PEER-REVIEWED JOURNAL OF COMPUTER SCIENCE (PRJCS)

ISSN Online : Open Access Scholarly Journal

Blockchain-Based Digital Identity Management And Verification Systems

Tintu George

Assistant Professor, Department of BCA AI, Sri Ramakrishna College of Arts & Science, Coimbatore, India

Article information

Received: 12th March 2026
Received in revised form: 25th March 2026
Accepted: 2nd April 2026
Available online: 9th April 2026

Volume: 1
Issue: 4
DOI: https://doi.org/10.5281/zenodo.19464963

Abstract

Digital identity management remains one of the most pressing challenges in the modern information economy. Traditional centralized identity systems suffer from single points of failure, pervasive data breaches, and an inherent lack of user control over personal information. This paper presents a comprehensive survey of blockchain-based digital identity management and verification systems, examining the architectural paradigms that underpin self-sovereign identity (SSI), federated identity, and decentralized identifier (DID) frameworks. We compare leading blockchain platforms—including Ethereum, Hyperledger Fabric, Solana, Bitcoin, and Polkadot—on critical metrics such as transaction throughput, consensus mechanisms, and smart contract capabilities. Through systematic analysis of real-world deployments in government, healthcare, and financial services, we evaluate the practical viability of decentralized identity solutions. Our comparative assessment reveals that self-sovereign models outperform centralized and federated approaches on security, privacy, and user control dimensions, while facing trade-offs in scalability and interoperability. The paper further identifies open challenges including regulatory alignment, key management usability, and cross-chain identity portability, proposing a research agenda for advancing blockchain-based identity toward mainstream adoption.

Keywords: - Blockchain, Digital Identity, Self-Sovereign Identity, Decentralized Identifiers, Verifiable Credentials, Identity Management, Distributed Ledger Technology

I. INTRODUCTION

The management of digital identities constitutes a foundational challenge for secure and privacy-preserving interactions in an increasingly connected world. As of 2025, the World Bank estimates that approximately 850 million people globally lack any form of officially recognized identification, while billions more depend on fragmented, institution-controlled digital identity systems that are vulnerable to large-scale data breaches [1]. The centralized model of identity management, wherein a single authority issues, stores, and verifies identity credentials, has dominated digital infrastructure for decades. However, high-profile incidents such as the Equifax breach of 2017, which exposed the personal data of 147 million individuals, have underscored the systemic vulnerabilities inherent in this paradigm [2].

Blockchain technology, first introduced by Nakamoto [3] as the underlying mechanism for Bitcoin, offers a fundamentally different approach to data management. By distributing trust across a decentralized network of nodes and employing cryptographic consensus protocols, blockchain eliminates the need for a central intermediary. Buterin [4] extended this vision with Ethereum, introducing programmable smart contracts that enable complex decentralized applications, including identity management systems. These developments have catalyzed a new wave of identity architectures that prioritize user sovereignty, data minimization, and cryptographic verifiability.

The concept of self-sovereign identity (SSI), articulated by Allen [5] in his seminal essay on the path to self-sovereign identity, represents a paradigm shift from institution-centric to individual-centric identity. In the SSI model, individuals control their own identity data through cryptographic key pairs and selectively disclose verifiable credentials to relying parties without exposing unnecessary personal information. The World Wide Web Consortium (W3C) has formalized this vision through the Decentralized Identifiers (DID) specification [6], which provides a standardized method for creating, resolving, and managing decentralized identifiers that are anchored on distributed ledgers.

Despite growing academic and industrial interest, blockchain-based identity systems face significant challenges. Mühle et al. [7] provided an early comprehensive survey of the landscape, identifying scalability, key management, and regulatory compliance as critical open problems. Dunphy and Petitcolas [8] further examined the tension between the immutability of blockchain records and the requirements of data protection regulations such as the European Union's General Data Protection Regulation (GDPR), particularly the right to erasure. These challenges have motivated a rich body of subsequent research exploring hybrid architectures, off-chain storage solutions, and privacy-enhancing technologies such as zero-knowledge proofs [9].

