A review on Student Document Management System based on Ethereum Blockchain (PERSONAL-D)

Yerramsetti Sri Uday Kiran Sai Mahesh[1], Velagapudi Rohith[2], Vennam Srinivas Reddy[3], Mrs.B. Ratnamala[4], Dr. Reddyvaari Venkateswara Reddy[5].
[1,2,3] B. Tech Student, Department of Computer Science & Engineering (Cybersecurity), CMR College of Engineering & Technology Hyderabad, Telangana.
[4]Assistant Professor, Department of Computer Science & Engineering (Cybersecurity), CMR College of Engineering & Technology Hyderabad, Telangana.
[5]Assistant Professor, Department of Computer Science & Engineering (Cybersecurity), CMR College of Engineering & Technology Hyderabad, Telangana.

Abstract*— The Student Document Management System based on Ethereum Blockchain is a revolutionary project aimed at improving the efficiency and security of document management in educational institutions. With the increasing digitization of student records and the need for reliable verification and authentication mechanisms, this system harnesses the power of blockchain technology to address these challenges. By leveraging the Ethereum blockchain, the system ensures immutability, transparency, and decentralization of student documents. Each document is securely stored on the blockchain, making it tamper-proof and resistant to unauthorized modifications. Smart contracts are used to automate document verification processes, reducing administrative overhead and eliminating the potential for human error. Furthermore, the system provides students with complete control over their documents, allowing them to securely share them with institutions, potential employers, or any relevant parties. The decentralized nature of the blockchain ensures that documents can be accessed from anywhere, at any time, without reliance on a central authority. In summary, the Student Document Management System based on Ethereum Blockchain revolutionizes the way student records are managed, providing enhanced security, efficiency, and transparency.

***Keywords*— Ethereum Blockchain, Security**

INTRODUCTION

The Student Document Management System based on Ethereum Blockchain is a cutting-edge project that aims to revolutionize the management of student records in educational institutions. By leveraging the power of blockchain technology, the system provides enhanced security, transparency, and efficiency. Student documents are securely stored on the Ethereum blockchain, ensuring immutability and protection against tampering. Smart contracts automate document verification processes, streamlining administrative tasks and reducing errors. With decentralized access, students have complete control over their records and can securely share them with relevant parties. This innovative system paves the way for a more secure and efficient document management process in educational settings. The objective of the Student Document Management System based on the Ethereum Blockchain project is to create a secure, efficient, and transparent system for managing student records in educational institutions. The project aims to leverage blockchain technology, specifically the Ethereum blockchain, to ensure the immutability and tamper-proof nature of student documents. By implementing smart contracts, the project seeks to automate document verification processes and reduce administrative overhead. The ultimate goal is to provide students with greater control over their records while improving the overall efficiency and security of document management in educational institutions.

1. Literature Review

The project focuses on creating an immutable certificate generation and validation system. To this end, we referred to some previously published publications and the work of various people in the field. Our literature search mostly focused on digital certificate validation, sophisticated storage systems, and blockchain technology. The title of the first piece was An Overview of Blockchain Technology. [1], which provided in-depth information about Blockchain. It introduced different terms about this technology and the most important concept called a smart contract. In a blockchain, the hash of the data is stored in the previous block and forms a long chain of nodes. When data is modified, its hash changes and does not match the hash value stored in the previous block, letting us know that the data is corrupted. The second article was titled Blockchain and Smart Contract for Digital Certificate [2]. Their design consisted of 3 actors. First were the institutions, second were the students and last was the service provider. The downside of their method was that they used a "single hash as a key" which makes it publicly available once they have the hash. Moving on to our next article, Tampered Birth Certificate [3]. Like the other paper, their design was almost the same, except that they used the AES algorithm and stored the data in IPFS. Their system was specifically for birth certificates. The downside was that the original document was never stored anywhere and could not generate certificates online. To solve the problem of document storage, we studied a separate article entitled Block IPFS (Blockchain Enabled Interplanetary File System for Forensic and Trusted Data Traceability) [4]. This article introduced us to IPFS data and its integration with Blockchain. They compared traditional IPFS with Blockchain and IPFS and the results showed that Block IPFS won in most categories such as download transactions, read transactions, and download transactions. The final work was an identity verification model based on Blockchain [5]. As with the second and third documents, their system consisted of an issuing authority that creates a document, runs a hash algorithm on it, and stores its value. Other systems used asymmetric encryption to boost security because they had access to public hash keys.

2. PERSONAL -D Security Challenges

Encryption and decryption: The encryption and decryption process are crucial for protecting the confidentiality and integrity of student documents. However, the strength of encryption algorithms and key management practices must be carefully implemented to ensure that the encryption keys are not compromised. Weak encryption or insecure key management can lead to unauthorized access to sensitive student records.

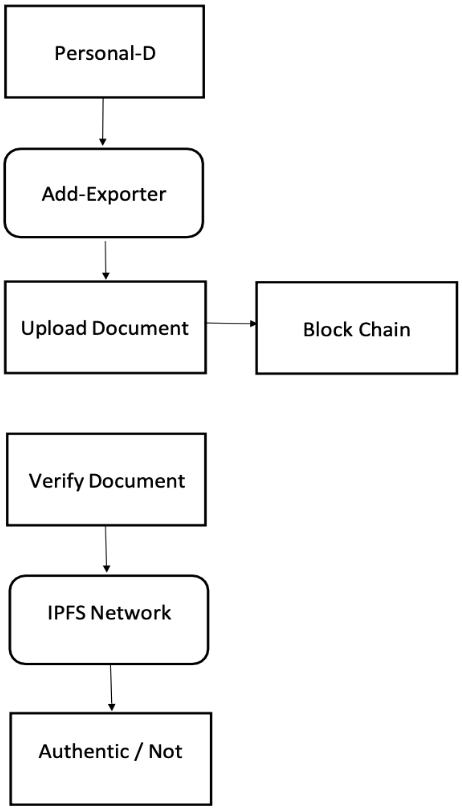
Ethereum smart contract vulnerabilities: Smart contracts are an integral part of the Ethereum blockchain and play a vital role in managing permissions and storing document hashes. However, as with any software, smart contracts can have vulnerabilities. It's important to conduct thorough security audits and code reviews to identify and mitigate potential smart contract vulnerabilities, such as reentrancy attacks or integer overflow/underflow vulnerabilities.

