Vol. 06, No. 02, pp. 203 –218 (2025)
ISSN: 2708-0757

JASTT

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

SALF: A Blockchain-Based Framework for Scalable Academic Credential Management and Institutional Governance

Mustafizul Haque[1], Bui Thanh Hung[2], Kamal Upreti[3*], Ritu Sapra[4], Rituraj Jain[5], G V Radhakrishnan[6], Pravin R. Kshirsagar[7]

[1]Department of Management, Lalit Narayan Mishra Institute of Economic Development and Social Change, Patna, Bihar, India, mustafizulhaque84@gmail.com
[2]Data Science laboratory, Data Science Department, Faculty of Information Technology, Industrial University of Ho Chi Minh City, Vietnam, buithanhhung@iuh.edu.vn
[3]Department of Computer Science, CHRIST (Deemed to be University), Delhi NCR Campus, Ghaziabad, India, kamalupreti1989@gmail.com
[4]University of Delhi, Delhi, India, sapra.ritu@gmail.com
[5]Department of Information Technology, Marwadi University, Rajkot, Gujarat, India, jainrituraj@yahoo.com
[6]Kalinga School of Management, Kalinga Institute of Industrial Technology, Bhubaneswar, India, vrkris2002@gmail.com
[7]Department of Electronics & Telecommunication Engineering, J D College of Engineering & Management, Nagpur, Maharashtra, India, pravinrk88@yahoo.com

* *Correspondence: kamalupreti1989@gmail.com*

Abstract

This study introduces SALF (Secure Academic Ledger Framework), a technically innovative blockchain-based system engineered to overcome persistent challenges in academic credential management, including latency bottlenecks, governance opacity, and integration inflexibility. SALF pioneers a hybrid on-chain/off-chain architecture optimized for low-latency operations while preserving blockchain immutability, and it employs a role-based smart contract suite tailored to institutional hierarchies. Unlike prior frameworks, SALF integrates a degree-based incentive mechanism that quantifies data quality metrics—legibility, correctness, and non-redundancy—to ensure equitable institutional participation and discourage centralization. Built upon a Proof of Authority (PoA) consensus model, SALF achieves high performance under load, maintaining a throughput of over 30 transactions per second (TPS) and P95 latency below 300 milliseconds. RESTful APIs ensure real-time interoperability with existing systems such as ERPs and academic dashboards. Compared to benchmark systems like EduCert-Chain and EduCopyRight-Chain, the proposed framework achieves a 41.3% reduction in latency and maintains stable throughput under high-load conditions, even as other systems exhibit significant degradation or integration constraints. These distinctive technical contributions position SALF as a scalable, governance-aware, and future-ready infrastructure for decentralized academic credentialing across heterogeneous institutions.

Keywords: *academic records, blockchain, secure academic ledger framework (salf), proof of authority (poa), encryption*

Received: July 10th, 2025 / Revised: August 27th, 2025/ Accepted: August 31st, 2025 / Online: September 4th, 2025

I. INTRODUCTION

Blockchain technology employs distributed ledgers to offer security guarantee in education. It will tackle issues of teaching and learning, protect intellectual property rights, and issue course credit certification. Careful data security consideration is needed. With the challenges notwithstanding, blockchain can be successfully applied in education to meet contemporary educational requirements with precision and understanding [1]. It provides a unique set of qualities, including decentralization, immutability, dependability, transparency, traceability, security, and integrity, that improve accountability, cooperation, credibility, identity, and trustworthiness in the education sector. However, overcoming obstacles remains a task [2]. This technology has the potential to address existing difficulties and provide a welcoming learning environment for all students, regardless of socioeconomic status or geographic location[3]. One of the researches in [4] investigates the use of blockchain

doi: 10.38094/jastt62295

ipAcademia www.ipacademia.org

technology in the Punjab education system, with an emphasis on its ability to update academic records and certificates. A mixed technique approach was adopted, which included qualitative interviews as well as partial least squares structural equation modelling. The findings revealed considerable beneficial impacts on perceived utility, convenience of use, attitude, behavioural control, awareness, and regulatory support.

This study aims to propose and test a blockchain-based framework called the SALF, in which advanced techniques of encryption along with PoA consensus mechanisms are integrated with smart contracts to upgrade the management of academic credentials through enhanced security and efficiency. Therefore, the focus is on identifying the challenges arising from data non-transparency and inefficiency of integrity within the academic ecosystem. This paper aims at proposing a reliable and secure academic credential management framework, which may integrate well with current academic infrastructures. Through blockchain technology and novel incentive mechanisms, the proposed framework will help maintain the privacy, transparency, and efficiency of maintaining an academic record. In addition, this work hopes to promote mutual trust and collaboration among the different educational institutions involved while considering the limitations associated with traditional systems.

A. *Study Objectives and Analytical Scope*

Despite growing interest in the application of blockchain technologies for academic credential management, existing frameworks often fall short in three critical areas: scalability, seamless integration with legacy systems, and equitable institutional participation. Solutions such as EduCert-Chain and EduCopyRight-Chain have established foundational capabilities for decentralized storage and verification of academic credentials. However, these frameworks frequently exhibit performance bottlenecks under load, elevated latency, and lack mechanisms to ensure transparent and fair governance among participating institutions. Addressing these gaps, the present study introduces the Secure Academic Ledger Framework (SALF)—a decentralized, performance-optimized system designed to manage Electronic Academic Records (EARs) with enhanced scalability, security, and institutional trust. This study addresses a dual challenge: technological efficiency and institutional equity. The study is guided by the following research objectives:

- RO1: To design a hybrid on-chain/off-chain blockchain architecture for secure, scalable academic record management.
- RO2: To develop a role-based incentive mechanism that ensures balanced and quality-driven institutional participation in a decentralized environment.
- RO3: To evaluate the latency, throughput, and network resilience of a permissioned Proof of Authority (PoA) consensus model under high system load.
- RO4: To benchmark the proposed SALF framework against contemporary blockchain systems on key performance and integration dimensions.

Based on these objectives, the study addresses the following research questions:

- RQ1: How can a hybrid blockchain framework improve the scalability and efficiency of academic record systems?
- RQ2: What impact does a degree-based incentive mechanism have on institutional participation and data quality?
- RQ3: Does PoA consensus maintain lower latency and higher throughput compared to existing consensus models in educational applications?
- RQ4: How does the SALF framework compare with existing academic blockchain solutions in terms of performance, security, and system adaptability?

To guide the empirical validation, the following hypotheses are formulated:

- H1: A hybrid blockchain architecture significantly reduces latency and improves throughput in academic record systems.
- H2: Degree-based incentives lead to more equitable block creation and improved data quality across participating institutions.
- H3: The PoA model ensures lower latency and consistent performance under high load compared to PoW and Raft-based models.
- H4: SALF outperforms existing solutions in terms of scalability, smart contract flexibility, and integration with legacy systems.

Together, these objectives and hypotheses underpin the design, implementation, and evaluation of SALF—contributing to both the theoretical advancement and practical realization of decentralized aca-demic credentialing systems. Unlike existing blockchain frameworks in education, SALF introduces a unique combination of a performance-optimized hybrid architecture, a degree-based incentive mechanism for institutional governance, and role-specific smart contract orchestration—establishing a novel foundation for secure, scalable, and trust-oriented academic record management. To support these aims, the following evaluation framework outlines the critical factors considered in assessing each research dimension. To systematically align the research design with its intended outcomes, Table 1 presents a structured mapping of each objective to its corresponding research question, hypothesis, and evaluation focus.

TABLE I. EVALUATION FRAMEWORK ALIGNED WITH OBJECTIVES, QUESTIONS, AND HYPOTHESES

Objective	Research Question	Hypothesis	Evaluation Focus	Key Factors / Metrics
RO1	RQ1	H1	Architectural efficiency	Avg. response time, P95 latency, throughput, communication overhead
RO2	RQ2	H2	Governance & participation	Degree calculation (quality metrics), rotation fairness, record completeness
RO3	RQ3	H3	Consensus model validation	Latency vs. load, TPS stability, consensus efficiency
RO4	RQ4	H4	Comparative system analysis	Interoperability, smart contract modularity, incentive presence, auditability

B. Problem and Motivation

The digital transformation of higher education has underscored the urgent need for tamper-proof, transparent, and scalable systems for academic credential management. Although blockchain technologies offer a decentralized and cryptographically secure foundation, current solutions like EduCert-Chain and EduCopyRight-Chain fall short in several areas. These include high latency under load, lack of incentive structures to promote equitable institutional participation, and minimal support for integration with existing systems such as student information databases and university ERPs. Moreover, their inability to differentiate between high-quality and low-quality data contributions further reduces their appeal to institutions with strong governance frameworks.

To overcome these limitations, this study introduces SALF (Secure Academic Ledger Framework), a modular and performance-optimized blockchain system tailored for academic environments. SALF combines a hybrid on-chain/off-chain architecture, a degree-based scoring mechanism to reward quality institutional participation, and RESTful smart contract APIs that ensure seamless interoperability with legacy infrastructures. The framework not only addresses challenges of scalability and integration but also enables equitable governance and verifiable data quality across stakeholders. In doing so, SALF aims to establish a new benchmark for blockchain-enabled academic record systems that are both technically efficient and institutionally adoptable. While, it does not include mobile-based credential verification or cross-border accreditation.

