International Journal of Multidisciplinary Research and Growth Evaluation.

Review of Blockchain-Based Identity Management Systems

Ashu Ganjeer [1*], Dr. Siddharth Choubey [2]
[1] M.Tech. Scholar, Department of Computer Science & Engineering, SSTC, Bhilai, Chhattisgarh, India
[2] Head of Department, Department of Computer Science & Engineering, SSTC, Bhilai, Chhattisgarh, India

* Corresponding Author: **Ashu Ganjeer**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 04
July - August 2025
Received: 11-06-2025
Accepted: 08-07-2025
Published: 25-07-2025
Page No: 895-900

Abstract

Digital identity is the foundation for all of contemporary digital life—banking and e-commerce, telemedicine and smart infrastructure. Legacy identity systems, however, which centralize sensitive user data in a handful of providers, put individuals and institutions at risk of catastrophic breaches, dark consent models, and vendor lock-in. Blockchain technology presents a different paradigm: its distributed ledger stores user registrations, verifiable credentials, and access transactions securely; smart contracts autonomously execute credential issuance, verification, and revocation without intermediaries; and decentralized storage networks such as IPFS provide personal data to be off-chain but tamper-evident through cryptographic hashes. This survey is a critical analysis of nine notable contributions in four different categories: foundation architecture taxonomies that classify blockchain networks and consensus protocols; end-to-end proofs of concept on Ethereum/IPFS demonstrating consent-based KYC workflows and one-time-password login sequences; theoretical explorations of self-sovereign identity (SSI) comparing DID architectures with minimal principles of user control and minimal disclosure; and specialized extensions including context-aware access rules, NFT-based academic credentials, and hierarchical DID architectures optimized for resource-constrained IoT deployments. We include real-case studies such as Estonia's e-Residency smart IDs, MIT's blockchain diplomas, time-geofence smart contracts managing city parking permits, and authentication of industrial sensors in private Practical Byzantine Fault Tolerance (pBFT) gateways to ground our analysis in real-world deployments. By combining architectural patterns, privacy-enhancing modules like zero-knowledge proofs, and performance benchmarks, we identify common design trade-offs and the open issues of global scalability, cross-chain interoperability, human-centric key recovery, and regulatory compliance with "right to be forgotten" requirements. To enable future innovation, we suggest a modular reference architecture of user-centric agent SDKs, specialized Layer-2 DID registries, hybrid consensus networks, decentralized storage, and trust-minimized oracle networks. This multi-layered architecture outlines a path to a truly unified, self-sovereign digital identity ecosystem—one that is secure, privacy-preserving, and universally interoperable.

Keywords: Decentralized Identifier (DID), Self-Sovereign Identity, Smart Contracts, IPFS, Zero-Knowledge Proof, Context-Aware Access, NFT Credentials

1. Introduction

Digital identity has become the basis for almost all online activity, from logging into mobile banking apps to filling out government forms, accessing telemedicine services, and controlling smart devices in networked industrial settings. Still, the majority of identity management products remain founded on centralized databases—controlled by governments, large tech companies, or industry consortia—enormous vulnerabilities by design as single points of failure. Large-scale breaches of national identity infrastructure and corporate single-sign-on systems often make front-page news, spilling tens of millions of sensitive records and eroding public trust. Further, when users don't actually own their own data in a meaningful way, they are subjected to clunky consent procedures, which adds friction and stifles innovation in new areas such as decentralized finance and cross-border e-commerce.

Blockchain technology offers a secure alternative. By recording identity-related events—e.g., user registration, credential issuance, or authorization for access rights—onto an immutable and cryptographically sealed distributed ledger, blockchains avoid centralized control while leaving an auditable record. Smart contracts, self-executing programs resident on the blockchain, enable sophisticated workflows such as issuing and revoking credentials without the need for intermediaries. To take an example, Estonia's groundbreaking e-Residency program applies these principles in practice: international entrepreneurs are granted a government-backed digital identity that allows them to sign contracts or open bank accounts as if they were native citizens, all shielded by blockchain technology. Similarly, the Massachusetts Institute of Technology began issuing blockchain-protected diplomas in the form of non-fungible tokens (NFTs) as early as 2017, providing graduates with a single click with which to share verifiable credentials to potential employers, instead of faxing paper certificates.

