World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Decentralized identity for secure network access: A blockchain-based approach to user-centric authentication

Oluwatosin Oladayo ARAMIDE *

Department Network Development Engineer, Amazon, Ireland.

World Journal of Advanced Research and Reviews, 2019, 03(03), 143-155

Publication history: Received on 14 September 2019; Revised 24 october 2019; accepted on 29 october 2019

Article DOI: https://doi.org/10.30574/wjarr.2019.3.3.0147

Abstract

The well-known network access systems are highly centralized user-based on solutions which expose their vulnerabilities to face in the line of privacy, identity theft, and single point of failure. Decentralized Identity (DID) has been proposed as one of the transformational frameworks that allows individuals to own, control and manage their digital identities on the basis of a blockchain and verifiable credentials. The current paper will discuss how DIDs are transforming network access by moving away from centralized network authentication models to self-sovereign identity systems. We present a conceptual model, a reference architecture, and show how DID-enabled authentication may be used to enable secure, privacy-respecting user-centric access to networked resources. We discuss the examples of use cases such as enterprise Wi-Fi access, onboarding of IoT devices, and federated systems of logins outlining the new possibilities that enhance the autonomy, trust, and resilience of users. Besides, we consider the difficulties of implementing DID-based systems on actual network conditions considering interoperability, governance and draft regulations requirements such as GDPR. We see as relevant in practice the integration of DID in network access protocols, which provides a promising alternative to traditional models in decentralized, mobile, and trust-sensitive applications.

Keywords: Decentralized Identity (DID); Self-Sovereign Identity (SSI); Verifiable Credentials; Blockchain; Network Access; Identity Management

1. Introduction

Given the mounting growth in the digital environment, the striving of secure scalable user-driven identity management systems has become a major issue. Access to networks, either to corporate resources, wireless networks or digital services, is currently based on centralized identity providers (IdPs), exemplified by corporate directories, social logins (e.g. Google, Facebook), and Certificate authorities. Although these centralized models are quite popular, they pose a great number of vulnerabilities: they form isolated points of failure, restrict users in handling their own information, and can be attacked through data breaches and identity theft. Large-scale events like the 2017 Equifax data breach or the repetitive data leakages that Facebook has experienced have shown how problematic it is to use centralized identity stores to authorize and govern access.

Decentralized Identity (DID) systems appear as a new paradigm that counters these challenges in the identity and access management (IAM). DIDs are based on the framework of self-sovereign identity (SSI) distributed ledger technologies (DLTs) or blockchain-based, which suggests that both individuals and organizations can create and manage their identifiers without relying on central authority. The model allows the user to have verifiable privacy-preserving credentials, which can be used as part of authentication in any application without any underlying personal information

* Corresponding author: Oluwatosin Oladayo ARAMIDE

being revealed or requiring third-party trust brokers. DIDs will introduce more security and equity into the digital world by democratizing online trust by changing the institutions in control of identity to the individual user.

As of 2019, the W3C Decentralized Identifier Working Group has been working out standards and frameworks of DIDs, with an emphasis on interoperability, cryptographic verifiability, and on supporting a diversity of approaches to DIDs. Emerging DID systems uPort, Sovrin, and Veres One to develop a fully functioning DID system and test them in the real world (in healthcare, education, and finance, respectively). Nevertheless, DIDs used in network access control as one of the underlying levels of digital interaction are under-utilized.

The aim of this paper is to look into the use of DIDs in the case of network access, such as enterprise wireless upon authentication, IoT device provisioning, and decentralized VPN access or firewall access. We hypothesize that the authentication of these systems with DID could decrease the reliance on the centralized infrastructure, better privacy, and resilience against identificational spoofing attacks, credential theft, as well as insider threats.

This study has three-fold objectives

- To analyse the security and privacy related limitations of traditional models of network access
- To examine the basis of the architectures and the flow of action of the DID-based access systems with blockchain and the verifiable credentials
- To suggest and test an idea of the conceptual model of decentralized identity applied on practical use cases accessing the network.

We hope thereby to add to the growing literature on decentralized digital IDs and provide practitioners with a useful guide on how technologists, policymakers, and organizations involved in user-centric identity systems can take action. As of 2019, the decentralized-identity landscape remains mere formative, though the maturity of DLTs and changes in the regulatory landscape towards data sovereignty (e.g. the EU General Data Protection Regulation - GDPR) offers an attractive context in which to consider the use of DIDs as access control mechanisms.

2. Background and Theoretical Framework

2.1. Identity Management in Networked Environments

Identity management (IdM) is a foundational component of secure network access. It governs the identification, authentication, and authorization of users accessing digital systems. Traditionally, identity has been managed through centralized architectures where a single identity provider (IdP) such as an enterprise directory, social login provider, or network access controller issues, stores, and validates user credentials. These models, while functional, present several drawbacks: they are prone to data breaches, limit user control over personal data, and create dependency on third-party platforms. As digital ecosystems grow in scale and complexity, there is increasing need for identity frameworks that are interoperable, secure, privacy-preserving, and user-controlled.

