ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808188

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SmartCreds: Verifying Academic Records on the Blockchain

Achutha JC, Pradeesh

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: The growing use of fake academic certificates is causing big problems for employers, schools, and students around the world. Checking these certificates using old methods is slow, expensive, and easy to cheat. This project suggests a new way to verify academic records using blockchain technology. This system makes sure that educational documents are real, clear, and safe. The records are turned into a special code and saved on a blockchain, which can't be changed.

People who check the certificates can quickly confirm they are real by using a unique code or a QR code, without needing outside help. The system works because blockchain is spread out across many computers, which stops people from changing the records, builds more trust, and makes it easier for everyone to check credentials from anywhere in the world.

KEYWORDS: Fake academic certificates, Security, Private storage.

I. INTRODUCTION

In today's digital era, academic credentials play a vital role in determining an individual's qualifications for employment, higher education, and professional opportunities. However, the rise in counterfeit degrees and falsified certificates has created a global challenge for institutions, employers, and verification agencies. Blockchain technology offers a promising solution by providing a decentralized, transparent, and tamper-proof platform for storing and verifying academic records. By converting credentials into unique cryptographic hashes stored on a distributed ledger, the system ensures that records cannot be altered or forged. The original documents remain securely stored off-chain to preserve privacy, while verification can be completed through codes.

This approach eliminates the need for third- party intermediaries, reduces verification time, and builds trust between academic institutions, employers, and students. Furthermore, the global accessibility of blockchain networks makes it possible to verify credentials from anywhere, creating a secure and efficient framework for academic record authentication in the modern world.

II. LITERATURE SURVEY

Blockchain technology is increasingly applied to academic credential verification because it ensures immutability, decentralization, and transparency. Traditional methods are slow, costly, and prone to forgery, whereas blockchain offers a secure, tamper-proof alternative. The W3C Verifiable Credentials (VC) standard defines issuer–holder–verifier roles, cryptographic proofs, and revocation mechanisms, enabling interoperability. Blockcerts is an early and widely adopted open standard, used in projects like MIT's digital diploma system. European initiatives such as EBSI also employ blockchain for cross-border credential recognition.

Two main architectures are identified: public blockchains (e.g., Bitcoin, Ethereum) for transparency and permanence, and permissioned ledgers (e.g., Hyperledger Fabric) for controlled access, privacy, and higher throughput.

Institutional pilots store cryptographic hashes of credentials on-chain while keeping original documents off-chain in secure storage or IPFS. Verification is typically done via QR codes or unique identifiers, enabling fast, independent authentication.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Privacy and regulatory compliance are addressed by storing minimal data on- chain and using revocation registries or status lists to invalidate credentials when necessary.

EXISTING SYSTEM

Existing academic credential verification systems mostly rely on centralized databases and manual processes where employers or institutions must contact the issuing authority directly, leading to delays, higher costs, and dependency on the institution's availability. Some universities provide online verification portals, but these are siloed and vulnerable to single points of failure or tampering. Limited blockchain- based initiatives, such as Blockcerts and W3C Verifiable Credentials, store credential hashes on-chain to enable faster, tamper-proof verification; however, adoption remains low, standardization is lacking, and these systems often operate as isolated pilots without integrated forgery detection, scalability solutions, or global interoperability.

PROPSED SYSTEM

The proposed system is designed to overcome the limitations of traditional and existing verification methods by integrating blockchain technology with secure off- chain storage and automated verification mechanisms. In this system, academic institutions act as trusted issuers, uploading student credentials to a secure off-chain repository such as IPFS (InterPlanetary File System) or encrypted cloud storage. Before storing, the document undergoes a Convolutional Neural Network (CNN)- based forgery detection process to identify any tampering, watermark alterations, or signature inconsistencies.

Once validated, a cryptographic hash (e.g., SHA-256) of the credential is generated and stored on a tamper-proof blockchain ledger via smart contracts.

This on-chain record contains only the hash and minimal metadata, ensuring privacy while guaranteeing immutability. The actual documents remain securely stored off-chain and are linked through a unique identifier or QR code.

For verification, employers or institutions simply scan the QR code or enter the unique ID.

