ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Optimization path and practice of whole process quality management mode of construction engineering project in the intelligent era

Hongli Zhang[1,*]

[1] Inner Mongolia Electric Power Survey & Design Institute Co., LTD Huhehaote 010000, Neimenggu, China

SUMMARY: *The research paper deals with the optimization route of whole-process quality management in construction engineering projects in the era of intelligence, and develops a comprehensive quality-control system, which is aimed at reviewing designs, construction implementation, electrical installation regulation, acceptance of hidden work, commissioning, and handing over at the end. In order to solve the practical issues of scattered quality information, low accountability, slow feedback, and poor interaction between civil and electromechanical systems, the study proposes blockchain, smart contracts, and advanced CP-ABE mechanism as the reliable technical basis of the quality-management platform, thus allowing sharing, dynamic access and full tracing of essential quality records, inspection findings, correction logs, and electrical commissioning information in a safe manner. The results of the experiments demonstrate that the given mechanism has obvious performance benefits in terms of platform-side quality data processing: ciphertext size is constant (5.8 KB), and upload time is regulated (9.2 ms) and memory consumption is low (13.9 MB and CPU usage is 26.1 percent under 25 attributes), whereas latency in tracing situations does not exceed 0.41 s with throughput exceeding 570 bits. The model also yields very high defense rates when Sybil and DoS and U2R attacks are considered. These findings suggest that the suggested methodology has the potential to offer a useful technical assistance to the intelligent development of whole-process quality management, particularly when it comes to quality adjustment and collaborative control in electrical engineering subsystems.*

Povzetek: The proposed research paper presents an intelligent whole-process quality management model of construction engineering projects, especially focusing on the coordinated control of electrical installation quality, system adjustment, and multi-party quality evidence circulation. With the use of blockchain, smart contracts and attribute-based encryption, the model can facilitate trusted quality record keeping, high-quality permission control as well as end-to-end traceability of inspection and correction actions. Experimental findings confirm the effectiveness of the model in terms of responsiveness, resource usage, and safety protection, and it is able to offer a reliable technical assistance to enhance the quality governance ability in intelligent construction settings.

KEYWORDS: *Intelligent construction; Electrical engineering adjustment; Blockchain traceability; Fine-grained access control*

*15024871185@163.com
https://doi.org/10.65102/is2026461
Published: 30 April, 2026

1 Introduction

The quality management of construction engineering projects can be seen beyond isolated inspection records or post-event acceptance documents in the intelligent era, but it has become more reliant on the continuous perception, real-time transmission, and structured storage, collaborative analysis, and prompt response to the process data throughout the whole project lifecycle. Since the design review, materials entry and structural construction, electrical installation, equipment commissioning, concealed-work acceptance and completion delivery, quality control has gained stronger attributes of multi-source heterogeneity, dynamic linkage and cross-organization cooperation. Of these connections, the quality adjustment of the electrical engineering subsystems such as power distribution installation, cable laying, temporary power utilization, electromechanical coordination and system commissioning have a direct influence on project safety, operation stability and end delivery performance.

Nevertheless, in accordance with the usual models of management, quality documents frequently lie in the hands of contractors, supervisors, owners, testing companies, and equipment vendors. It results in such common issues as inconsistent standards, slow rectification feedback, low traceability of responsibility, and low-quality coordination between civil works and electrical systems. Despite the fact that such digital tools as BIM platforms, IoT terminals, and mobile inspection systems have enhanced the efficiency of data collection to some degree, most of the construction sites do not have a unified system that could at the same time serve the trusted quality evidence repository role, dynamic authority control, the ability to trace processes, and smart quality adjustment. Thus, the whole-process quality management is fragmented in practice.

Taking into consideration this background, the given research shifts the position of blockchain and cybersecurity technologies as merely information sharing systems but a technical assistance route towards quality management optimization of the entire process of construction engineering projects. Through the combination of blockchain, smart contracts, and a better CP-ABE system, the paper builds an intelligent quality-governance model that encompasses all the aspects of quality data gathering, permission control, process traceability, rectification coordination, and adjustment of electrical subsystems. This paper aims at enhancing the continuity, transparency and responsiveness of project quality management to develop a practicable optimization process of construction projects that demand high coordination among civil, installation and power-related systems.

The paper is organized in this way: Section 2 provides a review of the existing literature on smart construction, overall quality management, and the traceability facilitated by blockchain, and fine-grained access control. Section 3 suggests an intelligent-quality management model to be used in construction engineering projects and describes the system architecture, mechanism of operation, and electricity quality adjustment path. Section 4 analyzes the performance and application feasibility of the suggested model using comparative experiments and simulations by scenarios. Section 5 talks about the optimization worth of the model in terms of quality cooperation, electrical sub-system regulation, and scalability as well as engineering relevance. Section 6 summarizes the work and offers directions to improve it.

2 Related Research

With the further development of intelligent construction, the amount of quality related information produced throughout the entire lifecycle of construction engineering projects has

grown significantly. The data do not remain confined to individual acceptance forms only, but they may be extended to drawing review documents, the outcomes of the process inspections, hidden-work documentation, commissioning conditions of items and electrical adjustment logs. Nevertheless, in multi-party collaborative settings, such quality data is often divided among various organizations and specialties, which leads to indistinct authority lines, poor accountability, slow corrective feedback, and inadequate coordination between civil works and electromechanical systems. In order to overcome these problems, more recent research has examined the application of blockchain and cybersecurity technologies to engineering quality governance, providing initial groundwork on trustworthy management of quality-data.

Concerning the design of the data sharing mechanism, Zhang et al. (2023) [6] developed a blockchain-based decentralized supply chain information sharing system that focuses on synchronizing and maintaining a consistency in data across various nodes. The system proved to be very resilient with regard to information integrity and transparency. Wang et al. (2024) [7] also presented a consortium blockchain-based data sharing system (BBS). It can facilitate the autonomy of sharing the engineering big data through developing multi-level node verification and access control measures, and has been applied in areas like energy management and transportation engineering. Also, the issue of the sensitivity of government data sharing was discussed by Liu and Zeng (2021) [8], who offered a solution incorporating smart contracts with role-based access control, which greatly improves the flexibility and safety of data invocation.

In terms of information traceability, Gao et al. (2024) [9] proposed a blockchain-based design review transaction system to digital building permits. Through chained records and timestamp hashing technology, this mechanism guarantees that every step of the architectural design review process can be traced and not denied. Concerning the construction information, Zhang et al. (2024) [10] set up a data bank called a tunnel data bank which uses the consortium blockchain mechanism to ensure the structural health monitoring data is processed in a traceable way, which effectively reduces the ambiguities of determining project liability. In the meantime, Hijazi et al. (2023) [11] tightly integrated BIM models and blockchain to create a Single Source of Truth (SSOT) structure that gives strong backing of data consistency in the construction supply chain.