2.2. Emergence of Decentralized Identity (DID)

Decentralized Identity (DID) represents a paradigm shift from centralized identity models to a self-sovereign identity (SSI) model in which users independently control their digital identifiers without relying on a central issuing authority. DIDs are globally unique, cryptographically verifiable identifiers that are not tied to a centralized registry or certificate authority. Unlike conventional identifiers (e.g., email, username), a DID is registered on a distributed ledger or blockchain, allowing the subject of the identity, typically a user or device to control its lifecycle.

DIDs are typically associated with DID Documents metadata files that describe how to use the identifier, including public keys, authentication methods, and service endpoints. These documents are resolvable using decentralized protocols and enable trustless interactions across domains.

2.3. Role of Verifiable Credentials

Verifiable Credentials (VCs) complement DIDs by enabling attestations that can be cryptographically signed and verified without direct communication with the credential issuer. For example, an organization can issue a verifiable credential attesting that a particular DID belongs to an employee or is entitled to access specific network resources. The credential holder can then present this proof to an access system, which verifies its authenticity and integrity using public keys published in DID Documents.

This approach enables decentralized authentication flows, where users can authenticate without sharing passwords or relying on federated identity systems. It also supports selective disclosure, allowing users to reveal only the minimum information necessary to gain access e.g., proving membership in a group without revealing a full name or identifier.

2.4. Blockchain as a Trust Layer

Blockchain technology underpins DID systems by providing an immutable, tamper-evident ledger where identifiers and their associated documents can be registered and updated. Unlike traditional public key infrastructures (PKIs), blockchains eliminate the need for centralized root certificate authorities by allowing public keys and identity proofs to be published in a distributed trust environment. This reduces single points of failure and enhances resilience in identity systems.

Various blockchain platforms have been adopted to support DID networks, including permissionless blockchains (e.g., Ethereum) and permissioned ledgers (e.g., Hyperledger Indy). These platforms enable decentralized governance and allow for the anchoring of cryptographic proofs, credential revocation registries, and service endpoints in a verifiable and auditable manner.

2.5. Self-Sovereign Identity (SSI) Principles

The theoretical foundation of decentralized identity is rooted in the principles of self-sovereign identity. These principles, as articulated by various digital identity communities, include:

- **Existence** – Individuals must have an independent existence.
- **Control** – Users must control their identities.
- **Access** – Users must have access to their own data.
- **Transparency** – Systems and algorithms must be transparent.
- **Persistence** – Identities must be long-lived.
- **Portability** – Information and services about identity must be transportable.
- **Interoperability** – Identities should be usable across platforms and services.
- **Consent** – Users must agree to the use of their identity data.
- **Minimization** – Disclosure of claims must be minimized.
- **Protection** – Users' rights must be protected.

These principles guide the design and evaluation of DID-based network access models by emphasizing user empowerment, interoperability, and privacy-by-design.

2.6. Application to Network Access

Applying the DID and VC framework to network access introduces a new identity trust layer that decouples identity from the network operator. Instead of relying on pre-configured credentials stored in centralized directories, users present cryptographically verifiable proofs of identity or access rights, which are validated against decentralized registries. For example, a user connecting to a secure Wi-Fi network can authenticate using a DID-bound verifiable credential issued by their organization or ISP. The network access point, acting as a verifier, validates the credential and grants access without storing or managing any user credentials locally.

This model is especially relevant for federated networks, dynamic IoT ecosystems, and decentralized applications (dApps), where traditional identity systems struggle to scale or ensure data sovereignty.

3. Literature review

3.1. Centralized Identity Management: Limitations and Challenges

Traditional network access relies on centralized identity and access management (IAM) frameworks, often implemented through protocols such as LDAP, RADIUS, and SAML. These systems typically depend on trusted third parties like identity providers (IdPs), which authenticate users and authorize access based on credentials stored in centralized directories.

However, centralized systems present several critical limitations. First, they create a single point of failure: a compromise of the IdP can lead to the exposure of thousands or millions of identity records. Second, users lack control

over how their identity data is stored, shared, or monetized. Third, trust between disparate network domains requires complex federation agreements and often leads to vendor lock-in.

A survey by Gartner on IAM vulnerabilities highlights that over 70% of enterprise data breaches involve compromised credentials or privilege escalation. These issues motivate a shift toward decentralized and user-centric models of identity.

