DECENTRALIZED DRIVE

UNIVERSITY OF ENGINEERING
&
MANAGEMENT, JAIPUR

DECENTRALIZED DRIVE

Submitted in the partial fulfillment of the degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE &ENGINEERING

Under

UNIVERSITY OF ENGINEERING & MANAGEMENT, JAIPUR

BY

DEVRADITYA SINGH CHOUHAN

University Roll no: 12021002026040

JAYESH NARAYAN SARKAR

University Roll no: 12021002001045

UNDER THE GUIDANCE OF

PROF. DIPTA MUKHERJEE

COMPUTER SCIENCE & ENGINEERING

UNIVERSITY OF ENGINEERING & MANAGEMENT, JAIPUR

Approval Certificate

This is to certify that the project report entitled "**UNI-CLEANER**" submitted by **Jayesh Narayan Sarkar and Devraditya Singh Chouhan and** in partial fulfillment of the requirements of the degree of **Bachelor of Technology** in **Computer Science &Engineering** from University **of Engineering and Management, Jaipur** was carried out in a systematic and procedural manner to the best of our knowledge. It is a bona fide work of the candidate and was carried out under our supervision and guidance during the academic session of 2023-2024.

_____

Prof. Dipta Mukherjee
Project Guide, Assistant Professor (CSE)
UEM, JAIPUR

_____ _____

Prof. (Dr.) Mrinal Kanti Sarkar
HoD, Dept. of CSE, UEM Jaipur

Prof. (Dr.) A Mukherjee
Dean Academics, UEM, JAIPUR

ACKNOWLEDGEMENT

The endless thanks goes to Lord Almighty for all the blessings he has showeredonto me, which has enabled me to write this last note in my research work.During the period of my research, as in the rest of my life, I have been blessedby Almighty with some extraordinary people who have spun a web of supportaround me. Words can never be enough in expressing how grateful I am to thoseincredible people in my life who made this thesis possible. I would like an attemptto thank them for making my time during my research in the Institute aperiod I will treasure.I am deeply indebted to my research supervisor, Professor Guide Name me such an interesting thesis topic. Each meeting with him addedinvaluable aspects to the implementation and broadened my perspective. He hasguided me with his invaluable suggestions, lightened up the way in my darkesttimes and encouraged me a lot in the academic life.

Devraditya Singh Chouhan

Jayesh Narayan Sarkar

ABSTRACT

A novel approach to safe and private data storage is provided by a decentralized photo storage drive. It disperses data throughout a network of nodes using blockchain technology, doing away with the requirement for a central authority. This guarantees the highest level of protection against illegal access and data breaches. Users still have complete control over their images, and encryption adds another degree of security. It lessens reliance on single-point failures and improves scalability and reliability by decentralizing storage. Additionally, it enhances privacy by eliminating middlemen and guaranteeing that stored photos are only accessible by authorized users. Adopting decentralization promotes a more transparent and democratic approach to data management, enabling people to properly protect their digital assets.

Table of Contents

List of Figures

1. CHAPTER

INTRODUCTION

Introducing a storage drive with a decentralized file system (DFS) could redefine data storage and management. Unlike traditional centralized systems, a DFS disperses data across numerous network nodes, eliminating reliance on a single point of control. This innovative approach ensures robustness and fault tolerance, as data redundancy is built into the system.

The decentralized storage drive offers users unparalleled control and security over their digital assets. Files are not stored in a central server; instead, they're distributed across the network, often using peer-to-peer (P2P) networking protocols. This means that users can access their files from anywhere, without worrying about server downtimes or data breaches.

One of the key advantages is autonomy: each node operates independently, making its own decisions regarding data storage and retrieval. This decentralization also enhances privacy and security, as there's no single point of vulnerability for potential attacks.

This storage solution caters to a wide range of use cases, from collaborative work environments to scenarios where internet connectivity is limited. It seamlessly integrates with existing systems and devices, ensuring a smooth transition for users.

By introducing a storage drive with a decentralized file system, you're not just offering a product; you're ushering in a new era of data sovereignty, where users have greater control and ownership over their digital footprint.

1.1 DECENTRALIZED FILE SYSTEM (DFS)

One essential cybersecurity technology is antivirus software, which guards computers and networks against malware, or harmful software. These tools identify, stop, and get rid of a variety of threats, including ransomware, spyware, trojan horses, worms, and viruses. To find and eliminate possible threats, antivirus programs use a mix of behavior monitoring, heuristic analysis, and signature-based detection. Updating antivirus databases on a regular basis is crucial to keeping them effective against newly emerging viruses. To improve total digital security and protect users from online threats, many antivirus programs come with capabilities like email filtering, firewall protection, and secure surfing in addition to real-time scanning.