Researchers have also investigated the access controls mechanisms to address the complex multi-party identities and dynamic data flow paths in engineering projects. Ma et al. (2024) [12] have created a blockchain sharing model that uses CP-ABE (attribute-based encryption) policies to support fine-grained permission policies and hide a cryptographic access policy. The method increases system flexibility and guarantees the confidentiality of the data. The Framework for Autonomous Data Sharing and Fault Detection (FADSF) was suggested by Sun et al. (2024) [13] to be used in intelligent connected situations. With the addition of dynamic key updates and smart access log audit, it allows sharing of the perception data of the vehicles in real time and holds them accountable. Simultaneously, Elapolu et al. (2024) [14] proposed blockchain-based engineering requirement traceability because it is essential to overcome the primary issues of constant change in requirements and unclear distribution of responsibilities in systems engineering.

Although existing research has integrated blockchain with cybersecurity mechanisms at various levels, the following limitations persist when applying these solutions to specific construction engineering scenarios: (1) Most system designs lack deep adaptation to the requirement for "multi-role dynamic permission coordination" in engineering projects; (2) Information traceability mechanisms often remain at the log-recording level, failing to establish a closed-loop system for responsibility attribution and evidence preservation; (3)

Some solutions exhibit practical gaps in performance, scalability, and deployment costs, hindering large-scale adoption in complex construction environments.

Based on this research landscape, the proposed model aims to achieve breakthroughs in three key areas: (1) Establishing an intelligent whole-process quality-management framework that supports dynamic multi-party collaboration and improves the precision and adaptability of authority control; (2) Designing a traceable and auditable chain-based evidence mechanism to ensure end-to-end verifiability of critical quality records, inspection behaviors, rectification results, and electrical adjustment data; (3) Optimizing model performance and deployment architecture based on project characteristics to ensure practical applicability in real construction quality-governance scenarios.

Table 1: Comparison and improvement directions of intelligent quality-management support technologies in construction engineering

Research ID	Application Domain	Technical Method	Achievements & Advantages	Existing Problems	Problems This Study Aims to Solve
Zhang et al. (2023)	Engineering supply-chain data sharing	Decentralized blockchain storage structure	High data transparency and consistency	Lack of fine-grained access control	Build an attribute-driven permission control strategy
Liu & Zeng (2021)	Cross-organizational government data sharing	Smart contracts + permission-mapping mechanism	Flexible access, isolated handling of sensitive data	Security strategy is rigid with poor dynamic adaptability	Introduce dynamic keys and access-audit mechanisms
Gao et al. (2024)	Architectural design review workflow	Blockchain-based notarization + transaction records	Full traceability throughout the review process	High real-time requirements; large latency	Combine edge computing to reduce response time
Hijazi et al. (2023)	BIM–blockchain integrated construction management	Single Source of Truth (SSOT) architecture	Strong data consistency assurance	Relies on centralized platform; high deployment cost	Modular component design to enhance system portability
Zhang et al. (2024)	Tunnel monitoring data processing and traceability	Consortium blockchain + identity authentication	Traceable and non-repudiable data	Coarse-grained permission management	Refine authorization granularity for better fine-grained control
Sun et al. (2024)	Intelligent connected sensing-data sharing	Dynamic key mechanism + chained access logs	Combines real-time sharing with auditability	Limited applicability; poor generalization	Standardize universal engineering-data interface formats

In summary, although existing research has provided valuable insights into blockchain-enabled engineering quality governance and process traceability, a unified mechanism capable of accommodating multi-party, multi-stage, and multi-format quality information throughout the whole project lifecycle has yet to be established.

3 Intelligent Whole-Process Quality Management Model for Construction Engineering Projects Supported by Blockchain and Cybersecurity Technologies

3.1 Construction of an Intelligent Whole-Process Quality Management Framework for Construction Engineering Projects

Against the background of intelligent construction and lifecycle-based quality governance, construction engineering projects generate large volumes of heterogeneous quality information across design, procurement, construction, installation, testing, adjustment, and delivery stages. These data include drawing review opinions, material inspection records, process acceptance forms, concealed-work images, sensor logs, equipment commissioning parameters, electrical system adjustment data, and rectification notices. Because these quality elements are distributed across multiple organizations and specialties, traditional quality management methods relying on isolated documents and manual coordination can hardly meet current requirements for process continuity, responsibility traceability, dynamic adjustment, and cross-disciplinary collaboration. Therefore, this paper constructs an intelligent whole-process quality management framework supported by blockchain and cybersecurity technologies, so as to provide a trusted operating mechanism for quality data circulation, authority control, evidence preservation, and electrical subsystem coordination in construction engineering projects.

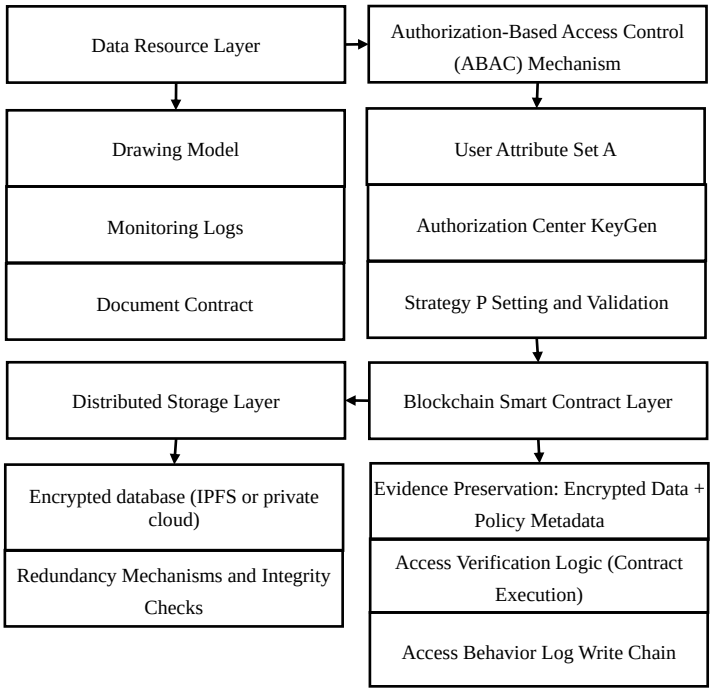

Figure 1: Overall architecture diagram of the intelligent whole-process quality management model for construction engineering projects

This model is divided into four main layers: the data resource layer, the permission management layer, the blockchain smart contract layer, and the distributed storage layer. Each level is both independent of each other and operates in coordination through interface standards, achieving a closed-loop management of the entire life cycle from data generation, permission distribution, access control to behavior auditing.

