Securing Document Exchange with Blockchain Technology: A New Paradigm for Information Sharing

Priyanka. A. Kadam[1] (Professor)
(Guide)
Department of Computer Engineering
TSSM's Bhivarabai Sawant College of
Engineering & Research Pune, India

Swaroop V. Suryakar[2]
B. E. Computer Engineering
TSSM's Bhivarabai Sawant College of
Engineering & Research Pune, India

Nishant R. Wagh[3]
B. E. Computer Engineering
TSSM's Bhivarabai Sawant College of
Engineering & Research Pune, India

Vaibhav B. Kale[4]
B. E. Computer Engineering
TSSM's Bhivarabai Sawant College of
Engineering & Research Pune, India

Rohit M. Bhavsar[5]
B. E. Computer Engineering
TSSM's Bhivarabai Sawant College of
Engineering & Research Pune, India

Abstract:- The rapid digitization of information sharing and document exchange in various sectors, including healthcare, finance, and governmental services, has underscored the critical need for robust security mechanisms. Traditional methods often fall short in ensuring the confidentiality, integrity, and availability of shared documents, leading to vulnerabilities in data privacy and security. This research paper introduces a groundbreaking approach to secure document exchange by leveraging the inherent properties of blockchain technology. Through a comprehensive analysis, we explore how blockchain's decentralized nature, cryptographic security, and immutability can be harnessed to create a secure and efficient platform for information sharing. We begin by delineating the current challenges in document exchange systems, such as susceptibility to cyber-attacks, fraud, and unauthorized access. Subsequently, we propose a blockchain-based framework that addresses these issues by enabling transparent and tamper-proof transactions, ensuring data integrity, and facilitating secure access control. Our methodology includes the development of a prototype system that employs smart contracts for automating and securing document exchange processes. Through rigorous testing and evaluation, we demonstrate the system's ability to withstand various security threats, including data breaches and interception attacks.

Keywords:- *Blockchain, Ethereum, Smart Contract, IPFS.*

I. INTRODUCTION

In today's digital era, the exchange of sensitive documents is ubiquitous across various industries, ranging from finance and healthcare to legal and government sectors. However, traditional methods of document exchange often suffer from vulnerabilities such as data breaches, unauthorized access, and to address these challenges, the integration of blockchain technology presents a promising solution. Blockchain, renowned for its immutable and decentralized nature, offers a secure and transparent platform for document exchange. By leveraging smart contracts and cryptographic hashing techniques, blockchain enables the creation of tamper-proof and verifiable records, ensuring the integrity and authenticity of exchanged documents.

The project "Securing Document Exchange with Blockchain Technology" is aimed at implementing a robust and efficient system for securely exchanging documents using a combination of cutting-edge technologies. The core components of this project include. A popular cryptocurrency wallet and gateway to blockchain applications, Metamask facilitates secure interactions with Ethereum-based decentralized applications (DApps) directly from web browsers.

As the programming language for Ethereum smart contracts, Solidity is utilized to develop self-executing agreements that govern the document exchange process. Smart contracts ensure automated and trustless execution of transactions, eliminating the need for intermediaries.

A JavaScript library for building user interfaces, react is employed to develop an intuitive and user-friendly frontend interface for interacting with the document exchange platform. React's component-based architecture allows for modular and scalable design.

A powerful development environment for Ethereum smart contracts, Hardhat streamlines the process of writing, testing, and deploying smart contracts. With features like built-in testing frameworks and scriptable tasks, Hardhat enhances the efficiency and reliability of smart contract development.

InterPlanetary File System (IPFS) serves as the decentralized storage layer for securely storing and retrieving documents. Pinata, a user-friendly IPFS pinning service, ensures high availability and accessibility of documents while maintaining data integrity and confidentiality.

By integrating these technologies, our project aims to provide a comprehensive solution for secure document exchange, offering benefits such as:

- Documents stored on the blockchain are immutable and tamper-proof, preventing unauthorized alterations.
- Blockchain's transparent and auditable nature enables stakeholders to track the entire lifecycle of documents, enhancing accountability and trust.

Elimination of central authorities reduces the risk of single points of failure and enhances resilience against cyber threats.

Cryptographic techniques ensure the privacy and confidentiality of exchanged documents, protecting sensitive information from unauthorized access.

