INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1050-1054

BLOCKCHAIN-BASED BANKING SYSTEM: A SECURE BANKING TRANSACTION

Ekta Anturkar[1], Umema Bhatkar[2], Saniya Inamdar[3], Sayali Karmode[4]

[1,2,3]Student of Department of Information Technology, MGM College of Engineering and Technology, Navi Mumbai, Maharashtra, India.

[4]Faculty of Department of Information Technology, MGM College of Engineering and Technology, Navi Mumbai, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS33332

ABSTRACT

Banking systems can transition from their traditional methodologies to a digital, immutable, distributed ledger that can be implemented via Blockchain, thanks to ever-evolving technologies. Blockchain technology is a peer-to-peer linked distributed structure that can solve the problem of maintaining and recording transactions in a banking system. Transparency, robustness, auditability, and security are all characteristics of blockchain. This paper aims to provide these functionalities in a distributed banking system based on blockchain that is comparable to current methodologies. It will also cover the limitations of blockchain implementation as well as the future scope.

Keywords: Banking, Blockchain Technology, Transaction, Security,

1. INTRODUCTION

A blockchain system may be considered as a simply incorruptible cryptographic database where vital and confidential user's information will be recorded. The system is maintained by a net- work of computers, which is accessible to anyone running the software. Blockchain operates as a pseudo-anonymous system that has nonetheless privacy problem in view that all transactions are exposed to the general public, even though it is tamper-proof inside the sense of data integrity. The access control to manage heterogeneous user's confidential records across a couple of MNC establishments and devices had to be cautiously designed. Blockchain itself isn't designed as a massive-scale storage system. Within the context of framework for secure banking, a decentralized storage solution would significantly complement the weak point of blockchain within the perspective. The blockchain network as a decentralized system is extra resilient in that there is no single-point assault or failure compared to centralized systems. However, because all the bit coin transactions are public and everyone has got right of entry to, there already exists analytics equipment that picks out the members within the community based totally on the transaction records [2]. The most important module is blockchain implementation comprises two kinds of records: blocks and transactions. In every block contains a timestamp and a link to a preceding block is supplied via the secure hash algorithm. During the storage, the transaction information into the blockchain system executes various algorithms like SHA for hash generation, mining for generating a valid hash, smart contract for system policy, and consensus for validating current blockchain on all Peer to Peer nodes. Therefore, banking application is more secure. Second thing is that data storage and accessibility. For this point use the Secret Shamir hashing technique and keyword as well as content-based cryptography techniques.

1.1. ARCHITECTURE OF BLOCKCHAIN

The blockchain is sequence of blocks which hold the information about transactions between nodes of a network. Block Header consists of Block version, Merkle tree, Time Stamp, n Bit, Nonce, and Parent Block Hash.

Block Version: This is like a set of rules that the block must follow. It ensures that everyone in the network is on the same page regarding how a block should be created and validated.

Merkle Tree: Imagine this as a way to organize all the transactions in the block. It's like a structure that summarizes and securely combines all the individual transaction details.

Time Stamp: This is just the time when the block is created. It helps to organize the blocks chronologically.

n Bit and Target Threshold: These are technical details that involve creating a hash (a unique code) for the block. Miners (participants who validate and add blocks) need to adjust some parameters to make sure the hash meets certain criteria, ensuring the security of the blockchain.

Nonce: Nonce is like a special tool that miners use to find the right combination of numbers needed to create a valid hash. They adjust the Nonce until they get the correct hash that meets the criteria.

Parent Block Hash: This is the hash value of the previous block in the chain. It's like a connection between blocks, making sure they are linked in a secure and unbreakable way.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

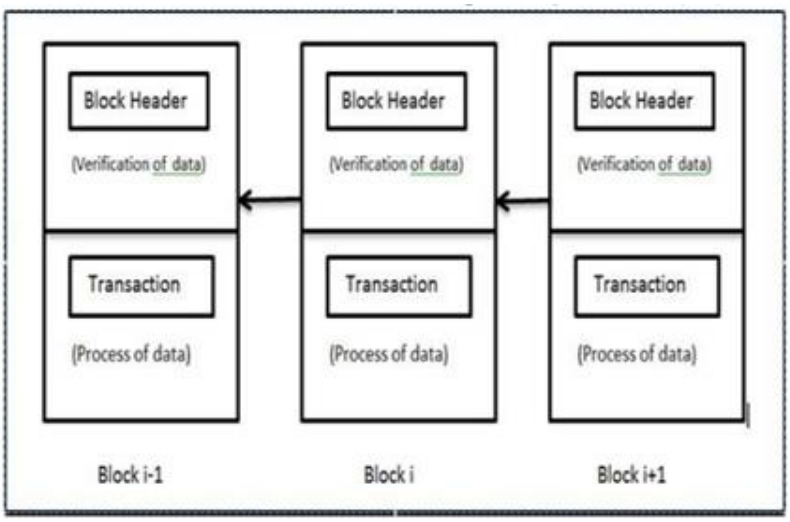
Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1050-1054

Mining and Hash Calculation: Miners are like puzzle solvers. They adjust the Nonce and use the information in the block header to calculate a unique hash for the block. This process is called mining. It ensures that each block is secure, unchangeable, and fits perfectly into the existing blockchain.

