RMD Sinhgad School of Engineering, Warje, Pune.

Department Of Information Technology

Digital Certificate using Blockchain

Group No:- 2

Presentation By:-

Ashutosh Mahadik
Vaishnavi More
Prathamesh Apsingekar
Devika Sawant

Guided by:- Suvarna Potdukhe

Sinhgad Institutes

Introduction

- Students must submit certificates for higher studies or job applications.
- Challenges arise due to document misplacement and forgery.
- Traditional verification processes are lengthy and manual.
- Difficulty for organizations to verify authenticity quickly.
- A decentralized application using Blockchain and IPFS for secure, tamper-proof certificate issuance and verification.

Motivation and Objective

Motivation:
- Increase in counterfeit academic documents.
- Demand for secure, verifiable digital documents.

Objective:
- Develop a system that enables Tamper-proof certificate issuance.
- Easy, reliable verification.
- Reduced dependency on manual verification processes..

Literature Survey

Paper	Year	Autor	Description
"A Blockchain-Based Accreditation and Degree Verification System",	2023	Aamna Tariq Hina Binte Haq Syed Taha Ali	This artical states Credential fraud undermines trust and incurs costs. Cerberus, a blockchain solution, offers efficient, secure credential verification with smart contract-based revocation, privacy features, and seamless integration, combating fake credentials effectively.
"A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification"	2023	Avni Rustemi Fisnik Dalipi Vladimir Atanasovski Aleksandar Aisteski	The article is about blockchain can transform education by securing digital certificates and improving credential verification. This review analyzes 34 studies (2018-2022), highlighting key themes, research gaps, and providing future recommendations for the field.
"Cost-efficient Blockchain-based e-KYC Platform using Biometric verification"	2024	Sahil Bhatia Lokendra Vaishwakarna Debasis Das	This paper proposes a blockchain-based e-KYC platform to streamline identity verification, reducing costs and security risks associated with traditional KYC. Users complete video KYC once, receive a reusable KYC key, financial institutions.

Literature Survey

Paper	Year	Autor	Description
"A Framework for Sharing Student-Owned Educational Data on Public Blockchain Network"	2024	MUSTAFA TANRIVERDİ	This artical is introduced, allowing students to own and manage their data through smart contracts on the public Ethereum network. Educational institutions can access and update data via Learning Management Systems (LMS), ensuring a decentralized, student-controlled data system. This framework enables secure, shared access to educational data across institutions.
"Blockchain based document verification system"	2023	Mayuresh Chaudhari, Kondaka Lakshmisudha	This article propose a blockchain-based solution for securely storing and verifying educational certificates. Documents are converted into a one-way hash and stored on the blockchain. Employers can verify authenticity by comparing the hash with the blockchain record. If altered, the hashes won't match, ensuring tamper-proof credential validation.

Problem Statement

- To implement a digital document verification system using blockchain to ensure secure and decentralized verification, providing guaranteed document authenticity and integrity .
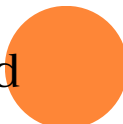
System Requirement & Specification

- Software Requirement

  - Ganache
  - IPFS
  - Metamask
  - Node.Js
  - Operating System : Windows OS

- Hardware Requirement

  - CPU type: Mid Range – CPU Intel i5
  - Clock speed: 3.0 GHz with multiple cores
  - Ram size: 8GB
  - Hard disk capacity: 1000GB
  - Keyboard - Standard Keyboard
  - Mouse - Two or Three Button Mouse
 - Monitor - LED Monitor

Project Requirement & Specification

- MetaMask
  MetaMask is a cryptocurrency wallet and gateway to Ethereum.

- Solidity
  Smart contract language for Ethereum; ideal for DeFi and NFTs.

- Ethers.js
  JavaScript library for easy Ethereum transactions and development.

- Blockchain
  Decentralized, immutable ledger; used in finance, healthcare, and more.

- React
  Frontend library for dynamic, secure UIs with smooth loading.

- Ganache
  Local Ethereum blockchain for fast contract testing.

