Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

A Survey on Distributed Ledger-Based Certificate Authentication System

Ms. Neha Beegam P E
Assistant Professor
Department of Computer Science and Engineering Federal Institute of Science and Technology Angamaly, India

Mr. Alen K Sangeeth
Department of Computer Science and Engineering Federal Institute of Science and Technology Angamaly, India

Mr. Athulraj Appukuttan
Department of Computer Science and Engineering Federal Institute of Science and Technology Angamaly, India

Mr. Alex Jo Tomy
Department of Computer Science and Engineering Federal Institute of Science and Technology Angamaly, India

Mr. Alex Rijo Joseph
Department of Computer Science and Engineering Federal Institute of Science and Technology Angamaly, India

Abstract - With the rapid digital transformation of educational and professional environments, certificate verification has become a critical security concern. Traditional certificate authentication systems rely on centralized repositories and manual verification processes, which are vulnerable to forgery, unauthorized modification, and operational inefficiencies. Blockchain technology offers a decentralized, immutable, and transparent framework that addresses these challenges. This survey presents an extensive review of blockchain-based certificate authentication systems proposed in recent literature. Various architectures, blockchain platforms, smart contract models, cryptographic mechanisms, and optimization techniques are analyzed. A detailed comparison is presented to highlight strengths, limitations, and open research challenges. The study aims to serve as a comprehensive reference for researchers and practitioners working on secure and scalable certificate verification solutions.

Keywords - Blockchain; Certificate Authentication; Artificial Intelligence; Distributed Ledger; Smart Contracts.

I. INTRODUCTION

Certificates act as formal evidence of academic qualifications, professional expertise, and skill development. With the widespread adoption of online education platforms and digital recruitment systems, certificate forgery has increased significantly. Traditional verification methods rely on centralized databases and manual validation, making them vulnerable to tampering, security breaches, and operational delays.

Blockchain technology introduces a decentralized and immutable ledger secured through cryptographic hashing and consensus mechanisms. Smart contracts automate certificate issuance, verification, and revocation, reducing dependency on intermediaries and improving trust.

The motivation behind blockchain-based certificate authentication arises from the increasing reliance on digital credentials in education, employment, and governance. Traditional certificate verification mechanisms are slow, institution-dependent, and vulnerable to forgery. In many cases, employers and universities must manually contact issuing authorities, resulting in delays and increased administrative cost.

The primary objective of blockchain-based certificate authentication systems is to establish a trusted, tamper-proof, and decentralized verification mechanism. Such systems aim to eliminate intermediaries, reduce verification time, and ensure global accessibility. Additional objectives include scalability to support large user bases, interoperability across institutions, and privacy preservation for certificate holders.

By achieving these objectives, blockchain-based systems can significantly improve trust and efficiency in credential verification ecosystems.

II. BACKGROUND AND EVOLUTION OF CERTIFICATE AUTHENTICATION SYSTEMS

Certificate authentication has evolved significantly from manual, paper-based verification methods to digital and automated systems. Early approaches relied on physical certificates issued by institutions, where verification required direct contact with issuing authorities. This process was slow, costly, and highly dependent on institutional trust.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

With the emergence of centralized digital databases, institutions began storing certificate records electronically. Although this reduced manual effort, centralized systems introduced new challenges such as single points of failure, insider attacks, and large-scale data breaches. High-profile incidents involving forged certificates further exposed the limitations of centralized verification models.

The introduction of cryptographic techniques improved data integrity, but trust was still placed in centralized authorities. Blockchain technology represents a paradigm shift by decentralizing trust and enabling tamper-proof record keeping. By distributing certificate records across multiple nodes, blockchain eliminates reliance on a single authority and provides verifiable proof of authenticity.

This evolution highlights why blockchain-based certifi- cate authentication systems are increasingly considered a promising solution for modern credential verification.

III. METHODOLOGY

This survey adopts a systematic methodology to ana- lyze and compare blockchain-based certificate authentica- tion systems proposed in existing literature. The method- ology is designed to ensure comprehensive coverage, objec- tive evaluation, and meaningful comparison of prior research works.

A. Literature Collection and Selection

Relevant research articles were collected from reputed digital libraries including IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier ScienceDirect, and Google Scholar. Keywords such as *blockchain-based certificate authentication*, *digital credential verification*, *decentralized identity*, and *smart contract-based authentication* were used during the search process. Only peer-reviewed journal articles, conference papers, and survey studies published in recent years were considered to ensure quality and relevance.

B. Screening and Classification

The collected studies were screened based on predefined inclusion criteria. Papers focusing on certificate authentication, credential verification, issuer validation, or decentralized identity management were shortlisted. The selected studies were then classified according to their blockchain type (public, consortium, or permissioned), authentication mechanism, storage strategy (on-chain or off-chain), and privacy model.

C. Analytical Framework

Each selected work was analyzed using a common analytical framework. Key aspects examined include system architecture, certificate issuance and verification workflow, cryptographic techniques employed, use of smart contracts, and trust management strategies. Special attention was given to performance-related parameters such as transaction cost, verification latency, scalability, and storage overhead.

D. Comparative Analysis

A comparative study was conducted to identify similari- ties and differences among existing approaches. The comparison focused on methodology, advantages, limitations, and applicability of each system. This analysis helped in identifying recurring challenges such as interoperability, scalability limitations, high transaction costs, and privacy concerns. The comparison results are summarized in tabular and graphical forms to enhance clarity.

E. Gap Identification and Synthesis

Based on the comparative analysis, research gaps and open challenges were identified. The synthesis of findings highlights the lack of large-scale real-world deployments, limited interoperability across heterogeneous blockchain systems, and the need for cost-efficient and privacy-preserving solutions. These observations form the basis for proposing future research directions discussed later in this paper.

