Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

A Bockchain-Based Solutions for Certificate Forgery: Enhancing Security and Reliability in Documents Authentication

Dr. Chanchal Antony
Associate Professsor and HOD
A J Institute of Engineering and Technology
Mangaluru,Karnataka,India

Prakruthi S Shetty
Student
A J Institute of Engineering and Technology
Mangaluru,Karnataka,India

Vaishishta P
Student
A J Institute of Engineering and Technology
Mangaluru,Karnataka,India

Vijeth Kumar
Student
A J Institute of Engineering and Technology
Mangaluru,Karnataka,India

Shreya S Shetty
Student
A J Institute of Engineering and Technology
Mangaluru,Karnataka,India

ABSTRACT
Document forgery is a widespread issue, as individuals manipulate sensitive content for personal gain. Traditional verification systems often neglect content integrity, leading to inefficiencies and false results in detecting forged documents. To address this, blockchain technology, coupled with the Interplanetary File System (IPFS), offers a solution. By leveraging blockchain's secure and transparent ledger, a new verification system can be established. Integrating IPFS enhances efficiency in detecting forged documents, providing a robust defense against fraud. With this method, document verification is guaranteed to go beyond availability alone, giving content integrity top priority for improved accuracy. Document verification systems that include blockchain and IPFS can lower the risks of forgery, promoting dependability and confidence.

General Terms
Blockchain Technology,Document Authentication, Counterfeit Detection, Blockchain Security, Document Integrity, Trustless Verification, Smart Contracts, Immutable Ledger

Keywords
document forgery, content integrity, verification system, blockchain, Interplanetary File System (IPFS), efficiency, fraud detection, trust, digital forensic.

1. INTRODUCTION

Counterfeit documents are fake papers designed to appear genuine. People create them to trick others into believing they're authentic. These fake documents can range from fake IDs to counterfeit currency. Some people utilize them dishonestly, such as when they conduct fraud or identity theft. To prevent misuse, real documents are equipped with special features such as holograms or watermarks that are difficult to replicate. In order to stop dishonest people from utilizing forged documents to violate the law, counterfeit document detection entails spotting irregularities like misspellings or unauthorized markings. It is also utilized in digital forensics.

The application of blockchain technology in digital forensics for counterfeit identification greatly facilitates the process of verifying the authenticity and integrity of digital documents. Blockchain's transparent and tamper-proof properties allow digital forensic analysts to monitor the origin and history of documents, verifying authenticity and preventing fraud. By providing a permanent and secure record of a document's authenticity, this method enhances the reliability of evidence in digital investigations.

Maintaining public safety, legal and financial system integrity, and national security all depend on the detection of counterfeit documents. Counterfeits can facilitate criminal activities such as identity theft, fraud, and even terrorism. Ensuring the authenticity of documents builds trust in financial transactions and safeguards institutions from being undermined. Robust detection mechanisms protect individuals and organizations from exploitation, maintain the accuracy of official records, and contribute to a secure and stable societal framework. Reliability of critical operations is maintained and the rule of law is upheld by effective counterfeit detection, which also stops the misuse of falsified documents.

The main issue with document verification systems is stopping documents from being faked. Document forgery happens when someone copies or pretends to be an original document, like copying a signature or ID number. Another issue is that existing systems do not verify whether the contents of a file are authentic; they merely verify that the file exists in the system.