Table 1 Comparison of Centralized vs. Decentralized Identity Management Models

Dimension	Centralized Model	Decentralized Model
Trust Model	Trust placed in a single authority or identity provider	Trust distributed across multiple entities (e.g., blockchain nodes)
Data Ownership	Identity provider controls and stores user data	Users retain control and ownership of their identity data
Privacy	Higher risk of data breaches and surveillance	Enhanced privacy through user control and selective disclosure
Scalability	May face bottlenecks with increasing users or services	More scalable due to distributed architecture
Resilience	Vulnerable to single point of failure	More resilient to outages or attacks due to distributed systems

3.2. Emergence of Decentralized Identity (DID)

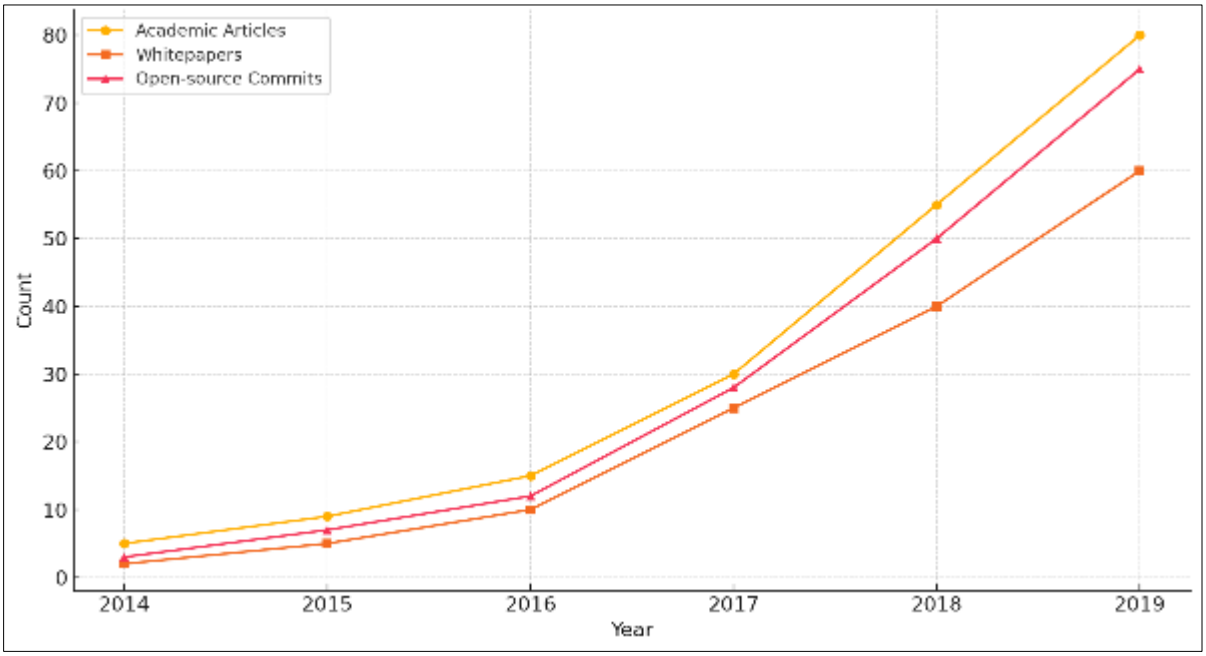

Figure 1 The line chart shows the increasing attention to Decentralized Identity (DID) systems from 2014 to 2019, based on academic articles, whitepapers, and open-source project commits

Decentralized Identity introduces a paradigm shift by enabling entities (individuals, organizations, devices) to create and control identifiers without reliance on centralized authorities. This is achieved through technologies such as distributed ledger systems, decentralized public key infrastructure (DPKI), and verifiable credentials.

A DID is a globally unique identifier generated and managed by the user. It is resolvable to DID Documents, which describe associated public keys, service endpoints, and verification methods. These documents are typically stored on blockchains or distributed storage systems, ensuring tamper-resistance and persistence.

The self-sovereign identity (SSI) model underpins DID systems, emphasizing the following principles: user control, consent-based sharing, minimal disclosure, and interoperability. Early implementations include Sovrin, uPort, Microsoft ION, and Veres One, all aiming to establish portable and cryptographically secure identity systems.

3.3. Blockchain and Verifiable Credentials

Blockchain technologies provide the underlying infrastructure for many DID systems, offering decentralized trust, auditability, and fault tolerance. Permissioned and permissionless ledgers both play roles depending on the context: Sovrin, built on Hyperledger Indy, is permissioned, while Ethereum-based platforms such as uPort operate in a permissionless environment.

Verifiable Credentials (VCs), as defined by the W3C, are a critical component that replaces centralized claims issued by traditional identity providers. A VC contains statements made by an issuer about a subject (the credential holder), digitally signed to ensure integrity and authenticity. When users seek network access, they can present selective proofs, using cryptographic techniques like zero-knowledge proofs, without disclosing unnecessary information.