- MongoDB
  Provides storage for any off-chain data, improving performance and scalability.
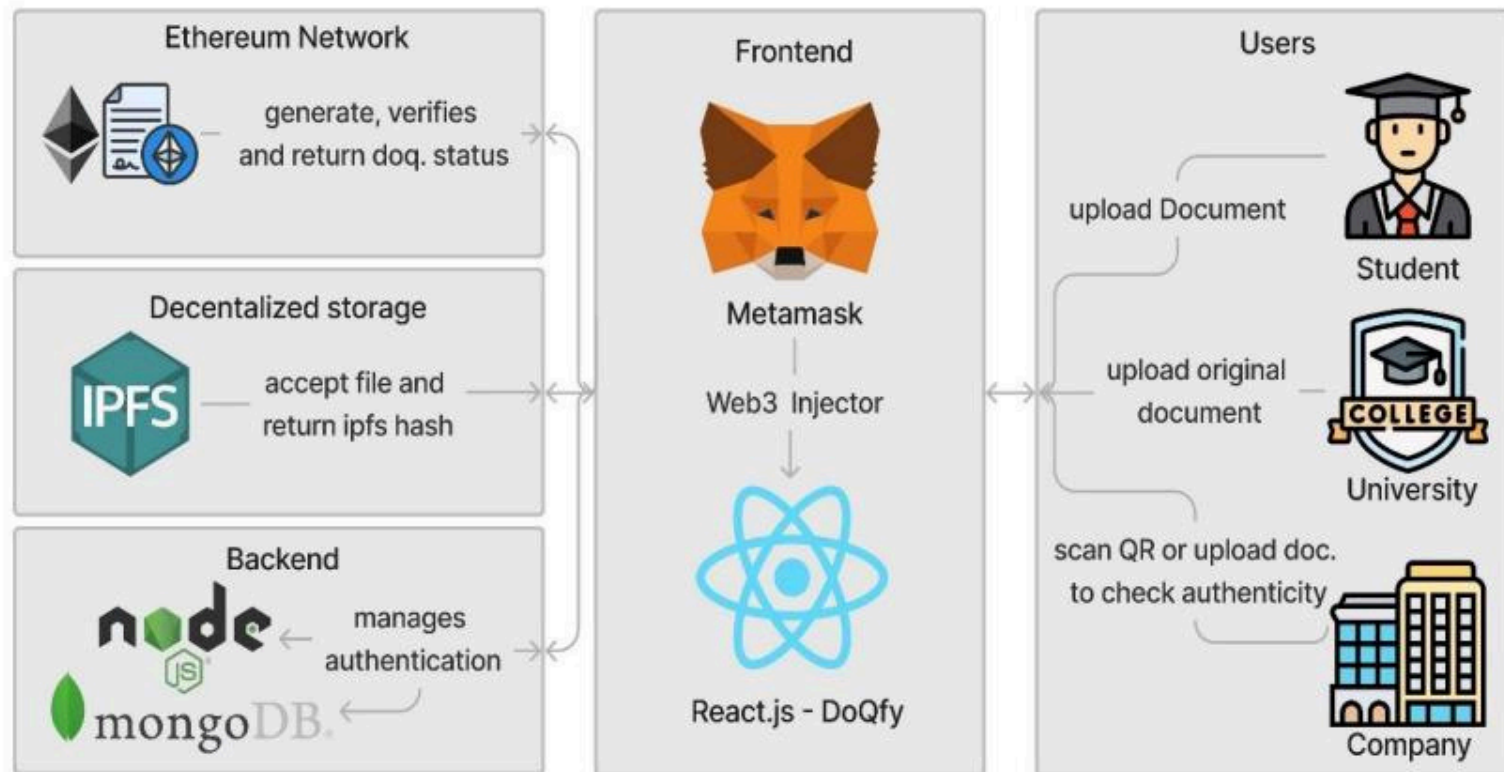
System Implementation

