Proceedings of the Second International Conference on Applied Artificial Intelligence and Computing (ICAAIC 2023)
IEEE Xplore Part Number: CFP23BC3-ART; ISBN: 978-1-6654-5630-2

2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) | 978-1-6654-5630-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAAIC56838.2023.10140585

The Impact of Adopting Blockchain-based Identity Access Management: Current Applications and Potential Directions

1st S. Pl. Subramaniyan
Symbiosis Institute of Digital and Telecom Management
(of Aff.) Symbiosis International (Deemed University)
Pune, India
spl.subramaniyan2123@sidtm.edu.in

2nd Sandeep Prabhu
Symbiosis Institute of Digital and Telecom Management
(of Aff.) Symbiosis International (Deemed University)
Pune, India
sprabhu@sidtm.edu.in

***Abstract*—The aim of this study is to delineate how blockchain based identity access management (IAM) contributes to the creation of a more secure infrastructure by increasing the user data's transparency, accountability, and reliability while lowering the time and cost associated with providing services. This research employs a qualitative use case approach to gather and analyse data, and it compares traditional identity management to the identity management system based on blockchain in order to elucidate the advantages of blockchain-based IAM in an enterprise ecosystem. The findings suggest that the blockchain can act as a decentralized repository for identity data that can be verified and integrated into identity management, giving everyone in a company's network access to the same information about which credentials are legitimate and who has access to the database identification's legitimacy without disclosing the data itself. Blockchain-based IAM is a model that emphasizes a user-centric approach, by giving users full control over their digital identities. This may lead to increased concern among enterprises and organizations about trusting their users i.e., employees. Less attention is paid to the use of blockchain in information and cybersecurity. Therefore, his article helps enterprises by outlining best practices for implementing blockchain technology-based IAM and its benefits for gaining a competitive advantage.**

***Index Terms*—Blockchain, Identity access management, Decentralized identity**

I. Introduction

Identity and access management (IAM) refers to all the procedures and tools used by an organization to identify, authenticate, and grant access to its services and systems as well as those of other organizations that are connected to it [1]. By enabling more interoperability across departments and other institutions, a digital identity lowers the level of bureaucracy and speeds up operations within organizations. However, cybercriminals can become more intrigued if these digital identities are housed on a single centralized server. The current identity management system which is solely based on this principle is not trustworthy or safe. You are required to prove your identity at every turn using a variety of official documents, such as a passport, voter ID, or pan card. Sharing numerous IDs can result in data breaches and privacy issues.

The blockchain technology, also known as "Distributed Ledger Technology", refers to the technology underlying decentralized databases that gives entities control over how their data evolves through a peer-to-peer network while utilizing consensus algorithms to ensure replication across the network's nodes [2]. Transparency, security, and many other advantages provided by the blockchain technology enhance the value of various industries. As a result, it is ready to transform identity management in a very secure manner [3].

Each block where data is recorded cannot be modified, which is what makes blockchain safe. Only until the majority of the network has agreed, can one write to the blockchain. This means that in order to update a piece of information, all blocks added after it must also be changed, and 51% of the network must consent to the change [2].

The goal of this paper is to enhance knowledge of blockchain-based IAM. Therefore the primary objective of this research is to comprehend the shortcomings of traditional IAM in terms of privacy and security and to shed light on how Blockchain-based IAM may influence businesses by looking at various use cases.

II. Literature Review

The decentralized networked systems are drawing more and more attention solely because of its robust characteristics. The Blockchain, a decentralized structure, is a network of digitally stored data that is connected cryptographically by blocks of transactions [4] [5]. Due to its dispersion across the nodes of the network's participants, a blockchain does not require a single reliable authority. The problem of maliciously altering the data is resolved since the majority of the network's nodes have to validate each block before it can be added to the chain [19].

Blockchain is considered to be the prime technology in the industrial revolution 4.0 significantly because of its capability to provide anonymity, security, and business to a variety of sectors [8]. As a result, governments and organizations are working very hard to expand the business and the market that encompasses blockchain. Currently, blockchain technology is

TABLE I
BLOCKCHAIN BASED IAM VS. CONVENTIONAL IAM

Advantages of Blockchain-based IAM	Disadvantages of Conventional IAM
Decentralized and immutable ledger ensures data integrity and security	Centralized database creates a single point of failure and potential security vulnerabilities [1]
Smart contracts enable automated, secure, and transparent transactions	Manual processes can be slow and inefficient
Identity providers can issue and verify user identities on the blockchain	Identity verification is often manual and error-prone
Identity consumers can request access to user identities and access permissions on the blockchain [7]	Access permissions are often siloed and difficult to manage across multiple systems and applications
Greater transparency and auditability due to the public nature of the blockchain	Lack of transparency and auditability can lead to compliance issues
Increased efficiency and reduced costs due to automation and elimination of intermediaries	High costs and complexity associated with managing a centralized IAM system

widely used in sectors including finance, shipping, distribution, manufacturing, and utilities that demand dependability and stability [9]. Blockchain adoption is expanding, especially in sectors where data security and dependability are essential.