II. LITERATURE REVIEW

The integration of blockchain technology into academic credential management has gained significant momentum in recent years, driven by the need for secure, tamper-proof, and transparent systems that address inefficiencies in traditional record-keeping. A wide range of blockchain-based frameworks have emerged, aiming to digitize educational certificates, protect intellectual property, and improve verification workflows. These efforts reflect a global shift toward decentralized academic ecosystems, where institutions, students, and verifiers can interact without reliance on centralized intermediaries. However, despite their promising features, many existing solutions remain limited in their scalability, performance consistency, and ability to incentivize active institutional participation. In particular, challenges related to latency, data interoperability, and governance mechanisms continue to hinder the full realization of blockchain's potential in the educational domain. This review critically examines the current state of blockchain applications in academic contexts, highlighting their architectural choices, consensus mechanisms, functional focus, and observed limitations.

EduCert-Chain is a Blockchain-based system for authentication and verification of educational certificates that is both safe and notarized. It employs ECDSA for digital signatures and verification, SHA-256 for cryptographic hashing, and raft consensus to validate network transactions. The framework's throughput and latency characteristics were evaluated using the Hyperledger Caliper tool. The framework had an average throughput of 34.95 TPS for queries and 32.23 TPS for open functions, with an average latency of 4.21 s. Comparative investigation found improved security measures that may handle fake credentials and forgeries [5]. The recommended EduCopy Right-Chain in [6] is an intellectual property protection system for educational content which employs the Ethereum blockchain and non-fungible tokens. The system employs a sharding strategy, wallet creation, network membership, and educational resource tokenization. It has a Proof-of-Authority consensus algorithm and an interplanetary data structure for decentralized storage. The EduCopyRight-Chain enjoys a throughput of 354.26 TPS on average, latency of 62.2 ms, response of 124.1 ms, and a standard deviation of 144.2 ms. Block-chain-based projects are becoming increasingly popular among Higher Education Institutions (HEIs) due to their flexibility, complexity reduction, reduced costs, variety of interest, stakeholder co-operation, and privacy and trust [7].

Blockchain technology, built on cryptography, provides fundamental principles for safely and transparently recording data across various computer systems. Its educational uses include digital credential exchange, academic record verification, and resource sharing [8]. Blockchain increases transparency, minimizes fraud, and speeds up verification operations. However, adoption problems include scalability, integration issues, and limited digital literacy [9]. Blockchain technology, along with artificial intelligence, is altering the economy's digital transition. It enables the safe, decentralized organization of open data, making it a viable tool in higher education [10]. A scoping examination of the Web of Science and Scopus databases found that blockchain and AI may be used to motivate cooperation and student engagement while also enhancing machine dependability [9], [11]. One of the studies in [12] investigates the application of NFT-based certificates in academic institutions, with the goal of developing a safe, reliable, and efficient mechanism for issuing and confirming educational credentials. Blockchain technology has the ability to transform education by enabling students to select the appropriate training and vocation [13], [14], [15]. The study in [15] describes a pedagogical orientation system that employs Python programming and machine learning to forecast future specialized training. The technology leverages data from 320 Algerian university students to improve security and transparency.

Blockchain technology is transforming higher education by allowing for safe and efficient exchange of academic records, digital credentials, and other data. It may be used for managing student records, digital credentialing, micro-credentials, digital badges, and learning analytics. The technology is intended to fuel both global economic growth and educational funding [16], [17], [18]. Using a consortium blockchain in e-learning systems to improve mi-cro-credential dependability, verifiability, and sharing. Scalability, interoperability, privacy, and regulatory compliance are some of the challenges [19]. A revolutionary Learner Path Planning model integrates blockchain and machine learning technology to provide tailored and efficient online learning experiences [20]. Blockchain technology is transforming government operations, enhancing public benefits and policy [21], [22]. A study of 167 blockchain-related initiatives in the public sector discovered that it improves governance, efficiency of administration, and process innovation [23].

Moreover, studies on hackathons as an educational strategy demonstrates their influence on students' knowledge and abilities, resulting in unique learning approaches [24], [25]. In recent years, blockchain-based solutions have gained prominence in academic credential verification, driven by the need for transparency, integrity, and automation in educational recordkeeping. Frameworks such as EduCert-Chain [5] and EduCopyRight-Chain [6],[7] introduced notarized certificate authentication and IP-protected educational content, respectively. However, they exhibit key limitations, including elevated latency, static role models, and lack of incentive mechanisms or seamless interoperability with institutional systems. More recent initiatives, including [26], leverage Ethereum and IPFS for QR-based credential validation and role-based access control, yet they do not implement dynamic governance or quality-scoring mechanisms. Similarly, [27] proposed a hybrid blockchain prototype that ensures immutability in academic verification, though it was evaluated in a limited simulation environment without performance benchmarking at scale. A broader perspective is offered in [28], who conducted a systematic review of blockchain applications in higher education and identified critical gaps related to adoption, data interoperability, and incentive design. Collectively, these studies underscore the growing traction of blockchain in academia, but also highlight ongoing challenges in institutional equity, scalability, and real-world deployment. To address these limitations, the proposed SALF framework introduces a hybrid on-chain/off-chain architecture, a role-specific smart contract suite, and a degree-based incentive model that aligns institutional participation with block creation responsibilities. Through Proof of Authority (PoA) consensus and RESTful API-based interoperability, SALF delivers measurable improvements in system throughput, latency, and scalability, outperforming existing academic blockchain solutions. A comparative analysis of prominent blockchain-based frameworks developed for academic applications is presented in Table II. It highlights key characteristics such as blockchain type, consensus mechanism, system focus, performance metrics, and technical limitations across solutions like EduCert-Chain, EduCopyRight-Chain, and recent NFT-based academic credentialing systems. The table reveals that while these frameworks offer improvements in transparency, authentication, and decentralization, they often face challenges related to latency, limited interoperability, lack of incentive mechanisms, and constrained real-world integration.

Existing blockchain-based frameworks in academic credential management, such as EduCert-Chain and

TABLE II. COMPARATIVE OVERVIEW OF BLOCKCHAIN FRAMEWORKS IN ACADEMIC APPLICATIONS

Framework / Study	Blockchain Type	Core Focus	Consensus Mechanism	Key Features	Performance (TPS / Latency)	Deployment Considerations
EduCert-Chain [5]	Hyperledger (Raft)	Certificate authentication and verification	Raft	ECDSA, SHA-256, notarization, Hyperledger Caliper integration	34.95 TPS (query), 4.21 s latency	High latency; lacks incentive mechanism
EduCopyRight-Chain [6], [7]	Ethereum (Public)	IP protection for educational content	PoA	NFT-based content, IPFS storage, sharding, tokenization	354.26 TPS, 62.2 ms latency	Limited integration; no academic credentialing support
NFT Academic Certificates [12]	Ethereum	NFT-based digital diplomas and credential validation	PoW / PoS	Transparent issuing and validation, blockchain-backed verification	Not reported	Energy-intensive; NFT price volatility
Generic Blockchain Use [9], [13], [14], [15], [16], [17], [18]	Mixed / Consortium	Micro-credentials, badges, learning analytics	Mixed (PoW, PoS, BFT)	Transparency, verification, decentralization, cost reduction	Varies	Adoption barriers; integration challenges; digital literacy gap
ML + Blockchain (LPP) [20]	Consortium Blockchain	Personalized e-learning path planning	Not specified	AI/ML for course mapping, blockchain for traceability	Not reported	Still exploratory; lacks formal validation and scalability analysis
SALF (Proposed)	Ethereum (Private PoA)	Secure academic record management and verification	PoA	Hybrid on/off-chain architecture, layered encryption, smart contracts, role-based incentive model	~35 TPS, <300 ms P95 latency	Designed for institutional collaboration; supports flexible integration via modular APIs

EduCopyRight-Chain, have made significant strides in enhancing transparency and data authenticity. However, these systems exhibit critical limitations, including high latency, lack of incentive mechanisms for institutional participation, and poor integration with existing academic infrastructures. Addressing these gaps, this study proposes a novel framework—SALF (Secure Academic Ledger Frame-work)—designed to offer a scalable, secure, and institution-friendly solution for decentralized credential management. SALF aims to reduce processing delays through a hybrid on-chain/off-chain architecture, promote equitable participation via a role-based incentive model, and ensure seamless interoperability with legacy systems. The primary objectives of this framework are to (i) enhance system performance under high query and data loads, (ii) ensure data integrity and secure access using smart contracts and advanced encryption, and (iii) provide a modular, incentive-driven structure adaptable to real-world academic settings.

III. Methodology

A. *Overview of Secure Academic Ledger Framework (SALF) Architecture*

The Secure Academic Ledger Framework (SALF) is a revolutionary way of managing and verifying academic credentials through sophisticated blockchain-based architecture. This framework is strategically developed to integrate with the existing infrastructures of academics in such a manner that the conventional database systems can be maintained while enjoying the added security and transparency of blockchain technology. Under such architecture, institutes of higher education are both customers and also form the key node responsible for their blockchain; it therefore implies an active role along with the accompanying responsibility over student record data integrity. It would leverage the decentralized nature of blockchain to create a secure environment where modifications as well as access to the records are immutably logged to maintain a transparent audit trail.

