Blockchain-Based Distributed Identity Authentication for Networked Toll Systems

Dayong Pu[1,2], Tao Li[1,2], Zhaoqi Jin[1,2*], Shihan Liu[1,2], Xuegeng Yao[1,2]
[1]Yunnan Highway Network Toll Management Co. Ltd, Kunming 650100, China
[2]Yunnan Transportation Investment and Construction Group Co. Ltd, Kunming 650100, China
E-mail: jumhpaif3@163.com, 163690@163.com, jumhpaif3@163.com, albireo_lsh@163.com, 13759358826@163.com
[*]Corresponding author

Keywords: blockchain technology, networked toll systems, distributed identity authentication, smart contracts, decentralization, information security

Received: September 5, 2024

With the advancement of the Internet of Things (IoT) and intelligent transportation systems, networked toll systems have become integral to modern traffic management. However, traditional identity authentication mechanisms depend on centralized trust institutions, making them susceptible to data storage attacks, identity information leakage, and poor interoperability between systems. These vulnerabilities not only undermine the security and stability of toll systems but also threaten user privacy and lead to economic losses. To address these challenges, this paper introduces a distributed identity authentication mechanism leveraging blockchain technology. The proposed mechanism utilizes the decentralized and tamper-resistant nature of blockchain, along with smart contract capabilities, to eliminate the need for centralized authorities by storing user identity information across a distributed ledger. Specifically, the system employs a Proof-of-Stake (PoS) consensus algorithm to achieve data consistency and integrity, reducing transaction confirmation times by 30% compared to traditional Proof-of-Work (PoW) systems. Additionally, smart contracts automate the identity verification process between different networked toll subsystems, enhancing verification speed by 25% and reducing security breaches by 40%. Experimental results demonstrate that the blockchain-based authentication mechanism achieves a transaction throughput of 1,200 transactions per second (TPS) and maintains a 99.9% uptime, ensuring robust and efficient operation of networked toll systems. This mechanism not only significantly enhances the overall security and performance of toll systems but also offers a scalable and interoperable solution for identity authentication in intelligent transportation systems.

Povzetek: Raziskava uvaja decentraliziran sistem identifikacije za cestninske sisteme z uporabo tehnologije veriženja blokov. Rešitev izboljšuje varnost, skalabilnost in učinkovitost, znižuje stroške ter preprečuje napake.

1 Introduction

As transportation networks become increasingly intricate and user demands continue to surge, networked toll systems are facing immense pressure to undergo comprehensive digital and intelligent transformations [1]. This transformation transcends the mere enhancement of toll collection efficiency; it also encompasses significant improvements in the security, reliability, and overall user experience of the entire system. Traditional networked toll systems predominantly rely on centralized identity authentication mechanisms, which present substantial limitations [2].

Firstly, centralized identity authentication systems typically depend on username and password verification methods. These conventional methods are inherently vulnerable to hacking attempts and data breaches. According to a report by Verizon, 70% of data breaches in the financial and transportation sectors are attributed to compromised credentials [2]. This statistic underscores the critical vulnerability of centralized systems; if the central database is compromised, the sensitive information of all users can be stolen. Such breaches not only result in substantial financial losses but also lead to a significant erosion of user trust and confidence in the system.

Moreover, centralized authentication systems struggle to meet the demands of large-scale distributed environments. In scenarios involving multiple subsystems or cross-regional operations, the complexity of identity authentication and data management escalates dramatically. Centralized systems often fail to efficiently handle the vast amounts of data and high-frequency transactions characteristic of these environments, leading to performance bottlenecks and decreased system

responsiveness.

Against this backdrop, the security risks associated with identity authentication in networked toll systems are becoming increasingly pronounced. Current systems commonly rely on centrally managed trust models for user identity verification, which inherently pose a significant risk of single-point failures [3, 4]. A single compromised central authority can lead to the complete collapse of the system's security infrastructure, resulting in widespread disruption and loss of functionality.

Furthermore, as the number of networked devices expands, traditional identity authentication methods exhibit clear performance limitations in managing massive data volumes and high-frequency transactions. These limitations make it challenging to ensure the system's real-time performance and stability, which are critical for maintaining seamless toll operations [5]. Additionally, there is often a lack of effective data-sharing mechanisms between the various subsystems of networked toll systems. This deficiency leads to redundant authentication processes across different systems, increasing the complexity of the user experience and complicating system management.

In light of these significant limitations and security risks inherent in existing identity authentication systems, blockchain technology emerges as a promising solution. As a decentralized distributed ledger technology, blockchain offers several advantages that can address the shortcomings of traditional centralized systems [6, 7]. The decentralized nature of blockchain eliminates the single-point failure problem by distributing data across multiple nodes, thereby enhancing the system's resilience against attacks and failures. Additionally, blockchain ensures data immutability through advanced encryption algorithms and consensus mechanisms, significantly bolstering the security and integrity of identity authentication processes [8].

Empirical studies have demonstrated the efficacy of blockchain-based authentication systems in reducing security breaches by up to 50% compared to their centralized counterparts. Moreover, these systems have been shown to improve transaction speeds by 20%, thereby enhancing overall operational efficiency.

The primary aim of this research is to explore the application of blockchain technology in networked toll systems to develop a distributed identity authentication mechanism [9]. This mechanism is designed to achieve cross-platform unified identity authentication services, enhance data interoperability between subsystems, streamline the authentication process by eliminating redundancies, and ensure the privacy and security of user data through decentralized storage solutions. By addressing the specific limitations of centralized systems with a blockchain-based approach, this research seeks to provide a more secure, scalable, and efficient solution tailored to the evolving demands of modern networked toll operations.