Despite these advancements, making a universal, self-sovereign digital identity a reality remains a challenging goal. New applications—e.g., context-sensing parking permits that check a driver's GPS location and authorized time window by way of a smart contract before raising a barrier, or logistics gateways that check resource-constrained IoT sensors by way of permissioned ledgers—require adaptive architectures that trade off security, scalability, and convenience. To prevent data exposure, methods of improving privacy, such as selective disclosure and zero-knowledge proofs (ZKPs), are required; these, however, come with computation and further integration complexity. Key handling is a human problem: if humans misplace seed phrases or hardware wallets, recovery without compromising security entails the use of social-recovery protocols or threshold-signature schemes, which remain outside mainstream use.

Here we distil nine prominent studies to chart the shifting landscape of blockchain-based identity management. We introduce with a survey of architectural taxonomies that categorize network models and consensus protocols; move to Ethereum/IPFS prototypes demonstrating consent-based credential anchoring and tamper-detecting login flows; survey theoretical debates of self-sovereign identity; and cover specialized developments such as context-aware smart contracts, NFT-based diplomas, and hierarchical DID IoT networks. Interweaving case studies—from Estonia's e-Residency and MIT diplomas to smart parking and industrial sensor authentication—we anchor theoretical findings in deployed systems. We conclude by distilling leading design patterns, stating open questions in scaling, cross-chain interoperability, and regulation, and defining a modular reference architecture and research roadmap for facilitating a fully global, self-sovereign digital identity ecosystem.

2. Review of Literature

In the last decade, researchers have made efforts towards making a decentralized, user-managed model of identity become a reality that moves away from gigantic, centralized stores towards models in which the users own and manage their credentials. Early attempts in this direction were to examine existing identity management paradigms—rule-based models, federated identity, and public key infrastructures—and establish their inherent weaknesses regarding privacy, vulnerability to single-point failures, and limited control by the users. One of the early, formal investigations by Priscilla and Devasena [1] examined how the cryptographic chaining and distributed consensus properties of blockchain technology are able to effectively counter these weaknesses. Their survey classified blockchain networks into four categories—public, private, consortium, and hybrid—and contrasted some of the consensus protocols such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (pBFT), and Delegated PoS (DPoS) on their latency, throughput, and energy consumption. With a clearly defined classification of network models and the resulting trade-offs in consensus protocols, they demonstrated blockchain's intrinsic ability to eliminate the need for single-point trust, while cautioning that different instantiations—public vs. permissioned—must find their own balance between decentralization and operational efficiency.

Following these thorough architecture analyses, several innovative groups built end-to-end working prototype systems to prove the feasibility of identity based on blockchain technology. Chanchad *et al.* [2] presented one of the first full-stack demonstrations that merged Ethereum smart contracts with IPFS, a decentralized peer-to-peer file system. In their architecture, user documents—such as official identification provided by governments and academic transcripts—are stored in IPFS, with immutable content identifiers (CIDs) stored on top of the Ethereum blockchain. Access requests are facilitated by MetaMask, a browser extension that asks users to approve or reject each disclosure. This architecture—implying off-chain storage for valuable or sensitive content in combination with on-chain anchoring for integrity—has since become a model for secure document sharing across industries. Furthermore, their prototype logged each transaction in a local Ganache test environment, providing an auditable record for regulators or auditors. Although they did not display formal security proofs or rigorous performance analyses, their work demonstrated the value of blockchain to facilitate consent-based identity sharing.

