ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 05 May 2026

EduNetChain: A Blockchain-Based Platform for Student–Alumni Interaction

[1] Dr. Varsha Mhaske, [2] Praneket Jadhav, [3] Harshad Wable, [4] Sakshi Nikam, [5] Kiran Kate

[1][2][3][4][5] Department of Computer Engineering, SVPM College Of Engineering, Malegaon Bk, India
Email: [1] varshamhaske13@gmail.com, [2] jadhavpraneket@gmail.com, [3] harshadswable9@gmail.com, [4] sakshinikam613@gmail.com, [5] kirankate114@gmail.com

Abstract— *EduNetChain is a blockchain-based system designed to address two key challenges in the education sector: secure academic credential verification and effective student–alumni interaction. Traditional verification methods are often centralized, time-consuming, and vulnerable to data tampering, while existing platforms lack structured communication between students and alumni for career support. The proposed system adopts a hybrid approach where academic records are stored in a secure database, and their cryptographic hashes are recorded on the blockchain to ensure data integrity and tamper-proof verification. The platform involves three primary stakeholders—students, alumni, and validators—where validators validate student data before generating blockchain-backed credentials, and alumni interact with students by sharing job opportunities and guidance. By integrating blockchain technology with a collaborative interaction model, EduNetChain enhances trust in academic verification while also creating a practical ecosystem for career development. The implementation demonstrates that the system is secure, efficient, and suitable for real-world deployment.*

Index Terms— *Academic Credential Verification, Blockchain, Cryptographic Hashing, Data Integrity, Decentralized Systems, Educational Technology, Smart Contracts, Student–Alumni Interaction*

I. INTRODUCTION

The education sector has witnessed a rapid shift toward digital systems for managing and verifying academic credentials. Certificates and degrees serve as primary proof of a student's qualifications and are widely relied upon by employers, institutions, and professional bodies. Despite this importance, the underlying systems used to issue and verify these credentials remain largely centralized and manual, making them slow, inefficient, and difficult to scale [1].

Ahmed et al. [1] highlight that centralized identity and credential systems are inherently vulnerable to single points of failure, where a breach or system outage can compromise the authenticity of thousands of records simultaneously. Halder et al.

[2] further demonstrate that without a tamper-proof mechanism, academic documents can be easily duplicated or falsified using widely available digital tools, making it increasingly difficult for organizations to distinguish genuine credentials from forged ones.

Said et al. [3] and Singh et al. [4] both emphasize that blockchain technology offers a reliable foundation for document verification due to its immutable and decentralized nature. Once data is recorded on a blockchain, it cannot be altered without detection, making it well-suited for maintaining the integrity of academic records.

Gayathiri et al. [5] similarly validate this approach by demonstrating that blockchain-based certificate systems significantly reduce verification time while improving overall reliability compared to traditional methods.

However, a critical gap exists in most existing blockchain-based systems — they continue to rely on a **single administrator** to approve and issue credentials. Said et al. [6] and Saleh et al. [8] note that this single-authority model reintroduces centralization into an otherwise decentralized system, creating a potential point of trust failure. If the approving authority is compromised, biased, or unavailable, the integrity of the entire verification process is at risk.

Beyond verification, Patil et al. [12] and Penugonda et al. [13] point out that there is a significant absence of platforms that meaningfully connect students and alumni within a verified ecosystem. Most existing solutions treat credential management and professional networking as entirely separate concerns, leaving students without structured access to mentorship, referrals, and career guidance from alumni.

To bridge these gaps, this paper presents **EduNetChain**, a blockchain-based platform that combines secure academic credential verification with a structured student–alumni interaction environment. The system introduces a **multi-validator consensus mechanism**, where credential approval requires a majority vote — specifically floor(N/2) + 1 votes — from independent validators, with each vote recorded transparently on the smart contract. This eliminates single-authority dependency and strengthens trust in the verification process. The platform engages three primary stakeholders — **students, validators, and alumni**— and aims to deliver a secure, scalable, and practically deployable solution for modern educational ecosystems.

