International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

A Peer-to-Peer File Storage System Using Blockchain and Interplanetary File System

Suman Mann[1], Harshit Chaudhary[2], Aryan khatri[3], Ritik Malik[4], Yatin Gupta[5]
[1] Associate Professor, MSIT, New Delhi, India
[2,3,4,5] B.Tech Student, MSIT, New Delhi, India

ABSTRACT: People's lives have been profoundly impacted by the headway of innovation which has worked on their lives from each viewpoint. Clearly, innovation assumes a significant part in each circle of life and information stockpiling and sharing is a significant part of it. Current information sharing and storage devices depend on trusted third parties (TTP) and because of the contribution of third parties, such frameworks need straightforwardness, security, trust and strength. To solve these issues, this paper proposes a blockchain-based secure information sharing application by consolidating the highlights of IPFS and Ethereum. In this proposed scheme ethereum blockchain, decentralized storage, encryption and IPFS are combined to build an application that maximizes the technological resources and provide with an effective storage website ,Ethereum blockchain, decentralized capacity, encryption, and InterPlanetary File System are consolidated to assemble an application that boosts the innovative assets and gives a viable storage site. To carry out the proposed situation, smart contracts are written in solidity and sent on the nearby Ethereum test network. The proposed plot accomplishes security, transparency, legitimacy of owner, access control and nature of information.

KEYWORDS: Blockchain, Decentralized, Ethereum, IPFS, Smart Contracts, Transparency.

1. INTRODUCTION

Blockchain Technology (BT) has been a massive hit among the tech enthusiasts over the last few years. [9] Blockchain is known as a global record to provide immutability and store the transactions in a chain of blocks and is being researched uninterruptedly. Ethereum[1] is a blockchain platform with its own programming language, called Solidity and is a decentralized public ledger for verifying and recording transactions. Ethereum consists of smart contracts (SCs)[10] that are programmable in different programming languages such as solidity.

Trust and security are the most prominent features of blockchain, which is ensured by no involvement of third parties. Nakamoto introduced a peer to peer currency that is known as bitcoin in 2008 [1]. This serves as a way to facilitate peer to peer transactions. Later, Nakamoto published a paper which laid the foundation of peer to peer transactions[4] using bitcoin. In today's world, blockchain is being utilized in different fields, like the internet of things (IoT), cloud, data handling, health care, and many more.
The major underscored obstacles in data trading and storage is regarding misinterpretation and misuse of data and it is due to data sharing approaches that are still lagging behind in providing trust and security, that is being established among the tech community. To solve this problem, different strategies are being proposed, for example, securing the profiles of every individual and specific access to the data instead of making all the data open access. Even these strategies are not full proof in providing stability to data, traceability regarding data usage and trust in the process of data sharing. That is why there developed a need and urgency to use blockchain in the backend of storage websites.

In this proposed solution, a blockchain-integrated file storage application for document sharing to facilitate peer to peer collaboration in a secure, and decentralized manner, with no involvement of a centralized trusted entity or third party is proposed. This solution utilizes a blend of new technologies that primarily consists of (InterPlanetary File System) IPFS[3] that is used to store data with a high integrity and accessibility to all. The proposed solution provides privacy and security that cloud storage cannot achieve because all the files are accessed through content-based searching rather than location-based searching in the cloud.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

2. RELATED WORK

Over the past few years decentralized technologies like blockchain and IPFS[21] are considered as fundamental technologies in redefining the future of data storage and data sharing, due to which various researchers and industrialists are taking part in creating a decentralized trust based and censorship resistant model[11].

Due to the advent of different technologies that are making the world more connected than before, the demand for data storage is at an all-time high. To meet these storage demands various cloud based centralized storage[3] solutions have emerged like iCloud, Google Drive and dropbox etc. But apart from some free amount of data storage[22] users have to pay a monthly fee. However this approach is inefficient and unsustainable in the long run. To provide an efficient way of solving this problem Vitalik Buterin[4] has provided a way of storing data in a decentralized way using Ethereum blockchain. According to Vitalik using ethereum smart contracts a decentralized file storage ecosystem[16] can be developed where users can be incentivized by renting out their hard drives and unused space.

