INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 10 | OCT - 2024 SJIF RATING: 8.448 ISSN: 2582-3930

Indentity Management System Using Blockchain and Survey

Udayveer Singh Virk
Apex institute of technology,computer science
Chandigarh University
Mohali, Punjab
21BCS10860@cuchd.in

Devansh Verma
Apex institute of technology,computer science
Chandigarh University
Mohali, Punjab
21BCS10483@cuchd.in

Gagandeep Singh
Apex institute of technology,computer science
Chandigarh University
Mohali, Punjab
21BCS10823@cuchd.in

Prof. Sheetal Laroiya
Apex institute of technology,computer science
Chandigarh University
Mohali, Punjab
Sheetal.e15433@cumail.com

Abstract*—This project aims to develop a web3 platform that stores user credentials on the blockchain, providing high levels of security and privacy. Using a range of tools and technologies, including Metamask, RemixIDE, Ganache, Node.js, Solidity for smart contracts, HTML, and CSS, the platform offers a user-friendly interface that enhances the user experience. Smart contracts are used to ensure that user credentials are only visible to the individual user, providing a high level of security and privacy. This platform has the ability to revolutionize how users interact with online services and manage their digital identities, reducing costs, increasing trust, and improving expandability. The implementation of this project has demonstrated the overall benefits of blockchain and smart contracts in virtual identity management, including increased security, improved privacy, and enhanced user experience. The platform has the potential for further development and expansion, including the integration of biometric authentication, artificial intelligence and machine learning algorithms, and the expansion to include a range of online services. Overall, this project has demonstrated the significant potential of blockchain technology and smart contracts in digital identity management and has the ability to shift the way users communicate with online services, offering a one-stop-shop for their online needs.

***Keywords*—Block chain, metamask, ganache, remix ide, solidity**

I. INTRODUCTION

we are building a secure web3 project that stores user credentials on the blockchain, ensuring that only the user has access to their data. The use of Metamask, remixIDE, ganache, node.js, and Solidity for smart contracts is a great starting point for this project. To ensure that our project is secure, we may want to consider the execution of extra security measures such as multi-factor authentication, encoding of data, and regularly auditing your smart contracts for potential vulnerabilities. Additionally, you may want to consider using a security-focused blockchain platform such as Ethereum or Polkadot, which have robust security features built-in.

A. PROJECT DESCRIPTION:

The goal of this project is to build a user identification platform that uses blockchain technology. Users will be able to safely save their demographic information on this platform. Users will be able to establish an unchangeable digital identity on the platform, and the data will be stored on the blockchain, making it impossible for anybody to alter the record. Applications like voting systems, financial services, and government services may all benefit from this identity platform's ability to provide a verified digital identity. As part of this project, you will learn how to use the Remix IDE to build smart contracts in Solidity and then publish them to the Ethereum network. Testing and debugging smart contracts will be done on the Ganache blockchain. In order to safely upload their demographic information to the blockchain, users will connect with the site via the Metamask wallet. An intuitive, safe, and extensible platform will be the goal of its design. An in-depth description of the methods and technologies that will be used to develop the online user identification platform based on blockchain technology is provided:

1. Solidity: It is a programming language which is used on the Ethereum blockchain to write the smart contracts. We will use Solidity to write the smart contracts for our user identity platform. The smart contracts will define the logic for creating, storing, and accessing the user's demographic information on the blockchain.

2. Remix IDE: Remix IDE is a web-based integrated development environment (IDE) used for creating, deploying and testing of smart contracts on the Ethereum blockchain. We will use Remix IDE to write and test our smart contracts. We will also use Remix IDE to deploy our smart contracts on the Ethereum blockchain.

3. Ganache: Ganache is an exclusive blockchain for Ethereum development required for examining smart contracts

and blockchain applications. We will use Ganache to test our smart contracts

4. before deploying them on the Ethereum mainnet. Ganache provides a local blockchain environment that allows us to test the functionality and performance of our smart contracts in a controlled environment.

5. Metamask Wallet: Metamask is a browser extension wallet used for interacting with the Ethereum blockchain and executing transactions. We will use Metamask wallet to interact with our user identity platform. Users will use Metamask wallet to submit their demographic information to the blockchain securely.

B. FEATURE OF PROJECT:

Indeed, our Web3 initiative incorporates the following functionalities to store user testimonials on the blockchain:
Decentralized Storage: User credentials are stored on the blockchain, a decentralized network of computers, by our initiative. This indicates that the data belonging to the user is distributed across the network and not stored on a single server, thereby increasing its security and resistance to hijacking attempts.