The data resource layer is responsible for standardized classification and identification of quality data across all stages of the project lifecycle. The data sources mainly include BIM review models, inspection records, construction documents, material acceptance reports, sensor logs, concealed-work evidence, rectification notices, electrical installation records, commissioning parameters, and power-system adjustment data, all of which show strong heterogeneity in format and update frequency. If there is a lack of a unified description method, it will lead to difficulties in implementing subsequent access control and on-chain evidence storage. The meta-information of data resources includes fields such as the unit to which the data belongs, generation time, business type, and sensitivity level, which are used to support permission control and access log recording. All resources must undergo format conversion and secure encryption processing before being registered and included in the chain to ensure their structural standardization and access security.

The permission management layer introduces Attribute-Based Access Control (ABAC) policies. Based on the roles, organizational identities, business permissions, etc. of the project participants as attributes, the access policy tree is dynamically generated, and the corresponding access key is assigned to each user. This process is accomplished by the "Authorization Center" in the model and mainly includes three functional modules: attribute verification, private key generation, and key distribution. During the system initialization phase, the system administrator generates the master key and the global public key, as shown in Formula (1):

$$\text{Setup}(1^{\lambda}) \rightarrow (PK, MK) \tag{1}$$

Among them, λ represents the security parameter, PK is the public parameter, and MK is the master key. The authorization center generates the corresponding private key SK_A based on the user attribute set A, and the process is as shown in Formula (2):

$$\text{KeyGen}(MK, A) \rightarrow SK_A \tag{2}$$

In the data release stage, the data owner encrypts the original data through the system public key PK and the defined access policy P, using a combination of symmetric encryption and attribute-based encryption to generate the ciphertext CT. The process is as shown in Formula (3):

$$Encrypt(PK, M, P) \rightarrow CT \tag{3}$$

Among them, M represents the content of the engineering data to be encrypted, P indicates the access control policy rule, and CT is the encrypted ciphertext. Subsequently, the ciphertext was written into the blockchain, along with data fingerprints, digest information and encrypted access policies, for the verification and comparison of subsequent access requests.

During the data request stage, users need to submit their attribute key SK_A to initiate a data access request to the chain. The system automatically calls the attribute matching function through the smart contract to compare the consistency between the requester's attributes and the data policy. If the verification is successful, it returns the key decryption

permission. If the policy conditions are not met, access will be denied. The decryption verification process is shown in formulas (4) and (5):

$$DelegateDecrypt(PK, CT, SK_A) \rightarrow CT' \tag{4}$$

$$Decrypt(CT', SK_A) \rightarrow M \text{or} \perp \tag{5}$$

Among them, CT' represents partially pre-decrypted ciphertext. Whether it can ultimately be restored to plaintext M depends on whether the requester has a matching attribute combination. If the verification fails, the system returns a special symbol $\perp$ to identify an illegal request.

Also, in order to handle dynamic situations like changes in engineering participants identities and transitions between task stages, the model has created a key revocation and resource policy update mechanism. Every time an attribute of users changes or their permissions are revoked, the system must re-generate the key and its associated ciphertext so that the previous permissions are invalidated and not unauthorized access can be made. The process of calculation is described in formulas (6) and (7):

$$Revoke(A) \rightarrow (SK_A^{\text{new}}, CT^{\text{new}}) \tag{6}$$

$$Update(P', CT) \rightarrow CT^{\text{new}} \tag{7}$$

In the above process, SK_A^{new} represents the updated new private key, CT^{new} represents the ciphertext version generated based on the new access policy or attribute, and P' represents the modified new policy. This mechanism is especially appropriate in high frequency situations like shift change, job modification, and rights transference in construction sites.

The model incorporates a data access log recording module at the smart contract layer to improve the operational transparency and behavioral auditability. All access requests, authorization verifications, and decryption operations are traceable in the form of transactions. Any abnormal operation can be traced back to the specific time, initiating entity and accessed resources to ensure that the subsequent responsibility division has legal effect. This mechanism demonstrates excellent security restraint capabilities in preventing data abuse, tampering and unauthorized distribution. As shown in Figure 2, it is the flowchart of the interaction between the key data flow and the smart contract of this shared model.

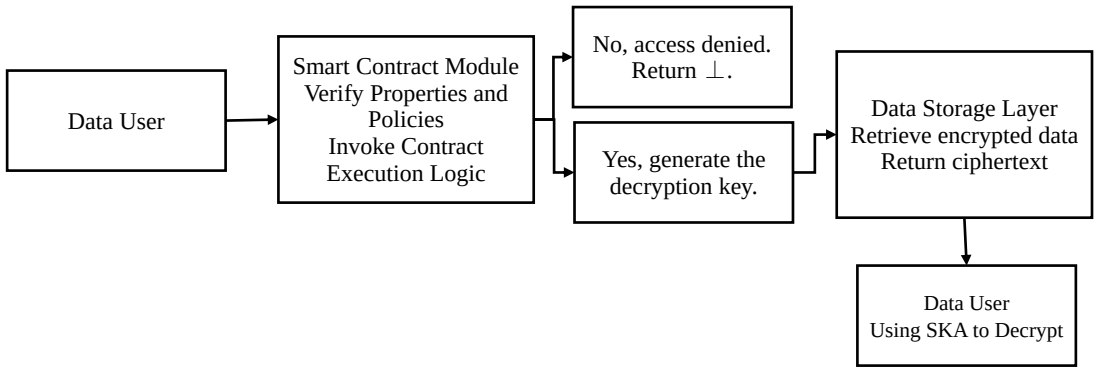

Figure 2: Flowchart of quality record submission, verification, and traceability interaction

Compared with the traditional methods Based on user Identity authentication (IBAC) or Role-Based Access Control (RBAC), The model based on attribute fusion blockchain mechanism proposed in this paper has significant advantages in terms of flexibility and

scalability. Firstly, the attribute control model does not rely on the unique identity of users and can support fine-grained authorization across organizations. Secondly, the distributed ledger feature of blockchain naturally avoids the single point of failure problem, ensuring the continuity and fault tolerance of data sharing. Finally, access control based on encryption policies can theoretically satisfy any complex policy expression and has good composability and scalability.

