Research Article

Mine Consortium Blockchain: The Application Research of Coal Mine Safety Production Based on Blockchain

Zilin Qiang,¹ Yingsen Wang,² Kai Song,² and Zijuan Zhao ²

¹School of Computer Science, University of Birmingham, Birmingham B15 2TT, UK

²College of Information and Computer, Taiyuan University of Technology, Taiyuan 030024, China

Correspondence should be addressed to Zijuan Zhao; zhaozijuan0064@link.tyut.edu.cn

Received 8 January 2021; Accepted 8 May 2021; Published 17 June 2021

Academic Editor: Zhe-Li Liu

Copyright © 2021 Zilin Qiang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To solve the problem that the safety data in the process of coal mine production are easy to be maliciously tampered with and deleted, a mine consortium blockchain data security monitoring system is proposed. The coal mine consortium blockchain includes supervision department, builds favourable centralized and decentralized production mode, and improves PBFT (Practical Byzantine Fault Tolerance) consensus mechanism to implement practical coal mine safety production. The evaluation shows that the architecture we proposed is more appropriate and efficient for the mine Internet of Things than the traditional blockchain architecture. The Hyperledger Fabric platform is used to build the mine consortium blockchain system to achieve the sensor data reliability, node consensus, safe operation automation management, and major equipment traceability.

1. Introduction

China's demand for coal energy is increasing year by year, and the scale of coal mining is gradually expanding. However, in the actual mining process, there are many mining problems, which may cause serious safety accidents to occur [1]. During the production process, in order to avoid the alarm and continue to produce, artificial tampering and deletion of sensor data result in the safety monitoring system failing to truly reflect the environmental changes in coal mines [2]; operators who do not operate strictly in accordance with regulations and abnormal equipment operation status are the biggest obstacles restricting coal mine production. However, the existing safety monitoring systems, personnel positioning systems, and major equipment systems cannot monitor the occurrence of these unsafe phenomena [3]. Thus, there is an urgent need to develop a platform that can prevent coal mines from tampering with sensor data and discover unsafe human behaviors and unsafe conditions in the production process in a timely manner [4], so as to ensure safe production in coal mines and provide more convenient supervision methods for supervision department.

Blockchain technology is a decentralized distributed ledger technology [5, 6]. Its characteristics of “nonforgery,” “full trace,” “traceability,” “open and transparent,” and “collective maintenance” are very consistent with the safety requirements of coal mine production. Literature [7] put forward the idea of applying blockchain technology to safe production information construction, so as to maximize resource sharing and provide convenient conditions for corporate supervision and government supervision. Literature [8] analyzed the construction method of agricultural product quality safety and efficient traceability system based on alliance blockchain. Literature [9] constructed a college safety education examination system based on blockchain technology, greatly enhancing the reliability of test-related data. The above studies have put forward the application concept of blockchain technology in information security from different scenarios, but the application of blockchain technology is still in the stage of theoretical exploration. At present, there is no theoretical research and model construction in the field of coal mine safety production with blockchain technology.

Therefore, a coal mine safety production system mode based on consortium chain technology is proposed in this

paper. First, the node architecture of the consortium chain integrated with the safety production model is constructed and the business process is analyzed. Then, specific analysis from the aspects of data reliability, safety production automation, traceability of major equipment, and consensus mechanism to provide a reference for the current theoretical research and actual construction of coal mine safety blockchain are conducted.

2. Consortium Blockchain Model Design

2.1. Application Model Architecture. In the model, the blockchain technology is used to integrate smart contract, consensus mechanism, and distributed database. Meanwhile, the supervision departments are incorporated into the consortium chain system to realize nontampering of data, intelligent production process, and traceability of equipment information. The application model architecture of the consortium chain is shown in Figure 1. The issuance of certificates is completed by Certification Authority (CA) [10] for the realization of identity authentication and authorization functions in the blockchain. Sensor nodes are responsible for recording coal mine data, uploading information to the chain through a consensus mechanism, and recording relevant data in the decentralized distributed ledger of the blockchain. After being authorized, the supervision institution completes the querying and tracing of the coal mine data in the ledger by calling smart contracts. The three are connected through this model to form an organic whole. For unsafe factors such as unsafe behaviors of people and unsafe condition of things, timely supervision and effective accountability can be achieved.

