Verification and Validation Documents Using Blockchain based QR Code

Author 1 **Author 2** **Author 3**

Kavin D **Sarath J V** **Sathish K**

kavin.ad20@bitsathy.ac.in **sarath.cs20@bitsathy.ac.in** **sathishk.cs20@bitsathy.ac.in**

ABSTRACT

This project introduces a novel approach for enhancing document security and authenticity through the integration of blockchain technology and QR codes. In an increasingly digital world, document verification and validation have become critical concerns for various industries. Our solution leverages blockchain's immutability and transparency to ensure the integrity and provenance of documents.The system generates a unique QR code for each document, storing a hash of the document's content on the blockchain. Users can then scan the QR code to verify the document's authenticity and track its history. This technology not only prevents document tampering but also simplifies the verification process, making it accessible to a wide range of users.We implement this concept to improve document security in domains such as academic credentials, legal contracts, and medical records, ensuring trust and reliability in an increasingly digital and interconnected world. This project showcases the potential of blockchain technology to revolutionize document verification and validation processes, offering a secure and efficient solution for a variety of industries.

INTRODUCTION

The digital age has led to a surge in the use of digital documents across various sectors, from education and healthcare to government services and finance. However, verifying the authenticity of these documents can be challenging. Traditional methods often rely on centralized databases, which are susceptible to hacking and manipulation. Additionally, these methods can be time-consuming and cumbersomeThis project introduces a novel approach for enhancing document security and authenticity through the integration of blockchain technology and QR codes. In an increasingly digital world, document verification and validation have become critical concerns for various industries. Our solution leverages blockchain's immutability and transparency to ensure the integrity and provenance of documents. The system generates a unique QR code for each document, storing a hash of the document's content on the blockchain. Users can then scan the QR code to verify the document's authenticity and track its history. This technology not only prevents document tampering but also simplifies the verification process, making it accessible to a wide range of users. We implement this concept to improve document security in domains such as academic credentials, legal contracts, and medical records, ensuring trust and reliability in an increasingly digital and interconnected world. This project showcases the potential of blockchain technology to revolutionize document verification and validation processes, offering a secure and efficient solution for a variety of industries.

1.1.THE PROBLEM

Current document verification methods face several limitations in Centralized Systems. Dependence on centralized databases creates a single point of failure vulnerable to cyberattacks and data breaches. Inefficient Verification Process, Traditional verification processes. can be lengthy requiring contacting issuing authorities. The ease of replicating physical documents creates a risk of fraudulent documents circulating undetected.

1.2 PROPOSED SOLUTION

This project introduces a secure and user-friendly system for document verification leveraging blockchain and QR codes. Blockchain Technology distributed ledger system ensures data integrity and prevents tampering with documents. Unique QR codes linked to document hashes offer a convenient way to initiate the verification process.

1.3 BENEFITS

This system offers numerous advantages over traditional methods of enhanced Security. Blockchain's immutable ledger ensures the authenticity and security of documents. Decentralized Verification anyone can verify documents without relying on centralized authorities. Improved Efficiency and Streamlined verification process with instant results through QR code scanning. The system makes it virtually impossible to create and circulate fraudulent documents.

1.4 PROJECT SCOPE

This report will delve into the technical aspects of the system, including .A detailed explanation of the proposed method using blockchain and QR codes. Exploration of cryptographic hash functions and their role in data integrity. Discussion on the use of encryption and decryption. Overview of QR code generation and its functionalities. Introduction to potential development tools like React JS, MetaMask, Ganache, and Django. Analysis of the system's results, effectiveness, and future potential. This project aims to provide a secure and efficient document verification system with far-reaching applications in various sectors.

LITERATURE SURVEY

2.1 TITLE : EXISTING DOCUMENT VERIFICATION AND AUTHENTICATION

AUTHOR : A. Vaskuri, H. Baumgartner, P. Kärhä, G. Andor, and E. Ikonen, "Modeling the spectral shape of InGaAlP-based red light-emitting diodes," *Journal of Applied Physics*, vol. 118, no. 20, pp. 203103-1–203103-7 (2022)

Traditional document verification methods rely on centralized databases maintained by issuing authorities, for example universities, government agencies. Users typically contact these authorities to verify the authenticity of a document, often involving a lengthy process with manual verification steps. Centralized systems are vulnerable to hacking and data manipulation. Verification processes can be time-consuming and require user effort. Difficulty in verifying physical documents without contacting the issuing authority.

2.2 TITLE :BLOCKCHAIN TECHNOLOGY FOR DOCUMENT MANAGEMENT

AUTHOR : Dipali Sanjay Chavan*1, Radhika Natwarlal Dayama*2, Pratik Prashant Joshi*3, Prajyot Pradip Pawar*4, Prof. A. D. Londhe*5 *1,2,3,4,5 Department of Information Technology, Smt. Kashibai Navale College of Engineering, Vadgaon(Bk.), India

Blockchain technology has emerged as a promising solution for secure document management due to its core features. Distributed Ledger: A tamper-proof record of transactions maintained across a network of computers, ensuring data integrity. Once recorded, data cannot be altered or deleted, guaranteeing the authenticity of documents stored on the blockchain.

All participants can access and verify the data on the blockchain, promoting trust and accountability.

2.3 TITLE :BLOCKCHAIN-BASED DOCUMENT VERIFICATION SYSTEMS

AUTHOR : Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain microgrid transactions. Energies. 2018 May;11(5):1154.

Several research projects explore utilizing blockchain for document verification. Some common approaches include Document Hashing. Documents are converted into a unique identifier before uploading onto the blockchain. Digital Signatures Issuing authorities digitally sign documents using cryptography, further enhancing verification. Smart Contracts Programmable contracts on the blockchain can automate specific actions related to document issuance or access control.

TITLE : QR CODES FOR VERIFICATION INITIATION

AUTHOR : Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.