To summarize, this chapter has created a smart quality-management model of the entire process containing the combination of the following: quality-resource hierarchical management, attribute-based authority control, blockchain trusted execution, and secure storage isolation. This framework does not only respond to common quality-governance situations like multi-party cooperation, frequent access to quality-records in construction projects, and dynamic adjustments of authority within construction projects, but also provides an architectural basis of designing traceability mechanisms and verifying performance later on. In the next section, the author will go into more detail about the exact design of the blockchain-powered quality traceability and dynamic authority mechanism.

3.2 Design of Quality Traceability and Dynamic Authority Mechanism Based on Blockchain

Despite the fact that the proposed framework has already secured the elementary support of safe quality-data exchange, there are still a number of practical issues associated with the whole process quality management in construction engineering. In the course of the project implementation, the roles of the owners, the general contractor, subcontractor, supervisor, the testing agency, and the commissioning team often shift as the construction phase progresses, indicating that the borders of authority to control quality documents should not be fixed. This issue is even more evident in electrical engineering adjustment conditions, when the installation information, testing reports, power distribution parameters, commissioning instructions, and rectification evidence have to be accessed by various stakeholders at different hours. If permission updates lag behind actual process changes, quality collaboration efficiency and responsibility clarity will both be affected. Therefore, this paper designs a blockchain-based quality traceability and dynamic authority mechanism to ensure that critical quality evidence can be securely invoked, finely controlled, and fully traced throughout the project lifecycle.

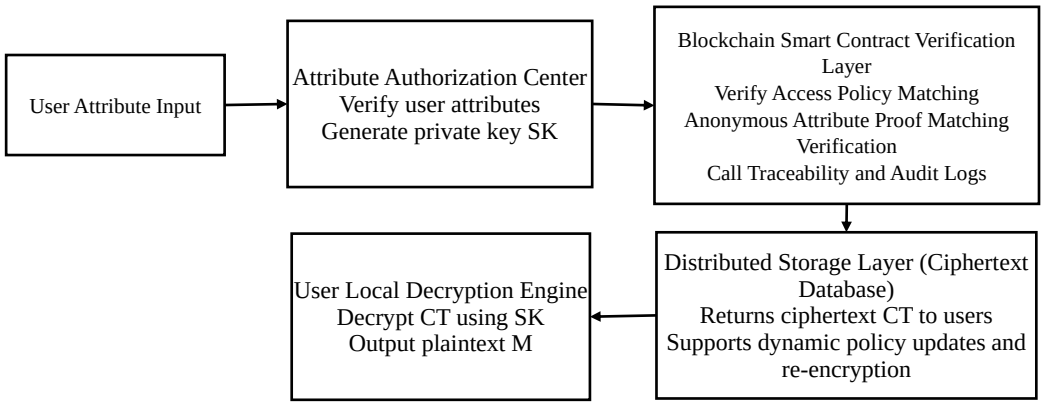

Figure 3: Structure diagram of blockchain-based quality traceability and dynamic authority mechanism

First, to address the issues of dynamic attribute updates and real-time changes in access policies, an asymmetric attribute-policy update mechanism was introduced. This mechanism

enables the user attribute set to be securely updated without exposing the private key, and the system can flexibly adjust the ciphertext structure and access permission according to the new policy. The expression of this update process is as follows:

$$\begin{cases} SK_{new} = U_{update}(Attr_{new}, SK) \\ CT_{new} = (AC_{new}, CT) \end{cases} \tag{8}$$

Among them, SK_{new} represents the updated attribute key, $Attr_{new}$ is the new attribute set of the user, AC_{new} represents the new access control policy, and CT_{new} is the updated ciphertext generated based on the policy change. This mechanism ensures that users can still maintain controlled data access capabilities in highly dynamic scenarios such as engineering role adjustments and outsourcing party replacements.

Secondly, to alleviate the key distribution pressure of the system when multiple users access concurrently, this paper designs a distributed key authorization center mechanism. This mechanism sets up multiple independent but on-chain collaborative authorization nodes in the blockchain network to jointly complete the tasks of key generation and distribution, effectively achieving load balancing and authorization transparency. Its mathematical expression is as follows:

$$\begin{gathered} \text{Distribute}(SK) = \\ \{\text{AuthC}enter_1, \text{AuthC}enter_2, \ldots, \text{AuthC}enter_n\} \end{gathered} \tag{9}$$

In the formula, $\text{Distribute}(SK)$ represents the set of authorized nodes responsible for the current key distribution task. This mechanism enhances the scalability and stability of the system in large-scale engineering projects, and is particularly suitable for multi-party key management in general subcontracting and subcontracting collaboration scenarios.

Thirdly, in terms of the expression of access control policies, traditional models mostly adopt Boolean threshold logic, which is difficult to support the complex access requirements in engineering data. Actual engineering permissions often involve multi-dimensional restrictions, such as stage constraints, organizational affiliation, job levels, access time periods, etc. A single logic is difficult to fully express them. To this end, this paper introduces a policy construction method based on logical expressions, taking attribute sets and logical structures as input, to dynamically generate access control policies that support nesting and constraint conditions. The constructor is defined as:

$$AC = AC_{construct}(Attributes, Logic) \tag{10}$$

Among them, $Attributes$ is the set of user-available attributes, $Logic$ represents the conditional expressions constructed by logical operations such as AND, OR, and NOT, and AC is the generated policy structure. The approach can be used in more complicated situations, e.g., Only safety management employees approved by the supervisory office during the construction process are allowed to use it between 8 a.m. and 6 p.m.

Fourth, regarding privacy protection, since access permissions in real life engineering sometimes include sensitive data like personnel organizational features and job permissions, the model provides a proof of anonymous attribute whereby the users can authenticate access permission without revealing their own attributes. The core process of this mechanism is as follows:

$$Proof = Prove_{\text{an}on}(SK, AC) \tag{11}$$

$$\{Acpt, Reject\} = Verify(Proof, AC) \tag{12}$$

In the above process, $Proof$ represents the anonymous attribute proof generated by the user, and the$Verify$ function determines whether it meets the data access policy AC based on this proof. If the verification is successful, return "Accept"; otherwise, return "Reject". This mechanism is particularly suitable for data authorization collaboration between subcontractors and regulators, effectively preventing the leakage of sensitive attributes.

