DOCUMENT VERIFICTION SYSTEM

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Use Case Report

submitted by

KAKARLA SANTHI PRIYA

22501A0572

Under the guidance of

Mr. A. Prashant, Asst. Prof.

Department of Computer Science and Engineering

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

2024-25

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

CERTIFICATE

This is to certify that the Use Case report entitled **“Document verification system”** that is being submitted by **K. Santhi priya (22501A0572)** as part of Assignment-1 and Assignment-2 for the **Blockchain Technology**(**20CS4601C)** course in **3-2** during the academic year **2024-25**.

Head of the Department
Dr. A. Jayalakshmi,
Professor and Head,
Department of CSE,
PVPSIT, Vijayawada

Course Coordinator
Mr. A. Prashant
Assistant Professor,
Department of CSE,
PVPSIT, Vijayawada

MARKS

ASSIGNMENT-1: ____/5

ASSIGNMENT-2: ____/5

INDEX

1. INTRODUCTION

Blockchain technology is a system that acts as a decentralised database which is a digital ledger that stores data and information throughout the entire network of a computer systems. Blockchain technology were introduced in 2006 with the existents of Bitcoin where it involves cryptocurrency. A cryptocurrency is a digitized currency that can be used to do a transaction and buy stuffs through online. With the help of blockchain technology all the transactions that have been made in the network are being kept safe since the system uses a distributed ledger that will let others know the credibility of a transactions. Blockchain technology had been used by many organizations now such as healthcare, inventory, management, finance and more. Blockchain technology has been helpful in implementing a system that will keep the transactions and storing the data in a safe manner and it is easier to track down the attacker with the implementation of blockchain technology. A document verification system will be able to increase its security feature with the help of blockchain technology. [7]

Technology has been evolved throughout the years where people nowadays depend on technology to carry out their daily lives. The current problem that relates to a document verification system is to prevent the document from being forged. Document forgery involves in copying and imitating the details of the original documents such as identity number and signature.

Other than that, there is a problem with the current system in detecting a forged file where it only checks for its availability of the file in the system. It does not go through content of the file to check for its integrity. There are not many systems that will go through the content of a document and verify each character in the document. Furthermore, the current document verification system has a low efficiency in detecting the forged file[4]. Current practices of document verification are not efficient and time consuming in getting the results. The verification of the file integrity is not accurate where sometimes it gives false results.

Another major issue with current document verification systems is the lack of transparency. Traditional verification methods often rely on centralized authorities, which means that users must trust a single entity to validate the authenticity of a document. This creates a single point of failure, making the system vulnerable to data manipulation, unauthorized modifications, or even corruption. Blockchain technology, on the other hand, enhances transparency by distributing verification across multiple nodes in a decentralized network. Each document verification transaction is recorded on an immutable ledger, ensuring that any changes made to a document are tracked and cannot be altered without consensus from the network. [4]

Lastly, scalability remains a major challenge in traditional document verification methods. As organizations generate and process a vast number of documents daily, centralized verification systems struggle to keep up with demand, leading to delays and inefficiencies. Blockchain technology offers a scalable solution by enabling parallel processing of verification requests through distributed networks.

2.BACKGROUND

2.1 Challenges in Traditional Document Verification Systems

One of the most pressing issues in traditional document verification systems is the prevalence of fraud and forgery. Counterfeit academic certificates, forged identity proofs, and fraudulent legal documents are frequently circulated, leading to significant financial and reputational losses

Beyond fraud, the lack of transparency in traditional verification systems often leads to disputes and mistrust. The process is typically opaque, making it difficult for third parties to independently verify the authenticity of a document, which can result in prolonged conflicts and legal complications [8]. These expenses, often passed on to end-users, make the process less accessible, particularly for individuals and smaller organizations [7]. Perhaps most critically, centralized systems are vulnerable to single points of failure, such as hacking, corruption, and data loss. If a central authority's database is compromised, the integrity of all documents stored within it is jeopardized, posing a significant risk to the entire system.

2.1.1. Fraud and Forgery

- **Counterfeit Documents**: One of the most significant issues is the prevalence of fraudulent documents, such as fake academic certificates, forged identity proofs, and counterfeit legal documents. These fraudulent activities lead to substantial financial and reputational losses for organizations and individuals alike.
- **Sophisticated Fraud Techniques**: Advances in technology have made it easier for fraudsters to create high-quality counterfeit documents that are difficult to detect using traditional methods.
- **Impact**: According to Ponemon Institute Research, the average total cost digital document leakage is about 3.62 million dollars. [6]

2.1.2. Lack of Transparency

- **Opaque Processes**: Traditional verification systems often operate in a centralized and opaque manner, making it difficult for third parties to independently verify the authenticity of a document. This lack of transparency can lead to disputes and mistrust among stakeholders.
- **Limited Auditability**: Without a transparent and immutable record of document transactions, it becomes challenging to trace the history of a document or verify its legitimacy, resulting in prolonged conflicts and legal complications [4].

2.1.3. High Costs

- **Operational Expenses**: Maintaining centralized verification systems involves significant costs, including infrastructure, personnel, and administrative expenses. These costs are often passed on to end-users, making the verification process expensive and less accessible, particularly for individuals and smaller organizations [7].
- **Inefficiencies**: Manual verification processes are time-consuming and labor-intensive, further driving up costs and reducing efficiency [2].

2.1.4. Vulnerability to Single Points of Failure

- **Centralized Systems**: Traditional systems rely on centralized databases or authorities, which are vulnerable to single points of failure. If a central authority's database is compromised due to hacking, corruption, or technical failures, the integrity of all documents stored within it is jeopardized.
- **Data Loss**: Centralized systems are also susceptible to data loss, which can have catastrophic consequences for organizations and individuals relying on those documents [5].

