INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

ECHAIN-ID: A DECENTRALIZED IDENTITY FRAMEWORK FOR VERIFIABLE ACADEMIC CREDENTIALS USING BLOCKCHAIN

[1]V Ramya, [2]K Vishnu Vardhan, [3]B Ram Manikanta, [4]CH Ajay Shreeram, [5]J Jaya Suraj

[1]Assistant Professor, [2]Student, [3] Student, [4] Student, [5] Student
[1]CSE(IOT, CYBER SECURITY INCLUDING BLOCK CHAIN TECHNOLOGY),
[1]VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, NAMBURU, INDIA

Abstract : EChain-ID : A decentralized framework that deploys blockchain technology to issue and verify academic records securely and instantly. Built on Ethereum using Solidity-based smart contracts and tested on Ganache, the system connects verified institutions through a common network. EChain-ID integrates W3C Decentralized Identifiers (DIDs) with encrypted Verifiable Credentials (VCs) for privacy-preserving, tamper-proof credential management. Off-chain storage via IPFS handles bulk credential data, while ECDSA and Ed25519 digital signatures make forgery virtually impossible. Learners hold their own digital identities, and degree verification takes seconds rather than days. Selective disclosure allows users to share only what is required. QR code-based access eliminates complex logins, and all interactions are logged for audit and compliance. This framework balances individual data control with organizational verification needs.

Keywords: Blockchain-enabled Credential Systems, Decentralized Identity (DID), Secure Qualification Verification, Smart Contract Validation, Academic Credential Verification

---

I. INTRODUCTION

1.1 THE NEED FOR SECURITY IN ACADEMIC CREDENTIALS

Evidence of learning and employment potential is typically expressed through educational qualifications. Institutions heavily depend on records and diplomas to assess competence. However, these documents are slow to verify, present fraud risks, and rely on centralized offices. Paper certificates can be easily duplicated, making forgery a major problem. Existing digital methods suffer from inconsistent storage, weak privacy protection, and poor coordination across universities and schools. Verification delays slow down hiring processes, increase administrative workload, and erode confidence in credential authenticity. A new type of digital infrastructure is gaining interest not merely for its ability to bring change, but for redefining how trust is established across networks. Records stored on a blockchain cannot be tampered with and eliminate central dependency. When academic credentials are incorporated into such a system, forgery becomes virtually infeasible and authentication occurs without back-and-forth intermediary relationships.Despite this promise, most existing systems remain incomplete. They neglect inclusive requirements such as mobile identity support or off-chain data handling. Access rules are often rigid, and privacy is treated as secondary. These are half-solutions, not full paths for institutions.

Enter **EChain-ID** developed to bridge credentialing and real-world functionality by connecting credential issuance with user-managed identity layers. Smart contracts supported by blockchain are matched with W3C standards for DIDs and Verifiable Credentials, shifting power to learners. Students own their credentials while institutions issue secure, immutable records. A hybrid model uses IPFS for bulk storage, keeping costs and performance balanced. Encryption and cross-border recognition further strengthen the system.

1.2 Weakness of Present Systems

Existing academic credential verification systems face structural, technical, and trust-based challenges. Traditional checks depend on centralized databases operated by institutions, resulting in slow back-and-forth communication. Paper-based processes increase the risk of distorted records or unauthorized access by insiders. Cross-border credential transfer lacks uniformity across platforms.Emerging blockchain-based technologies reduce record modification, but only address part of the problem. Storing only credential fingerprints on-chain without pairing them with self-sovereign identity tools leaves learners without full control. Systems storing all data on ledgers drive up costs and reduce scalability. Current platforms often disclose full documents during verification, lacking selective sharing functionality. Lifecycle controls such as automatic deactivation, monitoring logs, and role-based checks are largely absent. Most solutions are weak under real-world load and lack thorough analysis.

EChain-ID is designed to fill this gap built to meet standards, scale without difficulty, safeguard personal data, and operate without unnecessary human interaction Security, capacity, and reliability come together here through a blend of AES-256 and ECC ciphers, Huffman coding, plus Reed–Solomon checks all running in one combined flow. Layer upon layer, it builds strong shields using encryption, frees up space with smart shrinking of data, while standing firm when hit by JPEG tweaks or detection tools - something earlier methods often miss.

