Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability

Vikas Prajapati[1]

[1]Independent Researcher

Publication Date: 2025/03/26

Abstract: Blockchain technology, a decentralized and immutable ledger, has transformed identity and access management (IAM) by enhancing security, privacy, and trust in digital ecosystems. Ensuring safe authentication and data integrity is made possible by its integration with sophisticated cryptographic techniques like zero-knowledge proofs (ZKPs) and public-key infrastructure (PKI). Other methods include verifiable credentials (VCs) and decentralized identifiers (DIDs). This paper provides a comprehensive analysis of blockchain-based IAM systems, comparing leading blockchain platforms, including Ethereum, Hyperledger Indy, IOTA, and IoTeX, in identity management. The role of blockchain in mitigating identity-related threats, such as identity theft and unauthorized access, is explored through decentralization, immutability, and smart contract automation. Additionally, key security enhancements, including cryptographic mechanisms that strengthen decentralized identity solutions and privacy-preserving authentication, are examined. The potential of blockchain to establish a self-sovereign identity framework that fosters trust, scalability, and security in digital identity ecosystems is highlighted, paving the way for the next generation of identity management solutions.

Keywords: *Blockchain, Decentralized Identity (DID), Security, Privacy, Interoperability, Identity Management, Digital Identity, Smart Contracts.*

How to Cite: Vikas Prajapati (2025). Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability. *International Journal of Innovative Science and Research Technology*,
10(3), 1011-1020. https://doi.org/10.38124/ijisrt/25mar1062

I. INTRODUCTION

A blockchain, as it pertains to IAM systems, is a decentralized database that reliably documents transactions over a dispersed network of computers. There is revolutionary potential for this invention to strengthen security and confidence in IAM approaches, and it has its origins in the financial and digital realms [1]. Blockchain goes beyond ordinary identity management frameworks by using structural narratological ontology in conjunction with business ontological systems. Therefore, it markets itself as a semantic web-based approach to effective and secure IAM. Digital identity and access management are about to undergo a sea change as blockchain technology is integrated into IAM frameworks. This new framework will be more robust, decentralized, and reliable, and it will change the way security is perceived and implemented [2].

Modern systems need Identity Management (IDM) to be secure and private. The contemporary healthcare system is a huge field that may include a great deal of very sensitive patient data in a variety of formats [3]. In order to fully utilize this data, administrators, doctors, patients, and other healthcare professionals must always work together in a sophisticated manner. Consequently, identity management is just as important to this system because it houses all of the personal medical data. Traditional Identity Management institutions (IDMS), which are centralized and overseen by central authorities acting as identity providers, are employed by the majority of healthcare institutions [2].

Identity owners cannot stop others from using their data or prevent their own identities and privacy from being exploited as a result. Above all, establishing interoperability between various services is a difficulty. Self-sovereign identification (SSI), a decentralized identification based on blockchain, can establish a foundation of trust by granting users ownership and control over their identities [4]. The Issuer, the Identity Owner or Holder, and the Verifier are the three primary players in a decentralized ecosystem who work together to establish a trust triangle for the decentralized system. Two cornerstones of decentralized identification, Verifiable Credentials (VC) and Decentralized Identifiers (DID), lay the groundwork for owner-controlled, distributed ledger-based, verifiable digital identities [5].

For the safekeeping of patient information, both the IDMS and the EHR play an essential role. The key security requirements for medical systems are the following: document non-repudiation, auditability, privacy, authentication, and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1062

access limits. In addition to security requirements, usability and functionality factors should be considered, including scalability, interoperability, and the convenience of use while administering the system IDs. Because of the possibility of identity theft or misuse, users can be reluctant to divulge the sensitive information needed for medical care. The middlemen used in traditional IDMS can be removed with decentralized identity management (DIM).

The increasing reliance on digital identity systems across various sectors has raised concerns regarding security, privacy, and interoperability. Conventional, centralized identity management systems sometimes have issues with fraudulent access, data breaches, and identity theft. Concerns about privacy and difficulties in complying with ever-changing legislation like GDPR stem from consumers' lack of agency over their personal data. Blockchain-based decentralized identity (DID) systems offer a promising solution by enabling self-sovereign identity, cryptographic security, and transparent authentication mechanisms. Regulatory acceptability, interoperability across blockchain networks, and scalability are three obstacles that these systems must overcome. This study aims to provide a comprehensive survey of security, privacy, and interoperability in blockchain-based decentralized identity systems, analyzing existing frameworks, challenges, and emerging solutions to enhance trust, usability, and widespread adoption.

The paper is structured as follows: Section II covers blockchain-based decentralized identity concepts and platforms. Section III discusses security aspects, including cryptographic techniques and threats. Section IV addresses privacy concerns and challenges. Section V explores identity verification and authentication mechanisms. Section VI examines interoperability and standardization. Finally, Section VII presents the conclusion and future research directions.

II. FUNDAMENTALS OF BLOCKCHAIN-BASED DECENTRALIZED IDENTITY

Blockchain technology allows for the decentralization, transparency, and immutability of data records through the use of distributed ledgers [6]. It keeps track of an ever-expanding list of cryptographically protected transactions in a timestamped, sequential blockchain [7]. To make sure the data is unchangeable and verifiable, cryptographic techniques are used in every block [8]. The distributed ledger technology known as blockchain keeps all network nodes in sync and the data current because of its decentralized design [9]. Each block in a blockchain is connected to the one before it using cryptographic hashes, as shown in Figure 1. Because changing one block would need changing all blocks that follow it, this chaining of blocks makes unauthorized adjustments extremely difficult, if not impossible, to do. Block numbers, hashes of blocks past and present, transaction details, and timestamps are the main data elements included in each block.