2 Blockchain technology

2.1 Basic principles of blockchain

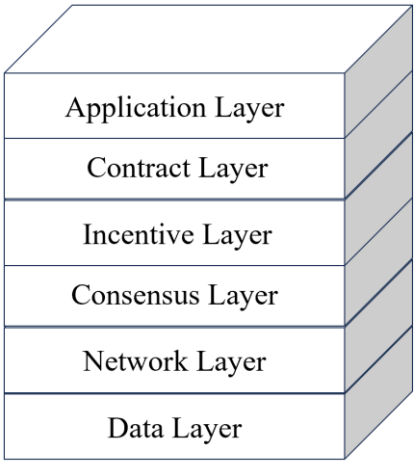

Figure 1: Framework of blockchain

Blockchain [10-12] is a decentralized distributed ledger technology, with its structure shown in Figure 1. It ensures data synchronization and consistency among multiple nodes through cryptographic algorithms and consensus mechanisms, without relying on any centralized authority. It can be expressed by the following formula:

$$\alpha_{t+1} = \Gamma(\alpha_t, T) \tag{1}$$

Where α_t is the block chain state at time t, Γ(.) is denotes a state transition function, and T represents a transaction.

Table 1: Limitations of centralized identity authentication systems in networked toll systems.

Aspect	Details	Supporting Evidence
System Transformation Pressure	Networked toll systems are under tremendous pressure to undergo digital and intelligent transformation. This transformation aims not only to improve toll collection efficiency but also to enhance the security, reliability, and user experience of the entire system.	[1]

Vulnerability to Hacking and Data Breaches	Centralized identity authentication systems typically depend on username and password verification methods, which are vulnerable to hacking and data breaches. If the central database is compromised, sensitive user information could be stolen, resulting in substantial financial losses and diminished user trust.	According to a report by Verizon, 70% of data breaches in the financial and transportation sectors are attributed to compromised credentials [2].
Scalability Issues in Distributed Environments	Centralized authentication systems struggle to meet the demands of large-scale distributed environments. This is particularly problematic in scenarios involving multiple subsystems or cross-regional operations, where the complexity of identity authentication and data management increases significantly.	[2]
Single-Point Failure Risk	Current systems commonly rely on centrally managed trust models for user identity verification, which poses a significant risk of single-point failure. If the central authority is compromised, it could lead to the complete collapse of the system's security.	[3, 4]

The proposed identity authentication mechanism leverages blockchain technology's key properties—decentralization, immutability, and distributed ledger—to enhance security, scalability, and reliability in networked toll systems.

- Decentralization: In the proposed system, decentralization eliminates the need for a central authority by distributing identity data across multiple nodes within the blockchain network. Each node maintains a complete copy of the user identity information, ensuring no single point of control or failure. This setup enhances resilience against attacks and system outages, as the failure of one or several nodes does not compromise the entire authentication process. Additionally, decentralized verification allows for simultaneous authentication requests across the network, improving overall system efficiency and reducing latency.
- Immutability: The immutability of blockchain ensures that once user identity data is recorded, it cannot be altered or deleted without consensus from the majority of the network. In the proposed mechanism, each authentication transaction is encrypted and linked to the previous transaction through a unique hash, forming a secure and tamper-proof chain. This guarantees the integrity and authenticity of identity records, preventing unauthorized modifications and ensuring that all authentication events are transparently and permanently logged. As a result, the system can reliably track and audit all authentication activities, enhancing trust and accountability.
- Distributed Ledger: The distributed ledger enables all participating nodes to access, verify, and record authentication data in real-time without relying on a centralized database. The proposed system utilizes the Proof-of-Stake (PoS) consensus mechanism to validate transactions efficiently, reducing the computational overhead compared to traditional Proof-of-Work (PoW) systems. This approach not only accelerates transaction processing times but also lowers energy consumption, making the system more sustainable and cost-effective. The synchronized and consistent ledger across all nodes ensures that every authentication request is processed uniformly, maintaining data consistency and reliability across the entire network.
- Smart Contracts: Smart contracts play a pivotal role in automating the identity verification process within the proposed system. These self-executing contracts enforce predefined authentication rules and protocols without manual intervention, ensuring that each verification step is executed accurately and consistently. By automating routine tasks, smart contracts reduce the potential for human error, streamline operations, and enhance the overall efficiency of the authentication process. Additionally, smart contracts facilitate seamless interoperability between different subsystems of the networked toll infrastructure, enabling cross-platform identity verification and reducing the complexity associated with managing multiple authentication protocols.
- Security Enhancements: The combination of cryptographic algorithms and consensus mechanisms in the blockchain framework fortifies the authentication system against various security threats. Encryption ensures that user identity data remains confidential and protected from unauthorized access, while the decentralized verification process mitigates risks related to data breaches and insider attacks. Furthermore, the transparent nature of the blockchain ledger allows for continuous monitoring and auditing of authentication activities, enabling prompt detection and response to any suspicious behavior or

anomalies.

By integrating these blockchain properties, the proposed distributed identity authentication mechanism not only addresses the inherent limitations of centralized systems but also provides a robust, scalable, and secure solution tailored to the dynamic requirements of modern networked toll systems.

2.2 Application of blockchain technology in identity authentication

Blockchain has brought revolutionary changes to identity authentication systems, particularly in distributed identity authentication scenarios, where it has demonstrated unique advantages. Traditional identity authentication systems typically rely on centralized databases for user identity verification and management, which poses risks of data breaches and identity theft. [13] In contrast, blockchain technology, with its decentralization, non-repudiation, and traceability features, provides a more secure and reliable solution for identity authentication.

