



# A Decentralized Identity and Trust Management Platform Using Blockchain for Cross-Domain Authentication

Sethalat Rodhetbhai<sup>1</sup> and Panjai Tantatsanawong<sup>2</sup>

## ABSTRACT

As digital ecosystems expand, secure and interoperable identity management across organizational boundaries has become increasingly important. This paper presents a blockchain-based platform for decentralized identity and trust management to support cross-domain authentication and authorization among autonomous organizations, such as government agencies and academic institutions. The proposed platform employs a consortium blockchain as a tamper-resistant credential and policy repository, enabling each organization to administer its own credentials while supporting verifiable identity sharing across domains. On-ledger trust relationships and authorization policies allow trusted interactions without relying on centralized identity authorities or pre-established bilateral agreements. A prototype was implemented using Hyperledger Fabric and evaluated in a multi-domain setting. The results demonstrate correct authentication behavior, sub-second authentication latency, measurable transaction throughput, and effective revocation propagation. Additional experiments under multi-domain and concurrent authentication workloads show that the platform preserves consistent authentication outcomes while maintaining latency within practical bounds. The proposed approach can be applied to multi-institutional environments, such as inter-university digital services, cross-agency e-government systems, and collaborative research infrastructures, where secure identity sharing and cross-domain access control are required.

## Article information:

**Keywords:** Blockchain, Consortium Blockchain, Cross-domain Authentication, Authorization, Decentralized Identity, Trust Management, Hyperledger Fabric

## Article history:

Received: February 20, 2026

Revised: March 12, 2026

Accepted: June 12, 2026

Published: July 11, 2026

(Online)

**DOI:** 10.37936/ecti-cit.2026203.266315

## 1. INTRODUCTION

In the era of digital transformation, the ability to securely authenticate users across organizational boundaries has become a critical requirement for public sector agencies, educational institutions, and inter-organizational alliances. As governments and institutions increasingly digitize their services and workflows, the demand for seamless, secure, and interoperable identity management systems continues to grow. Conventional authentication systems, which are generally centralized and limited to specific organizational domains, struggle to meet the requirements of cross-domain access. This inadequacy often results in isolated identity repositories, unnecessary duplication of user accounts, and increased vulner-

ability to data breaches stemming from centralized control points.

Cross-domain authentication enables secure access for users from one organization to services and data in another, eliminating the need for redundant identity setup or predefined mutual agreements. Existing solutions, such as federated identity systems based on protocols like SAML or OAuth [1], [2], offer partial remedies but depend on centralized trust anchors and governance frameworks, which introduce administrative overhead, scalability limitations, and trust bottlenecks [3], [4], [5].

Prior to the emergence of blockchain-based identity systems, several distributed or federated approaches were developed to support cross-domain authentication. Solutions such as Shibboleth [6] and

<sup>1,2</sup>The authors are with the Department of Computing, Faculty of Science, Silpakorn University, Nakhon Pathom, Thailand, Email: rodhetbhai\_s@su.ac.th and tantatsanawong\_p@su.ac.th

<sup>2</sup>Corresponding author: tantatsanawong\_p@su.ac.th

eduGAIN [7] rely on federated identity protocols such as SAML [1], allowing participating institutions to exchange authentication assertions within a federated trust model. Although these systems distribute identity management across domains, they still depend on centralized metadata registries, certificate authorities, and pre-negotiated trust frameworks. These dependencies introduce administrative overhead and limit scalability in dynamic cross-domain environments.

Furthermore, earlier peer-to-peer identity frameworks, including PGP's Web of Trust and SDSI/SPKI, sought to decentralize credential validation without centralized issuers. These models emphasized direct trust relationships and community-based endorsements; however, they lacked distributed consensus mechanisms and verifiable audit trails, making them vulnerable to trust fragmentation, scalability issues, and difficulty in revocation management [5], [8].

Blockchain technology can provide a decentralized foundation for identity and access management (IAM) by serving as a secure and tamper-resistant credential and policy repository, thereby reducing reliance on centralized authentication authorities. Its core characteristics—immutability, decentralization, and cryptographic integrity—can support verifiable identities and access policies without relying on a single controlling authority. By integrating decentralized public key infrastructure (DPKI) with distributed consensus mechanisms, blockchain-based authentication systems can provide a secure and tamper-resistant repository for credentials, trust relationships, and access policies across multiple domains. This approach supports cross-organizational identity verification while maintaining institutional autonomy and minimizing dependence on centralized identity providers. Where applicable, smart contracts can support the enforcement of identity validation rules and the automation of trust relationship management.

In recent years, research efforts have explored various decentralized identity frameworks leveraging blockchain technology, such as uPort, Sovrin, and Microsoft's ION, which aim to empower users with self-sovereign identity (SSI). These approaches emphasize user-centric credential management, verifiable claims, and selective disclosure. However, many of these solutions are primarily designed for individual identity use cases and lack integrated mechanisms for managing inter-organizational trust or facilitating cross-domain interoperability [4], [5], [9], [10], [11].

Recent academic studies have explored blockchain-based identity and trust management in various contexts. Existing studies have reviewed blockchain-based identity management systems and proposed blockchain-enabled identity federation frameworks to address challenges related to scalability, interoperability, privacy, security, and trust management [12],

[13], [14]. These studies demonstrate the potential of blockchain as an infrastructure for identity management; however, the design of dynamic inter-organizational trust governance for cross-domain institutional environments remains an open research challenge.

