International Journal of Mathematical, Engineering and Management Sciences
Vol. 7, No. 6, 844-858, 2022
https://doi.org/10.33889/IJMEMS.2022.7.6.053

AnonChain: A Secure File Sharing Framework using IPFS Integrated Blockchain

Shamama Anwar
Department of Computer Science and Engineering,
Birla Institute of Technology, Mesra, Ranchi, 835215, India.
E-mail: shamama@bitmesra.ac.in

Ruchika Tulsyan
Department of Computer Science and Engineering,
Birla Institute of Technology, Mesra, Ranchi, 835215, India.
E-mail: truchika12@gmail.com

Souvik Saha
Department of Computer Science and Engineering,
Birla Institute of Technology, Mesra, Ranchi, 835215, India.
E-mail: ahansaha@gmail.com

Sudip Kumar Sahana
Department of Computer Science and Engineering,
Birla Institute of Technology, Mesra, Ranchi, 835215, India.
Corresponding author: sudipsahana@bitmesra.ac.in

(Received on June 25, 2021; Accepted on January 25, 2022)

Abstract
Over the last decade, data sharing has become eminent in each aspect of the daily routine chores of industries and research alike. Traditionally, all data sharing platform depend on trusted third parties (TTP), owing to which they lack trust, security, immutability and transparency. But, with the advent of blockchain technology, the data sharing has got a whole new dimensionality. Blockchain is a distributed and decentralized ledger that records the source of a digital resources. The secure features of blockchain have helped it gain popularity and application in a variety of domains including sustainable manufacturing. It can aid in customer and product tracking, supply chain, quality checks, etc. Blockchain can further strengthen how products can be designed, engineered, manufactured, dispatched and tracked in the revolutionized Industry 4.0 initiative. All these activities involve sharing of voluminous data. Hence, this paper presents an efficient data-sharing system which takes the advantage of the transparency as well as the security provided by a blockchain. AnonChain (Anonymous Chain) is a file sharing platform that integrates Inter Planetary File Sharing (IPFS) with the blockchain technology to provide secure and anonymous file sharing.

Keywords- Decentralization, Blockchain, Peer-to-peer, IPFS, Anonymous chain, Encryption, Sustainability, Industry 4.0.

1. Introduction

Data sharing nowadays has become a normal part of our lives. From industrial usage to research and individual use, a large amount of data is shared daily. Data is shared in the form of emails, messages, research data, scientific results, literature, images, videos and so on. Data sharing has become one of the most fundamental steps to gain maximum benefit from research innovations. The great ease at which massive data can be shared and used from different locations have prompted the research consortiums to explore techniques for developing efficient data sharing systems. Initially, when the data sharing concept was at its nascent stage, it was mainly done through sharing of physical storage devices such as USB's, Floppy Disks, Hard Disks, etc. This process of sharing data was inefficient as it required the users to

manually share devices and was thus, infeasible for frequent sharing and for distant users. With the advent of networking, data became more accessible and data sharing over network became a common trend. However, data sharing through public network came with its own set of pitfalls. Although this annihilates the need for physical media transfer, it still has a major concern as there are intermediaries involved in sharing a centrally utilized infrastructure. The data faced a major security concern of being hacked or modified. Data mishandling and manipulation is still a major concern in data sharing. The solution to these concerns needs clarity so as to eliminate the threat to security, trust and privacy. This led to research initiatives for generating more safe procedures for sharing the data, and hence the advent of trusted third-party data sharing techniques. However, when data sharing is done through a third party, it becomes important to guarantee the credibility and authenticity of data and also ensure reliable transmission of data (Naz et al., 2019). Cloud servers came into existence and accessing the information from the internet meant interacting with the cloud servers, which store massive data, but has a centralized infrastructure, which comes along with its own set of risks such as data breaches, invasion of privacy, non-transparency, data ownership problems. Hence, the issue of trust and guarantee against data theft still is a major concern with third party initiatives. Moreover, most of the time, data owners lack complete control over the access and use of data (Khatal et al., 2021). Also, these techniques have many issues with distributed systems across multiple sites (Miltchev et al., 2008).

To eliminate these challenges associated with a third-party transfer, blockchain came into existence. It is a new trend in the world of information technology. Currently, it is used in a wide set of domains like healthcare, information security, data trading, Internet of Things (IoT) and many more because of its many striking features. It is an elementary yet inventive way of communicating between entities in a fully automated and safe manner. Moreover, with the help of blockchain, one can ensure the transparency of transactions as a public blockchain serves as a shared and immutable ledger and the information is available to anyone. A blockchain is a decentralized distributed database existing on multiple computers at the same time. Each block stores a timestamp, nonce, some data and the hash (link) of the previous block, forming a chain-like structure (Khatal et al., 2021). The chain keeps on growing as new blocks are added thus forming a blockchain. A cryptographic hash function is used to link the blocks, thus forming a chain. The first block in the chain is called the genesis block and it is the starting of the blockchain (Chen et al., 2019b). All the connected nodes in the peer-to-peer network get a copy of the complete blockchain. Each block once created calculates a hash and includes it in its header. Any changes made in the block will automatically alter the hash as well. Hashes help to detect any changes in blocks. Whenever a new block is created, it is sent to each node within the blockchain system. Each node then verifies the block and checks whether the information stated in it is correct. A consensus protocol is created by all the nodes in the blockchain network. A consensus protocol is a set of network rules, and if everyone abides by them, they become self-enforced inside the blockchain. This makes blockchain technology cryptographically secure and immutable by eradicating any third party involvement. Hence, the blockchain based data sharing system has a promising application and eliminates the security concerns of the other techniques. Data storage on the blockchain has a cost model. This is the only evident limitation for handling large data in blockchain. The limitation is in the storage capacity and processing power of network nodes. Large files cannot be efficiently stored on the blockchain and it becomes bloated if the data is replicated on all nodes and a lot of storage space is required for the same. If all the data (files) are replicated on the node, then mining the nodes also becomes expensive. These concerns gave rise to a doubt in the use of blockchain for sharing large files. To overcome these limitations there are several off-chain data storage solutions that have been designed to be friendly to the blockchain such as FileCoin, Storj, Sia and IPFS. FileCoin introduced how to store and retrieve data while keeping miners focused on storing data. Miners could earn FileCoin by providing storage to clients and clients spend these FileCoins hiring miners to store or distribute data. But this method did not fully eliminate the use of proof of work or reliance on another consensus protocol. It also needed scalability

