection measures for privacy, it is not suitable for corporate business activities in many cases. Alliance blockchain, the members of the alliance blockchain are different enterprise institutions or organizations, and each participating institution or organization runs one or more nodes in the blockchain. These nodes licensed by the network jointly participate, record transaction data, and manage the alliance blockchain, and the institutions in the system can read, write, and interact with the real data and the data on the chain through these nodes that join the network, record transaction data *etc.*

Private blockchain, private blockchain designates network participants by using an access control layer and usually uses a high-throughput consensus mechanism [11, 12]. So far, there is no application of private blockchain in traceability systems.

3.2 Traceability Technology Advantages

Although blockchain technology is relatively new, it has emerged in the traceability industry. Blockchain technology has several advantages, which are valuable and available for all kinds of participants in the supply chain.

(1) Blockchain allows each participant to upload information and data related to

products, and the system can also display the latest real-time updates of product information. In addition, every transaction in blockchain is recorded in sequence, so it provides a permanent audit trail to verify the authenticity of the product and track them through the traceable chain of supervision; (2) product traceability. At present, the supply chain needs to view product information, including product location, product source, batch number, production and order details. Blockchain can achieve wider product traceability across multiple partner companies without changing the company's own system; (3) simplify the auto-mation of supervision and discipline. With the blockchain, key data can be stored and provided to users in real time. Intelligent contracts are a component of blockchain-based systems, which automatically executes the rules and processing steps agreed by participants, thus simplifying, verifying, and executing the agreement terms between counterparties.

3.3 Homomorphic Cryptography in Blockchain

One of the most powerful aspects of blockchain technology is that it is a decentralized and distributed structure, which is used not only for the decentralization of data storage but also for the decentralization of management rights [13, 14]. Any change made by any data node to data can only be made after all nodes reach an agreement. Therefore, even if a hacker invades a node, the data cannot be tampered.

Although homomorphic encryption technology has not been completely realized, it has not been widely used. Homomorphic encryption is a special encryption method, which allows the ciphertext to be processed to get the same result as the plaintext, that is, ciphertext is directly processed and then encrypted to get the same result. From an algebraic point of view, it means homomorphism.

(a) If the $f(A) + f(B) = f(A + B)$

We call this cryptographic function an additive homomorphism.

(b) If the $f(A) \times f(B) = f(A \times B)$

We call this cryptographic function a multiplicative homomorphism.

(c) If the $f(A) + f(B) = f(A + B)$ and $f(A) \times f(B) = f(A \times B)$

Then, we call it a homomorphism algorithm.

The application of privacy protection technology in blockchain is still in the early stage, and the process of implementing homomorphic encryption for FISCO BCOS chain:

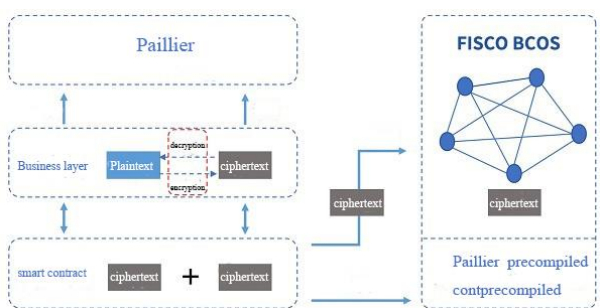

Fig. 2. Application of homomorphic encryption.

all the data on the chain can be encrypted by calling the paillier library, and the ciphertext data on the chain can be homomorphically added by calling the paillier pre-compiled contract to realize the ciphertext, and after the ciphertext is returned to the business layer, it can be decrypted by calling the paillier library. After the ciphertext is returned to the business layer, the decryption can be completed by calling the paillier library to get the execution result. The specific flow is shown in Fig. 2.

4. TRACEABILITY AND IMPLEMENTATION BASED ON BLOCKCHAIN TECHNOLOGY

After the user interaction module is implemented according to the requirements of traceability system, we consider the design of the underlying blockchain. In the whole traceability system design, the blockchain network is a part of the back-end business logic implementation, and the application interactive module calls the SDK to communicate with the traceability network. Here, for the sake of consistency of system language, we choose to use JavaSDK to manage the calling of channel, organization domain and user chain code.