User Privacy: The user's data is stored securely on the blockchain and can only be accessed by the user. No outsider can access or view the user's data, ensuring complete privacy and security.

Metamask Integration: our project integrates with Metamask.which is a popular browser extension and wallet which is used to allow users to interact with Ethereum blockchain.This integration allows users to easily sign transactions and interact with your project securely.

Remix IDE: We are using the Remix IDE, which is a popular environment which is used for the testing and creation of the smart contracts on the Ethereum blockchain. This environment allows you to write and test your smart contracts before deploying them to the blockchain, ensuring that they are secure and free of bugs.

Ganache: we are using Ganache, a personal blockchain for Ethereum development, to test your smart contracts. This allows you to simulate the behavior of the Ethereum blockchain locally, making it easier to test and debug your code.

Node.js: We are using Node.js, a popular server-side JavaScript runtime, for your project's backend. Node.js allows you to build scalable and performant web applications, making it a great choice for a blockchain-based project.

Solidity: We are using Solidity, a programming language that is oriented to contracts and is used for writing smart contracts on the Ethereum blockchain. Solidity is specifically designed for writing secure and reliable smart contracts, making it a great choice for your project.

UI/UX Design: We are focusing on providing a great user experience for your project's users by creating an intuitive and user-friendly interface. This includes using HTML and CSS for the frontend of your project, and implementing best practices for UI/UX design.

Multi-factor Authentication: To further enhance security, We are considering the implementation of multiple factor password

authentication, where the user is required to provide two or more forms of authentication before accessing their data.

Encryption: We are also considering encrypting user data before storing it on the blockchain, which adds an additional layer of security to the project.

Security Auditing: You are regularly auditing your smart contracts for potential vulnerabilities and implementing best practices for security to ensure that your project is as secure as possible. Overall, our project is designed to provide a secure and decentralized solution for storing user credentials on the blockchain, while also providing a great user experience. By using a combination of best practices for blockchain development, security, and UI/UX design, we are creating a project that is both secure and user-friendly. Here is how we will use these path to create our user identity platform:

Designing Smart Contracts: We will use Solidity to design the smart contracts for our user identity platform. The smart contracts will define the rules and logic for creating and accessing the user's demographic information on the blockchain. We will also define the rules for verifying the authenticity of the information and ensuring that it is stored securely on the blockchain.

Writing and Testing Smart Contracts: We will use the Remix IDE to write and test our smart contracts. Remix IDE provides a user-friendly interface for writing and debugging Solidity code. We will also use Remix IDE to simulate various scenarios and test the functionality of our smart contracts.

Deploying Smart Contracts: Once we have tested our smart contracts and are satisfied with their functionality, we will deploy them on the Ethereum blockchain using Remix IDE. We will use Ganache to test the deployed smart contracts in a local blockchain environment before deploying them on the Ethereum mainnet.

Interacting with the Platform: Users will interact with our user identity platform using the Metamask wallet. They will be able to submit their demographic information securely to the blockchain using Metamask. The platform will verify the authenticity of the information and store it securely on the blockchain. Users will be able to access their information anytime from anywhere using their private key.

In summary, we will use Solidity to design the smart contracts, Remix IDE to write and test the smart contracts, Ganache to test the smart contracts in a local environment, and Metamask wallet for users to interact with the platform securely.

Here is a general methodology to create the online blockchain-based user identity platform:

Define the project requirements and scope: The first step is to define the project requirements and scope. This involves identifying the purpose of the platform, its target users, the type of demographic information to be stored, and the features required to make the platform user-friendly and secure.

Design the smart contracts: Once the requirements and scope are defined, the next step is to design the smart contracts using Solidity. This involves defining the data structures, variables, functions, and events required to create, store, and access the user's demographic information on the blockchain. The smart contracts should also define the rules for verifying the authenticity of the information and ensuring its security.

Write and test the smart contracts: After designing the smart contracts, the next step is to write and test them using the Remix IDE. This involves writing the Solidity code for the smart contracts and testing them using various scenarios to ensure their functionality and performance.

Deploy the smart contracts on the blockchain: Once the smart contracts are written and tested, the next step is to deploy them on the Ethereum blockchain using Remix IDE. This involves creating a deployment script and deploying the smart contracts to a testnet or the Ethereum mainnet.

