ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Trusted sharing architecture of edge computing data based on blockchain in 5G network environment

Minyue Li[1] *and Yanmei Wei*[2,*]

[1] College of Information and Business, Jinan Preschool Education College, Jinan 250000, Shandong, China
[2] Information Network Center, Jinan Preschool Education College, Jinan 250000, Shandong, China

SUMMARY: *In 5G-enabled edge environments, massive data streams generated by heterogeneous terminals require low-latency, verifiable, and fine-grained sharing. In this paper, we propose a blockchain-based trusted data sharing architecture for edge computing, and design a collaborative mechanism that integrates slice-aware hierarchical storage, smart contract access control, and lightweight consensus scheduling. The hierarchical data path between devices, edge nodes, blockchain nodes and cloud side is constructed, which supports identity binding, traceability record, integrity verification and dynamic authorization. A practical prototype is implemented using Hyperledger Fabric, Docker, Python, and MySQL. The experiments were conducted in a prototype environment consisting of 48 logical nodes with 320,000 shared records and mixed service loads. The proposed architecture achieves an acknowledgment delay of 82.6 ms, a throughput of 2147 transactions/SEC, an integrity verification accuracy of 99.3%, and an unauthorized access interception rate of 98.7%. Compared with the static edge chain scheme, the synchronization overhead is reduced by 23.4%, and the efficiency of cross-node trust evaluation is improved by 19.8%. It has strong scalability, controllability and deployment value.*

KEYWORDS: *5G network; Blockchain; Edge computing; Trusted data sharing*

1 Introduction

The 5G network pushes up the terminal connection density, link reliability and service concurrency simultaneously, and the data generation location is further shifted from the centralized center to the edge side. Industrial terminals, Internet of vehicles devices, mobile sensor nodes and video acquisition units continue to form high-frequency heterogeneous data streams. In the process of data access, caching, forwarding, collaborative computing and cross-domain invocation, it is necessary to meet the requirements of low latency, verifiability, traceability and fine-grained authorization at the same time. The traditional cloud center sharing mode has obvious constraints in return path, single point trust and permission synchronization, which is difficult to adapt to the computing characteristics of multi-node concurrent interaction, dynamic access and proximal collaborative processing in 5G scenarios. Edge computing can sink computing and storage capabilities close to the location of the data source, and blockchain can provide decentralized accounting, tamper-resistant records and on-chain rule execution. The combination of the two provides a more realizable computing

*wymjnygz@126.com
https://doi.org/10.65102/is2026727
Published: 30 April, 2026

framework for trusted sharing in 5G environment.

Pal et al. studied the blockchain mechanism in iot access control and pointed out that on-chain policy enforcement and distributed authorization have obvious value in trusted access [1]. Zhu et al. proposed an edge fine-grained access control method based on smart contracts, so that permission determination can be completed automatically on the chain [2]. Vladyko et al. studied the communication mechanism of distributed edge computing supported by blockchain and verified its suitability in ultra-reliable and low-latency services [3]. Dong et al. proposed a data analysis scheme for the integration of edge computing and blockchain, which strengthened the data fusion and security processing capabilities of iot [4]. Rasheed et al. studied the trust verification mechanism of blockchain for 5G and above IoV communication, which provides support for trusted interaction in dynamic environment [5]. Liu et al. proposed a secure distributed storage method for blockchain-enabled edge computing, which enhanced data location and fault tolerance [6].

Wang et al. studied the privacy authentication scheme of blockchain, which improved the level of identity protection in the process of edge service access [7]. Li et al. proposed a blockchain authentication method for industrial Internet of things devices, introducing PUF mechanism into the trusted access process [8]. Zhang et al. studied a data sharing scheme with fine-grained authorization and revocation mechanism, which extends the application boundary of blockchain sharing control [9]. Xue et al. systematically sorted out the integration path of blockchain and edge computing in the Internet of Things, indicating that this direction has formed a strong trend of technology aggregation [10]. The existing results provide a good foundation for the research of trusted sharing, but there is still a lack of implementation expression for unified architecture in 5G high concurrent access, edge multi-node collaboration, on-chain right confirmation and lightweight consensus linkage.

Based on this, this paper constructs a trusted data sharing architecture based on blockchain and edge computing for multi-node collaborative sharing scenarios in 5G network environment. The architecture focuses on terminal data access, edge side preprocessing, on-chain right registration, sharing request verification and cross-node collaborative access, and integrates data flow organization, trusted verification, access control and lightweight consensus into a unified computing framework. By introducing a verifiable data processing link on the edge side, and deploying a fine-grained permission constraint and state record mechanism on the chain, the identity confirmation, content verification, authorization execution and access audit in the data sharing process can form a continuous linkage, so as to enhance the traceability, consistency and real-time response ability of the sharing process in the 5G high-concurrency environment.

The rest of this paper is arranged as follows. Section 2 reviews the related research on blockchain data sharing, edge computing security mechanism, trusted access control in 5G scenarios, and analyzes the technical characteristics of existing methods in terms of collaborative efficiency, rights management and chain-edge interaction. Section 3 presents the design of the trusted sharing architecture of edge computing data based on blockchain in 5G network environment, including the data flow organization, the on-chain right confirmation and trusted verification mechanism, the system hierarchical structure, and the collaborative implementation process of lightweight consensus and access control. Section 4 introduces the experimental data construction, platform configuration and performance evaluation results, and analyzes them in terms of confirmation delay, throughput, verification accuracy and access interception effect. Section 5 summarizes the content of the whole paper, and gives future research directions combined with architecture deployment and performance.

2 Related work

With the continuous improvement of 5G access density, edge node scale and cross-domain business collaboration, data sharing has shifted from a single platform internal call to continuous collaboration between terminals, edge, on-chain nodes and cloud-side services. Shared objects are no longer limited to static files or short-cycle records, but contain multi-class heterogeneous data such as state flows, control instructions, sensing results, access tokens, and audit summaries. The shortening of the computation path improves the efficiency of real-time processing, and makes identity verification, authorization synchronization, data right confirmation and cross-node consistency maintenance the core links in the architecture design. Around these computing requirements, existing research mainly focuses on the integration of blockchain and edge computing, trusted access in 5G environment, access control for sharing process, and multi-chain or cross-domain collaboration.

Ding et al. studied the resource pricing and budget allocation method of iot blockchain in edge computing environment, and proposed to link the resource allocation behavior with the collaborative computing process on the chain to improve the cost constraint and scheduling efficiency of blockchain services in multi-node deployment [11]. Babu et al. proposed Sec-edge trusted system, which introduces blockchain into the identity identification and access authentication process in 5G edge network, so that edge nodes can maintain high authentication reliability in dynamic network [12]. Liu et al. studied the anonymous authentication mechanism of blockchain in the edge computing environment, which enhanced the privacy protection ability in the authentication phase by hiding the identity mapping relationship and session characteristics [13]. Song et al. proposed a secure data sharing mechanism in cloud-edge collaboration scenarios, which incorporated key management, data scheduling and access constraints in the sharing process into the unified control link, and improved the security of data flow between heterogeneous nodes [14]. Guha Roy studied the blockchain edge security framework in Industry 4.0 scenarios, which strengthened the structural coupling between data processing, privacy isolation and security collaboration at the edge side [15].

To facilitate the comparison of the focus of different studies in trusted shared links, Table 1 organizes the representative methods in a structured way. The table focuses on four aspects: 5G adaptation, on-chain control ability, privacy support mode and architecture scalability, in order to observe the differences in the expression of the unified shared architecture of the existing schemes.

Table 1: Comparison of related methods for trusted sharing of 5G edges

Method Category	Representative Studies	Technical Focus	Main Advantages	Main Limitations
Resource Collaboration	Ding et al. [11]	Blockchain-based resource pricing and budget allocation	Supports cost control and scheduling optimization in multi-node deployment environments	Provides relatively weak coverage of ownership confirmation and auditing in shared data links
Trusted Access	Babu et al. [12], Liu et al. [13]	5G edge authentication and anonymous authentication	Strengthens node identity trustworthiness and access protection	Offers insufficient support for cross-node coordination after data sharing
Secure Sharing	Song et al. [14], Quan et al. [20]	Data sharing control and outsourced computing collaboration	Provides a relatively complete sharing process with a clear security control chain	Lacks sufficient analysis of convergence under high-concurrency edge transactions
Privacy and Security Framework	Guha Roy [15], Alharbi [16]	Edge security framework and on-chain access control	Facilitates the implementation of permission rules and security management on chain	Shows limited integrated modeling capability for multi-domain heterogeneous nodes
Cross-Domain Collaboration	Jin et al. [17], Minmin et al. [21]	Knowledge transfer and multi-chain cross-domain privacy enhancement	Extends cross-domain collaboration and trust propagation capabilities	Lacks fine-grained constraints for real-time sharing paths in 5G scenarios

Alharbi proposed an access control enabled blockchain framework, which binds data security management and authorization rule execution in on-chain logic, so that access determination has better verifiability and auditability [16]. Jin et al. studied the continuous knowledge transfer method in the decentralized edge computing architecture, and showed that the collaborative mechanism on the chain not only acts on data writing and verification, but also supports cross-node knowledge flow and state maintenance [17]. Zhang et al. proposed a blockchain privacy auditable authentication scheme for mobile cloud computing, and introduced a hierarchical access control structure to enable permission control and audit records to land synchronously [18]. Wang et al. studied a privacy access control system for industrial iot based on smart contract tokens, which maintains consistent constraints on access behavior through token mapping and contract execution [19]. Quan et al. proposed an edge trusted data sharing framework combining blockchain and outsourcing computing, so that data sharing, computation offloading and result verification formed a closed-loop process [20]. Minmin et al. studied the trusted edge and cross-domain privacy enhancement model under multi-blockchain, which extended the expressive ability of trust transfer and privacy protection in cross-domain sharing scenarios [21].