2.1.5. Inefficiency and Delays

- **Manual Processes**: Many traditional systems still rely on manual processes for document verification, which are prone to human error and delays[1] This inefficiency can lead to significant bottlenecks, especially in high-volume scenarios such as academic admissions, employment verification, or legal proceedings [1].
- **Lack of Interoperability**: Different organizations and institutions often use disparate systems that are not interoperable, making it difficult to share and verify documents across platforms [7].

2.1.6. Privacy Concerns

- **Data Breaches**: Centralized systems store sensitive personal and organizational data in a single location, making them attractive targets for cyberattacks. Data breaches can result in the exposure of confidential information, leading to identity theft and other privacy violations [5].
- **Lack of User Control**: In traditional systems, users have little to no control over their data once it is submitted for verification. This lack of control raises concerns about how their data is stored, used, and shared [4].

2.1.7. Scalability Issues

- **Limited Capacity**: Traditional systems are often not designed to handle large volumes of documents efficiently, leading to delays and backlogs during peak periods [6].
- **Inflexibility**: These systems are typically rigid and lack the flexibility to scale up or down based on demand, making them unsuitable for dynamic and fast-paced environments [7].

3.BLOCKCHAIN BASICS

Blockchain is a revolutionary technology that serves as a decentralized, distributed ledger for recording transactions. It is best known as the underlying technology for cryptocurrencies like Bitcoin, but its applications extend far beyond digital currencies. At its core, blockchain is designed to ensure transparency, security, and trust in digital transactions. Below are the key concepts that define blockchain technology:

3.1 Decentralization

Unlike traditional systems that rely on a central authority (e.g., banks or governments) to manage and verify transactions, blockchain operates on a decentralized network. This means that no single entity has control over the entire system. Instead, the ledger is maintained by a network of computers (nodes) that work together to validate and record transactions. Decentralization eliminates the need for intermediaries, reduces the risk of manipulation, and enhances trust among participants.

3.2 Immutability

One of the most critical features of blockchain is its immutability. Once a transaction is recorded on the blockchain, it cannot be altered or deleted. This is achieved through the use of cryptographic hashing, where each block contains a unique hash of the previous block, creating a chain of blocks that are linked together. Any attempt to tamper with a block would require altering all subsequent blocks, which is computationally infeasible[3]. This immutability ensures that the data stored on the blockchain is permanent and tamper-proof.

3.3 Smart Contracts

Smart Contracts are codes that can be executed by the Blockchain mining nodes. A smart contract is a self-executing code that can verify the enforcement of predefined terms and conditions.[4]. For example, in document verification system, smart contracts can be used to automate the process of verifying the authenticity of documents, such as academic certificates, identity proofs, or legal contracts[1]. Smart contracts eliminate the need for intermediaries, reduce the risk of human error, and ensure that transactions are executed efficiently and transparently. They are a key feature of blockchain platforms like Ethereum, which enable the development of decentralized applications (dApps).

3.4 Cryptographic Security

Blockchain relies on advanced cryptographic techniques to secure data. Each transaction is encrypted and linked to the previous transaction using a cryptographic hash. Additionally, participants in the network use digital signatures to verify their identity and authorize transactions. This ensures that only authorized parties can initiate transactions, and the integrity of the data is maintained.[4]

3.5 Consensus Mechanism

To ensure that all participants in the network agree on the state of the ledger, blockchain uses consensus mechanisms. These are protocols that validate transactions and add them to the blockchain. Common consensus mechanisms include Proof of Work (PoW), used by Bitcoin, and Proof of Stake (PoS), used by Ethereum 2.0. These mechanisms prevent fraudulent activities and ensure that the blockchain remains secure and trustworthy.[3]

3.6 Transparency and Traceability

All transactions on the blockchain are recorded in a public ledger that is accessible to all participants. This transparency allows anyone to verify the authenticity of transactions, fostering trust and accountability. Additionally, blockchain provides traceability, as every transaction is time-stamped and linked to previous transactions.

3.7 Data Integrity and Reliability

Blockchain ensures that data remains accurate and consistent across all nodes in the network. Due to its decentralized nature and cryptographic validation, once data is recorded, it cannot be tampered with or lost, making blockchain an excellent solution for maintaining secure and reliable records.[5]

3.8 Enhanced Privacy and Control Over Data

With blockchain, individuals and organizations can control their own data through private keys and permissioned access. Unlike centralized databases, where data is stored and controlled by a single entity, blockchain allows users to decide who can access their information, improving privacy and security.

3.9 Decentralized Identity Management

Blockchain enables individuals to have full control over their digital identity, eliminating the risk of identity theft. Users can share only necessary details for verification without exposing sensitive personal information, which is crucial for secure online authentication.[3]

4.USECASE OVERVIEW

The **Document Verification System** is a blockchain-based solution designed to address the challenges of fraud, inefficiency, and lack of transparency in traditional document verification processes. By leveraging blockchain technology, the system ensures that documents such as academic certificates, identity proofs, and legal contracts are tamper-proof, easily verifiable, and securely stored.