II. LITERATURE SURVEY

The challenge of securing academic credentials and enabling trustworthy verification has attracted considerable research attention in recent years. Scholars have explored a range of blockchain-based approaches to address the limitations of traditional centralized systems.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 05 May 2026

A. Blockchain-Based Identity and Credential Verification

Ahmed et al. [1] proposed a blockchain-based identity management system aimed at eliminating the risks associated with centralized storage, including data breaches and single points of failure. Their work laid a foundation for applying self- sovereign identity principles in academic environments, giving students greater control over their own credentials. Building on this, Halder et al.

[2] developed a digital degree issuance and verification system using blockchain, demonstrating that tamper-proof records could be maintained without relying on institutional intermediaries. Their system significantly reduced the time required for third-party verification compared to conventional approaches.

B. Document Verification and Cryptographic Techniques

Said et al. [3] introduced a document verification model that integrates cryptographic hashing and blockchain storage to detect unauthorized modifications in submitted records. Their approach established that even minor alterations in a document produce a completely different hash value, making forgery immediately detectable. Singh et al. [4] extended this concept by developing an Ethereum-based system where academic certificates are converted into digital formats, hashed, and stored on-chain to enable transparent and verifiable credential management. Gayathiri et al. [5] further demonstrated the practical feasibility of blockchain-based certificate validation, showing that the system could operate efficiently at scale while maintaining strong security guarantees.

C. Scalability and Interoperability

Said et al. [6] presented a comprehensive blockchain-based framework designed to support credential issuance and verification across multiple educational institutions, addressing the limitations of institution-specific solutions that cannot communicate with each other. Darshan and Vasanthakumar [7] took this further by integrating technologies such as IPFS and zero-knowledge proofs to enhance privacy and cross-platform compatibility, allowing credentials to be verified without exposing sensitive personal information. Saleh et al. [8] emphasized key security dimensions including authentication, authorization, confidentiality, and ownership within an enterprise blockchain framework, providing a structured approach to securing credential ecosystems.

D. Decentralized Applications and Student Control

Shawon et al. [9] developed DIUcerts, a decentralized application built on blockchain that enables cost-effective and scalable certificate verification without dependence on any central authority. Their work demonstrated that DApp- based solutions are practically viable for real-world deployment in educational institutions. Jain [10] further explored decentralized identity systems in education, arguing that students should have portable, self-managed credentials that reduce their dependency on institutions for verification. Suktam et al. [11] reinforced this perspective by highlighting blockchain's broader transformative potential in education, including improvements in administrative efficiency, transparency, and academic data integrity.

E. Student–Alumni Interaction Platforms

While significant progress has been made in credential verification, limited attention has been given to combining verification with collaborative user interaction. Patil et al. [12] proposed AlmaHub, a platform designed to facilitate structured communication between students and alumni, enabling mentorship and career support. However, their system lacks integration with any credential verification mechanism, leaving the authenticity of student profiles unvalidated. Similarly, Penugonda et al. [13] introduced Unibridge, an alumni engagement platform focused on networking and career opportunities, but without addressing credential authenticity or validation.

F. Research Gap

Based on the analysis of existing literature, two key gaps are identified. First, most blockchain-based credential systems depend on a single centralized authority for approval, which reintroduces trust vulnerabilities into an otherwise decentralized framework. Second, platforms that support student–

alumni interaction do not incorporate any mechanism for verifying the authenticity of student credentials. EduNetChain addresses both gaps by introducing a multi-validator consensus mechanism for on-chain credential approval and integrating it with a collaborative student–alumni interaction platform.

III. PROBLEM STATEMENT

The verification of academic credentials remains a persistent challenge across educational and recruitment ecosystems. Despite the availability of digital tools, most institutions continue to rely on centralized and manual processes for issuing and validating academic records. These approaches are not only time-consuming and administratively burdensome but also highly susceptible to document forgery, unauthorized modifications, and data loss [1][3].