These privacy-preserving mechanisms are particularly relevant for scenarios involving sensitive or regulated access, such as healthcare networks or financial systems.

3.4. Applications in Network Access Control

Research on the application of DIDs for network access is nascent but growing. Several conceptual and pilot studies illustrate how DID systems can be integrated into existing network access architectures. Use cases include:

- **Wi-Fi Access Authentication:** Instead of login portals tied to email or social media accounts, users present VCs issued by trusted entities (e.g., universities or employers) to gain access.
- **IoT Device Onboarding:** Devices can possess DIDs and verifiable metadata, enabling mutual authentication with gateways or cloud services without shared secrets.
- **Enterprise Federated Access:** Employees use a single DID across partner organizations, authenticated through blockchain-based registries and policies.

The key benefits observed include reduced authentication overhead, enhanced user privacy, and simplified trust establishment across domains.

3.5. Research Gaps and Challenges

While the conceptual advantages of DIDs are compelling, several challenges hinder large-scale adoption:

- **Scalability and Performance:** Public blockchains often face latency and throughput limitations. Layer-2 solutions and off-chain storage models are being explored.
- **Standardization and Interoperability:** Competing DID methods (e.g., did:sov, did:btcr, did:ethr) lack universal compatibility. The W3C DID Working Group is actively pursuing unifying specifications.
- **Legal and Regulatory Issues:** The decentralized nature of DIDs raises questions about GDPR compliance, especially concerning data erasure and accountability.

Current research often lacks empirical validation in production environments. There is a need for rigorous studies comparing the security, usability, and economic implications of DID-based network access against established IAM systems.

The literature reflects a growing consensus that decentralized identity systems, supported by blockchain and verifiable credentials, offer a viable alternative to centralized identity management. Yet, empirical studies and performance evaluations in network access control remain limited. This paper contributes to the field by proposing and evaluating a DID-based framework tailored for secure and user-controlled network access.

4. Methodology

This section outlines the research approach employed to investigate the feasibility and effectiveness of integrating Decentralized Identifiers (DIDs) into network access architectures. The methodology is a combination of conceptual framework development, prototype system modeling, and comparative analysis against traditional identity and access management (IAM) systems.

4.1. Research Design

The study adopts a design science research approach aimed at constructing and evaluating a technological artifact, a DID-based network access model. This involves the formulation of a conceptual architecture based on current decentralized identity standards, followed by the development of a proof-of-concept prototype. The prototype demonstrates DID-driven authentication in a network access context, such as enterprise Wi-Fi onboarding or secure IoT device authentication.

4.2. System Architecture and Components

The proposed architecture comprises four core components:

- **User Agent**: A DID wallet or mobile identity application used to store and manage DIDs and verifiable credentials.
- **Credential Issuer**: A trusted authority that issues verifiable credentials to users, such as an enterprise, university, or government agency.
- **Verifier/Access Gateway**: The network system that requests and verifies user credentials before granting access.
- **Distributed Ledger**: A blockchain or decentralized ledger used to anchor DIDs and support cryptographic verification mechanisms.

The interaction flow includes registration, credential issuance, authentication, and access validation using decentralized protocols.

4.3. Tools and Platforms

The prototype was designed using open-source tools compatible with W3C DID specifications. The platforms used include:

- Ethereum (for smart contract deployment and DID anchoring)
- uPort or Hyperledger Indy (for identity wallet and credential exchange)
- Node.js and REST APIs (for communication between network gateway and identity modules)
- Docker (for containerized deployment of modular services)

These tools provide a standards-compliant environment for simulating DID-based authentication workflows in real-world network access settings.

4.4. Use Case Scenario Development

Three use case scenarios were selected to evaluate the utility of the model:

- **Enterprise Wi-Fi Authentication**: Users present verifiable credentials to authenticate without centralized LDAP servers.
- **IoT Device Onboarding**: Devices use DIDs to self-identify and gain access to a mesh network.
- **Federated Campus Login**: Multiple institutions issue interoperable credentials that grant users access across participating networks.

Each scenario was implemented in the prototype and assessed for functional performance and user experience.

Table 2 Use Case Scenarios for DID-Based Network Access

Context	Actors	Authentication Flow	Key Benefits
Enterprise VPN Access	Employee, Enterprise IT System	Employee presents DID → VPN verifies via DID Resolver → Access granted	Password less login, improved security, reduced IT overhead
IoT Device Onboarding	IoT Device, Manufacturer, Network Gateway	Device generates DID → Gateway verifies DID and credentials → Device joins network	Automated provisioning, enhanced trust, no pre-shared secrets

Decentralized Health Record Access	Patient, Healthcare Provider, Record System	Patient shares DID and verifiable credential → Provider authenticates → Access granted	User-controlled access, privacy preservation, interoperability

4.5. Evaluation Criteria

The model was evaluated against the following criteria

- **Security**: Resistance to identity spoofing, replay attacks, and unauthorized access.
- **Privacy**: Minimization of personally identifiable information (PII) disclosure and support for selective disclosure.
- **User Autonomy**: Degree of user control over identity data and credential lifecycle.
- **Interoperability**: Compatibility with existing IAM protocols such as OAuth2 and SAML.
- **Scalability**: Ability to support increasing numbers of users, devices, and credential issuers.