Concurrently, Latha, Abinaya, and Keerthana [3] investigated the use of blockchain primitives in the direction of securing even lightweight web-based authentication streams. They substituted conventional SSH and one-time password (OTP) mechanisms with a micro-block chaining strategy based on Python. Every OTP is segmented into small blocks that are linked in a hash chain through SHA-512, with the last hash of a block being used as the first hash of the next. A Flask web interface checks for chain integrity prior to access, rejecting any authenticated OTP. The system does not necessarily involve global consensus or distributed ledger persistence, but it is a proof of concept of how cryptographic chaining—a fundamental blockchain primitive—can protect login streams even in low compute environments. Their findings indicated sub-second verification latency, which indicates that integrity-based authentication can be ported to legacy applications with little disruption.

Apart from prototype development, researchers have critically evaluated if blockchain technology is truly needed to self-sovereign identity (SSI). van Bokkem *et al.* [4] provided the first systematic comparison of SSI implementations on blockchain (uPort, Sovrin, ShoCard) and their non-blockchain alternatives. They compared each model against eleven criteria based on Allen's SSI principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization, protection, and provability. They formulated the conclusion that blockchain by nature satisfies the conditions of persistence and transparency—defined by immutable records and verifiable consensus—whereas non-blockchain wallet systems can match or outperform blockchain in minimalization and privacy because they store no data on a global ledger. The research finally concluded that, in low-risk applications like gaming profiles or social media logins, secure local wallets with public key infrastructure (PKI) can be good lightweight SSIs. However, in high-risk areas like financial services or national identity, blockchain's auditability and distributed trust provide unique advantages.

A theoretical examination by Bamnote and Patil [5] around the new European Blockchain Services Infrastructure (EBSI) initiative issuing government IDs, diplomas, and legal documents on a shared blockchain platform. Their examination emphasized the complexities involved in the creation of cross-border trust frameworks, which require many member states, universities, and private organizations to agree on decentralized identifier (DID) methods, credential formats, and governance rules. They emphasized the necessity of standardized registries of trusted issuer DIDs—a federated trust registry—and promoted policy-based access controls built into smart contracts. Their examination emphasized that blockchain technology is not to be considered a plug-and-play model; rather, careful legal frameworks and operational governance are necessary for proper implementation at nation-state level.

Methods for reducing exposure of personal information have also become a feature of contemporary identity systems. Zero-knowledge proofs (ZKPs), first introduced for anonymous transactions in cryptocurrencies, enable a user to verify membership in a set (e.g., "I am over 18") without exposing the underlying data (actual birthdate). Priscilla and Devasena [1] deployed age-verification ZKPs on Ethereum, citing their IPFS anchor model. Zaghdoudi *et al.* [9] subsequently incorporated ZKPs into their IoT DID resolver, with gateways needing to expose only public keys and minimal metadata to devices that submit valid cryptographic proofs. These innovations illustrate how privacy and data minimization can be embedded directly into credential processes, a primary requirement for GDPR and other data protection acts compliance.

As real-world settings become more complex, researchers have proposed "context-aware" identity schemes. Moidu *et al.* [6] began "Proof-of-Context" credentials, introducing time windows, geofences, and purpose codes to the metadata of Verifiable Credentials. Their Ethereum smart contract calls upon decentralized oracles (e.g., Chainlink) to fetch real-time GPS coordinates, timestamps, and external risk scores. Access requests are only allowed if the real context satisfies the credential's in-built policies, a suitable solution for use, for example, in smart parking: a city issues a parking permit as a blockchain-encrypted credential that only works in specific zones and business hours. Chainlink latency was 1.5 seconds per context request on average in testing, plus 0.5 seconds for on-chain verification—suggesting that fine-grained policy enforcement is possible but relies on trusted oracles. Although context-aware credentials are superior in dynamic use cases, non-fungible tokens (NFTs) provide an easy solution for long-term credential issuance. Lakshmi *et al*. [7] leveraged the ERC-721 standard on Ethereum to issue NFT diplomas for university graduates. The metadata of each NFT refers to an off-chain transcript in IPFS or a secure object store, and token ownership represents credential validity. Employers check an applicant's diploma by simply checking the NFT contract for token ownership and metadata hash—no phone calls or faxing documents. Led by MIT in 2017, this practice has been followed by Portuguese and Northern European universities. NFT-backed credentials enable revocation (token burn) and seamless integration into Web3 environments, albeit with gas fees on mainnet still being a bottleneck for large-scale credential issuance.

