IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Marketplace For Decentralised File Storage Using Public Blockchain

[1]Dev Bahl, [2]Devansh Taneja

[1]Analyst, [2]Software Developer

Abstract: In recent times, as technology progresses, Centralized cloud storage represents a transformative approach to enhancing file storage and resource sharing with notable efficiency. However, despite its convenience, it faces certain challenges, including high cost margins, file security concerns, limited network bandwidth availability, and the risks associated with single-party control. To address these limitations and improve storage efficiency, the adoption of decentralised file storage is proposed, incorporating appropriate incentives for both data owners and disk space providers.

I. INTRODUCTION

The primary objective of the system is to establish a public, decentralised, and secure platform for renting disk space. The platform operates on the principles of a free market, facilitating direct interactions between two key participants: **Data Owners (DO)**, who require disk space to store or back up private data, and **Disk Space Owners (DSO)**, who offer their available storage resources for this purpose.

Unlike traditional cloud storage solutions, the proposed File Storage Marketplace is fully decentralised. It eliminates the presence of a centralized authority or intermediary that could exert control over the interactions between DOs and DSOs. This decentralization ensures that no single entity has the capability to influence or restrict the cooperation between these participants in any manner.

Key assurances of the system include:

1. **Data Privacy:** The system guarantees that no external party, including the platform itself, can access the private data stored by Data Owners.

2. **Financial Security:** It ensures the safety of payments, preventing any unauthorized party from intercepting or stealing funds during transactions.

3. **Immutable Logic:** The cooperation and payment logic embedded within the system cannot be altered arbitrarily, ensuring consistent and transparent operations.

4. **Uninterrupted Access:** Participants cannot be forcibly removed or disconnected from the system, safeguarding their ongoing usage rights.

By leveraging blockchain technology and smart contracts, the platform aims to provide a robust, equitable, and transparent marketplace for decentralised file storage.

II. RELATED WORKS

A. *"Block Chain Based Decentralised Cloud Storage, International Journal of Engineering and Advanced Tech, Volume 8 Written by G.Abinaya, Preksha Kothari" [1]*

As described in [1], The study highlights several key findings in the realm of cloud storage and security. It identifies the vulnerabilities inherent in existing centralized cloud storage systems, such as data security risks, single points of failure, and limited privacy. To address these challenges, the research proposes a decentralised cloud storage model that leverages distributed architecture to enhance security, privacy, and resilience. Central to this solution is the use of Merkle Trees, a cryptographic structure that represents a binary tree composed of hash units, enabling efficient verification of data integrity. The implementation further incorporates advanced encryption and decryption algorithms to ensure secure data storage and access. Additionally, blockchain technology serves as the foundation for managing transactions and verifying data integrity, while smart contracts automate and enforce operational rules, fostering a transparent and trust less ecosystem.

III. PROPOSED SYSTEM

The proposed system addresses the escalating concerns faced by users of centralized cloud storage platforms. These concerns primarily include the risk of data breaches and the restrictive nature of services imposed by cloud service providers. To mitigate these issues, the system introduces a decentralised approach to file storage. It leverages the expanding global cryptocurrency market to facilitate the exchange of massive decentralised disk space. Disk Space Owners (DSOs) are incentivized for contributing their storage resources, thereby fostering a secure, efficient, and equitable storage ecosystem.

A significant limitation of the proposed system is its implementation across diverse platforms and systems. This challenge also encompasses gaining acceptance from the general public and governments, as widespread adoption requires alignment with varying technological environments, regulatory frameworks, and user preferences across different platforms.

IV. METHODOLOGY

Blockchain technology, best known as the foundation for cryptocurrencies such as Bitcoin and Ethereum, extends far beyond the financial sector due to its innovative approach to securely storing and transmitting information. At its core, blockchain operates as a distributed ledger, a decentralised method of maintaining records across a network of interconnected computers, commonly referred to as "nodes."

Distributed Ledger Technology (DLT) enables the secure recording and management of data across multiple nodes within a network. Unlike conventional record-keeping systems, which centralize data storage on a single server accessible to all users, blockchain decentralizes this process. Any user within the network can act as a node, although participating in this capacity requires substantial computational power. These nodes perform essential functions, including verifying, approving, and storing data within the ledger, ensuring the integrity and security of the recorded information.