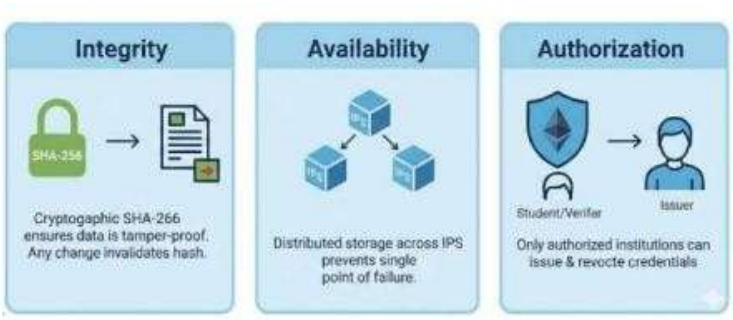

fig.1. EChain-ID Security Threat Model

Apart from lab settings, this study tests on everyday web photos. Because it uses such a broad range of visuals, the findings show how much squeeze a JPEG can take before breaking down. With each photo type handled separately, patterns emerge about what holds up and what does not. When pictures travel through messy networks, these results hint at what might survive. Real usage shapes every conclusion here.Still, the system pushes invisibility further by adjusting scale on the fly plus picking coefficients based on size - this keeps changes invisible even when carrying more hidden information securely. Hidden content stays unseen not just to people but also to detection software, which matters most when secrecy is non-negotiable.

This project ends with an architecture built for actual use - one that includes clear steps for setup, checks on computing demands, and detailed procedures tailored for adoption within live messaging systems or spaces where data protection matters most. A working version has been tested thoroughly; what once lived only in academic discussion now operates as a living tool, ready to enable hidden but safe exchanges across today's connected world.

1.3 Research Contributions

This paper presents EChain-ID: a decentralized model that transforms the validation of academic credentials from mere blockchain records into a complete credential trust ecosystem. The proposed design addresses weak security, insufficient scalability, and information disclosure tendencies found in existing approaches while aligning with established open protocols.The foundation begins with W3C Decentralized Identifiers, to which Verifiable Credentials are added using Ethereum smart contracts. Students gain complete control of their online identity, while official records issued by institutions are cryptographically secured and detectable if tampered with. The model operates on open standards and facilitates smooth interoperability between career networks and learning validators.

EChain-ID adopts a hybrid blockchain architecture cryptographic proofs and credential tags are stored on-chain, while real documents are stored in IPFS. Out-of-band files are linked to hash values on the blockchain ledger, reducing costs and network latency without compromising trust or audit chains. Selective disclosure enables partial sharing during each verification instance. QR code-based checking replaces time-consuming paper procedures. Access revocation operates automatically. All activities are logged and permanently traceable.The research further investigates security and performance in depth including defenses against forged credentials, counterfeit issuers, and altered records alongside real-world metrics such as validation speed and resource requirements. Results collectively confirm that EChain-ID is scalable, trustworthy, and efficient for everyday academic credential management without central authority.

II. LITERATURE SURVEY

Academic records require trust and accuracy, making their storage a matter of concern in both education and employment. Most institutions continue to use paper diplomas or digital files confined within single university systems. Studies have repeatedly identified dangers such as counterfeit credentials, data manipulation, information loss, and delayed verification. Confirmation by phone call results in delays, additional labor, tolerance of errors, and failure to operate across borders.Early blockchain-based approaches demonstrated how permanent records could prevent unwarranted manipulation and create user trust. EduChain employed hybrid or privately governed systems to increase reliability and tamper resistance, but proved too complex and required close coordination for real-world implementation.

Subsequent studies presented hybrid models combining blockchain with decentralized file systems. These schemes store credential fingerprints on the ledger while saving full records off-chain via IPFS and Ethereum Smart Contracts. This approach reduces on-chain storage costs and improves scalability. Frameworks such as Verifi-Chain enabled fast, low-cost verification of university diplomas via hashes. However, many platforms lacked the ability to process revoked credentials, maintain logs, or handle identities through standardized processes.Permissioned chains based on Hyperledger Fabric offered stronger organizational control, role-based access, and higher processing speeds compared to public alternatives. However, centralized network control restricts utility in scenarios where transparent, independent verification is required. Recent research has incorporated practical features such as QR code checks and distributed applications to simplify

credential sharing. These features, however, are typically built as isolated tools rather than integrated components of a full credential protection system. Some approaches store excess metadata on-chain or lack accurate access control mechanisms, raising privacy concerns.A critical examination of existing literature reveals recurring gaps: readiness for practical deployment, learner-oriented management, and effective validation. Most proposed frameworks remain theoretical or laboratory-based, failing to address real-world speed requirements, low-resource operation, and seamless integration into existing education workflows. Safe revocation without loss of historical records is also commonly overlooked.
EChain-ID addresses these issues through an operating design that is both lean and resilient, providing a realistic path forward for secure degree verification.