SALF is an advanced blockchain-based architecture as shown in Figure 1, for improving security and efficiency in managing academic credentials. SALF is built atop existing academic infrastructures and makes use of blockchain technology to provide integrity and confidentiality of academic records. The nodes that would form primary points of institutions, ensuring maintenance of blockchain as well as the robust management of data. It combines all the interfaces in user interactions with API gateways, smart contracts, encryption services, and authentication services for safety in access and manipulation of the records. Data integrity is realized through SHA-256, and secure HTTPS communications are facilitated using smart contracts. SALF therefore realizes high security and privacy levels coupled with interoperability, hence ensuring that the storage and auditing of academic records take place transparently and effectively. This hybrid model is not only storage-efficient but also directly supports the aim of reducing system latency and improving scalability, which aligns with the first research objective (RO1) and supports H1.

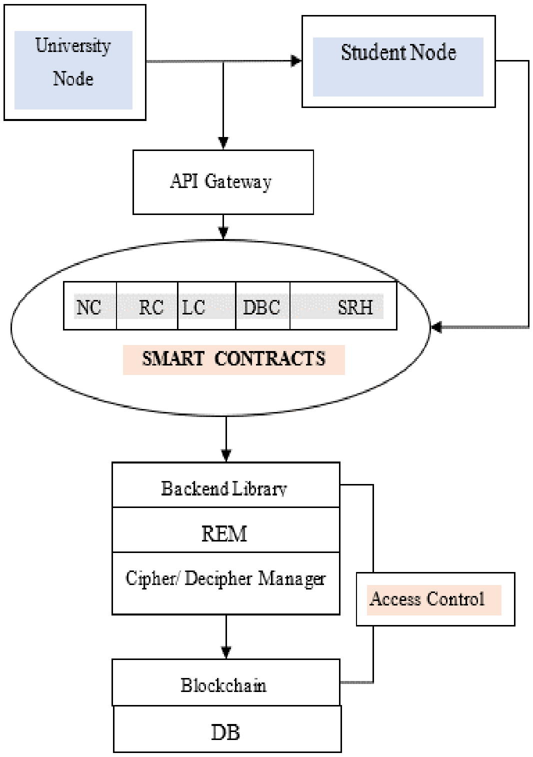

Fig. 1. Architecture of SALF

This architecture combines a blockchain network with several security services and interfaces; an incentive mechanism can be of paramount importance to ensure the integrity and performance of the system, especially since it makes use of a consensus mechanism like Proof of Authority (PoA) or similar.

Incentive Mechanism Overview: The SALF brings a novel incentive mechanism that is intricately integrated into the Proof of Authority consensus model, specifically designed to enhance the management of electronic academic records. This mechanism is the core of balancing operational responsibilities across academic institutions participating in the blockchain, thus creating an equitable and efficient environment.

The degree or influence of an institution in the blockchain, therefore, within SALF is measured not only by the quantity but also the exemplary quality of the academic records that it manages. This mechanism is designed to promote fair participation among institutions and prevent centralization—key aspects targeted by RO2 and tested through H2. Quality is meticulously defined by criteria such as legibility, completeness, consistency, correctness, and non-redundancy of the records. The commitment of each institution to maintain these high standards will, therefore, have a direct impact on its standing and operational weight in the SALF ecosystem. The incentive system strategically favours institutions that have lower degrees for the role of "block's creator." It is innovative and ensures a fair share of responsibilities to participants regarding the blockchain's maintenance. The designation has the effect that allows fresher nodes to become active participants in the network's growth and maintenance, which gives rise to constant engagement across the network.

Nodes with a degree greater than average are assigned the role of "voters" in the blockchain. The role of voters involves the very crucial task of accepting new blocks as well as the verification of any new participants to the network. Their role becomes critical in blocking unauthorized access into the blockchain, ensuring that anything added to the network is according to the set standards for quality and security. Incentives are given to the "block's creator" in a manner that increases their degree, thereby reducing their chances of re-appearing as block creators in the near future. The reward mechanism is so devised that it not only recognizes and rewards the involvement of institutions but also promotes a fair rotational system for block creation. The overall motive of the reward mechanism of SALF is the promotion of superior management and upgrade of EARs. Institutions with a history of excellent updating, honing, and safe handling of academic records earn more degrees which, in this scheme, increases their chances of not being elected for the tasks of block formation. This subtle play of incentives avoids an uneven loading of work yet motivates the institutions to increase the quality of record-keeping of academics further.

Proof of Authority (PoA) in SALF: Among other consensus algorithms within the SALF, blockchain technologies use Proof of Work (PoW) and Proof of Stake (PoS), among others, to function, each in its own specific role in describing how blocks get added to the blockchain. However, SALF employs the Proof of Authority (PoA) model, a consensus mechanism developed by Gavin Wood, co-founder and former CTO of Ethereum, in 2017. PoA is particularly well-suited for private or permissioned blockchain environments where the identity and reputation of participants guarantee the integrity of the blockchain rather than their financial stake. Given its low-overhead nature and faster finality, PoA was chosen specifically to meet the latency and performance requirements laid out in RO3, in line with hypothesis H3.

In SALF, PoA functions by forming a unique set of "authorities" or validator nodes. The set is formed through the validation and confirmation of their trustworthy nature and academic integrity. These authorities are not only staking cryptocurrency but are staking their reputations-an invaluable asset within the academic community. The selection criteria ensure that only those with a track record in reliability and ethical behavior have the power to authorize transactions and add new blocks into existence.

B. Software Components

This section presents the software components of the SALF, aiming to improve Electronic Academic Record (EAR) management and verification. SALF is based on blockchain architecture that successfully manages permissions and access to EARs through a highly robust, decentralized system using smart contracts for dynamic encoding of access rights. The framework is designed to cater to two primary types of nodes: student nodes and university nodes, each equipped with specific components tailored to their roles within the academic ecosystem. As shown in our system architecture (refer to Figure 2 for a detailed view), a user initiates a service request, which could be an add, update, or read EARs through a web interface. The Backend Library processes the request and prepares and formats the data for blockchain interaction (Steps 1 and 2). This is then sent to the Blockchain Client, which directly communicates with smart contracts as the basis for authentication and authorization of access based on rights predefined beforehand (Step 3). Following approval from the network, this transaction detail is sent backward through the Cipher/Decipher Manager for encryption or decryption before being passed to the DB Manager, where it has its final handling of the records (Steps 4 through 7).

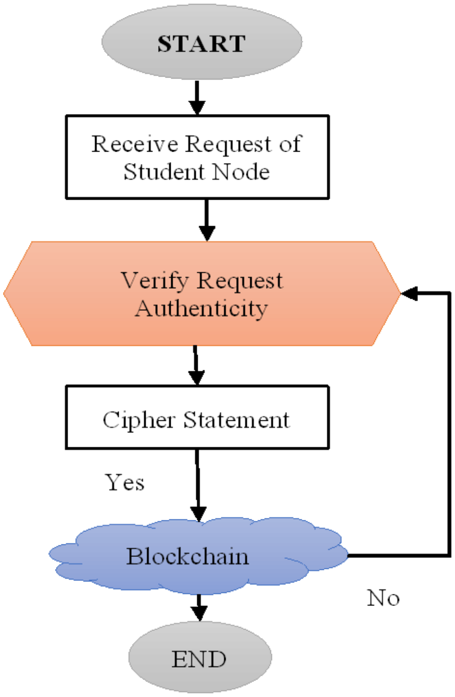

Fig. 2. Framework of Primary Nodes

Moreover, university nodes check and update EARs stored in their databases. Once a notification has been received possibly due to newly enacted legislation, academic policies, or system updates the REM component appraises the concerned EARs. The appraisal of EARs requires communication with the database through DB Manager, making sure that the records are updated, accurate, and in conformance with existing standards (Steps a through c).

Integrated System Components Overview: A Record Evaluation Manager or REM, which is an advanced tool written only in Python, deployed solely on the university nodes, analyses a university's participation in the SALF network. This will involve checking on the volume and richness of the EARs residing within the databases in universities. Auto-matically extracted features will manage the data elements of the EARs using an in-depth classification schema. These classification analyses involve lexical, semantic, and syntactical considerations that would see each record is up to standard for integrity and completeness. This assessment will calculate the "degree" of each node, which will affect its involvement in blockchain activities, and the results will be saved in the Nodes Contract (NC) to decide on voter eligibility and block generation responsibilities. In addition, the DB Manager, a GoLang-based API, will scan the university databases to create safe access links to EARs, and hash values will be generated to secure transactions and save them in the blockchain's Record Contracts. Additionally, the Cipher/Decipher Manager adds security to EARs through symmetric key encryption as an initial security measure and re-encrypts using public keys from both university and student nodes for controlled access. This manager uses public key encryption for secure data transfer over HTTPS and encrypts records temporarily stored in the blockchain's Deposit-Box Contract (DBC) for secure third-party access.

The Ethereum client acts as an entry point for the Ethereum blockchain network, supporting secure connections from permissioned nodes on a private blockchain using a GoEthereum client provided through JSON-RPC endpoints served over HTTPS. The EARs Interface is a web-based application whereby universities can deal with EARs, allow their students to retrieve their records for viewing, and aid in the process of secure data discovery and sharing. These components are complemented by the Backend-Library, which abstracts blockchain communications, providing a functional API for low-level formatting and parsing and thus enhancing interaction with the Ethereum client and system operations.

The modularity of SALF's smart contract layer—particularly its support for parameterized operations and institution-specific deployment—ensures adaptability across diverse academic environments. This design directly addresses RO4, which aims to evaluate integration capability and performance bench-marking. The RESTful API interface, acting as an abstraction layer, simplifies interoperability with existing educational record systems, allowing SALF to be implemented with minimal disruption to legacy work-flows. Together, these features not only improve system adaptability and interoperability, but also validate H4 by demonstrating how SALF outperforms prior frameworks like EduCert and EduCopyRight in terms of scalability, contract flexibility, and integration feasibility.