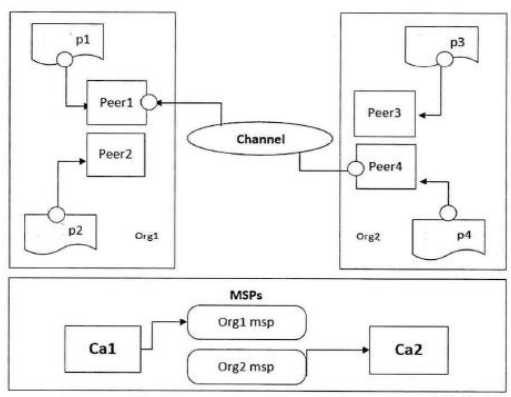

Fig. 3. Blockchain network node topology diagram.

4.1 Program Functional Module Division

The main challenges of data traceability systems are credible collection, credible storage, and credible verification of traceability information. The blockchain-based data traceability solution proposed in this paper aims to achieve credible data traceability by solving technical issues such as identity authenticity verification of the parties involved in data traceability, what traceability data should be recorded, and distributed storage of traceability data.

First, the solution provides the storage function of traceability data to solve the problem of possible tampering of traceability data, ensure the security and reliability of the stored data, and facilitate the credible verification of traceability data afterwards. Secondly, the scheme provides the verification function of traceability data, through which the scheme proposed in this paper can be tested, and the precondition is that the traceability

data has been stored successfully.

These two functions are mainly realized through the IoT devices (*i.e.*, IoT nodes) and data operators (*i.e.*, blockchain nodes) in the IoT environment. The IoT devices are the source of data and provide the data base for the blockchain; the blockchain nodes jointly participate in and maintain the blockchain network and are responsible for the recording and verification of traceability data. In addition, this paper also carries out the design of visualization module to facilitate the viewing of traceability data. From the perspective of functional implementation, the structure of functional modules is divided as shown in Fig. 4.

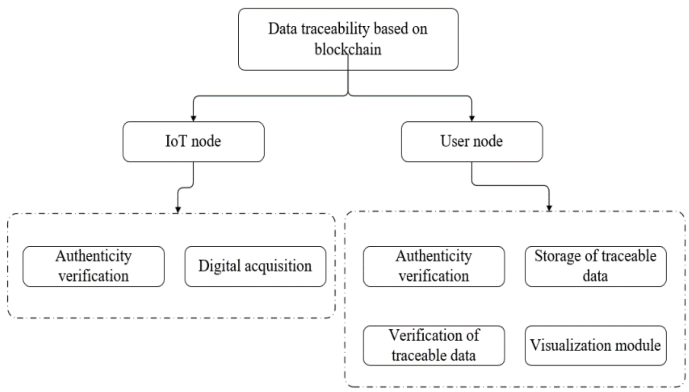

Fig. 4. Functional module structure.

The components in the functional module structure diagram can be divided into two categories: One is the physical components, including Internet of Things nodes and blockchain nodes. The other categories are functional components, including data collection, authentication, traceable data storage and traceable data verification. IoT devices (mainly various types of data collection devices) collect data information from the environment, and transmit the data to gateway nodes or data operators, *etc.* Their main function is data collection in order to provide data for blockchain after trusted authentication. In this paper, we focus on the design of the storage function of traceability data, the design of the verification function of traceability data and the design of the visualization module.

4.1.1 Storage technology for data traceability

To achieve secure and trustworthy data traceability, the definition of traceability data and safe and reliable storage are very critical. In this paper, the storage of traceability data is realized in two parts. First, a traceability data model in the IoT environment is established based on the PROV data model to describe traceability records in order to track changes in data and identify entities that cause changes; then, a set of smart contracts for traceability data management is designed based on the traceability data model. After the compiled contract is deployed to the blockchain, when a transaction meets the pre-set conditions, it will trigger the automatic execution of the contract to achieve data storage. Due to the characteristics of blockchain, it is difficult to tamper with the data after it is uploaded, thus ensuring the reliability of traceability data.

4.1.2 Validation techniques for data traceability

The verification function of traceability data can test the correctness of the scheme proposed in this paper. After the participating parties store the data on the blockchain, other nodes can obtain the traceability data of the traceability object from the blockchain to verify the authenticity of the traceability data. The contract contains the logic of the traceability data verification function. Here, the normal case of untampered data and the abnormal case of possible tampered data are considered, and if the data is untampered, other nodes can obtain the real traceability data from the blockchain, containing some attributes, agents and a series of operations performed on the traceability object, *etc.* Conversely, if the data is tampered, the obtained traceability data is empty.

