Natural and Applied Sciences International Journal (NASIJ)
eISSN: 2788-4619 (online)
https://ideapublishers.org/index.php/nasij
Vol. 7, No. 1 (January-December), 2026, pp. 54-77
https://doi.org/10.47264/idea.nasij/7.1.4
Original Research Article

Blockchain-based verification of academic credentials: A multi-node consensus approach using MultiChain

Khadija Sarwar*[1] | Syed Abid Ali Shah[2] | Umar Ayaz Khan[3] | Muhammad Hassan[4] | Hafzan Ul Haq[4] | Izaan Shakil[4]

1. Faculty of Computer Science and Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Swabi, Pakistan.
2. Electrical and Computer Engineering, Faculty of Engineering, University of Porto (FEUP), Portugal.
3. Institute of Computing, Kohat University of Science and Technology (KUST), Kohat, Pakistan.
4. Department of Computing, Hamdard University, Islamabad Campus, Pakistan.

* Corresponding Author Email: khadijasarwar18@gmail.com

Abstract: Forgery of academic certificates and the absence of an independent, third-party-free mechanism to verify their authenticity remain persistent problems for universities, employers, and regulatory bodies. Traditional attestation relies on physical signatures and centralized record-keeping, both of which are vulnerable to tampering, loss, and collusion. This paper presents a blockchain-based academic credential verification system built on the MultiChain platform that organizes participants into a hierarchical, permissioned network rooted at a Higher Education Commission (HEC) node, followed by university admin nodes and their respective departmental child nodes. Certificate upload requests are subjected to a 51% node-majority consensus mechanism within each university group before being permanently committed to the blockchain, ensuring that no single actor can unilaterally issue or alter a credential. A public verification portal, implemented using Flask and hosted independently of any single institution, allows any individual or organization worldwide to instantly verify a student's degree by submitting their Computerized National Identity Card (CNIC) number, without needing to contact the issuing institution. The system was implemented using Python, Flask, and MultiChain 2.0, and tested through a complete certificate lifecycle: submission, multi-node voting, consensus-based approval, and public retrieval. Results confirm that the system successfully prevents unilateral document forgery, provides tamper-evident and immutable storage of academic records, and enables one-click, lifetime-valid verification. The proposed architecture demonstrates a practical, institution-agnostic path toward eliminating credential fraud while decentralizing trust away from any single authority.

Article History

Received: 10-Feb-2026

Revised: 12-May-2026

Re-revised: 10-Jul-2026

Accepted: 11-Jul-2026

Published: 19-Jul-2026

Keywords: Blockchain, Academic credential verification, MultiChain, Certificate forgery, Consensus mechanism, Decentralized trust, Flask.

How to Cite: Sarwar, K., Shah, S. A. A., Khan, U. A., Hassan, M., Haq, H. U., & Shakil, I. (2026). Blockchain-based verification of academic credentials: A multi-node consensus approach using MultiChain. *Natural and Applied Sciences International Journal (NASIJ), 7*(1), 54-77. https://doi.org/10.47264/idea.nasij/7.1.4

1. Introduction

Blockchain is a decentralized data structure in which identical copies of a distributed ledger are maintained across multiple participating computers, referred to as nodes, rather than being controlled by a single central administrator. Data within a blockchain is organized into blocks; once a block reaches capacity, it is cryptographically linked to the preceding block, forming an immutable chain of records. A defining property of this structure is that data already committed to the chain cannot be deleted, modified, or silently updated, which gives blockchain-based systems strong guarantees of integrity, traceability, and resistance to tampering. These properties make blockchain particularly well suited to applications that require authentication, validation, and long-term verifiability of records — a category into which academic credentials naturally fall.

1.1. Motivation

Academic certificates are among the most consequential documents an individual will ever present, governing access to employment, further education, licensure, and professional mobility. Yet the mechanisms used to verify them have changed little in decades: a physical seal, a signature, or, at best, a phone call or email to the issuing institution's registrar office. Each of these mechanisms depends on trust in an intermediary and does not scale to a world in which employers, immigration authorities, and other institutions routinely need to verify credentials issued years earlier, often across national borders. Motivated by the rising incidence of credential fraud and the administrative burden that manual verification places on both issuing institutions and verifying parties, this work explores whether a decentralized, blockchain-based ledger can replace signature-based attestation with a system that is simultaneously more secure, more transparent, and more accessible — giving certificate holders direct ownership of a verifiable record while holding issuing institutions accountable for the accuracy of what they publish.

1.2. Problem Statement

Document forgery is a widespread and growing problem, and at present there is no standardized digital mechanism by which a certificate can be proven to have been issued directly by a legitimate academic institution. The prevailing practice of physical attestation is fundamentally signature-based, and a signature can be forged or issued through mutual collusion between a document holder and a corrupt official, converting an illegitimate document into one that appears legitimate on paper. Furthermore, no existing system allows a party located anywhere in the world to independently verify the validity of an academic certificate without relying on a third-party intermediary or directly contacting the issuing institution.

1.3. Aim and Objectives

The aim of this work is to design and implement a blockchain-based digital certificate verification system that stores academic records in a tamper-proof and immutable format, thereby preserving document integrity and enabling direct, intermediary-free verification. Specifically, the system is designed to:

- Establish a permissioned, hierarchical blockchain network in which a national regulatory authority (modeled here on Pakistan's Higher Education Commission,

HEC) forms the root of trust, delegating admin-level authority to individual universities.
- Require that any new certificate be approved by a majority (51%) of the relevant university's authorized nodes before it is permanently written to the chain, preventing any single compromised or malicious actor from unilaterally issuing a fraudulent record.
- Provide a publicly accessible verification portal through which any individual or organization can retrieve and confirm a certificate's authenticity by submitting only the certificate holder's national identity number (CNIC), without needing to involve the issuing institution.
- Ensure that once published, a certificate's authenticity record persists for the lifetime of the individual, remaining accessible even if the issuing institution later closes or becomes unavailable.

1.4. Paper Organization

The remainder of this paper is organized as follows. Section II reviews prior work on blockchain-based certificate and identity authentication systems and positions the proposed method relative to this literature. Section III describes the system methodology, including the node hierarchy and the consensus-based certificate approval process. Section IV presents the requirement analysis, system architecture, and technology stack. Section V reports implementation results and testing outcomes. Section VI concludes the paper and outlines directions for future work.

2. Literature Review

Blockchain-based certificate and identity authentication has attracted growing research interest over the past decade, driven largely by the same forgery and trust problems motivating this work. This section synthesizes prior efforts along six axes — foundational blockchain and consensus technology, blockchain-based authentication and credentialing architectures, security limitations of the underlying platforms, recent advances in privacy and identity binding, national and institutional case-study deployments, and broader surveys of the field — before positioning the proposed method relative to this body of work.

2.1. Foundational Blockchain and Platform Technologies

The underlying technology on which all subsequent credentialing systems depend traces back to Nakamoto's proposal of a purely peer-to-peer electronic cash system secured by proof-of-work consensus, which first demonstrated that a distributed ledger could achieve agreement among mutually untrusting parties without a central authority (Nakamoto, 2008). Ethereum extended this model with a Turing-complete virtual machine and programmable smart contracts, enabling arbitrary application logic — rather than only currency transfer — to execute deterministically across a distributed network (Buterin, 2014; Wood, 2014). For enterprise and consortium settings where full public permissionless access is undesirable, permissioned platforms such as Hyperledger Fabric (Androulaki, 2018) and MultiChain (Greenspan, 2015) were developed to give participating organizations control over network membership, data visibility, and the mining process, while retaining a shared, tamper-evident ledger. MultiChain in particular replaces open proof-of-work mining with a round-robin permissioned validation scheme among known, identifiable participants, which is the

foundation of the node-hierarchy and consensus-approval design adopted in this paper (Section III) (Greenspan, 2015). Zheng et al. provide a widely cited overview of blockchain architecture and consensus mechanisms that contextualizes these platform choices within the broader design space (Zheng, 2017).