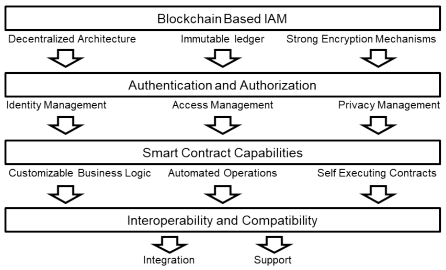

Fig. 1. Blockchain based IAM

This research explores the potential of a blockchain-based decentralized identity and access management system. Any IAM system's primary goal is to securely link the "identifier" and the "attributes" together. IAM systems in the past were centralized and managed by a single party. A "Trusted third party" provided the authentication and authorisation, a number of IAM models have previously been offered using this concept compromising the security [10].

IAM systems that are poorly built might exacerbate security issues already present and make it easier to gather personal data from users. A strong IAM system should have a balance of affordability, integrity, trustworthiness, and interoperability, according to experts [11].

Therefore, we have demonstrated how the blockchain-integrated IAM has the potential to be the engine that drives our identification and access management systems towards self-sovereign identity in this research through a few use cases. We have also shown how a data management system based on the principle of decentralization ensures maintenance of ownership and control over their data.

TABLE II
SYSTEMATIC LITERATURE REVIEW

No	Year	Title	Author
1	2019	BPDIMS: a blockchain-based personal data and Identity management system	Benedict Faber et al.
2	2019	A blockchain based identity management system considering reputation	Zhao and Liu
3	2019	Analysis of identity management systems using blockchain technology	Haddouti and Kettani
4	2019	Blockchain for identity management: the implications to personal data protection	Wie Liang Sim et al.
5	2020	Blockchain-based identity management systems: A review	Yang Liu et al.
6	2021	Identity and access management system based on blockchain identity	Ishaq Azhar Mohammed
7	2021	Blockchain based authentication for identity management	Hardjanto Nusantoro et al.
8	2021	Novel identity management system using smart blockchain technology	A. Shobanadevi et al.
9	2021	The practicality of adopting blockchain-based distributed identity management in organizations: a meta-synthesis	Mulaji and Roodt
10	2022	A systematic literature mapping on secure identity management using blockchain technology	Rathee and Singh
11	2022	Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey	Ahmed et al.
12	2022	DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data	Saidi et al.
13	2022	A Review on Blockchain Based Identity Management System	Hariharasudan and Quraishi
14	2022	Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review	Alanzi and Alkhatib
15	2022	The Changing Landscape of Identity and Access Management with Blockchain-Based Self-Sovereign Identity	Chawla and Gupta
16	2022	Blockchain-related identity and access management challenges:(de) centralized digital identities regulation	Mecozzi et al.
17	2022	Trust models for blockchain-based self-sovereign identity management: A survey and research directions	Lim et al.
18	2022	Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work	Satybaldy et al.
19	2022	Blockchain Technology: Applications and Open Issues	Das and Mishra

III. RESEARCH METHODOLOGY

Through apps and services, the digital and physical aspects of our lives are increasingly entwined. The various forms and applications of digital identity that we interact with serve as our physical representation in the digital world [12]. The trends listed below motivated this research and subsequent solutions to degree of security and trust required for technology future:

- The need to strengthen information security and process management to ward off cybercrime and identity theft.
- The ability of decentralization to benefit the individual.
- The desire for greater access to and efficiency in the delivery of social services as well as increasing economic

engagement.

This research utilizes a qualitative use case research methodology, where several use cases from different industries were examined in terms of how blockchain technology may be incorporated into enterprise identity access management solutions and the added commercial benefits. Whitepapers, articles, reports, and other online databases were used to gather the data for this study. The collected literature's relevance was then examined.

