

AUTHENTICATION AND LICENSING OF FILES USING BLOCKCHAIN

Sunil.B. Wankhede¹, Shrey Solanki², Tasneem Suterwala³, Nihal Yende⁴

¹Professor, Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai

^{2,3,4}Student, Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai

Abstract - The project refers to the official deployment of the owner's digital asset, which is stored on a blockchain, which is a distributed ledger of transactions. Images, videos, audios, music, text, and documents are all acceptable formats for this file. The blockchain acts as a public record, allowing anybody to check the legitimacy of a product and determine who owns it. Making a duplicate file by forging the original has become more popular in recent years. In a De-Centralized Database, the files are kept as nodes. Furthermore, these data are subject to Digital bragging rights, demonstrating the owner's validity. The blockchain method is a system for storing documents in the form of e-documents in a secure manner on a blockchain network. The immutability attribute protects the file from being replaced by another product and ensures that it is permanently stored in Distributed Databases. Furthermore, the distributed ledger system's blockchain property will help to maintain the files untouched and unaffected indefinitely.

Key Words: Blockchain, Decentralised, Ethereum, Smart Contract

1.INTRODUCTION

In our present lifestyle, file storage has become quite vital. Theft and forgery of any type of file is becoming more common by the day. As a result, there is a critical requirement for such files to be protected and authenticated in order to prevent them from being destroyed, modified, or forged into another file. Blockchain technology is a revolutionary advancement that has the potential to disrupt or perhaps replace conventional business structures that rely on third parties for trust. A second generation of blockchains (such as Ethereum) was developed in 2014, allowing for the programming and execution of software (so-called smart contracts) on all participating blockchain nodes. Any product used here is a digital asset that is stored on a blockchain, which is a distributed ledger of transactions. The blockchain acts as a public record, allowing anybody to check the legitimacy of a product and determine who owns it. Unlike other digital goods, which can be infinitely replicated, each file contains a unique digital signature in the form of a 32-bit hash value, indicating that it is unique. While anybody may see the transactions, only the uploader is the official owner — a type of digital bragging rights. This platform can be used to publish a variety of digital artefacts, including photographs, videos, audios, music, text, documents, and voting.

2.LITERATURE SURVEY

Traditional business processes have been severely disrupted by blockchains since apps and transactions that previously required centralized systems or trusted third parties to authenticate them can now operate in a decentralized manner with the same level of confidence. Transparency, robustness, auditability, and security are all fundamental qualities of blockchain architecture and design. A blockchain can be thought of as a distributed database organized as a list of ordered blocks with immutable committed blocks. This is particularly advantageous in the banking sector, as banks can collaborate on the same blockchain and push their clients' transactions. Blockchain supports transaction audits in this way, in addition to providing transparency. Companies invest in this technology because it has the ability to decentralize their systems and reduce transaction costs by making them safer, more transparent, and in certain circumstances faster. As a result, blockchains aren't merely a fad. The sheer quantity of cryptocurrencies exemplifies this. The relevance of blockchain has surpassed 1900 and is continuing to increase. Because of the diversity of bitcoin applications, such rapid growth may soon cause interoperability issues. Furthermore, as blockchain is employed in industries other than cryptocurrencies, the environment is fast changing, with Smart Contracts (SCs) playing a key role. So, a SC is an agreement between parties that, notwithstanding their lack of confidence for one another, the provisions of the agreement are automatically implemented. SCs, in

and interactions, establishing a new paradigm with practically endless uses.

2.PROPOSED SYSTEM

The proposed method takes advantage of blockchain's immutability to keep files safe and accessible across the internet. The blockchain network is used to store files.

Construction of the Blockchain Network: Each node in the blockchain system will start out as a separate and autonomous entity until they are connected. Every node will have a blockchain-based database of its own. Before a P2P link is formed between these blockchain-based databases, just the "genesis-block" will exist. We'll need a third-party piece of hardware, which we'll refer to as the bottle-server, to connect all of the nodes in the blockchain network.

This server will be available for nodes to connect to. The bottle server will accept incoming connections up to a certain threshold quantity. Through a verification process, the bottle-server will ensure that the connecting nodes are permitted nodes. The IP addresses of the incoming nodes are taken into account by the bottle-server as they are received. After the threshold is reached, the bottle-server establishes P2P connections between all nodes by interconnecting them. After each pair of nodes establishes a P2P connection, synchronization is performed across all of their blockchains to ensure that updates to the blockchain are reflected evenly.