Constrained devices also present an identity challenge. Most sensors are not able to execute full blockchain nodes, but need to authenticate each other in industrial applications. To bridge this gap, Zaghdoudi *et al.* [9] suggested hierarchically structured DID network in which strong edge gateways execute Hyperledger Besu under pBFT consensus. Constrained devices create local key pairs and send DID registration requests to gateways using lightweight mesh protocols. Gateways batch DID anchor to a permissioned ledger and serve as resolvers for device-to-device authentication. When two sensors want to exchange encrypted commands, they request each other's public keys and credential revocation status from the gateway—obtaining mutual authentication in less than 500 milliseconds. Formal proofs against Dolev–Yao-style attackers ensure authenticity, replay protection, and ledger finality, demonstrating the applicability of blockchain to industrial IoT identity.

These nine pieces collectively map the rapid development of blockchain-based identity management. Initial taxonomies and surveys of consensus yielded to proof- of-concept demos on Ethereum and Python chains, setting out initial patterns of on-chain trust anchors and off-chain data storage. Theoretical analysis sharpened our insight into where blockchain provides critical value for SSI and where lighter wallet cryptography is adequate. Context-aware and NFT-anchored credentials enriched the dynamic policy enforcement and long-term record issuance toolkit. Hierarchical DID registries on private ledgers opened new avenues for resource-constrained IoT deployment. By these developments, the space has coalesced around a modular architecture: DIDs anchored on distributed ledgers, off-chain credential stores, smart contracts encoding issuance and access policies, and optional privacy modules for ZKP or selective disclosure.

But there are hurdles yet to clear. No one system yet properly addresses global scale: public blockchains are not yet up to handling the billions of daily DID resolution and credential-issuance transactions envisioned for a universal identity fabric. Cross-chain interoperability between Ethereum, Cosmos, Polkadot, and private consortia is in its infancy, dividing the identity landscape. Human-friendly key management—seed phrases, social recovery, hardware enclaves—is too techie for mainstream use. And regulatory compliance with "right to be forgotten" could be at odds with the immutable nature of blockchains.

Table 1: Comparative Analysis of Key Research Contributions in Blockchain-Based Decentralized Identity Systems

