IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

Doc-Chain Trustshield Transforming Verification through Blockchain Brilliance

Sandhya S[1], Badithala Srija[2], Bakyashree A[3], Illuri Ravalika[4], Jothilakshmi R[5]

U.G. Student, Department of Information Technology, R.M.D. Engineering College, Kavaraipettai, Tamil Nadu, India[1,2,3,4]

Associate Professor, Department of Information Technology, R.M.D. Engineering College, Kavaraipettai, Tamil Nadu, India[5]

ABSTRACT: Today, the authentically of the documents in the digital world has reached the scale of importance that the traditional methods which were inner adjusted to the previous unmodified fraud methods do not work anymore. It is a game-changer when it comes to document verification; did you know that Doc-Chain TrustShield is the one that truly introduces the concept? The TrustShield system offers institutions easy upload and deleting of the files that they use with their credentials and addresses to the blockchain. These are achieved thanks to SHA-512 technology hashs, provided by blockchain system for an impossibility of any records being altered or for the fake ones to be created. In addition to that, where a third party wants to check certificates digitally a hashing mechanism is used to authenticate them. Eventually the connected result is database authenticity which is instantly confirmed. The proper technique is not disclosed through the architecture of the system, the implementation and the evaluation but the other attributes of system such as verifying documents technique scaling which is meant to minimize fraud.

KEYWORDS: Document verification, Blockchain technology, TrustShield, SHA-512 hashing, ECDSA algorithms, Tamper-proof, Transparency, Fraud prevention, Decentralization, Authentication ecosystem.

I. INTRODUCTION

1.1 PROBLEM STATEMENT

The Statement of the Problem part emphasizes the lingering problems in the conventional document verification procedure, such as the vulnerability of being faked, the dependence on centralized institutions, and the unavailability of interoperability. This result becomes even worse since we now see the development of digital credentials that can be altered or counterfeited. As a retort to this challenge, the Doc-Chain initiative seeks to exploit blockchain technologies for building a secure, decentralized, and immutable authentication system. Through the use of cryptographic methods and decentralized consensus mechanism, our solution aims solving the challenge of document fraud and identity theft, consequently the integrity and authenticity of verified documents are enhanced across industries.

1.2 OBJECTIVES OF THE STUDY

The Objectives section of the study address the main goals and orientations of the Doc-Chain, indicating the principal targets, in form of next levels and stages, to be attained.

The primary objectives of the study are as follows:

1. Enhance Document Verification: This project is aimed at strengthening the authentication procedure by developing the supporting system with the help of blockchain technology and cryptography so that the integrity, authenticity and security of the verified documents would be maintained.
2. Establish Decentralized Trust: The concept aims to bring in place a protocol of decentralized consensus interactions and distributed ledger technology that will enable the creation of a trustless environment in which independently verified and authenticated documents can be accessed, checked and verified without third party and central authority participation.
3. Streamline Verification Procedures: The main objective of Doc-Chain TrustShield is to make the verifying

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

process as efficient and automatic as possible, which will save time, effort and money. At the same time it will break a metaphorical barrier with manual verification procedures, increasing both the exposition and the efficiency.

4. Ensure Interoperability: The task is purposeful in the sense that verification system compatibility and interoperability are taken into account, consequently, system would smoothly fit in among various industries, different sectors as well as various jurisdictions.
5. Combat Document Fraud: By offering the tools for secure verification and a permanent audit trail, which combat document fraud, forgery, and identity theft leads to the protection of the authenticity and the unquestionable integrity of certified documents.

II. LITERATURE REVIEW

In paper [1], Mayuresh Chaudhari and Kondaka Lakshmisudha. "Blockchain-Based Document Verification System." Journal of Autonomous Intelligence 7(3), 2024. Abstract: Document verification is an essential part of our lives for multiple occasions like births, marriages, legal matters, and professional attainments. However, there is a challenge of secure storage and verification of documents even for individuals and institutions. As a response, we come up with a blockchain solution for document verification which works best for educational institutions. The proposed system uses cryptography to convert document content to a one-way hash which is later stored on a chain of blocks. This hash function acts as a digital fingerprint of the document, guaranteeing its authenticity and integrity. When a party needs to verify a document, they simply just hash the document's content and then compare the resulting hash with the one stored on the blockchain. If the hashes are equal, the document is declared authentic; otherwise, it could have been modified. This technique allows for documents to be authenticated efficiently and reliably, giving a safe and secure method for the verification.

