International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Blockchain-based two-level QR Code: A new era of secure data sharing

Lalu Prasad Jamana [1], Swapna Annapareddy [2], Lakshmi Narayana Kolipakula [2], Ganesh Dasu [2] * and Sadhik Shaik [2]

[1] *Assistant Professor, Department of Computer Science and Engineering (CSE), Aditya College of Engineering and Technology, Surampalem - Pin 533437, Andhra Pradesh, India.*

[2] *UG Student, Department of Computer Science and Engineering (CSE), Aditya College of Engineering and Technology, Surampalem - Pin 533437, Andhra Pradesh, India.*

International Journal of Science and Research Archive, 2025, 15(01), 147-154

Publication history: Received on 24 February 2025; revised on 01 April 2025; accepted on 03 April 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.1.0933

Abstract

In today's digital world, secure data sharing is of paramount importance. This research introduces a blockchain-based two-level QR code system, which provides an innovative solution for secure and efficient data management. The system is structured with two key modules: a user module, allowing controlled access to data, and an admin module, ensuring encrypted data storage and oversight. Each data entry is uniquely linked to a QR code, enabling seamless and secure information retrieval. By leveraging blockchain technology, the system establishes a decentralized and tamper-proof framework that enhances data transparency and mitigates security risks [1,2]. Advanced encryption techniques further fortify the system, safeguarding sensitive information from unauthorized access and ensuring data integrity [3]. This combination of blockchain technology and encryption creates a trustworthy and robust platform for data sharing [4]. Designed for simplicity and reliability, the system offers a user-friendly experience, setting a new benchmark for secure and reliable data management solutions.

Keywords: Blockchain; Qrcode; Datasecurity; Secure Dataharing; Cryptography; Decentralization; Data; Integrity; Encryption; Immutability; Accesscontrol

1. Introduction

In the realm of modern digital communication, the need for secure and efficient data sharing has grown exponentially. This research introduces an innovative blockchain-based two-level QR code system aimed at redefining secure data management. The system uniquely integrates two essential modules: a user module, which facilitates controlled access to data, and an admin module, ensuring robust encryption and efficient data oversight. A defining feature of this system is the assignment of unique QR codes to data entries, enabling users to securely retrieve information while maintaining data confidentiality. Leveraging blockchain technology, the system provides a decentralized and immutable framework, significantly enhancing data transparency and security [5]. The incorporation of advanced encryption techniques further reinforces its ability to safeguard sensitive information against breaches and unauthorized access [6]. This research underscores the system's capacity to combine technological innovation with user-centric design, offering a secure, reliable, and scalable solution for addressing the challenges of modern data sharing.

Building upon this foundation, the proposed system stands out for its ability to seamlessly merge cutting-edge technologies into a cohesive, secure, and accessible data-sharing framework. The integration of blockchain technology ensures that every transaction within the system is immutable and transparent, fostering trust among users and administrators [7]. Each unique QR code serves as a secure gateway to data, effectively eliminating the risks associated with traditional data-sharing methods, such as unauthorized access or tampering [8].

* Corresponding author: J.Lalu Prasad.

What makes this system particularly noteworthy is its dual emphasis on usability and security. While robust encryption techniques shield sensitive information, the user-friendly interface ensures a seamless experience for individuals and organizations alike. From healthcare and education to business and personal data management, the system's versatile applications highlight its potential to address diverse needs across industries.

This research not only presents a solution to current data-sharing challenges but also lays the groundwork for future advancements in secure and efficient data management, leveraging the strengths of both QR code technology and blockchain innovation.

Expanding on the system's innovative capabilities, the blockchain-based two-level QR code framework effectively bridges the gap between advanced technology and practical usability. By decentralizing data management through blockchain, the system guarantees unparalleled security, making unauthorized tampering nearly impossible. The unique QR code mechanism acts as a key to unlock specific data entries, ensuring that access remains personalized and tightly controlled. This approach not only minimizes vulnerabilities but also creates an auditable trail of every interaction, reinforcing accountability and trust.