This paper contributes a systematic and up-to-date survey of blockchain-based digital identity management systems. We analyze the architectural foundations of centralized, federated, and self-sovereign identity models, comparing their properties across security, privacy, user control, scalability, and interoperability dimensions (Figure 1). We evaluate leading blockchain platforms on transaction throughput and identity-specific capabilities (Figure 2), and we examine real-world deployments spanning government, healthcare, and financial sectors. The remainder of this paper is organized as follows: Section II reviews the background and related work; Section III presents the comparative framework and analysis; Section IV discusses real-world case studies; Section V examines challenges and future directions; and Section VI concludes the paper.

II. BACKGROUND AND RELATED WORK

The evolution of digital identity management can be characterized through four distinct generations. The first generation comprised siloed identity systems, where each service provider maintained its own user database with independent credentials. The second generation introduced centralized identity providers (IdPs) such as OAuth and OpenID Connect, which allowed users to authenticate across multiple services using a single set of credentials managed by a trusted third party [10]. The third generation brought federated identity models, exemplified by Security Assertion Markup Language (SAML) federations and the European eIDAS framework, enabling cross-organizational identity verification while distributing trust among multiple authorities [11]. The fourth and most recent generation is blockchain-based self-sovereign identity, which shifts control entirely to the individual user through cryptographic mechanisms and decentralized verification [5].

Blockchain technology provides several properties that are directly applicable to identity management. Immutability ensures that identity records, once anchored, cannot be retroactively altered. Decentralization eliminates single points of failure and reduces the risk of mass data breaches. Transparency enables auditability of identity transactions without compromising individual privacy when combined with appropriate cryptographic techniques. Nakamoto's [3] original Bitcoin protocol demonstrated these properties in the context of financial transactions, while Ethereum [4] generalized them through Turing-complete smart contracts that can encode complex identity verification logic.

The W3C Decentralized Identifiers (DID) specification [6] provides the technical foundation for blockchain-based identity. A DID is a globally unique identifier that is created, owned, and controlled by the identity subject, independent of any centralized registry or certificate authority. DIDs resolve to DID Documents that contain public keys, authentication methods, and service endpoints. Complementing DIDs, the W3C Verifiable Credentials (VC) data model [12] defines a standard format for tamper-evident digital credentials that can be cryptographically verified by any relying party. Together, DIDs and VCs form the core building blocks of the SSI stack.

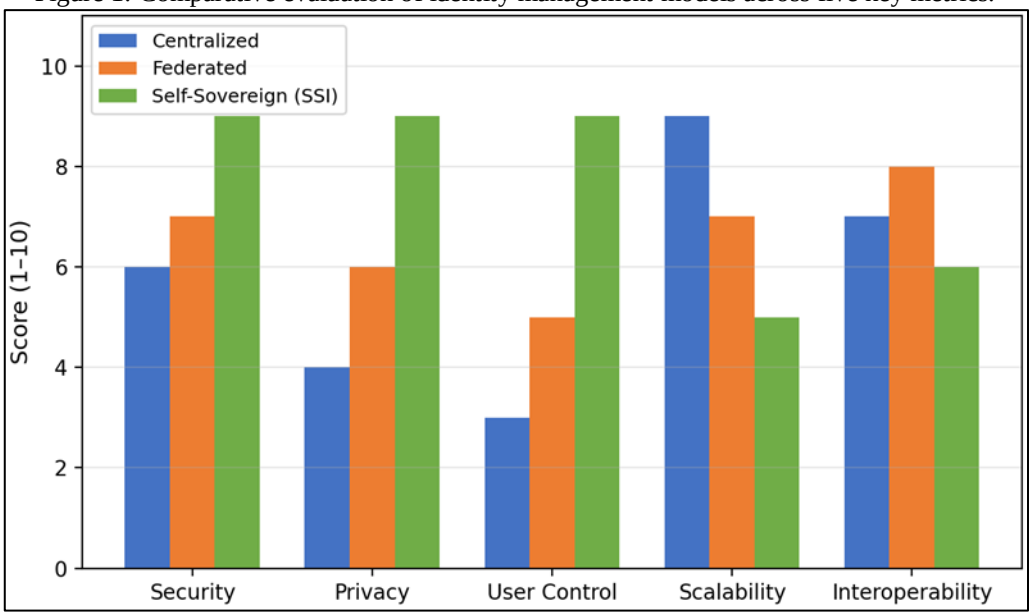
Mühle et al. [7] conducted one of the earliest comprehensive surveys of blockchain-based identity management, categorizing existing systems according to their architectural choices and identifying key design trade-offs. Their analysis highlighted that while blockchain provides strong integrity guarantees, the storage of personal data on-chain raises significant privacy concerns. Dunphy and Petitcolas [8] extended this analysis by examining the compatibility of blockchain-based identity systems with existing legal frameworks, concluding that pure on-chain solutions are fundamentally incompatible with GDPR's right to erasure and that hybrid architectures storing only cryptographic hashes and proofs on-chain are necessary for regulatory compliance.