IV. RELATED WORKS

R. Priyadarshini *et al.* [1] proposed a faster, integrated, and trusted certificate authentication and issuer validation system based on blockchain technology. The study primarily focuses on addressing critical challenges in traditional certificate verification systems, such as certificate forgery, centralized trust dependency, delayed verification, and lack of issuer authenticity. By leveraging blockchain technology, the proposed system aims to provide a decentralized, tamper-resistant, and transparent mechanism for certificate issuance and verification.

The authors designed a blockchain-based framework us- ing Ethereum smart contracts, where digital certificates are processed by generating cryptographic hashes using secure hashing algorithms. These hashes, along with relevant metadata such as certificate identifiers and issuer information, are permanently stored on the blockchain. To enhance verification efficiency and reduce computational overhead, Bloom Filters are integrated into the system. Bloom Filters enable rapid membership testing, allowing the system to quickly determine whether a certificate exists in the blockchain without performing exhaustive searches.

The framework also introduces an issuer validation mechanism to ensure that only authorized and legitimate institutions are allowed to issue certificates. This dual-layer validation approach strengthens trust by verifying both the certificate and the issuing authority. Experimen- tal analysis demonstrates that the proposed system significantly improves verification speed compared to conventional blockchain-based certificate authentication approaches, while also reducing gas consumption through optimized data structures.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

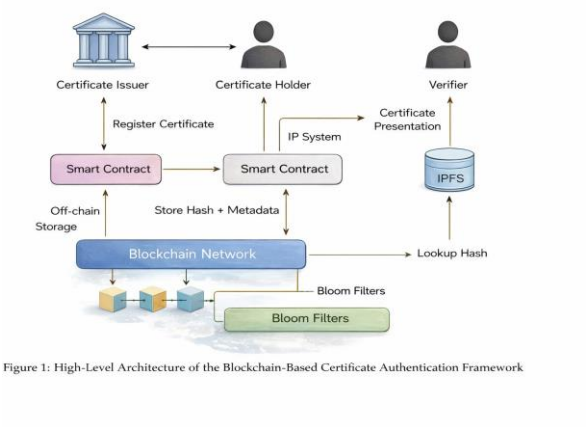

Figure 1: High-Level Architecture of the Blockchain-Based Certificate Authentication Framework

Performance evaluation results reported by the authors indicate high accuracy in certificate verification and improved efficiency in terms of search time and transaction cost. The use of Bloom Filters plays a key role in achieving scalable verification, particularly when handling large volumes of certificates. The system demonstrates strong resistance to certificate forgery and unauthorized modification due to the immutable nature of blockchain storage.

Table 1: Performance Evaluation Results Reported by Priyadarshini et al.

Metric	**Traditional System**	**Proposed System**
Verification Time	High	Low
Accuracy	Moderate High	High Reduced
Gas Consumption	Low	High
Forgery Resistance		

Despite its advantages, the proposed system exhibits certain limitations. Since it is implemented on the public Ethereum blockchain, transaction costs may increase significantly during periods of network congestion, affecting scalability. Additionally, the evaluation is conducted primarily in controlled experimental environments, and challenges related to real-world deployment, regulatory compliance, and long-term operational cost are not extensively explored. These limitations highlight the need for further research on cost-efficient, scalable, and hybrid blockchain architectures for certificate authentication systems.

A. Mondal *et al.* [4] proposed a blockchain-based secure e-certificate management system with the objective of enhancing the integrity, authenticity, and accessibility of digital academic certificates. The study addresses major weaknesses of traditional centralized certificate repositories, such as susceptibility to forgery, single points of failure, and limited transparency in verification processes. By integrating blockchain with decentralized storage mechanisms, the authors aim to provide a tamper-resistant and scalable solution for digital certificate management.

In the proposed system, academic certificates are stored off-chain using the InterPlanetary File System (IPFS), while cryptographic hashes of the certificates along with relevant metadata are recorded on the blockchain. This hybrid storage approach significantly reduces on-chain storage overhead while preserving data integrity. The blockchain acts as a trusted ledger that maintains immutable references to certificate data, enabling secure verification without revealing sensitive information.

During certificate issuance, the issuing authority uploads the certificate to IPFS and obtains a unique content identifier (CID). A hash of this CID is then stored on the blockchain through smart contracts. For verification, the verifier retrieves the certificate from IPFS using the CID and recomputes its hash, which is compared against the blockchain record. A matching hash confirms authenticity and ensures that the certificate has not been altered.

Furthermore, the system supports decentralized verification by allowing third-party verifiers to validate certificates without requiring direct communication with the issuing institution. This capability significantly reduces verification latency and administrative overhead, particularly in large-scale academic and professional ecosystems. The framework also benefits from the fault tolerance of IPFS, improving certificate availability even under network disruptions.

However, the authors note that system performance and responsiveness may vary depending on network conditions and blockchain transaction throughput. Additionally, issuer trust management and efficient certificate search mechanisms are not explicitly addressed, indicating potential areas for improvement. Nevertheless, the proposed framework demonstrates the effectiveness of combining blockchain and decentralized storage technologies in enhancing the security, efficiency, and reliability of digital certificate management systems.