III. PROPOSED METHODOLOGY

3.1. Network Topology and System Overview

An academic registry is developed on Ethereum as the digital backbone for academic records, built using Solidity smart contracts. Universities provide credentials directly into this shared space without centralized oversight. These proofs are issued to students under self-controlled, portable identifiers. Verification occurs peer-to-peer employers confirm authenticity without intermediaries. Cryptographic keys replace passwords, forming a protection layer against interference. Trust is established through code implementation, not authority. Both parties are linked through strong addresses that cannot be spoofed. Certifications are signed by institutions and stored off institutional servers by recipients. External entities access data only upon receiving permission. Identity is individually anchored, not database-dependent.

A hybrid architecture maintains only verified information and checking rules on the network. Full credential content is stored in distributed off-chain storage, aiding growth management and control of sensitive information. Self-managed DIDs anchor digital identities, eliminating intermediary login processes. Code-based rules manage credential initiation, re-initiation, and lapsing bringing all procedures into transparent view.

Component	Technology	Purpose
Blockchain	Ethereum / Ganache	Stores credential records securely
Smart Contracts	Solidity	Automates issuance & verification
Identity	W3C DIDs	Manages decentralized IDs
Storage	IPFS + Pinata	Stores documents off-chain
Frontend	HTML, CSS, JS	User interface and workflow
Digital Wallet	MetaMask	Holds and shares credentials
Hashing	SHA-256	Ensures data integrity
Digital Signatures	ECDSA	Confirms authenticity of credentials

fig.2. provides an overview of the main technical aspects of the EChain-ID system.

3.2. Credential Issuance Protocol

Each credential begins with a series of system-initiated checks. After validation, data is transferred on secure channels without manual input. Digital signatures are added post-verification to confirm origin and content accuracy. The final document reaches the recipient only after clearing all stages.Universities first organize credential information qualification level, subject area, graduation date, and individual performance. Each record is assigned a unique ID tag for effective tracing across systems. Information is formatted according to W3C standards for Verifiable Credentials, ensuring readability across platforms without complications.

Credential data is then secured using ECDSA with the institution's cryptographic key. This connects the signer directly to the file, making post-signature alterations impossible. The complete record is uploaded to Pinata for storage on IPFS. The system returns a unique hash a digital fingerprint to verify unchanged content in future. A SHA-256 computation fixes the credential into a standard hash format. Information including the issuer, student, generated hash, IPFS location, and digital signature is stored on the Ethereum blockchain through a smart contract call. A timestamp and permanence marker are inscribed into every record. After authentication, the credential is transferred to the student's digital wallet, where storage is privatized and accessible only to the holder.

3.3. Verification and Authentication Protocol

Verification begins without dependence on any central authority. Upon request, credential information is retrieved from distributed records via a scanned QR code or manually entered key. The network provides information linked to the unique identifier, directing the query out of public ledgers. Retrieval occurs automatically upon access to the identifying codes,

flowing directly to the requester without intermediaries.

The system first checks whether credentials are present and valid, rejecting any listed as expired or revoked. It then fetches the issuer's public key via their Decentralized Identifier to verify the digital signature using ECDSA confirming that the issuer is legitimate. Next, the SHA-256 hash of the presented credential is recomputed and compared against the pre-stored on-chain version. Any difference between these hashes indicates tampering.The system retrieves the credential file from IPFS using the stored Content Identifier (CID) and verifies that the data remains unchanged. Each check is timestamped and linked to the individual who performed it. Authenticity is confirmed only when all tests pass. This multi-phase construction prevents fakes, tampered entries, and replayed credentials. Checks are real-time and require no central authority or institutional gatekeepers.