Ahmed et al. [1] and Said et al. [3] collectively highlight that centralized storage architectures introduce a single point of failure, where a security breach or system compromise can affect the integrity of an entire institution's credential database. As digital editing tools become more sophisticated, the creation of counterfeit certificates has grown easier, making it increasingly difficult for employers and institutions to distinguish authentic documents from fabricated ones [2][4].

A further limitation observed in existing blockchain- based solutions is their continued dependence on a **single administrative authority** to validate and approve student credentials. Saleh et al. [8] and Said et al. [6] note that this model, despite leveraging blockchain for storage,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 05 May 2026

reintroduces centralization at the approval stage. A single compromised, biased, or unavailable authority can disrupt the entire credential issuance process, undermining the trust that blockchain is meant to provide. There is therefore a clear need for a **decentralized validation mechanism** where approval authority is distributed across multiple independent validators, and decisions are made through a transparent majority consensus rather than a single entity.

In addition to verification challenges, there is a significant lack of platforms that integrate credential validation with structured student–alumni interaction. Patil et al. [12] and Penugonda et al. [13] demonstrate that while alumni engagement platforms exist, they operate independently of any verification mechanism, leaving student credentials unvalidated within networking contexts. As a result, students are deprived of meaningful access to mentorship, referrals, and career guidance from alumni, while alumni lack a reliable way to assess the authenticity of student profiles before engaging with them.

Therefore, there is a need for a unified, secure, and scalable system that addresses both challenges — one that ensures tamper-proof credential verification through decentralized validator consensus and simultaneously enables meaningful, trust-based interaction between students and alumni within a single integrated platform.

IV. PROPOSED SOLUTION

To address the limitations identified in existing systems, this paper proposes **EduNetChain**, a blockchain-based platform that integrates decentralized academic credential verification with a structured student–alumni interaction environment. The system is built on a hybrid architecture, where academic data is maintained in a centralized database while its cryptographic representation is recorded on the blockchain to ensure integrity and tamper-proof validation. Storing complete academic records directly on-chain would introduce high gas costs and scalability limitations. Therefore, EduNetChain stores only cryptographic hashes on-chain while maintaining full records in off-chain databases.

The proposed system consists of three primary stakeholders: **students, validators, and alumni**. Each stakeholder plays a specific and well-defined role in maintaining the functionality and trustworthiness of the platform.

- **Students** are responsible for registering on the platform and submitting their academic details, including personal information, educational qualifications, skills, and supporting documents. Once submitted, a validation request is automatically generated and dispatched to the validator pool for review. Any subsequent update to a student's profile triggers a fresh validation request, ensuring that all changes are subject to the same consensus-based approval process before being reflected on the blockchain.
- **Validators** form the trust layer of the system. Each validator independently reviews incoming student registration and update requests and casts their vote — approve or reject — directly on the smart contract. This ensures that every vote is transparently recorded on-chain and cannot be manipulated. The system enforces a majority consensus threshold of **floor(N/2) + 1 votes**, where N represents the total number of active validators. Only upon reaching this threshold is the student's credential hash generated and recorded on the blockchain. This decentralized approval mechanism eliminates dependency on any single authority and significantly strengthens the integrity of the verification process.
- **Alumni** interact with verified students through the platform. They can view student profiles, post job opportunities, provide referrals, and offer career guidance. Since student credentials are backed by multi-validator consensus and recorded on the blockchain, alumni can trust the authenticity of the information before engaging with students.

The core functionality of the system lies in its **decentralized credential verification mechanism**. When a student's registration or update request receives the required majority votes from validators, the system generates a cryptographic hash of the student's academic data using the Keccak-256 algorithm. This hash acts as a unique digital fingerprint of the data and is recorded on the blockchain through a smart contract. Any modification in the original data results in a completely different hash value, making tampering immediately detectable. During verification, the system recomputes the hash of the current data and compares it with the hash stored on the blockchain. A matching result confirms authenticity, while a mismatch flags the record as altered.

In addition to verification, EduNetChain provides a **communication and interaction layer** that enables direct engagement between students and alumni. Features such as messaging, job posting, and application tracking are integrated into the platform. Access to messaging is governed by role-based rules a student can message an alumni only if their application has been accepted, and an alumni can message a student only if a verified job or referral relationship exists between them. This controlled interaction model ensures that all communication within the platform is purposeful and trust-based.