Blockchain functions as a secure digital ledger distributed across a network, recording and validating transactions through cryptographic principles. Blocks of transactions are linked

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

together, forming an unalterable chain. This decentralized system, beyond cryptocurrencies, finds utility in various sectors like healthcare and supply chain management, ensuring security and trust by eliminating central authorities and resisting fraud.
Counterfeit documents are fake papers designed to deceive, imitating authentic ones like currency or academic certificates. They pose legal risks and threaten public safety, necessitating robust detection methods. These methods include visual inspection, UV light examination, and advanced technologies like machine learning. Blockchain technology, with its tamper-resistant record-keeping, provides a promising solution to combat document fraud, enhancing verification processes.
Paper documents are typically used to issue documents or other records pertaining to students.Student records, typically on paper, are vulnerable to counterfeiting and loss.These documents can be misplaced or compromised, and they are simple to forge. Blockchain offers a secure alternative, making data alteration difficult. Certificates issued by organizations can be easily manipulated, posing risks to both issuers and recipients. Blockchain integration improves verification, addressing document fraud and ensuring authenticity, though awareness and successful implementation remain crucial for its effectiveness.
Blockchain technology has been used recently to improve document verification procedures and combat document fraud and misuse. This technique aims to stop the issuance of forged documents and altered certifications.

2. LITERATURE SURVEY

[1] Omsar S. Salesh, Osman Ghazali, and Muhammad Ehsan Rana proposed a system using the Hyperledger Fabric framework to verify educational certificates. They highlighted that academic credentials represent a person's skills and knowledge gained through education, making them valuable targets for forgery. Their system aims to enhance document verification by utilizing the Hyperledger platform, where each user receives a unique identification from the system administrator. Data transfer to and from the Hyperledger is secured using encryption API endpoints. However, a drawback of their system is that documents uploaded by owners can be viewed on demand for a limited time period.

[2] Leka, E. and Selimi, B. developed and evaluated a blockchain-based secure application for verifying academic certificates. The application, built on Ethereum, utilizes smart contracts to distribute, store, and verify academic credentials. Its primary goals are to improve the security and efficiency of the verification process and do away with the requirement for third-party verification techniques.Additionally, it incorporates AES encryption to ensure data confidentiality. However, a drawback of their solution is that it lacks detailed information on authorization and confidentiality aspects.

[3] Prof. Ashly Thomas, Sherin Mary Shaji, and Mili Rafi presented a blockchain-based certificate management and validation system. The administrator, the student, and the verifier are the three primary users of the system. The hyperledger fabric stores student data entered by the administrator through composer RestServer. A hash code is created and a digital signature is added once the institution verifies the preview of the certificate. In the hyperledger, only certified certificates are kept. Students are given QR codes to obtain their certificates. One disadvantage, though, is that the system needs to connect through composer Rest Server as it cannot connect directly to the hyperledger fabric.

[4]Curmi and Inguanez developed a blockchain-based platform for certificate verification. They created a prototype for registering institutions, faculties, and students, facilitating the issuance of certificates. This platform offers an interface for students to access their certificates, which are stored on the blockchain, removing the need for third-party verification. However, a drawback is that the research did not explore how the validity of documents stored on the blockchain is verified, which should be addressed in future phases.

[5] Clemens Brunner, Fabian Knirsch and Dominik Engel introduced SPROFF, a platform designed for issuing and verifying documents on a public blockchain. SPROFF allows issuers to upload document hashes to the blockchain without any restrictions. It employs a key derivation function to generate private keys from a master key and uses a public-private key pair to prove document ownership. Recipients need to register with an issuing institution to upload documents, and key management is handled using a Hierarchical Deterministic Wallet. While SPROFF follows Web of Trust principles, it lacks integration for attribute-based identification for receivers, which is a drawback that needs to be addressed.

[6] Jayesh G.Dongre, Sonali M. Tikam, Dr. Kishore.T.Patil and Vasudha Gharat, focused on detecting fraud in educational degrees and verifying student certificates using blockchain. They highlighted identity document forgery, where authorized documents are altered and copied for unauthorized use, facilitated by various tools and strategies. The researchers examined existing methods for countering document forgery and identified their limitations in effectively combating identity fraud. They emphasized the need for new techniques to address this issue, as identity fraud often involves creating false identities using a mix of genuine and fabricated information. This can lead to fraudulent activities such as applying for credit or making purchases using someone else's identity. The flaw that was brought to light was how often fake graduation certificates appeared because there was no effective anti-forgery system in place.