improvements (Benet, 2017). Storj, on the other hand focuses on storage solutions rather than distribution and quality of service (QoS) is one of the concerns of the Storj team (Wilkinson et al., 2014). Sia, although a fully decentralized system requires a deposit of Sia coins to rent out space similar to FileCoins. It also has scalability issues (Vorick and Champine, 2014).

To overcome this limitation, the paper uses the Inter Planetary File System (IPFS) along with blockchain technology to enable a more efficient data sharing system. IPFS is a versioned file system that can store and track file versions over time. It is a hypermedia protocol and peer-to-peer network for storing and sharing data in a distributed file system. It uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices and also uses Distributed Hash Tables (DHT). In these table, the data is scattered over a network of computers and is coherently synchronized to enable efficient access and lookup between nodes (Naz et al., 2019). When a file is added to IPFS, the file along with all the blocks within it, is given a unique fingerprint called a cryptographic hash. Each node stores only the content it is interested in, plus some indexing information that helps figure out which node is storing what. When a file is looked up to view or download, the network finds the nodes that are storing the content behind that file's hash. There is no requirement of remembering the hash, though every file can be found by human-readable names using a decentralized naming system.

The goal of the current work is to develop a model that mainly operates on the concept of decentralization while maintaining the data integrity and security. In recent times, blockchain based applications have always proved to be secure and hence, are trusted by the users, making researchers more curious about the blockchain technology. The methodology discussed in the paper eliminates all the problems involved in a traditional centralized data sharing system, using the decentralized blockchain technology. The system aims at developing a data (file) sharing app, AnonChain (Anonymous Chain) which is a IPFS integrated blockchain-based system where the files can be shared securely and anonymously without the need for a third party which is also tamper free and maintains a complete log of all the files shared giving users a sense of trust, security and transparency. The contribution of this paper can be highlighted as:

- A blockchain based decentralized file storage application.
- An anonymous file sharing platform backed by the IPFS technique.
- There is no third party involvement in file storage or sharing.
- Provides a greater sense of trust among users as the application is secure and transparent.

The remainder of the paper is organized in three sections. The next section discusses about some prominent literature on the blockchain and file sharing system. Section 3 discusses the methodology used and its implementation in details. Finally, section 4 concludes the work with some directions for the future improvement in the current work.

2. Literature Review

The roots of the blockchain technology lies in a paper released by Haber and Stornetta (1990), explaining the importance of time-stamping a document (Haber and Stornetta, 1990). They introduced techniques which made altering a document's timestamp impossible i.e., a document cannot be back-dated or forward-dated. One of the solutions proposed was to include bits of the previous document in the next document, thereby linking both the documents cryptographically. The time-stamping concept has now become an important aspect in the blockchain structure. Many believe that blockchain was originally created by Nakamoto (2009). After creating the concept of blockchain, Satoshi also created a blockchain based application called 'Bitcoin'. He coined the term 'electronic coin' and defined it as a chain of digital signatures which are cryptographically linked together. Bitcoin made it huge on the market and is still considered as one of the best cryptocurrencies (Nakamoto, 2009). After the Bitcoin release, the blockchain

technology became widely popular among researchers and in general, the public as well. Since, Satoshi was the one who invented Blockchain and Bitcoin as well, people generally confuse both being effectively the same thing, which is not the case. In the beginning era of blockchain application or usage the concentration was on crytocurrency. Blockchain such as bitcoin (Crosby et al., 2016) and Ethereum (Wood, 2014) were evolved as fundamental technologies of cryptocurrency. With the success of the security mechanism in blockchain it slowing began finding applications in various fields such as biomedical and healthcare (Ekblaw et al., 2016; Kuo et al., 2017), industries (Friedlmaier et al., 2018; Mohamed and Al-Jaroodi, 2019), manufacturing (Abeyratne and Monfared, 2016; Turgay, 2018), construction engineering (Wang et al., 2017), supply chain management (Saberi et al., 2019; Das et al., 2021), voting systems (Kshetri and Voas, 2018; Yu et al., 2018) to name a few. A very notable application worth mentioning is the use of blockchain in the Industry 4.0 scenario. Various researchers have emphasized on the recognition if key role players in sustainable manufacturing commonly known as enablers (Jamwal et al., 2021a). Similar framework is also in need to achieve sustainability in both small and large scale industries (Jamwal et al., 2021b) and also to study the impact of sustainable manufacturing that focuses on minimizing negative environmental affect (Jamwal et al., 2021c). The impact of data sharing is unprecedented in such a case as it has to be timely and trustworthy. Blockchain based application for data/ file sharing will prove to be boon in this sector, which is further discussed in this paper.

