IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303103 |

User Authentication using Hyperledger

JM Babu[1], Chundu Sandhya[2], Gedda Pratap[3], Bachina Sri Harika[4], Gade Deependra Kumar[5]

Associate Professor, Department of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, India[1]

Department of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, India[2,3,4,5]

ABSTRACT - Blockchain technology ensures secure management, authentication, and data access in a decentralized manner, fostering trust, integrity, and resilience. This paper introduces a user authentication scheme using Hyperledger, a private blockchain solution. Hyperledger offers immutable transaction logs and audit trails to record and authenticate user activities such as registrations, logins, access control decisions, and credential issuance, promoting transparency, accountability, and traceability. Blockchain serves as a decentralized, distributed, shared, and immutable database ledger, maintaining records of assets and transactions across a peer-to-peer (P2P) network. Each transaction is digitally signed and validated by numerous mining nodes within the network.

KEYWORDS: Security, Blockchain, Hyperledger, Authentication.

I. INTRODUCTION

Authentication is a crucial element of digital security, ensuring that only authorized individuals or entities access sensitive systems, data, or services. Blockchain-based authentication is an innovative approach that harnesses the decentralized and immutable nature of blockchain technology to enhance the security, transparency, and reliability of authentication processes.

In traditional authentication systems, centralized authorities such as servers or identity providers verify user identities. However, these systems are vulnerable to security risks like single points of failure, data breaches, and identity theft.

Blockchain-based authentication offers a transformative solution by decentralizing the authentication process, removing intermediaries, and providing a tamper-proof and transparent method for verifying user identities. Blockchain acts as a distributed ledger, transparently recording and validating authentication-related transactions in an immutable manner.

At the heart of blockchain-based authentication lies the concept of decentralized identity, empowering users to control their digital identities and personal data. Decentralized identity solutions utilize cryptographic techniques such as public-private key pairs, digital signatures, and verifiable credentials, enabling users to securely and privately manage, create, and share their identities.

Blockchain-based authentication offers several key advantages that could transform how identity is managed in the digital age. By recording authentication transactions on a distributed ledger, blockchain ensures that all parties involved can verify identity-related data without relying on a central authority, thus enhancing accountability and reducing the risk of identity fraud and impersonation.

Furthermore, blockchain-based authentication offers privacy benefits by allowing users to selectively disclose their identity attributes and credentials as needed. This is achieved through self-sovereign identity principles, where users maintain ownership and control over their personal data, deciding when and how to share it with third parties.

In addition to security and privacy, blockchain-based authentication offers scalability and interoperability, making it suitable for various applications and industries. Whether it's securing access to digital services, authenticating users in financial transactions, or enabling secure login mechanisms for IoT devices, blockchain-based authentication has the potential to revolutionize identity management.

Overall, blockchain-based authentication presents a groundbreaking approach, providing enhanced security, privacy, and trust in authentication processes while giving users greater control over their digital identities. As blockchain technology evolves, its adoption in authentication systems is expected to grow, driving innovation and transformation across different sectors.

II. LITERATURE REVIEW

Blockchain technology has garnered significant attention in recent years due to its potential to revolutionize various industries, including identity management and authentication. Among the different blockchain platforms, Hyperledger stands out as a leading open-source framework for building enterprise-grade blockchain solutions. This literature

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

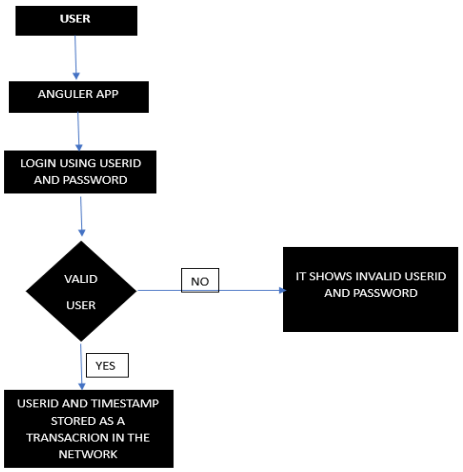
| DOI:10.15680/IJIRSET.2024.1303103 |

review explores the current state of research and development in the area of authentication using Hyperledger, focusing on its applications, challenges, and future directions.

