Journals Pub

International Journal of
Software Computing and Testing

ISSN: 2456-2351
Volume 10, Issue 1, 2024
January–June
DOI (Journal): 10.37628/IJSCT

https://journalspub.com/journal/ijsct

Review IJSCT

Certificate Issuing and Verification Application Using Blockchain

Jenifer A.[1], Pratik Mahadik[2], Shreyaskar Sanskar[3], Tannya Gupta[4], Yamini Meshram[5,*]

Abstract

With roughly a million students graduating each year, both those seeking further education and those entering the workforce rely on verifiable certificates. However, traditional paper certificates are vulnerable to counterfeiting, leading to frequent forgeries. To address this concern, this paper proposes a secure and reliable system utilizing blockchain technology for issuing digital certificates. This system creates tamper-proof digital certificates by calculating unique hash values for each electronic certificate and storing them on the blockchain. Paper certificates are then linked to QR codes and verification codes, enabling employers or institutions to effortlessly confirm a certificate's authenticity through quick mobile scans or website inquiries. This innovative approach offers a more secure and convenient solution for verifying educational credentials and fostering trust and transparency within the academic and professional landscape.

Keywords: Blockchain-based digital certificates, educational credential verification, anti-counterfeit certificates, hash-based certificate verification, mobile verification of certificates

INTRODUCTION

The rise of information technology, facilitated by the internet and mobile devices, has significantly altered human lifestyles. Virtual currencies, initially designed for online use, are now being increasingly embraced in real-world scenarios. Fueled by the convenience of the internet, various virtual currencies are flourishing, with Bitcoin, Ether, and Ripple emerging as the most popular ones. Their recent surge in value has drawn considerable attention. Consequently, people are increasingly recognizing the significance of blockchain, the underlying technology powering these transformative currencies. Blockchain, characterized by its decentralized and tamper-proof database, holds immense potential for a wide array of applications. It serves as a distributed ledger extensively employed for recording diverse transactions. Once consensus is achieved among different nodes, the transaction gets appended to a block that already contains records of multiple transactions. Each block includes the hash value of its preceding block for continuity. These blocks are interconnected to form a blockchain. Data is distributed across various nodes, ensuring decentralization of the system. Consequently, nodes collectively maintain the database. In blockchain, a block gains validation only after being verified by multiple parties. Additionally, the data within blocks cannot be arbitrarily altered. For instance, a smart contract based on blockchain establishes a trustworthy system by eliminating doubts regarding the authenticity of information.

***Author for Correspondence**
Yamini Meshram
E-mail: sce20cs041@sairamtap.edu.in

[1]Assistant Professor, Department of Computer Science and Engineering, Sri Sairam College of Engineering, Bengaluru, Karnataka, India
[2-5]Student, Department of Computer Science and Engineering, Sri Sairam College of Engineering, Bengaluru, Karnataka, India

Received Date: May 02, 2024
Accepted Date: May 16, 2024
Published Date: May 29, 2024

Citation: Jenifer A., Pratik Mahadik, Shreyaskar Sanskar, Tannya Gupta, Yamini Meshram. Certificate Issuing and VerificationApplication using Blockchain. International Journal of Software Computing and Testing. 2024; 10(1): 21–28p.

RESEARCH BACKGROUND

The rapid advancement of informatics has accentuated the need for robust data protection. Graduates, embarking on further education or job-hunting endeavors, require various certificates for

application processes. Nevertheless, the tangible form of these credentials exposes them to the risk of being lost or damaged. Reapplying can be a lengthy process, often necessitating visits to various issuing institutions in person. Electronic certificates provide a remedy by simplifying the application process and minimizing paper consumption. However, the accessibility of digital copies is accompanied by a rise in counterfeit certificates, including falsified degrees, licenses, and accolades. This poses a challenge for institutions in authenticating the legitimacy of submitted documents. To tackle this pressing concern, the research introduces a fresh certification system that utilizes blockchain technology.