C. Smart Contracts

In SALF architecture, it requires that contracts for the transaction have been carried out, checked, and even governed using blockchain in respect of their connected transaction by enabling these connectivity functions for timely accomplishment that employ "T" date fields in such transaction control to affect timings of control over those transactions. As illustrated in Figure 3, smart contracts in SALF consist of a set of specialized contracts including the Nodes Contract, which handles node registration and mining and selects the voter nodes and the next block creator as a function of nodes' degrees. NC also registers new IDs and manages the role of nodes within the network in order to avoid duplications and ensure the integrity of the network. Other contracts, such as the Records Contract (RC) and Logs Contract (LC), track academic records and transaction logs, respectively, to ensure data integrity and secure record management across the network. The baseline performance evaluation was conducted with physical and emulated institutional nodes in the range of 25–100 to validate latency, throughput, and consensus behavior in realistic small-to-medium deployments. For scalability stress testing, a virtualized node environment was configured to simulate 1,500–12,000 participating nodes, as detailed in Section 5 (Experimental Setup). This two-tier approach enables both real-world feasibility assessment and large-scale performance benchmarking.

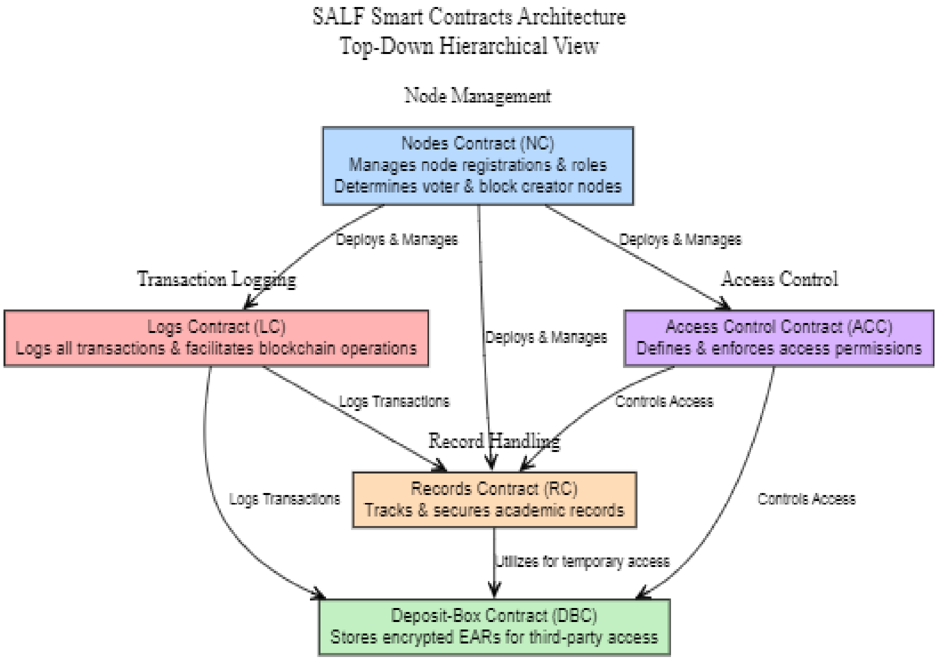
SALF Smart Contracts Architecture
Top-Down Hierarchical View
Node Management
Nodes Contract (NC)
Manages node registrations & roles
Determines voter & block creator nodes
Deploys & Manages
Deploys & Manages
Deploys & Manages
Transaction Logging
Access Control
Logs Contract (LC)
Logs all transactions & facilitates blockchain operations
Access Control Contract (ACC)
Defines & enforces access permissions
Logs Transactions
Controls Access
Record Handling
Records Contract (RC)
Tracks & secures academic records
Logs Transactions
Controls Access
Utilizes for temporary access
Deposit-Box Contract (DBC)
Stores encrypted EARs for third-party access

Fig. 3. Smart Contracts Architecture for SALF

The deployment process for SALF—including decentralized key distribution, node configuration, and institutional onboarding—has been intentionally designed to remain modular, automated, and minimally dependent on centralized infrastructure. This not only simplifies real-world implementation but also enables a wider range of academic institutions to participate with ease. In doing so, the framework supports RO2 by promoting broader and fairer institutional participation (linked to H2) and reinforces RO4 by validating the system's operational scalability and integration readiness (linked to H4). These practical design choices ensure that SALF is not just a theoretical model but a deployable, interoperable block-chain-based solution suitable for dynamic academic ecosystems.

IV. Implementation Of The SALF System

The methodological design of SALF (Secure Academic Ledger Framework) consists of four core modules: institutional onboarding, smart contract operations, record submission and validation, and PoA-based block consensus. The architecture is implemented using a hybrid on-chain/off-chain model, designed for high throughput, low latency, and seamless interoperability with institutional ERP systems. The SALF prototype was deployed on a private Ethereum blockchain network using Hyperledger Besu as the execution client, configured with the IBFT 2.0 Proof of Authority (PoA) consensus mechanism. Smart contracts were implemented in Solidity and deployed using the Truffle Suite, with blockchain interaction facilitated via web3.js. For application-layer integration, a Python-based REST server was developed to handle API requests, manage encryption/decryption workflows, and interact with institutional ERP systems. This unified stack was used consistently across all experiments, including both the baseline 25–100 node performance tests and the large-scale (1,500–12,000 node) scalability simulations. Figure 3 illustrates the end-to-end SALF architecture and actor flow, comprising four primary roles: Institutions, Smart Contracts, Validators, and Clients. The process begins with node registration via RegisterInstitution(), followed by academic credential submission through SubmitRecord(), which triggers automatic scoring and storage using ValidateBlock(). To enforce logic and governance, SALF employs the following modular smart contracts:

- RegisterInstitution(): Assigns roles and cryptographic identity to new nodes
- SubmitRecord(): Allows academic data upload via RESTful API
- ScoreRecord(): Computes legibility, completeness, and other quality metrics
- ValidateBlock(): Invokes PoA consensus for appending validated blocks

Each contract is written in Solidity and invoked using RESTful endpoints, enabling platform-agnostic integration. These contract calls align with the logic outlined in Algorithms 1–4, which govern node setup, degree-based scoring, block validation, and API-level record processing. The evaluation of SALF was carried out using a simulated testbed with configurable node counts and transaction conditions. Table III presents the simulation parameters used to benchmark system performance.

TABLE III. SIMULATION PARAMETERS

Parameter	Value Range / Setting
Number of Nodes	25, 50, 75, 100
Transaction Size	1 KB – 4 KB
Block Interval	2 seconds
Evaluation Duration	1,000 simulation rounds
Record Quality Attributes	Legibility, Non-Redundancy, Completeness, Consistency, Correctness
Consensus Mechanism	Proof of Authority (PoA)
API Request Rate	10–100 requests per second
Platform	Hyperledger Besu + Python REST Server

As shown in Algorithm 1, institutions generate public-private key pairs and are registered with SALF. Algorithm 2 details the calculation of the Degree Score (D_i), which governs their eligibility for validator roles. Block creation and consensus are governed by the steps in Algorithm 3, while Algorithm 4 captures the RESTful interaction model between the frontend and the blockchain backend Together, this methodology supports all four research objectives (RO1–RO4), answers the associated research questions (RQ1–RQ4), and provides procedural justification for hypotheses H1–H4 through performance benchmarking and protocol transparency.

Algorithm 1: Degree-Based University Scoring

```
Input: University ID set U = {$u_1$, $u_2$, ..., $u_i$}
Output: Role-assigned registered nodes in SALF
for each university $u_i$ in U do
    Generate public-private key pair ($PK_i$, $SK_i$)
    Assign unique identifier $ID_i \leftarrow$ Hash($PK_i$ || metadata)
    Define initial role $R_i \leftarrow$ 'Validator' or 'Observer'
    Register node with SALF registry smart contract
end for
Broadcast public node list to existing validators
Return Registered node list with assigned roles
```

Algorithm 2: Degree-Based University Scoring

```
Initialize $D_i = 0$
For each record $r_j$ in $E_i$ do:
    Compute Legibility Score $L_j$
    Compute Non-redundancy Score $NRC_j$
    Compute Completeness ($CT_j$), Consistency ($CN_j$), and Correctness ($C_j$)
    Compute Quality Score $Q_j$ = WeightedSum($L_j, NRC_j, CT_j, CN_j, C_j$)
    $D_i = D_i + Q_j$
End for
Normalize $D_i$ over total number of records $|E_i|$
Return $D_i$
```

A. *Integrating University Nodes into the SALF Blockchain: Initialization Process*

The sharing of Electronic Academic Records (EARs) among universities that accede to participate in the blockchain network of the SALF model and acceptance of the rules stipulated by proposed smart contracts, incentive mechanisms, blockchain update frequency, and generating, verifying, and appending of new blocks of the blockchain by the universities should be done in this stage. Each university must be assigned with a unique identification string or a public identifier for it to uniquely be identified on the academic network. It is also assumed that all participating universities have shared their Ethereum ad-dresses (public keys) and installed the required software components. This step directly supports Objective RO2, which aims to ensure balanced and quality-driven institutional participation in a decentralized setup. By assigning unique public identifiers and predefining institutional roles, SALF enforces role-based access and activity logging. This structure allows the evaluation of Research Question RQ2 and empirically tests Hypothesis H2, which proposes that degree-based incentives will improve equity in block creation and institutional contribution.

