Jaypee Institute of Information Technology, Noida, Sector-62

MINOR PROJECT - 2
(15B29CI691)

PROJECT SYNOPSIS

CryptShare: A Decentralized Secure Document Sharing Platform

SUBMITTED BY:

Sambhav Goel 21104033, B15
Akshita Gupta 21104053, B15
Megha Chauhan 21104057, B15

INTRODUCTION

This project aims to develop a user friendly decentralized document sharing platform that prioritizes user control, security and transparency. Unlike the traditional solutions reliant on centralized servers our platform will leverage the power of blockchain technology to:

- **Eliminate the need for trusted intermediaries** - A trustless environment is established which means that the users **don't need to trust a central authority** to maintain the integrity and security of their documents; they would maintain complete control over their documents.
- **Enhance security** - The documents will be stored in a decentralized manner using IPFS, which will make them resistant to data breaches and unauthorized access. We will also have end-to-end encryption which further protects sensitive information.
- **Promote Transparency** - All the document interactions and access attempts will be immutably recorded on the blockchain, which will ensure a transparent and verifiable audit trail.

OBJECTIVE

CryptShare — a decentralized secure document sharing platform will offer the following key benefits:

- **Enhanced Security:** Eliminate the risk of data breaches and unauthorized access commonly associated with centralized storage solutions by leveraging the secure and decentralized nature of blockchain technology and IPFS.
- **Increased Transparency:** Provide an immutable record of document history and access attempts on the blockchain, fostering trust and accountability among users in the document sharing process.
- **User Control:** Empower users to maintain complete ownership and control over their documents. This includes the ability to decide who can access their documents and the level of access granted (e.g., view, edit, download).

- **Censorship Resistance:** Utilize a public blockchain to ensure the platform is resistant to censorship attempts. This allows users to access and share documents freely, even in restrictive environments.

The features provided by CryptShare would include:

- **User-friendly Interface:** The platform will provide a user-friendly interface for uploading, managing, and sharing documents. Users can easily set access permissions, define expiration dates, and collaborate with others in real-time.
- **Granular Access Control:** Smart contracts will enable fine-grained access control, allowing users to specify who can view, edit, or download documents. Permissions can be further customized based on specific user roles or groups.
- **Audit Trail and Transparency:** All document interactions, including uploads, edits, and access attempts, will be recorded on the blockchain. This provides a tamper-proof audit trail for enhanced transparency and accountability.
- **End-to-End Encryption:** Documents can be encrypted at rest (on IPFS) and in transit (during sharing), ensuring data privacy and confidentiality. Users retain the sole control over decryption keys, further enhancing security.

TECHNICAL COMPONENTS

The project will be making use of the following technology to create a secure and decentralized document sharing platform:

- **Blockchain:** The platform will utilize a public blockchain, such as Ethereum, to store document metadata and access control information. This ensures transparency, immutability, and distributed trust in the system.
- **Smart Contracts:** These self-executing contracts will govern the access permissions and document sharing process. They will define the conditions under which users can view, edit, or share documents, eliminating the need for manual authorization.

- **Cryptographic Hashing:** Documents will be encrypted using robust hashing algorithms. This ensures that any modification to the document content will result in a completely different hash value, allowing for easy detection of tampering.
- **InterPlanetary File System (IPFS):** This decentralized storage network will be used to store the actual document content. IPFS offers fault tolerance, efficient data retrieval, and content addressing, ensuring document accessibility and integrity.

TECHNOLOGY STACK TO BE USED

1. Backend
    a. Programming Language: **Go**
    b. Blockchain Platform: **Ethereum**
    c. Smart Contract Framework: **Solidity**
    d. IPFS-Library: **go-ipfs**

2. Frontend
    a. JavaScript Framework: **React**
    b. IPFS-Library: **ipfs-http-client**

CONCLUSION

A decentralized secure document sharing platform offers a promising solution for individuals and organizations seeking a secure and transparent way to share sensitive information. While challenges exist around scalability and user adoption, the potential benefits of enhanced security, user control, and censorship resistance make it an attractive area for further exploration and development.