DockLock - Documentation Locker using Blockchain

A

Report submitted in partial fulfilment of the requirement for the

degree of

B.Tech.

In

Computer Science & Engineering
(Internet of Things)

By

Aayushman Mishra (2101641550002)

Abhishek Gupta (2101641550006)

Krishna Varma (2101641550046)

Kushagrah Pathak (2101641550047)

Under the guidance of

Miss Puja Kumari

(Assistant Professor)

Project Id: 23_CS_IOT_3A_06

PSIT
Kanpur

Pranveer Singh Institute of Technology, Kanpur
Dr A P J A K Technical University
Lucknow

DECLARATION

This is to certify that Report entitled “DockLock - Documentation Locker using Blockchain”which is submitted by me in partial fulfilment of the requirement for the award of degree B.Tech. in Computer Science and Engineering to Pranveer Singh Institute of Technology, Kanpur Dr. A P J A K Technical University, Lucknow comprises only my own work and due acknowledgement has been made in the text to all other material used.

Date:

Aayushman Mishra (2101641550002)
Abhishek Gupta (2101641550006)
Krishna Varma (2101641550046)
Kushagrah Pathak (2101641550047)

Approved By:

Prof. (Dr.) Vishal Nagar
Dean
Computer Science and Engineering
PSIT, Kanpur

Certificate

This is to certify that Report entitled “DockLock - Documentation Locker using Blockchain” which is submitted by Aayushman Mishra (2101641550002), Abhishek Gupta (2101641550006), Krishna Varma(2101641550046), Kushagrah Pathak (2101641550047), in partial fulfillment of the requirement for the award of degree B.Tech. in Computer Science & Engineering to Pranveer Singh Institute of Technology, Kanpur affiliated to Dr. A P J A K Technical University, Lucknow is a record of the candidate own work carried out by him under my/our supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Date:

Signature

Miss Puja Kumari

(Assistant Professor)

-

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B.Tech. Project undertaken during B.Tech. Third Year. We owe special debt of gratitude to our project supervisor Mr Rajat Verma, Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur for his constant support and guidance throughout the course of our work. His sincerely, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavours have seen light of the day.

We also take the opportunity to acknowledge the contribution of Professor Dr. Vishal Nagar, Dean, Department of Computer Science & Engineering, Pranveer Singh Institute of Technology, Kanpur for his full support and assistance during the development of the project.

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

Signature

Name: Aayushman Mishra

Roll No.:2101641550002

Signature

Name: Abhishek Gupta

Roll No.:2101641550006

Signature

Name: Krishna Verma

Roll No.:2101641550046

Signature

Name: Kushagrah Pathak

Roll No.:2101641550047

ABSTRACT

.

A Document Locker using blockchain technology is a revolutionary approach to safeguarding your critical documents, whether they are personal records, financial documents, legal contracts, or any other sensitive information. This technology leverages the principles of blockchain to create an immutable, decentralized, and highly secure storage solution.

In an increasingly digitized world, the need for secure and trustworthy methods of document storage and management has never been more critical. Traditional approaches to safeguarding sensitive information, such as passwords and physical file cabinets, have demonstrated vulnerabilities to data breaches and tampering. Enter the Document Locker using blockchain technology – a groundbreaking solution that leverages the power of blockchain to redefine how we protect and manage our most important documents. In the past, raw data are transferred to a cloud server to be stored and analyzed. However, this centralized solution has caused serious concerns regarding several aspects, such as the necessity to trust the cloud infrastructure security, control loss once data is externalized, and lack of data handling transparency. Consequently, blockchain-based data management emerged as a platform to facilitate transparent data transactions between untrustworthy involved parties on the network. Indeed, peer-to-peer-network-based data management is a more fair system as compared to a system where all transactions are handled by a central server. This decentralization of data management allows us for better storage and access of documents one can store. A blockchain based storage facility can be incorporated in day to day file management. One way of doing this includes the usage of smart contracts.

TABLE OF CONTENT

LIST OF FIGURES

Chapter I. Motivation

1.1 Motivation

The concept of "Doclock" using blockchain technology refers to **securing and authenticating documents** through the use of blockchain. Blockchain is a **decentralized and distributed ledger** that ensures transparency, immutability, and security of data [1]. Here are some motivations for implementing a Doclock system using blockchain:

1. Immutability

Blockchain provides a tamper-proof and immutable record of transactions. Once a document is added to the blockchain, it cannot be altered or deleted. This ensures the integrity of the document over time, making it a reliable source of truth.