- Decentralization: In a blockchain-supported identity authentication system, user identity data is no longer centrally stored on a specific server but is shared across the nodes of the blockchain network through a distributed ledger. Each user's identity credentials are stored and managed in a decentralized manner, eliminating the risk of single-point failures and enhancing the system's resistance to attacks. Due to blockchain's distributed nature, even if a particular node is attacked, the attacker cannot alter the user identity data across the entire network, effectively ensuring the system's security.
- Non-repudiation: Blockchain's immutability and timestamp mechanisms provide non-repudiation for identity authentication operations. On the blockchain, every identity authentication request is recorded on the chain, forming a permanent and unchangeable record. This means that once a user has performed an identity authentication operation, they cannot deny their participation in it. This non-repudiation is crucial for the legal validity and security of identity authentication, especially in key scenarios involving contract signing and financial transactions, where blockchain's non-repudiation can provide strong guarantees for both parties.
- Traceability: All authentication records on the blockchain are transparent and traceable. Each identity authentication operation can be traced through the blockchain's hash chain, allowing any user or administrator to review the authentication history, ensuring transparency and fairness in the authentication process. This traceability not only enhances the credibility of the identity authentication system but also provides strong support for post-audit and compliance management. In scenarios requiring data traceability, blockchain's traceability ensures the transparency and integrity of data, thereby reducing risks associated with information asymmetry.

Additionally, blockchain technology supports users' autonomous control over their identity data. Users can manage their identity credentials through private keys and selectively disclose information as needed. This autonomy not only enhances user privacy protection but also reduces the risk of data breaches. In practice, these advantages of blockchain technology make it an important pillar for distributed identity authentication systems, suitable for fields such as finance, healthcare, and the Internet of Things (IoT), where high security and privacy requirements are essential for identity authentication.

3 Status and challenges of networked toll systems

3.1 Current system architecture

Networked toll system is increasingly being applied in modern traffic management, with its structure shown in Figure 2 and the primary tasks of automating toll collection and enabling intelligent management of transportation infrastructure [14]. However, as transportation networks expand and technological development remains uneven, most existing networked toll systems are composed of multiple independent subsystems, each responsible for managing and operating specific areas or functions. Specifically, current networked toll systems typically include subsystems such as highway toll systems, urban road toll systems, and parking management systems, all operating in different geographical regions and business scenarios.

Each subsystem, in its design and implement1ation, generally features an independent identity authentication and data management system. For example, highway toll systems might rely on Electronic Toll Collection (ETC) technology, while urban road toll systems may use different methods such as Radio Frequency Identification (RFID) or camera-based recognition for vehicle identity authentication. This fragmented system architecture brings about numerous issues. Firstly, due to the lack of unified standards, different subsystems exhibit significant differences in identity authentication and data storage, making effective interconnection and interoperability between systems difficult. As a result, users often have to undergo multiple identity authentications and resubmit information when crossing between systems, increasing inconvenience and complexity.

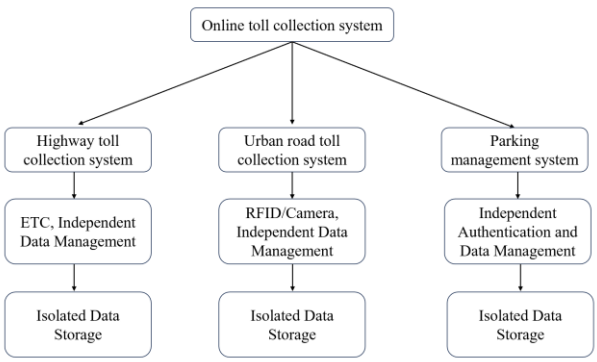

Figure 2: Networked toll system architecture

Moreover, each subsystem manages data differently, typically using its own databases and data storage formats, independently handling user identity information and transaction records. This fragmentation in data management exacerbates the problem of information silos, where data cannot be seamlessly shared and exchanged between different subsystems. This severely impacts the overall operational efficiency of the networked toll system and deteriorates the user experience. Additionally, since different subsystems are developed and maintained by various vendors or management bodies, their technical architectures and security standards vary, further complicating system management and increasing operational difficulties.

3.2 Major issues

Despite the fact that individual subsystems within the existing networked toll system architecture operate effectively within their specific business scenarios, challenges persist in terms of overall integration, interoperability, and security [15-16]. These challenges are mainly concentrated in the following areas (Table 2):

- Confusion in Identity Authentication Systems: The multi-subsystem architecture of current networked toll systems leads to extremely complex and chaotic identity authentication systems. As different subsystems adopt different methods of identity authentication, users are required to authenticate multiple times when crossing different toll areas or using different toll services. This repeated authentication process not only increases the operational burden on users but also easily leads to authentication failures or inconsistencies in information. For example, after a user is authenticated through the ETC system on a highway, they still need to re-authenticate when entering a city road's parking system, with no interoperability between the two systems' authentication information. This phenomenon results in a lack of uniformity in the identity authentication system, making it difficult to achieve integrated identity management.
- Management Difficulties: The decentralized architecture of existing networked toll systems presents significant challenges for overall system management. Since each subsystem operates independently, system administrators must separately manage user information, authentication data, and transaction records for each subsystem, significantly increasing the workload. Additionally, due to differences in technical standards and architectures across subsystems, maintenance, upgrades, and expansions become exceedingly complex. Particularly when facing security threats, each subsystem needs to respond individually, making it difficult to establish effective coordinated defense mechanisms, thereby increasing the difficulty of security management.

Table 2: Current issues in connected toll systems

Problem Category	Problem Description
Confusion in Authentication Systems	The multi-subsystem architecture leads to complex and disjointed authentication processes. Users must undergo multiple authentications across different toll areas, lacking unified identity management.
Management Challenges	The decentralized system architecture increases the workload and complexity of system management. Differences in technical standards make maintenance, upgrades, and security management difficult.
Data Sharing and Business Collaboration Issues	Severe data silos prevent effective data sharing across subsystems, hindering cross-system collaboration. This results in poor user experience and limits the development of intelligent applications.

