HBRP PUBLICATION

Advancement of Computer Technology and its Applications
Volume 6 Issue 1

Block Chain- Based Secure Storage and Access Scheme System for Data in IPFS

Dr Nanda Gopal S. M.[1]*, Aashi Pradhan[2], Anupriya Singh[3], Amal Arshad[4], Gurram Jyoti[5]
[1]Associate Professor, Department of CSE, HKBCE, Bangalore, India
[2,3,4,5]Student, Department of CSE, HKBCE, Bangalore, India

Corresponding Author
E-Mail Id: *nandhagopal.cs@hkbk.edu.in*

ABSTRACT

With decentralized participant nodes cooperating to maintain a trustworthy database, block-chain is fundamentally a consensus system managed by several parties. In the current national network ecosystem, publishing is open to everybody. Knowledge files are a crucial information source that show how busy publishers are. Additionally, superior information resources can advance society. The opposite is true with inferior pirated files. The majority of firms currently use centralized servers to control how individuals distribute knowledge files. A distrusted third party must also be included in order to analyse and encrypt the data contained in files. Due to the lack of clear standards for identical intellectual files, file retention transactions become opaque, intellectual property is violated, and consistent file management systems cannot be maintained between institutions. We suggest an Interplanetary File System based Block-chain storage paradigm. (IPFS). The issue of storing transactions in a block and accessing them from that block is solved by immutability. In the proposed system, the file is saved in IPFS and the hash value of the message is stored in Block-chain, which reduces Block-chain size. IPFS stores the file as a hash value of the file. Block is append-only, protecting user privacy while making files and data easier to retrieve. The method also transfers files in the synchronized block-chain and uses the consensus of all participating nodes to assure traceability. This essay describes the upload and transfer of files along with the method's framework and guiding principles. Finally, the method's efficiency is compared, evaluated, and its advantages and disadvantages are covered. In this suggested system, the file is kept in IPFS while implementing the decentralized block chain process, reducing the size of the block chain, and other features. The hash value of the file is what is saved in IPFS as the file. Block is append-only, which safeguards user privacy while enabling quick access to files and data. Finally, the approach we provide is based on the Interplanetary File System, a block-chain storage paradigm (IPFS). The issue of storing transactions in a block and accessing them from that block is solved by immutability. The block chain stores the message's hash value.

Keywords: *Block chain, decentralization, direct acyclic graph (DAGs), distributed hash table (DHTs), ethereum, IPFS SHA (secure hash algorithm), secured and shared storage*

INTRODUCTION

For large enterprises that function globally, storing a large volume of data has become a problem in the modern day. These companies have therefore resorted to cloud storage, which has excellent data storage and transfer capabilities [1].On the other hand, these cloud storage providers take on the role of trustworthy third parties. As a result, a number of security and confidentiality problems develop. The most promising solution at this time is IPFS, or Interplanetary File System, a peer-to-peer protocol [8]. A client can

access a useful abstraction layer that enables them to just call the hash of the file they want in order to fetch any of those files. Following this, IPFS transmits the file to the client by searching the nodes for it [12]. This obviously has a security flaw. Anyone with access to the PDF file's hash may download it from IPFS. Consequently, IPFS in its current form is not appropriate for sensitive material. IPFS is not a suitable fit for exchanging private information like medical records or images unless we do anything with it. The application model will considerably develop network technology, and we now have tools that interact with IPFS distribution technology. Bit-coin was the birthplace of distributed shared accounts. All of the system's nodes keep track of the block-chain, which serves as a database to keep track of all system transactions.

Numerous additional fields and businesses, including as healthcare, energy management, and supply chains [2,3], have adopted block chain technology. When creating peer-to-peer (P2P) communication technology, block chain is decentralized, tamper-proof, traceable, and attack-proof. Block chain technology makes use of distributed storage, consensus algorithms, smart contracts, and other tools. Communication quality and convergence speed of information are major concerns in a P2P network. Because of the way the private chain's authorized nodes function, which falls under the category of the block chain's nature, nodes trust one another more, which increases the protection of privacy.

