JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Review on Blockchain-Based Decentralized Identity Management

[1]Prof.Mahesh Sonje, [2]Prof.Gauri Sonawane, [3]Prof.Kalyani Borse
[1]Assistant Professor, [2]Assistant Professor, [3]Assisatant professor
[1]Computer Science and Design
[1]MET Institute of Technology(P)-Btech ,Nashik

Abstract : This article examines how worldwide organizations are utilizing blockchain technology for decentralized identification (DID) management to enable safe access to information resources. The adoption of blockchain technology for enterprise applications like identity management has been difficult since it was first presented as a cryptocurrency. One of the more compelling use cases for blockchain adoption is DID. In contrast to conventional, central, or federated identity management models, DID use cases assist users across domains and industry pioneers better protect their personal data and application access control. The authors of this exploratory work use qualitative secondary case-based study research approach to comprehend the difficulties facing the existing state of digital identity management and investigate the potential advantages of DID as an emerging model for identity management. They thus put out a conceptual cube framework for examining and analyzing different DID systems. making a contribution to digitally secure identification theory and practice. Blockchain-based decentralized identity management offers a viable way to increase the scalability and security of healthcare systems. customary identity Because management systems are centralized, they are non-scalable, prone to attacks and data breaches, and a single point of failure. On the other hand, private can be protected while ensuring safe and transparent access to patient data using decentralized identity management built on the blockchain.With this method, patients maintain control over their personal health information while allowing medical staff to access certain data as necessary. We suggest BDIMHS, a permissioned blockchain-based decentralized identity management system for healthcare systems that integrates Hyperledger Aries and Hyperledger Indy. Further explanations of the necessary features are created, and high-level protocols for network startup, enrollment, registration, issuance, verification, and revocation are provided. features. With the use of selective disclosure, zero-knowledge proofs, decentralized identifiers, verifiable credentials, and zero-knowledge proofs, the suggested method enhances data security, privacy, immutability, interoperability, and patient autonomy. We also assess the security and performance of the suggested solution and talk about possible implementation issues in the healthcare industry.

***IndexTerms* -Distributed ledger technology, blockchain, interoperability, information security, and decentralized identity management,BDIMHS**

I. INTRODUCTION

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 [1]. 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 three main elements of the decentralized ecosystem that form the triangle of trust for the decentralized system are the Issuer, Identity Owner or Holder, and Verifier. Verifiable Credentials (VC) and Decentralized Identifiers (DID) are the two pillars of decentralized identity that form the basis of distributed ledger-based verifiable digital identities that are fully controlled by their owners [5]. The IDMS and the electronic healthcare system are crucial to each other since they handle healthcare data. The primary security criteria related to maintaining access restrictions, authentication, privacy, auditability, integrity, and non-repudiation of documents include with the medical systems. Functionality and usability criteria, such as scalability, interoperability, and ease of use when it comes to administering the system IDs, are in addition to security needs. 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). Our goal is to explore and test the viability of blockchain-based DIM and its potential application in healthcare systems, since end-user control is underemphasized in existing IDMSs. The area of decentralized identity management has gained significant attention and is considered extremely promising, with many advantages for healthcare applications. Decentralized identity management in electronic health systems was examined by Bouras et al. [1], with an emphasis on safeguarding private information. They contrasted the current options using the concepts of identity management. A symmetric key cryptography-based access control policy approach for Hyperledger-based healthcare data interoperability was presented by Tanwar et al. [6]. They examined blockchain-based EHR systems and assessed performance parameters.A blockchain-based decentralized identity management system with distinct health identifiers was presented by Javed et al. [3]. They assessed performance parameters and put a smart contract into action on Ethereum. A blockchain-based Personal Health Record (PHR) architecture with multi-party authorization and cryptographic threshold mechanisms was proposed by Madine et al. [7]. Off-chain storage was employed, and security and constraints were assessed. A permissioned blockchain-based identity management and user authentication system that satisfies medical security criteria and is resistant to many types of attacks was proposed by Xiang et al. [8] for e-health. Mikula and colleagues [9] presented a prototype of Hyperledger Fabric identification and access management for EHR based on blockchain. They highlighted healthcare institutions' adoption of private or consortium blockchain. BlocHIE, a blockchain-based platform for exchanging medical data that uses PHD-Chain and EMR-Chain to preserve healthcare data, was proposed by Jiang et al. [10]. For the purpose of meeting privacy and authenticity criteria, they integrated off-chain storage with on-chain verification. Using Aries and the Hyperledger Indy blockchain, Manoj et al. [11] presented a blockchain-based architecture for managing consent and patient verification. They evaluated current options using identity management concepts as a basis. A symmetric key cryptography-based access control policy approach for Hyperledger-based healthcare data interoperability was presented by Tanwar et al. [6]. They examined blockchain-based EHR systems and assessed performance parameters. A blockchain-based decentralized identity management system with distinct health identifiers was presented by Javed et al. [3]. They assessed performance parameters and put a smart contract into action on Ethereum. A blockchain-based Personal Health Record (PHR) architecture with multi-party authorization and cryptographic threshold mechanisms was proposed by Madine et al. [7]. They assessed security and constraints while utilizing off-chain storage. A permissioned blockchain-based identity management and user authentication system for e-health was introduced by Xiang et al. [8]. It is resistant to several types of assaults and satisfies medical security regulations. A prototype for the creation and validation of verified credentials for EHR access was presented by Mikula et al. [9]. A Decentralized Self-Management of Data Access Control (DSMAC) utilizing Role-based access control and DID-supported smart contracts was presented by Saidi et al. [12]. They concentrated on SSI's security needs within the healthcare system. In this work, we suggest a DIM that, by eliminating intermediaries and enabling users to govern their own healthcare identities, delivers sustainability, stability, availability, and security—the trust layer that is lacking across a variety of healthcare platforms. We introduce the BDIMHS scheme design for healthcare systems. We present an implementation of the Proof of Concept (PoC), perform a heuristic security analysis, and contrast the security and privacy objectives with other alternatives.[18]