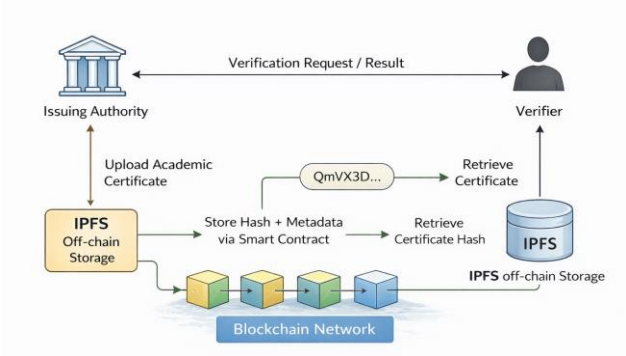

Figure 2: Hybrid IPFS–Blockchain Architecture for Secure E-Certificate Management

Experimental results presented by the authors indicate that the use of IPFS significantly improves storage efficiency and system scalability. The decentralised architecture en- sures

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

high availability of certificates and resilience against data tampering. The system also reduces dependency on is- suing institutions during verification, thereby enabling faster and more reliable certificate validation.

Table 2: Performance Characteristics of Mondal *et al.*'s System

Performance Metric	Observation
Storage Overhead	Low (Off-chain via IPFS)
Verification Integrity	High Strong Improved
Tamper Resistance System	Moderate
Scalability Verification	
Latency	

Despite its advantages, the proposed system exhibits certain limitations. The framework does not include a robust mechanism for issuer authentication or trust management, making it vulnerable to unauthorized certificate issuance if issuer identities are compromised. Additionally, certificate lookup and verification performance may degrade with an increasing number of records, as no optimized search or indexing techniques are employed. These limitations highlight the need for integrated issuer validation and efficient lookup mechanisms in future blockchain-based certificate management systems.

S. Sharma *et al.* [2] presented an unforgeable digi- physical academic certificate framework aimed at address- ing both digital and physical certificate forgery. The pri- mary motivation of this work is to overcome limitations of conventional digital certificate systems, where physical certificates can still be duplicated or manipulated without any effective linkage to their digital counterparts. By integrating blockchain technology with physical authentication mechanisms, the authors propose a hybrid certification model that ensures end-to-end authenticity and integrity.

In the proposed system, each academic certificate is is- sued in both digital and physical forms, tightly coupled through a unique physical identifier such as a QR code or embedded secure tag. During certificate issuance, the is- suing authority generates a digital certificate and computes its cryptographic hash. This hash is permanently stored on the blockchain, while the physical certificate embeds a refer- ence to this blockchain record. As a result, any unauthorized modification of either the digital or physical certificate can be instantly detected during verification.

The verification process involves scanning the physical identifier present on the certificate to retrieve the corresponding blockchain record. The verifier compares the hash embedded in the physical certificate with the hash stored on the blockchain. If both values match, the certificate is validated as authentic; otherwise, it is flagged as forged or tampered. This approach enables instant, decentralized verification without the need for direct interaction with the issuing institution, thereby improving verification efficiency and trustworthiness.

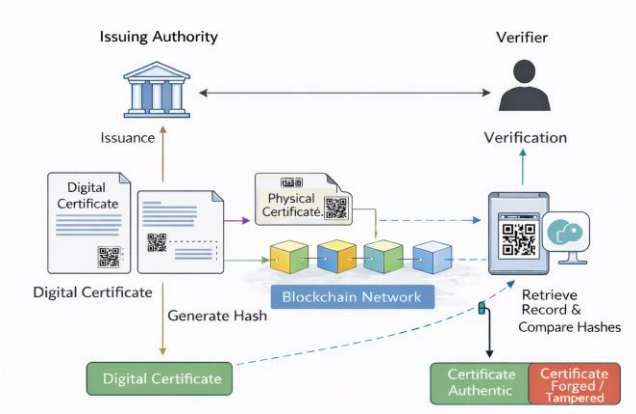

Figure 3: Digi-Physical Certificate Issuance and Verification Framework

Experimental evaluation reported by the authors demonstrates that the digi-physical framework significantly enhances resistance to certificate forgery when compared to traditional paper-based and purely digital systems. The immutability of blockchain records ensures strong data integrity, while the physical–digital binding improves real-world applicability in academic and professional certification environments.

Table 3: Security Characteristics of Digi-Physical Certificate Authentication System

Security Metric	Observation
Physical Forgery Resistance	Very High
Digital Tamper Resistance	High (Blockchain-based)
Verification Speed Issuer	Fast Minimal
Dependency Deployment	High
Complexity	

However, the proposed framework introduces additional deployment complexity arising from the management of physical identifiers and secure certificate printing processes. Moreover, large-scale deployment may involve increased operational costs and logistical overhead. These observations indicate the need for future research focusing on lightweight digi-physical authentication mechanisms and cost-efficient deployment strategies to enable scalable certificate verification systems.

R. Rahardja *et al.* [3] proposed a blockchain-based digital certificate authentication framework aimed at improving the security, scalability, and accessibility of certificate verification across multiple institutions. The primary motivation of this work is to address the limitations of centralized certificate management systems, including single points of failure, lack of interoperability, and delayed cross-institutional verification.
The authors designed a consortium blockchain architec- ture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

in which multiple trusted educational institutions collectively maintain the distributed ledger. In the proposed framework, digital certificates are issued by authorized institutions, and cryptographic hashes of certificates are stored on the blockchain to ensure immutability and tamper resistance. Smart contracts are employed to automate certificate issuance, validation, and revocation, enabling efficient and transparent verification without direct interaction with the issuing authority.