1.2 PREREQUISITES

1.2.1 React.js

React.js is a well-liked JavaScript package that is great for creating UIs because of its virtual DOM and component-based design. By dissecting interactive user interfaces into reusable components, it makes the process of building them simpler. React is perfect for creating dynamic web applications that update seamlessly because of its effective rendering and state management.

1.2.2 Ether.js

A robust JavaScript library called Ether.js is intended for the development of decentralised apps, or DApps, on the Ethereum network. It offers programmers a set of tools and features to easily manage accounts, communicate with Ethereum smart contracts, and complete transactions. Ether.js makes the development process for Ethereum-based projects easier with its extensive documentation and vibrant community assistance.

1.2.3 Hardhat

A well-liked Ethereum smart contract development environment is called Hardhat. It provides a set of tools for contract compilation, deployment, testing, and debugging. Hardhat's comprehensive plugin architecture and built-in support for TypeScript make it a trustworthy and quick development tool for blockchain engineers.

1.2.4 Solidity

The programming language Solidity, which is statically typed, is used to create smart contracts on the Ethereum network. Because of its syntax, which is comparable to JavaScript, developers may easily use it. Solidity ensures dependability and trust in decentralised systems by facilitating the secure and effective construction of contracts. It promotes blockchain technology innovation by enabling complicated contract structures using features like inheritance and libraries.

1.3 SECURITY AND PRIVACY

A decentralised method for storing photos provides strong privacy and security characteristics. To maintain privacy, photos are protected and only authorised users with encryption keys can view them. To improve privacy, access control systems limit viewing permissions to accounts that have been granted permissions. The system's decentralised architecture offers resilience against data breaches by lowering the possibility of unauthorised access and single points of failure. Furthermore, user control over their data minimises exposure to widespread surveillance and protects their right to privacy. In general, user control, security, and encryption are given top priority in decentralised picture storing systems to protect private images and sensitive data.

1.3 IPFS

The InterPlanetary File System, or IPFS, is a decentralised protocol that was created to provide a permanent, decentralised way for people to share and store files online. A unique cryptographic hash is assigned to every file in IPFS, which is a content-addressed system as opposed to conventional HTTP-based networks. Files may now be distributed effectively and securely since they are kept on a network of nodes rather than on centralised servers. IPFS has advantages such enhanced data integrity, resistance to censorship, and lower bandwidth use due to content caching. It can be used in many different domains, such as content distribution, distributed storage, and decentralised applications (dApps).

2. CHAPTER

FEATURES DFS PROVIDES

2.1 SECURITY

Security is ensured by access controls, encryption, and decentralised architecture in a decentralised photo storing system. Robust encryption techniques safeguard images, and access is limited via permissioned accounts and multi-factor authentication. By giving users control over their data and minimising the chance of data breaches, this decentralised method lowers the exposure to surveillance. Decentralised photo archiving solutions offer piece of mind by protecting priceless memories from any dangers with strong security safeguards.

2.2 COMPATIBILITY

2.2.1 CROSS PLATFORM

Accessibility is guaranteed across a variety of operating systems, including Windows, macOS, Linux, iOS, and Android, thanks to cross-platform support. Users get flexibility and convenience as they may easily retrieve their stored images from any device. This wide compatibility improves the user experience by enabling people to easily manage their photo collections on a variety of platforms and devices

2.2.2 WEB INTERFACE

There is no need to install any particular software because the online interface provides a user-friendly platform that can be accessed from any modern web browser. Convenience and accessibility are increased as users can upload, view, and manage their photo collections with ease. With this method, managing images is made easier and consumers may interact with their stored photos from any internet-connected device with ease.

2.3 LIMITLESS PHOTO UPLOADING

In a decentralized photo storing system, the photo uploading limit may be determined by transaction fees or gas fees associated with blockchain-based storage transactions. These fees are essential for processing and validating uploads on the decentralized network. Depending on network congestion and blockchain activity, users may encounter variable upload limits based on their willingness to pay higher transaction fees for expedited processing. This dynamic approach ensures fair resource allocation while accommodating fluctuations in network demand. Users can manage their upload limits by adjusting transaction fees according to their preferences and urgency, ensuring a balanced and efficient photo storage experience within the decentralized ecosystem.

3. CHAPTER

DIFFERENCE BETWEEN DFS DRIVE AND LOCAL STORAGE DRIVE

3.1 ARCHITECTURE

Decentralised Photo Storing System: A single point of control is removed in a decentralised photo storing system by distributing photos over a network of nodes. The numerous nodes storing photographs provide redundancy and fault tolerance, reducing the possibility of data loss or disturbance. The resilience, availability, and security of users' stored photos are improved by this distributed design.