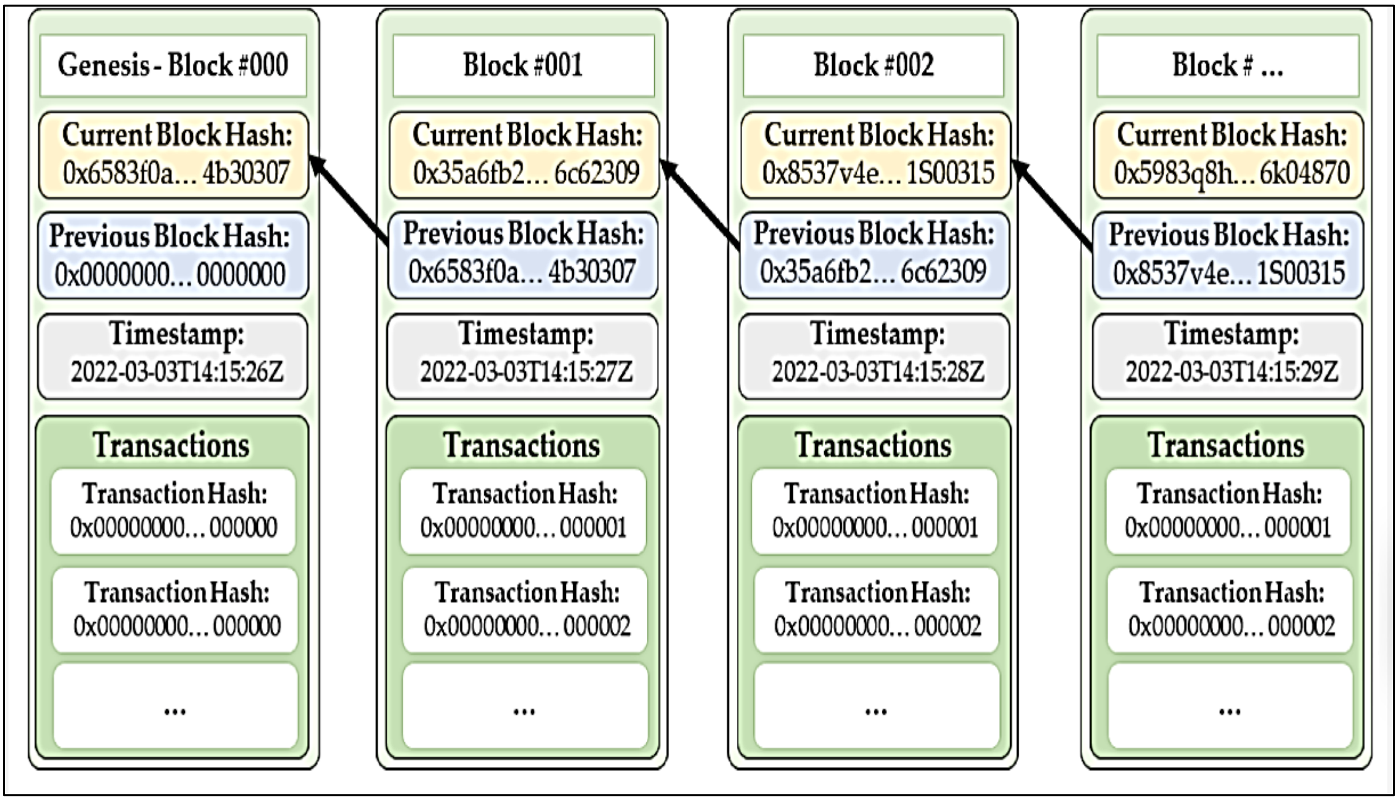

Fig 1 Representative Blockchain Structure.

The problems and restrictions of conventional centralized systems are tackled by the idea of a blockchain-based decentralized identification system. In a decentralized identity system, individuals are in complete control of their personal data and can autonomously administer their identities without the need for centralized authorities or intermediaries. Table I compares central identifiers, self-sovereign identification, and verifiable credentials as part of a decentralized identity system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1062

Table 1 Presenting the Core Components of a Decentralized Identity System using Different Aspects

Component	Definition	Function	Key Benefits	Challenges
Self-Sovereign Identity (SSI)[10].	Users have full control over their digital identities.	Enables users to manage, share, and authenticate identity data without intermediaries.	Enhances privacy, user autonomy, and data ownership.	Requires user education, adoption, and trust frameworks.
Decentralized Identifiers (DIDs)	Unique, blockchain-based cryptographic identifiers.	Provides a secure, persistent, and verifiable digital identity.	Eliminates centralized control, improves security.	Standardization, key management, and interoperability issues.
Verifiable Credentials (VCs)	Digitally signed claims about an individual or entity.	Allows selective disclosure of information while ensuring authenticity.	Tamper-proof, cryptographically secure, and privacy-preserving.	Revocation mechanisms, scalability, and credential storage.
Blockchain Ledger	A distributed and immutable record-keeping system.	Stores identity-related transactions in a decentralized manner.	Eliminates single points of failure and ensures transparency.	Scalability, high transaction costs, and regulatory concerns.
Smart Contracts	Self-executing contracts stored on the blockchain	Automates credential issuance, verification, and revocation	Reduces manual processes and enhances efficiency.	Security vulnerabilities and complex implementation.
Identity Wallets	Secure digital wallets for storing DIDs and VCs.	Enables users to manage and share identity data securely.	User-friendly, secure, and decentralized storage.	Risk of wallet loss, security breaches, and interoperability.