The system also incorporates **skill gap detection** and **job recommendation** features. The skill gap module analyzes a student's existing skills against the requirements of active job and referral posts, identifying areas for improvement. The job recommendation module scores available opportunities based on skill match and educational background, returning personalized ranked recommendations to the student.

Overall, EduNetChain combines decentralized validator consensus, blockchain-backed credential integrity, and a collaborative interaction model into a single unified platform — delivering both trust in academic verification and a practical ecosystem for career development.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 05 May 2026

V. SYSTEM ARCHITECTURE

The architecture of EduNetChain is designed as a hybrid system that integrates user interaction, multi- validator verification, decentralized storage, and blockchain-based credential validation into a unified framework. As shown in Fig. 1, the system consists of two primary stakeholders — students and alumni along with a validator consensus layer, a smart contract module, a dual storage layer comprising Supabase and MongoDB, and a blockchain ledger on the Ethereum Sepolia testnet.

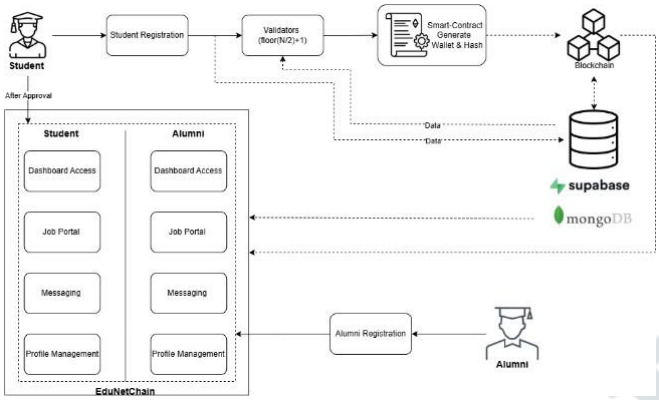


Fig. 1: EduNetChain System Architecture

Student Registration and Validator Consensus

The process begins with student registration, where users create their profiles by providing academic details such as degree, institution, branch, year of passing, and student ID, along with personal information and supporting documents including resume and certificates. Upon registration, a verification request is automatically created in the system. This request is reviewed by a panel of validators — faculty members authorized by the Super Admin — who independently cast their votes to approve or reject the student's credentials. The consensus rule applied is floor(N/2)+1, meaning a strict majority of active validators must approve before the student is verified. This mechanism is application-level majority consensus and not blockchain mining consensus such as Proof-of-Work or Proof-of-Stake.This multi-validator approach eliminates single-point control and ensures that no individual can unilaterally approve a fraudulent credential.

Smart Contract — Wallet Generation and Hash Creation

Once the required validator consensus is reached, the system triggers the smart contract module. A unique blockchain wallet address is generated for the student, and a keccak256 cryptographic hash is computed from the student's verified academic data name, email, degree, institution, branch, year, and student ID. This hash, along with individual field hashes, is submitted to the smart contract deployed on the Ethereum Sepolia blockchain via the issueCredential function. The hash is recorded permanently and immutably on the blockchain ledger. This step ensures that the academic credential becomes tamper-proof — any modification to the original data in the database will produce a different hash, which will not match the blockchain record, immediately flagging the data as tampered.

Dual Storage Layer — Supabase and MongoDB

As shown in Fig. 1, the system uses two storage components. Supabase Storage is used for file storage — resumes and certificates uploaded by students during registration are stored here and made accessible to validators during the review process. MongoDB serves as the primary database for all structured data — student profiles, alumni profiles, verification requests, validator votes, job postings, messages, comments, and notifications. This separation ensures efficient querying and scalability for application data while keeping file storage decoupled and independently managed.