Local Storage Device: Data is saved directly on a physical device, such as a hard disc or SSD, when it is connected to a user's device. Every photograph on the gadget is stored locally, and there is no data transfer. By doing this, consumers can be confident they always have instant access to their photographs and don't have to rely on other networks or services for storage or retrieval.

3.2 ACCESSIBILITY

A decentralised photo storage system offers unmatched flexibility and convenience since images may be accessed from any network-connected device. Users may see and manage their photo collections anytime, anywhere, without being limited to a particular device or location thanks to the seamless access to their photos from different internet-connected devices.

Since local storage devices are controlled directly on the device, users maintain total control over the photos they store on them. Usually, the user or a designated system administrator is in charge of access permissions, which permits customised security measures. This guarantees that users can safeguard, arrange, and manage their photo collections in accordance with their security needs and personal preferences.

3.3 FAULT TOULERENCE AND REDUNDANCY

In a decentralized photo storing system, data redundancy is inherent as photos are stored across numerous nodes. This distributed storage approach strengthens fault tolerance and resilience, ensuring that even if some nodes fail, photos remain accessible and intact. An offline antivirus platform operates independently of an internet connection, allowing it to scan and protect systems without relying on online databases or updates.

Local Storage Device: Depending on the user-implemented backup plans, there can be restricted redundancy and fault tolerance. If the local storage device malfunctions, there could be data loss or corruption.

3.4 NO DATA DELETION

Data cannot be removed in the conventional way in a decentralised file system (DFS) photo storage system since it is distributed. Complete removal of data becomes difficult once it has been uploaded to the DFS network and replicated across several nodes. Other nodes allow access to the data even in the event that a node is compromised or goes unavailable. The user or system administrator can, however, quickly erase data from a local storage device and remove it from the device's storage medium. When compared to locally stored data, which is more subject to change, this distinction emphasises the durability and stability of data kept in a decentralised system.

3.5 CENTRALIZATION VS DECENTRALIZATION

Hard disk drives (HDDs) and solid-state drives (SSDs) are examples of local storage drives. They are physical devices that are directly connected to one computer or network and are used to store data. These drives house data centrally, with access usually restricted to devices connected to the same local network. Users can access and manage their data locally, but for wider accessibility, remote access may need extra configurations such as network sharing protocols or cloud storage.

A portion of the data is stored on each node of a network of nodes in decentralized storage systems. As data isn't centralized in one place, this method improves redundancy and resilience. The system keeps working even in the event that some nodes fail. In order to guarantee data security and integrity, these systems frequently use replication and encryption techniques. In a decentralized system, accessing data usually entails communicating with the network as opposed to a single physical device.

3.6 SCALABILITY

Adding more drives or physically upgrading hardware is usually required to scale local storage, which can be a costly and complex process. It includes buying new drives, installing them, and setting up the system to detect and make use of the extra storage space. Furthermore, advanced knowledge may be needed to manage larger storage infrastructures in order to guarantee optimal performance, dependability, and compatibility with current hardware and software setups.

Scalability for decentralized storage systems is seamless because more nodes can be added to the network. Performance and storage capacity grow in tandem with network expansion. Since every additional node adds to the total storage pool, this scalability is possible without requiring a substantial overhaul of the infrastructure or hardware upgrades. Furthermore, dynamic allocation

algorithms are frequently used in decentralized systems to effectively use resources throughout the network and guarantee peak performance as the system grows.

3.7 SECURITY

User configurations, the strength of the device's security measures, and network security measures all play a major role in security and privacy for data stored on local drives. To protect sensitive data, users must use encryption, access controls, and frequent backups. To avoid unwanted access and data breaches, it's also essential to keep firewalls and antivirus software updated. Frequent security audits and patching assist in reducing vulnerabilities and guaranteeing the integrity of data on local storage devices.

Decentralized storage systems incorporate distributed access control and encryption to prioritize security and privacy. These steps strengthen security against unwanted access and guarantee the privacy of data. Distributing data among several nodes also makes the system more resilient to targeted attacks because a compromised node does not compromise the system as a whole. Because of the layers of redundancy added by this distributed architecture, it is more difficult for hostile actors to manipulate or compromise the integrity of the system.

4. CHAPTER

SMART CONTRACT

Dynamic access permissions and picture integration are now features of smart contracts. It is now possible for users to directly insert photos into agreements, which improves comprehension. With access rights, users can grant or remove access to individual accounts, allowing for controlled resource sharing. Most importantly, the contract ensures data integrity and confidentiality by preventing unauthorised access to user accounts. Uploaded photos can be safely seen by authorised individuals, encouraging transaction transparency. Conditional agreements are made possible by conditional access characteristics, which further improve flexibility. This development is a big step towards more adaptable and safe blockchain applications.

