International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 8, Number 2, Year 2026
DOI: https://doi.org/10.62051/ijcsit.v8n2.09
Journal homepage: https://wepub.org/index.php/IJCSIT/index

A Blockchain-Based Identity Collaboration Model for Cross-Airport Employee One-Card Systems

Hao Tu [1, 2], Tie Cao [1, 2], Jinhong Wei [1, 2]

[1] The Second Research Institute of CAAC, Chengdu, China
[2] Civil Aviation Electronic Technology Co., Ltd, Chengdu, China

ABSTRACT

With the deepening of civil aviation group operations, the collaborative management of employee identity and permissions across member airports faces challenges such as data silos, cumbersome mutual recognition processes, and high trust costs associated with centralized systems. This paper proposes a collaborative model for civil aviation employee one-card systems based on Blockchain and Decentralized Identifiers (DIDs). This model stores core employee identity markers, permission attributes, and key behavioral records on the chain, establishing a unified, cross-airport trustworthy digital identity system characterized by "One Card, One Chain, One Identity." By designing a permission synchronization and verification mechanism based on smart contracts, it enables rapid identity verification and compliant access for employees at any airport within the group. The paper focuses on a cross-chain relay scheme to address secure and trustworthy data interaction between different airport chains. The model constructed herein provides an innovative technical framework and implementation pathway for large civil aviation groups to achieve efficient, secure, and auditable cross-domain identity collaboration management.

KEYWORDS

Blockchain; Smart Contract; Group-based Control

1. INTRODUCTION

In the context of the group-oriented and networked development of civil aviation, large aviation groups typically operate multiple airports distributed across different regions. To achieve refined operations and security management, these groups equip all employees with a unified "Employee One-Card" integrating functions such as identity recognition, access control, and logistical services. However, current systems often adopt a model of independent construction by each airport coupled with centralized control, presenting significant pain points: Firstly, data silos are prominent, making it difficult for group headquarters to obtain a real-time, trustworthy overview of permission data across all airports. Secondly, cross-airport business collaboration is inefficient. When employees need to work across airports on official duties, identity mutual recognition requires lengthy application, approval, and data synchronization processes, resulting in poor user experience and high management costs. Finally, centralized systems concentrate trust and risk. A failure or malicious attack on the primary data center could affect authentication services across the entire network, and records of permission changes are susceptible to internal tampering.

Blockchain technology, with its characteristics of decentralization, tamper-resistance, traceability, and transparent consensus, offers a new approach for building a trustworthy collaborative system across organizations and regions [1]. Its core value lies in establishing a trust infrastructure involving multiple parties without relying on a single central authority [2]. Decentralized Identifiers (DIDs), as

a significant application paradigm of blockchain, empower users to autonomously control their identity markers and related credentials, enabling verifiable claims in different scenarios. This naturally suits the identity mutual recognition needs among multiple legal entities within large groups [3].

Therefore, addressing the requirements for cross-airport employee identity collaboration management in civil aviation groups, this paper proposes a one-card system model based on blockchain DIDs. Without altering the existing physical carriers or front-end card reading facilities of airport one-card systems, this research focuses on the trustworthy sharing and automated execution of backend identity data and permission rules. It designs a blockchain collaborative architecture that supports efficient cross-airport mutual recognition, strengthens unified group control, and ensures data privacy security, thereby enhancing overall operational safety and management efficiency.

2. DESIGN OF THE DID-BASED ONE-CARD IDENTITY COLLABORATION MODEL

2.1. System Architecture Overview

The model adopts a consortium blockchain architecture (e.g., akin to frameworks like Hyperledger Fabric [4]). Participating nodes include: group headquarters nodes (serving as regulatory and root trust anchors) and member airport nodes (acting as credential issuers and verifiers). The system is logically divided into three layers: the Application Layer (individual airport one-card application systems), the Blockchain Service Layer (DID identifier management, smart contracts, cross-chain services), and the Infrastructure Layer (blockchain network, storage). The physical card or mobile virtual card held by an employee is associated with a globally unique DID, serving as the primary index for their digital identity on the chain.