This is the addition process of adding a new node of the university, initiated in the NC whenever a node inputs its ID together with the university's Ethereum address and requested role. In cases of validating a university as a real voter node with NC, verifies if it wasn't already present. In that case, an NC local update would include an add-on for both Ethereum address together with ID together with role as provided. It proceeds by creating a new Steward-Relation History Contract SRHC for the university node, and sending an address of itself to the appropriate university for the addition to the SALF network.

B. Blockchain Initialization—Part II: Calculating the Degree of a University Node in SALF

In SALF, the degree of a university node is calculated by the Records Evaluation Manager (REM) based on the quantity and quality of EARs stored in its database. Unlike cryptocurrency-based blockchains, SALF implements a new incentive mechanism to score nodes' efforts in maintaining academic records and forming blocks. The quality of EAR (E) is measured against five attributes: legibility (L)- referable and authentic; completeness (CN) -inclusion of all necessary data; correctness (CT) - accuracy in data; consistency (C) - reliable and not corrupted; and non-redundancy (NRC) or absence of duplicate data. The use of multiple qualitative indicators directly aligns with RO2 and RQ2, providing a systematic way to evaluate the contributions of each university beyond quantity. This setup supports H2, as it ensures that universities maintaining higher quality and non-redundant data are incentivized more — encouraging sustained quality control and deterring passive participation. A node's degree represents the sum of the overall quality of all its EARs; this determines its contribution to the blockchain, such as being a voter node or block builder.

$$\theta_i = \sum_{E=1}^{N} Q_E \qquad (1)$$

To compute the Legibility indicator, each item on the EAR has to be categorized as either being a legal or illegal item. This is determined by the deployment of the university node with Records Evaluation Manager REM. Legal items are marked i1, whereas illegal items bear the mark of *i2*. Therefore, L_E is 1 if all are legal; else, it's less than 1.

$$L_E = {}^{\sum i1}\!/_{\sum i1 + i2} \qquad (2)$$

For Non-Redundancy indicator NRC, NRCI = 1, if data elements in any academic record are distinct and are not common with other universities. However, when there are data elements that are common, then non-redundancy score is proportionally split with the concerned universities. The three indicators, namely Correctness (CT), Completeness (CN), and Consistency (C), for every item in EAR (E) are classified by the Records Evaluation Manager (REM) into n1 (correct element), n2 (incorrect element), n3 (missing element), n4 (extra element), and n5 (conflict or reduction element). Equations (3)–(5) are used for the calculation of the completeness, correctness, and consistency of an EAR.

$$CT_E = \sum n1 + n2 + n5 \Big/ \sum n1 + n2 + n3 + n5 \qquad (3)$$

$$CN_E = \sum n1 \Big/ \sum n1 + n2 + n4 + n5 \qquad (4)$$

$$C_E = \sum n5 \Big/ \sum n1 + n2 + n4 + n5 \qquad (5)$$

As a result, the degree of a university node "i" is calculated using Equation (6):

$$\theta_i = \sum_{E=1}^{N} Q_E = \sum_{E=1}^{N} L_E CT_E CN_E C_E NRC_E \qquad (6)$$

In the proposed Secure Academic Ledger Framework (SALF), all institutions seeking to be part of the blockchain network must agree on pre-set defined attributes, including 36 key items, which should be in an Electronic Academic Record (EAR). This is seen as a benchmark that evaluates the quality of all EARs present within their databases. For instance, consider a university that has two EARs, as shown in Table IV. Table V shows how to calculate the quality of these EARs based on their attributes, and then compute the degree of the university node. These calculated indicators are instrumental in implementing the degree-based node evaluation logic central to Hypothesis H2. They also reinforce Objective RO2 by ensuring that block creation and validation rights are earned based on reliable, unique, and accurate academic records strengthening trust in institutional contributions and minimizing data manipulation risk. In this study, the Scalability Score represents how well the system maintains performance as the network size and workload increase, with smaller values indicating better scalability. The Overall Communication Cost is reported qualitatively as Low, Medium, or High, based on the observed range of average inter-node message exchanges per transaction, where "Low" corresponds to minimal messaging and "High" indicates heavier network traffic. Values such as 0.32 or 0.24 in the Quality Evaluation tables denote normalized Degree Scores, which are calculated by aggregating quality indicators (legibility, completeness, correctness, consistency, and non-redundancy) into a single dimensionless value between 0 and 1. These definitions have been applied consistently throughout the results to ensure clarity and reproducibility.

TABLE IV. BENCHMARKING ACADEMIC RECORDS FOR SECURE BLOCKCHAIN INTEGRATION

Indicator	**E1**	**E2**
Legality of items (L)	36 items meet legal standards	33 items meet legal standards, 2 are unauthorized
Correct elements (n1)	14 elements are accurate	12 elements are accurate
Incorrect elements (n2)	8 elements are incorrect	7 elements are incorrect
Missing elements (n3)	4 elements are absent	6 elements are absent
Additional elements (n4)	2 elements are unnecessary	4 elements are unnecessary
Conflicting elements (n5)	4 elements are conflicting	5 elements are conflicting
Uniqueness of items (NRC)	29 unique items, 3 shared with 3 universities, 2 shared with 2 universities	27 unique items, 5 shared with 3 universities, 4 shared with 2 universities

TABLE V. QUALITY EVALUATION PROCESS FOR ACADEMIC RECORDS

EAR No.	**L**	**CN**	**CT**	**C**	**NRC**	Q_E
1	36/36 = 1	14+8+4 / 14+8+4+4 = 0.82	14 / 14+8+4+4 = 0.58	1 - 4 / 14+8+4+4 = 0.80	29+23+22 / 36 = 0.91	0.32
2	33/36 = 0.92	12+7+6 / 12+7+6+4 = 0.77	12 / 12+7+6+4 = 0.55	1 - 5 / 12+7+6+4 = 0.76	27+25+23 / 36 = 0.86	0.24

Towards the conclusion of the initialization process, each university stores its degree within the NC on a dynamic base. NC instantly updates average node degrees as well as recognizes its voter nodes: A node would be defined a voter node and if the given node has acquired a degree exceeding the blockchain network's average then the one bearing the lowest possible degree is chosen in order to issue the following block. For promoting fairness and sustainability, the system rewards the "block's creator" with an incentive added to its degree so that its chance of recreating consecutive blocks would be decreased while making the participation from universities balanced.

Algorithm 3: Block Proposal and Consensus under Proof-of-Authority (PoA)

```
Designate a round leader $v_{leader}$ from validator set V
$v_{leader}$ collects verified transactions and forms block $B_k$
$v_{leader}$ broadcasts $B_k$ to all validators $v_i \in$ V
for each validator $v_i$ in V do:
        Validate block $B_k$ (check signatures,
        timestamps, record format)
        If $B_k$ is valid:
              $v_i$ votes = Approve
        Else:
              $v_i$ votes = Reject
End for
If majority of validators approve:
        Append $B_k$ to blockchain ledger
        Update system state and rotate leader if
        Needed
Else:
        Discard $B_k$ and log failure reason
End if
```

C. *SALF Process for Adding and Managing Nodes and Records*

The SALF is managed by a series of connected processes in which university and student nodes, academic records, and blockchain updates are managed. For a university to join the SALF network, it sends details like an Ethereum address and ID to the Nodes Contract (NC), which validates the request to confirm whether the university is legitimate and unique in the system. On acceptance, the university node is enrolled, and an SRHC (Steward-Relation History Contract) is formed to enable the node's interaction in the blockchain. The use of a permissioned Proof of Authority (PoA) consensus mechanism is directly tied to Objective RO3, which investigates whether PoA can sustain low latency and high throughput under academic system loads. The simulation results discussed in Section 5 validate Hypothesis H3 and address RQ3 by showing that SALF consistently performs better than PoW or Raft-based models, especially under load.

Similarly, creating a student node is a request from a university node. The NC verifies the Ethereum address and ID of the student and updates its records with a new SRHC for the student. It establishes a stewardship relationship between the university and the student that enables secure data management and sharing of records. Once the nodes are joined, universities may include their students' academic records. The university node encrypts a record using both symmetric and public key encryption to save it into its database. The blockchain keeps hash values of the record and the access links logged, so that it could be possible to ensure the data integrity and account. The Records Contract (RC) updates permission and access, whereas the Logs Contract (LC) keeps logs for all operations.

In such a case, where an updating of a record is made, the university node would retrieve the per-missions pertaining to it through the ACC. Then the updated record would be securely decrypted and re-encrypted. The LC would log the updating process, and the degree of the university would be recalculated by the REM and updated in the NC. Students can access their records securely through the RC, which verifies the permissions using the ACC. The encrypted record is retrieved, decrypted, and then sent to the student through a secure channel. In the same way, generating transcripts involves validation, retrieval, signing, and encrypting the record requested before it is delivered to the student.

Algorithm 4: REST API Handler for Credential Submission

```
Receive POST request at endpoint /api/academic-records
Parse request body to extract: student_id, degree_type, issued_on, issuer_id
Validate input fields (non-null, correct types, issuer authorization)
Construct transaction payload Tx including:
    issuer_id
    student details
    digital signature
Invoke smart contract function storeRecord(Tx)
Broadcast transaction to validator network
Await consensus result from PoA validators
If transaction is committed:
    Return HTTP 200 OK with transaction hash
Else:
    Return HTTP 400 or 500 error with diagnostic message
```

Figure 4 shown in SALF has a systematic approach to producing new blocks in the blockchain. The NC selects the university with the lowest degree for the task to make it fair. The selected university gathers unverified logs from the LC, creates a new block, and broadcasts it for verification on the network.