Blockchain is considered to be the most important technology in paving the way towards a decentralized and censorship resistant future. To explore different possibilities of blockchain Min Xu, Xingtong Chen & Gang Kou[15] reviewed the current academic research conducted by different organizations on blockchain. They delved deeper in various research themes of blockchain and provide a pragmatic approach of using blockchain. They conduct a thorough analysis of different business and economic aspects of blockchain. Apart from this, different technical terms related to blockchain like smart contracts, cryptography and proof of work are also discussed. In the modern era of decentralization there have been numerous attempts of creating a distributed file storage system. Among these some have been extremely successful. And one such technology is the InterPlanetary FileSystem(IPFS)[3]. In his research Juan Benet came up with a peer to peer file system[4] that attempts to overcome the problems faced by traditional centralized file systems. It is similar to how torrenting works. BitTorrent is a great example of how a decentralized file system could work[16]. IPFS follows content based addressing to uniquely identify different files present in the network. Juan states that IPFS forms a merkle tree[23] like structure and it combines a distributed hash table for maintaining the addresses of different files.

3. WHY ETHEREUM?

Centralized systems have been targeted multiple times in recent years and a list of some prominent attacks have been organized by us

Following are some of the major ones that caused the most commotion and harm.

1) The Bangladesh bank heist is considered to be the most astounding one, as it managed to by-pass the most secured SWIFT banking system. The gang managed to make $81 million from the attack!

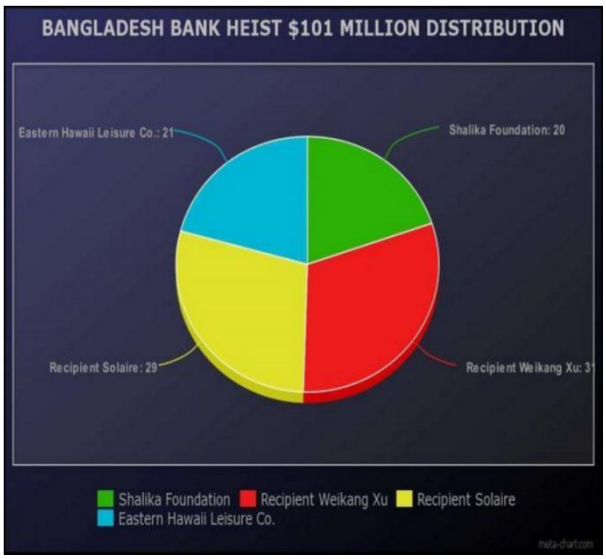

Figure 1: The money trail of Bangladesh Bank heist

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

2) Mafia Boy(2000)- Mafia Boy virus was a dos(denial of service) attack that was developed by a teenager in Canada and it caused immense damages to some big conglomerates.

Ethereum is a non-proprietary blockchain platform which allows users to build a range of decentralized and distributed applications[5]. Similar to Bitcoin, it is a platform made and used by various open source communities worldwide. In contrast to Bitcoin protocol, adaptability and versatility were kept in mind while designing ethereum. It is simple and easy to create new applications on the Ethereum platform, and the new Homestead release helps in providing security to anyone using those applications. Ethereum integrates different technologies and features and also introduces different innovations and modifications of its own.

Ethereum comprises different accounts and all accounts have a state associated with them. Ethereum maintains a global state of all these accounts. These accounts are divided in two types:

- Contract Accounts, these contain smart contracts which are executed by EOAs.
- Externally Owned Accounts (EOAs),these are associated with private keys and public addresses.

Ethereum Accounts:

The states in ethereum are made from accounts, and every account has an address of 20 byte and different state transitions. An account in ethereum constitutes of these four fields:

- Account's storage: (by default null)
- Nonce: It is defined as a counter which is used to ensure every transaction is unique.
- Account balance of current account
- Contract code of the account, if present

"Ether" is known as the main internal Ethereum's crypto-fuel, which is used for handling transaction costs.