Another major application of blockchain is in data sharing which this paper intends to explore. File sharing is an inherent part of any organization and specifically if it needs to be shared across geographically far locations, a more efficient and quick sharing mechanism was needed. Blockchain has become a new face for such scenarios as it provides a more secure and robust way to share vital data. Some of the initial work in this domain included more theoretical concepts. A system comprising of five different roles: storage provider, data owner, user, miner and re-encryption proxy was proposed in (Cui et al., 2018). Each node in the proposed system can play at least one role. In case of multiple roles, a node cannot be a storage provider and a proxy at the same time. The data owner could upload the encrypted keys to the proxies and the encrypted files to the storage providers. The blockchain included file reading and writing transactions for verification of access control polices to manage user access. However, the paper lacked an implementation of the same. A similar model with two components was proposed by (Zikratov et al., 2017): the user side and the server side. The user side component was basically a web-based application where the user had accessibility to handle the file. The server side dealt with session management including authentication.

More further researches in this domain led to the conception of a decentralized file storage system. A blockchain based application which aims to secure academic research to prevent the leakage of vital research work was proposed in (Rajalakshmi et al., 2018). Smart contracts and IPFS technology are combined to make this application. But in this paper as well, the users have to go through a registration and authentication process before they use the application. Since, the blockchain focuses on decentralization; going through a registration and sign up system gives away some part of the user's privacy i.e. the user can not completely remain anonymous. FileShare is another decentralized application (dApp) which is based on Ethereum. FileShare aims to share files and provide data provenance. It mainly uses Ethereum blockchain (Smart contracts specifically) and IPFS for its functioning. But to use this application, one must sign up and create an account for unique identification of users, hence, a third party is involved which the users have to trust (Khatal et al., 2021).

In the above referenced papers, the involvement of a third party makes users question the security of the shared information and the privacy of the user's credentials. This is one of the major disadvantages of these papers. Our aim is to give the users complete power over the application. Application oriented file sharing systems have also been discussed in the literature. Since medical data sharing involves sharing a huge and

varied amount of data, it is an ideal implementation of the data sharing platform. A medical data sharing model using blockchain was proposed in (Chen et al., 2019a). Patients have multiple electronic medical records nowadays for different hospitals. The application focuses to keep all the fragmented data of patients in a single place so that multiple records for a patient are not created and the patient has control on the records that s/he provides to the doctors. A similar medical data sharing platform was also presented in (Chen et al., 2019b). The proposed storage and sharing scheme do not depend on any third-party and no single party has absolute power to affect the processing. The paper described the permissions of three types of transaction and introduced a service framework for sharing medical records to describe the process of personal medical data management.

The use of IPFS in data storage system using blockchain is a revolutionizing concept. Some prominent work in this field has been highlighted here. A blockchain-based solution and framework for document sharing and version control to facilitate multi-user collaboration and track changes in a trusted, secure environment was proposed by (Nizamuddin et al., 2019). The system proposed was decentralized and had no involvement of a centralized trusted entity or third party. This solution was based on utilizing Ethereum smart contracts to manage the data flow. The method made use of the benefits of IPFS (Inter Planetary File System) to store documents on a decentralized file system and also automated interactions between multiple actors. In IPFS based systems, the miners deposit the transaction data into the IPFS network and pack the returned IPFS hash of the transaction into the block (Zheng et al., 2018). A similar work that addresses the issues of blockchain while handling massive amount of data was presented in (Sari and Sipos, 2019; Vimal and Srivatsa, 2019; Kumar et al., 2020). Most of the work referenced above make use of Ethereum for implementation (Nizamuddin, 2018; Steichen et al., 2018).

The paper proposes a technique for decentralized file sharing by exploiting the features of the blockchain and eliminate all the challenges mentioned in the preceding literature. The paper combines blockchain with IPFS technology. Unlike Ethereum, in IPFS users do not have to register or create an account to start sharing the files, thus making it anonymous. There is no sign-up process which means users can remain completely anonymous while sharing the files on the network. Users also need not share their real credentials to upload the files, thereby ensuring that none of the users can be traced over the internet. This helps in maintaining the anonymity of the users. This also removes the third party involvement and their access to user data. Hence, it offers the same features of the blockchain through a much simpler system.

3. Anonchain: The Proposed File Sharing Network Implementation

The proposed framework aims to provide a file sharing platform with the accessibility and security features of a blockchain, integrated with the offline storage feature of IPFS. The system also complies to the other features of blockchain like enhanced security, distributed ledger, decentralized technology and consensus protocol to name a few. Unlike the client server model, there is no central authority controlling the blockchain and the group of nodes forming the blockchain collectively maintain the network. A peer-to-peer network is established between the nodes which follow the consensus protocol to make the right decisions. An enhanced security is achieved in the blockchain using hashing and encryption techniques. Every node in the blockchain's peer-to-peer network also stores a copy of the complete encrypted blockchain (distributed ledger of data). This distributed ledger is updated every time a file is uploaded to the network to reflect any updates that occur, preventing any data loss in case any particular node's data gets corrupted, thereby, increasing the availability and immutability of the network. The interested readers may refer to (Kim et al., 2018; Stephen and Alex, 2018; Kim, 2020; Subha, 2020) for further reading on the same. The proposed model aims at providing a data (file) storage facility which is decentralized and also keeps the user anonymous, hence the name AnonChain. The system basically consists of three main modules: (i) Creating a blockchain; (ii) Uploading a file; (iii) Downloading a file (Figure 1).

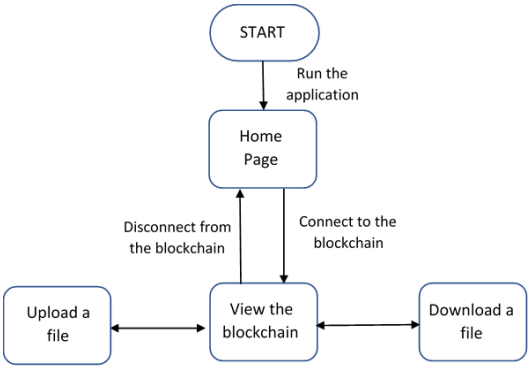


Figure 1. Proposed workflow.