From the perspective of method types, the existing work has formed three representative

technical routes. One is mainly based on on-chain authentication and identity binding, emphasizing access credibility and node identifiability. One class is dominated by smart contracts and token control, emphasizing right mapping, revocation propagation and behavior auditing in the sharing process. The other category focuses on multi-chain collaboration, outsourcing computing or knowledge transfer, emphasizing data flow and state negotiation in cross-domain scenarios. These researches provide important support for trusted sharing. However, how to balance low-latency transmission, on-chain right confirmation, edge execution and cross-node consistency in a unified architecture still needs more detailed computing organization.

From the existing research, it can be seen that blockchain authentication, smart contract authorization, edge-side security processing and cross-domain privacy enhancement have formed a relatively clear technical foundation. Existing methods have given effective implementations in the aspects of access credibility, access control accuracy, shared link protection and multi-node cooperation. However, most of the works are still focused on a single link, and the common practice is to emphasize one part of authentication, storage or privacy protection. The linkage expression between high concurrent access, heterogeneous cooperation of edge nodes, on-chain right confirmation synchronization and continuous verification of shared state in 5G environment is not complete. Especially in the continuous process of data entering edge nodes from the terminal side, then registering on the chain and calling across nodes, permission mapping, trust verification, lightweight consensus and access audit are often scattered in different modules, lacking a unified organization way of trusted data sharing.

Based on the above research basis, this paper takes the edge data sharing process in 5G network environment as a unified computing object, and integrates data flow organization, on-chain right confirmation, trusted verification, lightweight consensus and access control coordination into the same architecture to build a trusted data sharing link for multi-node real-time interaction. This processing method no longer stays in the local mechanism improvement, but emphasizes the continuous constraint relationship before, during and after sharing, so that terminal access, edge processing, on-chain registration, authority execution and result audit can form a closed-loop connection, and also provides a direct technical undertake for the architecture design and performance evaluation in the following.

3 Trusted sharing architecture design of edge computing data based on blockchain in 5G network environment

3.1 Analysis of data flow organization and trusted sharing requirements in 5G edge networks

5G edge network synchronously sinks the connection, computing and forwarding capabilities to the location close to the data source, and the data generated by the terminal side is no longer transmitted back by a single path, but continuously flows between the access layer, edge layer and on-chain cooperation layer. Industrial control terminals, vehicle units, video nodes and mobile sensors will generate state streams, event streams and media streams in a short period of time, which not only require millisecond response, but also require source verifiability, content traceability and call auditability. Therefore, data flow organization is not only a process of transmission scheduling, but also involves continuous computing steps such as access identification, edge caching, digest extraction, permission mapping and shared writeback. Only when the path state, node load and trust constraints are incorporated into the unified link, the subsequent on-chain registration and sharing control can remain stable.

In 5G edge network, multi-source terminals will continuously inject heterogeneous data into edge nodes at different rates. Therefore, it is first necessary to characterize the real-time arrival load of nodes at time t, and its expression can be written as follows.

$$\lambda_i(t)=\sum_{k=1}^{m} a_{ik}(t)\, r_k(t) \tag{1}$$

Here, $\lambda_i(t)$ represents the data arrival intensity entering edge node i at time t, $a_{ik}(t)$ represents the access correlation coefficient between service source k and node i, and $r_k(t)$ represents the instantaneous generation rate of service source k. Equation (1) is used to describe the load scale of multi-class terminal services converging to edge nodes under 5G access conditions. The expression converts the access relationship between discrete traffic sources and edge nodes into a computable load intensity, which provides a quantitative basis for subsequent cache allocation, priority division and sharing timing selection.

To illustrate the way of data organization discussed in this section, Fig. 1 puts the data channel, control channel and trusted sharing trigger relationship in the 5G edge network in the same structure. 5G edge-sharing links have obvious hierarchical characteristics. Terminal data is first entered into different slices according to business types, and then cleaned, compressed and statuses encoded by edge nodes. After that, verifiable summaries and shared constraints are written to the on-chain index. After the request arrives, the system performs near-end scheduling according to the index status, node load and permission results, and writes the execution results back to the audit link for subsequent verification and responsibility location.

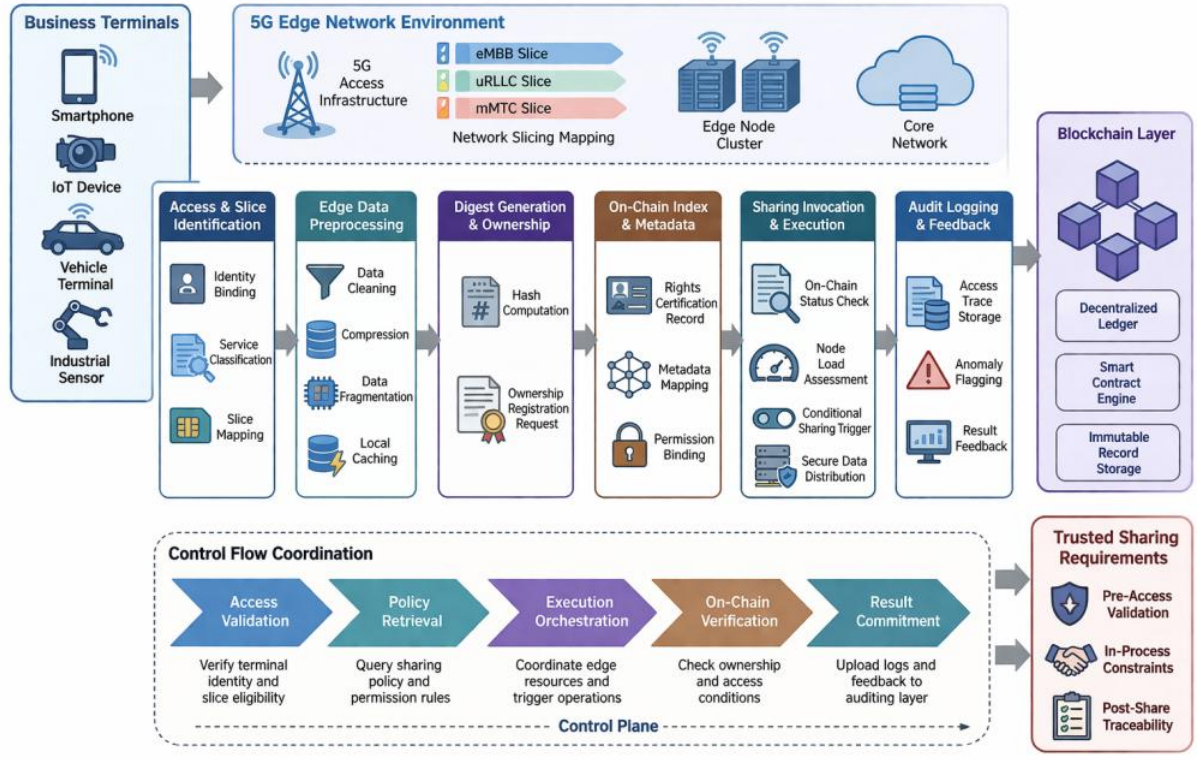

Figure 1: Data flow organization and trusted sharing requirement structure diagram in 5G edge network

Once data arrives at the edge node, transmission, caching and local processing will jointly

determine the response speed of the shared preparation phase, so the total processing delay of node i can be further expressed as follows.

$$\tau_i(t)=\tau_i^{tx}(t)+\tau_i^{buf}(t)+\tau_i^{proc}(t) \tag{2}$$

Here, $\tau_i(t)$ represents the total delay corresponding to node i completing a shared preparation process, $\tau_i^{tx}(t)$ represents the transmission delay, $\tau_i^{buf}(t)$ represents the queuing cache delay, and $\tau_i^{proc}(t)$ represents the local preprocessing delay. Equation (2) splits the source of delay on edge nodes into three parts, which facilitates the identification of system bottlenecks. The significance of this formula is not to simply sum up, but to unify the network link state, node queue pressure and local computing power consumption into the same evaluation framework, so as to provide an analysis basis for the delay compression of trusted shared links.