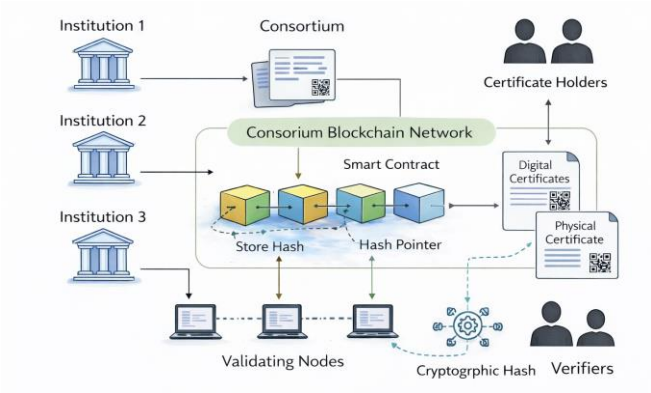

Figure 4: Consortium Blockchain-Based Certificate Authentication Framework

The system supports decentralized verification, allowing external entities such as employers or academic institutions to validate certificates by querying the blockchain. By restricting validator participation to trusted organizations, the framework achieves higher throughput and lower latency compared to public blockchain solutions. The consortium model also facilitates governance control and compliance with institutional policies.

Experimental evaluation reported by the authors demonstrates improved verification efficiency and reduced response time when compared to traditional centralized verification systems. The framework effectively prevents certificate forgery and unauthorized modification due to the immutable nature of blockchain storage and cryptographic verification mechanisms.

Table 4: Summary of Features and Performance in Rahardja et al.

Aspect	Description
Blockchain Type	Consortium Blockchain
Certificate Storage	On-chain certificate hash
Verification Method	Smart contract-based validation
Performance Forgery	Low latency, high throughput
Resistance	High

Notwithstanding these benefits, certain limitations remain in the proposed framework, the proposed framework ex- hibits certain limitations. The consortium blockchain model introduces governance and trust management challenges, as participating institutions must agree on validator selec- tion, consensus rules, and operational policies. Addition- ally, limiting validator participation reduces openness and public verifiability compared to fully decentralized public blockchains. The framework also lacks a detailed discussion on cross-consortium interoperability and large-scale deployment feasibility, highlighting areas for further research.

G. Ghani *et al.* [5] presented a permissioned blockchain-based network for managing and verifying student credentials, with the primary objective of addressing security, privacy, and performance limitations of public blockchain-based academic certification systems. The authors emphasize the need for controlled participation and institutional governance in academic environments, where unrestricted public access may raise regulatory and privacy concerns.

The proposed system is implemented using Hyperledger Fabric, a permissioned blockchain platform that enables fine-grained access control and identity management. Academic institutions act as authorized peers in the network, and only trusted entities are allowed to issue, update, or verify student credentials. Digital certificates are generated and their cryptographic hashes are stored on the blockchain, ensuring data integrity and resistance to tampering. Smart contracts, implemented as chaincode, automate credential issuance and verification processes.

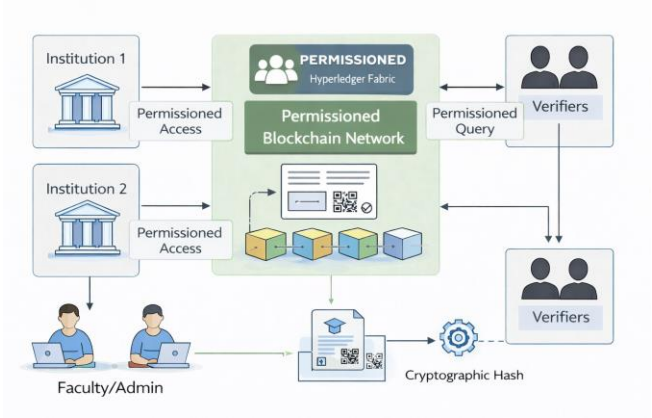

Figure 5: Permissioned Blockchain Network for Student Credential Management

The framework ensures efficient credential verification by allowing verifiers to query the blockchain ledger di- rectly without contacting the issuing institution. Perfor- mance evaluation results reported by the authors demon- strate low transaction latency and high throughput compared to public blockchain solutions, making the approach suitable for large-scale institutional deployments. The system also provides enhanced privacy protection by restricting data ac- cess to authorized participants, in compliance with academic and regulatory requirements. Furthermore, the use of smart contracts automates validation workflows and minimizes human intervention during the verification process. This architectural design improves operational efficiency while maintaining a high level of trust and data integrity. In addition, the decentralized record-keeping mechanism reduces depen-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

dency on centralized databases, thereby lowering the risk of data breaches and system failures. The modular structure of the framework also allows easy integration with existing institutional IT infrastructures, supporting practical adoption.

Table 5: Feature Analysis of the Permissioned Blockchain Framework

Aspect	Description
Blockchain Type	Permissioned (Hyperledger Fabric)
Access Control	Identity-based, role-managed
Certificate Storage	On-chain hash values
Performance	Low latency, high throughput
Privacy Protection	High

Although the proposed framework achieves improved performance and privacy preservation, it introduces certain limitations. The permissioned nature of the blockchain reduces transparency and global public verifiability, which are key advantages of decentralized public blockchain systems. Since validator participation is restricted to selected institutions, the network relies on trust within the consortium, partially reintroducing centralized governance characteristics.

Additionally, institutional governance increases administrative overhead, including validator management, pol- icy enforcement, and coordination among participating entities. Interoperability across independent blockchain networks also remains a challenge, especially when different platforms and data standards are used. Without standardized credential formats and cross-chain mechanisms, seamless verification across systems becomes difficult.

These limitations highlight the need for hybrid architectures that balance privacy, performance, transparency, and decentralization to ensure practical and scalable deployment of blockchain-based certificate authentication systems.

A. Garba *et al.* [7] proposed a privacy-preserving certificate authentication framework that addresses confidentiality concerns in blockchain-based credential verification systems. The primary motivation of this work is to prevent unnecessary exposure of sensitive certificate information during the verification process while maintaining authenticity and integrity. The authors argue that although blockchain ensures immutability, naive storage or verification of certificates may lead to privacy leakage due to the transparency of distributed ledgers.