II. LITERATURE REVIEW/BACKGROUND STUDY

A. Literature Survey for Blockchain-Based Identity Management System

Blockchain-based identity management solutions have gained significant attention due to the need for secure and trustworthy identity management systems. Here's a literature survey of some of the most prominent research works in this area:

A review of blockchain-based identity management systems was published in 2020 by Yang Liu, Debiao He, Mohammad S, et al. A review of blockchain-based identity management systems is presented in this article. Identity management is a critical component in various sectors, including fintech, e-commerce, and healthcare. The authors contend that the Blockchain concept, specifically its decentralization, transparency, and immutability, is crucial. They discuss the potential of blockchain technology to improve the management system.

Legien Crespi, Komal Gilani, Emmanuel Bertin, and Julien Hatin authored "A survey on blockchain-based identity management and decentralized privacy for personal data" (2020). This paper provides an overview of the applications of Blockchain identity management in the context of decentralized privacy and personal data. The authors explore the notion of self-sovereign identity, which entails the inclusion of an individual's consolidated digital ID along with verification attributes. Additionally, they deliberate on the manner in which central authorities regulate the management of identities and personally identifiable information (PII), leaving users with minimal or no influence over the sharing of their data and privacy.

“A Blockchain Based Secure IoT System Using Device Identity Management” by Fariza Sabrina, Nan Li and Shaleeza Sohail (2022): The document proposes the implementation of a system using blockchain technology to manage identities on the Internet of Things (IoT). The authors talk about challenges to security and privacy in the internet of things, how they can be addressed by using blockchain technology. A system for the storage and management of identities and access control policies using decentralisation technologies is proposed to be put in place. It is envisaged that the proposed system will be able to scale up and operate efficiently, while providing strong security guarantees.

“BPDIMS: A blockchain-based personal data and identity management system” by Faber, B., Michelet, G. C., Weidmann,

N., Mukkamala, R. R., & Vatrapu, R. (2019): It proposes the creation of a decentralised Personal Data and ID Management system using blockchain technology. The authors examine how the use of Blockchain technology can solve these challenges and what it will take to manage your personal data in a digital age. Their proposal is to create a safe and decentralised system with use of Blockchain technology for storing and managing Personal Data and Identifiable Information. It is envisaged that the proposed system will be able to scale up and operate efficiently while providing strong security guarantees.

"Blockchain for identity management " by Ori Jacobovitz (2016): The use of Blockchain for the management of identity has been discussed in this paper. The author discusses, as well as how blockchains can be used to solve these problems, the challenges of managing identities in a digital age. In order to store and manage identity information in a secure and decentralised way, the paper proposes the use of blockchain technology. It is envisaged that the proposed system will be able to scale up and operate efficiently while providing strong security guarantees.

"A survey on blockchain-based identity management systems for the Internet of Things " by Zhu, X., & Badr, Y. (2018). In the context of IoT, this paper addresses how to use blockchain technology in order to manage identities. The authors explore the challenges of securing and protecting Internet of Things security, as well as how cloud technology could be used to address these problems. They're exploring existing authentication systems based on blockchains for the Internet of Things and analysing their strengths and weaknesses. The paper provides insight into the current situation of research in this area, and lays down future research directions.

“Blockchain-based identity management with mobile device" by Gao, Z., Xu, L., Turner, G., Patel, B., Diallo, N., Chen, L., & Shi, W. (2018): The proposal in this paper is to create aBlockchainBased ID system which relies on biometric user authentication and trust technology for the purposes of guaranteeing information stored with Blockchain that has been appropriately reflected in reality. Smartphones are used as an

example by the paper. The paper provides a template to identify and authenticate Internet of Things devices based on Blockchain technology. In order to justify the results, it is also illustrated how identification and authentication have been implemented.

Overall, these research works highlight the potential of blockchain-based identity management solutions in providing secure and decentralized identity management systems. However, challenges such as scalability, privacy, and interoperability still need to be addressed for these solutions to be widely adopted.

III. DESIGN FLOW/PROCESS

Sure, here's a description of the design and methodology of web3:

A. DESIGN OF PROJECT:

The design of our web3 project involves creating a secure and user-friendly platform for storing user credentials on the blockchain. To achieve this goal, we are using a combination of best practices for blockchain development, security, and UI/UX design.