Before sharing is triggered, the system also needs to uniformly evaluate whether the data object has the conditions for on-chain registration and cross-node invocation. Therefore, the trust score of the current data of node i can be defined as follows.

$$\theta_i(t)=\alpha c_i(t)+\beta h_i(t)+\gamma f_i(t), \quad \alpha+\beta+\gamma=1 \tag{3}$$

where $\theta_i(t)$ represents the trust score of the current data object of node i, $c_i(t)$ represents the source identity matching degree, $h_i(t)$ represents the summary integrity score, $f_i(t)$ represents the time freshness, and α, β, γ represent the corresponding normalized weights of the three dimensions. In Formula (3), the three aspects of identity trust, content trust and time trust are compressed into a unified score, which is used to decide whether to enter the stage of on-chain right confirmation and cross-node sharing. The scoring mechanism enables the system to perform pre-screening before sharing is triggered, avoiding unverified or insufficient timeliness data occupying on-chain and edge resources.

When the sharing request is directed from node i to node j, only a high trust score is not enough to support effective scheduling. Link quality and receiver node load also need to be taken into account. Therefore, the effective scheduling benefit of sharing between nodes can be written as follows.

$$\rho_{ij}(t)=\frac{\theta_i(t)\, b_{ij}(t)}{1+q_j(t)} \tag{4}$$

Here, $\rho_{ij}(t)$ represents the effective scheduling gain when node i initiate sharing to node j, $b_{ij}(t)$ represents the normalized weight of link bandwidth between node i and node j, and $q_j(t)$ represents the current queue length of receiving node j. Equation (4) illustrates that the sharing scheduling does not depend on the bandwidth condition alone, but a joint trade-off among data trustworthiness, link quality, and receiver side load. Only when the trust score is high, the link availability is strong, and the queuing pressure of the destination node is controllable, the system is more suitable to initiate a shared call.

When multiple shared links exist concurrently, the system finally needs to evaluate the effectiveness of the current data organization strategy at the global level. Therefore, the overall sharing utility can be further expressed as follows.

$$\Omega(t)=\sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij}(t)\,\rho_{ij}(t)-\eta\sum_{j=1}^{n} q_j(t) \tag{5}$$

Here, $\Omega(t)$ represents the overall shared utility of the system at time t, $x_{ij}(t)$ represents the shared decision variable between node i and node j, and η represents the queue penalty coefficient. Equation (5) evaluates the effect of the current data flow organization strategy from a global perspective, where the former term represents the cumulative benefit brought by all effective shared paths, and the latter term represents the weakening of system stability by high queue pressure. This formula can further extend the local benefit of a single shared link to the overall network level, so that the system can still maintain a better data distribution structure and a more stable shared execution state under the condition of multi-node concurrency.

Based on the above analysis, the data flow organization in 5G edge network is not a simple extension of the traditional upload and download structure, but a continuous calculation process around arrival load, delay decomposition, trust score, shared revenue and overall utility. This organization also directly determines the stable operation boundary of subsequent on-chain execution and edge scheduling.

3.2 Blockchain-driven data right confirmation and trusted verification mechanism

In 5G edge network, the trustworthiness of data sharing does not depend on whether the single forwarding is successful, but on whether the data object has completed the identity solidification, ownership binding and state registration before entering the shared link. The terminal side continuously generates control data, sensing data and media data, and the edge nodes perform cleaning, compression and objectification processing on these heterogeneous content. If the processing results only stay at the local cache layer, it is difficult for different nodes to form a unified judgment on the source, scope of use and responsibility of the same object. The distributed ledger structure provided by blockchain can write the subject identity, time label, data summary and policy constraints into the on-chain index that cannot be tampered with, so that shared objects always maintain a clear identity boundary when flowing across nodes. Compared with the centralized directory service, this method does not rely on a single point to maintain the mapping relationship, which is more suitable for high concurrent access and multi-node cooperation in 5G environment.

In order to clearly illustrate how the data object completes the right confirmation registration before entering the shared link, Fig. 2 puts the relationship between the terminal subject, the edge processing node, the index unit on the chain and the shared object in the same structure. The data generated by the terminal is preprocessed at the edge side, regenerated into summary, time identification and subject mapping, and then enters the right confirmation unit on the chain to form a unique record. When the shared node calls the target data, it does not need to reconstruct the ownership relationship, but quickly determines the object source, policy scope and callable state according to the index on the chain. This organization enables clear identity, clear boundaries, and traceable accountability as data moves across nodes.

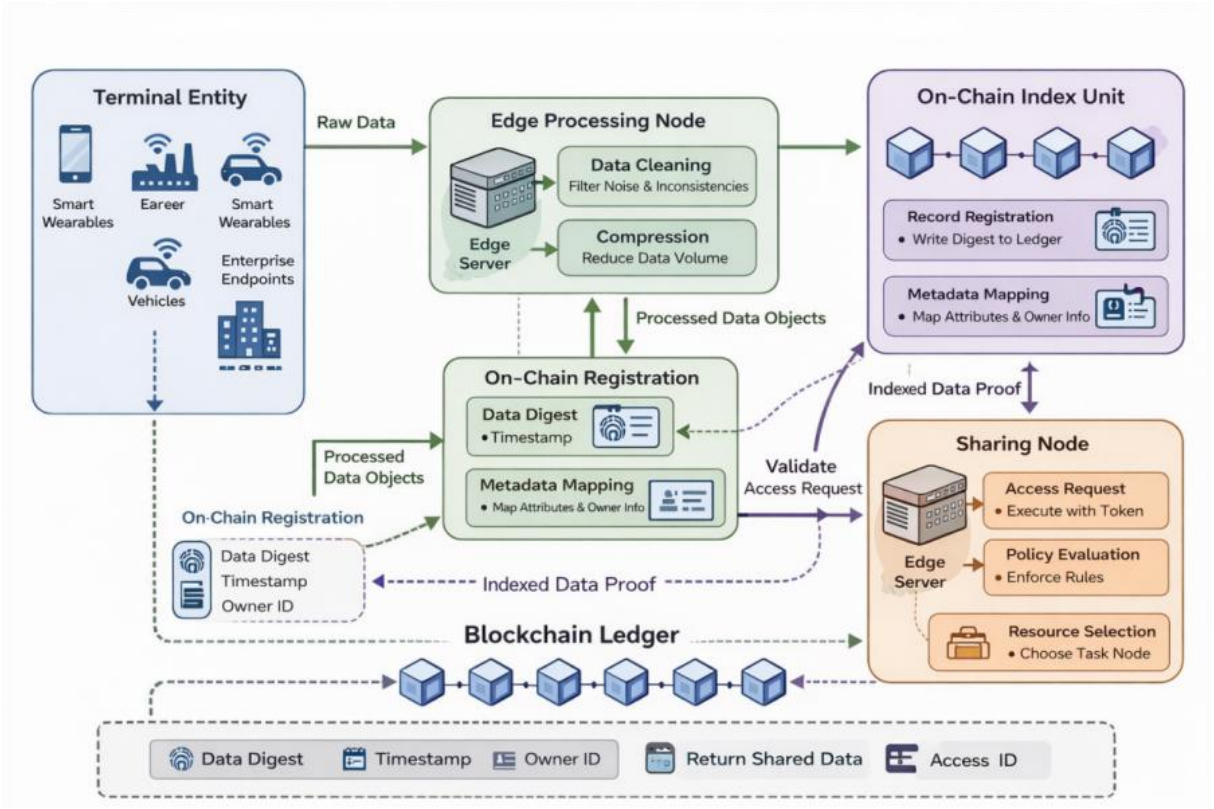

Figure 2: Blockchain-driven data right confirmation link structure diagram

In the on-chain right confirmation phase, the data object must first be compressed into a uniquely identifiable index expression, and then the lookback, comparison and state synchronization in subsequent shared calls can be established on the unified identity. Therefore, the data fingerprint can be expressed as:

$$\phi_d = H(M_d \| T_d \| O_d \| P_d) \tag{6}$$

Here, ϕ_d represents the on-chain fingerprint identity of data object d, $H(\square)$ represents the hash mapping function, M_d represents the object metadata set, T_d represents the registration timestamp, O_d represents the generation of subject identity, and P_d represents the policy label set. This formula is used to compress the identity information other than the content into a unique index, so that the object still has stable identifiability after leaving the original node. Once the on-chain fingerprint is formed, the subsequent verification process no longer relies on repeated parsing of the original content, but can carry out rapid verification around the index.

After completing the on-chain registration, the system also needs to make a comprehensive judgment on the trust degree of the shared object, so that the content consistency, time validity and policy consistency can be measured uniformly. Therefore, the object verification trust degree can be defined as:

$$v_d = \omega_1 c_d + \omega_2 e^{-\Delta t_d/\sigma} + \omega_3 p_d, \quad \omega_1 + \omega_2 + \omega_3 = 1 \tag{7}$$

Here, v_d represents the validation confidence of data object d, c_d represents the summary consistency score, Δt_d represents the time difference between the current verification time and the registration time, σ represents the time decay scaling factor, and ω_1

to ω_3 represent the normalized weights. This formula compreses the three factors of content, time and policy into the same evaluation space, so that the system can judge whether the object has enough credibility before the sharing call occurs. For high-frequency access scenarios in 5G edge environment, this continuous score is more stable than simple binary decision, and is more suitable for dynamic verification under multi-node cooperation.