The vast number of certificates generated by students throughout their educational careers in India (approximately 9 million graduates annually) [1], necessitates efficient and secure management systems. Traditional paper-based certificates pose challenges in tracking, verification, and vulnerability to forgery. The paper suggests utilizing blockchain technology as a solution to tackle these issues. Leveraging the principles of confidentiality, integrity, and availability, blockchain technology offers a secure platform for issuing and verifying digital certificates. The system outlined involves certificate issuers generating and having them validated before sending them to students. Each certificate is assigned a unique hash key, enabling any authorized organization to easily verify its authenticity through a dedicated portal. This approach not only minimizes the risk of lost or damaged certificates for students but also streamlines the verification process for employers and institutions.

Numerous research endeavors have investigated how blockchain technology could enhance the security and efficacy of certificate issuance within higher education [2]. Employing a 5D framework covering organizational, infrastructural, methodological, social, and economic aspects, this study underscores the technical merits of blockchain-driven certification systems. The decentralized and immutable characteristics of blockchain technology provide considerable advantages. Firstly, it ensures the authenticity and integrity of certificates by eliminating the risk of fraud and unauthorized alterations. Additionally, smart contracts can automate tasks related to certificate issuance, leading to increased efficiency, and reduced manual intervention. Furthermore, public blockchains enable easy access and verification of certificate details for various stakeholders, promoting transparency within the system. These results indicate that blockchain technology holds promise for transforming certificate administration in higher education through improvements in security, integrity, and accessibility.

An expanding body of research investigates how blockchain technology could transform different facets of the educational system, including the issuance and authentication of certificates [3]. This systematic literature review highlights the increasing scientific interest in blockchain applications within education. The paper emphasizes the potential of blockchain to address limitations in current certificate verification systems. By offering a decentralized, tamper-proof, and secure infrastructure, blockchain technology can enable faster, more reliable, and independent verification of academic credentials. The authors identify 34 relevant studies published between 2018 and 2022, focusing on past, present, and future research directions. Their analysis explores six key themes related to blockchain-based academic certificate verification, including security, transparency, fraud prevention, and smart contracts. The review particularly highlights areas in research that require further exploration by the academic community. By outlining future research directions and practical applications, this work provides valuable insights for researchers, policymakers, and practitioners seeking to leverage blockchain technology within the educational landscape.

Traditional academic certificate verification processes can be time-consuming and inefficient for employers seeking to confirm the authenticity of credentials [4]. The paper points out that the extended verification periods represent a bottleneck in the recruitment process. Employers typically rely on contacting issuing institutions to authenticate certificates, leading to delays in offering employment. This study proposes that blockchain technology offers a solution by providing a secure and verifiable distributed ledger. By leveraging cryptography and hashing mechanisms, blockchain can ensure the authenticity and prevent counterfeiting of academic certificates. Additionally, blockchain serves as a

shared platform for storing and accessing educational documents, streamlining the verification process, and minimizing verification times for employers.

The vulnerability of manually maintained student academic records is a growing concern in educational institutions [5]. These records serve as a critical performance history for students and are essential during interviews, further studies, or career pursuits. However, the traditional paper-based system is susceptible to tampering and unauthorized modifications, potentially impacting a student's academic standing. This study proposes blockchain technology as a solution for creating secure "Smart Certificates." Blockchain's distributed ledger system offers immutability and tamper-proof storage, ensuring the integrity of academic records. By leveraging smart contracts, the paper suggests a viable alternative for secure issuance, verification, and exchange of certificates, eliminating the risk of manipulation and fostering trust within the educational ecosystem.

A study explores challenges in managing student achievements in the digital age [6]. The paper identifies limitations in traditional transcripts, which often lack detailed performance data, and security concerns surrounding the involvement of intermediaries in issuing and verifying credentials. These factors necessitate more efficient and secure verification methods. The study suggests the UniverCert platform, a prototype developed on a consortium blockchain network. This platform empowers educational institutions to collaborate and manage student data securely, facilitating tracking of student progress, verification of academic performance, and document sharing with authorized stakeholders.

The prevalence of forged educational certificates is a significant concern, impacting the credibility of both institutions and graduates [7]. The paper highlights the limitations of traditional issuance processes, which lack transparency and verification mechanisms, making them vulnerable to counterfeiting. This vulnerability can damage the reputation of institutions and graduates alike. To address this challenge, the research proposes a digital certificate system built on blockchain technology. Blockchain's inherent immutability offers a solution by creating tamper-proof records with verifiable authenticity. The system outlines a process for generating electronic certificates with unique hash values stored on the blockchain. Additionally, QR codes and inquiry strings linked to the blockchain data are affixed to the physical certificates, enabling convenient verification via mobile devices or dedicated websites. This approach promotes transparency in certificate issuance while offering a secure and reliable method for verifying the authenticity of educational credentials.

