



Cross-domain Joint Traceability Scheme Based on Layered Blockchain

Jinhui Li¹ and Lifeng Cao^{1,*} and Xiaoqin Wang²

¹ He'nan Province Key Laboratory of Information Security, Zhengzhou, China

² China Electronics Technology Group Corporation Seventh Research Institute, Guangzhou, China

*caolf302@sina.com

Abstract. With the acceleration of the digitalization process, data sharing has become an important driving force to promote the development of various industries. However, organizations or departments involved in data sharing usually belong to different trust domains, and the differences in trust domains have brought a series of security challenges that cannot be ignored while promoting data sharing. By establishing a perfect cross-domain behavioral traceability system, it can contribute to the rapid localization of the problem after the occurrence of security time, or the analysis of the traceability data to discover the potential security risks in advance. This paper proposes a cross-domain joint traceability scheme based on layered blockchain, which realizes the traceability of the target user's information about the privileges received by the user in the system architecture and its cross-domain access behaviors in a multi-trust domain scenario. A method for evaluating the comprehensive reputation value of nodes based on the Fuzzy Analytic Hierarchy Process (FAHP) is designed. From the perspective of multiple factors, it realizes the ranking of the reputation values of the nodes that execute authorization behaviors. Finally, a security analysis and a performance analysis were conducted on the proposed cross-domain joint traceability scheme based on the layered blockchain.

Keywords: Blockchain, Access Control, Behavioral Traceability.

1 Introduction

With the rapid development of information technology, big data, cloud computing and other foreword technologies are deeply integrated into various fields and widely used in various scenarios. With the rapid development of information technology, big data, cloud computing and other foreword technologies are deeply integrated into various fields and widely used in various scenarios. This trend has led to increasingly frequent interactions among enterprises, departments, organizations, and users. Whether it is the collaborative cooperation between enterprises, the information sharing within organizations, or the interaction between users and devices, all have become closer and more efficient, thus establishing a complex and dynamic cross-domain interaction network

© The Author(s) 2025

G. M. Lee et al. (eds.), *Proceedings of the 2025 4th International Conference on Bigdata Blockchain and Economy Management (ICBBEM 2025)*, Advances in Intelligent Systems Research 195,

https://doi.org/10.2991/978-94-6463-742-7_36

[1]. In the digital era, data has become a crucial asset. As one of the core means to ensure data security, access control plays an important role. The aim of access control is to ensure that only authorized entities can access specific data resources. In traditional centralized systems, access control mainly relies on a central server to verify users' identity information and authorize their access. However, it has shown obvious deficiencies in complex cross-domain environments. Moreover, the differences in security policies between systems complicate cross-domain identity authentication and access control for users. At the same time, issues such as data privacy protection, audit traceability, responsibility tracing, and compliance verification become particularly prominent during cross-domain data sharing. These challenges require resolution through standardized cross-domain collaboration mechanisms and technological innovation.

Increasingly frequent cross-domain data interactions have prompted people to explore new solutions, and blockchain technology, with its decentralized, non-modifiability, and traceable features, has brought new ideas for solving cross-domain access control problems. In terms of access control, smart contracts can be utilized to precisely control the access rights of each role to data according to the cooperation agreements among all participating parties. Only users whose access rights meet the restrictions are allowed to access the corresponding data, which improves the flexibility and security of access control. However, access control based on blockchain technology is not without flaws. With the continuous increase in data volume and access operations, the user access records in the system are also growing rapidly, which makes the tracking and review of users' access behaviors more complicated. In the face of massive access behavior data, it is difficult for administrators to quickly and accurately locate specific access events. For example, in a cross-domain collaborative project, the access rights of users with different ownerships to the project data vary depending on the project stage and their responsibilities. The decentralized storage of cross-domain access records has increased the difficulty of sorting out and auditing these records.

Cross-domain joint traceability is a method that integrates data, technologies, and resources from multiple parties to achieve traceability of the entire process of access control between domains. Every link, from the access request initiated by the user, the granting of permissions, the verification of permissions, to the execution of the final access operation, can be clearly presented. It contributes to the discovery of potential inter-domain access control vulnerabilities. In addition, cross-domain joint traceability provides strong support for auditing user access behavior and checking access control compliance. In the current context where data security and privacy protection are highly concerned, the regulatory authorities can conduct a comprehensive review of the access behaviors of users from other departments to data resources based on the accurate traceability records on the blockchain. This can effectively prevent unauthorized access behaviors and truly safeguard private data from being infringed upon.

Aiming at the above situation, this paper proposes a cross-domain joint traceability scheme based on layered blockchain. For the joint traceability of the access behaviors generated when users conduct cross-domain access in a multi-trust domain scenario, a layered blockchain cross-domain joint traceability architecture without an authoritative center is designed to accurately achieve joint traceability of a certain user's cross-domain access behaviors within the entire domain. A node comprehensive reputation

evaluation method based on the Fuzzy Analytic Hierarchy Process (FAHP) is adopted to elect consensus nodes, so as to ensure that the access applications, authorization records and access behaviors of users during cross-domain access can be reliably recorded on the blockchain.

The remaining structure of this paper is as follows: In the second part, the related work is introduced. The third part presents the cross-domain joint traceability scheme based on the layered blockchain and its joint traceability algorithm. The third part describes the method for evaluating the comprehensive reputation value of nodes based on FAHP. The fourth part analyzes and evaluates the scheme proposed in this paper. Finally, the fifth part summarizes this paper and prospects the future work.

2 Related Work

Establishing a comprehensive data management and sharing framework is of great significance for data management across trust domains [2]. Cross-domain data sharing has been widely applied in various fields, yet it is confronted with enormous obstacles, mainly the privacy issues. Aiming at the problems of role naming conflicts, inter-domain management conflicts, and difficulties in cross-domain sharing brought about by the traditional Role-Based Access Control (RBAC) model in the complex multi-domain environment and in the face of numerous users, Li et al. [3] proposed a role-based access control model for inter-system cross-domain (RBAC-IC) in a multi-domain environment. They divided roles into abstract roles and specific roles, and designed the operation process of the access control model to achieve fine-grained cross-domain sharing. For the scenario of frequent authorization changes, Jiang et al. [4] proposed a Spectral Clustering (SC) and Risk-Based Access Control model (SC-RBAC) to quantify the accuracy of the risk of user access behaviors based on the user's historical access data, and then assigns access privileges to the user through the constructed access control function. In order to control users' access to cross-domain data resources, He et al. [5] proposed a cross-domain access control protocol CDAC. According to the user reputation evaluation strategy proposed in the protocol, the network management node can evaluate users' cross-domain requests. The security level of users is evaluated based on their access behaviors, and different priorities are assigned to achieve the cross-domain access control of users by different gateway nodes. However, it cannot ensure that users' historical access behaviors are comprehensive and reliable. Their historical access behaviors are easily tampered with, which will affect the true evaluation of users' security levels.