To further illustrate how on-chain verification and traceback after right confirmation form a closed loop, Fig. 3 organizes the verification request, index retrieval, digest comparison, rule matching, audit writeback and traceback update into continuous channels. The process of trusted verification covers three levels: content consistency, policy consistency and call consistency. After the sharing request is initiated, the system first checks the index on the chain, and then compares the summary, ownership label and call rule jointly. Only after passing the verification, the object is allowed to enter the sharing execution phase. After the sharing is completed, the access results and state changes are written back to the audit link for follow-up tracking and responsibility judgment. The verification method formed in this way can reduce the false call and false authorization caused by the state asynchrony in the high-frequency shared environment.

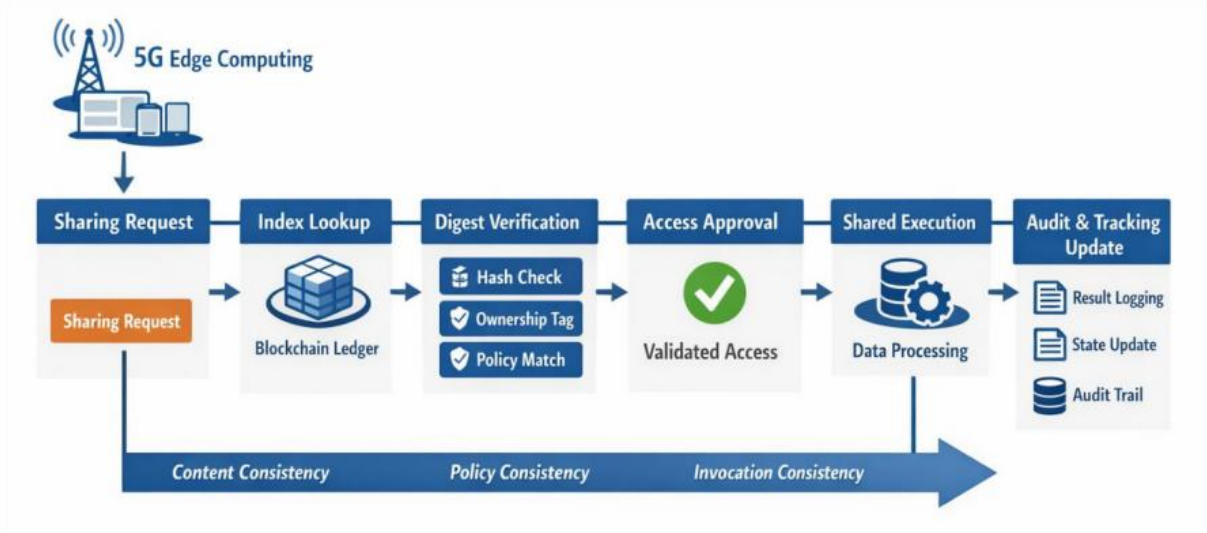

Figure 3: Blockchain-driven trusted verification and tracing flowchart

When state updates of the same data object continue to occur in multiple shared calls, whether the on-chain tracking links remain coherent needs to be further characterized. Therefore, the tracking strength under cross-block calls can be written as follows.

$$\xi_d^{(l)} = \sum_{u=1}^{l} \frac{\kappa_u}{1+\delta_u} \tag{8}$$

Here, $\xi_d^{(l)}$ represents the cross-block tracing strength of data object d in l consecutive calls, κ_u represents the index validity corresponding to the u call, and δ_u represents the state offset caused by the u call. This formula is used to measure the on-chain coherence of an object in multiple rounds of sharing. If the index continues to be valid and the state offset is small, the tracking strength remains high. If there are frequent state conflicts or index mismatches, the tracking strength will decrease. Through this index, the system can evaluate the trusted continuity of shared objects from the sequence level, which provides a stable index basis for subsequent scheduling of shared architectures.

Through the above right confirmation and verification mechanism, the data object has completed subject binding, summary consolidation, policy association and state tracking expression before entering the shared link, and the edge node can directly perform consistency verification based on the on-chain index when issuing subsequent sharing calls, without repeating the construction of ownership judgment. In this way, the object identity, verification credibility and tracking continuity are compressed into a unified record structure, so that the validity confirmation before sharing and the accountability back check after sharing can be carried out based on the same index system. For high-frequency interaction scenarios in 5G edge networks, this mechanism can provide stable and trusted inputs for node scheduling, permission execution and state synchronization in subsequent architectures.

3.3 Design of trusted data sharing architecture for 5G edge computing environment

The trusted data sharing architecture for 5G edge computing environment needs to organize the access layer, edge processing layer, on-chain control layer and cloud side coordination layer according to a unified data life cycle. The focus of the architecture design is not to simply stack chain, edge, and cloud, but to let data generation, local processing, on-chain registration, shared call, and result audit form a continuous computing path. The terminal layer is responsible for generating business data and status labels, the edge node is responsible for cleaning, compression, caching and objectification processing, the blockchain layer is responsible for saving the right confirmation index, authorization record and shared state, and the cloud side coordination layer is responsible for cross-domain index synchronization, global policy issuance and long-term archiving. The hierarchical structure thus formed not only retains the advantage of low latency of edge nodes, but also uses on-chain records to maintain consistency and traceability in the sharing process. Considering the differences in service slices in 5G networks, control data emphasizes delay priority, media data emphasizes throughput stability, status data emphasizes accurate source, and audit data emphasizes complete record. Therefore, the architecture cannot only rely on a single path forwarding, but needs to dynamically select shared paths and storage levels according to service attributes.

In order to clearly express the trusted data sharing structure for 5G edge environment, Fig. 4 puts the terminal device layer, edge processing layer, blockchain control layer and cloud side coordination layer into the same system. The terminal layer is responsible for generating original data and status labels, the edge layer is responsible for completing cleaning, compression, caching and objectization processing, the blockchain layer is responsible for saving the right confirmation index, authorization results and sharing records, and the cloud side is responsible for cross-domain synchronization, global policy issuance and archive management. In this hierarchical manner, the data content body, the summary body, and the control body are processed separately, thus maintaining consistency and auditability in the sharing process while maintaining a low latency response.

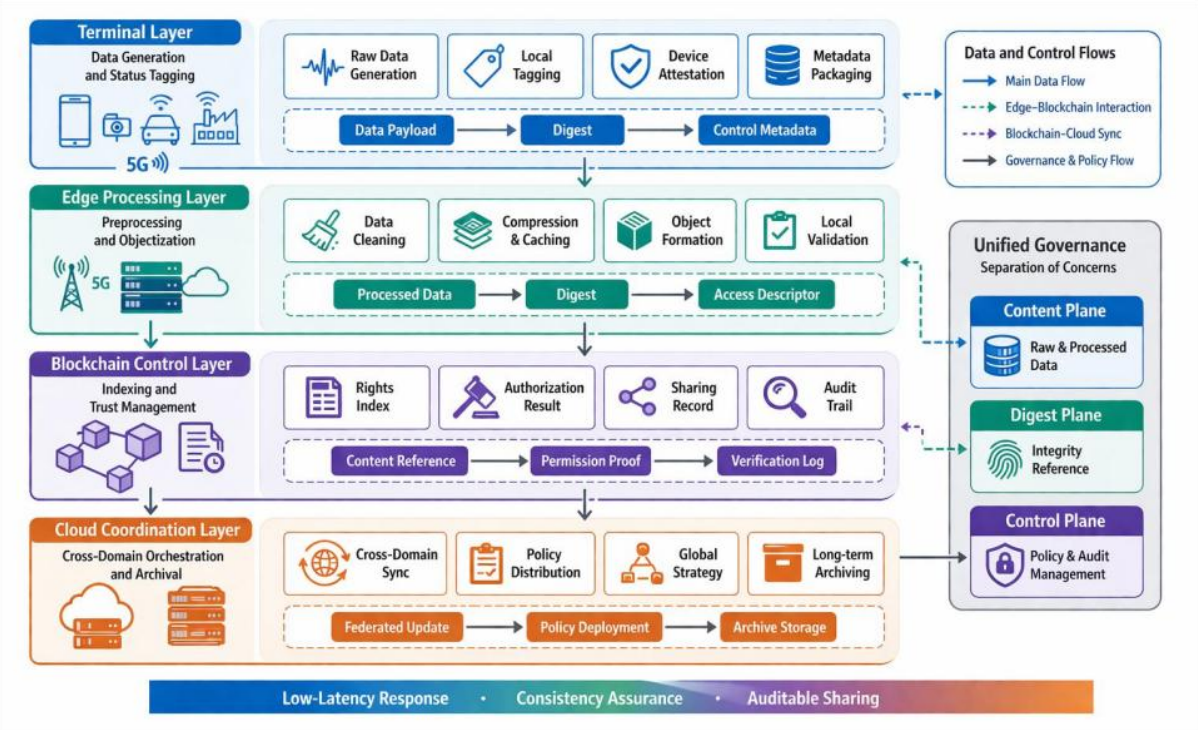

Figure 4: Data trusted sharing architecture diagram for 5G edge computing environment

Under the condition of concurrent sharing of multiple nodes, whether an edge node is suitable to accept the current request depends on the combined effect of resource allowance, link status and target node load. Therefore, the resource orchestration intensity between nodes can be expressed as follows.

$$y_{ij}(t)=\frac{u_i(t)\, b_{ij}(t)}{1+l_j(t)} \tag{9}$$

Here, $y_{ij}(t)$ represents the resource orchestration intensity of the service request mapping from node i to node j at time t, $u_i(t)$ represents the amount of schedulable resources at the source node, $b_{ij}(t)$ represents the link bandwidth weight, and $l_j(t)$ represents the current load of the destination node. This formula is used to measure whether a sharing request is suitable for execution on a specific edge node. It unifies the resource margin, link quality and target load into the same orchestration space, which can avoid the shared tasks being continuously concentrated on high voltage nodes, thereby improving the local congestion on the edge side.