Document verification system using blockchain consists of many software designs which include Ethereum Blockchain, Truffle Suite, IPFS Cluster, AES encryption and web application. Ethereum blockchain will be the blockchain platform to store the IPFS hash value from the IPFS Cluster which points to the file that has been stored in the IPFS[7]. Distributed HashTables(DHTs) are widely used to coordinate and maintain metadata about peer-to-peer systems.[8] Truffle Suite is the platform that is used to develop an application uses the test Ethereum network without using any computational power and resources. Finally, web application will be used as the interface for the document verification system where the user will upload and verify a document. [8]

4.1 Objectives of the usecase

4.1.1 Investigate the Limitations of Ethereum Blockchain and IPFS:

The system aims to explore the limitations of Ethereum blockchain and Interplanetary File System (IPFS) in the context of developing a document verification system. This includes understanding how these technologies can be effectively integrated to address the challenges of document forgery and verification. [7]

4.1.2 Verify Document Integrity:

The system is designed to verify the integrity of documents by ensuring that the content of the document has not been tampered with or forged. This is achieved by comparing the hash value of the original document stored on the blockchain with the hash value of the document being verified.[8]

4.1.3 Provide a Secure Storage System:

The system aims to provide a secure and tamper-proof storage solution for documents using blockchain technology. By storing document hashes on the blockchain and the actual documents on IPFS, the system ensures that documents are safe from forgery and unauthorized modifications.

4.1.4 Ensure Data Security and Privacy:

The system aims to enhance data security and privacy by using AES encryption to encrypt documents before they are uploaded to the system. This ensures that only authorized users with the correct password can access the document's content.[7]

4.1.5 Enable Decentralized and Transparent Verification:

By leveraging blockchain technology, the system ensures that the verification process is decentralized and transparent. This eliminates the need for intermediaries and builds trust among users by providing a tamper-proof and auditable record of all transactions.

4.2 Scope of the project

The Document Verification System based on blockchain technology aims to address the growing issue of document forgery. The scope of the project encompasses the development of a decentralized system that leverages Ethereum blockchain for storing document hashes and Interplanetary File System (IPFS) for decentralized document storage. The system is designed to handle various types of documents, including academic certificates, identity proofs, and legal contracts, ensuring that they are protected from unauthorized modifications and forgery [2].

The system integrates smart contracts to automate the verification process, eliminating the need for manual intervention and reducing the risk of human error. By using AES encryption, the system ensures that documents are securely encrypted before being uploaded, allowing only authorized users with the correct password to access the content [7]. The scope also includes the development of a user-friendly web application that allows users to easily upload, verify.

Furthermore, the system is designed to provide transparency and traceability by maintaining an immutable record of all transactions on the blockchain. This ensures that any changes or modifications to the document can be easily detected, thereby enhancing trust and accountability [5]. The project also explores the use of IPFS Cluster to create a private network for document storage, ensuring that sensitive information is only accessible to authorized peers [7].

4.3 Design of the project

The entire design of the document verification system is illustrated in the **Fig. 4.3**

4.3.1 User layer

The User Layer consists of two main entities: the Document Holder and the Verifier. The Document Holder is responsible for uploading documents to the system, providing the encrypted document and the encryption password as inputs. The Verifier is responsible for verifying documents by submitting the document, encryption password, and transaction hash as inputs. This layer represents the end-users who interact with the system to upload and verify documents.

4.3.2 Web Application (User Interface)

The Web Application serves as the User Interface (UI) for the system. It provides an intuitive interface for users to upload files or verify files. The UI includes input fields for the Document Holder to upload encrypted documents and for the Verifier to submit documents for verification.

4.3.3 Blockchain Layer

The Blockchain Layer is powered by Ethereum Blockchain, which stores the IPFS hash value and encryption password for each document. Smart contracts are used to automate the verification process by comparing the hash of the submitted document with the hash stored on the blockchain. Ganache is used as a local test Ethereum blockchain for development purposes, while Metamask acts as an Ethereum wallet to manage accounts and pay transaction fees.

