INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

A Decentralized Blockchain Framework for Secure Certificate Verification and Fraud Mitigation

Dr.K.Upendra Babu, Jalla Guru Gopala Sai Varun, Mummadi Usha Shri, Thallapelli Kishore
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research,
Chennai, India
upendrababu.cse@bharathuniv.ac.in, saivarun8203@gmail.com,
ushashri2005@gmail.com kishorethallapelli14@gmail.com

Abstract : **This study presents a decentralized framework for certificate verification built upon blockchain principles to establish a secure and tamper-resistant validation ecosystem. Instead of preserving the original certificate document on the ledger, the framework records a cryptographic fingerprint generated through the SHA-256 hashing mechanism, thereby protecting privacy while ensuring integrity. Each issued credential is linked with a unique certificate reference and a machine-readable Quick Response (QR) code to enable rapid verification. The proposed architecture strengthens trust by preventing post-issuance manipulation and reducing dependence on intermediary validation authorities. Experimental observations indicate that the framework improves verification speed, enhances transparency, and significantly minimizes credential fraud risks.**

Keywords— *Blockchain, Certificate Authentication, Distributed Ledger, SHA-256, QR Code Verification, Fraud Prevention.*

I. INTRODUCTION

The digitalization of job ecosystems has greatly increased the need for reliable ways to verify credentials. Universities, certification bodies and employers often require proof of qualifications and professional certifications before granting admissions, jobs or access to institutions. However traditional validation methods still rely heavily on documents, email confirmations or databases managed by institutions. These approaches are often inefficient have delayed response times and are vulnerable to document forgery.

The rise of editing tools and digital document manipulation techniques has made it harder to identify certificates. As a result organizations need an authentication model that guarantees the integrity and traceability of issued credentials.

Distributed ledger technology provides a solution to this challenge by establishing an immutable and decentralized storage model. Once certificate metadata is recorded in the ledger altering it becomes nearly impossible without detection. This study proposes a blockchain-driven certificate verification framework where the cryptographic digest of the certificate is permanently recorded. The system also integrates QR-enabled validation to simplify real-time authentication for stakeholders like employers and educational institutions.

Traditional certificate verification systems mainly rely on processes or centralized databases maintained by issuing institutions. In manual verification organizations often contact the issuing authority via email, phone or official correspondence, which's time-consuming and prone to delays and human errors. Centralized digital systems although faster have vulnerabilities like points of failure and risks of unauthorized data modification. These systems lack transparency. Require trust in a central authority, which may not always be reliable or accessible. These limitations highlight the need for an approach that ensures both security and trust without relying on intermediaries.

Blockchain technology has emerged as a solution of addressing these challenges due to its decentralization, immutability, transparency and cryptographic security. A blockchain is a distributed ledger that records transactions across nodes ensuring that once data is stored it cannot be altered or deleted without consensus from the network. This tamper-proof nature makes blockchain ideal for storing and verifying information, like educational certificates.

By leveraging cryptographic hashing and digital signatures, blockchain ensures that each certificate is uniquely identifiable and resistant to forgery or unauthorized modification.

II. LITERATURE SURVEY

The idea of blockchain systems started with a concept: making transactions without needing someone in the middle that you have to trust. On people looked at how blocks could be connected with cryptography to keep things safe even when you are not sure about the people involved.

Later people started to think about using blockchain for more than money for things that need to be trusted and checked.
Many people have said that blockchain is a way to keep records safe because it is hard to change things once they are written and you can see everything that has happened.

In schools people have looked at using blockchain to keep track of what students have achieved like badges and certificates from schools. This work shows that using blockchain can help stop people from making records and make everyone more confident that the records are real.

What people have written about this topic says that using blockchain to check if academic records are real is an idea and can help stop fraud.

With blockchain getting better people have suggested ways to use it to check if certificates are real. One way is to store a code called a hash for each certificate on the blockchain so it cannot be changed. Each certificate gets its special code, like a fingerprint. If someone tries to change the certificate the code will be different so you can tell if it is fake. You can also use QR codes to make it easy for people to check certificates. This makes certificates faster and makes people trust the system more.