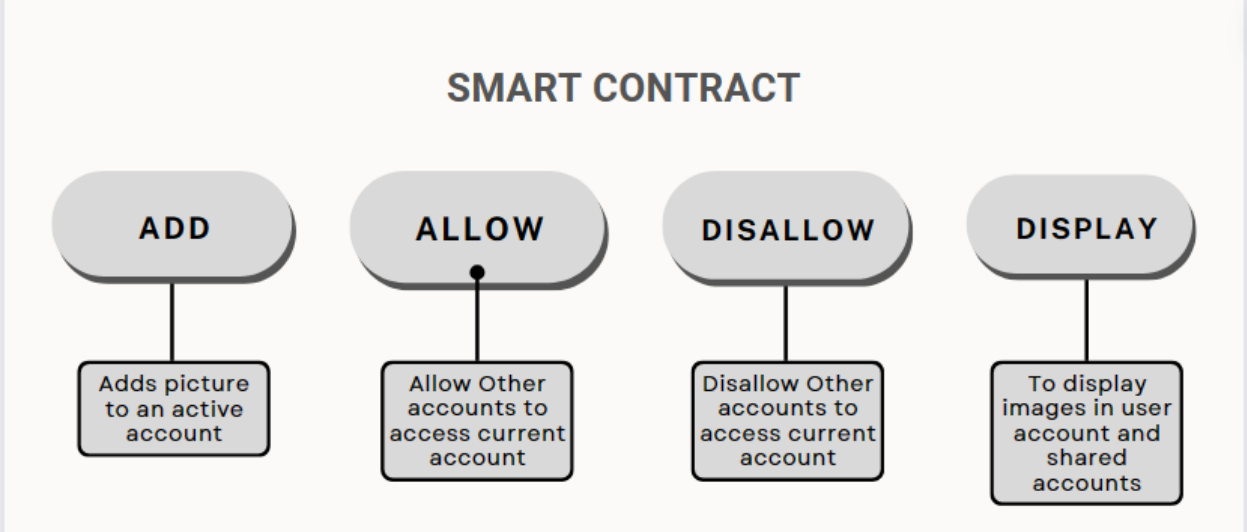

Fig 4.1: Smart contract

4.1 IMAGE INTEGRATION (Add)

Users can safely upload photos to their accounts with this smart contract. Data integrity is ensured by directly storing photos within the contract through cryptographic verification. Users can manage access rights to control who can see the photos they submit. User confidentiality is maintained by preventing unauthorised access attempts. This expedited procedure improves the user experience and makes transparent communication within the blockchain ecosystem possible.

4.2 ACCESS PERMISSION (Allow)

Within predetermined bounds, this smart contract makes authorised access to other users' accounts possible. Users can provide certain accounts with temporary access using cryptographic verification. Security and privacy are guaranteed by dynamically regulated access rights. The prevention of unauthorised attempts to access restricted accounts protects user privacy. This function encourages teamwork while preserving strong control over data accessibility across the blockchain network.

4.3 RESTRICTED ACCESS (Disallow)

Strict access controls are implemented by this smart contract, enabling users to limit and remove access to other user accounts. Users can set temporary permissions and establish access settings via cryptographic authentication. In order to protect user privacy and data integrity, unauthorised attempts to access restricted accounts are automatically denied. Users are always in complete control of their rights, and they can revoke access at any time. This guarantees strong security protocols and cultivates confidence within the blockchain network.

4.4 IMAGE DISPLAY (Display)

The safe display of photos from user profiles to other accounts with permission is made possible by this smart contract. The contract checks for permissions using cryptographic verification before displaying images. Transparency and cooperation are encouraged by the safe viewing of photos uploaded by the account holder by authorised users. Data confidentiality is maintained by blocking attempts at unauthorised access. This functionality facilitates easy access to visual content while upholding stringent security protocols, improving user experience and promoting trust within the blockchain network.

METHODOLOGY

A decentralized photo storing system operates by distributing photos across a network of nodes, eliminating reliance on a central server. Each photo is encrypted, assigned a unique cryptographic hash, and stored on multiple nodes for redundancy. Access to photos is controlled through permissioned accounts and encryption keys, ensuring security and privacy. Users can upload, view, and manage their photos from any device connected to the network. This distributed architecture enhances fault tolerance and resilience, as photos remain accessible even if some nodes fail. With no single point of control, users retain autonomy over their data, minimizing the risk of data breaches and preserving privacy rights.

