Genba Sopanrao Moze College Of Engineering, Balewadi, Pune 411045

Academic Year 2024-2025

B.E. Sem II

Project Title:

SAFEGUARD:Blockchain Based File Storage System

Presentation On:

SAFEGUARD: Blockchain Based File Storage System

Presented By:
Rupika Patil
Esha Nalawade
Tejal Tayade

Guided By:
Dr. Vajid Khan

INDEX

- Introduction
- Literature Survey
- Problem Statement
- Objectives
- General Overview
- Proposed System
- Algorithm
- DFD
- Class Diagram
- System Requirements
- Result
- Applications
- Conclusion
- Future Scope
- References

INTRODUCTION

As data generation grows exponentially across industries, traditional centralized storage solutions face critical limitations, including security vulnerabilities, high operational costs, and lack of user control. These systems are prone to single points of failure, data breaches, and censorship, often controlled by a few major providers.

This project implements a decentralized file storage system using blockchain technology. Users can securely upload, store, and download files, with each file's metadata stored in immutable blockchain blocks.

The system leverages Proof of Work (PoW) to prevent unauthorized alterations or deletions of files. Additionally, the application ensures data integrity using SHA-256 encryption. By integrating blockchain with file storage, this project provides enhanced security and decentralization, enabling transparent file management within a peer-to-peer network. Various Proof of Work algorithms are tested to optimize the blockchain's difficulty level.

Literature Survey

Title	Year	Idea	techniques	Result	Limitation
A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain	2021	Blockchain technology and related core technologies	Explored the method of providing security.	Presented a way of securing blockchain use and removal protocol to explore the method of providing security	Considering the environment in which a vast volume of data is sent, efficiency studies were also required in addition to security studies.
Blockchain–Cloud Integration.	2022	Collect and verify cloud data provenance by embedding provenance data into blockchain transactions	Designed and built ProvChain, a system	ProvChain delivered security characteristics such as tamper-proof prove,user privacy, and dependability with little overhead for cloud storage applications.	Built ProvChain on top of an open-source architecture.
Blockchain-based Decentralized Storage Scheme.	2019	Decentralize safe storage of data.	Encrypted data using the AES 256-bit encryption method.	Platform for users rent out their unused storage and earn cryptocurrency.	Flexible scheduling method, in which files can be viewed several times and a payment system

Title	Year	Idea	Techniques	Result	Limitations
storj:A decentralized cloud storage service	2015	Present Storj ,a decentralized cloud storage service that uses a network of nodes to store and manage data	Decentralized network,smart contracts cryptographic techniques	The paper discusses the architecture and features of the system,and examines its performance and scalability	The system has not yet been fully implemented or tested
Decentralized storage system	2020	provides an overview of decentralized storage systems,including their design,features,and performance	Literature review	Discusses the benefits and challenges of decentralization,and examines various use cases and application of decentralized storage	Does not provide a comprehensive analysis of all decentralized storage systems,and does not developed into technical details of specific system
Rent your disk:A decentralized cloud storage system	2018	Presents a decentralized cloud storage system called rent your disk,which allows users to rent out their excess storage capacity to others	Blockchain, distributed hash table	The system users a blockchain to track and verify transactions,and employs a distributed hash table to facilitate data storage and retrieval	The system has not yet been fully implemented and tested

Title	Year	Idea	Techniques	Result	Limitation
Decentralized cloud storage systems	2018	History, motivation and challenges of decentralized cloud storage systems, and compares and contrats different approaches to decentralization	Review	Various security and privacy concerns, and examines the potential future developments and trends in the field.	Provide a comprehensive analysis of all decentralized storage systems, and does not delve into technical details of specific systems.
Filecoin : A decentralized storage network	2017	Describes the design and implementation of Filecoin, a decentralized storage system that uses a token-based system to incentivize and reward nodes for providing storage.	Token-based system, consensus algorithm, network architecture	The paper discusses the technical details of the system, including its consensus algorithm and network architecture.	The system has not yet been fully implemented or tested.
On Blockchain-Enhanced secure data storage and sharing in vehicular Edge Computing networks	2021	vehicular edge computing networks (VECNets) have emerged to provide massive storage resources with powerful computing on network edges	blockchain; smart contracts; privacy and security	overcoming the increasing complexity of applications accompanied by difficulties in the provision of large volumes of data storage, trust management, and security	the proposed system is controlled by multiple authorized RSUs, which will execute a consensus mechanism to reach an agreement before storing the data to the blockchain network.
Secure data storage and recovery in industrial blockchain network environment	2020	a secure data storage and recovery scheme in the blockchain-based network is proposed by improving the decentration, tampering-proof, real-time monitoring, and management of storage systems.	Blockchain network, consensus mechanism, distributed storage.	focused on data security issues in the industrial network and designed a storage and repair scheme for fault-tolerant data coding.	Results show that the proposed method is suitable for the energy-limited network.