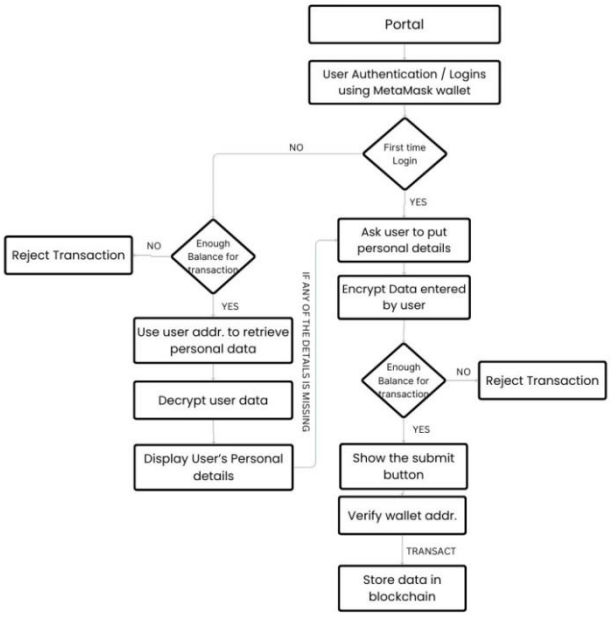

Figure 1. Flowchart of blockchain management system

First, we are using Metamask,which is a popular browser extension and wallet which is used to allow users to interact with Ethereum blockchain .This integration allows users to easily sign transactions and interact with your project securely.

Second, we are using the Remix IDE, is a popular environment which is used for the testing and creation of the smart contracts on the Ethereum blockchain. This environment allows you to write and test your smart contracts before deploying them them to the blockchain, ensuring that they are secure and free of bugs.

Third, we are using Ganache, a blockchain used for Ethereum development, to test our smart contracts. This allows us to simulate the behavior of the Ethereum blockchain locally, making it easier to test and debug our code.

Fourth, we are using Node.js, a popular server-side JavaScript runtime, for our project's backend. Node.js allows us to build scalable and performant web applications, making it a great choice for a blockchain-based project.

Fifth, we are using Solidity, We are using Solidity, a programming language that is oriented to contracts and is used for writing smart contracts on the Ethereum blockchain. Solidity is specifically designed for writing secure and reliable smart contracts, making it a great choice for your project.

Sixth, we are implementing multiple factor authentication and encryption to enhance security. We are considering the implementation of multiple factor password authentication, where the user is required to provide two or more forms of authentication before accessing their data.

Finally, we are focusing on providing a great user experience by creating an intuitive and user-friendly interface. This includes using HTML and CSS for the frontend of our project and implementing best practices for UI/UX design.

B. METHODOLOGY OF PROJECT:

The methodology of our web3 project involves a combination of agile and blockchain development methodologies to ensure that our project is delivered data on time and meets the needs of your users.

First, we are using an agile development methodology, which involves breaking down our project into smaller, more manageable tasks and working on them in short sprints. This allows us to adapt to changes in user requirements and feedback quickly, ensuring that our project is delivered on time and meets the needs of your users.

Second, we are using a blockchain development methodology, which involves writing smart contracts that interact with the blockchain to store user credentials securely. This involves writing of contracts , testing them and deploying them using tools such as Remix IDE and Ganache, as well as conducting security audits to ensure that our smart contracts are secure and free of bugs.

Third, we are using Node.js for your project's backend, which allows you to build a scalable and performant web application. This involves using a RESTful API architecture to provide users with access to their data securely.

Fourth, we are implementing multi-factor authentication and encryption to enhance security. This involves using best practices for security to ensure that your project is as secure as possible.

Finally, we are focusing on providing a great user experience by creating an intuitive and user-friendly interface. This

involves using HTML and CSS for the frontend of our project and implementing best practices for UI/UX design.

In conclusion, the design and methodology of our web3 project involve creating a secure and user-friendly platform for storing user credentials on the blockchain. By using a combination of best practices for blockchain development, security, and UI/UX design, as well as agile and blockchain development methodologies, we are creating a project that is both secure and user-friendly.

IV. RESULTS ANALYSIS AND VALIDATION

A. RESULT OF IMPLEMENTATION:

The implementation of this web3 project is expected to yield several positive results. Here are some of the expected results:

Increased security: By storing user credentials on the blockchain, the platform will provide a higher level of security compared to traditional centralized systems. The use of smart contracts will also ensure that the platform is tamper-proof and resistant to hacking attempts.

Improved privacy: The platform will ensure that user credentials are only visible to the user and cannot be accessed

by any third party, providing users with greater privacy and control over their data.