In order to determine whether the on-chain index state is synchronized with the edge cache state, it is also necessary to quantify the degree of consistency between the two types of state vectors. Therefore, the chain edge synchronization consistency can be written as:

$$\zeta(t)=1-\frac{\|I_b(t)-I_e(t)\|_1}{\|I_b(t)\|_1+\varepsilon} \tag{10}$$

Here, $\zeta(t)$ denotes the consistency between the index state on the chain and the edge cache state at time t, $I_b(t)$ denotes the index vector on the chain, $I_e(t)$ denotes the edge cache state vector, $\|\square\|_1$ denotes the one-norm, and ε denotes the tiny constant preventing the denominator from being zero. This formula is used to measure the effect of chain edge synchronization. If there is a deviation between the record on the chain and the edge content,

the consistency value decreases, and the system needs to trigger synchronization correction. It transforms the abstract state into quantifiable synchronization index consistently, which is convenient for subsequent performance evaluation.

When multiple edge nodes undertake shared tasks at the same time, the system also needs to give the normalized load distribution results based on the comprehensive ability of nodes. Therefore, the proportion of shared load undertaken by node j at the current time can be expressed as follows.

$$\psi_j(t)=\frac{w_j(t)}{\sum_{r=1}^{n} w_r(t)} \tag{11}$$

Here, $\psi_j(t)$ represents the proportion of shared load borne by node j at time t, and $w_j(t)$ represents the comprehensive available capacity score of node j. This formula is used to give the normalized load distribution results when multiple nodes are sharing concurrently, so that the system can schedule according to the ability of nodes rather than simple polling. This can maintain a more reasonable balance between throughput and stability, and reduce the excessive occupancy of a single node.

The above architecture design organizes terminal access, edge processing, on-chain control and cloud-side coordination into a continuous data life cycle structure, so that the data content body, summary body and control body can carry computing, recording and constraint functions at different levels respectively. The joint expression of resource orchestration, hierarchical storage, edge synchronization and load distribution makes the shared link no longer depend on the ability of a single node, but can be dynamically adjusted according to service attributes and node status. The resulting architectural boundaries provide clear module interfaces and operating conditions for confirmation sequencing in the subsequent lightweight consensus process, policy matching in access control, and state writeback in execution feedback.

3.4 Trusted sharing implementation method of lightweight consensus and access control cooperation

In the 5G edge environment, the continuity of trusted data sharing depends not only on whether the on-chain registration is completed, but also on whether the state convergence and authorization execution can be completed with low overhead between nodes. If the consensus process is too heavy, the edge nodes will consume a lot of computing power in the sorting and confirmation phase, and the real-time sharing ability will decrease. If the access control process is too loose, the data objects can flow quickly, but the permission boundary will be gradually unstable in the cross-node call. Therefore, lightweight consensus and access control need to be designed as the same collaborative link, and cannot be treated separately. Here, the lightweight consensus module is responsible for quickly forming the writing sequence and state confirmation results between candidate edge nodes, and the access control module is responsible for performing authorization judgment according to the on-chain policy and node context, and the two maintain linkage through a shared state bus. Once the consensus is written, the authorization result can be bound to the latest index. Once the authorization policy changes, the consensus module will also adjust the write priority and acknowledgment object according to the latest state, so as to maintain the continuous control of the shared link.

To illustrate how lightweight consensus and access control interact in shared execution, Fig. 5 organizes shared request, candidate screening, status confirmation, permission matching, contract execution, and feedback writeback into a closed-loop process. After receiving the sharing request, the edge node first filtered the candidate confirmation path

according to reputation, delay and load, and then the contract module matched the calling subject, resource label and policy constraint, and finally wrote the execution result and state change back to the index synchronously. The closed-loop mechanism formed in this way can prevent the authorization state from disconnecting from the on-chain record while maintaining the confirmation efficiency.

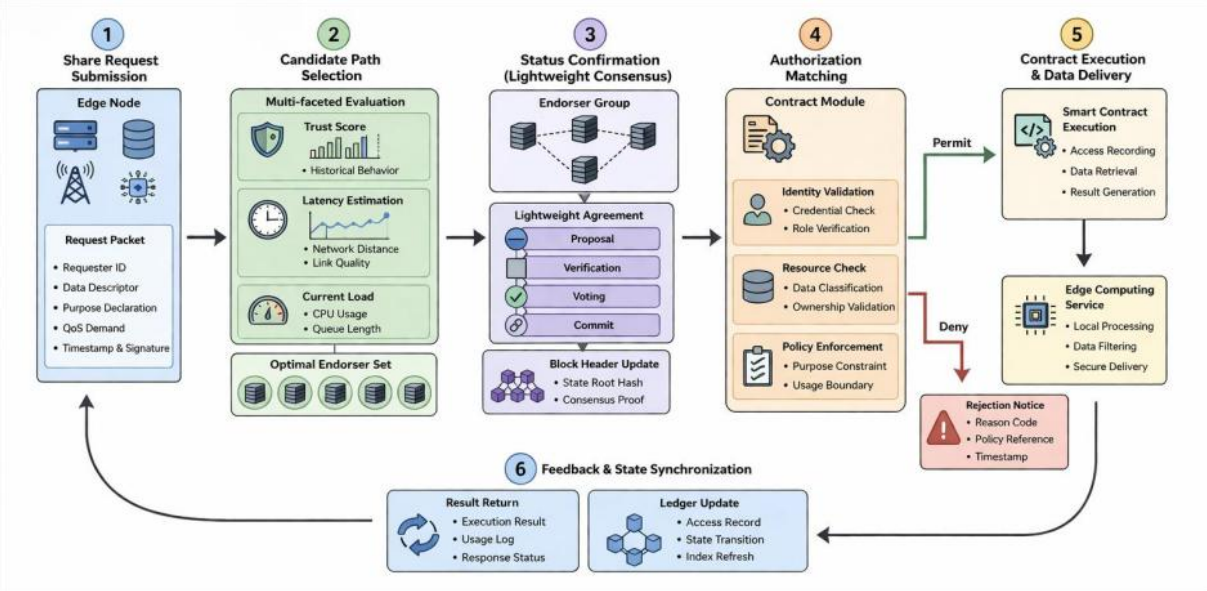

Figure 5: Flowchart of trusted sharing implementation in collaboration of lightweight consensus and access control

In the lightweight consensus stage, whether a candidate node is suitable to enter the confirmation sequence of the current round depends on the comprehensive results of reputation status, communication delay, queue pressure and cache adaptation degree. Therefore, the consensus score of a candidate node can be defined as follows.

$$g_i(t)=\beta_1 R_i(t)+\beta_2 \frac{1}{L_i(t)+1}+\beta_3 \frac{1}{Q_i(t)+1}+\beta_4 S_i(t) \tag{12}$$

Here, $g_i(t)$ represents the comprehensive consensus score of candidate node i at time t, $R_i(t)$ represents the node reputation value, $L_i(t)$ represents the communication delay, $Q_i(t)$ represents the queue pressure, $S_i(t)$ represents the cache state fitness, and β_1 to β_4 represents the normalized weight. This formula is used to select the nodes that are more suitable to undertake the confirmation task of this round from the multi-dimensional state, avoid the nodes with high delay or high congestion from repeatedly entering the critical write path, and reduce the invalid confirmation overhead on the edge side.

In the access control phase, whether the fine-grained authorization conditions are satisfied between the calling subject and the target resource needs to be described by the matching relationship in the attribute space. Therefore, the matching strength of permissions between users and resources can be expressed as follows.

$$\mu_{ur}(t)=\frac{\sum_{k=1}^{m} a_{uk}(t)\, b_{rk}(t)}{\sqrt{\sum_{k=1}^{m} a_{uk}^2(t)}\sqrt{\sum_{k=1}^{m} b_{rk}^2(t)}} \tag{13}$$

Here, $\mu_{ur}(t)$ represents the permission matching strength between user u and resource r, $a_{uk}(t)$ represents the user attribute vector, and $b_{rk}(t)$ represents the resource policy vector. The formula is used to describe the attribute compatibility degree between the calling subject and the target object, so that the access control can complete the fine-grained judgment in the way of vectorization, instead of relying on the fixed template matching item by item. For high-frequency request scenarios in 5G edge environments, this representation is more suitable for fast execution.