PROBLEM STATEMENT

"Centralized file storage is prone to data loss, tampering, and unauthorized access. This project aims to develop a blockchain-based file storage system that ensures secure, decentralized, and tamper-proof file management.”

OBJECTIVES

- To research about web technology and blockchain.
- To enable secure upload and download of files.
- To use Proof of Work (PoW) to validate and add blocks, ensuring tamper-resistance.
- To ensure data authenticity and permanence without centralized control.
- To provide a secure and efficient storage solution by leveraging blockchain technology.

GENERAL OVERVIEW

The **Blockchain-based File Storage** project is a decentralized web application developed to provide secure and tamper-proof file storage using blockchain technology. Traditional centralized storage systems are often vulnerable to data breaches, single points of failure, and unauthorized access. This project addresses those concerns by leveraging a peer-to-peer (P2P) network where files are distributed across multiple nodes, ensuring data redundancy and availability. Each file upload is recorded as a transaction on the blockchain, making the storage process transparent and immutable. .

ALGORITHM

Algorithm 1: PoW with Random Nonce

Step 1: Initialize the block's nonce with 0.

Step 2: Enter a loop:

Generate a random number as the new nonce.

Assign this nonce to the block.

Generate the hash of the block using [.generate _hash().]

Step 3: Check if hash is valid:

A hash is valid if it starts with n leading zeros (where n = difficulty level).

Step 4: If the hash is **not valid**, repeat from Step 2 with a new random nonce.

If a **valid hash is found**, the block is ready to be added to the blockchain.

Algorithm 2: PoW with Incremental Nonce

1. **Start nonce at 0**.

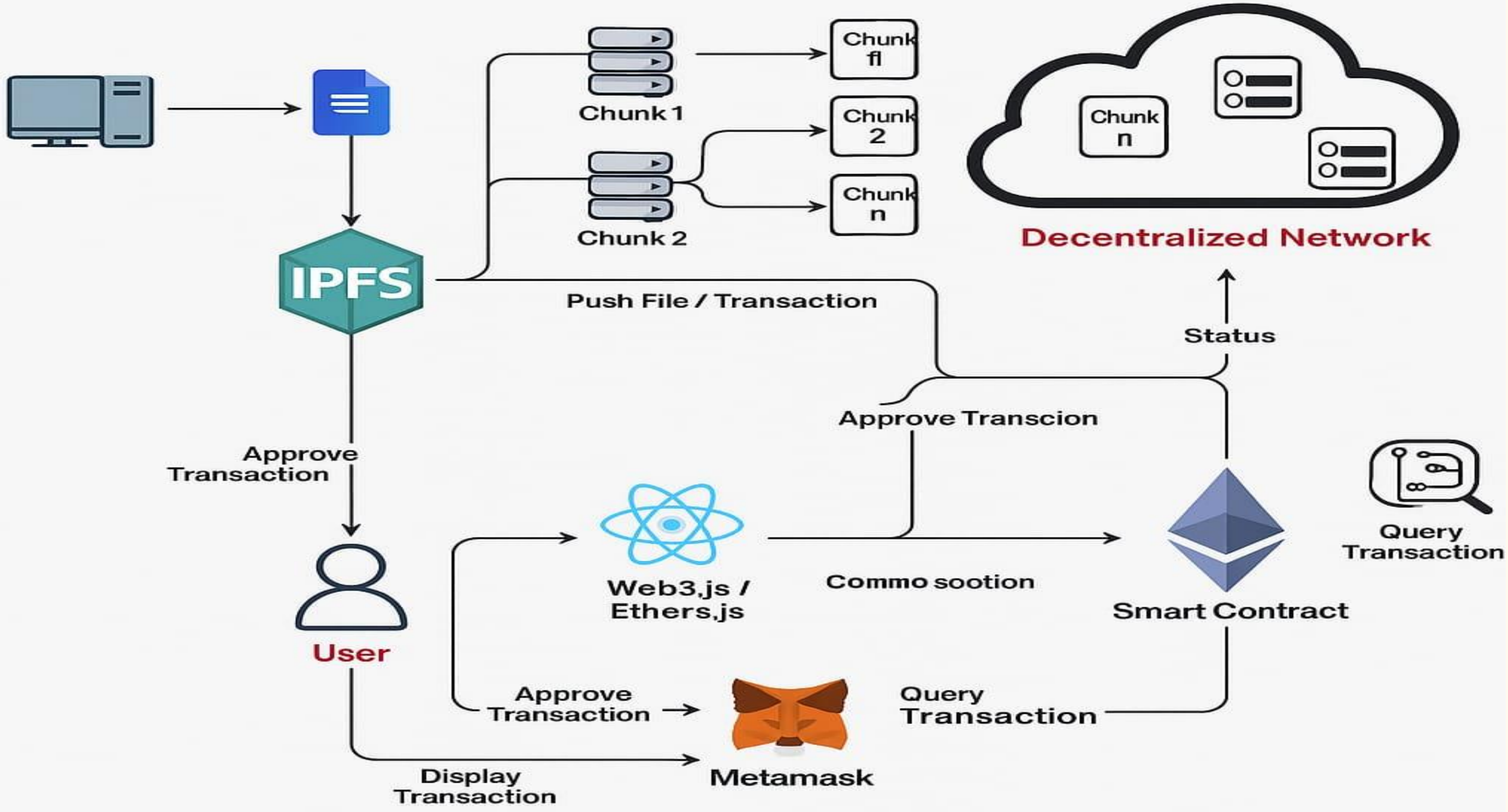
2. Enter a loop:
   - Assign current nonce to the block.
   - **Generate the hash** using .generate_hash().