The content kinds and file sizes of knowledge files vary [9]. The data on the block chain increases and makes it too difficult to store after being directly stored there and updated frequently for synchronization. The interplanetary file system relieves storage load on the block chain itself by connecting all participating nodes to a single storage system as a distributed file storage system. In addition, IPFS uses content-based addressing to alleviate the issue of data redundancy in the network. This study's primary contribution can be summed up as follows:

- The local IPFS private network in the model boosts content publishers' productivity when they submit NDN encryption knowledge files.
- To accomplish efficient real storage, the model stores the file's content in the IPFS private network along with the owner of the content and its matching hash value in a block-chain.

This paper has the following organizational structure: Section 3 introduces the uploading and forwarding of files in depth using real-world examples, whereas Section 1 focuses primarily on the technology and principals involved in the model. The proposed approach is assessed by experimental simulation. The section provides a summary of the analysis and conclusions of the suggested plan and other related studies.

THEORY

Block Chain

Data base is access by many node in a computer network to a chain of blocks which contains a piece data is most basic definition of block chain a block gets finished connected to the block before it forms block chain Level Conclusion.

Block Chain System Components

IPFS

IPFS is a global point-to-point storage system was first intended to refine the current hypertext transfer protocol and then assemble computer device using the same file system to create a sizable distributed IPFS offers a hidden shared network that is safer and effective in

addition to a node network this content search strategy uses a DHTS to discover the needed by giving each file in the network.

Data link
Time-stamped bundles of transaction data and code are delivered to the node.

Network layer
Included in the description are the message transmission protocol and data verification mechanism for the networking mode of the block chain system.

Consensus Layer
Fix the problem of efficiently obtaining consensus in a distributed system with the consensus layer [14].

Smart Contracts
The block chain implementations space is broadened by its which offer a complete block chain technological solution[13]. Fundamental logic for system typically housed smart contract which acts as the block chains main technology service module and offers strong technical support applications a network often same one powers the block chain execute it pieces of computer code that have the possible to update ledgers on plan with dispersed storage they function. A distinct hash value based on the files content upon request IPFS will synchronously download and splice files to speed up its access for huge storage files automatically splitting it in the models overall effectiveness a three-node IPFS private storage network was built numerous servers for storage within the framework.

SHA – 256
Secure Hash Algorithm is hashed using this method the input data is compressed into a smaller unintelligible form by a hashing technique algorithms and bitwise operations the sha-256 technique uses padded message blocks of 264-1 bits to get a 25 6-bit hash value with a maximum message size of 512 bits internally sha-256 computes a 256- bit hash for security however for printing and storage this can be reduced to 196 or 128 bits as a result a shortened sha-256 offers a significant increase in security at the expense of a small loss in human usability in printed citations at the cost of a slight performance loss compared to MD5. Unlike the MD5 method, there are no known attacks on truncated SHA-256.

PEER to PEER
P2P is network devices connected to another to form P2P is used to store files. After it has been set up nodes all are of similar power [11].

DAG (Direct Acyclic Graph)
Distributed systems use the dag 2 they employ Merkle DAGs which each node has a distinct id this is a reference to the definition of CID content addressing refers to the method of locating a data object such a Merkle DAG node using its hash value which used by IPFS and suited for representing directories and files can be organized in a variety of ways before generating a Merkle DAG representation IPFS frequently divides our content into blocks by dividing a file into blocks various components can be derived from sources and promptly validated in that they have a CID for everything turtles all the way down is a good analogy for Merkle DAGs assume for the moment that we have a file with an assigned CID what if this file is a part of a folder with several other files in it additionally CID numbers will be given to these files exactly what is the CID for that folder a hash of the CID from the files beneath them would be used i.e. the contents of the folder the blocks that make up these file each have a unique CID blocking content and using Merkle DAGs have the additional benefit of

enabling the sharing of Merkle between similar files DAG portions, allowing parts of distinct Merkle DAGs to refer to the same subset.

DHTS (Distributed Hash Table)

To determine peer is looking for IPFS utilize table that keeps track of key-value associations4 a DHTS is one that is disseminated across all peer in a network to find the necessary information we seek the aid of our co-workers the libp2p project is a component of ecosystem that provides the DHTS and controls peer connections and communication it's important to note that p2p can be used for many systems outside like IPFS can our belongings have been located and we know where they are at the moment now we must access that content by connecting to it exchange to request and send blocks to other peers IPFS employs a module called bit swap by using bit swap we may connect to the peer or peers who have the content we need transfer them our wish list a list of all the blocks were interested in and request the blocks they have for us by hashing those blocks content to generate CIDs we can check they match the CIDs required we could clone.

