IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, September 2023

"Document Verification System at College Level using Blockchain"

Sakshi Asode[1], Tejaswini Dumbare[2], Achal Ghadge[3], Samiksha Thombare[4]

Department of Information Technology

Marathwada Mitra Mandal's College of Engineering, Karvenagar, Pune, Maharashtra, India

Abstract*: Blockchain technology promises to be hugely trending and empowering in education domain computing applications. The digital is becoming an integral part of modern life. So as the use of the digital world increases there are more chances of decrease is the security level. So more the use of digitization more the frauds and less the security. In some cases of personal data, leakage has brought back into the focus the security issues with the different identity sharing mechanisms. A customer is expected to provide his identity for authentication by different agencies. So the document verification process deals with the identification of the user. And in turn, provides the required security. The document verification procedures which are used by the colleges are completely dependent on the encryption. This system can be efficient by using Blockchain technology, which has the potential to automate a lot of manual processes and it is also resistant to hacks of any sort. The immutable blockchain block and its distributed ledger is the perfect complement to the process of document verification. With the addition of smart contacts, fraud detection can be automated..*

Keywords: Blockchain, verification, Security, Privacy

I. INTRODUCTION

In today's digital age, the verification and authenticity of documents play a vital role in various domains, ranging from finance and healthcare to legal and supply chain management. However, traditional methods of document verification often rely on centralized systems, manual processes, and intermediaries, which can be time-consuming, prone to errors, and susceptible to fraud.

To overcome these challenges and ensure a more secure and efficient document verification process, blockchain technology emerges as a revolutionary solution. Blockchain, originally introduced as the underlying technology for cryptocurrencies like Bitcoin, is a decentralized and immutable ledger that records transactions across a network of computers. It offers unprecedented transparency, security, and trust by eliminating the need for intermediaries and enabling participants to validate and authenticate information in a decentralized manner.

The application of blockchain technology to document verification brings numerous benefits, including enhanced integrity, security, transparency, and efficiency. By leveraging the unique properties of blockchain, documents can be stored, verified, and accessed in a tamper-proof and auditable manner, providing a high level of trust and immutability.

This project aims to explore the implementation of blockchain for document verification, revolutionizing the way documents are verified and validated in various industries. By leveraging blockchain's decentralized and transparent nature, the project aims to establish a robust system that ensures the authenticity and integrity of documents throughout their lifecycle.

In the following sections, we will delve into the details of how blockchain technology can be leveraged for document verification, outlining its key features, advantages, and potential use cases. By harnessing the power of blockchain, we can pave the way for a more secure, efficient, and trustworthy document verification process that meets the demands of our increasingly digital world.

A Blockchain-based security management system is for providing security to the document verification and to implement the document verification process in a simpler and more secured way. Blockchain technology is a new technology which is based on mathematical, cryptographic and economic principles for maintaining a database between various participants without the necessity of any third partyor central authority. It is a secured distributed database,

DOI: 10.48175/IJARSCT-13025

tamper evident, wherein the validity of a transaction can be verified byparties in the transaction. One of the main tasks of the college is to ensure information security of data of the students, Confidentiality and the state of their account to guarantee their safety and integrity, in the process of exchange and processing of information. Thus, by using the capabilities of innovative information technology i.e. the Blockchain technology information security can be achieved.

II. LITERATURE SURVEY

Study 1: A Secure and Dynamic Multi Keyword Ranked Search Scheme over Encrypted Cloud Data.
Summary:
1. Implement dynamic deletion and updating in documents.
2. Data loss possible in this schema
Key Findings: This paper propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search.

Study 2: CrowdBC: A Blockchain-based Decentralized Framework for Crowd sourcing.
Summary:
1.Encryption not used in this system
Key Findings Use decentralized framework for crowd sourcing systems.