2. Decentralization

Unlike centralized systems, blockchain operates on a decentralized network of nodes. This eliminates the need for a central authority to validate and verify documents. Decentralization **enhances reliability and reduces the risk** of a single point of failure or manipulation.

3. Security

Blockchain uses cryptographic techniques to secure data, making it **highly resistant to tampering** or unauthorized changes. This enhanced security is crucial for sensitive documents such as legal contracts, medical records, and intellectual property.

1.2. Background of the problem:

The problem of ensuring the integrity, security, and authenticity of documents has been a longstanding challenge in various industries [22]. **Traditional methods of document management often rely on centralized databases**, physical signatures, and manual verification processes, which can be susceptible to fraud, tampering, and inefficiencies [2].

Here's a background on the issues associated with document management that have led to the exploration of blockchain solutions.

1. **Fraud and tempering**

   Traditional document systems are vulnerable to fraud, as malicious actors can manipulate or forge documents without leaving a clear trace. Tampering with critical documents such as legal contracts, financial records, or academic transcripts can have severe legal and financial consequences.

2. **Complex Verification Processes**

   Authentication and verification of documents often involve lengthy and complex processes, requiring multiple intermediaries and manual checks. This complexity can result in delays, increased costs, and potential errors in the verification process.

1.3 Current System

As of last knowledge update in January 2022, various projects and systems based on blockchain technology have been developed to address the challenges associated with document management and verification. Keep in mind that the landscape is dynamic, and new developments may have occurred since then [3].

It's important to stay updated on the latest developments in this rapidly evolving field, as new projects and advancements are continuously emerging [21]. Additionally, the adoption and success of blockchain-based document management systems depend on factors such as regulatory acceptance, industry collaboration, and user adoption.

1.4 Issues in Current System

Current documentation lockers, while providing digital convenience, suffer from several critical issues. Centralized storage makes them **vulnerable to hacking and data breaches**, leading to privacy concerns and potential document manipulation. Additionally, reliance on centralized authorities creates single points of failure, **risking data loss in case of server crashes or outages**. Furthermore, traditional systems **lack transparency** and auditability, making it difficult to verify document authenticity and track access history.

Blockchain technology offers a promising solution by addressing these concerns through its core principles: decentralization, immutability, and transparency [4]. By distributing document records across a network of nodes, blockchain creates a tamper-proof ledger, ensuring data integrity and preventing unauthorized modifications. Its open nature allows for transparent audit trails, enhancing accountability and trust.

While challenges like scalability and energy consumption remain, blockchain-based documentation lockers hold immense potential to revolutionize document management, offering enhanced security, reliability, and trust.

1.5. Functionality Issue

Blockchain-powered documentation lockers promise a secure and transparent future for storing and sharing sensitive documents. However, these systems are not without their challenges. One key area of concern is functionality.

1. **Limited Scalability:** Blockchains can handle a finite number of transactions per second, which can be limiting for large-scale document storage and sharing. Imagine a highway with too many cars; things get congested and slow down.

2. **Limited Functionality:** Compared to traditional lockers, blockchain-based systems may lack features like advanced search, version control, and collaborative editing.

1.6. Security Issue

The implementation of a documentation locker using blockchain introduces several security considerations that must be carefully addressed. While blockchain is renowned for its inherent security features, vulnerabilities can arise in the implementation, smart contracts, or the surrounding ecosystem. Smart contract vulnerabilities, such as coding errors or flaws in the execution logic, can potentially **lead to unauthorized access or manipulation of stored documents [5]**. Additionally, the reliance on cryptographic keys for document access and verification introduces a new layer of security concerns, as the compromise of private keys could result in unauthorized access or loss of sensitive information. Ensuring the secure storage and handling of cryptographic keys becomes paramount.

Furthermore, the decentralized nature of blockchain networks, while providing resilience against certain attacks, also **introduces challenges related to network security and consensus mechanisms**. Ongoing vigilance, regular security audits, and adherence to best practices are essential to mitigate these security issues and enhance the robustness of a documentation locker using blockchain technology [6].