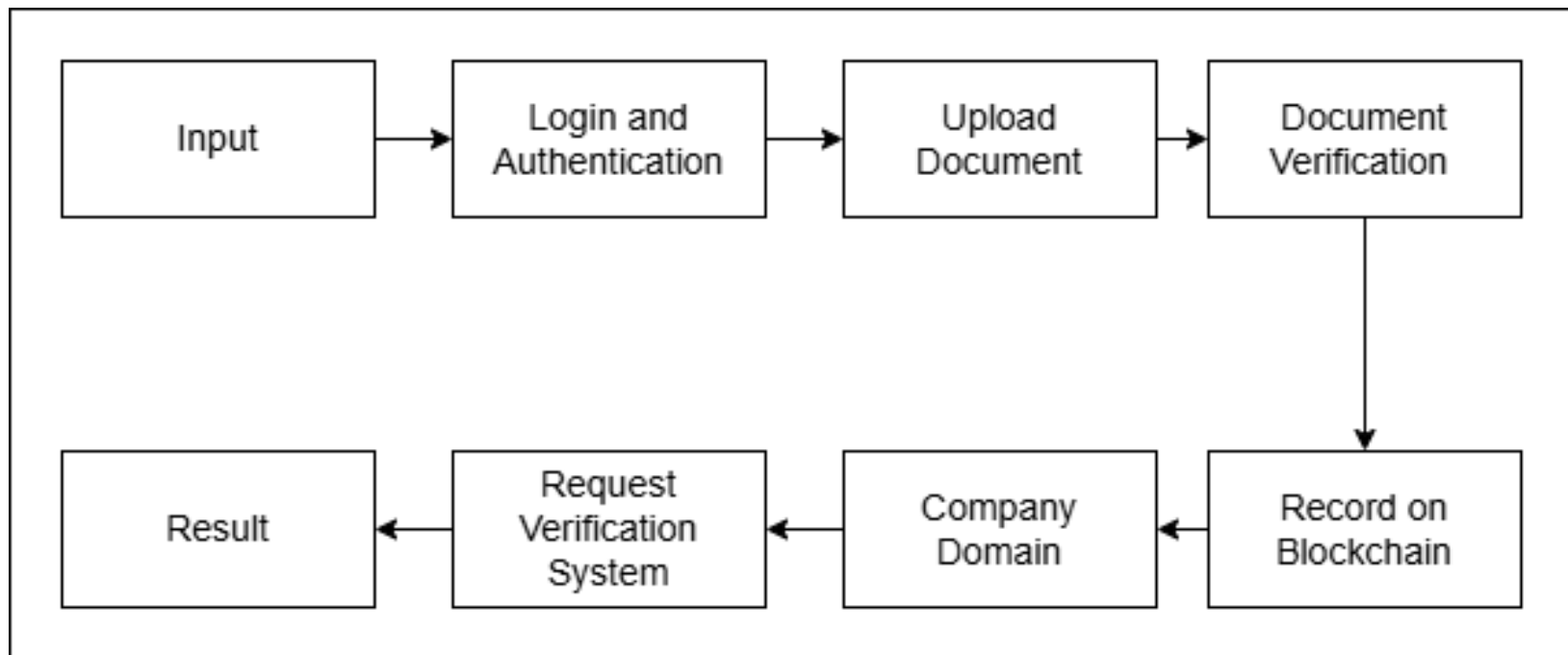## Flowchart
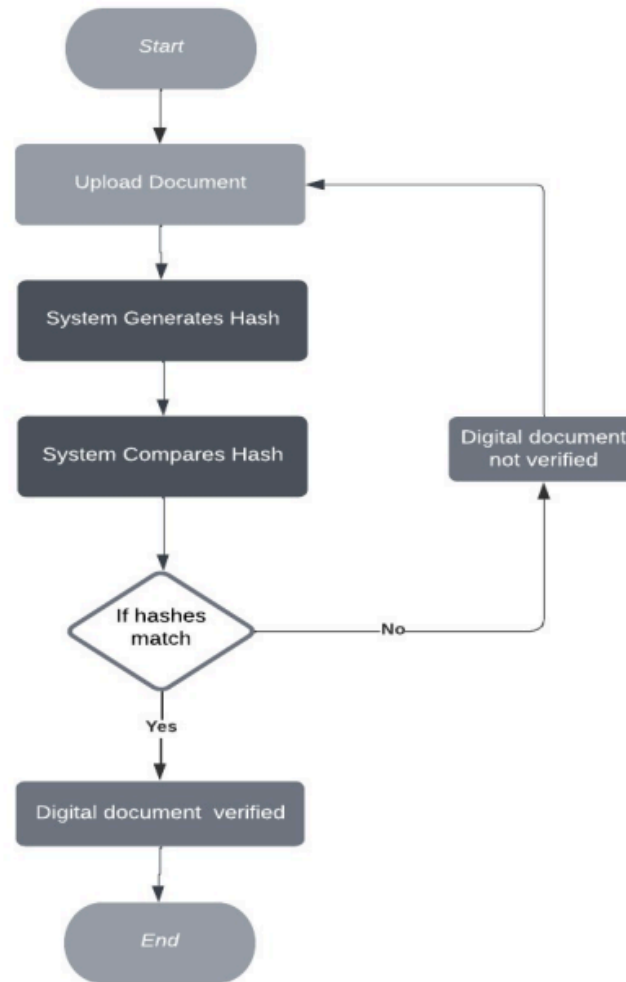
Flowchart