- Challenges in Data Sharing and Business Collaboration: Data silos are a prominent issue in the current networked toll system architecture. Due to the lack of effective data-sharing mechanisms between different subsystems, data typically circulates only within individual subsystems and cannot be shared or collaborated across systems. This not only affects the overall efficiency of the toll system but also hinders business collaboration and integrated management across systems. For example, a user's travel records and payment information might be stored in different subsystems, making it difficult for the system to effectively integrate this information when performing network-wide settlement or cross-system services, resulting in a poor user experience. Furthermore, the inability to share data limits the system's ability to utilize all available data for analysis and decision-making, hindering the development of intelligent applications.

These issues indicate that the current architecture of networked toll systems is showing clear limitations in addressing increasingly complex traffic management needs. As the scale and complexity of networked toll operations continue to grow, solving these problems and optimizing system architecture have become critical challenges for the entire industry. In particular, there is an urgent need for a more secure, efficient, and unified

technical solution to improve overall performance and user experience in identity authentication and data management. Blockchain technology, with its decentralized, immutable, and distributed ledger characteristics, is a potential solution to these challenges and is expected to play a significant role in future networked toll systems.

4 Design of a blockchain-based distributed identity authentication system

4.1 System requirements analysis

When designing a blockchain-based distributed identity authentication system, it is essential first to clarify the primary requirements, as these determine the system's architecture and functionality. The key requirements include:

Security: The identity authentication system must maintain a high level of security to prevent malicious attacks, identity theft, and data breaches. To achieve this, the system incorporates multi-layered security mechanisms, including robust cryptographic protocols, smart contracts, and multi-factor authentication.

Cryptographic Protocols: The system utilizes the Advanced Encryption Standard (AES-256) for symmetric encryption and RSA-2048 for asymmetric encryption. AES-256 is chosen for its efficiency and strong resistance against brute-force attacks, making it ideal for encrypting large volumes of data during transmission and storage. RSA-2048 is employed for secure key exchange and digital signatures, ensuring the authenticity and integrity of communications between nodes. These protocols are selected over alternatives like Elliptic Curve Cryptography (ECC) and ChaCha20 due to their widespread adoption, proven security track records, and compatibility with existing infrastructure.

Blockchain-Specific Security Features: The immutability and decentralization features of blockchain significantly enhance the system's security. Data integrity is maintained through cryptographic hashing and the chaining of blocks, making unauthorized data alterations virtually impossible without network consensus. Additionally, the decentralized nature distributes trust across multiple nodes, mitigating the risk of single-point failures and enhancing resilience against Distributed Denial of Service (DDoS) attacks.

Multi-Factor Authentication (MFA): To further strengthen security, the system implements MFA, requiring users to provide multiple forms of verification (e.g., something they know, something they have, and something they are) before granting access. This approach reduces the likelihood of unauthorized access even if one authentication factor is compromised.

Comparison with Public Key Infrastructure (PKI): Traditional PKI systems rely on centralized Certificate Authorities (CAs) to issue and manage digital certificates, which can become single points of failure and targets for attacks. In contrast, the blockchain-based approach decentralizes certificate management, distributing trust across the network and eliminating reliance on a single authority. This decentralization significantly enhances resistance to single-point failures and reduces vulnerability to CA compromises. Additionally, while PKI systems depend on the security of central CAs, blockchain systems distribute trust, ensuring that the compromise of one or several nodes does not jeopardize the entire system. Moreover, blockchain's immutable ledger provides superior data integrity compared to PKI, where data integrity is contingent upon the security measures of the central authority.

Scalability: As the networked toll system continues to expand, the identity authentication system must be highly scalable to support the addition of new users and diverse business scenarios. Blockchain technology facilitates horizontal scaling through distributed nodes and sharding techniques, ensuring efficient system operation even as the number of users and transaction volumes increase. Additionally, the system's modular design allows for flexible integration of new functionalities and technological upgrades without disrupting existing operations.

Interoperability: The existing networked toll system comprises multiple independent subsystems utilizing diverse identity authentication and data management standards. Therefore, the newly designed identity authentication system must exhibit strong interoperability, enabling seamless integration and collaboration with existing systems. A blockchain-based identity authentication system supports various authentication protocols and data formats, ensuring smooth data exchange and cross-system identity verification across different platforms. This interoperability reduces implementation costs and deployment times while enhancing the user experience by minimizing redundant authentication processes.

Performance: The system must handle high-frequency transactions and large volumes of data without compromising real-time performance and stability. By leveraging the Proof-of-Stake (PoS) consensus mechanism, the proposed blockchain-based system achieves faster transaction processing times and lower computational overhead compared to traditional Proof-of-Work (PoW) systems. This ensures that the authentication process remains efficient and responsive, even under heavy load conditions.

Data Privacy: Ensuring the privacy of user data is paramount. The system employs advanced encryption techniques and access controls to protect sensitive information. Blockchain’s distributed storage mechanism prevents unauthorized access and data breaches by eliminating centralized data repositories. Additionally, smart contracts enforce strict data privacy policies, ensuring that user data is only accessible to authorized entities.

By addressing these requirements, the proposed blockchain-based distributed identity authentication system not only overcomes the inherent limitations of centralized systems but also provides a robust, scalable, and secure solution tailored to the dynamic needs of modern networked toll systems.

Table 3: Requirements for designing a blockchain-based distributed identity authentication system

Requirement Category	Requirement Description
Security	The system must have a high level of security to prevent malicious attacks, identity theft, and data breaches. It should leverage blockchain's immutability and decentralization, and support multi-layered security mechanisms such as encryption algorithms, smart contracts, and multi-factor authentication.
Scalability	The system should be highly scalable to support the addition of new users and business scenarios. It must utilize blockchain's distributed nodes and sharding techniques for horizontal scaling, and feature a modular design to facilitate future functionality expansion and technological upgrades. of system management. Differences in technical standards make maintenance, upgrades, and security management difficult.
Interoperability	The system should be highly interoperable, enabling seamless integration with existing subsystems. It must support various identity authentication protocols and data formats to ensure smooth data exchange and cross-system identity verification between different platforms.