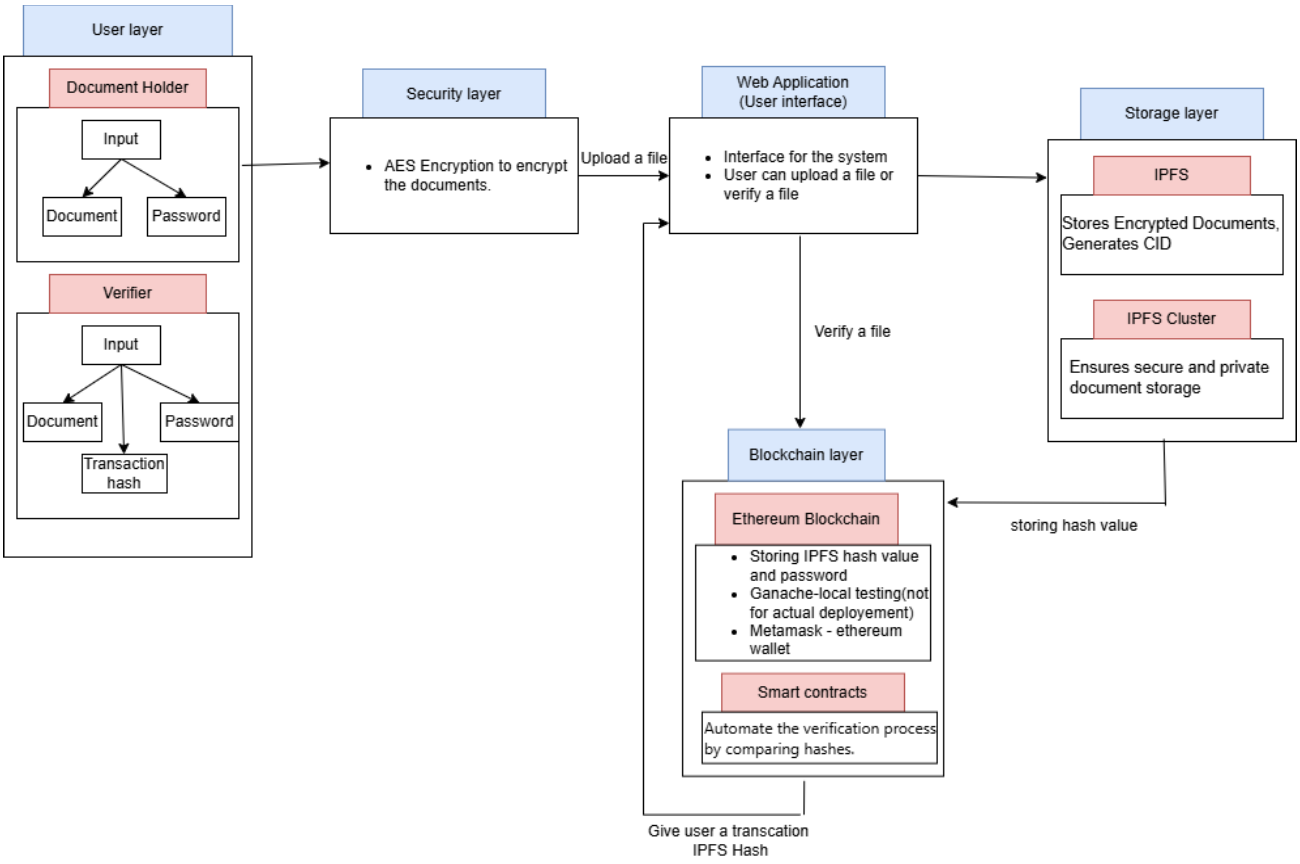

User layer
Document Holder
Input
Document
Password
Verifier
Input
Document
Password
Transaction hash
Security layer
AES Encryption to encrypt the documents.
Upload a file
Web Application (User interface)
Interface for the system
User can upload a file or verify a file
Storage layer
IPFS
Stores Encrypted Documents, Generates CID
IPFS Cluster
Ensures secure and private document storage
Verify a file
storing hash value
Blockchain layer
Ethereum Blockchain
Storing IPFS hash value and password
Ganache-local testing(not for actual deployement)
Metamask - ethereum wallet
Smart contracts
Automate the verification process by comparing hashes.
Give user a transcation IPFS Hash

Fig. 4.3- Overall design

4.3.4 Storage Layer

The Storage Layer consists of IPFS (InterPlanetary File System) and IPFS Cluster. IPFS is used to store the encrypted documents and generate a unique Content Identifier (CID) for each document. IPFS Cluster ensures that documents are securely stored and shared only with authorized peers in a private network.

4.3.5 Security Layer

The Security Layer ensures the security and integrity of the system. It includes AES encryption, which is used to encrypt documents before they are uploaded, ensuring that only authorized users with the correct password can access the content. Cryptographic hashing is used to generate unique hashes for each document, making it easy to detect any changes or tampering. This layer ensures that the system is secure and resistant to unauthorized access or modifications.

5.IMPLEMENTATION

5.1 Uploading process

The document verification system ensures that uploaded files are authentic, securely stored, and tamper-proof. To achieve this, the system leverages AES encryption, IPFS for decentralized storage, and Ethereum blockchain with smart contracts to maintain security and transparency. The overall work flow of uploading process is illustrated in **Fig-5.1**

5.1.1 Encryption of the Document

Before uploading, the user must encrypt the document using the AES (Advanced Encryption Standard) algorithm to ensure confidentiality. The encryption process can be performed using Microsoft products (2007 or later) or File Explorer. This step ensures that even if an unauthorized party accesses the file, they cannot decrypt it without the correct password.

5.1.2 File Submission to the System

Once the document is encrypted, the user uploads the file along with the encryption password through the system’s web application. The system checks if:

- The uploaded file is in PDF format.
- The file is properly encrypted using AES.
- The file is not corrupted.

If any of these conditions fail, the system rejects the upload and prompts the user to correct the issue. Otherwise, the process continues.

5.1.3 Uploading to IPFS (InterPlanetary File System)

If the document meets all criteria, the system sends it to the IPFS Cluster via the IPFS daemon. IPFS, a decentralized storage protocol, ensures that the document is stored securely and can be retrieved using a unique hash value. This hash serves as a digital fingerprint for the file, verifying its authenticity and preventing tampering.

5.1.4 Smart Contract Execution

Before storing the IPFS hash value and encryption password on the Ethereum blockchain, the system triggers a smart contract, which performs the following actions:

1. **Validation**: The smart contract verifies that the file meets all requirements (PDF format, encrypted, and successfully uploaded to IPFS).
2. **Transaction Initiation**: The smart contract generates a transaction to store the IPFS hash and password securely on the blockchain.
3. **User Confirmation**: The system requests the user’s confirmation for the transaction. The user must approve and pay a small gas fee in ETH (Ether) to complete the process.

4. **Storage on Blockchain**: Once confirmed, the smart contract permanently stores the IPFS hash and password in a new block on the Ethereum blockchain, ensuring immutability and preventing unauthorized modifications.

5.1.5 Confirmation and Completion

- After the transaction is confirmed on the blockchain, the system provides the user with the IPFS hash and transaction hash for future verification.
- The user can use this hash to retrieve and verify the document's authenticity later.
- The immutable nature of the blockchain ensures that once the document is stored, it cannot be altered or deleted, maintaining trust in the verification system.