People have also been working on making systems that use blockchain with technologies, like smart contracts and special ways to store files. One good idea is to use contracts to make, check and cancel certificates automatically. These contracts make sure that rules are followed without needing someone in the middle which reduces mistakes. Also people use systems like the InterPlanetary File System to store files outside of the blockchain but still keep a record of them on the blockchain. This makes the system work better. Can handle more users.

Some people have also looked at making the system more secure by using cryptography and digital signatures. This makes sure that only the right people can make certificates and that you can check who made them. This adds a layer of security and keeps the certificates safe.. There are still problems with managing the keys used for security and making the system simple to use.

Other researchers have looked at using blockchain with technologies to make the system better. For example they have suggested using chatbots to make it easy for people to interact with the system. They have also used applications, called DApps to let people use the blockchain directly. These new ideas help make the system easier to use and more popular.

Even though blockchain has come a way in helping to check certificates and stop fraud there are still some problems. Many of the systems that exist now are for specific schools or areas and they do not work well together. Also the blockchain can get slow and expensive when many people are using it. There are also concerns about keeping information safe when it is stored on the blockchain. Moreover using blockchain can be. Requires technical knowledge, which can stop more people from using it.

Overall what people have written says that blockchain is a way to solve the problems of checking certificates and stopping fraud. It is a way to make secure and transparent systems because it is decentralized and cannot be changed. However we need to make systems that can handle users work with other systems keep information private and are easy to use.
The system we are suggesting builds on what has been done by using blockchain with good storage and easy-, to-use interfaces to make a practical and secure way to check certificates.

III. PROBLEM STATEMENT

Traditional certificate verification methods have problems. They are slow and not very secure. Mostly verification involves talking to the institution that issued the certificate, which takes a lot of time and work. These processes can take days or even weeks especially when checking across institutions or countries.

There is another issue with how certificate data is stored. It is usually kept in one place, like a database server. This creates a point of failure. If someone gets access or the server crashes it can affect the data.

Forged certificates are also hard to detect by looking at them. With digital editing tools bad actors can make fake certificates that look real.

We need a way to verify certificates. It should be automated, secure and not rely on one authority.

Current verification methods are mostly manual. Use centralized systems. Manual verification is slow. Involves direct communication with the issuer. Centralized digital systems are faster. Have issues like single points of failure and vulnerability to cyberattacks. They also lack transparency.

Another big challenge is that different institutions have their systems and procedures. This makes it hard to verify certificates across institutions or countries.

Institutions shutting down or losing records also causes problems. It can make certificate verification impossible.

There is also no way to revoke certificates. If a certificate is issued by mistake or for reasons it is hard to invalidate it. This allows bad certificates to be used without detection.

Therefore we need a decentralized and reliable certificate verification system. It should eliminate the need for intermediaries ensure data integrity and enable verification. A blockchain-based framework can help address these challenges by using distributed ledger technology and automation to create a system for certificate authentication.

The proposed system aims to provide an scalable solution for certificate verification. It will leverage security to prevent fraud and ensure data integrity. With this system verification will be instant. It will eliminate the need for intermediaries.

By using a decentralized approach the system will ensure that certificate data is not stored in one place reducing the risk of a point of failure. The system will also enable institutions to verify certificates in time making the process more efficient.

Overall the proposed blockchain-based framework has the potential to address the challenges associated with certificate verification methods. It will provide a decentralized and reliable solution, for certificate authentication and fraud mitigation.

IV. PROPOSED SYSTEM

The new system has a way to check if certificate records are real and not changed. It does this without storing the certificate on the blockchain. Instead it makes a code from the certificates digital information.

This code is like a name for the certificate and it is stored in a new block. Each block has the certificate code the time it was made the code from the block before it and a special block name. The blocks are linked together in a way that makes it easy to see if someone tried to change anything.

To make it easier to use each certificate gets an ID and a QR code. The QR code has a link to the certificate or a safe way to check if it is real. This means that schools and employers can check if a certificate is real using their phones.

When someone checks a certificate it gets coded again. The new code is compared to the one, on the blockchain. If the codes are the same then the certificate is real. If they are not the same then the system says the certificate is not real or has been changed. The certificate records and the blockchain work together to keep everything honest.

To simplify the verification process, each certificate is associated with a Quick Response (QR) code. The QR code contains a reference to the certificate's blockchain record, allowing users to verify authenticity instantly using a mobile device. This feature enhances user experience and ensuquick access to verification services. Additionally, the system provides multiple verification methods, including certificate ID-based verification and file upload verification, making it flexible and user-friendly.