However, the lack of a unified trust standard and collaborative mechanism among different domains makes it difficult to achieve efficient and secure cross-domain access. Scholars have utilized the unique features brought about by blockchain technology to provide system stability and security for cross-domain access control. Aiming at the identity authentication and security trust issues faced by the Public Key Infrastructure (PKI) system, Zhang et al. [6] proposed a lightweight blockchain-based PKI identity management and authentication architecture. They also designed a trust chain based on smart contracts to replace the traditional Certificate Authority (CA) trust chain, so as to

avoid the communication pressure caused by the transmission of a large number of certificates. However, it is difficult to ensure that there is no risk of data privacy leakage in users' previous cross-domain access behaviors. Sun et al. [7] constructed a blockchain-based trustworthy and efficient cross-domain access control system. It inherits blockchain and role mapping technologies to achieve a reliable and verifiable cross-domain access process, and uses smart contracts to make access decisions according to the roles and access policies recorded on the blockchain. However, it fails to achieve a comprehensive traceability of the historical access behaviors of roles. Aiming at the problem of potential privacy leakage during cross-domain data sharing, Yao et al. [8] designed a blockchain-based intelligent cross-domain access log system for doctors, which is used to record, query and analyze the cross-domain access behaviors of doctors after authorization. Through the DBscAN clustering analysis of doctors' cross-domain access logs, abnormal phenomena in cross-domain access can be detected, so as to dynamically control the cross-domain access behaviors of doctors and reduce the risk of data leakage. However, the process of uploading the logs to the blockchain is completed by several fixed and unchanging nodes, which cannot prevent internal attacks.

3 Cross-domain Joint Traceability Scheme Based on Layered Blockchain

User nodes have access behaviors to data resources in various trust domains within a multi-trust domain environment. Based on the access behavior information and authorization information recorded and stored in each domain, the behaviors of all users accessing data resources can be traced. This can provide guidance for the cross-domain access policies in the entire domain. At the same time, it also plays a role in supervising users' authorizations and their access behaviors. In response to the problem that in high-frequency cross-domain access scenarios under multiple trust domains, centralized authentication and access services are prone to security risks due to malicious attacks or single-point failures, this paper proposes a cross-domain joint traceability scheme based on a layered blockchain. This scheme aims to achieve joint traceability of users' access behaviors across the entire domain, ensuring that access behaviors across different trust domains can be accurately traced, verified, and authorized, and safeguarding the security, integrity, and traceability of information.

3.1 System Architecture

The authentication for cross-domain joint traceability is carried out by means of identity signature authentication. A non-authoritative-center signature authentication scheme is designed to achieve decentralized, reliable, and secure authentication and access for tracing the access behaviors of users across different trust domains. The architectural structure of the cross-domain joint traceability model based on the layered blockchain is shown in Fig. 1. The multi-trust domain system is divided into two layers, the upper layer and the lower layer. The lower layer is composed of various trust

domains. Each trust domain will conduct a comprehensive evaluation of the reputation values of the nodes within its own domain, so as to elect a group of delegated node groups. The delegated node groups elected by each domain jointly form the global delegated node group, which becomes the upper-layer entrusted agency center. The delegated node groups of each domain can communicate with each other, transmit data in the upper-layer center, and jointly maintain the cross-domain access policies of the entire trust domain.

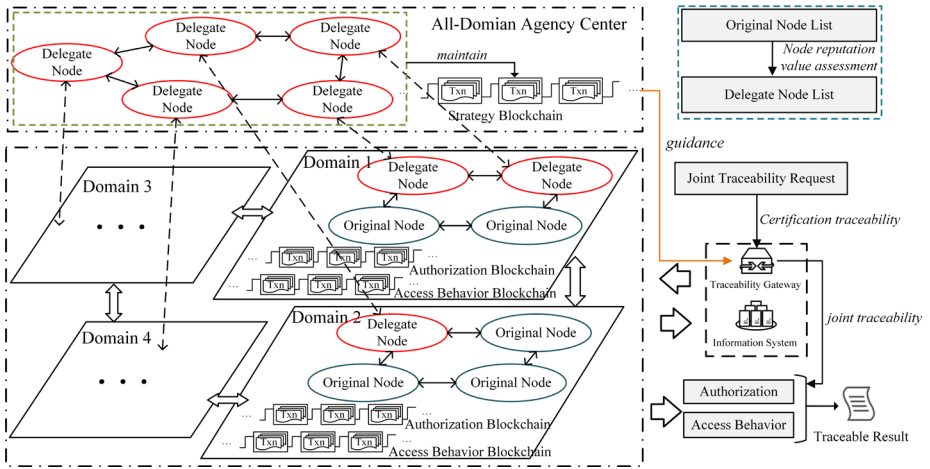


Fig. 1. The architectural structure of the cross-domain joint traceability model based on the layered blockchain.

Description of elements in a cross-domain joint traceability architecture based on layered blockchain:

(1) Ordinary Node: Ordinary user nodes that fail to be successfully elected as delegated nodes store the data of the authorization chain and the access behavior chain of their own domains locally. When a node conducts authentication joint traceability within its own trust domain, it first needs to send a traceability authorization application to the delegated node in its own domain. After obtaining the traceability authorization certificate of its own domain, it can conduct access traceability on the user access behavior data within the authorized scope. When a node conducts cross-domain authentication joint traceability, it needs to hold the traceability authorization certificate of its own domain. It sends a cross-domain authentication application to the delegated node of its own domain, and the delegated node of its own domain forwards the application to the delegated node of the target access domain. After the node obtains the traceability authorization certificate of the target domain, it can conduct joint traceability on the user access behavior data within the authorized scope in the target domain.

(2) Delegate Node: There are multiple delegate nodes in a trust domain, which are elected by ordinary nodes with high comprehensive reputation value. In addition to having the rights and interests of ordinary nodes, delegated nodes also have the

responsibility of issuing traceability authorization certificates to ordinary nodes in multiple trust domains.