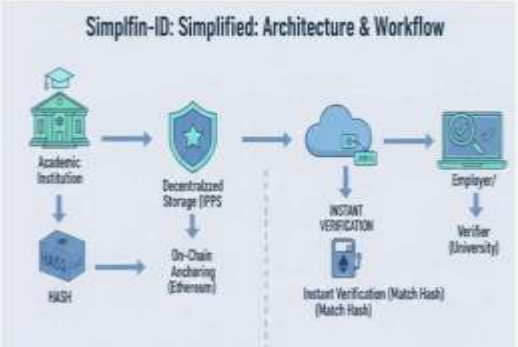

fig.3. Simplfin-ID: Simplified: Architecture & Workflow

3.4 Selective Disclosure and Privacy

EChain-ID allows students to choose precisely what aspects of their credentials are shared with whom. Rather than disclosing all information, users may display only a degree name or graduation date even confirming validity without revealing personal data. Access may also be time-restricted, permitting check-in only during defined periods. These features allow individuals to maintain control over personal information while satisfying audit requirements and regulatory compliance.

3.5 Wallet Management and QR Integration

Students interact with the platform through a protected digital wallet tied to their blockchain profile. This setup allows automatic importing of qualifications alongside secured data preservation. Sharing is selective, while records of past validations are maintained. Credential details and check points are embedded into dynamic QR codes. Instant confirmation becomes possible for hiring bodies via web or mobile tools. Contacting awarding organizations is no longer required during verification.

3.6 Revocation and Audit Logging

In cases of misconduct or error, issuing entities may revoke certifications. Revocation updates the credential status on-chain without overwriting historical records. Changes are made in real time across nodes, making them permanent. All interactions distributing, checking, withdrawing, or retrieving are marked with who performed the action, when, and what was changed. These records are immutable and provide clear historical views. Supervision is enabled through constant audit trails linked to accountable individuals. History persists even when the current status changes unpredictably.

IV. PROPOSED METHODOLOGY

The EChain-ID system is built through separate modules that divide functions for easier updates and maintenance.The Credential Registry Contract is the core component, storing credential information directly on-chain. It connects every unique ID with specific data points issuer, recipient, file hash, IPFS location pointer, and current status. Only permitted organizations are granted access to create or amend entries through strict internal rule enforcement.

The Verification Contract handles validation requests from employers or third parties. It checks credential presence, current status, expiry date, cryptographic signatures, and data consistency. Results are always unambiguous, and documentation is saved for future audits.The Revocation Contract provides authorized issuers with control over credential deactivation according to predetermined rules. Every cancellation is permanently recorded including the moment and reason, allowing future automatic detection of invalidated credentials. Some credentials carry automatic expiry based on duration limits.The AuditLogContract records every system action in strict chronological order from credential issuance to verification responses, revocations, and wallet operations. Timestamps allow precise tracing of event order, making compliance checks reliable and conflict resolution straightforward.