2. Literature review

The literature on secure data sharing highlights the growing significance of integrating advanced technologies like blockchain and QR codes for enhanced security and efficiency. Several studies emphasize blockchain's decentralized and immutable ledger as a transformative solution to data integrity and transparency issues, effectively mitigating risks like unauthorized access and tampering [9,10]. Research on QR code systems explores their versatility in securely encoding and sharing information across diverse applications [11]. However, challenges such as scalability, encryption vulnerabilities, and user accessibility remain key concerns [12]. Existing studies underline the potential of combining blockchain with QR code technology to address these challenges, offering tamper-proof, encrypted, and user-friendly data-sharing frameworks [13]. Moreover, advanced encryption techniques have been widely explored to further fortify sensitive data [14]. Despite these advancements, gaps exist in implementing comprehensive systems that balance usability, scalability, and security. This research builds upon existing studies, proposing a blockchain-based two-level QR code system to address these limitations while setting new benchmarks in secure data management.

2.1. Existing system

In the current landscape, QR codes are widely used for storing and sharing information in a variety of applications, from payments to product tracking. However, existing QR code-based systems often lack strong security mechanisms to protect the data they store. Most QR code systems either store plain text or provide minimal encryption, which leaves data vulnerable to unauthorized access or tampering [15]. Additionally, the centralized nature of these systems increases the risk of data breaches, as all information is typically stored in a single database, making it a target for malicious actors [16]. Furthermore, once a QR code is generated, the data can be easily accessed by anyone with the code, unless additional encryption and authentication measures are implemented [17]. The lack of transparency and immutability in these systems also raises concerns about data integrity. While some systems implement basic encryption, they do not leverage blockchain technology, which offers decentralized security features and guarantees the integrity of transactions. The existing systems also do not allow for robust user management, leaving room for unauthorized users to gain access to sensitive information. As a result, the current QR code-based data storage and retrieval systems are often insufficient in providing the level of security and transparency required for handling sensitive or critical data.

2.2. Disadvantage of existing system

- Lack of strong data security and encryption.
- Vulnerable to unauthorized access and tampering.
- Centralized systems create a single point of failure.
- Limited transparency and immutability of stored data.
- Insufficient user authentication and access control.
- Existing systems often operate in isolation, limiting seamless data exchange across platforms.

2.3. Proposed system

The QR Code App aims to overcome the limitations of existing QR code-based systems by integrating encryption and blockchain technology to ensure the security, integrity, and transparency of data [18]. In this system, users can securely upload data, which is then encrypted and converted into a QR code. The encrypted data stored within the QR code is

protected from unauthorized access, and users can only decrypt it by scanning the code with the appropriate access credentials [19]. Blockchain technology is used to maintain a tamper-proof ledger, ensuring that data transactions are immutable and transparent. The app supports two roles: users and administrators. Users can easily register, log in, and manage their encrypted data. Administrators can authenticate users, monitor access, and manage user accounts through a dedicated admin panel. By combining encryption and blockchain, the system provides secure data storage and retrieval, reducing the risk of unauthorized access or tampering. The use of blockchain ensures transparency and immutability of transactions, making the data exchange process secure, auditable, and trustworthy. The proposed system addresses the security vulnerabilities of existing QR code systems, offering a more robust solution for both personal and organizational data management.

2.4. Advantages of proposed system

Enhanced data security through encryption and blockchain technology.

- Tamper-proof storage and retrieval of data.
- Transparency and immutability of data transactions using blockchain.
- Robust user authentication and access control.
- Decentralized system reduces risk of data breaches.
- Secure and reliable solution for personal and organizational data management.