The structure of a blockchain organizes data into discrete units called "blocks," each of which contains a finite amount of information. As new data is added, additional blocks are created, forming a continuous and interconnected sequence—hence the term "blockchain." Each block is uniquely identified by a cryptographic "hash," a secure code that protects the information within it. The hash not only safeguards the block's data from unauthorized access but also establishes its position within the chain by referencing the preceding block and linking it to the subsequent block.

This cryptographic linking of blocks ensures the immutability and security of the blockchain, making it highly resistant to tampering or unauthorized modifications. As a result, blockchain technology offers a robust solution for applications requiring secure, transparent, and decentralised record-keeping, with potential use cases spanning industries such as healthcare, supply chain management, and governance, in addition to its foundational role in cryptocurrency.

Smart Contracts are self-executing digital contracts whose terms and conditions are directly written into code. They automatically enforce and execute the contractual obligations once predefined conditions are met, eliminating the need for intermediaries. These contracts are deployed and run on a blockchain, ensuring transparency, security, and immutability. Since blockchain technology is decentralised, smart contracts are resistant to tampering or alteration, offering a high level of trust between parties involved in a transaction.

Smart contracts can be applied in various domains, such as finance, supply chain management, and decentralised applications (dApps), by automating processes like payment execution, data verification, and dispute resolution. For example, in a decentralised file storage system, a smart contract could automatically release payment to a Disk Space Owner (DSO) once a Data Owner (DO) confirms that the file storage is successful, eliminating delays and reducing potential conflicts.

Fig 4.1: Smart Contracts

Blockchain Escrow is a service that uses blockchain technology to hold funds or assets in a secure, transparent manner until specific conditions are fulfilled. Typically, an escrow service involves a third-party intermediary to manage transactions between two parties. In contrast, blockchain escrow operates without a central authority by utilizing smart contracts to ensure that funds are only released once agreed-upon conditions are met.

For example, in a blockchain escrow system for a cryptocurrency transaction, the buyer deposits the agreed amount of cryptocurrency into the escrow account controlled by the smart contract. The funds remain locked until the seller has delivered the agreed-upon goods or services. Once the buyer confirms receipt of the goods or services, the smart contract automatically releases the funds to the seller. If the conditions are not met within a specified timeframe, the smart contract can return the funds to the buyer, ensuring fairness and trust in the transaction process.

Blockchain escrow enhances security by reducing the risk of fraud, as it ensures that both parties fulfil their obligations before the exchange of funds. It also provides a transparent, immutable record of the transaction, which can be audited by any party involved, further fostering trust and accountability in decentralised transactions.

Fig 4.2: Blockchain Escrow

Together, smart contracts and blockchain escrow provide an efficient, secure, and transparent framework for managing digital transactions, ensuring that agreements are automatically executed, and assets are safeguarded until conditions are met. These technologies have a wide range of applications, from decentralised finance (DeFi) platforms to digital marketplaces, where trust and security are paramount.

Merkle tree is a data structure that offers several unique features, making it particularly useful for Bitcoin mining and other applications. It is employed to organize and store all transactions within a given block. The primary advantage of using a Merkle tree is that it allows a node to efficiently prove to another node that a specific transaction is contained within a particular block of transactions. This is especially important for Simplified Payment Verification (SPV) nodes and light clients, which do not store the entire blockchain and are only interested in specific transactions or blocks.

By utilizing a Merkle tree, it becomes possible to confirm the existence of any given transaction ID without the need to expose the entire tree. For instance, to verify that a transaction ID is included in a Merkle tree containing eight transactions, only three hashes are required, significantly reducing the amount of data needed for verification. This capability provides considerable performance benefits, especially for light clients that rely on other nodes for transaction verification, as they do not retain the full blockchain.

