NExUS : Networked Exchange using IPFS and P2P in a decentralized, Universal System leveraging the Blockchain Technology

Shivani Suresh
Reg No.:2021503050
Department of Computer Technology
MIT Campus, Anna University
Chennai, India

Swathy K S
Reg No.:2021503052
Department of Computer Technology
MIT Campus, Anna University
Chennai, India

R B Shyamala
Reg No.:2021503558
Department of Computer Technology
MIT Campus, Anna University
Chennai, India

***Abstract*—This project explores the development and implementation of a robust decentralized file sharing system leveraging blockchain technology, fostering a peer-to-peer paradigm for secure and decentralized data exchange. The methodology encompasses a detailed examination of the blockchain creation process, dissecting block structures, and their components, including block numbering, timestamping, cryptographic proof generation, and the establishment of block chains via the SHA-256 hashing algorithm. In addition, this project explores the creation of a peer-to-peer network facilitated by Socket Programming, ensuring exclusive data access within the blockchain for authorized nodes. The concept of a unique file key/password shared between sender and receiver is introduced to enhance data security within the blockchain network. This abstract highlights the upload and download processes, emphasizing encryption methodologies employing AES encryption, coupled with the seamless integration of IPFS to optimize storage efficiency. Furthermore, this research sheds light on the cryptographic elements of the system, specifically the use of the SHA-256 hashing algorithm and AES encryption, emphasizing their contributions to data integrity and confidentiality. Finally, the study presents empirical results derived from rigorous testing of the system, using multiple nodes, providing concrete evidence of its effectiveness in enabling secure file sharing while ensuring blockchain consistency and decentralization. This research underscores the viability of blockchain-based solutions in addressing contemporary challenges related to data sharing and security.**

***Index Terms*—Decentralized File Sharing, Blockchain Integration, Peer-to-Peer Network, AES Encryption, Data Security, IPFS Storage.**

I. Introduction

The advent of blockchain technology has revolutionized various industries by introducing the concept of decentralized, transparent, and tamper-resistant data management. Among its diverse applications, decentralized file sharing has emerged as a compelling use case, offering a secure and efficient solution for peer-to-peer data exchange. This research project embarks on a comprehensive exploration of a decentralized file sharing system that harnesses the potential of blockchain technology to ensure a secure, decentralized, and peer-to-peer data sharing mechanism.

In an era where data is increasingly recognized as a valuable asset, the need for secure and controlled data sharing is paramount. Traditional centralized file sharing systems, while functional, often raise concerns regarding data privacy, security, and the reliance on intermediaries. The adoption of blockchain technology addresses these concerns by fundamentally altering the way data is stored, accessed, and shared.

The methodology underlying this research project is multifaceted, beginning with the creation of a blockchain infrastructure tailored to the requirements of decentralized file sharing. The block structure, comprising essential components such as block numbering, timestamping, cryptographic proofs, and the linkage of blocks through the SHA-256 hashing algorithm, forms the bedrock of the blockchain's architecture. This structure not only ensures data immutability but also facilitates transparent tracking of file transactions within the network.

Furthermore, the establishment of a peer-to-peer network using Socket Programming enables exclusive access to the blockchain's data by connected nodes. This network acts as the conduit for data sharing, ensuring that only authorized users participate in the blockchain's operations. Access permissions are granted through a user-initiated process of connecting to the blockchain network, reinforcing the system's permissioned approach.

Central to this research project is the concept of a unique file key/password, serving as a linchpin in enhancing data security within the blockchain network. The file key is shared exclusively between the sender and receiver of shared files, providing an additional layer of confidentiality and access control. Detailed descriptions of the upload and download processes underscore the critical role of encryption methodologies, employing AES encryption, in safeguarding file content. The integration of the InterPlanetary File System (IPFS) augments data storage efficiency, ensuring that the blockchain remains lightweight and scalable.

In addition to encryption techniques, this research project delves into the cryptographic components of the system, most notably the application of the SHA-256 hashing algorithm.

