IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Secure E-Wallet Using Blockchain

Madhavi R.P.
Associate Professor
Dept. of Computer Science
B.M.S College of Engineering

Anika Singh
UG Scholar
Dep.t of Computer Science
B.M.S College of Engineering
Banglore

Anshumaan Chandra
UG Scholar
Dep.t of Computer Science
B.M.S College of Engineering
Banglore

Laasya Hosadurga
UG Scholar
Dep.t of Computer Science
B.M.S College of Engineering
Banglore

Vaishali Kathariya
UG Scholar
Dep.t of Computer Science
B.M.S College of Engineering
Banglore

***Abstract*—The tumultuous events of the past decade, characterized by the unprecedented challenges posed by the Covid-19 pandemic, have catalyzed a profound shift in societal norms and behaviors. The emergence of the "No Contact" era has triggered a seismic transformation in financial transactions, propelling the transition from conventional physical currency exchanges to digital payments. This metamorphosis has highlighted the pivotal role of digital payment systems in facilitating seamless and secure financial transactions in an increasingly digitized world.While digital payment systems have enhanced convenience and security, persistent challenges such as transaction errors, connectivity disruptions, and concerns regarding transaction transparency persist. Addressing these challenges requires the development of a robust and privacy-centric payment system leveraging blockchain technology.This paper advocates for the creation of a novel payment ecosystem that prioritizes privacy and permission mechanisms enforced through a sophisticated blockchain architecture. Integrated with web applications, this ecosystem aims to provide users with secure and transparent financial transactions.In summary, the integration of web applications into a privacy-centric payment ecosystem underpinned by blockchain technology holds the potential to address the challenges facing modern financial transactions while ensuring privacy, security, and transparency.**

Index Terms –Blockchain, E-wallet, web applications

I. INTRODUCTION

The onset of the Covid-19 pandemic heralded a period of unprecedented upheaval and transformation, reshaping the fabric of human interactions and transactions on a global scale. Against the backdrop of this crisis, the concept of contactless interactions gained newfound prominence, precipitating a rapid and decisive shift towards digital payment solutions. This pivotal moment in the evolution of payment methods marked a departure from traditional cash exchanges to the realm of internet banking, and subsequently to the burgeoning domain of e-wallet transactions. The surge in the adoption of payment gateways, digital wallets, and internet banking platforms underscored a growing preference for expeditious and seamless financial transactions in an increasingly interconnected world.

In response to these evolving trends, the integration of web applications has emerged as a key output of this transformative period. Web applications serve as the interface through which users access and interact with various digital payment platforms, offering convenience, accessibility, and enhanced user experience. By enabling users to initiate transactions, manage accounts, and monitor financial activities from any internet-enabled device, web applications have become indispensable tools in the realm of digital finance.

While digital payments have undoubtedly bolstered security measures against theft and fraud, persistent challenges such as erroneous transactions, network failures, and opacity in transaction processes continue to pose significant hurdles in the realm of online payment systems. To address these challenges and fortify the security of financial transactions, there exists an urgent imperative to develop a robust and privacy-centric payment system that harnesses the transformative potential of blockchain technology.

This paper advocates for the creation of a novel payment ecosystem that prioritizes privacy and permission mechanisms enforced through a sophisticated blockchain architecture, thereby fortifying the security of financial transactions and laying the groundwork for a decentralized and secure financial landscape. By integrating web applications with blockchain-based payment systems, this proposed ecosystem aims to enhance transparency, mitigate risks, and empower users with greater control over their financial transactions in the digital age.

II. LITERATURE SURVEY

Paper[1] Addressing the challenges of financial institutions sharing sensitive data and mitigating unknown risks in data security, the study introduces a blockchain-based solution utilizing proxy re-encryption. This approach encompasses both a data sharing protocol and a paradigm for data sharing. Leveraging the decentralized storage, distributed management, and tamper-resistant nature of blockchain technology, researchers establish a secure data sharing mode. The approach implements access control mechanisms on the blockchain platform and simultaneously maintains encrypted data in distributed databases and the blockchain to prevent unauthorized access or leakage of sensitive data. Key components of this data sharing protocol include identity-based proxy re-encryption and distributed key generation technologies. Proxy nodes are selected using the proof-of-stake algorithm, facilitating secure data sharing among users through the re-encryption of sensitive data.