➢ *Blockchain Platforms for Decentralized Identity System*

- *Ethereum*

The Ethereum platform, created by Vitalik Buterin in late 2015, is a leading framework for creating decentralized applications (DApps) on the blockchain. The inclusion of Ethereum into IoT ecosystems aimed to solve the dual problems of bolstering the security of IoT devices and creating decentralized IoT networks. Results from studies demonstrating its use in sectors as diverse as agriculture, healthcare, transportation, finance, and supply chain management were consistent with this integration. The decentralized network, encryption mechanisms, smart contracts, and consensus algorithm that make up Ethereum are meticulously selected to provide strong security.

- *Hyperledger Indy*

Hyperledger offers a wide range of tools and frameworks designed to meet the specific needs of organizations and institutions, solidifying its position as a leading blockchain technology provider. Hyperledger Fabrics, Indy, Sawtooth, and Besu are among its frameworks [11]. Hyperledger contains the same components as Ethereum, including digital signatures and hashes, chain code, and zero-knowledge-proof (ZKP).

- *IOTA Blockchain:*

The IOTA platform uses a Directed Acyclic Graph (DAG) topology for its distributed ledger instead of a blockchain. Scalability, cheap prices, and safe data transmission between devices are its primary goals while designing it for the IoT environment[12]. Tangle Technology, Zero Fees, Decentralized Consensus, MAM (Masked Authenticated Messaging), IOTA Tokens (MIOTA), Smart Contracts (IOTA Smart Contracts - ISCP), Qubic, and Decentralized Identity (DID) are all essential parts of the IOTA platform [56].

- *IoTeX Blockchain*

The IoTeX blockchain technology was specifically designed to meet the demands of the IoT ecosystem [13]. The unique requirements of IoT devices and applications prompted its development as a solution to the problems encountered by existing blockchains. Notable features and components of the IoTeX blockchain platform [14].

III. SECURITY ASPECTS IN BLOCKCHAIN-BASED IDENTITY SYSTEMS

DID systems based in blockchain technology deliver improved security protection compared to conventional identity management approaches [15]. Cryptographic techniques combined with decentralized trust models in these systems work to eliminate threats that come from data breaches alongside unauthorized access and identity fraud. The analysis examines security threats that exist in conventional identity systems in addition to blockchain-based security improvements as well as cryptographic methods and the obstacles that decentralized identity frameworks face [16].

➢ *Security Threats in Traditional Identity Systems*

Security risks emerge when identity management systems operate from a central location because it create vulnerabilities which affect the system.

- *Single Point of Failure*

Identity databases that operate under central authority attract numerous cybercriminals who try to exploit them. A single security breach can reveal information about numerous millions of user credentials [17].

- *Identity Theft and Phishing Attacks*

Attackers take advantage of vulnerable authentication methods which produces unauthorized access and impersonation incidents [18].

- *Data Breaches and Unauthorized Access*

Frequent data leaks occur because of weak encryption alongside bad access controls and dangerous insider threats.

- *Privacy Violations*

Users hold restricted power to handle the storage as well as sharing and processing of their identity information at third-party service provider platforms.

- *Security Enhancement with Blockchain-based DID*

Blockchain-based decentralized identity systems address traditional security concerns through:

- *Decentralization:*

Eliminates central authorities, reducing the risk of single-point failures. Identity data is distributed across a blockchain network[19].

- *Cryptographic Security*

Identity attributes and credentials are secured using advanced cryptographic algorithms [20], ensuring data integrity and authenticity.

- *Immutability*

There is no way to change the immutable record of identity-related transactions stored on the blockchain.

- *User Control and Self-Sovereignty*

Individuals have complete ownership of their digital identity, minimizing reliance on third-party intermediaries.

- *Verifiable Credentials (VCs)*

Users can choose which aspects of their identities to reveal without disclosing extraneous personal data.

- *Smart Contracts for Automated Identity Management*

Self-executing contracts enable secure identity verification, credential issuance, and revocation without manual intervention.

- *Cryptographic Techniques in Decentralized Identity*

Cryptographic techniques play a crucial role in securing decentralized identity systems by ensuring authentication, privacy, and data integrity [21].

- *Public-Key Infrastructure (PKI)*

The robust authentication mechanism in decentralized identity systems depends on Public-Key Infrastructure (PKI) which applies asymmetric cryptography. The system depends on pairs of public and private keys for its secure authentication process. Digital signatures act as essential tools for authentic verification and integrity assessment of digital credentials because this stops unauthorized interference and identity misrepresentation. Securing identity management systems becomes possible through Decentralized Identifiers (DIDs) which use exclusively created cryptographic keys to operate without requiring centralized authority control.

- *Zero-Knowledge Proofs (ZKPs)*

A decentralized identity system gains privacy benefits through Zero-Knowledge Proofs because users prove claims while shielding, it reveals specific sensitive information. Through its cryptography users can prove authenticity by maintaining full anonymity [22]. Users can strengthen their privacy by adopting selective disclosure because it enables them to reveal only age verification credentials while withholding other personal data. The privacy benefits of ZKPs enable digital identity users to remain protected from observation and tracking as well as misuse of their data during service interactions.