II.Literature review

This is a review of the literature based on the given references:

Bouras, M. A. et al., 2020: The use of distributed ledger technology (DLT) to protect eHealth identity privacy is covered in this study. It probably gives a summary of how DLT applications are now being used in eHealth, emphasizing privacy issues and possible future paths.[1]

X. Xiang and associates (2022): This paper proposes a decentralized authentication and access control protocol designed especially for blockchain-based e-health systems. The protocol tries to solve issues with access control and security in these kinds of systems.[2]

Javed, I. T. et al. (2021). The study presents Health-ID, a decentralized identity management system built on blockchain technology and intended for remote healthcare. It probably goes over the features and design of Health-ID, highlighting how it improves security and privacy in situations involving remote healthcare.[3]

Cucko, V. et al. (2022): With its focus on categorizing self-sovereign identity aspects, this study is expected to shed light on the salient traits and attributes of DLT-based self-sovereign identity systems. It might aid in comprehending the fundamental ideas behind identity management in decentralized settings.[4]

P. Jenkins and N. Naik (2021): The Sovrin network, a distributed ledger-based self-sovereign identity system, is examined in this paper. The Sovrin network's architecture, security features, and possible uses in decentralized digital identity management are probably evaluated in this study.[5]

Tanwar, S. and others (2020): A blockchain-based electronic health record system designed for Healthcare 4.0 applications is suggested in this article. The design, application, and possible advantages of using blockchain technology to securely and effectively manage electronic health records may be covered.[6]

Madine, M. M., and others (2020): A completely decentralized multi-party consent management system for safely exchanging patient health records is presented in this study. It probably goes over the design, safety precautions, and privacy-friendly elements of the suggested system in an effort to guarantee safe data exchange in medical environments.[7] A permissioned blockchain-based identity management and user authentication approach for e-health systems is introduced in

X. Xiang et al. (2020) publication. It probably provides a thorough methodology or framework, with a focus on security and privacy, for managing identities and authenticating users in e-health contexts.[8] The literature review addresses a number of topics related to the use of distributed ledger and blockchain technology in eHealth systems, with a particular emphasis on data sharing, identity management, access control, security, and privacy. These research advance our knowledge of how Distributed Ledger Technology (DLT) may tackle important eHealth problems and open the door to safer and more effective healthcare systems.[8]