1.7 Problem Statement

The implementation of a documentation locker using blockchain technology faces several critical challenges, leading to a compelling problem statement [20]. Scalability emerges as a central concern, with the potential for increased transaction volumes causing congestion and reduced efficiency within the blockchain network. Integrating the documentation locker seamlessly with existing systems introduces complexities, including compatibility issues and the need for workflow adjustments, which may disrupt established processes. Security becomes a paramount issue, **encompassing vulnerabilities in smart contracts**, cryptographic key management, and the broader blockchain ecosystem. These vulnerabilities pose risks of unauthorized access, data manipulation, and compromise of sensitive information. The absence of standardized protocols impedes interoperability, hindering the smooth exchange of documents across diverse blockchain implementations. Additionally, achieving legal recognition for documents stored in the blockchain encounters challenges, as regulatory frameworks struggle to adapt to the evolving landscape of blockchain technology [21]. Addressing these challenges is crucial for the successful implementation of a documentation locker using blockchain, requiring comprehensive solutions to ensure scalability, security, interoperability, and legal compliance

1.8 Proposed Work

The proposed work on the Documentation Locker focuses on enhancing its functionality, security, and user experience. The key objectives include:

1. Scalability Enhancement
2. Integration with Existing System
3. Advanced Security Measures
4. Standardization Protocol

6. User Experience Optimization

By addressing these objectives, the proposed work aims to position the Documentation Locker as a secure, scalable, and user-friendly solution for document management within the organization.

1.9 Organization of Report

This report provides an overview of the organization's efforts in implementing a Documentation Locker using blockchain technology. The purpose of the Documentation Locker is to offer a secure, scalable, and interoperable solution for managing sensitive documents within our organization. This report outlines the project's goals, progress, challenges, and proposed strategies for future development [7].

Chapter II. Literature Review

2.1 Literature Review

A literature review on a documentation locker using blockchain would typically involve exploring various academic and industry publications that discuss the integration of blockchain technology into document management systems [8]. Below is a hypothetical literature review outline for such a topic:

1. Introduction to Blockchain Technology:

- Overview of blockchain technology and its fundamental principles.
- Explanation of how blockchain works, including decentralized and distributed ledger concepts.

2. Blockchain in Document Management Systems:

- Review of literature on the application of blockchain in document management systems.
- Exploration of how blockchain ensures immutability and tamper-proofing of documents.
- Discussion on the role of smart contracts in automating document-related processes.

3. Security and Trust in Documentation Lockers:

- Examination of how blockchain enhances security in document storage and sharing.
- Review of studies assessing the trustworthiness of blockchain-based documentation lockers

4. Decentralization and Redundancy:

- Exploration of the benefits of decentralization in document storage and access.
- Discussion on how blockchain ensures redundancy and fault tolerance in documentation lockers.

5. Interoperability and Integration:

- Review of literature on the interoperability of blockchain-based documentation lockers with existing systems.
- Discussion on challenges and solutions for integrating blockchain into document workflows.
- Exploration of case studies highlighting successful integration strategies.

6. Use Cases and Case Studies:

- Analysis of specific use cases where blockchain has been successfully applied to documentation lockers.
- Examination of case studies in various industries such as healthcare, finance, or legal

7. Future Trends and Research Directions:

- Exploration of emerging trends in blockchain-based document management.
- Identification of gaps in current research and suggestions for future research directions.
- Discussion on potential advancements in blockchain technology that could impact documentation lockers.

8. Challenges and Limitations:

- Identification and analysis of challenges associated with implementing blockchain in documentation lockers.
- Exploration of scalability issues and potential solutions.

- Review of literature discussing regulatory and compliance challenges.

9. Conclusion:

- Summarization of key findings from the literature review.
- Emphasis on the potential of blockchain in enhancing the security, transparency, and efficiency of documentation lockers.
- Closing remarks on the importance of continued research in this area.

2.1 Methodology

Methodology for a documentation locker using blockchain involves breaking down the project into manageable tasks and defining the steps needed to achieve your goals [9]. Here's a suggested planning framework:

1. Define Project Goals and Objectives:

I. Clearly articulate the overall goals and objectives of implementing the documentation locker.

II. Specify the desired outcomes and benefits.

2. Conduct a Feasibility Study:

I. Evaluate the feasibility of the project by considering technical, economic, legal, and operational aspects.
II. Identify potential challenges and assess their impact on the project.
III. Stakeholder Identification and Engagement:
IV. Identify and engage with key stakeholders, including end-users, administrators, IT staff, and decision-makers.
V. Understand their requirements and expectations.