[2]

Existing blockchain relay protocols necessitate instantaneous verification of each relayed block header by the destination blockchain. However, the high computational cost associated with on-chain block header verification poses challenges, particularly in the deployment of relays between Ethereum-based blockchains, resulting in substantial operating costs. To overcome these limitations, researchers introduce a novel relay technique. This approach employs a validation-on-demand pattern along with financial incentives to significantly reduce the operational cost of relays across Ethereum-based blockchains, up to 92 percent. Consequently, this relay architecture enables decentralized interoperability between blockchains such as Ethereum and Ethereum Classic.

[3] As blockchain technology advances, research on digital currency, particularly Central Bank Digital Currency (CBDC), is gaining traction. CBDC holds significant importance for a nation's economic development, requiring more stringent supervision and manageable decentralization compared to other cryptocurrencies. Thus, establishing a technical foundation aligned with economic principles, efficient consensus mechanisms, and network architecture prioritizing resource conservation becomes imperative for the successful implementation of CBDC.

[4]In recent decades, significant technological advancements have reshaped various aspects of human life, notably in the realm of transactions. The introduction of digital payments and currencies has ushered in a new era in financial transactions, revolutionizing how individuals conduct monetary exchanges. However, the adoption of digital currency has been influenced by divergent government policies, which have both facilitated and impeded its acceptance. Despite this, the usage of digital payments continues to rise steadily. Nonetheless, digital payments still lag behind traditional cash transactions due to concerns surrounding security issues, threats, and vulnerabilities, as well as public skepticism regarding their security features. To address these challenges, the study advocates for the utilization of secure and privacy-conscious technologies like blockchain, offering potential enhancements to existing digital payTo streamline transaction processes and enhance operational efficiency while minimizing risks, governments and financial institutions worldwide are under pressure to reduce the duration of payment, clearing, and settlement cycles. To achieve this goal and establish industry-accepted standards, numerous consortia have been established. However, seamless information exchange among different banks and financial entities remains a distant objective. In this paper, a novel architecture is proposed to seamlessly integrate e-wallets from various banks and blockchain-using organizations. This proposed design aims to serve as the foundation for implementing digital ledger technology within the Indian financial sector. Utilizing a swarm-based peer-to-peer network, the suggested approach is anticipated to alleviate the burden on banks' Core Banking Solutions, thus easing strain on servers at data centers.

[6]

A Mobile Ad-hoc Network (MANET) is a network devoid of infrastructure, characterized by nodes that move randomly. MANETs can be established anywhere through the utilization of nodes that move in an unpredictable manner. However, the decentralized nature of MANETs renders them susceptible to numerous security vulnerabilities. These vulnerabilities pose unresolved security risks, making it equally challenging to identify and address these issues. Some security risks are particularly severe, capable of causing network collapse. Researchers are actively developing solutions to mitigate these threats. Among the essential tools for safeguarding MANETs from defects and malicious behaviors is the Network Intrusion Detection (NID) system.

[7],

The electronic voting system plays a pivotal role in reducing the percentage of absentee voting while ensuring the security of the ballots. Leveraging blockchain technology, a distributed and decentralized ledger, transactions are recorded efficiently and verifiably.

[8]Blockchain's importance in the electronic voting system lies in its ability to safeguard votes from tampering through cryptographic methods, ensuring the integrity of data stored in blocks. Integrating Aadhar authentication into the electronic voting system prevents duplication or tampering of votes. By combining biometric data with voter VIDs obtained from the Aadhar database to cast the vote and utilizing digital signatures as encryption keys for votes within the block, this recommended approach establishes a secure e-voting system.