The model specifically includes a data credibility module, a safe operation automation module, and a major equipment traceability module, as shown in Figure 2. The interconnection of mine sensor information is realized, and all the sensor information in the underground is encapsulated into a block [11]. Conduct a consensus review of the information before being chained, and the information cannot be tampered with after being chained, solving the problem of sensor data being tampered with in coal mine [12]; establish a compliant process operation contract in coal mine safety production, add user identity verification, build an equipment information record chain independent of monitoring data, realize equipment information monitoring and traceability, and solve the problem of illegal operation in the safety production process. It can be seen that the system software can be basically divided into three submodules to solve the unsafe behavior of people, the unsafe condition of things, and the unsafe factors of the environment.

2.2. Node Architecture and Business Process. The model node architecture and workflow are shown in Figure 3, including modules such as CA, sorting service, and endorsement node [13].

2.2.1. CA. In this model, the internal authority of the coal mine safety production company acts as a CA (digital

certificate authority) node, which relies on the Membership Service Provider (MSP) in the consortium chain system, and it is responsible for receiving the registration application of the user node and returning the registration password for login, so that users can obtain identity certificate. After successful application, the CA will provide the private key to the user node in the form of a password. Finally, users store the certificate signing request and private key in a secure location on the server or local drive. The user's identity will be verified in all operations in the blockchain network to confirm whether it belongs to a sensor node, a supervisory node, or other nodes.

2.2.2. Sorting Service. The sorting service is responsible for sorting the data packets returned by each sensor. The sorting service arranges the transaction information into a certain order based on the rules according to the timestamp and packs it to facilitate data transmission [14] endorsement strategy and endorsement nodes.

The client initiates a sensor data package proposal. The consortium chain system does not automatically send data. Instead, the client specifies which nodes the block is sent to for endorsement verification; that is, the client specifies the endorsement policy [15]. The endorsement strategy defines the necessary combination conditions for the specific node that executes the proposal in the channel (i.e., the private chain) and its response result.

The endorsement node mainly performs verification, simulation execution, and endorsement of the proposal. After each endorsement node receives the block, it will verify the data in it. If the proposal does not meet the endorsement policy, it will not take effect locally.

2.2.3. Node Confirmation. Node confirmation is mainly responsible for checking the legality of transactions and updating and maintaining the state of the blockchain and ledger. Before the data packet is recorded in the ledger, it must be confirmed by the node confirmation, and only the confirmed data can be recorded in the blockchain ledger.

2.2.4. World State. Various information is recorded in the world state, such as sensor node data, smart contract bytecode, data customized by each smart contract, and chain configuration parameters [16]. The world state represents the current state, that is, the current value of each state data recorded.

2.2.5. Client and SDK. Through the client and SDK interface, users can specify endorsement strategies to endorsement nodes, send data information and device information to the sorting service, and participate in transaction verification.

3. Sensor Data Reliability

To realize the interconnection of mine sensor information and the decentralized storage of sensor data, all sensor

FIGURE 1: Model architecture of coal mine production consortium chain.

FIGURE 2: Submodule system structure.

information in the mine is encapsulated by the model into blocks. Consensus review is conducted on the information before the cochain, and the information cannot be tampered with after the cochain to ensure that the sensor data during the collection, transmission, and storage is true and reliable.

The completed module can not only provide closed-loop data services of safety management but also be embedded in the coal mine information safety monitoring system software system based on blockchain technology to provide data services. When the module is embedded in the system, the existing security monitoring system is improved, and a reliable system for sensor data is built. The system can set the user's functional authority and data authority according to the module characteristics and preset solutions suitable for

different users in various abnormal scenarios. When the module detects that the sensor data have been tampered with, the system dynamically pushes abnormal information and response emergency solutions to users at all levels combined with the data of the existing intelligent perception analysis system of artificial intelligence, Internet of Things, and big data and provides users at all levels with a feedback channel for abnormal information or solution error information. After verification, the effective feedback information will be added to the optimization algorithm of the system. The sensor data reliability includes the following specific functional modules. The structure is shown in Figure 4.

Account management is to record and change the members in the consortium chain network. Part of the

FIGURE 3: Node architecture and workflow.

FIGURE 4: Sensor data reliability.

functions of this module depend on the MSP of the consortium chain, and they are responsible for maintaining the IDs of all nodes in the system and issuing node identity certificates. The basic function module realizes the main functions of the safe production consortium chain, namely, the upload, download, query, and update of sensor data. The smart contract module is responsible for maintaining all chain codes in the system and realizes operations such as storage, compilation, update, and installation of chain codes. For the safety production consortium chain proposed in this paper, this module provides support for basic functions and audit traceability functions. The traceability module is responsible for packaging operation logs and device information into blocks and connecting them into chains while performing operations on the sensor data chain. Similar to the operation of the data link, the query of the operation log is to retrieve all the information in the behavior chain and return the specified log information to realize the postaudit function of the sensitive operation of the sensor data.