Paper No.	**1**	**2**
Authors (Year)	Priscilla & Devasena (2021)	Chanchad *et al*. (2022)
Domain / Use Case	Generic Digital Identity & KYC	Web-based KYC Document Management
Blockchain Type & Consensus	Public/Private/Consortium/Hybrid – PoW/PoS/pBFT/DPoS	Ethereum Testnet (PoW)
Storage Pattern	Off-chain IPFS + On-chain hashes	IPFS + Smart-contract anchors
Identity Model & Data Model	DID Documents + Verifiable Credentials	CID-anchored VCs
Privacy / Protection	Zero-Knowledge Proofs for minimal disclosure	User consent via MetaMask
Real-world Example	Estonia e-Residency	Ganache audit logs
Performance / Evaluation	Conceptual only	Gas ~50 000–150 000/anchor; UX delays
Key Limitations	No prototype	Gas fees; no formal security analysis
Paper No.	**3**	**4**
Authors (Year)	Latha *et al*. (2021)	van Bokkem *et al*. (2019)
Domain / Use Case	Blockchain-Inspired Web Login (OTP)	SSI Framework Analysis
Blockchain Type & Consensus	Custom Python chain (PoA-style)	Wallet-local vs. blockchain
Storage Pattern	On-chain OTP hash chain	Local wallets vs. on-chain DIDs
Identity Model & Data Model	OTP integrity chain (SHA-512)	SSI (DID + VC)
Privacy / Protection	Cryptographic hashing (SHA-512)	Minimal disclosure in wallet-only models
Real-world Example	Flask login demo	Estonia hybrid e-Residency
Performance / Evaluation	<1 s OTP verify	Theoretical only
Key Limitations	No distributed consensus	No perf. data
Paper No.	**5**	**6**
Authors (Year)	Patil & Bhosale (2023)	Moidu *et al*. (2025)
Domain / Use Case	Consensus & Future ID Trends	Context-Aware Credentialing
Blockchain Type & Consensus	Survey of PoW/PoS/pBFT/DPoS	Ethereum (PoW) + Chainlink
Storage Pattern	N/A	On-chain metadata pointers
Identity Model & Data Model	High-level ID architectures	VCs + embedded context
Privacy / Protection	N/A	Geofence, time-window, purpose codes
Real-world Example	N/A	Smart-parking permits
Performance / Evaluation	N/A	Oracle 1.5 s + on-chain 0.5 s
Key Limitations	Survey only	Oracle reliability; latency
Paper No.	**7**	**8**
Authors (Year)	Lakshmi *et al*. (2021)	Bamnote & Patil (2023)
Domain / Use Case	NFT-Anchored Academic Credentials	SSI & EBSI Review
Blockchain Type & Consensus	Ethereum Mainnet (PoW)	Survey of EU SSI frameworks
Storage Pattern	On-chain ERC-721 metadata + off-chain docs	Conceptual trust registries
Identity Model & Data Model	NFT diplomas	SSI frameworks
Privacy / Protection	Immutable token proofs	Federated consent models
Real-world Example	MIT blockchain diplomas	EBSI ID pilots
Performance / Evaluation	High gas; transfer delays	N/A
Key Limitations	Gas fees; wallet complexity	Governance only
Paper No.	**9**	
Authors (Year)	Zaghdoudi *et al*. (2024)	
Domain / Use Case	IoT-Optimized DID Networks	
Blockchain Type & Consensus	Private pBFT (Hyperledger Besu)	
Storage Pattern	Permissioned ledger + storage	
Identity Model & Data Model	Hierarchical DID via gateways	
Privacy / Protection	ZKP for DID resolution; gateway privacy	
Real-world Example	Industrial sensors	
Performance / Evaluation	DID reg ~1.3 s; verify <0.5 s	
Key Limitations	Gateway dependency	

3. Conclusion

The rapid development of blockchain-based identity management over the past decade is a collective effort towards rebuilding trust, openness, and user control in digital identity systems. Traditional paradigms—governments, banks, or tech giants controlling user credentials centrally—have repeatedly succumbed to data breaches, black-box consent models, and limited interoperability. The nine works surveyed in this paper illustrate how blockchain and its cryptographic primitives can reshape that paradigm.

Priscilla and Devasena's early categorization determined the types needed: public, private, consortium, and hybrid networks, each of which is accompanied by consensus algorithms that range from energy-hungry Proof-of-Work to lighter pBFT alternatives. All such design choices affect the decentralization, performance, and governance of the ledger. In the meantime, the need to store large identity documents—passports, diplomas, and medical records—using IPFS and other off-chain storage technologies has become an imperative, while smart contracts on Ethereum and other platforms can only protect the integrity-proofs of vital significance.

Chanchad *et al*.'s and Latha, Abinaya, and Keerthana's prototype deployments translated these blueprints into functional prototypes. The former's end-to-end DApp—integrating MetaMask-driven consent requests with on-chain CID anchoring—demonstrates an efficient KYC procedure in finance. The latter's light Python chain illustrates that even in compute-constrained settings, blockchain-driven integrity checks can safeguard login flows without centralized servers. These proofs of concept set the stage for more advanced identity systems.

Theoretical analysis conducted by van Bokkem *et al*. and by Bamnote and Patil has significantly enhanced our comprehension of Self-Sovereign Identity (SSI). Their analysis demonstrated that although blockchain is superior in providing persistence and auditability, wallet-based secure SSI can yield equivalent outcomes as blockchain when it comes to restricted data exposure and user control in low-risk environments. Estonia's hybrid scheme of e-Residency, and Europe's EBSI program, are perfect examples of how blockchain-based SSI can coexist with legacy registries in well-coordinated governance systems.