The complexity and lack of transparency in traditional document verification processes create vulnerabilities for forgeries, particularly within educational certificates [8]. The paper emphasizes the challenges highlighted by the Indian Ministry of Education regarding the difficulty of authenticating documents due to cumbersome procedures and the absence of robust anti-counterfeiting mechanisms. This paves the way for the creation of fake certificates, jeopardizing the credibility of both institutions and graduates. To address this issue, the research proposes a digital certificate system leveraging blockchain technology. Blockchain's core functionalities—immutability and secure data storage—offer a solution for creating tamper-proof and verifiable digital certificates. The paper outlines a system where electronic certificates with unique hash values are stored on the blockchain. Additionally, QR codes and inquiry strings linked to this blockchain data are integrated into the physical certificates, enabling convenient verification through mobile devices or dedicated websites. This approach tackles the limitations of traditional systems by promoting transparency in issuance and offering a secure, reliable method for verifying the authenticity of educational credentials.

Several studies explore blockchain technology's potential to enhance the efficiency and security of academic certificate management [9]. This paper introduces BCert, a blockchain-based system designed for secure storage, distribution, and verification of academic credentials. BCert leverages Ethereum smart contracts, offering a secure and tamper-proof distributed ledger for recording all transactions and asset ownership. To ensure document validity, the system utilizes a cryptographic hash function. This

unique hash, generated from the certificate data, is stored on a public blockchain within a transaction signed by the issuing institution's private key. Furthermore, BCert integrates the InterPlanetary File System (IPFS) for decentralized file storage of the actual certificates. To address data confidentiality, the paper proposes encrypting documents using the Advanced Encryption Standard (AES) algorithm before creating blockchain transactions. This combined approach offers a secure, transparent, and efficient system for managing academic certificates.

While traditional blockchain protocols offer traceability and fairness through trusted nodes, vulnerabilities exist [10]. The paper identifies two key security concerns: the potential for compromised or dishonest central nodes, and the risk of sensitive data leakage during data access. These vulnerabilities can threaten the privacy of participants within the blockchain network.

To tackle these challenges, the study suggests a secure control mechanism for accessing data based on digital certificates. This method leverages a combination of blockchain and digital certificate technologies. The design offers a secure authentication protocol specifically for privacy data stored on the blockchain, eliminating the need for third-party verification of encrypted identity signatures. Additionally, the paper introduces a high-efficiency network forwarding protocol to support secure multi-party contract signing. This combined approach aims to protect the privacy of both contracts and participant identities within the blockchain network. The study is supported by experimental results demonstrating the efficiency and effectiveness of the proposed scheme in terms of communication overhead, storage overhead, and detection rate.

IMPACT OF BLOCKCHAIN-BASED DIGITAL CREDENTIALS

The proposed certificate issuing and verification application utilizing blockchain technology offers a multitude of advantages for individuals, institutions, and society. Here, we explore some key benefits:

1. *Enhanced trust and credibility:* Blockchain technology provides a secure and tamper-proof method for verifying the authenticity of digital certificates.
2. This helps build trust among educational institutions and employers, as they can rely on the authenticity of the credentials provided. Consequently, the system leads to a more reliable representation of academic and professional qualifications.
3. *Reduction in certificate forgery: The* inherent security features of blockchain make it exceptionally difficult to forge digital certificates. This substantially diminishes the likelihood of fraud in educational and employment settings. By mitigating fraudulent activity, the system protects the reputation of legitimate institutions and professionals.
4. *Efficiency and convenience:* Digital certificates offer ease of access and sharing compared to traditional paper certificates. This reduces the administrative burden on institutions, students, and employers. The issuance and verification of certificates become more efficient processes, resulting in time and resource savings for everyone involved.
5. *Global accessibility:* Digital certificates based on blockchain technology can be accessed and authenticated globally, from any location. This presents a significant advantage for international students and professionals seeking employment abroad. The system facilitates the recognition of qualifications across borders, simplifying the process of pursuing opportunities globally.
6. *Privacy and data control:* The application empowers users with greater control over their academic and professional data. People have the option to select which information they disclose and to whom, thereby safeguarding against potential misuse of their personal information. This fosters a sense of privacy and data ownership for users within the certificate ecosystem. By implementing these benefits, the proposed blockchain-based certificate system fosters a more secure, trustworthy, and efficient environment for issuing and verifying academic and professional credentials.