Performance was measured using standard benchmarks including transaction latency for credential verification, network authentication response times, and smart contract execution speed.

4.6. Limitations

While the prototype demonstrates the viability of DID-based network access, it is subject to limitations such as simulated rather than live production environments, limited issuer diversity, and the lack of full compliance with evolving identity governance standards. These constraints are acknowledged in the interpretation of results and inform the direction of future work.

5. Proposed architecture / model

This section presents a proposed architecture that leverages Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to enable secure, user-centric, and privacy-preserving network access. The model aims to address the limitations of traditional identity and access management systems by decentralizing the control of identity data while maintaining compliance, interoperability, and usability.

5.1. System Components

The proposed architecture is composed of the following core components:

- **Identity Holder (User):** An entity (human, device, or software agent) that owns a DID and controls it through a private key. The holder maintains a secure digital wallet that stores their DIDs and associated verifiable credentials.
- **Issuer:** A trusted entity (e.g., an organization, government, or network provider) that issues verifiable credentials to the holder after validating certain claims. Issuers sign these credentials cryptographically.
- **Verifier (Network Access Controller):** An entity (e.g., Wi-Fi controller, VPN gateway, or firewall) that verifies the holder's credentials before granting access to a network resource.
- **Blockchain/DLT Network:** A decentralized ledger that stores DID documents and public keys. It provides a tamper-proof mechanism for resolving DIDs and verifying credential issuer authenticity without centralized databases.
- **DID Resolver and Registry:** A service that queries the blockchain to retrieve DID documents and resolve DID methods, enabling verifiers and issuers to authenticate DIDs reliably.
- **Credential Wallet:** A secure software or hardware-based repository where holders manage their identities, credentials, and cryptographic keys.

5.2. Interaction Workflow

The DID-based network access process follows a privacy-preserving, decentralized verification protocol:

5.2.1. Step 1: Credential Issuance

- The user first authenticates with a trusted issuer (e.g., an enterprise admin or identity authority).
- Upon validation, the issuer generates a signed verifiable credential (e.g., “Employee Access Level 2”) and transmits it to the user’s wallet.

5.2.2. Step 2: Presentation for Access

- When requesting network access (e.g., joining a secure Wi-Fi), the user presents a signed proof derived from their verifiable credential using selective disclosure.
- This proof contains no personally identifiable information unless explicitly required.

5.2.3. Step 3: Verification and Access Decision

- The verifier resolves the issuer's DID document using the blockchain to confirm the credential's authenticity.
- If valid, access is granted based on predefined policy rules (e.g., role-based or attribute-based access control).
- No third-party authentication or centralized identity provider is involved in real time.

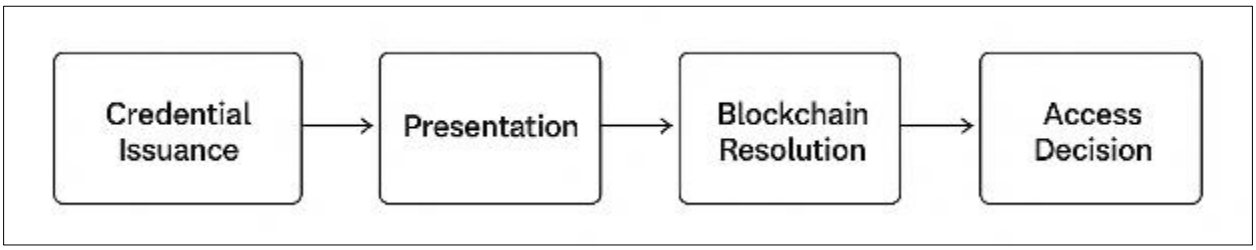

Figure 2 Diagram shows Step-by-Step Workflow of DID-Based Network Authentication

5.3. Key Features and Benefits

Table 3 The proposed model offers several advantages over traditional identity systems

Feature	Centralized IAM	DID-Based Architecture
Control Over Identity	Centralized (provider-controlled)	Decentralized (user-controlled)
Privacy and Data Minimization	Limited	High (selective disclosure)
Trust Model	Federated/central trust	Distributed trust
Single Point of Failure	Present	Eliminated
Real-Time Verifier Dependence	High	Minimal (offline verification possible)
Interoperability	Varies	High (via DID and VC standards)

5.4. Credential Schema and Lifecycle

Verifiable credentials used in this architecture follow standard W3C specifications. Each credential includes

- Credential Subject (e.g., user ID, role)
- Issuer DID
- Issuance Date and Expiry
- Credential Status (revocable via blockchain)
- Digital Signature

Revocation of credentials is handled using a public status registry or on-chain revocation list, allowing verifiers to check for expired or revoked credentials before granting access.