2.2. Construction and Issuance of the DID Identity Model

Upon employee onboarding, their home airport, acting as the issuer, creates a DID identifier for them on the chain. Verifiable Credentials bound to this DID include: hashes of basic identity information (e.g., employee ID, name, unit), job roles, initial access permission zones, etc. Sensitive raw data remains stored in local databases at respective airports; only hashes or zero-knowledge proofs are stored on-chain to ensure privacy. Permission changes (e.g., authorizing new zones, suspending permissions) are updated via transactions to the state record corresponding to the DID or by issuing new permission credentials by the authorizing airport. All operations are immutable after consensus.

2.3. Cross-Airport Authentication Process Based on Smart Contracts

When an employee travels to Airport B, their card swipe action triggers Airport B's system to send a query and verification request to the blockchain network. A series of pre-deployed smart contracts execute automatically:

Identity Validity Verification Contract: Checks if the DID is valid and has not been revoked.

Permission Matching Contract: Verifies, based on Airport B's local security policy (encoded into the contract), whether the permission credentials currently held by the DID meet the requirements for entering the specific area.

Access Record Attestation Contract: Upon successful verification, generates an access record containing timestamp, location, and DID identifier, stored on-chain for audit tracing.

This process achieves collaborative authentication where "data remains stationary, while algorithms circulate." Airport B does not need to synchronize the full employee dataset from Airport A in advance but can make real-time decisions solely through on-chain verifiable credentials.

2.4. Cross-Chain Interaction Scheme Supporting Group-Based Control

To balance the data autonomy needs of individual airports with group-wide oversight, the model introduces a cross-chain relay mechanism. Each airport can maintain a sub-chain (focusing on high-frequency local permission operations), while the group headquarters maintains a main chain (storing core DID identifiers and summaries of key permission events). Through relayers or sidechain technology, trustworthy transfer of assets (i.e., identity states) and messages between sub-chains and the main chain is achieved. The group headquarters can perform compliance monitoring and auditing via the global view on the main chain, while during cross-airport mutual recognition, detailed credential status on the counterparty's sub-chain can be queried via the relay bridge. The architecture of this scheme is shown in Fig. 1.

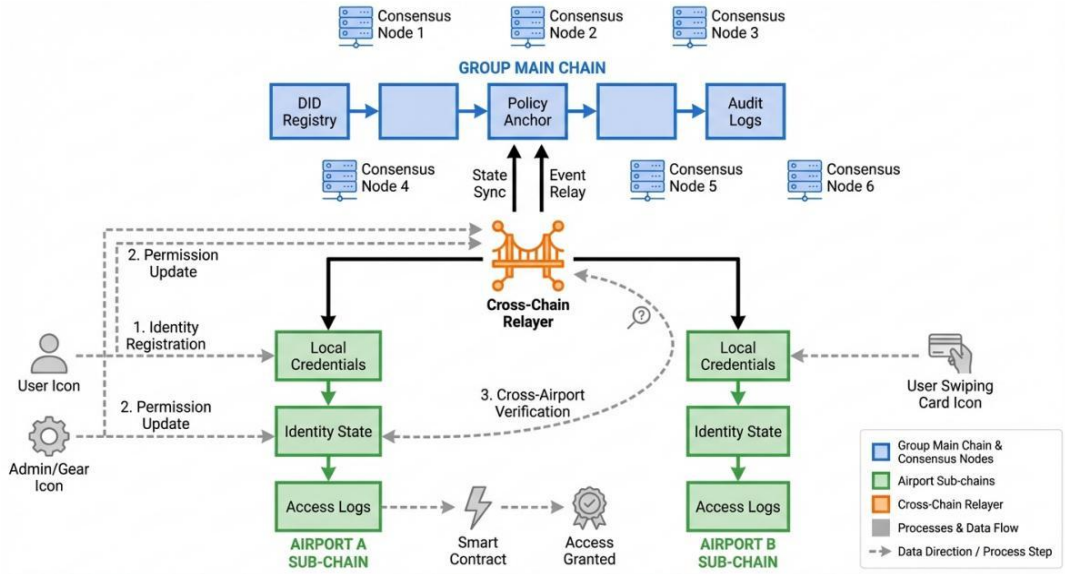

Figure 1. Blockchain Collaborative Architecture Diagram for Civil Aviation One-Card System Based on Cross-Chain Relays

The group main chain and airport sub-chains are connected via relays, illustrating data flows and contract invocation relationships for identity registration, permission updates, and cross-airport verification.