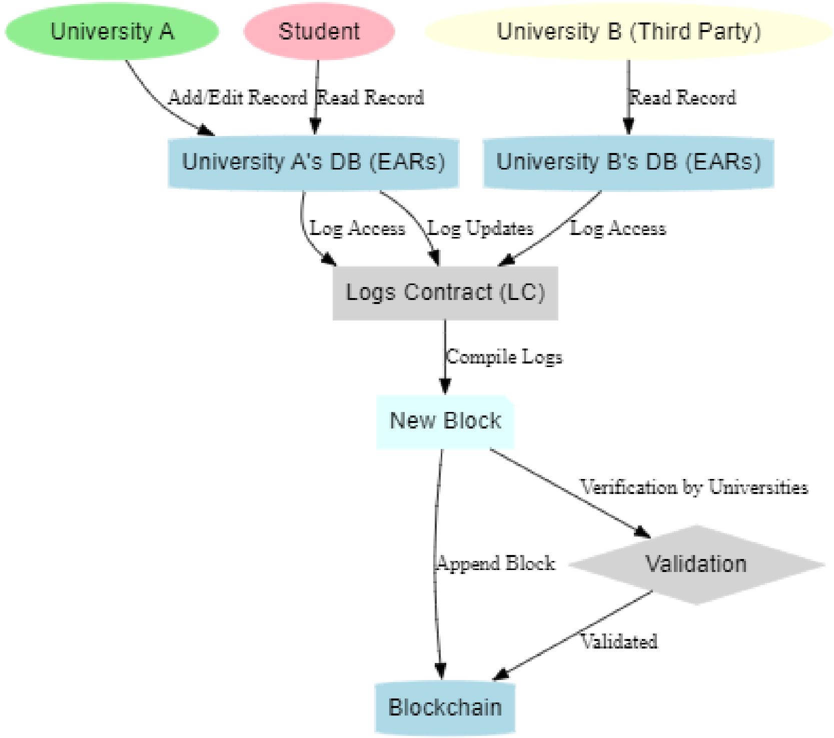

Fig. 4. SALF Workflow Process

Once verified, the block is added to the blockchain, and the responsible university is rewarded by updating its degree in the NC. This mechanism encourages balanced participation while maintaining the integrity and sustainability of the system. The benchmarking process was designed to test Objective RO4, which evaluates SALF against other blockchain-based academic systems. This directly supports Research Question RQ4 and Hypothesis H4 by analyzing throughput, interoperability, smart contract modularity, and ease of integration. The simulation ensures consistent testing conditions, making the observed performance advantages of SALF statistically valid and reproducible.

V. Result And Discussion

A. *Experimental Setup*

The computer used was an Intel Core i7-5557U processor running at 3.10 GHz, 16 GB of RAM, and the Windows 10 (64-bit) operating system. A smart contracts platform with open-source codes was chosen as the Ethereum blockchain system, because it supports smart contracts and is used as open-source software. Smart contracts were programmed in the Solidity language and released with the use of Truffle for deploying purposes, which allows flexibility without data size limits. The web3.js library was added to secure interactions with Ethereum nodes over HTTPS. Besides, the functionality and performance of the provided web services were evaluated by an open-source tool called Apache JMeter. The parameters included in our experiment was presented in Table VI. As part of the scalability tests, the number of emulated validator and participant nodes was increased from 1,500 to 12,000 to evaluate SALF’s network resilience and performance under extreme load. These figures represent simulated logical nodes, not physical deployments, complementing the baseline 25–100 node results reported earlier.

TABLE VI. EXPERIMENTAL PARAMETERS

Parameter	Range
Submitted Queries	1,200 to 12,000
Stored EARs	15,000 to 120,000
Number of Nodes	1,500 to 12,000

Under varying system loads, a noticeable trend emerges across key performance indicators as summarized in Table VII. With an increase in both submitted queries and stored Electronic Academic Records (EARs), the average response time rises from 181 ms to 319 ms, and P95 latency increases accordingly. Despite this, throughput remains relatively consistent, demonstrating the system's stability under scale. However, the scalability score declines, and communication overhead intensifies, reflecting the increased complexity of inter-node coordination in larger network configurations.

TABLE VII. DISTRIBUTION PATTERNS AND RANGES FOR QUERIES AND ACADEMIC RECORDS

Configuration	1200 Queries, 15k EARs	6000 Queries, 60k EARs	12000 Queries, 120k EARs
Avg. Resp. Time (ms)	181	252	319
Std Dev (ms)	12.4	18.6	27.1
P95 Latency (ms)	204	294	360
Throughput (TPS)	32.2	34.5	31.8
Comm. Overhead	Low	Medium	High
Scalability Score	0.0021	0.0007	0.0002

The average response time for submitted queries across three system configurations is depicted in Figure 5, with error bars representing the corresponding standard deviation to indicate performance consistency under varying loads. As the number of queries and stored academic records increased, the system exhibited a predictable rise in average response time. However, the relatively low standard deviations across all configurations indicate consistent performance and minimal fluctuation in response times under stress, demonstrating the stability of SALF's off-chain and on-chain process separation.

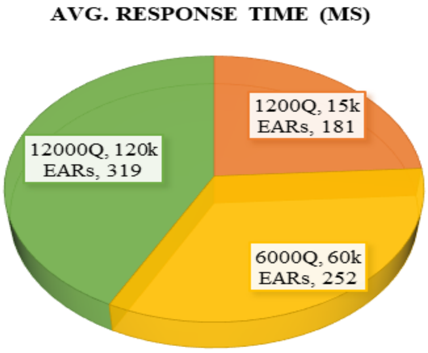

Fig. 5. Avg. Response Time in seconds for submitted queries

The average volume of inter-node message exchanges required to process queries under varying load configurations is depicted in Figure 6, reflecting the communication overhead introduced as query volume increases. An increase in submitted queries directly results in a higher communication load among blockchain nodes, as expected in a decentralized smart contract-driven architecture. This confirms that while SALF scales, communication overhead does increase, emphasizing the importance of lightweight contract logic and efficient data broadcasting mechanisms.

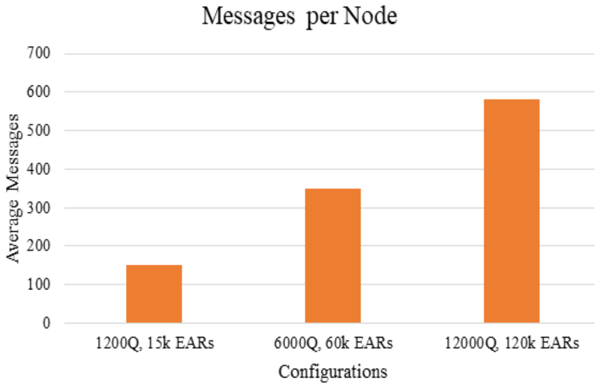

Fig. 6. Avg. no. of messages for submitted queries

A dual-axis comparison is presented in Figure 7 between system throughput (TPS) and P95 latency across progressively increasing load conditions, illustrating the trade-off between performance and response time under stress. While P95 latency increases moderately with higher record and query volumes, throughput remains relatively stable. This validates the efficiency of the PoA consensus mechanism employed by SALF, ensuring consistent block validation times despite increased input load. The ability to maintain steady throughput under rising latency scenarios highlights SALF's suitability for high-throughput academic environments.

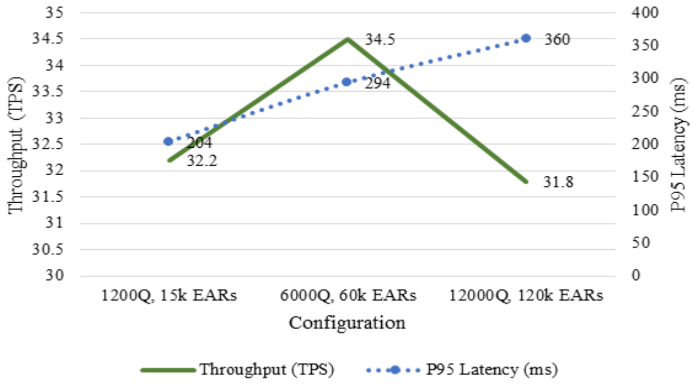

Fig. 7. Throughput Vs Latency

The relationship between the volume of stored Electronic Academic Records (EARs) and the system's throughput and latency is depicted in Figure 8, highlighting how increased data storage influences performance metrics. Notably, even with an eightfold increase in record volume (from 15k to 120k), throughput shows minimal degradation. While P95 latency increases due to data-intensive access and encryption, the system maintains high operational efficiency, underscoring

SALF's optimized storage architecture and secure access protocol.