Web3 represents a fundamental shift from traditional Web2, with decentralization being at its core. Unlike Web2, where applications are typically built and deployed on a single server or database managed by a central cloud provider, Web3 applications, or decentralised apps (dApps), operate on blockchains or decentralised networks of peer-to-peer nodes. These networks, or a combination of both, form a crypto-economic protocol that ensures the decentralization of services. In Web3, developers are incentivized to compete in providing high-quality services, as participants in the network are motivated by rewards to create, govern, and improve the ecosystem.

Cryptocurrency plays a significant role in this environment, as it offers financial incentives through tokens for anyone contributing to the development or governance of Web3 projects, further encouraging participation and growth within the decentralised space.

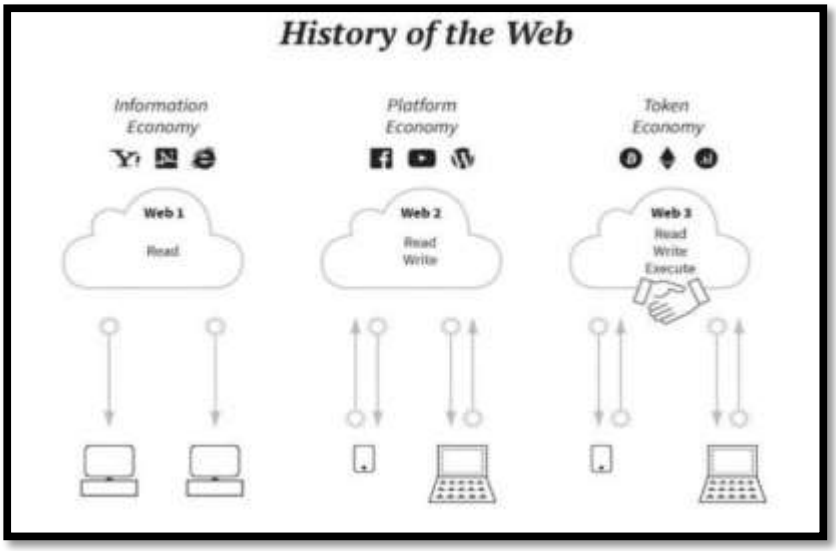

Fig 4.3: History of Web

ARCHITECTURE DIAGRAM

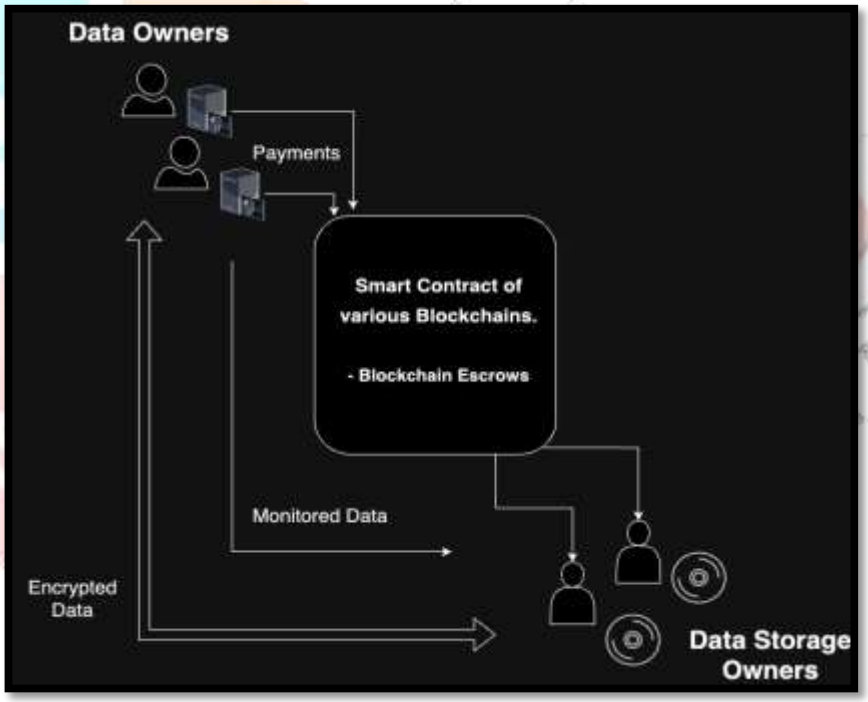

Fig 4.4: Architectural Diagram

UML FLOWCHART DIAGRAM

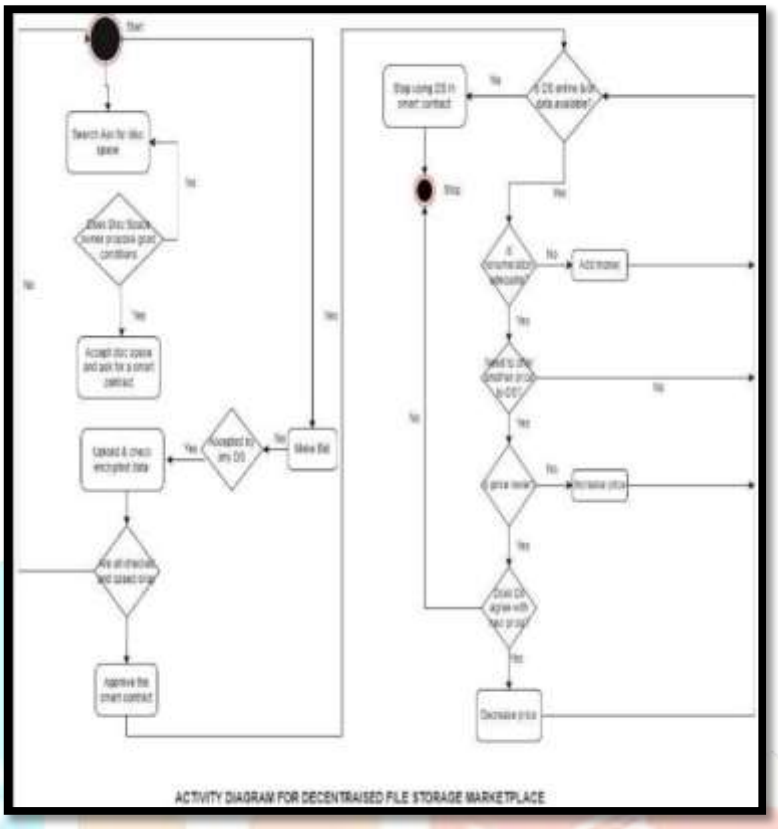

Fig 4.5: UML Activity Diagram

V. ALGORITHMS USED

Proof of Work (PoW) is the consensus algorithm initially employed by the first blockchain network to validate transactions and append new blocks to the chain, a process known as transaction confirmation. In this mechanism, miners—individuals or entities within the network—compete to complete the computational work required to process transactions, ensuring the integrity of the blockchain.

