e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

EFFICIENT PAPERLESS AUTHENTICATION OF STUDENTS USING BLOCKCHAIN

Anuprita Girme*1, Prof. Pooja Hajare*2, Shubhada Jadhav*3, Harshal Pandhare*4, Athrava Katke*5

*1,3,4,5UG Student, Department Of Computer Engineering, Sinhgad Academy of Engineering, Pune, Maharashtra, India.

*2Professor Department Of Computer Engineering, Sinhgad Academy of Engineering, Pune, Maharashtra, India.

DOI: https://www.doi.org/10.56726/IRJMETS63470

ABSTRACT

This paper explores the transformative integration of blockchain technology, QR codes, and Firebase Cloud in the realm of document creation and verification. The innovation is driven by blockchain's decentralized ledger and smart contract capabilities, which enhance document integrity through an indelible digital signature. QR codes are incorporated into the verification process, making it more user-friendly. When affixed to documents, these QR codes provide direct access to corresponding blockchain entries, containing critical information such as timestamps and cryptographic hashes. This integration enhances both the speed and security of document verification. Firebase Cloud, a scalable real-time cloud database, is strategically integrated to ensure secure storage and efficient retrieval of blockchain-anchored documents. The combination of blockchain's immutability, the quick verification enabled by QR codes, and the dynamic storage features of Firebase Cloud creates a robust system that redefines the standards of document security, authenticity, and accessibility.

Keywords: QR Codes, Cryptographic Hash, Digital Signature, Blockchain Technology, Smart Contracts, User-Friendly.

I. INTRODUCTION

In the current era of rapid technological advancement, the integration of blockchain technology, QR codes, and cloud computing has introduced a groundbreaking approach to document creation and verification. This powerful synergy strengthens the security and authenticity of documents while reshaping how sensitive information is handled. This paper explores the complex framework of blockchain-driven document creation, the use of QR codes for seamless verification, and Firebase Cloud's role in providing secure storage and retrieval solutions. At the core of this innovation is blockchain technology, which serves as a decentralized and tamper-resistant ledger that ensures the integrity and immutability of data. By employing smart contracts and cryptographic hashing, documents are created with a permanent digital signature, fostering a high degree of trust. Each block within the blockchain holds distinct data, forming a transparent, chronological chain of information. This development not only minimizes the risk of fraud but also establishes a strong basis for the subsequent verification stages. To facilitate and democratize the document verification process, the integration of QR codes emerges as a highly effective tool. When affixed to documents, these QR codes provide instant access to corresponding blockchain records, encapsulating crucial details like timestamps, document IDs, and cryptographic hashes. Scanning the QR code with a suitable device allows users to quickly retrieve the document's history and confirm its authenticity. This combination of blockchain and QR technology simplifies verification while enhancing both accessibility and user experience. The final aspect of this approach involves leveraging Firebase Cloud for the secure storage and retrieval of blockchain-linked documents. Firebase offers a scalable, real-time cloud database that integrates smoothly with blockchain systems. Through automated interactions, documents are securely stored in the cloud, ensuring both redundancy and ease of access. This enhances the durability of document repositories and allows for efficient retrieval when required. The combination of blockchain's unchangeable nature and Firebase Cloud's adaptive storage capabilities creates a reliable ecosystem for safeguarding important information. After going through all the available research paper some of the paper we have listed here are as follows:

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Sr. No	Paper Title	Publication Details	Description
1	Improved Visual Sharing Scheme for QR Code Applications	2022 IEEE	Generation of valid QR codes that can be decoded with some specifications, Methods, Algorithms etc.
2	Blockchain and Smart Contract for Digital Certificate	2020 IEEE	properties of the blockchain, enhancement of various paper-based certificates
3	BlockSIM: A practical simulation tool for optimal network design, stability and planning.	2020, IEEE	Info about blockchain, mainly its about its applications and how we can use its properties like stability , integration
4	Certificate Validation through Public Ledgers and Blockchain	2019, Italian Conference on Cyber security (ITASEC17),	Validation of certificates using encryption and decryption technology
5	Authentication of Printed Document Using Quick Response (QR) Code	2019, IEEE	Document verification, QR generation, Updating, etc.