V. METHODOLOGY AND ALGORITHM

A. *System Architecture*

The system is made up of four parts that work together. These parts are certificate issuance, cryptographic processing, blockchain ledger management and verification interface.

The certificate issuance part lets people who are allowed to do so upload certificates using a website made with Flask. When a certificate is uploaded the cryptographic processing part makes a code called a SHA-256 hash that is unique to the file.

The blockchain ledger management part makes a block in the blockchain that has this special code in it. This new block is linked to the block in the chain, which helps keep everything in order and makes sure it cannot be changed.

The verification interface part checks certificates in time by using the certificate ID or by scanning a QR code. This is how the system architecture works with the blockchain ledger management and the other parts, like the certificate issuance and cryptographic processing and verification interface. The verification interface and the blockchain ledger management and the cryptographic processing and the certificate issuance all work together to make the system work properly.

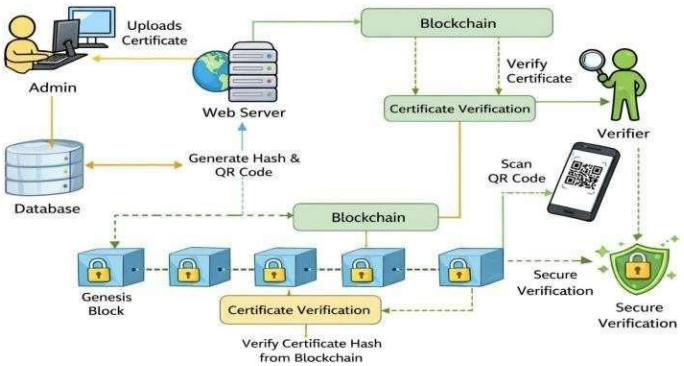

Fig. 1. System architecture of the blockchain-based certificate verification framework.

B. *Algorithm*

The administrator logs into the system. Uploads the certificate through the web interface. The system then processes the file to create a special code.

The system uses this code. Adds a timestamp and a reference to the previous code. Once this is added to the blockchain it cannot be changed. The system also creates an identifier and a QR code for the certificate. When someone wants to verify the certificate the system checks the code again. Compares it with the one stored on the blockchain. If they

match the certificate is legitimate. If they do not match it means someone has tampered with the certificate.

The system stores information about the certificates on the blockchain. When an institution issues a certificate the system creates a version of it. This digital version has all the details, like the students information and the course details. The system then uses an algorithm to create a code for the certificate. This code is stored on the blockchain so it cannot be changed.

The system stores the codes and some other important information on the blockchain. However it stores the certificate files separately using a database or a decentralized storage system. This helps the system work faster and more efficiently. When someone wants to verify a certificate the system checks the code on the blockchain with the code of the submitted certificate.

There are three types of users in the system: the issuer, the certificate holder and the verifier. The issuer is usually an institution that issues certificates. The certificate holder is the person who receives the certificate like a student. The verifier is the person who checks the certificate like an employer. The system allows the verifier to check the certificate without contacting the issuer. This makes the process faster and more efficient.

Each certificate has a QR code that links to the certificates record on the blockchain. This allows users to verify the certificate quickly using their devices. The system also provides ways to verify certificates making it easy to use.

The system uses contracts to automate many tasks. These contracts manage the issuance, verification and revocation of certificates. They ensure that the system follows the rules and minimizes errors.

The system is designed to be secure. It uses the blockchain to prevent changes and ensure the integrity of the data. The system also uses techniques to protect the certificates. The blockchains decentralized nature ensures that the system is reliable and available.

The system can be used by institutions and platforms making it scalable and interoperable. It can be used to create a verification network, where certificates from different organizations can be verified through a single platform. This is particularly useful for education and employment systems.

In summary the blockchain-based certificate verification system is a efficient and scalable solution for managing and verifying digital credentials. It eliminates the need for authorities ensures the integrity of the data and enables instant verification. This helps to prevent certificate fraud and builds trust among stakeholders. The system is based on blockchain technology. Uses certificate verification to ensure the authenticity of digital certificates. The certificate verification process is a part of the system and it uses blockchain to store certificate fingerprints in the form of cryptographic hash values. The system also uses certificate verification to confirm the legitimacy of certificates. It uses blockchain to ensure the integrity of the data. The blockchain-based certificate verification system is a tool for managing and verifying digital credentials and it has the potential to revolutionize the way we verify certificates. The certificate verification system is a component of the blockchain-based system and it plays a crucial role, in ensuring the authenticity of digital certificates.