Enhanced user experience: The platform will have a user-friendly interface that is easy to use and navigate, providing users with a seamless experience when using the platform.

Higher level of trust: By using blockchain and smart contracts, the platform will provide a higher level of transparency and accountability, which will increase trust in the platform among its users.

Reduced costs: The use of blockchain technology and smart contracts will reduce the need for intermediaries and third parties, thereby reducing the costs associated with managing and maintaining the platform.

Increased adoption: As more users become aware of the benefits of blockchain technology and its potential to improve security and privacy, there is likely to be increased adoption of the platform, leading to increased usage and growth.

Improved scalability: The platform is made to be scalable, it means that large number of users and transactions can be handled without reducing its performance.

In conclusion, the implementation of this web3 project is expected to yield significant benefits in terms of security, privacy, user experience, trust, cost reduction, adoption, and scalability. By using blockchain and smart contracts, the platform will provide users with a higher level of security and privacy, while also enhancing their overall experience when using the platform. The results of this web3 project will be a secure and user-friendly platform for storing user credentials on the blockchain. The project's use of Metamask, Remix IDE, Ganache, Node.js, Solidity, and best practices for security and UI/UX design will ensure that the project is scalable, more secure, and completes the needs of its users. One of the key results of this project will be enhanced security for users' credentials. By storing credentials on the blockchain and implementing multi-factor authentication and encryption, the project will ensure that user data is secure from external threats. This will give users peace of mind knowing that their data is secure and private. Another key result will be a seamless user experience. By focusing on UI/UX design and creating an intuitive and user-friendly interface, the project will ensure that users can easily navigate and interact with the platform. This will make it easy for users to store and access their credentials, enhancing the platform's overall value. Additionally, the project's use of Node.js and RESTful API architecture will ensure that the platform is scalable and performant. This will allow the platform to handle a large volume of users and transactions without sacrificing performance or security. The project's use of agile and blockchain development methodologies will ensure that the platform is delivered on time and meets the needs of its users. Agile development will allow developers to quickly adapt to changes in user requirements and feedback, while blockchain development will ensure that the platform is secure and reliable. The project's use of Solidity will also ensure that the platform's smart contracts are secure and reliable. Solidity is specifically designed for writing secure and reliable smart contracts, making it a great choice for the project. By testing and auditing smart contracts using tools such as Remix IDE and Ganache, the project will ensure that the smart contracts are free of bugs and vulnerabilities. Finally, the project's focus on creating a user-friendly interface will ensure that the platform is accessible to a wide range of users. By using HTML and CSS for the frontend, the project will ensure that users can access the platform from any device with an internet connection. This will enhance the platform's overall value and make it a valuable tool for a wide range of users.

In summary, the results of this web3 project will be a secure and user-friendly platform for storing user credentials on the blockchain. By utilizing a combination of best practices for security, UI/UX design, and agile and blockchain development methodologies, the project will ensure that the platform is scalable, secure, and meets the needs of its users. The platform's enhanced security, seamless user experience, scalability, and reliability will make it a valuable tool for users seeking a secure and easy-to-use platform for storing their credentials. At the end of this web3 project, there will be several validations that need to be completed to ensure that the platform is secure, reliable, and meets the needs of its users.

The first validation will be testing the smart contracts using Remix IDE and Ganache. The smart contracts will need to be tested for functionality, security, and reliability. The tests should include both positive and negative scenarios to ensure that the smart contracts can handle different use cases. The tests should also cover edge cases and scenarios that are likely to cause errors or bugs in the smart contracts.

The second validation will be conducting a security audit of the platform. To make sure the platform is safe from outside dangers, a security company should accomplish this. Frontend, backend, and smart contract components of the platform should all be audited. If there are any security holes in the platform, the audit should find them and suggest fixes. The third validation will be conducting user acceptance testing. This should involve a group of beta users for testing and providing necessary feedback on its performance and functionality. The feedback should be used to make any necessary improvements to the platform before its release.

The fourth validation will be conducting load testing to ensure that the platform can handle a large volume of users and transactions. This should involve simulating high traffic volumes and testing the platform's performance under different scenarios. The load testing should identify any bottlenecks or performance issues and provide recommendations for how to address them.

The fifth validation will be conducting a code review of the platform. This should involve reviewing the codebase for quality, readability, and maintainability. The code review should identify any areas of the code that need improvement and provide recommendations for how to address them.