[7] A. Gayathiri, J. Jayachitra, and Dr. S. Matilda presented a blockchain-based application for certificate validation. They described how to use sampling and quantization to turn paper certificates into digital ones, and how to create hash values using a chaotic method. Using an admin login, the application enables administrators to register students and upload their certificates, converting analog photographs into digital ones. After that, certificates can be verified by logging into a verifier. The absence of secrecy, though, was a disadvantage because every transaction is accessible to every peer on the blockchain network.

[8] Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., proposed a new blockchain-based solution for verifying education records. The goal of this solution is to establish a safe space where students are in charge of their academic records. Institutions can provide certificates of accomplishment by utilizing cutting-edge blockchain technologies, which students

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

can readily obtain and distribute to others. This solution's drawback is that it's limited to academic records and certifications.

[9] Affandi Husain, Majid Bakhtiari, and Anazida Zainal discussed the problem of fraud, particularly document forgery, where individuals replicate original documents to deceive systems or others for personal gain, like money laundering or illegal entry into a country. Various methods of document forgery exist, including Print, Copy and Paste (PPC), imitation, Reversed Engineered Imitation (REI), Scan, Edit and Print (SEP). Nevertheless, there hasn't been any testing or implementation of their suggested barcode-based printed document integrity verification method to determine how well it works to safeguard the authenticity and integrity of printed documents.

[10] Barbara Guidi, Andrea Michienzi, and Laura Ricci discussed an approach for verifying file integrity using the Interplanetary File System (IPFS). IPFS finds data based on its content, which is represented by a hash, as opposed to conventional systems that rely on domain names. They emphasized IPFS's pinning services, which inhibit automatic data destruction by sustaining data presence in the network through the operation of long-lived host nodes on cloud service providers. They did point out that there are difficulties in putting Decentralized Social Applications into practice, especially when it comes to data availability, scalability, and privacy—all of which centralized servers might not be able to provide.

[11] Muhammad Dhiyaul Rakin Zainuddin and Kan Yeep Choo investigated a blockchain-based method for document verification. They emphasized the benefits of blockchain technology, including its connection with IPFS and Ethereum blockchain, which allows it to securely store documents and distinguish between original and changed files. Nevertheless, they pointed out a flaw in the encryption process, stating that the system depends on external software and does not have a built-in mechanism for encrypting files.

[12] Rafah Amer Jaafar PP and Saad Najim Alsaad P suggested a blockchain-based remedy to stop the faking of educational certificates. Using IPFS as a decentralized file system and the Hyperledger Fabric platform, they created a decentralized architecture for certifying diplomas. Their approach stores certificate files on IPFS and only the IPFS hash on the blockchain, ensuring immutability and lowering the amount of data storage required. The system has the potential to validate educational qualifications more cheaply and with less labor, but it lacks the implementation of the Hyperledger Fabric network, which would allow it to cover more companies and use more channels.

[13] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi suggested a Public Key Infrastructure (PKI) solution based on blockchain to improve the security and dependability of certificate revocation data. Their method has the benefit of not requiring a single point of failure and is comparatively simple to apply using already available open source platforms. The blockchain may experience scalability challenges as the volume of transactions and users rises, which could result in performance concerns. This is a disadvantage.

[14] Anthonya, Michael Christian Leea, Rafaelle Richel Pearla, Ivan Sebastian Edberta, and Derwin Suhartono suggested creating an anti-counterfeit system with blockchain technology. Their method is to confirm each product's legitimacy within the system. Nevertheless, the system's existing limitations include its limited size and reliance on manual input. To reduce the possibility of human error and expedite the input process, automation is required.