4.1.3 Visualization techniques for data traceability

In order to visualize the process of storing and querying traceability data by blockchain nodes, this paper designs a JavaScript web application based on React to provide a visual graphical interface. The front-end interface contains the two main functions implemented in the blockchain-based data traceability scheme, namely uploading traceability data to the blockchain and obtaining traceability records from the blockchain, and the application is designed to facilitate checking the success of traceability data storage and querying traceability records.

4.2 Blockchain Technology-Based Data Traceability Implementation Solution

Structurally speaking, the Internet of Things can be divided into three parts: sensor control layer, network layer and application layer. The perception layer is the data source for network layer transmission, and also the database of application layer computing. Various sensors and gateways are the important components of the sensing layer, and the network layer. The application layer is the interface between the Internet of Things and users, and realizes various intelligent applications on the basis of the normal operation of the sensing layer and the network layer.

Combining the functional structure of the Internet of Things and the division of program functional modules, this paper designs the data traceability function implementation architecture based on blockchain, as shown in Fig. 6. The architecture consists of four parts, which are IoT devices, blockchain network built by blockchain nodes, smart contracts and the front-end of the application. In the following, each part will be described separately.

(1) IoT equipment

From the bottom to top, IoT devices (mainly various data acquisition devices, including sensors, RFID tags, card readers, *etc.*) are used to collect data information from the environment, and transmit the data to gateway nodes or user nodes for processing, which is used as the source of blockchain data.

(2) Blockchain Network

The blockchain network is jointly established by geth customers, which is used to store traceability data and provide basic traceability data query services. Blockchain nodes participate in and maintain the blockchain, and are responsible for generating and storing blockchain data, and providing necessary calculations for the blockchain network.

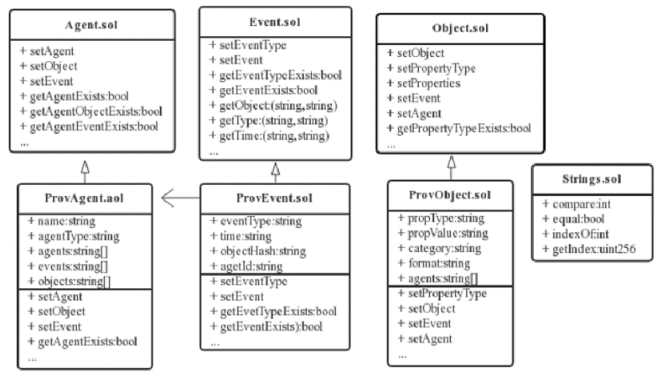

Fig. 5. Smart contracts class diagram.

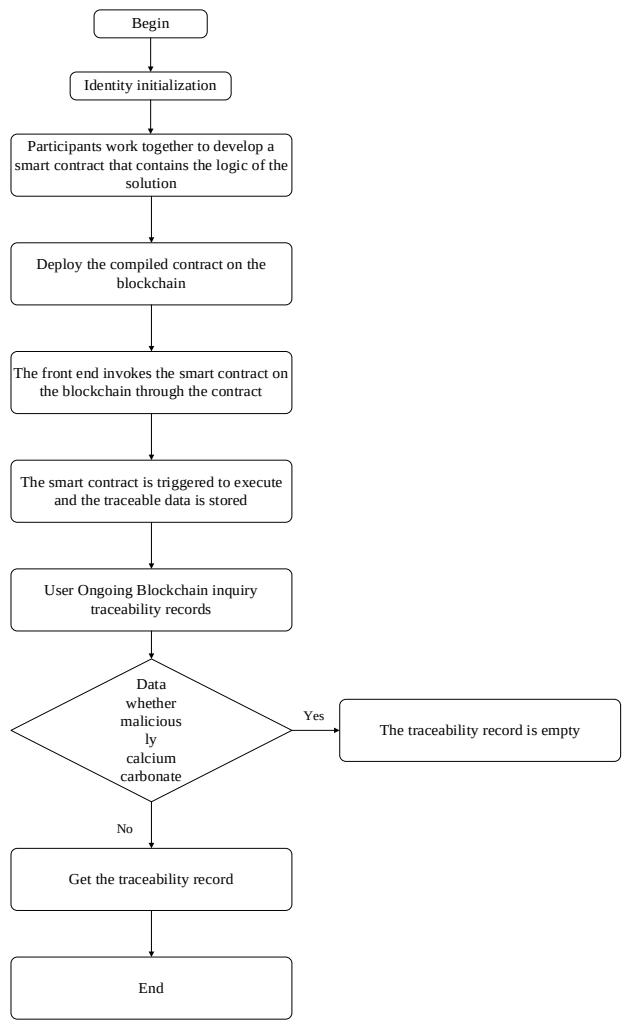

Fig. 6. Overall flow chart of the program.