However, existing academic studies primarily focus on identity management efficiency or system architecture, and limited work has addressed integrated trust management and cross-domain interoperability under a unified decentralized framework. In particular, quantitative evaluations across multiple organizational domains remain insufficiently explored in the literature.

Several blockchain-based authentication models store credentials or access policies directly on-chain and, in some cases, use smart contracts to automate access control. Although these approaches demonstrate the potential of blockchain for identity security, they often do not provide an integrated credential and policy repository or a scalable trust management framework for dynamic multi-organizational environments. Despite these advancements, existing blockchain-based frameworks still present gaps when addressing cross-domain organizational trust at scale. Although Sovrin theoretically supports decentralized identity sharing across different entities through verifiable credentials, its design primarily targets individual-level self-sovereign identity rather than organizational trust management. The platform does not natively provide comprehensive mechanisms for federated trust coordination or scalable cross-domain identity repository management among autonomous organizations [3], [4].

In summary, although pre-blockchain distributed identity systems advanced the decentralization of trust, they lacked the tamper-resistant and transparent infrastructure needed to support broadly verifiable cross-domain identity management. Blockchain technology offers a promising solution by providing immutable ledgers and decentralized consensus, enabling more robust cross-domain identity repositories and federated trust coordination without dependence on centralized intermediaries. Developing a decentralized and interoperable cross-domain authentication platform that supports autonomous credential management and dynamic inter-organizational trust governance remains an open research challenge. This study aims to bridge the gap by designing a platform that leverages blockchain to support decentralized identity and trust management across autonomous organizational domains.

The proposed platform is particularly suitable for environments that require secure cross-domain authentication, authorization, and trust management among autonomous organizations. For example, in a multi-university ecosystem, students from one institution can access digital learning resources hosted

by another institution using their home credentials. Similarly, in e-government systems, citizens authenticated by one agency can securely access services provided by other agencies without re-registration. These use cases highlight the need for dynamic and decentralized trust coordination mechanisms beyond traditional federated identity frameworks.

To address these limitations, this research proposes the design and development of a decentralized identity and trust management platform based on a consortium blockchain. The platform aims to provide a practical, tamper-resistant identity repository and dynamic trust coordination mechanism that enables secure cross-domain authentication among autonomous organizations. The following sections describe the system model, implementation, and evaluation of the proposed platform.

The main contributions of this work are summarized as follows:

- i. A consortium-blockchain-based credential and policy repository that enables cross-domain authentication and authorization among autonomous organizations without requiring pre-established bilateral agreements.
- ii. An on-ledger trust and authorization policy management model that supports dynamic establishment and revocation of inter-organizational trust relationships.
- iii. A prototype implementation on Hyperledger Fabric and scenario-based evaluation, reporting key performance and operational metrics including authentication/authorization latency, transaction throughput, and revocation propagation delay.

## 2. OBJECTIVES

The primary objectives of this research are as follows:

1) To design and develop a blockchain-based decentralized identity and trust management platform that securely stores verifiable credentials in a distributed, tamper-resistant repository and enables interoperable authentication across organizational domains without centralized identity providers.

2) To establish mechanisms for federated trust management that allow participating organizations to create, revoke, and evaluate trust relationships without requiring pre-established bilateral agreements.

3) To provide a service-oriented architecture comprising modular components, such as credential management, authentication, and authorization services, accessible via secure APIs for both internal and cross-domain interactions.

4) To evaluate the feasibility, security, and interoperability of the proposed platform through prototype implementation and scenario-based analysis in multi-organizational environments.

## 3. MATERIALS AND METHODS

The methodology of this research includes the design of the system architecture, implementation of core services, and evaluation of the platform in a simulated cross-domain environment. The following subsections detail each component, starting with the proposed system model.

### 3.1 System Model Architecture

The proposed system architecture centers on a distributed entity credential repository built on a consortium (permissioned) blockchain network, where participating organizations jointly govern network operations and trust management. This infrastructure supports decentralized credential and trust management for cross-domain authentication and authorization. The permissioned blockchain serves as a secure and tamper-resistant repository, facilitating trusted interactions among participating organizations—even in the absence of full mutual trust.

In this model, multiple organizations collaborate to form a consortium-based trust network. The consortium establishes a shared set of policies to govern cross-domain access permissions, allowing trusted entities (e.g., users or devices) from one organization to access services and resources—such as applications, databases, storage systems, and APIs—offered by other participating members.

Each organization operates and maintains its own peer nodes within the blockchain network. Applications developed by a specific organization can interact not only with their own peer nodes but also with those operated by other member organizations in the network.

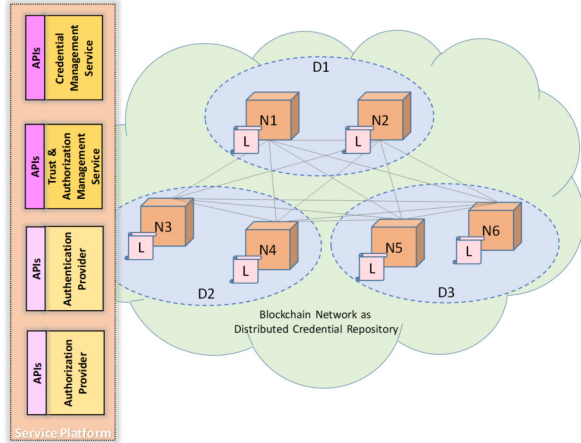
Each organizational domain's administrators retain exclusive control over the identity credentials of entities within their domain. Meanwhile, all immutable transaction records are disseminated and securely stored across the blockchain peer nodes that constitute the credential repository. These credentials, once recorded on the blockchain ledger, can be verified for authenticity by any member organization within the consortium.