[15] Vipul Badhe, Pooja Nhavale, Sonal Todkar, Prajakta Shinde and Prof. Kiran Kolhar investigated a blockchain-based digital certificate system designed to validate educational credentials. They investigated a number of strategies to reduce certificate fraud and guarantee the secrecy, security, and accuracy of graduation certificates. They sought to reduce certificate forgery via a novel blockchain-based strategy. Nevertheless, even with its automated and transparent certificate issuance procedure, the system has a number of shortcomings with regard to data security and privacy. Although this makes it simple for businesses or organizations to acquire certificate details, privacy and data security issues still need to be addressed.

3. METHODOLOGY

The "A Blockchain based solution for certificate forgery" project requires studying blockchain technology and document verification methods before creating a web application. The application's implementation for document verification will leverage blockchain integration, and a rigorous testing procedure will ensure the system's functioning and security.

3.1 Objectives

The aim of employing blockchain technology for the purpose of detecting counterfeit documents is to improve security and legitimacy while confirming different kinds of records, such legal or academic certifications. The idea behind this is to develop an immutable record-keeping system that guarantees document integrity by utilizing blockchain's resistance to tampering. By making it exceedingly difficult for counterfeiters to change or falsify papers without being discovered, this strategy seeks to combat fraud. The ultimate goal is to provide a dependable and effective process for confirming the legitimacy of papers, protecting against fraud and upholding public confidence in official records..

3.2 Proposed Methodology

1) User Initiates Document Upload:
- When a user wants to upload a document, they start the process by initiating the upload.
- The flowchart splits into two paths from here.

2) Path 1: HASH Generation:
- The system creates a hash for the uploaded document in this path. A hash is a distinct character string that serves as a representation of the file's content.
- The method of hash generation guarantees the integrity of the document both during transmission and storage.
- Later on, the resulting hash is utilized for verification.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

3) Path 2: Unsupported File Type:

- If the uploaded file type is not supported (e.g., an unsupported format like an executable file), the system displays an error message.
- The user is informed that the file type is not accepted.

4) Document Verification:

- After successful document upload, the user initiates document verification.
- The flowchart continues from here.

5) File Type Supported

- The system checks if the file type is supported. If it is, the verification process proceeds.
- Otherwise, an error message indicates that the file type is unsupported.

6) Generate Document Hash:

- Similar to the first path, the system generates a hash for the uploaded document.
- This hash is compared with the one generated during upload to ensure consistency.

7) Blockchain Verification:

- The system compares the generated hash with the hash stored on the blockchain.
- If they match, the document is verified successfully.
- If not, an error message indicates that verification failed.