- *Homomorphic Encryption*

The data protection of decentralized identity systems improves through Homomorphic encryption because it enables computations on encrypted data without decryption requirements. Homomorphic encryption enables secure identity verification because it allows encrypted data processing without decryption to minimize data exposure risks [23]. The verification process becomes possible while maintaining full unauthorized access to users' sensitive information through privacy-preserving computation. Deputy director integrity systems gain operational security through homomorphic encryption which safeguards users' privacy and protects their data against regulatory requirements.

- *Potential Security Challenges and Attacks*

Despite their security benefits, decentralized identity systems face potential vulnerabilities that must be addressed.

- *Sybil Attacks*

Man-made internet manipulation occurs when cybercriminals establish numerous fake accounts to deceive network controls. To stop Sybil attacks the network requires proof-of-personhood mechanisms consisting of biometrics with reputation-based identity verification and rates that control new identity generation.

- *Key Management Issues*

Users who employ decentralized identity systems manage cryptographic keys which create vulnerabilities due to potential key misplacement and theft [24]. The protection of user identities becomes possible through secure recovery techniques combined with multiple signatures authentication so users can install Hardware Security Modules (HSMs) as protection.

- *Smart Contract Vulnerabilities*

Smart contracts automate identity management but can be exploited through code vulnerabilities and reentrancy attacks. Formal verification, rigorous auditing, and upgradeable contracts with security patches help safeguard identity-based blockchain applications [25].

IV. PRIVACY CONSIDERATIONS IN DECENTRALIZED IDENTITY SYSTEMS

The decentralized blockchain architecture is one of the most important proposed solutions to the centralized IDMS problem methods because of its robust security features and cutting-edge technologies. Several aspects of the blockchain, including its distributed ledger, peer-to-peer (P2P) communication, immutability, and others, can alleviate issues with existing central systems [26]. Ethereum and the smart

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1062

contract, two ground-breaking ideas introduced in 2013, helped to decentralize IDMs. Smart contracts eliminate the need for a middleman by enabling parties to conduct transactions and tasks directly with one another using self-executing software that runs whenever conditions are met. Blockchain technology has numerous advantages that can improve user privacy. The most crucial aspect is decentralization. Furthermore, the danger of a SPOF can be reduced by avoiding total reliance on a single authority. The user is shielded from dependence on third parties when it utilizes the blockchain, which means that their behavior cannot be monitored or studied. But there are still obstacles, including scalability, that blockchain technology must overcome despite its numerous benefits[27].

- *Privacy Risks in Blockchain-Based Identity*

The nature of blockchain technology makes it possible for transaction data to be broadly shared among all nodes, which might undermine the privacy of that data [28]. A number of cryptocurrency alternatives, such as Zerocash, have so evolved with the goal of improving privacy protection [29]. The zero-knowledge proof mechanism is what makes Zerocash possible to conceal the people involved and their transaction data [30]. Such cryptocurrencies abound as well, including Litecoin, Monroe [31], Zerocoin [32], and so on. User identity privacy protection involves not just individual users being concerned about the security of their personal data but also businesses being reluctant to provide rivals access to important company information [33]. For example, even if the Bitcoin transaction address is a pseudonym and does not divulge any personal information, there is still a need to ensure that Bitcoin transactions are secure. It is still possible for attackers to deduce personal identifying information by analyzing blockchain data, which includes details like ID and IP addresses, and then linking transactions to accounts. Scholars in this area have so put up several privacy safeguards.

- *Privacy-Enhancing Technologies*

PETs are methods and instruments that shield people's identities. To maximize data security and privacy while minimizing the quantity of personal data collected, used, and shared, enterprises can employ privacy-by-design principles, which are built into PETs, to include data governance practice [34].

- *Anonymization Techniques:*

Anonymization techniques are commonly employed to enhance privacy by changing the state of a dataset to remove subject identity while preserving its usefulness [35]. Smart healthcare systems may operate in a more secure environment and prevent critical patient data from escaping thanks to anonymity technology [36]. Big medical data may be anonymized in a variety of ways, with the most common ones centering on the k-anonymity, l-diversity, and t-closeness models of anonymity protection.

- *Cryptographic Techniques:*

The adoption of cryptographic techniques has prevented the leaking of people's private information in FL [37]. These techniques include zero-knowledge proofs, safe multi-party computing, and homomorphic encryption. To protect sensitive data during client-to-client parameter exchanges, FL employs homomorphic encryption, a type of encryption that enhances privacy[38]. This method involves encoding parameters before performing operations such as adding or multiplying.

- *Perturbation Techniques:*

To ensure the security of models and sensitive data, a perturbation strategy incorporates noise into the initial dataset. The data may be rendered differentially private [39] by introducing noise into the model parameters or data, and the parties are unable to ascertain whether a particular record takes part in the learning process or not. A popular perturbation method in FL frameworks, the differential privacy approach finds widespread use in medical applications [40][41]. This statistical probability model-based PET strategy aims to mask dataset data in order to protect healthcare data from inference attacks on FL frameworks and other types of data sensitivity[42].

V. INTEROPERABILITY IN BLOCKCHAIN-BASED IDENTITY

There are two methods by which blockchain networks can accomplish interoperability, depending on the kind of organizational integration. To begin, the interoperability of the BC system may be accessed, or any centralized organization can be improved or synchronized with the blockchain system. Secondly, the safe and rapid interaction at the local SDK level is enabled by the same BC network architecture that is organization-specific [43]. Hash and Merkel proofs will accompany every transaction relayed from a single blockchain network, establishing the transaction's legitimacy. Transactions are relayed and proof of legality is maintained via an intermediary blockchain network. Interoperability processes might differ depending on the application.