II. METHODOLOGY

The traditional method of document verification typically involves an authority using a signature, which can be a lengthy and cumbersome process. If a verified copy is needed later, the entire process must often be repeated, or a separate party has to verify the document again. Additionally, fraudulent activities carried out by some individuals can lead to uncertainty about the authenticity of documents. This project addresses these challenges by proposing a solution architecture and execution model that incorporates digital signatures and document correlation factors for secure and efficient document verification. Existing System: The current document verification system is largely dependent on manual, paper-based processes, which are not only slow but also susceptible to security risks. While some documents use barcodes for verification, barcodes have several vulnerabilities, including the possibility of duplication and the risk of becoming damaged, compromising the verification process. Proposed System: Tamper-Proof Verification: By leveraging the immutable characteristics of blockchain technology, a secure record of the document's authenticity is created, ensuring that it cannot be altered or tampered with after its creation. Transparent Verification Process: This system also enables a transparent verification process, allowing anyone with access to the QR code to verify the document's validity by viewing its record on the blockchain's distributed ledger.

Smart Contract

In our project, smart contracts can be used to define the logic for QR code transactions. For instance, you can automate the process of generating QR codes when certain conditions are met (e.g., a transaction completion). This enhances trust and reduces the potential for human error in managing QR codes.

SHA-256 Hash Generation

Utilize SHA-256 to hash the data embedded in the QR codes. By generating a hash, you ensure data integrity; any change to the original data will alter the hash, signalling tampering. This is crucial for verifying that the information associated with each QR code remains unchanged and secure.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Mining Algorithm

Discuss how mining algorithms contribute to the overall security of the blockchain. For example, if using a Proof of Work (PoW) algorithm, you can explain how the computational effort required to validate transactions adds a layer of security to QR code generation, preventing fraud or unauthorized changes.

Consensus Algorithm

Analyse the consensus algorithms that govern how nodes agree on the state of the blockchain. Highlight the importance of these algorithms (such as Proof of Stake or Delegated Proof of Stake) in ensuring that QR code transactions are verified and recorded reliably across the network, thus maintaining the integrity of the entire system.

QR Code Generation

Delve into the technicalities of QR code generation that links to our blockchain solution. Explain how each QR code can store a unique identifier that references a smart contract on the blockchain. This allows for easy verification of the QR code's authenticity and the related transaction, facilitating seamless interactions.

Hardware Specifications

1. RAM: At least 4GB for optimal system performance.
2. CPU: Dual-core processor (Intel Core i3 or AMD equivalent) or higher.
3. Storage: A minimum of 128GB SSD or HDD for storing candidate-related data.

Software Requirements:

1. Visual Studio 2017 or newer.
2. Operating System: 32-bit.
3. C# and .NET for backend development.
4. React.js for frontend development.
5. Firebase Cloud for cloud-based functionalities.
6. Tailwind CSS: A utility-first CSS framework for styling.
7. CSS (Cascading Style Sheets) for additional design and styling.