QR codes are machine-readable codes that can store data. In document verification systems, QR codes can be embedded within the document itself. By scanning the QR code using a mobile app or web interface, users can initiate the verification process.QR codes provide a convenient and user-friendly way to access document verification information.

3.1 SYSTEM OBJECTS

This section provides a high-level overview of the key objects involved in the document verification system using blockchain and QR codes.

ISSUING AUTHORITY :

An entity authorized to issue official documents for example universities, government agencies, corporations.

Roles:

1. Uploads digital versions of documents onto the blockchain network.
2. May digitally sign documents for enhanced verification.
3. Maintains control over document issuance within their domain.

3.2 DOCUMENT

The digital representation of an official record for example diploma, certificate, ID card.The original term for collecting, preserving, organizing, describing, retrieving, reproducing and disseminating documents was bibliography. These days, all of those actions are categorized as documentation. Having been in use for almost a century, this broad phrase includes document archiving, records management, information services, and bibliographies.

Properties:

4. Stored electronically in a secure format.
5. Hashed for creating a unique identifier.
6. May contain metadata for additional information for example : document type, issuing authority.

3.3 BLOCKCHAIN NETWORK

3.4 BASIC DESIGN OF BLOCK CHAIN NETWORK

A distributed ledger technology that securely stores and verifies data across a network of computers. Stores the document hash and associated metadata. Ensures the immutability and integrity of document data.Provides a transparent and verifiable record of document issuance.Blockchain technology is a distributed ledger that connects a decentralized network on which users can send transactions and build applications without the need for a central authority or server. Blockchain powers dozens of useful apps that provide value across a wide range of industries, including gaming, fashion, and finance. It also powers networks like Bitcoin and Ethereum. Blockchain has a great chance to become a key technology in our digital future with further improvement.

A unique identifier created by applying a cryptographic hash function to the document. Digitize physical documents or convert digital files into a standardized format. Generate cryptographic hashes of each document to create unique identifiers. Store the document hashes on the blockchain along with relevant metadata, such as timestamps and document identifiers

Properties:

Impossible to recreate the original document from the hash.Sensitive to change any modification to the document results in a different hash. And here we used **SHA-256** for efficient verification on the blockchain.

3.5 QR CODE

A machine-readable code that can store encoded data.Generate QR codes containing unique identifiers linked to each document hash. Embedded within the digital document or displayed on a physical document printout.Ensure QR code readability and compatibility with standard QR code scanning applications on smartphones.Stores the document hash or other relevant information for verification.Initiates the verification process by scanning the code with a mobile app or web interface.

3.6 VERIFICATION APP/INTERFACE

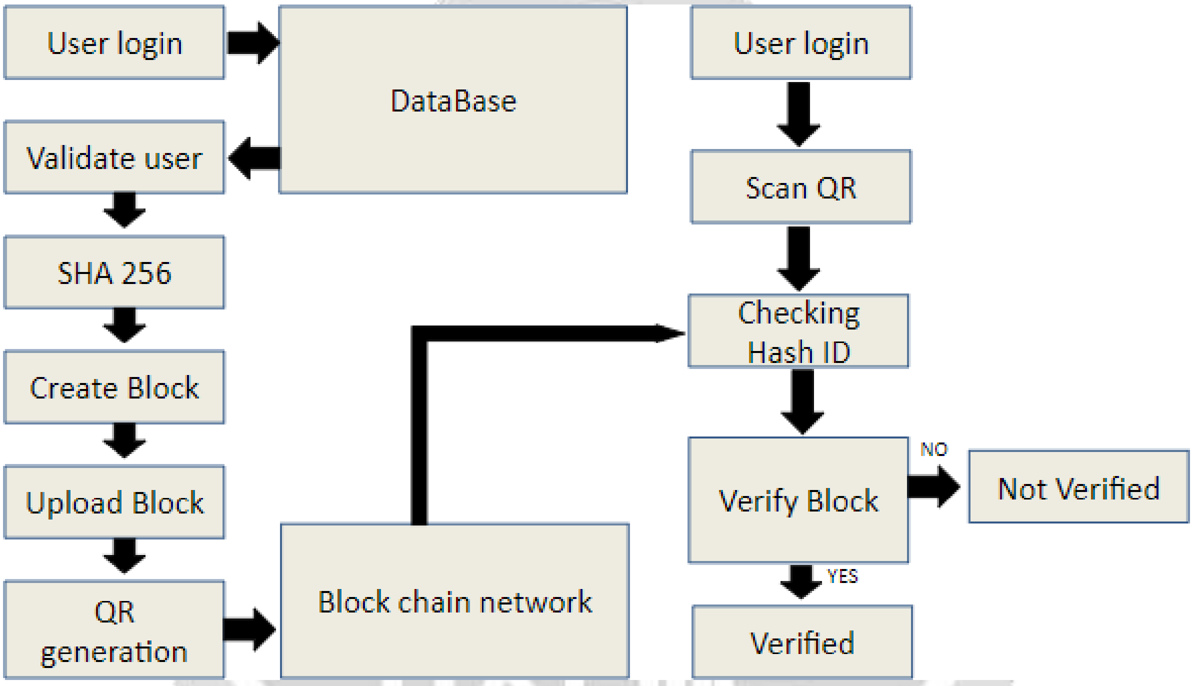
A software application mobile app or web platform used to verify document authenticity. Provides a user-friendly interface for scanning QR codes or entering document details.Interacts with the blockchain network to retrieve the document hash.Compares the retrieved hash with the one embedded in the QR code or document itself. Smart contracts retrieve the corresponding document hash from the blockchain and compare it with the hash generated from the scanned document.If the hashes match, the document is deemed authentic, and a verification success message is returned to the user. Otherwise, an error message is displayed. Displays verification results, indicating document authenticity or potential tampering.These objects work together to create a secure and efficient document verification system. Issuing authorities upload documents, the blockchain ensures data integrity, QR codes provide a convenient way to access verification information, and the verification app facilitates user interaction and result display. Understanding these objects is crucial for comprehending the system's functionality.