VI. IMPLEMENTATION

The framework uses Python as the programming language because it is flexible with cryptographic operations and backend integration.

The Flask framework is used to build the web interface and manage server-side interactions.SHA-256 hashing is implemented using Pythons built-in libraries ensuring consistent and secure digest generation.The blockchain is a custom linked data structure where each block contains the certificate hash, timestamp, nonce (if required) and previous block linkage.QR code generation is integrated through Python-based encoding libraries enabling creation of machine-readable validation identifiers.

The frontend interface enables two operations:

- certificate issuance by authorized administrators
- certificate validation by external users.

The backend handles application logic, data processing and communication between the frontend and the blockchain network.It is implemented using server-side technologies such as Node.js or Python (Flask/Django).

The backend manages tasks such as:

- certificate data validation
- hash generation
- QR code creation
- interaction with contracts.

It also maintains an off-chain database, typically using MongoDB to store certificate metadata and user information.

The system has a frontend that's easy to use and works on the web. This is where people like certificate issuers and holders can talk to each other. We use things like HTML and JavaScript to make it simple. The frontend does things like make certificates let people upload them scan QR codes. Show if a certificate is real or not. We want to make sure anyone can use this even if they are not good with computers.

The backend is where all the work happens. It talks to the frontend and the blockchain network. We use things like Node.js to make the backend work. It does things like check certificates to make sure they are correct make QR codes and talk to contracts. The backend also stores information in a database, like who has a certificate and what's on it. We use something, like MongoDB for this. This way we do not have to store everything on the blockchain, which makes things faster. The system has a frontend and a backend. The backend is very important for the certificate system to work. The certificate system relies on the backend to do things like manage certificates and talk to the blockchain network.

This hybrid storage approach improves performance by reducing dependency on blockchain storage for large data.

The blockchain layer forms the core of the system. Is implemented using platforms such as Ethereum, Binance Smart Chain or Celo.

Smart contracts are written in Solidity. Deployed on the blockchain network to manage certificate-related operations.

These contracts define functions for:

- issuing certificates
- storing hash values
- verifying authenticity
- revoking certificates.

Once deployed smart contracts operate autonomously. Ensure that all transactions are executed securely and transparently without human intervention.

During the certificate issuance process an authorized institution logs into the system. Enters the required certificate details.

The backend generates a certificate and applies a cryptographic hashing algorithm, such as SHA-256 to produce a unique hash value.

This hash is then sent to the contract and stored on the blockchain along with a unique certificate ID.

Simultaneously a QR code is. Linked to the certificate's verification record.

The digital certificate is then provided to the user along with the QR code for verification.

The verification process is implemented in two ways:

- file-based verification
- ID/QR-based verification.

In file-based verification the user uploads the certificate and the system recalculates its hash value.

This hash is compared with the hash stored on the blockchain to determine authenticity.

In ID or QR-based verification the system retrieves the certificate record directly from the blockchain using the provided identifier.

If the values match and the certificate is not revoked the system confirms its validity;otherwise it is flagged as invalid or tampered.This approach ensures accuracy and eliminates the possibility of undetected modifications.

Certificate revocation is implemented through contracts allowing authorized issuers to update the status of a certificate when necessary.

Once a certificate is revoked its status is permanently recorded on the blockchain and any subsequent verification attempts will reflect this update.

This ensures that fraudulent or invalid certificates cannot be reused.The system is tested under scenarios to evaluate its performance and effectiveness.

Key evaluation metrics include: security, verification speed,

system reliability, user experience.

The results demonstrate that the proposed system significantly reduces verification time compared to methods enabling near-instant validation of certificates.

The use of blockchain ensures data integrity and resistance to tampering while the decentralised architecture eliminates single points of failure.

Experimental observations also indicate improvements in transparency and trust as all certificate transactions are recorded on a verifiable ledger.

The integration of QR code-based verification enhances accessibility and simplifies the process for end users.