4. Safety Operation Automation Management

Smart contract is a computer protocol that can automatically execute the contract, and its characteristic is to allow trusted transactions without a third party [17]. However, at present, there is no complete template for smart contracts, and there are still higher risks and vulnerabilities. The DAO in Ethereum is a typical attack by hackers using smart contract vulnerabilities [18].

The multiple private chain architecture deployed with smart contracts is shown in Figure 5. This model stores data content with different permissions separately into chains and records the hash value returned by the sensor data transmission system in the form of transactions. The node security level is divided into three levels, named “confidential,” “secret,” and “public” [19]. According to the levels and functions of various departments such as coal mine production and supervision, different permissions are assigned to correspond to three private chains. The identity information issued by the MSP of the blockchain is divided

into three identities: administrator, authorized member, and ordinary member. General confidential private chain data can only be operated by administrators, secret private chain data can be operated by administrators and authorized members, and public data can be operated by all members including ordinary members. In addition, this model packs operation logs and equipment information on the chain in the form of transactions in the blockchain network to facilitate postaudit and realize the traceability of data sources.

Smart contracts are deployed on three different private chains to ensure data privacy and isolation. Each private chain can deploy multiple smart contracts, and the contracts can call each other. Data can be queried across private chains, but data cannot be changed. Each smart contract specifies the production process of its own equipment or product. If the department refuses to implement the specified production process for saving costs, the testing equipment will record the operating data and automatically deduct funds from the relevant departments and conduct other types of processing based on the smart contract. Inside the smart contract, specific processes and logical relationships are stipulated, such as processes A and B or joint confirmation of organizations A and B.

5. Major Equipment Traceability

For the traditional traceability system, the regulations of traceability system are formulated by relevant institutions such as government and enterprises. After the regulations are formulated, all production links are required to comply with the regulations. A new traceability scheme based on blockchain technology is adopted in this model. The scheme aims to establish a decentralized product traceability system maintained by nontrusted participants. The traceability scheme based on blockchain technology is adopted to store traceability information in the blockchain, and the decentralized characteristics of the blockchain are used to realize a decentralized traceability system [20]. A multiple private chain plus consortium chain architecture with high throughput and high security is used, and the Merkle tree is used to correlate the information stored in the two. The Merkle tree structure is shown in Figure 6.

In the coal mine production environment, coal mine data are detected by sensors in real time. To ensure data traceability of the blockchain system, once the data are entered, they cannot be tampered with and cannot be deleted. Therefore, the amount of data will continue to increase with time, which may cause problems such as excessive data volume. This problem can be effectively solved by the Merkle Tree structure in the safe production blockchain system.

Suppose that there is a transaction with a value of Hash4 in the block to be verified, it is only necessary to know Hash3, Hash12, and Hash5678. The hash of Hash34 and Hash1234 and the root node are calculated. If the finally calculated root node hash is consistent with that recorded in the block header, it means that the transaction exists in the block. The key to Merkle tree verifying transactions lies in two points: (1) Hash is calculated by the Merkle tree layer by layer from bottom to

top, so as long as the hash value of another adjacent node is known, it can be calculated up to the root node; (2) the hash value of the root node can be accurately used as the unique digest of a group of transactions [21]. Based on these two points, the existence of a transaction can be verified.

The greatest advantage of the Merkle tree is that each transaction can be deleted directly and individually, and the hash value of this transaction is just kept. In this way, for the entire block, the cryptographic security and integrity of the block are not changed, but the amount of data can be greatly reduced (the hash value has 32 bytes, and a transaction generally takes more than 400 bytes). If there is only one transaction in a block that has no subsequent transactions, deleting all other transactions will greatly reduce the amount of data in the entire block. Hence, in the safe production blockchain, there is usually no need to worry about the problem of excessive data caused by the increasing amount of data with the Merkle tree.

6. Consensus Mechanism

Consensus mechanism refers to the process of reaching a unified agreement on the state of the network in a decentralized manner, which helps to verify that information is added to the ledger, ensuring that only real transactions are recorded on the blockchain [22]. It means that a certain node modifies a certain data in the block during storage, but other nodes have no consensus on this block, and the modification operation is invalid.