The proposed framework combines blockchain technol- ogy with cryptographic hashing and Bloom Filters to enable efficient and privacy-aware certificate verification. Instead of storing complete certificate details on-chain, the system stores only cryptographic representations, thereby minimizing the risk of sensitive data disclosure. Bloom Filters are employed to perform fast membership verification, allowing verifiers to confirm the authenticity of certificates without accessing the original certificate content or revealing user-specific details.

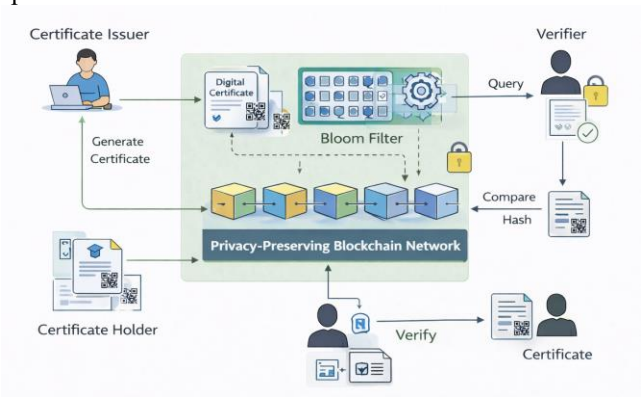

Figure 6: Privacy-Preserving Blockchain-Based Certificate Authentication Framework

The verification process enables a verifier to check certificate validity by comparing hashed values against the blockchain-stored records, ensuring both integrity and anonymity of credential data. This approach eliminates the need for direct interaction with the issuing authority, thereby reducing verification latency and administrative overhead. Experimental evaluation results reported in the study indicate that the proposed approach significantly reduces verification time and storage overhead while preserving user privacy. In addition, the use of cryptographic hashing and Bloom Filters enables fast membership checks without exposing sensitive certificate information. The decentralized nature of the framework further improves system reliability by avoiding single points of failure and supporting distributed verification. The system demonstrates robustness against common security threats such as certificate forgery, replay attacks, and unauthorized data access, making it suitable for secure and privacy-aware digital credential verification.

Table 6: Feature Summary of the Privacy-Preserving Authentication Framework

Aspect	Description
Privacy Technique	Hashing + Bloom Filters
Data Exposure	Minimal (no plaintext storage)
Verification Speed	High High
Forgery Resistance	Privacy-aware
Blockchain Transparency	

However, the proposed framework presents certain limitations. The reliance on Bloom Filters introduces a small probability of false positives, which may impact verification accuracy in edge cases. Additionally, the system depends on auxiliary components such as browser extensions or mid-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

dleware for verification, potentially limiting usability and real-world adoption. The approach also does not fully address key management challenges and cross-platform interoperability, indicating areas for further research in privacy-preserving credential authentication systems.

T. Nguyen *et al.* [6] presented a comprehensive survey on decentralized authentication mechanisms for Web 3.0 environments, focusing on the limitations of traditional centralized identity and authentication models. The study highlights how centralized authentication systems suffer from single points of failure, privacy leakage, censorship risks, and data monopolization, which are incompatible with the decentralized vision of Web 3.0.

The authors systematically analyze decentralized authentication paradigms built on blockchain technology, decentralized identifiers (DIDs), and verifiable credentials. These systems enable users to maintain full ownership and control over their digital identities, eliminating reliance on centralized identity providers. The survey examines the role of smart contracts, cryptographic signatures, public–private key infrastructure, and distributed ledgers in enabling trust- less authentication and authorization processes across decentralized applications.

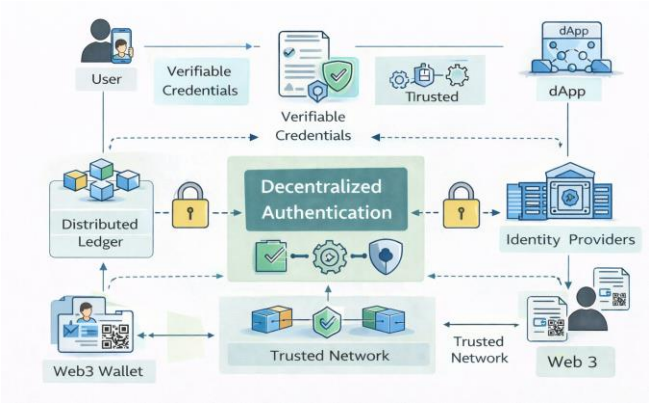

Figure 7: Decentralized Authentication Framework for Web 3.0 Ecosystems

The paper provides a detailed taxonomy of decentralized authentication approaches, categorizing them based on identity management models, trust assumptions, privacy guarantees, and scalability characteristics. It also discusses integration challenges related to usability, interoperability across blockchains, regulatory compliance, and performance overhead. Security and privacy implications such as key management, correlation attacks, and metadata leakage are critically examined.

Table 7: Summary of Decentralized Authentication Mechanisms in Web 3.0

Aspect	Description
Authentication Model	Decentralized, user-controlled
Key Technologies	Blockchain, DIDs, Verifiable Credentials
Privacy Control	User-centric, selective disclosure
Trust Model	Trustless / distributed
Application Scope	Web 3.0 and dApps

Although the survey provides an extensive conceptual and architectural overview, it primarily focuses on high- level design principles and comparative analysis rather than implementation-specific evaluation. The lack of empiri- cal performance benchmarking and real-world deployment analysis limits direct applicability to practical certificate authentication systems. Furthermore, issues related to scalability, user experience, and seamless integration with legacy systems remain open challenges, indicating potential research directions for applying decentralized authentication models to blockchain-based certificate verification frameworks.

