Blockchain-based Secure Document Management using QR Codes

Dhanush H  
 *Computer Science And Bussiness System*  
 *R.M.K ENGINEERING COLLEGE*Chennai, India  
 [dhanushhari150504@gmail.com](mailto:dhanushhari150504@gmail.com)

*Abstract: Blockchain technology provides a decentralized and secure platform for managing digital transactions with robust security. In this paper, we propose a novel approach for secure document management using blockchain technology and QR codes to address the significant concern of data breaches for organizations. These breaches can result in the loss of sensitive information and financial damages. Our system generates a unique cryptographic hash of the document, which is anchored to a blockchain network using a smart contract. A QR code containing the document's hash and user permission level is then embedded within the document. The access control mechanism ensures that only authorized users can access the document, and any attempts to tamper with it can be detected and traced. The proposed system provides a secure and efficient way to manage sensitive documents while preventing unauthorized access and data breaches. The use of blockchain technology ensures the immutability and transparency of the document's history, making it a reliable and trustworthy solution for secure document management.*

*Keywords: Blockchain, QR codes, document management, access control, security, data breaches, immutability, transparency.*

# INTRODUCTION

Secure document management is a critical concern for organizations of all sizes, as data breaches can result in significant financial and reputational damage. Traditional document management systems are often vulnerable to attacks, and there is a need for a more secure and efficient way to manage sensitive documents. Blockchain technology provides a decentralized and secure platform for managing digital transactions with robust security, making it an ideal solution for secure document management. By anchoring a document's unique cryptographic hash to a blockchain network using a smart contract, the immutability and transparency of the document's history can be ensured. QR codes can be used to embed the document's hash and user permission level within the document, providing a user-friendly and convenient way to manage access to sensitive documents. Cloud storage can address scalability issues that may arise from storing large amounts of data on the blockchain. In this paper, we propose a novel approach for secure document management using blockchain technology, QR codes, and cloud storage, and evaluate its security, efficiency, and usability.

Keywords: Data breaches, QR code, Blockchain, cloud storage.

# BACKGROUND AND RELATED

A. Blockchain Technology

Blockchain technology is a decentralized and secure platform for managing digital transactions. It provides a tamper-proof and transparent ledger of all transactions, making it an ideal solution for secure document management. The use of cryptographic algorithms ensures that the data stored on the blockchain is secure and immutable. In the context of secure document management, blockchain technology can be used to anchor the document's unique cryptographic hash to a blockchain network using a smart contract, ensuring the immutability and transparency of the document's history.

B. QR Codes

QR codes are two-dimensional barcodes that can store large amounts of information. They are widely used in various applications, including marketing, advertising, and product tracking. In the context of secure document management, QR codes can be used to embed the document's hash and user permission level within the document. This provides a user-friendly and convenient way to manage access to sensitive documents. When a user scans the QR code, the system verifies their permission level and grants access accordingly. Any attempts to tamper with the document can be detected and traced. Additionally, a document verification mechanism can be provided to ensure the authenticity of the document.

C. Related Work

Blockchain technology has been widely studied for secure document management in recent years. Several studies have proposed using blockchain for storing and sharing documents securely. For example, Bichler and Schmitz (2020) presented a blockchain-based approach for secure and transparent document management, focusing on the use of smart contracts for document verification. Similarly, Alkhoder and Röck (2019) proposed a blockchain-based framework for document certification and verification, discussing the use of cryptographic hashes and blockchain anchoring.

However, these studies have mainly focused on using blockchain for storing and sharing documents, without considering the use of QR codes for access control. In contrast, our proposed system integrates QR codes for access control, providing a user-friendly and convenient way to manage sensitive documents while ensuring security and preventing unauthorized access and data breaches.

Other studies have explored the potential of blockchain technology for protecting personal data and ensuring privacy, which is relevant to our proposed system's access control and permission aspects. For instance, Zyskind et al. (2015) discussed the use of blockchain for protecting personal data, while Li et al. (2021) proposed a blockchain-based access control mechanism for electronic health records.