- **Structural Interoperability:** Permits data interchange without requiring systems to alter data format, which is useful for sharing information across related entities (e.g., healthcare, education, etc.).
- **Semantic Interoperability:** Makes it possible for the systems to understand the data as was. That data is same in both structure and meaning [44]. As an example, while numerical values are used to represent temperature, the units of measurement used are Celsius or Fahrenheit.
- **Process Interoperability:** Integrates company procedures to facilitate computer systems sharing a common understanding. To facilitate the rapid and consistent recording of patient information, for instance, healthcare providers should standardised business processes.

- *Blockchain-Based Interoperability Framework*

The elimination of middlemen in financial transactions between blockchain networks is made possible via interoperability. The blockchain network (BCN) is considered to be compatible with interoperable city services [45]. Figure 2, is an example of a blockchain-based interoperable services framework that eliminates the need for translation or downtime when consumers engage with various municipal services via BCN.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1062

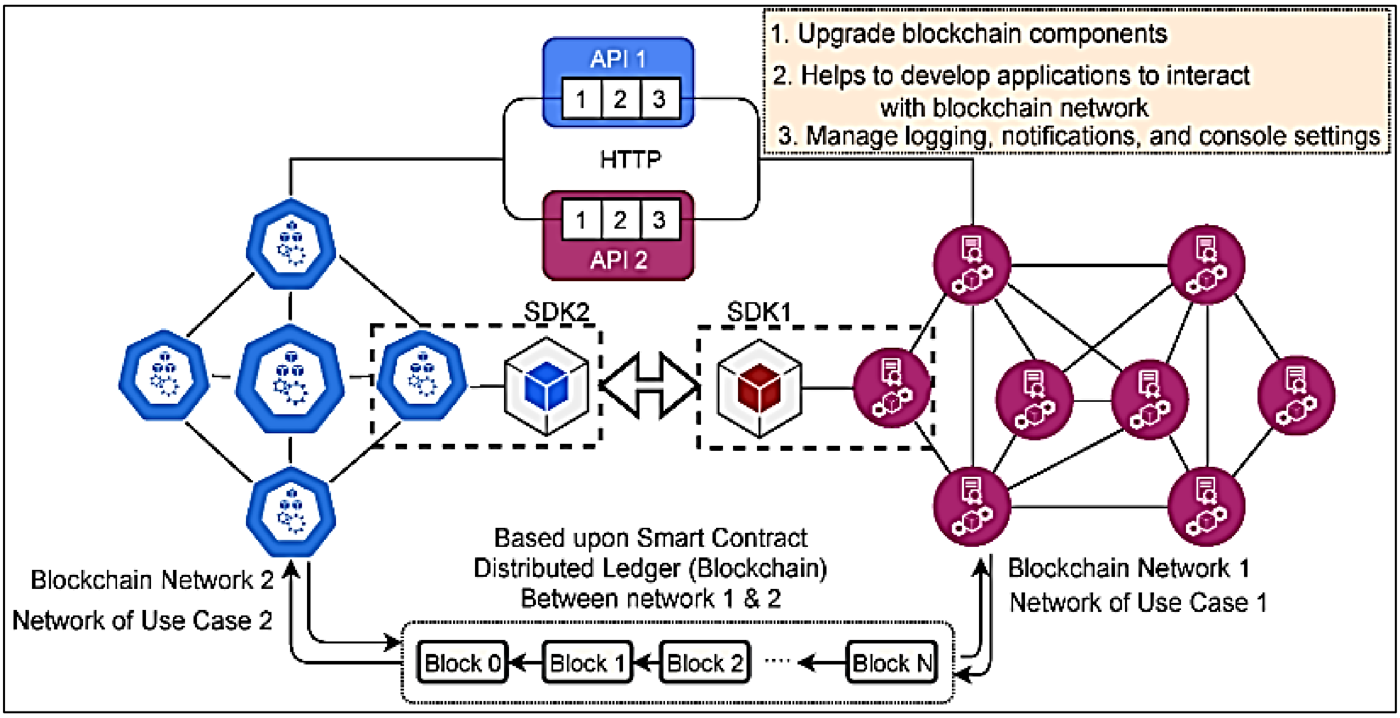

Fig 2 Blockchain-Based Interoperability Framework.

A system that can accommodate several chains and open protocols is suggested by the framework [46]. Blockchains may talk to one other directly, without the need for middlemen or trust procedures, due to the open protocol. The architecture's central BCN connects several organizations and serves as the P2P architecture's fundamental layer.

➢ *Challenges and Open Research Issues*

There are significant obstacles to interoperability due to the many blockchain protocols. The fundamental obstacle to a network that can communicate with one another is the fact that protocols differ in their fundamental technical aspects, such as their consensus models, transaction methods, smart contracts, and so on. The key to guaranteeing compatibility could lie in a number of standardization initiatives. Table 2 provides the future directions.

Table 2 Future Directions

Challenges	Details
Consensus Algorithm	The difficulties of cross-platform transactions can be reduced using a consensus method that is not dependent on any particular protocol.
Throughput	An ongoing issue in BC is the need for a scalable framework; more improvement in interoperability is possible.
Public and Private BC linkage	The process of interoperability can be accelerated; it defines a universal standard.
Block Structure	Block architectures are protocol-specific, making standardization a challenge when it comes to interoperability.