[9] Digital markets have emerged recently to expedite the delivery of software and services to customers, fostering the rapid development of digital goods, services, and applications. Traditionally, marketplaces have acted as intermediaries between producers and consumers, charging producers a commission based on consumer payments. However, this commission-based model often results in an imbalance in value distribution and financial losses for both producers and consumers. To address this issue, a decentralized digital marketplace concept based on blockchain technology has been introduced, eliminating the need for a centralized intermediary

[10] The decentralized approach empowers market participants to conduct transactions reliably and without the involvement of a middleman. Researchers have conducted surveys on Telecommunication Services Marketplaces (TSMs), organizations that predominantly leverage blockchain technology to instill trust and eliminate intermediaries.

III. OBJECTIVES

1. To elucidate the transformative impact of the Covid-19 pandemic on the evolution of digital payment systems and the broader financial landscape, with a specific focus on the integration of web applications as a key objective of the paper.
2. To highlight the persistent challenges faced by existing digital payment systems, including transaction errors,

connectivity disruptions, and transparency concerns, and to explore how the integration of web applications can address these challenges.

3. To propose a novel payment system architecture that prioritizes privacy and permission mechanisms enforced through blockchain technology, while also considering the role of web applications in enhancing user experience and accessibility.

4. To advocate for the integration of digital wallets with diverse banking institutions as part of the proposed architecture, emphasizing the importance of collaboration between traditional financial institutions and emerging digital payment platforms facilitated through web applications.

5. To foster a peer-to-peer network that effectively distributes transaction loads and enhances overall data center security in the financial sector, leveraging the connectivity and scalability offered by web applications to optimize transaction processing and ensure robust security measures.

IV. METHODOLOGY

The methodology employed in this study involves the utilization of a swarm-based peer-to-peer networking architecture. Each participating bank is equipped with a designated number of miners, akin to super nodes, that are resilient and resistant to failures. The network addresses of all miners are disclosed to customers requesting an e-wallet from their bank, allowing them to initiate the registration process. During registration, a public and private key pair is generated, with the public key automatically updated by the miner. The e-wallet program synchronizes the user's cash book with the blockchain data when an offline user is ready to conduct a transaction. Transactions, defined as payments or monetary transfers digitally signed by the initiator or recipient using their private keys, are recorded in the blockchain by miners. The key scenarios addressed by miners include cash transfers from personal bank accounts to e-wallets, money exchanges between distinct e-wallets, and cash transfers from e-wallets to bank accounts.

The methodology encompasses three primary transaction scenarios that are facilitated and recorded by miners in the blockchain. These scenarios include cash transfers from personal bank accounts to e-wallets, money exchanges between two distinct e-wallets, and cash transfers from e-wallets to bank accounts. Each transaction is digitally signed by the initiator or recipient using their private keys, ensuring the security and transparency of the transaction process within the blockchain network.

SHA-256 is a widely used cryptographic hash function that generates a unique fixed-size hash value (256 bits) for any given input data. By applying SHA-256 to transaction data before adding it to the blockchain, the integrity of the transaction history can be ensured. Integrating SHA-256 into the methodology enhances the security of the blockchain by mitigating various types of attacks. One significant threat is data tampering, where malicious actors attempt to modify transaction data stored in the blockchain. By applying SHA-256 to transaction data, any alteration to the original data will result in a completely different hash value. Therefore, even a small change in the input data will produce a vastly different hash value, making it virtually impossible for attackers to modify transaction records without detection.

Another threat is replay attacks, where attackers intercept and duplicate legitimate transactions to fraudulently repeat them at a later time. SHA-256 ensures that each transaction is uniquely hashed before being added to the blockchain, acting as a digital fingerprint for the transaction. This prevents replay attacks as each transaction is securely timestamped and cannot be duplicated without authorization.

Furthermore, SHA-256 helps prevent data forgery by securely hashing each transaction before adding it to the blockchain. This cryptographic hash serves as a digital seal, verifying the authenticity and integrity of the transaction data. Any attempt to forge transactions or introduce counterfeit data into the blockchain would be immediately detected due to the inconsistency between the original data and its hash value.

