Digital Identity Using Decentralized System in Blockchain

[1] Prof. Kajol Patel, Research Scholar, Information Technology, Parul Institute of Engineering & Technology, Parul University, Email- 2123004136010@paruluniversity.ac.in

[2] Dr. Daxa Vekariya, Assistant Professor, Computer Engineering, Parul Institute of Engineering & Technology, Parul University, Email- daxa.vekariya18436@paruluniversity.ac.in

Abstract: In an era where digital identity theft and centralized data breaches pose significant challenges to online security and privacy, blockchain technology emerges as a promising solution. This paper presents a comprehensive review of blockchain-based decentralized systems for digital identity management. It examines the fundamental principles of blockchain technology and its application in establishing secure, transparent, and user-controlled digital identity systems. The review explores various blockchain-based identity platforms, protocols, and standards, highlighting their features, strengths, and limitations. Additionally, it discusses real-world use cases and pilot projects that demonstrate the feasibility and potential benefits of blockchain-based digital identity solutions. Furthermore, the paper analyzes the challenges and future research directions in this rapidly evolving field. Through this review, stakeholders in the digital identity ecosystem can gain insights into the capabilities and implications of blockchain technology for enhancing online identity management.

I. Introduction

a. What is blockchain?

Blockchain is a decentralized, distributed ledger technology that enables the secure recording, storage, and verification of transactions across a network of computers. At its core, blockchain consists of a series of interconnected blocks, each containing a bundle of transactions. These blocks are cryptographically linked together in a chronological order, forming a continuous chain of blocks, hence the name "blockchain."

One of the key features of blockchain is its decentralized nature. Instead of relying on a central authority or intermediary to validate and record transactions, blockchain operates on a peer-to-peer network of nodes. Each node maintains a copy of the entire blockchain ledger, and transactions are verified through a consensus mechanism agreed upon by the network participants.

Blockchain technology offers several advantages, including:

- **Transparency:** The transparent nature of blockchain allows all network participants to view and verify transactions recorded on the ledger. This transparency helps foster trust among users and ensures the integrity of the data.

- **Immutability:** Once a transaction is recorded on the blockchain, it cannot be altered or tampered with retroactively. This immutability is achieved through cryptographic hashing and consensus mechanisms, making blockchain a secure and tamper-proof system of record-keeping.

- **Decentralization:** Blockchain operates on a decentralized network of nodes, eliminating the need for intermediaries or central authorities to validate transactions. This decentralization increases resilience against censorship, fraud, and single points of failure.

- **Security:** The cryptographic algorithms and consensus mechanisms used in blockchain ensure the security and integrity of transactions. Transactions are verified and added to the blockchain in a secure and trustless manner, reducing the risk of unauthorized access or manipulation.

Blockchain technology has found applications beyond its original use case in cryptocurrencies like Bitcoin. It is increasingly being adopted across various industries, including finance, supply chain management, healthcare, real estate, and digital identity management, among others. As blockchain continues to evolve, it holds the potential to revolutionize traditional systems of record-keeping, streamline processes, and drive innovation in the digital economy.

b. What is decentralized in blockchain?

Decentralization in the context of blockchain refers to the distribution of control and decision-making across a network of nodes rather than relying on a central authority. This decentralization is a fundamental characteristic of blockchain technology and sets it apart from traditional centralized systems.

Here's what decentralization means in blockchain:

Decentralized Network: In a blockchain network, there is no single point of control or authority. Instead, the network consists of a distributed and interconnected group of nodes, with each node maintaining a copy of the entire blockchain ledger. This distributed architecture ensures that no single entity has control over the network, enhancing resilience and reducing the risk of censorship or manipulation.

Decentralized Validation: Transactions on the blockchain are validated and confirmed through a consensus mechanism agreed upon by the network participants. Instead of relying on a central authority to validate transactions, blockchain uses consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), or others to achieve agreement among nodes. This decentralized validation process ensures the integrity and security of transactions without the need for intermediaries.

Decentralized Governance: In some blockchain networks, governance decisions, such as protocol upgrades or changes, are made through a decentralized governance mechanism. This may involve voting by network participants or other forms of consensus to determine the direction of the blockchain's development. Decentralized governance ensures that decisions are made collectively by the community rather than by a central authority.

Decentralized Data Storage: The data recorded on the blockchain is distributed across multiple nodes in the network. Each node maintains a copy of the blockchain ledger, ensuring redundancy and fault tolerance. Decentralized data storage reduces the risk of data loss or corruption and enhances the reliability and availability of the blockchain network.

Overall, decentralization in blockchain is a key principle that promotes transparency, security, and resilience by distributing control and decision-making authority among network participants. It enables trustless interactions, removes the need for intermediaries, and empowers individuals to participate in and contribute to the network's operation and governance.