Case study research is based on in-depth , multi-faceted study that examines complex situations where it is difficult to distinguish between the phenomenon and the environment [13]. According to Gummesson (1981), the case study approach offers a number of benefits, including the capacity to fully comprehend the event or phenomenon under research and the capacity, given the numerous sources, to observe similar events and phenomena to the subject under study [14].

The following are the research questions answered by this study:

- Can users regain control over their identities and track how their data is utilized with blockchain-based IAM?
- Does blockchain-based identity management have unique use cases, and how does it differ from conventional IAM in terms of the advantages it offers to users in the business ecosystem?

IV. Analysis

A. Analysis of blockchain-based use cases for identity access management and its benefits

This section will examine various use cases for blockchain-based IAM applications, the concept of decentralized identity systems that underpins them, as well as the benefits of the application and how it affects business.

In order to perform the identification, authentication, and authorization of users who tries to access various services or systems within corporate resources, identity and access management (IAM) solutions are vital [15]. Access can relate to everything from users logging into software and staff setting up hardware to citizens using government services and all kinds of user verification, certification, and evidence. Several procedures fall under this category [16]. Identity attributes are the names given to identities, such as occupation, citizenship, affiliation with a service provider, eligibility for government benefits, and demography. These labels serve as evidence of who we are, not simply digital reproductions [17].

Blockchain is a distributed and decentralized database technology that also uses cryptographic techniques to ensure records are fraud proof. Through the use of timestamped messages and underlying cryptographic primitives such as hash functions and digital signatures, the blockchain creates globally verifiable proof of the presence or absence of records in the distributed database. This proof is always secure and computationally verifiable [18]. It has been regarded as a significant advancement in record keeping with applications that go well beyond cryptocurrencies that allows for the sequential storage and retrieval of data [19].

The following are the use cases that depicts how the aforementioned benefits of decentralized database technology are being leveraged into IAM systems:

B. Government Services- Adoption of Blockchain based IAM in South Korea

1) Background: A nation known for being a leader in the technology development and advances, South Korea has been aggressively experimenting with blockchain-based innovation. According to a study conducted by the United Nations on the state of digital governments amongst 193 UN members states globally, South Korea is ranked one amongst the top countries which renders humongous number of quality online services. The recent adoption of an amendment to South Korea's electronic signature law that eliminated the nation's public certificate system has raised expectations for the country's private certificate market as well as interest in mobile identification and decentralized identification based on blockchain technology. Decentralized Identity Alliance Korea Association and the a program for decentralized identity were recently established in South Korea [18].

2) Problem: Governments have long struggled with providing immediate access to services because of the strict requirements for fraud prevention and exhaustive physical identification verification. For an example, renewal of passport or driver's license typically involves going to a physical location, having your identity documents with you, and waiting in line, which is frustrating for people in the modern world [20].

As a result, South Korean government agencies intend to create digital ID cards that can be accessed via a mobile application and are issued and administered by a central national body. The provision of identity authentication services along with operational and statistical tools for the administration of service users in order to accomplish real-time identification utilizing identity data connected to the central government agency is another objective of incorporation of the identification and authentication system [21].

3) Solution Implemented: To solve this problem, South Korea's Ministry of Public Administration and Security established a decentralized blockchain based identity system. The chain code that Hyperledger employs is kept in a database using the hash map storage technique, which maintains information as key and value pairs. The DB level is used to represent these characteristics because its data format enables more flexible customization of the database design.

Through the chain code, a request for identification is made, and the identification details which are kept in the blockchain is then looked up to provide the answer [22]. Mobile ID cards go through digitally signed validation and private key-based validation, and the outcome is saved in the blockchain as a hash map, similar to what Level DB does. To avoid fraud and manipulation and to guarantee reliability, the data can be saved on the blockchain as a hash card if the status of a mobile ID card changes.

4) Benefits Achieved: Government services in Korea that use blockchain-based IAM have reduced overhead costs for customer service related to infrastructure, validation, customer support centres and more. This has improved information sharing across the nation and resulting in the annual saving of several hundred million dollars from tax payers, as well as improved customer service and satisfaction [20].

In the case of existing identity management systems, identity card data has been transmitted to a centralized system for authentication & verification by a governing commercial or official authority. Being open to various counterfeiting and hacking scenarios, it was difficult for individuals and organizations to develop trust in it. Hacking and counterfeiting issues have been transparently resolved by using blockchain technology in place of the centralized server that controls identification details across a network that is distributed [21]. Additionally, users are in charge of managing their own private information and making decisions on information sharing.