Figure 2: Decentralized system of Blockchain

3.1 LIFECYCLE OF A TRANSACTION IN ETHEREUM

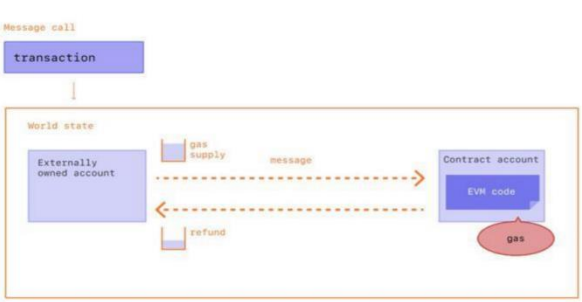

Figure 3: Lifecycle of a transaction in ethereum

In Ethereum during any state transition following process is followed by every transaction on ethereum:

1. Firstly the validity and structure of a transaction is confirmed by validating that the given signature and nonce matches the nonce in the sender's account and in case of any issues an error is generated.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

2. After that GAS PRICE is used to calculate transaction fee. After this the sender's account address is determined using the given signature. Then the sender's account balance is reduced accordingly, along with the increment in nonce. In case of insufficient account balance an error is returned.
3. After this if the transaction specifies a receiver then we are dealing with a message call otherwise it is a contract creation. To start a transaction some initial amount of START GAS is initialized and some amount is reduced to pay for bytes in transaction.
4. Check if the receiver has an associated contract code. If it is not the case, the message call was successful. Then the contract code is executed until completion or it runs out of gas.
5. If there is a failure in a transaction due to the sender not having enough, all state changes are reverted except the payment of the fees and the same is deposited to the miner's account.
6. In case of a successful transaction fees for any remaining gas is returned to the sender and fees for gas consumed is given to the miner.

4. PROPOSED MODEL

This model allows users to store and retrieve files in a censorship resistant fashion where all the files are stored in a decentralized way in the InterPlanetary File System(IPFS). The following diagram depicts the workflow of the proposed model:

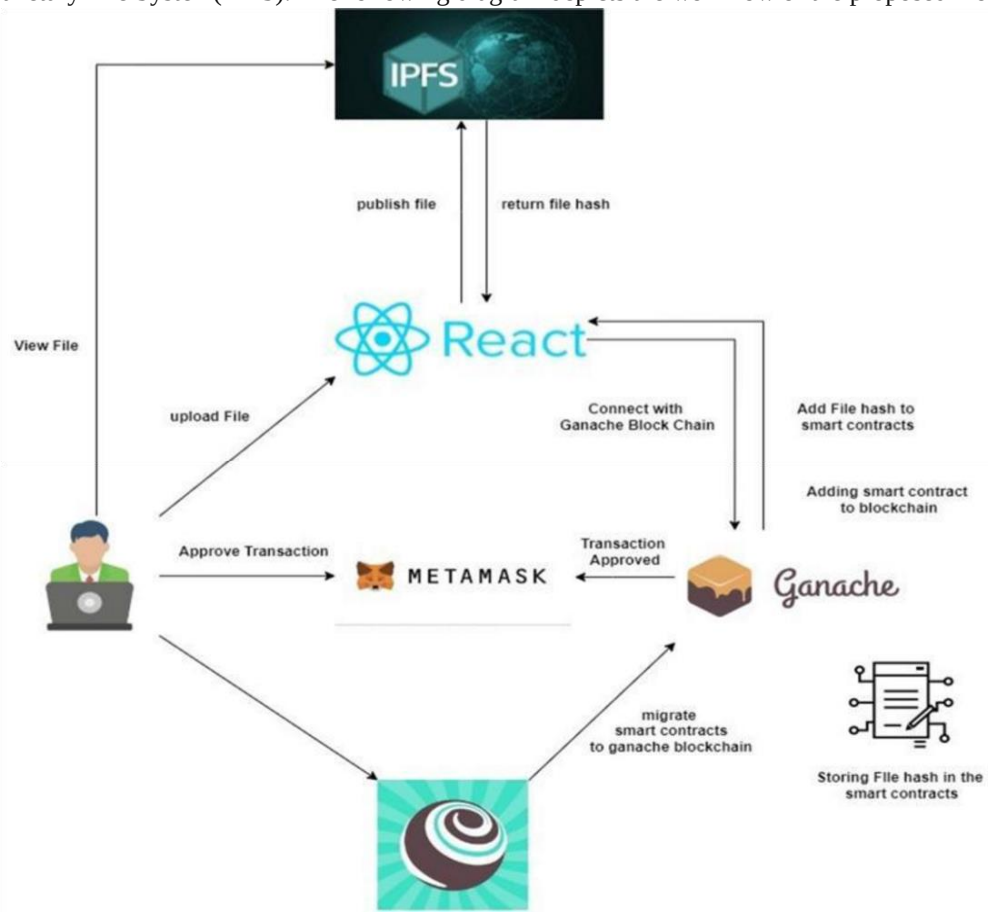

Figure 4: Flowchart of the working model for the proposed application

In traditional apps a web browser communicates to a centralized server which connects to a database to store and retrieve files but in our model a browser will use a cryptographic wallet to communicate to the ethereum blockchain which will contain aur smart contracts and we will be using smart contracts to store the location of files which are stored on the interplanetary file system.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

Users will directly interact with a web application built using Reacts and this app will interact with the ethereum blockchain as well as the InterPlanetary File System(IPFS). Whenever the web application is opened first all smart contracts are loaded onto the ethereum blockchain. Whenever a user uploads a file our app will interact with IPFS which will return a file hash and this hash will be stored on a smart contract which will be added to the ethereum blockchain.

5. IMPLEMENTATION

The proposed solution uses smart contracts to store the location of files present in the InterPlanetary File System (IPFS) [3]. Solidity is used to write smart contracts in an efficient way which are later stored on the Ethereum blockchain.

File Upload Smart Contract Overview:

5.1. File Structure

The File Upload smart contract provides the functionality of storing different file hashes on the ethereum network. Each file has a predefined structure. This structure consists of data such as file size, file hash(as returned by the IPFS),file type, file description and file name. As soon as the Contract is created, the constructor is triggered and the aforementioned values are mapped to the created object which is of type File(structure defined in smart contract). The Smart Contract maintains a File Count which gets incremented whenever a new File is added. FileCount is used as an ID management system to provide different IDs for each file and to prevent overriding of data.

```
struct File{
 uint fileId;
 string fileHash;
 uint fileSize;
 string fileType;
 string fileName;
 string fileDescription;
 uint uploadTime;
 address uploader;
}
```

5.2. Error Handling

The proposed system necessitates error free uploading of files. As mentioned above every file must adhere to a predefined structure and whenever a user uploads a file, before uploading this file to IPFS all the required parameters are checked. This is done by using the ‘require’ function of solidity which ensures validity of conditions which cannot be detected before execution.

As a file is uploaded on the IPFS it returns a file hash along with some other metadata which is sent to ethereum smart contracts where a file object is created and all the metadata along with the file hash is mapped onto this object. To handle the mapping and uploading of this file on ethereum network a function is used which triggers an event. This event appends the newly created block or object onto the ethereum network.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