(3) Intelligent Contract

In the part of smart contract, the solidity language supports the flexible writing of smart contract scripts that are applicable to applications and need to be strictly executed by all network nodes to describe the business logic realized by blockchain-based data scheme, mainly including the logic of traceability data storage and traceability data query *i.e.* (e) Verification.

(4) Front-End Page Display

Based on the normal operation of blockchain network and successful deployment of contracts, each participant can realize the functions of storing traceability data and verifying traceability records based on the front-end page.

First, the Solidity language is used to write a smart contract with data traceability system logic and the whole network nodes need to strictly execute the smart contract, and the solc compiler is used to compile the Resolve the contract into EVM byte code. Data traceability participants upload files and store them in the blockchain. After the data storage is successful, the data uploaders and other parties can verify the traceability data by querying the blockchain for traceability records.

4.3 Testing and Results Analysis

The running system of the experiment is Ubuntu16.04, which is based on the implementation of the ethereum blockchain platform. The client chosen is the geth client (short for go-ethereum), which is officially recommended by ethereum and currently more popular. client. All geth clients participate and maintain the blockchain together.

According to the storage test scheme of traceability data, it is tested and subsequent tests can be performed only when the MetaMask password is entered correctly. The account is imported, and the result is shown in Fig. 7. The balance of Ether for Account3 user is 100ETH at this time, and the storage of data will consume a certain amount of Ether.

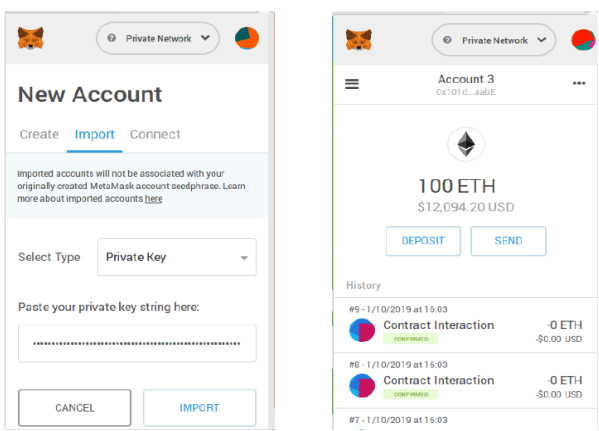

Fig. 7. Before and after account importation.

In the front-end of the application, after the user uploads the file and clicks submit, the corresponding transaction will be generated, and the transaction will be signed by MetaMask, and the specific block and transaction information is shown in Fig. 8.

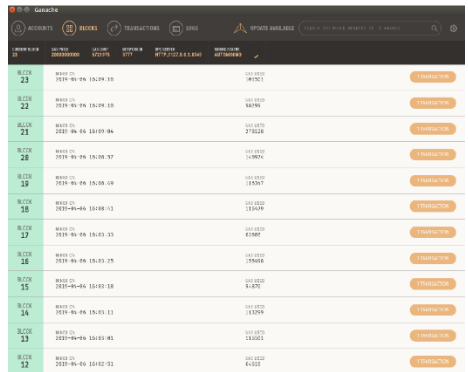

Fig. 8. Block generation diagram.

First, considering the case that normal data has not been tampered with, the test is executed according to the normal verification test case of traceability data, and after the traceability data is stored successfully, the traceability records are queried to the blockchain, and the test results are shown in Fig. 9, which are consistent with the expected results of the test case.

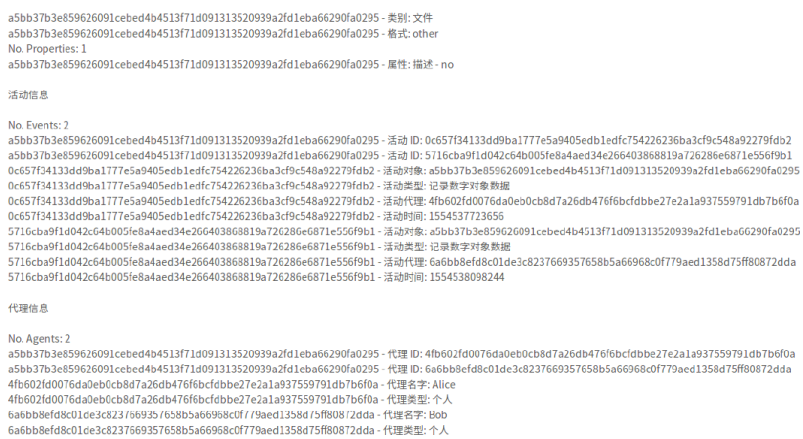

Fig. 9. Validation block generation diagram for traceability data.