2.2. Blockchain-Based Authentication and Credentialing Architectures

Early work in this space approached certificate and identity verification from a personal-data-ownership perspective. Zyskind et al. proposed turning a blockchain into an automated, trustless access-control manager for personal data, giving individuals rather than a central registrar control over who may access their records (Zyskind et al., 2015) — a principle later echoed throughout the credentialing literature. Building on this idea in the specific context of higher education, Turkanović et al. proposed EduCTX, a blockchain-based global credit and grading platform modeled on the European Credit Transfer and Accumulation System, in which higher-education institutions act as peers issuing verifiable academic credit tokens (Turkanović et al., 2018). Around the same period, MIT's Media Lab, in collaboration with Learning Machine, released Blockcerts, an open standard and open-source toolchain for issuing, viewing, and verifying tamper-proof academic certificates anchored to a public blockchain, which has since been piloted for issuing digital diplomas at MIT and other institutions (MIT Media Lab, 2016). Sharples and Domingue proposed a related but broader vision — the Blockchain and Kudos system — for recording educational achievement, reputation, and reward across an individual's lifelong learning record, extending the scope of blockchain credentialing beyond single degree certificates (Sharples & Domingue, 2016).

A second line of research addressed certificate authentication more directly by replacing centralized institutional databases with a decentralized ledger, explicitly targeting the collusion and forgery risks of physical attestation (Dalal et al., 2020; Charitha & Baba, 2022). Dalal et al. (2020) proposed a blockchain-based system for jointly verifying student identity and educational certificates, aiming to eliminate reliance on manual document checks, while Charitha and Baba (2022) independently developed a comparable certificate-verification system and evaluated it against the specific fraud patterns commonly seen in degree mills. A comparable architecture from the University of Birmingham's IT Innovation group demonstrated a working academic-certificate authentication pilot within a single institution (Univ. of Birmingham, 2019). Pathak et al. surveyed a broader set of such certificate-verification systems, comparing their goals and implementation trade-offs and noting that most remain single-institution proofs of concept rather than the type of inter-institutional, nationally rooted hierarchy proposed in this paper (Pathak et al., 2022). Most recently, Cardenas-Quispe and Pacheco reported a hybrid, six-node blockchain prototype implemented in Python and Docker for issuing and verifying professional academic credentials via QR-coded signatures and Byzantine consensus (Cardenas-Quispe & Pacheco, 2025) — a design philosophy methodologically close to the present work, though limited to a single simulated institution rather than the multi-university, nationally rooted hierarchy developed here. Nguyen and Lin's EduLedger similarly targets decentralized management of academic transcripts rather than terminal degree certificates, illustrating that the underlying ledger-based approach generalizes across different categories of academic records (Nguyen & Lin, 2023).

2.3. Security Limitations of the Underlying Platforms

A recurring concern across the reviewed literature is the theoretical vulnerability of blockchain

networks to a majority ("51%") attack, in which a coalition controlling a majority of validating power could approve fraudulent transactions or rewrite history. Aponte-Novoa et al. conducted an empirical mining-behavior study of 51% attacks across multiple proof-of-work networks, documenting real-world incidents and quantifying the conditions under which such attacks become economically viable (Aponte-Novoa et al., 2021), while Sayeed and Marco-Gisbert systematically assessed existing consensus-layer defenses and found that none of the evaluated protection mechanisms provide adequate protection against a determined majority attacker, arguing for new policies that do not rely solely on the longest-chain rule (Sayeed & Marco-Gisbert, 2019). Xiao et al. provide a comprehensive survey of distributed consensus protocols spanning classical Byzantine fault-tolerant algorithms through Nakamoto-style and hybrid designs, offering a systematic basis for comparing the trade-offs between throughput, fault tolerance, and attack resistance across consensus families (Xiao et al., 2020). Separately, Atzei et al. (2017) produced an early and widely cited taxonomy of Ethereum smart-contract vulnerabilities, showing that flaws at the Solidity, EVM-bytecode, and blockchain-protocol levels can each be independently exploited to steal or lock funds, underscoring that a ledger's cryptographic immutability does not by itself guarantee the correctness of the application logic built on top of it. Qu et al. (2018) and Nguyen and Dang (2018) each raise related concerns specific to credential and IoT-entity verification contexts, noting that decentralization alone does not eliminate the need for careful protocol- and application-level security engineering. Yao et al.'s (2019) PBCert system further highlights that even privacy-preserving certificate-validation schemes must explicitly defend their smart-contract logic, since a defect there can silently undermine the guarantees the blockchain layer is otherwise designed to provide.

2.4. Recent Advances in Privacy and Identity Binding

More recent work has begun to address the tension between transparency, which public verification requires, and privacy, to which certificate holders and institutions are entitled. Berrios Moya et al. recently proposed ZKBAR-V, a zero-knowledge-proof-enabled academic record verification system that uses zkEVM smart contracts and decentralized identifiers to let a verifier confirm a credential's authenticity without exposing the underlying record contents, directly addressing this transparency–privacy trade-off in a live prototype (Berrios-Moya et al., 2025). Complementary to this, Mühle et al. survey the essential architectural components of self-sovereign identity systems, distinguishing identifier-registry and claim-registry models and clarifying how blockchain-anchored identifiers can be combined with user-held credentials without requiring a central identity authority (Mühle et al., 2018) — a design pattern closely related to how the present system separates the HEC's narrow onboarding role from each university's independent certificate-issuing authority (Section III). Biometric binding has also been proposed as a complementary mechanism to tie a credential more tightly to the individual presenting it, reducing the risk of a valid but stolen or borrowed certificate being fraudulently presented by someone other than its rightful holder, though this direction remains comparatively early-stage relative to the base authentication architectures discussed above.

2.5. National and Institutional Case-Study Deployments (2023–2025)

A distinct and increasingly active strand of recent literature reports blockchain credentialing systems deployed, or piloted, at the scale of a specific country's higher-education sector rather than as single-institution demonstrations. Al Hemairy et al. describe a national blockchain platform built for the United Arab Emirates to validate, authenticate, and establish cross-institutional equivalency of academic certification, reporting system-performance results from

an operational deployment spanning multiple accredited universities (Al Hemairy et al., 2024). Fartitchou et al. (2024) present BlockMEDC, an Ethereum- and IPFS-based system for securing digital certificates across Moroccan universities, developed explicitly in alignment with that country's national digital-transformation strategy for higher education. In a similar vein, Farabi et al. (2025) introduce ShikkhaChain, a role-based Ethereum and IPFS platform for issuing, verifying, and revoking academic credentials in Bangladesh, targeting a developing-country context in which verification is reported to remain predominantly manual. Each of these national deployments independently confirms the practical viability of blockchain-based credentialing at scale, but each also adopts a single, flat issuing hierarchy per country rather than the two-tier, regulator-to-university delegation model proposed in this paper, and none reports an explicit majority-consensus safeguard governing individual certificate issuance within a participating institution.