Recent advances have focused on enhancing the privacy and scalability of blockchain-based identity systems. Zero-knowledge proofs (ZKPs), particularly zk-SNARKs and zk-STARKs, enable identity holders to prove specific attributes (such as being over 18 years of age) without revealing the underlying data [9]. Hyperledger Indy, a purpose-built blockchain for decentralized identity, incorporates Camenisch-Lysyanskaya (CL) signatures to support selective disclosure and predicate proofs natively [13]. Meanwhile, layer-2 scaling solutions such as Ethereum's rollups and state channels have been explored to address the throughput limitations that constrain identity systems built on public blockchains [14].

III. COMPARATIVE FRAMEWORK AND ANALYSIS

To systematically evaluate the landscape of digital identity management, we developed a comparative framework encompassing five key dimensions: security, privacy, user control, scalability, and interoperability. Each dimension is scored on a scale of 1 to 10 based on a synthesis of the existing literature and technical specifications. We apply this framework to three identity paradigms: centralized, federated, and self-sovereign identity. Figure 1 presents the comparative results.

Figure 1: Comparative evaluation of identity management models across five key metrics.



As illustrated in Figure 1, the self-sovereign identity model achieves the highest scores on security (9/10), privacy (9/10), and user control (9/10), reflecting its cryptographic foundations and individual-centric design. The centralized model, while scoring highest on scalability (9/10) due to the efficiency of single-authority operations, is notably weakest on privacy (4/10) and user control (3/10), as the identity provider retains full custody of personal data. The federated model occupies an intermediate position across all dimensions, offering moderate improvements in privacy and user control over the centralized model but falling short of the SSI model's guarantees [7], [8].

A critical factor in the practical deployment of blockchain-based identity systems is the choice of underlying blockchain platform. Different platforms offer distinct trade-offs in terms of transaction throughput, consensus mechanism, smart contract capabilities, and permissioning model. Table 1 presents a detailed comparison of five major blockchain platforms that have been employed or proposed for identity management applications.

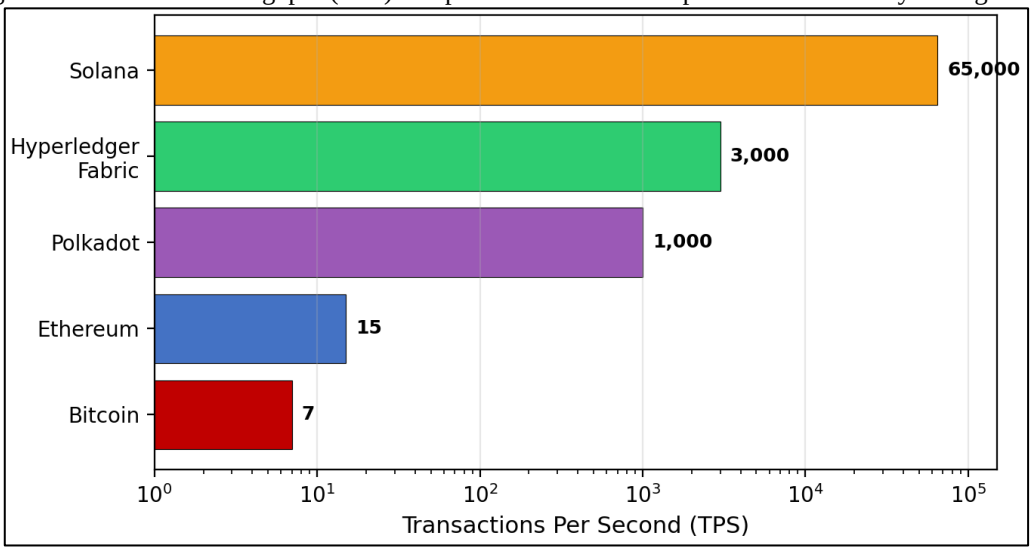
Table 1. Comparison of Blockchain Platforms for Digital Identity Management