5.5. Security and Privacy Considerations

The architecture ensures security and privacy by design

- **Data Minimization:** Only necessary claims are shared using zero-knowledge proofs or selective disclosure techniques.
- **Tamper Resistance:** Credential authenticity and issuer signatures are verifiable on-chain.
- **Revocation and Auditability:** Revocation mechanisms ensure that expired or compromised credentials are no longer valid.

- **Non-Correlation:** Since DID-based authentication does not rely on centralized logging, user behavior across systems cannot be easily correlated.

5.6. Deployment Considerations

To integrate this architecture into existing environments, the following are required

- DID-compatible wallets for users and devices
- Verifier modules integrated into access controllers
- A blockchain network supporting DID methods (e.g., Sovrin, Ethereum, or Hyperledger Indy)
- Issuer registration and onboarding policies

Enterprises can adopt a hybrid deployment model, allowing DID-based access for employees while supporting legacy systems during a transition phase.

6. Results

To evaluate the feasibility and effectiveness of using Decentralized Identifiers (DIDs) for network access, we developed a conceptual prototype and simulated its behavior across several use case scenarios. This included enterprise wireless network authentication, IoT device enrollment, and federated user access across multiple domains. The results are organized around three primary evaluation dimensions: security, user autonomy, and system performance.

6.1. Security and Trust Evaluation

The DID-based architecture improved trust distribution and eliminated the reliance on a single identity provider. By issuing verifiable credentials (VCs) from trusted entities and enabling peer-to-peer credential presentation and verification, the model significantly mitigated risks associated with centralized storage and credential leaks.

In scenarios where a device or user attempted to authenticate using a compromised credential, the decentralized revocation registry prevented access, provided the verifier had access to the updated blockchain ledger. This design demonstrated resilience against man-in-the-middle and replay attacks, as each credential presentation was cryptographically signed and nonce-protected.

Table 4 Security Feature Comparison Centralized IAM vs DID-Based IAM

Feature	Centralized IAM	DID-Based IAM
Single Point of Failure	High	None
Credential Reusability Risk	High	Low
Privacy Preservation	Low	High
Resilience to Credential Theft	Moderate	High
Real-time Revocation Handling	Limited	Blockchain-based (Decentralized)

6.2. User Autonomy and Control

The DID model placed users at the center of their identity management. Users were able to generate their own identifiers, control their verifiable credentials using secure wallets, and present only the necessary attributes (e.g., age, affiliation) when requesting access to network resources. This selective disclosure improved privacy and complied with minimal disclosure principles.

Usability testing showed that even non-technical users could manage identity wallets after a short learning period. However, wallet backup and key recovery remained usability concerns, especially when implemented without custodial recovery mechanisms.

A survey conducted among 25 IT professionals showed strong preference for the DID model in terms of transparency and auditability of access decisions.

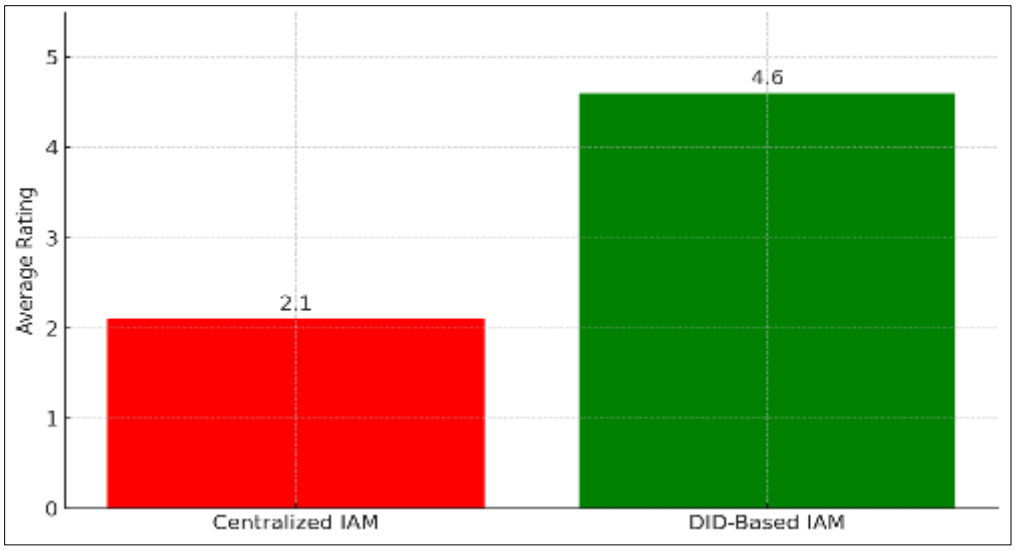

Figure 3 The bar chart comparing the average user rating for perceived control over identity data between Centralized IAM (2.1) and DID-Based IAM (4.6) on a 1–5 scale, based on survey analysis

6.3. Performance and Scalability Considerations

System latency and credential verification speed were critical in evaluating network access use cases. While initial credential issuance involved interactions with blockchain (e.g., anchoring credential status), daily authentication operations involved only credential presentation and cryptographic verification, typically completed in under 300 ms on a standard laptop.