On the augmentation side, Tan-Vo et al. (2024) recently combined blockchain-based certificate management with machine-learning fraud detection and optimistic-rollup scaling techniques, showing that anomaly-detection models can be layered on top of a blockchain ledger to flag suspicious issuance patterns before they are committed on-chain. This direction is complementary to, rather than a substitute for, the node-level consensus mechanism proposed in this paper, and represents a promising avenue for strengthening the system described in Section III (discussed further in Section VI).

2.6. Systematic Reviews of the Field

Reflecting the field's growth, Rustemi et al. recently conducted a systematic literature review of blockchain-based academic certificate verification, screening 1,744 candidate papers down to 34 directly relevant studies published between 2018 and 2022 and identifying six major research themes along with persistent gaps around practical, production-grade institutional deployment (Rustemi et al., 2023). Their findings echo the pattern observed across the individually reviewed systems above: architectural proposals and small-scale pilots are well represented, but end-to-end systems that model a full inter-institutional issuance hierarchy — from a national regulatory root, through individual university approval workflows, to public verification — remain comparatively rare.

2.7. Comparative Synthesis and Positioning of the Proposed Method

Despite differing implementations, the systems reviewed here share common underlying principles: decentralization of trust, transparency of the verification process, and automation of issuance logic through programmable rules rather than manual institutional discretion. Where they diverge most significantly is in their architectural trade-offs — some prioritize full public visibility of records to maximize ease of verification (Dalal, 2020; Charitha & Baba, 2022; Turkanović et al., 2018; MIT Media Lab, 2016), while others, such as ZKBAR-V, restrict on-chain visibility to preserve holder privacy at the cost of additional cryptographic overhead [20]. Consistent with the gap identified by Rustemi et al. (2023) and by Pathak et al. (2022), the practical, production-oriented implementation of such a system within an actual academic institution's operational workflow — spanning registrar-level record submission, multi-party institutional approval, and public-facing verification — has rarely been demonstrated end-to-end. Even the national-scale deployments reviewed above (Farabi et al., 25; Fartitchou et al., 2024; Al Hemairy, 2024), which do demonstrate real institutional adoption, uniformly rely on

a single flat issuing layer per country and do not report a majority-consensus safeguard operating within each participating university before a certificate is committed.

The method proposed in this paper is positioned to close this gap. It adopts the decentralization and transparency principles common to prior systems (Zyskind et al., 2015; Turkanović et al., 2018; MIT Media Lab, 2016), but combines them with a concrete, institution-ready workflow built on a permissioned platform explicitly designed for this purpose (Greenspan, 2015): a nationally rooted permission hierarchy (Section III) in which no single university employee can unilaterally publish a credential, a majority-consensus approval mechanism that deliberately repurposes the 51% threshold identified as a network-level vulnerability in prior consensus research (Sayeed & Marco-Gisbert, 2019; Aponte-Novoa et al., 2021, Xiao et al., 2020) as a safeguard within a single university's node group rather than across the entire network, and a public CNIC-based verification portal that requires no institutional intermediary at query time. This design directly targets the scalability, governance, and practical-deployment gaps identified across the reviewed literature, while remaining compatible with future integration of the privacy-preserving, identity-binding, and fraud-detection techniques surveyed above (Mühle et al., 2018; Berrios-Moya et al, 2025; Tan-Vo et al., 2024).

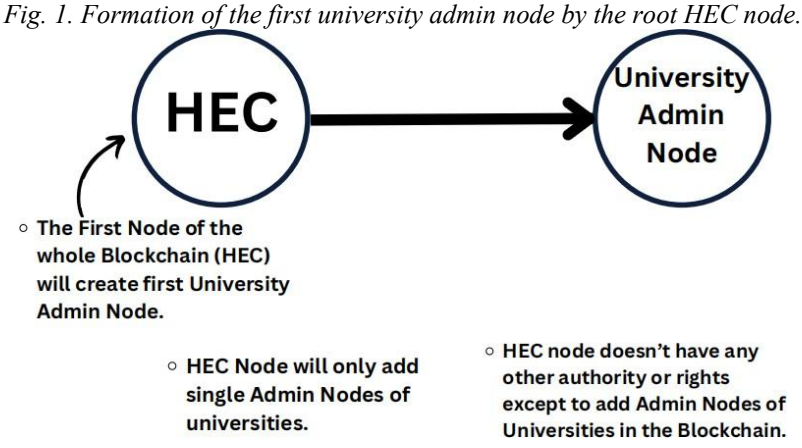
3. Methodology

The proposed system is implemented as a permissioned blockchain network using the MultiChain platform, structured as a strict hierarchy of trust that mirrors the real-world regulatory relationship between a national higher-education authority and the universities it accredits. This section describes the formation of the network, the delegation of administrative authority, the consensus mechanism used to approve new certificates, and the process by which a member of the public verifies a credential.

3.1. Network Formation and Node Hierarchy

The blockchain is seeded by a single root node, designated the HEC node, representing the national Higher Education Commission. This node is the sole entity authorized to onboard new universities into the network: for each accredited university, the HEC node creates exactly one university admin node, assigning it a unique address generated by MultiChain (Fig. 1). Critically, the HEC node's authority is deliberately narrow — beyond creating university admin nodes, it holds no further rights over any university's internal records, preventing the root authority itself from becoming a single point of failure or a vector for censorship of individual institutions.

Fig. 1. Formation of the first university admin node by the root HEC node.



Once created, each university admin node independently builds out its own private sub-network by adding child nodes corresponding to the specific university offices involved in degree issuance — for example, the registrar, admissions and examination officers, and heads of department (Fig. 2). This delegated structure allows each university to model its own internal approval workflow without requiring changes to the network's root layer, and confines any compromise of a single university's credentials to that university's own node group rather than the network at large.

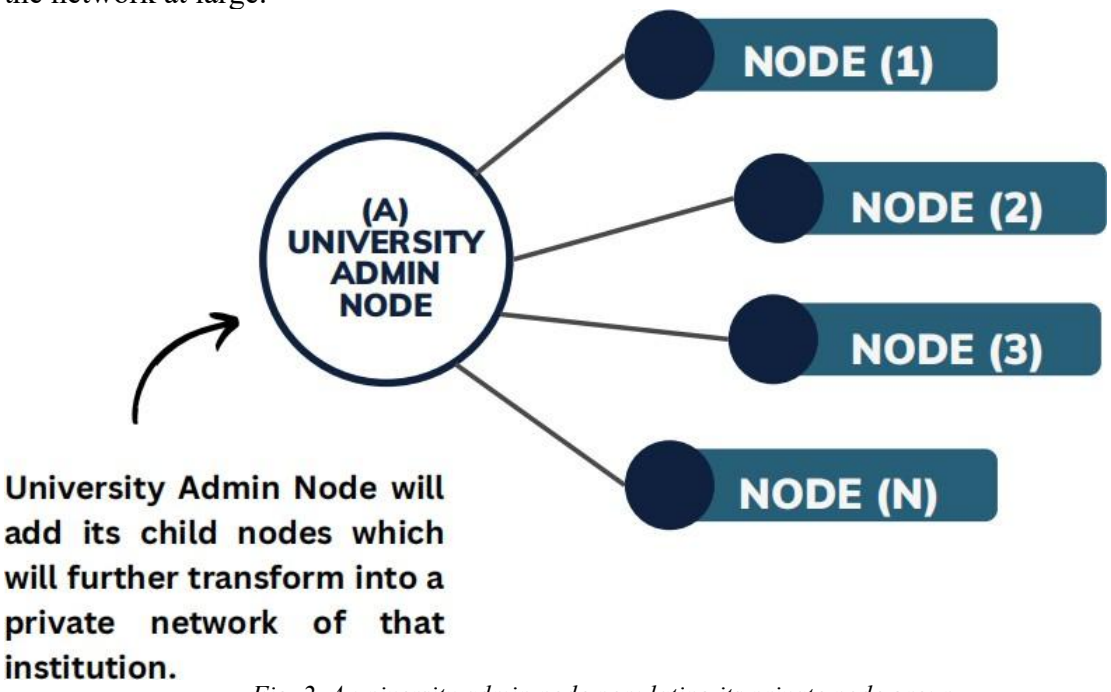


Fig. 2. A university admin node populating its private node group.