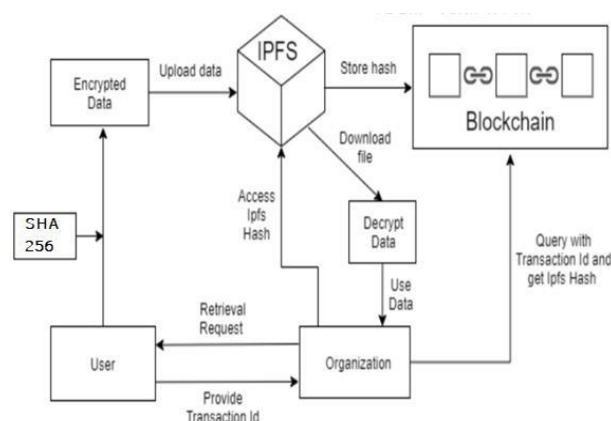
Only the approved nodes that make up the blockchain network are allowed to enter/transfer data into the blockchain network. The approved node creates a soft copy of the original file, which is then sent into the blockchain network after perfect verification. Due to the synchronization between all nodes in the blockchain network, this e-copy of the certificate will be added to each node's blockchain.

After the e-file is transferred, the document's owner is given a secret file-code generated by the SHA-256 hashing technique. This file-code can be used to receive an electronic copy of the document later.

Accessing the document: The user will utilize the API to retrieve data from the blockchain network in order to access the document. This API will connect to the bottle-server first, and then get the IP address of any random node in the blockchain network from the bottle-server. During document uploading, this API will accept two parameters as input:

- 1.Password for Metamask account verification.
- 2.Obtaining the document-code.

Architecture Diagram



the context of blockchain, are scripts that run decentralized and are kept on the blockchain without relying on any trusted authority. Blockchain-based systems that support SCs, in particular, allow for more sophisticated processes

System Architecture:

The user selects a file to be uploaded to the Ethereum Network, as shown in the diagram, and the data in the file is first encrypted using the SHA-256 method. For each unique file saved in the blockchain database's IPFS (Inter-

Planetary File System), the encryption method outputs a 32-bit hash value. As a result, this encrypted file is now ready to be posted to the Ethereum Network as a blockchain node. With valid authentication and certification of its identity to the system, the authorised owner can study, access, and recover the file from any remote location.

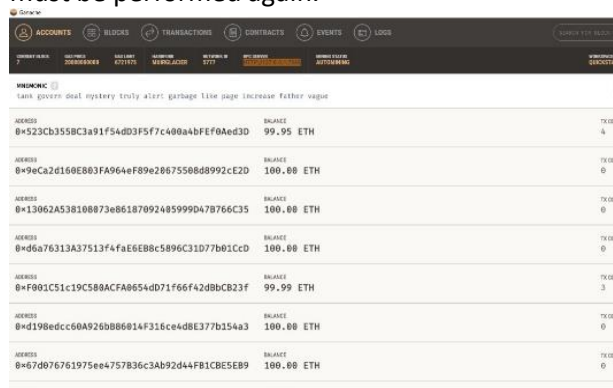
3.METHODOLOGY

A) IMPLEMENTATION

i)Installation of Personal Ethereum Blockchain Tool

This study's application development method is described below, with the goal of verifying digital certificates supplied to participants using an Ethereum network blockchain

Personal Ethereum Blockchain Tool installation. Ganache, a Personal Ethereum blockchain application, was first installed and set to run at <http://localhost:8545> in order to create a smart contract on the Ethereum blockchain. Ganache, as illustrated in Figure, has ten accounts, each with a default balance of 100 ethers. This number of accounts and the amount of Ethereum held can both be modified if needed. These accounts can be used to send and receive Ethereum transactions as well as perform smart contract operations. By producing a block for each process, the Ganache blockchain may also give miner approval. As a result, there is no need to wait for the transactions to be approved. Smart contracts or transactions created in this application, on the other hand, vanish as soon as the app is closed. As a result, all transactions must be performed again.



ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS

Fig- Ganache, Personal Blockchain for Ethereum

ii)Development of Smart Contract

A Solidity language development environment (IDE) is required to construct Ethereum-based smart contracts.