T. Merlec *et al.* [8] proposed a blockchain-based degree verification framework designed to enhance the authenticity and integrity of academic qualifications while reducing reliance on centralized verification authorities. The study addresses the growing incidence of degree forgery and the inefficiencies associated with manual, institution-centric verification processes in international academic and employment contexts.

The proposed framework adopts a consortium-oriented blockchain architecture in which higher education institutions act as trusted participants responsible for issuing and maintaining degree credentials. Instead of storing full degree documents on-chain, the system records cryptographic hashes of academic credentials on the blockchain, ensuring immutability and tamper resistance. Smart contracts are utilized to automate degree issuance and verification, enabling third-party verifiers to validate credentials without direct interaction with the issuing institution.

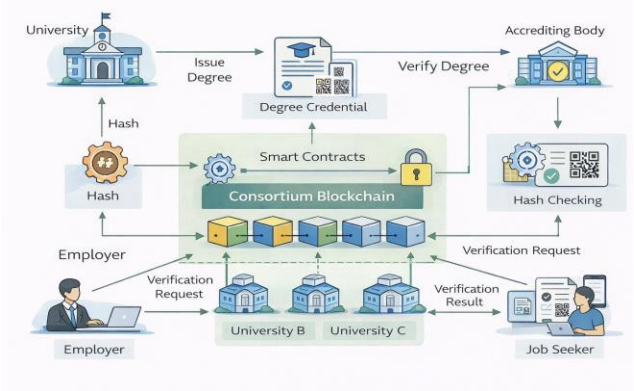

Figure 8: Blockchain-Based Degree Verification Framework

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

The verification process enables employers, universities, and accreditation bodies to authenticate academic and professional credentials by comparing the cryptographic hash of a presented certificate with the corresponding hash securely recorded on the blockchain. Since blockchain records are immutable and distributed across multiple nodes, any alteration to the original credential immediately results in a hash mismatch, thereby preventing tampering and unauthorized modification. This decentralized validation mechanism eliminates the reliance on a single centralized authority and ensures transparent, real-time verification across institutional boundaries.

Furthermore, the framework enhances trust by leveraging distributed consensus mechanisms and smart contract enforcement, which regulate issuer permissions and automate validation workflows. By storing only cryptographic representations of certificates on-chain while maintaining detailed records off-chain, the system optimizes storage efficiency without compromising security. Experimental evaluations reported in the study indicate a significant reduction in verification latency and operational overhead compared to conventional centralized verification systems. In addi- tion, the decentralized architecture demonstrates improved resilience against data breaches, single-point failures, and fraudulent credential issuance, thereby establishing a more robust and scalable certificate authentication ecosystem.

Table 8: Feature Summary of Blockchain-Based Degree Verification System

Aspect	Description
Blockchain Type	Consortium blockchain
Credential Storage	On-chain hashes Smart
Verification Approach	contract-based
Forgery Resistance	High
Interoperability	Institutional collaboration

However, the proposed framework introduces certain limitations. The consortium-based trust model restricts openness and public verifiability, which are key advantages of public blockchains. Additionally, interoperability across independent consortium networks is not fully addressed, potentially limiting global scalability. The study also provides limited analysis of long-term operational costs and real-world deployment challenges, indicating the need for further investigation into large-scale adoption of blockchain-based degree verification systems. Furthermore, governance complexity and lack of standardized cross-chain protocols may hinder seamless integration across institutions.

V. COMPARISON STUDY

Several studies have proposed blockchain-based approaches for certificate authentication and credential verification to enhance security, transparency, and trust in digital credential management. These approaches differ in terms of methodology, blockchain architecture, privacy mechanisms, and verification models. Some systems emphasize fast verification and issuer validation, while others focus on privacy-preserving authentication and decentralized identity management.

Despite their advantages, existing solutions face challenges such as interoperability issues, scalability limitations, deployment complexity, and integration with institutional systems. To highlight these differences and identify research gaps, a comparative analysis of representative blockchain-based certificate authentication systems is presented in Table IX.

Table 9: Comparison Study of Blockchain-Based Certificate Authentication Systems

Paper	Methodology	Advantages	Disadvantages
Paper 1	Blockchain- based certificate authentication with issuer validation	Fastverification and improved trust manage- ment	Deployment complexity and interoper- ability issues
Paper 2	Digi-physical certificate verification using QR/NFC	Prevents forgery and enables instant verification	High hard- ware cost and integration overhead
Paper 3	Decentralized identity and self-sovereign authentication	Privacy-preserving and user-controlled verification	Interoperability challenges across iden- tity systems
Paper 4	Survey of blockchain- based verification approaches	Identifies trends and research gaps	Lacks experimental evaluation
Paper 5	Blockchain- based trans- parent univer- sity ranking	Prevents ranking ma- nipulation	Complex data integration process
Paper 6	Smart contract-based aca- demic accred- itation	Secure and auditable credential validation	Limited scalability for large datasets
Paper 7	Automated certificate transactions using smart contracts	Efficient and transparent execution	High gas cost and limited flexibility
Paper 8	Smart contract vulnerability detection framework	Improves contract secu- rity	Focused only on integer overflow
Paper 9	Lightweight blockchain- based cer- tificate verification	Low latency and high efficiency	Limited large-scale evalua- tion
Paper 10	Blockchain- based access control for certificates	Fine-grained access control and traceabil- ity	High computational over- head