This algorithm, known for its one-way, deterministic, and collision-resistant properties, plays a pivotal role in generating unique hashes for both blockchain blocks and shared files. These hashes provide the foundation for data integrity and authentication, bolstering the security and reliability of the entire system.

To validate the practicality and efficacy of the decentralized file sharing system, empirical testing was conducted using multiple nodes. The results of these tests highlight the system's ability to facilitate secure file sharing while maintaining blockchain consistency and decentralization. This research project serves as a testament to the viability of blockchain-based solutions in addressing contemporary challenges related to data sharing and security.

In the subsequent sections, we delve into the intricacies of creating the blockchain, establishing a peer-to-peer network, implementing cryptographic encryption, and integrating with IPFS, providing a comprehensive understanding of the underlying methodology and its practical implications.

II. Related Works

In the groundbreaking work presented in [1], Zhou and collaborators address the critical need for secure and controlled access to academic paper reviews. The introduction of a permissioned blockchain serves as a cornerstone, ensuring that only designated users with authorized credentials can access the shared files. Encryption using a shared key adds an additional layer of security, and the innovative storage of this key on the blockchain guarantees that decryption capabilities are exclusive to the intended recipients. To safeguard against potential tampering, the incorporation of a timestamping mechanism ensures the files' integrity, providing a comprehensive and robust solution for secure academic paper review processes.

In the realm of scalable and trustworthy file-sharing systems, as proposed in [2] by Cui et al., the utilization of a distributed hash table (DHT) emerges as a key architectural choice. This decentralized approach to file storage enhances security by preventing single points of failure. The integration of blockchain technology to record file transactions solidifies the system's trustworthiness, creating an immutable ledger that safeguards against any attempts to tamper with the files. The synergy between DHT and blockchain results in a resilient and scalable solution, addressing the challenges associated with secure and scalable file sharing.

In the context of peer-to-peer (P2P) file-sharing systems, Pradhan and team, as detailed in [3], propose a holistic blockchain-based security framework. By leveraging blockchain, the system strategically stores comprehensive file metadata, including essential details such as file name, size, and hash. The file hash plays a pivotal role in verifying the authenticity of files, contributing to the overall security of the P2P network. Furthermore, the incorporation of a reputation system introduces a social trust layer, enabling the community to rate users and mitigate potential risks associated with the distribution of infected files. This multifaceted approach ensures not only the security of the files but also the integrity of the entire P2P file-sharing ecosystem.

In the innovative system outlined in [4] by Anthal and colleagues, a unique combination of the InterPlanetary File System (IPFS) and blockchain technology is introduced. Storing files on the IPFS network provides a decentralized and distributed file storage solution, while the blockchain records ownership transactions. This dual-layered strategy guarantees the tamper-proof nature of files, securing their ownership and transaction history in an immutable ledger. Empowering users with control over their own files within the IPFS network, this system not only enhances data security but also introduces a novel paradigm for decentralized and user-centric file management.

III. Proposed Work

A. Proposed Architecture

The research project on decentralized file sharing, harnessing the capabilities of blockchain technology, unfolds as a comprehensive and multi-dimensional endeavor, strategically designed to augment the realms of security, efficiency, and accessibility within the domain of peer-to-peer data exchange. This ambitious initiative can be distilled into several key phases, each intricately tailored to address specific facets of the overarching goal. The proposed work can be categorized into the following key phases:

1. **Blockchain Development- Blockchain Architecture Design:** In this phase, the research will focus on designing a blockchain structure optimized for decentralized file sharing. This includes defining the block structure, block numbering, timestamping mechanism, cryptographic proof generation, and implementing the SHA-256 hashing algorithm for block linkage. The research aims to create a robust blockchain backbone that ensures data integrity and security.

2. **Peer-to-Peer Network Establishment- Socket Programming Implementation:** The project will implement Socket Programming to create a peer-to-peer network for blockchain participants. The research will develop methods for connecting nodes to the blockchain network securely and efficiently. Access control mechanisms will be explored to ensure that only authorized users are part of the network.