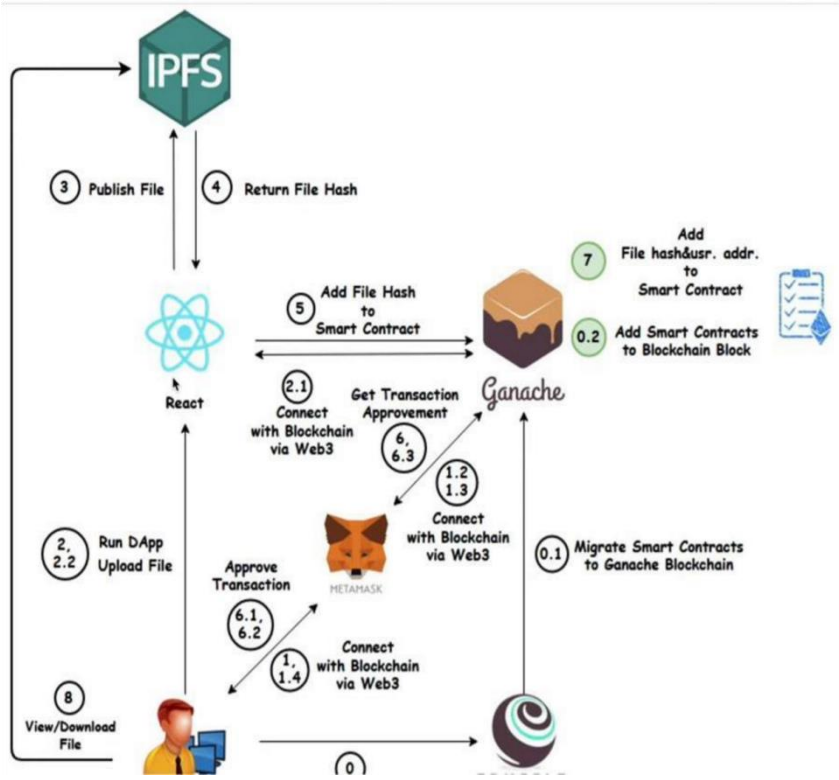

Figure 5: Technical diagram of the implementation of application

6. EXPERIMENTAL ANALYSIS

The proposed paper provides a solution to the problems faced by cloud storage. A series of Experimental Analysis is drawn in order to compare Blockchain-based file storage and centralized cloud storage.

S. No.	Parameter of Analysis	Blockchain-based file storage	Centralized Cloud Storage
1.	Security	More secure as the users' files are broken and distributed across multiple nodes on the network to avoid a single point of failure.	Less secured as data is stored at a particular single system called central storage system , so there is a single point of failure.
2.	Privacy	As the data is spread across a large network of nodes, it isn't possible to steal it by attacking the entire network of nodes as it is impractical.	The data can be altered or lost as the host company has the authority to control or disclose the data to any third parties.
3.	Censorship	No risk of censorship as there is no involvement of third parties in controlling the data.	Susceptible to censorship as the data is controlled by a central authority.
4.	Liveliness	Liveness is a property with which a system will keep running even if certain components of it are not performing up to par. Here, even if one of the nodes goes down, the rest of the network will be more than capable of making up for the slack.	In a centralized cloud storage, if the server is down for whatever reason, the entire system goes down and this compromises with the liveliness of the application.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

7. RESULTS

Proposed application uses decentralized storage, i.e Blockchain technology and IPFS for secured storage and sharing of data. The results obtained after successfully implementing the application are full of positive outcomes. Following points brief the parameters that have been a result of successful implementation of the application :-

i) Safe and secure - Unlike centralized storage systems which have a single point of failure, in a decentralized storage system files are distributed across multiple nodes of a network.

ii) Privacy - Proposed application ensures protection of data without any reliance on third parties.

iii) Complete control over the data- one of the main problems with the cloud storage service is that the data is handled by third parties. These parties are only motivated to make profit out of the data that you provide But in the proposed application, access rules are set by the data owners, avoiding the release of data to any unauthorized party.

iv) Faster: Using peer-to-peer technology, our application cuts out the middleman. This notably speeds up transmissions, especially when compared to peak times as everybody will be using the centralized cloud at the same time.

8. CONCLUSION

In this proposed paper, a blockchain-integrated secure data sharing and storage of digital assets(data) is presented. The main objective of this proposed paper is to provide a censorship resistant and secured environment for storing and sharing of data. Combining the features of blockchain-based storage and IPFS provides the solution. IPFS returns data hashes that are encrypted and stored in smart contracts, so that a user who has a cryptographic wallet can access the data. Since the data is stored in an encrypted manner the safety and authenticity of user data is ensured.

The main issue with cloud storage is that integrity and security of data is not guaranteed but blockchain ensures security of data because it does not rely on any third-party trusted centralized authority.