ETHEREUM

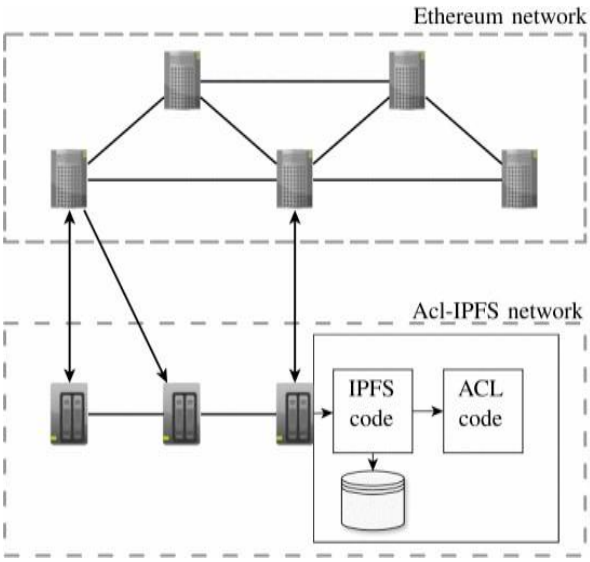

Fig. 1: *Acl-IPFS.*

Block chain technology underpins the decentralized, international software platform known as Ethereum [5]. Users can trade in both the company's own cryptocurrency, ether, and unique tokens using this platform. It distinguishes itself by integrating smart contracts extensively. They make it possible for code to be executed and for the results to be stored on the block chain with the same level of security as financial transactions [7]. The most well-known of these languages, Solidity, can produce a special type of bytecode that is read by the Ethereum Virtual Machine. Ethereum has a ton of state, which allows code running on the block chain huge alter the system's state, which depends on factors like account balances and contract storage [6] .The block chain keeps track of additions, deletions, and modifications to permissions, making it possible to build an access control system based on intelligent contracts.

ARCHITECTURE

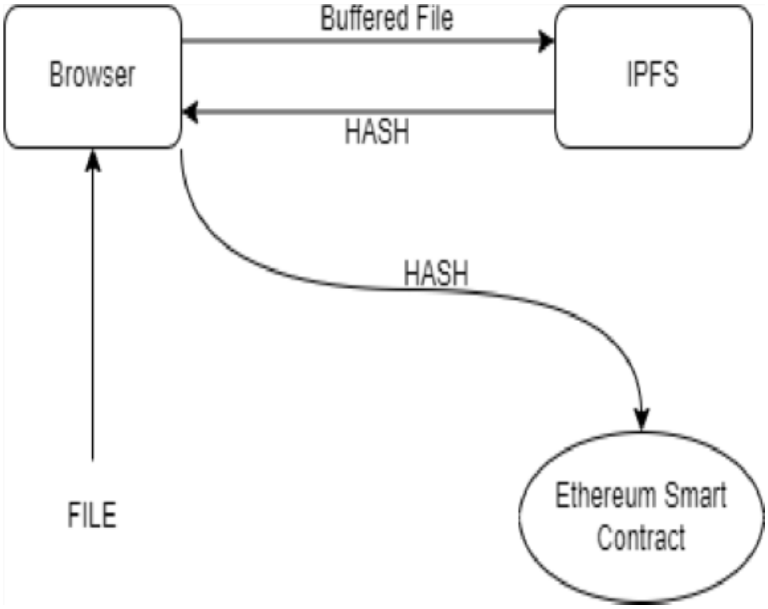

Fig. 2: *Basic File Upload Architecture.*

File Addition

Each file uploads to IPFS generates block all ids related to the file are logged in this stage he permissions package then receives these and utilize the add block procedure to register files with the smart contract. To achieve this, basic transactions are compiled. Thanks to the authorization.

File Retrieval

Transactions can also be validated using the appropriate content IDs [4]. The IPFS function resumes execution if the transactions are successful, stores the blocks locally, and then registers as a content identifier provider. To convert the message digest into hex format, utilize the salting technique.