3. Requirements Gathering:

I. Conduct detailed requirements gathering sessions with stakeholders.

II. Document both functional and non-functional requirements, including document types, access controls, encryption, and integration needs.

4. Define Scope and Deliverables:

I. Clearly define the scope of the project, outlining what is included and what is not.

II. Identify the deliverables at each stage of the project.

5. Select Blockchain Platform:

I. Choose a suitable blockchain platform based on project requirements.

II. Consider factors such as scalability, consensus mechanisms, and developer community support.

6. Smart Contract Design:

I. Define the functionality of smart contracts governing document-related processes.

II. Specify conditions for document storage, retrieval, access permissions, and any automated processes within the smart contracts.

7. System Architecture Design:

I. Develop the overall architecture of the documentation locker system.

II. Define how the blockchain network will interact with the front-end user interface and back-end document storage.

III. Consider scalability, security, and interoperability.

8. Documentation:

I. Develop comprehensive documentation for users, administrators, and developers.

II. Include user manuals, system architecture documentation, and troubleshooting guides.

9. Quality Assurance:

I. Implement quality assurance processes throughout the development lifecycle.

II. Conduct peer reviews, code reviews, and testing to ensure the quality of the documentation locker system.

10. Project Review and Evaluation:

I. Conduct a project review after deployment to assess the success of the implementation.

II. Gather feedback from stakeholders and identify areas for improvement.

Planning of work in ‘Documentation locker using blockchain’ comprised of three stages; identification, selection, and evaluation –

1. Identification:

The objective of the project is to **develop a decentralized storage system** using blockchain. Initially the data owner first registers themselves. After registering successfully, the owner logs in and uploads a file using the file picker. The system checks the file size and ensures storage availability in the network. The file is uploaded when enough storage is available [10]. Then the system performs steps. **The uploaded file is encrypted using AES 256 bit algorithm**. The encryption key is generated using the owner’s wallet address and randomly generated salt value. This encryption key along with an IV is used to encrypt the owner's data. This maintains the confidentiality of the data.

2. Selection:

In order to implement these decentralized storage systems we need to implement Smart Contracts using Remix IDE and the **source code is written into a contract using Solidity**. These contracts will then be deployed on the web using Ganache which runs our Ethereum based blockchain storage system on the web [11].

3. Evaluation:

This part includes the evaluation of our suggested design model. We will be looking out for some major points such as **handling contracts, maintaining a smooth user experience by**

the way of providing easy access to their data and simultaneously securing them. Another point of evaluation will be to check upon the student friendly environment of the application which is the whole purpose of the design [12]. We will also be looking at the interfacing of API's between the web application and the smart contracts. for reviews and evaluation -

- Conduct a project review after deployment to assess the success of the implementation.