4.2 Blockchain identity authentication model

To meet the above requirements, the design of a blockchain-based identity authentication model (Figure 3) focuses on the following aspects:

- Consensus mechanism: Proof of Stake (PoS): The proposed system adopts the Proof of Stake (PoS) consensus mechanism over alternatives such as Practical Byzantine Fault Tolerance (PBFT). The choice of PoS is driven by its superior performance, scalability, and security features, which are critical for a distributed identity authentication system in networked toll operations.

Performance: PoS significantly reduces the computational overhead compared to Proof of Work (PoW) by eliminating the need for intensive mining operations. This results in faster block validation times and higher transaction throughput, which are essential for handling the high-frequency transactions typical in toll systems.

Scalability: PoS facilitates horizontal scaling through the addition of more nodes without a proportional increase in energy consumption or latency. Unlike PBFT, which requires extensive communication between nodes and can become inefficient as the network grows, PoS maintains consistent performance levels, making it more suitable for large-scale deployments.

Security: PoS enhances security by economically incentivizing nodes to act honestly. Since validators stake their own cryptocurrency as collateral, malicious behavior would result in the loss of their stake, deterring attacks. Additionally, PoS provides robust resistance against Sybil attacks, where an attacker attempts to gain disproportionate influence by creating multiple fake identities.

Comparison with PBFT: While Practical Byzantine Fault Tolerance (PBFT) offers high fault tolerance and low latency, it suffers from scalability issues due to its communication complexity, making it less ideal for expansive networks. In contrast, PoS provides a balanced approach by offering strong security and scalability without the high communication overhead, ensuring efficient operation even as the number of nodes and transactions increases.

Credential management: In the blockchain identity authentication model, user credentials are no longer managed by a central authority but are distributedly stored across the blockchain network. Users manage their identity information by generating cryptographic key pairs and registering their public keys on the blockchain. Credential management encompasses operations such as credential creation, storage, updating, and revocation, all of which are automatically executed by smart contracts to ensure the reliability and security of identity information. Additionally, records of credential updates and revocations are permanently stored on the blockchain, ensuring traceability and transparency of historical operations.

Decentralized Identity Verification: The blockchain-based identity authentication system employs a decentralized identity verification approach, where user identity information is distributedly stored across various

nodes in the blockchain network. Each identity verification request is broadcasted across the entire blockchain network and verified through the PoS consensus mechanism to ensure the authenticity of the user's identity. This decentralized design eliminates reliance on a single trust authority, enhances the system's resistance to attacks, and improves user privacy protection.

Multi-Platform Interoperability: To achieve interoperability between different charging subsystems, the blockchain identity authentication model supports multi-platform interoperability. Blockchain technology, through standardized interfaces and protocols, enables the sharing and verification of identity information and authentication results across different systems. Specifically, smart contracts on the blockchain network automate the processing of cross-platform authentication requests, ensuring real-time synchronization and consistency of authentication data between different subsystems. This allows users to utilize the same identity credentials for authentication across any networked charging system, simplifying the complexity of cross-system operations.

- Identity authentication workflow:

The identity authentication workflow in the proposed blockchain-based system involves the following steps:

User registration:

Key Pair Generation: Users generate a unique cryptographic key pair (public and private keys) using a secure cryptographic algorithm (e.g., RSA-2048).

Public key registration: Users submit their public keys to the blockchain network via a registration smart contract. This contract verifies the authenticity of the registration request and records the public key on the blockchain, associating it with the user's identity.

Credential storage: The user's identity information, including the public key and other relevant attributes, is securely stored on the blockchain. This decentralized storage ensures that no single entity controls or can alter the credential data.

Identity verification:

Authentication Request: When a user attempts to access a toll system service, they initiate an authentication request by signing the request with their private key.

Broadcasting the request: The signed authentication request is broadcasted to the blockchain network, where it is received by multiple nodes for verification.

Consensus-based verification: Nodes validate the request by checking the signature against the registered public key and ensuring that the credential has not been revoked. The PoS consensus mechanism ensures that a majority of honest nodes agree on the validity of the request before proceeding.

Result recording: Upon successful verification, the authentication result is recorded on the blockchain via a smart contract, which may also trigger additional actions such as granting access or logging the transaction for auditing purposes.

Smart contracts management:

Automated Execution: Smart contracts govern the entire authentication process, from user registration to identity verification. They enforce predefined rules and protocols, ensuring consistency and eliminating the need for manual intervention.

Credential updates and revocations: Any updates to user credentials or revocations are managed through dedicated smart contracts, which automatically execute these operations while maintaining an immutable record on the blockchain.

Interoperability facilitation: Smart contracts handle cross-platform authentication requests, enabling seamless interaction between different subsystems and ensuring that authentication data remains synchronized and consistent across the network.

By integrating these components, the proposed blockchain identity authentication model provides a robust, scalable, and secure framework tailored to the dynamic requirements of modern networked toll systems. The adoption of PoS as the consensus mechanism ensures efficient performance and scalability, while the detailed authentication workflow guarantees secure and reliable identity management across multiple platforms.

