Grenze International Journal of Engineering and Technology, June Issue

Data Security System using Blockchain Technology

Aparna R[1], Indushree Manjunatha Hegde[2], Meghana V S[3], Khushi Vardiya[4] and Komal[5]
[1-5]Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India
Email: raparna@sit.ac.in, { indushree.1si19is023@gmail.com,meghana.1si19is035@gmail.com,
khushi.1si19is028@gmail.com, komal.1si19is030@gmail.com}

***Abstract*— Security has grown to be of utmost importance to both organizations and individuals in the current digital age. It has been shown that conventional centralized systems are susceptible to hacks, data breaches, identity theft, and unauthorized access. The proposed project suggests a data security solution that harnesses the potential of blockchain technology and consensus algorithms to address this issue. It makes use of some of the fundamental properties of blockchain, like decentralization, immutability, and transparency, to build a reliable and impenetrable infrastructure for data management and storage. The use of a distributed ledger reduces the danger of a single point of failure and improves data integrity by storing data across numerous nodes. In addition, the immutability of blockchain records guarantees that once information is entered to the ledger, it cannot be changed or removed without agreement from the network's users. Further, to ensure the quality and consistency of the data kept in the blockchain, the system adds a consensus mechanism, such as proof-of-stake, to validate and verify transactions. The decentralized consensus model decreases the possibility of data manipulation or tampering by doing away with the necessity for a central authority. A strong solution to protect student data is provided by the suggested blockchain-based data security system for a student portal. The system improves trust, privacy, and security in the educational ecosystem by utilizing the inherent characteristics of blockchain, such as decentralization, transparency, immutability, and cryptographic security. This promotes a safer and more dependable digital infrastructure for students, educators, and educational institutions alike.**

***Index Terms*— Data Security, Consensus and Blockchain.**

I. INTRODUCTION

Students and educational institutions have greatly benefited in recent years from the digitalization of educational systems. But as our reliance on technology grows, we have serious worries about the security and privacy of student data. Educational institutions are prime targets for hostile actors because they hold enormous volumes of sensitive information, including financial information, academic records, and personal information.

Traditional data security strategies, such as perimeter-based defense and centralized databases, have been shown to be ineffective against sophisticated cyber threats. The confidentiality and integrity of student data are at risk because these systems are vulnerable to single points of failure, unauthorized access, and other security flaws. To overcome these obstacles, a novel strategy is needed that makes use of cutting-edge technologies to build a strong and reliable data security system.

With its inherent qualities of decentralization, transparency, immutability, and cryptographic security, blockchain technology, which was first introduced as the underlying technology underpinning cryptocurrencies like Bitcoin,

Grenze ID: 01.GIJET.10.2.525

has emerged as a potent alternative. A new paradigm may be formed to guarantee the confidentiality, integrity, and accessibility of student data by bringing blockchain concepts to the field of student data security
Blockchain-based data security mechanism for a student management, intends to provide secure and open environment for managing, storing, and exchanging student data. The solution improves trust, privacy, and security within the educational environment by utilizing the decentralized and tamper-resistant properties of blockchain.
The key idea behind the suggested solution is the use of a blockchain as a distributed, unchangeable ledger. The blockchain is used to securely encrypt and store student data, including attendance, academic records, and personal information. The integrity of the data is ensured by linking each entry to a distinct identifier. Additionally, smart contracts that enforce predetermined rules and permissions based on user roles and authentication procedures are used to control access to student data. A consensus mechanism, such as proof-of-stake, is also incorporated into the system to confirm and verify the transactions that are stored on the blockchain.
Overall, the proposed blockchain-based data security system offers a potential response to the problems traditional student data management systems must deal with. The solution improves data privacy, security, and transparency by using the inherent qualities of blockchain, promoting a secure and dependable environment for students, teachers, and educational institutions. The technical elements and advantages of the suggested system will be covered in detail in the parts that follow, and we will show how they could completely alter how student data is protected and handled in the modern era.