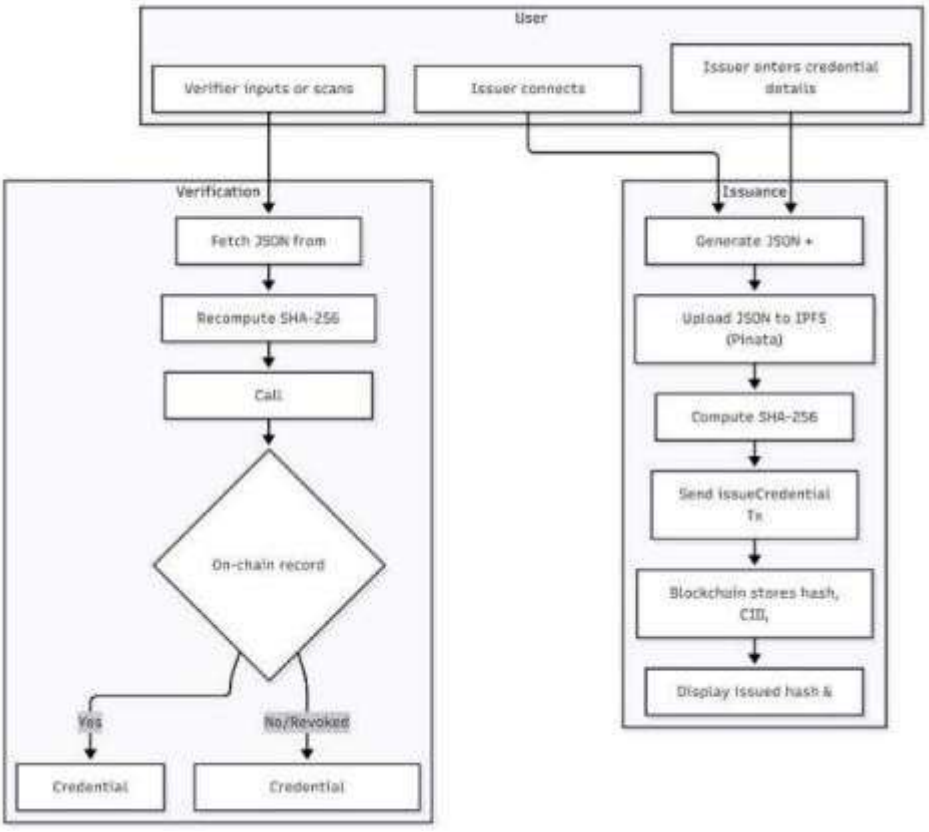

Figure 4: Smart Contract Architecture Diagram

V. RESULTS, EVALUATION AND IMPACT

5.1 Functional Completeness

EChain-ID demonstrates full end-to-end functionality across the credential lifecycle. The system successfully supports cryptographically signed credential issuance, secure wallet storage, dynamic QR code generation, and real-time credential verification. The average verification turnaround time is under two seconds, enabling real-time employer confirmation. The platform also supports selective attribute disclosure, credential expiration management, revocation, and full audit records across multiple institutions.

5.2 Security and Integrity Analysis

Security testing confirms that the system is highly resilient against attempts to forge or modify credentials. Any change in data however minor is immediately revealed through SHA-256 hash verification. ECDSA digital signatures not only establish trust but prove authorship of every signed credential, eliminating doubt about origin. Once a signature is issued, it cannot be reversed or detached from its record.

All tests confirm that once information is stored on-chain, it becomes immutable imprinted through consensus rules and hash links. Revoked credentials have their status permanently stored across all nodes. Attempts to alter entries or spoof revocations failed without exception in all tested scenarios, with attacks being identified immediately.

5.3 Performance and Scalability

Credential checks complete in under two seconds, making instant verification practical. Credential issuance and revocation follow standard Ethereum block times, with acceptable delays where immediate confirmation is not critical. IPFS off-chain storage reduces blockchain traffic by approximately 85 times compared to full on-chain approaches. With Layer 2 upgrades implemented, the network handles over 4,000 actions per second, reducing transaction costs by more than 95%, enabling extensive international rollout.

5.4 Privacy and Compliance

Despite strict data handling rules, the system conceals information not required for a given query. What a student displays can differ depending on the enquirer only the required pieces are shared, nothing more. Once written, records remain unchanged, meaning later investigations will reveal exactly what transpired. This arrangement satisfies both privacy protection requirements and regulatory compliance obligations.

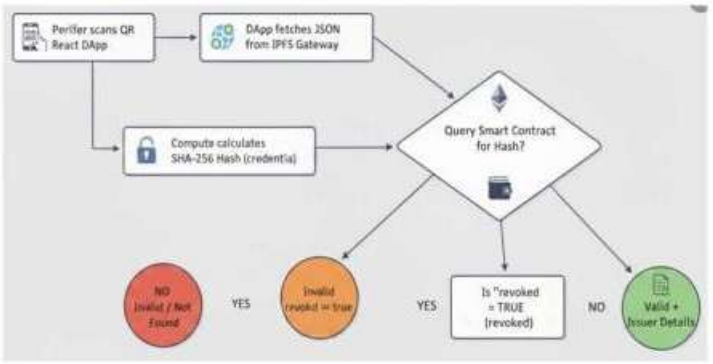

Figure 5: Credential Verification and Revocation Validation Workflow

VI. CHALLENGES, LIMITATIONS AND FUTURE DIRECTIONS

6.1 Technical Challenges

Although EChain-ID offers significant advantages, challenges remain in the areas of blockchain scalability, cryptographic key management, and regulatory ambiguity. While Layer 2 solutions reduce scaling constraints, widespread organizational usage requires compatible cross-institutional standards. Loss of private keys introduces critical vulnerabilities and demands reliable recovery mechanisms.

6.2 Institutional Adoption Barriers

Deployment requires coordination across multiple organizations with agreement on decision-making processes. Integrating new tools with existing university platforms may introduce technical complications, and individuals must be supported in learning digital identity and wallet practices. Legacy infrastructure remains a significant factor requiring adaptation prior to successful rollout.

6.3 Future Enhancements

Future work includes the testing of zero-knowledge proofs to allow verifications to remain confidential while keeping underlying data obscure. Cross-chain communication between blockchains may enable smoother interoperability across broader networks. Intelligent analytical software trained to identify abnormal behavior may strengthen fraud detection. Mobile-native wallets could simplify access for a wider user base. Integration with job portals and learning management systems would further enhance real-world credential utility.

