Blockchain-Based Secure File Verification and Sharing System

Group No 10

Contents

Introduction

Blockchain + IPFS helps us create a decentralized system where no single authority controls the files, ensuring trust and integrity.

01 Increasing need for secure file storage & sharing

02 Traditional cloud storage → centralized, risk of tampering

03 Blockchain + IPFS → decentralized, tamper-proof solution

04 Goal: File Integrity, Ownership, and Secure Sharing

OBJECTIVES

Objective 01

Ensure File Integrity

- Verify that uploaded files remain untampered using cryptographic hash values stored on blockchain.

Objective 02

Enable Secure File Sharing

- Provide controlled and permission-based file access using smart contracts.

Objective 03

Decentralize File Storage

- Use IPFS to store files across distributed nodes instead of centralized servers.

Objective 04

Enhance Data Ownership & Privacy

- Allow users to fully control their files and manage access without third-party dependence.

Objective 05

Maintain Transparent Access Logs

- Record immutable history of file uploads, access requests, and permissions on blockchain.

Objective 06

Support File Encryption

- Add AES encryption before upload so that even if IPFS link leaks, files remain confidential.

LITERATURE SURVEY

Year	Author(s)	Contribution	Limitations
2019	R. Kumar, M. Z. A. Bhuiyan, and A. Y. Zomaya	Proposed a **Blockchain–IPFS framework** for decentralized storage and access of digital content.	Encrypts only IPFS hashes → Actual files aren't encrypted, so content can still be exposed.
2020	Tian-Sheuan Chang, Hsiaoshan Huang	This paper proposes a secure file sharing system combining **blockchain, IPFS, and an IPFS proxy** to handle access control and group key management.	No individual Access Control

Research Gaps

- **Large Files Issues**

Blockchain networks have limited storage system when dealing with large.

- **Efficient File Versioning**

Limited work on handling multiple versions of files with blockchain audit trails.

- **Security Enhancements**

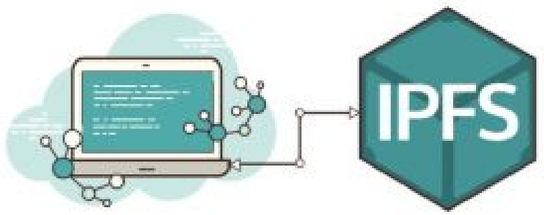
Few solutions implement AES or hybrid encryption before IPFS upload for stronger confidentiality.

- **Integration with Wallet-Based Authentication**

Research has focused on integrity, but secure user authentication (e.g., MetaMask/WalletConnect) is underexplored.

What Is IPFS?