(3) All-Domain Agency Center: The All-Domain Agency Center at the upper layer of the system is jointly composed of the delegated nodes in all trust domains. It is responsible for transmitting the cross-domain authentication access applications of the nodes in the lower layer at the upper layer, and maintaining the access strategy chain of the upper layer. It records the access control policies among various trust domains. When conducting joint traceability of the access behavior of a certain node user, it will provide guidance based on the access policies stored in the strategy chain.

(4) Information System: Each trust domain has its own maintained information system, which is available for the node users within the domain to access the owned data resources.

(5) Traceability Gateway: It is used for nodes to trace the access behaviors of target nodes within the domain to which the gateway belongs to the multi-domain data resources.

(6) There are three types of blockchains in the system: the authorization chain, the access behavior chain, and the strategy chain. Among them, the authorization chain and the access behavior chain are maintained by each domain independently, while the strategy chain is maintained by the upper-layer agency center.

1. The authorization chain: Besides recording the authentication access certificate that grants the node to apply for access to the data resources in this domain, the traceability authorization certificate information of the node is stored and recorded. When tracing the cross-domain access behavior of a target node, one should first send an application for a traceability authorization certificate to the delegated node group of one's own domain. The delegated node will then issue a traceability authorization certificate of the domain to this node. The authorized node can directly trace the access behavior records of the node in this domain. If it is necessary to trace the access behavior of a target node in other domains, first, apply to the delegated node of one's own domain for the cross-domain access strategy of the domain where the target node is located as recorded in the strategy chain, and obtain the information of the trust domains to which the target node can apply for cross-domain access. Then, send a cross-domain traceability authorization request to the target domain through the delegated node of one's own domain. After receiving the request, the delegated node of the target domain will evaluate the identity information of the requester. After determining the permissions of this node, it will issue a traceability authorization certificate to it, and the target domain will record its authorization in the authorization chain within the domain. The information includes the number of the applying node, the number of the domain to which the node belongs, the traceability authorization certificate issued to this node by the domain, the number of the node that grants the permissions to this node, the timestamp and other information.

2. The access behavior chain: It records the access behaviors of nodes when they access the data resources within the domain. When a node in a certain domain applies to access the data resources of its target domain, whether the access is successful or not will trigger an event, which in turn activates the smart contract under the data resources, generating a record of the node's access behavior. This record will be logged in the

access behavior chain of the target domain. The information includes the number of the accessing node, the number of the accessed data resource, the timestamp, as well as the detailed content of the data resource accessed by the node and the access mode, etc.

3. The strategy chain: It records the cross-domain authentication access policies among trust domains. When a node applies for access to the data resources in a target domain, it needs to obtain the authentication access certificate of that target domain. When forwarding the authentication application information to the delegated node of its own domain, the cross-domain access policies recorded in the strategy chain among domains are used to confirm whether the application meets the standards. This chain is used in the system to ensure the complete traceability of users' access behavior trajectories to data resources. The strategy information mainly includes key elements such as the trust relationships among trust domains, the identifiers of strategy formulators and approvers, the effective time of the strategy, and its validity period.

3.2 Cross-domain Joint Traceability Scheme Process

To realize the traceability of cross-domain access behaviors of user nodes in multi-trust domain scenarios, we design the process of the proposed cross-domain joint traceability scheme.

Nodes Apply for Intra-Domain Traceability authorization Certificates. When tracing the cross-domain access behavior of a target node, one must hold the traceability authorization certificate within the domain before applying for the traceability authorization certificate of the domain where the target node is located. A request for registering a traceability authorization certificate within the domain should be sent to the delegated node within the domain. The specific process is shown in Fig.2 below.

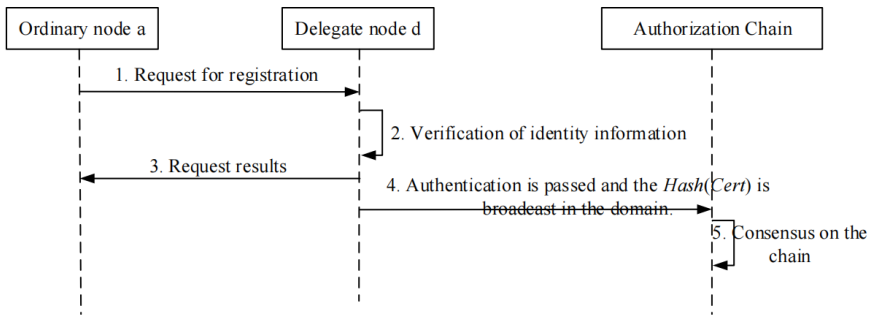


Fig. 2. Application Process for Intra-Domain Certificates.

1. The node a under the trust domain A sends an enrollment traceability authorization certificate request $Register_a$ to the delegated node d in the domain.

$$Register_a = Sig_{sk_a}(ID_a, ID_{D_A}, RegInfo_a, N_1, pk_a)$$

In which, ID_a denotes the node number of node a , ID_{D_A} denotes the number of trust domain A , $RegInfo_a$ denotes the details of the registration message of node a , $RegInfo_a = (regTime_a, regTimeLimit_a, regLevel_a)$. $regTime_a$ denotes the timestamp of the registration message of node a , $regTimeLimit_a$ denotes the duration of the registration certificate, $regLevel_a$ denotes the level of authority of the registration certificate, N_1 denotes a random number, pk_a, sk_a denotes the public and private key of node a , and $Sig()$ denotes the message signature.

2. After receiving the registration request message $Register_a$ from node a in the domain, delegate node d verifies its identity information, and if the verification passes, assigns the audited and rated privileges to node a , generates the traceability authorization certificate $Cert_a$ for it, and sends the authorization message $CertMeg_a$ to node a . Instead, it returns the re-request message.

$$Cert_a = (ID_a, ID_{D_A}, ID_d, ID_{D_A}, certTime_a, certTimeLimit_a, certLevel_a)$$

$$CertMeg_a = Sig_{sk_d}(timestamp, ID_d, ID_{D_A}, E_{pk_a}(Cert_a), N_2, pk_d)$$

In which, $CertTime_a$ denotes the authorization time of the certificate of the node a , $CertTimeLimit_a$ denotes the authorization time limit of the certificate, $CertLevel_a$ denotes the authority level of the certificate, and $E_{pk_a}()$ denotes the public key encryption information of the node a is used.

3. The delegate node d broadcasts $Hash(Cert_a)$ in the domain, reaches a consensus and records it in the authorization chain in the domain.