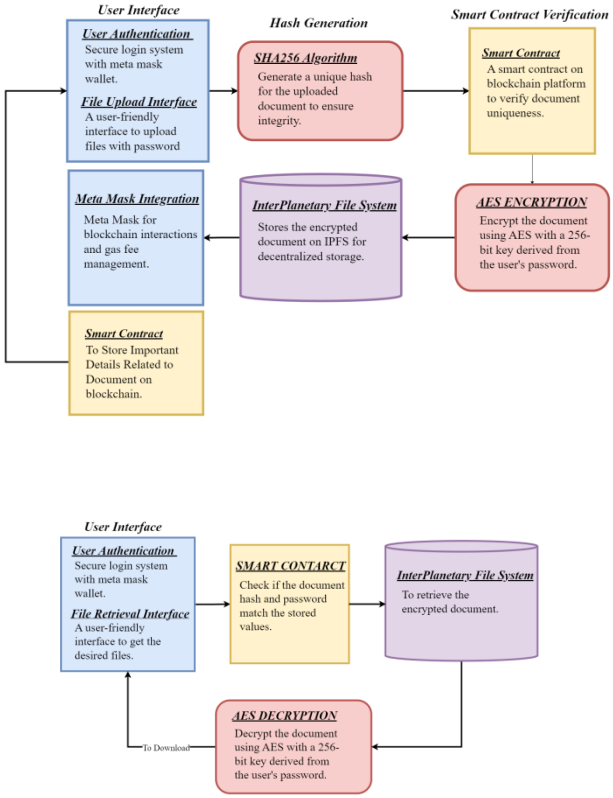
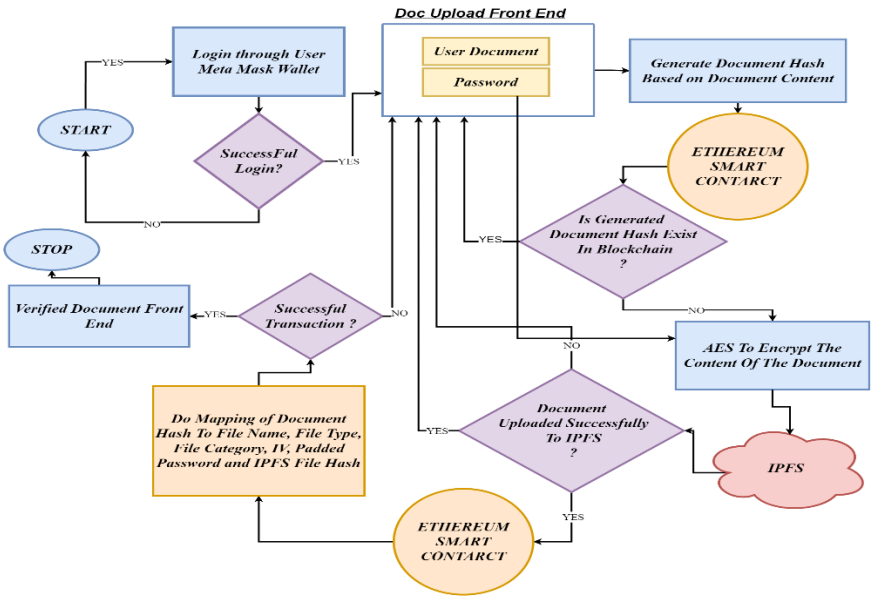


Fig.1: System Architecture

3.3 Workflow



Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

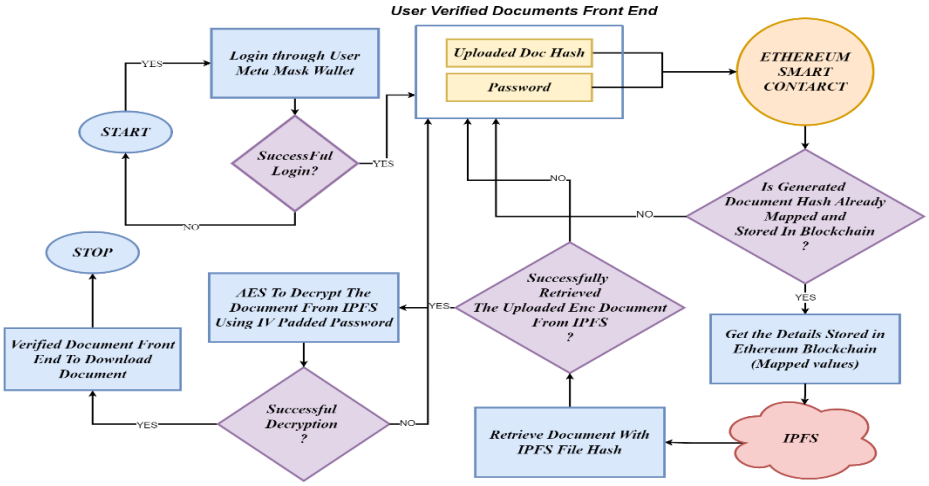


Fig.2: Workflow diagram

- User logs in and uploads a file with a password.
- The file content is hashed using SHA256 for verification.
- If the content is unchanged, the hash is sent to a smart contract for verification.
- If the hash exists, it's confirmed. If not, encryption begins.
- AES encrypts the file with the password and other parameters.
- Encrypted file is split and stored on IPFS, with a main hash.
- IPFS hash, along with other details, is sent to a smart contract.
- Transaction is initiated via MetaMask, deducting gas fee.
- Frontend receives transaction and document hashes.
- To retrieve the document, front end sends hash and password to smart contract.
- Contract verifies and retrieves details if correct.
- Encrypted file is fetched from IPFS.
- AES decrypts using password and IV.
- Decrypted file is available for download