In order to unify the results of lightweight consensus and access control into the same execution evaluation framework, the system also needs to jointly measure the confirmation efficiency and authorization effectiveness. Therefore, the benefit of collaborative confirmation can be written as follows.

$$\eta_{ir}(t)=\frac{g_i(t)\,\mu_{ur}(t)}{1+\tau_{ir}(t)} \tag{14}$$

Here, $\eta_{ir}(t)$ represents the cooperative acknowledgement gain when node i performs a shared acknowledgement on resource r, and $\tau_{ir}(t)$ represents the total delay from the initiation of the acknowledgement to the completion of the authorization. This formula combines the consensus score with the permission matching strength, and then uses the delay term to constrain it, which indicates that the confirmation efficiency and authorization effectiveness must reach a good level at the same time, and the system can obtain a high shared execution revenue. It makes consensus and access control not two modules of separate evaluation, but a joint indicator in the same operating link.

In this section, lightweight consensus and access control are placed in the same collaborative link, so that node confirmation, permission determination and feedback writeback are no longer separate local processes, but a unified control mechanism that is carried out continuously around shared requests. The combination of candidate node screening, attribute matching, collaborative benefit calculation and closed-loop feedback correction made the shared link maintain the stability of authorization boundary while maintaining the efficiency of confirmation, and could continuously modify the subsequent scheduling state according to the execution results. Based on this implementation, the subsequent experimental part can systematically evaluate the actual running performance of the proposed architecture in terms of confirmation delay, shared throughput, verification accuracy and access interception effect.

4 Experimental design and performance evaluation

4.1 Experimental data construction and running environment configuration

The experimental data in this section are built around the trusted sharing process in 5G edge network, and the data sources include terminal perception records, edge cache status, on-chain index logs, access control results and audit writeback information. The data sample covers industrial control messages, video clip index, environmental monitoring status and cross-node call records at the same time, forming a total of 320,000 effective shared records. Each record contains seven fields, including object identification, source node number, timestamp, summary value, policy label, call result and feedback status, which are used to support right verification, chain edge synchronization, sharing scheduling and access interception analysis. In order to keep the evaluation process stable, the samples were divided into training set,

validation set and test set according to 7∶2∶1.

The experimental platform is deployed in Ubuntu22.04 environment, the core development language is Python3.10, the blockchain framework uses Hyperledger Fabric2.5, the container orchestration uses Docker24.0, and the database system uses MySQL8.0. A total of 48 logical nodes are configured on the edge side, of which 32 are responsible for shared processing and cache synchronization tasks, 8 are responsible for on-chain index maintenance and sorting confirmation tasks, and the remaining nodes are responsible for audit writeback and cross-domain coordination tasks. The server hardware is configured with an Intel Xeon Silver4314 processor, 128GB memory, and an NVIDIA RTX4090 graphics processing unit. The on-chain smart contract is implemented using Go language, and the node communication is a hybrid method of gRPC and MQTT to simulate the shared interaction under multi-source concurrent conditions.

All experiments were repeated ten times independently, and the mean and standard deviation were recorded. The database mainly includes four table structures: Node_State, Share_Log, Chain_Index and Audit_Result, which are used to store node status, shared records, on-chain index and audit results respectively, so as to provide a unified experimental basis for subsequent analysis of throughput, confirmation delay, verification accuracy and access interception effect. The above configuration is consistent with the prototype deployment scheme in the summary, which can support on-chain right confirmation, shared verification and cross-node collaborative experiments.

4.2 Performance evaluation

In order to make the operation effect of the proposed architecture can be compared under uniform conditions, this section evaluates from six dimensions of average confirmation delay, system throughput, integrity verification accuracy, unauthorized access interception rate, synchronization overhead and cross-node trust evaluation efficiency. Cloud-Center, Edge-Only and Chain-Edge-Static are selected as control schemes. Each scheme was repeated ten times independently under the conditions of the same node scale, the same traffic load and the same data set division, and the mean value, standard deviation and significance results were counted to ensure the repeatability and comparability of the evaluation conclusions.

In order to observe the distribution of confirmation delay when node scale and traffic load change simultaneously, Fig. 6 puts 16, 24 and 32 edge nodes and low, medium and high mixed traffic load into the same heat map.

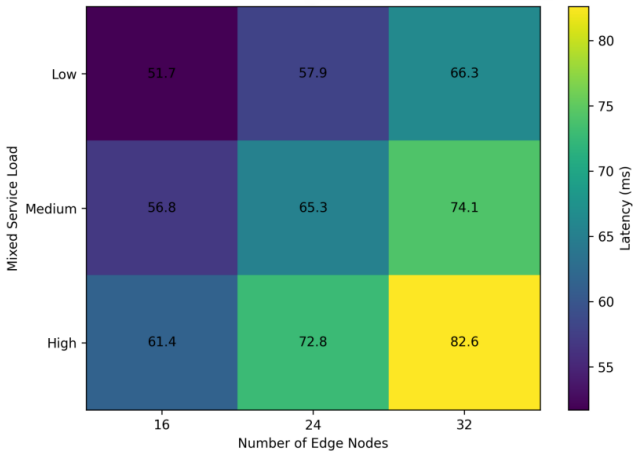

Figure 6: Heatmap (ms) of average acknowledgement delay for node size and traffic load

As shown in Fig. 6, when the number of nodes and business load increase simultaneously, Cloud-Center shows obvious delay aggregation, and the average confirmation delay reaches 164.3ms under the condition of 32 nodes and high load. Although the Edge-Only scheme reduces the center backhaul waiting, the delay increase is still obvious after 24 nodes. Chain-Edge-Static maintains a relatively smooth growth in the range of medium and high load, but still reaches 103.5ms at 32 nodes due to the fixed index maintenance and confirmation path. In contrast, the proposed architecture maintains the lowest delay in all load ranges. The confirmation delay of high load with 16, 24 and 32 nodes is 61.4 ms, 72.8 ms and 82.6 ms, respectively, indicating that after the cooperation of on-chain right confirmation, edge scheduling and lightweight consensus, The state convergence speed is more suitable for high-frequency sharing scenarios in 5G edge networks.

In order to compare the overall performance of different schemes from the perspective of multi-dimensional indicators, Fig. 7 uses the radar chart to express the five results of system throughput, integrity verification accuracy, unauthorized access interception rate, synchronization overhead control and cross-node trust evaluation efficiency.

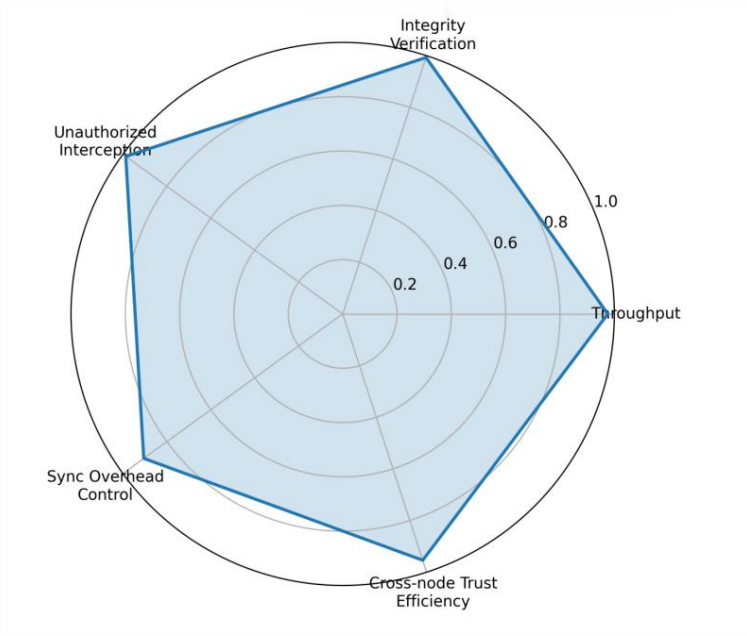

Figure 7: Radar chart of multi-index comprehensive performance

Fig. 7 shows that the proposed architecture maintains a relatively balanced outspread profile in all five dimensions. The system throughput reaches 2147 TPS, the integrity verification accuracy reaches 99.3%, and the unauthorized access interception rate reaches 98.7%. Compared with Chain-Edge-Static, the synchronization overhead is reduced by 23.4%, and the efficiency of cross-node trust evaluation is increased by 19.8%. This result shows that the advantage of the proposed architecture is not limited to a single delay metric, but reflected in the synchronous improvement of shared throughput, edge consistency and trust determination ability.

In order to put the core metrics in the same table for direct comparison, Table 2 lists the overall results of the four schemes in terms of confirmation delay, throughput, verification accuracy, access interception rate, synchronization overhead, and cross-node trust evaluation efficiency.