3.2. Consensus-Based Certificate Approval

Within a university's node group, any authorized child node can initiate a certificate upload request by submitting a student's academic record and supporting document through a standard web form. This request is not committed to the blockchain immediately; instead, it is broadcast to every other node in the same university group for review. Each receiving node casts a vote to either agree or disagree with the request.

A request is committed to the blockchain only once it has been accepted by a simple majority — a minimum of 51% — of the university's authorized nodes (Fig. 3). For a representative 20-node university group, this corresponds to at least 11 nodes agreeing before a certificate becomes permanent. This threshold is deliberately chosen: it is large enough that a single compromised or malicious node cannot unilaterally issue a fraudulent certificate, while remaining small enough that legitimate degree issuance is not blocked by the unavailability of a small minority of reviewers. The overall approval logic is summarized in Algorithm 1.

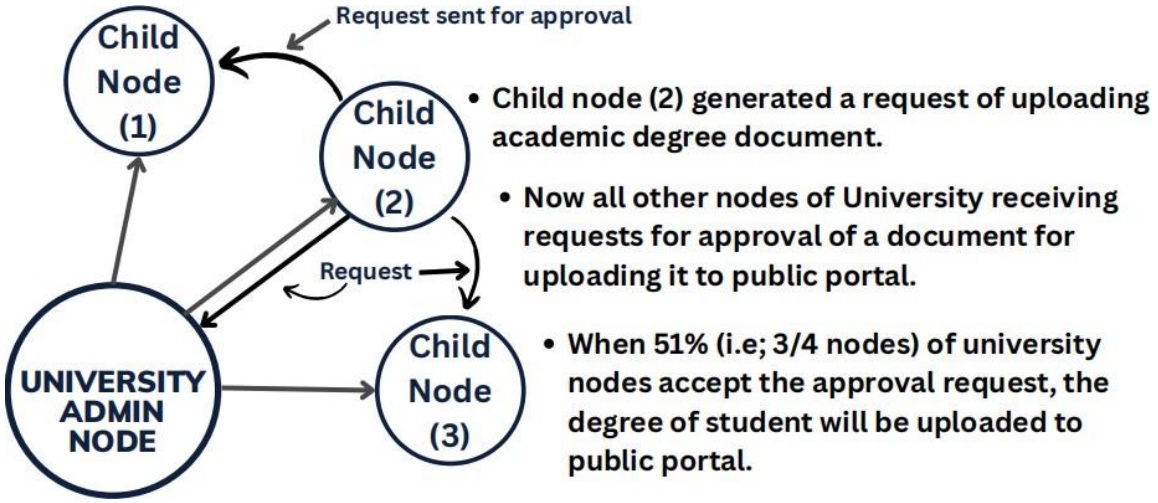


Fig. 3. Certificate upload request circulated for majority approval within a university group.

Algorithm 1: Consensus-Based Certificate Approval

```
Input: Certificate request R submitted by node n_i in university group G
1: Broadcast R to all nodes n_j in G, j != i
2: agree <- 1   // submitting node implicitly agrees
3: for each n_j in G do
4:     n_j casts vote v_j in {agree, disagree}
5:     if v_j = agree then
6:         agree <- agree + 1
7:     end if
8: end for
9: if agree / |G| >= 0.51 then
10:    Commit R permanently to the blockchain
11: else
12:    Reject R
13: end if
```

3.3. Degree Verification Process

Once 51% agreement is reached, the node that originally submitted the request performs a final confirmation action that writes the certificate — along with the student's name, CNIC, institute, degree title, and a reference to the accompanying PDF — permanently onto the blockchain. Because every participating node maintains an identical copy of the ledger, the resulting record is simultaneously replicated across the entire university group, eliminating any single authoritative copy that could be selectively altered after the fact.

3.4. Public Verification

The final stage of the methodology addresses direct verification by parties external to the issuing institution. A public-facing web portal, decoupled from any individual university's internal systems, allows any user — a recruiter, another academic institution, or a regulatory body — to query the blockchain directly by entering only the certificate holder's CNIC. The portal retrieves the matching record from the immutable ledger and displays the student's verified academic details together with the original degree document, without requiring the verifying party to contact the issuing university or rely on any intermediary (Fig. 4). Because

the underlying record can never be altered once committed, this verification remains valid for the lifetime of the individual, even if the issuing institution later ceases to exist.

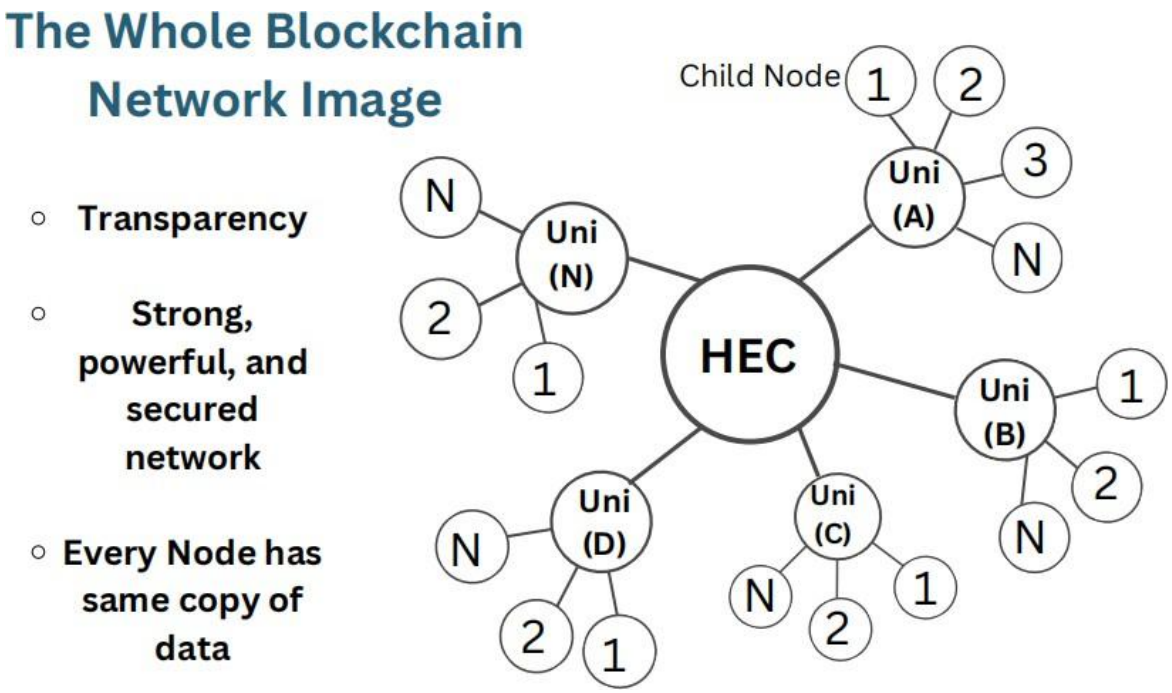


Fig. 4. Complete network topology showing the HEC root, university admin nodes, and their respective child node groups.