The **Advanced Encryption Standard (AES)**, a widely used encryption technique, supports various key sizes, including 192-bit and 256-bit keys for high-security applications. Additionally, it incorporates a 128-bit variant known as WSSDecryptAES for decryption processes. This method enables efficient and secure decryption, particularly using AES192 for robust encryption needs.

VI. CONCLUSION

In conclusion, the proposed system leverages blockchain technology and smart contracts to revolutionize file storage by creating a decentralised, secure, and transparent marketplace for disk space renting. By eliminating centralized control, it ensures equitable participation and fosters trust between Data Owners (DO) and Disk Space Owners (DSO). The system's assurances of data privacy, financial security, immutable logic, and uninterrupted access provide a robust foundation for users seeking reliable and efficient storage solutions. This innovative approach not only addresses the limitations of traditional cloud storage but also paves the way for a more democratic and resilient data storage ecosystem.

REFERENCES

[1] Block Chain Based Decentralised Cloud Storage, International Journal of Engineering and Advanced Tech, G.Abinaya, Preksha Kothari

[2] Block Chain - Based Decentralised Storage Scheme, Yan Zhu, Chunli LV, Zichuan Zeng, Jingfu

[3] Decentralised File Storing and Sharing System using Blockchain and IPFS, Mihir Nevpurkar, Chetan Bandgar, Ranjeet
Deshmukh, Jay Thombre, Rajashri Sadafule, Suhasini Bhat