3. **Check if the hash is valid** (starts with required number of zeros).

4. If not valid:
   - Increment nonce by 1.
   - Go back to Step 2.

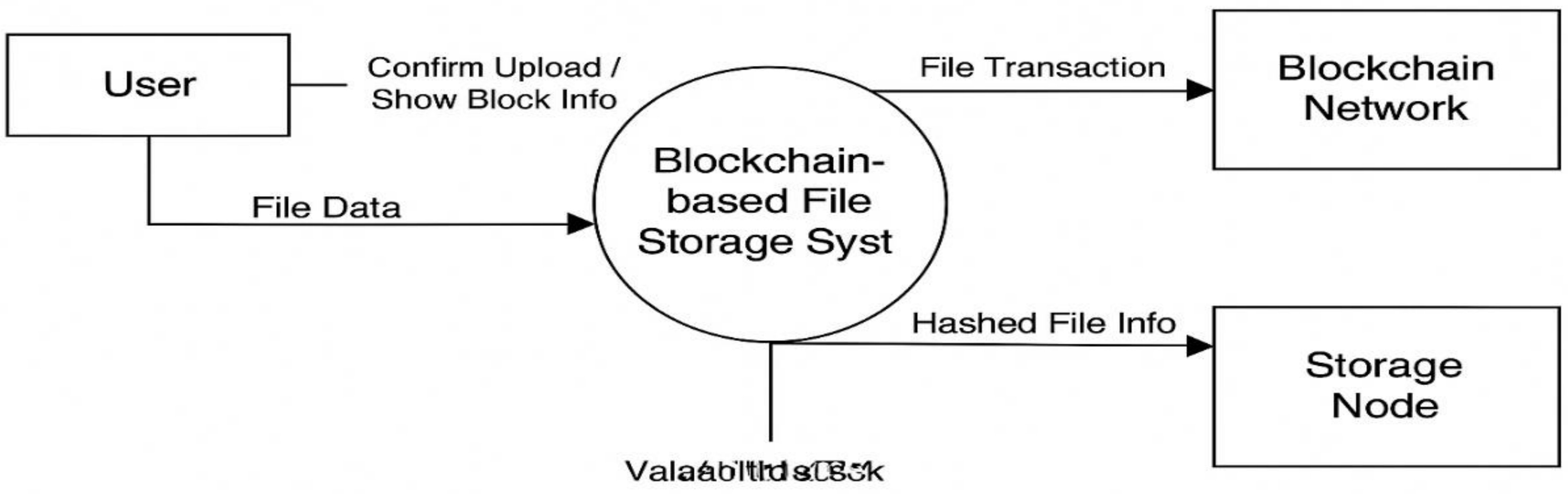
5. If valid:
   - The block is mined and ready to be added.

System Architecture



DFD Diagram

DFD Level 0



Level 0 DFD (Contd Dnm´)