III. MODELING AND ANALYSIS

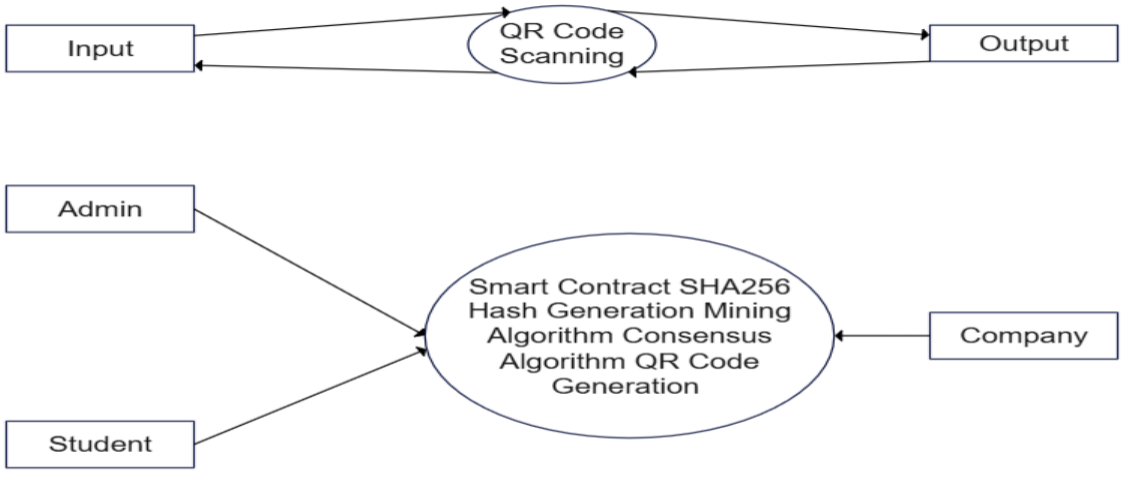


Figure 1: 3D view of building.

Description of Data Flow Diagrams:

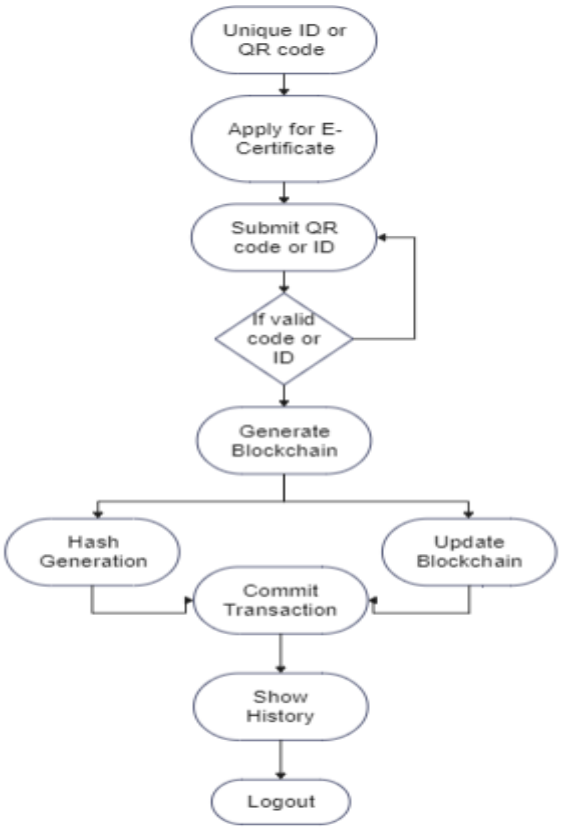
1. QR Code Scanning DFD (Top Diagram):

The top section of the DFD illustrates a basic process of QR code scanning, where an **Input** is provided to initiate the QR scanning operation. The QR **Code Scanning** process interacts with both the **Input** and **Output** elements, serving as an intermediary to facilitate the flow of data from input to output. This setup highlights the fundamental function of QR code scanning as a means to capture, process, and deliver data through a streamlined process flow.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

2. Blockchain-based Verification System DFD (Bottom Diagram):

The bottom section of the DFD represents a more complex blockchain-enabled verification system. It includes entities such as **Admin**, **Student**, and **Company**, which are connected to a central process. This process encapsulates various blockchain components like **Smart Contracts**, **SHA-256 Hash Generation**, **Mining Algorithm**, **Consensus Algorithm**, and **QR Code Generation**. Each participant (Admin, Student, and Company) interacts with this central system to facilitate secure data transactions, verifications, and integrity checks through cryptographic methods, thereby ensuring the accuracy and authenticity of information in a decentralized environment.