PROPOSED METHOD

This section outlines the proposed method for verifying and validating documents using blockchain technology and QR codes .Our proposed method outlines a comprehensive approach to implementing a blockchain-based QR code verification system for enhancing document security and integrity. Below are the key components and steps involved in the proposed method.

4.1System Workflow

Document Issuance like Issuing authorities, universities, government agencies upload the digital document to a secure blockchain network. Document Hashing. A cryptographic hash function is used to generate a unique identifier hash for the document. This hash acts as a fingerprint for the document's content. The document hash, along with additional metadata example document type, issuing authority information, is stored on the blockchain. The original document might be stored in a secure, off-chain location. A unique QR code is generated that encodes the document's hash and potentially other relevant information. This QR code is then embedded within the digital document or printed on a physical document.



4.1**BLOCK DIAGRAM**

4.2 Verification Process:

1. Users scan the QR code using a mobile app or web interface.
2. The app retrieves the document's hash from the blockchain using the information encoded in the QR code.
3. The app compares the retrieved hash with the hash embedded within the QR code.
4. The authenticity of the document is confirmed if the hashes match. If not, it is marked as possibly fake.

Blockchain Security is the immutability and distributed nature of the blockchain that ensures the integrity of document data and prevents tampering. Anyone with access to the blockchain and the verification app can verify a document's authenticity, eliminating the need for centralized authorities. QR code scanning and instant hash comparison enable a quick and user-friendly verification process. The system makes it highly difficult to create and distribute fraudulent documents with matching hashes.

This proposed method offers significant advantages over traditional verification methods and Enhanced Security. Blockchain technology provides a more secure and tamper-proof environment for document storage. Increased Trust users can be confident in the authenticity of verified documents due to the decentralized verification process and Improved Efficiency Streamlined QR code scanning and verification significantly reduce processing time compared to traditional methods. Reduced Costs elimination of manual verification processes and reliance on centralized authorities can lead to cost savings. The proposed method leverages the strengths of blockchain and QR code technology to create a secure, efficient, and user-friendly system for document verification and validation. The following sections will delve deeper into the technical aspects of the system, such as cryptographic hash functions and the role of specific development tools.This project utilizes a cryptographic hash function to ensure the authenticity and immutability of documents stored on the blockchain. A cryptographic hash function is a one-way mathematical function that converts any input data, for example a document into a unique fixed-size output hash. The same input data always produces the same hash output. It's computationally infeasible to find two different inputs that generate the same hash output. Small changes to the input data result in significant changes to the hash output.

4.3Importance in Document Verification:

Documents are converted into their unique hash before uploading to the blockchain. This hash serves as a fingerprint for the document's content.Verification Process during verification, the system recalculates the hash of the document example downloaded from a secure source and compares it to the hash stored on the blockchain. If the calculated hash matches the one on the blockchain, it confirms that the document hasn't been tampered with since its upload. Any alteration to the document will result in a different hash, indicating potential forgery.

Common Hash Functions:

- SHA-256: A widely used and secure hash function with a 256-bit output.
- SHA-3: The successor to SHA-2 family, considered resistant to potential attacks on SHA-2

This explanation highlights the importance of cryptographic hash functions in ensuring data integrity for document verification using blockchain technology.

ALGORITHM

5.1 Encryption and Decryption in Blockchain-Based Document Verification

While encryption plays a less central role in the core functionality of this project, understanding its potential use can be beneficial. Here's a breakdown of encryption and decryption in the context of document verification using blockchain and QR codes

Encryption:

Encryption scrambles data using a secret key password or passphrase. This scrambled data is unreadable without the corresponding decryption key. In the context of document verification. Encrypting specific sensitive fields within a document can provide an additional layer of security. For example, social security numbers or financial information might be encrypted before embedding them in the QR code with limited Impact on Verification. Encryption itself doesn't directly impact the document verification process using blockchain and QR codes. The core verification relies on the document hash stored on the blockchain.

Decryption :

Decryption reverses the encryption process using the same key to access the original, readable data. Decryption might not be necessary for most document verification scenarios. The QR code would typically contain only the document hash and other non-sensitive information needed for verification. Accessing Encrypted Fields for specific fields are encrypted, the user with the appropriate decryption key can access the original data after successful document verification.

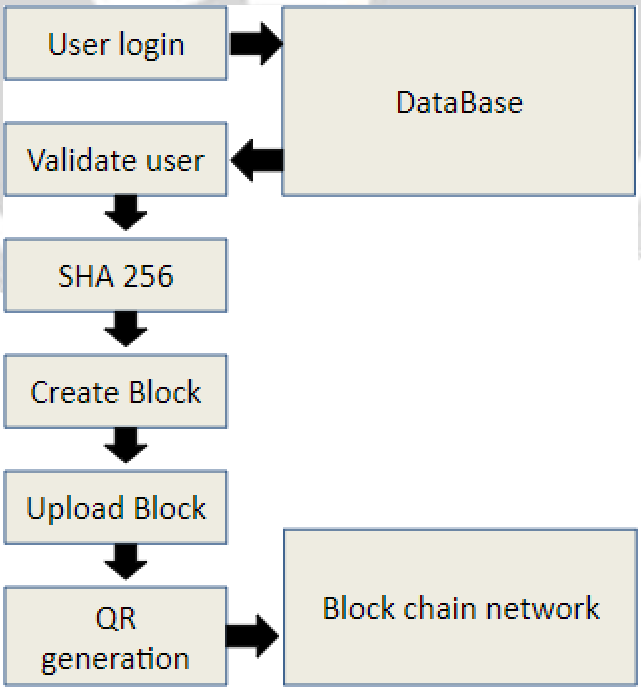
5.2Alternatives for Sensitive Data

The primary focus of this project should be on document hashing and verification using blockchain. Encryption can be considered as an optional add-on for specific document types requiring additional security for sensitive information balancing security and accessibility. While encryption enhances security, it can also introduce additional steps and potential complexities for users. Striking a balance between security needs and ease of use is crucial in the design of the verification system.