Nodes Apply for Cross-Domain Traceability authorization Certificates. If a node aims to trace the access behavior of a node in the target domain, it needs to hold the traceability authorization certificate of the target domain. The node sends a cross-domain registration traceability authorization certificate request to the delegated node in the target domain, and the specific process is shown in Fig.3 below.

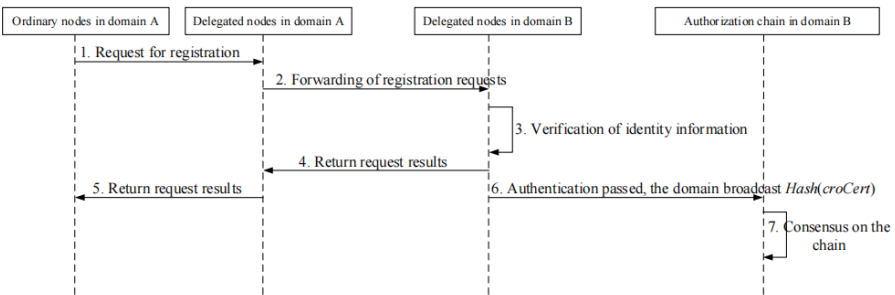


Fig. 3. Process of Applying for Cross-Domain Certificates.

1. When the node a under the trust domain A applies for joint traceability of the cross-domain access behavior of the nodes in the target domain D_{goal} , it needs to send a request for registering the cross-domain traceability authorization certificate $croRegister_a$ to the delegated node d_A under the belonging domain D_A ,

$$croRegister_a = Sig_{sk_a}(ID_a, ID_{D_A}, ID_{D_{goal}}, RegInfo_a, Cert_a, N_3, pk_a)$$

In which, $ID_{D_{goal}}$ denotes the number of the target domain, and $Cert_a$ is the authentication certificate of a in D_A . A certificate is issued for the delegated node in the target domain for a as a reference to enable the management of the privileges of a .

2. The delegate node d_A receives the cross-domain enrollment request from the node a in the domain, verifies its identity and certificate authenticity, and transmits a 's cross-domain enrollment request $transReg$ to the delegate node in the trust domain numbered $ID_{D_{goal}}$,

$$transReg = Sig_{sk_{d_A}}(ID_{d_A}, ID_{D_A}, ID_{D_{goal}}, croRegister_a, pk_{d_A})$$

3. When the delegated node d_{goal} in the target domain of D_{goal} receives $transReg$ from d_A in D_A , it verifies the identity of d_A and a . If the verification passes, it assigns privileges to a based on the evaluation and generates a cross-domain traceability authorization certificate $croCert_a$, and sends the authorization message $croCertMeg_a$ to d_A . Instead, it returns a re-request message.

$$croCert = (ID_a, ID_{D_A}, ID_{d_{goal}}, ID_{D_{goal}}, certTime_a, certTimeLimitL_a, certLevel_a)$$

$$croCertMeg_a = Sig_{sk_{d_{goal}}}(timestamp, ID_{d_{goal}}, ID_{D_{goal}}, E_{pk_a}(croCert_a), N_4, pk_{d_{goal}})$$

4. d_{goal} broadcasts a 's authorization certificate $Hash(croCert_a)$ in D_{goal} , which is eventually recorded in the authorization chain in D_{goal} .

5. d_A receives the $croCertMeg_a$ sent from d_{goal} , verifies its identity and transmits the authorization message $transCertMeg_a$ to a .

$$transCertMeg_a = Sig_{sk_{d_A}}(timestamp, ID_{d_A}, ID_{D_A}, croCertMeg_a)$$

Cross-domain Joint Traceability. When a node obtains the traceability authorization certificate in the target domain, it can conduct joint traceability of the cross-domain access behavior of the nodes within the target domain. It sends its joint traceability request to the traceability gateway of the target domain, and the gateway verifies the node's traceability authorization certificate. If the verification is passed, the cross-domain access behavior of the target node will be returned to the node according to its

traceability authority. The cross-domain joint traceability process for the target node is shown in Fig.4 below.

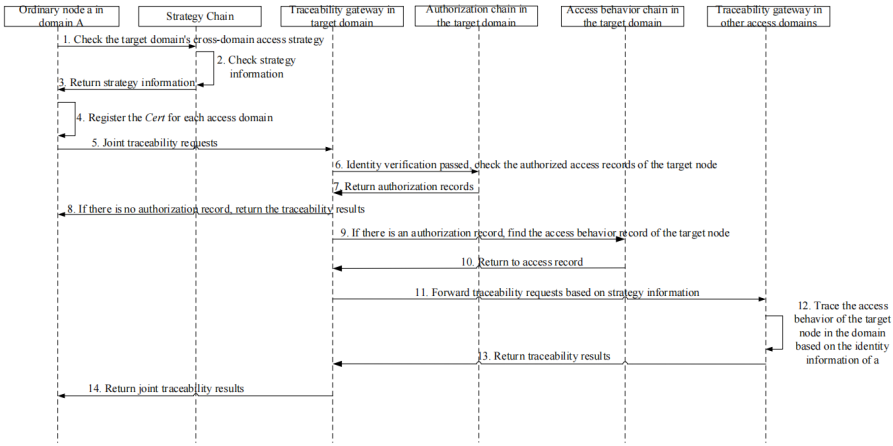


Fig. 4. Cross- Domain Joint Traceability Process.

1. When node a in domain D_A carries out joint traceability on the cross-domain access behavior of node g in target domain D_{goal} . It is first necessary to obtain the cross-domain access strategy of D_A and D_{goal} according to the strategy chain, check the trust domains that node g can apply for access, and apply for registration of the traceability authorization certificate of each trust domain according to the cross-domain access strategy.

2. Node a sends a joint traceability request $TraceReq_a$ to the traceability gateway of D_{goal} ,

$$TraceReq_a = Sig_{sk_a}(timestamp, ID_a, ID_{D_A}, ID_g, CroCertSet_a, pk_a)$$

Where $CroCertSet_a$ is the set of traceability authorization certificates issued by each access domain for a ,

$$CroCertSet_a = (< ID_{D_1}, CroCert_1 >, < ID_{D_2}, CroCert_2 >, \dots)$$

3. After receiving the joint traceability request from node a to node g , the traceability gateway of D_{goal} verifies the identity information of node a . If the identity verification passes, it checks the authorization information of the node recorded in the authorization chain in the domain. If the identity verification passes, check the authorization information of node A recorded in the authorization chain in the domain. If no authorization record for g exists, the traceability gateway returns the traceability result to a . If there is an authorization record, check the access behavior record of node g recorded in the access behavior chain in the domain according to the privilege level of

the traceability authorization certificate of node a , and generate the historical behavior record $\langle ID_{goal}, ID_g, timestamp, certLevel_a, AccRec_g \rangle$ of node g in this domain.