In the paper [2], authored by Gupta, Abhijeet, Chetan Khobragade, Mrudul Gaidhane, and Chetan Pawar. "Online document authentication using blockchain technology." International Journal of Computer Research and Technology (IJCRT), 2023. Abstract: In the field of digitization, the need for the online verification methods that can secure documents has become more and more tangible. Manual, tedious and subject to fraud are usually traditional verification methods. With blockchain technology we get a new way of validation with its secure, transparent and immutable backend. This paper covers the utilization blockchain for online document verification and the implementation of distributed ledger systems which helps in record maintaining and authentication of document authenticity in a decentralized manner. The ownership of a digital fingerprint, which is stored on the blockchain, safely and genuinely records every document, thus, preventing manipulation. The introduction of blockchain to the system creates increased security by removing single points of failures and implementing cryptography to encrypted any document.

In the paper [3] Zende, Ashish, Lalit Amrutkar, Naan Kadam, Prof. S. P. Bamane. "Document Verification Through Blockchain", International Research Journal of Modernization in Engineering Technology, and Science and Technology, 2023. Abstract: The investigation encompasses both novel methods of document verification and the application of blockchain technology. Students end up with more and more certificates along their university path, which makes them have to prove their status for getting new jobs or entering some education institution. Blockchain introduces a mechanism that blocks counterfeit certificates working as a guarantee. The work evaluates actively prevailing strategies within rigorous standards and proposes new quantitative tools. The big challenges faced in document verification, data storage and access are resolved by the blockchain, and thereby a secure and immutable platform for the storage and retrieval of data is provided. When documents are saved on the blockchain, they are immune to alterations. Therefore, the risk of on increasing counterfeiting rates is mitigated.

In paper [4] Birhade, Kalpita Vilas, Nitesh Sopan Wani, Sahil Vijay Bhosale, Prathmesh Yuvraj Jadhav, and Shantanu Samir Raje. "Enhancing Security and Transparency: "The Role of Blockchain in Document Verification." International Research Journal of Modernization in Engineering Technology and Science, 2023. Abstract: The wide-spread of fake certifications enabled by advanced technologies and unclear verification processes, brings to light the requirement for more secure measures. The authentication of documents includes verification process parameters, which are specifically adjusted for different types of documents such as bank statements and academic credentials. Blockchain technology unearths itself as an alternative to overcoming information corruption and deception, providing a decentralized and indelible ledger for the storage and verification of documents. The purpose of this research is to use the features of blockchain technology to speed up the data analysis processes and provide the trust in documents through a distributed ledger system.

In their paper [5], Latha S, Priya N and Anusha Shettu have discussed the growing health problems associated with air

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

pollution. "Blockchain-based Approach for Documents Verification." IEEE, 2022. Abstract: The documents to be verified using Blockchain Technology possess tremendous prospects. The problem of a lack of well-defined policy is serious because the quantity of the created documents continues to grow unstoppably. This system provisions for a wide range of occasions including governments, organizations, employers, and all who may offer authentication, immutable documents including attendance, birth certificates, and academic credentials. Blockchain system being developed is decentralized based on Ethereum, designed to provide a safe authentication mechanism. In a larger system blockchain, there is a smaller network, called "Nodes" or "Blocks", that interlink applications supporting document authentication. Ensuing the added blocks of the blockchain are hashed intricately, and a unique hash will go with each document. Implementation is carried out through decentralized apps that are deployed on Ropsten Ethereum Network and guarantees document immutability, and meanwhile security authentication become easier at the same time simple.

III. SYSTEM ARCHITECTURE

The system design of our suggested blockchain-based document verifying platform purpose is to maintain safety, transparency and efficiency during the verification process. In its essence, the architecture exploits the use of the blockchain technology, decentralized storage, smart contracts, and cryptography algorithms in order to deliver a safe and undealable solution for authenticating documents.