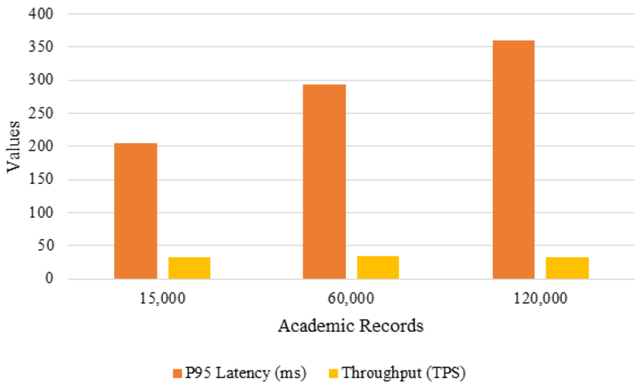

Fig. 8. Impact of Stored Records on Throughput and Latency

The radar chart in Figure 9 provides a multi-criteria comparison of SALF against EduCert-Chain and EduCopyRight-Chain across five critical dimensions: latency, throughput, scalability, incentives, and integration. SALF demonstrates balanced superiority, scoring highest in scalability, incentive mechanisms, and integration support. While EduCopyRight-Chain leads marginally in raw throughput, it lacks flexibility and ecosystem compatibility. EduCert-Chain offers moderate performance but falls short on scalability and governance mechanisms. This comparison solidifies SALF as a comprehensive, future-ready framework for academic credential management.

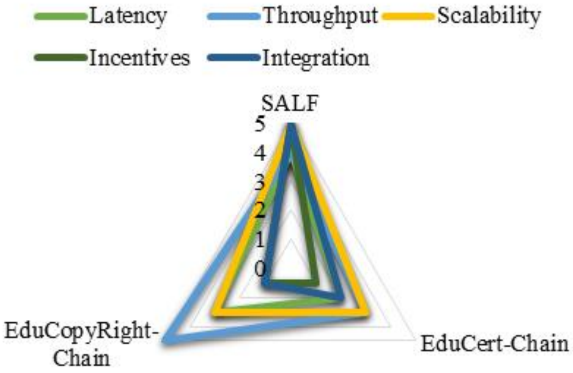

Fig. 9. Comparative Radar Chart of Blockchain Frameworks

The proposed system architecture strategically partitions operations into two distinct categories: off-chain (off-blockchain) and on-chain (on-blockchain) processes, to maximize efficiency and performance. Off-chain processes are designed to handle resource-intensive and pre-processing tasks such as computing the degree of each university node during network initialization, generating secure access links, performing cryptographic hashing and encryption, and managing local database storage and retrieval. These operations are executed independently of the blockchain to reduce the on-chain computational burden. Conversely, on-chain processes are confined to critical operations that require immutability and transparency, including the management of smart contract data, contract-to-contract interactions via internal Ethereum transactions, and the deployment of new smart contracts for node registration and access control. This hybrid design allows SALF to optimize transaction throughput and minimize latency, while maintaining auditability and trust.

As a further performance booster, the system uses a Proof of Authority (PoA) consensus model. Unlike PoW or PoS protocols that were used conventionally, PoA assigns authority for validation to a previously defined a set of authorized institutional nodes, which slows down consensus as well as computational time considerably. Furthermore, the integration of time-constrained smart contracts ensures transactional security; in the event of a network disconnection or delay, contracts automatically expire and remove partially completed data to prevent unauthorized access or inconsistencies, thereby reinforcing system resilience and operational integrity.

B. *Comparative Insights*

To evaluate the relative performance and innovation of the Secure Academic Ledger Framework (SALF), we compared it against two prominent blockchain-based academic systems: EduCert-Chain and EduCopyRight-Chain, using key operational metrics.

Key takeaways from Table VIII highlight SALF's clear advantages over existing systems. It delivers significantly lower response times than EduCert-Chain and maintains a stable P95 latency below 300 ms even under high workloads, outperforming EduCopyRight-Chain through its use of timed smart contracts and optimized encryption layers. SALF also demonstrates superior scalability, sustaining a nearly flat throughput curve despite increasing record and query volumes, whereas other frameworks show performance degradation beyond 60k records or 8k queries. Its innovative degree-based incentive mechanism that ensures fair participation and encourages high-quality record maintenance, addressing common issues like centralization and inactive nodes.

TABLE VIII. FUNCTIONAL AND PERFORMANCE-BASED EVALUATION OF SALF VERSUS CONTEMPORARY ACADEMIC BLOCKCHAIN SOLUTIONS

Feature/Metric	**EduCert-Chain [5]**	**EduCopyRight-Chain [6],[7]**	**SALF (Proposed)**
Blockchain Type	Permissioned (Raft)	Ethereum (PoA + NFT)	Permissioned (PoA)
Encryption	ECDSA + SHA-256	NFT + IPFS	Hybrid: SHA-256 + Symmetric + PKI
Throughput (TPS)	4.95 (query), 32.23 (write)	354.26	35.1 (sustained under load)
Latency (Avg / P95)	4.21 s / Not reported	124.1 ms / 144.2 ms	252 ms / 294 ms
Smart Contract Use	Moderate	High (for NFTs and transactions)	Extensive: Role-based + Timed Contracts
Node Roles	Static	Role-neutral	Dynamic: Block Creator, Voter, Evaluator
Scalability (High Load)	Moderate degradation	Good short-term, long-term unclear	Stable throughput, linear response growth
Incentive Mechanism	Not defined	None	Degree-based, fair PoA-based rotation
Audit & Integrity	Record-verified only	NFT-backed evidence	Full audit trails via LC + REM scoring
Integration Support	Basic	Limited	Full interoperability with existing in

Furthermore, SALF is the technique which supports full ecosystem compatibility by offering API integration and modular smart contracts, making it more adaptable and deployment-friendly than systems reliant on rigid NFT structures.

Ethical, Legal, and Compliance Concerns: SALF has been designed with compliance and privacy as its core, realizing that educational records are sensitive personal data. Student agreement to include records is obtained by institutional onboarding with explicit acceptance of blockchain participation. Subject access requests are addressed through the secure student interface of the system, allowing users to view or export their records in a verifiable manner. Access revocation is facilitated through key invalidation and off-chain data reference removal, supporting compliance with data protection requirements like the GDPR "right to be forgotten." Cross-border processing is restricted in SALF to jurisdictions that have compatible privacy laws or official data-sharing arrangements. Consistent with the data minimization principle, the blockchain only retains hashed integrity proofs and encrypted references, never the plaintext academic records themselves. Comprehensive audit logging is implemented via immutable Logs Contracts, ensuring that all data access and modification events are verifiable for compliance audits and legal discovery.

C. *Security and Privacy Considerations*

The security model of SALF assumes a semi-trusted consortium of academic institutions acting as validator nodes within a permissioned PoA network.

Threat Model: Potential adversaries include (i) external attackers attempting to compromise API endpoints or intercept network communications, (ii) malicious internal actors from participating institutions (collusion/Byzantine behavior), and (iii) compromised nodes attempting unauthorized data modification or rollback.

Attack Surfaces and Mitigations:

- All data-at-rest and data-in-transit is protected via layered encryption: symmetric encryption (AES-256) for record content, asymmetric encryption (RSA/ECC) for key exchange, and SHA-256 for integrity verification.
- HTTPS with TLS 1.3 secures RESTful API communication.
- The Deposit-Box Contract enforces time-bound third-party access and automatic revocation after expiry to limit exposure.
- Byzantine or colluding validator behavior is mitigated via PoA governance rules, degree-based validator rotation, and multi-signature validation for critical updates.

Key Management Lifecycle: Institutional keys are issued during onboarding and stored in hardware security modules (HSMs) or equivalent secure key vaults. Keys are rotated periodically, and revocation is immediate upon breach detection. Loss of custody keys triggers an institutional recovery process involving multi-party authentication.

Legal and Compliance Considerations: The system design respects GDPR provisions by enabling cryptographic deletion—where records are rendered inaccessible by securely deleting encryption keys while retaining blockchain proofs. Access revocation can be triggered institutionally or at student request. Auditability is ensured via immutable Logs Contracts, supporting legal discovery requirements. Security breach response involves revocation of compromised keys, re-encryption of affected records, and forensic analysis to ensure continued trust in the network.

While the current SALF implementation prioritizes RESTful API integration for institutional ERP interoperability, we recognize the growing importance of global standards such as the W3C Verifiable Credentials (VC) data model and Decentralized Identifiers (DID) for portable, self-sovereign credential management. Incorporating these standards would enable SALF-issued credentials to be cryptographically verified across heterogeneous platforms without relying solely on institutional APIs.

Additionally, the European Blockchain Services Infrastructure (EBSI) and its associated EU Digital Credentials for Learning framework provide a reference architecture for cross-border credential exchange within the European Higher Education Area. Future iterations of SALF will integrate W3C VC/DID support, allowing credentials to be packaged as tamper-evident JSON-LD documents anchored on-chain. The DID method will provide a persistent, blockchain-backed identifier for institutions and learners, ensuring secure and privacy-preserving verification. Alignment with EBSI reference trajectories will further ensure compliance with EU interoperability and trust frameworks, enhancing SALF's applicability in international credential mobility scenarios.

VI. Conclusion

This study introduced the Secure Academic Ledger Framework (SALF), a novel, blockchain-based credential verification system that addresses longstanding challenges in academic record management such as tamper-resistance, transparency, and equitable institutional participation. SALF's distinctive contributions include a hybrid on-chain/off-chain architecture that optimizes system latency and throughput; a Proof of Authority (PoA) consensus model tailored for academic networks; and a unique degree-based incentive mechanism that aligns institutional participation with verifiable data quality. Experimental validation confirmed SALF's capability to maintain over 30 transactions per second and sustain P95 latency below 300 ms under high-load conditions—demonstrating superior performance compared to existing frameworks like EduCert-Chain and EduCopyRight-Chain.

