International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 4, Jul-Aug 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Block-Chain Based Certificate Verification System

Khalid Rashid[1], Manaal Farakh[2], Mohammad Rameez Bhat[3]

[1]Assistant Professor, Department of Computer Science and Engineering,
[2,3]Student, Department of Computer Science and Engineering,
[1,2,3]SSM College of Engineering, Pattan, Jammu and Kashmir

ABSTRACT

The increase in the rate of academic certificate forgery and the inadequacies of the traditional verification methods have necessitated the creation of a more secure and efficient credential management system. Current verification methods are mostly manual and rely on centralized databases that are vulnerable to data breaches, malicious changes, single points of failure and long verification times.

The increase in the rate of academic certificate forgery and the inadequacies of the traditional verification methods have necessitated the creation of a more secure and efficient credential management system. Current verification methods are mostly manual and rely on centralized databases that are vulnerable to data breaches, malicious changes, single points of failure and long verification times.

The proposed system allows authorized educational institutions to securely issue, manage, verify, revoke and maintain the integrity and authenticity of credential records and issue academic certificates. Each certificate is assigned a unique cryptographic hash generated by the SHA-256 hashing algorithm, which is then permanently stored on the Ethereum Sepolia blockchain network. After being stored on the block chain, the certificate data cannot be altered or deleted and is tamper-proof, which prevents forgery and unauthorized changes.

The application layer connects to the blockchain through a back-end system developed with the Go programming language, facilitating secured and efficient operations in relation to certification. Every certificate created can also be related to a unique QR code, which makes verification easier at any time. The authenticity of the certificate can be verified either by uploading the certificate document or by directly scanning the provided QR code. In this case, users are not required to create an account or to have access to the organization's databases. The proposed solution increases security, transparency, accessibility, and trust by reducing both verification time and administrative costs.

How to cite this paper: Khalid Rashid | Manaal Farakh | Mohammad Rameez Bhat "Block-Chain Based Certificate Verification System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-4, August 2026, pp.478-483, URL: www.ijtsrd.com/papers/ijtsrd141924.pdf

IJTSRD141924

KEYWORDS: *Blockchain; Academic Certificate Verification; Certificate Revocation; Ethereum Sepolia; SHA-256; Smart Contracts; QR Code; Go Programming Language.*

1. INTRODUCTION

In the context of the digital revolution, the management of academic records has become more convenient than ever before. Nonetheless, there are some problems that arise despite technological progress made in this field. In particular, the process of academic certificate management and validation is currently one of the main challenges that still must be addressed by relevant organizations. Usually, it takes a lot of effort, time, and resources to complete the certification procedure. Moreover, there are some security-related risks involved.

Perhaps, the most severe problem associated with the current situation in the sphere of academic credential management concerns the high risks of forgery and manipulation of the mentioned data. Nowadays, one can easily obtain false certificates since they may be created by using digital software solutions. Centralized management systems storing academic records are also rather vulnerable from the point of view of possible unauthorized access and potential threats to data integrity and safety

Blockchain technologies have been developed as an innovative method for securing digital information. Contrary to ordinary databases, information about digital certificates stored via blockchain technologies is not related to any organization or individual since it belongs to a decentralized network. [1]

To resolve the issues, this paper suggests implementing a blockchain-based certificate verification and revocation system that will provide an effective means of handling academic credentials and issuing certificates from the part of authorized educational institutions. All issued certificates are subject to validation through SHA-256 hashing algorithm and stored on Ethereum Sepolia blockchain as unique cryptographic hashes. Once placed in a blockchain database, the certificates become unalterable and untouchable, which effectively eliminates the problem of fraudulent manipulation. [7], [10]

Moreover, the system features Go-based backend infrastructure that ensures a secure connection between the application layer and the blockchain network to perform necessary actions related to certificate validation

Ease of Use: A Go-based backend facilitates communication between users and the blockchain, while QR-code integration enables quick and convenient certificate verification. The system allows authorized institutions to issue certificates securely and enables employers, organizations, and individuals to verify certificate authenticity without requiring account registration.

The primary objective of this work is to develop a reliable, transparent, and tamper-resistant framework for academic certificate management. By leveraging blockchain technology, the proposed system aims to reduce verification time, prevent certificate forgery, improve trust among stakeholders, and provide a scalable solution for modern educational environments.

2. RELATED WORK

To solve problems like falsification of certificates, inefficiency in the verification process and dependence on central databases some researchers have tried to use the blockchain technology in verification of academic certificates. Different scholars have already noticed that credential handling can be effectively and securely addressed by blockchain.