Instead of encrypting sensitive data within the document, here are some alternative approaches. Sensitive fields can be completely redacted from the document displayed to the user. Verification can still occur using the hash stored on the blockchain. Issuing Separate Credentials for highly sensitive documents, consider issuing separate credentials containing the sensitive information directly on the blockchain. These credentials can be accessed only by authorized users.Encryption offers an extra layer of security for specific scenarios, but it's not essential for the core functionality of blockchain-based document verification. Focus on secure document hashing and verification while considering the appropriate balance between security and user experience for your project.

5.3 QR Code Generation :

While machine learning isn't typically the core functionality for QR code generation in document verification systems, it can be an interesting area for further exploration and potential future integration. This section will focus on traditional QR code generation and briefly touch on potential applications of machine learning.This section explained traditional QR code generation, highlighting its functionalities and tools. While machine learning isn't currently the core focus, it presents potential future avenues for enhancing QR code security, customization, and data efficiency in document verification systems.Note: This section provides a brief overview for a 2-page explanation of QR code generation. You can expand on the details of data encoding, module arrangement, and version selection with diagrams and technical specifications. The machine learning section can be further researched to explore specific algorithms and potential applications in this context.



HASHING ALGORITHM

5.4 Traditional QR Code Generation

QR codes are two-dimensional barcodes capable of storing various data types, including text, URLs, and even small images. They are widely used for applications like product tracking, information sharing, and mobile payments. The information you want to encode example document hash is first converted into a specific format suitable for QR code storage. Error correction codes are added to ensure data integrity even if parts of the QR code are damaged. The encoded data is then mapped onto a grid of black and white squares modules that make up the QR code. Specific arrangements ensure proper data reading and error correction during scanning version Selection of QR codes come in different versions depending on the amount of data they can store. The appropriate version is chosen based on the size of the encoded information.

5.5QR Code Generation Tools

Numerous open-source libraries and online tools are available for generating QR codes. These tools typically require you to input the data you want to encode and choose the desired version and error correction level . While not central to the core functionality of document verification, machine learning could be explored for QR Code Machine learning algorithms might be used to create visually appealing or unique QR code designs while maintaining readability. Machine learning could potentially optimize data encoding within the QR code, minimizing redundancy and maximizing information storage capacity and that models might be trained to detect and differentiate between legitimate and forged QR codes based

5.6 QR Code Generation not Machine Learning Focused :

While machine learning isn't typically involved in the core functionality of QR code generation for document verification, this section will delve into the functionalities of QR codes and their application in this project. Quick Response codes are two-dimensional barcodes capable of storing various data types, including text, URLs, and even small images. They consist of black and white squares arranged in a square grid pattern. The data is encoded within the arrangement and size of these squares. QR codes can hold a significant amount of information compared to traditional barcodes. The specific capacity depends on the version complexity of the QR code used. QR codes incorporate error correction mechanisms. Even if a portion of the code is damaged or obscured, the error correction allows for successful data retrieval.

5.7 QR Code Generation Tools and Libraries

Several open-source libraries and online tools can generate QR codes. These tools typically require the data to be encoded as input and then generate the corresponding QR code image. Here are some popular options:

Python Libraries	Py-QR, qrcode
JavaScript Libraries:	qrcode.js
Online QR Code Generators	https://www.qr-code-generator.com/

TOOLS FOR QR GENERATION

If a malicious actor tampers with the QR code data, it might lead to an incorrect verification result. Encryption of sensitive information within the QR code can mitigate this risk. Phishing Attacks of the malicious actors could potentially create fake QR codes leading to phishing websites. User education is essential to be cautious about scanning unknown QR codes. QR codes provide a convenient and user-friendly way to initiate document verification within this project. By embedding the document's hash and potentially other relevant information, QR codes streamline the verification process and offer a secure entry point for users to confirm document authenticity.

5.8 Potential Applications of Machine Learning

While not central to the core functionality, machine learning offers intriguing possibilities for future advancements in QR code generation for document verification . Machine learning algorithms could be used to hide additional data within the QR code's visual elements without affecting its readability. This hidden data could contain access control information or additional verification details.

QR Code Anti-Tampering:

Machine learning models could analyze the QR code Structure and detect any potential manipulations or modifications, enhancing security and tamper-proof verification.

Visually Appealing QR Codes:

Machine learning algorithms could be trained to generate QR codes with aesthetically pleasing designs or integrate them seamlessly with existing document layouts.

5.9 Challenges and Considerations

Introducing complexity through machine learning techniques shouldn't compromise the core functionality of reliable and quick QR code scanning. Implementing complex algorithms for QR code generation might introduce processing delays, impacting user experience and integration with the Blockchain system as any machine learning integration needs to be carefully considered for seamless interaction with the underlying blockchain-based verification system.

EDIX TREES AND SOLIDITY

This section explores two potential technologies relevant to blockchain development, but their application in this specific project may be optional.