Blockchain is based on principles of decentralization which helps in preventing a single point of failures. But since handling large files on blockchain can reduce speed and efficiency of the network we have leveraged the benefits of the InterPlanetary File System. It relies on cryptographic hashes which we have stored on our ethereum blockchain. Users can access their files from IPFS by getting the location from smart contracts stored in their ethereum accounts which are linked to their cryptographic wallets.

In future, our focus will be to provide access control sharing where users can share data with selected parties on the blockchain.

REFERENCES

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Revie ,2008.
2. Mann, Suman., Gosain, Anjana. and Sabharwal, S. OO Approach forDeveloping Conceptual Model for A Data Warehouse. Journal of Technology and Engineering Science, 1(1).2009.
3. Gosain, A., & Mann, S.. Object oriented multidimensional model for a data warehouse with operators. International Journal of Database Theory and Application, 3(4).2010
4. Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3.37,2014.
5. J. Benet, “Ipfs-content addressed versioned p2p file system”, 2014
6. D.Vorick and L.Champine, Sia,”Simple Decentralized Storage”,Business Transformation through Blockchain, 2014.
7. Wood, Gavin. "Ethereum: A secure decentralized generalised transaction ledger." Ethereum project yellow paper ,2014.
8. Gosain, Anjana, and Suman Mann. "Empirical validation of metrics for object oriented multidimensional model for data warehouse." Internationaljournal of system assurance engineering and management 5, no. 3 2014.
9. H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search", IEEE World Congress. Services (SERVICES), 2017.
10. J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases challenges and solutions", Symmetry Journal, vol. 9, no. 8, 2017.
11. Peck, Morgen E. “Do You Need a Blockchain?” IEEE Spectrum: Technology, Engineering, and Science News, IEEE Spectrum, 2017
12. T. Aste, P. Tasca and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry", Computer Journal, vol. 50,2017.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 05 Issue 02 February 2022
DOI: 10.47191/ijcsrr/V5-i2-34, Impact Factor: 5.825
IJCSRR @ 2022
www.ijcsrr.org

13. Eliza Mik, “Smart contracts: terminology, technical limitations and real world complexity”,Law Innovation and Technology,2017
14. Zibin Zheng; Shaoan Xie; Hongning Dai; Xiangping Chen; Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”,IEEE, 2017.
15. D. Macrinici, C. Cartofeanu and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study", Telematics Inform, vol. 35, 2018.
16. Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang,”Blockchain challenges and opportunities: a survey”,International Journal Of Web and Grid Services,2018.
17. W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System", IEEE Access, vol. 6, 2018
18. Xu, Min, Xingtong Chen, and Gang Kou. "A systematic review of blockchain.",Financial Innovation 5.1,2019
19. P. Jiang, F. Guo, K. Liang, J. Lai and Q. Wen, "Searchain: Blockchainbased private keyword search in decentralized storage", Future Gener. Comput. Syst., vol. 107, 2020.
20. Stephen Chan, Jeffrey Chu, Yuanyuan Zhang, Saralees Nadarajah, ”Blockchain and Cryptocurrencies”,Journal Of Risk And Financial Management,2020.
21. Mann, Suman, Tanya Jain, and Aakash Vyas. "The Blockchain Revolution: Paradigm Shifts in Traditional Voting Practices." InternationalJournal of Computer Applications 975,2020
22. Mann, Suman, and Meenu Siwach. "Data Model Quality Metrics of Data Warehouse: A Survey." Proceedings of the International Conference on Innovative Computing & Communications (ICICC). 2020.
23. Mann S, Siwach M, Dalal S, Poonia SK.”Land Holding Using Blockchain.”,International Journal of Current Science Research and Review,2021.

Cite this Article: *Suman Mann, Harshit Chaudhary, Aryan khatri, Ritik Malik, Yatin Gupta (2022). A Peer-to-Peer File Storage System Using Blockchain and Interplanetary File System. International Journal of Current Science Research and Review, 5(2), 582-589*