International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Blockchain - Based Personal Identity Security System

Mohini Vasdeo[1], Sujal Arora[2], Vaibhav Sharma[3]

[1, 2, 3]Department of Computer Science and Engineering, Bachelor of Technology, SRM Institute of Science & Technology, NCR Campus, Delhi NCR Campus, Ghaziabad (U. P), India
[1]*mohinivasdeo[at]gmail.com*
[2]*sujal. iistst33[at]gmail.com*
[3]*vaibhavsharma. even[at]gmail.com*

Abstract: ***In today's digital ecosystem, where our identities are becoming increasingly integral to our sense of self, it has become crucial to preserve and manage identities as private data. The current centralized control of identity management raises concerns over privacy and security, leading to the need for a decentralized approach. Blockchain technology, which has gained popularity in the cryptocurrency industry, has emerged as a promising solution with its decentralized approach. Our major project aims to explore the use of blockchain technology in implementing a self - sovereign identity management system. Self - sovereign identity is a concept that allows individuals to take control of their own identities and manage them without relying on centralized authorities. In our project, we will provide a unified perspective of the core principles underlying self - sovereign identity, covering the components of identity proofs and authentication solutions for various self - sovereign identity implementations. We will analyze the various existing options and identify research gaps and obstacles involved in developing a comprehensive identity management system. We will focus on the architecture of a self - sovereign identity management system and discuss the relevant actors involved in such a system. We will explore how blockchain technology can be used to solve the problem of distributed user - centric identity. We will also examine how privacy can be ensured in compliance with legal mandates, such as the General Data Protection Regulation (GDPR). Our project will involve the development of a prototype system that will demonstrate the potential of a blockchain - based self - sovereign identity management system. The prototype will provide a proof - of - concept for the proposed system, highlighting the potential benefits and challenges of adopting a blockchain - based self - sovereign identity management system. Our project's conclusion will provide insights into the potential of this approach, highlighting the obstacles and trade - offs involved in developing a comprehensive identity management system.***

Keywords: Blockchain, Self - sovereign identity, Identity management, Decentralization, Privacy, Security, Authentication, Identity proofs, GDPR, Prototype

1. Introduction

As our identities become increasingly integral to our sense of self, Identity Management in the field of Information and Communication Technologies has become a crucial component in establishing our credibility. Because of this, it is crucial to preserve and manage identity as private data in order to forestall any unintended wrongdoing. Managing centralized control on identity appears to be permissive in the current state of the digital ecosystem as it pertains to how individuals are represented. Blockchain technology has recently made its mark as a revolutionary approach to exceeding expectations with its decentralized approach. Blockchain technology, which has recently gained traction due to its use in the crypto - currency industry, has the potential to significantly alter the identity management landscape as well. Privacy safeguards are especially important in the identity management space. However, there has been little systematic research into how the identity management feature of blockchain technology helps ensure privacy in compliance with legal mandates.

The current identity management ecosystem has been under scrutiny due to rising surveillance and security breaches that threaten user privacy. Businesses collect massive amounts of customer data in order to tailor their services to individual customers. This information is then used for economic development, population analysis, and other predictive and profiling purposes. Users are often in the dark about the service provider's collection and use of their personal information. Users have minimal say over how their data is used and shared because identity management and personal identity information (PII) are handled by centralized authorities. Additionally, due to the collection of PII, service providers become the primary target of attacks, security breaches, and privacy exploitation.

In this work, we give a unified perspective of the core principles underlying self - sovereign identity. This view covers the components of identity proofs and authentication solutions for a variety of self - sovereign identity implementations, among other topics. We went over an overview of the many methods to identity management, including an introduction to the architecture, a discussion of the relevant actors involved in such a system, and a look at how blockchain technology can be used to solve the problem of distributed user - centric identity. In conclusion, we will analyze the many existing options, highlight the research gaps, and comment on the obstacles and trade - offs involved in the process of developing a comprehensive identity management system.

2. Literature Survey

[1] With the growth of e - health, more countries have achieved progress in electronic medical treatment. Trends include digitizing medical equipment and structuring electronic medical records. Medical data's rapid rise will

increase it's worth making people's lives easier. Obviously, safely storing so much data is a pressing issue. Medical data's uniqueness necessitates strong privacy protection. Data privacy requires a secure solution. Many methods use single - server architecture, which has some inherent flaws (such as single - point faults). Blockchain can fix such issues, however, privacy protection is lacking. This study proposes a medical data privacy protection system that uses blockchain, group signature, and asymmetric encryption to enable accurate medical data sharing and patient data privacy. This paper verifies its security and privacy criteria theoretically and practically through system implementation.