1.A file hash containing the content address is created by fusing the message digest (Mds) and hash value. A hash of the content's address is maintained on the block chain network to help reduce the distributed ledger's size. When a hostile node observes the relevant transaction, it may try to claim the same content identification and obtain access to smart contract privileges while doing

2.Although this is theoretically possible, there is no guarantee that the adversarial node will succeed because the two transactions compete for network acceptance and the acceptance of the first transaction will render the acceptance of the second transaction invalid due to smart contract validation. Despite this, it has the ability to halt a process and assess whether a transaction was successful or not.

Since the blocks are not stored locally, the rightfully owning node cannot distribute any file chunks because it is not a provider in this situation. When a new block is created through mining, IPFS offer distinct hash for each transaction that is saved. Using a special IPFS hash value. Content access can be used to access a transaction a suggested

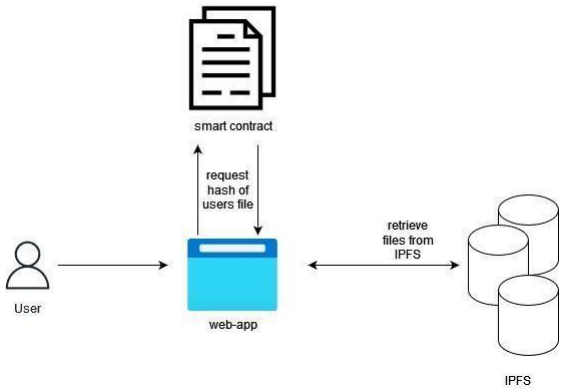

Fig. 3: *File Retrieval Architecture.*

If the appropriate permissions have been set, the node can ask for and get the blocks corresponding to the files. To achieve this, it searches the network for block providers and establishes contact with them in order to get the blocks required to recreate the file. The request will not be taken into consideration if the authorization has either not yet been obtained or has already been cancelled. Following confirmation of the transaction, the file is uploaded to IPFS. IPFS provides the hash value of a file after it has been uploaded, enabling retrieval.

The public and private keys linked to a node's Ethereum account are obtained when it sends a request. The request is signed, and this data is also added to the public key. By verifying the public key that has been provided and from which the address can be deduced, other nodes can utilise this additional information to confirm the identity of the network member.

CONCLUSION

Data sharing is pressing issue require notice document block chain technologies utilize the foundation data sharing scheme proposed to study also designs and implements data sharing system and evaluates system performance findings help of platform characteristics to solve data storage and access control problems distributed file system IPFS is used for data storage. Which solves the issue of database storage security and eliminates the risk of data leakage thanks to its decentralized properties8block chain alliance technology and IPFS are combined to form a data sharing system and a method of creating hash tables in memory is proposed to increase the speed of data retrieval realized a data sharing system formed by IPFS module block-chain module encryption and decryption module and quick search module upload data using the browser write data using the block-chain module in the background encrypt or decrypt files using the encryption and decryption module store data utilizing the IPFS back-end module set up a background web service to run block-chain and IPFS nodes create an internal shared network and provide frontend service interfaces send search instructions through the browser to the fast search engine in the background to achieve Fast data search and finally submit the safety and performance evaluation results to its platform decentralization prevention data tampering data security and maintaining data[13].

Spontaneously among nodes are benefits of the data sharing platform based on block- chain and IPFS technology which overcomes the key challenges of data sharing [3]. The majority of block-chain applications in commercial banks are still being developed and tested and there is

still a long way to go before they are employed in life and production additionally there are significant challenges in gaining regulatory authorities and the markets acceptance.

Table 1: *Comparison of Model performance.*

Model Contrast	Secure storage	Smart Contract	IPFS	Forwarding Efficiency	Network Management
SSS	Yes	No	No	No	No
Content espresso	No	No	No	Yes	No
DFS	Yes	No	No	Yes	No
E-resource	Yes	Yes	Yes	Yes	No
Our model	Yes	Yes	Yes	Yes	No

ACKNOWLEDGEMENT

We would like to express our deepest gratitude to our principal Dr. Tabassum Ara, our HOD Dr. Ashok Kumar P S, Dept. of Computer Science and Engineering and our Guide Dr. Nandha Gopal S M for their constant support and guidance in giving us valuable inputs and timely feedback.