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

VI. SYSTEM ARCHITECTURE

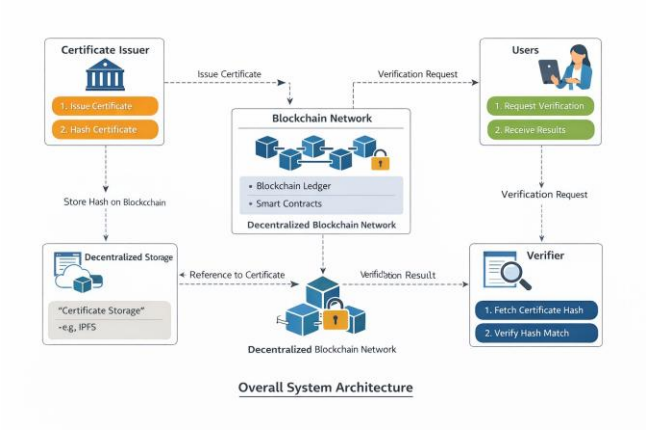

Figure 9: Overall System Architecture

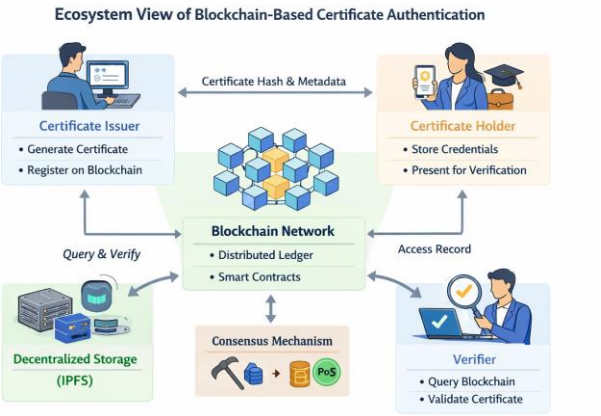

Figure 10: Ecosystem View of Blockchain-Based Certificate Authentication

VII. SYSTEM MODEL AND WORKFLOW

A typical blockchain-based certificate authentication system consists of multiple stakeholders including certificate issuers, certificate holders, verifiers, and the blockchain network. The issuer is responsible for generating certificates and registering them on the blockchain. Certificate hold- ers store their credentials and present them for verification when required. Verifiers validate certificates by querying the blockchain without contacting the issuer directly.

The workflow begins with certificate issuance, where the issuer computes a cryptographic hash of the certificate and stores it on the blockchain via a smart contract. During verification, the verifier recomputes the hash of the presented certificate and compares it with the on-chain record. A match confirms authenticity, while a mismatch indicates tampering or forgery.

This decentralized workflow ensures transparency, immutability, and real-time verification across institutional boundaries

VIII. IMPLEMENTATION

The implementation of blockchain-based certificate authentication systems involves the integration of distributed ledger technology, cryptographic mechanisms, and smart contracts to ensure secure and efficient certificate issuance and verification. A typical implementation begins with defining system roles such as certificate issuers, certificate holders, verifiers, and blockchain network participants. Issuing institutions generate digital certificates and compute cryptographic hashes, which are recorded on the blockchain to ensure immutability and tamper resistance.

Smart contracts are deployed to automate key operations including certificate registration, verification, and revocation. These contracts enforce access control rules, ensur- ing that only authorized issuers can register certificates on the blockchain. To reduce on-chain storage overhead, most implementations store only hash values and metadata on the blockchain, while the actual certificate files are main- tained using off-chain storage solutions such as the Inter- Planetary File System (IPFS). During verification, the veri- fier recomputes the certificate hash and compares it with the blockchain-stored record to validate authenticity.

The choice of blockchain platform significantly influ- ences implementation complexity and performance. Public blockchains such as Ethereum offer transparency and decentralization but incur higher transaction fees and latency. In contrast, permissioned and consortium blockchains provide better control, lower latency, and improved scalability, making them suitable for institutional environments. Integration with existing institutional databases and applications is typically achieved through application programming interfaces (APIs) and middleware services.

A. Implementation Challenges

Implementing blockchain-based certificate authentication systems involves several practical challenges. High transaction fees on public blockchains may limit scalability, particularly when handling large volumes of certificate issuance and verification requests. Network latency can also impact real-time verification performance during peak usage periods.

Interoperability with legacy institutional systems remains a major challenge, as existing infrastructures are often not designed to support decentralized technologies. Institutions may require significant system upgrades and process reengineering to adopt blockchain-based solutions. Additionally, user adoption poses challenges related to usability, key management, and awareness of decentralized systems.

Regulatory compliance and data protection laws must also be carefully considered, especially when handling sensitive personal information. The immutable nature of blockchain records raises concerns regarding data privacy and the right to erasure under certain legal frameworks.

Addressing these challenges requires the adoption of hybrid system architectures, where blockchain components are integrated with traditional systems. The use of off- chain storage, layer-2 scaling solutions, and consortium or

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

permissioned blockchains can help reduce cost and improve performance. Furthermore, effective policy-level coordination among educational institutions, regulatory bodies, and technology providers is essential to enable secure, compliant, and scalable deployment.

IX. PERFORMANCE EVALUATION METRICS

Performance evaluation is essential to assess the feasibil- ity of blockchain-based certificate authentication systems. Key metrics include transaction cost, verification latency, throughput, and storage overhead.

Transaction cost directly affects scalability, particularly in public blockchains. Verification latency impacts user expe- rience. Throughput determines system capacity during peak periods. Storage overhead depends on on-chain and off- chain storage strategies.

Most existing studies evaluate performance in test en- vironments, indicating the need for real-world deployment analysis. Such evaluations often overlook practical factors like network congestion and varying workload conditions that impact system performance.