[2] The Internet has transformed business, education, healthcare, and banking. Internet connectivity simplifies daily life. The Internet can uniquely identify machines, not people, hence a method to identify entities on the Internet is needed. On the Internet, service providers keep usernames and passwords on a central server. These servers become honeypots for hackers to steal user identification information, and service providers can use data mining and AI to profit from it. The self - sovereign identification system is a blockchain - based, decentralized, user - centric identity system managed by the identity owner. This article will examine blockchain - based self - sovereign identification implementations such as Sovrin, Uport, EverID, LifeID, Sora, and SelfKey, as well as their architectural components and use cases.

[3] Bringing actual documents to register is a bother. If lost, the process is slowed and can lead to identity theft. This article aims to create a blockchain - like decentralized system to allow registered users to access their personal data. This system serves user, authority, and third - party consumers (requester). Most systems are vulnerable to big data breaches. Blockchain technology, like Aadhaar, may fix this problem, according to some study. This initiative proves that blockchain identification helps society take ownership of their personal data. Most blockchain research focuses on business storage, but personal identities should also be digitized. An individual - owned identity verification system will boost data trust.

[4] Identity fraud is fatal. The method used to create and authenticate legal papers is to blame. An individual must convince the authorities to issue an identification paper by providing all supporting evidence. This technique is vulnerable because it gives the identification document issuer power. Sharing an identity proof copy is also required for authentication. Often, dishonest people receive identity proofs. This can lead to socially harmful identity document misuse. Blockchain is a trustless, decentralized network that anyone can utilize. Putting personal IDs on blockchain solves the identity management challenge. A blockchain - based system has been suggested to securely create, manage, and verify identification and credentials. Only identity owners can share pertinent information. Thus, identity fraud will be prevented.

[5] As our identities become increasingly integral to our sense of self, Identity Management in the field of Information and Communication Technologies has become a crucial component in establishing our credibility. Because of this, it is crucial to preserve and manage identity as private data in order to forestall any unintended wrongdoing. Managing centralized control on identification seems to be permissive in the current state of the digital environment as it pertains to how individuals are portrayed. Blockchain technology has recently made its mark as a revolutionary technique to exceeding expectations with its decentralized approach. Blockchain technology, which has recently gained traction due to its use in the cryptocurrency industry, has the potential to significantly alter the identity management landscape as well. Privacy safeguards are especially important in the identity management space. While identity management in blockchain technology is essential for meeting the requirements of regulations, there has been little systematic research into this topic. In this research, we want to address this knowledge gap by conducting a systematic evaluation of the literature on whether or not the identity management functionality of blockchain technology helps or hurts privacy in the context of the General Data Protection Regulation (GDPR).

[6] In order to ensure the safety of users' and businesses' online information, a blockchain - based insurance system is presented. This system offers two different insurance service models: one for users' private information and the other for businesses' sensitive data. Proof of claims is stored on the blockchain and updated automatically to ensure its integrity. Insurers and policyholders can quickly and easily establish mutual trust through the use of smart contracts.

[7] Even secured communication between people, services, and devices through centralized digital organizations is risky in the digital revolution. Service providers' centric solutions duplicative, insecure, and inconvenient. The self - sovereign Identity idea, which incorporates the individual's unified digital identity and authenticated qualities, empowers data users to own and learn from their data. Distributed digital identities must be authenticated and verified for privacy and security. This paper presents a cohesive vision of self - sovereign Identity, encompassing identification and authentication solutions for distinct solutions. Identification management techniques, architecture, actors, and blockchain technology for distributed user - centric identity were discussed. Finally, we review existing solutions, research gaps, and identity management system problems and trade - offs.

3. Problem Definition

In today's Internet - driven age of knowledge, identity management has moved to the forefront of importance due to the widespread use of digital identities by a vast population. Since most people today spend considerable time online and make use of many services that can only be accessed through the Internet, most of them now have a digital identity. While the current techniques of identity management have been developed with the success of service providers in mind, they have proven inefficient for users who must remember a plethora of different passwords to gain access to the various websites they need.