4. System Architecture and Design

This section describes the overall system architecture, the functional and non-functional requirements the design must satisfy, and the technology stack used to realize the system described in Section III.

4.1. System Architecture

Fig. 5 illustrates the deployed system architecture. The HEC node sits at the root of the network and is connected to a set of independent university chains, each representing a single institution's private group of admin and child nodes. A separate public node is exposed to end users; unlike the institutional nodes, it holds strictly read-only visibility into the blockchain, permitting outside parties to retrieve a certificate's verification result by CNIC without ever gaining write access to the ledger. This separation of read and write privileges is a deliberate design choice: it allows the verification portal to be hosted independently, and even scaled or mirrored across multiple public endpoints, without expanding the set of parties who can influence what gets written to the chain.

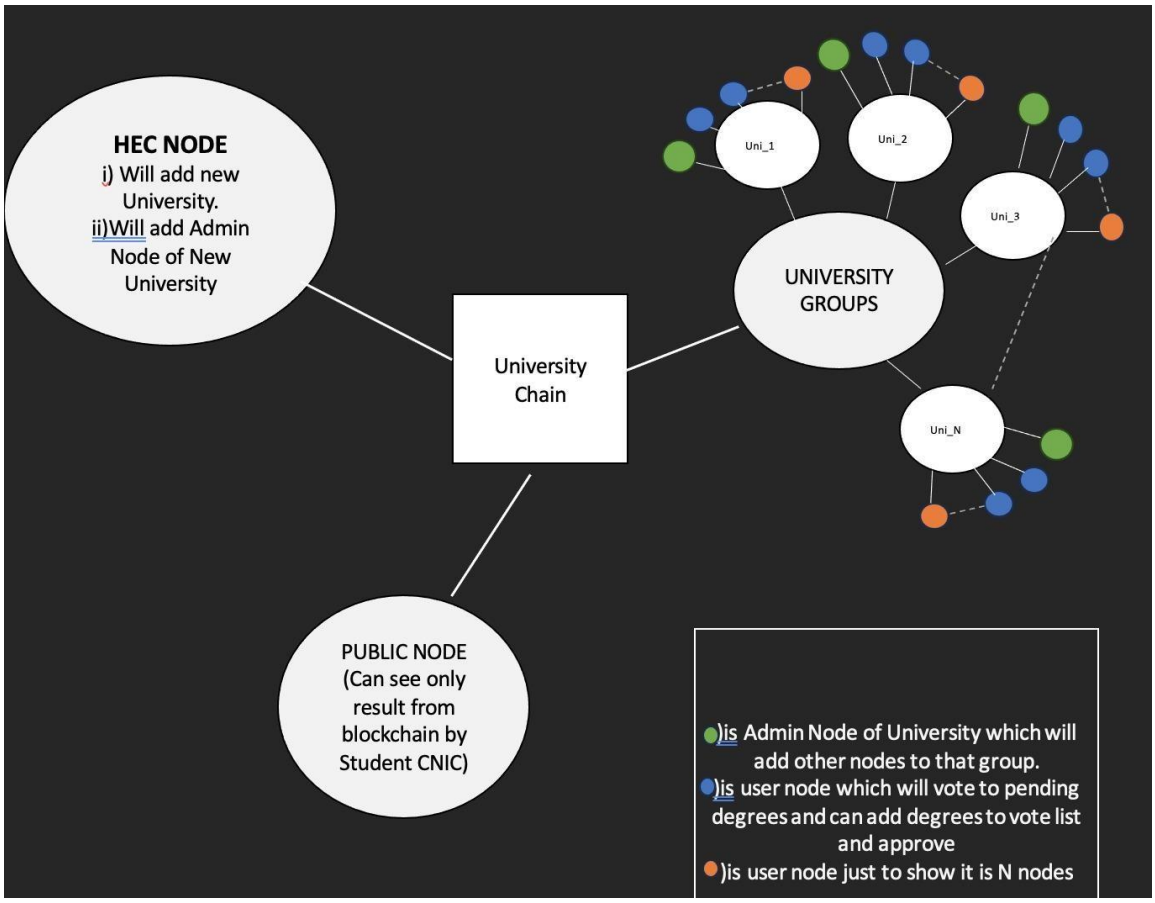


Fig. 5. Deployed system architecture showing the HEC root, university chains, and the read-only public verification node.

Two supporting views clarify how a user interacts with this architecture in practice. The use-case view (Fig. 6) shows that the public-facing surface of the system is deliberately minimal: a user submits a CNIC and receives back a rendered certificate, with all blockchain and server-side complexity hidden behind this single interaction. The workflow view (Fig. 7) traces a certificate's path end-to-end — from submission at an individual university node, through inter-university and intra-group approval routing, to storage as an approved PDF record, and finally to retrieval through the public view layer.

Fig. 6. Use-case view of end-user interaction with the public verification portal.

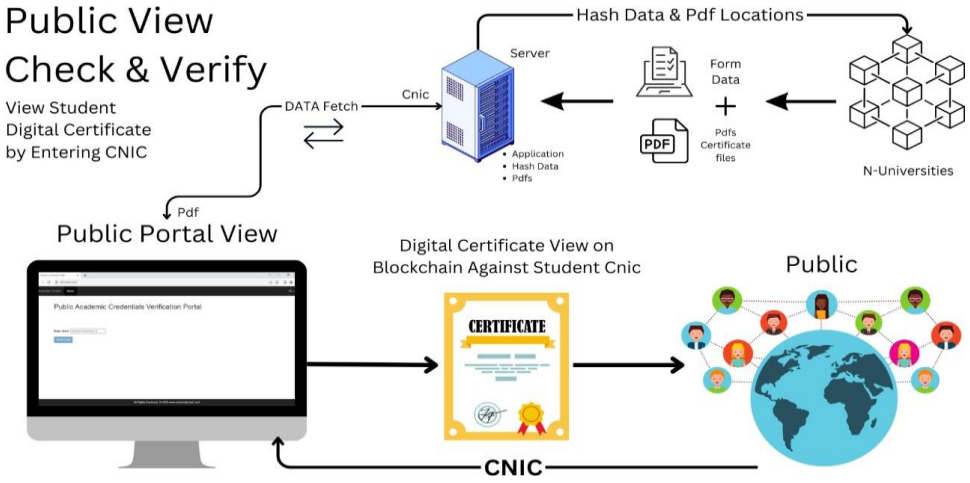
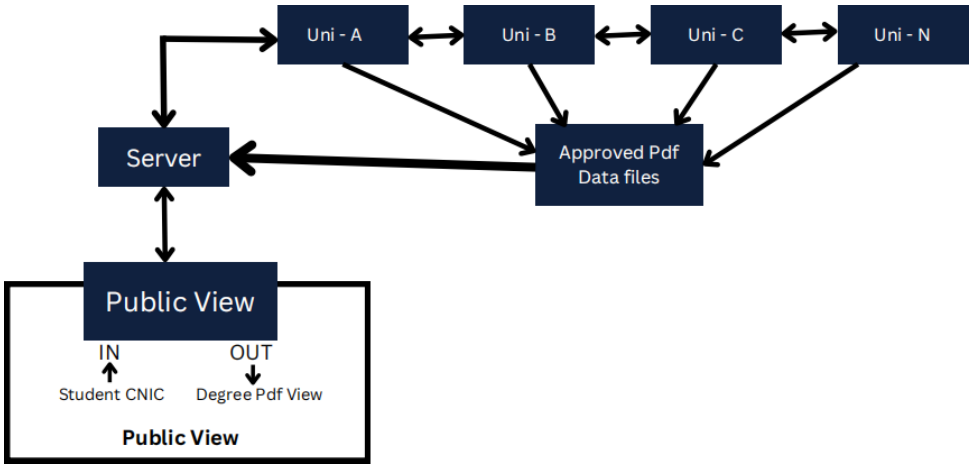


Fig. 7. Workflow of a certificate record from submission to public availability.