The blockchain creation requires creating blocks which stores all the shared information and is visualized as a series of cryptographically linked blocks. Each block has a defined structure and changes in any one block is reflected in the next one via hashing (Treiblmaier, 2020). One can view the complete blockchain and all its blocks, but the information shared is encoded using a hashing algorithm. Using a robust encryption algorithm ensures that only those authorized can view the decoded file contents. Files can be uploaded by any user connected to the blockchain. The uploader decides on a secure file key, to restrict the 'authorization of access' so that only intended viewers can view the file. Files can further be downloaded by any connected user on the blockchain. But if the user does not have the correct key, he would not be able to see the correct file. He/She will see only gibberish. Only those with the correct key and the correct hash of the shared file will be able to access it from the blockchain, making it extra secure. Both the uploader and the receiver as well do not need to register or login for using the application making the users completely anonymous. A detailed description of the workflow follows.

3.1 Creation of Blockchain in a Peer - to – Peer Network

In AnonChain App, as soon as the user opens the web app, he/she views the home page of the application. This page gives a brief summary about the application's working and the way it is supposed to be used by the user. There is a 'Connect to Blockchain' button which allows the users to get connected to the AnonChain's peer-to-peer network so that they can start sharing the files anonymously. The main page of the App is included in Figure 2. Figure 2(a) and 2(b) shows the homepage of the application (App) developed.

3.1.1 Block Structure

The first block is then created which is called the genesis block (Bhadoria et al., 2020) and it has the following structure (Figure 3):

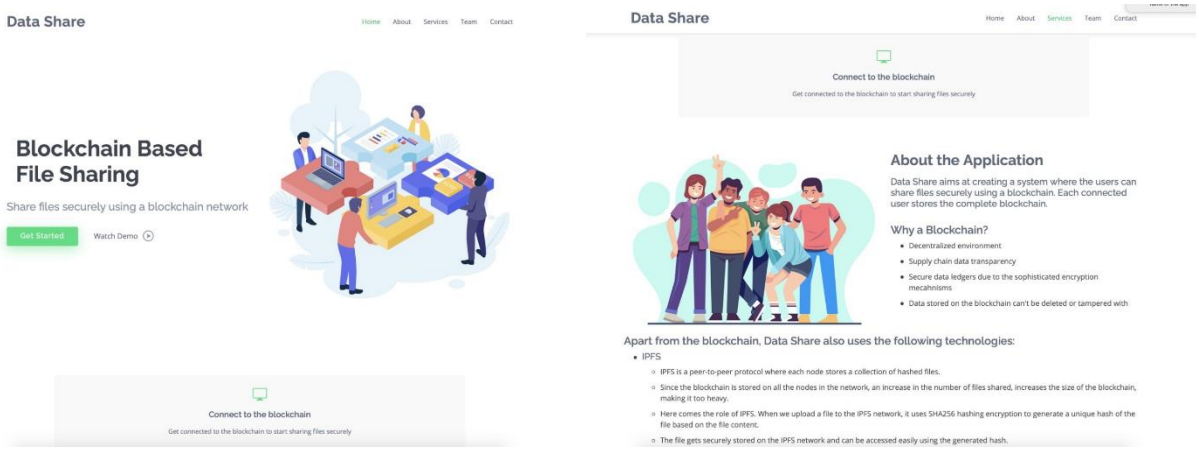
- ***Block number:*** Simply displays the index number of the block. Block 0 refers to the genesis block.
- ***Timestamp:*** This field indicates as to when the block was created and added to the blockchain.
- ***Proof:*** Also called a nonce, it stands for "number only used once" which is a number added to a hashed or encrypted block in a blockchain that, when rehashed, meets the difficulty level restrictions i.e by varying the proof we can vary the hash generated so that a new block can be created.

- ***Previous hash:*** This field represents the hash of the previous block. (Since, the genesis block is the first block, there is no previous hash here). The hash of the entire block is generated using a hashing algorithm.

- ***Sender:*** The person who uploads the file enters his identity proof or name when he uploads the file (not applicable for genesis block).

- ***Receiver:*** Displays who the intended receiver of the file shall be (not applicable for genesis block).

- ***Hash of the file shared:*** The uploaded file is first encrypted with the file key given by the uploader using an encryption mechanism and subsequently using a hashing algorithm when it is uploaded to IPFS. The hash, then received from the IPFS after the encryption is the hash of the shared file which is added to the block (not applicable for the genesis block).



(a) (b)

Figure 2. The homepage for the AnonChain app.

3.1.2 Creating the Peer - to - Peer Network

In order to create a peer to peer network (p2p) for the blockchain to function, all the connected nodes must be in the same network. Only those users who are connected to the blockchain's p2p network should have access to the blockchain's data (Vimal and Srivatsa, 2019). This p2p network is created using Socket Programming. The blockchain created here is a permissioned blockchain which requires access to be a part of the blockchain. This access is granted when a user clicks on 'Connect to the blockchain' displayed on the home screen. Using socket programming, the list of connected nodes gets updated as soon as a new user gets connected or disconnected to the network and the updated list is broadcasted to the entire p2p network (Li et al., 2018). As soon as all the connected nodes get the updated list of the nodes in the network, the consensus protocol works smoothly whenever a new block is added or the blockchain gets updated. Thus, the peer to peer network works effectively. The consequent block structures are represented in Figure 4.

Figure 3. Genesis block structure.