Mikula and Jacobsen, R. H. (2018): This study examines the use of blockchain technology for identity and access management in electronic health records. It probably will include the possible advantages and difficulties of applying blockchain technology to the protection and control of patient access.[9]

(2018) S. Jiang et al. The authors introduce BlocHIE, a blockchain-based network intended for the interchange of medical data. The design and features of BlocHIE are probably covered in this paper, which focuses on how blockchain technology might enable the safe and effective sharing of healthcare data across stakeholders.[10]

T. Manoj et al. (2022): For entity authentication in electronic health records, this study suggests a decentralized identification system based on blockchain technology. It probably goes over how the system was designed and put into practice, highlighting how it improves security and privacy when handling electronic health records.[11]

H. Saidi et al. (2022): The authors present DSMAC, a blockchain-based privacy-aware decentralized self-management system for health data access control. The privacy-preserving characteristics of DSMAC and its possible uses in healthcare data management are probably covered in this study.[12]

W3C (2022): Verifiable Credentials Data Model v1.1 and Decentralized Identifiers (DIDs) v1.0 are two new standards released by the World Wide Web Consortium (W3C). These specifications most likely include norms and recommendations for applying blockchain technology to the implementation of decentralized identity and verified credentials. [13][14]

Yang X. and Li W. (2020): The study introduces a blockchain-based digital identity management system that is zero-knowledge proof. It probably talks about using zero-knowledge proofs to improve security and privacy in blockchain-based digital identity management systems.[15]

Theodouli, A. et al., 2020: For the Internet of Vehicles (IoV) ecosystem, this work suggests an identity and trust management structure based on blockchain technology. It probably talks about the architecture and design of the framework, with an emphasis on how blockchain technology can make connections between infrastructure and automobiles safe and reliable.[16]

Tobias Looker and O. T. Sam Curren (2022): Presenting Didcomm Messaging v2.x, the authors most likely talk about a specification for DID-based decentralized messaging and communication. This research may shed light on the use of decentralized IDs for safe and compatible communication in a range of decentralized systems, including medical systems.[17]

In general, the study of the literature addresses a number of issues regarding blockchain-based identity and access management in the healthcare industry, such as standards, platform development, privacy, authentication, and access control.

III.Methodology

Research Design:
This study employs an exploratory case-based qualitative methodology, drawing guidance from Yin (2014) and Eisenhardt (1989). The case study approach is deemed suitable for gaining an in-depth understanding of contemporary, real-life phenomena, particularly those situated within their context where limited control can be exerted (Yin, 2014). Furthermore, case study research is recommended for exploring novel areas, such as information systems, where research is scarce (Benbasat et al., 1987). Consequently, this methodology aligns with the research's objective, which seeks to comprehend the characteristics and features of the emerging context of Decentralized Identifiers (DID).[19]

Case Selection and Analysis:
Utilizing multiple cases lays a robust foundation for theory development, facilitating generalizability and grounding in comparison to single-case studies (Eisenhardt & Graebner, 2007; Davis et al., 2007). Thus, seven cases were meticulously developed with the aim of achieving generalizability. The investigation employed thematic analysis, axial coding, and a rigorous validation process, emphasizing consensus among researchers to ensure the precision, reliability, and validity of the findings (Miles & Huberman, 1994).

Case Study Design:
The case study design adhered to replication logic, where each case underwent individual analysis before researchers conducted a cross-case analysis to delineate emerging common theoretical patterns (Yin, 2014). Unlike pure grounded theory approaches, this research strategy, as per Eisenhardt (1989), does not begin with a blank theoretical slate. Instead, it relates the cross-case analysis to existing theoretical constructs wherever feasible, and augments the theoretical linkages by identifying novel relationships within and between the constructs. The iterative nature of building qualitative theory is evident in the research design, facilitating a comprehensive understanding of the investigated phenomena.

IV.Conclusion

In summary, an exploratory case-based qualitative methodology was utilized in this study to examine the developing environment of Decentralized Identifiers (DID). The case study approach was determined to be suitable for obtaining a comprehensive comprehension of real-life phenomena that are immersed within their contextual restrictions, based on the recommendations of Eisenhardt (1989) and Yin (2014).

This study attempted to accomplish grounding and generalizability through the production of seven carefully chosen instances, providing a strong framework for theory building. The study employed axial coding, theme analysis, and a stringent validation procedure to guarantee the accuracy, dependability, and validity of the results.