C. Health Care- A self-sovereign patient identity built on blockchain for the healthcare industry

1) Background: The healthcare ecosystem includes humongous participants which includes doctors, specialists, patients and insurers. Having total control over patient data was previously valuable to healthcare institutions [23]. Traditional methods store cross-organizational and intra-organizational data, as well as patient medical data, in sizable repositories in secure data centres. However, large healthcare data and the number of services and sources offering healthcare data are expanding dramatically as a result of the broad use of digitalization. Clinicians, hospitals, and other medical facilities currently record, exchange, and analyse health data using health information systems (HIS) [24]. Combining this patient data with the digital identity raises difficult problems as new sources, including wearables and mobile devices, have arisen.

D. Problem

As access rights to patient data frequently change hands between actors and traceability is essential in case of issues, healthcare providers need an unchanging and verifiable history. The risks due to security and the price to earn the trust are raised because of maintaining rights in a centralized server or database where one governing entity has control.

E. Solution Implemented

Asymmetric peer-to-peer networks with decentralized control are what make up blockchain-based identity systems. Each peer in an asymmetric cryptography network receives both private and public keys. The peer identification address is represented by the public key (or, more precisely, the public key hash), and the private key is used to decrypt the transactions connected to the public key [25]. DLT is the immutable and in these systems, when a block has been validated via a consensus mechanism, like a proof-of-stake, a number of new transactions are gathered from the block and added to the DLT [7] . The transactions associated to the earlier blocks are therefore more dependable and are therefore more generally accepted by the network since the blocks are linked and classified according to the time of their confirmation. Older blocks are more difficult to modify or remove transactions from. This is due to the fact that a hacker would have to alter both block n and the blocks that are linked to it (block nC1, block nC2, etc.) in order to alter or remove transactions in block n and avoid being detected. Decentralized architecture further ensures security by storing duplicate DLT data across all network nodes. Therefore, even if part of the network's data storage nodes is lost, DLT can still be recovered.

V. Benefits achieved

Accurate and verifiable identification of patients, providers, and organizations, such as hospitals, pharmacies, academic institutions, and other research organizations, is essential for achieving good health care outcomes. Blockchain makes secure ID possible and increases integrity and transparency while avoiding the production of multiple versions of IDs [26]. As data from wearable medical devices and the Internet of Things (IoT) start to flow, trustworthy data reconciliation with electronic health records, for instance, will become possible [3]. Blockchain-based IAM improves the accuracy and integrity of pertinent data by documenting each time a record is viewed or modified [26]. Healthcare providers must submit this precise and current information about their location and the services they offer, both personally and as a business.

VI. Discussion

A. Theoretical Implications

The aforementioned case studies demonstrate how current identity management systems communicate identification record information to a centralized server for authentication and verification via corporate or governmental authorities. Building trust in the system is difficult for people and businesses because it is prone to numerous hacking and counterfeiting incidents [27]. Additionally, by replacing the centralized server which handles the identification details across a network which is decentralized and by backing blockchain technology, problems with hacking and counterfeiting can be immensely eliminated. Users will also be able to manage their personal data and choose how it is being shared [28].

Although blockchain-based identity systems have several advantages, implementing blockchain still has a number of challenges:

- It is essential to do user research to discover whether people can perceptually understand what the decentralized identity management characteristic means provided that there is lack of knowledge and user experience with systems based on blockchain technology [23].
- The main barrier to develop new methods on building idensities that are secure and reliable is the absence of rigorous restrictions for processing and storage of personal data. A distinct responsibility breakdown and cooperation of the pertinent political and regulatory bodies are necessary for the deployment of technologies such

as blockchain in the public sector [3]. To maximize their application and usability, national laws and regulations must be instilled.

B. Research constraints

- Limited real-world applications: While blockchain-based IAM solutions have been created, there are currently only a few real-world use cases. As a result, it can be difficult to gauge the true impact of such solutions.
- Absence of standardization: Due to the absence of standardization in the blockchain industry, there are no standardized metrics or evaluation standards for evaluating the effectiveness of blockchain-based IAM solutions [2].
- Limited collaboration: Collaboration with stakeholders, such as businesses, developers, and regulators, can be crucial for the success of case study based research methodology. However, there is limited collaboration in progress of research and the adoption of blockchain-based IAM use cases and solutions respectively.
- Real-world testing limitations: Due to governmental, legal, and technical restrictions, testing blockchain-based IAM solutions in real-world scenarios are difficult. Additionally, there is less possibility to assess the solutions in practical context, necessitating the need for simulated testing environments.
- Limited resources: The number of blockchain-based IAM use cases explored are constrained by the amount of time, money, and technical expertise needed to do research on individual use cases.