Fifth, the data distribution process adopts an improved ciphertext broadcasting mechanism. The system automatically delivers the ciphertext to the user set that meets the policy based on access authorization. The process is represented as:

$$\text{Transmit}(CT) = (User_1, User_2, \dots, User_m) \tag{13}$$

This mechanism records the ciphertext delivery trajectory on the chain. By combining the block timestamp with the user's public key, it can achieve complete data flow traceability and provide a clear evidence chain for data abuse or forwarding behavior.

To further prevent potential risks such as key leakage and unauthorized abuse, the model is equipped with a key revocation and blacklist mechanism. When a user's key is detected to be leaked or misused, the system can add them to the blacklist based on their attributes or identities and perform key reconstruction and policy replacement operations. The expression is as follows:

$$SK_{revoked} = Revoke(SK_{\text{compromised}}, EL, PP, MK)$$

Among them, $SK_{\text{compromised}}$ represents the leaked key, BL is the current blacklist, PP is the system's public participation, MK is the primary key, and $SK_{revoked}$ is the newly generated alternative key. This mechanism ensures that the system has a certain ability to recover from attacks and supports a regular key rotation strategy. In conclusion, the data access control and traceability framework constructed based on blockchain and the optimized CP-ABE mechanism not only effectively resolves the limitations of traditional models in terms of attribute changes, policy expression, and performance bottlenecks, but also significantly enhances the implementation ability and operational security of the system in engineering practice.

4 Experimental Verification and Practical Effect Analysis of the Intelligent Whole-Process Quality Management Model

4.1 Performance Analysis of the Quality Data Authority-Control Mechanism

To systematically evaluate the operational performance of the proposed authority-control and traceability mechanism in whole-process quality management scenarios, this study constructs a simulation platform for construction quality collaboration. The experimental environment remains consistent with that described above. The evaluation focuses on the processing efficiency, key-management capability, storage scalability, attack resistance, and information stability of the platform when handling quality records generated from inspection, acceptance, rectification, and electrical adjustment activities. In order to maintain comparability of technical results, KP-ABE and SP-ABE are selected as benchmark

algorithms, while the improved CP-ABE mechanism proposed in this paper is treated as the core support technology of the intelligent quality-management model.

In terms of computational efficiency, 160KB of engineering logs were selected as the encryption objects. The encryption and decryption operations of CP-ABE, KP-ABE and SP-ABE algorithms were performed respectively, and the average time consumption was recorded. Each group of experiments was repeated 50 times and the average value was taken to eliminate random fluctuations. The result is shown in Figure 4.

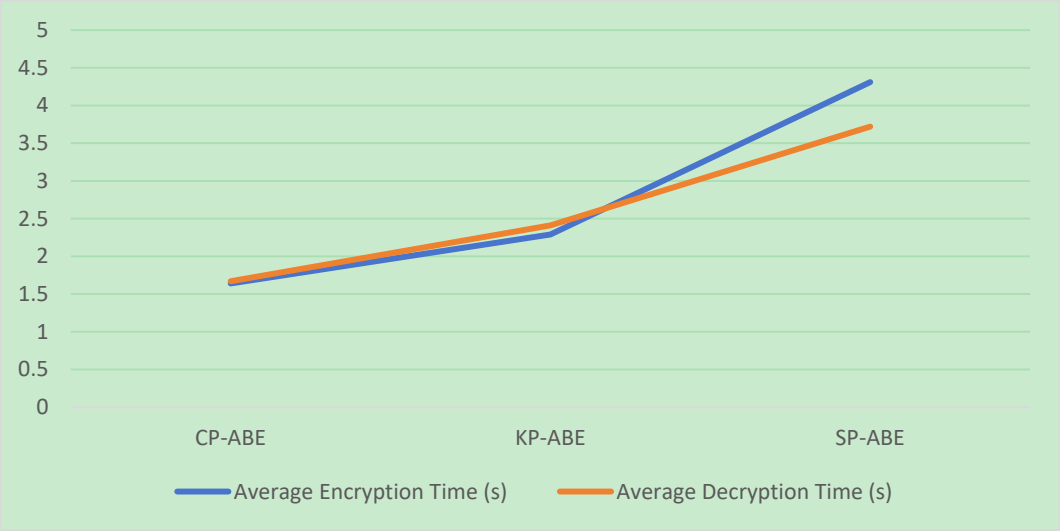

Figure 4: Average processing time of different algorithms in quality data encryption and decryption

It can be seen from Figure 4 that as the plaintext scale increases, the encryption and decryption times of the three algorithms all show an upward trend. However, the CP-ABE algorithm always maintains the lowest latency in overall performance, indicating that the proposed access control mechanism has obvious advantages in computing resource consumption and can effectively support high-frequency access and large-scale data processing tasks. Meet the demand for real-time response at the engineering site.

Furthermore, to evaluate the applicability of the model in terms of security control, a four-index system of "refined access control capability", "privacy protection mechanism support", "convenience of encryption key management" and "key secure distribution capability" was constructed. The functional coverage of the four types of encryption models was compared, and the results are shown in Table 2.

Table 2: Support Capabilities of Different Algorithms in the dimension of security Control (Support is 1, non-support is 0)

Algorithm Type	Fine-Grained Access Control	Privacy Protection	Key Management Convenience	Secure Distribution Capability
ABE	0	1	0	1
SP-ABE	0	1	1	1
KP-ABE	1	1	0	1
CP-ABE	1	1	1	1

As can be seen from Table 2, the CP-ABE algorithm performs excellently in all four capabilities. Not only does it achieve the ability to express permission control on a

fine-grained basis, but it also improves the operational convenience of key distribution and administration. It is particularly suitable for typical scenarios in engineering projects where multiple parties collaborate, roles are dynamically changed, and data is accessed at multiple levels. In terms of system scalability, the research simulated the storage space required by each algorithm's access control model under different user scales (400-800 people), and the results are shown in Figure 5.