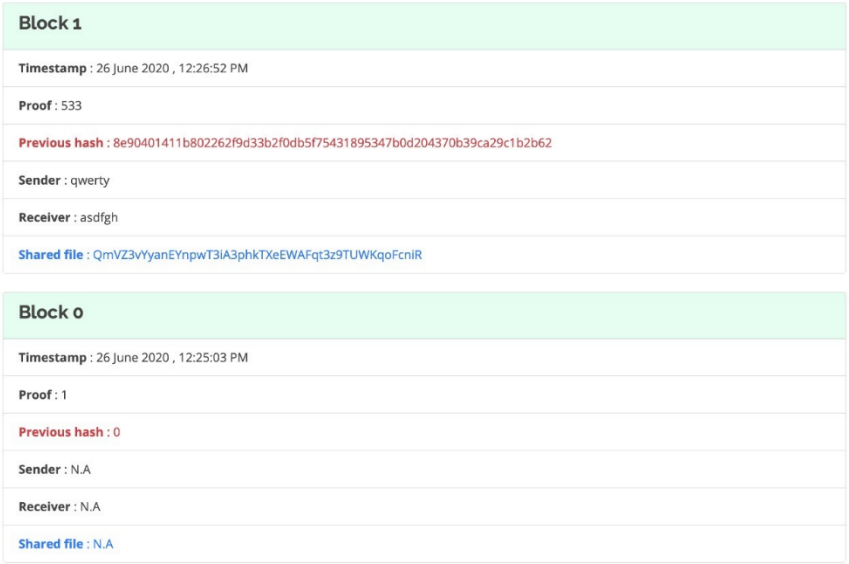


Figure 4. The blockchain structure.

A cryptographic hash algorithm is used to generate each block's hash. Accordingly, this aids to uniquely recognize each block in the entire blockchain. As soon as a block is created, it automatically creates a hash and any changes made in the block would bring about a change in the calculated hash as well. Thus, any changes made to the block can be easily detected using a hashing. The final element within the block is the hash from the previous block. This creates a chain of blocks and is the main element behind blockchain's security. This hashing process makes the blockchain immutable and noneditable. A full copy of the system is received by each new user (node) joining the system. On creation of s new block, it is sent to each node in the blockchain. Each node then verifies the block and checks whether the information stated in it is correct. The block is only added to the local blockchain in each node if it is ratified by all the nodes.

The SHA 256 Algorithm is used for creating the hashes (Martino and Cilardo, 2020). It is used to generate a unique hash of the entire block that is in turn used by the corresponding blocks to form the chain (via the previous hashes). IPFS as well, uses this algorithm to generate the hash of the shared file. The SHA-256 hashing algorithm is employed because of its many features like:

- One-way: Once the hash is generated, we can not revert to the original data from the hash.
- Deterministic: For a particular input, the hash generated, always remains the same i.e. same input always gives the same hash.
- Quick computation of the hash.
- Avalanche-effect: Even a slight change in the input will bring about a large change in the final hash, making it untraceable.
- Withstand collisions: There is a very rare chance that the hash generated for two different inputs will be the same.

3.1.3 Integrating with IPFS

The blockchain created in this paper relies on IPFS for keeping it lightweight and scalable. If the files were stored directly on the blockchain, it would render the blockchain very heavy and inefficient. Combining IPFS and blockchain, enables us to access the IPFS's power of decentralized storage and enhance the blockchain's security and accessibility (Nizamuddin et al., 2019; Singhal et al., 2020). Instead of storing the file directly on the blockchain, the files are stored on the IPFS network while the blockchain stores only the file's hash. Each file will have a unique hash as IPFS employs the SHA-256 hashing algorithm. Thus, the file is stored in a secure decentralized network and is easily accessible through the blockchain. The file can be retrieved using its generated hash easily. Hence, IPFS eliminates the bottleneck of storing entire files on the blockchain (Manoj and Krishnan, 2020).

3.2 Uploading a File

To upload a file using the proposed framework, the user has to navigate to the 'Connect to the blockchain' page after starting the application to get connected to the blockchain network. Consequently, clicking on the 'Upload a file' section takes the user to an upload file page. Here the user fills in the necessary details which are: (i) Sender Name; (ii) Receiver Name; (iii) File key; (iv) The file to be uploaded. The file key is the uploader's personal key and it is his/her responsibility to share it accordingly to the authorized people. Both the file key and the file contents are fed to the AES encryption algorithm which converts it to an encrypted version of the original file. Upon clicking the upload button, a request is sent to the IPFS network for the file to be added in it. After the file is uploaded successfully, IPFS returns a unique hash (IPFS internally uses SHA-256 hashing algorithm) of the file. Finally, the sender's name, receiver's name and the file hash are added to the newly created block, which is subsequently added to the blockchain. The user can view the new block added on the blockchain as soon as he/she clicks on the 'View blockchain' button. The entire workflow in depicted in Figure 5 and the 'Upload a file' page is shown in Figure 6.

3.3 Downloading a File

Similarly, to download a file using the proposed framework, the user has to navigate to the 'Connect to the blockchain' page after starting the application to get connected to the blockchain network. Consequently, clicking on the 'Download a file' section takes the user to a 'download file' page (Figure 7). Here the user has to fill the necessary details which are: (i) File hash; and (ii) File key. The intended recipient can download the file using the uploader's file key. Upon clicking the download button, a request is sent to the IPFS network to retrieve the AES encrypted file from the IPFS network. Now the file key and the encrypted file contents extracted from the IPFS network are fed to the AES encryption algorithm which yields the decrypted original file. The user can view the blockchain by clicking on the 'View blockchain' button. The entire workflow is depicted in Figure 8.