In which, $AccRec_g$ includes an authorization record and an access behavior record of the node g , which contains only data information up to the permissions that the node a is able to trace back. For the part without permissions, only the number of the data resource and its corresponding access permission are included.

4. The traceability gateway in D_{goal} forwards the joint traceability request of node a to the traceability gateways of each trusted domain that trusts D_{goal} according to the cross-domain access strategy of D_{goal} in the strategy chain.

5. When the traceability gateway of each domain receives the request, it executes step 3 and sends the historical behavior records $\langle ID_i, ID_g, timestamp, certLevel_a, AccRec_g \rangle$ of g in each domain to the traceability gateway of D_{goal} .

6. The traceability gateway of D_{goal} packages the received information about g 's access behavior in each domain and returns the joint traceability result $TraceRes$ to node a .

$$TraceRes = (ID_d, ID_{goal}, timestamp, AccRecSet_g)$$

In which, $AccRecSet_g$ is a collection of historical behavioral records sent by the domains.

The cross-domain joint traceability algorithm is shown below.

Algorithm 1. The cross-domain joint traceability algorithm.

Input: $TraceApplyInfo$ // traceability application information

Output: $TraceInfo$ # traceability results

- 1: **if** $TraceApplyInfo.ID_{target}$ **is in** $TG_{target}.D_{home}$: // Determine whether the target node in the traceability application information exists in the domain to which the target traceability gateway belong
 - 2: **if** $TraceApplyInfo.croTraCert$ **is in** $CertChain$: // Determine whether the cross-domain traceability authorization certificate in the traceability application information is correct and valid.
 - 3: $TraceInfo = null$
 - 4: **if** $ID_{target}.accCert$ **is in** $CertChain$: // Determine if the target node has applied for an access authorization certificate in this domain
 - 5: $CertChain.record_{ID_{target}} \rightarrow TraceInfo$
 - 6: **search** $AccessChain.record_{ID_{target}}$ **limited in** $TraceApplyInfo.certLevel$ // The information obtained by traceability is limited to the privilege level of the traceability certificate.
 - 7: $AccessChain.record_{ID_{target}} \rightarrow TraceInfo$
 - 8: **transfer** $TraceApplyInfo$ **to** TG_{other} **by** $StrategyChain$
-

```

9:   TraceInfoother → TraceInfo
10:  return TraceInfo
11:  else return TraceInfo // If the authenticated access certificate of the target node does
    not exist, the traceback result is put back directly
12:  end if
13:  end if
14:  end if

```

4 Method of Assessing Comprehensive Credibility Value of Nodes

This paper designs the architecture of a cross-domain joint traceability mechanism under multiple trust domains based on the characteristics of the consortium blockchain. In order to ensure that the bookkeeping of the consortium blockchain under multiple trust domains and the nodes within each trust domain reaches a consensus, a reliable method for evaluating the comprehensive reputation value of nodes is proposed. The node reputation value evaluation method based on FAHP is adopted to evaluate the comprehensive reputation values of nodes in the system, so as to elect and form the delegated nodes of each domain. By using this method, the reputation value of nodes can be dynamically adjusted by combining the historical behavior of nodes in the system, which helps to identify and exclude malicious nodes. It effectively solves the degradation of data security under the full domain space caused by the authorization behavior of the nodes after they are successfully elected as delegated nodes and the existence of deceptive behavior when data is uploaded to the consensus.

4.1 Calculation of Initial Reputation Values of Nodes under Each Trust Domain

Before joining the layered cross-domain joint traceability architecture, each trust domain only needs to maintain the blockchain data in each domain. After joining the architecture, the reputation value of the nodes in the domain needs to be evaluated because the delegate nodes in each domain need to be elected to jointly form the upper-level delegate agent center. At this time, cross-domain access behavior is not involved, so in the initial reputation value assessment of the nodes in each domain. So, in the evaluation of the initial reputation value of each domain node, the success rate, processing efficiency and online rate of each node in the historical performance of the blockchain in the domain are used as the evaluation indexes of the initial reputation value S .

$$S_i = V_{s_i} + V_{e_i} + V_{o_i}$$

In which, V_{s_i} denotes the success rate assessment value of node i , V_{e_i} denotes the processing efficiency assessment value, and V_{o_i} denotes the online rate assessment value.

V_s represents the honesty of a node in processing transactions and is a key indicator of whether a node is loyal or not. V_s is determined by the total number of times a node participates in transaction processing and the number of times it successfully participates in transaction processing.

$$V_{s_i} = w_s * \frac{Tp_i}{Tps_i}$$

Where, w_s denotes the weight of node success rate in the initial reputation value evaluation, denotes the number of times node Tp_i has successfully participated in transaction processing, and Tps_i denotes the total number of times it has participated in transaction processing.

V_e represents the node's ability to process transactions, and is the key indicator for evaluating the node's response speed and execution capability. V_e is determined by the average transaction processing time of the node and the shortest transaction processing time among all nodes.

$$V_{e_i} = w_e * \frac{MinTime}{AvgTime_i}$$

Where, w_e denotes the weight of node processing efficiency in the initial reputation value assessment, $MinTime$ denotes the shortest time for a node in the domain to complete a transaction, and $AvgTime_i$ denotes the average time taken by node i to participate in transaction processing.

V_o represents the proportion of time that a node participates in a transaction and is the key indicator for determining the stability of a node. V_o is determined by the length of time that a node has been joined to the trust domain and the length of time that it has been online.

$$V_{o_i} = w_o * \frac{olt_i}{t_i}$$

Where, w_o denotes the weight of the node online rate in the initial reputation value assessment, olt_i denotes the length of time that node i has been joined to this trust domain, and t_i denotes the length of time it has been online.

4.2 Node Reputation Value Evaluation Method Based on FAHP

The objective is determined as electing nodes with high reputation values to jointly form a consensus node group. In the system, the consensus node group is crucial for

maintaining the security, consistency and high efficiency of the system, and the reputation value of a node is a key factor for measuring whether it is suitable to become a consensus node.