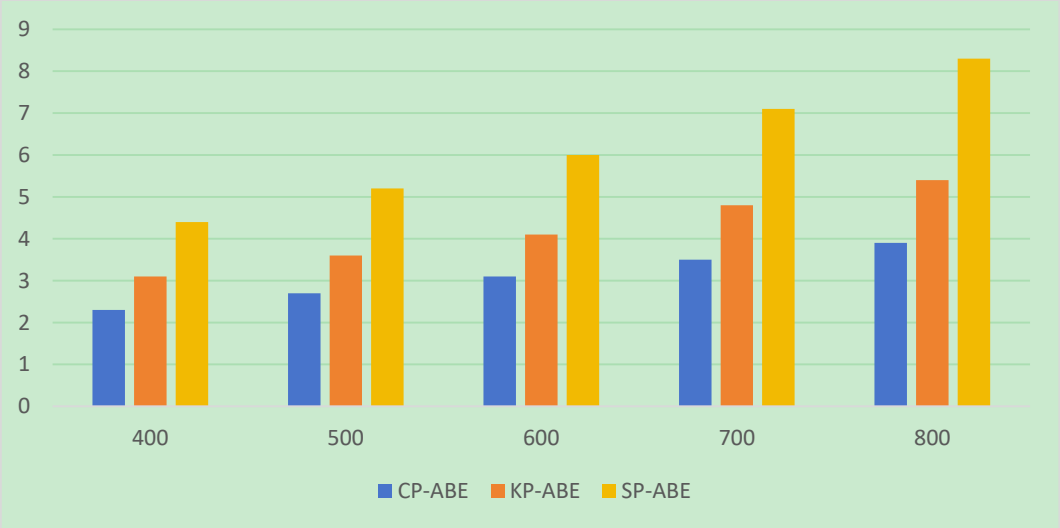

Figure 5: Storage-space variation of different algorithms under the growth of quality-management participants

The results show that with the growth of the number of users, the storage requirements of all algorithms increase linearly. However, the space required by the CP-ABE algorithm is significantly lower than that of other models. Especially in the scale of 800 people, its storage occupation is only 47% of that of the SP-ABE model, which greatly alleviates the performance burden of the system in the scenario of massive users. It provides a stronger scalability foundation for the deployment of engineering platforms. To further test the model's anti-attack capability in a distributed network environment, three typical attack scenarios - Sybil attack, DoS attack and U2R (User Privilege escalation) attack - were simulated. The resistance success rates of different models were recorded respectively, and the results are shown in Table 3.

Table 3: Resistance Success Rates of Different Models against Three Types of Attacks (Unit: %)

Attack Type	CP-ABE	KP-ABE	Model in Reference [20]
Sybil	99.21	91.35	97.58
DoS	97.54	90.67	95.33
U2R	98.43	91.82	96.05

It can be seen from Table 3 that the CP-ABE model demonstrates extremely high defense capabilities in all three attack scenarios. Its security is comprehensively superior to the KP-ABE algorithm and existing models, fully verifying the stability and reliability of the proposed model in complex engineering collaborative networks. Finally, to evaluate the stability of information leakage of the system under high load, 1000, 2000, and 3000

concurrent user requests were set to monitor the changes in the information leakage rate. The results are shown in Figure 6.

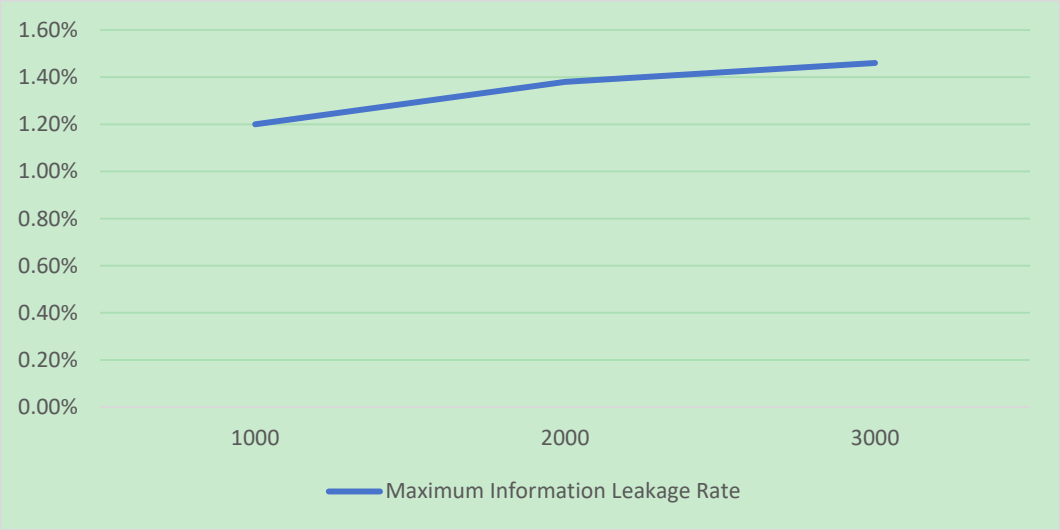

Figure 6: Variation curves of information leakage rate under different quality-platform loads

As can be seen from Figure 6, with the increase in the number of user requests, the information leakage rate shows an upward trend, but the growth rate gradually slows down, indicating that the model has strong high-load adaptability and stability, and still maintains a good privacy control effect in the sudden access scenarios of engineering projects. In conclusion, the experimental results comprehensively verify the feasibility and superiority of the blockchain-based authority-control mechanism built on the CP-ABE algorithm from the perspectives of encryption and decryption performance, completeness of security mechanisms, system scalability, attack resistance, and information stability, providing efficient, secure, and scalable technical support for whole-process quality-record management, traceability control, and collaborative quality governance in construction engineering projects.

4.2 Analysis of the Practical Application Effect of the Whole-Process Quality Traceability Model

To verify the practical application effect of the proposed model in construction engineering quality governance, this study further evaluates the platform from the perspectives of quality-record generation efficiency, traceability response capability, and local resource occupation. The test process is built around typical business scenarios such as inspection record uploading, concealed-work evidence storage, quality rectification confirmation, electrical commissioning data submission, and cross-party review of adjustment results. Under this setting, KP-ABE and SP-ABE are still used as comparison objects, while the CP-ABE-based mechanism is deployed as the underlying support module of the intelligent whole-process quality management model.