II. Related Works

A review of numerous articles and research projects being done on the subject to data security system has been conducted in this part.
In research paper[1], the authors examine the potential of block chain technology in enhancing data security and privacy within the context of the Internet of Things (IoT). The authors acknowledge that a lot of sensitive data is produced by IoT devices, raising questions about the security and privacy of such data. They look at the viability of using block chain as a solution to these problems. They go through several strategies and methods, such as data encryption, access control, and decentralized consensus procedures, that have been put forth by researchers to use blockchain technology for safeguarding IoT data. The survey carried out by Simaiya et al.'s sheds light on the present state of research in this area and highlights the possible advantages and drawbacks of blockchain technology for boosting data security and privacy in the Internet of Things. For researchers and practitioners interested in using blockchain to secure IoT data and reduce privacy issues, this work is an invaluable resource.
Similar research [2], Nakamoto's work on Bitcoin introduced the idea of a decentralized and immutable ledger, which has sparked a number of research on using blockchain for secure data transfer and storage. To further improve the security of data stored on blockchains, numerous alternative cryptographic methods and consensus procedures have been suggested. To safeguard data integrity and secrecy, for instance, Merkle tree-based data structures and asymmetric encryption methods have been used. Studies have also concentrated on how to combine blockchain with other technologies like the Internet of Things (IoT) and cloud computing to offer a comprehensive security framework. Overall, the literature emphasizes the potential of blockchain technology to address data security issues and provides insightful information on how to adopt and optimize it to provide strong data protection.
Similar research [3], contrast the advantages and disadvantages of Proof of Work (PoW) and Proof of Stake (PoS) consensus algorithms. The authors acknowledge that the widespread use of PoW in blockchain networks like Bitcoin is a result of its decentralization and security characteristics. Highlights the PoW's energy inefficiency and computation requirements, raising concerns about sustainability. The authors investigate the PoS approach to address these issues, which replaces the resource-intensive mining process with a system where validators are selected based on the quantity of bitcoin they hold. In order to evaluate the benefits and downsides of both PoW and PoS,. They investigate things like stake concentration effects, the possibility of double-spending assaults, and resil
The authors recognize that the Proof of Work (PoW) consensus mechanism used by Ethereum currently has drawbacks in terms of scalability, energy use, and centralization issues in [8]. The Casper FFG protocol, which combines Proof of Stake (PoS) with Byzantine fault tolerance to obtain consensus, is presented in the article as a solution to these problems. The authors present a thorough literature review of Byzantine fault tolerance, PoS, and related ideas while stressing the advantages and disadvantages of the Casper FFG protocol. They go over how the protocol increases scalability, efficiency, and security while also improving the fairness and security of the

validation process. The survey contributes to ongoing research on consensus mechanisms in blockchain systems and is a useful tool for comprehending the conception and use of the Casper FFG protocol in Ethereum.
Similar research [4], author has investigated the energy consumption patterns of two prominent consensus mechanisms: Proof of Work (PoW) and Proof of Stake (PoS). The authors acknowledged that PoW-based blockchains, such as Bitcoin, require substantial computational power and energy consumption due to the competitive mining process. To address this issue, they explored the PoS mechanism, which replaces the energy-intensive mining process with a more energy-efficient staking process. To support their findings, the authors surveyed relevant literature on blockchain energy consumption, including studies analyzing the environmental impact and energy efficiency of different consensus algorithms. By synthesizing and comparing existing research, author has contributed to the understanding of energy consumption in blockchain systems, shedding light on the potential benefits and trade-offs between PoW and PoS consensus mechanisms.

III. Motivation

In today's rapidly evolving digital landscape, the security of data has become a paramount concern. With the increasing frequency of data breaches and unauthorized access incidents, there is an urgent need for an innovative solution that can safeguard the privacy and integrity of information.
Blockchain is useful in this context because it provides a decentralized and tamper-resistant platform for storing and managing data. It ensures transparency, immutability, and data integrity, making it difficult for unauthorized parties to access or manipulate the information without proper authorization.
The motive of the project is to provide a robust and resilient defense against potential threats using blockchain technology. Through the development and implementation of this cutting-edge solution, we strive to empower educational institutions with the means to protect sensitive student data, ensuring a secure and trustworthy environment for learning and growth. Another intention is to use Consensus algorithm to enhance the overall security and integrity of the system by establishing trust among the network participants and maintaining a consistent and verifiable record of student data.

