Blockchain File saving and verification System with IPFS

Mini Project report submitted in
Partial fulfillment of requirement for the award of Degree
of

Bachelor of Technology in Information Technology

Submitted by

Mihir Mishra (157)
Kartik Chavan (155)
Tushar Sakharkar (175)
Pratiksha Rathod (114)
Sharvari Nimbalkar (119)

Guided by

Mr. Piyush Dhule
Designation
Department

Department of Information Technology
Nagar Yuwak
Shikshan Sanstha's
Yeshwantrao Chavan College of Engineering
(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)
Nagpur – 441 110

November 2022

Yeshwantrao Chavan College of Engineering,Nagpur

CERTIFICATE

This is Certified that the Mini Project report entitled "Blockchain File saving and verification System with IPFS" has been successfully completed by Mihir Mishra, Kartik Chavan, Tushar Sakharkar, Pratiksha Rathod, Sharvari Nimbalkar under the guidance of Prof. Mrs. Piyush Dhule in recognition to the partial fulfillment for the award of the degree of Bachelors of Technology in Information Technology, Yeshwantrao Chavan College of Engineering (An Autonomous Institution Affiliated to Rashtrasant Tukdoji Maharaj Nagpur University).

Co-Guide	**Guide**
Name of Co-Guide	Name of Guide
Designation	Designation
Department of Information Technology	Department of Information Technology
Y.C.C.E, Nagpur	Y.C.C. E, Nagpur

Prof. Jagdish Yadav	**Prof. R. C. Dharmik**
In-charge, Training	**Head,**
Department of Information Technology	Department of Information Technology
Y.C.C.E, Nagpur	Y.C.C. E, Nagpur

ACKNOWLEDGEMENT

I wish to express my sincere and deepest gratitude to my guide **Mr. Piyush Dhule** for his valuable and unique guidance. I would also like to thank him for the constant source of help, inspiration and encouragement in the successful completion of my technical seminar. It has been my privilege and pleasure to work under his expert guidance.

I would like to thank **Prof. R. C. Dharmik** (HOD) for including a technical seminar in our curriculum which helps me to improve my technical knowledge. I would again like to thank Dr. U. P. Waghe, Principal (YCCE) who has provided all institutional facilities as and when

I express my thanks to all the staff members of Information Technology department who have directly or indirectly extended their kind co-operation in the completion of my technical seminar report.

Mihir Mishra
Kartik Chavan
Tushar Sakharkar
Pratiksha Rathod
Sharvari Nimbalkar

V Sem-B

INDEX

I. Introduction

Ensuring the reliability of software systems is important for safety of user's data. A file saving system is designed to store the data efficiently and without any data loss. Along with storing it is also important for user to verify whether the file is in his account or not. A file is opened by user in any other application and the probability is more that the file is not safe as we open it in another application. Also some unauthorized flies can be present so detecting them is also required .The files are stored in first come first serve basis, so we have made special attention and made efforts to design a file system that easily identifies the files. The IPFS used in our project ensures data integrity, as each file and block is given a unique hash, verifying the content has not been tampered with. IPFS retrieves data from the nearest or fastest nodes, reducing bandwidth usage. The integration of IPFS with blockchain technology provides an additional layer of security and immutability to the file storage system.

This project aims to make a web app that can store important files and data safely and user can verify whether the data is in his account or not.

II. Literature Review

When people want to obtain things through illegitimate means, fraud frequently results. One type of fraud that involves copying and pretending to be the original document's details—such as the identifying number and signature—is known as document forging. Different types of document forgeries exist, including Scan, Edit, and Print (SEP), Reversed Engineered Imitation (REI), Print, Copy, and Paste (PPC), and imitation.

The ability to create an unauthorized document that would fool the system or people to obtain desired outcomes, including money laundering or unauthorized entry into a country, was the primary goal of all the forgeries. To avoid the issues that have arisen, a very efficient document verification system must be created.

Examining previous research on file storage, data integrity, and verification techniques would be a part of a literature review for an application that saves and verifies files.

Below is a synopsis of the main points to be discussed:

1.**File Storage and Management**: Read up on various file storage methods, such as distributed file systems, cloud storage, and local storage.