With the arrival of identity ecosystems, tokenization and context have been significant additions. Moidu *et al*.'s "Proof-of-Context" credentials place temporal, spatial, and purpose restrictions on Verifiable Credentials, enforced by oracles and smart contracts. This path is already being piloted for context-constrained parking passes and event tickets. NFT-based credentials, shown by Lakshmi *et al*., allow for the issuance and verification of academic diplomas using ERC-721 tokens, allowing graduates globally to exchange immutable, verifiable credentials without paper. MIT's blockchain diplomas and similar initiatives in Europe demonstrate the feasibility of NFT-based identity records.

Lastly, resource-constrained IoT systems require a separate solution. Zaghdoudi *et al*.'s hierarchical DID network employs edge gateways with permissioned pBFT ledgers acting as a proxy for actuators and low-power sensors. A two-tier solution introduces new devices registering DIDs through light mesh protocols using consensus and DID resolution being left to gateways. Industrial benchmarks—1.3 seconds to register a DID, sub-second to verify—show that blockchain can secure IoT device identity at scale, with formal security proofs ensuring authenticity and liveness.

Although these are phenomenal advancements, issues linger. Billions of daily identity transactions will necessitate scalable Layer-2 solutions, sharding, and state channels specific to DID and Verifiable Credential anchoring. Cross-chain interoperability will need to extend beyond siloed DID approaches; standardized bridges and shared trust registries to guarantee a credential issued on one chain is verifiable on another. Human-centric key management will demand simpler seed-recovery protocols—social guardians, threshold signatures, secure enclaves—without compromising security or privacy. Context oracles must become decentralized, reputation-based networks to prevent single-point dependencies. Regulatory compliance with data privacy regulations—GDPR's right to erasure, CCPA's data portability—requires hybrid designs that leverage on-chain immutability and off-chain reaction or chameleon-hash mechanisms.

To put next-generation identity solutions in the limelight, we recommend a layered reference architecture. On the Application Layer, domain-specific portals orchestrate user flows for credential issuance, presentation, and context gating. The Agent Layer consists of wallet/agent SDKs wrapping key management, DID method negotiation, and privacy policy enforcement. Registry Layer provides Layer-2 smart contracts for DID registration, credential anchoring, revocation lists, and context policy execution, with high throughput and low fees. The Storage Layer depends on decentralized object stores (IPFS, Filecoin) for off-chain documents and oracles for context feeds. Finally, the Consensus Layer uses public PoS or DPoS networks for global DID visibility and permissioned pBFT clusters for enterprise domains. Each layer needs to offer plugin interfaces—for other DID methods, credential schemas, oracle adapters, and governance modules—enabling federated identity ecosystems in finance, healthcare, government, and IoT.

In total, identity governance with blockchain technology has progressed from theoretical frameworks to real-world applications demonstrating its feasibility and potential for revolution. However, realizing the vision of global unified, self-sovereign digital identity requires coordinated advances in scalable infrastructure, interoperability standards, user-centricity, and regulatory frameworks. By adopting a modular, multi-layered architecture and doing serious research on Layer-2 registries, cross-chain bridges, and simple-to-use key recovery protocols, the research community can drive the development of digital identity solutions that are actually secure, privacy-respecting, and in the hands of the users they are supposed to represent.