Student Portal — After Approval

As indicated in Fig. 1 by the "After Approval" label, a student gains access to the EduNetChain platform only after their credentials have been verified through the validator consensus process and recorded on the blockchain. The Student Portal provides four core features. Dashboard Access gives the student a personalized view of their verification status, blockchain wallet address, credential hash, AI-based job recommendations, and profile views. The Job Portal allows students to browse job postings, referrals, and career tips posted by alumni, and apply directly through the platform. Messaging enables students to communicate with alumni, subject to a controlled access rule — a student can only initiate a conversation with an alumni after that alumni has accepted their application on a post, ensuring meaningful and spam-free interactions. Profile Management allows students to update their contact information, skills, projects, and experience, while their core academic credentials remain permanently locked after verification.

Alumni Portal

Alumni register separately through the Alumni Registration flow shown in Fig. 1 and gain immediate access to the platform without requiring blockchain verification, as they are established graduates rather than current students seeking credential issuance. The Alumni Portal mirrors the Student Portal in structure but serves a different purpose. Dashboard Access provides alumni with their professional profile and activity overview. The Job Portal allows alumni to create and manage job postings, referral opportunities, and career guidance tips for students. Messaging allows alumni to communicate with students who have applied to their posts and with other alumni freely. Profile Management allows alumni to maintain their professional information including current company, position, and experience.

Verification Mechanism

The verification mechanism is implemented through the smart contract and the tamper detection system. When a credential check is triggered — either by a validator during the review process or by a recruiter on the public verification

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 05 May 2026

page — the system fetches the student's current data from MongoDB, recomputes the keccak256 hash, and queries the blockchain using the student's wallet address to retrieve the originally stored hash. If the two hashes match, the credential is displayed as verified. If they do not match, the system flags the data as tampered, indicating that the database record has been modified after blockchain storage. This provides a continuous and reliable integrity check that operates independently of any central authority.

Overall Design Philosophy

The architecture effectively separates three distinct responsibilities. MongoDB and Supabase handle data storage and file management with efficiency and scalability. The validator consensus layer handles trust establishment through distributed human verification. The blockchain layer handles permanent, tamper-proof proof of that verification. By combining these three layers, EduNetChain achieves a system where every student on the platform is a verified identity, every interaction between students and alumni is built on institutional trust, and every credential can be independently verified by any recruiter or institution without contacting the college directly.

VI. ALGORITHMS

Credential Hashing and Blockchain Issuance

Input: Student profile data (name, email, degree, institution, branch, year, skills, documents) Output: Transaction hash (txHash), Wallet address

1. On admin approval trigger, the student data is serialized into a JSON string.
2. A cryptographic hash of the complete data is generated using Keccak-256.
3. Individual hashes are generated for key fields such as name, email, degree, institution, and resume.
4. If the student does not have a wallet address, a new Ethereum wallet is generated and assigned.
5. The system invokes the smart contract function issueCredential() to store the hashes on the blockchain.
6. If credential issuance fails due to an existing record, a fallback function storeVerification() is executed.
7. The generated hash, transaction hash, and timestamp are stored in the database.
8. The transaction hash and wallet address are returned.

Role-Based Messaging Access Control

Input: senderId, senderRole, receiverId, receiverRole
Output: Boolean (allowed / denied)

1. If both sender and receiver are alumni, communication is allowed.
2. If both sender and receiver are students, communication is allowed.
3. If a student attempts to message an alumni, the system checks whether the alumni has accepted the student's application.
4. If an accepted application exists, communication is permitted; otherwise, it is denied.
5. If an alumni attempts to message a student, the system verifies whether the student has been accepted for a job or referral by that alumni.
6. If such a relationship exists, communication is permitted; otherwise, it is denied.
7. In all other cases, communication is denied.

Skill Gap Detection Input: studentId
Output: gaps[], strengths[], totalJobsAnalyzed

1. The student's skills are fetched and normalized.
2. Active job and referral posts are retrieved from the database.
3. A predefined set of common skills is used as a reference.
4. Each job description and requirement is analyzed to identify skill occurrences.
5. A demand map is created to count the frequency of each skill.
6. Skills not present in the student's profile but in demand are identified as gaps.
7. Skills present in both the student's profile and demand map are identified as strengths.
8. The top demanded skills are returned along with analysis results.