System Architecture

System Architecture
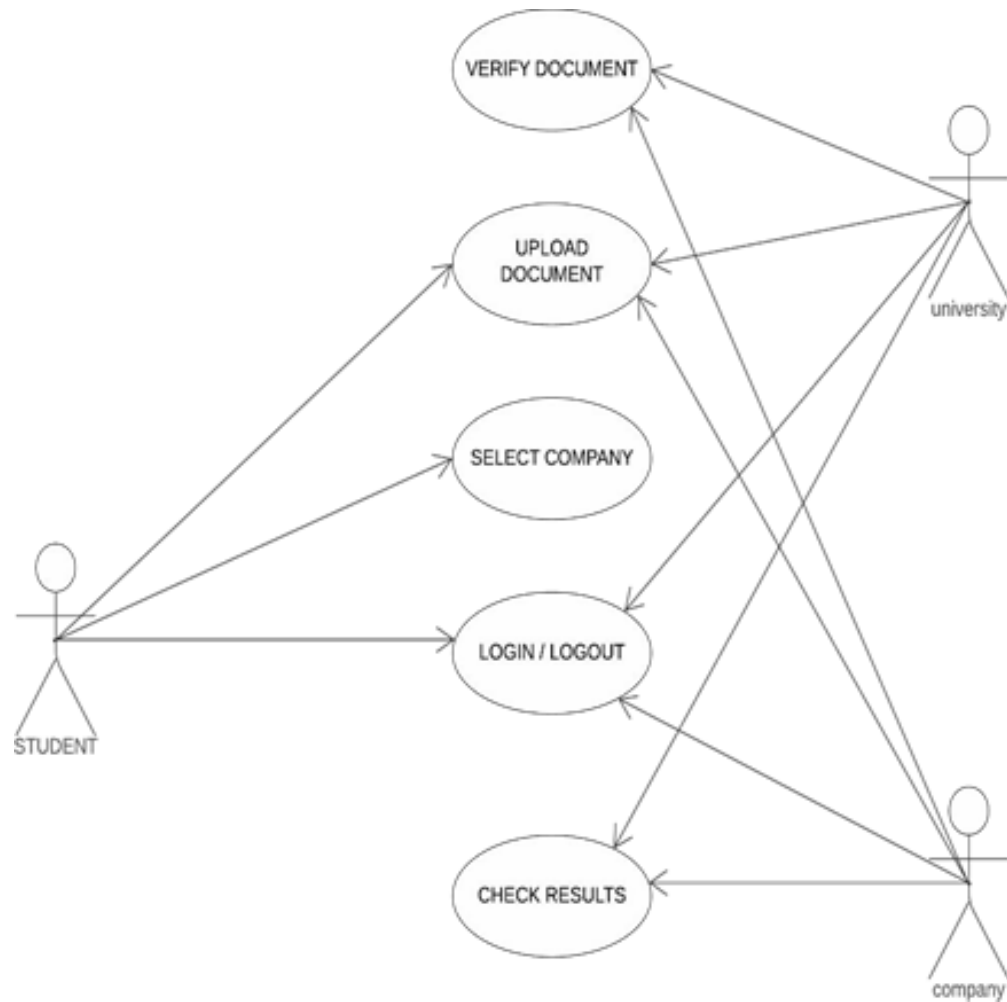
High Level design of the Project