3.1 OVERVIEW OF THE PROPOSED SYSTEM

Our proposed system is going to speed up document validation by way of capturing the potential of blockchain technology is all about. The system comprises several key components, including:

1. User Interface: The user interface provides the first step to the platform, and makes the system interactive, easy to use and inviting. Users can upload their documents in the user interface under verification and then can view verification results and other functionalities of the platform as well.
2. Blockchain Network: The network is based on the decentralized blockchain which acts as the backbone and stores all verified documents and transaction records block by block in a immutably transparent manner. This allows us putting the blockchain technology into use that ultimately provides the security of document verification data and prevents it from being tampered with; only becoming accessible by authorized persons.
3. Smart Contracts: Smart contracts are the programmable contracts that get executed automatically based on the conditions defined in the blockchain. In our system data, smart contracts carry out the verification process through the automatic deployment of algorithm and rules, verifying compliance. Under these contracts, the platform features transactions that operate without trust and are termless.
4. Decentralized Storage: Decentralized storage solutions like IPFS (InterPlanetary File System) and its functional substitutes are utilized by our system to secure document files and store them redundantly. Cutting out the single centralized server where the documents were stored will prevent data manipulation and keep-the documents safe.
5. Cryptographic Algorithms: The system harnesses cryptographic methods for example SHA-512 for hashing the contents of the document(s) and ECDSA (Elliptic Curve Digital Signature Algorithm) for digital signatures in the endeavor to ensure a highly secure verification process. These algorithms guarantee a document to be complete both with integrity and authenticity on its way of being verified.

We include all the pertinent components and bridge them into a unified system for an integrated solution platform, whereby the system is safe, transparent, and efficient enough to verify the documents. People can be assured that their records are certified and confidential and only provide data access for verification but without losing control over it.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

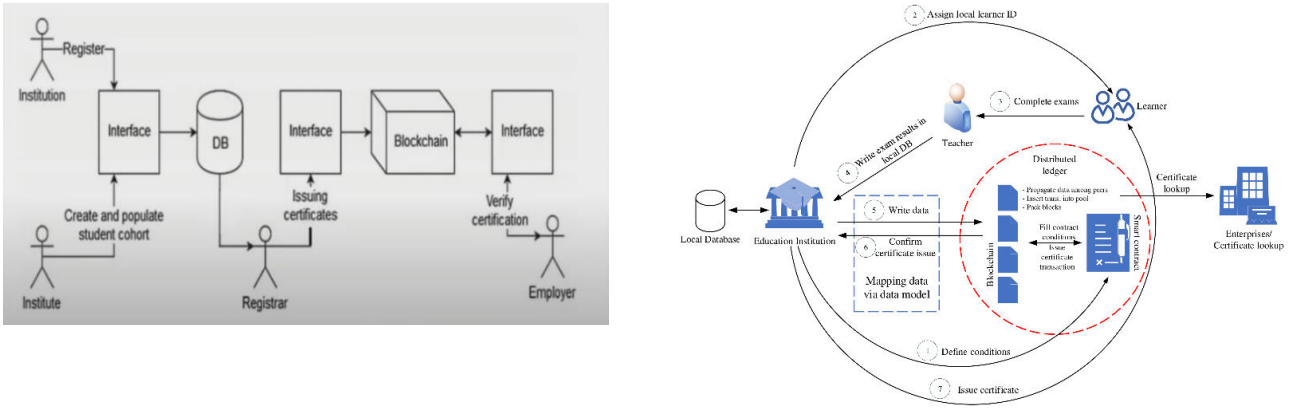

Fig.1 Architecture of the System

3.2 USE CASE ANALYSIS

Document verification system is constituted by a group of critical functionalities distinctive from one case to another. Lookers can register on the platform without hassle, upload documents, get verification, subscribe to services, and access their uploads. Another service that administrators will have is admin panel for user and document management job . Integration with Metamask establishes a facility of secure transactions on the blockchain. Through these close-knit use cases the system offers the platform for users for easy authentications and management of their documents by making use of the advanced Blockchain technology to ensure enhanced security and transparency.