However certain challenges, such as transaction costs and latency, in public blockchain networks are observed, which can be addressed through optimisation techniques or the use of consortium blockchains.

VII. RESULTS AND DISCUSSION

The framework we came up with was tested in different situations. We used fake certificate files to see how it worked. What we found out is that it can verify things fast. In just a few milliseconds. This makes it perfect for verifying things in time.

When we uploaded a certificate to check the special code we used to verify it matched the one on the blockchain. So the verification was successful.. If we made even a small change to the certificate like changing the way the text looked or adding something new the code would be completely different. This meant the verification would fail away.

This shows that our verification system is very good at catching small changes. It is also very reliable. Our system is much better, than the way of doing things, which was to check everything by hand. This old way took a time and people could make mistakes. Our system is faster. Does not need people to do the work. We also added a way to use QR codes to make it easier to use on devices.

The system also shows significant improvement in transparency and traceability. Every transaction, including certificate issuance, verification, and revocation, is recorded on the blockchain, creating a permanent and auditable record.
This feature allows stakeholders such as institutions,

employers, and students to access verification data without relying on intermediaries. As a result, trust is established among all parties, and the chances of fraudulent activities are minimized.

TABLE I
COMPARISON OF VERIFICATION APPROACHES

Method	Speed	TamperProof	Decentralized	QR Support
Manual	Slow	No	No	No
Database	Medium	Partial	No	Optional
Proposed	**Fast**	**Yes**	**Yes**	**Yes**

VIII. CONCLUSION AND FUTURE SCOPE

This study is about a way to verify certificates using a blockchain system. The blockchain system is really good, at keeping certificates stopping people from cheating. It uses a kind of code called SHA-256 hashing and stores everything in a way that cannot be changed. This makes it really hard for someone to alter a certificate without being caught. The system is also very fast. Does not require a lot of work to manage.

We also made it possible to use a QR code to get to the certificates, which makes it easier to use in schools and companies. The results of our study show that using blockchain technology is a way to make sure digital certificates are trustworthy.

In the future we might be able to make the system better by adding something called smart contracts. These would help us give out certificates take them away and keep track of when they expire. We could also work with universities and companies to create a big network that lets everyone verify certificates. Other things we might add include an app special computers that store the blockchain in the cloud and a way to use artificial intelligence to catch people who are trying to cheat.

REFERENCES

[1] A. A. Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational blockchain: A secure degree attestation and verification traceability architecture," Applied Sciences, vol. 11, no. 22, p. 10917, 2021.

[2] A. Gayathiri, J. Jayachitra, and S. Matilda, "Certificate validation using blockchain," in Proc. Int. Conf. Smart Structures and Systems, 2020, pp. 1–4.

[3] A. J. E. Andrade and F. C. Amate, "A decentralized academic certificate issuance system using smart contracts," arXiv preprint arXiv:2601.08513, 2026.

[4] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A systematic literature review on blockchain-based systems for academic certificate verification," IEEE Access, vol. 11, pp. 68521–68539, 2023.

[5] M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi, "Security analysis of a blockchain-based protocol for the certification of academic credentials," arXiv preprint arXiv:1910.04622, 2019.

[6] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.

[7] M. Hasan, A. Rahman, and M. J. Islam, "DistB-CVS: A distributed secure blockchain-based online certificate verification system," in Proc. Int. Conf. Advanced Information and Communication Technology, 2020, pp. 460–465.

[8] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," European Conference on Technology Enhanced Learning, 2016.

[9] N. Malsa, V. Vyas, J. Gautam, A. Ghosh, and R. N. Shaw, "Certbchain: A step-by-step approach towards building a blockchain-based distributed application for certificate verification system," in Proc. IEEE ICCCA, 2021, pp. 800–806.

[10] Q. Tang, "Towards using blockchain technology to prevent diploma fraud," IEEE Access, vol. 9, pp. 168678–168688, 2021.

[11] R. Q. Saramago, L. Jehl, H. Meling, and V. Estrada-Galiñanes, "A treebased construction for verifiable diplomas with issuer transparency," arXiv preprint arXiv:2109.11590, 2021.

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

[13] T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, and others, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain," EURASIP J. Inf. Security, vol. 2021, no. 7, pp. 1–15, 2021.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," IEEE International Congress on Big Data, 2017.