Study 3: Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains,"
Summary:
1.No need of Encryption System.
2. Data loss possible in this schema
Key Findings: Unlike existing blockchain-based energy trading system, we establish a consortium blockchain based on LAGs to audit and verify transaction records among PHEVs. We design a localized P2P Electricity Trading system with Consortium blockchain (PETCON) to achieve trustful and secure electricity
trading

Study 4: Security and privacy In decentralized Energy trading through multisig natures, blockchain and anonymous messaging streams,"
Summary:
1.not performed the pure performance simulations and comparison between the solutions since they are redundant.
2.The centralized solution is of constant complexity while the decentralized solution is at least linear
Key Findings: we address the problem of providing transaction security in decentralized smart grid energy trading without reliance on trusted third parties. We have implemented a proof-of-concept for decentralized energy trading system using blockchain technology, multi signatures, and anonymous encrypted messaging streams, enabling peers to anonymously negotiate energy prices and securely perform trading transactions

Study 5: "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis,"
Summary: Not Able to up-to-date Bitcoin protocol architectural analysis and presented the system's major architectural components.
Key Findings: Bit coin is continually improved by an open source community, and various Bit coin libraries, APIs, and alternative implementations are being developed. Nevertheless, there is no up-to-date protocol specification or architecture description since the official whitepaper

III. RELATED WORK

- Stampery: Stamper is a blockchain-based document verification platform that aims to provide secure and immutable document certification. It utilizes blockchain technology to create a timestamped proof of existence for documents, ensuring their integrity and authenticity. Stampery supports various blockchain networks, including Bitcoin and Ethereum.

- Evernym: Evernym is a digital identity platform that incorporates blockchain technology for document verification. It enables individuals to store and manage their digital identity credentials securely on a blockchain, allowing them to share verified documents with trusted parties while maintaining control over their personal data.
- Sovrin Foundation: The Sovrin Foundation is a non-profit organization that focuses on building a global public utility for self-sovereign identity. Their platform utilizes blockchain to create a decentralized and secure infrastructure for verifying and managing digital identity documents.
- Factom: Factom is a blockchain-based document verification and data integrity platform. It enables organizations to create an immutable record of their documents and data by anchoring them to the Bitcoin blockchain. Factom provides proof of existence and tamper-proofing capabilities for various types of documents, including legal records, financial data, and audit trails.
- Guard time: Guard time is a company that has developed a blockchain-based technology called Keyless Signature Infrastructure (KSI). KSI provides an integrity layer for digital assets and documents, ensuring their authenticity and protecting against tampering. It has been applied in various sectors, including supply chain management, healthcare, and government.
- IBM Blockchain: IBM has been actively involved in developing blockchain solutions for document verification. They have explored the use of blockchain in supply chain management and digital identity verification, which can be applicable to document verification systems as well. IBM Blockchain offers tools and platforms for building secure and transparent blockchain-based applications.

IV. PROPOSED SYSTEM

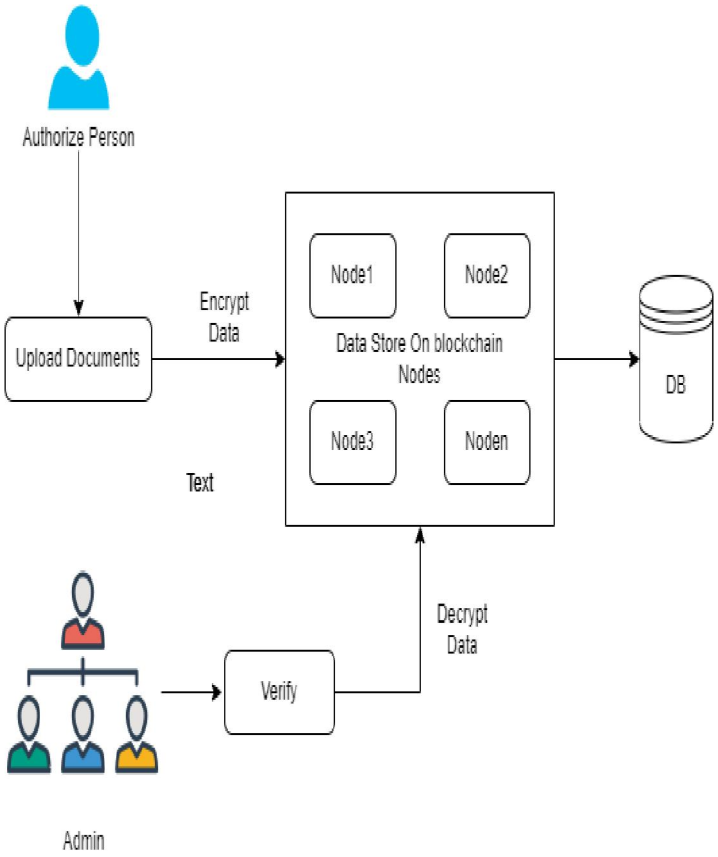


Figure 1. System Architecture

DOI: 10.48175/IJARSCT-13025

Our proposed system aims to develop a document verification using block chain. The system follows a multi-step process, as outlined below:

Uploading Process:

- The purpose of a document verification system is to verify the availability and integrity of the file.
- Before the verifying process, the file must be uploaded first into the system to indicate that the submission of the file is the original file, and it must be verify based on the existence and content of the original file.
- The requirements for the user to upload the file to the system are to ensure that it is in a pdf format and being encrypted using AES algorithm which uses password before using the system.
- The encryption process can be done through Microsoft product and file explorer where the requirement to use it
  is using Microsoft version 2007 or newer.
- The process of uploading the file to the system starts by submitting the password
  that is used to encrypt the file together with the encrypted file into the system.
- First, the system will take the submitted encrypted file to be uploaded into the IPFS Cluster which will go through the IPFS daemon.
- After the file has been uploaded to the IPFS, IPFS will an identity to the file which will be used to access the file called as the IPFS hash value.
- The IPFS hash value together with the password that has been submitted earlier
  will be transferred and stored into the Ethereum blockchain where it is stored in a form of a block.
- Before the storing process of IPFS hash value and the password to the file, the system will ask the user to confirm the transactions made by paying transaction fees using ethers.
- After the confirmation of the transactions, blockchain will store the IPFS hash value together with the password of the encrypted file.
- The uploading processes can be design using procedural design which will be described in a flow chart. Figure 2 shows the flow chart design.

Verification Process:

- The first phase of the process of the using the document verification system is by going through the file encryption process where the file will be encrypted using AES algorithm.
- To be verified, the password to the encrypted file and the transaction hash of the file when uploading into the system.
- These three components must be entered into the application to perform the verification process.
- When these three components have been entered into the system, the verification process starts by using the transaction hash to fetch the transaction block that has the same transaction hash in the blockchain.
- Then, the system will decode the metadata inside the transaction block to obtain the IPFS hash value and the password of the file.
- After that, the submitted file will be hashed, and the verification process of the file is by comparing the hash value of the submitted file with the hash value that has been fetched from the transaction block in the blockchain.
- Then, the submitted password will be compared with the password that has been stored in the blockchain.
- Since there are three different components that is needed for the system to verify the file, there will be a total of four scenarios where if each of the components entered to the system is incorrect or verified. Figure 3 shows the flow chart design.

