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 05, May 2024, pp: 17-20

STUDENT ATTENDANCE MANAGEMENT SYSTEM USING BLOCKCHAIN

Tejas prasade[1], Ronak waghela[2], Bhagyashree Yadav[3], Sayali Karmode[4]

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

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

ABSTRACT

The Conventional Approaches To Controlling Student Attendance In The Classroom Include Flaws That Make Them Manipulable. This Study Offers An Innovative Solution That Uses Blockchain Technology To Control Student Attendance In Order To Overcome These Issues. The Goal Of The Blockchain-Based Student Attendance Management System Is To Guarantee Authenticity And integrity by offering a safe, transparent, and unchangeable record of student attendance.

Keywords: Attendance, Blockchain Technology, Transaction, Security,

1. INTRODUCTION

An essential component of educational institutions is the management of student attendance, which promotes successful learning outcomes, accountability, and student participation. However, manual errors, manipulation potential, and a lack of transparency are common problems with traditional ways of managing attendance. The implementation of blockchain technology has shown promise in recent times as a means of resolving these issues by offering an unchangeable and secure foundation for data management. Originally created as the foundational technology for digital currencies such as bitcoin, blockchain functions as a distributed ledger, recording transactions over a network of computers.

Every transaction, or block, is cryptographically connected to the one before it, creating a chain of blocks that cannot be changed backward without the network's users' agreement. Blockchain's decentralized structure guarantees By utilizing preset parameters like time, place, and biometric authentication, these smart contracts may automatically confirm attendance, relieving instructors of administrative duties and lowering the possibility of human error. Additionally, the confidentiality and integrity of student attendance data are improved using blockchain technology. The decentralized nature of blockchain ensures that there is no single point of failure, making it highly resistant to tamperin ,hacking, or data manipulation. Each transaction on the blockchain is cryptographically secured, and consensus mechanisms ensure that the integrity of the data is maintained across the network.

1.1. ARCHITECTURE OF BLOCKCHAIN

The blockchain is a collection of blocks that contains data regarding exchanges between network nodes. Block version, Merkle tree, Time Stamp, n Bit, Nonce, and Parent Block Hash make up the Block Header.

Block Version: This resembles a set of guidelines that the block ought to abide by. It makes sure that everyone in the network understands the proper way to generate and validate a block.

Merkle Tree: Consider using this to arrange every transaction in the block. It functions similarly to a structure that securely compiles and summaries every detail of each individual transaction.

Time Stamp: This is simply the moment at which the block is formed. The blocks are better arranged chronologically.

n Bit and Target Threshold: These are the technical aspects that entail generating a block's hash, or unique code. In order to ensure the blockchain's security, miners—participants who validate and add blocks—must modify a few parameters to ensure the hash satisfies specific requirements.

Nonce: Miners employ nonce, which is akin to a specialized tool, to determine the precise set of integers required to produce a valid hash. Until they obtain the right hash that satisfies the requirements, they modify the Nonce.

Parent Block Hash: This is the chain's previous block's hash value. It ensures that the blocks are connected in a safe and reliable manner, much like a connection between blocks.

Mining and Hash Calculation: Miners tackle puzzles in a similar way. To create a unique hash for the block, they modify the Nonce and make use of the data in the block header. We term this process mining. It guarantees that every block is safe, immutable, and precisely aligned with the current blockchain.

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

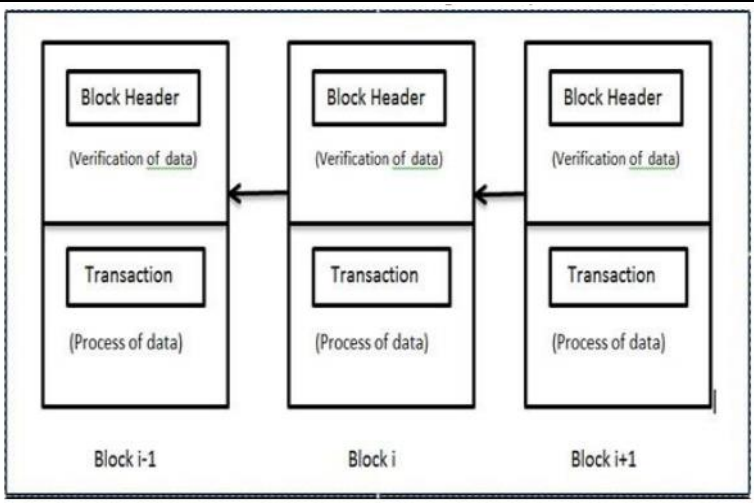
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 17-20



2. PROBLEM DEFINITION AND OBJECTIVES

We are not all conscious of how quickly the world is changing. Cryptocurrencies and blockchain technology are an irreversible development that is upending traditional business models and our financial interactions. It is crucial to comprehend and be aware of this blockchain wave as a result. The current systems function as database systems with centralized architecture.