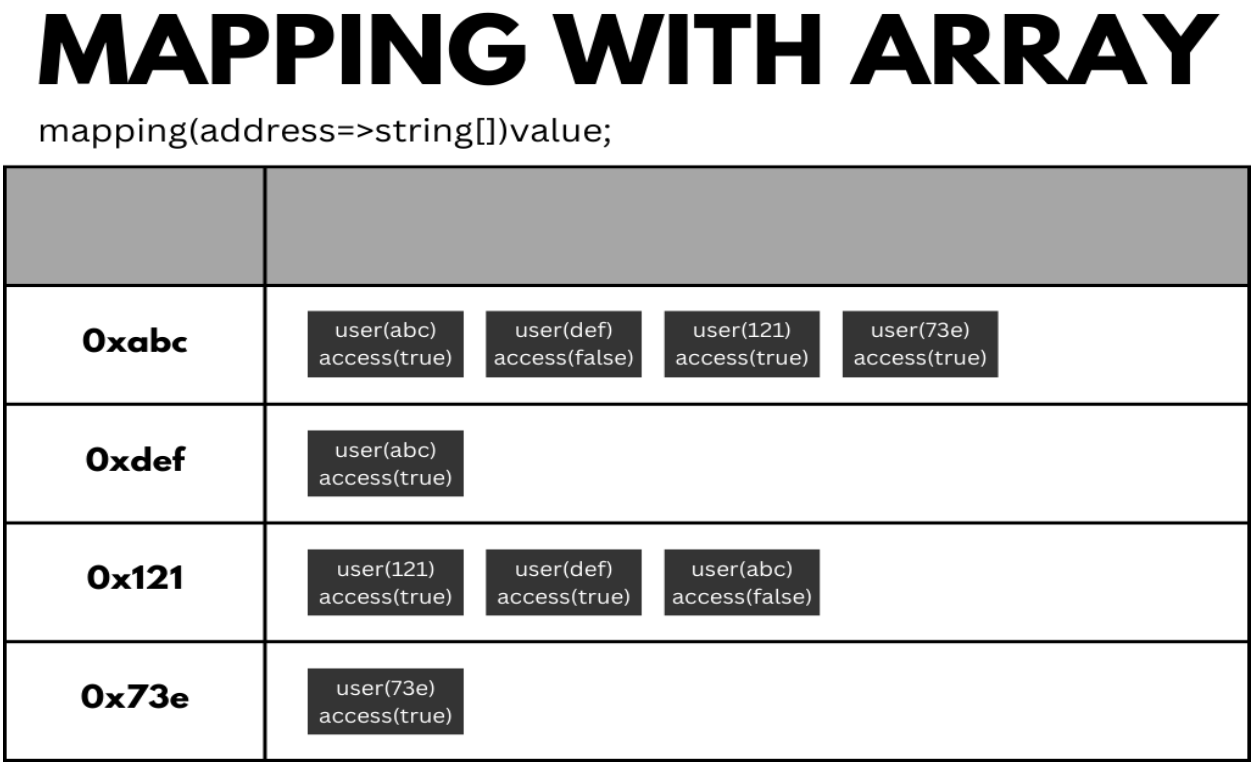

FIG 1.1: Mapping with Array

NESTED MAPPING

```
mapping(address=.mapping(address=>bool))ownership;
```

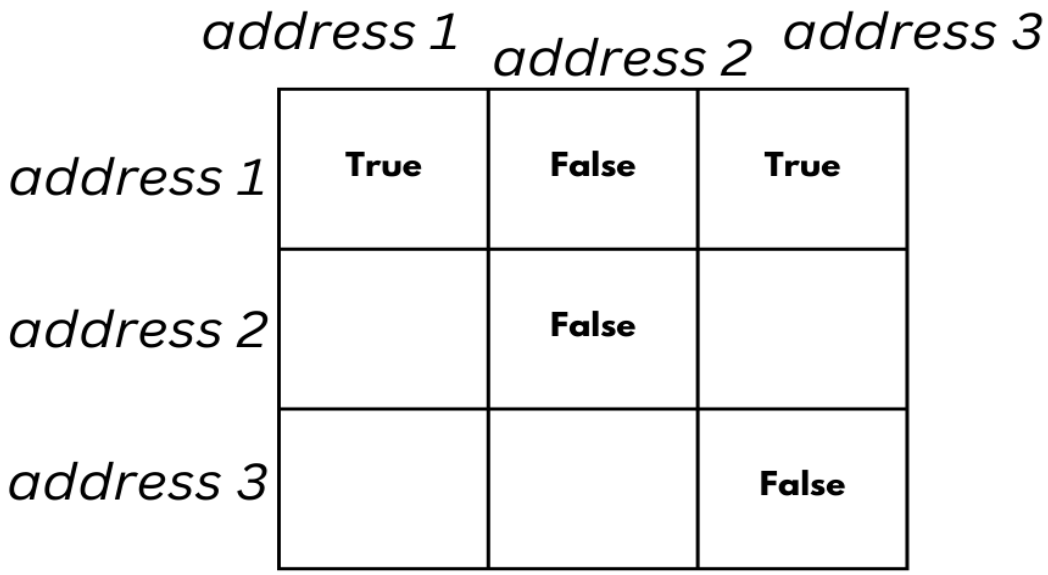

Fig 1.2: Nested Mapping

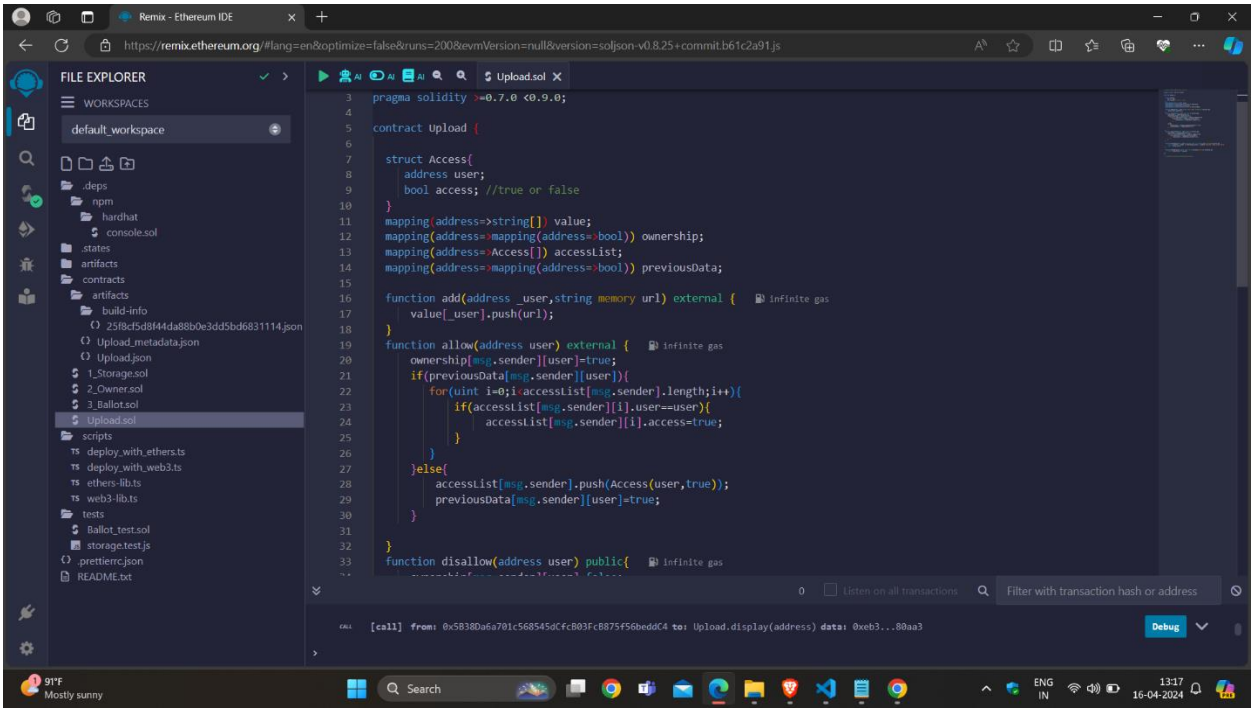

Fig 1.3: Solidity code to connect to Metamask part-1

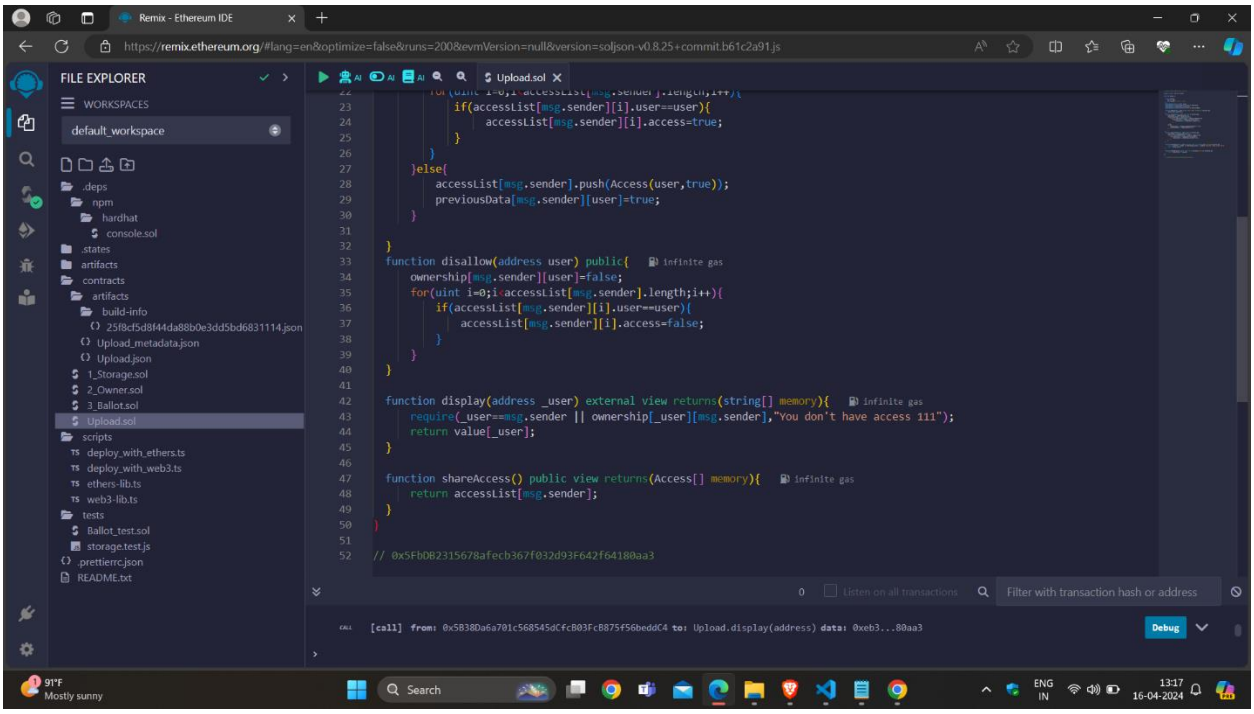

Fig 1.4:Solidity code to connect to Metamask part-2

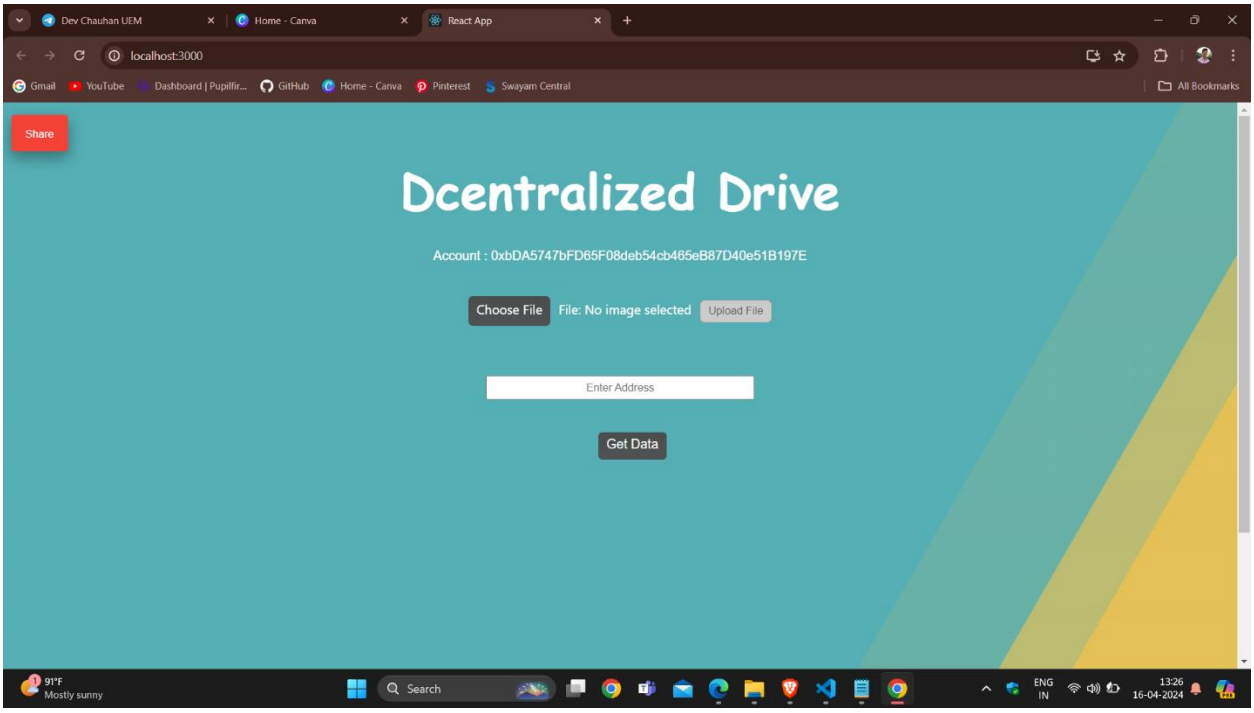

Fig 1.5: UI of DFS

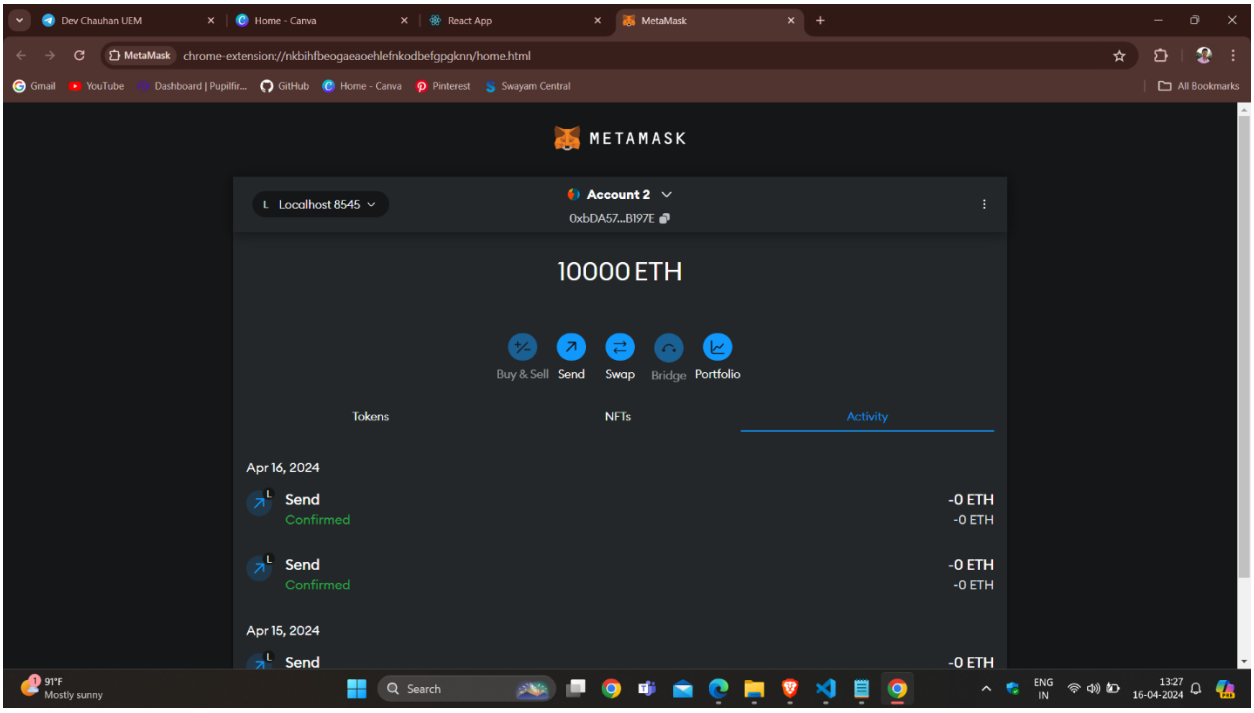

Fig 1.6: MetaMask

FUTURE SCOPE

Decentralised photo storing systems have a bright future ahead of them, with a number of possible innovations in the works:

1.Enhanced Security Measures: To further fortify the security and privacy of saved images, advanced encryption techniques, Password verification, decentralised identity management systems, and blockchain technology are integrated.

2. AI and Machine Learning Integration: Using AI and machine learning techniques to improve photo organisation and search capabilities through advanced photo analysis, content identification, and personalised recommendation systems.

3. Enhanced User Experience: To improve convenience and user experience, user-friendly interfaces, AI-driven photo organisation tools, and seamless cross-platform accessibility are being developed.

4. Decentralised Marketplaces: By utilising blockchain-based smart contracts to create decentralised marketplaces where users may purchase, sell, or licence digital photographs, new opportunities for content providers and photographers are created.

CONCLUSION

To sum up, a decentralised image storage system is a revolutionary method to data management that has many benefits over conventional centralised alternatives. Decentralised image storage systems provide improved security, fault tolerance, and data redundancy by utilising peer-to-peer protocols and distributed networks. In addition to reducing the possibility of single points of failure, this architecture gives users more control over their photographs, including privacy and access control.

Decentralised image storing systems also have a bright future ahead of them thanks to continuous improvements in blockchain integration, interoperability standards, and incentive structures that spur creativity. Decentralised solutions provide a strong substitute that complies with changing user expectations and legal requirements as regulatory compliance tightens and knowledge of data privacy issues rises.

Decentralised picture storing systems are well-positioned to play a big part in the future of digital asset management because they provide a scalable, resilient, and privacy-preserving method of maintaining image data. These platforms have the power to completely change how photos are shared, saved, and retrieved, ushering in a new era of decentralised data management as use grows and technology advance.

BIBLIOGRAPHY

1. Metamask

Home | MetaMask developer documentation

2. Soiidity

Home | MetaMask developer documentation

3. Synchronization

kshitijofficial/Dgdrive3.0 (github.com)