As illustrated in Figure 1, the system service platform is composed of four core components:

- **Credential Management Service (CMS):** Responsible for issuing, updating, querying, and revoking entity credentials within organizational domains. The platform securely records all credential operations in the blockchain repository.
- **Trust and Authorization Management Service (TAMS):** Manages the creation, revocation, and evaluation of trust relationships and authorization policies between organizations, facilitating cross-domain resource sharing.
- **Authentication Provider (AEP):** Verifies the authenticity of entity credentials stored on

the blockchain and issues authentication responses (such as verified profiles or certificates) to requesting clients.

- **Authorization Provider (AOP):** Provides detailed authorization attributes or access control information based on authenticated entity profiles, assisting resource providers in enforcing fine-grained access policies.

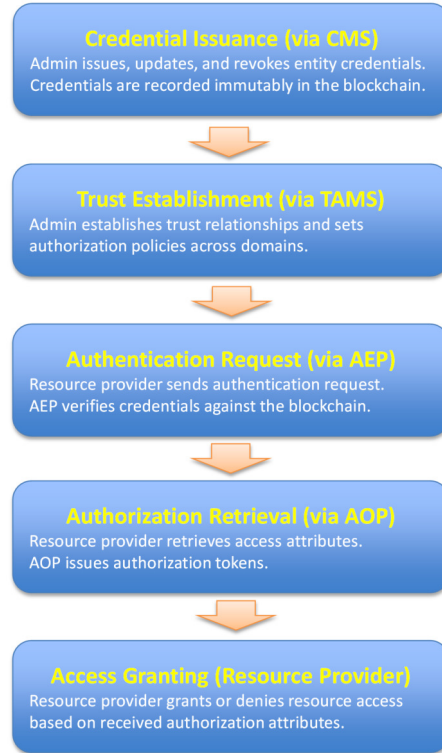


**Fig.1:** System Model Architecture.

To illustrate the interaction among core components, Figure 2 presents a high-level workflow of the platform operation. The system workflow proceeds through the following steps:

1. **Credential Issuance:** Domain administrators use the CMS to create, update, or revoke credentials for entity members within their organizational domain. The blockchain ledger securely records all credential transactions.
2. **Trust Establishment:** Administrators define inter-organizational trust relationships and authorization policies using the TAMS, enabling trusted cross-domain access.
3. **Authentication Request:** When an entity attempts to access a cross-domain resource, the resource provider queries the AEP to verify the validity and status of the entity's credentials against the blockchain repository.
4. **Authorization Retrieval:** Upon successful authentication, the resource provider requests additional authorization attributes from the AOP to determine the specific access rights for the entity.
5. **Access Granting:** Based on the authorization attributes and policies, the resource provider grants or denies access to the requested resources.

This workflow supports secure and decentralized cross-domain authentication and authorization while reducing reliance on centralized identity and trust intermediaries.



**Fig.2:** High-Level Workflow of the Decentralized Identity and Trust Management Platform.

The following subsections describe each core component of the platform in detail, corresponding to the stages outlined in the high-level workflow.

### 3.1.1 Credential Management Service (CMS)

This component provides administrative APIs through which domain administrators can manage entity credentials within their organizational domains. Client applications can submit requests to create, query, update, or revoke credentials. The blockchain-based repository immutably records all credential operations.

The administrative APIs are designed as secure RESTful services operating over HTTPS, utilizing digital signatures to ensure the integrity and authenticity of credential management transactions.

**Input:** Credential issuance, update, query, and revocation requests submitted by domain administrators.

**Output:** Immutable blockchain transaction records reflecting credential status changes.

### 3.1.2 Trust and Authorization Management Service (TAMS)

This component empowers domain administrators to establish and manage trust relationships with other organizational domains. It allows administrators to register or revoke inter-organizational trust dynamically and to define authorization policies

that govern cross-domain access to domain-owned resources.

Trust establishment and policy configuration operations are facilitated through secure RESTful APIs, allowing dynamic updates to trust relationships without manual coordination.

**Input:** Trust establishment, revocation requests, and authorization policy management.

**Output:** Updated trust relationships and authorization policies stored on the blockchain ledger.

### 3.1.3 Authentication Provider (AEP)

This component is responsible for verifying the credentials of entity members using the distributed blockchain repository. It exposes a set of APIs for resource providers, acting as clients, to request authentication services. Upon successful verification, the AEP issues an authentication assertion or verified entity profile, which the client application subsequently presents to the AOP to request an access token.

The authentication service APIs return verified authentication assertions in the form of JSON Web Tokens (JWTs) or Verifiable Presentations, enabling interoperability across domains [10], [15].

**Input:** Authentication requests containing entity credentials submitted by resource providers.

**Output:** Authentication assertions or verified entity profiles for use in authorization processes.

### 3.1.4 Authorization Provider (AOP)

This component serves as an interface for resource providers to request additional authorization details of an authenticated entity, based on its authentication assertion or verified profile. The AOP accepts authentication assertions from client applications, validates them, and issues access tokens containing authorization attributes and access control information.

The platform handles authorization queries and access token issuance through secure RESTful APIs. The AOP issues access tokens using standardized formats, such as JWTs, which include authorization claims and validity periods [15].