6.1 Radix Trees

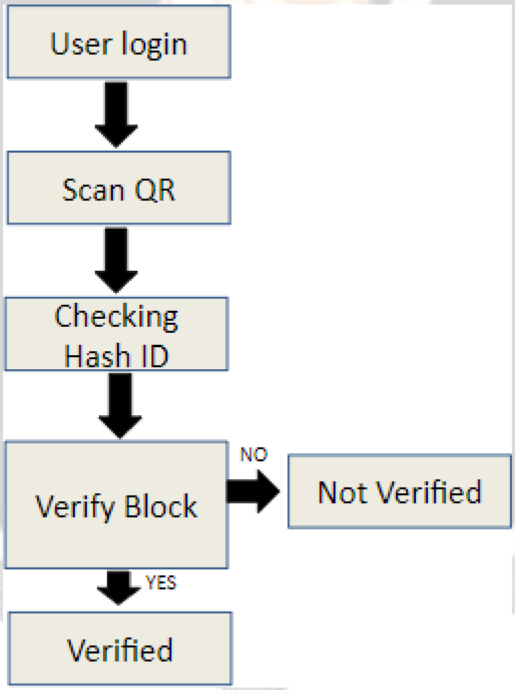
Radix trees, also known as Patricia trees, are a specialized data structure used for efficient storage and retrieval of data on blockchains. They offer several advantages of Compact Storage: Radix trees optimize storage space by sharing common prefixes of data entries. Data retrieval is faster compared to traditional linear searches, especially for large datasets. Radix trees can be used to prove the existence of data on the blockchain without revealing the actual data itself. While not core to the document verification functionality, Radix trees might be considered for Storing additional document metadata on the blockchain if efficiency is a concern for a large number of documents. Implementing advanced search functionalities within the verification app .

Redix is a term that appears to be a typographical error. It is a popular open-supply, in-memory statistics shape used as a database, cache, and message broker. Redis is often employed in blockchain development for various tasks such as caching frequently accessed data, managing session states, and facilitating communication between different components of a decentralized application. Its high-performance, low-latency characteristics make Redis an ideal choice for scenarios where quick access to data is paramount, which aligns well with the demands of blockchain applications.

6.2Solidity

A high-level programming language called Solidity was created expressly for creating smart contracts on blockchains like Ethereum. Smart contracts are self-executing programs stored on the blockchain that can automate specific tasks when predefined conditions are met. This project may not necessarily require Solidity if document verification relies on simple data storage and retrieval on the blockchain. However, Solidity could be considered for Implementing more complex logic on the blockchain, such as automated document issuance with access control rules. Integrating the verification system with existing blockchain-based applications using smart contracts.

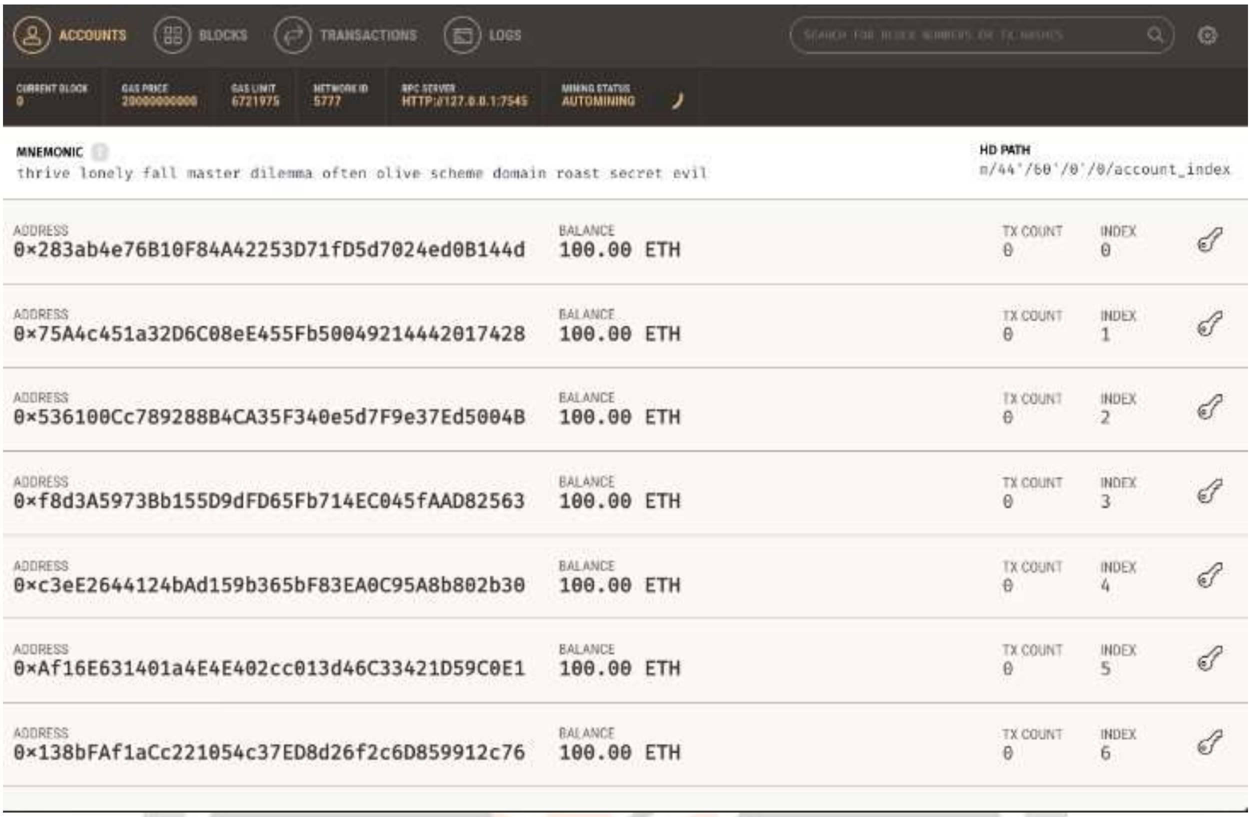
In contrast, Solidity is a programming language created especially for creating smart contracts on blockchain systems like Ethereum. Self-executing contracts, or smart contracts, have the conditions of the contract explicitly encoded into the code. They automatically enforce and execute these terms when predetermined conditions are met. Solidity simplifies the process of creating smart contracts by providing a familiar syntax similar to JavaScript and other high-level programming languages. It includes features such as inheritance, libraries, and complex user-defined types to enable developers to build sophisticated decentralized applications efficiently. Solidity code is compiled into bytecode, which is then deployed onto the Ethereum Virtual Machine, where it is executed and enforced across the Ethereum network. In summary, while Redis plays a crucial role in supporting the infrastructure and performance optimization of blockchain applications, Solidity serves as the primary language for creating the smart contracts that power decentralized applications on platforms like Ethereum. Understanding and effectively utilizing both components are essential for developing robust and efficient blockchain solutions.