- Gather feedback from stakeholders and identify areas for improvement

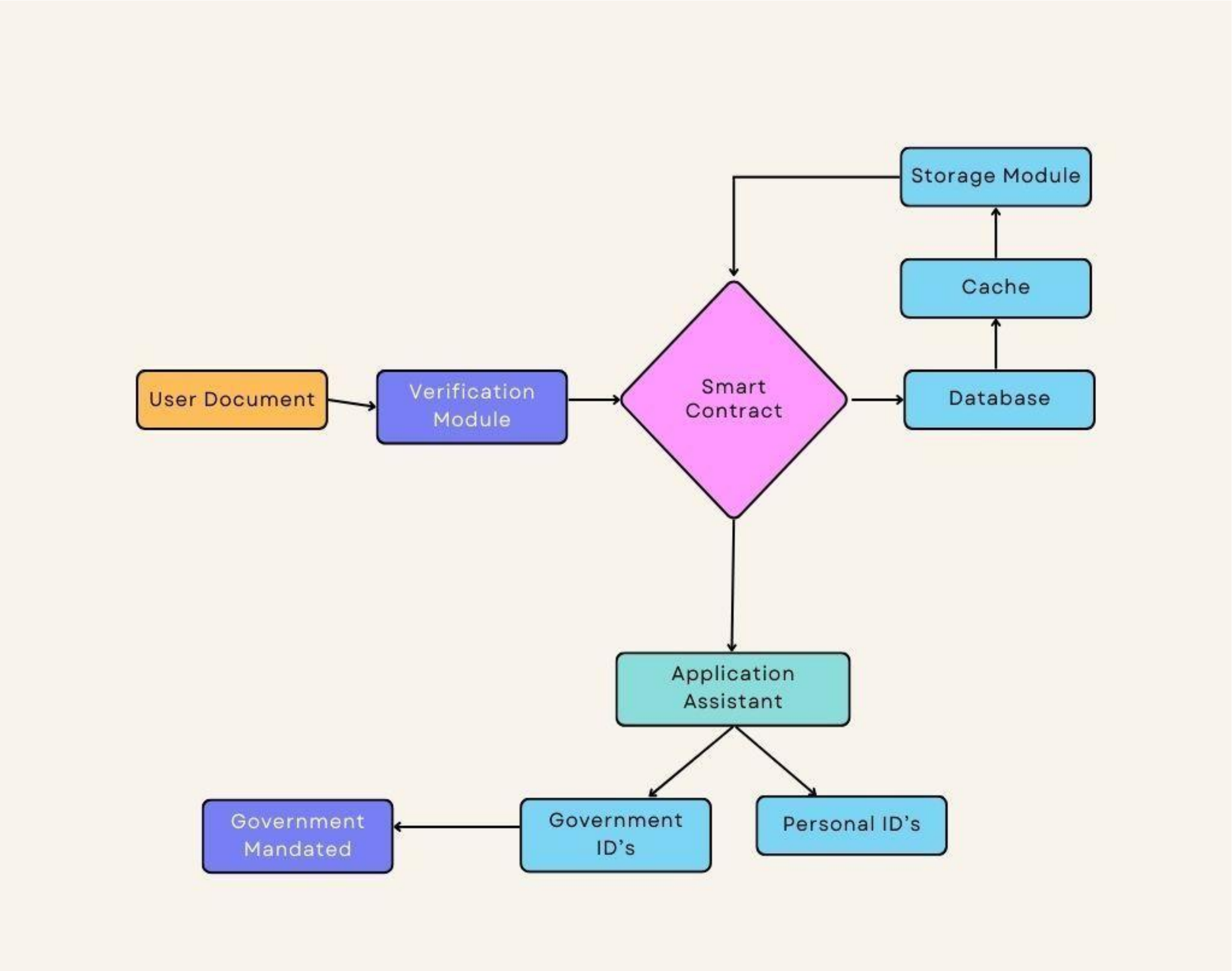

Fig 2.1 Authentication Diagram

Chapter III. Implementation

3.1 Creating a Wallet

Install MetaMask in your Chrome browser and enable it. Once it is installed, click on its icon on the top right of the browser page. Clicking on it will open it in a new tab of the browser.
Click on "Create Wallet" and agree to the terms and conditions by clicking "I agree" to proceed further. It will ask you to create a password.
After you create a password, it will send you a secret backup phrase used for backing up and restoring the account. Do not disclose it or share it with someone, as this phrase can take away your Ethers.

3.2 Adding Ethereum to the wallet

In case you want to test the smart contract, you must have some dummy ethers in your MetaMask wallet. For example, if you want to test a contract using the Robsten test network, select it and you will find 0 ETH as the initial balance in your account. To add dummy ethers, click on the "Deposit" and "Get Ether" buttons under Test Faucet. Once the dummy ethers are added to the wallet, you can start writing smart contracts on the Remix Browser IDE in the Solidity programming language.

3.3 Using Remix to write a Smart Contract

We will use Remix Browser IDE to write our Solidity code. The remix is the best option for writing smart contracts as it comes with a handful of features and offers a comprehensive development experience.
It is usually used for writing smaller-sized contracts. Remix's features include:

- Warnings like gas cost, unsafe code, checks for overlapping variable names, whether functions can be constant or not
- Syntax and error highlighting
- Functions with injected Web3 objects
- Static analysis

- Integrated debugger
- Integrated testing and deployment environment
- Deploy directly to Mist or MetaMask

3.4 Deploying the contract

Deploy the smart contract at the Ethereum test network by pressing the deploy button at the Remix window's right-hand side [20]. Wait until the transaction is complete. After the transaction commits successfully, the address of the smart contract would be visible at the right-hand side of the remix window.