The retrieved information enables resource providers to determine the appropriate level of access granted to the entity.

**Input:** Authorization queries based on authenticated entity profiles or access tokens.

**Output:** Authorization attributes and access control decisions provided to the requesting resource providers.

### 3.1.5 Trust Model

The proposed platform adopts a consortium-based trust model in which participating organizations establish trust relationships through on-ledger policy definitions rather than relying on centralized trust authorities or pre-established bilateral agreements.

In this model, each organization acts as an independent trust domain, maintaining full control over its own identity credentials while participating in a shared blockchain network. Trust relationships between domains are dynamically established, updated, and revoked through the Trust and Authorization Management Service (TAMS), with all trust-related operations immutably recorded on the blockchain ledger.

Unlike traditional federated identity systems that rely on centralized metadata registries or static trust configurations, the proposed trust model supports decentralized and policy-driven management of inter-organizational trust relationships. The platform evaluates trust decisions at runtime using blockchain-stored policies, thereby supporting flexible cross-domain authentication and authorization while reducing manual coordination among participating organizations.

This approach ensures that trust relationships remain transparent, auditable, and dynamically adaptable to changing organizational requirements, making it suitable for multi-organizational environments with evolving trust conditions. During authentication, the AEP enforces trust decisions by validating applicable policies against trust relationships stored on the blockchain. This trust decision process can be formally modeled as a policy evaluation function  $T(D_i, D_j, C) \rightarrow \{0, 1\}$ , where  $D_i$  and  $D_j$  denote the source and target domains, respectively, and  $C$  represents the validity of the presented credential. The function returns 1 if the trust relationship and policy conditions are satisfied, and 0 otherwise.

## 3.2 Implementation Approach

The proposed decentralized identity and trust management platform was implemented as a prototype system deployed on a consortium blockchain network. The following subsections outline the key elements of the implementation approach and the subsequent testing methodology.

### 3.2.1 Prototype System Design

The prototype system uses Hyperledger Fabric, a permissioned blockchain framework under the Hyperledger project. Hyperledger Fabric is designed specifically for consortium (permissioned) blockchain environments and supports smart contracts, known as “chaincode,” to automate network operations [16], [17].

In the prototype, each participating organizational domain operates its own peer node(s), installed and configured within Docker container environments. The distributed ledger functions as a credential repository, securely recording credential transactions and trust relationships among participating organizations.

The system components—Credential Management Service (CMS), Trust and Authorization Management Service (TAMS), Authentication Provider (AEP), and Authorization Provider (AOP)—have been developed. Each component exposes secure RESTful APIs to facilitate interactions among organizational domains and client applications.

The prototype system incorporates several supporting applications to facilitate its operation. The Entity Management Application enables domain administrators to manage entities within their organizational domains. This tool offers a graphical user interface (GUI) that interacts with the blockchain credential repository through the CMS's RESTful APIs.

Another essential tool enables domain administrators to manage trust relationships across organizational domains and to control access permissions for external entity members. This trust management application interfaces directly with the TAMS component.

Additionally, the prototype system includes a User-End Application to demonstrate its cross-domain authentication capability. This application allows users to present their personal credentials for verification through the AEP's RESTful APIs. After successful verification, users can obtain an access certificate or access token and use it to request access from resource providers.

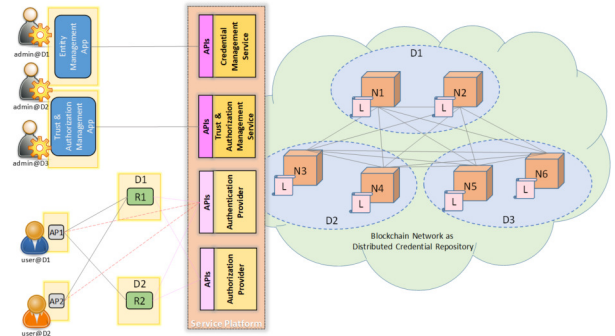
The overall implementation architecture of the testbed prototype, including the deployment of CMS, TAMS, AEP, and AOP services over a Hyperledger Fabric network, is illustrated in Figure 3 [16].

The architecture consists of the Service Platform, supporting applications, and a distributed blockchain network.

- Domain administrators use the Entity Management App and Trust and Authorization Management App to interact with the Credential Management Service (CMS) and Trust and Authorization Management Service (TAMS), respectively, through secure RESTful APIs.
- End users utilize user-end applications (AP1, AP2) to authenticate via the Authentication Provider (AEP) and obtain access authorization via the Authorization Provider (AOP).
- The backend blockchain network is composed of peer nodes (N1–N6) organized into organizational domains (D1–D3), with each node maintaining a replicated ledger (L) that acts as a distributed credential repository.

### 3.3 Experimental Assumptions and Network Model

To ensure reproducibility, this study defines the experimental setup as a consortium network consisting of multiple organizational domains connected through a local network infrastructure. Each organizational domain uses one blockchain peer node de-



**Fig.3:** Overall architecture of the prototype system.

ployed within a virtualized environment.

Network communication delay is assumed to follow a stable local network latency model with negligible packet loss. Within Hyperledger Fabric, transaction execution, endorsement, and validation processes primarily contribute to processing delays.

The workload design included two modes: sequential authentication requests for baseline evaluation and concurrent authentication requests for extended multi-domain scenarios. The experimental design included 1,000 requests per run, with each experiment repeated five times. The system operates in a controlled local environment with minimal external network interference, allowing the evaluation to isolate the performance characteristics of the proposed architecture.