QR GENERATION DIAGRAM

6.3 MetaMask and Ganache

Introduction to MetaMask as a browser extension wallet that enables users to interact with Ethereum-based DApps directly from their web browsers. Explanation of MetaMask functionalities, including account management, transaction signing, and network switching. Overview of Ganache as a local blockchain development tool that provides a personal Ethereum blockchain for testing and development purposes. Steps for setting up and configuring Ganache for local development, including creating accounts, importing or exporting accounts, and adjusting blockchain settings. Integration of MetaMask with Ganache for seamless testing and development of DApps locally.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
0	20000000000	6721975	5777	HTTP://127.0.0.1:7545	AUTOMINING

MNEMONIC
thrive lonely fall master dilemma often olive scheme domain roast secret evil

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×283ab4e76B10F84A42253D71fD5d7024ed0B144d	100.00 ETH	0	0
0×75A4c451a32D6C08eE455Fb50049214442017428	100.00 ETH	0	1
0×536100Cc789288B4CA35F340e5d7F9e37Ed5004B	100.00 ETH	0	2
0×f8d3A5973Bb155D9dFD65Fb714EC045fAAD82563	100.00 ETH	0	3
0×c3eE2644124bAd159b365bF83EA0C95A8b802b30	100.00 ETH	0	4
0×Af16E631401a4E4E402cc013d46C33421D59C0E1	100.00 ETH	0	5
0×138bFAf1aCc221054c37ED8d26f2c6D859912c76	100.00 ETH	0	6

GANACHE IMPLEMENT

6.4 Django and Web3 Integration

Introduction to Django as a high-level Python web framework used for backend development.Overview of Django's architecture, including models, views, templates, and Object-Relational Mapping . Explanation of Django REST Framework for building RESTful APIs to interact with frontend applications. Integration of Django with Web3.js, a JavaScript library for interacting with Ethereum nodes, to enable backend communication with the Ethereum blockchain. Examples of Django-based projects leveraging Web3 integration for tasks such as querying blockchain data, sending transactions, and interacting with smart contracts.

RESULTS AND DISCUSSION

7.1 Development Process and Challenges

This section details the development process of the document verification system using blockchain and QR codes. Describe the specific tools and technologies used for example chosen blockchain platform, programming languages, development frameworks. Mention any significant challenges encountered during development, such as Integration complexities between different components like blockchain, QR code generation, verification app. Security considerations and ensuring robust protection against potential vulnerabilities.User interface or experience design challenges to create a user-friendly verification process.

7.2 System Testing and Results

7.2.1 Discuss the testing methodologies employed to evaluate the system's functionality, performance, and security. This might include,

7.2.2 Verifying if the system can successfully.

7.2.3 Upload documents onto the blockchain.

7.2.4 Generate and embed QR codes within documents.

7.2.5 Enable users to scan QR codes and initiate verification.

7.2.6 Accurately verify document authenticity by comparing hashes.

7.2.7 Assessing the system's response time for document verification and overall processing efficiency.

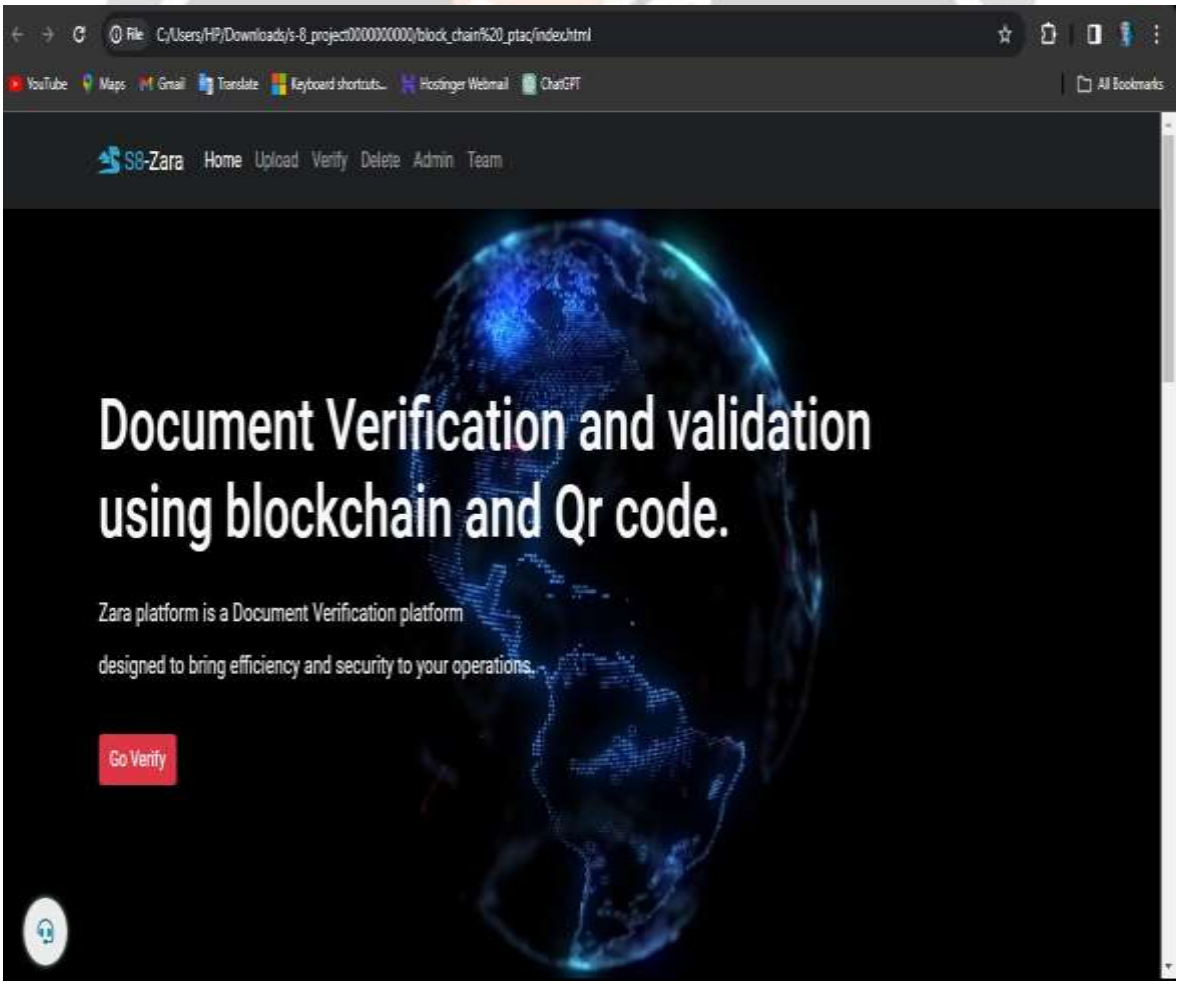
7.2.8 Evaluating the system's resistance to potential attacks like data manipulation or unauthorized access.