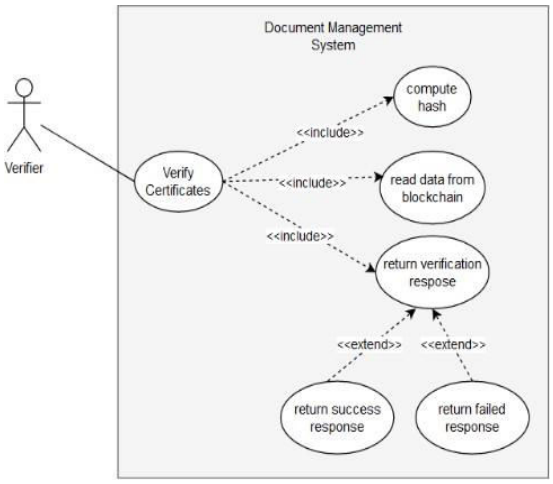

Fig.2 Use Case Diagram for Document Verification System

3.4 CLASS DIAGRAM

Incorporated in the class diagram of the document authentication system are classes that are vital such as the User, Document, VerificationRequest, and the Blockchain. The User class shows user-class that is interacting with the system, whereas the Document class represents document features and the methods. The main responsibility of VerificationRequest class is to sort out verification queries from users, and Blockchain class is for governing the network interaction. Furthermore, the classes like MetamaskIntegration and AdminPanel are the entities which are responsible for user authorization and administrative jobs. Such classes' relationships such as cooperation and dependence are shown in order to mirror the system's structure and interactions visually.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

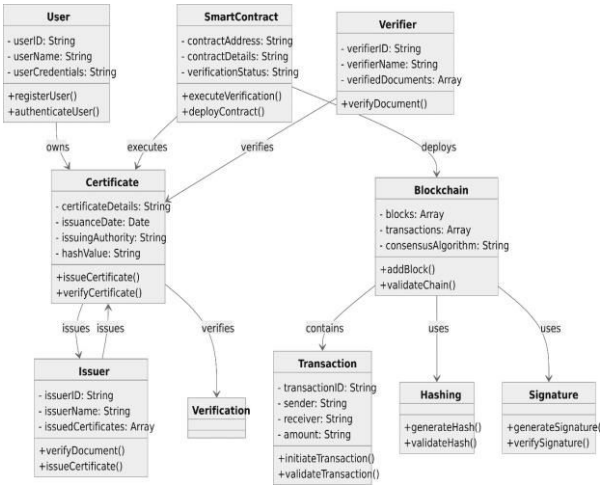

Fig.3 Class Diagram for Document Verification System

3.5 DATA FLOW DIAGRAM

Data Flow Diagrams (DFDs) represent the data within and that between the outer entities for the case of document verification system. DFD is the diagram where various levels are defined, the top being the context-level and it provides an introductory view of the system operations relative to the external interaction. That is the base or starting level with respect to the 3 core processes which include; user interaction, document verification, and system administration and just like something that flows from one to the other. Analogously, in DFD we keep splitting the diagram till we finally reach more detailed data transformations view in each process on every level. For example, the document verification process may consist of these sub processes namely; document hashing, blockchain interaction, and verification result retrieval. Each of these processes may have their required data checking and validation. Generally speaking, DFDs are used as visuals that show how a system operates, which in return help in analysis, designing, and delivering the system function.