II. Blockchain for digital identity

Blockchain technology holds immense promise for digital identity management by offering secure, decentralized, and user-controlled solutions. Here's how blockchain can be applied to digital identity:

- **Decentralized Identity Ownership:** Blockchain enables individuals to have full ownership and control over their digital identities. Instead of relying on centralized entities like governments or corporations to verify and manage identities, individuals can store their identity credentials on a blockchain in a self-sovereign manner.

- **Immutable Identity Records:** Once identity information is recorded on a blockchain, it becomes immutable and tamper-proof. This ensures the integrity and security of identity records, reducing the risk of identity theft, fraud, or unauthorized changes.

- **Privacy Preservation:** Blockchain-based identity solutions can enable selective disclosure of identity attributes, allowing individuals to share only the necessary information for a specific transaction or interaction. This enhances privacy and minimizes the exposure of sensitive personal data.

- **Interoperability:** Blockchain protocols and standards, such as Decentralized Identifiers (DIDs) and Verifiable Credentials, promote interoperability among different identity systems and applications. This enables seamless integration and exchange of identity information across various platforms and services.

- **Reduced Identity Verification Costs:** Traditional identity verification processes often

involve multiple intermediaries, leading to high costs and inefficiencies. Blockchain-based identity solutions streamline the verification process by eliminating intermediaries and providing a more cost-effective and automated approach.

- **Identity Verification in Decentralized Applications (DApps):** Blockchain enables seamless integration of identity verification mechanisms into decentralized applications (DApps). Users can verify their identities on the blockchain to access DApps securely and participate in various decentralized services such as finance, governance, and social networking.

- **Digital Identity for Underserved Populations:** Blockchain-based digital identity solutions have the potential to empower underserved populations, such as refugees, migrants, and individuals without official documentation, by providing them with secure and portable digital identities that are not dependent on traditional identity documents or centralized authorities.

- **Compliance and Regulatory Requirements:** Blockchain-based identity solutions can help organizations comply with regulatory requirements, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, by providing secure and auditable identity verification processes.

III. Working of digital identity

To understand how a blockchain identity management system works, we should know about the technical components involved in the process.
There are five technical components and interfaces that could be involved in the Blockchain based Identity Management Process:

- Native Android/iOS App for individuals.
- Native Android/iOS App for third-party companies/verification companies.
- Inter-Planetary File System to store the user's PII.
- Microservices programmed using Node.JS.
- Permissioned Blockchain Component.

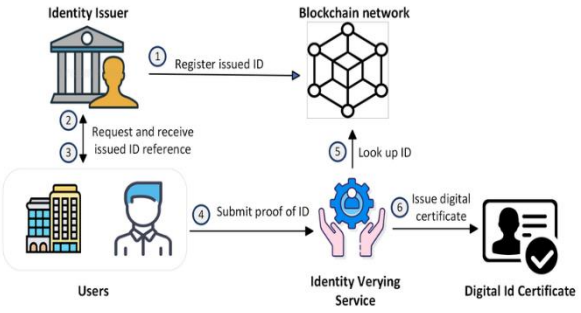

Fig. 1 Working of digital [1]

IV. Conclusion

Nowadays people are used to surf and do online stuff regarding finance, booking, food ordering, visa, online shopping, online transaction and what not and for this you will require digital reorganization for activating the systems regarding their need so by using blockchain mechanism it will provide secure management with security key and It will provide more authentication with IOT systems.

Refences:

1. El Haddouti, S., & El Kettani, M. D. E. C. (2019, April). Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-7). IEEE.

2. Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2019). A taxonomic approach to understanding emerging blockchain identity management systems. *arXiv preprint arXiv:1908.00929*.

3. Panait, A. E., Olimid, R. F., & Stefanescu, A. (2020). Identity Management on Blockchain--Privacy and Security Aspects. *arXiv preprint arXiv:2004.13107*.

4. Zohaib Rafique, February 2021. Blockchain in Digital Identity. ResearchGate

5. Buccafurri, F., Lax, G., Russo, A., & Zunino, G. (2018, October). Integrating digital identity and blockchain. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 568-585). Springer, Cham.

6. V Anjana and Malini Raman. 2021, Impact of blockchain on digital identity, TCS BaNCS,Research journal

7. Rivera, R., Robledo, J. G., Larios, V. M., & Avalos, J. M. (2017, September). How digital identity on blockchain can contribute in a smart city environment. In 2017 International smart cities conference (ISC2) (pp. 1-4). IEEE.

8. Takemiya, M., & Vanieiev, B. (2018, July). Sora identity: Secure, digital identity on the blockchain. In 2018 ieee 42nd annual computer software and applications conference (compsac) (Vol. 2, pp. 582-587). IEEE.

9. Sullivan, C., & Burger, E. (2019). Blockchain, digital identity, e-government. In Business Transformation through Blockchain (pp. 233-258). Palgrave Macmillan, Cham.

10. Bakre, A., Patil, N., & Gupta, S. (2017). Implementing decentralized digital identity using blockchain. International Journal of Engineering Technology Science and Research, 4(10), 379-385.

11. Al-Khouri, A. M. (2012). PKI in government digital identity management systems. European Journal of ePractice, 4(4).

12. Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. Procedia computer science, 123, 116-121.