Fig 2.0

DFD Diagram

DFD Level 1

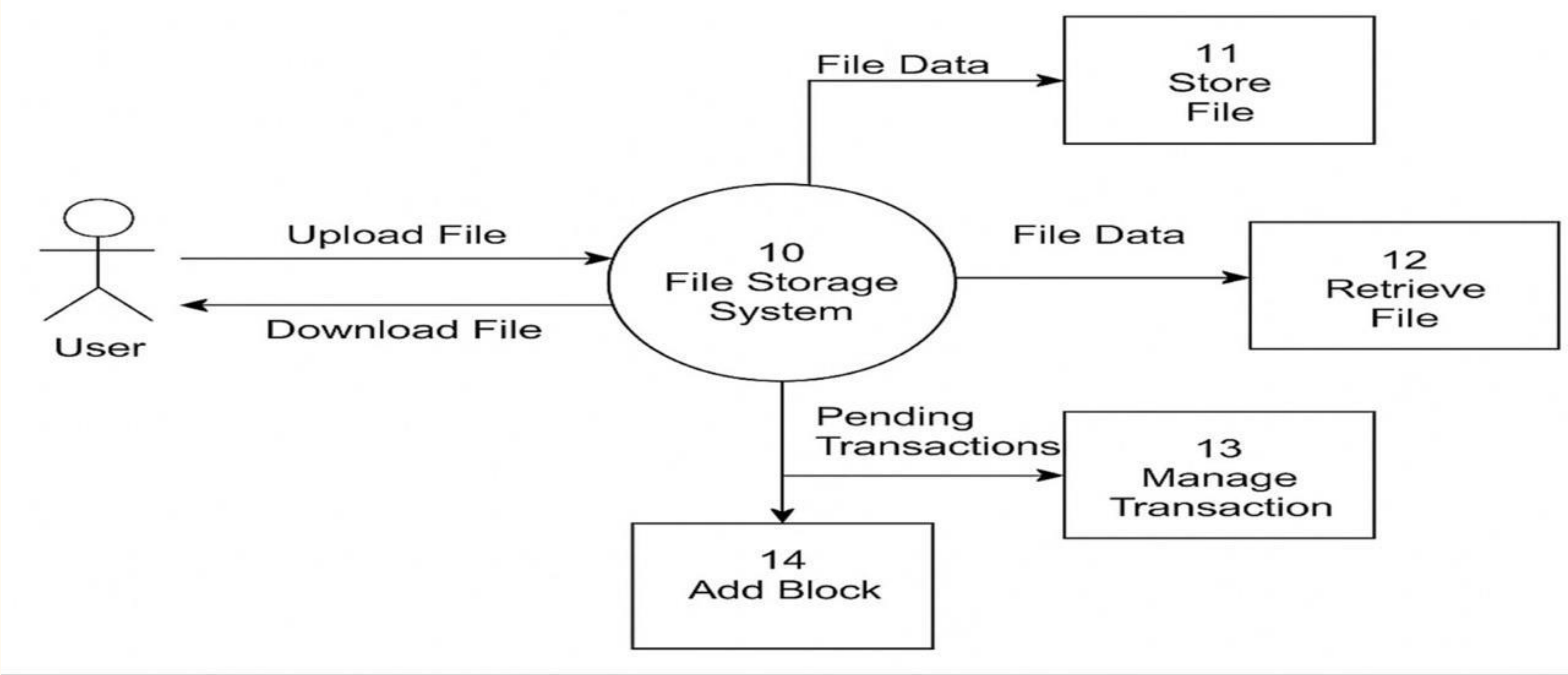
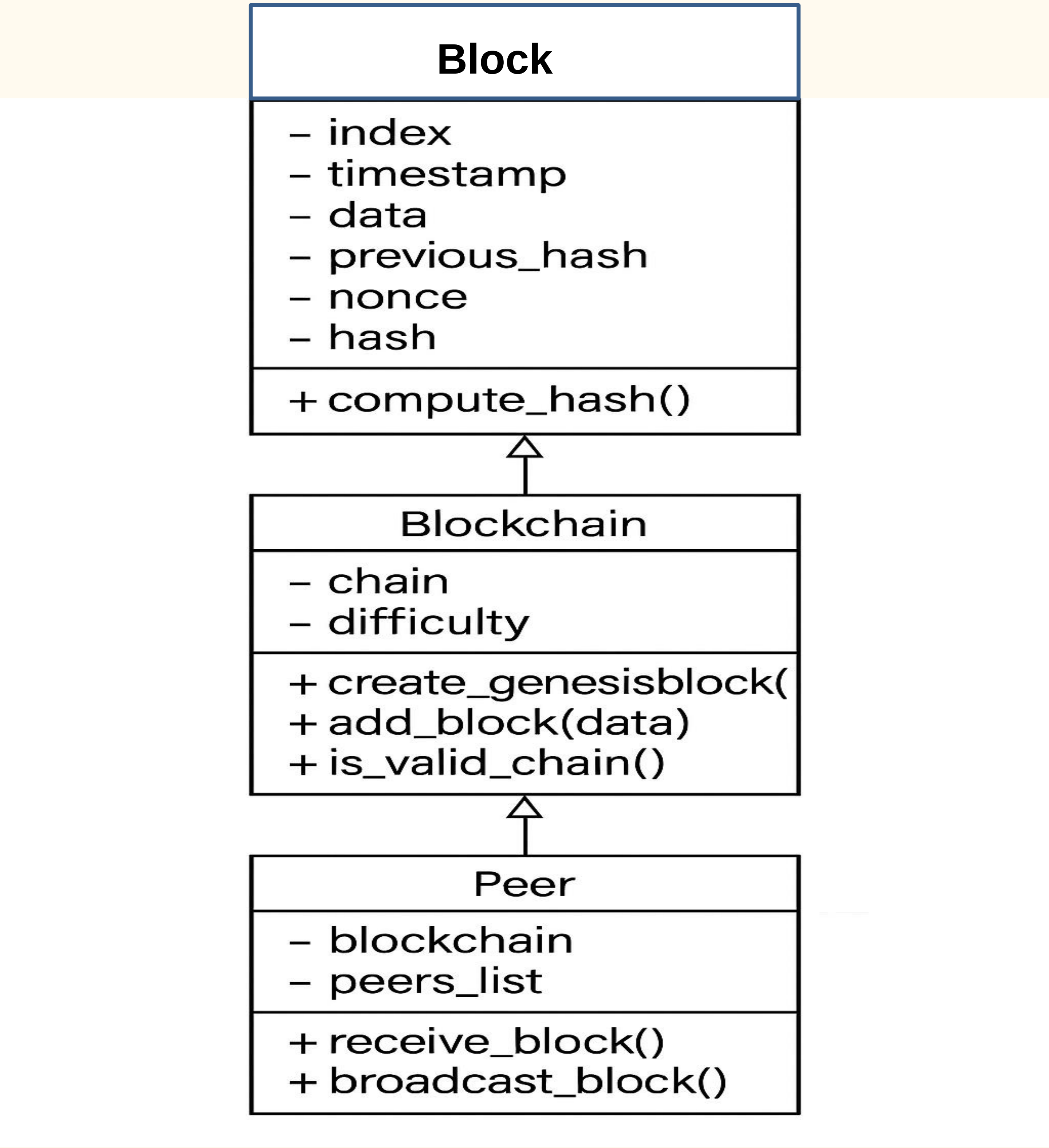