2.1 Goals and Objectives

The objectives of this research paper are as follows:

- To guarantee the transparency and immutability of attendance records, implement a blockchain-based student attendance system.
- Employ cryptographic elements of blockchain technology to improve the security of student attendance data. Put strong authentication and encryption procedures in place to protect attendance records from manipulation, tampering, and unwanted access.
- Use blockchain smart contracts to enable the real-time recording and verification of student attendance. To ensure accuracy and dependability, automate the attendance recording process based on established parameters like time, location, and biometric authentication.
- To increase each stage's operational efficiency.

2.2 Limitations

Regulatory compliance: Educational establishments are required to make sure that they are in compliance with data protection laws like FERPA and GDPR. Concerns about data ownership, permission, and storage procedures are brought up legally and regulatory when sensitive student information is kept on a blockchain.

- User adoption: Stakeholder resistance to the adoption of blockchain-based attendance systems may originate from a lack of knowledge with the technology or worries about its security and veracity. Gaining users' faith in the system and educating them may take a lot of time and work.
- Centralized risk: Despite the fact that blockchain is sometimes hailed for its decentralization, many implementations actually depend on centralized elements like node infrastructure or consensus processes.
- Environmental Impact: Certain blockchain networks employ Proof of Work consensus processes, which take a significant amount of energy. Technological Obsolescence: Blockchain technology is still developing, with new breakthroughs and developments appearing on a regular basis.

3. LITERATURE REVIEW

Give a summary of blockchain technology's application in the education sector, highlighting how it could be able to help with issues related to student attendance tracking. Introduce the idea of blockchain-based, transparent, and secure decentralized ledger systems. Examine the drawbacks and inefficiencies of the conventional approaches used in educational institutions to monitor student attendance. Talk about the significance of precise attendance monitoring for administrative and educational goals. Find and compile scholarly publications, research papers, and conference proceedings that have undergone peer review and that discuss or assess blockchain-based attendance systems. Examine each study's methods, conclusions, and contributions, concentrating on the advantages and difficulties of

implementing blockchain technology. Examine the architectural and technological elements of blockchain-based attendance systems, taking into account smart contracts, blockchain platforms, consensus techniques, and data privacy issues. Talk about several strategies. provide case studies or pilot projects that demonstrate the use of blockchain technology for tracking student attendance in authentic learning environments. Analyze the results, difficulties encountered, and lessons discovered from these implantations, taking into account user opinions and system functionality.

4. PROPOSED SYSTEM

Four fundamental modules—user authentication, user and transaction verification, authentication server, and authorization—play crucial roles in the blockchain-based security system. In this sense, blockchain refers to a digital, immutable database that virtually instantly records transactions in a chronological manner. Imagine it as an unchangeable digital notebook where each transaction is recorded in the exact order that it happens.

Blocks and transactions are the two primary record types in the blockchain system. Similar to a page in a notebook, a block also carries a timestamp that indicates the date and time of the transactions on it. Crucially, every page is connected to the previous one using a safe hash technique. Because of the chain that is created by this linkage, it is difficult for someone to tamper with previous transactions because everyone in the network would be alerted and the entire chain would alter. A notary public for each page of your digital notebook, guaranteeing the legitimacy of each transaction, is how it works.

This blockchain foundation is expanded with the protection gateway, which offers an additional degree of security. It functions similarly to a virtual gatekeeper by checking and validating users and transactions using data from the blockchain. In this approach, the system adds a strong layer of security to the entire process by guaranteeing that only authorized individuals can access certain data or carry out specific transactions. To put it simply, the security system makes sure that every transaction is genuine, transparent, and impervious to tampering. It functions similarly to an extremely secure digital notepad with a watchful gatekeeper.

5. ADVANTAGES

Transparency: An unchangeable and transparent ledger of attendance records is made possible by blockchain technology. Transparency and accountability are ensured by providing real-time attendance data access to all parties involved, including administrators, students, and instructors.

Security: The confidentiality and accuracy of attendance records are guaranteed by blockchain cryptography characteristics. Due to the cryptographic security of each transaction and its correlation with the preceding one, it is very impossible for unauthorized parties to manipulate or alter attendance data.

Decentralization: Because blockchain relies on a decentralized network of nodes, managing attendance records no longer requires a central authority.

Faster Transactions: Blockchain-based banking systems use smart contracts to automate procedures and eliminate middlemen, enabling almost immediate transactions.

6. CONCLUSION

An important development in educational administration is the use of blockchain technology to create a student attendance system. Many of the issues with conventional attendance management systems can be solved by educational institutions by utilizing the decentralized, transparent, and unchangeable features of blockchain technology.

An attendance system built on blockchain has many important advantages, such as cost-effectiveness, automation, transparency, and security. Blockchain's transparent and unchangeable ledger guarantees tamper-proof, accurate, and reliable attendance records, which promotes accountability and confidence among stakeholders.

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] 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.