The system retrieves the claimed document, recomputes its hash, and compares it with the blockchain record. If they match and the credential is not listed in the revocation registry, it is deemed authentic. Any mismatch or low-confidence detection from the CNN triggers an alert and sends the document for manual review.

The blockchain can be either permissioned (e.g., Hyperledger Fabric) for restricted access among trusted parties or public (e.g., Ethereum) for global availability.

III. SYSTEM ARCHITECTURE

The system architecture for verifying academic records on the blockchain consists of several integrated components designed to ensure secure, tamper-proof, and easily verifiable credentials. The process begins with a user interface—accessible via web or mobile—that allows universities to issue credentials, students to store and share them, and employers to verify authenticity. Uploaded credentials pass through an ingestion service, which standardizes formats and extracts metadata, followed by a forgery detection module powered by a convolutional neural network (CNN) to detect tampering. Verified files are stored securely in encrypted off-chain storage, such as IPFS or cloud services, while their cryptographic hashes (e.g., SHA-256) and minimal metadata are anchored on the blockchain via smart contracts. The blockchain stores only the hash, issuer signatures, and revocation registry entries to maintain privacy, while the original documents remain off-chain. A verification API enables employers or third parties to submit documents or scan QR codes to recompute the hash, check the blockchain for a match, and confirm the credential's validity and revocation status. The system also maintains an audit log of all transactions and verification events, anchored periodically on-chain for immutability. Identity and access management ensure only authorized issuers can add records, while encryption, role-based access controls, and compliance with W3C Verifiable Credentials standards preserve privacy and interoperability. This architecture can be deployed on a permissioned blockchain for institutional control, a public blockchain for transparency, or a hybrid model for balancing scalability, privacy, and permanence.The system architecture for verifying academic records on the blockchain consists of several integrated components designed to ensure secure, tamper-proof, and easily verifiable credentials. The process begins with a user interface—accessible via web or mobile—that allows universities to issue credentials, students to store and share them, and employers to verify

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

authenticity. Uploaded credentials pass through an ingestion service, which standardizes formats and extracts metadata, followed by a forgery detection module powered by a convolutional neural network (CNN) to detect tampering.

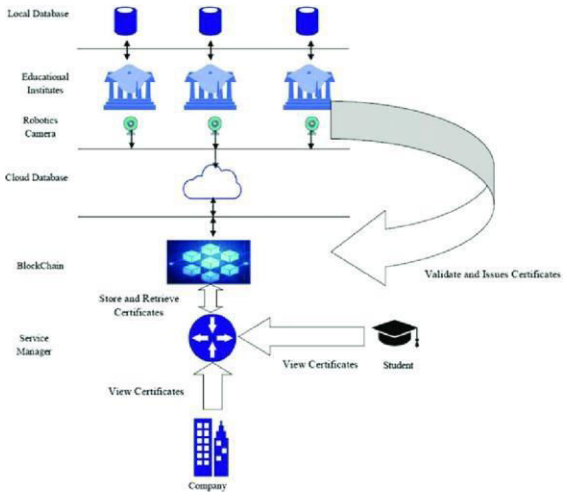

Fig 3.1 System Architecture

IV. METHODOLOGY

Academic administrators commence the credential issuance process by uploading a digital certificate—such as a degree or transcript—via a secure Admin Portal. The system immediately applies a robust cryptographic hash function (e.g., SHA- 256) to the certificate, producing a unique and tamper-evident hash key. This hash key, paired with the student's unique identifier (USN), is formatted into a JSON record and optionally augmented with a CID if the full certificate is uploaded to an off-chain storage solution like IPFS. The JSON record is then submitted to a smart contract on the blockchain—this smart contract securely records and stores the hash key and USN (and optionally the CID), guaranteeing immutability and transparent auditability.

During verification, a user or guest inputs the hash (or USN hash), prompting the system to fetch the stored certificate metadata from the blockchain and retrieve the full document from IPFS. A fresh hash is generated from the retrieved data and compared against the blockchain record This approach achieves secure, efficient, transparent, and cost-effective credential verification without exposing sensitive certificate contents on-chain.