4.2. Functional Requirements

The system is required to support the following core functions:

- Issuing application: Handles the core certificate lifecycle — requesting, reviewing, and signing a credential referencing an academic degree. Prior to being written to the chain, the document's hash is combined into a Merkle tree, and the resulting Merkle root is submitted as part of the transaction, allowing later verification of document integrity without re-transmitting the full file.
- Verification application: Retrieves a previously issued certificate's transaction and hash data via the blockchain API and validates it against the presented document by confirming the issuing address, recomputing and matching the certificate hash, confirming presence in the Merkle tree, matching the recorded Merkle root, and checking validity/expiry status.
- Node connection management: Supports the controlled connection and disconnection of nodes from the network, consistent with the permissioned onboarding process described in Section III.

- Mining and permissioning: Designated nodes act as miners, appending validated transactions to the distributed ledger, while a permissioning layer governs which nodes may connect, issue assets, or create new blocks.

4.3. Non-Functional Requirements

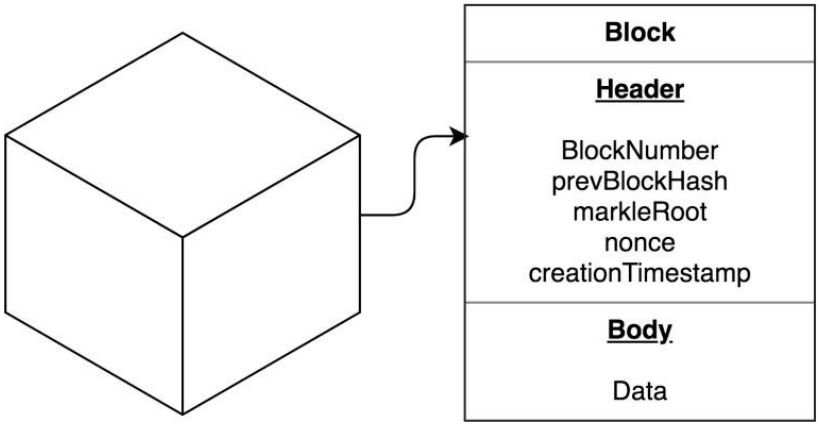
Beyond core functionality, the system is designed to satisfy the following quality attributes, each of which follows directly from the properties blockchain is expected to provide in this domain:

- Data security: Since ledger data is visible to every participating node, access and privacy controls must be maintained at the application layer even though the underlying data structure is inherently transparent.
- Immutability: Unlike ordinary digital files, which can be freely copied and altered, committed records must remain provably unchanged, with the distributed nature of the ledger itself serving as the guarantee against silent modification.
- Anonymity: Verification transactions should not expose unnecessary personal information beyond what is required to confirm a certificate's authenticity.
- Decentralized storage: Certificate data must be replicated across the network rather than held by any single centralized authority, consistent with the architecture in Fig. 5.
- Permanent availability: Records must remain accessible indefinitely, including in scenarios where the original issuing institution ceases to operate.
- Proof of activity: The system relies on an activity-verification mechanism to maintain an accurate and consistent state of the public ledger across all participating nodes.

4.4. Block Structure

Each block in the chain follows the standard structure of a header and a body (Fig. 8). The header contains the block number, a hash pointer to the previous block, the Merkle root of the certificates included in the block, a nonce, and a creation timestamp; the body holds the certificate data itself. The default block size used in this implementation is 8 MB, which was found sufficient to accommodate typical certificate metadata and associated document references without requiring block-size tuning.

Fig. 8. Structure of a single block, showing header fields and the certificate data payload.



4.5. Technology Stack

The system was implemented using the following tools and platforms:

- MultiChain 2.0 — provides the underlying permissioned blockchain, node addressing, streams, and the RPC interface used for reading and writing certificate transactions.
- Python 3.x — used to implement the backend logic connecting the web-facing forms to the MultiChain RPC API, handling both data submission and retrieval.
- Flask — a lightweight Python web framework used to serve the issuing, admin, and public verification interfaces, chosen for its minimal overhead relative to full-stack frameworks.
- HTML5 / CSS3 — used for structuring and styling the front-end forms and the public verification portal.
- Visual Studio Code — the development environment used throughout implementation and testing.

The reference deployment environment used a Core i3-class machine (or equivalent) with a minimum of 2 GB of RAM and 1 GB of available disk space, running a 64-bit Windows OS (Windows 8, 10, 11, or Server 2012 or later) — reflecting the system's intentionally lightweight resource footprint relative to typical enterprise blockchain deployments.

5. Implementation and Results

To validate that the architecture described in Sections III and IV behaves as intended, the system was implemented as a working Flask application connected to a live MultiChain network and exercised through a complete certificate lifecycle: submission, inter-node voting, consensus-based approval, on-chain commitment, and public retrieval. This section reports the test methodology used and the resulting system behavior at each stage.

5.1. Test Methodology

Testing focused on confirming that the Flask application correctly enforces the workflow defined in Section III — specifically, that a certificate cannot be committed to the blockchain without first passing through node-level review, and that once committed, it becomes reliably retrievable through the public portal. Table I summarizes the primary test case used to validate this end-to-end behavior.

TABLE I: Test Case: Certificate Submission and Blockchain Commitment

Request	Generate an upload request for a student certificate by submitting a record.
Action	Click the submit button to dispatch the request to all nodes in the university group.
Expected Result	The successfully uploaded certificate can be viewed and verified on the blockchain by entering the student's CNIC through the public portal.

5.2. Certificate Submission and Node-Level Voting

A node user initiates the process through a degree submission form requiring the student's full name, CNIC, institute, degree title, and the corresponding PDF certificate (Fig. 9). Upon submission, the request is propagated to every other node in the same university group, each of which is presented with a pending-request view offering an accept/reject vote (Fig. 10). The submitting node's own dashboard simultaneously reflects the request's pending status, allowing it to track approval progress in real time.