At first, all the ERC20 tokens will be stored in the wallet of a user who is deploying the smart contract.

To check the tokens in your wallet, go to the metamask window, click add tokens, enter the smart contract address and click ok. You would be able to see the number of tokens there.

1. To make your smart contract live, switch to the main ethereum network at metamask
2. Add some real ethers.
3. Now again, deploy your smart contract using remix as mentioned in the above steps.
4. When a smart contract is deployed successfully, visit http://www.etherscan.io and search your smart contract address there. Select your smart contract.
5. Now you need to verify your smart contract here, click "verify the contract."
6. Copy your smart contract code and paste it at Etherscan. Select the same compiler version that you selected at remix to compile your code.
7. Check "optimization" to Yes, if you had selected optimization at remix; otherwise, select No.
8. Click Verify.
9. It will take a few minutes and your smart contract will be live if no issue occurs.
10. You can now run your smart contract methods at Etherscan.

3.5 Tools Required

- **Truffle**

  Truffle is an Ethereum development framework that allows developers to write and test smart contracts. Written in JavaScript, Truffle contains a compiler for the Solidity programming language. Truffle Contract is a JavaScript library that allows importing of compiled smart contracts.

- **Web3.js**

  It is an Ethereum JavaScript API that interacts with the Ethereum network via RPC calls.

- **Visual Studio Code**

  A functional code editor.

- **Ganache CLI**

  It is an Ethereum remote procedure call client within the Truffle framework that is also known as TestRPC.

- **Parity**

  It is a secure and fast Ethereum client for handling Ethereum accounts and tokens.

- **Node.js**

  It is a javascript runtime environment used for server-side programming. Node.js is required to test the Ethereum smart contract's functionality while ensuring its secure and proper operation. You need to install a package manager, for example, Yarn along with Node.js.

Chapter IV. Testing/ Analysis

4.1 Selecting a Test Network

You might also find the following test networks in your MetaMask wallet:

- Robsten Test Network
- Kovan Test Network
- Rinkeby Test Network
- Goerli Test Network

4.2 Testing our Smart Contract

1. Try to run all your smart contract methods like transfer, total supply, and balance(in the above smart contract example). These methods are present at the right-hand side of the remix window and you can run all the processes from there itself.
2. Try to transfer some tokens to other ethereum wallet addresses and then check the balance of that address by calling the balance method.
3. Try to get total supply by running the total supply method.

Chapter V. CONCLUSION AND FUTURE ENHANCEMENT

5.1 Conclusion

The longstanding problem of counterfeit and altered documents within institutional structures has been exacerbated by issues such as poor communication between document issuers and verifiers, and the absence of a standardized method for record-keeping. However, in recent times, the employment of blockchain technology has emerged as a potential solution to these concerns [14]. Through the replacement of traditional hard-copy documents with their digital counterparts, **the system endeavours to streamline and optimize the verification process for electronic documentation**, enhance fraud detection capabilities, and maximize cost-effectiveness. Given the inherent transparency of the system's publishing and verification protocols, coupled with its ability to authenticate and validate provided information, blockchain-based technology is able to effectively curtail the creation of fraudulent electronic

documentation.

Blockchain technology, an innovation that was originally introduced for Bitcoin and subsequently adopted by many other cryptocurrencies, has the potential to try to alter nearly every aspect of our existence, including but not limited to, finance, supply chain management, identity verification, and voting systems. Despite its widespread adoption and increased popularity, the blockchain sector is still in its infancy, offering ample opportunities for novel and innovative applications of this technology, particularly in the realm of creating a system of collective trust among its users [15].

5.2 Future Scope

Blockchain technology holds immense potential for the future of online document verification, owing to its decentralized, immutable, and tamper-proof nature, which eliminates the requirement for a central authority and enables multiple parties to access the same information [16]. The wide range of potential applications of blockchain technology in online document verification includes but is not limited to:

- Identity Verification: Identity documents like passports, licences, and national ID cards can be safely stored and verified using blockchain technology. These documents can be authenticated using blockchain in real time and without the need for a centralised authority.