2.4.1. Block diagram

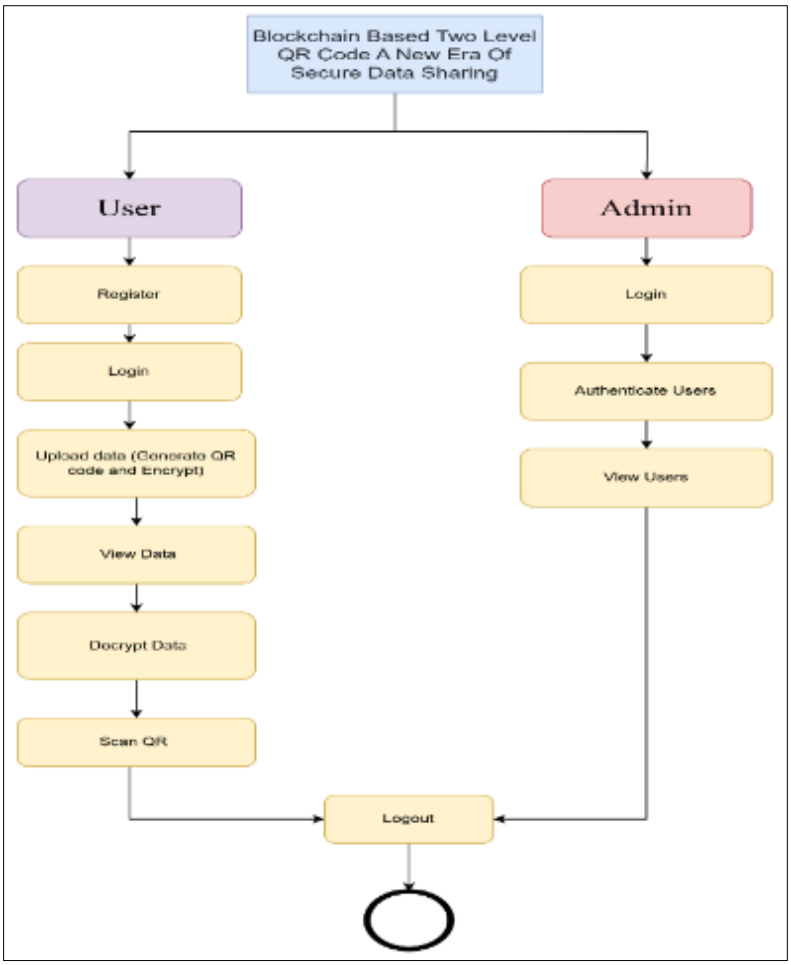

Figure 1 Block Diagram showing user roles and admin roles within the system

3. Methodology

The methodology for the QR Code App leverages blockchain technology to ensure data integrity and security throughout the data management process. The system is designed to store, encrypt, and retrieve data using QR codes, with a strong emphasis on security through encryption and decentralization with blockchain. The methodology involves the following steps:

3.1. User Registration and Authentication

Users begin by registering on the platform, where they provide their basic information, such as email, username, and a secure password. After registration, users can log in using their credentials. The login process is secured using a multi-factor authentication mechanism to ensure only authorized users can access the platform.

3.2. Data Encryption and QR Code Generation

Once authenticated, users can upload data to the system. The data is then encrypted using a strong encryption algorithm such as AES (Advanced Encryption Standard). The encrypted data is transformed into a QR code that can be stored or shared. This ensures that the data, while being transferred or stored, remains secure and can only be accessed by those with the appropriate decryption keys.

3.3. Blockchain Integration

Blockchain technology is integrated to ensure the integrity and immutability of the stored data. Every user transaction, such as data upload and QR code generation, is recorded on a blockchain, providing a decentralized and tamper-proof ledger. This ensures that once data is uploaded, it cannot be altered or deleted without detection. Blockchain also guarantees transparency, making it possible to trace the history of any data transaction.

3.4. Data Retrieval and Decryption

Users can scan the QR code to retrieve the encrypted data. Upon scanning, the system authenticates the user and allows access to the original data by decrypting it with the correct credentials. The decryption process ensures that only authorized users can view the data.

3.5. Admin Role Management:

The admin has a dedicated panel to manage user accounts, authenticate logins, and monitor user transactions. Blockchain ensures that all administrative actions are securely recorded, maintaining full transparency and accountability.