DOI: 10.48175/IJARSCT-13025

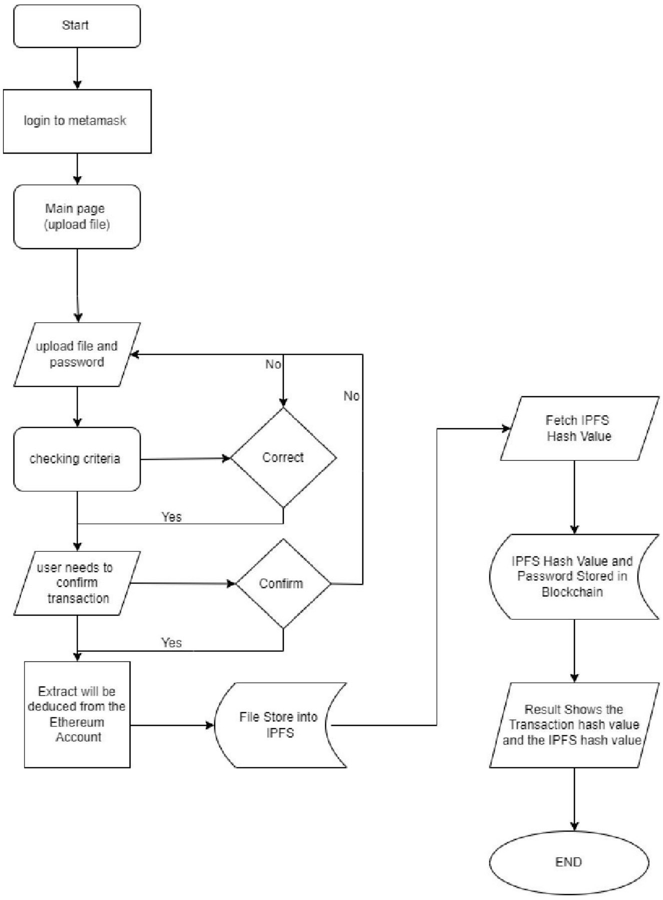

Start
login to metamask
Main page (upload file)
upload file and password
No
No
checking criteria
Correct
Yes
user needs to confirm transaction
Confirm
Yes
Extract will be deduced from the Ethereum Account
File Store into IPFS
Fetch IPFS Hash Value
IPFS Hash Value and Password Stored in Blockchain
Result Shows the Transaction hash value and the IPFS hash value
END

Fig. 2. Flowchart of Uploading Process

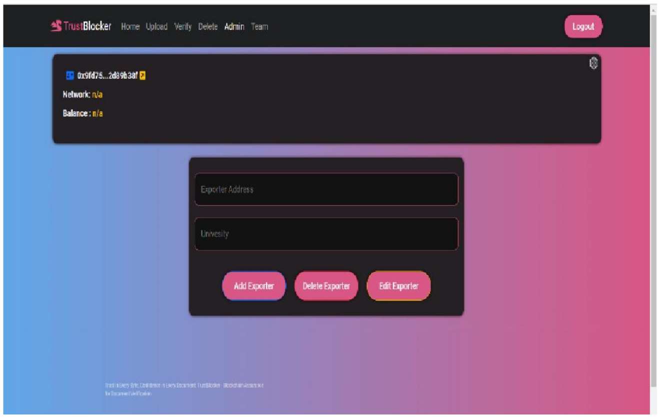
History Log Process:

- This is an extra feature of the system where the user can check the history log of the transactions made in the system.
- The system will fetch the transaction blocks from the blockchain to be displayed from the application for the user to monitor.
- It will fetch the latest ten transactions made from the system and it will decode the metadata data from the blockchain to be displayed to the application.

V. RESULT AND DISCUSSION

5.1 Registration:

A user, whether he is a student or teacher, or validator needs to register themselves first on the portal. The teacher i.e. the Certificate issuer will only be able to generate certificates. The Student can download his/her Document, and the Validator will be able to validate and view the document. So each actor has their own features and doesn't have access to the features they do not need. Once a User is registered he/she will now be able to access the system from the login window. If the credentials entered match the registration credentials which was stored in DB, the user will be logged in, or else an error will be thrown.



0x9fd75...2d89b38f

Network: n/a

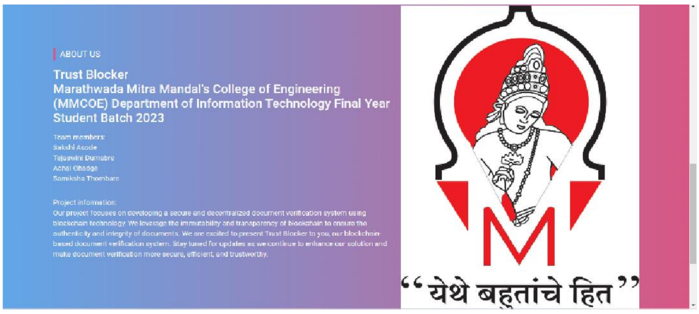
Balance : n/a

Exporter Address

Univesity

Trust in Every Byte, Confidence in Every Document: TrustBlocker - Blockchain Assurance for Document Verification

Fig 4. Registration Page


ABOUT US

Trust Blocker
Marathwada Mitra Mandal's College of Engineering (MMCOE) Department of Information Technology Final Year Student Batch 2023

Team members:
Sakshi Asode
Tejaswini Dumbre
Achal Ghadge
Samiksha Thombare

Project information:
Our project focuses on developing a secure and decentralized document verification system using blockchain technology. We leverage the immutability and transparency of blockchain to ensure the authenticity and integrity of documents. We are excited to present Trust Blocker to you, our blockchain-based document verification system. Stay tuned for updates as we continue to enhance our solution and make document verification more secure, efficient, and trustworthy.

Fig 5. Login page

5.2 Certificate Issuer:
The Certificate issuer has two options to generate certificate. Either to fill in details in a form to generate a single certificate or to upload a CSV to make certificates in bulk.