3. **Enhanced Data Security- File Key Integration:** The research will delve into the implementation of a unique file key/password system, emphasizing its role in enhancing data security. The project will design protocols for securely sharing file keys between senders and receivers, ensuring confidentiality and access control.

4. **AES Encryption Implementation:** The proposed work includes the implementation of AES encryption for file encryption and decryption. Research will focus on robust encryption techniques to safeguard file content and maintain

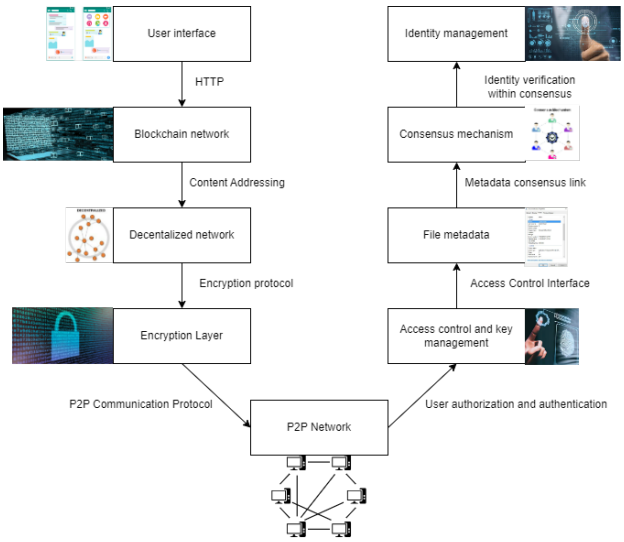

Fig. 1. Proposed Architecture

data privacy during transmission and storage.

5. **Integration with IPFS-IPFS Integration:** The research project will explore the seamless integration of the InterPlanetary File System (IPFS) to optimize file storage efficiency within the blockchain network. This integration will involve defining protocols for storing file hashes on IPFS while ensuring their accessibility through the blockchain.

6. **Cryptographic Components- SHA-256 Hashing Algorithm:** The research will further investigate the application of the SHA-256 hashing algorithm in generating unique and secure hashes. The emphasis will be on data integrity, immutability, and authentication within the blockchain network.

7. **Empirical Testing and Validation- Testing and Evaluation:** The proposed work will involve rigorous testing of the decentralized file sharing system using multiple nodes. Comprehensive tests will be conducted to assess the system's performance, security, and scalability in real-world scenarios.

B. Proposed Algorithm

The articulated process encapsulates a holistic and meticulous strategy for erecting a robust blockchain network, weaving together intricate cryptographic methodologies with advanced networking principles. At its core, the blockchain structure is meticulously defined, featuring pivotal elements such as Block number, Timestamp, Proof, and Previous Hash. The security integrity of each block is staunchly reinforced through the application of the SHA-256 hashing algorithm, a cryptographic cornerstone that guarantees the immutability of data within the entire ledger.

A distinctive facet of this process lies in its cryptographic prowess, where an elevated level of security is introduced through the generation of unique keys/passwords for individual files. These file keys undergo a sophisticated layer of protection by being encrypted with the advanced AES encryption algorithm. This dual-layered security protocol ensures that sensitive data housed within the blockchain remains shielded against unauthorized access and potential breaches.

Simultaneously, the integration of a modified key expansion algorithm acts as a bulwark, fortifying the cryptographic infrastructure and contributing to the overarching resilience of the entire system. This parallel integration is complemented by the establishment of a peer-to-peer network through socket programming—a pivotal stride towards decentralization. This network architecture enables seamless communication among nodes within the same network, fostering a distributed and consensus-driven environment. The decentralized nature of this network not only enhances overall security but also acts as a deterrent against single points of failure and malicious attacks.