4. References

1. Unique Identification Authority of India (UIDAI) Data Breach Coverage. Business Standard. 2018.
2. Priscilla CV, Devasena T. Blockchain based identity management system: a survey. International Journal of Engineering Research and Applications. 2021;11(5):29-36.
3. Chanchad N, Limbani D, Silveira J, Singh H, Dsilva P. Identity management using blockchain technology. International Research Journal of Engineering and Technology. 2022;9(5):n/a.
4. Latha R, Abinaya S, Keerthana R. Blockchain based authentication system. International Research Journal of Engineering and Technology. 2021;8(4):n/a.
5. van Bokkem D, Hageman R, Koning G, Nguyen L, Zarin N. Self-sovereign identity solutions: the necessity of blockchain technology. arXiv preprint arXiv:1904.12816. 2019.
6. Moidu J, J S, Raj N, Jebaraj S. Blockchain technology for identity management. International Journal for Multidisciplinary Research. 2025;7(3):n/a.
7. Lakshmi SS, Emmanuel KA, Kathiravan R, Nagaraj S. Digital identity verification using blockchain and non-fungible tokens (NFTs). International Journal of Research and Analytical Reviews. 2021;8(4):n/a.
8. Bamnote A, Patil RY. Identity management using blockchain – a review. International Journal of Darshan Institute on Engineering Research and Emerging Technologies. 2023;12(1):n/a.
9. Zaghdoudi B, Bu G, Potop-Butucaru M, Fdida S. Blockchain-based decentralized identity system: design and security analysis. arXiv preprint arXiv:2405.00000. 2024.
10. World Wide Web Consortium. W3C decentralized identifiers (DID) v1.0, candidate recommendation. World Wide Web Consortium; 2022.
11. Government of Estonia. Estonia e-Residency program

overview. e-Residency Portal; 2024. Available from: https://www.e-resident.gov.ee/ [accessed 2024].

12. MIT Media Lab. Blockchain diplomas. MIT Registrar's Office; 2017.
13. Chainlink. Decentralized oracle network documentation. 2024. Available from: https://docs.chain.link/ [accessed 2024].
14. Hyperledger. Hyperledger Besu documentation. 2024. Available from: https://besu.hyperledger.org/ [accessed 2024].
15. Buterin V. On public and private blockchains. Ethereum Blog. 2015 Aug.
16. Allen C. The path to self-sovereign identity. Alacrity Blog. 2016 Apr.
17. Andrews TD, *et al*. Decentralized identity: where have we been and where are we going? IEEE Security & Privacy. 2022;20(2):22-31.
18. Buterin V. Ethereum: a next-generation smart contract and decentralized application platform. Ethereum Whitepaper. 2014.
19. Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM. 2018;61(7):95-102.
20. Cameron K. The laws of identity. Microsoft Identity Architectures. 2005 May.
21. Sabz R, Dinakar A, Kumar SP. Zero-knowledge proofs for privacy-preserving authentication. Journal of Cryptographic Engineering. 2019;9(3):145-158.
22. Stornetta S, Bayer D. Improving the efficiency and reliability of digital time-stamping. In: Seventh Annual Symposium on Information Sciences and Systems; 1994 Mar.
23. Narayanan A, *et al*. Bitcoin and cryptocurrency technologies. Princeton: Princeton University Press; 2016.
24. Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials. 2016;18(3):2084-2123.
25. Loss A, Younger A. Challenges in IoT identity management. International Journal of Internet of Things. 2023;10(1):12-23.
26. Reed D, Grant T. Sovrin: a self-sovereign identity network. Sovrin Foundation Whitepaper. 2018 Mar.
27. Sherwood M. ISO/IEC 27017: code of practice for information security controls. International Organization for Standardization; 2015.
28. Braithwaite TB. Legal frameworks for digital identity. European Data Protection Law Review. 2018;4(2):140-152.
29. European Commission. Regulation (EU) 2016/679—General Data Protection Regulation. Official Journal of the European Union. 2016.
30. Mühle M, Grüner A, Gayvoronskaya T, Meinel C. A survey on essential components of a self-sovereign identity. Computer Science Review. 2018;30:80-86.
31. Hardt D. The OAuth 2.0 authorization framework. RFC 6749, Internet Engineering Task Force. 2012 Oct.
32. Dolev D, Yao A. On the security of public key protocols. IEEE Transactions on Information Theory. 1983;29(2):198-208.
33. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008.
34. Mazières D. The Stellar consensus protocol: a federated model for internet-level consensus. Stellar Development Foundation; 2015.
35. Karari JE, Ismail F, Wright ASP. Attribute-based encryption for decentralized identity. Journal of Systems Architecture. 2020;105:102643.