There are currently three mainstream algorithms:

- (1) Proof of Work (PoW): the principle of the PoW mechanism is that the more work is done, the greater the benefit is. PoW can be divided into two phases, solution and verification. The solution phase requires a lot of complex calculations to compare computing power to obtain a mathematical solution; in the verification phase, the correctness of the mathematical solutions of other nodes can be verified through simple calculations. PoW requires a lot of complex calculations to ensure the correctness and consistency of the blockchain network [23]. Therefore, it is necessary to consume a lot of energy such as electricity, and it takes a long time to reach a consensus, so the PoW mechanism is inefficient.
- (2) Proof of Stake: PoS is also a kind of consensus proof, which is similar to equity certificates and voting systems, so it is also called “stake proof algorithm” [24]. It is completed relying on tokens, and the person holding the most tokens will announce the final information, which is not suitable for most blockchain application scenarios.
- (3) Practical Byzantine Fault Tolerance: PBFT is also a common consensus proof. It is different from the previous two mechanisms. PBFT is based on calculations and there is no token reward. Everyone on the chain participates in voting. The right to publicize information can be got when the objection is less than $(N-1)/3$ nodes.

FIGURE 5: Smart contract deployment architecture.

FIGURE 6: Merkle tree.

The PBFT is adopted in the security management model, which can regularly evaluate the availability of nodes and dynamically add or delete authentication nodes to ensure overall operating efficiency.

In the PBFT consensus process, nodes are divided into master nodes and slave nodes. The master nodes are mainly composed of coal mine safety management departments, and the slave nodes are composed of sensor nodes. The consensus process without node failure is shown in Figure 7. The master node is responsible for data packaging, and the slave node is responsible for data verification. Both types of nodes have the function of interacting with the client.

First, the client sends a request to any node (from node 1 in the figure), and the node broadcasts the data request sent by the client to the entire network. After collecting multiple requests, the master node sorts them into the list, produces preprepared certificates, and broadcasts the preprepared certificates to the entire network. After it is received by the

slave node, it verifies the certificate and replies to the master node for information approval. After the master node receives the approval information of all the slave nodes, it packs the approval information and sends it to all the slave nodes, and the slave node verifies the correctness of the approval information of other slave nodes. When all nodes indicate that they receive block information from other slave nodes, other nodes will package the data information on the cochain.

7. Simulation and Analysis

This section tests the performance of the coal mine consortium blockchain and compares it with traditional PBFT, two classic public blockchain platforms, Bitcoin, and Ethereum to highlight the advantages of our model. Finally, the Hyperledger Fabric platform is used to construct the coal mine consortium blockchain system. We focus on the

FIGURE 7: PBFT consensus process.

FIGURE 8: The performance of throughput and latency of coal mine consortium blockchain.

analysis of the indicators of throughput and latency. Throughput is used to describe the number of data requests that can be processed per second in the coal mine consortium blockchain and is an important indicator to measure the performance of the consensus algorithm. The number of transactions packaged per unit time is expressed as TPS (transactions per second) in blockchain: $\text{Transactions}/\Delta t$. Latency refers to the time from issuing a data request from the master node to the response of the entire blockchain platform.

Hyperledger Caliper is used to perform the pressure test, setting up 100 nodes to continuously send transaction requests to the coal mine consortium blockchain system and observe its throughput and latency by increasing send rates.

Figure 8 shows the performance of the proposed coal mine consortium blockchain model in throughput and latency. Throughput rises as send rate increases, when send rate reaches around 270 tps, it no longer keeps increasing, but maintains a steady state. When send rate was lower than 27 tps, the latency increases slowly and remains below 1500 ms at a relatively low level. When send rate is greater than 270 tps, the latency increases rapidly.

In order to evaluate the effectiveness of the proposed coal mine consortium blockchain model, we compared the throughput of the consortium blockchain with traditional PBFT and two classic blockchain model: Bitcoin and Ethereum. The result shows that the coal mine consortium blockchain model has obvious advantages in throughput. Bitcoin uses the POW consensus mechanism, which requires a lot of computing power and only produces one block every 10 minutes on average. Ethereum uses a POW and POS consensus mechanism; it takes about 10 seconds per block. The data required by the comparison experiment is from two different public data sets [25, 26], which collected part of the data generated by the two public blockchains in the real transaction. Compared with the traditional PBFT, the improved PBFT increases the verification step, but the communication time is greatly reduced, which not only increases the security in the process of block transmitting but also reduces the communication traffic as shown in (Figure 9).