IPFS network security: The Interplanetary File System (IPFS) network is used to store encrypted student documents. While IPFS itself has some built-in security features, such as content-addressable storage and cryptographic hash functions, it is still important to ensure the security of the stored data. Unauthorized access to the IPFS network or compromising the integrity of the stored documents can pose significant risks to the system.

Blockchain in Document Management:

Blockchain is useful for the Student Document Management System as it provides immutability and tamper resistance, ensuring the integrity of student records. Its decentralized and transparent nature eliminates the need for a central authority, enhancing security. Smart contracts automate verification processes, reducing errors and providing reliable results. Students have decentralized control over their records, promoting data ownership. Blockchain streamlines data management, leading to cost and time savings. Its auditability enables accountability and prevents unauthorized changes. Overall, blockchain enhances data integrity, reduces administrative burdens, strengthens security, and empowers students with control over their records.

5.1 ENCRYPTION



5.2 DECRYPTION

Figure: SYSTEM DESIGN

Procedure Steps:

Add Exporter: In this step, the system enables authorized access by allowing the owner to add exporters through the input of their Ethereum address. This ensures that only designated individuals or entities can access the student records securely.

Upload Document: Users can upload a document by clicking on the "Upload Document" button and selecting the desired file from their computer. This initiates the process of securely storing the document within the Interplanetary File System (IPFS) network, safeguarding it against unauthorized access or tampering.

Document Encryption and Storage: The system encrypts the uploaded document using robust encryption algorithms to protect its confidentiality. The encrypted document is then stored within the decentralized IPFS network, ensuring data integrity and secure storage.

Document Hash Recording: To maintain the authenticity and immutability of the document, the system generates a unique hash (cryptographic fingerprint) of the encrypted document. This hash is recorded on the Ethereum blockchain, providing a reliable and tamper-resistant reference point for verification purposes.

Verify Document: Users can verify the authenticity of a document by entering its hash into the provided input field and clicking the "Verify Document" button. The system retrieves the encrypted document from IPFS, decrypts it, and compares its computed hash with the recorded hash on the blockchain.

Document Retrieval and Decryption: Upon initiating the verification process, the system retrieves the encrypted document from the IPFS network using the recorded hash. It then applies the appropriate decryption algorithm to restore the document to its original form for comparison and verification.

Hash Comparison and Verification Result: The system computes the hash of the decrypted document and compares it with the recorded hash on the blockchain. Based on the comparison result, the system provides a clear message indicating whether the document is authentic or not, thus ensuring the integrity and transparency of the student records and mitigating the risks associated with unauthorized access or tampering.

3. CONCLUSION

In conclusion, the Student Document Management System based on Ethereum Blockchain offers a transformative solution to the challenges faced in managing student records in educational institutions. By leveraging the security, transparency, and decentralization features of blockchain technology, this system ensures the integrity and authenticity of student documents. The use of smart contracts automates verification processes, reducing administrative burden and potential errors. With decentralized access, students have greater control over their records, empowering them to securely share information with relevant parties. The system's immutability and tamper-proof nature provide a robust defense against unauthorized modifications. Furthermore, the system promotes efficiency, scalability, and easy accessibility to documents, facilitating streamlined operations and reducing reliance on centralized authorities. By revolutionizing document management in the education sector, this solution enhances trust, privacy, and data control while improving overall security and efficiency in managing student records.

4. REFERENCES

[1]Suganthalakshmi,M.R.,Praba,M.G.C.,Abhirami,M.K.andPuvaneswari,M.S.(2022)Blockchain Based Certificate Validation System https://www.irjmets.com

[2]ZHayes,A.(2022)BlockchainFacts.https://www.investopedia.com/terms/b/blockchain.asp

[3]Garg,R.(2021)BlockchainEcosystemforEducation&EmploymentVerification.Proceedingsof13th International Conference on Network & Communication Security (NCS 2021), Toronto, 25-26 September 2021.

[4]ZibinZheng, ShaoanXie, Hong-NingDai, XiangpingChen, Superintendent of Blockchain Technology: Architecture, Interconsensus kaj Estontage Tendencoj, IEEE 6th Internacia Grand Datuma Congress, 2017.

[5]Jiin-Chiou, Narn-YihLee, ChienChi, YI-HuaChen, "BlockchainandSmartContractforDigital Certificate", IEEE International Conference on Applied Systems Innovation 2018 - Publication.

[6]MaharshiShah,PriyankaKumar, "TamperProofBirthCertificateUsingBlockchainTechnology", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Number 5S3, February

[7]EmmanuelAllotey, Reza.Parizi, QiZhang, Kim-KwangRaymondChoo, "BlockIPFS- A Blockchain-Enabled Interplanetary File System for Forensics and Trusted Data Traceability", IEEE International Conference on Blockchain,

[8] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, D-ro Seema Shah, "Blockchain-Based Identity Verification Model", International Conference on Emerging Trends in Communication and Networking (ViTECoN),