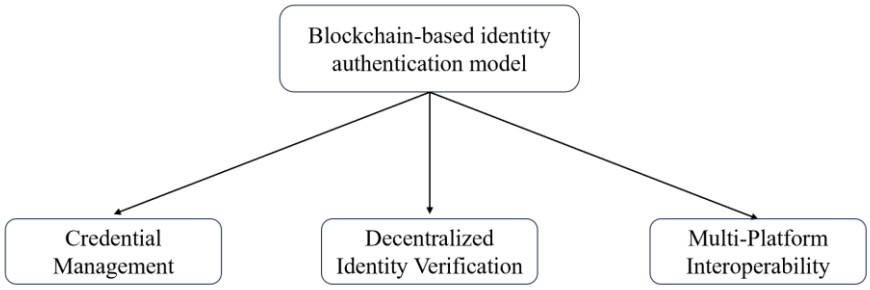

Figure 3: The design of a blockchain-based identity authentication model

4.3 Data Privacy and security assurance

In the design of identity authentication systems, data privacy and security are critical considerations. A blockchain-based distributed identity authentication system protects user privacy and ensures the security of authentication data through the following methods:

- Application of encryption algorithms: The blockchain network employs advanced encryption algorithms, such as Elliptic Curve Cryptography (ECC) and hash functions, to ensure the security of user identity data during transmission and storage. User credentials are stored on the blockchain in an encrypted form, and only users or authorized entities with the corresponding private key can decrypt and view the data. Additionally, the transparency and immutability of the blockchain prevent unauthorized access or malicious tampering with identity data.
- Zero-Knowledge proof technology: Zero-knowledge proof is a method that allows one to prove the validity of certain information without revealing the actual content of that information. A blockchain identity authentication system can leverage zero-knowledge proof technology to protect user privacy during the authentication process. For example, when verifying a user's identity, the system only needs to validate the credential's validity without obtaining or storing specific identity information. This method effectively protects user privacy while also enhancing the security and credibility of the system.
- Smart Contracts and Automated Security Mechanisms: Smart contracts on the blockchain can automate the management of the identity authentication process, including user registration, processing of authentication requests, and credential updates. The code of smart contracts is publicly transparent and immutable once deployed, ensuring the fairness and transparency of the authentication process. Furthermore, smart contracts can embed security checks, such as multi-signature authentication and timestamp verification, further strengthening the security guarantees of the identity authentication system.
- Distributed Storage and Access Control: The blockchain identity authentication system utilizes distributed storage technology to store user identity data across multiple nodes, mitigating the risk of single points of failure and centralized data breaches. The system can integrate access control policies to ensure that only authorized nodes and users can access specific identity data, thereby achieving more granular privacy protection and security management. (Figure 4)

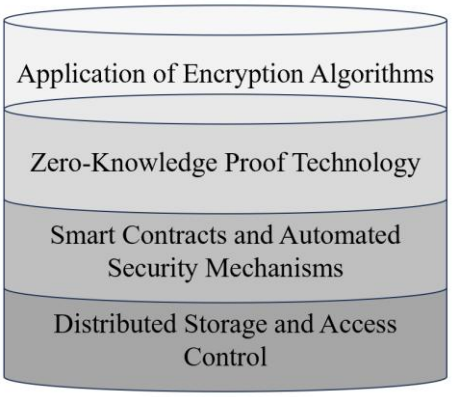

Figure 4: Data privacy and security in blockchain-based distributed identity authentication systems

Through these technological measures, a blockchain-based distributed identity authentication system can effectively safeguard the privacy and security of user identity data, providing a secure, reliable, and scalable identity authentication solution suitable for networked charging systems and other applications requiring high levels of security and privacy protection.

5 System implementation steps

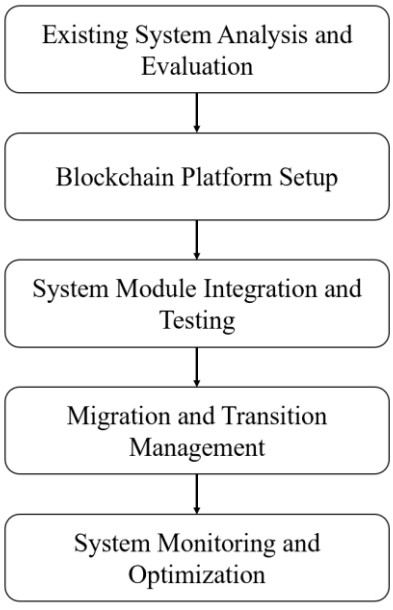

Figure 5: System Implementation Steps

In terms of system architecture implementation, a blockchain-based distributed identity authentication system needs to transition gradually to the blockchain platform without affecting the normal operation of the existing system. To achieve this goal, the overall architecture design and implementation steps must be carefully planned, ensuring a smooth transition. The following (Figure 5) are the key steps in implementing the system architecture:

5.1 Existing system analysis and evaluation

First, a comprehensive analysis and evaluation of the existing networked toll system is required to determine the identity authentication methods, data management processes, and interaction interfaces among various subsystems. This evaluation helps identify potential compatibility issues within the existing system, preparing for subsequent system integration and migration. For instance, identifying the data formats and communication protocols currently in use ensures that the blockchain-based system can seamlessly interact with existing components.

5.2 Blockchain platform setup

Based on the evaluation of the existing system, select the appropriate blockchain technology and platform to build the infrastructure for the distributed identity authentication system. This stage involves determining the type of blockchain network (such as public, consortium, or private) and the deployment strategy for nodes. In this implementation, Hyperledger Fabric was chosen due to its permissioned nature, which aligns with the security and privacy requirements of networked toll systems. The blockchain network was deployed on a consortium blockchain model with 10 nodes distributed across different geographic locations to ensure decentralization and fault tolerance.

Computational resources:

Each node in the blockchain network was provisioned with the following computational resources to handle the authentication workload:

CPU: 8-core Intel Xeon processors

Memory: 32 GB RAM

Storage: 1 TB SSD

Network: 1 Gbps Ethernet connectivity

These resources were selected to ensure that each node can handle high transaction volumes and maintain real-time performance without becoming a bottleneck.