C. Limitations of implementing blockchain based IAM

- Latency Size and Bandwidth: The latency, size, and bandwidth have all been significant sources of worry. Due to the small number of bitcoin transactions that occur each second, blockchain technology has a somewhat delayed response, and the system's processing speed is quite slow.
- Demand for blockchain talent: The blockchain developers and experts are highly in demand and it is imperative to educate and train the people who handle the systems based on blockchain as it primarily involves sensitive data.
- Scalability: Scalability is one of the biggest obstacles to implementing an IAM system based on blockchain. Blockchain technology is still in its early stages, and current systems can only handle a limited number of transactions per second. This is a major hurdle when it comes to implementing large-scale IAM systems.
- Interoperability: There are currently many different blockchain platforms available, each with its own protocols and standards. This makes it difficult to create a standardized blockchain-based IAM system that is interoperable with all platforms.
- Integration: Implementing a blockchain-based IAM system requires significant changes to existing infrastructure, which can be challenging and time-consuming. Integration with existing systems and applications can also be a challenge.
- Governance: Another challenge is establishing a governance model which assures the security and integrity of the system. Since blockchain systems are decentralized, it can be difficult to determine who is responsible for maintaining the system and enforcing rules and regulations.

D. Practical Implications

By enabling decentralization, which gives users control over their personal data, identity and access management solutions based on blockchain promise to drastically reduce the amount of personal and business data that is breached and pave the path to eradicate the illegal use of these data [16]. The suggested blockchain-based solution accelerates the identification process and makes an online service platform more user-friendly. Operational expenses can be immensely reduced by enhancing this identification methods, accelerating service delivery, and completely doing away with physical cards or tickets that need to be issued again after being lost [11].

Regarding the use of blockchain technology, there are still a few problems that need to be solved. The following are the first considerations to make:

- The latency, size, and bandwidth have all been significant sources of worry. Due to the small number of bitcoin transactions that occur each second, blockchain technology has a somewhat delayed response, and the system's processing speed is quite slow.
- The blockchain developers and experts are highly in demand and it is imperative to educate and train the people who handles the systems based on blockchain as it primarily involves sensitive data.

a) Blockchains: delayed response, System processing speed: low: Blockchain technology, while innovative, the latency, size and bandwidth have all been significant pieces of worry which results in relatively slow response time and processing speed. This is due to the decentralized nature of the system, where every node on the network must verify and agree on every transaction that occurs [6]. This process takes time, and as the number of transactions increases, so does the time it takes to process them. Additionally, the size of the blockchain grows with each transaction, making it more challenging to maintain and store the data.

Furthermore, the bandwidth available for blockchain transactions can also contribute to delays in processing speed. As the number of nodes on the network increases, the available bandwidth must be shared among them, leading to slower transaction processing times [6]. While efforts are being made to increase the speed and efficiency of blockchain technology, these limitations remain a significant source of concern for those looking to implement it on a larger scale.

E. Future Directions

To create a healthy digital identity environment, corporate technology must advance quickly. Leadership from the private and public sectors should encourage transparent and cooperative environments where ideas and innovations are shared with business for the good of the community [27]. However, they should most importantly establish criteria for both communication and quality. Additionally, they can have an impact by being adaptable in their approach to change and implementing digital transformation into their management and infrastructure practices. Institutions need to change their governance frameworks and practices instantly if they wish to play a more innovative and adaptable game [22].

VII. Conclusion

A literature review and explanation of use cases for implementing a real system in the public sector and healthcare were used in this study to present the advantages and disadvantages of management systems. blockchain-based identity. The findings of this study demonstrate how the implementation of a blockchain can considerably improve a user's ownership over their own data in terms of transparency, accountability, and dependability, while also speeding up and decreasing the cost of service delivery and eventually enhancing administrative effectiveness.

However, the implementation of this technology is difficult, and integrating new technologies in the public sector calls for a prolonged and cautious approach. Therefore, for blockchain-based identity access management being successfully incorporated into ecosystems, interdisciplinary research must go beyond the conventional technology based methodology and necessitate a profound comprehension of the political and economic ramifications.

References

[1] Chawla, M., & Gupta, S. (2022). "The Changing Landscape of Identity and Access Management with Blockchain-Based Self-Sovereign Identity". In ICT Infrastructure and Computing: Proceedings of ICT4SD 2022 (pp. 691-702). Singapore: Springer Nature Singapore.