Proposed approach: Utilizing Blockchain to Enhance Trust in Digital Credentials This paper proposes a novel digital certificate system utilizing blockchain technology to address the widespread

challenge of certificate forgery. In Taiwan, with roughly one million graduates annually, the current paper-based system lacks robust anti-forgery mechanisms, making it susceptible to fraudulent certificates. This research proposes a blockchain-powered solution that leverages the inherent immutability of blockchain to create secure, tamper-proof, and verifiable digital certificates.

The proposed system involves generating electronic files for certificates, calculating unique hash values for each, and storing them securely within the blockchain ledger. This distributed ledger technology ensures the authenticity and permanence of the data, effectively preventing unauthorized alterations. To facilitate convenient verification, the system issues QR codes and inquiry string codes linked to the corresponding certificates on the blockchain. These codes can be scanned using mobile devices or accessed through website inquiries for instant verification of a certificate's authenticity.

Beyond enhanced security, the blockchain-based digital certificate system offers a multitude of advantages. It fosters trust and credibility in educational institutions and employers by providing a reliable method for verifying the legitimacy of presented credentials. This system also significantly reduces the risk of certificate forgery, protecting the integrity of academic and professional qualifications. Additionally, it streamlines the certificate issuance and verification processes, leading to improved efficiency for institutions, students, and employers. Furthermore, the system facilitates global accessibility, allowing for seamless verification of qualifications across international borders. Finally, it empowers users with greater control over their academic and professional data, ensuring privacy and preventing misuse of personal information.

PROPOSED SYSTEM ARCHITECTURE DIAGRAM

The creation of this system is informed by valuable insights obtained from an extensive review of the literature. By meticulously incorporating the identified advantages and addressing potential challenges within existing blockchain research, this project aims to create a robust and efficient solution for combating certificate forgery. The societal benefits of this system are far-reaching, encompassing increased trust in educational institutions, reduced instances of fraud, improved efficiency in credential verification, global recognition of qualifications, and enhanced privacy control for users (Figures 1–4).

SYSTEM FUNCTIONALITY

The proposed blockchain-based digital certificate system offers a feature-rich set of functionalities designed to combat certificate forgery and enhance trust in credential verification. Here is a breakdown of its core capabilities:

1. *User management:* The system facilitates user registration and authentication for various roles within the ecosystem, including educational institutions (issuers), employers (verifiers), and students (certificate holders). Secure authentication processes ensure credentialed access to the platform and safeguard user identities.

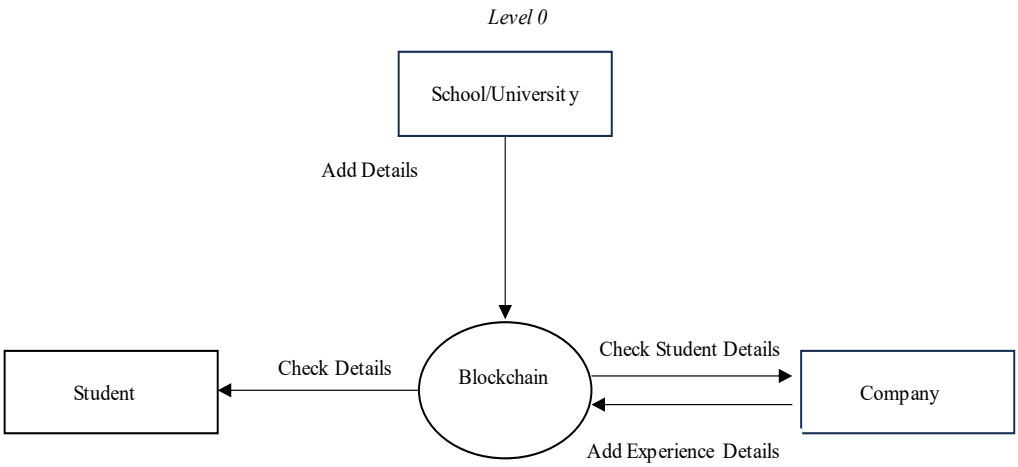

Figure 1. System architecture (Level 0).