Platform	Consensus	TPS	Smart Contracts	Identity Framework	Permissioned
Bitcoin	PoW	~7	Limited (Script)	None native	No
Ethereum	PoS	~15	Yes (Solidity)	ERC-725/735, uPort	No
Hyperledger Fabric	PBFT	~3,000	Yes (Chaincode)	Indy/Aries	Yes
Solana	PoH+PoS	~65,000	Yes (Rust/C)	Custom DIDs	No
Polkadot	NPoS	~1,000	Yes (ink!)	KILT Protocol	No

As shown in Table 1, considerable variation exists among platforms in both throughput and identity-specific capabilities. Bitcoin, with a throughput of approximately 7 transactions per second (TPS), is poorly suited for identity applications requiring high-frequency credential issuance and verification. Ethereum's throughput of approximately 15 TPS on the base layer similarly constrains large-scale deployments, though layer-2 solutions can substantially increase effective throughput [14]. Hyperledger Fabric, a permissioned blockchain, achieves approximately 3,000 TPS and benefits from its integration with Hyperledger Indy and Aries, purpose-built frameworks for decentralized identity and verifiable credential exchange [13]. Solana's throughput of approximately 65,000 TPS makes it theoretically attractive for high-volume identity operations, though its identity ecosystem is less mature. Polkadot, with its parachain architecture and the KILT Protocol for decentralized identity, offers a middle ground of approximately 1,000 TPS with strong interoperability features [15].

Figure 2 provides a visual comparison of the transaction throughput across these platforms, displayed on a logarithmic scale to accommodate the wide range of values.

Figure 2: Transaction throughput (TPS) comparison of blockchain platforms for identity management.



The throughput comparison in Figure 2 reveals a performance gap spanning four orders of magnitude between the slowest (Bitcoin at 7 TPS) and fastest (Solana at 65,000 TPS) platforms. This variation has profound implications for identity system design. High-throughput platforms can support real-time credential verification at scale, while lower-throughput platforms may require off-chain or layer-2 architectures to achieve acceptable performance for identity workloads [14]. Notably, the permissioned nature of Hyperledger Fabric enables it to achieve high throughput while maintaining the access control mechanisms preferred by enterprise and government identity deployments [13].

IV. CASE STUDIES OF BLOCKCHAIN IDENTITY DEPLOYMENTS

The transition from theoretical frameworks to practical deployments represents a critical test for blockchain-based identity systems. In this section, we examine notable real-world implementations spanning government, humanitarian, and enterprise domains. Table 2 summarizes the key characteristics of these deployments.

Table 2. Case Studies of Blockchain-Based Digital Identity Deployments

Project	Country/Org	Platform	Use Case	Status	Year
e-Residency 2.0	Estonia	KSI Blockchain	National digital ID	Operational	2014
ID2020	UNHCR/Global	Hyperledger / Multi	Refugee identity	Pilot	2017
Sovrin Network	Global (NGO)	Hyperledger Indy	SSI public utility	Operational	2017
uPort / Serto	ConsenSys	Ethereum	Self-sovereign identity	Operational	2017
ION (MS)	Microsoft	Bitcoin (Layer-2)	Decentralized identifiers	Operational	2019
NHS COVID Pass	UK	Hybrid / Private DLT	Vaccine credential verification	Concluded	2021
KILT Protocol	BOTLabs/EU	Polkadot	Verifiable credentials	Operational	2021
Worldcoin (WLD)	Global	Optimism (L2)	Biometric proof-of-personhood	Operational	2023