Description of Blockchain-based E-Certificate Issuance Process Flowchart:

This flowchart represents a blockchain-based system for issuing and verifying e-certificates. The process begins with the generation of a **Unique ID or QR Code** for each user. The user then proceeds to **Apply for an E-Certificate**, initiating the request for certification. Following this, the user **Submits the QR Code or ID**, which enters a validation step. At this point, the system checks if the provided QR code or ID is valid. If validated, the process moves to **Generate Blockchain**, where a new blockchain record is created to store the certificate details securely.

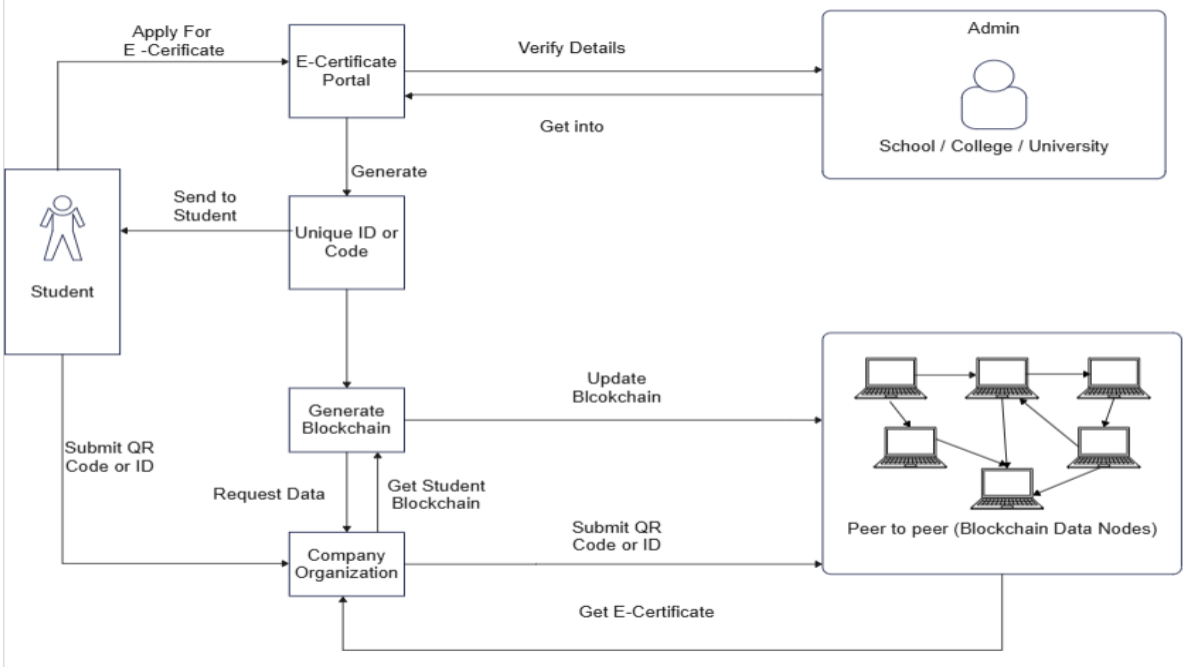
The next stage involves three parallel processes:

1. **Hash Generation** – which provides a cryptographic hash to ensure data integrity,
2. **Commit Transaction** – which adds the certificate information to the blockchain, and
3. **Update Blockchain** – which synchronizes this new information across the network.

After the transaction is committed, the user has the option to **Show History** of transactions, providing a transparent record of certificate-related activities. The final step allows the user to **Logout** from the system, completing the process. This flowchart highlights the integration of blockchain for secure and transparent certificate issuance, leveraging cryptographic hashing and decentralized updates to enhance the reliability and authenticity of e-certificates.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

IV. RESULTS AND DISCUSSION



System proposed a new dynamic certificate generation approach using own custom blockchain.

This system allows students to apply for E-certificates, stores their details securely on the blockchain, and enables companies to verify the authenticity of the certificates using QR codes or unique IDs. Below is a detailed explanation of each step in the diagram and its purpose.