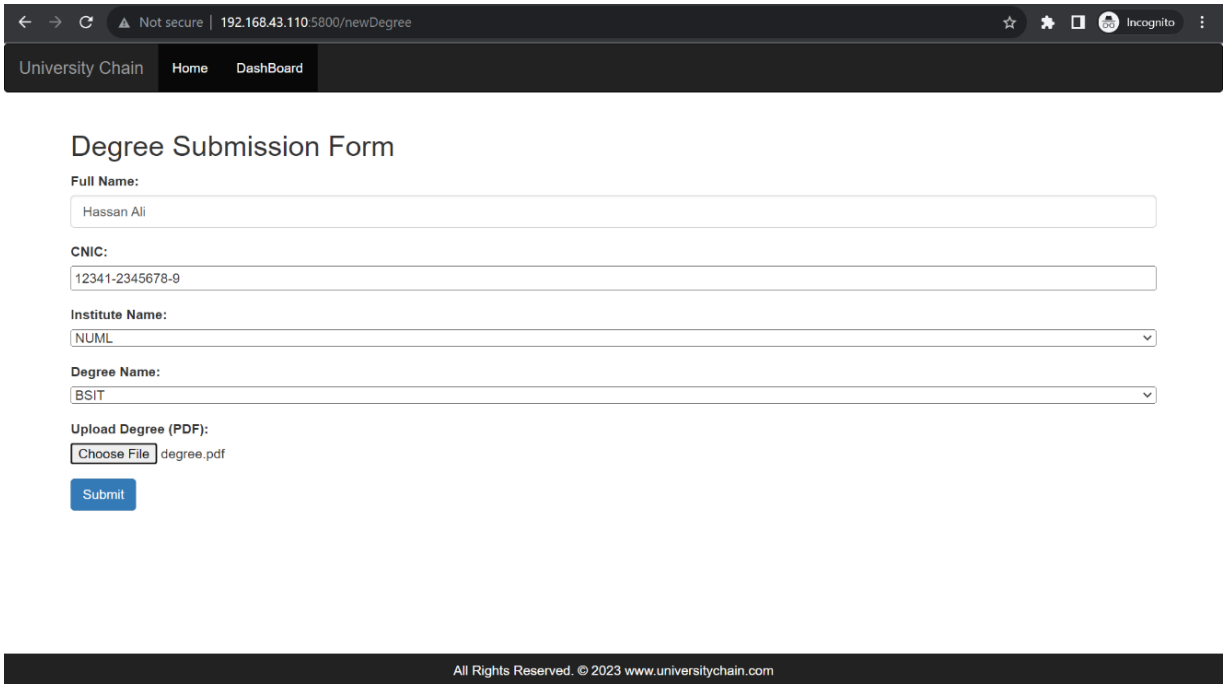


Fig. 9. Node-user interface for submitting a new certificate upload request.

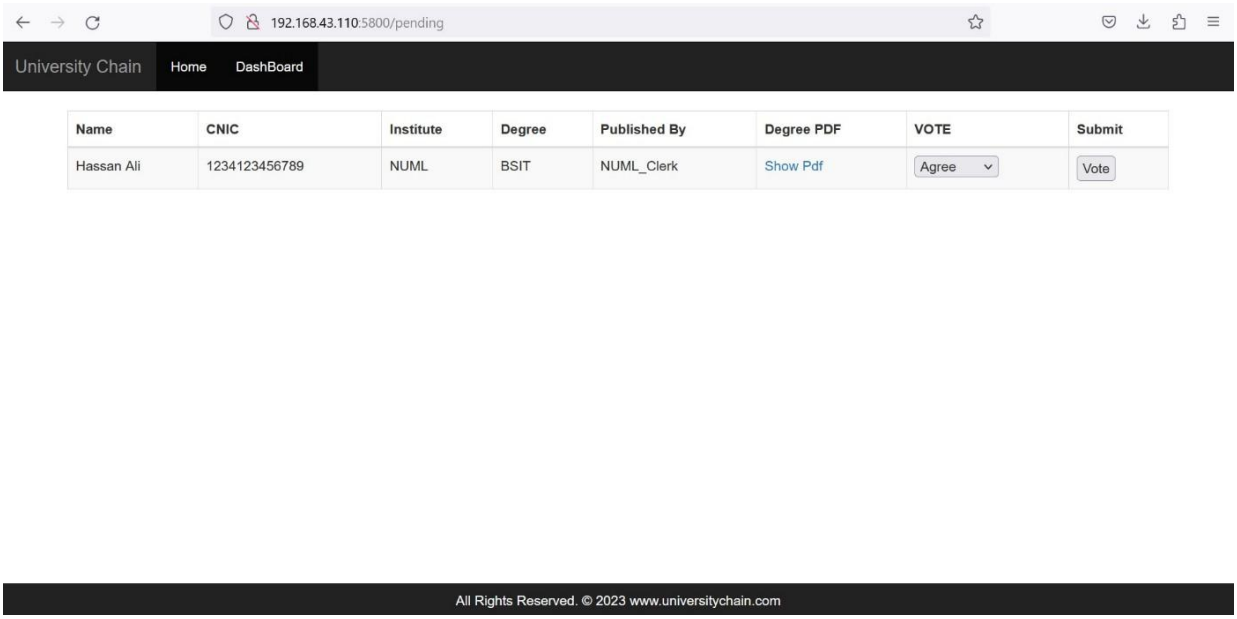


Fig. 10. A peer node reviewing and casting an agree/disagree vote on a pending certificate request.

5.3. Consensus Confirmation and On-Chain Commitment

Once the 51% agreement threshold defined in Algorithm 1 is met, the request transitions to a ready-to-approve state on the submitting node's dashboard, exposing a final confirmation control (Fig. 11). Selecting this control permanently commits the certificate to the blockchain; prior to this explicit confirmation step, the request remains reversible, giving the submitting party a final checkpoint even after majority approval has been reached.

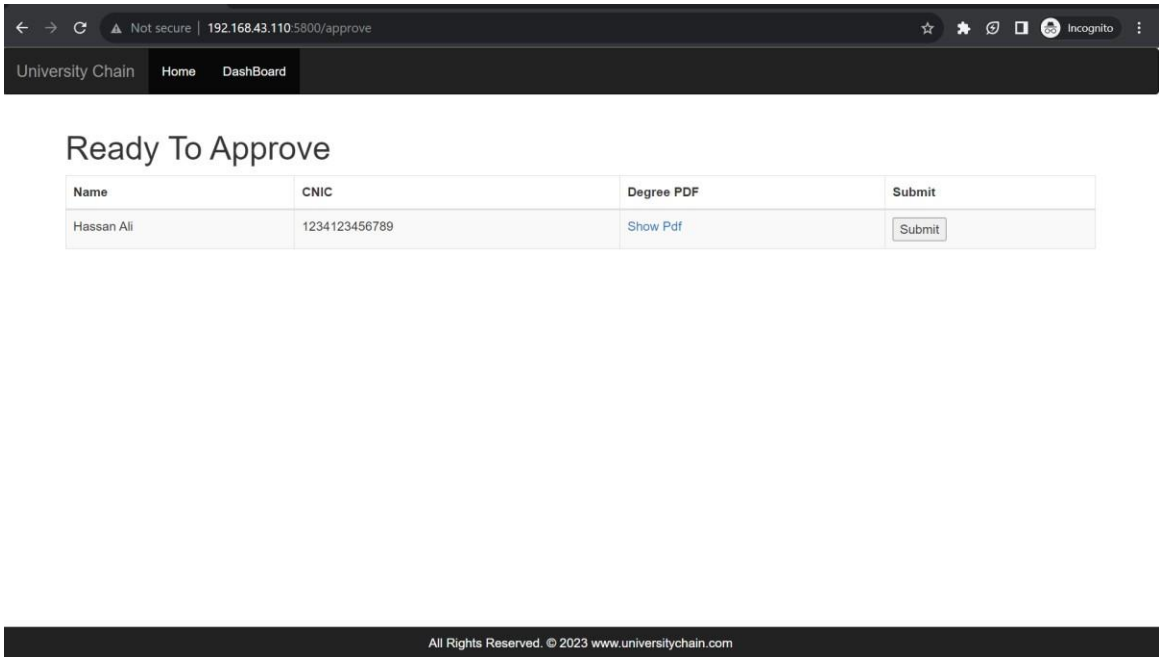


Fig. 11. Final commitment step following successful majority consensus.