In their study Rustemi et al. did a systematic literature review of blockchain-based systems used for the purpose of verification of academic certificates. They discussed the pros provided by the blockchain technology in their paper. They include decentralization, transparency, immutability and more. However, they mentioned some limitations that restrict the use of blockchain technology like scalability and interoperability. [3]

Reddy et al. suggested a blockchain framework for ensuring the safety and authenticity of graduate certificates. This study was focused on the use of blockchain technology for the secure storage of records and reliable authentication procedures. Enhanced security and decreased reliance on third parties were considered the key features of the solution. Nevertheless, the question of transaction fees, the potential for scalability, and integration with the institutional structure still needed to be solved. [2]

Kumutha and Jayalakshmi provided an overview of blockchain use cases in the field of certificate verification in academia. The authors pointed out that implementing blockchain technology can substantially decrease document forgery and ensure greater transparency in record management processes. In addition, the implementation challenges of blockchain in this area were considered, such as user adoption and lack of standardization. [4]

Kareem and Shakir examined several approaches for verifying blockchain-based certificates and concluded that blockchain technology provides reliable protection from certificate alterations. According to Kareem and Shakir, most blockchain based approaches to academic certificate verification have focused primarily on issuing and verification, but not on long-term maintenance, certificate revocation, and governing measures. [5]

QR-code based approaches to verifying students' credentials have been extensively explored recently and prove effective due to fast access to the necessary information and convenient format. While QR code-based verification makes the entire process more accessible and faster, most of such approaches rely on centralized databases that can be tampered with.

The Cerberus framework is an example of a blockchain-based approach to verifying degrees that successfully solves the real-world problem of degree fraud. The Cerberus approach includes using smart contracts, certificate revocation features, and mechanisms of public verification. Nonetheless, the authors mention several issues related to privacy management, scalability, and the possibility of integrating the Cerberus approach into the current educational ecosystem. [6]

It can be seen from the discussion above that the use of blockchain technology can be very helpful when

developing efficient systems for managing academic credentials. However, there are still many limitations.

3. PROPOSED SYSTEM

The proposed system is a blockchain-based academic certificate issuing, verifying, and revoking system aimed at providing a convenient and secure solution for managing such credentials. While most of the existing blockchain systems require educational organizations and their members to create cryptocurrency wallets to interact with the blockchain, the proposed system makes interaction with the interaction with the blockchain invisible to users to keep its security advantages and simplicity of use at the same time.

According to the proposed system, any educational institution must sign up for the service to get an opportunity to perform certificate management operations. The registered organizations gain access to an interface that allows them to manage academic certificates on the network without dealing with cryptocurrency wallets. The blockchain creates a SHA-256 cryptographic hash from the certificate details and writes this information to the Ethereum Sepolia blockchain. All transactions are done using the public issuing wallet set up by the system provider. The public address of this wallet is known and helps confirm that the issuing entity of the certificates is legitimate and trusted. The use of the one public issuing wallet allows achieving consistency and transparency in the process of issuing credentials in a reliable way. [7], [10]

Once the certification is completed successfully, a certificate card with a unique QR-code is provided for the issuing institution. This is a convenient format to present the digital certificate and make the document easy to share. The QR-code of the certificate is directly connected to the blockchain record and can be scanned to verify the certificate.

Another essential characteristic of the developed system is that it allows public verification. Anyone can verify a certificate without having a user profile on the platform, opening an account, or using a blockchain wallet. One needs to either scan the QR-code printed on the digital card or upload the certificate through the verification portal. Automatically, the certificate hash will be compared with the respective blockchain data entry. Furthermore, there is support for certificate revocation. Authorized bodies may revoke the issued certificates from the dashboard when required. The status is permanently stored in the blockchain, so that invalid certificates cannot be submitted as valid credentials. To increase accessibility while still offering security features, it is essential not to require wallet management by users and offer free public access. Digital certificate cards are issued by means of QR codes.

4. SYSTEM ARCHITECTURE

The architecture of the proposed system provides secure and transparent certificate issuance, efficient verification, and management using blockchain technology. The main components of the system include the Institution Registration Module, Institution Dashboard, Blockchain Layer, Certificate Management Module, and Verification Portal.

The first element of the architecture is the Institution Registration Module. As mentioned above, before using the system, the institution needs to be registered and authorized. Upon being allowed to use the platform, the institution receives access to the Institution Dashboard.

The Institution Dashboard is a tool used by institutions to perform certificate operations. These may include certificate issuance, view issued certificates, and revoking certificates. The interface allows institutions to avoid the need for interaction with blockchain wallets and smart contracts.