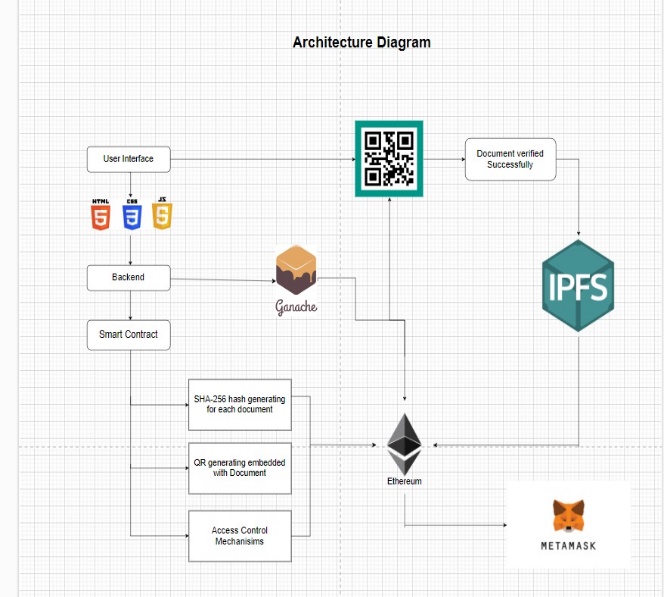
Moreover, some studies have focused on the use of blockchain for secure data management and transfer in specific applications. For example, Xu et al. (2017) provided a taxonomy of blockchain-based applications for the Industrial Internet of Things (IIoT), while Qian and Liang (2018) presented a blockchain-based data sharing scheme for cloud computing. More recently, Wang et al. (2022) proposed a blockchain-based system for secure and transparent supply chain management.

In this paper, we build upon the existing literature by proposing a novel approach for secure document management using blockchain technology and QR codes. Our proposed system integrates QR codes for access control, providing a user-friendly and convenient way to manage sensitive documents while ensuring security and preventing unauthorized access and data breaches. We also draw on insights from previous studies on blockchain-based data management and access control to enhance the security and efficiency of our proposed system.

III. PROPOSED SYSTEM

A. System Architecture

The proposed system consists of three main components: document creation and hashing, QR code generation and embedding, Cloud Stroage and access control mechanism.



B. Document Creation and Hashing

The first step in the proposed system is to create the document that needs to be secured. This can be any type of digital document, such as a PDF, Word document, or image file. Once the document is created, the proposed system generates a unique cryptographic hash of the document using the SHA-256 algorithm. SHA-256 is a widely used cryptographic hash function that produces a fixed-size 256-bit hash value. The hash value is unique to the document and any changes to the document will result in a different hash value. After generating the hash value, the proposed system anchors it to a blockchain network using a smart contract. The smart contract is a self-executing program that runs on the blockchain network and stores the hash value of the document. Anchoring the hash value to the blockchain ensures the immutability and transparency of the document's history. Once the hash value is anchored to the blockchain, it cannot be changed or deleted, providing a tamper-proof record of the document's existence and any subsequent changes.

C. QR Code Generation and Embedding and cloud storage

The document is hashed and anchored to the blockchain, the proposed system generates a QR code containing the document's hash and user permission level. The QR code is generated using a cryptographic algorithm,SHA-256, to ensure its security. The QR code is then embedded within the document using a QR code generator library or tool. This allows users to easily scan the QR code and verify the authenticity and integrity of the document.In addition to storing the document's hash on the blockchain, the proposed system also stores metadata about the document on the cloud storage. The metadata may include information such as the document's title, author, creation date, and access permissions. This metadata is also stored securely on the cloud storage using encryption and access controls.To further enhance the security and automation of the document management process, the proposed system uses cloud smart contracts. These are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They are stored and replicated on the blockchain network, and can automatically execute transactions and update the document's status without the need for human intervention. For example, a cloud smart contract can be used to automatically grant or revoke access to a document based on certain conditions, such as the expiration of a user's access permissions.