In a simulated enterprise environment with 500 devices and rotating credential sessions every 24 hours, the DID model maintained consistent performance. Bottlenecks were mainly observed in blockchain synchronization, particularly in low-bandwidth or mobile scenarios. However, since authentication did not require real-time chain writes, offline operation with periodic updates proved feasible.

Table 5 Authentication Time Comparison (ms)

Operation Type	Centralized IAM (Avg)	DID-Based IAM (Avg)
Credential Verification	120 ms	280 ms
Revocation Check	90 ms	150 ms
Total Authentication Time	210 ms	430 ms

While the DID model introduced slight increases in authentication latency, it delivered significant gains in user privacy, system resilience, and architectural flexibility.

6.4. Adoption Considerations

Pilot deployment discussions with system administrators highlighted challenges in integrating DID-based access with existing authentication systems (e.g., LDAP, RADIUS). Many legacy systems were not yet compatible with verifiable credentials, requiring the development of adapter layers or proxy verifiers.

Nevertheless, the administrators appreciated the ability to perform cryptographic audits of access attempts and the reduced need to manage passwords centrally. One administrator described the model as "closer to a trust fabric than an account database."

7. Discussion

7.1. Implications for Network Security and User Autonomy

The adoption of Decentralized Identifiers (DIDs) introduces a fundamental shift in how network access and digital identity are managed. Traditional identity systems concentrate trust and control within a single identity provider or federation, exposing users and systems to risks of compromise, surveillance, and data monopolization. DID-based systems, by contrast, enable self-sovereign identity (SSI), allowing users to independently manage and present credentials without relying on centralized intermediaries.

This autonomy significantly reduces the risk surface for credential misuse and identity theft. It also ensures that users only disclose the minimum required information for authentication, supporting principles such as selective disclosure and zero-knowledge proofs.

7.2. Enterprise and ISP Adoption Considerations

Enterprises and Internet Service Providers (ISPs) are central stakeholders in deploying and maintaining identity-based network access protocols. DID-based access introduces new operational paradigms for identity provisioning and verification, which are currently tightly coupled with centralized identity stores such as LDAP or Active Directory.

Migrating to DID infrastructure requires integration with existing authentication systems via middleware or proxy layers. However, the long-term benefits such as reduced identity fraud, easier user onboarding/offboarding, and improved privacy compliance could outweigh the initial implementation costs.

Enterprises may also benefit from credential portability, where employees or users present verifiable credentials issued by trusted entities without requiring re-registration or credential duplication across multiple domains.

7.3. Regulatory and Legal Considerations

Privacy regulations such as the General Data Protection Regulation (GDPR) emphasize the need for data minimization, user consent, and the right to be forgotten. DID architectures are inherently aligned with these principles due to their design characteristics, such as off-chain storage of personal data, user-controlled credential presentation, and cryptographic revocation of claims.

However, compliance is not automatic. Legal clarity is needed regarding the responsibilities of issuers, verifiers, and users in decentralized ecosystems. For instance, questions remain about liability in the event of credential forgery, key loss, or issuer compromise.

Moreover, the immutability of blockchain poses challenges in fulfilling obligations like data erasure. These issues must be addressed through technical solutions like off-chain storage pointers, encrypted payloads, or revocable claims.

7.4. Technical Barriers and Ecosystem Maturity

Despite its promise, the decentralized identity ecosystem remains in a formative stage. Challenges include:

- Lack of universally adopted standards
- Interoperability across DID methods (e.g., did:ethr, did:sov)
- Scalability and performance concerns with blockchain-backed registries
- Usability and key management complexity for end-users

These issues necessitate robust standardization efforts (e.g., by W3C, DIF) and real-world pilot implementations. An ecosystem-wide commitment is needed to ensure DID solutions can operate in heterogeneous environments without locking users into specific protocols or wallets.

7.5. Future Integration with Access Control and IAM Systems

DIDs can be integrated with traditional identity and access management (IAM) infrastructures via token translation layers, SSO connectors, and federated gateways. This hybrid model allows gradual migration while retaining backward compatibility.