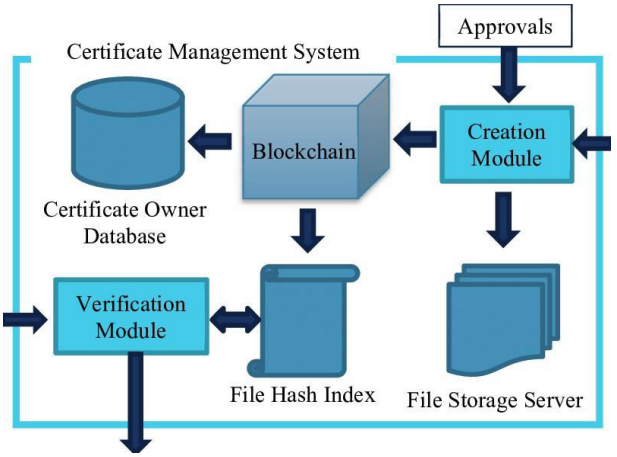

Fig 4.1 Methodology

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808188

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. DESIGN AND IMPLEMENTATION

The system starts when an institution's admin enters certificate information such as the student's name, USN, course, grade, issue date, and issuer. This information is then turned into a JSON object with a specific order, which can be hashed using SHA-256 in a predictable way. This hash uniquely identifies the certificate. The full certificate document is stored off-chain, like on IPFS. The IPFS content identifier (CID) and the hash of the USN are added to a JSON manifest. This manifest includes the certificate data, hash, USN hash, IPFS CID, issuer, and timestamp. It is saved locally and then used to call the issueCertificate function in a smart contract on a blockchain, like Solidity on an Ethereum-based chain. The contract stores just the certificate hash and some related metadata, like the issuer, CID, timestamp, and revocation status. It also makes sure only authorized admins can issue or revoke certificates and sends events for use in off-chain systems. When verifying, users or guests can paste the certificate hash or upload the certificate. This triggers a check of the blockchain record, fetches the certificate from IPFS using the CID, recalculates its hash, and confirms it matches the on-chain hash and hasn't been revoked. Each certificate has a QR code that leads directly to the verification UI,clear, and cost-effective for issuing and checking academic credentials.

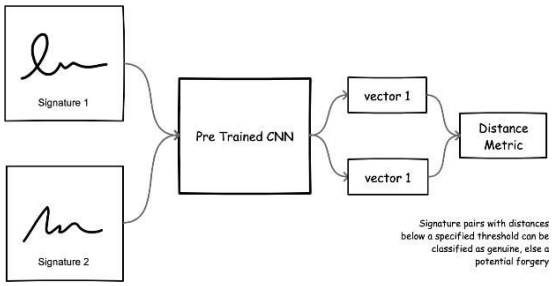

Fig 5.2 Working of Conventional Neural Network

VI. OUTCOME OF RESEARCH

Although peer-reviewed studies with hard metrics are limited, collective insights from pilot initiatives and whitepapers suggest that implementing blockchain-based academic credential verification significantly enhances security through immutable hashing of certificate data, accelerates the verification process by enabling instant validation without institutional intermediaries, and reduces administrative overhead overall. These systems also offer better transparency and auditability, empowering graduates to share verifiable digital credentials easily. Emerging hybrid designs that layer blockchain integrity with off-chain encryption, digital signatures, and selective data disclosure are being explored to strike a balance between transparency, privacy.

VII. RESULT AND DISCUSSION

Blockchain-powered academic credential verification notably enhances security, efficiency, and trust. Systems that store certificate hashes—and sometimes minimal metadata—on an immutable ledger dramatically reduce fraud, ensure data integrity, and streamline verification. Studies highlight reductions in verification times from days or weeks down to mere seconds, along with substantial cost savings due to reduced administrative burden.some adopters report over 50% faster verification, while institutions like the University of Nicosia have issued thousands of tamper-proof credentials since 2018.At the same time, challenges persist: privacy concerns arise from immutable metadata stored on the blockchain— especially under privacy regulations like GDPR and FERPA—and scalability and integration with legacy systems remain barriers to broader adoption.Researchers advocate hybrid architectures—such as dual-blockchain (public/private), decentralized identifiers (DIDs), and zero- knowledge proofs (ZKPs)—to preserve verification transparency while safeguarding sensitive data.Overall, blockchain credentialing systems offer compelling benefits in integrity, transparency, and efficiency; future adoption hinges on resolving privacy issues, regulatory alignment, and seamless integration into existing educational infrastructures.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808188