In addition to employing SHA-256 for securing transaction data within the blockchain, this methodology further enhances the security of blockchain wallets by implementing a robust method utilizing a 12-word seed phrase. The 12-word seed phrase, serving as a master key to access the wallet, undergoes rigorous encryption using the SHA256 algorithm. This process fortifies the protection of user funds against unauthorized access by adding an extra layer of cryptographic security. By encrypting the seed phrase with SHA-256, the methodology ensures that even if the seed phrase is intercepted, it remains virtually impossible for malicious actors to decipher it without proper authorization. Consequently, users can have greater confidence in the safety and integrity of their funds stored within the blockchain wallet, knowing that their access keys are fortified by advanced cryptographic measures.

V. CONCLUSIONS:

This paper presents a secure e-wallet design that uses blockchain technology. It's the first of its kind to require e-wallets to work with blockchain. It also outlines a way for e-wallets from different banks and organizations to communicate easily. This approach helps reduce the strain on banks' systems, lessens server workload, and spreads out processing tasks across different centers.

VI. REFERENCES

[1] R. Q. Wkh *et al.*, “$) Lqdqfldo Gdwd Vhfxulw \ Vkdulqj Vroxwlrq Edvhg Rq Eorfnfkdlq Whfkqrorj \ Dqg Sur [\ Uh Hqfu \ Swlrq Whfkqrorj \,” pp. 5–8.

[2] P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte, “ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains,” *Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020*, pp. 204–213, 2020, doi: 10.1109/Blockchain50366.2020.00032.

[3] J. Zhang *et al.*, “A Hybrid Model for Central Bank Digital Currency Based on Blockchain,” *IEEE Access*, vol. 9, pp. 53589–53601, 2021,

doi: 10.1109/ACCESS.2021.3071033.

[4] A. Vijayan, A. M. Ashique, M. K. Karunattu, A. John, and M. J. Pillai, "Digital Payments: Blockchain based Security Concerns and Future," *Proc. - Int. Conf. Smart Electron. Commun. ICOSEC 2020*, no. Icosec, pp. 429–435, 2020, doi: 10.1109/ICOSEC49089.2020.9215431.

[5]
K. Singh, N. Singh, and D. Singh Kushwaha, "An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain," *2018 Int. Conf. Comput. Power Commun. Technol. GUCON 2018*, pp. 165–169, 2019, doi: 10.1109/GUCON.2018.8674919.

[6]
N. P. Sable, V. U. Rathod, P. N. Mahalle, and D. R. Birari, "A Multiple Stage Deep Learning Model for NID in MANETs," *2022 Int. Conf. Emerg. Smart Comput. Informatics, ESCI 2022*, pp. 1–6, 2022, doi: 10.1109/ESCI53509.2022.9758191.

[7]
T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," *2nd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2020 - Conf. Proc.*, no. Icimia, pp. 71–75, 2020, doi: 10.1109/ICIMIA48430.2020.9074942.

[8]
R. V. Tkachuk, D. Ilie, K. Tutschku, and R. Robert, "A Survey on Blockchain-Based Telecommunication Services Marketplaces," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 228–255, 2022, doi: 10.1109/TNSM.2021.3123680.

[9] D. P. Gadekar, N. P. Sable, A. H. Raut, "Exploring Data Security Scheme into Cloud Using Encryption Algorithms" *International Journal of Recent Technology and Engineering (IJRTE)*, Published By:Blue Eyes Intelligence Engineering & Sciences Publication, ISSN: 2277-3878, Volume-8 Issue-2, July2019, DOI: 10.35940/ijrte.B2504.078219, SCOPUS Journal.

[10] N. P. Sable, S. R. Powar, Q. Fernandes, N. A. Gade, and A. B. Shingade, "Pragmatic Approach for Online Document Verification Using Block-Chain Technology," *ITM Web Conf.*, vol. 44, p. 03001, 2022, doi: 10.1051/itmconf/20224403001.