Self - sovereign identities that make use of decentralization are now possible thanks to the development of blockchain

technology. Despite this progress, bugs continue to be a problem. None of the currently available solutions are capable of satisfying the needs of flexibility required for digital identities to be used across a variety of online services. However, in the real world, an individual can demonstrate their identification using a variety of documents in addition to their Aadhar card. These systems are only able to handle Aadhar management.

4. Methodologies

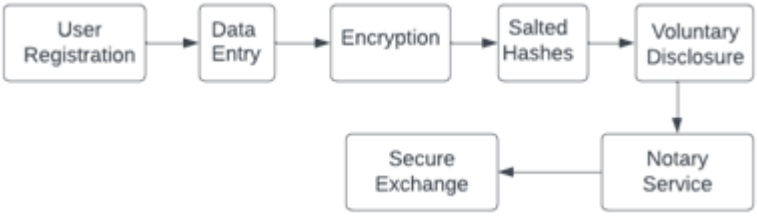

Figure 4.1: System overview of the proposed system

1) Module 01: Identity Management Module

a) The Identity Management Module is a crucial component of a Blockchain - based Personal Identity Security System.
b) It administers identity data storage, access, and sharing on the blockchain network.
c) It enhances security features by encrypting and storing sensitive user data on the blockchain.
d) It verifies users' identities through various authentication procedures, including biometric authentication and digital signatures.
e) It allows users to update and regulate access to their data.
f) It employs cutting - edge cryptographic methods and protocols to prevent the misuse or alteration of sensitive user information.
g) It provides a decentralized system that eliminates the need for a centralized authority to maintain and regulate identification data.
h) It offers users complete control over their identification data.

2) Module 02: Blockchain Security Module

a) The Blockchain Security Module ensures secure and decentralized storage and management of personal identification data.
b) Access control is the foundation of the security suite, which includes public - key cryptography and two - factor authentication.
c) Encryption techniques, such as symmetric and asymmetric encryption, are used to secure data transmissions.
d) Data integrity is maintained through the use of hash functions to create a unique digital fingerprint for data.
e) Auditability is provided through a distributed ledger, which records transactions permanently and openly.

3) Module 03: Access Control Module

a) Access control is an essential component of a blockchain - based personal identity security system's security module.
b) The access control module includes several smaller modules that work together to ensure the security of user - identifying information.
c) Authentication is the primary component that requires multi - factor authentication to verify a user's identity.
d) Authorization limits access to sensitive information by defining user roles and accompanying permissions using role - based access control.
e) Decryption uses public key cryptography to encrypt and decrypt identification data.
f) Access Control Auditability records and documents all access to time - sensitive identification information in an immutable and auditable format using distributed ledgers.
g) The access control module ensures that only authorized parties have access to personal identifying data stored on the blockchain.

5. Results

Blockchain - based personal identity security systems have shown promise in improving the security and privacy of personal identity data. These systems use decentralized ledgers and smart contracts to manage identity data, enforce rules and procedures, and provide a transparent audit trail of all transactions. Studies have found that these systems can effectively manage and secure identity data, while allowing for granular access controls and verifying identities without the need for centralized authorities. The systems use a combination of biometric and other identity data stored on the blockchain to verify the identity of users while maintaining their privacy and security.

Blockchain - based personal identity security systems are effective in preventing identity theft and fraud by using decentralized ledgers and smart contract technology. However, challenges still exist in implementing these systems, such as the need for large and diverse datasets for training and ensuring the system does not perpetuate biases or stereotypes. Interoperability with existing identity systems and standards is also a challenge.

The potential benefits of blockchain - based personal identity security systems are significant, including improving security and privacy and preventing identity theft and fraud. Continued research and development is necessary to maximize these benefits, including developing more advanced smart contracts and incorporating other types of data into analysis. Transparency and accountability are also important to ensure user confidence in the security and privacy of personal data.

Overall, blockchain - based personal identity security systems have the potential to significantly improve the way we manage and secure personal identity data. With further research and development, blockchain - based systems can help to promote a more secure and responsible digital society, and help prevent the harm caused by identity theft and fraud.

6. Conclusion

In conclusion, blockchain - based personal identity security systems have shown to improve the security and privacy of personal identity data and prevent identity theft and fraud. However, there are still challenges to overcome, including the need for large datasets and ensuring interoperability with existing systems. It is also important to ensure transparency and accountability in these systems to build user confidence. Continued research and development is necessary to maximize the potential benefits of these systems.