3. ANALYSIS OF KEY MECHANISMS IN THE MODEL

3.1. Data Privacy and Security Controls

The model employs techniques such as on-chain hashing, selective disclosure, and zero-knowledge proofs to ensure trustworthy data sharing while preventing over-exposure of sensitive employee information [5]. Each airport, as the controller of its own data, strictly manages data access permissions through public-private key cryptography.

3.2. Performance and Scalability Considerations

Identity verification transactions are low-frequency but high-security operations; the performance of a consortium blockchain can meet practical needs. By storing high-frequency daily access logs off-chain (e.g., on IPFS or local databases) and only placing hashes of critical events on-chain, on-chain

storage pressure can be significantly reduced. Sub-chain sharding design also facilitates horizontal scalability.

3.3. Comparative Advantages Over Traditional Centralized Models

As shown in Table 1, across four dimensions—trust foundation, cross-domain collaboration efficiency, data auditability, and system robustness—the proposed model demonstrates clear advantages over the traditional centralized mode, particularly in reducing collaboration trust costs and enhancing tamper-resistance.

Table 1. Comparison Between Blockchain Model and Traditional Centralized Model

Comparison Dimension	Traditional Centralized Model	Blockchain DID Collaboration Model
Trust Foundation	Relies on a single central authority	Distributed multi-party consensus
Cross-Airport Collaboration Efficiency	Low (requires manual intervention, data sync delays)	High (automated contract execution, real-time verification)
Data Auditability	Centralized logs, risk of internal tampering	Full-chain traceability, immutable records
System Robustness	Central node failure affects entire network	Multi-node maintenance, high fault tolerance

4. DISCUSSION AND CHALLENGES

Despite its theoretical advantages, the practical implementation of this model in the civil aviation domain still faces several challenges.

First, there are technical integration challenges, such as how to seamlessly interface with existing access control systems, HR systems, and others to achieve a smooth transition. Second, there is a lack of standards and specifications, as the civil aviation industry currently lacks unified standards for blockchain applications and DID data formats. Third, changes in management processes are required, necessitating a redefinition of the boundaries of responsibility and collaborative workflows between the group and individual airports, as well as among airports themselves. Fourth, there are computational and storage costs associated with the additional IT investment needed for operating and maintaining consortium blockchain nodes.

Future work will focus on establishing industry-level application standards, designing lightweight node deployment schemes for hybrid cloud environments, and exploring the integration with technologies such as biometric recognition.

5. CONCLUSION

This paper addresses the business requirement for cross-airport employee identity collaboration management within civil aviation groups by designing a one-card system model based on blockchain and decentralized digital identities. By creating a unified, trustworthy digital identity on the blockchain, utilizing smart contracts to automate cross-airport permission verification rules, and employing cross-chain technology to balance data autonomy with global oversight, the model effectively resolves existing issues such as complex mutual recognition processes, low data credibility, and centralized risk concentration. The research demonstrates that blockchain technology provides a feasible technical pathway for building the next-generation, trustworthy identity collaboration infrastructure for group-based and networked civil aviation operations, contributing to the enhancement of overall aviation safety operational efficiency and intelligent management levels.

Subsequent research will focus on prototype system development and pilot validation to further evaluate its performance and benefits in real-world, complex environments.

CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this paper.

REFERENCES

[1] Zhang, P., Zhou, M., & Fortino, G. Security and trust issues in Fog computing: A survey. Future Generation Computer Systems, 2018, 88: 16-27.

[2] Weiguo Feng, Jianwei Liu, Zongyang Zhang. A Review of the Application of Blockchain Technology in Identity Management. Journal of Computer Research and Development, 2020, 57(10): 2015-2030.

[3] Moubarak, J., Filiol, E., & Chamoun, M. Comparative analysis of blockchain platforms for identity management. In Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP), 2020: 597-606.

[4] Androulaki, E., et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, 2018: 30.

[5] Zyskind, G., Nathan, O., & Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the IEEE Security and Privacy Workshops, 2015: 180-184.