Job Recommendation by Skill Match Scoring Input: studentId

Output: Recommendations[] (top ranked jobs)

1. The student's skills and educational background are retrieved.
2. Active job and referral posts are collected and processed.
3. For each job, a matching score is initialized.
4. The job description is analyzed for skill matches.
5. For every matching skill, the score is incremented.
6. Additional weight is added if the student's degree matches the job requirements.
7. Jobs are ranked based on the computed scores.
8. The top-ranked jobs are returned as recommendations.

VII. IMPLEMENTATION DESIGN

A. Smart Contract Implementation: The core smart contract is developed using Solidity and deployed using Hardhat. The contract maintains mappings to store credential hashes, verification records, and post hashes. A write-once constraint is enforced to ensure that credentials cannot be modified once issued. Access control is implemented using an owner-based restriction, allowing only authorized entities to issue credentials. The smart contract enforces write-once credential issuance and owner-based authorization to prevent unauthorized modification or replay attacks.

B. Backend Services: The backend is implemented using Node.js and Express.js. It includes modules for cryptographic hashing, blockchain interaction, and file storage. The hashing module generates Keccak-256 hashes for student data, while the blockchain service interacts with the deployed smart contract using

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 05 May 2026

ethers.js. File storage is handled through cloud storage and IPFS integration.

C. **Authentication and Authorization:** The system uses JSON Web Tokens (JWT) for authentication. Upon successful login, access and refresh tokens are issued, with refresh tokens securely stored using hashing. Role-based access control is implemented to manage permissions for students, alumni, administrators, and recruiters.

D. **Credential Issuance Workflow:** The process begins with student registration, where academic details and documents are submitted. The administrator verifies the submitted data and triggers the credential issuance process. The system generates cryptographic hashes and records them on the blockchain through a smart contract. The transaction details are stored in the database, and the student is notified of successful verification.

E. **Frontend Implementation:** The frontend is developed using React and styled with Tailwind CSS. It provides separate interfaces for students, alumni, administrators, and recruiters. Key features include profile management, job posting and applications, messaging, and public credential verification.

F. **Technology Stack:**

Component	Technology
Frontend Framework	React + Vite
Styling	Tailwind CSS
Backend Runtime	Node.js + Express.js
Database	MongoDB Atlas + Mongoose
Authentication	JWT + bcrypt
File Upload	Multer + Supabase Storage
Blockchain Network	Ethereum Sepolia Testnet
Smart Contract	Solidity
Blockchain Client	Ethers.js
Contract Deployment	Hardhat
RPC Provider	Alchemy
Hashing Algorithm	keccak256

VIII. RESULTS

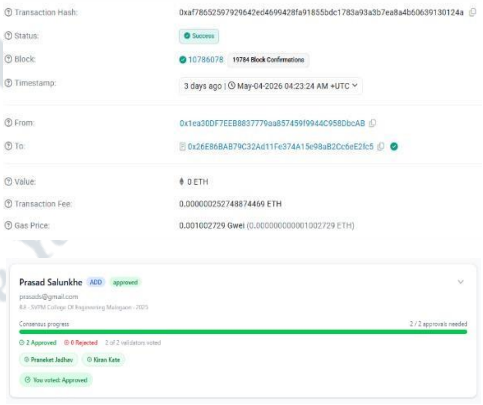
- **Credential Verification Results:** The primary objective of EduNetChain is to provide tamper-proof, blockchain-backed credential verification for students. The system was tested with 25 registered students, of which 20 were successfully verified through the multi-validator consensus mechanism, achieving a verification success rate of 80%. Each verified student was assigned a unique Ethereum wallet address, and their credential data was hashed using the keccak256 algorithm before being stored on the Ethereum Sepolia blockchain.