As shown in Table 2, blockchain-based identity deployments span a diverse range of use cases and maturity levels. Estonia's e-Residency program, one of the earliest government-led digital identity initiatives, leverages the KSI (Keyless Signature Infrastructure) blockchain to provide tamper-evident identity services to over 100,000 e-residents globally [16]. The system anchors cryptographic hashes of identity events on a blockchain, enabling citizens and e-residents to verify that their identity records have not been altered. This approach exemplifies the hybrid on-chain/off-chain architecture recommended by Dunphy and Petitcolas [8] for regulatory compliance.

The Sovrin Network, built on Hyperledger Indy, represents one of the most ambitious attempts to create a global public utility for self-sovereign identity [13]. Operating as a permissioned public blockchain with a distributed governance model, Sovrin enables any entity to issue, hold, and verify credentials using W3C-standard DIDs and verifiable credentials [6], [12]. The network's design incorporates privacy-preserving features including zero-knowledge proofs for selective disclosure and pairwise pseudonymous DIDs that prevent correlation across relying parties [9].

Microsoft's ION (Identity Overlay Network) takes a distinctive approach by anchoring decentralized identifiers on the Bitcoin blockchain through a layer-2 protocol based on the Sidetree specification [17]. By batching thousands of DID operations into a single Bitcoin transaction, ION overcomes the throughput limitations of the Bitcoin base layer while inheriting its security guarantees. This design demonstrates that even low-throughput blockchains can support large-scale identity systems when combined with appropriate layer-2 architectures.

More recently, the Worldcoin project has introduced biometric proof-of-personhood using iris scanning combined with blockchain-based identity verification on the Optimism layer-2 network [18]. While technologically innovative, this project has generated significant controversy regarding biometric data privacy, informed consent, and the centralization of biometric template storage, highlighting the ongoing tension between technical capability and ethical governance in blockchain identity systems.

V. CHALLENGES AND FUTURE DIRECTIONS

Despite substantial progress, blockchain-based digital identity systems face several persistent challenges that must be addressed for widespread adoption. First, the problem of key management remains a critical usability barrier. In SSI systems, the loss of a private key effectively results in identity loss, as there is no centralized authority to perform account recovery. Social recovery mechanisms, wherein trusted contacts can collectively authorize key rotation, have been proposed [19], but their practical effectiveness and security properties require further investigation.

Second, regulatory alignment continues to present challenges. The tension between blockchain immutability and the GDPR right to erasure identified by Dunphy and Petitcolas [8] remains unresolved in practice. While off-chain storage with on-chain hashes provides a partial solution, questions persist regarding the legal status of on-chain cryptographic hashes when the off-chain data is deleted. The emergence of the EU's eIDAS 2.0 regulation and the European Digital Identity Wallet framework [20] introduces new requirements for cross-border identity interoperability that blockchain solutions must accommodate.

Third, interoperability across different blockchain networks and identity ecosystems remains limited. While the W3C DID specification [6] provides a common syntax, the resolution mechanisms and trust frameworks vary significantly across implementations. Cross-chain identity portability—the ability to use credentials issued on one blockchain platform for verification on another—requires further standardization and the development of bridge protocols. Polkadot's cross-chain messaging protocol and Cosmos's Inter-Blockchain Communication (IBC) protocol offer promising architectural foundations, but their application to identity-specific use cases is still nascent [15].

Fourth, the scalability-decentralization trade-off, often referred to as the blockchain trilemma, directly impacts identity system design. As shown in Figure 2, public blockchains such as Bitcoin and Ethereum achieve strong decentralization but limited throughput, while high-throughput platforms such as Solana have faced criticism regarding validator concentration and network reliability. Layer-2 solutions, including rollups and state channels, represent the most promising near-term approach to resolving this trade-off for identity applications [14].