- Educational Certificates: Academic credentials are easily verifiable by employers and educational institutions worldwide because to the ability of educational institutions to issue and preserve them on blockchain.

- Medical Records: Blockchain technology allows for the secure and open sharing of medical records by healthcare providers. This will assist in lowering errors and enhancing patient outcomes.

- Legal Documents: A blockchain-based record of ownership and transaction history can be created by storing legal documents including contracts, deeds, and patents.

- Financial Documents: Financial firms can utilise blockchain to track and verify documents like investment contracts, insurance policies, and loan agreements.

In general, blockchain-based online document verification has the potential to greatly reduce fraud and raise transparency across a range of businesses [17]. We can anticipate seeing more cutting-edge uses for blockchain in document verification as the technology develops.

5.3 Future Enhancement

Enhancing a Documentation Locker using blockchain technology can bring several benefits such as increased security, transparency, and immutability [18]. Here are some future enhancement ideas for a Documentation Locker using blockchain:

Immutable Document History:

- Implement a blockchain to create an immutable ledger of document changes and access logs. Each document revision or access attempt is recorded in the blockchain, providing a transparent and tamper-proof history.

Smart Contracts for Access Control:

- Use smart contracts to automate access control policies. Define rules within the smart contract that determine who can access, modify, or transfer ownership of a document. This ensures that access permissions are enforced automatically without the need for a centralized authority

Decentralized Storage:

- Integrate decentralized storage solutions, such as InterPlanetary File System (IPFS) or similar protocols, to store documents.

- This ensures that documents are distributed across a network of nodes, reducing the risk of data loss and increasing resilience against attacks.

Digital Signatures and Attestations:

- Utilize blockchain-based digital signatures and attestations to verify the authenticity of documents [19]. This can be especially useful for legal or contractual documents, where the parties involved can sign and timestamp the document on the blockchain, providing a tamper-evident record.

Tokenization of Documents:

- Consider tokenizing documents as non-fungible tokens (NFTs) on a blockchain. This provides a unique and verifiable representation of each document, making it easy to track ownership, provenance, and transfer of documents securely.

Interoperability with Other Blockchains:

- Ensure interoperability with other blockchain networks. This can facilitate cross-platform document sharing and authentication, allowing users to interact with documents stored on different blockchain networks seamlessly.

Consensus Mechanisms for Governance:

- Implement decentralized consensus mechanisms for governance purposes. Allow stakeholders to participate in decision-making processes regarding the rules and policies governing the Documentation Locker. This enhances the democratic and decentralized nature of the system.

Integration with Identity Management Systems:

- Integrate with blockchain-based identity management systems to enhance user authentication and authorization processes. This ensures that only authorized users with verified identities can access and modify documents within the locker.

REFERENCES

[1] S. T. Ahmed and M. S. Hossain, "An online document verification system using blockchain

technology," 2018 IEEE International Conference on Electrical, Computer and Communication

Engineering (ECCE), Cox's Bazar, 2018, pp. 720-723.

[2] F. C. C. De Souza, F. V. Dos Santos, R. A. L. Righi and A. S. Kofuji, "A blockchain-based online document verification system for academic certificates," 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, 2018, pp. 528-534.

[3] S. H. Kim, S. H. Kim and M. Y. Chung, "A blockchain-based approach for online document verification," 2018 International Conference on Information and Communication Technology Convergence (ICTC).

[4] B. C. Lee, J. W. Kim and J. H. Kim, "Blockchain-Based Online Document Verification System for Government and Business Applications," in IEEE Access, vol. 6, pp. 15593-15599, 2018.

[5] S. Roy and A. Jain, "An Online Document Verification System using Smart Contracts and Blockchain Technology," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0206-0211.

[6] S. A. Sultana and S. T. Ahmed, "A Blockchain-Based Secure Online Document Verification System," 2020 IEEE 12th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 2020, pp. 71-74.

[7] F. Ahmad, N. Naseer, and A. Zaman, "Secure Online Document Verification using Blockchain," 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020, pp. 214-219.

[8] H. A. Alshahrani and S. A. Alshebeili, "A Blockchain-based Online Document Verification System for E-Learning," 2021 IEEE International Conference on Computer and Information Technology (CIT), Riyadh, Saudi Arabia, 2021, pp. 1-4. www.ijcrt.org © 2023 IJCRT | Volume 11, Issue 6 June 2023 | ISSN: 2320-2882 IJCRT2306173 International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org b569

[9] B. K. Das and D. N. Kundu, "Online Document Verification System using Blockchain Technology," 2021 International Conference on Computational Intelligence and Data Science (ICCIDS), Kolkata, India, 2021, pp. 1-6.