13. Stokkink, Q., & Pouwelse, J. (2018, July). Deployment of a blockchain-based self-sovereign identity. 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. 1336-1342). IEEE.

14. Zhao, W., Yang, N., Li, G., & Zhang, K. (2021, October). Research on Digital Identity Technology and Application Based on Identification Code and Trusted Account Blockchain fusion. In 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) (pp. 405-409). IEEE.

15. Choudhari, S., Das, S. K., & Parasher, S. (2021, April). Interoperable Blockchain Solution For Digital Identity Management. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-6). IEEE.

16. Ghosh, B. C., Ramakrishna, V., Govindarajan, C., Behl, D., Karunamoorthy, D., Abebe, E., & Chakraborty, S. (2021, May). Decentralized cross-network identity management for blockchain interoperation. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-9). IEEE.

17. 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.

18. Grüner, A., Mühle, A., Gayvoronskaya, T., & Meinel, C. (2018, July). A quantifiable trust model for blockchain-based identity management. 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. 1475-1482). IEEE.

19. Rahat, A. H., Rumon, M. R., Joti, T. J., Tasnin, H., Akter, T., Shakil, A., & Hossain, M. I. (2022, January). Blockchain Based Secured Multipurpose Identity (SMID) Management System for Smart Cities. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0737-0744). IEEE.

20. El Haddouti, S., & El Kettani, M. D. E. C. (2019, April). Analysis of identity management systems using blockchain technology. In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-7). IEEE.

21. Gururaj, P. (2020, February). Identity management using permissioned blockchain. In 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI) (pp. 1-3). IEEE.

22. Pillai, A., Saraswat, V., & Ramachandran, A. V. (2021, December). Protection Guidelines for Blockchain Based Digital Identity. In International Conference on Hybrid Intelligent Systems (pp. 636-646). Springer, Cham.

23. Sin, E. S., & Naing, T. T. (2021). Digital identity management system using blockchain technology. In International Conference on Innovative Computing and Communications (pp. 895-906). Springer, Singapore.

24. Pillai, A., Saraswat, V., & Vasanthakumary Ramachandran, A. (2021, October). Attacks on blockchain based digital identity. In International Congress on Blockchain and Applications (pp. 329-338). Springer, Cham.

25. Song, Z., Yu, Z., Shang, W., & Li, Y. (2021, August). A Digital Copyright Protection Method Based on Blockchain. In International Conference on Blockchain and Trustworthy Systems (pp. 486-

498). Springer, Singapore.

26. Čučko, Š., & Turkanović, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study. IEEE Access, 9, 139009-139027.

27. Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE security & privacy, 16(4), 20-29.

28. Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of blockchain technologies. IEEE Security & Privacy, 17(1), 72-77.

29. Qiao, K., Tang, H., You, W., & Zhao, Y. (2019, April). Blockchain privacy protection scheme based on aggregate signature. In 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA) (pp. 492-497). IEEE.

30. Zhao, W., Yang, N., Li, G., & Zhang, K. (2021, October). Research on Digital Identity Technology and Application Based on Identification Code and Trusted Account Blockchain fusion. In 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) (pp. 405-409). IEEE.

31. Biswas, B. N., Bhitkar, S. D., & Pundkar, S. N. (2021, May). Secure Login: A Blockchain based web application for Identity Access Management System. In 2021 2nd International Conference for Emerging Technology (INCET) (pp. 1-5). IEEE.

32. Malik, G., Parasrampuria, K., Reddy, S. P., & Shah, S. (2019, March). Blockchain based identity verification model. In 2019 international conference on vision towards emerging trends in communication and networking (ViTECoN) (pp. 1-6). IEEE.

33. Khan, S., Jadhav, A., Bharadwaj, I., Rooj, M., & Shiravale, S. (2020, March). Blockchain and the identity based encryption scheme for high data security. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1005-1008). IEEE.

34. Belurgikar, D. A., Kshirsagar, J. K., Dhananjaya, K. K., & Vineeth, N. (2019, March). Identity solutions for verification using blockchain technology. In 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE) (pp. 121-126). IEEE.

35. Alilwit, N. (2020, November). Authentication based on blockchain. In 2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC) (pp. 1-6). IEEE.

36. Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. Business & Information Systems Engineering, 63(5), 603-613.

37. Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12, pages 906–917, New York, NY, USA, 2012. ACM.

38. Tyler Moore. The promise and perils of digital currencies. International Journal of Critical Infrastructure Protection, 6(34):147 – 149, 2013.

39. Jennifer J. Xu. Are blockchains immune to all malicious attacks? Financial Innovation, 2(1):25, 2016.

40. C. Victoria Priscilla and T. Devasena, March 2021. Aadhaar Identity System using Blockchain Technology. Volume 174 – No. 26.

41. Rishabh Garg, July 2021, Digital Identity Leveraging Blockchain, Barnes & Noble Inc.,Basking Ridge New Jersey,US