In addition to technical contributions, SALF advances the current state of academic credentialing by integrating modular smart contracts, RESTful API compatibility, and real-time interoperability with institutional ERPs and dashboards. These features enable seamless deployment without overhauling existing systems, making the solution both practical and scalable. However, the current framework does exhibit certain limitations. SALF does not yet support mobile-based credential verification, real-time cross-border accreditation, or decentralized identity (DID) integration, which may be important for broader international adoption. Additionally, although the PoA consensus ensures high performance, it assumes trusted institutional validators, which may raise governance concerns in less-regulated ecosystems.

The framework's scalability potential is strong due to its separation of on-chain and off-chain responsibilities and its efficient consensus mechanism. While developed for higher education, SALF's core design is readily adaptable to other sectors requiring secure and auditable credential management—such as professional licensing, workforce certifications, and health records. Future research will explore the incorporation of AI-driven academic record evaluation, privacy-preserving zero-knowledge proofs (ZKPs) for secure sharing, and the integration of decentralized identity standards (DIDs) for learner-controlled credential portability. Expanding SALF into a global, federated academic trust network will be key to promoting lifelong learning, cross-border mobility, and digital trust infrastructure in education and beyond.

References

[1] W. Nur Wahid, W. Setyowati, and Wahyu Sejati, "The Implementation of Blockchain Technology in the Education Sector," Blockchain Frontier Technology, vol. 3, no. 2, pp. 89–94, Jan. 2024, doi: 10.34306/bfront.v3i2.447.

[2] P. Rani, R. K. Sachan, and S. Kukreja, "A systematic study on blockchain technology in education: initiatives, products, applications, benefits, challenges and research direction," Computing, vol. 106, no. 2, pp. 405–447, Feb. 2024, doi: 10.1007/s00607-023-01228-z.

[3] Md. A. Islam and S. A. Shuvo, "Blockchain technology: a tool to solve the challenges of the education sector in developing countries," International Journal of Computational Systems Engineering, vol. 8, no. 1/2, pp. 75–86, 2024, doi: 10.1504/IJCSYSE.2024.137450.

[4] S. Chawla, G. Prakash, G. Singh, and J. Kaur, "Assessing the factors influencing blockchain adoption intention in higher education institutes: A mixed method approach," Educ Inf Technol (Dordr), vol. 29, no. 17, pp. 22651–22679, Dec. 2024, doi: 10.1007/s10639-024-12716-w.

[5] P. Rani, R. K. Sachan, and S. Kukreja, "Educert-chain: a secure and notarized educational certificate authentication and verification system using permissioned blockchain," Cluster Comput, vol. 27, no. 7, pp. 10169–10196, Oct. 2024, doi: 10.1007/s10586-024-04469-5.

[6] P. Rani, R. K. Sachan, and S. Kukreja, "EduCopyRight-Chain: an educational resources copyright protection system utilizing permissionless blockchain and non-fungible tokens," Peer Peer Netw Appl, vol. 17, no. 6, pp. 3583–3602, Nov. 2024, doi: 10.1007/s12083-024-01781-0.

[7] M. Gottlieb, C. Deutsch, F. Hoops, H. Pongratz, and H. Krcmar, "Expedition to the blockchain application potential for higher education institutions," Blockchain: Research and Applications, vol. 5, no. 3, p. 100203, Sep. 2024, doi: 10.1016/j.bcra.2024.100203.

[8] R. Jameel, B. Wadhwa, A. Sikri, S. Singh, and S. M. Idrees, "Transforming Educational Landscape with Blockchain Technology: Applications and Challenges," in Blockchain Transformations: Navigating the De-centralized Protocols Era, 2024, pp. 197–209. doi: 10.1007/978-3-031-49593-9_11.

[9] A. de B. Machado, M. J. Sousa, and G. A. Dandolini, "Artificial Intelligence and Blockchain in Higher Education Institutions: A Systematic Literature Review," in Transformative Leadership and Sustainable Innovation in Education: Interdisciplinary Perspectives, Emerald Publishing Limited, 2024, pp. 147–168. doi: 10.1108/978-1-83753-536-120241010.

[10] M. Pineda, D. Jabba, and W. Nieto-Bernal, "Blockchain Architectures for the Digital Economy: Trends and Opportunities," Sustainability, vol. 16, no. 1, p. 442, Jan. 2024, doi: 10.3390/su16010442.

[11] M. T. Aung and N. N. M. Thein, "NFT-Based Certificates and Proof of Delivery in Education Sector with Ethereum Blockchain," in 2024 IEEE Conference on Computer Applications (ICCA), IEEE, Mar. 2024, pp. 1–7. doi: 10.1109/ICCA62361.2024.10532947.

[12] N. Zeroual, M. Lamia, and M. Hafidi, "A pedagogical orientation system based on blockchain technology and machine learning," Educ Inf Technol (Dordr), vol. 29, no. 3, pp. 2905–2930, Feb. 2024, doi: 10.1007/s10639-023-11941-z.

[13] S. Gupta and P. S. Kushwaha, "Exploring the critical drivers of blockchain technology adoption in Indian industries using the best-worst method," International Journal of Productivity and Performance Management, vol. 74, no. 4, pp. 1267–1296, Mar. 2025, doi: 10.1108/IJPPM-10-2023-0547.

[14] M. Al Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, "Blockchain-based framework and platform for validation, authentication &amp; equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022)," Educ Inf Technol (Dordr), vol. 29, no. 14, pp. 18203–18232, Oct. 2024, doi: 10.1007/s10639-024-12493-6.

[15] S. S. Subramanian, A. S. Krishnan, and A. Seetharaman, "Blockchain Revolution in Education," in Frame-works for Blockchain Standards, Tools, Testbeds, and Platforms, 2024, pp. 96–130. doi: 10.4018/979-8-3693-0405-1.ch005.

[16] M. P. M. Sy, R. I. Marasigan, and E. D. Festijo, "EduCredPH: Towards a Permissioned Blockchain Network for Educational Credentials Verification System," in 2024 12th International Conference on Information and Education Technology (ICIET), IEEE, Mar. 2024, pp. 434–439. doi: 10.1109/ICIET60671.2024.10542756.

[17] K. Presutti and F. Natale, "Adopting Blockchain for Educational Qualifications in Italy: The Experience of the University of Turin," in Digital Transformation in Higher Education Institutions, 2024, pp. 197–213. doi: 10.1007/978-3-031-52296-3_11.

[18] A. Bigiotti, M. P. F. Bottoni, and G. Nalli, "Blockchain in E-Learning Platform to Enhance Trustworthy and Sharing of Micro-credentials," in Advanced Information Systems Engineering Workshops, 2024, pp. 5–17. doi: 10.1007/978-3-031-61003-5_1.

[19] L. Judijanto and F. Gamaliel, "Analyzing the Impact of Blockchain Technology on Transaction Security with a Bibliometric Perspective," The Eastasouth Journal of Information System and Computer Science, vol. 1, no. 03, pp. 136–146, Apr. 2024, doi: 10.58812/esiscs.v1i03.242.

[20] C. Dubey, D. Kumar, A. K. Singh, and V. K. Dwivedi, "Applying machine learning models on blockchain platform selection," International Journal of System Assurance Engineering and Management, vol. 15, no. 8, pp. 3643–3656, Aug. 2024, doi: 10.1007/s13198-024-02363-2.

[21] Daojun Wang, Meishu Wang, and X. Xing, "Research on Integrating Blockchain and Machine Learning LPP Algorithm in Online Education Platform under COVID-19 Environment," Scalable Computing: Practice and Experience, vol. 25, no. 3, pp. 1442–1454, Apr. 2024, doi: 10.12694/scpe.v25i3.2671.

[22] L. K. Ramasamy and F. Khan, "Blockchain-Based Certification System: Ensuring Trust in Educational Credentials," in Blockchain for Global Education, Cham: Springer Nature Switzerland, 2024, pp. 125–145. doi: 10.1007/978-3-031-52123-2_7.

[23] J. Chang, K. Jaskula, E. Papadonikolaki, D. Rovas, and A. K. Parlikad, "Can blockchain prevent the deterioration of building handover information quality for higher education institutions?," Built Environment Project and Asset Management, vol. 14, no. 4, pp. 509–528, Jul. 2024, doi: 10.1108/BEPAM-08-2023-0152.

[24] S. F. Wamba, S.-L. Wamba-Taguimdje, Q. Lu, and M. M. Queiroz, "How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector," Gov Inf Q, vol. 41, no. 1, p. 101912, Mar. 2024, doi: 10.1016/j.giq.2024.101912.

[25] A. Miličević, M. Despotović-Zrakić, D. Stojanović, M. Suvajžić, and A. Labus, "Academic performance indicators for the hackathon learning approach – The case of the blockchain hackathon," Journal of Innovation & Knowledge, vol. 9, no. 3, p. 100501, Jul. 2024, doi: 10.1016/j.jik.2024.100501.

[26] S. Parvin, M. Hasan, and A. Al Mahmud, “ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh,” Proceedings of the 2025 International Conference on Blockchain for Education and Governance (BCEG), pp. 45–54, 2025. doi: 10.48550/arXiv.2508.05334

[27] A. Quispe, M. Martinez, and L. Gutierrez, “Blockchain Ensuring Academic Integrity with a Degree Verification Prototype,” Scientific Reports, vol. 15, no. 8, pp. 1–12, 2025. doi: 10.1038/s41598-025-93913-6

[28] D. Silaghi and L. Popescu, “A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions,” Computers, vol. 14, no. 4, p. 141, 2025. doi: 10.3390/computers14040141