• Examine studies on file storage solutions' scalability, fault tolerance, And data redundancy.

2.**Verification and Integrity of Data**:

Examine techniques for guaranteeing data integrity, including error detection codes, hashing algorithms, and checksums.

Blockchain transforms becomes a potent instrument when a transaction takes place within it, confirming the data's integrity. Blockchain is therefore appropriate for securely keeping the papers.

III. Analysis for Project Scope

The following lists the essential elements and things to think about for your project scope analysis:

1. **The project's goals**

• Clearly state the main goals of the application, including data integrity checking, safe file storage, and an intuitive user interface.

2. **Capabilities and Features**:

• Enumerate the features your application will have, such as access control , encryption, checksum checking, and file upload/download.

Types of Users:

• Identify the different user categories (individuals, companies, etc.) and the corresponding responsibilities and permissions they have within the pro gramme.

3. **Technology Pyramid:**

Indicate which platforms and technologies such as database frameworks, and programming languages
will be used to build your application.

4. **Safety Procedures:**

Describe the security precautions that must be taken, including

Blockchain analysis is a process of investigating, classifying, and monitoring blockchain addresses and transactions to understand the activities of various actors on the blockchain

IV Work Done

1. Requirement Analysis: We conducted a thorough analysis to understand the requirements and objectives of the project. This phase included defining user requirements, technical specifications, and system architecture. The system's requirements encompass three key components:

- **IPFS:-**IPFS is a command-line system that must be available for the uploading process. IPFS Cluster utilizes the IPFS daemon's API to store files and share them with selected peers. To initialize the IPFS daemon, a command is entered through the command prompt.

- **IPFS Cluster:** This standalone application ensures the successful upload and sharing of files on IPFS. It also relies on the IPFS daemon API. After initializing the IPFS daemon, IPFS Cluster can start the clustering process of peers using the same command-line method.

- **Ethereum Blockchain**: Ethereum blockchain is essential for verifying file existence and integrity within IPFS. It requires significant computational power. In this document verification system, Truffle Suite, specifically Ganache, is used to provide an Ethereum test network for development. Ganache offers its

user interface, allowing users to select the network connected to the document verification system.

2. **System Design implementation**: We designed the architecture of the web application and its integration with a blockchain network. This included selecting the appropriate blockchain platform and creating the necessary smart contracts

- **Uploading Process: -**

The document verification system's primary goal is to ensure file availability and integrity. Users must upload the original file in PDF format, encrypted with AES and a password, using Microsoft products (2007 or newer). The system sends the encrypted file to the IPFS Cluster via the IPFS daemon, creating an IPFS hash for file access. Both the IPFS hash and the password are stored on the Ethereum blockchain after user confirmation and payment of transaction fees in ethers. This process is depicted in a procedural design,

- **Verification System: -**

The document verification system's primary objective is to ensure file availability and integrity. Users upload an original PDF file encrypted with AES and a password using Microsoft products (version 2007 or newer). The system sends the encrypted file to the IPFS Cluster, generating an IPFS hash for file access, and stores the hash and password on the Ethereum blockchain after user confirmation and payment of transaction fees in ethers. The verification process involves three components: transaction hash, IPFS hash value, and password. These components are used to retrieve and compare data from the blockchain to verify the file's integrity. There are four possible scenarios based on the correctness of these components.

- **History Log Process: -**

This is an extra feature of the system where the user can check the history log of the transactions made in the system. The system will fetch the transaction blocks from the 236 M. D. R. Zainuddin and K. Y. Choo blockchain to be displayed from the application for the user

to monitor. It will fetch the latest ten transactions made from the system and it will decode the metadata data from the blockchain to be displayed to the application