IV. Problem Statement

Developing a blockchain-powered data security system employing consensus algorithms, aiming to fortify the protection of student data. With the proliferation of data breaches and unauthorized access incidents in today's world, this solution is designed to ensure the confidentiality and integrity of crucial educational information.

V. Design And Implementation

The flow chart in Fig 1 depicts the data security process for a student management system that employs blockchain technology and the Proof of Stake consensus method[1].
The procedure starts with the User Interface, which allows authorized users to generate announcements and test results. Data Validation checks the entered data for accuracy and completeness. Following that, the Proof of Stake Consensus process validates the data and assures its security.
Following validation, a new block containing data is produced. This block is subsequently merged into the current blockchain, ensuring the data's immutability and transparency.
Proof-of-Stake (PoS) is a consensus mechanism that plays a crucial role in the proposed blockchain-based data security system. Unlike traditional consensus mechanisms like Proof-of-Work (PoW), PoS does not rely on computational power but instead on the ownership of cryptocurrency tokens. In a PoS system, participants, referred to as validators, are chosen to create new blocks and validate transactions based on the number of tokens they hold and are willing to stake as collateral.
In addition to using less energy than PoW, this method offers a more scalable and effective way to reach consensus in blockchain networks. We can increase the overall security and dependability of the student data management process by implementing PoS in the system and ensuring the authentication and verification of transactions that are recorded on the blockchain.
PoS has a number of benefits over PoW, one of which is energy efficiency. PoS uses a lot less processing resources because validators are not required to solve challenging mathematical puzzles. This not only lessens the impact on the environment but also enables scalability and quicker transaction processing. Additionally, PoS offers a higher level of protection against attacks like 51% attacks. An attacker in a PoS system would have to have a majority

interest in the network in order to execute such an attack, which becomes more challenging and expensive as the network expands. As a result, PoS-based blockchain networks are more secure and resistant to centralization.

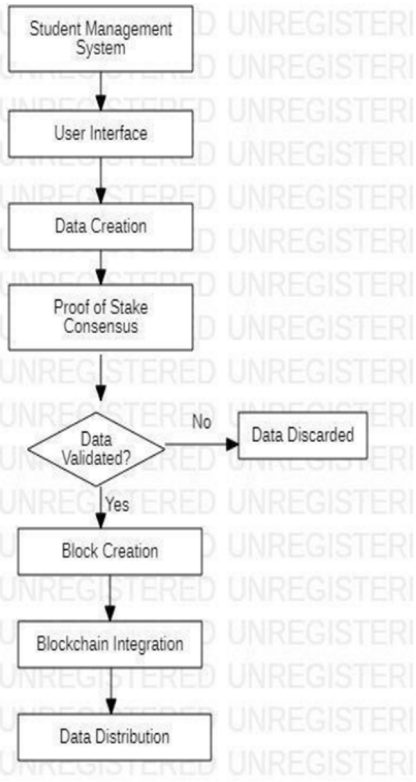

Figure 1: System Flow

VI. System Testing

The immutability of blockchain ensures the reliability and integrity of data. Once a block is added to the chain, it cannot be changed or removed without consensus from the network users. This guarantees that student records stored on the blockchain are trustworthy and authentic. The PoS consensus method further reduces the likelihood of unauthorized changes or data tampering by selecting validators based on their stake in the system.