## 4. EXPERIMENT AND RESULTS

### 4.1 System Environment Setup

The testing environment consisted of:

- A minimum of three simulated organizational domains, each with its dedicated blockchain peer node.
- RESTful API servers representing the CMS, AEP, and AOP services.
- A client application simulating entity members and resource providers requesting cross-domain authentication and access.
- Blockchain network configuration parameters, including endorsement policies and access control rules.

The prototype uses Hyperledger Fabric v2.2.15 as the underlying permissioned blockchain framework. The network employed a Raft-based ordering service with 3 orderer nodes to provide crash fault tolerance. Each organization operated one peer node with both endorsing and committing roles within a single consortium. The network used one application channel shared by all member organizations [16].

For transaction validation, the endorsement policy was configured as “majority-of-N” (e.g., 2-of-3 organizations in a 3-domain setup) for credential issuance, credential revocation, and trust-policy update trans-

actions. Read-only queries do not require endorsement under this configuration. The network configuration used a block size of 50 transactions and a batch timeout of 1s. These parameters were held constant throughout the experiments to isolate baseline performance and avoid confounding effects from batching and ordering configurations. The peer state database used CouchDB to support rich queries. The deployment used TLS for all service endpoints and Fabric components. The chaincode was deployed as an external service and invoked via the Fabric Gateway SDK.

## 4.2 Testing Scenarios

The evaluation design mapped each testing scenario to one or more evaluation metrics to assess the platform's reliability, efficiency, and operational feasibility.

The experimental assessment examined the prototype through several key scenarios:

- **Cross-Domain Authentication:** Verifying whether an entity from one organization can successfully authenticate and obtain an authentication assertion accepted by another organization's resource provider.

- **Access Token Issuance and Enforcement:** Validating that authenticated entities receive access tokens with appropriate permissions, and that resource providers enforce access control based on token attributes.

- **Dynamic Trust Management:** Testing the registration and revocation of trust relationships between organizations and observing the impact on authentication and authorization outcomes.

- **Credential Revocation Handling:** Verifying that the system propagates credential revocations correctly and denies authentication attempts using revoked credentials.

## 4.3 Evaluation Metrics

To assess the performance and reliability of the platform, the evaluation measured the following metrics:

- **Success Rate of Authentication Requests:** The percentage of authentication requests that are successfully verified and completed, indicating the reliability of the authentication process across domains.

- **Authentication and Authorization Latency:** The time taken to complete an authentication request and receive an authentication assertion, as well as the time taken to request and receive an access token after successful authentication. Latency was measured end-to-end at the client from request transmission to response receipt, including network RTT over HTTPS.

- **Transaction Throughput:** The number of credential management and trust operations processed per second.

- **Revocation Propagation Delay:** The time taken for credential revocation updates to propagate across the blockchain network.

The results of these tests provided insights into the feasibility, operational performance, and security of the proposed platform for real-world cross-domain authentication and trust management scenarios.

The insights gathered from the testing phase will be analyzed and discussed in the subsequent section to evaluate the prototype's effectiveness in supporting decentralized cross-domain authentication.

## 4.4 Results

### 4.4.1 Cross-Domain Authentication

The cross-domain authentication test used 1,000 authentication requests per run, with requests originating from a resource provider in domain D2 and targeting entity credentials managed by domain D1. For each experiment, the evaluation used five repeated runs and reports the mean, median, and tail latency (p95/p99). The success rate calculation considered only valid credential presentations.

Table 1 summarizes the success rate under key authentication scenarios. The results show that the authentication logic achieves a 100% success rate for valid credentials and a 0% acceptance rate for revoked credentials, revoked trust relationships, and untrusted issuer domains, demonstrating its correctness and robustness. These results further support the trust decision model defined in Section 3.1.5, in which policy-driven trust evaluation across domains determines authentication outcomes.

Beyond the single-direction scenario ( $D2 \rightarrow D1$ ), the evaluation included extended experiments to represent decentralized environments with more realistic multi-domain interactions. Authentication requests were generated across multiple domains, including  $D1 \rightarrow D2$ ,  $D2 \rightarrow D3$ , and  $D3 \rightarrow D1$ , to evaluate system behavior under multi-directional interactions.

Furthermore, the extended experiments included concurrent authentication requests from multiple domains to simulate simultaneous access patterns in a decentralized system. These experiments assess the platform's ability to handle parallel authentication requests without centralized coordination.

Table 2 presents the results of the extended multi-domain and concurrent authentication scenarios. The system maintains consistent authentication success rates across different domain interaction patterns, indicating that the proposed platform correctly supports decentralized cross-domain authentication.

**Table 1:** Success rate under key scenarios.

| Scenario                                           | Requests         | Success rate | Expected outcome                  |
|----------------------------------------------------|------------------|--------------|-----------------------------------|
| S1: Cross-domain authentication (valid credential) | $5 \times 1,000$ | 100.0%       | Authenticated assertion issued    |
| S2: Credential revoked                             | $5 \times 1,000$ | 0.0%         | Rejected due to revocation status |
| S3: Trust relationship revoked                     | $5 \times 1,000$ | 0.0%         | Rejected due to trust policy      |
| S4: Untrusted issuer domain                        | $5 \times 1,000$ | 0.0%         | Rejected by issuer validation     |

**Table 2:** Multi-domain and concurrent authentication results.

| Scenario               | Requests                    | Success rate | Note                      |
|------------------------|-----------------------------|--------------|---------------------------|
| D1 $\rightarrow$ D2    | $5 \times 1,000$            | 100.0%       | Valid credentials         |
| D2 $\rightarrow$ D3    | $5 \times 1,000$            | 100.0%       | Cross-domain verification |
| D3 $\rightarrow$ D1    | $5 \times 1,000$            | 100.0%       | Multi-directional test    |
| Concurrent (3 domains) | $3 \times (5 \times 1,000)$ | 100.0%       | Parallel requests         |

#### 4.4.2 Latency Results (Authentication and Authorization)

authentication latency includes: (i) REST request processing at AEP, (ii) ledger query and policy validation, and (iii) JWT assertion generation. Authorization latency (AOP) represents the additional time required to issue a token after receiving a valid authentication assertion [15], [16].