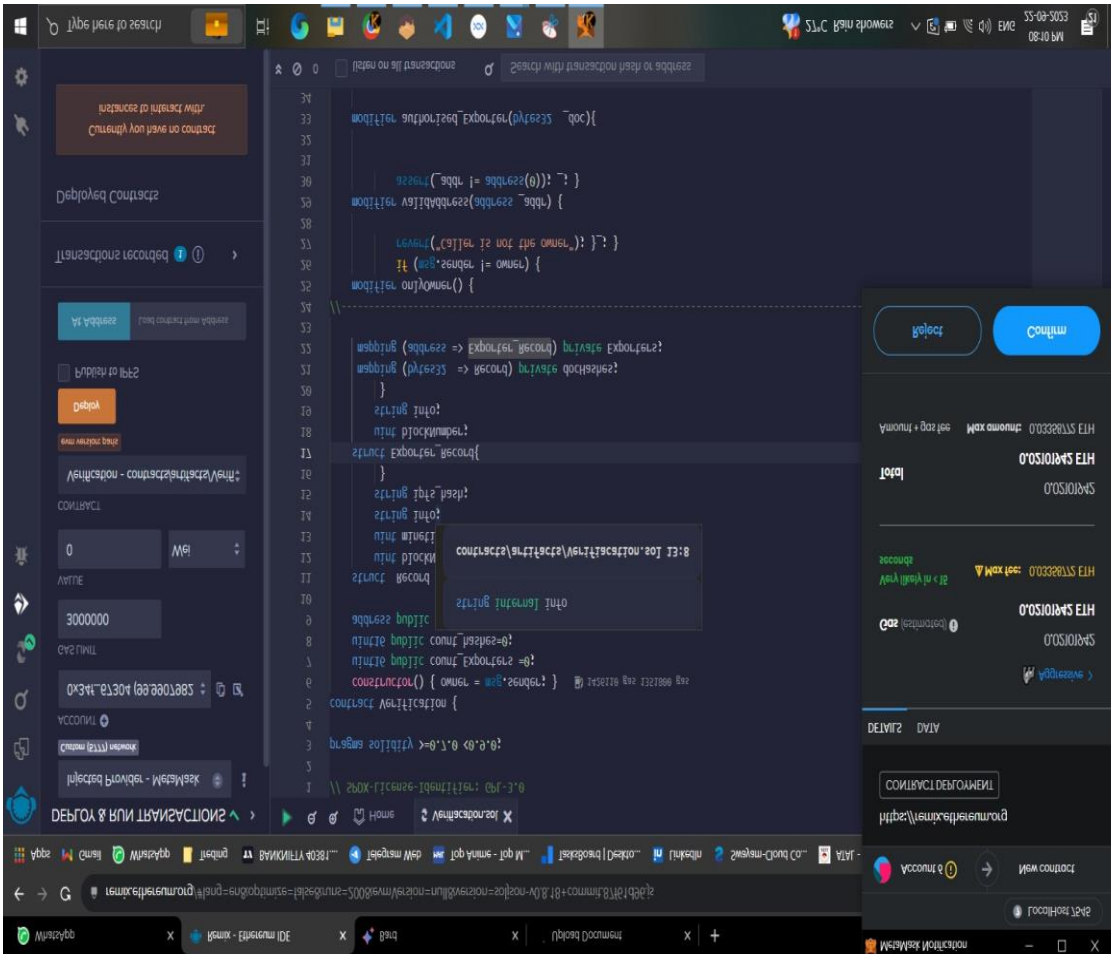
3. **Development:** The development phase involved creating the web application's front-end and back-end components. It also included the coding of smart contracts and their deployment on the blockchain.

4. **Testing and Debugging:** Rigorous testing was performed to ensure the application's functionality and security. This involved unit testing, integration testing, and security testing to identify and resolve any issues.

5. **User Interface Design:** We designed an intuitive and userfriendly interface to allow users to easily upload, save, and verify files.

6. **Blockchain Integration:** We integrated the web application with a blockchain network to enable the secure and transparent storage of file data. Files were hashed, timestamped, and stored on the blockchain for verification.

7. **Documentation:** Comprehensive documentation was prepared to provide guidelines for users, administrators, and future developers regarding the application's functionality and architecture.