A series of tests were conducted to verify whether the application meets the specified requirements. These tests followed a test flow initiated from the user interface and covered the use case process and various business rules. The objective was to ensure that the application functions in accordance with the established requirements. Functionalities such as user login after registration, admin's ability to register new students and teachers, posting announcements by the admin and teachers, triggering email notifications for announcements, successful selection of a proctor by newly registered students, and verification of chat functionality between teachers and students were thoroughly tested. Through these tests, the application's performance was assessed, and any discovered issues or discrepancies were addressed to ensure its functionality and overall usability

VII. Result Analysis

The utilization of the Proof-of-Stake (PoS) consensus method and a blockchain-based student management system has yielded significant outcomes and consequences. By leveraging the decentralized nature of blockchain, the system's security has greatly improved, as it eliminates a single point of failure and makes it challenging for malicious actors to tamper with student records. The PoS consensus mechanism ensures that only trusted individuals can contribute new blocks to the network, minimizing the risk of unauthorized alterations. Additionally, the cryptographic methods employed by blockchain further enhance the security of student data.

Moreover, the adoption of a blockchain-based approach has enhanced transparency and auditability. The public ledger provides a transparent record of all transactions and modifications made to student information, promoting

accountability and enabling interested parties to verify the accuracy of the data. Every alteration or update is documented as a new block, eliminating the possibility of undetectable data manipulation. This creates an immutable audit trail that can be traced back to the initial entry, ensuring data integrity and fostering trust in the system.

VIII. Conclusion

The implementation of a data security system for student management, which utilizes blockchain technology and the Proof of Stake consensus algorithm, offers numerous advantageous features. By integrating blockchain, the solution enhances data security and integrity, making it highly resistant to unauthorized access or alteration. The Proof of Stake consensus mechanism ensures that announcements undergo a thorough validation process within a decentralized network, fostering trust and enabling the rapid and secure development, validation, and delivery of announcements. The utilization of blockchain technology enables the system to maintain an immutable and tamper-proof record of announcements, ensuring transparency and accountability. In summary, this project presents a robust and secure platform for managing student information and communication, creating a reliable and efficient environment for educational institutions

References

[1] Nivethini, P., S. Meena, V. Krithikaa, and G. Prethija. "Data security using blockchain technology." Int. J. Adv. Netw. & Appl. (IJANA) (2019).

[2] Patil, Annapurna P., Gaurav Karkal, Jugal Wadhwa, Meer Sawood, and K. Dhanush Reddy. "Design and implementation of a consensus algorithm to build zero trust model." In 2020 IEEE 17th India Council International Conference (INDICON), pp. 1-5. IEEE, 2020.

[3] Simaiya, Sarita, Umesh Kumar Lilhore, Sanjeev Kumar Sharma, Kamali Gupta, and Vidhu Baggan. "Blockchain: A New Technology to Enhance Data Security and Privacy in Internet of Things." Journal of Computational and Theoretical Nanoscience 17, no. 6 (2020):2552-2556.

[4] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops, pp. 180-184. IEEE, 2015.

[5] Jain, Akshita, Sherif Arora, Yashashwita Shukla, T. Patil, and S. Sawant-Patil. "Proof of stake with casper the friendly finality gadget protocol for fair validation consensus in ethereum." International Journal of Scientific Research in Computer Science, Engineering and Information Technology 3, no. 3 (2018): 291-298.

[6] Thin, Wai Yan Maung Maung, Naipeng Dong, Guangdong Bai, and Jin Song Dong. "Formal analysis of a proof-of-stake blockchain." In 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS), pp. 197-200. IEEE, 2018.

[7] Vashchuk, Oleksandr, and Roman Shuwar. "Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake." Electronics and Information Technologies 9, no. 9 (2018): 106-112.

[8] Zhang, Rong, and Wai Kin Victor Chan. "Evaluation of energy consumption in blockchains with proof of work and proof of stake." In Journal of Physics: Conference Series, vol. 1584, no. 1, p. 012023. IOP Publishing, 2020.

[9] Seang, Sothearath, and Dominique Torre. "Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies." France: Universite Cote d'Azur-GREDEG-CNRS. Str 3, no. 4 (2018).

[10] Kim, Jun-Tae, Jungha Jin, and Keecheon Kim. "A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority)." In 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp. 932-935. IEEE, 2018.