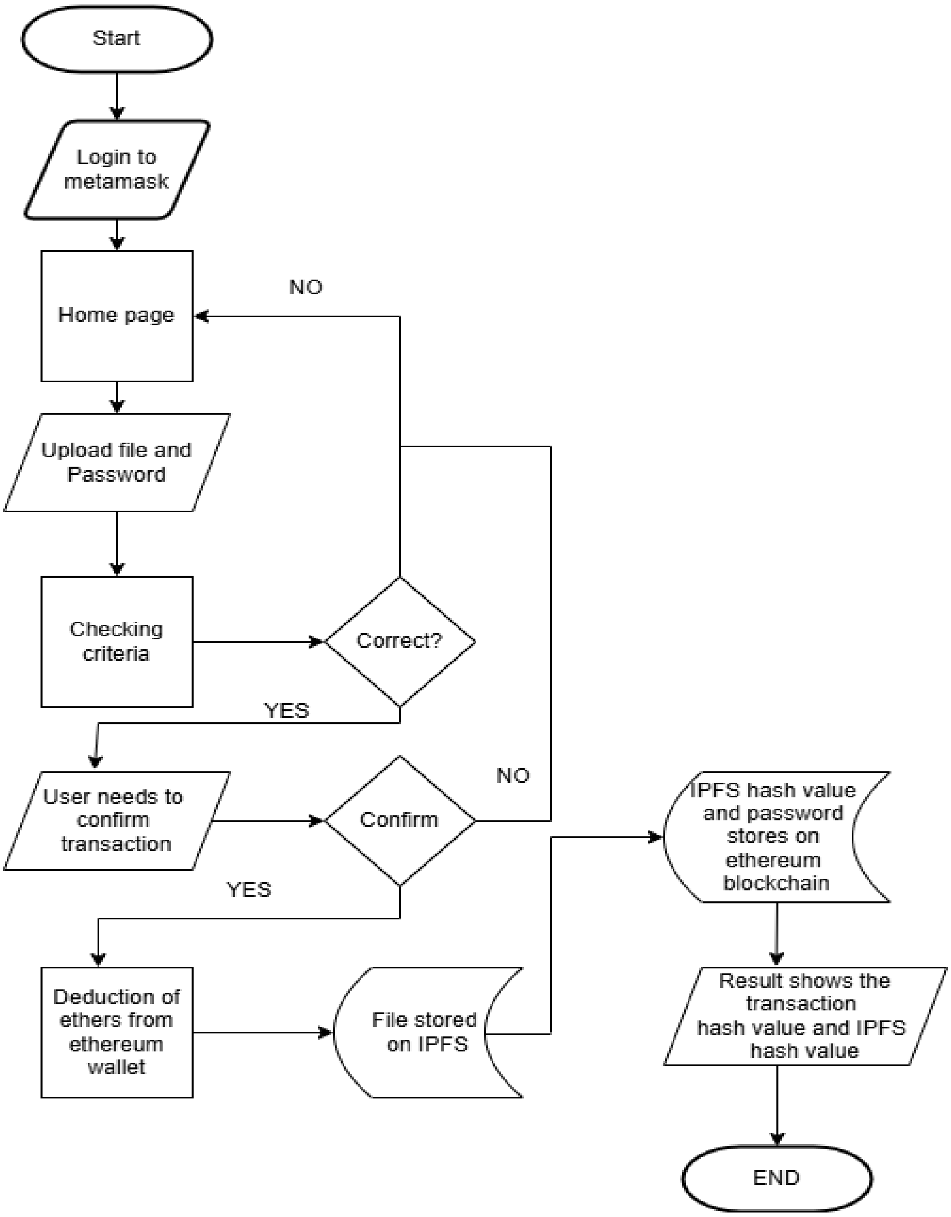

Start
Login to metamask
Home page
NO
Upload file and Password
Checking criteria
Correct?
YES
User needs to confirm transaction
Confirm
NO
YES
Deduction of ethers from ethereum wallet
File stored on IPFS
IPFS hash value and password stores on ethereum blockchain
Result shows the transaction hash value and IPFS hash value
END

Fig. 5.1-Flow diagram for uploading process

5.2 Verification process

The verification process ensures that an uploaded document remains authentic, untampered, and accessible. It involves retrieving the file details from the blockchain and comparing them with the submitted file to validate its integrity. The system relies on transaction hash, encryption password, and IPFS hash to verify authenticity.

5.2.1: User Input Submission

To begin the verification process, the user must provide:

1. The encrypted file they want to verify.
2. The encryption password used during upload.
3. The transaction hash generated when the file was uploaded to the blockchain.

These three components are mandatory for verification to proceed. If any component is missing, the system rejects the request.

5.2.2: Fetching Data from Blockchain

Once the user submits the required details, the system triggers a smart contract deployed on the Ethereum blockchain. The smart contract performs the following actions:

- Validates the transaction hash provided by the user.
- Fetches the stored IPFS hash and encryption password from the blockchain.
- Verifies that the transaction exists and the stored data has not been tampered with.

If the transaction hash does not match any stored data, the smart contract returns an error indicating that the file does not exist in the blockchain.

5.2.3 Retrieving the Original File

Once the smart contract confirms the transaction hash's validity, the system uses the IPFS hash to fetch the encrypted file from the IPFS network. This ensures that the system always references the correct version of the document. If the file cannot be found using the IPFS hash, it may indicate data loss or corruption, and the system will alert the user.

5.2.4 Hashing the Submitted File

The system computes the cryptographic hash of the user-submitted file. This hash is then compared with the IPFS hash retrieved from the blockchain via the smart contract.

- If the computed hash matches the blockchain-stored IPFS hash, the file is authentic and untampered.
- If the computed hash does not match, the file may have been altered or corrupted.