Table 2: Comparison results of key performance indicators

Scheme	Average Confirmation Latency / ms ↓	Throughput / TPS ↑	Integrity Verification Accuracy / % ↑	Unauthorized Access Interception Rate / % ↑	Synchronization Overhead Ratio / % ↓	Cross-Node Trust Evaluation Efficiency / $req \cdot s^{-1}$ ↑
Cloud-Center	124.8 ± 6.3	1584 ± 48	95.8 ± 0.5	91.4 ± 0.7	18.7 ± 0.6	1280 ± 37
Edge-Only	97.6 ± 5.8	1826 ± 42	97.1 ± 0.4	94.8 ± 0.6	15.9 ± 0.5	1456 ± 41
Chain-Edge-Static	91.2 ± 5.6	1978 ± 39	98.2 ± 0.3	96.5 ± 0.4	12.4 ± 0.4	1672 ± 35
Proposed	82.6 ± 5.4	2147 ± 36	99.3 ± 0.2	98.7 ± 0.3	9.5 ± 0.3	2003 ± 32

Table 2 illustrates that the proposed architecture outperforms the other three control schemes in all core metrics. Compared with Cloud-Center, the confirmation delay is reduced by 33.8%, the throughput rate is increased by 35.5%, and the proportion of synchronization overhead is reduced to 9.5%, which shows that the collaborative organization of on-chain index and edge scheduling does change the efficiency structure of shared links. Compared with the Edge-Only scheme that only emphasizes proximal processing, although the on-chain registration and verification processes are added, the overall throughput and latency of the proposed architecture are still better than those of the control schemes, indicating that the introduction of blockchain does not cause unacceptable performance loss, but reduces the consumption caused by repeated verification through unified index and policy enforcement.

In order to observe the dispersion degree of the sharing success rate under repeated experimental conditions, Fig. 8 shows the distribution of the results of the four schemes in ten independent rounds of experiments in the form of box plots.

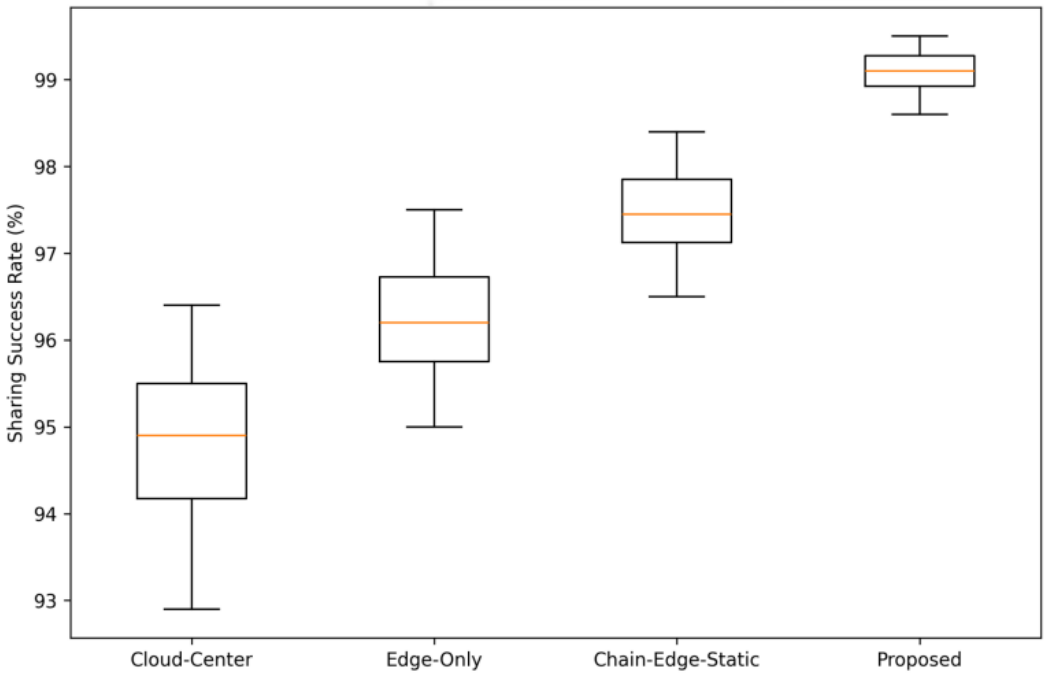

Figure 8: Boxplot of sharing success rate distribution under ten rounds of experiments

Fig. 8 shows that the proposed architecture achieves a median of 99.1% with the narrowest box range and the least outliers, indicating that it has a more stable operation performance under repeated experimental conditions. The wide upper and lower quartiles of

Cloud-Center indicate that centralized backtransmit links are prone to share result fluctuations under high concurrency conditions. Although Chain-Edge-Static has a higher median, its distribution is still wider than that of the proposed architecture, which indicates that the static confirmation path has local instability under complex traffic load.

In order to test the ability of the access control module to distinguish legitimate requests from illegal requests, Fig. 9 shows the true positive rate and false positive rate changes of the four schemes under different determination thresholds in the form of ROC curves.

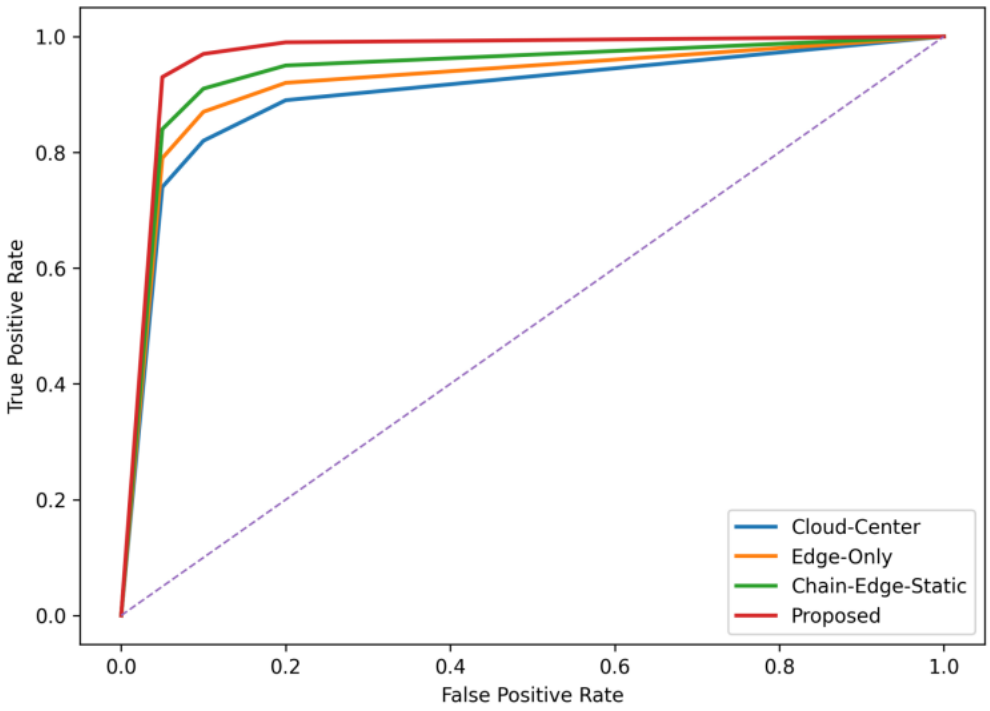

Figure 9: ROC curve of access control classification effect

Fig. 9 shows that the ROC curve of the proposed architecture is closest to the top left corner, and the AUC reaches 0.992, which is significantly higher than the other three schemes. This indicates that after the on-chain index, policy matching and state feedback update form a closed loop, the boundary between legitimate access and illegal access is clearer, and it can maintain a high recognition ability at a low false positive rate. For high-frequency sharing requests in 5G edge environment, this classification stability can effectively reduce the impact of false interception on normal business.

In order to show that the confirmation delay difference is not caused by random fluctuations, Table 3 shows the one-way ANOVA results of the four schemes in ten repeated rounds of experiments.

Table 3: One-way ANOVA results for the average confirmation delay

Source	Degrees of Freedom (DF)	Sum of Squares (SS)	Mean Square (MS)	F Value	p Value
Between Groups	3	14862.7	4954.2	91.37	< 0.001
Within Groups	36	1952.4	54.2	–	–
Total	39	16815.1	–	–	–

Table 3 shows that the F-measure of the difference between the groups reaches 91.37, and the corresponding p-value is less than 0.001, indicating that the difference between the different architectures in the average confirmation delay is statistically significant. This means that the advantage of the proposed architecture in confirmation delay does not come from the accidental result of a single round of experiments, but from the differences in the way the shared links are organized itself.

In order to verify the contribution of each component module to the overall performance, Table 4 further presents the ablation experimental results.