The Certificate Management Module receives certificate data entered by institutions via the institution dashboard. Upon receiving this data, the system generates SHA-256 hash, which uniquely identifies the data related to the certificate. Then, the certificate hash is sent to the blockchain layer where it will be stored. Additionally, the system creates a digital certificate card with certificate data and QR code that is tied to the blockchain certificate record. [10]

The Blockchain Layer comprises of smart contracts running on the Ethereum Sepolia chain. Rather than having separate wallets for each institution, all blockchain transactions will be made using one publicly-known issuing wallet controlled by the application. The wallet address will be known to the public, which will allow for any stakeholder to confirm the issuance of certificates by an approved source. The blockchain will securely store the certificate hashes and revocation statuses. [7]

The Verification Portal will offer a publicly available portal for the validation of certificates. No account creation or possession of any cryptocurrency wallet is needed to validate a certificate. Verification can be performed in two ways – by scanning the QR code printed on the certificate card, or by uploading the certificate. The application will locate the certificate entry on the blockchain and compare the hashes to validate its authenticity. Verification results will be instantly provided.

The above architecture represents a combination of accessibility and security offered by blockchain technology.

5. IMPLEMENTATION

The suggested solution leverages web technologies, blockchain and cryptography tools to make the process of certificate issuance and verification secure. The frontend is developed to provide the intuitive user interface for educational establishments and public users, while all back-end functions such as authentication, processing certificates, interacting with blockchain, and verifying certificates are performed automatically.

To handle certificate records and their revocation status, a smart contract is deployed on the Ethereum Sepolia test network. For transaction handling purposes, a specific platform wallet is set up via MetaMask. Private keys to access this wallet are stored in the backend server in a secure manner. In other words, these keys are used only to sign transactions that educational establishments make on the Ethereum network. This approach makes it unnecessary for educational establishments to set up and use cryptocurrency wallets, thus simplifying certificate issuance process. [7], [9]

Backend communicates with Ethereum blockchain via Infura, which is used as an RPC provider. Through this integration, blockchain transaction handling is possible. Namely, submitting certificate hashes, getting information about certificate records on Ethereum blockchain, and managing their revocation status are made possible via Infura. Institutional authentication will be performed by registration/login process. The authentication process for institutions is carried out via the safe registration and logging in procedure. After the successful log-in of an institution to the platform, the backend system creates a temporary session key which will be used to authorize each following request. Institutions' ability to create or revoke certificates is verified by session keys only. [8]

The issuance process of a certificate involves creating a unique SHA-256 hash based on certificate data. Afterward, the created hash is sent to the smart contract and written in Ethereum Sepolia blockchain. Once the record is created, a digital certificate card with all information and a unique QR-code attached to the certificate stored on the blockchain is created. [7], [10]

The platform also offers a public verification website that can verify a digital certificate. In contrast to issuing institutions, public users do not need to go through the process of registration or creation of blockchain wallets to perform the task. For verification purposes, they either scan the QRcode located on a digital certificate card or upload a digital certificate to the site. Then, the backend creates the hash based on the uploaded certificate and compares it with the record available on the blockchain through a smart contract. [7], [10]

For verification, there is also a public verification portal available in the system. As opposed to issuing institutions, public users are not expected to register or create an account on the platform. There are two methods for certificate verification; either scan the QR code contained in the digital certificate card or upload the certificate file directly into the platform. The backend creates a hash of the uploaded certificate and then compares it with the hash stored on the blockchain via the smart contract. Depending on the match, the system will determine the validity status of the certificate. [7], [10]

The proposed architecture utilizes the benefits of the blockchain technology along with secure sessions to achieve certificate management.

6. RESULTS AND DISCUSSION

The blockchain-based certificate verification system was effectively developed and tested in an Ethereum Sepolia blockchain environment. In the process, the system proved its capability to issue, verify, and even revoke academic certificates in a secure manner and ensure transparency of information. The combination of blockchain technology with SHA-256 hashing and QR-code based verification helped maintain a tamper-proof record of the certificates and also make them verifiable through the system. [7], [10]

Both the modules of institution registration and authentication worked flawlessly as expected. Institutions with appropriate authorization had access to the dashboard through which they could issue certificates in a straightforward process, without any need to interact directly with the blockchain wallets. It was ensured that only authorized institutions would be able to execute certificate issuance and revocation operations through session-based authentication.

During certificate issuance, the system generated a unique SHA-256 hash for each certificate, and this hash was then recorded in the Ethereum Sepolia blockchain by means of the smart contract. The transactions were permanently recorded in the blockchain and could not be modified thereafter. After the blockchain registration, the unique QR code-based certificate was automatically generated and given to the issuing institution. The verification component was tested using the two existing verification techniques. For the first technique, users submitted their certificates into the verification portal.