4 RESULT SNAPSHOT

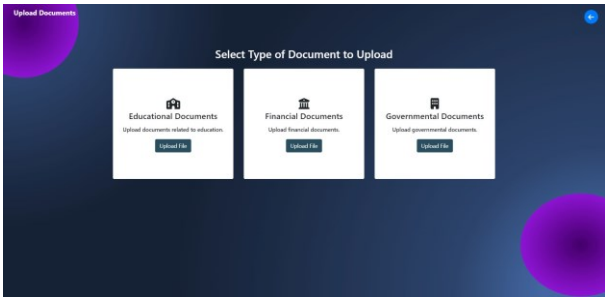


Fig.3: Web page for uploading of documents

The Figure 4.1 shows the webpage intended for document uploading. The website has three main document categories: essentially, educational documents, information pertaining to finances or transactions, and documents from the government. Thus, when uploading a document, the user can select any category of their choosing.

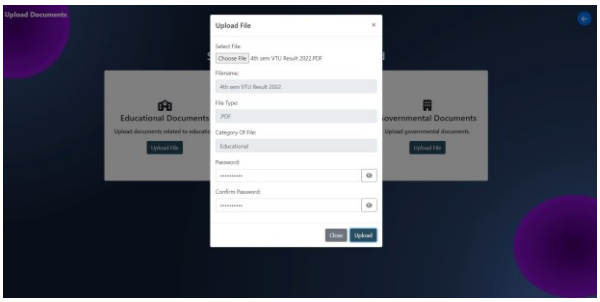
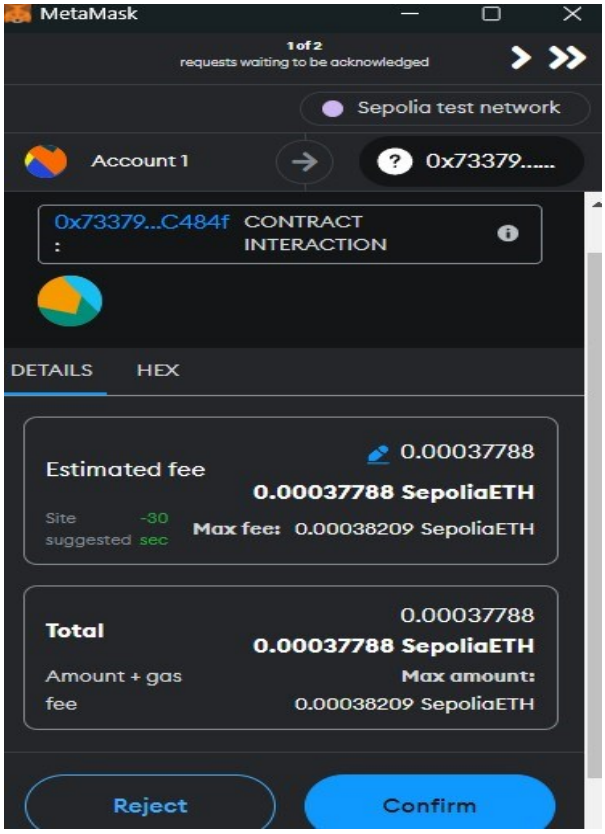


Fig.4: Document upload form

The Figure 4.2 shows document upload form. Here the user chooses a file from their device to start the document upload procedure. This file is available in a number of forms, including PNG, JPEG, and PDF. Upon selecting a document, certain fields on the upload form are automatically filled up. The process is made simpler for the user by automatically filling in the file name, identifying the file type (such as image or PDF), and assigning a file category (such as personal, work-related, or educational).The user needs to enter a password before they can continue with the upload. In order to maintain security and guarantee that only authorized users can submit documents, this password is essential. To make sure the password is typed correctly, the user must confirm it. The user can click "Upload" to continue after finishing the password entry and confirmation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024