According to the cross-domain access and traceability requirements of nodes in multiple trust domains, the computing power, storage capacity, network connection stability, legality and accuracy of historical transaction records, honest behaviors and malicious behaviors of nodes are taken as the evaluation factors of the comprehensive reputation value of nodes. When using the FAHP to evaluate the comprehensive reputation value of nodes, the hierarchical structure diagram is constructed as shown in Fig.5 below.

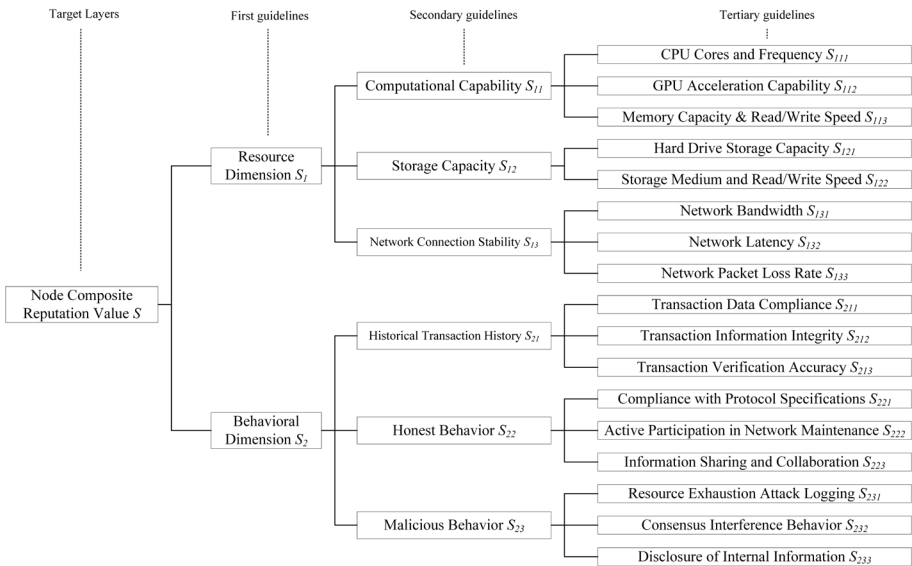


Fig. 5. The Hierarchical Structure Diagram.

According to the characteristics of the nodes in the blockchain system and the requirements for electing nodes, the experts in the evaluation team quantify the relative importance among various indicators in each layer of the indicator system in the form of triangular fuzzy numbers, and obtain the triangular fuzzy judgment matrix \tilde{A} .

$$\tilde{A} = \begin{bmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{n1} & \cdots & \tilde{a}_{nn} \end{bmatrix}$$

The element $\tilde{a}_{ij} = (l_{ij}, m_{ij}, u_{ij})$ of this matrix is a triangular fuzzy number, where l denotes the lower limit, m denotes the middle value, and u denotes the upper limit. The specific scoring rules for each indicator are shown in Table 1 below.

Table 1. Table of specific scoring rules.

\tilde{a}_{ij}	\tilde{a}_{ji}	Description of relative importance
(1,1,1)	(1,1,1)	i is as important as j
(1,1,3)	(1/3,1,1)	i and j are almost equally important
(1,3,5)	(1/5,1/3,1)	i is slightly more important than j
(3,5,7)	(1/7,1/5,1/3)	i is more important than j
(5,7,9)	(1/9,1/7,1/5)	i is significantly more important than j

The triangular fuzzy judgment matrix \tilde{A} is transformed into the crisp value matrix A . The center of gravity method is used to transform the element \tilde{a}_{ij} in \tilde{A} into the crisp value a_{ij} , which is computed as $a_{ij} = \frac{l_{ij} + m_{ij} + u_{ij}}{3}$, to obtain the crisp value matrix A .

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

Utilizing the characteristic equation $|\lambda I - A| = 0$, I is the unit matrix, $|\cdot|$ denotes the determinant, solving to get the eigenvalue λ , and finding the maximum eigenvalue λ_{max} . Then using the system of chi-square linear equations $(A - \lambda_{max}I)w = 0$, solving to get the eigenvector w , and normalizing w to get the weight vector $w = (w_1, w_2, \dots, w_n)$, w reflecting the degree of relative importance of each index in the evaluation system.

After obtaining the weight vector w , the comprehensive reputation value S of the node can be evaluated, $S = S_0 + w_1V_1 + w_2V_2 + \dots + w_nV_n$, S_0 denotes the initial reputation evaluation value of the node, $V = \{V_1, V_2, \dots, V_n\}$ denotes the set of scores of each metric factor of the node, and V_i denotes the score of the i th metric factor of the node.

However, before evaluating the comprehensive reputation value of a node, a consistency check is required to determine whether the logical relationships in the evaluation process are reasonable and to ensure the true importance of each indicator factor. Thus, a fuzzy consistency matrix C is constructed.

$$C = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{bmatrix}$$

Where, $c_{ij} = \frac{1}{n} \sum_{k=1}^n \frac{(a_{ik} - a_{jk}) + (\lambda_{max} - n)w_k}{w_i - w_j}$ (when $w_i - w_j \neq 0$).

Calculate the consistency ratio CR , $CR = \frac{CI}{RI}$. When $CR < 0.1$, the consistency of the judgment matrix is found to be acceptable. Where CI is the consistency index, $CI = \frac{\lambda_{max} - n}{n - 1}$; RI is the random consistency index B (determined according to the matrix order).

The algorithm for evaluating the comprehensive reputation value of nodes based on FAHP is proposed as follows.

Algorithm 2. Evaluating the comprehensive reputation value of nodes based on FAHP.