Evaluation results reported in existing literature demon- strate that blockchain-based certificate authentication sys- tems significantly outperform traditional approaches in terms of verification time and resistance to forgery. Pub- lic blockchain implementations generally achieve verifica- tion within seconds, whereas traditional systems may re- quire hours or days.

However, performance varies depending on blockchain type, consensus mechanism, and storage strategy. Ethereum- based systems often incur higher transaction costs, while permissioned blockchains provide lower latency at the cost of reduced decentralization. Off-chain storage mechanisms such as IPFS reduce on-chain load and improve scalability.

Most evaluations are conducted in test environments, highlighting the need for large-scale real-world performance benchmarking. Future studies should focus on long-term op- erational cost, network congestion effects, and user experi- ence metrics.

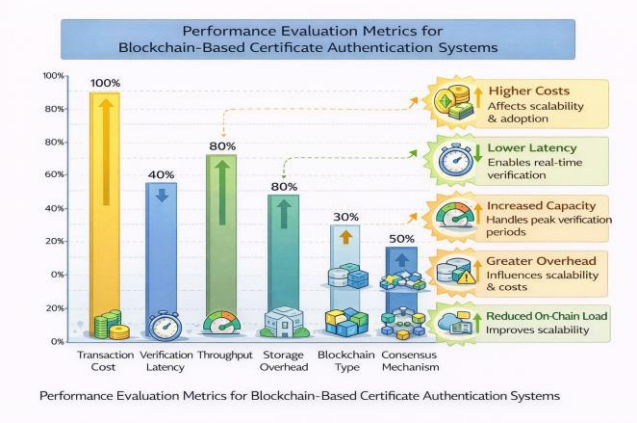

Figure 11: System Performance Indicators for Blockchain- Enabled Certificate Verification

X. CONCLUSION

This survey examined blockchain-based certificate au- thentication systems and highlighted their potential to en- hance security, transparency, and trust in digital credential verification. By leveraging decentralization, cryptographic integrity, and smart contracts, blockchain technology ef- fectively addresses key limitations of traditional centralized certificate management approaches, such as forgery, data tampering, and inefficient verification processes.

The study reviewed various blockchain architectures and design strategies, revealing important trade-offs related to scalability, cost, privacy, and interoperability. While blockchain-based solutions enable faster and more reliable certificate verification across institutional boundaries, chal- lenges such as transaction cost, system scalability, gover- nance complexity, and real-world deployment constraints re- main. In addition, privacy preservation and interoperabil- ity across heterogeneous blockchain networks continue to be open research issues.

Future research should focus on developing cost-efficient, interoperable, and scalable frameworks by leveraging hybrid architectures, layer-2 solutions, and privacy-enhancing tech- nologies. Addressing these challenges will be critical for en- abling large-scale, secure, and widely adopted blockchain- based certificate authentication systems in academic, profes- sional, and governmental domains.

X. FUTURE RESEARCH DIRECTIONS

Future research in blockchain-based certificate authenti- cation should focus on developing hybrid blockchain archi- tectures that balance decentralization, performance, and cost efficiency. Layer-2 scaling solutions such as sidechains and state channels can significantly reduce transaction fees and improve throughput.

Privacy-preserving techniques including zero-knowledge proofs, secure multi-party computation, and decentralized identity frameworks can enhance confidentiality while main- taining verifiability. Cross-chain interoperability is another promising direction, enabling certificate verification across multiple blockchain networks.

Integration with national digital identity systems and gov- ernment registries can further strengthen trust and adoption. Finally, large-scale pilot deployments and longitudinal stud- ies are necessary to evaluate real-world performance, usabil- ity, and sustainability.

REFERENCES

[1] R. Priyadarshini *et al.*, "A Faster, Integrated, and Trusted Certificate Authentication and Issuer Valida- tion System Based on Blockchain," *IEEE Access*, vol. 13, pp. 27037–27055, 2025.

[2] S. Sharma *et al.*, "Unforgeable Digi-Physical Aca- demic Certificates," *IEEE Access*, vol. 13, 2025.

[3] R. Rahardja *et al.*, "Blockchain-Based Digital Certifi- cate Authentication Framework," *Journal of Web En- gineering*, 2024.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

[4] A. Mondal *et al.*, "Blockchain-Based Secure E- Certificate Management System," *IEEE Access*, vol. 11, pp. 45621–45634, 2023.
[5] G. Ghani *et al.*, "Permissioned Blockchain Network for Student Credentials," *IEEE Access*, 2023.
[6] T. Nguyen *et al.*, "Decentralized Authentication for Web 3.0," *ACM Computing Surveys*, 2023.
[7] A. Garba *et al.*, "Privacy-Preserving Certificate Au- thentication," *IEEE TIFS*, 2022.
[8] T. Merlec *et al.*, "Blockchain-Based Degree Verifica- tion," *Future Internet*, 2022.
[9] S. Lamkoti and R. Kulkarni, "Blockchain for Aca- demic Certificates," *Education and Information Tech- nologies*, 2022.
[10] K. Adja *et al.*, "Decentralized PKI Using Blockchain," *IEEE Security & Privacy*, 2020.
[11] A. Killedar and R. Joshi, "Smart Contract-Based Aca- demic Certificates," *Blockchain: Research and Appli- cations*, 2021.
[12] Y. Zhang *et al.*, "Secure Certificate-Based Access Con- trol," *IEEE TNSE*, 2021.
[13] H. Wang *et al.*, "LightLedger Certificate Authentica- tion," *IEEE TNSE*, 2021.
[14] M. Turkanovic´ *et al.*, "EduCTX Platform," *IEEE Ac- cess*, 2018.
[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008.