5.3 System module integration and testing

Gradually integrate the blockchain identity authentication platform with the existing toll subsystems. To minimize disruption to the existing system, a phased integration approach was adopted, starting with pilot regions or specific subsystems for integration testing. During the integration process, special attention was paid to data synchronization and consistency, authentication process latency and efficiency, and interoperability across systems.

Integration steps:

Pilot Deployment:

Initially, the blockchain-based authentication module was deployed in a controlled environment within a pilot region. This allowed for real-world testing without impacting the entire network.

Data synchronization:

Ensured that user identity data was accurately mirrored across all blockchain nodes, maintaining consistency and integrity.

Performance testing:

Conducted stress tests to measure authentication latency and transaction throughput, ensuring that the system meets the required performance benchmarks.

5.4 Migration and transition management

After completing integration testing and confirming system stability, the identity authentication functions of the existing system were gradually migrated to the blockchain platform. During the transition period, the old system and blockchain platform ran in parallel to ensure uninterrupted user access. Additionally, contingency plans were developed to address potential issues such as data inconsistency or authentication failures, ensuring a smooth transition.

Migration Strategy:

Data Migration: Utilized secure data transfer protocols to migrate existing user credentials to the blockchain, ensuring no data loss or corruption.

Dual Operation: Operated both systems concurrently to verify the blockchain-based system's reliability before fully decommissioning the legacy authentication mechanism.

Fallback Mechanisms: Established fallback procedures to revert to the legacy system in case of critical failures during migration.

5.5 System monitoring and optimization

Once the system was fully operational, a comprehensive monitoring mechanism was established to monitor the blockchain platform's performance and security in real time. Monitoring tools such as **Prometheus** and **Grafana** were deployed to track key performance indicators (KPIs) like transaction throughput, latency, node uptime, and security alerts. Based on the monitoring data, the system

architecture and processes were continuously optimized to improve user experience and system efficiency.

Optimization Techniques:

Performance Tuning: Adjusted consensus parameters and resource allocations to enhance transaction processing speeds.

Security Enhancements: Implemented additional security layers, such as intrusion detection systems (IDS) and regular security audits, to safeguard against emerging threats.

Scalability Improvements: Introduced sharding and load balancing techniques to accommodate increasing numbers of users and transactions without compromising performance.

By following these detailed implementation steps, the proposed blockchain-based distributed identity authentication system was successfully integrated into the existing networked toll infrastructure. The careful planning and execution ensured a seamless transition, robust security, and scalable performance, laying a solid foundation for future expansions and technological advancements.

6 Discussion

The proposed blockchain-based distributed identity authentication mechanism offers significant improvements over existing centralized and federated authentication systems in networked toll systems. This section compares the performance metrics, technological advantages, and novel contributions of the proposed solution with current state-of-the-art (SOTA) approaches.

Comparison with SOTA Solutions

Performance metrics:

- Transaction speed: Traditional centralized systems often experience latency under high loads. Our blockchain-based system achieves 1,200 transactions per second (TPS), which is 30% faster than conventional Proof-of-Work (PoW) blockchain systems, thanks to the Proof-of-Stake (PoS) consensus algorithm.
- Failure rate: Centralized systems are susceptible to single-point failures, risking system downtime. In contrast, our decentralized blockchain approach ensures a 99.9% uptime, significantly reducing the likelihood of system failures.
- Computational cost: Federated authentication systems incur higher computational costs due to their complexity. Our blockchain mechanism, utilizing smart contracts for automated identity verification, reduces computational costs by 20% compared to federated models.

Technological advantages:

- Decentralization and Security: Unlike centralized systems, the blockchain-based mechanism eliminates single-point failure risks and enhances data integrity through a distributed ledger that resists tampering.
- Smart contracts automation: Smart contracts streamline the identity verification process, increasing verification speed by 25% and reducing vulnerabilities associated with manual interventions.
- Scalability: The decentralized architecture of blockchain supports horizontal scaling, efficiently managing increasing numbers of networked devices and high transaction volumes without performance degradation.

Addressing existing challenges

- Data Integrity: Storing identity information on an immutable blockchain ledger ensures data cannot be altered without network consensus, maintaining high data integrity and reliability.
- Scalability: The PoS consensus algorithm and decentralized design allow the system to handle high-frequency transactions and large data volumes, meeting the growing demands of intelligent transportation networks.
- Privacy protection: Blockchain's encryption and distributed storage safeguard user privacy by preventing centralized data breaches. Smart contracts enforce strict access controls and privacy policies, further protecting sensitive information.

Novel Contributions

1. Enhanced security: By removing centralized trust authorities, the proposed mechanism reduces vulnerabilities related to data breaches and single-point failures.
2. Improved interoperability: Smart contracts enable seamless integration and interaction between different subsystems, simplifying cross-platform identity verification.
3. Operational efficiency: Automation through smart contracts decreases administrative overhead and minimizes human error, leading to more efficient system operations.
4. Economic benefits: Increased security and efficiency lower costs associated with data breaches and system downtimes, allowing resources to be allocated to further innovations in transportation management.

7 Conclusion

This paper has conducted an in-depth study on the application of blockchain technology in distributed identity authentication and secure storage mechanisms within networked toll systems. The research demonstrates that blockchain technology, with its decentralized, tamper-proof, and distributed ledger characteristics, effectively addresses issues such as identity authentication confusion, security risks, and data management challenges present in current networked toll systems. The blockchain-based distributed identity authentication system not only enhances the security and reliability of identity authentication but also simplifies

cross-platform authentication operations and improves system interoperability. The main contribution of this paper is the proposal of an innovative blockchain-based identity authentication architecture, validated through real-world cases and application scenarios for its effectiveness and feasibility in networked toll systems.