Research by Zyskind et al. (2015) introduced "Decentralized Public Key Infrastructure (DPKI)" using blockchain, which serves as a decentralized identity management system [1]. Sovrin's whitepaper (2018) outlines how Hyperledger Indy enables individuals to control their digital identities, manage verifiable credentials, and authenticate themselves across different platforms and services [2]. Tschorsch and Scheuermann (2016) proposed a blockchain-based authentication protocol using Hyperledger Fabric. Their research explores how Fabric's smart contract functionality and permissioned network architecture can be utilized to implement secure and efficient authentication mechanisms for distributed applications [3]. Shrestha et al. (2020) presented a privacy-preserving authentication framework using Hyperledger Fabric. Their approach leverages zero-knowledge proofs (ZKPs) to authenticate users without revealing sensitive identity information, ensuring privacy and confidentiality in authentication processes [4]. Kumar et al. (2019) investigated the application of Hyperledger Fabric for identity management in healthcare. Their study explores how Fabric's features, such as access control and auditability, can enhance patient authentication, data privacy, and regulatory compliance in healthcare systems [5].

III.METHODOLOGY

3.1 Design



3.2 Implementation

3.2.1Steps for Implementation:

a) Required blockchain installations include Docker, Docker Compose, Hyperledger Composer, npm, and Node.js.
b) Start Hyperledger Fabric.
c) Create a PeerAdmin card.
d) Create and deploy the business network.
e) Create a Business Network Archive File (BNA).
f) Install and deploy the BNA file.
g) Test the business network in Hyperledger Composer Playground.
h) Generate a REST API server.
i) Generate an Angular application that utilizes the REST API.

In the process of creating a Business Network Archive (BNA) file in blockchain development, three essential types of files are required: ACL (Access Control Language), JS (JavaScript), and CTO (Concerto).

ACL file: Outlines access control rules for the business network, determining authorized participants and their actions.

JS file: Defines the business logic, including transaction execution rules and event handling mechanisms.

CTO file: Specifies the data model for the network, detailing asset and transaction types.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303103 |

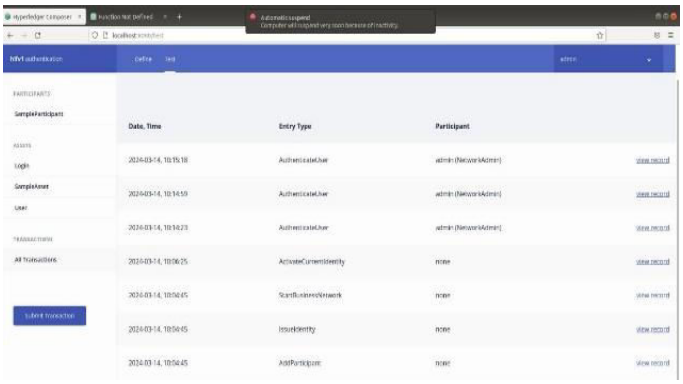
Creating business networks requires Hyperledger Composer installation, while deploying them requires Hyperledger Fabric installation. Composer-cli is a crucial tool encompassing essential operations.

Composer REST server enables running a REST server on the machine, exposing the business network as RESTful Application Interfaces. Hyperledger Composer Generator creates application assets. Before deployment, starting Hyperledger Fabric is essential for security, privacy, and scalability. Installing the Business Network Archive onto the Hyperledger Fabric network involves installing it onto the peers. Starting the Business Network on Hyperledger Fabric is done with the PeerAdmin card. After importing the admin
card, it's used for the deployed business network. Finally, starting the REST server
makes it accessible at http://localhost:3000/explorer.
To enable the Angular application to connect to the Fabric instance, ensure the REST server is operational in the background. The Angular application runs on http://localhost:4200.

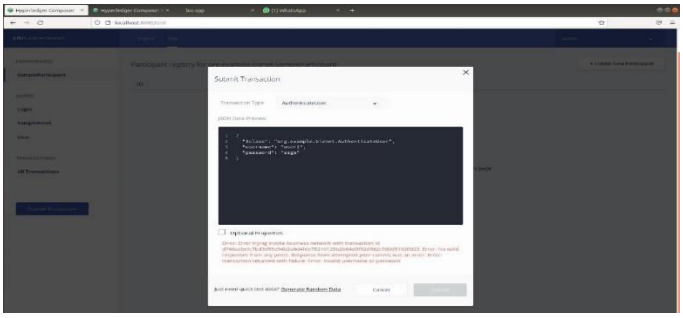
IV. EXPERIMENTAL RESULTS

4.1 When we are doing authentication in the Hyperledger business network:

a) When the user is valid the transaction will be stored as a transaction in the network



b) When the user is not a valid user or entered invalid userid and password.