Transaction Counter stores the number of transactions that are completed by the block [12].



2. PROBLEM DEFINITION AND OBJECTIVES

The world is changing incredibly fast, and we are not all aware of it. Blockchain technology and crypto-currencies are an irreversible advancement that is disrupting established industries and the ways in which we interact financially. For that reason, understanding and being aware of this blockchain wave is incredibly important. The existing systems work as centralized architecture in database system.

2.1 Goals and Objectives

The objectives of this research paper are as follows:

- Implement cryptographic techniques to secure transactions and user identities, reducing the risk of fraud and unauthorized access.
- Utilize smart contracts to automate and enforce secure transaction protocols, minimizing the potential for human errors.
- Establish a secure and tamper-resistant data structure using blockchain, ensuring the integrity of transaction records.
- To improve the efficiency operations at each stage.

2.2 Limitations

- Technology Maturity: Blockchain technology is still evolving, and the maturity of certain features, protocols, and tools may limit the project's ability to leverage the latest advancements.
- Speed of Transactions: While blockchain ensures security, the time taken to reach a consensus on transactions may not meet the real-time processing expectations of the banking industry.
- Data Privacy Concerns:Despite cryptographic measures, concerns related to the privacy of sensitive customer data may arise, particularly in the context of adhering to stringent data protection regulations.
- Human Error in Smart Contracts: Smart contracts are code-based, and errors in the code or vulnerabilities may lead to unexpected outcomes, emphasizing the need for rigorous testing and auditing.
- Limited Adoption: The widespread adoption of blockchain in the banking sector may take time, and the project may face challenges in gaining industry-wide acceptance.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

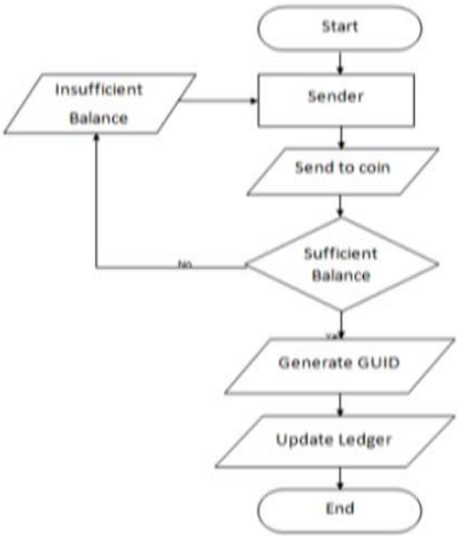
e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1050-1054

2.2 Flowchart



3. LITERATURE REVIEW

Satoshi Nakamoto et.al [4] mentioned a peer to peer electronic cash system (Bitcoin). 2016. Online Payments or transaction where directly send from one party to another without going through a financial institution which undergoes peer to peer communication. Digital signatures play a role in protection at a limit. The proposed system uses a verification of data and secure transmission of money through bank validation. Smart Contracts also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened. Currently CSIRRO team has proposed a new approach to integrate Block on IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Block wheels are especially used to provide access control system for Smart- Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features; however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms. Moreover, this technology cannot provide a general form of block-chain solution in case of IOT usage.

4. PROPOSED SYSTEM

In the security system developed using blockchain, there are four essential modules that play key roles: user authentication, user and transaction verification, authentication server, and authorization. Blockchain, in this context, is a digital and unchangeable ledger that records transactions in a chronological order, almost instantly. Think of it like an uneditable digital notebook where every transaction gets written down in the order it occurs. in the blockchain implementation, we have two main types of records: blocks and transactions. A block is like a page in the notebook, and each page has a timestamp, showing when the transactions on that page happened. Importantly, each page is linked to the one before it through a secure hash algorithm. This linkage creates a chain, making it hard for anyone to tamper with past transactions because it would change the entire chain, and everyone in the network would notice. It's a bit like having a notary public for every page of your digital notebook, ensuring the authenticity of every transaction. The protection gateway is an extension of this blockchain framework, adding an extra layer of security. It's like a virtual gatekeeper that uses the information in the blockchain to check and verify users and transactions. This way, the system ensures that only authorized users can access certain information or perform specific transactions, adding a robust layer of security to the overall process. So, in simple terms, the security system is like a super-secure digital notebook with a vigilant gatekeeper, ensuring that all transactions are authentic, transparent, and tamper-proof.

5. ADVANTAGES

Immutable Ledger: This feature enhances transparency and trust in banking transactions, reducing the risk of fraud.

Enhanced Security: Blockchain employs cryptographic techniques to secure transactions, making it extremely difficult for unauthorized parties to tamper with the data. Transparent Transactions: Every transaction on a blockchain network is transparent and verifiable by all participants. This transparency fosters trust among users. Faster Transactions:

Blockchain-based banking systems enable near-instantaneous transactions by removing intermediaries and automating processes through smart contracts.