- Develop a new blockchain standard that mandates the use of current collaborative protocols. As an example, GS1 is a supply chain data standard developed by IBM and Microsoft that allows for interoperability.
- Along with the conventional block structure, you need also implement case-specific common and interoperable consensus procedures.
- Outline the corporate blockchain's common standards, such as its block structure and consensus mechanism [47].

VI. LITERATURE REVIEW

The literature review in this paper emphasizes how blockchain-based decentralized identification systems have become a viable way to improve security, privacy, and interoperability across a range of industries.

Polychronaki et al. (2024) analyze these studies side by side to determine how far down the DID implementation curve each is, to point out current obstacles, and to propose areas for future study at the crossroads of educational metaverse applications and decentralized identification. Entering the new era of Web 3.0, when user privacy and decentralized information are key, new technologies are changing the management of personal data. focuses on the metaverse's decentralized identity management (DID), notably in the field of education, which has quickly adopted digital technologies for e-learning, especially in the wake of the COVID-19 epidemic. A number of concerns around interoperability, security, and privacy have arisen in response to the growing integration of technologies like blockchain, AI, and VR/AR into educational systems [48].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1062

Kotey et al. (2024) show a way for blockchains to function together in a decentralized system. The decentralized nature of blockchains is preserved by this system. Data encryption and hash-based verification further guarantee the security of information transmitted across blockchains. Light client verification, which is based on Simplified Payment Verification, is utilized as an additional layer of security to guarantee that only legitimate transactions are added to the destination blockchain after consensus [49].

Hulea, Miron and Muresan (2024) explore the use of Hyperledger Fabric technology to create a DPP that will enhance product lifecycle management as part of the EU's strategy for a circular economy. Sustainable consumption and improved recycling habits may be achieved by the thorough product information that this research provides. This information should cover materials, origin, usage, and end-of-life instructions. This method takes use of the benefits of both the cheqd.io platform, which uses decentralized identifier (DID) technology for unique product identification, and the Hyperledger Fabric blockchain network, which is designed for enterprises for DPP data management. This integration improves security and efficiency [50].

Zhao, Zhong and Cui (2023) suggests a concept for smart home access management and authentication that uses decentralized identifiers (DIDs). A distributed environment is built by taking use of the blockchain-based DIDs' inherent decentralization, which effectively decreases an impact of the "single point of failure." Using DIDs and an enhanced capability-based access control scheme, this model makes it easy to authenticate users, simplify authentication, and grant them access to other homes with just one registration. All of this makes the smart home system more secure and convenient for everyone involved [51].

Sabrina, Li and Sohail (2022) provide an innovative method for managing devices' identities in blockchain-based IoT systems, which offer dual data security. The first is a simple time-based identification technique that validates data using hub identification. The second improvement is the incorporation of a powerful blockchain application into data storage, which allows for immutable data exchange and user-friendly access. They have successfully developed their prototype and found that it meets all of the system criteria. Additionally, they have demonstrated that their identity management strategy works well on blockchain platforms and can be used in large-scale settings [52].

Venkatraman and Parvin (2022) put out a method for managing computational assets in an IoT ecosystem that includes software, users, devices, and data operations using a blockchain framework. Within the context of a business case, they plan and execute the development of a proof-of-concept prototype that demonstrates the use of smart contracts on a distributed and federated blockchain platform to facilitate the safe authentication of IoT resources and operations and the highly trusted storage of associated data. The proliferation of the IoT has presented new security, privacy, and trust issues for identity management systems that have developed around outdated authentication methods and data modeling techniques [53].

Table 3 summarizes key aspects of decentralized identity management, highlighting their focus areas, key findings, challenges, and contributions in blockchain, IoT, and smart authentication systems shown below.

Table 3 Summary of Literature Review Based Decentralized Identity Systems

Study	Primary Focus	Technology Used	Application Area	Key Challenges Addressed	Proposed Solution
Polychronaki et al. (2024)	DID implementation in metaverse education	Blockchain, AI, VR/AR	Education (e-learning platforms)	Privacy, security, and interoperability in educational metaverse	DID-based identity management framework for e-learning
Kotey et al. (2024)	Decentralized blockchain interoperability	Blockchain, Hash-based verification, Simplified Payment Verification	Cross-blockchain communication	Secure, seamless blockchain interoperability	Hash-based verification, light client verification
Hulea, Miron & Muresan (2024)	DID-based product lifecycle management	Hyperledger Fabric, Decentralized Identifiers (DID), cheqd.io	Circular economy, product lifecycle management	Product traceability, recycling efficiency, security	DID-based DPP using Hyperledger for secure tracking
Zhao, Zhong & Cui (2023)	DID-based authentication and access control for smart homes	Blockchain, Capability-Based Access Control (CBAC)	Smart Homes	Single point of failure, cross-household access	DID-based authentication with CBAC scheme
Sabrina, Li & Sohail (2022)	Blockchain-based IoT identity management	Blockchain, Time-based identification protocol	IoT-based systems	Data security, scalability for large-scale IoT applications	Lightweight time-based ID protocol and blockchain storage

Venkatraman & Parvin (2022)	Blockchain-based ID management for IoT assets	Blockchain, Federated and Distributed Identity Management	IoT ecosystem (devices, software, users, operations)	Secure ID management in IoT, trust, authentication challenges	Federated blockchain ID system with smart contracts