InterPlanetary File System



Peer-to-Peer (P2P) distributed file system

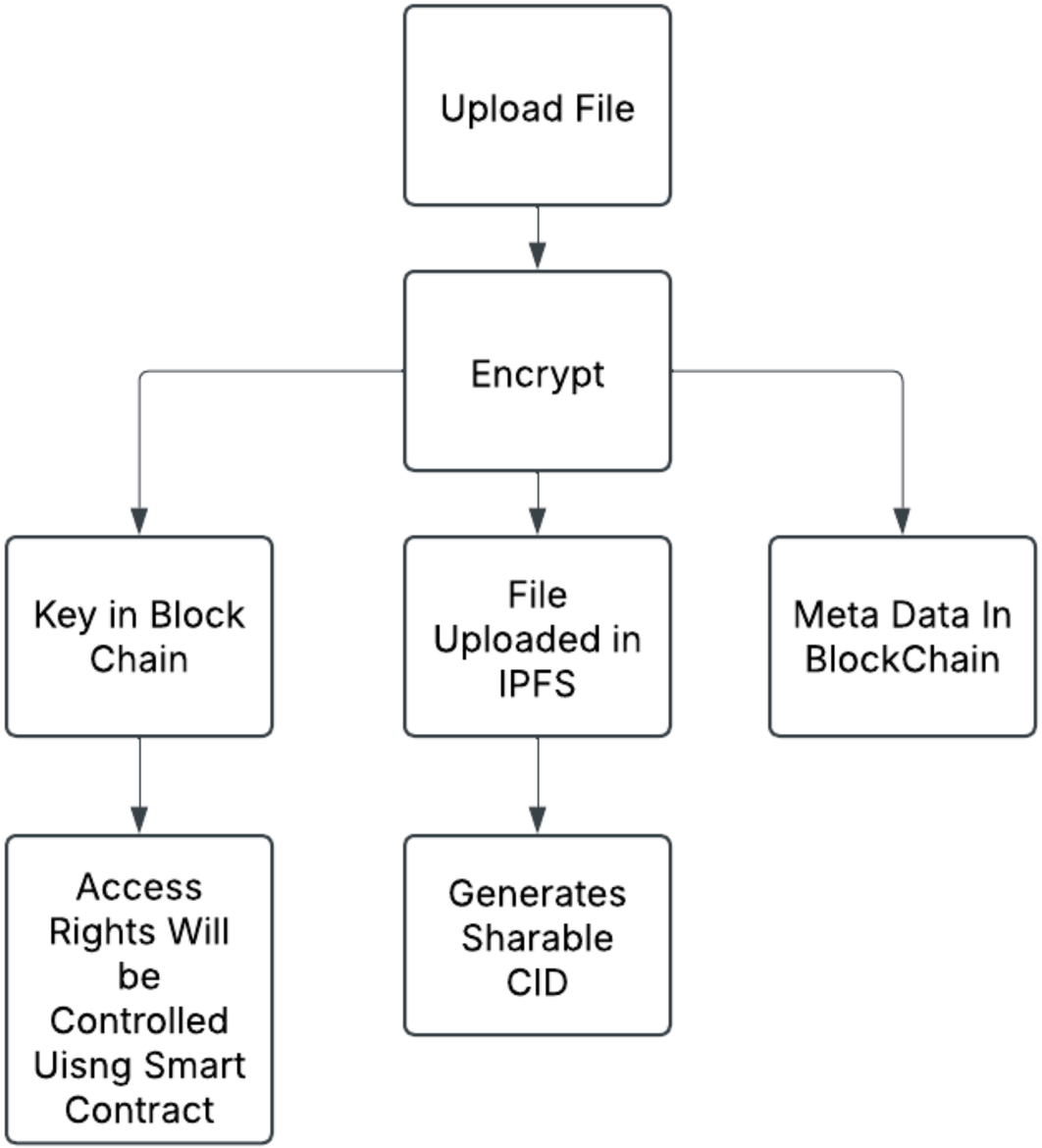
Uses content-based addressing (via unique hash called CID)

Decentralized – no central server, data fetched from nearest peers

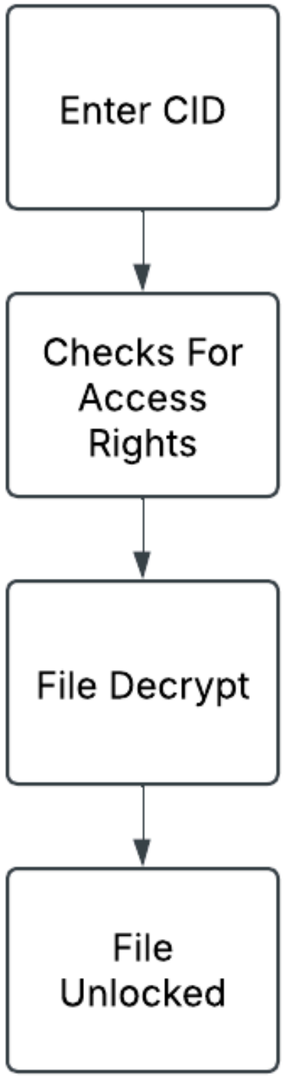
Tamper-proof – hash ensures data integrity

Faster & efficient – retrieves files from multiple sources

Sender’s Side



Receiver’s Side



TECH STACK

- Ethereum + Solidity → Smart Contracts
- IPFS (InterPlanetary File System) → Decentralized File Storage
- Web3.js + MetaMask → Blockchain interaction & authentication
- React.js / HTML & CSS → User Interface

Thank You!!!