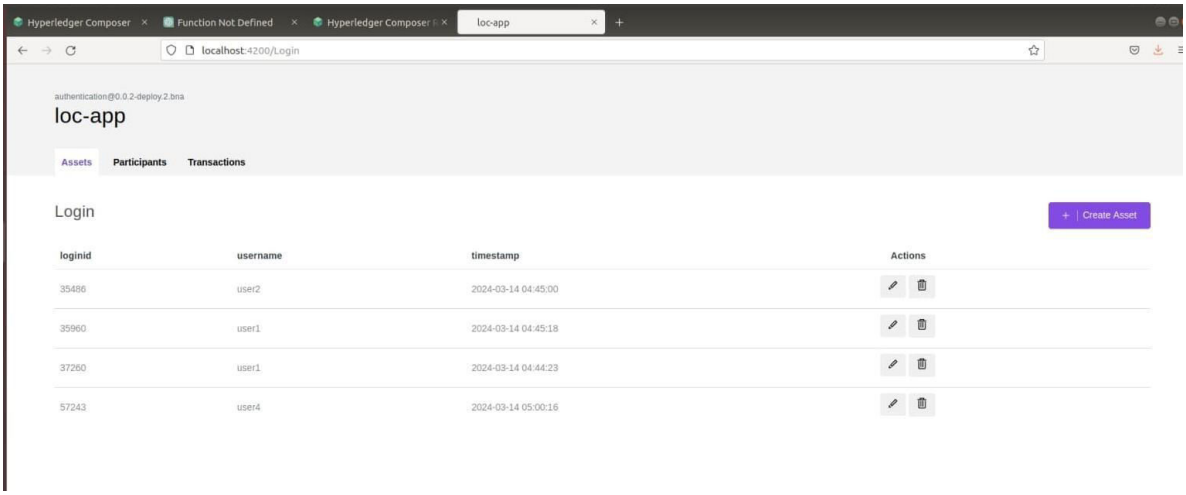
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

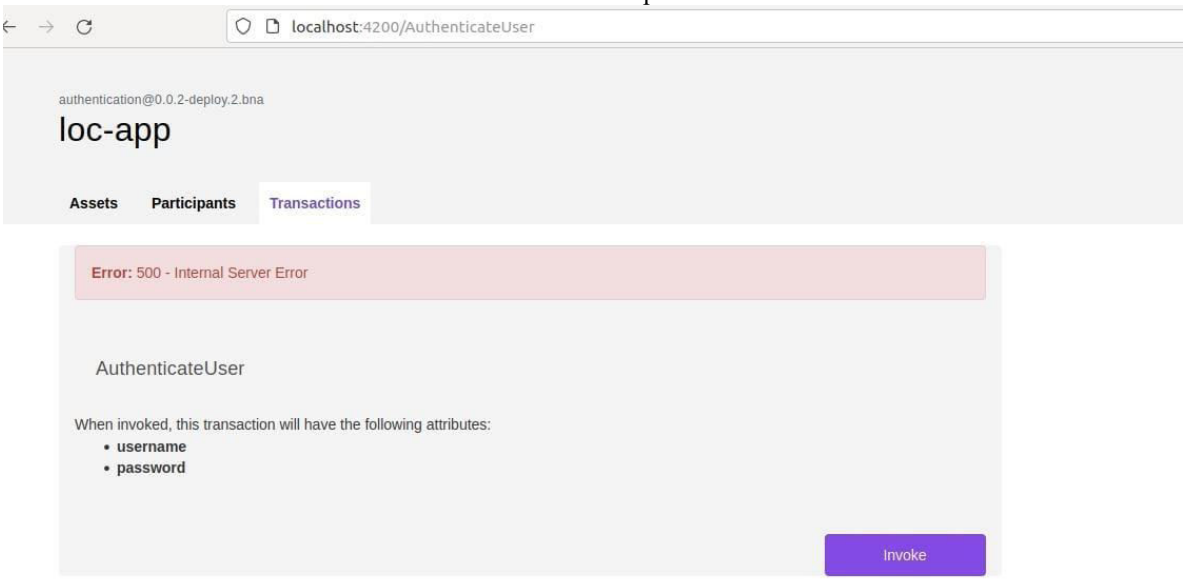
| DOI:10.15680/IJIRSET.2024.1303103 |

4.2 Results in the angular app:

a) when the user is valid the transaction will be stored as a transaction and the admin can see the transaction in the angular app