[10] Leible, Stephan and Schlager, Steffen and Schubotz, Moritz and

Gipp, Bela. (2019). A Review on Blockchain Technology and

Blockchain Projects Fostering Open Science. Front. Blockchain 2:16. doi: 10.3389/fbloc.2019.00016

[11] Joshi, Archana and Han, Meng and Wang, Yan. (2018). A survey on security and privacy issues of blockchain technology. Mathematical Foundations of Computing. 1. 121-147. 10.3934/mfc.2018007.

[12] Chen, Wubing and Xu, Zhiying and Shi, Shuyu and Zhao, Yang and Zhao, Jun. (2018). A Survey of Blockchain Applications in Different Domains. 17-21. 10.1145/3301403.3301407.

[13] Gilani, Komal and Bertin, Emmanuel and Hatin, Julien and Crespi, Noel. (2020) A survey on blockchain-based identity management and decentralized privacy for personal data. BRAIN 2020: 2nd conference on Blockchain Research and Applications for Innovative Networks and Services, Sep 2020, Paris, France. pp.97-101, 〈10.1109/BRAINS49436.2020.9223312〉.〈hal-02650705〉

[14] Wang, Junyao and Wang, Shenling and Junqi, Guo and Du, Yanchang and Cheng, Shaochi and Li, Xiangyang. (2019). A Summary of Research on Blockchain in the Field of Intellectual Property. Procedia Computer Science. 147. 191-197. 10.1016/j.procs.2019.01.220.

[15] Rouhani, Sara and Deters, Ralph. (2019). ”Security, Performance, and Applications of Smart Contracts: A Systematic Survey,” in IEEE Access, vol. 7, pp. 50759-50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[16] Yue, Dongdong and Li, Ruixuan and Zhang, Yan and Tian, Wenlong and Peng, Chengyi. (2018).”Blockchain Based Data Integrity Verification in P2P Cloud Storage,” 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, Singapore, 2018, pp. 561-568, doi: 10.1109/PADSW.2018.8644863.

[17] Teymourlouei, Haydar and Jackson, Lethia. (2019). Blockchain: Enhance the Authentication and Verification of the Identity of a User to Prevent Data Breaches and Security Intrusions.

[18] Zhu, Xingxiong. (2020). Blockchain-Based Identity Authentication and Intelligent Credit Reporting. Journal of Physics: Conference Series. 1437. 012086. 10.1088/1742-6596/1437/1/012086.

[19] Arjomandi, Larry M. and Khadka, Grishma and Xiong, Zixiang and Karmakar, Nemai C. (2018).”Document Verification: A CloudBased Computing Pattern Recognition Approach to Chipless RFID,” in IEEE Access, vol. 6, pp. 78007-78015, 2018, doi: 10.1109/ACCESS.2018.2884651.

[20] Musarella, Lorenzo and Buccafurri, Francesco and Lax, Gianluca and Russo, Antonia. (2019). Ethereum Transaction and Smart Contracts among Secure Identities.

[21] Lakmal, Chanaka and Dangalla, Sachithra and Herath, Chandu and Wickramarathna, Cham in and Dias, Gihan and Fernando, Shantha. (2017). ”IDStack — The common protocol for document verification built on digital signatures,” 2017 National Information Technology Conference (NITC), Colombo, 2017, pp. 96-99, doi: 10.1109/NITC.2017.8285654.

[22] HamithaNasrin, M. and Hemalakshmi, S. and Ramsundar, Prof G. (2019). “A review on implementation techniques of Blockchain enabled smart contract for document verification”.

[23] Ghazali, Osman and Saleh, Omar S. (2018). A Graduation Certificate Verification Model via Utilization of the Blockchain Technology. Journal of Telecommunication, Electronic and Computer Engineering, 10, 29-34.

[24] Shah, Maharshi and Kumar, Dr. Priyanka. (2019). “Tamper proof Birth certificate using Blockchain Technology”, International Journal of Recent Technology and Engineering (IJRTE).