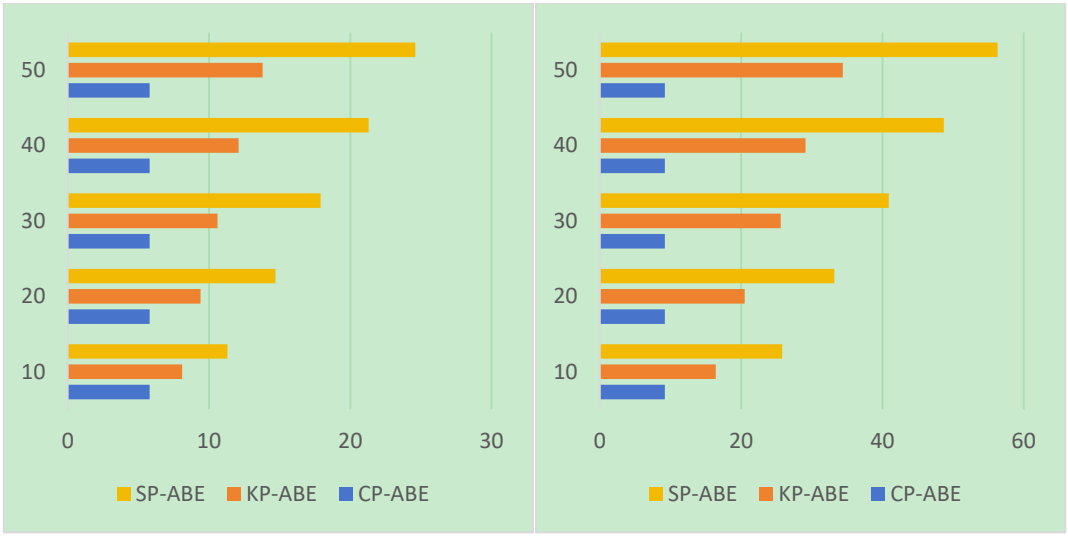

Figure 7: Comparison of ciphertext length and upload delay of different algorithms in quality-record processing

As can be seen from Figure 7, the ciphertext length generated by the CP-ABE model remains constant at 5.8KB when the number of attributes increases, indicating that its encryption strategy has good stability in terms of space complexity and greatly reduces the on-chain storage pressure. In terms of upload time consumption, the CP-ABE algorithm averages only 9.2ms and does not fluctuate with the change of the number of attributes. It is significantly superior to the KP-ABE and SP-ABE algorithms, indicating that this model has better on-chain release efficiency and time control ability in practical applications. To investigate the system's occupation of local computing resources under different encryption conditions, the memory and CPU usage rates of three algorithms in multi-attribute scenarios were tested. The experimental results are shown in Figure 8.

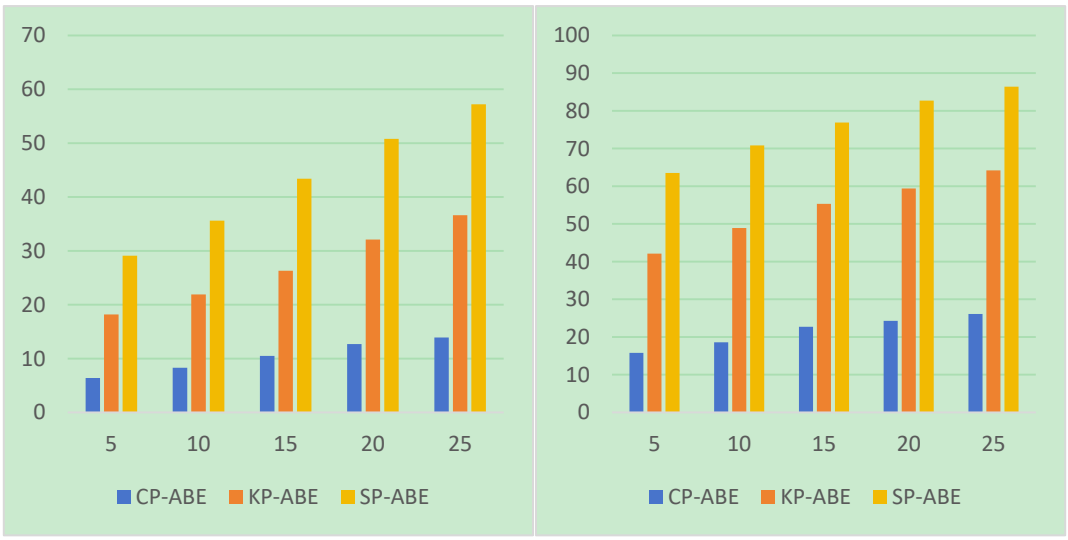

Figure 8: Resource occupation of different algorithms during quality-record encryption

From the results in Figure 8, it can be seen that CP-ABE has significantly lower memory and CPU usage than KP-ABE and SP-ABE under the same number of attributes. Especially when there are 25 attributes, the memory consumption of CP-ABE is only 13.9MB, and the CPU usage remains at 26.1%, which is reduced by more than 50% compared with SP-ABE.

This indicates that the application of this algorithm on embedded terminals or lightweight nodes has higher adaptability and can effectively control resource costs. In addition, to evaluate the impact of the CP-ABE mechanism on the traceability processing of engineering data from the perspective of the overall system operation, this study designed a comparative experiment on latency and system throughput, and set data distribution tasks under different attribute scales to simulate the transaction execution rate and processing load of blockchain nodes. The results are shown in Table 4.

Table 4: System Performance Comparison of Different Algorithms in Traceability Verification Scenarios

Number of Attributes	Latency (s) CP-ABE	Latency (s) KP-ABE	Latency (s) SP-ABE	Throughput (bit) CP-ABE	Throughput (bit) KP-ABE	Throughput (bit) SP-ABE
10	0.31	0.66	1.55	602.3	375.8	119.6
20	0.35	0.70	1.67	598.4	364.7	111.3
30	0.37	0.73	1.74	590.1	351.6	102.8
40	0.39	0.76	1.79	582.7	340.2	95.1
50	0.41	0.81	1.85	574.3	329.6	88.9

It can be seen from the data in Table 4 that as the number of attributes increases, the latency of the three algorithms slightly rises. However, the latency of CP-ABE always remains within 0.41 seconds, and the throughput is stably maintained above 570 bits, which is significantly better than other algorithms. Especially in a multi-user concurrent data verification environment, CP-ABE can respond quickly and maintain high concurrent processing efficiency, effectively ensuring the real-time performance and traceability of on-chain traceability records. The above analysis results show that the blockchain traceability mechanism driven by CP-ABE not only has significant advantages in ciphertext-structure stability, upload efficiency, and resource-occupation control, but also demonstrates good system-response ability and throughput performance in practical whole-process quality-management scenarios, and can meet the traceability requirements of quality records under multiple participants and multiple authority levels. It provides a solid technical guarantee for the trusted circulation of quality evidence, the closed-loop handling of rectification activities, and the accountability mechanism of quality-management behaviors.