**Table 3:** Latency statistics (ms) for 3-domain consortium.

| Operation                       | Mean | Median | p95 | p99 | Std. Dev. |
|---------------------------------|------|--------|-----|-----|-----------|
| Authentication (AEP)            | 235  | 210    | 390 | 520 | 62        |
| Authorization token (AOP)       | 105  | 95     | 170 | 220 | 28        |
| Credential query (CMS read)     | 82   | 75     | 130 | 160 | 19        |
| Credential issuance (CMS write) | 410  | 380    | 690 | 820 | 95        |
| Trust update (TAMS write)       | 460  | 430    | 760 | 910 | 110       |

#### 4.4.3 Extended Latency Analysis (Multi-domain and Concurrent Scenarios)

To further evaluate the performance of the proposed platform under realistic decentralized conditions, extended latency experiments were conducted based on the multi-domain and concurrent authentication scenarios described in Section 4.4.1.

The evaluation measured authentication latency

across multiple domain interactions, including D1  $\rightarrow$  D2, D2  $\rightarrow$  D3, and D3  $\rightarrow$  D1. It also considered concurrent request conditions involving simultaneous authentication requests from multiple domains.

The results in Table 4 show that the average authentication latency increases moderately under concurrent workloads due to additional ledger-query, policy-validation, and network communication overhead. However, the latency remains within acceptable bounds for interactive applications.

These findings indicate that the proposed platform maintains acceptable latency characteristics while supporting decentralized and parallel authentication processes.

**Table 4:** Extended latency statistics (ms) under multi-domain and concurrent authentication scenarios.

| Scenario               | Mean | Median | p95 | Std. Dev. | Note              |
|------------------------|------|--------|-----|-----------|-------------------|
| D1 $\rightarrow$ D2    | 238  | 214    | 398 | 65        | Multi-domain      |
| D2 $\rightarrow$ D3    | 242  | 218    | 405 | 68        | Cross-domain      |
| D3 $\rightarrow$ D1    | 247  | 221    | 415 | 70        | Multi-direction   |
| Concurrent (3 domains) | 285  | 260    | 485 | 92        | Parallel requests |

#### 4.4.4 Transaction Throughput

The write-path evaluation used a mixed transaction workload consisting of credential issuance, credential revocation, and trust updates. Throughput refers to the number of committed transactions per second (tx/s) at the peer ledger. Table 5 reports throughput for the 3-domain setup, and Figure 4 compares transaction types.

**Table 5:** Throughput (tx/s) by transaction type.

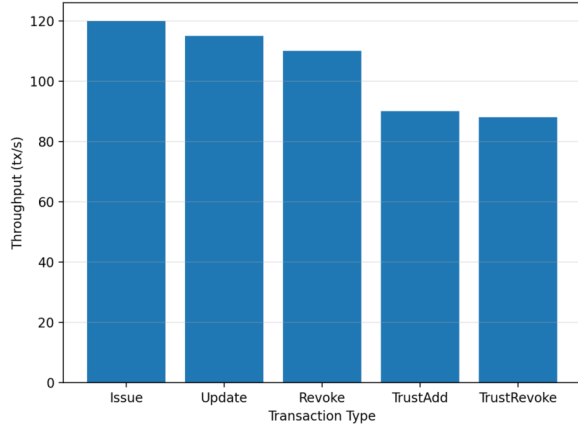
| Transaction type                  | Mean tx/s | p95 tx/s | Notes                         |
|-----------------------------------|-----------|----------|-------------------------------|
| Credential issuance (CMS write)   | 120       | 110      | Includes endorsement + commit |
| Credential revocation (CMS write) | 110       | 102      | Revocation flag update        |
| Trust update (TAMS write)         | 90        | 84       | Policy write path             |

#### 4.4.5 Revocation Propagation Delay

Revocation propagation delay refers to the time interval between submitting a revocation transaction at the CMS and the point at which all peers observe the updated credential status. This metric captures ordering, block creation, and commit latency. Table 6 reports summary statistics, while Figure 5 shows the empirical cumulative distribution function (CDF).

### 4.5 Baseline Comparison

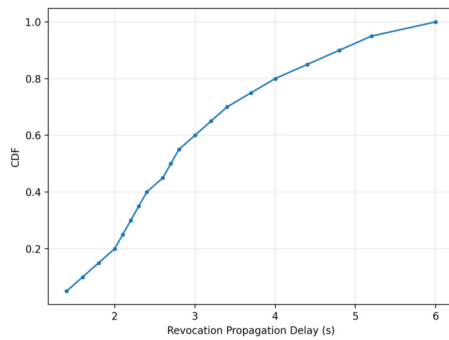
The study evaluated the advantages of the proposed architecture through a baseline comparison



**Fig.4:** Throughput comparison across transaction types.

**Table 6:** Revocation propagation delay (s) in 3-domain consortium.

| Metric    | Mean | Median | p95 | Max |
|-----------|------|--------|-----|-----|
| Delay (s) | 2.7  | 2.4    | 4.8 | 6.1 |



**Fig.5:** CDF of revocation propagation delay.

with representative identity management approaches. Traditional centralized identity systems rely on a single authentication authority, creating a single point of failure and limiting scalability in multi-domain environments. Federated identity systems improve interoperability but depend on static trust relationships and centralized federation governance.