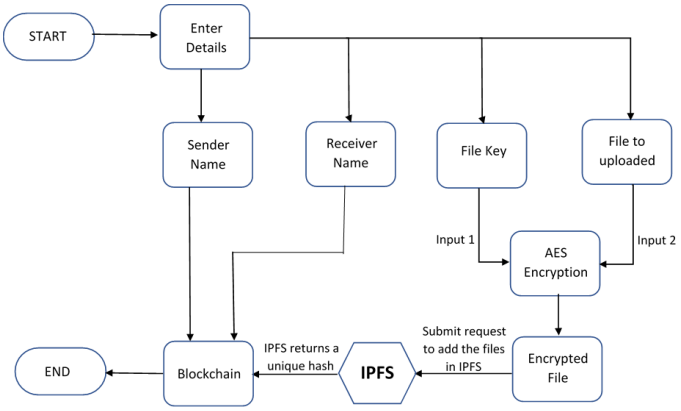


Figure 5. Workflow for uploading a file.

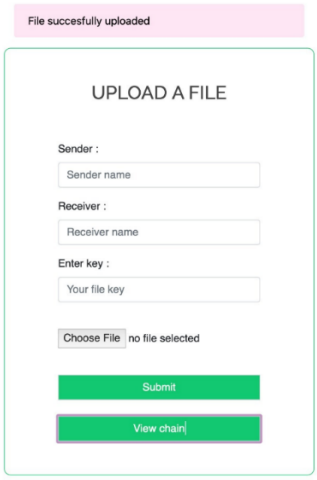


Figure 6. Uploading a file page.

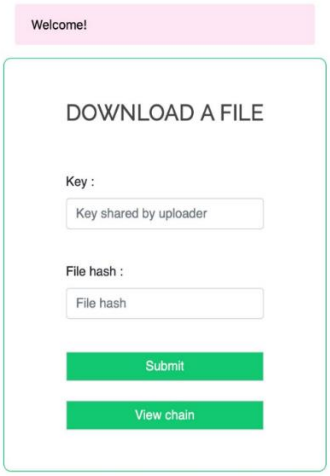


Figure 7. Downloading a file page.

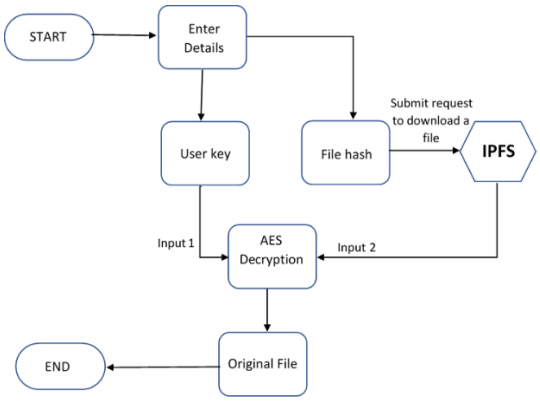
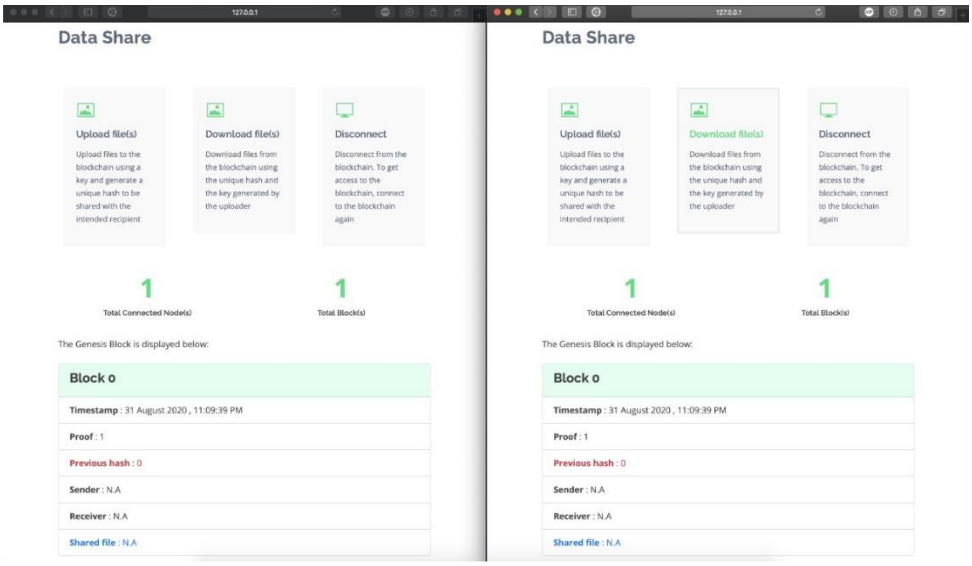
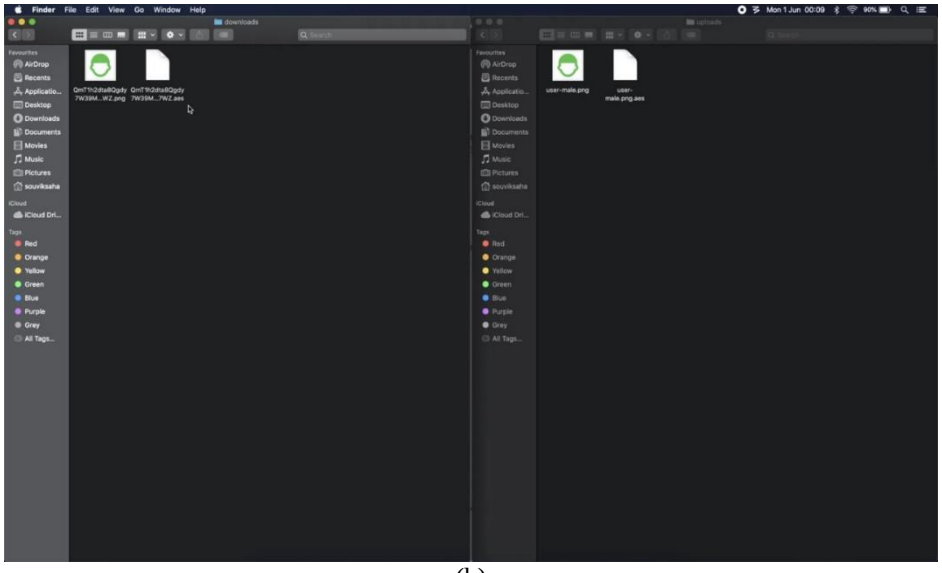