Replication logic was used in the case study approach, whereby each instance was analyzed separately before researchers performed a cross-case analysis to find similar theoretical patterns. As opposed to strictly grounded theory methods, this In accordance with Eisenhardt's (1989) research methodology, new linkages were found within and between these constructs and previous theoretical constructs were merged when appropriate.

In general, this research advances knowledge about the traits and attributes of Decentralized Identifiers (DID) in relation to developing technologies. Through the use of a thorough approach, this study offers insightful information that can guide future advancements and uses in the decentralized identity management space.

V.REFERENCES

[1] 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, vol. 20, no. 2, p. 483, 2020.

[2] X. Xiang, J. Cao, and W. Fan, “Decentralized authentication and access control protocol for blockchain-based e-health systems,” Journal of Network and Computer Applications, vol. 207, p. 103512, 2022.

[3] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, “Health-ID: A blockchain-based decentralized identity management for remote healthcare,” Healthcare, vol. 9, no. 6, 2021.

[4] v. Cuˇ cko, v. Be ˇ cirovi ´ c, A. Kamišali ´ c, S. Mrdovi ´ c, and M. Turkanovi ´ c, “Towards the classification of ´ self-sovereign identity properties,” IEEE Access, vol. 10, pp. 88 306–88 329, 2022.

[5] N. Naik and P. Jenkins, “Sovrin network for decentralized digital identity: Analysing a self-sovereignidentity system based on distributed ledger technology,” in 2021 IEEE International Symposium on Systems Engineering (ISSE), 2021, pp. 1–7.

[6] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” J. Inf. Secur. Appl., vol. 50, 2020.

[7] M. M. Madine, K. Salah, R. Jayaraman, I. Yaqoob, Y. Al-Hammadi, S. Ellahham, and P. Calyam, “Fully decentralized multi-party consent management for secure sharing of patient health records,” IEEE Access, vol. 8, pp. 225 777–225 791, 2020.

[8] X. Xiang, M. Wang, and W. Fan, “A permissioned blockchain-based identity management and userauthentication scheme for e-health systems,” IEEE Access, vol. 8, pp. 171 771–171 783, 2020.

[9] T. Mikula and R. H. Jacobsen, “Identity and access management with blockchain in electronic healthcare records,” in 21st Euromicro Conference on Digital System Design, DSD’18. IEEE Computer Society, 2018, pp. 699–706.

[10] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, “BlocHIE: A blockchain-based platform for healthcare information exchange,” in IEEE International Conference on Smart Computing SMARTCOMP. IEEEComputer Society, 2018, pp. 49–56.

[11] T. Manoj, K. Makkithaya, and V. Narendra, “A blockchain based decentralized identifiers for entityauthentication in electronic health records,” Cogent Engineering, vol. 9, no. 1, p. 2035134, 2022.

[12] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras, and J. H. M. Emati, “DSMAC: privacy-awaredecentralized self-management of data access control based on blockchain for health data,” IEEE Access, vol. 10, pp. 101 011–101 028, 2022.

[13] W3C, “Decentralized identifiers (dids) v1.0,” 2022, https://www.w3.org/TR/did-core/.

[14] ——, “Verifiable credentials data model v1.1.” W3C, 2022, https://www.w3.org/TR/vc-data-model/.

[15] X. Yang and W. Li, “A zero-knowledge-proof-based digital identity management scheme in blockchain,” Comput. Secur., vol. 99, p. 102050, 2020.

[16] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, “Towards ablockchain-based identity and trust management framework for the iov ecosystem,” in 2020 Global Internetof Things Summit, GIoTS 2020. IEEE, 2020, pp. 1–6.

[17] O. T. Sam Curren, Tobias Looker, “Didcomm messaging v2.x editor’s draft,” 2022, https://identity.foundation/didcomm-messaging/spec/.
[18] Ashish Singla, Management Development Institute, Gurgaon, India*Decentralized Identity Management Using Blockchain: Cube Framework for Secure Usage of IS Resources,2023
[19] Blockchain-based Decentralized Identity Management for Healthcare Systems Arnaf Aziz Torongo ID Mohsen Toorani ID