5. CONCLUSION

The correspondence between virtual space and the real world, and the correspondence between code and law, make us closer to the essence of law, when it comes to new technologies legislation like blockchain. The code of blockchain technology, which sets rules to reach consensus, is the law of this distributed computer community that has wholly realized “from identity to contract”, and its regulation highlights the principle of combining self-regulation and other code in cyberlaw: on the one hand, it directly sets obligations for blockchain information service providers and incorporates the endogenous regulation of blockchain. On the one hand, it directly stipulates the obligations for blockchain infor-

mation service providers, and absorbs endogenous control of blockchain by technical means; On the other hand, it promotes autonomy of public sphere by integrating technical standards and authorizing enterprises to enforce laws.

Fund: Project Type: Philosophy and Social Science Research Project in Fujian Province, Project Name: Research on New Internet-related Crime Trends and Governance Issues in my country in the 5G Era, Project Number: JAS20191

REFERENCES

1. *Advances in Elliptic Curve Cryptography*, Cambridge University Press, UK, 2005.
2. D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, Vol. 1, 2001, pp. 36-63.
3. L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proceedings of the 4th International Conference on Advanced Computing and Communication Systems*, 2017, pp. 1-5
4. K. Croman, C. Decker, I. Eyal, *et al.*, "On scaling decentralized blockchains," in *Proceedings of International Conference on Financial Cryptography and Data Security*, 2016, pp. 106-125.
5. R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proceedings of the 12th ACM International Conference on Availability, Reliability and Security*, 2017, pp. 1-10.
6. A. Ramachandran and M. Kantarcioglu, "SmartProvenance: A distributed, blockchain based dataprovenance system," in *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy*, 2018, pp. 35-42.
7. B. Bera, S. Saha, A. K. Das, *et al.*, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled Internet of drones environment," *IEEE Transactions on Vehicular Technology*, Vol. 69, 2020, pp. 9097-9111.
8. C. M. S. Dhasarathan, S. P. Khapre, A. K. Shukla, *et al.*, "Blockchain-enabled decentralized reliable smart industrial internet of things (BCIIoT)," *Advances in Computer and Electrical Engineering Innovations in the Industrial Internet of Things (IIoT) and Smart Factory*, 2021, pp. 192-204.
9. S. Garg, G. S. Aujla, A. Erbad, *et al.*, "Guest Editorial: Blockchain envisioned drones: Realizing 5G-enabled flying automation," *IEEE Network*, Vol. 35, 2021, pp. 16-19.
10. U. Bodkhe, S. Tanwar, K. Parekh, *et al.*, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, Vol. 8, 2020, pp. 79764-79800.
11. C. Rupa, G. Srivastava, T. R. Gadekallu, *et al.*, "A blockchain based cloud integrated IoT architecture using a hybrid design," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Collaborative Computing: Networking, Applications and Worksharing*, 2021, pp. 550-559.
12. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, *et al.*, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, Vol. 8, 2020, pp. 111223-111238.
13. G. Kumar, R. Saha, W. J. Buchanan, *et al.*, "Decentralized accessibility of e-commerce

products through blockchain technology," *Sustainable Cities and Society*, Vol. 62, 2021, p. 102361.
14. D. J. Samuel R. and R. Kanna B., "Cybernetic microbial detection system using transfer learning," *Multimedia Tools and Applications*, Vol. 79, 2018, pp. 5225-5242.

Xiafei Yan was born in Huixian, Henan, P. R. China, in 1983. She graduated from the Zhongnan University of Economics and Law in 2012. She studied in School of Fujian Police University. Her research interests include Criminal investigation and Big data technology. E-mail: yanfei010156@163.com

Xu Zheng was born in Xianyou, Fujian, P. R. China, in 1989. He graduated from the Fuzhou University in 2009. He studied in School of Fujian Police University. His research interests include Blockchain Technology. E-mail: 1483619459@qq.com