Data Flow Diagram


```
┌─────────┐      ┌──────────────┐      ┌──────────┐      ┌──────────────┐
│  Input  │ ───> │  Login and   │ ───> │  Upload  │ ───> │  Document    │
│         │      │Authentication│      │ Document │      │ Verification │
└─────────┘      └──────────────┘      └──────────┘      └──────────────┘
                                                                 │
                                                                 v
┌─────────┐      ┌──────────────┐      ┌──────────┐      ┌──────────────┐
│ Result  │ <─── │   Request    │ <─── │ Company  │ <─── │  Record on   │
│         │      │ Verification │      │  Domain  │      │  Blockchain  │
│         │      │   System     │      │          │      │              │
└─────────┘      └──────────────┘      └──────────┘      └──────────────┘
```

Data Flow Diagram

Use Case Diagram

Use Case Diagram

Processing Stages:

Step 1: Start
The system initiates the document verification process.

Step 2: Upload Document
You upload "Contract_2023.pdf" for verification.

- **Example:** You drag and drop "Contract_2023.pdf" into the verification system.

Step 3: System Generates a Hash for the Uploaded Document
The system creates a hash (a unique digital code) for the uploaded document. This code is like a "fingerprint" that reflects the exact contents of the file.

- **Example:** The system calculates a hash value like "ABC123XYZ" for "Contract_2023.pdf."

Step 4: Retrieve the Original Hash

The system retrieves the original hash value that was previously saved for this document when it was first verified.

- **Example**: The original hash saved for "Contract_2023.pdf" is also

Step 5: Compare the Hashes

The system compares the hash of the uploaded document with the original stored hash.

- **Example**: The system checks if the newly generated hash "ABC123XYZ" matches the original stored hash "ABC123XYZ".

Step 6: Determine Verification Status
- **If the hashes match**: The document is verified as authentic (it hasn't been changed).

- **Example**: The hashes are the same ("ABC123XYZ" = "ABC123XYZ"), so "Contract_2023.pdf" is confirmed to be unchanged and is verified.

- **If the hashes do not match:** The document is flagged as "not verified" (indicating it has been altered).

- **Example**: If the new hash had been different, say "DEF456UVW", then the system would flag "Contract_2023.pdf" as "not verified."

Step 7: End the Process
The verification status is finalized, and the system concludes the process.

- **Example**: If verified, the document status is marked as "Verified." If altered, it's marked as "Not Verified."

Conclusion

- Prevents tampering and ensures document authenticity
- Speeds up verification, saving time and costs
- Builds transparency and confidence across industries
- Suitable for various sectors and document types
- Secure solution for digital document management

References

- Dimitrov, D. Blockchain-Based Solutions for Digital Copyright Management: A Systematic Review. Journal of Information Science Theory and Practice, 8(1), 28-49.

- Y. G. Sucahyo, Y. Ruldeviyani, A. Gandhi et al., "An empirical study on factors that influence the digital startup sustainability: The mixed methods approach in indonesia," in 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS). IEEE, pp. 119–124.

- Storonsky, S., & Simpson, I. Blockchain: Opportunities for Private Enterprises in Copyright Management. International Journal of Innovation Management, 22(1), 1850005.

- G. Dusil and D. Cerny, "The next evolution in funding innovation," in Inter- national Joint Conference on Neural Networks (IJCNN). IEEE, pp. 1–4.

- R. Ji, Y. Tian, and M. Ma, "Collaborative filtering recommendation algorithm based on user characteristics," in 2020 5th International Conference on Control, Robotics and Cybernetics (CRC), 2020, pp. 56–60.

Thank you