Despite challenges, blockchain - based personal identity security systems offer significant potential benefits by promoting a more secure and responsible digital society and providing individuals with more control over their personal identity data. Further research and development is needed to maximize these benefits, including exploring more advanced smart contracts, incorporating other types of data, and ensuring transparency and accountability in the systems.

Overall, the use of blockchain - based personal identity security systems has the potential to significantly improve the way we manage and secure personal identity data. By promoting a more secure and responsible digital society, blockchain - based systems can help to prevent the harm caused by identity theft and fraud, and provide individuals with more control over their personal identity data. As such, it is important to continue research and development in this area, and to work towards implementing these systems in a way that is both effective and ethical.

7. Future Scope

The future scope of blockchain - based personal identity security systems is vast, with many opportunities for further research and development. Here are some possible areas of future enhancement:

Interoperability: Developing standards and protocols for interoperability between different blockchain - based personal identity security systems can improve the effectiveness and scalability of these systems.

Decentralized Identity Management: Developing decentralized identity management systems that can be used across different applications and services can provide users with greater control over their personal identity data.

Privacy - Preserving Technologies: Developing privacy - preserving technologies, such as zero - knowledge proofs and differential privacy, can improve the privacy and security of personal identity data stored on blockchains.

User - Centric Design: Designing blockchain - based personal identity security systems that are user - centric, intuitive, and easy to use can increase user adoption and trust.

Legal and Regulatory Frameworks: Developing legal and regulatory frameworks that govern the use of blockchain - based personal identity security systems can provide users with greater legal protections and ensure responsible use of the technology.

Overall, the future scope of blockchain - based personal identity security systems is vast, with many opportunities for further research and development. By continuing to explore new technologies, standards, and frameworks, we can unlock the full potential of these systems and create a more secure and responsible digital society.

References

[1] Wang, B.; Li, Z. Healthchain: A Privacy Protection System for Medical Data Based on Blockchain. Future Internet 2021, 13, 247. https: //doi. org/10.3390/fi13100247

[2] J. Kaneriya and H. Patel, "A Comparative Survey on Blockchain Based Self Sovereign Identity System, " 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp.1150 - 1155, doi: 10.1109/ICISS49785.2020.9315899.

[3] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah and M. - A. Fatima, "Blockchain - Based Identity Verification System, " 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2019, pp.253 - 257, doi: 10.1109/ICSEngT.2019.8906403.

[4] Patole, D., Borse, Y., Jain, J., Maher, S. (2020). Personal Identity on Blockchain. In: Sharma, H., Govindan, K., Poonia, R., Kumar, S., El - Medany, W. (eds) Advances in Computing and Intelligent Systems. Algorithms for Intelligent Systems. Springer, Singapore. https: //doi. org/10.1007/978 - 981 - 15 - 0222 - 4_41

[5] W. L. Sim, H. N. Chua and M. Tahir, "Blockchain for Identity Management: The Implications to Personal Data Protection, " 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 2019, pp.30 - 35, doi: 10.1109/AINS47559.2019.8968708.

[6] Y. Guo et al., "WISChain: An Online Insurance System based on Blockchain and DengLu1 for Web Identity Security, " 2018 1st IEEE International Conference on Hot Information - Centric Networking (HotICN), Shenzhen, China, 2018, pp.242 - 243, doi: 10.1109/HOTICN.2018.8606011.

[7] K. Gilani, E. Bertin, J. Hatin and N. Crespi, "A Survey on Blockchain - based Identity Management and Decentralized Privacy for Personal Data, " 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 2020, pp.97 - 101, doi: 10.1109/BRAINS49436.2020.9223312.

[8] V. Hariharasudan and S. J. Quraishi, "A Review on Blockchain - Based Identity Management System, " 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp.735 - 740, doi: 10.1109/ICIEM54221.2022.9853110.

[9] Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Raymond Choo, K. - K. (2020). Blockchain - based identity management systems: A review. In Journal of Network and Computer Applications (Vol.166, p.102731). Elsevier BV. https: //doi. org/10.1016/j. jnca.2020.102731

[10] Shobanadevi, A., Tharewal, S., Soni, M. et al. Novel identity management system using smart blockchain technology. Int J Syst Assur Eng Manag 13 (Suppl 1), 496–505 (2022). https: //doi. org/10.1007/s13198 - 021 - 01494 - 0