Fig,6: Transaction message in metamask wallet

The Figure 3 shows a transaction message in metamask wallet. Once the user clicks on upload, it initiates the document upload process and then a pop up appears which indicates the estimated fees and time taken to upload the document.Upon confirming the transaction the document will be uploaded and an upload successful message pops on the front end

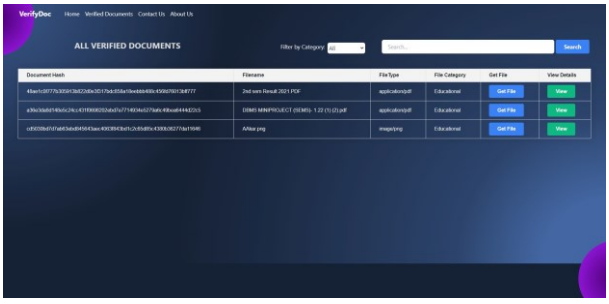


Fig.7: Verification of documents

The Figure 4.4 is connected to the document's verification. The entire content of the document is encrypted using AES when it has been successfully uploaded, saved in IPFS, and a document hash is produced. Every document that is stored in the IPFS has a distinct document hash. As a result, the document hash linked to the document can be used to confirm the content of the document.

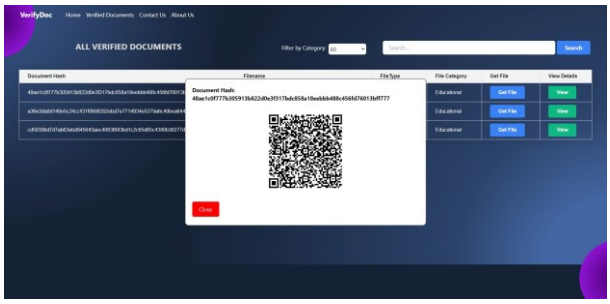


Fig.8: Viewing of the document detail

Figure 4.5 shows a QR code that can be used to access the document. By scanning the QR code, the user can obtain a quick summary of the document that includes information on the file name, type, transaction hash value, and the identity of the person who verified the document.

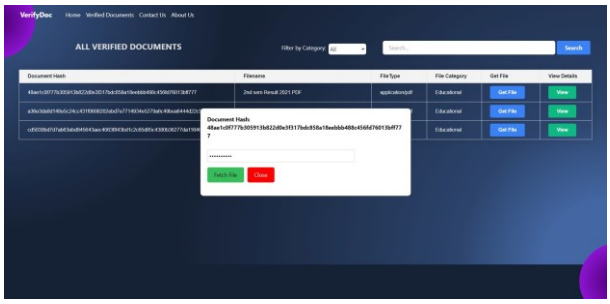


Fig.9: Downloading of document

The Figure 4.6 shows the progress of the document's download. The user must provide the same password that he used to submit the document in order to download it; otherwise, the user will not be able to access it.

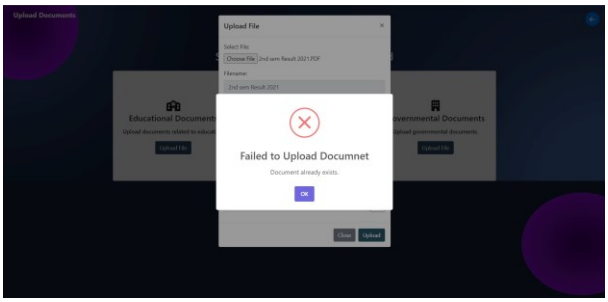


Fig.10: Uploading of a tampered/fake document

The Figure 4.7 shows the snapshot of uploading of the altered document. If a person tampers with a document and tries to upload the tampered document or tries to re-upload the original document, then the website rejects to upload the document \