Table 4: Results of ablation experiments

Model Configuration	Average Confirmation Latency / ms ↓	Throughput / TPS ↑	Integrity Verification Accuracy / % ↑	Unauthorized Access Interception Rate / % ↑
Full Model	82.6 ± 5.4	2147 ± 36	99.3 ± 0.2	98.7 ± 0.3
Without On-Chain Ownership Confirmation	89.4 ± 5.9	2068 ± 41	96.8 ± 0.4	96.1 ± 0.5
Without Lightweight Consensus	108.7 ± 6.6	1834 ± 45	98.5 ± 0.3	97.9 ± 0.4
Without Access Control Collaboration	91.8 ± 5.7	2096 ± 39	98.9 ± 0.3	94.2 ± 0.6

Table 4 shows that the accuracy of integrity verification decreases to 96.8% after removing the on-chain right confirmation, indicating that the unified index and ownership binding are the basis for ensuring the verification accuracy. After removing the lightweight consensus, the confirmation delay increased to 108.7 ms, indicating that the state convergence efficiency was directly affected by the confirmation path design. After removing the access control coordination, the interception rate of unauthorized access decreases to 94.2%, which indicates that policy matching and feedback writeback have a direct effect on the shared security boundary. The complete model remains optimal in all four indicators, indicating that the three types of mechanisms are not loosely superimposed, but form substantial performance coupling in the same shared link.

In summary, it can be seen that the proposed architecture realizes the synchronous improvement of confirmation delay, system throughput, verification accuracy and access interception ability in 5G edge sharing scenario, indicating that on-chain right confirmation, edge hierarchical scheduling, lightweight consensus and access control collaboration do not introduce additional uncontrollable burden. On the other hand, it reduces the performance loss caused by repeated verification, invalid forwarding and policy mismatch through unified index and state loop closure.

4.3 Discussion

Compared with the centralized sharing mode, the proposed architecture shows advantages in operation efficiency, state consistency and access control accuracy. The performance improvement is not a local change caused by single module replacement, but comes from the overall cooperation of data flow organization, on-chain weight confirmation, edge hierarchical processing and closed-loop feedback synchronization. The on-chain index compresses the object identity, policy label and audit state into a unified record, which

reduces the overhead caused by repeated parsing and verification when sharing across nodes. The edge-side hierarchical scheduling shorted the waiting path of high-frequency requests in the near-end execution, and made the acknowledgment delay and synchronization overhead decrease synchronously.

From the perspective of operation mechanism, the architecture does not weaken the edge sharing efficiency because of the introduction of blockchain. On the contrary, with the cooperation of lightweight consensus and access control, state writing, permission matching and result writeback can be carried out continuously around the same shared request, thereby avoiding the mismatch phenomenon that the index is updated first and the policy arrives later. The experimental results show that the confirmation delay, throughput, integrity verification accuracy and unauthorized access interception rate are improved synchronously, indicating that a stable coupling relationship has been formed between on-chain control and edge execution.

From the perspective of deployment adaptability, the proposed architecture is more suitable for high-frequency, fine-grained and multi-node concurrent data sharing scenarios. After the node scale is expanded, the key indicators maintain a small fluctuation range, which indicates that the structure has extended stability. However, the inter-chain synchronization overhead under the condition of cross-domain sharing will still rise with the expansion of the coordination scope. Subsequent research can focus on cross-link reference compression, lightweight policy caching, and adaptive scheduling granularity, so that the architecture can remain stable and available in the complex 5G edge environment.

5 Conclusion

Focusing on the trusted data sharing requirements in 5G network environment, this paper constructs a data sharing architecture for the collaboration of blockchain and edge computing, and completes the system design from five levels: data flow organization, on-chain right confirmation, trusted verification, lightweight consensus and access control collaboration. The architecture integrates terminal access, edge processing, on-chain index and cloud-side coordination into the unified computing link, so that data objects have clear identities before sharing, maintain consistent states in sharing, and complete audit and writeback after sharing. The experimental results show that the proposed architecture is superior to the control scheme in terms of the average confirmation delay, system throughput, integrity verification accuracy and unauthorized access interception rate. The average confirmation delay is 82.6 ms, the system throughput reaches 2147 TPS, the integrity verification accuracy reaches 99.3%, and the unauthorized access interception rate reaches 98.7%. Compared with the static edge chain scheme, the synchronization overhead is reduced by 23.4%, and the efficiency of cross-node trust evaluation is improved by 19.8%. It shows that the index-driven shared control method on the chain can effectively reduce the additional overhead caused by repeated verification, invalid forwarding and policy mismatch, and maintain good operation stability and deployment feasibility under the condition of multi-node concurrency.

However, there are still some limitations in this paper. The current experimental scale is mainly built on 48 logical nodes and 320,000 shared records, and the inter-chain synchronization cost in a wider range of cross-domain cooperation scenarios, the ability fluctuation of heterogeneous nodes, and the local congestion propagation effect under extreme load conditions have not been further verified. Although the existing architecture can maintain high verification accuracy and low confirmation delay under mixed traffic load conditions, its long-term performance on cross-chain sharing, continuous policy update and resource-constrained edge devices still needs further evaluation. Future research can focus on

cross-link reference compression, adaptive cache migration, lightweight policy update mechanism and low-power edge deployment, which can further enhance the scalability, robustness and engineering adaptation level in complex network environments while maintaining shared credibility, state consistency and access control accuracy.

References

[1] Pal S, Dorri A, Jurdak R. Blockchain for IoT access control: Recent trends and future research directions[J]. Journal of network and computer applications, 2022, 203: 103371.

[2] Zhu Y, Wu X, Hu Z. Fine grained access control based on smart contract for edge computing[J]. Electronics, 2022, 11(1): 167.

[3] Vladyko A, Elagin V, Spirkina A, et al. Distributed edge computing with blockchain technology to enable ultra-reliable low-latency V2X communications[J]. electronics, 2022, 11(2): 173.

[4] Dong J, Song C, Zhang T, et al. Integration of edge computing and blockchain for provision of data fusion and secure big data analysis for Internet of Things[J]. Wireless Communications and Mobile Computing, 2022, 2022(1): 9233267.

[5] Rasheed I, Asif M, Khan W U, et al. Blockchain-Based Trust Verification and Streaming Service Awareness for Big Data-Driven 5G and Beyond Vehicle-to-Everything (V2X) Communication[J]. Wireless Communications and Mobile Computing, 2022, 2022(1): 7357820.

[6] Liu D, Zhang Y, Jia D, et al. Toward secure distributed data storage with error locating in blockchain enabled edge computing[J]. Computer Standards & Interfaces, 2022, 79: 103560.

[7] Wang Y, Jia X, Xia Y, et al. A blockchain-based conditional privacy-preserving authentication scheme for edge computing services[J]. Journal of Information Security and Applications, 2022, 70: 103334.

[8] Li D, Chen R, Liu D, et al. Blockchain-based authentication for IIoT devices with PUF[J]. Journal of Systems Architecture, 2022, 130: 102638.

[9] Zhang L, Zou Y, Yousuf M H, et al. BDSS: Blockchain-based Data Sharing Scheme With Fine-grained Access Control And Permission Revocation In Medical Environment[J]. KSII Transactions on Internet & Information Systems, 2022, 16(5).

[10] Xue H, Chen D, Zhang N, et al. Integration of blockchain and edge computing in internet of things: A survey[J]. Future Generation Computer Systems, 2023, 144: 307-326.

[11] Ding X, Guo J, Li D, et al. Pricing and budget allocation for IoT blockchain with edge computing[J]. IEEE Transactions on Cloud Computing, 2022, 11(2): 1608-1621.

[12] Babu E S, Barthwal A, Kaluri R. Sec-edge: Trusted blockchain system for enabling the

identification and authentication of edge based 5G networks[J]. Computer communications, 2023, 199: 10-29.

[13] Liu S, Chai Y, Hui L, et al. Blockchain-based anonymous authentication in edge computing environment[J]. Electronics, 2023, 12(1): 219.

[14] Song Z, Ma H, Zhang R, et al. Everything under control: Secure data sharing mechanism for cloud-edge computing[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2234-2249.

[15] Guha Roy D. Blockedge: a privacy-aware secured edge computing framework using blockchain for industry 4.0[J]. Sensors, 2023, 23(5): 2502.

[16] Alharbi A. Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System[J]. Sensors, 2023, 23(6): 3020.

[17] Jin W, Xu Y, Dai Y, et al. Blockchain-based continuous knowledge transfer in decentralized edge computing architecture[J]. Electronics, 2023, 12(5): 1154.

[18] Zhang Y, Xiong L, Li F, et al. A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing[J]. Journal of Systems Architecture, 2023, 142: 102949.

[19] Wang W, Huang H, Yin Z, et al. Smart contract token-based privacy-preserving access control system for industrial Internet of Things[J]. Digital Communications and Networks, 2023, 9(2): 337-346.

[20] Quan G, Yao Z, Chen L, et al. A trusted medical data sharing framework for edge computing leveraging blockchain and outsourced computation[J]. Heliyon, 2023, 9(12).

[21] Minmin H, Lingyun Y, Xue P, et al. Trusted edge and cross-domain privacy enhancement model under multi-blockchain[J]. Computer Networks, 2023, 234: 109881.