Fig 2.1

UML Class Diagram



Block

– index
– timestamp
– data
– previous_hash
– nonce
– hash

+ compute_hash()

Blockchain

– chain
– difficulty

+ create_genesisblock(
+ add_block(data)
+ is_valid_chain()

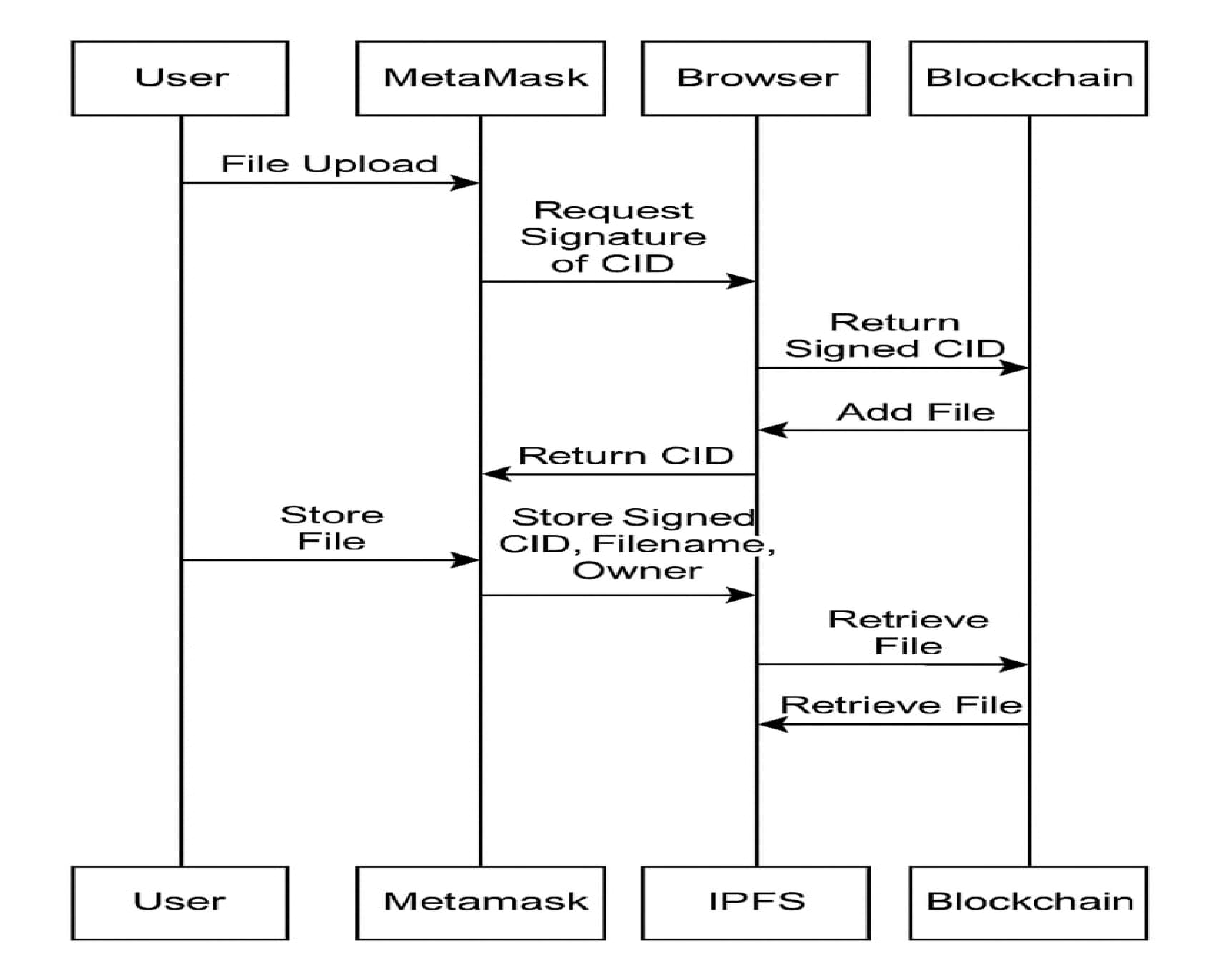
Peer

– blockchain
– peers_list

+ receive_block()
+ broadcast_block()

Fig 3.0

Sequence Diagram



System Requirements

Software Requirements:

Operating System: Windows 10/11, Linux, or macOS

Programming Language: Python 3.x