Future research directions include the integration of artificial intelligence with blockchain-based identity for automated credential verification and fraud detection, the development of quantum-resistant cryptographic primitives for long-term identity security, and the design of governance frameworks that balance decentralization with accountability. Additionally, the application of blockchain-based identity to emerging domains such as decentralized autonomous organizations (DAOs), metaverse environments, and Internet of Things (IoT) device identity presents rich opportunities for further investigation [21].

VI. CONCLUSION

This paper has presented a comprehensive survey of blockchain-based digital identity management and verification systems, examining the evolution from centralized to self-sovereign identity paradigms and evaluating the technical and practical dimensions of current implementations. Our comparative analysis demonstrates that self-sovereign identity models, enabled by blockchain technology and standardized through W3C's DID and Verifiable Credentials specifications, offer substantial advantages in security, privacy, and user control over traditional centralized and federated approaches (Figure 1). However, these benefits come with trade-offs in scalability and interoperability that require continued research and engineering effort.

The evaluation of blockchain platforms (Table 1, Figure 2) reveals that no single platform dominates across all dimensions relevant to identity management. Permissioned platforms such as Hyperledger Fabric offer the throughput and access control features favored by enterprise and government deployments, while public platforms such as Ethereum benefit from larger developer ecosystems and stronger decentralization guarantees. Layer-2 solutions are emerging as a critical enabler for scaling identity operations on public blockchains.

Real-world deployments (Table 2) demonstrate both the viability and the challenges of blockchain-based identity in practice. From Estonia's national digital identity system to global humanitarian identity initiatives and enterprise SSI platforms, these case studies illustrate the diverse contexts in which blockchain identity is being applied. As regulatory frameworks evolve, particularly with the EU's eIDAS 2.0, and as cryptographic techniques such as zero-knowledge proofs mature, blockchain-based identity systems are positioned to play an increasingly central role in the global digital identity infrastructure.

REFERENCES

[1] World Bank, "Identification for Development (ID4D) Global Dataset," Washington, DC, 2023. [Online]. Available: https://id4d.worldbank.org/

[2] U.S. Government Accountability Office, "Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," GAO-18-559, Aug. 2018.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.

[5] C. Allen, "The path to self-sovereign identity," *Life With Alacrity*, Apr. 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[6] W3C, "Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations," W3C Recommendation, Jul. 2022.

[7] Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[8] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[9] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Proc. 3rd Int. Conf. Security in Communication Networks (SCN)*, Amalfi, Italy, 2002, pp. 268–289.

[10] D. Hardt, "The OAuth 2.0 Authorization Framework," IETF RFC 6749, Oct. 2012.

[11] European Commission, "Regulation (EU) No 910/2014 on Electronic Identification and Trust Services (eIDAS)," *Official Journal of the European Union*, Jul. 2014.

[12] W3C, "Verifiable Credentials Data Model v1.1," W3C Recommendation, Mar. 2022.

[13] Hyperledger Foundation, "Hyperledger Indy: Distributed Ledger Purpose-Built for Decentralized Identity," 2023. [Online].

[14] V. Buterin, "An Incomplete Guide to Rollups," *vitalik.ca*, Jan. 2021. [Online].

[15] KILT Protocol, "KILT Protocol: A Blockchain Identity Protocol for Issuing Self-Sovereign, Verifiable Credentials," 2023. [Online]. Available: https://www.kilt.io/

[16] e-Residency Republic of Estonia, "e-Residency: The New Digital Nation," 2024. [Online]. Available: https://www.e-resident.gov.ee/

[17] D. Buchner, O. Steele, and T. Looker, "Sidetree v1.0.0: A Scalable DID Method for Any Decentralized Ledger," Decentralized Identity Foundation, 2023.

[18] Worldcoin Foundation, "Worldcoin Whitepaper," 2023. [Online]. Available: https://whitepaper.worldcoin.org/

[19] V. Buterin, "Why We Need Wide Adoption of Social Recovery Wallets," *vitalik.ca*, Jan. 2021. [Online].

[20] European Commission, "Proposal for a Regulation on a European Digital Identity Framework (eIDAS 2.0)," COM(2021) 281 final, Jun. 2021.

[21] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet of Things (iThings)*, Chengdu, China, 2016, pp. 433–436.