Metric	Result
Total Students Registered	25
Students Successfully Verified	20
Students Pending Verification	5
Verification Success Rate	80.0%
Students Assigned Wallet Address	20

Total keccak256 Hashes Stored	20
Credential Versions on Blockchain	1
Blockchain Transaction Hash	0xaf7865...130124a
Blockchain Network	Ethereum Sepolia Testnet
Chain ID	11155111
Current Block Number	10,805,813
Gas Price at Testing	0.001 Gwei

Sample Verified Credential (actual data from system):

Field	Value
Student Name	Prasad Salunkhe
Institution	SVPM College of Engineering Malegaon
Degree	B.E. Computer Science
Year	2025
CGPA	9.3
Wallet Address	0xEf91C753...F4a01E
Credential Hash	0x172a6f...4e01f
Transaction Hash	0xaf7865...130124a
Issued At	2026-05-04 04:23:27 UTC



- **On-Chain Verification:** The system provides a public credential verification endpoint (/verify-credential) that requires no login. Any recruiter or institution can verify a student's credential by entering the student's wallet address. The verification is performed by calling verifyHash() on the smart contract, which is a read-only operation and completes in under 1 second.

Operation	Method	Time
Credential Issuance	issueCredential()—blockchain write	12–15 seconds
Credential Verification	verifyHash()—blockchain read	< 1 second
keccak256 Hash Generation	cryptoService. js	< 1 ms
JWT Authentication	Middleware check	< 5 ms
Tamper Detection	Hash comparison	< 1 second

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

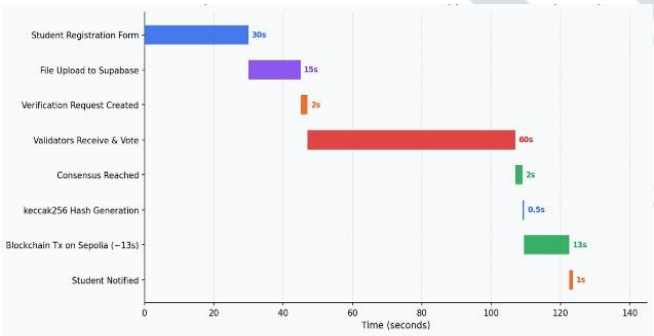
Volume 13 Issue 05 May 2026

- **Post Integrity:** All posts created within the system are hashed and recorded on the blockchain. This enables detection of any unauthorized modifications by comparing stored hashes with recomputed values, ensuring content integrity.
- **Role-Based Access Control:** The system enforces strict role separation across 5 portals with isolated session namespaces.

Test	Result
Unverified student login	Blocked — 403 returned
Unauthenticated API call	Blocked — 401 JWT rejection
Student accessing validator route	Blocked —isValidator check fails
Validator approving without majority	Blocked — consensus not reached
Super admin brute force login	Blocked — 20 req / 15 min rate limit
Cross-portal session interference	None — separate localStorage namespaces
Credential issued without onlyOwner	Blocked —contract reverts

- **System Performance:** The system demonstrates efficient performance across key operations. Credential issuance requires blockchain transaction confirmation, typically taking 12–15 seconds, while credential verification is performed through read-only blockchain calls and completes almost instantly.

Authentication operations are executed with minimal latency using JWT-based mechanisms.



IX. FUTURE WORK

Although EduNetChain provides a secure and practical solution for decentralized academic credential verification and student–alumni interaction, several directions remain open for further development.

One important area is the formalization of an **on- chain update policy** for student credentials. Currently, the behavior of existing blockchain records upon re-validation — whether the old hash is replaced or a new versioned record is added — is under active consideration. A well-defined update mechanism will strengthen the auditability and completeness of the credential lifecycle on-chain.

The system can also be extended to support **dynamic validator management**, where validators can be added or removed based on participation history or reputation scoring. Introducing a **validator incentive mechanism** — where honest and timely voting is rewarded — would further encourage active and fair participation within the consensus process.

Another promising direction is the integration of **NFT-based digital certificates**, where verified academic credentials are issued as non-fungible tokens. This would provide students with unique, transferable, and independently verifiable digital assets representing their academic achievements.