5 Discussion

To address the long-standing problems of fragmented records, delayed feedback, unclear responsibility, and weak cross-specialty coordination in construction engineering quality management, this paper proposes an intelligent whole-process quality management model supported by blockchain and CP-ABE. According to the experimental findings, the model has obvious advantages when compared with the conventional approaches in terms of processing efficiency, authority flexibility, and the scalability of the system, which means that it can be used not only as a reliable tool to store quality evidence but also as a dynamic means to organize inspection, acceptance, rectification and adjustment processes. The importance of the model is particularly noticeable in electrical engineering subsystems in practical project settings. Since installing a power distribution system, laying cables, commissioning equipment, and electromechanical joint debugging are all high-density

quality records and multi-party processes, conventional management cannot guarantee simultaneous updates of responsibilities and quality records. The model developed in this paper offers a practicable solution to this issue through incorporating trusted on-chain storage, granular authority distribution, and full traceability of quality behaviors. This is why its importance should be seen beyond enhancing data safety but ensuring the structural optimization of the whole-process quality management in intelligent construction projects.

6 Conclusion

This paper focuses on the optimization path of whole-process quality management in construction engineering projects in the intelligent era, and constructs an intelligent quality-governance model supported by blockchain and CP-ABE. By introducing trusted evidence storage, fine-grained authority control, and end-to-end traceability into the management of quality records, inspection behaviors, rectification processes, and electrical adjustment data, the proposed model enhances the continuity, transparency, and responsiveness of project quality control. The experimental results show that the underlying mechanism maintains stable ciphertext length at 5.8 KB and upload time at 9.2 ms; under 25 attributes, memory usage is only 13.9 MB and CPU utilization is 26.1%; under larger user scales, storage occupation remains significantly lower than that of comparison models; resistance success rates against Sybil, DoS, and U2R attacks all exceed 97%; and latency in traceability scenarios remains within 0.41 s with throughput above 570 bits. These results verify that the proposed model has good application value in intelligent construction environments, especially in the collaborative quality control of electrical installation, power-system adjustment, and multi-specialty commissioning. Future work can further strengthen the integration of BIM, IoT sensing, and edge-side quality analysis, so as to improve the real-time adjustment capability of the whole-process quality management system.

References

[1] Hu Z, Yang Y, Wu J, et al. A secure and efficient blockchain-based data sharing scheme for location data[C]//Proceedings of the 2022 4th International Conference on Blockchain Technology. 2022: 110-116.https://doi.org/10.1145/3532640.3532655

[2] Shishehgarkhaneh M B, Moehler R C, Moradinia S F. Blockchain in the construction industry between 2016 and 2022: a review, bibliometric, and network analysis[J]. smart cities, 2023, 6(2): 819-845.https://doi.org/10.3390/smartcities6020040

[3] Elbashbishy T S, Ali G G, El-adaway I H. Blockchain technology in the construction industry: mapping current research trends using social network analysis and clustering[J]. Construction management and economics, 2022, 40(5): 406-427. https://doi.org/10.1080/01446193.2022.2056216

[4] Yong J, Lei X, Huang Z, et al. A Blockchain-Based Supervision Data Security Sharing Framework[J]. Applied Sciences (2076-3417), 2024, 14(16). https://doi.org/10.3390/app14167034

[5] Basheer M, Elghaish F, Brooks T, et al. Blockchain-based decentralised material

management system for construction projects[J]. Journal of Building Engineering, 2024, 82: 108263. https://doi.org/10.1016/j.jobe.2023.108263

[6] Zhang G, Yang Z, Liu W. Blockchain-based decentralized supply chain system with secure information sharing[J]. Computers & Industrial Engineering, 2023, 182: 109392. https://doi.org/10.1016/j.cie.2023.109392

[7] Wang S, Yang M, Jiang S, et al. BBS: A secure and autonomous blockchain-based big-data sharing system[J]. Journal of Systems Architecture, 2024, 150: 103133. https://doi.org/10.1016/j.sysarc.2024.103133

[8] Liu Y, Zeng J. Government data sharing based on blockchain[C]//Proceedings of the 2021 3rd International Conference on Blockchain Technology. 2021: 123-128. https://doi.org/10.1145/3460537.3460562

[9] Gao H, Zhong B, Ding L. A blockchain-based engineering design review service trading scheme for digital building permits[J]. Automation in Construction, 2024, 165: 105496. https://doi.org/10.1016/j.autcon.2024.105496

[10] Zhang D M, Nie C, Zhang J Z, et al. Consortium blockchain-based tunnel data bank for traceable sharing and treatment of structural health monitoring data[J]. Automation in Construction, 2024, 167: 105720.https://doi.org/10.1016/j.autcon.2024.105720

[11] Hijazi A A, Perera S, Calheiros R N, et al. A data model for integrating BIM and blockchain to enable a single source of truth for the construction supply chain data delivery[J]. Engineering, Construction and Architectural Management, 2023, 30(10): 4645-4664.https://doi.org/10.1108/ECAM-03-2022-0209

[12] Ma W, Wei X, Wang L. A security-oriented data-sharing scheme based on blockchain[J]. Applied Sciences, 2024, 14(16): 6940.https://doi.org/10.3390/app14166940

[13] Sun Y, Liu C, Li J, et al. FADSF: A Data Sharing Model for Intelligent Connected Vehicles Based on Blockchain Technology[J]. Computers, Materials & Continua, 2024, 80(2). https://doi.org/10.32604/cmc.2024.048903

[14] Elapolu M S R, Rai R, Gorsich D J, et al. Blockchain technology for requirement traceability in systems engineering[J]. Information Systems, 2024, 123: 102384. https://doi.org/10.1016/j.is.2024.102384

[15] Wang Z, Guan S. A blockchain-based traceable and secure data-sharing scheme[J]. PeerJ Computer Science, 2023, 9: e1337.https://doi.org/10.7717/peerj-cs.1337

[16] Xiao L, Sun W, Chang S, et al. Research on the construction of a blockchain-based industrial product full life cycle information traceability system[J]. Applied Sciences, 2024, 14(11): 4569. https://doi.org/10.3390/app14114569

[17] Bahnas N, Adel K, Khallaf R, et al. Monitoring and controlling engineering projects with blockchain-based critical chain project management[J]. Automation in Construction, 2024, 165: 105484.https://doi.org/10.1016/j.autcon.2024.105484

[18] Wu H, Jiang S, Cao J. High-efficiency blockchain-based supply chain traceability[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(4): 3748-3758. https://doi.org/10.1109/TITS.2022.3205445

[19] Chen Z. Enhancing the engineering supervision process in China: A solution enabled by integrating hybrid blockchain system[J]. Innovation and Green Development, 2023, 2(4): 100091. https://doi.org/10.1016/j.igd.2023.100091

[20] Xu Y, Chi M, Chong H Y, et al. When BIM meets blockchain: A mixed-methods literature review[J]. Journal of Civil Engineering and Management, 2024, 30(7): 646-669. https://doi.org/10.3846/jcem.2024.21638