VI. ALGORITHMS

Ethereum Blockchain:

- Blockchain system that have been used in designing the document verification system is Ethereum blockchain. Ethereum is an open source blockchain-based platform that
- uses ETH as its cryptocurrency to be used for transactions. For the document verification system, Ethereum blockchain will become a place to store the identity of the file which is the IPFS hash value instead of the file because it will cost a less of computational power and resources to store a small credentials.
- Large files require a higher computational power which cost higher gas price to store the large files into the Ethereum blockchain.
- Therefore, IPFS will be use as a decentralized storage for the file and the credentials that points to the file which is the IPFS hash value will be stored into the block of the Ethereum blockchain.

IPFS Cluster:

- Interplanetary File System (IPFS) is a storage file system that works in a public network in nature.
- In a document verification system, security of the file must be considered in a high priority as it may contains sensitive information.
- A file storage must be known only to the selected peers in the organizations to keep it safe and secure from the unknown people.
- IPFS Cluster introduced a way where sharing content of the file in the IPFS to be secure where the files will only be shared to the certain number of peers depends on the user.

DOI: 10.48175/IJARSCT-13025

- IPFS Cluster provides data coordination across a swarm of IPFS daemons by replicating, allocating, and tracking a global pin set distributed among multiple peers on the network.
- IPFS Cluster acts as a private network where only selected peers can share and view all the files uploaded into the IPFS.
- It is a separate system from IPFS where it is a standalone application which uses the IPFS daemon's API.
- There is no centralized hosting in the cluster where every peer in the network can pin a file into the IPFS Cluster.

AES Encryption Algorithm:

- There are different types of encryption algorithm in a symmetric encryption. The symmetric algorithm encryption that will be used to encrypt the file is from the modern symmetric encryption which is called as AES encryption.
- AES encryption is one of the block ciphers that operates on 128-bit blocks. There are three phases in the process of encrypting using AES algorithm which are initial round, rounds, and final round. Each of the phases uses different types of algorithms to encrypt the data.
- AES algorithm uses only a single key to encrypt and decrypt the data. AES will make the encryption process to be robust from hacking because of its length in key sizes.
- For document verification system, the file will be encrypted with a password which uses AES algorithm whereby if there is a user who wants to read the content of the file, the user needs to enter the password or the key to decrypt the file.

Web Application

- User interface must be created to make the document verification system to be user friendly.
- A web application will be made to create the user interface for the document verification system using blockchain.
- Web application is created as the frontend of the system where the user will interact with the system to upload and verify a document or file and the Ethereum blockchain will be the backend of the system.
- The web application created will be a decentralized application as it is using Ethereum blockchain as its backend.
- It is developed by using HTML, JavaScript, and CSS which uses a lot of external packages and library to make the application works.

VII. CONCLUSION

In many ways, Blockchain today is comparable to where the Internet was in early 20s. The development of information technology and electronic business every day has an increasingly significant impact on all spheres of the modern life. Blockchain technology is designed to change the traditional perception of how people interact through a network. The main advantage of the Blockchain technology is the complete synchronization of processes, integrity and uniqueness of all processed information, regardless of mining and tokens. Blockchain technology helps to improve distributed databases in terms of storage, synchronization, loss and integrity of data. Its early days, but industry leaders aresponsoring a wide range of blockchain use cases supported by industry consortiums. Having seen the potential of this technology and the challenges, we think the opportunity is clear but the blue sky is too far off and companies need to validate use cases and business/technical viability before implementing blockchain.

REFERENCES

[1] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," IEEEIntell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.

[2] Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.

[3] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," IEEE Trans. Ind. Informat., vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[4] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Trans. Depend. Sec. Comput.

[5] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in Proc. IEEE 11the Int. Conf. Eur. Energy Market, 2014, pp. 1–6.

[6] S. Barber et al, "Bitter to better-how to make bitcoin a better currency," in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414

[7] I. Alqassem et al., "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in Proc. IEEE Internet Things, IEEE Int.Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput. 2014, pp. 436–443.

[8] K. Croman et al., "On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptography Data Security, 2016, pp. 106–125.

[9] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks andMoney. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.

[10] L. Luu et al., "A secure sharding protocol for open blockchains," Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.

DOI: 10.48175/IJARSCT-13025