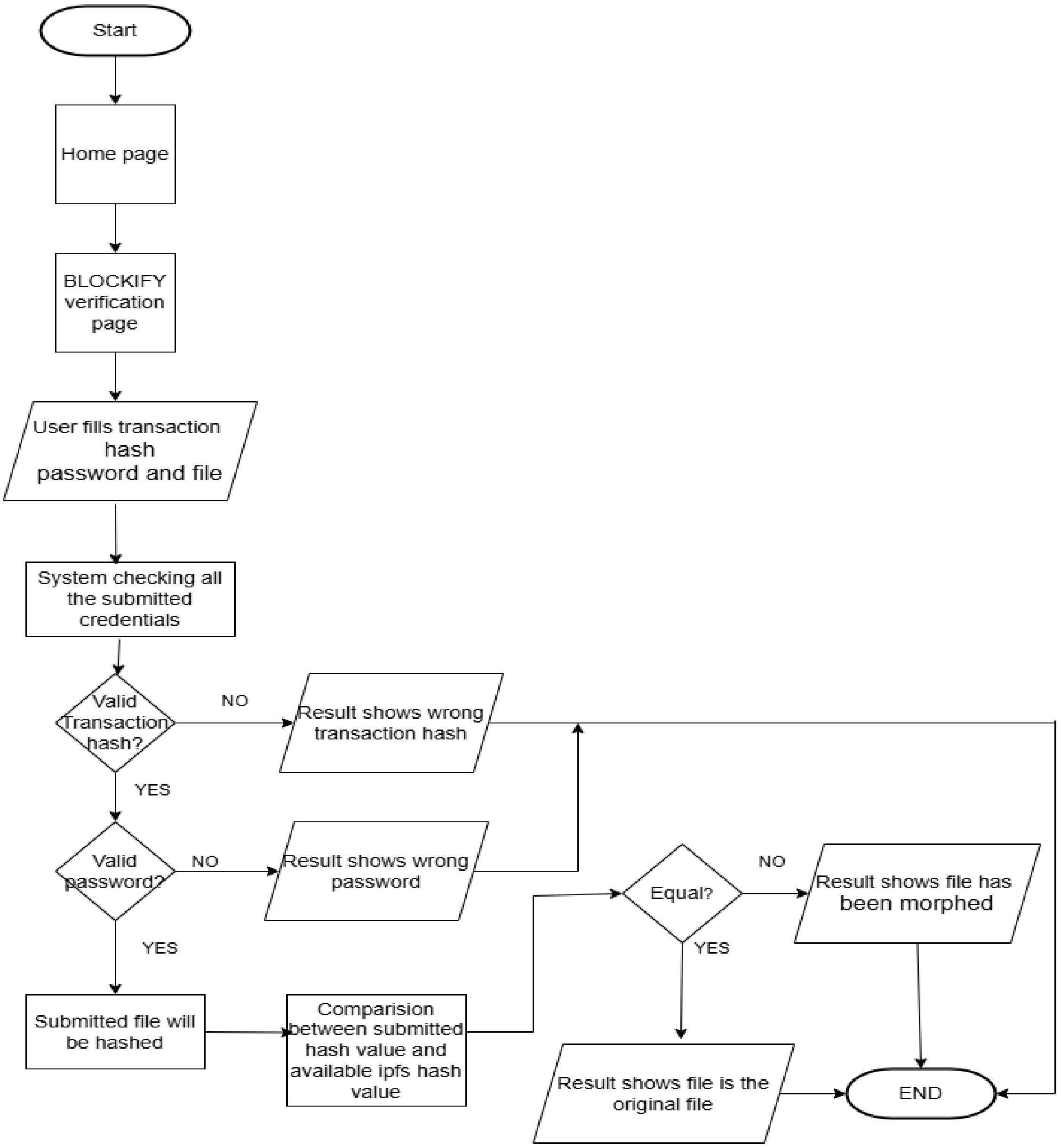
5.2.5 Password Validation

As per **Fig-5.2** the system verifies whether the submitted encryption password matches the one stored on the blockchain. The system sends a query to the smart contract, which checks the stored password against the submitted password.

- If the password matches, the smart contract confirms that the document is valid.
- If the password does not match, the system rejects the verification request.

5.2.6 Final Verification Outcome

If the file hash and password match, the document is verified as authentic. If the transaction hash is invalid, the file was never uploaded. A mismatch in the file hash indicates tampering, while an incorrect password prevents verification.



Start
Home page
BLOCKIFY verification page
User fills transaction hash password and file
System checking all the submitted credentials
Valid Transaction hash?
NO
Result shows wrong transaction hash
YES
Valid password?
NO
Result shows wrong password
YES
Submitted file will be hashed
Comparision between submitted hash value and available ipfs hash value
Equal?
NO
Result shows file has been morphed
YES
Result shows file is the original file
END

Fig. 5.2-Flow diagram for verification process

5.3 Defining smart contracts

5.3.1 Uploading a document

This function allows users to store document details (IPFS CID and password) on the blockchain.

How It Works:

1. Users provide a transactionHash, cid, and password.
2. The contract saves the details in the documents mapping.
3. It emits an event DocumentUploaded for tracking uploads.

Code snippet:

```
function uploadDocument(string memory transactionHash, string memory cid, string memory password) public {
   documents[transactionHash] = Document(cid, password);
   emit DocumentUploaded(transactionHash, cid, password);
}
```

5.3.2 Verifying a Document

This function verifies whether a given document matches the stored details.

How It Works:

1. Users input transactionHash, submittedCid, and submittedPassword.
2. The contract fetches stored document details using transactionHash.
3. It compares the submitted and stored values using keccak256 hashing.
4. If they match, the document is verified (true); otherwise, verification fails (false).