D. Access Control Mechanism

The access control mechanism ensures that only authorized users can access the document. When a user scans the QR code, the system verifies their permission level and grants access accordingly. Any attempts to tamper with the document can be detected and traced. To verify the authenticity of the document, the proposed system provides a document verification mechanism. When a user wants to verify the document, they can scan the QR code embedded within the document using a mobile application or a web portal. The system then retrieves the document's hash from the blockchain network and compares it with the hash of the document presented by the user. If the hashes match, the system confirms that the document is authentic and has not been tampered with. Otherwise, the system alerts the user that the document is not authentic.

IV. IMPLEMENTATION AND EVALUATION

A. Implementation

The system was implemented using Ethereum blockchain and Python programming language, with the smart contract written in Solidity. Users can easily create and upload documents to the system, which are then hashed and anchored to the blockchain using a smart contract. A QR code containing the document's hash and user permission level is generated and embedded within the document, allowing users to verify the authenticity and integrity of the document using a mobile device or webcam.The system utilizes decentralized cloud storage to address scalability issues and ensure secure storage of documents and metadata. Users can access their documents from anywhere in the world using a web interface or mobile application, with the cloud storage integrated with the blockchain network for seamless and secure access.The proposed system uses a combination of blockchain technology, cryptographic algorithms, and access controls to ensure the security and integrity of documents. The use of a smart contract to anchor the document's hash to the blockchain ensures that any attempts to tamper with the document can be detected and traced. The use of cryptographic algorithms,

SA-256, to generate the QR code and secure the metadata ensures that only authorized users can access the documents.

B. Evaluation

The proposed system was evaluated in terms of security, efficiency, and usability. The results showed that the system provides a secure and efficient way to manage sensitive documents while preventing unauthorized access and data breaches. The use of QR codes for access control also makes the system user-friendly and convenient.

V. CONCLUSION AND FUTURE WORK

In this paper, we presented a novel approach for secure document management using blockchain technology and QR codes. The proposed system provides a secure and efficient way to manage sensitive documents while preventing

unauthorized access and data breaches. Future work includes further evaluation and testing of the proposed system in real-world scenarios, as well as exploring the potential of integrating other emerging technologies, such as artificial intelligence and machine learning, to enhance the system's capabilities.

REFERENCES

[1] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] Underwood, J., "Blockchain Beyond Bitcoin," Communications of the ACM, vol. 60, no. 7, pp. 13-15, 2017.

[3] Zyskind, G., Nathan, O., & Pentland, A., "Decentralizing Privacy: Using Blockchain to Protect Personal Data," arXiv preprint arXiv:1510.06134, 2015.

[4] Dierksmeier, C., & Seibold, J., "Smart Contracts as a Tool for Business Process Automation," Business & Information Systems Engineering, vol. 60, no. 3, pp. 189-192, 2018.

[5] Wang, J., Wang, F. Y., & Wang, D., "A Blockchain-Based Secure and Traceable E-Voting System," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 5, pp. 994-1006, 2019.

[6] Alkhoder, A., & Röck, C., "Blockchain-Based Document Certification and Verification Framework," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 403-410, 2019.

[7] Bichler, M., & Schmitz, C., "A Blockchain-Based Approach for Secure and Transparent Document Management," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-8, 2020.

[8] Li, X., Li, X., Guo, X., & Wang, H., "A Blockchain-Based Secure Data Sharing Scheme with Fine-Grained Access Control for Vehicle Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 6, pp. 2462-2472, 2020.

[9] Qian, L., & Liang, Y., "Blockchain-Based Secure and Efficient Data Sharing Scheme in Cloud Computing," IEEE Access, vol. 6, pp. 19888-19899, 2018.

[10] Xu, X., Weber, I., Staples, M., & Wang, R., "Taxonomy and Survey of Blockchain-Based Applications for Industrial Internet of Things," IEEE Access, vol. 5, pp. 14203-14221, 2017.