Expanding the platform to support **multi-institution integration** would allow multiple colleges and universities to participate in a shared validator network, enabling cross-institutional credential verification and improving adoption at scale. Alongside this, exploring **zero-knowledge proofs** would allow credentials to be verified without exposing sensitive personal data, significantly enhancing user privacy.

Finally, developing a **mobile application** with real- time notifications, job alerts, and chat would improve accessibility and user engagement. Optimizing blockchain performance through layer-2 solutions or alternative networks would also reduce transaction costs and improve scalability for large-scale deployments.

X. CONCLUSION

In this paper, **EduNetChain** has been presented as a blockchain-based platform that addresses two persistent challenges in the education sector — the unreliability of academic credential verification and the absence of a structured, trust-based interaction environment for students and alumni. Traditional credential systems remain heavily dependent on centralized authorities and manual processes, making them vulnerable to forgery, data tampering, and single points of failure. The proposed system tackles these limitations through a hybrid architecture that combines efficient database storage with blockchain-based integrity verification.

A key contribution of this work is the introduction of a **multi-validator consensus mechanism**, where credential approval is no longer dependent on a single administrative authority. Instead, a pool of independent validators collectively reviews and votes on student registration and profile update requests through a smart contract, with approval requiring a majority threshold of floor(N/2) + 1 votes. Since every vote is recorded transparently on- chain, the process is tamper-proof, auditable, and free from unilateral control. This design brings the credential issuance process closer to the true spirit of decentralization that blockchain technology promises.

The system engages three primary stakeholders — students, validators, and alumni — each with clearly defined roles. Students submit their academic data for consensus-based verification, validators collectively govern the approval process on-chain, and alumni interact with verified

student profiles to offer job opportunities, referrals, and career guidance. The integration of role-based messaging, skill gap detection, and job recommendation features further strengthens the platform as a practical career development ecosystem.

Overall, EduNetChain demonstrates that secure, decentralized credential verification and meaningful student–alumni collaboration can be effectively unified within a single platform. The system is designed to be scalable, transparent, and suitable for real-world deployment, offering a reliable foundation for modernizing academic credential management in educational institutions.

REFERENCES

[1] M. R. Ahmed, A. K. M. M. Islam, S.Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," 2022.

[2] S. Halder, S. Bera, S. Ghosh and S. Chakraborty, "Digital Degree Issuing and Verification Using Blockchain," in *IEEE Conference*, 2022.

[3] A. S. S. Said, N. Salim and M. R. M. Said, "Document Verification Using Blockchain," in *IEEE Conference*, 2021.

[4] A. Singh, S. P. Chauhan and A. K. Goel, "Blockchain Based Verification ofEducational and Professional Certificates," in *ICCCSC*, 2022.

[5] A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate Validation Using Blockchain," in *IEEE ICSSS*, 2020.

[6] S. H. e. a. Said, "A Comprehensive Blockchain-Based System for Educational Qualifications Verification," *IEEE Access*, 2025.

[7] D. S. Darshan and S. Vasanthakumar, "Secure and Interoperable Academic Credential Verification Using Blockchain," in *IEEE ICINVENTS*, 2025.

[8] O. S. Saleh, O. Ghazali and M. E. Rana, "Blockchain-Based Framework for Educational Certificates Verification,"*Journal of Critical Reviews*, vol. 7, no. 3, 2020.

[9] M. S. K. e. a. Shawon, "DIUcerts DApp: A Blockchain-Based Solution for Verification of Educational Certificates," in *IEEE ICCCNT*, 2021.

[10] A. Jain, "Blockchain-Based Decentralized Identity Systems in Education," *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, vol. 2, no. 4, 2024.

[11] W. Suktam, S. Lapchit and J. Supsin, "Blockchain in Education: Transforming Learning, Credentialing, and Academic Data Management," *Journal of Education and Learning Reviews*, 2024.

[12] S. S. e. a. Patil, "AlmaHub: An Engaging, Supportive Alumni-Students Interaction Platform," in *IEEE Conference*, 2023.

[13] S. D. Penugonda, K. K. Jajala and G. S., "Unibridge: Revolutionizing Alumni Engagement," in *ICPCSN*, 2025.