II. LITERATURE SURVEY

[1] Prof. Mr. M. Velludurai et al. proposed a system that improves data security by encoding and disseminating data to multiple peers in the system. The operating system uses the AES 256-bit encryption algorithm to encrypt data that ensures the confidentiality of user data. The encrypted data is then transmitted and stored to peers on the network using the IPFS protocol.

[2] Shin-Yi Lin et al. introduced a research status of application, existing problems and solutions for blockchain smart contract. It analyses the deployment process of smart contract based on Ethereum, Hyperledger Fabric and EOSIO, and compared the advantages and disadvantages of developing smart contract on three platforms. In addition, it compares and analyses the blockchain with DAG-based blockchain, and introduces the deployment process of DAG-based smart contract.

[4] Hamed Taherdoost highlighted the transformative potential of smart contracts in various industries due to their decentralized, self-executing, and verifiable nature. The research also emphasized the need for a comprehensive evaluation of blockchain-based smart contracts to understand their current state, applications, and potential impact.

[8] Mruthyunjaya Mendu et al. studied about huge scope of research in blockchain technologies for the research scholars, professors and practitioners. As E-Governance is one of the very common services that are in the targets of hackers, crackers and sniffers, these platforms can be secured using advanced decentralized cloud integrations. On the deployment of these services on decentralized clouds, the performance evaluation and comparison with the traditional web environment can be done. Besides, this type of implementation shall avoid the scope of corruption in web-based services.

[9] Muqaddas Naz et al. presented a blockchain-based secure data sharing and delivery of digital assets framework. The main aim of this proposed scenario was to provide data authenticity and quality of data to customer as well as a stable business platform for owner. A decentralized storage IPFS provides the solution for bloating problem at owner’s end.

[10] Wei-Shan Lee et al. proposed SPChain as a means of achieving a secure and GDPR-compliant digital asset management framework by leveraging the security and non-tampering features of blockchain. At the same time, AI models were combined to make digital assets more accessible to a larger number of applications and to enable better creativity.

III. METHODOLOGY

A. Existing Methodology

A lot of use cases for blockchain technology include anchoring on-chain transactions to safely kept documents that are too big or contain too sensitive data to be kept in your immutable shared ledger. For these kinds of scenarios, Kaleido's Document Exchange was developed, offering a private storage that is exclusively yours. Our technique creates a unique link between off-chain data and an on-chain asset, token, or transaction. Please have a look at our IPFS File Store service if you want an IPFS distributed peer-to-peer file sharing system that allows any member of your consortium to access every file.