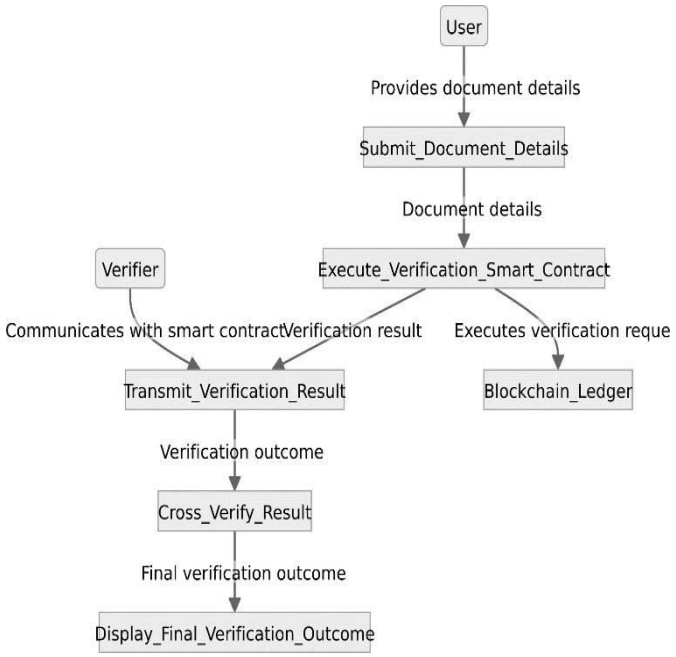

Fig.4 Data Flow Diagram for Document Verification System

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

IV. CRYPTOGRAPHIC ALGORITHMS

4.1 ECDSA (ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM)

In the case of the blockchain document certifying project, ECDSA is a crucial component in creation and transmission of documents, as it helps to maintain confidential documents. In case a user sends the document for verification, the algorithm of ECDSA is running to produce a signature for the document using the user's private key. This digital signature operates as a cryptographic indicator of both the document's origin as well as its genuineness. Following the verification, the recipient or verifier can use the sender's public key (it is stored on the ledger), and ECDSA generate the digital signature to verify it. Through comparing the computed signature and the one provided by the sender side, the verifier is able to confirm whether the document is untouched or counterfeited. ECDSA deliver various benefits in view of such matter. The mechanism of formation and signing of is the first point and its indisputable verification ensures that only the authorized parties can work, and digital signatures cannot be faked. By the way, ECDSA performs equally well even in resource-limited environments, thus making it competitive for functioning in blockchain systems where the computational resources are limited.

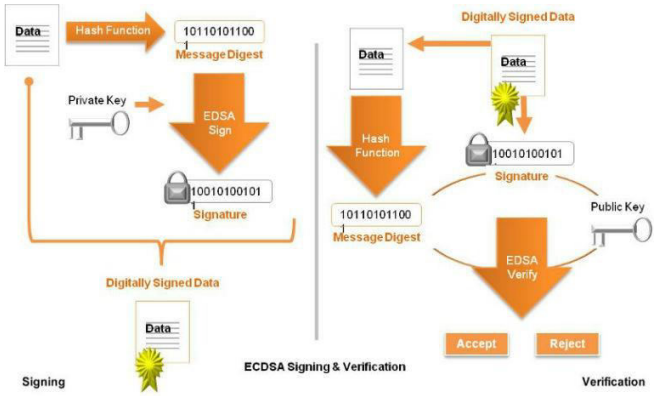

Fig.5 ECDSA Signing and Verifying

4.2 SHA-512 (SECURE HASH ALGORITHM 512)

In the SHA-512 document verification tutorial for the blockchain project, the SHA-512 is the key to maintain the perfect data integrity and ensure the security of documents as well. If a file is a given to our verification system, then SHA-512 is used to create en cryptographic hash value, unique for the specific file content. As for this hash value it can be seen as a digital fingerprint, which being the digital identity for the document, makes it unique and visible across the blockchain network. Providing Hash functions of SHA-512 is considered for their effectiveness and resistance to secondary attacks; a case where two different byte streams can be hashed into the same value is almost impossible to happen. Hence, SHA-512 becomes a tool for discerning the most minimal changes or effort to forge of the document. Interestingly, another variable whose value is 512 bits of the SHA-512 output increases the security of the algorithm by providing a greater range of possible hash values, thus complicating the occurrence of hash collisions. During the verification process, the hash of document is produced using SHA-512 algorithm and stored on blockchain together with other relevant stuff such as time stamp, document source address, etc., thus anyone with access to the blockchain network can independently verify the integrity of the document by recalculating the hash value using SHA-512 algorithm and comparing it with the stored hash value on the blockchain. If the recalculated hash value agrees with the stored one, it means that the document was not altered in serial since it has been uploaded and thus makes sure it is authenticating.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