REFERENCE

1. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors*, *18*(8), 2575..
2. Nartey, C., Tchao, E. T., Gadze, J. D., Yeboah-Akowuah, B., Nunoo-Mensah, H., Welte, D., & Sikora, A. (2022). Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm. *EURASIP Journal on Wireless Communications and Networking*, *2022*(1), 1-27.
3. Huang, H. S., Chang, T. S., & Wu, J. Y. (2020, July). A secure file sharing system based on IPFS and blockchain. In *Proceedings of the 2020 2nd International Electronics Communication Conference* (pp. 96-100).
4. Meng, L., & Sun, B. (2022). Research on Decentralized Storage Based on a Blockchain. *Sustainability*, *14*(20), 13060.
5. Clack, C. D. (2018). A blockchain grand challenge: Smart financial derivatives. *Frontiers in Blockchain*, 1.
6. Kashyap, R., & Piersson, A. D. (2018). Impact of big data on security. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 283-299). IGI Global.
7. Debe, M., Salah, K., Rehman, M. H. U., & Svetinovic, D. (2019). IoT public fog nodes reputation system: A decentralized solution using Ethereum blockchain. *IEEE Access*, *7*, 178082-178093.
8. Sharma, P., Jindal, R., & Borah, M. D. (2021). Blockchain-based decentralized architecture for cloud storage system. *Journal of Information Security and Applications*, *62*, 102970.
9. Leibfried, P., & Petry, H. (2022). Blockchain in der Finanzberichterstattung. *Controlling & Management Review*, *66*(1), 54-59.
10. Liu, H., Peng, B., Liu, Z., Zhang, Y., & Xu, Z. (2022). Research on Logistics Information Management

System Based on Blockchain Perspective. *Academic Journal of Business & Management*, *4*(1).

11. Kumari, A., Chintukumar Sukharamwala, U., Tanwar, S., Raboaca, M. S., Alqahtani, F., Tolba, A., ... & Mihaltan, T. C. (2022). Blockchain-Based Peer-to-Peer Transactive Energy Management Scheme for Smart Grid System. *Sensors*, *22*(13), 4826.
12. Henningsen, S. (2022). Blockchain in der Chemie: Hype oder Innovationstreiber.
13. Lin, S. Y., Zhang, L., Li, J., Ji, L. L., & Sun, Y. (2022). A survey of application research based on blockchain smart contract. *Wireless Networks*, *28*(2), 635-690.
14. Subathra, G., Antonidoss, A., & Singh, B. K. (2022). Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme. *Security and Communication Networks*, *2022*.
15. Deepak, N. R., & Balaji, S. (2016, April). Uplink Channel Performance and Implementation of Software for Image Communication in 4G Network. In *Computer Science On-line Conference* (pp. 105-115). Springer, Cham.
16. Thiagarajan, R., Balajivijayan, V., Krishnamoorthy, R., & Mohan, I. (2022). A robust, scalable, and energy-efficient routing strategy for UWSN using a Novel Vector-based Forwarding routing protocol. *Journal of Circuits, Systems and Computers*.
17. NR, D., GK, S., & Kumar Pareek, D. (2022). A Framework for Food recognition and predicting its Nutritional value through Convolution neural network.
18. Thanuja, N., & Deepak, N. R. (2021, April). A convenient machine learning model for cyber security. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 284-290). IEEE.
19. Shanmugam, P., Venkateswarulu, B., Dharmadurai, R., Ranganathan, T., Indiran, M., & Nanjappan, M. (2022). Electro search optimization based long short- term memory network for mobile malware detection. *Concurrency and Computation: Practice and Experience*, *34*(19), e7044.
20. Deepak, N. R., GK, S., & Bhagappa (2021, Nov). The Smart Sailing Robot for Navigational Investigation is Used to Explore all the Details on the Zone of the Water Pura. Indian Journal of Signal Processing (IJSP), 1(4).
21. Deepak, N. R., & Thanuja, N. Smart City for Future: Design of Data Acquisition Method using Threshold Concept Technique.
22. Kiran, M. P., & Deepak, N. R. (2021, May). Crop prediction based on influencing parameters for different states in india-the data mining approach. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1785-1791). IEEE.
23. Deepak, N. R., & Balaji, S. (2015, December). Performance analysis of MIMO-based transmission techniques for image quality in 4G wireless network. In *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-5). IEEE.