6. CONCLUSION

This system proposes a secure and efficient method for storing data on the cloud using blockchain technology and encryption. By decentralizing the structure, it ensures data security. The security model, inspired by banking transactions, employs efficient algorithms, minimizing time requirements while providing high-level data security on the cloud. This architecture makes the system robust against unauthorized users attempting to steal or expose user information. In conclusion, the security level of banking transactions has significantly improved, enhancing the overall convenience of the banking process.

of blockchain-based voting systems represent an important step towards modernizing electoral processes and fostering trust in democratic institutions.

7. REFERENCES

[1] S. Gore, S. Hamsa, S. Roychowdhury, G. Patil, S. Gore and S. Karmode, "Augmented Intelligence in Machine Learning for Cybersecurity: Enhancing Threat Detection and Human-Machine Collaboration," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 638-644, doi: 10.1109/ICAISS58487.2023.10250514.

[2] Layth Almahadeen, Renzon Daniel Cosme Pecho, Murugananth Gopal Raj, Nichenametla Rajesh, Zainab Mohammed Imneef, Sayali Karmode Yelpale, “Digital Investigation Forensic Model with P2P Timestamp Blockchain for Monitoring and Analysis” , Journal of Electrical System, Vol. 1, No 1, (2024): 09-17 (DOI : https://doi.org/10.52783/jes.656)

[3] Sayali Karmode, Security Challenges for IoT Based Applications & Solutions Using Fog Computing: A Survey, Journal of Journal of Cybersecurity and Information Management, Vol. 3 , No. 1 , (2020) : 21-28 (Doi : https://doi.org/10.54216/JCIM.030103)

[4] M. S. K. Yelpale, “Security and privacy challenges in cloud computing: a review,” Journal of Cybersecurity and Information Management, vol. 4, no. 1, pp. 36–45, 2020. View at: Google Scholar

[5] Sayali Karmode Yelpale, “IOT Technology for Pandemic Situation”, NJITM, vol. 4, no. 2, pp. 25–27, Jan. 2022 https://mbajournals.in/index.php/JoITM/article/view/806.

[6] Karmode, S. S., & Bhagat, V. B. (2017). DETECTION AND BLOCKING SOCIAL MEDIA MALICIOUS POSTS. International journal of modern trends in engineering and research, 4(5).

[7] Kermode, S. S., & Bhagat, V. B. (2016). A Review: Detection and Blocking Social Media Malicious Posts. Int. J. Mod. Trends Eng. Res, 3(11), 130-136. doi: 10.21884/IJMTER.2016.3133.Q4M8O .

[8] Prof. Bhushan B. Thakare, Prof. Sayali Karmode Yelpale, “Smart Home with Edge Computing”, International Journal of Interdisciplinary Innovative Research & Development (IJIIRD), Vol 6, 2021 https://ijiird.com/wpm content/uploads/CSE016-1.pd

[9] Sayali Karmode, “Blockchain Technology Security Issues and Concerns : A Review”, International Research Journal of Modernization in Engineering Technology and Science, Vol 6, Issue 03, March 2024

[10] Sabout Nagaraju and Latha Parthiban, “Trusted framework for online banking in public cloud using multifactor authentication and privacy protection gateway,” Open Access Journal of Cloud Computing: Advances, Systemsand Applications (2015)

[11] Dorri, S. S. Kanhere and R. Jurdak, “Blockchainin internet of things: Challenges and Solutions,” arXiv: 1608.05187 [cs], 2019.

[12] Sukhodolskiy,Ilya, and Sergey Zapechnikov. “A blockchain-based access control systemfor cloud storage.” Young Researchers in Electrical and Electronic Engineering (EICon-Rus), 2018 IEEE Conference of Russian IEEE, 2018.

[13] Yang, Huihui, and Bian Yang. “A Blockchain-based Approach to the Secure Sharing of Healthcare Data.”Proceedings of the Norwegian Information Security Conference. 2020.

[14] Goyal, Vipul, et al. “Attribute-based encryption for fine-grained access control of encrypted data.”Pranav Chavan, Harshraj Deshmukh, Aakash Dhotre, Aditya Gharat, Sayali Karmode, “Blockchain Democracy Evaluating a Secure Voting System”, International Research Journal of Modernization in Engineering Technology and Science, Vol 6, Issue 03, March 2024 DOI : https://www.doi.org/10.56726/IRJMETS50478

[15] B. J. Dange, Kaustubh Manikrao Gaikwad, H. E. Khodke, Santosh Gore, S. N. Gunjal, Kalyani Kadam, Sayali Karmode, “Machine Learning for Quantum Computing Bridging the Gap between AI and Quantum Algorithms”, Int J Intell Syst Appl Eng, vol. 12, no. 21s, pp. 600–605, Mar. 2024.