3.6. Project objectives

- **Integrate Blockchain Technology**
- Establish a decentralized and tamper-proof ledger to enhance data transparency and ensure data immutability.
- **Advanced Encryption Methods**
- Utilize cutting-edge cryptography techniques to provide robust encryption for sensitive data within QR codes.
- **Two-Level QR Code Functionality**
- Design a dual-tier QR code mechanism to facilitate secure data sharing and controlled access.
- **User-Friendly Interface**
- Develop a seamless user experience that balances accessibility and security for both technical and non-technical users.
- **Integration Across Platforms**
- Ensure compatibility with various platforms to support diverse applications, from healthcare to business environments.
- **Enhanced Access Control**
- Establish advanced authentication mechanisms, such as multi-factor authentication, to restrict unauthorized data access.

4. Output

Figure 2 Admin login page

Figure 3 Crop information provided by user

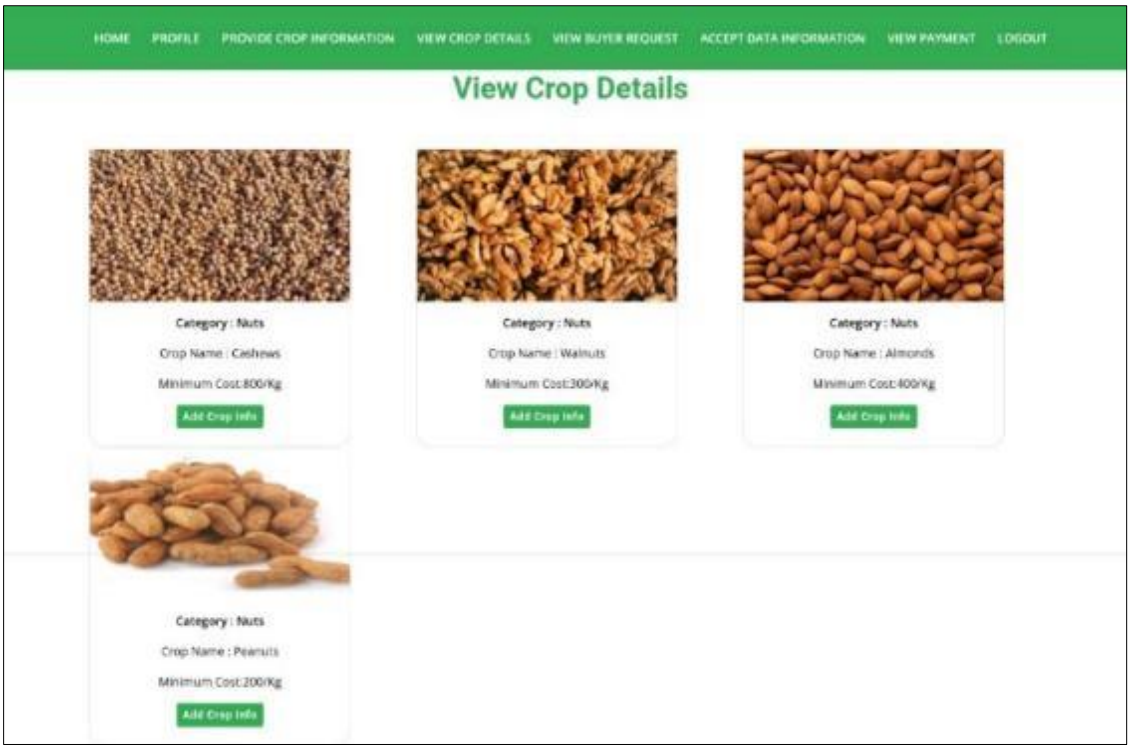

Figure 4 Displaying crop details

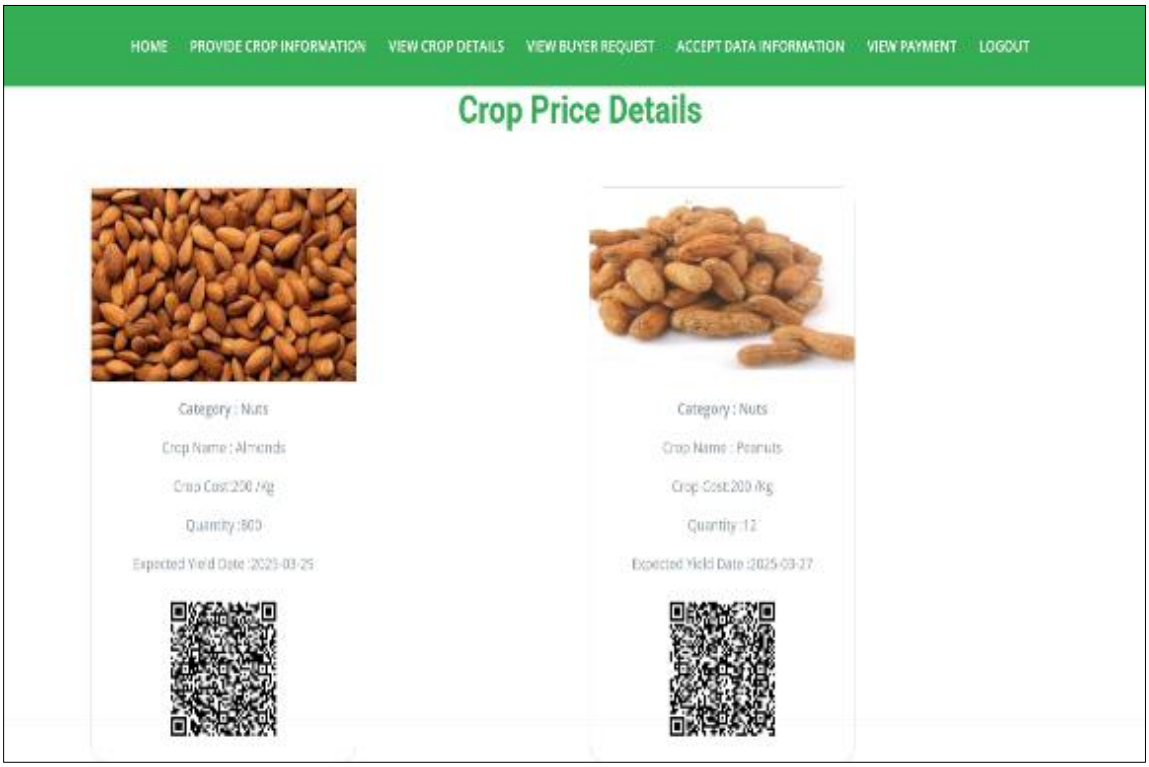

Figure 5 Displaying price details of crops

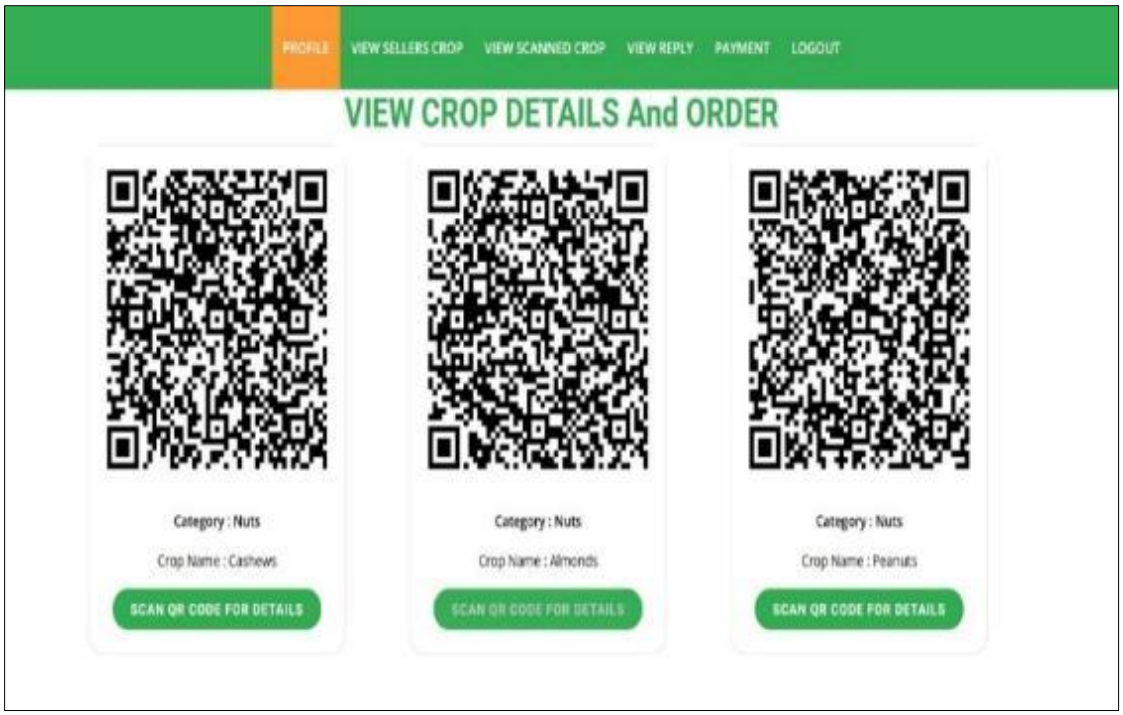

Figure 6 Displaying crop details and user order via secure QR

5. Conclusion