In contrast, the proposed blockchain-based approach enables decentralized trust coordination through consensus-backed state management. In centralized IAM systems, authentication latency is typically below 100 ms, whereas the proposed system introduces additional latency due to consensus and ledger validation processes. However, this overhead enables improved auditability, fault tolerance, and dynamic trust management compared to centralized approaches.

This comparison highlights the trade-offs between centralized efficiency and decentralized governance, demonstrating the suitability of the proposed approach for cross-domain institutional environments. While existing studies have examined blockchain-

based identity management and decentralized identity federation models [12], [13], [14], multi-domain performance evaluation under concurrent authentication scenarios remains limited. The proposed platform addresses this gap by evaluating decentralized cross-domain authentication across multiple organizational domains and parallel request conditions.

Table 7 summarizes the trade-offs among centralized, federated, and blockchain-based identity management approaches. The proposed platform introduces higher processing overhead than centralized authentication, but provides stronger auditability, decentralized governance, and dynamic trust management.

**Table 7:** Baseline comparison of identity management approaches.

| Approach               | Centralized IAM         | Federated identity    | Proposed blockchain-based platform |
|------------------------|-------------------------|-----------------------|------------------------------------|
| Trust model            | Central authority       | Federation governance | Consortium consensus               |
| Dynamic trust update   | No                      | Limited               | Yes                                |
| Auditability           | Limited                 | Moderate              | High                               |
| Latency characteristic | Low                     | Low-Medium            | Medium                             |
| Main limitation        | Single point of failure | Static trust metadata | Consensus overhead                 |

## 4.6 Discussion

The experimental results suggest three practical observations. First, cross-domain authentication can be completed within sub-second latency under the evaluated workload, indicating that the proposed approach is feasible for interactive services. Second, write-path operations (e.g., credential issuance, revocation, and trust-policy updates) incur higher latency than read-path authentication because they require endorsement, ordering, validation, and ledger commit phases, which is consistent with permissioned blockchain transaction semantics. Third, revocation propagation delay is primarily governed by block formation and commit latency; therefore, tuning block parameters (e.g., batch timeout and block size) directly affects the trade-off between operational throughput and revocation responsiveness. Overall, these results indicate that transaction finality and configuration choices, rather than application-layer processing, primarily shape the platform's performance. They also emphasize the need to carefully select blockchain and policy parameters to balance auditability, security responsiveness, and operational efficiency in consortium deployments.

In addition to the baseline evaluation, the extended multi-domain and concurrent authentication scenarios presented in Section 4.4.1 further demonstrate the robustness of the proposed platform in decentralized environments. The results indicate that the system maintains consistent authentication suc-

cess rates and acceptable latency characteristics under multi-directional and parallel request conditions.

These findings highlight the scalability of the proposed architecture in handling dynamic interactions among multiple organizational domains. Unlike traditional centralized or federated identity systems, which rely on predefined trust relationships or centralized coordination, the proposed blockchain-based approach supports dynamic trust establishment and decentralized authentication. The concurrent workload results further indicate that the platform maintains acceptable latency despite the additional consensus and ledger validation overhead.

Although blockchain consensus mechanisms introduce additional processing overhead compared with centralized systems, they improve auditability, fault tolerance, and governance transparency, which are critical for cross-domain institutional environments.

## 5. CONCLUSION

This paper presented a decentralized identity and trust management platform that enables cross-domain authentication and authorization among autonomous organizations by leveraging a permissioned (consortium) blockchain as a tamper-resistant credential and policy repository. Each organization retains administrative autonomy over its own members by issuing, updating, querying, and revoking credentials through the Credential Management Service (CMS). At the same time, the shared ledger immutably records all credential lifecycle events to support auditability and traceability. Inter-organizational trust relationships and authorization policies are established and revoked dynamically via the Trust and Authorization Management Service (TAMS), allowing cross-domain access without requiring pre-established bilateral agreements.

For runtime access, the Authentication Provider (AEP) verifies presented credentials against the distributed repository and issues an authentication assertion (e.g., JWT or verifiable presentation). The Authorization Provider (AOP) subsequently issues access tokens embedding authorization attributes and validity constraints, enabling resource providers to enforce fine-grained access decisions in a standardized and interoperable manner. A prototype implementation on Hyperledger Fabric demonstrates the feasibility of exposing these capabilities through secure RESTful APIs and operating the ledger across multiple organizational domains.

The proposed approach offers several advantages: (i) reduced dependence on centralized identity providers and single points of failure, (ii) improved auditability and accountability through immutable records of credential and trust-policy changes, (iii) preservation of organizational autonomy while enabling interoperable cross-domain access, and (iv) responsive security control through revocation and

trust-policy updates that the platform enforces consistently across the consortium. Nevertheless, the platform also entails trade-offs. Consortium deployment introduces governance and operational overhead (e.g., membership management, policy coordination, and key management), and blockchain replication and endorsement/commit processing may impose performance costs compared to purely centralized repositories, particularly for write-path operations.