VII. CONCLUSION AND FUTURE WORK

The drawbacks of conventional centralized frameworks are addressed by blockchain-based decentralized identity management systems, which provide a safe, open, and independent method of managing identity and access. By leveraging cryptographic security, decentralized identifiers, and verifiable credentials, these systems enhance user privacy, reduce identity fraud, and eliminate single points of failure. Additionally, the integration of smart contracts automates identity verification and credential issuance, further improving efficiency and security. Various blockchain platforms, such as Ethereum, Hyperledger Indy, IOTA, and IoTeX, provide robust solutions tailored to different identity management needs. The broad use of decentralized identification systems is contingent upon resolving issues with scalability, interoperability, and compliance with regulations. High computational costs and scalability concerns are two of the obstacles that blockchain-based identity management confronts, despite its advantages. Additionally, regulatory uncertainties and the need for widespread adoption hinder its seamless integration into existing systems. Future studies should focus on developing standardized protocols for interoperability, enhancing privacy-preserving techniques through zero-knowledge proofs, and ensuring seamless integration with existing identity management systems. Additionally, advancements in AI-driven identity verification and quantum-resistant cryptographic methods could further strengthen decentralized identity security. The development of safe and scalable blockchain-based identification solutions will depend on the concerted efforts of academics, government officials, and business leaders to tackle these issues as digital ecosystems progress.

REFERENCES

[1]. S. S. Galazova and L. R. Magomaeva, "The transformation of traditional banking activity in digital," Int. J. Econ. Bus. Adm., 2019, doi: 10.35808/ijeba/369.
[2]. N. Sfetcu, Philosophy of Blockchain Technology - Ontologies. 2019. doi: 10.58679/mm73548.
[3]. M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for ehealth identity privacy: State of the art and future perspective," Sensors (Switzerland). 2020. doi: 10.3390/s20020483.
[4]. S. Cucko, S. Becirovic, A. Kamisalic, S. Mrdovic, and M. Turkanovic, "Towards the Classification of Self-Sovereign Identity Properties," IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3199414.
[5]. N. Naik and P. Jenkins, "Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology," in ISSE 2021 - 7th IEEE International Symposium on Systems Engineering, Proceedings, 2021. doi: 10.1109/ISSE51541.2021.9582551.
[6]. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, October 2008," Cited on, 2008.
[7]. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," Ethereum Proj. Yellow Pap., 2014.
[8]. M. M. Merlec and H. P. In, "Blockchain-Based Decentralized Storage Systems for Sustainable Data Self-Sovereignty: A Comparative Study," Sustainability, vol. 16, no. 17, 2024, doi: 10.3390/su16177671.
[9]. F. E. Alzhrani, K. A. Saeedi, and L. Zhao, "A taxonomy for characterizing blockchain systems," IEEE Access, vol. 10, pp. 110568–110589, 2022.
[10]. S. Gulyamov and S. Raimberdiyev, "Personal Data Protection as a Tool to Fight Cyber Corruption," Int. J. Law Policy, vol. 1, no. 7, Sep. 2023, doi: 10.59022/ijlp.119.
[11]. H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge internet of things," Sensors, vol. 21, no. 2, p. 359, 2021.
[12]. K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, 2021, doi: DOI: 10.48175/IJARSCT-6268B.
[13]. Suhag Pandya, "Innovative blockchain solutions for enhanced security and verifiability of academic credentials," Int. J. Sci. Res. Arch., vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.
[14]. Y. Kareem, D. Djenouri, and E. Ghadafi, "A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things," Futur. Internet, vol. 16, no. 8, 2024, doi: 10.3390/fi16080285.
[15]. Suhag Pandya, "Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System," Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 865–876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.
[16]. M. Kuperberg, "Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective," IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1008–1027, 2020, doi: 10.1109/TEM.2019.2926471.
[17]. S. Murri, S. Chinta, S. Jain, and T. Adimulam, "Advancing Cloud Data Architectures: A Deep Dive into Scalability, Security, and Intelligent Data Management for Next-Generation Applications," Well Test. J., vol. 33, no. 2, pp. 619–644, 2024, [Online]. Available: https://welltestingjournal.com/index.php/WT/article/view/128
[18]. S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, p. 5, 2023.