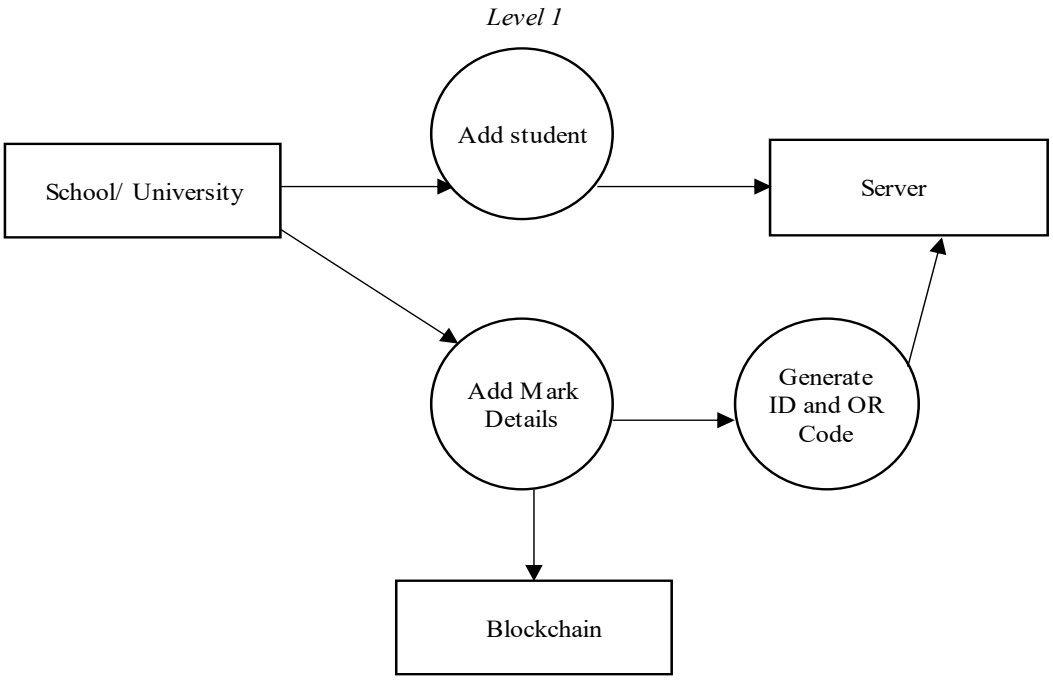

Figure 2. System architecture (Level 1).

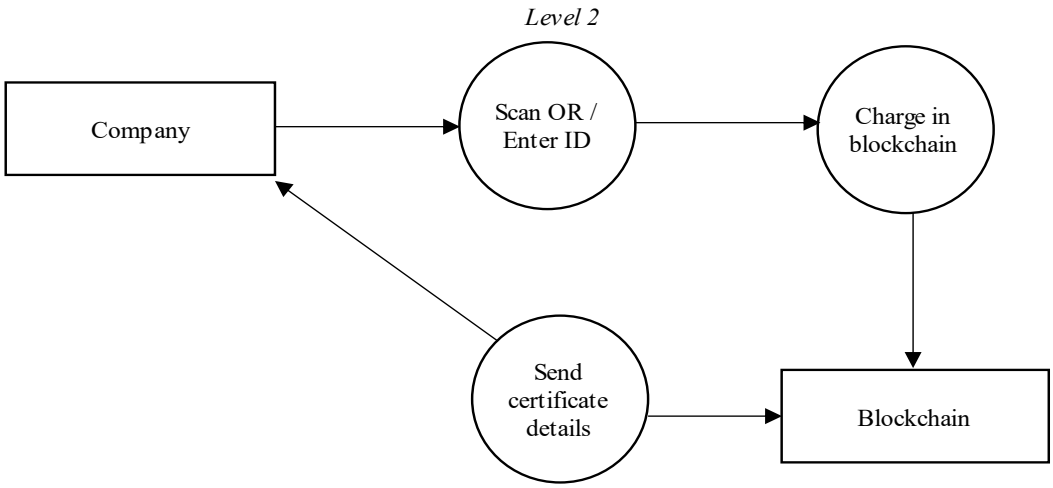

Figure 3. System architecture (Level 2).