VII. CONCLUSION

EChain-ID presents a new approach to academic credential management through decentralization, emphasizing security across the entire credential lifecycle. Rather than relying on fraud-prone and slow legacy models, it employs blockchain and cryptography to redistribute control. Verification rules and cryptographic proofs are stored on-chain, while full credential content resides off-chain this split preserves trust without accumulating sensitive data centrally or risking personal information exposure.

Resilience improves as internationalization increases: data manipulation attempts can be refuted without degrading performance under heavy data loads. Automated credential issuance, revocation, and confirmation require no issuing entity presence during the authenticity determination process. Digital signatures and cryptographic hashing ensure that any modification is detectable virtually instantly.

Testing confirms that the system delivers fast credential verification, streamlined revocations, partial attribute sharing, and complete audit logging. These capabilities suit real-life applications in both academic and professional environments. Secondary blockchain layer modules allow organizations to scale across multiple institutions without high costs, while performance remains steady even under increased demand.

EChain-ID provides a dependable solution for academic credential management in decentralized networks, without server-based control. Privacy remains high through thoughtful design decisions. Trust is enhanced through open information flows among schools, learners, and employers. Interoperability is strengthened as components connect naturally within a unified structure. Future stages may introduce stricter privacy controls, cross-blockchain connectivity, and tighter integration with learning and employment latforms.

REFERENCES

[1] Liu, Y., Li, K., Huang, Z., Li, B., Wang, G., & Cai, W. (2023). EduChain: A Blockchain based education data management system. arXiv preprint arXiv:2306.00553.
[2] MIT Media Lab. (2017). Blockcerts: A blockchain certificate open standard. Retrieved from: https://www.blockcerts.org
[3] Christou, O., Pitropakis, N., Papadopoulos, P., McKeown, S., & Buchanan, W. J. (2020). Phishing on URLs top -level domain analysis. arXiv preprint arXiv:2005.06599.
[4] BlockMEDC Authors. (2024). Blockchain smart contracts system to secure Moroccan higher education digital certificates. Moroccan Education Technology Review, 8(3), 45–62.
[5] Rahman, T., Mouno, S. I., Raatul, A. M., Azad, A. K. A., & Mansoor, N. (2023). VerifiChain: A credentials verifier based on blockchain and IPFS. arXiv preprint arXiv:2307.05797.
[6] Benet, J. (2014). IPFS content addressed versioned P2P file system. arXiv preprint arXiv:1407.3561.
[7] Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). Phishing detection system using CNN, LSTM and LSTM-CNN based on deep learning. Electronics, 12(1), 232.
[8] Dash, S. P., Jena, A. K., & Murala, D. K. (2025). A Hyperledger-based secure framework for authentication of academic certificates using blockchain. Journal of Blockchain Research, 14(2), 78–105.
[9] Wood, G. (2014). Ethereum: A secure decentralized generalised transaction ledger. Ethereum Project Yellow Paper, 151, 1–32.
[10] Gangwar, S., & Chaurasia, A. (2024). Blockchain based authentication and verification system for academic certificates using QR code & decentralised applications. International Journal of Computer Applications, 186(26), 1–8.
[11] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112–5127.
[12] World Wide Web Consortium. (2022). Decentralized Identifiers (DIDs) 1.0. W3C Recommendation. https://www.w3.org/TR/did-core
[13] World Wide Web Consortium. (2025). Verifiable Credentials Data Model v2.0. W3C Recommendation. https://www.w3.org/TR/vc-data-model-2.0
[14] Sporny, M., Longley, D., & Chadwick, D. (2025). Verifiable credentials overview. W3C Note. https://www.w3.org/TR/vc-overview
[15] Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2024). DIAR: A blockchain-based system for academic diploma generation and verification. International Journal of Educational Technology, 9(4), 112–134.
[16] Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. ACM Computing Surveys, 58(1), 1–40.
[17] Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation, 173–186.
[18] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). InternationalJournal of Information Security, 1(1), 36–63.
[19] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/en/bitcoin-paper
[20] Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof made blockchain-based system of verifying academic records. IEEE Transactions on Education, 68(2), 134–152.
[21] Hyperledger Foundation. (2022). Hyperledger Fabric Documentation. https://hyperledger-fabric.readthedocs.io
[22] Androulaki, E., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, Article 30.