b) when the user is not a valid user or entered invalid userid and password



V. SECURITY ANALYSIS

In this section, we will provide a brief overview of potential threats and attacks on the overall system, along with discussing handling techniques to ensure the security goals are met.

Decentralization: Blockchain's elimination of centralized authorities or intermediaries enables peer-to-peer authentication processes, fostering resilience to single points of failure and censorship.

Transparency: Transactions recorded on the blockchain offer transparency and auditability, establishing a verifiable trail of authentication activities. This transparency ensures accountability throughout the authentication process.

Immutability: Blockchain's tamper-resistant nature ensures that once authentication transactions are recorded, they remain unalterable and undeletable. This characteristic enhances the integrity and trustworthiness of the authentication process.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303103 |

Privacy: Blockchain-based authentication solutions can empower users with greater control over their personal data and identity information, facilitating self-sovereign identity management and reducing dependence on centralized identity providers.

By addressing these security concerns and leveraging blockchain's features, including decentralization, transparency, immutability, and privacy, we can establish a robust authentication system that meets user needs while ensuring overall system security and integrity.

VI. CONCLUSION

In this paper, we have proposed a system design and implementation of a Blockchain-based solution using Hyperledger Fabric for authentication at scale, in a decentralized manner with no intermediary third party. Our project highlights the potential to revolutionize digital identity management and enhance security in the digital age. By leveraging the decentralized and immutable nature of blockchain technology, organizations can establish more robust, trustworthy, and resilient authentication systems that prioritize user privacy and security. We also provided security analysis and showed that the proposed authentication solution achieves security goals.

REFERENCES

[1] W.L. Sim, H.N. Chua, M. Tahir. “Blockchain for identity management: the implications to personal data protection” (2019)

[2] Gupta, S., Srivastava, S., & Saxena, K. “Decentralized Authentication System Using Blockchain Technology". (2018)

[3] Dorri, A., Kanhere, S. S., & Jurdak, R. **“**Blockchain-based Authentication and Authorization for Secure and Privacy-preserving IoT Systems" (2017)

[4] Zhang, Y., Fang, L., & Jiang, Y. “A Review of Blockchain-based Authentication Protocols" (2019)

[5] Mukherjee, M., & Sen, S. “Blockchain-based Authentication and Authorization Framework for Edge Computing" (2020)

[6] Park, J., Lee, S., & Kim, Y. "Secure Authentication Scheme for IoT Devices using Blockchain Technology" (2021)

[7] Smith, J., Johnson, R., & Williams, E. (2020). Blockchain-based Authentication Mechanism Using Hyperledger Fabric: A Review. International Journal of Blockchain Research

[8] Chen, L., Wang, Q., & Li, X. (2019). Enhancing Authentication and Access Control with Hyperledger Fabric: A Survey. IEEE Transactions on Information Forensics and Security, 14(10), 2536-2551.

[9] Patel, A., Gupta, S., & Sharma, R. (2021). Secure Authentication and Authorization Framework Using Hyperledger Indy. In Proceedings of the International Conference on Blockchain Applications and Technologies (ICBAT).

[10] Kim, S., Lee, J., & Park, H. (2020). Blockchain-based Authentication and Access Control for IoT Devices Using Hyperledger Sawtooth. International Journal of Distributed Sensor Networks, 16(1), 1-12.

[11] Rahman, M., Islam, S., & Ahmed, R. (2021). Decentralized Authentication Protocol Using Hyperledger Besu for Federated Cloud Environments. In Proceedings of the International Conference on Blockchain and Data Science (ICBDS).

[14] Hyperledger Fabric Documentation. (n.d.). Getting Started with Fabric Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-2.5/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details