The platform can support multi-institution digital services that require cross-domain authentication and authorization while preserving organizational autonomy. A representative use case is a consortium-based MOOC ecosystem, where learners enrolled at different universities authenticate using their home institution's credentials and subsequently access courses hosted by a central MOOC platform or partner universities under consistent trust and access policies. Similar deployment patterns can support inter-university digital libraries, research services, shared academic resources, and cross-agency e-government services that require secure identity verification and access control across administrative boundaries.

Future work will focus on strengthening privacy protection (e.g., minimizing on-chain metadata and reducing linkability), extending policy expressiveness for complex access-control models, and conducting broader evaluations across diverse workloads and operational conditions to assess the platform's scalability and robustness.

## ACKNOWLEDGEMENT

This research was partially supported by the Department of Computing, Faculty of Science, Silpakorn University, Nakhon Pathom, Thailand.

## AUTHOR CONTRIBUTIONS

Conceptualization, Sethalat Rodhetbhai and Panjai Tantatsanawong; analysis, Sethalat Rodhetbhai; methodology, Sethalat Rodhetbhai; software, Sethalat Rodhetbhai; writing—original draft preparation, Sethalat Rodhetbhai and Panjai Tantatsanawong; writing—review and editing, Sethalat Rodhetbhai and Panjai Tantatsanawong; supervision, Panjai Tantatsanawong. All authors have read and agreed to the published version of the manuscript.

## References

- [1] OASIS, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," Mar. 2005. [Online]. Available: <https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [2] D. Hardt, Ed., "The OAuth 2.0 Authorization Framework," Internet Engineering Task

- Force (IETF), RFC 6749, Oct. 2012. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6749>
- [3] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista and M. Conti, “A Survey on Decentralized Identifiers and Verifiable Credentials,” in *IEEE Communications Surveys & Tutorials*, vol. 27, no. 6, pp. 3641–3671, Dec. 2025.
- [4] R. N. Zaeem *et al.*, “Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study,” in *Proceedings WI-IAT '21: IEEE/WIC/ACM International Conference on Web Intelligence*, , pp. 583–590, Dec. 2021.
- [5] Z. Yan, X. Zhao, Y. Liu and X. Luo, “Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda,” *Information & Management*, vol. 61, no. 7, p. 104026, Nov. 2024.
- [6] Shibboleth Consortium, “Shibboleth Identity Provider v5 Release Notes,” Jul. 2025. [Online]. Available: <https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199500367/ReleaseNotes>
- [7] GÉANT eduGAIN, “eduGAIN Policy Framework Constitution (Version 4.0),” Nov. 2023. [Online]. Available: <https://edugain.org/wp-content/uploads/2023/11/eduGAIN-Constitution-v4-final.pdf>
- [8] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, “OpenPGP Message Format,” Internet Engineering Task Force (IETF), RFC 4880, Nov. 2007. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc4880>
- [9] W3C Decentralized Identifier Working Group, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, Jul. 2022. [Online]. Available: <https://www.w3.org/TR/did-core/>
- [10] W3C Verifiable Credentials Working Group, “Verifiable Credentials Data Model v1.1,” W3C Recommendation, Mar. 2022. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>
- [11] Decentralized Identity Foundation, “ION: Identity Overlay Network (DID Method),” Jun. 2025. [Online]. Available: <https://identity.foundation/ion/>
- [12] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan and K.-K. R. Choo, “Blockchain-based identity management systems: A review,” *Journal of Network and Computer Applications*, vol. 166, p. 102731, 2020.
- [13] M. K. B. Shuhan, S. M. Hasnayeem, T. K. Das, M. N. Sakib and M. S. Ferdous, “Decentralised identity federations using blockchain,” *International Journal of Information Security*, vol. 23, pp. 2759–2782, 2024.
- [14] S. El Haddouti, A. Ouaguid and M. D. E.-C. El Kettani, “Fedidchain: An innovative blockchain-enabled framework for cross-border interoperability and trust management in identity federation systems,” *Journal of Network and Systems Management*, vol. 31, no. 2, p. 42, 2023.
- [15] M. Jones, J. Bradley, and N. Sakimura, “JSON Web Token (JWT),” Internet Engineering Task Force (IETF), RFC 7519, May 2015. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc7519>
- [16] Hyperledger Fabric Project, “Hyperledger Fabric Documentation,” Jul. 2025. [Online]. Available: <https://hlf.readthedocs.io/en/latest/>
- [17] Hyperledger Fabric Project, “hyperledger/fabric: Releases,” GitHub, Aug. 2025. [Online]. Available: <https://github.com/hyperledger/fabric/releases>



**Sethalat Rodhetbhai** is a Lecturer in the Department of Computing, Faculty of Science, Silpakorn University (SU), Thailand. He received his academic training in computer science and computer engineering and has been actively involved in teaching, research, and academic services. His research interests include computer networks, computer security, distributed systems, ubiquitous computing, and mobile computing.



**Panjai Tantatsanawong** is an Associate Professor in the Department of Computing, Faculty of Science, Silpakorn University (SU), Thailand. He received Doctor of Technology in Computer Science, Asian Institute of Technology (AIT), Thailand. He received Master of Science in Computer Science, Chulalongkorn University (CU), Thailand and Bachelor of Science, Mahidol university, Thailand. His research interests are data and information processing, internet of things, computer network and artificial intelligent.