Framework: Flask(for backend server and API handling)

Web Technologies: HTML, CSS

Python Libraries: flask, requests, hashlib, json, threading, uuid

Web Browser: Google Chrome, Mozilla Firefox(for frontend access)

IDE/Code Editor: Visual Studio Code, PyCharm, or any preferred text editor

Git: For version control and project collaboration

HARDWARE REQUIREMENTS

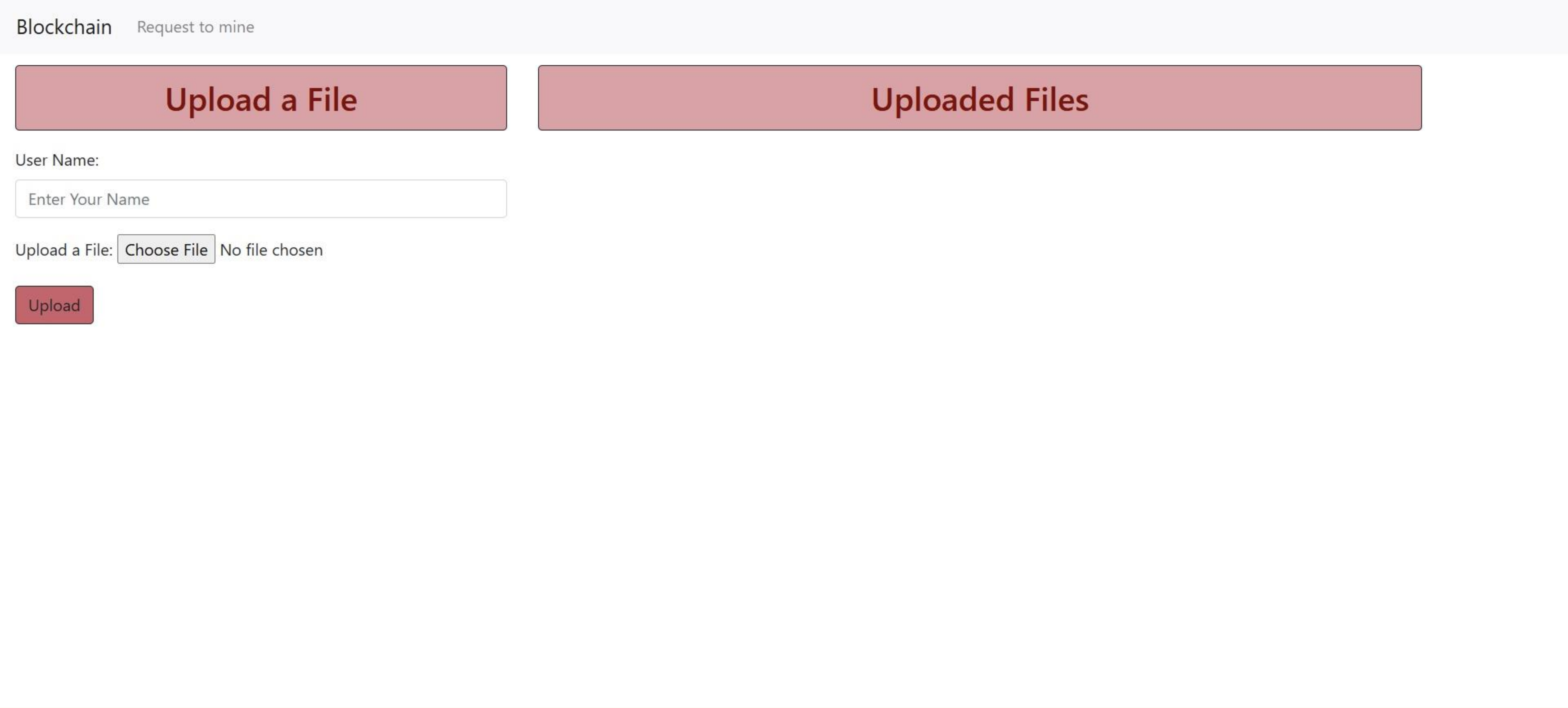
1.CPU
Dual-core processor (Intel i3 / Ryzen 3)