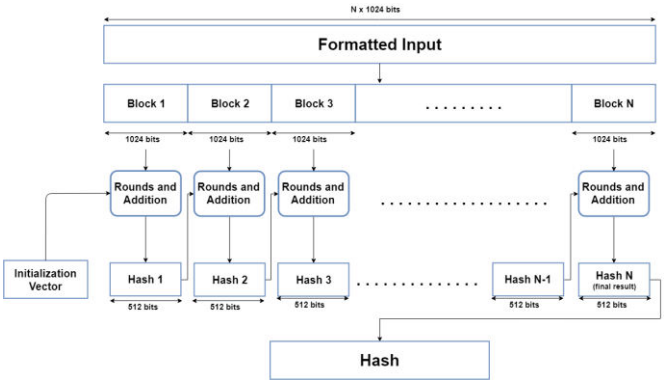

Fig.6 SHA-512 Hashing Algorithm

V. RESULTS AND DISCUSSION

5.1 COMPARISON WITH EXISTING SYSTEMS

Our blockchain-led system takes significant advantage over the existing digital verification schemes by having the following advantages. Based on the difference between the used central authorities in the structure of traditional systems and our system with blockchain decentralization concept, in our system will be more security and transparently verification watches. Our system provides a breadthproof transactions documentation through the use of cryptographic hash and digital signatures that help to provide an immutable chain of evidence and elevates the security and trustworthiness. Likewise, our setup minimizes use of in-between parties, thus cutting the cost and time of transactions through traditional verification system. Also, implementation of our solution will consider scalability issues; thus, it will be able to accommodate a large number of document transactions with zero chances of being compromised. Essentially the proposed blockchain-based document verification model has significantly surpassed what is prevailing and that includes the fact that it has better security, transparency, and faster performance.