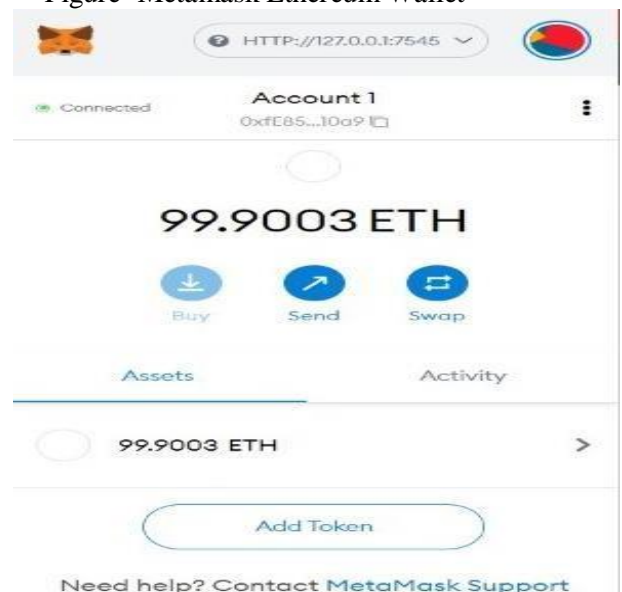
Writing smart contracts in Solidity can theoretically be done with a notepad-like programme. To work with the Solidity language, there are a variety of development environments that include a user interface and a command prompt. Truffle is an example of one of these settings. However, such development environments are required since both observing coding errors while developing the code and sending the smart contract to the blockchain require an Ethereum account. A personal Ethereum blockchain that may be used to generate and deploy smart contracts, as well as develop DApps (decentralized applications) that operate on localhost.



Fig- Remix Solidity IDE

Smart contracts are also deployed via the Metamask Ethereum wallet, which can be loaded as an add-on on browsers like Chrome or Firefox. As a result, a smart contract created on the Truffle platform can be sent to either the test network or the actual Ethereum blockchain, using an account or wallet with sufficient Ethereum.

Figure- Metamask Ethereum Wallet



Remix is a Solidity IDE that is used to write, compile, and debug Solidity programmes in this study. Solidity is a contract- oriented programming language for creating smart contracts at a high level. Ganache was utilized with Remix, a web-based IDE for designing smart contracts. To better reflect the real Ethereum blockchain, the contract development process was finished using Ropsten Ethereum Test Network and Parity Platform after the fundamental smart contract was developed. The values entered in these fields on the certificate cannot be changed. If the user wants to re-download the certificate, the process information in the profile field is verified, and if the process is identified on the chain, the smart contract is not permitted to run again.

The User Interface Page



As shown in Figure, A document verification page has been created to function in conjunction with the Moodle system, allowing third parties to check the validity of the generated digital certificate. After the document control code on the digital certificate is typed into this page and the transaction information of the control code is located in the IPFS database, the data stored in the blockchain is fetched through smart contract and the document's validity is proven. As a result, the authorized owner of the e-file receives an authenticated access right as well as a copy right.

WORKING

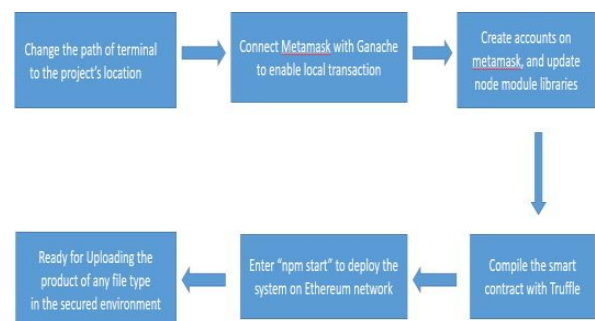
The storage, retrieval, and access to data are the most important challenges in document verification for government agencies and other organizations. As a result, blockchain technology



was developed to address these issues with data storage and access. Blockchain technology creates a centralized platform for storing, retrieving, and accessing files. The technology's entire nature lies in distributed, shared, open ledgers that can be verified by anybody.

Public blockchains are open to everyone, but private blockchains are limited to one, two, or a few businesses. Later on, new firms may join or leave the network. As a result of participating, the operational and overhead costs of completing the task of file verification are reduced. By participating in a blockchain, one may assure correct data storage, retrieval, security, and access.