Figure 8. Workflow for downloading a file.

To test the application, several instances of AnonChain were run on the system locally at different ports, which served as different and independent nodes. From these nodes, a connection to the blockchain network was established and files were shared using file keys. Figure 9 simulates a state when two instances of the application are running and also shows the blockchain as witnessed by the two nodes when they initially connect to the blockchain. Figure 9(a) shows the screen instance of the sender of the file or the user which intends to share the file. Figure 9(b) shows the directory states of the receiver's nodes after a file was uploaded from the sender's node and downloaded by the receiver's node using the file key given by the uploader in the first node. The blockchain gets updated in both the nodes after the subsequent file uploads.



(a)



(b)

Figure 9. Two nodes sharing a file.

4. Conclusion

Blockchain can be set up to operate in a variety of ways, using different mechanisms to secure a consensus on transactions, seen only by authorized users. Blockchain depends on scalability and does not work well if the file size is too big, but when combined with IPFS, it could overcome this disadvantage and help redefine the way we interact with information and identity. AnonChain thus, holds an enormous potential in the future for application in various fields. This technology could not only save our time and money, but it can also revolutionize many industries and provide more sustainable solutions to the manufacturing industry for sustainability and growth. A limitation currently is that it runs on a local network but it can be made to function on any public network with web hosting, thereby making it more scalable. Another limitation is that, AnonChain currently accepts individual files (.txt, .png, .jpg, .jpeg, etc.) but it can be updated to accept folders as well. As future initiatives, upon proper exploration, AnonChain could prove to be a boon for other leading industries like digital advertising, cyber security, supply chain management, networking and forecasting. It may also prove to be an advanced solution for sustainability issues in Industry 4.0.

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

References

Abeyratne, S.A., & Monfared, R.P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology, 5(9)*, 1-10.

Benet, J. (2017). Filecoin research roadmap for 2017. *Protocol Labs*. 1-6.

Bhadoria, R.S., Arora, Y., & Gautam, K. (2020). Blockchain hands on for developing genesis block. *In Advanced Applications of Blockchain Technology* (pp. 269-278). Springer, Singapore.

Chen, W., Mu, Y., Liang, X., & Gao, Y. (2019a, July). Medical data sharing model based on blockchain. *In Journal of Physics: Conference Series (*Vol. 1267, No. 1, p. 012014). IOP Publishing.

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019b). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems*, *43*(1), 1-9.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: beyond bitcoin. Appl. Innov. Rev. (2016). Sutardja Center for Entrepreneurship & Technology Report, Berkeley University. http://scet. berkeley. edu/wp-content/uploads/AIR-2016-Blockchain. pdf.

Cui, S., Asghar, M.R., & Russello, G. (2018, July). Towards blockchain-based scalable and trustworthy file sharing. *In 2018 27th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-2). IEEE. Hangzhou, China.

Das, K., Annand, A., & Ram, M. (2021) A global supply network design model: A resilient management approach. *International Journal of Mathematical, Engineering and Management Sciences*, *6*(2), 660-676.

Ekblaw, A., Azaria, A., Halamka, J.D., & Lippman, A. (2016, August). A case study for blockchain in healthcare:"MedRec" prototype for electronic health records and medical research data. *In Proceedings of IEEE Open & Big Data Conference (*Vol. 13, p. 13).

Friedlmaier, M., Tumasjan, A., & Welpe, I.M. (2018, January). Disrupting industries with blockchain: The industry, venture capital funding, and regional distribution of blockchain ventures. *In Venture capital funding, and regional distribution of blockchain ventures (September 22, 2017). Proceedings of the 51st Annual Hawaii International Conference on System Sciences (HICSS*). http://dx.doi.org/10.2139/ssrn.2854756.

Haber, S., & Stornetta, W.S. (1990, August). How to time-stamp a digital document. *In Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer. Berlin, Heidelberg.

Jamwal, A., Agrawal, R., Sharma, M., & Giallanza, A. (2021a). Industry 4.0 technologies for manufacturing sustainability: A systematic review and future research directions. *Applied Sciences*, *11*(12), 5725.

Jamwal, A., Agrawal, R., Sharma, M., Kumar, A., Luthra, S., & Pongsakornrungsilp, S. (2021b). Two decades of research trends and transformations in manufacturing sustainability: A systematic literature review and future research agenda. *Production Engineering*, *16*,1-25. https://doi.org/10.1007/s11740-021-01081-z.

Jamwal, A., Agrawal, R., Sharma, M., Kumar, V., & Kumar, S. (2021c). Developing a sustainability framework for industry 4.0. *Procedia CIRP*, *98*, 430-435.

Khatal, S., Rane, J., Patel, D., Patel, P., & Busnel, Y. (2021). FileShare: A blockchain and ipfs framework for secure file sharing and data provenance. *In Advances in Machine Learning and Computational Intelligence* (pp. 825-833). Springer. Singapore.