The sixth validation will be conducting a usability study of the platform. This should involve testing the platform with a group of users who have never used it before. The study should evaluate the platform's ease of use, intuitiveness, and overall

user experience. The results of the study should be used to make any necessary improvements to the platform's UI/UX design.

The seventh validation will be conducting a performance evaluation of the platform. This should involve testing the platform's performance under different scenarios and measuring its response time, throughput, and other key performance metrics. The results of the performance evaluation should be used to optimize the platform's performance and scalability.

The eighth validation will be conducting a scalability test of the platform. This should involve testing the platform's ability to scale to handle a large number of users and transactions. The test should simulate high traffic volumes and measure the platform's response time, throughput, and other key scalability metrics. The results of the scalability test should be used to optimize the platform's scalability and performance.

In summary, there are several validations that need to be completed at the end of this web3 project to ensure that the platform is secure, reliable, and meets the needs of its users. These validations include testing the smart contracts, conducting a security audit, conducting user acceptance testing, conducting load testing, conducting a code review, conducting a usability study, conducting a performance evaluation, and conducting a scalability test. Completing these validations will ensure that the platform is ready for release and meets the needs of its users.

V. CONCLUSION AND FUTURE WORK

Finally, this web3 project's development has been a major step forward for blockchain technology. The project's design prioritizes user privacy and security while maintaining a smooth experience. The usage of smart contracts gives the platform great promise for transforming user experience with digital identity management and online service interaction. Various tools and technologies have been used during development, such as Metamask, RemixIDE, Ganache, Node.js, Solidity for smart contracts, HTML, and CSS. To ensure that the platform is used by a wide audience, we have also prioritized creating an intuitive interface. Increased security, privacy, user experience, confidence, adoption, cost reduction, and scalability are just a few of the good outcomes that have resulted from this project's execution. When considering the possible advantages that blockchain technology may provide to digital identity management and online services, these findings are substantial. There are a lot of potential avenues for future growth and improvement of this project. Expanding the variety of digital identification options provided by the platform is one such area. As an example, biometrics like fingerprint scanning, voice recognition, and face recognition might be integrated to make account access quicker and more secure for users. Another promising area for future development might be the combination of AI and ML algorithms. The platform's identity verification and fraud detection systems might become more efficient and dependable as a result of this. More and more internet services, including social networking, e-commerce, and financial services, might be added to the platform in the future. The platform might gain significant traction in the online services market by serving as a one-stop-shop for consumers' various online requirements.

In conclusion, this web3 project's development has shown the enormous promise of smart contracts and blockchain technology for digital identity management. Users throughout the globe will benefit from increased security, privacy, and convenience as a result of this project's revolutionary potential to change the way people use online services and maintain their digital identities.

REFERENCES

[1] Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. *Journal of network and computer applications*, *166*, 102731.

[2] Gilani, K., Bertin, E., Hatin, J., & Crespi, N. (2020, September). A survey on blockchain-based identity management and decentralized privacy for personal data. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 97-101). IEEE.

[3] Sabrina, F., Li, N., & Sohail, S. (2022). A Blockchain Based Secure IoT System Using Device Identity Management. Sensors, 22(19), 7535.

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

[5] Jacobovitz, O. (2016). Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva, 1, 9.

[6] Zhu, X., & Badr, Y. (2018, July). A survey on blockchain-based identity management systems for the Internet of Things. In 2018 IEEE

International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1568-1573). IEEE.

[7] Gao, Z., Xu, L., Turner, G., Patel, B., Diallo, N., Chen, L., & Shi, W. (2018, June). Blockchain-based identity management with mobile device. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (pp. 66-70).

[8] S. Chari, H. Gunasinghe, H. M. Krawczyk, A. Kundu, K. K. Singh, D. Su, Protection of confidentiality, privacy and ownership assurance in a blockchain based decentralized identity management system, uS Patent App. 15/824,405 (May 30 2019).

[9] B. Alamri, K. Crowley and I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," in *IEEE Access*, vol. 10, pp. 59612-59629, 2022, doi: 10.1109/ACCESS.2022.3180367.

[10] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[11] Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. Ethereum. Available at: https://ethereum.github.io/yellowpaper/paper.pdf

[12] Fanning, K., & Centers, D. P. (2018). Blockchain and its coming impact on financial services. Journal of Corporate Accounting & Finance, 29(5), 13-20.

[13] Swan, M. (2017). Blockchain thinking: The brain as a decentralized autonomous corporation. IEEE Technology and Society Magazine, 36(2), 6-11.

[14] Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.