Algorithm 1 Cryptoblock

Procedure CryptoBlock
Step 1: Create a blockchain structure in which a single block contains Block number, Timestamp, proof, previous hash.
Step 2: The hash of the entire block is generated using SHA_256 hashing algorithm.
    Divide the padded message into 512-bit blocks.
    For each block:
    Prepare the message schedule W[0..63].
    Initialize working variables (a, b, c, d, e, f, g, h) with the current hash values.
    Perform 64 rounds of processing, updating the working variables and hash values using bitwise operations and constants
Step 3: Create a peer-to-peer network using socket programming, where all nodes are connected in same network.
Step 4: Unique key/ password for a particular file should be generated, which is shared between sender and receiver, which increases security of file in blockchain network. The file key is encrypted using AES encryption
    Initialize an array of words (W[0], W[1], ..., W[Nb*(Nr+1)-1])
    Copy the original key into the first Nk words of W (Nk depends on key size)
    for i = Nk to Nb*(Nr+1)-1:
if i mod Nk == 0: **then**
    temp = SubWord(RotWord(W[i-1])) XOR Rcon[i/Nk]
else if Nk $>$ 6 and i mod Nk == 4: **then**
    temp = SubWord(W[i-1])
else
    temp = W[i-1]
end if
W[i] = W[i-Nk] XOR temp
Intergration of blockchain with IPFS, to keep it scalable and lightweight.

Furthermore, the strategic fusion of the blockchain with the InterPlanetary File System (IPFS) underscores a commitment to scalability and lightweight storage solutions. Leveraging IPFS, the blockchain network becomes adept at efficiently managing and distributing substantial volumes of data across nodes, significantly enhancing system efficiency and responsiveness. This amalgamation of cryptographic best practices, decentralized networking, and seamless integration with IPFS positions the proposed blockchain system as a formidable and comprehensive solution for secure, scalable, and distributed data management.

In essence, this holistic approach is a concerted effort to tackle the pivotal challenges within the blockchain domain, aiming to cultivate a cutting-edge and resilient ecosystem that sets new standards in the evolving landscape of blockchain technology.

Blockchain Structure Creation

1) Create a block structure with Block number, Timestamp, Proof, and Previous Hash.
2) Generate the hash of the entire block using SHA-256.

Cryptographic Key Generation

1) Generate a unique key/password for a specific file.
2) Encrypt the file key using the AES encryption algorithm.
3) Initialize an array of words for key expansion.

Key Expansion Algorithm

1) Copy the original key into the array of words.
2) Perform key expansion using a modified algorithm with 64 rounds, involving bitwise operations and constants.

Peer-to-peer Network Setup

1) Implement a peer-to-peer network using socket programming.
2) Connect all nodes within the network for decentralized communication.

Integration with IPFS

1) Integrate the blockchain with IPFS for scalable and lightweight storage.
2) Ensure seamless integration to manage and distribute large volumes of data efficiently.

IV. Results and Analysis

To rigorously evaluate the functionality and effectiveness of our project, a comprehensive testing procedure was implemented. Two instances of Data Share were concurrently executed on the local computer, each assigned to different ports, thereby simulating the operation of distinct and independent nodes—let's refer to them as Node A and Node B. These instances served as separate entities within the blockchain network, enabling us to assess the system's robustness and reliability. Initiating the testing protocol, we established connections from both Node A and Node B to the blockchain network. Leveraging the concept of file keys for secure file sharing, we conducted a series of operations to validate the system's capability to upload and download files seamlessly across the network.