7.2.9 Present the results of the testing process, highlighting any successes and areas for improvement.

7.3 Effectiveness Analysis

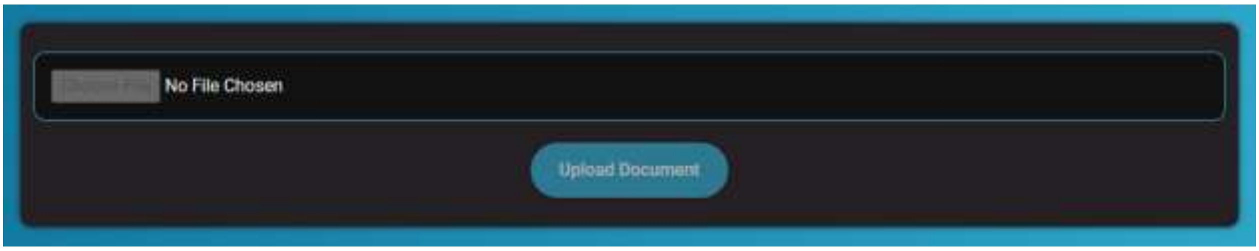
Analyze the effectiveness of the proposed system in achieving its objectives discuss how the system utilizes blockchain's immutability and cryptographic hash functions to prevent document tampering.Decentralized Verification explain that how users can verify documents without relying on centralized authorities.Improved Efficiency that describe the time savings and streamlined verification process offered by QR code scanning.Reduced Fraud Analyze how the system makes it difficult to create and circulate fraudulent documents. Compare the proposed system with existing document verification solutions. Discuss the advantages of your system, such as increased security, improved user experience, or broader applicability across various document types.

MAIN PAGE VIEW

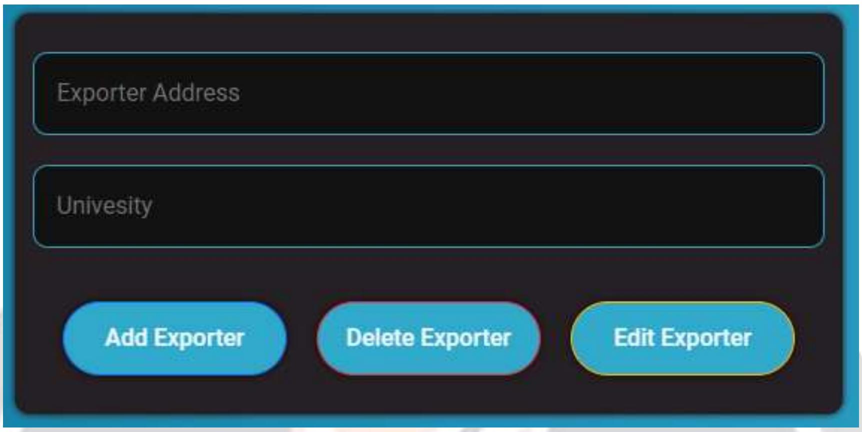


Document Verification and validation using blockchain and Qr code.

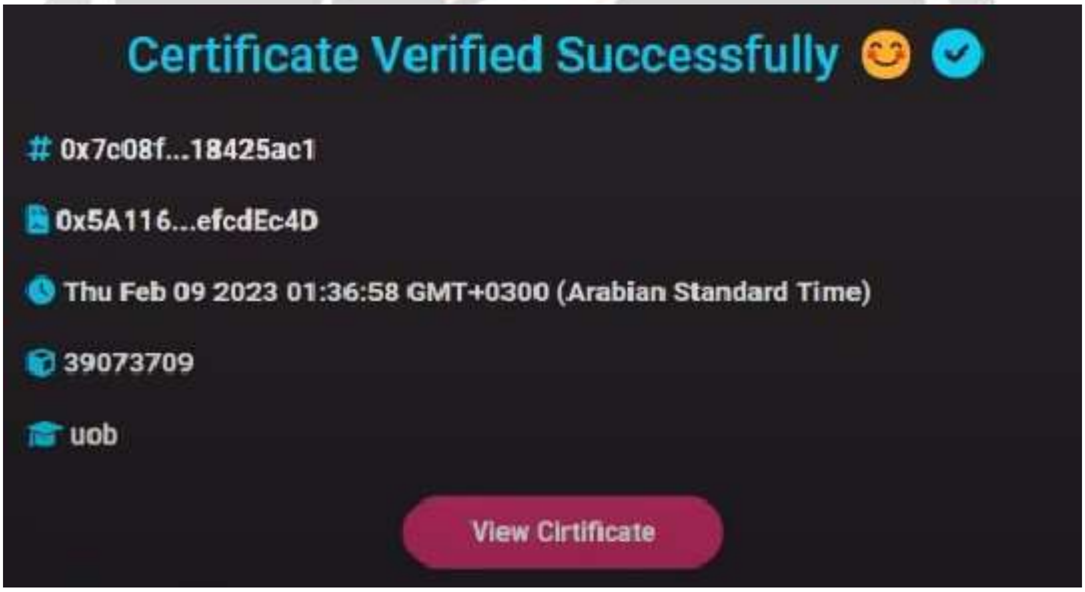
Zara platform is a Document Verification platform designed to bring efficiency and security to your operations.