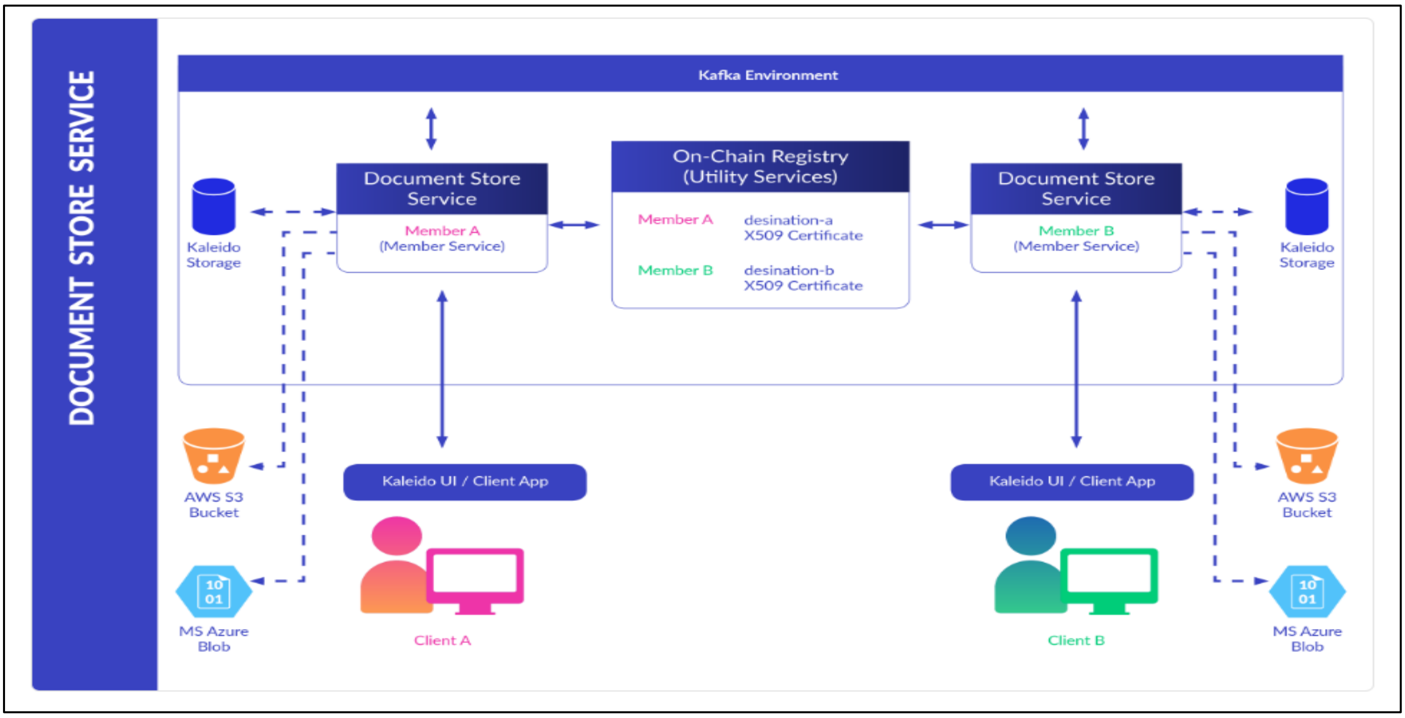

Fig 1 Architecture Diagram

B. *Algorithms*

➢ *Cryptographic Hash Function*

Ensure the integrity of documents and blocks in the blockchain. SHA-256 (Secure Hash Algorithm 256-bit) is widely used in blockchain implementations. It produces a unique, fixed-size hash value from input data of any size (e.g., documents), which is crucial for verifying document integrity and generating block hashes.

- Function generateHash(input):
- Return SHA256(input)

➢ *Digital Signatures*

Verify the authenticity of documents and transactions. ECDSA (Elliptic Curve Digital Signature Algorithm) is commonly used for creating and verifying digital signatures in blockchain networks. It ensures that a document or transaction was created by a known sender (authentication) and was not altered in transit (integrity).

- Function createSignature(document, privateKey):
- Return ECDSA_Sign(document, privateKey)
- Function verifySignature(document, signature, publicKey):
- Return ECDSA_Verify(document, signature, publicKey)

➢ *Smart Contracts*

Automate and enforce access control and document exchange rules. Depending on the blockchain platform, smart contracts can be written in various languages (e.g., Solidity for Ethereum). The logic for access control and document verification would be implemented as functions within the smart contract.

- // Solidity example for Ethereum-based systems
- Contract Document Exchange {
- Function authorize Access (uint documentId, address userId) public { // Implementation}
- Function verify Document (uint document Id, string memory document Hash) public view returns (bool) {// Implementation}

IV. RESULTS AND ANALYSIS

The described algorithm aims to provide a secure and efficient document exchange system leveraging blockchain, encryption, and decentralized storage technologies. By implementing the proposed steps, the system can achieve robust security, privacy, and integrity for users' data and transactions. Ongoing monitoring, testing, and updates are essential to maintaining the system's security posture and addressing emerging threats.