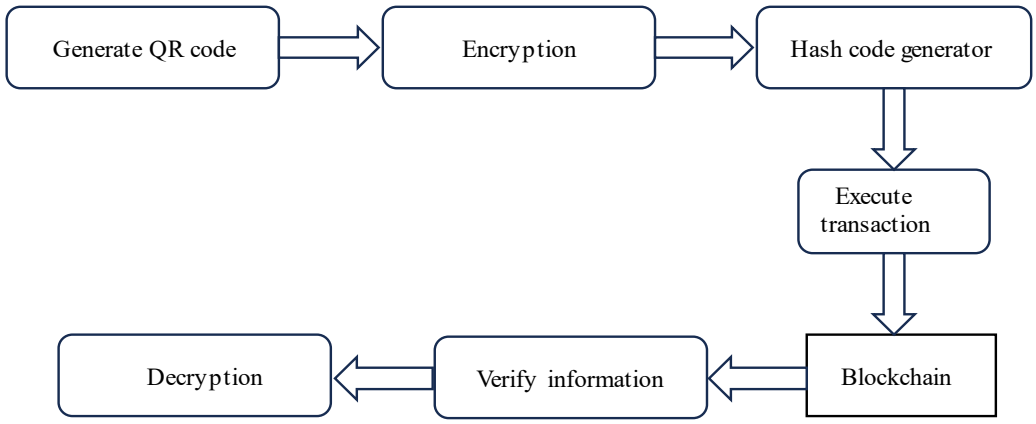

Figure 4. Block diagram.

2. *Certificate issuance:* Authorized institutions can securely issue digital certificates through the system. The process involves entering relevant student and institution information for each certificate. An electronic file corresponding to the paper certificate is then generated and stored within a secure database.
3. *Data integrity and security:* To guarantee data integrity, a unique hash value is calculated for each electronic certificate file. This cryptographic fingerprint is linked to the corresponding certificate data, ensuring its authenticity and immutability.
4. *Blockchain integration:* The system integrates with a chosen blockchain network to provide a secure and tamper-proof repository for certificate data. The calculated hash value, along with other relevant data elements, is stored within blocks on the blockchain, guaranteeing immutability and protection against unauthorized modifications.
5. *Convenient verification methods:* For each issued digital certificate, the system generates a unique QR code and inquiry string. These codes are embedded within the physical certificate, enabling effortless verification using readily available mobile devices or a dedicated website interface.
6. *Efficient certificate verification:* Users seeking to verify a certificate, such as employers or educational institutions, can utilize the QR code scanning functionality or enter the inquiry string. The system then verifies the certificate's authenticity by cross-referencing the corresponding data stored securely on the blockchain.
7. *Automated verification with smart contracts (optional):* For enhanced efficiency and automation, the system can be integrated with smart contracts deployed on the blockchain. These smart contracts can autonomously validate certificate authenticity and provide immediate verification results.
8. *User notifications (optional):* The system can be configured to send notifications to certificate holders upon issuance of new certificates or when their credentials are accessed for verification purposes. Issuing institutions can also receive notifications when certificates are verified, allowing them to track the usage of issued credentials.
9. *Robust security measures:* The system emphasizes the security of user data by incorporating strong security measures like encryption and access control protocols. These measures safeguard sensitive information and prevent unauthorized access or data breaches.
10. *Regulatory compliance:* The system is designed to adhere to all relevant data protection and privacy regulations, ensuring responsible and ethical handling of user data.
11. *Scalability and performance:* The system architecture is designed to efficiently handle a high volume of certificate issuance and verification requests. This guarantees seamless functionality and quick responsiveness, even as the user base expands and transaction volume rises.
12. *Backup and recovery:* The system integrates strong backup and recovery protocols to protect against data loss resulting from unforeseen events. This ensures the availability and integrity of critical certificate data in the event of system failures or disruptions.