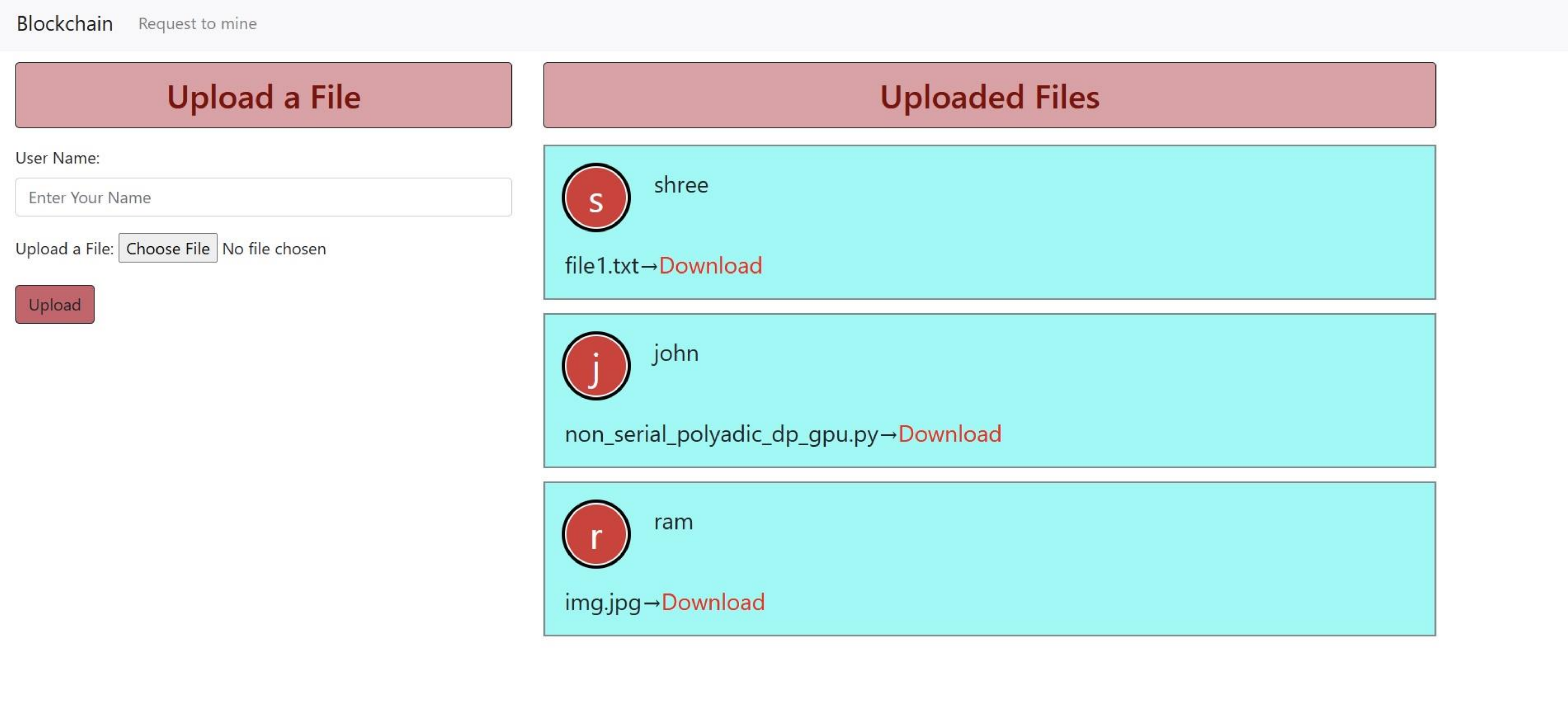
2.RAM
4 GB

3.Storage
10 GB free disk space

4.OS
Windows / Linux / macOS

RESULT:


Blockchain
Request to mine
Upload a File
Uploaded Files
User Name:
Enter Your Name
Upload a File:
Choose File
No file chosen
Upload



Upload a File

User Name:

Enter Your Name

Upload a File: No file chosen

Uploaded Files

shree

file1.txt→Download

john

non_serial_polyadic_dp_gpu.py→Download

ram

img.jpg→Download

APPLICATION

1.Education & Credential Verification

Universities or training centers can store degrees, certificates, or transcripts in IPFS and link them on-chain. Researchers can publish papers, datasets, or lab results on IPFS and store the hash on chain.