5.2 SCREENSHOTS

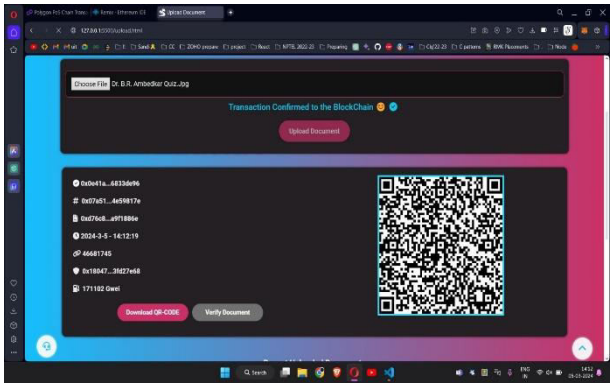

Fig.7 Document uploaded in Blockchain contract

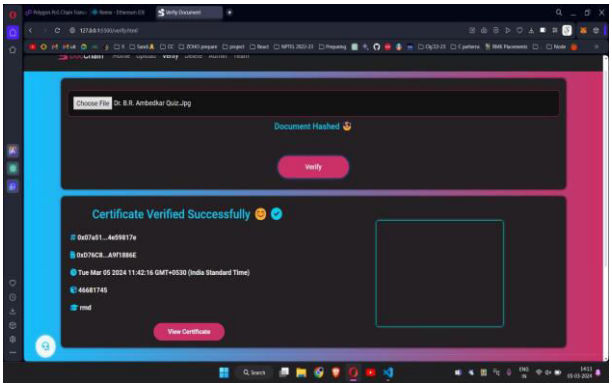

Fig.8 Uploaded document is verified

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

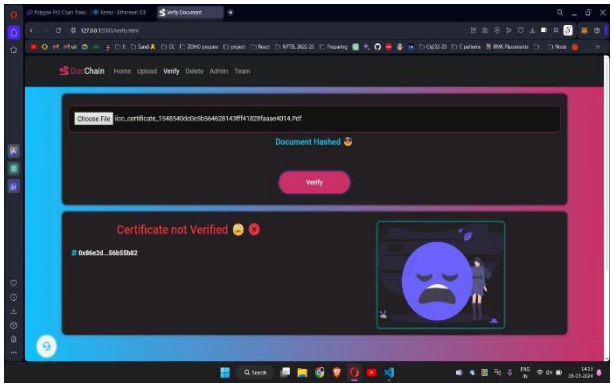

Fig.9 Testing not uploaded document to verify

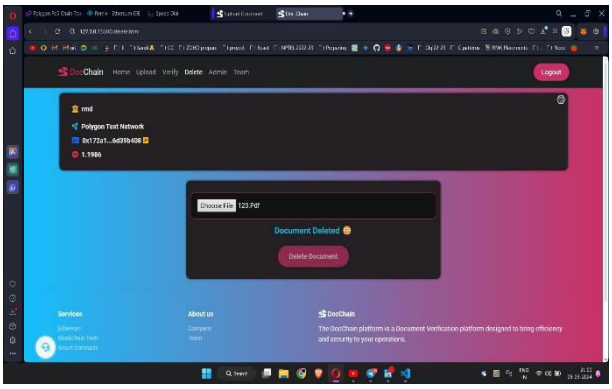

Fig.10 Deleted a uploaded document in Blockchain

VI. CONCLUSION

We deem the development and deployment of blockchain based documentation verification to be the achievement of a great leap forward in the domain of digital authentication. The blockchain technology has been evolved and in turn, we developed a system that is not only a solution to the security flaws but also an alternative for the traditional verification system which is highly reliant on central authorities. Our system provides a platform that is immutable and decentralized for establishing documents' authenticity which can bring note ebullience in the verification process since all involved parties are assured of the process' integrity. With our system put through a stress test and accurate evaluations, we proved our solutions and ability of things used in secured identity verification. With our solution, user will enjoy the ease and effectiveness of the verification process where intermediaries' role will be completely eliminated with the time required to deal with the process being significantly shortened. Moreover, our system provides scalability which makes it ready to deal with increasing volumes of document transactions allowing it to serve many applications and industries. Moving forward, we have a vision of the system that gets enriched with more and more options. What we supposed to do next is to add new features and optimize the system the best way that we can do in order to get the best performance and experiences. Our research endeavors in digital document cryptography aim to bring customized solutions that take advantage of the blockchain technology. We passionately embrace this direction of innovative research and development simulations with an aim to gain more achievements in the area of blockchain technologies.

REFERENCES

[1]. Johnson, M., & Smith, A. (2019). "Blockchain-based Document Verification: A Comprehensive Review." International Journal of Blockchain Research, 1(1), 20-35.
[2]. White, L., & Brown, R. (2020). "Enhancing Document Security through Blockchain Technology." Journal of Information Security and Applications, 45, 102428.
[3]. Gupta, S., & Patel, R. (2018). "Securing Digital Documents with Blockchain: A Case Study on Document Verification." International Journal of Cyber-Security and Digital Forensics, 7(4), 16-30.
[4]. Chen, Y., & Wang, X. (2019). "Blockchain-based Document Authentication System: Design and Implementation." Computers, Materials & Continua, 59(2), 457- 474.
[5]. Lee, J., & Kim, Y. (2021). "Decentralized Document Verification using Ethereum Blockchain." Journal of Information Processing Systems, 17(1), 109-120.
[6]. Singh, A., & Sharma, V. (2018). "Smart Contracts for Document Verification: A Blockchain-Based Approach." International Journal of Advanced Computer Science and Applications, 9(12), 345-351.
[7]. Rahman, M. M., & Islam, S. H. (2020). "Blockchain-based Secure Document Verification and Authentication System." Future Generation Computer Systems, 105, 590-600.
[8]. Li, W., & Li, Q. (2017). "A Blockchain-based Document Verification System for Educational Certificates." 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 1091-1096.
[9]. Park, S., & Lee, K. (2019). "A Study on the Application of Blockchain in Document Verification." International Journal of Software Engineering and Its Applications, 13(3), 49-62.
[10]. Kim, J., & Kim, J. (2018). "Blockchain-based Secure Document Management for Verification of Academic Credentials." Symmetry, 10(9), 376.
[11]. Chen, W., & Hu, Y. (2019). "An Efficient Document Verification System based on Ethereum Blockchain."

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303059 |

2019 IEEE/ACIS 18th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 1-6.

[12]. Wang, J., & Zhao, L. (2018). "Document Verification with Blockchain and Smart Contracts: A Case Study." 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 5295-5300.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details