The system would then generate the certificate hash and compare it against the data stored on the blockchain. For the second technique, users would be able to verify their certificates using the QR code embedded in the certificate. Both approaches provided accurate results in a timely fashion without needing users to create accounts and use cryptocurrency wallets.

Testing of the certificate revocation component was also successful. Authorized entities were able to cancel issued certificates using the dashboard. Upon cancellation, the certificate status would be changed on the blockchain network, and the new status would accurately reflect the changes when users attempt verification in the future.

In contrast to the existing systems, the proposed solution provides enhanced security, transparency, accessibility, and efficiency. The absence of manual validation processes decreases processing time, whereas blockchain technology ensures that no one makes any changes to the certificate records without permission. Also, public validation is possible without registering on the platform, which improves user-friendliness.

According to experiment results, the developed system proves to be an effective and dependable solution to the problem of handling academic credentials. Combining blockchain technology, cryptographic hash functions, QR code validation, and safe institution authorization solves many issues that were inherent to conventional methods of certificate validation.

7. CONCLUSION

In conclusion, the present paper described a blockchain technology application that is intended to be used for academic certificate management. The use of such technologies would eliminate such shortcomings associated with traditional systems as susceptibility to forgery, unauthorized changes, data breaches, long verification time, and others. The suggested system makes use of Ethereum Sepolia blockchain, cryptographic hashing algorithm SHA-256, and smart contracts to provide maximum security and immutability for academic credentials. [7], [10]

To create and revoke certificates using the blockchain-based system, authorized institutions can make use of an exclusive dashboard. This means that users do not have to manage their private blockchain wallets; all transactions would be conducted by means of a publicly known issuing wallet.

One of the significant features implemented in the suggested system is the development of the digital certificate card embedded with QR codes facilitating instant certificate validation. This allows public users, employers, and organizations to verify the certificate holder's credentials without creating any account and using cryptocurrency wallets. Furthermore, the session-based authorization process ensures that any certificate issuance or revocation processes can only be carried out by authorized organizations.

As per the results obtained from the experiments conducted, the suggested method not only improves the security aspect but also cuts down the verification time as well as certificate tampering. Overall, the integration of Blockchain immutability with advanced cryptographic verification processes leads to a trustworthy platform for managing academic certificates. The suggested framework makes a valuable contribution towards fostering trust in educational credentials.

8. FUTURE WORK

While the suggested solution has been proven successful in providing safe certificate issuance, verification and revoking capabilities, there are several possible directions for improvements in future iterations of the platform.

One of the possible directions for future research is the implementation of the current solution into a live blockchain environment. In addition to that, it can be supplemented with various additional security measures, such as multi-factor authentication, role-based access controls and more advanced auditing tools. Another important improvement to be considered is the possibility to manage credentials issued by multiple educational organizations using the same platform within the framework of federated governance.

Another enhancement to be added to the platform is the creation of dedicated mobile apps to be used in the process of certificate issuing and verification. It can be coupled with the implementation of decentralized identity frameworks and self-sovereign identities that will give individuals more freedom when dealing with their certificates. Finally, another area of research lies in creating a platform that is compatible with existing education management systems and digital credential solutions from governmental authorities.

REFERENCES

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

[2] T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, Ch. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, “Proposing a Reliable Method of Securing and Verifying the Credentials of Graduates Through Blockchain,”

EURASIP Journal on Information Security, vol. 2021, no. 1, Art. 7, 2021.

[3] A. Rustemi, B. Selimi, and A. Imeri, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," 2023.

[4] S. Kumutha and T. Jayalakshmi, "Blockchain-Based Academic Certificate Verification: A Review," EAI Endorsed Transactions on e-Learning, vol. 10, no. 1, 2024.

[5] S. Kareem and H. Shakir, "Review of Academic Certificate Verification Processes Using Blockchain Technology," International Journal of Advanced Computer Science and Applications, vol. 14, no. 3, pp. 245–252, 2023.

[6] A. Tariq, H. Binte Haq, and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1503–1514, Aug. 2023.

[7] Ethereum Foundation, "Ethereum Documentation." [Online]. Available: https://ethereum.org/docs/

[8] Infura, "Ethereum API and Developer Tools Documentation." [Online]. Available: https://docs.infura.io/

[9] MetaMask, "MetaMask Developer Documentation." [Online]. Available: https://docs.metamask.io/

[10] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)," FIPS PUB 180-4, Aug. 2015.