2.Legal and Government document storage

Government departments or legal firms can upload important documents (contracts, IDs, licenses) to a secure decentralized system. Smart contracts can be used to manage access rights and document status (e.g., valid, expired, revoked).

3.Medical Records Management

Hospitals and patients can store sensitive health records on IPFS with encrypted access, while blockchain ensures: Audit trails of data access.Ownership and privacy preserved via smart contracts.

ADVANTAGES

1. Data Integrity and Immutability

Blockchain technology guarantees immutability. When a file’s hash is stored on the blockchain, it cannot be altered. This ensures that the file has not been tampered with or corrupted, preserving its authenticity over time.

2.Enhanced Security

Blockchain uses cryptographic techniques to secure data. Each transaction or file record is linked using secure cryptographic hashes, making it extremely difficult for malicious actors to manipulate or forge records.

3. User Ownership and Control

Users can manage their own files without relying on a third party. Smart contracts can assign ownership and access rights, giving users full control over who can view or interact with their files.

4. Transparency and Auditability

Every file-related action (such as uploads) is recorded on a public or permissioned ledger. This allows for complete transparency and the ability to audit changes or activities associated with each file.

5.Data Integrity and Proof of Ownership

Each file is hashed and its hash is stored on the blockchain.

Any unauthorized change alters the hash, making tampering immediately detectable.

DISADVANTAGES

1. Limited Storage Capabilities

Blockchains are not suitable for storing large files directly due to size and cost constraints. Instead, only the hash or pointer to the file is stored on-chain, with the actual file stored off-chain (e.g., in IPFS). This adds complexity and requires managing multiple systems.

2. Legal and Compliance Challenges

Once data (or even just metadata) is written to the blockchain, it cannot be changed or deleted. This raises concerns for data protection laws like GDPR, which require the ability to delete personal data upon request.

4. Requires Technical Knowledge

Users need to understand how to use wallets (e.g., MetaMask), IPFS gateways, and blockchain networks.

Non-tech users may find it difficult to interact with the system without a friendly UI.

3. Scalability Issues

Public blockchains have limitations in terms of transaction throughput. If the system handles a large number of users or files, performance may degrade due to network congestion or long confirmation times.

CONCLUSION

The **Blockchain-based File Storage System** successfully demonstrates how decentralized technologies can be leveraged to overcome the limitations of traditional file storage architectures. The use of **Proof of Work (PoW)** consensus ensures that every block added to the chain is verified and computationally validated, thus maintaining the integrity of the system. Two distinct PoW strategies were implemented and compared, providing insights into their relative performance and resource usage under varying difficulty levels.

FUTURE SCOPE

1.In future work, we will apply several methods for training and testing model.

2.Our experimental results show the practicality of our scheme. To put it in a nutshell, we leave the following questions for future research:Further optimizing the security and privacy of the proposed scheme based on the above technologies, Adding more functions to better comply with GDPR requirements, Exploring how to improve the efficiency of generation and verification of zero- knowledge proof.

3. Folder Structure & File Organization

Implement a file explorer with folder creation, drag & drop, and search functionality.

Tagging or categorizing files for better UX.

REFERENCES

1) Yangheran Piao, Kai Ye, Xiaohui Cui designed "A Data Sharing Scheme for GDPR Compliance Based on Consortium Blockchain to achieve data security sharing", Future Internet 2021, 13, 217.

2) Abhirup Khanna, Anushree Sah, Vadim Bolshev, Alessandro Burgio, Vladimir Panchenko, Marek Jaisinski designing Blockchain–Cloud Integration: "A survey for blockchain–cloud services being offered by existing Cloud Service providers ",Sensors 2022, 22, 5238.

3) Yan Zhu , Chunli Lv , Zichuan Zeng, Jingfu Wang , Bei Pei designed "Blockchain-based Decentralized Storage Scheme for a decentralized storage system based on blockchain technology", J. Phys. Conf. Ser. 2019, 1237, 042008.

4) S. Leitner ,2015,Storj:"A decentralized cloud storage service for data integrity and security."

5) H. Hassanpour, 2020, "Decentralized storage system for data security."

6) Y. Zahang, 2018, "Rent your disk : A decentralized cloud storage system" to provide on-demand and pay-per-use storage model with low computing cost.

7) Kamble et al. designed "Decentralized cloud storage systems", 2018 using blockchain technology.

8) J. Benet, "Filecoin : A decentralized storage network", 2017.

9) Firdaus M, Kyung-Hyune Rhee, “Blockchain-Enhanced Secure data storage and sharing in vehicular edge computing networks”, Appl.Sci.2021,11,414.

10)Wei Liang, Yongkai Fan, “Secure data storage and recovery in industrial blockchain network environments”, 2021.

Thank you!