Work Flow :

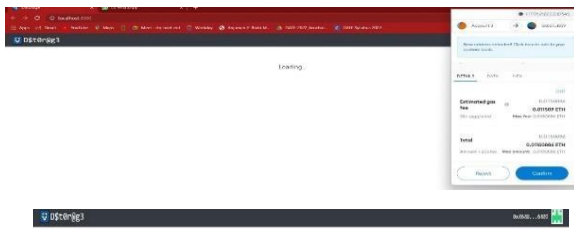


Documents Verification Process:

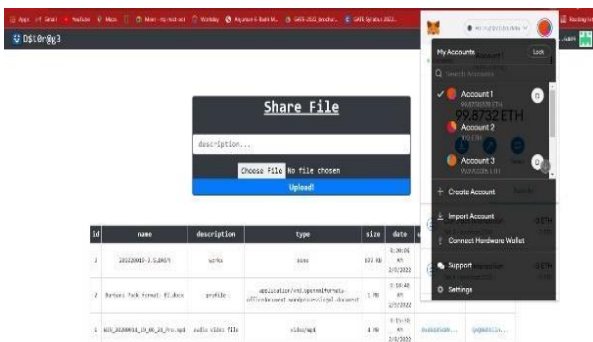
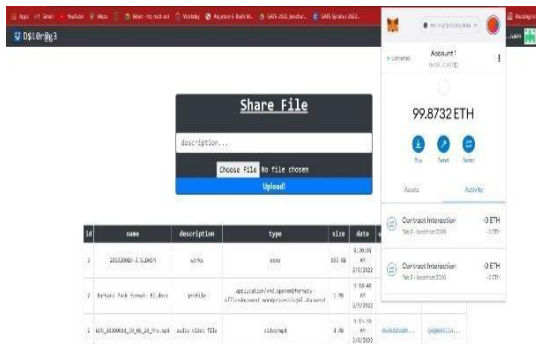
The technique turns or encodes a file into a cryptographic digest or cryptographic hash when a user provides it. - b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53a b94fc248f4f553 is the permanent hash of every file/data. If you submit the same document for verification more than once, the hash and transaction markers will match each time. The markers will not match if the file has any modifications. The user will also have the ability to grant or deny access to the file to the specified organization or individual.

Verifying Files on a Blockchain Network:

There are a variety of methods for verifying the existence of a file on the blockchain at the moment. To validate the file's existence, the simplest option is to re-upload it. The proof of the file's existence is validated during re-uploading, as the cryptographic digest and transaction marker are also verified. Checking the bitcoin blockchain's transaction record to validate the presence of a time-stamped file is another option. Returning to the original time-stamped file's verification page also confirms its existence. As a result, the presence of a time-stamped file from a previous date is established



#	name	description	type	size	date	uploader/view	hash/link/gp
1	20120809-1-5.0015	works	text	101 kb	3/30/2012 20/02/2012	upload/nd	Qm9kLn...
2	kernel-hack_forum-82.03c	profile	...	1 kb	3/30/2012 24/02/2012	upload/nd	Qp8a5h...
3	82-200803-23_0m-3-1m.net	audio voice file	video/...	1 kb	3/30/2012 16/02/2012	upload/nd	Qp8a5h...



5.FUTURE SCOPE

We have established a circumstance in which we can make e- file storage simple and give 100 percent document availability wherever and at any time. We've also safeguarded the document's genuinity by verifying it and preventing it from being tampered with by a third party. As a result, the distributed ledger system's blockchain

property will help to maintain the data untouched and unaffected indefinitely.

3. CONCLUSIONS

One of the most important advantages of blockchain technology is data security. Blockchain is a big, public online ledger in which each node saves and verifies an equivalent amount of data. This blockchain-based technology will allow totally secure document storage over the internet, protecting it from third-party tampering. It will also ensure that an e-document is always available as and when the owner of that e-document need it.

REFERENCES

1. International Research Journal of Engineering and Technology (IRJET) on Secure E-Files Storage using Blockchain.
2. A Review on Blockchain Security by Remya Stephen and Aneena Alex.
3. Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain", Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.
4. Yong Shi, "Secure storage service of electronic ballot system based on block chain algorithm", Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.
5. Zhenzhi Qiu, "Digital certificate for a painting based on blockchain technology", Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.