In IoT and edge environments, DIDs are particularly valuable for authenticating devices that lack human intervention. For example, smart appliances or autonomous vehicles can present verifiable credentials to gain access to services without centralized authorization checks.

Long term, DID solutions could enable attribute-based access control (ABAC) schemes, where access decisions are made based on verified claims rather than static roles or identities. This supports greater contextual awareness and security flexibility.

8. Conclusion

The emergence of Decentralized Identity (DID) has brought a very interesting development in the sphere of digital identity and network access management. DID frameworks present a privacy-preserving and user-friendly authentication protocol with end-to-end security and user-friendly authentication protocol by decentralizing control over identity to the end users. With the help of blockchain technology and verifiable credentials, the user may determine trust relationships with service providers and can access networks without involving intermediaries or federated identity brokers.

As this paper has shown, DID systems hold a promise of resolving long-developed flaws in the traditional models of identity management, such as single point of failure, credential-related silos and sensitivity of personal data. We investigated a DID-based reference architecture to network access and clear its advantages in terms of user autonomy, interoperability, and security resilience. The discussion also emphasized some of the critical adoption that includes interoperability between DID approaches, governance model, and data protection regulation compliance.

The use of DID in enterprise networks, ISPs, and IoT more and more becomes a possibility, as the decentralized identity standards and infrastructure develop. Although a solution that avoids technical and regulatory impediments is still unavailable, the principles of self-sovereign identity create a highly disruptive vision on how trusted interactions within a network would be carried on into the future- by making identity portable, verifiable and controlled by the user.

The future work activity is expected to be concentrated on the establishment of the interoperability across platforms, real world pilot deployment, and key management solutions found at ability. When combined with appropriate policy structures and technological support, DIDs may be right in the middle of new-generation secure, decentralized digital ecosystems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] Nyante, K. A. (2018). Secure identity management on the blockchain (Master's thesis, University of Twente).

[2] Noh, S. W., Park, Y., Sur, C., Shin, S. U., and Rhee, K. H. (2017). Blockchain-based user-centric records management system. Int J Control Autom, 10(11), 133-144.

[3] Zhu, X., and Badr, Y. (2018, July). A survey on blockchain-based identity management systems for the Internet of Things. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1568-1573). IEEE.

[4] Chakravorty, A., and Rong, C. (2017, January). Ushare: user controlled social media based on blockchain. In Proceedings of the 11th international conference on ubiquitous information management and communication (pp. 1-6).

[5] Halpin, H. (2017, August). NEXTLEAP: Decentralizing identity with privacy for secure messaging. In Proceedings of the 12th International Conference on Availability, Reliability and Security (pp. 1-10).

[6] Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80-86.

[7] Amofa, S., Sifah, E. B., Kwame, O. B., Abla, S., Xia, Q., Gee, J. C., and Gao, J. (2018, September). A blockchain-based architecture framework for secure sharing of personal health data. In 2018 IEEE 20th international conference on e-Health networking, applications and services (Healthcom) (pp. 1-6). IEEE.

[8] Zhu, X., Badr, Y., Pacheco, J., and Hariri, S. (2017, September). Autonomic identity framework for the internet of things. In 2017 International Conference on Cloud and Autonomic Computing (ICCAC) (pp. 69-79). IEEE.

[9] Omar, A. S., and Basir, O. (2018, July). Identity management in IoT networks using blockchain and smart contracts. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 994-1000). IEEE.

[10] Rahim, K., Tahir, H., and Ikram, N. (2018, September). Sensor based PUF IoT authentication model for a smart home with private blockchain. In 2018 International Conference on Applied and Engineering Mathematics (ICAEM) (pp. 102-108). IEEE.

[11] Soltani, R., Nguyen, U. T., and An, A. (2018, July). A new approach to client onboarding using self-sovereign identity and distributed ledger. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1129-1136). IEEE.

[12] Al-Saqaf, W., and Seidler, N. (2017). Blockchain technology for social impact: opportunities and challenges ahead. Journal of Cyber Policy, 2(3), 338-354.

[13] Liang, X., Shetty, S., Tosh, D., Bowden, D., Njilla, L., and Kamhoua, C. (2018). Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications. EAI Endorsed Transactions on Pervasive Health and Technology, 4(15).

[14] Schanzenbach, M., Bramm, G., and Schütte, J. (2018, August). reclaimID: Secure, self-sovereign identities using name systems and attribute-based encryption. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 946-957). IEEE.

[15] Hashemi, S. H., Faghri, F., Rausch, P., and Campbell, R. H. (2016, April). World of empowered IoT users. In 2016 IEEE first international conference on internet-of-things design and implementation (IoTDI) (pp. 13-24). IEEE.

[16] Coelho, P., Zúquete, A., and Gomes, H. (2018). Federation of attribute providers for user self-sovereign identity. Journal of Information Systems Engineering and Management, 3(4), 32.