Code snippet

```
function verifyDocument(string memory transactionHash, string memory submittedCid, string memory submittedPassword) public view returns (bool) {
   Document memory document = documents[transactionHash];
if(keccak256(abi.encodePacked(document.cid))==keccak256(abi.encodePacked(submittedCid))&&keccak256(abi.encodePacked(document.password))==keccak256(abi.encodePacked(submittedPassword))) {
     return true;
   } else {
      return false; } }
```

6.BENIFITS

6.1 Improved Data Security

- **Immutable Records**: Once a document is stored on the blockchain, it cannot be altered or deleted. This ensures that the document's integrity is maintained, preventing tampering or forgery.
- **Cryptographic Hashing**: Each document is assigned a unique cryptographic hash (e.g., SHA-256), which acts as a digital fingerprint. Any changes to the document will result in a completely different hash, making tampering easily detectable.
- **Decentralized Storage**: Documents are stored on a decentralized network (e.g., IPFS), reducing the risk of data breaches or single points of failure.
- **Encryption**: Documents are encrypted using **AES encryption** before being uploaded, ensuring that only authorized users with the correct password can access the content.[7]

6.2 Enhanced Transparency

- **Public Ledger**: All transactions (e.g., document uploads and verifications) are recorded on a public blockchain ledger, making the process transparent and auditable.
- **Traceability**: Every action related to a document (e.g., upload, verification) is time-stamped and linked to previous transactions, allowing users to track the document's history.
- **Trustless System**: Blockchain eliminates the need for intermediaries (e.g., notaries, third-party verification services), as the system itself ensures trust through cryptographic proofs.

6.3 Efficient Patient Consent Management

- **Smart Contracts**: Smart contracts automate the process of managing patient consent. For example, a smart contract can ensure that a document is only accessed or shared if the patient has explicitly granted consent.
- **Granular Control**: Patients can specify who can access their documents and under what conditions (e.g., time-limited access, specific purposes).
- **Auditability**: All consent-related transactions are recorded on the blockchain, providing a transparent and immutable record of who accessed the document and when.[3]

6.4 Fraud Prevention

- **Unique Digital Signatures**: Each document is assigned a unique digital signature (e.g., IPFS hash), making it impossible to forge or duplicate the document without detection.

- **Real-Time Verification**: Documents can be verified in real-time by comparing their hash with the one stored on the blockchain, ensuring that only authentic documents are accepted.

6.5 Cost Efficiency

- **Elimination of Intermediaries**: By removing the need for intermediaries (e.g., notaries, third-party verification services), blockchain reduces the cost of document verification.
- **Automation**: Smart contracts automate the verification process, reducing the need for manual intervention and minimizing human error.

6.6 Global Accessibility

- **Cross-Border Verification**: Blockchain-based document verification systems can be accessed from anywhere in the world, making it easy to verify documents across borders without relying on local authorities.
- **Interoperability**: Blockchain systems can be integrated with other platforms and systems, enabling seamless data sharing and verification.

6.7 Regulatory Compliance

- **Auditable Records**: Blockchain provides a tamper-proof and auditable record of all transactions, making it easier for organizations to comply with regulatory requirements (e.g., GDPR, HIPAA).
- **Data Ownership**: Patients have full control over their data and can grant or revoke access at any time, ensuring compliance with data protection regulations.

The integration of blockchain technology into a document verification system offers a transformative solution that enhances data security, transparency, and efficiency. By leveraging blockchain's immutable and decentralized nature, the system ensures tamper-proof document storage, automated consent management, and real-time verification, fostering trust and compliance across industries. This innovative approach addresses the limitations of traditional systems, making it a robust and reliable solution for secure document verification in the digital age.

The use of blockchain in a document verification system offers numerous benefits, including improved data security, enhanced transparency, efficient patient consent management, fraud prevention, cost efficiency, global accessibility, and regulatory compliance. These benefits make blockchain an ideal solution for secure and efficient document verification.

7.CHALLENGES

7.1 Scalability Issues

- **Transaction Speed**: Public blockchains like Ethereum have limited transaction speeds (e.g., 15 transactions per second). This can be a bottleneck for large-scale applications that require high throughput.
- **Storage Limitations**: Storing large files directly on the blockchain is impractical due to high costs and limited storage capacity. While IPFS is used for decentralized storage, managing large volumes of data can still be challenging.

7.2 Complexity of Implementation

- **Technical Expertise**: Developing and deploying blockchain-based systems requires specialized knowledge of blockchain technology, smart contracts, and decentralized storage systems like IPFS.
- **Integration with Existing Systems**: Integrating blockchain with existing document management systems can be complex and time-consuming.[7]

7.3 Privacy Concerns

- **Public Blockchain**: While blockchain provides transparency, storing sensitive data (e.g., medical records) on a public blockchain can raise privacy concerns. Even though the data is encrypted, the metadata (e.g., transaction details) is visible to all participants.
- **IPFS Public Network**: Files stored on the public IPFS network can be accessed by anyone with the CID, which may not be suitable for sensitive documents.[6]

7.4 Regulatory and Legal Challenges

- **Compliance**: Ensuring compliance with data protection regulations (e.g., GDPR, HIPAA) can be challenging, especially when dealing with cross-border data sharing.
- **Legal Recognition**: Some jurisdictions may not yet recognize blockchain-based records as legally valid, which could limit the system's adoption.

7.5 User Adoption

- **User Experience**: Blockchain-based systems can be complex for non-technical users, requiring them to manage private keys, pay gas fees, and interact with smart contracts.
- **Awareness and Trust**: Many users may not be familiar with blockchain technology or may not trust it due to its association with cryptocurrencies and speculative activities.[4]

7.6 Energy Consumption

- **Proof of Work (PoW)**: Blockchains that use PoW consensus mechanisms (e.g., Ethereum 1.0) consume significant amounts of energy, raising environmental concerns.[3]
- **Sustainability**: Transitioning to more energy-efficient consensus mechanisms (e.g., Proof of Stake) is essential for long-term sustainability.[2]

7.7 Interoperability

- **Cross-Chain Compatibility**: Different blockchains may not be compatible with each other, making it difficult to share data across multiple platforms.
- **Integration with Legacy Systems**: Integrating blockchain with existing legacy systems can be challenging due to differences in technology and protocols.