Kim, J.W. (2020). Blockchain technology and its applications: Case studies. *Journal of System and Management Sciences*, *10*(1), 83-93.

Kim, S., Kwon, Y., & Cho, S. (2018, October). A survey of scalability solutions on blockchain. *In 2018 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1204-1207). IEEE. South Korea.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, *35(4)*, 95-99.

Kumar, R., Marchang, N., & Tripathi, R. (2020, January). Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. *In 2020 International Conference on Communication Systems & Networks (COMSNETS)* (pp. 1-5). IEEE. Bengaluru, India.

Kuo, T.T., Kim, H.E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24(6)*, 1211-1220.

Li, J., Wu, J., & Chen, L. (2018). Block-secure: Blockchain based scheme for secure P2P cloud storage. *Information Sciences*, *465*, 219-231.

Manoj, M.K., & Krishnan, S.S.R. (2020). Decentralizing privacy using blockchain to protect private data and challenges with IPFS. *In Transforming Businesses with Bitcoin Mining and Blockchain Applications* (pp. 207-220). IGI Global. https://doi.org/10.4018/978-1-6684-7132-6.ch063.

Martino, R., & Cilardo, A. (2020). Designing a SHA-256 processor for blockchain-based IoT applications. *Internet of Things*, *11*, 100254. https://doi.org/10.1016/j.iot.2020.100254.

Miltchev, S., Smith, J M., Prevelakis, V., Keromytis, A., & Ioannidis, S. (2008). Decentralized access control in distributed file systems. *ACM Computing Surveys (CSUR)*, *40*(3), 1-30.

Mohamed, N., & Al-Jaroodi, J. (2019, January). Applying blockchain in industry 4.0 applications. *In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0852-0858). IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Naz, M., Al-zahrani, F.A., Khalid, R., Javaid, N., Qamar, A.M., Afzal, M.K., & Shafiq, M. (2019). A secure data sharing platform using blockchain and interplanetary file system. *Sustainability*, *11*(24), 7054.

Nizamuddin, N., Hasan, H.R., & Salah, K. (2018, June). IPFS-blockchain-based authenticity of online publications. *In International Conference on Blockchain* (pp. 199-212). Springer, Cham. https://doi.org/10.1007/978-3-319-94478-4_14.

Nizamuddin, N., Salah, K., Azad, M.A., Arshad, J., & Rehman, M.H. (2019). Decentralized document version control using Ethereum blockchain and IPFS. *Computers & Electrical Engineering, 76*, 183-197.

Rajalakshmi, A., Lakshmy, K., Sindhu, M., & Amritha, P. (2018). A blockchain and ipfs based framework for secure research record keeping. *International Journal of Pure and Applied Mathematics*, *119*(15), 1437-1442.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117-2135.

Sari, L., & Sipos, M. (2019, May). FileTribe: Blockchain-based Secure file sharing on IPFS. In *European Wireless 2019; 25th European Wireless Conference* (pp. 1-6). VDE. Aarhus, Denmark.

Singhal, N., Sharma, M.K., Samant, S.S., Goswami, P., & Reddy, Y.A. (2020). Smart KYC using blockchain and IPFs. *In Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies* (pp. 77-84). Springer. Singapore.

Steichen, M., Fiz, B., Norvill, R., Shbair, W., & State, R. (2018, July). Blockchain-based, decentralized access control for IPFS. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1499-1506). IEEE. Canada.

Stephen, R., & Alex, A. (2018, August). A review on blockchain security. In *IOP Conference Series: Materials Science and Engineering* (Vol. 396, No. 1, p. 012030). IOP Publishing.

Subha, T. (2020). Assessing security features of blockchain technology. In: Raj, P., Saini, K., Surianarayanan, C. (eds) *Blockchain Technology and Applications* (pp. 115-138). Auerbach Publications.

Treiblmaier, H. (2020). Toward more rigorous blockchain research: Recommendations for writing blockchain case studies. In *Blockchain and Distributed Ledger Technology Use Cases* (pp. 1-31). Springer, Cham.

Turgay, S. (2018). Multi objective simulated annealing approach for facility layout design. *International Journal of Mathematical, Engineering and Management Sciences*, *3(4)*, 365-380.

Vimal, S., & Srivatsa, S.K. (2019). A new cluster p2p file sharing system based on IPFS and blockchain technology. *Journal of Ambient Intelligence and Humanized Computing*, 1-7. https://doi.org/10.1007/s12652-019-01453-5.

Vorick, D., & Champine, L. (2014). Sia: Simple decentralized storage. Retrieved May, 8, 2018.

Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management. *Frontiers of Engineering Management*, *4*(1), 67-75. https://doi.org/10.15302/J-FEM-2017006.

Wilkinson, S., Boshevski, T., Brandoff, J., & Buterin, V. (2014). Storj a peer-to-peer cloud storage network. 1-18.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*(2014), 1-32.

Yu, B., Liu, J.K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., & Au, M.H. (2018, September). Platform-independent secure blockchain-based voting system. In *International Conference on Information Security* (pp. 369-386). Springer, Cham. https://doi.org/10.1007/978-3-319-99136-8_20.

Zheng, Q., Li, Y., Chen, P., & Dong, X. (2018, December). An innovative IPFS-based storage model for blockchain. In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)* (pp. 704-708). IEEE. Santiago, Chile.

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017, April). Ensuring data integrity using blockchain technology. In *2017 20th Conference of Open Innovations Association (FRUCT)* (pp. 534-539). IEEE. Russia.

Publisher's Note- Ram Arti Publishers remains neutral regarding jurisdictional claims in published maps and institutional affiliations.