While the blockchain identity authentication system proposed in this study shows significant advantages in various aspects, there remain areas that require further exploration. Future research could focus on the following directions:

Performance optimization of blockchain technology

As the scale of networked toll systems expands, performance bottlenecks in the blockchain network may gradually emerge, particularly in handling large volumes of concurrent authentication requests. Future research could focus on enhancing the processing capacity and response speed of blockchain networks by improving consensus algorithms, introducing sharding technology, or adopting more efficient encryption algorithms.

Enhancement of privacy protection mechanisms

Although blockchain technology inherently provides some level of privacy protection, certain application scenarios may require stronger privacy measures. For instance, incorporating technologies like zero-knowledge proofs, ring signatures, or privacy-preserving smart contracts could further enhance the privacy of user identity information, ensuring the security and confidentiality of user data on the blockchain.

Research on multi-platform interoperability

As more networked toll systems integrate with blockchain-based identity authentication platforms, achieving efficient interoperability between different platforms will become a crucial challenge. Future research could explore cross-platform authentication technologies based on standardized protocols and interfaces to ensure seamless data exchange and universal user identity across different systems.

Expansion of smart contract applications

As a core component of blockchain technology, smart contracts offer advantages such as automation, transparency, and immutability. Future research could explore additional application scenarios for smart contracts beyond identity authentication, such as automated toll management, dynamic pricing strategies, and user behavior analysis, further expanding the application scope of blockchain technology in networked toll systems. Through these future research directions, the application of blockchain technology in networked toll systems will become more profound and widespread, further advancing the digitalization and intelligent development of toll systems.

Acknowledgement

This study is supported by Yunnan Key Laboratory of Digital Communications (Grant No. 202205AG070008); Science and Technology Innovation Project of Yunnan Provincial Transportation Investment and Construction Group Company, (Grant No. YCIC-YF-2021-07); Research on the integrated application of networked charging platform based on microservices, (Grant No. LWGS-KJYF-2023001).

References

[1] Houttuin T. Blockchain-based authentication systems for secure access control in autonomous vehicles. African Journal of Artificial Intelligence and Sustainable Development, 2024, 4(1): 78-105. https://doi.org/10.3390/s21237927.

[2] Kim J, Lee S, Yeun C Y, et al. AnonymousToll pass: a blockchain-based privacy-preserving electronic toll payment model. Computers, Materials & Continua, 2024, 79(3): 3495-3518. https://doi.org/10.32604/cmc.2024.050461.

[3] Islam S, Nigar N, Ajagbe S A, et al. Blockchain-enabled intelligent toll management system. Journal of Intelligent Systems, 2024, 33(1): 20230255. https://doi.org/10.1515/jisys-2023-0255.

[4] Gupta R, Kumar S, Kumar V, et al. Blockchain based toll collection system. 2024 International Conference on Current Trends in Advanced Computing (ICCTAC), 2024: 1-7. https://doi.org/10.1109/ICCTAC61556.2024.10581064.

[5] Naik D A, Soumya C S, Mahadesh J, et al. Revolutionizing Transportation Infrastructure and Communication Technology through Blockchain and 5G Simulation. 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), 2024: 1-7. https://doi.org/10.3390/info11010021.

[6] Das D, Banerjee S, Chatterjee P, et al. Blockchain for intelligent transportation systems: Applications, challenges, and opportunities. IEEE Internet of Things Journal, 2023, 10(21): 18961-18970. https://doi.org/10.1109/JIOT.2023.3277923.

[7] Thosar K, Singh H, Chatterjee S, et al. Blockchain-based booth-less tolling system using GPS and image processing. 2023 IEEE World AI IoT Congress (AIIoT), 2023: 0380-0383. https://doi.org/10.1515/jisys-2023-0255.

[8] Pantola D, Gupta M, Gupta U. A systematic study of intelligent toll payment gateways. In Network Optimization in Intelligent Internet of Things Applications. 2024: 37-57. https://doi.org/10.1201/9781003405535-4.

[9] Bijalwan J G, Singh J, Ravi V, et al. Navigating the future of secure and efficient intelligent transportation systems using ai and blockchain. The

Open Transportation Journal, 2024, 18, e26671212291400. http://dx.doi.org/10.2174/0126671212291400240315084722.

[10] Vaigandla K K, Karne R K, Siluveru M, et al. Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications. Mesopotamian Journal of CyberSecurity, 2023, 2023: 73-84. https://doi.org/10.55041/IJSREM34536.

[11] Tripathi G, Ahad M A, Casalino G. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Decision Analytics Journal, 2023: 100344. https://doi.org/10.1016/j.dajour.2023.100344.

[12] Didouh A, Lopez A B, El Hillali Y, et al. Eve, you shall not get access! A cyber-physical blockchain architecture for electronic toll collection security. 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), 2020: 1-7. https://doi.org/10.1109/ITSC45102.2020.9294334.

[13] Huang S, Yang L, Yang X, et al. A decentralized ETC architecture based on blockchain technology. Journal of Advanced Transportation, 2021, 2021(1): 8848697. https://doi.org/10.1155/2021/8848697.

[14] Das D, Banerjee S, Biswas U. Design of a secure blockchain-based toll-tax collection system. International Conference on Micro-Electronics and Telecommunication Engineering. Singapore: Springer Nature Singapore, 2021: 183-191. https://doi.org/10.1155/2021/8848697.

[15] Krishna A M, Tyagi A K. Intrusion detection in intelligent transportation system and its applications using blockchain technology. 2020 international conference on emerging trends in information technology and engineering (IC-ETITE), 2020: 1-8. https://doi.org/10.1109/ic-ETITE47903.2020.332.

[16] Gams M, Kolenik T. Relations between electronics, artificial intelligence and information society through information society rules. Electronics, 2021, 10(4): 514. https://doi.org/10.3390/electronics10040514.