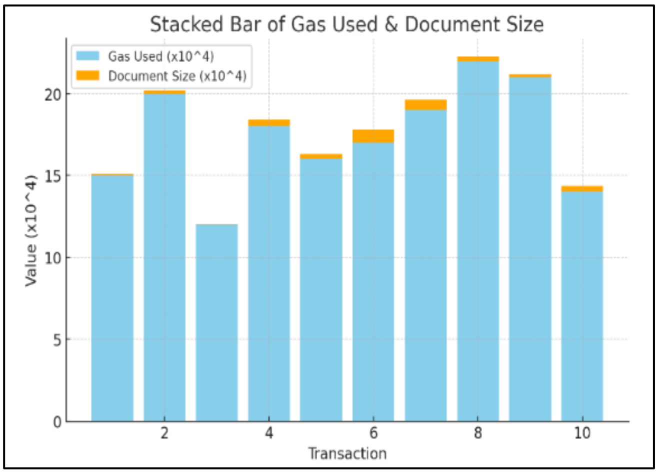

Fig 2 Graph of Gas used Wrt Document Size

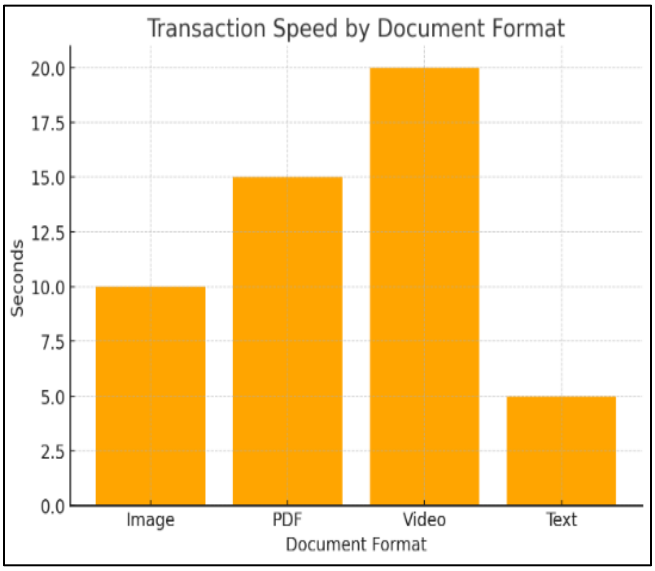

Fig 3 Graph of Transaction Speed Wrt Document Format

The first graph indicates that as the document size increases, so does the gas used, suggesting a correlation between the size of the document and the cost of the transaction on the blockchain.

The second graph is a bar chart showing transaction speed by document format. It illustrates that the transaction time varies with document format, with 'Video' taking the longest and 'Text' the least amount of time.

V. CONCLUSION

The project demonstrates the potential of blockchain technology in securing document exchange. By leveraging MetaMask, Solidity, React, Hardhat, and Pinata IPFS, we have developed a platform that addresses key concerns such as privacy, authenticity, and data integrity. Through the use of smart contracts, document exchange is transparent, tamper-proof, and decentralized. MetaMask integration enhances security, while react ensures a user-friendly experience. Hardhat facilitates development and testing, ensuring reliability. Pinata IPFS provides decentralized storage, further enhancing security. Overall, this project showcases the power of blockchain technology in revolutionizing document exchange, offering a secure and efficient solution for users worldwide.

REFERENCES

[1]. Prof. Mr. M. Velludurai, Rahul Gond, Omkar Acharekar, Snehal Sanap, Anushka Nipurte, “Blockchain Based File Sharing System”

[2]. Shin-Yi Lin, Lei Zhang, Jing Li, Li-li Ji, Yue Sun,“A survey of application research based on blockchain smart contract”

[3]. Jiachi Chen, Xin Xia, David Lo, John Grundy, Xiaohu Yang, “Maintenance-related concerns for post-deployed Ethereum smart contract development: issues, techniques, and future challenges”.

[4]. Hamed Taherdoost, “Smart Contracts in Blockchain Technology: A Critical Review”.

[5]. Hua Yi Lin, “Secure Data Transfer Based on a Multi-Level Blockchain for Internet of Vehicles”.

[6]. Alfred Daniel John William, Santhosh Rajendran, Pradish Pranam, Yosuva Berry, Anuj Sreedharan, Junaid Gul and Anand Paul, “Blockchain Technologies: Smart Contracts for Consumer Electronics Data Sharing and Secure Payment”.

[7]. Jia Yu and Bo Ren, “Compression Function Design of Secure Hash Alogrithm Based on Block Cipher.”

[8]. Mruthyunjaya Mendu, Dr. B Krishna, Sallauddin Mohmmad, Y Sharvani, Ch Vinay Kumar Reddy, “Secure Deployment of Decentralized Cloud in Blockchain Environment using Inter-Planetary File System”.

[9]. Muqaddas Naz, Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid, Ali Mustafa Qamar, Muhammad Khalil Afzal and Muhammad Shafiq, “A Secure Data Sharing Platform Using Blockchain and Interplanetary File System”.

[10]. Wei-Shan Lee, John A, Hsiu-Chun Hsu and Pao-Ann Hsiung, “SPChain: A Smart and Private Blockchain-Enables Framework for Combining GDPR-Compliant Digital Assets Management with AI Models”.