Input: \tilde{A}, V_{node} // \tilde{A} : triangular fuzzy judgment matrix; V_{node} : set of factor scores for each indicator of the node

Output: S_{node} // S_{node} : aggregate set of reputation values for the nodes

1: **foreach** $\tilde{a}'_{ij}, \tilde{a}''_{ij}$ **in** \tilde{A}', \tilde{A}'' : // $\tilde{a}'_{ij} \in \tilde{A}', \tilde{a}''_{ij} \in \tilde{A}''$, \tilde{A}' : Triangular fuzzy judgment matrices

for secondary guidelines, \tilde{A}'' : Triangular Fuzzy Judgment Matrix for Tertiary Guidelines

2: $a'_{ij} = \frac{l'_{ij} + m'_{ij} + u'_{ij}}{3}, a''_{ij} = \frac{l''_{ij} + m''_{ij} + u''_{ij}}{3}$

3: $a'_{ij} \rightarrow A', a''_{ij} \rightarrow A''$

4: **end**

5: **compute** $\lambda'_{max}, \lambda''_{max}$ **by** $|\lambda I - A| = 0$

6: **compute** w', w'' **by** $(A - \lambda_{max} I)w = 0$

7: **compute** $w'^{normalized}, w''^{normalized}$ **by** $w_{normalized} = \frac{w}{|w|}$,

$|w| = \sqrt{w_1^2 + w_2^2 + \dots + w_n^2}$

8: **foreach** a'_{ij}, a''_{ij} **in** \tilde{A}', \tilde{A}'' :

9: $c'_{ij} = \frac{1}{n} \sum_{k=1}^n \frac{(a'_{ik} - a'_{jk}) + (\lambda'_{max} - n)w'_k}{w'_i - w'_j}, c'_{ij} \rightarrow C'$

10: $c''_{ij} = \frac{1}{n} \sum_{k=1}^n \frac{(a''_{ik} - a''_{jk}) + (\lambda''_{max} - n)w''_k}{w''_i - w''_j}, c''_{ij} \rightarrow C''$

11: **end**

12: **compute** CR', CR'' **by** $CR = \frac{CI}{RI}, CI = \frac{\lambda_{max} - n}{n - 1}$

13: **if** $CR' < 0.1 || CR'' < 0.1$:

14: **return** 0

15: **else**

16: **for** $i = 1$ **to** $|V_{node}|$:

17: $S_i = S_0^i + \sum_{k=1}^{n'} w'_k (\sum_{j=1}^{n''} w''_j V_{ij})$ // n' : number of secondary guideline factors;

n'' : Number of tertiary guideline factors corresponding to secondary guideline factors

18: $S_i \rightarrow S_{node}$

19: **end**

20: **end**

21: **return** S_{node}

5 Security Analysis

5.1 Authentication Security

The cross-domain joint traceability architecture proposed in this paper is implemented based on blockchain technology. When conducting joint traceability of user behaviors, the hash value $Hash(Cert)$ of the in-domain traceability authorization certificate and the hash value $Hash(croCert)$ of the cross-domain traceability authorization certificate stored in the authorization chain of the affiliated domain are used as authentication credentials. Given the one-way nature of the hash function, even if an attacker obtains the hash values, they are unable to decrypt and obtain the user's traceability authorization certificate, thus ensuring the security of the certificate. During the process of a node registering and applying for a traceability certificate, nodes communicate with each other using public key encryption and decryption as well as digital signature technologies, which ensures that the information will not be tampered with or leaked during the information transmission process, and realizes a secure authentication and authorization process.

5.2 Non-Falsifiability

In the cross-domain joint traceability architecture, by taking advantage of the tamper-proof characteristic of the blockchain, the access authorization records and traceability authorization records (including permissive authorization and rejection authorization) of each domain, as well as the records of users' access behaviors to data resources, are stored in the authorization chain and the access behavior chain within the domain. No node is able to forge false authorization record information. On the one hand, false authorization information cannot be recorded in the authorization chain through the in-domain consensus. On the other hand, unreasonable or false authorization records will lead to a decrease in the comprehensive reputation value of the delegated node, turning it into an ordinary node and making it unable to continue the authorization behavior. This effectively prevents the security issues caused by the delegated node being attacked or bribed. In addition, both the authorization certificates and the records of access behaviors are stored on the blockchain, effectively preventing problems such as illegal denial of access in the information system.

5.3 Traceable

In the system architecture, the access authorization records and access behavior records under each trust domain are all recorded in the blockchain. After obtaining the traceability authorization certificate of the domain where the target node is located, cross-domain joint traceability can be carried out to track the process of the target node being granted and accessing data resources. This helps prevent malicious authorization (including incorrect authorization and excessive authorization) of the target node by the delegated node, verify whether the cross-domain access complies with the cross-domain access policies stored in the strategy chain, and prevent the information system from illegally denying access to users with access authorization.

5.4 User Privacy Security and Credibility

In the cross-domain joint traceability architecture, the security of users' personal privacy is mainly reflected in the confidentiality of users' access behaviors, so the restricted access to users' historical access behaviors is a key point. In the architecture proposed in this paper, when tracing the access behavior of a certain user, one must first apply for a traceability authorization certificate of the domain where the target user is located. After successfully obtaining the certificate endorsed by the delegated node of the target domain, joint traceability can be carried out on the user access records within the granted access rights. For access records that exceed the traceability rights of the certificate, the traceability request node is not allowed to access them, which effectively protects the users' personal privacy security and, at the same time, ensures the restricted traceability of users' highly sensitive access records.

5.5 Avoiding Abuse of Power

When conducting joint traceability of the access behavior of a certain user node, it is necessary to obtain the traceability authorization certificate of the domain where the target node is located and the permission to conduct joint traceability of access records. The traceability authorization certificate of the requesting node is endorsed by the delegated node in the target domain. If the delegated node abuses its authorization power to authorize ordinary nodes, leading to data security issues, or maliciously modifies the authorization information when reaching a consensus on uploading the authorization information to the chain within the domain, its comprehensive reputation value will be reduced. If, after the evaluation of the comprehensive reputation value, the delegated node becomes an ordinary node due to the decrease in its comprehensive reputation value and the value drops below a certain threshold, the traceability authorization certificates of the requesting nodes endorsed by this delegated node will be invalidated. These nodes holding invalid certificates need to go through the authentication and authorization process again before they can conduct joint traceability of the access behavior records of the user nodes in the target domain of the certificate.

5.6 Performance Analysis

The proposed cross-domain joint traceability architecture based on hierarchical blockchain, due to its unique hierarchical structure, ensures that the consensus of the upper-layer proxy centers remains unaffected even when more system nodes join. The comprehensive reputation evaluation and ranking of nodes in the proposed scheme guarantee the stability and reliability of the blockchain stored within the architecture. If malicious nodes attempt to attack or tamper with block data, or if malicious delegate nodes provide unauthorized endorsements, their reputation scores will be significantly lowered during the evaluation process. As a result, such nodes will be excluded from the elected delegate nodes, and the certificates endorsed by them will become invalid. This mechanism effectively ensures the security of the system architecture.