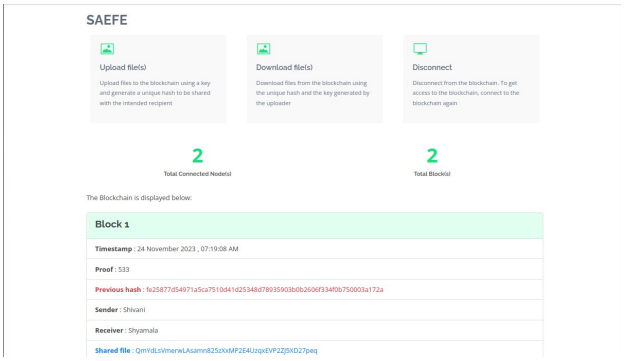

Fig. 2. Connected Nodes

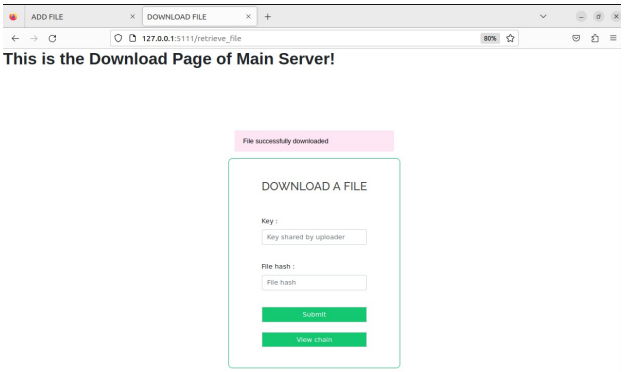

Fig. 3. Successful Download of file using Generated File Hash

From Node A, a file labeled 'x' was uploaded to the blockchain using the designated file key 'P'. Subsequently, the system demonstrated its bidirectional functionality as the same file, 'x', was downloaded from Node B using the identical key 'P'. This bidirectional file exchange process affirmed the efficacy of our file sharing mechanism and highlighted the system's ability to maintain file integrity across different nodes.

Continuing the testing sequence, we replicated the process with a distinct file, 'y', initiated from Node B. This time, the file 'y' was uploaded to the blockchain using the file key 'Q', and, in turn, downloaded from Node A utilizing the corresponding key 'Q'. This comprehensive file-sharing exercise not only validated the system's versatility in handling multiple files but also affirmed its seamless interoperability between independent nodes.

Crucially, after each file-sharing operation, the blockchain was dynamically updated at both Node A and Node B. This synchronization mechanism ensured that the transaction history and ownership details of the shared files were consistently recorded and reflected in the blockchain ledger across all par-

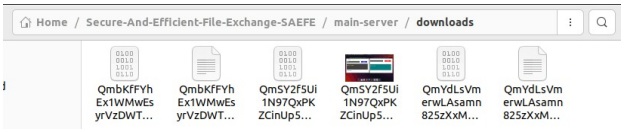

Fig. 4. Downloaded file through sharing mechanism

ticipating nodes. This comprehensive testing regimen not only validated the individual functionalities of file uploading and downloading but also underscored the system's robustness in maintaining a coherent and synchronized blockchain network.

V. Conclusion

In the context of this research endeavor, we have introduced a meticulously crafted architecture that serves as the backbone for a secure and scalable decentralized file sharing system, leveraging the transformative potential of blockchain technology. Our design philosophy places a paramount emphasis on user control, data integrity, and privacy, addressing critical concerns in the contemporary landscape of digital information exchange.

At the core of our architecture is a user-friendly interface, engineered to enhance accessibility and usability. The user-centric approach aims to empower individuals with intuitive tools for seamless interaction with the decentralized file sharing system. A robust blockchain network forms the bedrock of transparent transactions, facilitating a secure and auditable ledger of file-sharing activities. The integration of the Inter-Planetary File System (IPFS) further propels decentralization by providing a distributed and resilient storage solution for files, ensuring the system's scalability and fault tolerance.

Crucially, our architecture incorporates encryption measures to bolster security, ensuring that files are shielded from unauthorized access and potential breaches. The integration of peer-to-peer communication establishes a decentralized network infrastructure, fostering a collaborative environment where users can interact directly without intermediaries. Meanwhile, access control mechanisms and identity management protocols are implemented to guarantee that only authorized individuals have privileged access to shared resources, bolstering the overall security and integrity of the system.

As a result, our architecture serves as a robust foundation for secure, transparent, and decentralized file sharing. The emphasis on user-centric design, combined with blockchain transparency and decentralized storage, positions our system at the forefront of emerging technologies in the realm of secure data exchange. To further validate and optimize the proposed architecture, our future endeavors will involve real-world testing and ongoing optimization, ensuring that the system aligns seamlessly with evolving technological landscapes.