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

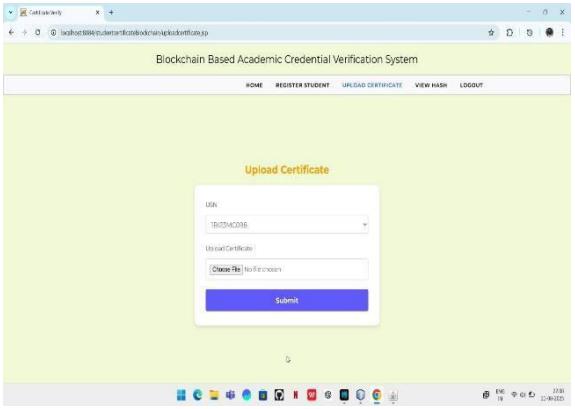

Fig 7.1 Image of upload Page

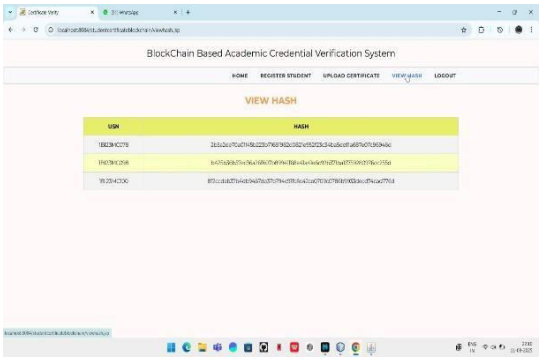

Fig 7.2 Image of Result

VIII. CONCLUSION

Blockchain-based academic credential verification system—where administrators issue certificates, compute a hash from structured certificate data (including the USN), store it in a JSON manifest alongside off-chain storage metadata (e.g., IPFS CID), and enable users or guests to verify authenticity using the hash—demonstrates a powerful and forward-looking approach to securing academic credentials. By leveraging the immutability of blockchain, your system ensures that issued credentials are tamper-proof and transparently verifiable without intermediaries. At the same time, storing full certificate data off- chain keeps transaction costs efficient while preserving privacy. Users benefit from faster, decentralized verification (via hash or USN-based lookup), improved portability, and self-service access—transforming how credentials are shared and validated

REFERENCES

1. Verifi-Chain: A Credentials Verifier using Blockchain and IPFS Demonstrates how certificate data is stored via IPFS and verified through its hash on a blockchain smart contract. It embodies the hybrid approach of off-chain storage and on-chain validation.
2. Trustworthy Verification of Academic Credentials through Blockchain Technology (iJOE, 2024) A structured three-layer system composed of Data, Blockchain, and Application layers, enabling issuance and on-chain verification of academic credentials with smart contracts and frontend interfaces.
3. Decentralized Certificate Verification Application via Blockchain (Grenze International Journal, 2023) This approach captures certificate content as JSON for IPFS storage, maintains a revocation list also in JSON, and validates credentials using on-chain hash comparisons.
4. A Blockchain Framework for Academic Certificates Authentication (TheScientificWorldJournal/THESAI) Illustrates a complete DApp model where certificate data is hashed, stored via IPFS, and validated using Ethereum

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

smart contracts and QR code-enabled access.

5. Privacy-Preserving Student Credential Verification Using Blockchain (IJIET, 2023) Focuses on encrypting credential data on IPFS, storing only hashes on-chain, and providing selective disclosure through smart contracts for enhanced user privacy.
6. Hyperledger-Based Secure Framework for Academic Certificate Verification Showcases a permissioned architecture using Hyperledger Fabric, integrating IPFS for document storage and smart contracts for verification, aimed at institutional deployments.
7. Academic Certificate Verification via Blockchain (IJCA, 2024) Details a system where certificate files are hashed and stored on IPFS, with the hash recorded on-chain to reduce forgery risk and administrative workload.
8. Blockchain Academic Credential Interoperability Protocol (BACIP) (arXiv, 2024)
9. Proposes a standardized approach using dual-blockchain architecture, JSON-LD formatting, and optional zero-knowledge proofs to balance privacy with transparency.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com