DEPLOY & RUN TRANSACTIONS
Injected Provider - MetaMask
ACCOUNT
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT
Deploy
Publish to IPFS
At Address
Transactions recorded
Deployed Contracts
Currently you have no contract instances to interact with.
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.0 <0.9.0;
contract Verification {
constructor() { owner = msg.sender; }
struct Exporter_Record{
mapping (address => Exporter_Record) private Exporters;
mapping (bytes32 => Record) private docHashes;
modifier onlyOwner() {
modifier validAddress(address _addr) {
modifier authorised_Exporter(bytes32 _doc){
Reject
Confirm
DETAILS
DATA
Gas
Total
0.02101942 ETH
CONTRACT DEPLOYMENT
https://remix.ethereum.org
New contract

V. Results and Discussion

Result :-

Secure File Storage: Files uploaded to the web application are securely hashed and stored on the blockchain, ensuring their immutability and integrity.

Verification: Users can verify the authenticity of files by comparing the hash stored on the blockchain with the calculated hash of the uploaded file. This provides a reliable method for file verification.

Transparency: The blockchain's decentralized nature ensures transparency and trust in the file storage and verification process.

User-Friendly Interface: The web application offers an intuitive user interface that simplifies the process of uploading and verifying files.

Discussion: -

The project's success is attributed to the effective integration of blockchain technology into the web application. The blockchain

ensures the security and transparency of file storage and verification. Some points for discussion include:

Blockchain Trust: The blockchain's immutable and decentralized nature ensures trust in the stored files. Any changes or tampering with the files can be easily detected.

Security: The use of public and private keys for file access and verification adds an additional layer of security to the system.

Scalability: The system can be easily scaled to accommodate a larger number of users and files while maintaining the same level of security.

Future Enhancements: Future enhancements could include implementing a user management system, adding more blockchain features, and improving the user interface.

VI. Summary and Conclusion

The project successfully achieved its objectives of creating a web application that securely saves and verifies files using blockchain technology. The implementation of smart contracts, blockchain integration, and a user-friendly interface resulted in a robust and reliable system for file storage and verification. This project promotes transparency, security, and trust in the digital file management process.

Blockchain is a technology that provides a lot of features and benefits in creating a document verification system. The integration between Ethereum blockchain and IPFS helps in distinguishing between the original file and the modified file. Blockchain provides a better storage system where it can keep all the related credentials safe and secure from any attack as it is permanently stored in the blockchain. There are still some limitations
to the system that need to be considered for future work. The limitation of the system is related to the encryption method where the system does not provide any file encryption method since it uses other software. Other than that, the system checks for any changes made to the file and not going through the content of the file. Optical Recognition Character (OCR) can be implemented into the system to overcome the limitation of checking the content of the file. For future work, these limitations need to be considered to create a better document verification system based on blockchain technology.
In conclusion, the project demonstrates the potential of blockchain technology in ensuring the integrity and security of digital assets. It provides a solid foundation for future developments in the field of secure file storage and verification.

VII . References

[1] R. Smith, “Peer review: a flawed process at the heart of science and journals,” Journal of the royal society of medicine, vol. 99, no. 4, pp.178–182, Apr. 2006.

[2] Murkute, Amod, and Tanuja Sarode. (2015) "Forecasting market price of stock using artificial neural network." International Journal of Computer

[3] Li, Lei, Yabin Wu, Yihang Ou, QiLi, Yanquan Zhou, and Daoxin Chen. (2017) "Research on machine learning algorithms and feature extraction for time series." IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 1-5.

[4] Kumar, Manish, and M. Thenmozhi, (2006) "Forecasting stock index movement: A comparison of support vector machines and random forest"

[5] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.

[6] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.

[7] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. [Online]. Available: https://ethereum.org/whitepaper/

[9] Ivan, “InterPlanetary File System Explained – What is IPFS?” Moralis Academy, 8 April 2021. [Online]. Available: https://academy.moralis.io/blog/interplanetary-file-system-explained-what-is-ipfs.

[10] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, “BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability,” in 2019 IEEE International Conference on Blockchain (Blockchain), USA, 2019

[11] Barbara Guidi, Andrea Michienzi, Laura Ricci, “Data Persistence in Decentralized Social Applications: The IPFS approach,” in 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Italy, 2021..

[12] 2. B. Thuraisingham, “Blockchain Technologies and Their Applications in Data Science and Cyber Security,” in 2020 3rd International Conference on Smart BlockChain (SmartBlock), Texas, 2020.