[2] Das, S., Rout, J., & Mishra, M. (2022, March). Blockchain Technology: Applications and Open Issues. In 2022 International Co nference on Communication, Computing and Internet of Things (IC3IoT) (pp. 1-6). IEEE.

[3] Ren, Y., Zhu, F., Qi, J., Wang, J., & Sangaiah, A. K. (2019). Identity management and access control based on blockchain under edge computing for the industrial internet of things. Applied Sciences, 9(10), 2058.

[4] Mohammed, I. A. (2019). A systematic literature mapping on secure identity management using blockchain technology. International Journal of Innovations in Engineering Research and Technology, 6(5), 86-91..

[5] Mohammed, I. A. (2021). IDENTITY & ACCESS MANAGEMENT SYSTEM BASED ON BLOCKCHAIN. IDENTITY, 8(6).

[6] Mecozzi, R., Perrone, G., Anelli, D., Saitto, N., Paggi, E., & Mancini, D. (2022, August). "Blockchain-related identity and access management challenges:(de) centralized digital identities regulation". In 2022 IEEE International Conference on Blockchain (Blockchain) (pp. 443-448). IEEE.

[7] Hariharasudan, V., & Quraishi, S. J. (2022, April). A Review on Blockchain Based Identity Management System. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 735-740). IEEE.

[8] McDonough, S., & McDonough, S. (1997). Research methods as part of English language teacher education. English Language Teacher Education and Development, 3(1), 84-96.

[9] Lee, J. H. (2017). BIDaaS: Blockchain based ID as a service. IEEE Access, 6, 2274-2278.

[10] Rathee, T., & Singh, P. (2021). A systematic literature mapping on secure identity management using blockchain technology. Journal of King Saud University-Computer and Information Sciences.

[11] Lim, SY, Fotsing, PT, Almasri, A, Musa, O, Kiah, MLM, Ang, TF & Ismail, R 2018, 'Blockchain technology the identity management and authentication service disruptor: A survey', International Journal on Advanced

[12] Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019). BPDIMS: A blockchain-based personal data and identity management system.

[13] Yin, R. (1984). Case study research: Design and methods Sage Publications Beverly Hills.

[14] Gummesson, E., "Qualitative Methods in Management Research". Sage Publication, California, pp: 83-156, 1981

[15] Saidi, H., Labraoui, N., Ari, A. A., Maglaras, L. A., & Emati, J. H. M. (2022). "DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data". IEEE Access, 10, 101011-101028.

[16] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in Principles of Security and Trust, M. Maffei and M. Ryan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 164–186.

[17] Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey". IEEE Access, 10, 113436-113481.

[18] Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. Journal of Enterprise Information Management.

[19] Alanzi, H., & Alkhatib, M. (2022). "Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review". Applied Sciences, 12(23), 12415.

[20] Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. Technology Innovation Management Review, 7(10).

[21] Batubara, F. R., Ubacht, J., & Janssen, M. (2018, May). Challenges of blockchain technology adoption for e-government: a systematic literature review. In Proceedings of the 19th annual international conference on digital government research: governance in the data age (pp. 1-9).

[22] Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. Technology Innovation Management Review, 7(10). Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. Journal of Enterprise Information Management.

[23] Xiang, X., Wang, M., & Fan, W. (2020). A permissioned blockchain-based identity management and user authentication scheme for E-health systems. IEEE Access, 8, 171771-171783.

[24] Houtan, B., Hafid, A. S., & Makrakis, D. (2020). A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access, 8, 90478-90494.

[25] Mikula, T., & Jacobsen, R. H. (2018, August). Identity and access management with blockchain in electronic healthcare records. In 2018 21st Euromicro conference on digital system design (DSD) (pp. 699-706). IEEE.

[26] Satybaldy, A., Hasselgren, A., & Nowostawski, M. (2022). Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work. Blockchain in Healthcare Today, 5(Special Issue).

[27] Lim, S. Y., Musa, O. B., Al-Rimy, B. A. S., & Almasri, A. (2022). Trust models for blockchain-based self-sovereign identity management: A survey and research directions. Advances in Blockchain Technology for Cyber Physical Systems, 277-302.

[28] Alketbi, A., Nasir, Q., & Abu Talib, M. (2020). Novel blockchain reference model for government services: Dubai government case study. International Journal of System Assurance Engineering and Management, 11(6), 1170-1191.