While blockchain-based document verification systems face challenges such as scalability issues, high costs, privacy concerns, and regulatory hurdles, these obstacles are not insurmountable. With ongoing research, technological advancements, and collaboration between stakeholders, many of these challenges are being actively addressed. For instance, the transition to Proof of Stake (PoS) and Layer 2 solutions is already improving scalability and reducing energy consumption, while private blockchains and enhanced encryption techniques are mitigating privacy concerns. Additionally, governments and regulatory bodies are increasingly recognizing the potential of blockchain, paving the way for clearer guidelines and legal frameworks.

Despite these challenges, the transformative potential of blockchain technology in document verification cannot be overlooked. Its ability to provide immutable, transparent, and decentralized solutions ensures enhanced security, trust, and efficiency in managing sensitive documents. As the technology matures and adoption grows, blockchain is poised to become a cornerstone of secure and reliable document verification systems, revolutionizing industries such as healthcare, education, government, and legal services. The future of document verification lies in harnessing the power of blockchain to create a more secure, transparent, and efficient digital ecosystem.

8 CONCLUSION

8.1 Conclusion

Blockchain-based document verification systems offer a revolutionary approach to ensuring data security, transparency, and efficiency. By leveraging blockchain's immutability, decentralization, and smart contracts, these systems address critical issues such as document forgery, fraud, and inefficient verification processes. Key benefits include tamper-proof records, real-time verification, automated consent management, and cost savings through the elimination of intermediaries. However, challenges such as scalability, high costs, privacy concerns, and regulatory hurdles remain, requiring ongoing research and innovation.

8.2 Future enhancements:

To improve the efficiency and adoption of blockchain-based document verification systems, several enhancements can be implemented. Scalability can be addressed through sharding and Layer 2 solutions, allowing the system to handle a higher number of transactions efficiently.[6] Simplifying the user experience is crucial, as developing user-friendly interfaces and providing training for non-technical users can encourage broader adoption. Ensuring regulatory compliance by collaborating with regulators to align with standards such as GDPR and HIPAA will help maintain legal integrity and user trust. Additionally, reducing costs by optimizing gas fees and exploring decentralized storage solutions can make blockchain adoption more financially viable.[6] Integrating emerging technologies such as AI and IoT can further enhance fraud detection and automation, making verification systems more robust. Lastly, advancing smart contracts to support complex policies, such as multi-party consent and conditional access, can improve security and flexibility in document verification processes.

Looking ahead, the future of blockchain-based document verification systems is promising. Advancements in scalability solutions (e.g., sharding, Layer 2 protocols), energy-efficient consensus mechanisms (e.g., Proof of Stake), and enhanced privacy features (e.g., zero-knowledge proofs) are expected to address current limitations. Additionally, increased collaboration between industry stakeholders, governments, and regulatory bodies will pave the way for clearer guidelines and broader adoption.

As blockchain technology continues to evolve, it has the potential to become a cornerstone of secure and efficient document verification across industries such as healthcare, education, government, and legal services. By addressing current challenges and embracing future enhancements, blockchain-based systems will play a pivotal role in building a trustworthy, transparent, and interconnected digital ecosystem. The journey toward widespread adoption may be gradual, but the transformative impact of blockchain on document verification is undeniable, promising a future where data integrity and user trust are paramount.

9.SDG’s ADDRESSED

SGD 4 – Quality Education

Why It’s Addressed:

- Blockchain ensures the authenticity of academic records, eliminating fake degrees and enhancing trust in education.
- Students, employers, and institutions can instantly verify credentials, reducing fraud and administrative burdens.

Example: Universities store diplomas on blockchain, allowing employers to verify them without intermediaries, ensuring transparency and reducing document forgery.

SDG 9 – Industry, Innovation, and Infrastructure

Why It’s Addressed:

- A blockchain-based document verification system enhances digital infrastructure by enabling secure, decentralized, and tamper-proof data storage.
- Reduces dependency on centralized verification agencies, improving efficiency and reliability.

Example: Organizations integrate blockchain for automated verification of contracts, identity documents, and compliance records, fostering innovation in digital trust solutions.

10.REFERENCES

[1] Suganthalakshmi, M.R., Praba, M.G.C., Abhirami, M.K., & Puvaneswari, M.S. (2022). Blockchain Based Certificate Validation System.

[Link: https://www.irjmets.com]

[2] A. Husain, "Printed Document Integrity Verification Using Barcode," JurnalTeknologi (Sciences & Engineering), vol. 70:1, pp. 99–106, 2014

https://www.researchgate.net/publication/273311225_Printed_Document_Integrity_Verification_Using_Barcode

[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

[Link:https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends]

[4] Nizamuddin, N., Salah, K., Azad, M.A., Arshad, J., & Rehman, M. (2019). Decentralized Document Version Control Using Ethereum Blockchain and IPFS.

[Link:https://www.researchgate.net/publication/331917264_Decentralized_Document_Version_Control_using_Ethereum_Blockchain_and_IPFS]

[5] IBM, "What is blockchain technology?" IBM, [Online].

Visited on March 15, 2025 from https://www.ibm.com/think/topics/blockchain

[6] Han, J., & Son, Y. (2023). Design and Implementation of a Decentralized Document Management System.

[7] Zainuddin, M. D. R., & Choo, K. Y. (2023). Design a Document Verification System Based on Blockchain Technology.

https://www.researchgate.net/publication/368491012_Design_a_Document_Verification_System_Based_on_Blockchain_Technology

[8] Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System.

Visited on March 15, 2025 from https://arxiv.org/abs/1407.3561

11.APPENDIX A

https://drive.google.com/drive/folders/1YUgWSgh-rABsdyLl-VeGsiTGlbMTAmz9?usp=drive_link