Looking ahead, the envisaged trajectory of decentralized file sharing systems suggests transformative potential for data exchange in an increasingly interconnected world. As technology continues to evolve, the adoption and refinement of decentralized architectures promise to redefine the dynamics of digital communication, offering a paradigm shift towards more secure, transparent, and user-controlled data sharing ecosystems.

References

[1] I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman and N. Shariati, "A Blockchain-based File-sharing System for Academic Paper Review," 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, Australia, 2019, pp. 1-10, doi: 10.1109/ICSPCS47537.2019.9008695.

[2] S. Cui, M. R. Asghar and G. Russello, "Towards Blockchain-Based Scalable and Trustworthy File Sharing," 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 2018, pp. 1-2, doi: 10.1109/ICCCN.2018.8487379.

[3] S. Pradhan, S. Tripathy and S. Nandi, "Blockchain based Security Framework for P2P Filesharing system," 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 2018, pp. 1-6, doi: 10.1109/ANTS.2018.8710078.

[4] J. Anthal, S. Choudhary and R. Shettiyar, "Decentralizing File Sharing: The Potential of Blockchain and IPFS," 2023 International Conference on Advancement in Computation and Computer Technologies (InCACCT), Gharuan, India, 2023, pp. 773-777, doi: 10.1109/InCACCT57535.2023.10141817.

[5] S. Sivanantham, M. Sakthivel, V. Krishnamoorthy, N. Balakrishna and V. Akshaya, "Reliable Data Storage and Sharing using Block chain Technology and Two Fish Encryption," 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2022, pp. 561-565, doi: 10.1109/ICIRCA54612.2022.9985510.

[6] M. Jain and M. Jailia, "Proposed model to decentralized storage of educational data for privacy preservation using Blockchain," 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2022, pp. 1-5, doi: 10.1109/ICCCI54379.2022.9740654.

[7] Y. Liu, Z. Wu, Y. Liu, K. Wang, W. Fan and L. Lin, "Research on data sharing mechanism of power material supply chain based on blockchain," 2021 IEEE 4th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China, 2021, pp. 345-350, doi: 10.1109/AUTEEE52864.2021.9668810.

[8] K. Sivasankari and V. S. Sathyamithran, "IPFS Enabled Robust Mechanism for File Storage and Retrieval Using Block Chain," 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 2022, pp. 01-05, doi: 10.1109/ICERECT56837.2022.10059644.

[9] M. Jain, M. Jailia and M. Agarwal, "Performance Analysis of Blockchain Technology using Inter Planetary File System (IPFS) database in comparison with Block chain database," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICCCI56745.2023.10128177.

[10] P. N. Kumar, B. Selvakumar, V. R, K. Rajkumar, K. K. Kumar and A. S. Kamaraja, "Smart Grid Peer-to-Peer Exchanging Energy System using Block Chain," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1036-1040, doi: 10.1109/ICCMC56507.2023.10084032.

[11] H. C. Chou, "A Blockchain-based Collaboration Framework for Educational Material Sharing," 2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), Kuching, Malaysia, 2020, pp. 1-5, doi: 10.1109/R10-HTC49770.2020.9356955.

[12] S. Geetha, Teena, C. ML and K. Jayaram, "Block Chain Based File Tracking and Management System for Pension Applications," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 1078-1083, doi: 10.1109/IITCEE57236.2023.10091068.

[13] E. S. T. K. Reddy, M. Sathvik, V. Rajaram and C. P. Rao, "An Intelligent Tender Management System using Block Chain and IPFS," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 1497-1502, doi: 10.1109/ICSCSS57650.2023.10169649.

[14] S. Malgaonkar, S. Surve and T. Hirave, "Distributed files sharing management: A file sharing application using distributed computing concepts," 2012 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, 2012, pp. 1-4, doi: 10.1109/ICCIC.2012.6510207.

[15] R. Chen and Z. Li, "Blockchain-Based Mechanism for Electronic Healthy Records Sharing Using Fine-grained Authorization," 2021 7th International Conference on Computer and Communications (ICCC), Chengdu, China, 2021, pp. 1557-1564, doi: 10.1109/ICCC54389.2021.9674391.