In conclusion, the proposed blockchain-based two-level QR code system represents a groundbreaking approach to secure data sharing. By synergizing blockchain technology with advanced encryption methods, the system delivers unparalleled security, transparency, and efficiency in data management. The two-tier QR code mechanism ensures precision in access control while maintaining user-friendly functionality. With its decentralized framework and tamper-proof capabilities, the system addresses critical challenges posed by conventional data-sharing methods. Furthermore, its scalable and versatile design opens avenues for applications across industries, reinforcing its relevance in the modern digital era. This research not only introduces a robust solution but also sets the stage for future innovations in secure and reliable data sharing frameworks.

Compliance with ethical standards

The authors declare that they have no conflict of interest.

References

[1] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[2] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[3] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[4] Buterin, ‘‘Ethereum white paper,’’ GitHub Repository, vol. 1, p. 2223, Jan. 2013.

[5] M. Swan, Blockchain: Blueprint for a New Economy. Newton, MA, USA: O’Reilly Media, 2015.

[6] D.Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Baltimore, MD, USA: Penguin, 2016.

[7] W. Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken, NJ, USA: Wiley, 2016.

[8] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, ‘‘BlockStack: A global naming and storage system secured by blockchains,’’ in Proc. USENIX Annu. Tech. Conf., 2016, p. 18194.

[9] V. Buterin, ‘‘Ethereum white paper,’’ GitHub Repository, vol. 1, p. 2223, Jan. 2013.

[10] M. Swan, Blockchain: Blueprint for a New Economy. Newton, MA, USA: O’Reilly Media, 2015.

[11] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Baltimore, MD, USA: Penguin, 2016.

[12] W. Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken, NJ, USA: Wiley, 2016.

[13] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, ‘‘BlockStack: A global naming and storage system secured by blockchains,’’ in Proc. USENIX Annu. Tech. Conf., 2016, p. 18194.

[14] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[15] A. Back, "Hashcash - a denial-of-service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002. [16] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[16] W. Feller, "An introduction to probability theory and its applications," 1957.

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

[18] K. D. Werbach, "Trust, But Verify: Why Blockchain Needs the Law," Berkeley Technology Law Journal, vol. 33, no. 2, pp. 487–552, 2018.

[19] M. Pilkington, "Blockchain Technology: Principles and Applications," Research Handbook on Digital Transformations, pp. 225-253, 2016.