1. Student Applies for E-Certificate

- **Step**: A student initiates the process by applying for an E-certificate through an online portal.
- **Purpose**: This step collects the student's information such as name, institution, course details, and credentials for generating an official certificate.

2. E-Certificate Portal Verification

- **Step**: The E-certificate portal forwards the student's application to the **admin** for verification.
- **Admin**: The admin consists of entities like schools, colleges, or universities that are responsible for verifying the student's information.
- **Purpose**: This ensures that the student is eligible for the E-certificate and that all provided data is accurate.

3. Unique ID or QR Code Generation

- **Step**: After verification, the E-certificate portal generates a **unique ID** or **QR code** for the student.
- **Purpose**: The unique ID or QR code acts as a digital identifier for the E-certificate, ensuring that it is unique to the individual. This ID is later used for verification by third parties such as companies.

4. Blockchain Update

- **Step**: The system generates a block on the blockchain that includes the student's verified information (such as their unique ID, E-certificate data, etc.). The blockchain is updated by adding this new block to the distributed ledger.
- **Purpose**: The blockchain provides a **tamper-proof** and **decentralized** storage system, ensuring that the certificate data is secure and cannot be altered after issuance. It also enables transparent and decentralized access to the certificate information.

5. Student Receives Unique ID or QR Code

- **Step**: The unique ID or QR code generated for the student is sent back to them.
- **Purpose**: The student can now use this unique identifier as proof of their certified status. This ID or QR code will be required during verification processes by external entities.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

6. Company/Organization Requests Data

- **Step**: A company or organization that wants to verify the student's E-certificate submits the unique ID or QR code to the blockchain system.
- **Purpose**: This is part of the verification process where external organizations (e.g., potential employers) request access to a student's certificate data to verify its authenticity.

7. Student Information Retrieval

- **Step**: Upon receiving the unique ID or QR code from the company, the blockchain retrieves the corresponding student information.
- **Purpose**: This ensures that the company receives verified and accurate information directly from the blockchain, removing any chance of certificate forgery or tampering.

8. Peer-to-Peer (P2P) Blockchain Network

- **Step**: The student's information is stored in a **peer-to-peer blockchain network**, which is a decentralized system consisting of several data nodes.
- **Purpose**: The P2P network ensures that the certificate information is distributed across multiple nodes, which improves security, transparency, and availability. No single node has full control of the data, preventing any possibility of centralized tampering or data loss.

9. Company Organization Retrieves E-Certificate

- **Step**: After submitting the QR code or unique ID, the company retrieves the student's E-certificate or related information from the blockchain.
- **Purpose**: This step completes the verification process, where the company gets secure and verifiable data regarding the student's credentials. This can be used to make decisions about employment, further education, or any other related processes.

V. CONCLUSION

In today's rapidly changing landscape of information management and verification systems, the combination of blockchain, QR codes, and cloud computing has proven to be a revolutionary approach. This detailed examination of these technologies for document creation and verification highlights their combined ability to offer unmatched security, authenticity, and accessibility. Blockchain technology, with its decentralized and tamper-proof ledger, ensures document immutability through the use of smart contracts and cryptographic hashing. This development not only reduces the risk of fraud but also provides a transparent, chronologically organized chain of information. The integration of the SHA-256 algorithm within the blockchain process strengthens the security of document encryption, offering a highly secure digital signature

VI. REFERENCES

[1] Y. Cheng, Z. Fu and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2393-2403, Sept. 2022, doi: 10.1109/TIFS.2018.2819125.

[2] J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455

[3] Pandey, Santosh et al. "BlockSIM: A practical simulation tool for optimal network design, stability and Planning." 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (2019): 133-137.

[4] Baldi, Marco et al. "Certificate Validation Through Public Ledgers and Blockchains." Italian Conference on Cybersecurity (2017).

[5] T. Arief, W. Wirawan and Y. K. Suprapto, "Authentication of Printed Document Using Quick Response (QR) Code," 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, 2019, pp. 228-233, doi: 10.1109/ISITIA.2019.8937084.