Finally, we use Hyperledger Fabric platform to build the coal mine consortium blockchain system, so as to implement the coal mine output transaction, query, and other operations. Figure 10 shows the mineral trading of the coal mine

FIGURE 9: Throughput comparison.

FIGURE 10: The mineral trading of consortium blockchain.

```
Successfully loaded user1 from persistence
Assigning transaction_id: 1659a9d01a5826d15b4aa8b874c2b45883861ed7b6a1cc6c601a2bcf62e279af
Transaction proposal was good
Successfully sent Proposal and received ProposalResponse: Status - 200, message
- ""
The transaction has been committed on peer localhost:7051
Send transaction promise and event listener promise have completed
Successfully sent transaction to the orderer.
Successfully committed the change to the ledger by the peer
```

FIGURE 11: Performance of the underlying of the coal mine consortium blockchain.

TABLE 1: The test result of the Hyperledger Caliper.

Test	Name	Send rate	Avg latency (s)	Throughput (tps)
1	Transaction	100	0.11	100
2	Transaction	110	0.14	110
3	Transaction	120	0.18	120
4	Transaction	130	0.21	130
5	Transaction	140	0.26	140
6	Transaction	150	290	150
7	Transaction	160	0.29	160

TABLE 1: Continued.

Test	Name	Send rate	Avg latency (s)	Throughput (tps)
8	Transaction	170	0.36	170
9	Transaction	180	0.39	172
10	Transaction	190	0.43	180
11	Transaction	200	0.44	197
12	Transaction	210	0.44	205
13	Transaction	220	0.49	208
14	Transaction	230	0.54	228
15	Transaction	240	0.62	235
16	Transaction	250	0.68	246
17	Transaction	260	0.73	257
18	Transaction	270	0.78	266
19	Transaction	280	0.99	265
20	Transaction	290	1.6	267
21	Transaction	300	2.8	264
22	Transaction	320	4.1	263
23	Transaction	340	5.4	265
24	Transaction	360	6.2	266
25	Transaction	380	7.1	269

consortium blockchain. Figure 11 shows the performance of the underlying blockchain after the mineral trading, including the hash value of this transaction.

8. Summary

The decentralized, intelligent, and tamper-resistant characteristics of blockchain technology are in line with the requirements of coal mine safety production, and blockchain technology has broad development prospects in the field of coal mine safety production. Our method enhances the safety of coal mine safety production using blockchain. However, we deployed a small number of nodes to test the performance of our platform. And our model assumes that most nodes are normal. So, in a real large-scale deployment, message consistency and accuracy may not be guaranteed. For future work, we will improve our consensus algorithm flow, especially the detailed view-change. And we will deploy our platform in a public blockchain (e.g., Ethereum). Although blockchain technology has different degrees of application and research in various industries, it is still in its infancy, and there are deficiencies such as low efficiency and waste of resources. As a result, blockchain technology has not yet been widely applied.

In cooperation with Jingying Technology in Taiyuan, this paper proposes a coal mine safety production consortium chain model combined with blockchain technology and safety requirements in the field of coal mine production. It incorporates supervision departments into the system to form a good and supervisable business model where centralization and decentralization coexist. The module structure, node structure, and business process of the model are analyzed and corresponding countermeasures are proposed aiming at the problems of data reliability, safety automation management, and major equipment traceability to promote the research and development of blockchain technology in the field of coal mine safety production.

Appendix

We use the Hyperledger Caliper in Section 6 to evaluate the performance of the coal mine consortium blockchain. Transaction requests are continuously sent to the blockchain model over an HTTP port at a specific rate to monitor the related performance of the consortium blockchain. The test result is shown in Table 1.

Data Availability

Previously reported data were used to support this study. The datasets are cited at relevant places within the text as references [19, 20]. And the pressure test of our model is shown in Appendix in this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] R. Zong, W. Wu, and F. Liu, "Coal mine production safety measures and accident statistics in China," *Coal Technology*, vol. 39, no. 1, pp. 205–207, 2020.
- [2] C. Tunc and S. Hariri, "CLaaS: cybersecurity lab as a service," *Journal of Internet Services and Information Security*, vol. 5, no. 4, p. 19, 2015.
- [3] I. Kotenko, I. Saenko, and A. Kushnerevich, "Parallel big data processing system for security monitoring in internet of things networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 8, no. 4, pp. 60–74, 2017.
- [4] B. Bordel, R. Alcarria, M. Ángel Manso, and A. Jara, "Building enhanced environmental traceability solutions: from thing-to-thing communications to generalized cyber-physical systems," *Journal of Internet Services and Information Security*, vol. 7, no. 3, pp. 17–33, 2019.
- [5] J. Li, Y. Huang, Y. Wei et al., "Searchable symmetric encryption with forward search privacy," *IEEE Transactions on Dependable & Secure Computing*, vol. 18, no. 1, pp. 460–474, 2019.