5 CONCLUSION

In this paper, we provide a blockchain-based fix for the issue of certificate forgeries. Detecting fake documents using blockchain technology is a potential way to fight fraud and forgeries. Because blockchain technology is tamper-resistant and decentralized, it may be used by companies to create transparent and safe processes for authenticating documents. This protects against fraudulent actions and ensures the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

integrity of official documents while also improving security and streamlining the verification process. As technology develops, there is a great deal of promise for lowering risks and fostering confidence in document verification procedures across a range of businesses by incorporating blockchain into counterfeit detection efforts. To further increase the precision and effectiveness of forgery detection, future studies can investigate the integration of blockchain technology with cutting-edge fields like artificial intelligence and machine learning. Furthermore, extending the use of blockchain-based verification systems to additional industries might improve general dependability and confidence in online transactions and document management.

6 EVALUATION STEPS

Description	Result
If Meta Mask Extension is available	Redirect to login request
If the meta mask account is created	Redirect to home page
Choosing original document of any format	Upload successful
Accepting the transaction if the account has enough Ethers	Stores Document hash
Checking whether the document is original or not.	Verified document
Checking whether the user can download the document or not	Download success

7 REFERENCES

[1] Omsar S. Salesh, Osman Ghazali and Muhammad Ehsan Rana, “Blockchain based framework for educational certificates verification”, Journal of Critical Reviews, Volume- 7, Issue-3, 2020.

[2] Leka, E. and Selimi, B., 2021. Development and Evaluation of Blockchain based Secure Application for Verification and validation of Academic Certificates. Annals of Emerging Technologies in Computing (AETiC), 5(2), pp.22-36.

[3] Mili Rafi, Sherin Mary Shaji and Prof. Ashly Thomas, “Certificate Management and Validation system using Blockchain”, International Research Journal of Engineering and Technology (IRJET), Volume-7, Issue-5, May 2020.

[4] Curmi, A. and Inguanez, F., 2018, July. “Blockchain based certificate verification platform”. In International Conference on Business Information Systems (pp. 211-216). Springer, Cham.

[5] Clemens Brunner, Fabian Knirsch and Dominik Engel, “SPROFF: A Platform for Issuing and Verifying Documents in a Public Blockchain”, 5th International Conference on Information Systems Scurity and Privacy (ICISSP) 2019.

[6] Jayesh G.Dongre, Sonali M. Tikam, Dr. Kishore.T.Patil and Vasudha Gharat, “Education Degree Fraud Detection and Student Certificate Verification using Blockchain”, International Journal of Engineering Research & Technology, ISSN, Volume-9, Issue-7, July 2020.

[7] A. Gayathiri, J. Jayachitra and Dr.S.Matilda, “Certificate validation using blockchain”, IEEE 7th International Conference on Smart Structures ans Systems ICSSS 2020.

[8] Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September.“A novel blockchain-based education records verification solution”. In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).

[9] Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September.“A novel blockchain-based education records verification solution”. In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).

[10] Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September.“A novel blockchain-based education records verification solution”. In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).

[11] Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September.“A novel blockchain-based education records verification solution”. In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).

[12] Rafah Amer Jaafar PP, Saad Najim Alsaad P. "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric", TEM Journal. Volume 12, Issue 4.

[13] Marco Baldi , Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi “Certificate Validation through Public Ledgers and Blockchains” .In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

[14] Anthonya, Michael Christian Leea, Rafaelle Richel Pearla, Ivan Sebastian Edberta, Derwin Suhartono “Developing an anti-counterfeit system using blockchain technology” published in 7th International Conference on Computer Science and Computational Intelligence 2022, ISSN - 1877-0509.

[15] Vipul Badhe, Pooja Nhavale, Sonal Todkar, Prajakta Shinde, Prof. Kiran Kolhar “Digital Certificate System for Verification of Educational Certificates using Blockchain" published in International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011, Volume 7, Issue : September-October-2020.