5.7 Performance Analysis

This paper conducts an efficiency analysis of the proposed cross-domain authentication scheme and makes a comparison with other research schemes. During the comparison, the primary focus is placed on the computational overhead of the authentication and authorization scheme presented in this paper and that of other competing schemes. Meanwhile, any factors that have no bearing on cross-domain authentication are deliberately disregarded. Compared with other cross-domain authentication schemes, assuming that there is no cross-domain certificate in the cross-domain authentication process, the calculation comparison results are shown in Table 2 below, and the following regulations are made: Public Key Encryption is denoted as PE, Public Key Decryption as PD, Asymmetric Signature as AS, Asymmetric Signature Verification as AV, and Hash Operation as H.

Table 2. Computation overhead comparison.

Scheme	Calculation Overhead	Time-Consuming /ms
Literature [9]	6PE+6PD+4AS+4AV+8H	101.542
Literature [10]	2PE+2PD+2AS+AV+2H	33.634
This Paper	PE+PD+2AS+2AV+2H	25.797

Literature [9] proposes to use blockchain technology to construct a Public Key Infrastructure (PKI) to issue authorization certificates for nodes. To ensure the security of the certificates, an independent trusted intermediary separate from the Certificate Authority (CA) is added to achieve the purpose of detecting attacks on the PKI. However, this brings extremely high overhead costs, which are significantly higher than the computational overhead of this paper. Literature [10] proposes a multi-layer blockchain structure and uses a public blockchain to provide cross-domain identity authentication services. Compared with the scheme in this paper, although there is one less calculation of signature verification, there are two more calculations of the public key-based encryption and decryption algorithms. The computational overhead in the same environment is slightly higher than that of the scheme in this paper. Therefore, it is believed

that the cross-domain authentication and access architecture proposed in this paper has better authentication efficiency in a multi-trust domain environment.

The computational overhead of the node comprehensive reputation value evaluation method based on FAHP proposed in this paper mainly depends on the number of evaluation indicators n and the number of nodes m . Its computational overhead is: $o(n^3) + o(m \times n^2)$. In the scheme proposed in this paper, the number of evaluation indicators is relatively small. Therefore, the computational overhead of the node comprehensive reputation value evaluation method based on FAHP is within an acceptable range. In the multi-trust domain scenario, there are a large number of nodes. However, for the multi-domain blockchain network, there are sufficient hardware resources. The computational tasks of FAHP can be distributed among multiple nodes, which is sufficient to support the computational requirements of this algorithm. Therefore, the proposed method demonstrates high feasibility and scalability in practical applications.

6 Conclusion

In order to address the security risk issues that the centralized authentication and access service in high-frequency cross-domain access under multiple trust domains is prone to due to malicious attacks or single-point failures, this paper proposes a cross-domain joint traceability scheme based on a hierarchical blockchain. This scheme is based on a hierarchical blockchain structure. The upper-layer blockchain stores the cross-domain access policies among various trust domains, while the lower-layer blockchain stores the authentication and authorization records of each domain and the access behavior records of access nodes to the data resources within the domain, providing a reliable basis for joint traceability of the source when security risk issues occur. In addition, according to various factors of nodes, the Fuzzy Analytic Hierarchy Process is used to evaluate their comprehensive reputation values, which enables the election of more honest delegated nodes to ensure the accuracy and rationality of authorization. At the same time, it meets the requirement of more accurately and dynamically adjusting the reputation values of nodes based on multiple factors. Through the analysis in terms of security and efficiency, it is proven that this scheme has good security and efficiency.

When the continuous increase in the cross-domain access behavior of nodes brings consensus pressure and storage pressure on nodes to this hierarchical cross-domain architecture, it is necessary to further conduct research on improving the cross-domain consensus efficiency and reducing the block storage overhead. Next, we will conduct research on consensus algorithms suitable for cross-domain scenarios. The aim is to improve the consensus efficiency of the architecture on the basis of ensuring the security and reliability of cross-domain sharing. In addition, we will also conduct research on reducing the huge storage overhead caused by the continuously increasing cross-domain access behavior records of nodes to ensure the continuous and stable development of the system.

In the future, we hope that this solution can be implemented in more fields, providing reliable technical support for cross-domain data sharing and joint traceability. We will build blockchain nodes in each participating domain and configure a consensus

mechanism suitable for cross - domain scenarios. Cross - domain shared communication will be achieved through standardized interfaces and security protocols. Finally, we will test and optimize the cross - domain joint traceability system in combination with specific application scenarios.

References

1. Wenhao, Q., Meng, S., Seyed Reza Aghaseyed, H. (2023). Facilitating big-data management in modern business and organizations using cloud computing: a comprehensive study. *Journal of Management & Organization*, 29(4), 697-723.
2. Xiaoyong, D., Tong, L. Wei, L. (2024). Cross-domain Data Management. *Computer Science (Chinese)*, 51(01), 4-12.
3. Li, Y., Du, Z., Fu, Y., Liu, L. (2022). Role-Based Access Control Model for Inter-System Cross-Domain in Multi-Domain Environment. *Applied Sciences*, 12(24), 13036.
4. Rong, J., Shanshan, H., Yimin, Y., Weiping, D., (2023). An access control model for medical big data based on clustering and risk. *Information Sciences*, 621, 691-707.
5. QuanWen, H., Hui, L., Jia, H., Xiaoding, W. (2021). A Novel Cross-domain Access Control Protocol in Mobile Edge Computing. In: 2021 IEEE Global Communications Conference (GLOBECOM). Madrid, Spain, pp. 1-6.
6. Hai, Z., Feng, Z. (2023). Cross-domain identity authentication scheme based on blockchain and PKI system. *High-Confidence Computing*. 3(1).
7. Shuang, S., Shudong, C., Rong, D. (2020). Trusted and Efficient Cross-Domain Access Control System Based on Blockchain. *SCIENTIFIC PROGRAMMING*. 8832568, 13.
8. Chuanjia, Y., Rong, J., Bin, W., Pinghui, L., Chenguang, W. (2024). A cross domain access control model for medical consortium based on DBSCAN and penalty function. *BMC MEDICAL INFORMATICS AND DECISION MAKING*. 24(1), 260.
9. Maurizio, T., Franco, A., Andrea, D., Christian H, S. (2020). A blockchain based PKI validation system based on rare events management. *Future Internet*. 12(2), 40-48.
10. Jinhua, Z. Xiaowei, L., Xin, Z., Yuqin, Z., Ran, D., Dengqi, Y. (2021). Cross domain authentication and key agreement protocol based on blockchain in edge computing environment. *Journal of Cyber Security (Chinese)*. 6(1), 54-61.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