- [6] Q. Shao, C. Jin, Z. Zhang et al., "Blockchain: architecture and research progress," *Chinese Journal of Computers*, vol. 41, no. 5, pp. 969–988, 2018.
- [7] J. Li, M. Wang, J. Zhang et al., "Application of block chain technology in the construction of safety production informatization," *An Quan*, vol. 41, no. 2, pp. 88–93, 2020.
- [8] J. Luo, "Analysis of an efficient traceability system for agricultural product quality and safety based on alliance blockchain," *Computer Knowledge and Technology*, vol. 16, no. 6, pp. 272–273, 2020.
- [9] C. Fan, Y. Li, G. Zhang et al., "Study on the blockchain based safety education examination system for colleges and universities," *Guangdong Chemical Industry*, vol. 46, no. 14, pp. 211–212, 2019.
- [10] J. Li, H. Yan, Y. Zhang et al., "Efficient identity-based provable multi-copy data possession in multi-cloud storage," *IEEE Transactions on Cloud Computing*, vol. 24, no. 12, 2019.
- [11] C. Gritti, M. Önen, R. Molva, S. Willy, and P. Thomos, "Device identification and personal data attestation in networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 9, no. 4, pp. 1–25, 2018.
- [12] B. Todd and K. Andersson, "Network security of internet services: eliminate DDoS reflection amplification attacks," *Journal of Internet Services and Information Security*, vol. 5, no. 3, p. 22, 2015.
- [13] J. Zhang, Y. Qiu, and H. Jin, "Research on the SDK national secret transformation plan of the fabric platform of hyperledger," *Network Security Technology & Application*, vol. 231, no. 3, pp. 37–39, 2020.
- [14] Networks—Peer-to-Peer Networking, "Researchers from beijing jiaotong university report details of new studies and findings in the area of peer-to-peer networking (performance analysis of hyperledger fabric platform: a hierarchical model approach)," *News of Science*, vol. 13, no. 3, 2020.
- [15] J. Long, "Design of blockchain system in BDCP using hyperledger fabric," in *Proceedings of the 2019 World Symposium on Software Engineering (WSSE 2019)*, pp. 79–83, Wuhan, China, September 2019.
- [16] R. Campbell, *Transitioning to a Hyperledger Fabric Quantum-Resistant Classical Hybrid Public Key Infrastructure*, Capitol Technology University, Laurel, ML, USA, 2019.
- [17] Z. Zheng, S. Xie, H.-N. Dai et al., "An overview on smart contracts: challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, 2020.
- [18] H. Ren and Z. Xie, "The criminal risk of smart contracts in the blockchain 2.0 era and countermeasures—taking the DAO hacking incident as an example," *Crime and Reform Research*, no. 3, pp. 2–7, 2020.
- [19] D. Wu, Y. Xiang, C. Wang et al., "Data protection technology for information systems based on blockchain," *Journal of Command and Control*, vol. 4, no. 3, 2018.
- [20] C.-S. Shih, W.-Y. Hsieh, and C. L. Kao, "Traceability for vehicular network real-time messaging based on blockchain technology," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 10, no. 4, pp. 1–21, 2019.
- [21] X. Weng, P. Zhang, W. Wang et al., "Remote attestation mechanism for platform integrity based on unbalanced-hash tree," *Journal of Computer Applications*, vol. 2, pp. 433–437, 2014.
- [22] Y. Huang, B. Li, Z. Liu et al., "ThinORAM: towards practical oblivious data access in fog computing environment," *IEEE Transactions on Services Computing*, vol. 13, no. 4, 2019.
- [23] D. Larimer, "Delegated proof-of-stake white paper," *IEEE Access*, vol. 7, 2014.
- [24] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," 2015, https://ripple.com/files/ripple_consensus_whitepaper.pdf.
- [25] "Bitcoin historical data," 2018, <https://www.kaggle.com/mczielinski/bitcoin-historical-data>.
- [26] Ethereum, "Ethereum historical data," 2021, <https://www.kaggle.com/kingburrito666/ethereum-historical-data>.