METHODOLOGY

The system revised in this study operates through a secure and efficient workflow for issuing and verifying digital certificates:

1. *Electronic file generation and hash calculation:* Upon issuing a paper certificate, the system first generates an electronic file containing relevant data associated with the certificate. Concurrently, a unique hash value is calculated for the e-file using a robust cryptographic hashing algorithm. This hash value acts as a digital fingerprint for the certificate data.
2. *Blockchain integration:* The calculated hash value, along with other pertinent certificate data elements, is securely stored within a block on the chosen blockchain network. The inherent immutability of blockchain technology safeguards the tamper-proof storage of this data, guaranteeing the authenticity and integrity of the certificate.
3. *QR code and inquiry string generation:* To facilitate convenient verification, the system generates a unique QR code and inquiry string linked to the corresponding certificate data stored on the blockchain. These codes are then affixed to the physical paper certificate, enabling effortless access for verification purposes.

4. *Certificate verification:* To verify the genuineness of a certificate, users (employers, educational institutions, etc.) can either utilize a mobile phone to scan the QR code or enter the inquiry string through the dedicated website interface. The system retrieves the corresponding data securely stored on the blockchain and performs a verification process. This verification process confirms if the hash value of the presented certificate data matches the one stored on the blockchain, ultimately ensuring the legitimacy of the certificate.

CONCLUSION

The successful implementation of the envisioned blockchain-based digital certificate system relies on continued advancements in several key areas. These include ongoing developments in blockchain technology itself, smart contract functionality, identity management systems, user authentication protocols, and the establishment of interoperability standards. Additionally, robust cybersecurity measures and a supportive regulatory framework are crucial for ensuring the system's reliability, security, and legal recognition.

However, beyond technological advancements, the system's success hinges on addressing several critical dependencies. Seamless operation requires widespread access to reliable internet connectivity. Educational institutions must be willing to adopt this innovative technology for issuing certificates. Collaboration with employers is essential to ensure recognition and acceptance of blockchain-based credentials. Furthermore, the system must comply with evolving data privacy regulations. Building public trust in the security of blockchain technology and garnering government support through regulatory frameworks are also paramount. Successfully navigating these dependencies and maintaining alignment with ongoing technological and regulatory developments will be critical for achieving widespread adoption and ensuring the long-term success of the envisioned digital certificate system.

REFERENCES

1. Saja K, Stecyk A. Blockchain-based certification: enhancing transparency and trust in higher education. Eur Res Stud J. 2023;26(3):363–80. DOI: 10.35808/ersj/3219.
2. Rustemi A, Dalipi F, Atanasovski V, Risteski A. A systematic literature review on blockchain-based systems for academic certificate verification. IEEE Access. 2023;11:64679–96. DOI: 10.1109/ACCESS.2023.3289598.
3. Dubey KB, Goyal M. Smart certificate using blockchain. J Comput Sci. 2022;18:877–84. DOI: 10.3844/jcssp.2022.877.884.
4. Shakan Y, Kumalakov B, Mutanov G, Mamykova Z, Kistaubayev Y. Verification of university student and graduate data using blockchain technology. Int J Comput Commun Control. 2021;16. DOI: 10.15837/ijccc.2021.5.4266.
5. Hargude R, Ashutosh G, Nawale A, Adsure PS. Generating e-certificate and validation using blockchain. Int J Creative Res Thoughts. 2021;9(7):a86-a92.
6. Hargude R, Ashutosh G, Nawale A, Adsure S, Engineer S. Verification and validation of certificate using blockchain. Int J Creative Res Thoughts. 2021;9(6):e714–e718.
7. Lamkoti RS, Maji D, Gondhalekar AB, Shetty H. Certificate verification using blockchain and generation of transcript. Int J Eng Res Technol. 2021;10:539–44.
8. Leka E, Selimi B. Bcert: a decentralized academic certificate system distribution using blockchain technology. Int J Inf Technol Secur. 2020;12(4):103–18.
9. Liu B, Xiao L, Long J, Tang M, Hosam O. Secure digital certificate-based data access control scheme in blockchain. IEEE Access. 2020;8:91751–60. DOI: 10.1109/ACCESS.2020.2993921.
10. Kumar KD, Senthil P, Kumar DM. Educational certificate verification system using blockchain. Int J Sci Technol Res. 2020;9(3):82–5.