UPLOADING PAGE VIEW



ADMIN CONTROL


Certificate Verified Successfully 😊 ✓

0x7c08f...18425ac1

0x5A116...efcdEc4D

Thu Feb 09 2023 01:36:58 GMT+0300 (Arabian Standard Time)

39073709

uob

DOCUMENT VERIFICATION RESULT VIEW

7.4 Future Research and Improvements

Outline potential areas for future research and development to enhance the system Explore integration with existing document issuance and management platforms.Investigate the use of advanced cryptographic techniques for additional security.Consider incorporating features like access control mechanisms for document sharing. Reaffirm the potential of the proposed system for secure and efficient document verification. Briefly mention the broader impact this technology can have on various sectors relying on document authenticity.

CONCLUSION

The implementation of blockchain hashing methods for document verification and validation offers a strong approach to address issues of data integrity and trustworthiness in diverse sectors. by leveraging the decentralized and immutable nature of the blockchain era, this assignment has tested its ability to streamline verification tactics, enhance safety, and reduce the chance of fraudulent sports. Through the usage of cryptographic hashing strategies, files can be securely time stamped and saved on the blockchain, ensuring their authenticity and preventing unauthorized changes. Moreover, the transparency and auditability provided via blockchain generation foster extra responsibility and self assurance amongst stakeholders. transferring ahead, continued research and development on this area preserve promise for revolutionizing report control systems across industries, paving the way for more efficient and dependable procedures inside the virtual age.In end, the adoption of blockchain-based totally hashing strategies for report verification and validation represents a tremendous milestone within the quest for at ease and tamper-evidence facts management structures. Through harnessing the inherent functions of blockchain era, which includes decentralization, transparency, and immutability, this task has efficaciously addressed vital challenges associated with record integrity and trustworthiness.

Through using cryptographic hashing algorithms, files are transformed into specific digital fingerprints, or hashes, that are then securely recorded at the blockchain. This technique now not simplest guarantees the authenticity of files but also safeguards them against unauthorized adjustments or tampering, as any alteration to the file might bring about a totally exceptional hash fee, as a consequence alerting stakeholders to potential tampering tries.moreover, the decentralized nature of blockchain ensures that there is no single factor of failure or manage, making it exceptionally resilient to cyberattacks and facts breaches. This decentralization additionally promotes extra transparency and accountability, as all transactions at the blockchain are seen to all members, thereby lowering the risk of fraud and manipulation. Moreover, the timestamping feature of the blockchain era allows the introduction of a verifiable and immutable record of when a report changed into created or changed, in addition enhancing its credibility and criminal validity.

Moreover, the integration of smart contracts into the blockchain environment can automate and streamline the document verification procedure, getting rid of the need for intermediaries and lowering administrative overheads. clever contracts can be programmed to execute predefined movements, which includes verifying the authenticity of documents based on predefined criteria, thereby expediting the verification procedure and minimizing human intervention. This automation now not handiest complements efficiency however additionally reduces the probability of errors and inconsistencies associated with manual document verification techniques.looking ahead, the sizeable adoption of blockchain-based totally record verification and validation structures holds sizeable ability for revolutionizing numerous industries, including finance, healthcare, deliver chain management, and criminal offerings. The enhanced safety, transparency, and performance supplied by using blockchain generation can pressure big cost financial savings, improve regulatory compliance, and foster greater acceptance as true with and confidence amongst stakeholders. however, to fully understand these benefits, it is imperative to address challenges along with scalability, interoperability, and regulatory compliance, as well as to continue innovating and refining blockchain answers to satisfy the evolving desires of corporations and society at big.In conclusion, the implementation of blockchain hashing techniques for record verification and validation represents a transformative step towards constructing a greater secure, transparent, and truthful virtual infrastructure

REFERENCE

1. A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and Solutions,”ar Xiv:1608.05187 [cs], 2016. [Online].

2. Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian.IEEE, 2018.

3. Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data."Proceedings of the Norwegian Information Security Conference. 2017.

4. Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security.Acm, 2006.

5. Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.

6. Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.

7. Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.

8. Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. Energies. 2018 May;11(5):1154.

9. Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.

10. Ouaddah, Aafaf, AnasAbouElkalam, and AbdellahAitOuahman. "FairAccess: a new Blockchain-based access control framework for the Internet of Things." Security and Communication Networks 9.18 (2016): 5943-5964.

11. Kiviharju, Mikko. "Enforcing Role-Based Access Control with Attribute-Based Cryptography in MLS Environments."

12. He, Qingsu, et al. "A privacy-preserving Internet of Things device management scheme based on blockchain." International Journal of Distributed Sensor Networks 14.11 (2018): 1550147718808750.

13. Rahulamathavan, Yogachandran, et al. "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption." 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).IEEE, 2017.

14. Wu, Axin, et al. "Efficient and privacy-preserving traceable attribute-based encryption in blockchain." Annals of Telecommunications (2019): 1-11.

15. Sui, Zhimei, et al. "An Encrypted Database with Enforced Access Control and Blockchain Validation."