[19]. S. Pandya, "A Systematic Review of Blockchain Technology Use in Protecting and Maintaining Electronic Health Records," Int. J. Res. Anal. Rev., vol. 8, no. 4, 2021.
[20]. S. Murri, "Data Security Environments Challenges and Solutions in Big Data," Int. J. Curr. Eng. Technol., vol. 12, no. 6, pp. 565–574, 2022.
[21]. K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," in 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020, 2020. doi: 10.1109/BRAINS49436.2020.9223312.
[22]. M. Alizadeh, K. Andersson, and O. Schelen, "Comparative Analysis of Decentralized Identity Approaches," IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3202553.
[23]. G. Zhao, B. Di, and H. He, "A novel decentralized cross-domain identity authentication protocol based on blockchain," Trans. Emerg. Telecommun. Technol., 2022, doi: 10.1002/ett.4377.
[24]. R. K, S. G, S. Kumar, and S. T, "A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies," Int. J. Innov. Res. Adv. Eng., 2023, doi: 10.26562/ijirae.2023.v1006.25.
[25]. A. Goyal, "Integrating Blockchain for Vendor Coordination and Agile Scrum in Efficient Project Execution," Int. J. Innov. Sci. Res. Technol., vol. 9, no. 12, 2024.
[26]. Abhishek Goyal, "Driving Continuous Improvement in Engineering Projects with AI-Enhanced Agile Testing and Machine Learning," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 1320–1331, Jul. 2023, doi: 10.48175/IJARSCT-14000T.
[27]. H. Alanzi and M. Alkhatib, "Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review," Appl. Sci., vol. 12, p. 12415, 2022, doi: 10.3390/app122312415.
[28]. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," J. Netw. Comput. Appl., vol. 126, pp. 45–58, 2019.
[29]. E. Ben Sasson et al., "Zerocash: Decentralized anonymous payments from bitcoin," in 2014 IEEE symposium on security and privacy, 2014, pp. 459–474.
[30]. S. Yuan, W. Yang, X. Tian, and W. Tang, "A Blockchain-Based Privacy Preserving Intellectual Property Authentication Method," Symmetry (Basel)., vol. 16, no. 5, 2024, doi: 10.3390/sym16050622.
[31]. A. Biryukov and S. Tikhomirov, "Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash," Pervasive Mob. Comput., vol. 59, p. 101030, 2019.
[32]. I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in 2013 IEEE symposium on security and privacy, 2013, pp. 397–411.
[33]. S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure : Ensuring Compliance and Security in Utility Systems," Int. J. Innov. Res. Creat. Technol., vol. 8, no. 2, pp. 1–8, 2022.
[34]. F. Mosaiyebzadeh et al., "Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey," Electronics, vol. 12, no. 12, 2023, doi: 10.3390/electronics12122703.
[35]. G. Dhiman et al., "Federated learning approach to protect healthcare data over big data scenario," Sustainability, vol. 14, no. 5, p. 2500, 2022.
[36]. V. S. Thokala, "Improving Data Security and Privacy in Web Applications : A Study of Serverless Architecture," Int. Res. J., vol. 11, no. 12, pp. 74–82, 2024.
[37]. A. Blanco-Justicia, J. Domingo-Ferrer, S. Mart\'\inez, D. Sánchez, A. Flanagan, and K. E. Tan, "Achieving security and privacy in federated learning systems: Survey, research challenges and future directions," Eng. Appl. Artif. Intell., vol. 106, p. 104468, 2021.
[38]. S. Arora and S. R. Thota, "Ethical Considerations and Privacy in AI-Driven Big Data Analytics," Int. Res. J. Eng. Technol., vol. 11, no. 05, 2024.
[39]. X. Xiao, G. Wang, and J. Gehrke, "Differential privacy via wavelet transforms," IEEE Trans. Knowl. Data Eng., vol. 23, no. 8, pp. 1200–1214, 2010.
[40]. Q. Li, Z. Wu, Z. Wen, and B. He, "Privacy-preserving gradient boosting decision trees," in Proceedings of the AAAI Conference on Artificial Intelligence, 2020, pp. 784–791.
[41]. S. Arora, S. R. Thota, and S. Gupta, "Data Mining and Processing in the Age of Big Data and Artificial Intelligence - Issues, Privacy, and Ethical Considerations," in 2024 4th Asian Conference on Innovation in Technology (ASIANCON), IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ASIANCON62057.2024.10838087.
[42]. S. Jordan, C. Fontaine, and R. Hendricks-Sturrup, "Selecting privacy-enhancing technologies for managing health data use," Front. Public Heal., vol. 10, p. 814163, 2022.
[43]. S. Lu et al., "CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle," Sensors, 2023, doi: 10.3390/s23041864.
[44]. S. Biswas, K. Sharif, F. Li, A. K. Bairagi, Z. Latif, and S. P. Mohanty, "GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data - A COVID-19 Perspective," IEEE Consum. Electron. Mag., 2021, doi: 10.1109/MCE.2021.3074688.
[45]. E. Abebe et al., "Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (industry track)," in Middleware Industry 2019 - Proceedings of the 2019 20th International Middleware Conference Industrial Track, Part of Middleware 2019, 2019. doi: 10.1145/3366626.3368129.
[46]. R. Neisse et al., "An Interledger Blockchain Platform for Cross-Border Management of Cybersecurity Information," IEEE Internet Comput., 2020, doi: 10.1109/MIC.2020.3002423.
[47]. S. Biswas et al., "Interoperability Benefits and Challenges in Smart City Services: Blockchain as a Solution," Electronics, vol. 12, no. 4, 2023, doi: 10.3390/electronics12041036.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1062

[48]. M. Polychronaki, M. G. Xevgenis, D. G. Kogias, and H. C. Leligou, “Decentralized Identity Management for Metaverse-Enhanced Education: A Literature Review,” Electronics, vol. 13, no. 19, 2024, doi: 10.3390/electronics13193887.
[49]. S. D. Kotey, E. T. Tchao, A. S. Agbemenu, A.-R. Ahmed, and E. Keelson, “A Framework for Full Decentralization in Blockchain Interoperability,” Sensors, vol. 24, no. 23, 2024, doi: 10.3390/s24237630.
[50]. M. Hulea, R. Miron, and V. Muresan, “Digital Product Passport Implementation Based on Multi-Blockchain Approach with Decentralized Identifier Provider,” Appl. Sci., vol. 14, no. 11, 2024, doi: 10.3390/app14114874.
[51]. X. Zhao, B. Zhong, and Z. Cui, “Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes,” Electronics, vol. 12, no. 15, 2023, doi: 10.3390/electronics12153334.
[52]. F. Sabrina, N. Li, and S. Sohail, “A Blockchain Based Secure IoT System Using Device Identity Management,” Sensors, vol. 22, no. 19, 2022, doi: 10.3390/s22197535.
[53]. S. Venkatraman and S. Parvin, “Developing an IoT Identity Management System Using Blockchain,” Systems, vol. 10, no. 2, 2022, doi: 10.3390/systems10020039.