5.4. Public Verification

Following commitment, the certificate becomes immediately retrievable through the public verification portal. A user enters the student's CNIC (Fig. 12) and the system returns the matched record — student name, CNIC, institute, and degree title — together with a link to view the original certificate PDF (Fig. 13). Selecting this link renders the certificate document directly in-browser (Fig. 14), completing the verification without any interaction with the issuing institution.

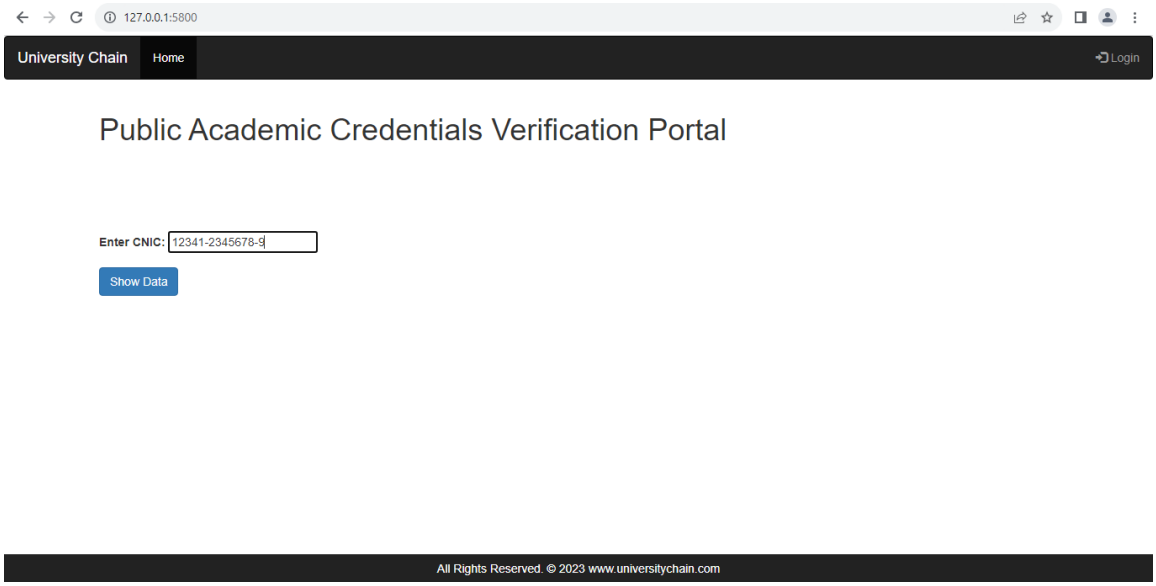


Fig. 12. Public portal accepting a CNIC query.

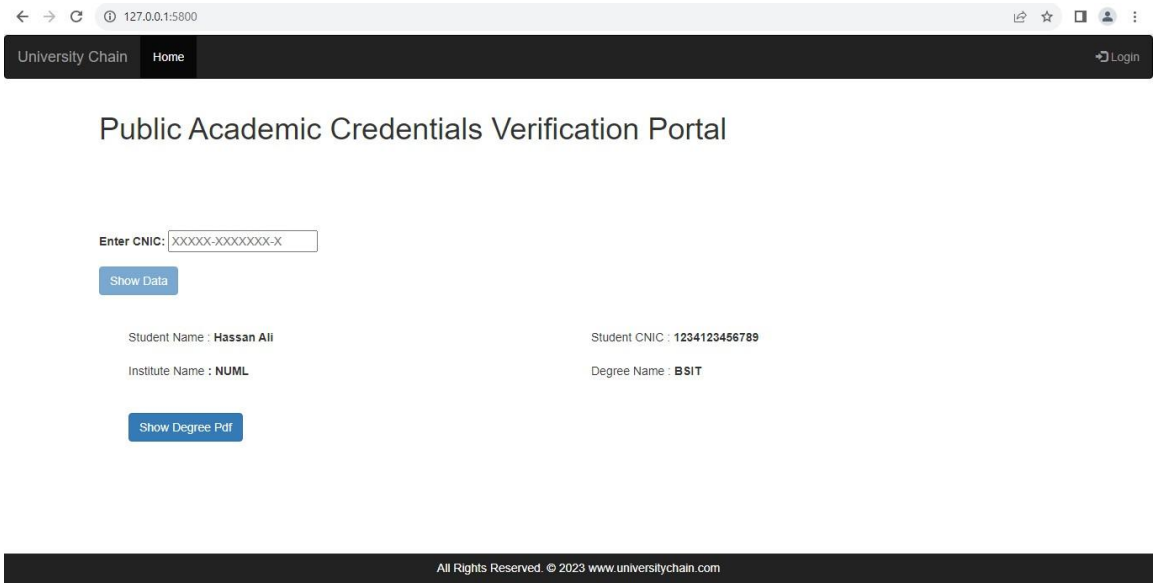


Fig. 13. Verified student record returned against the submitted CNIC.

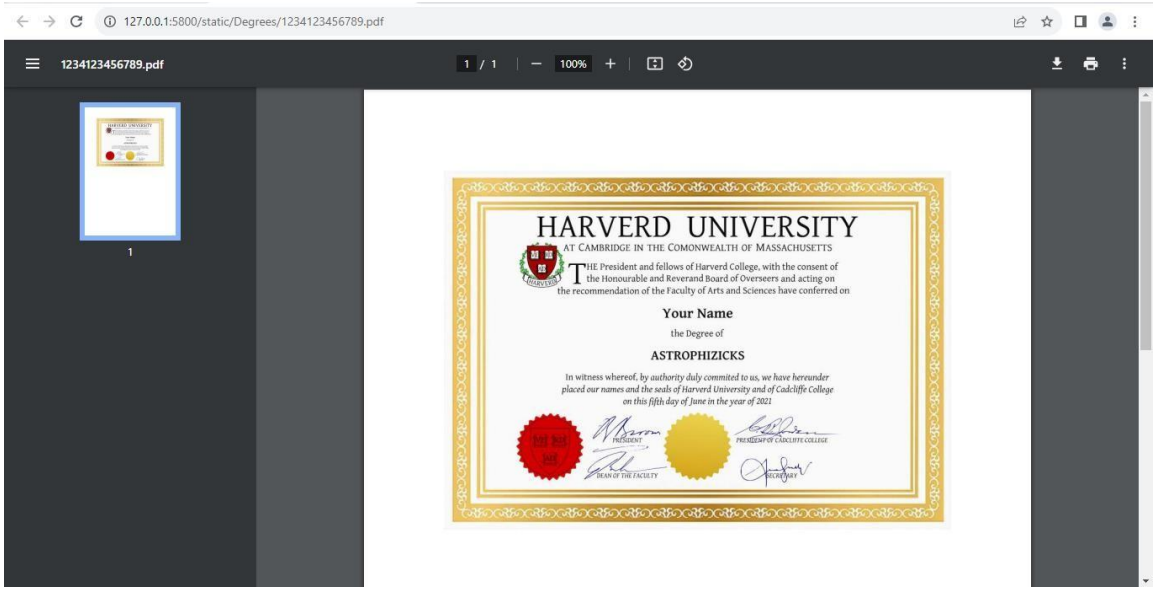


Fig. 14. Original degree certificate rendered directly from the blockchain-linked record.

5.5. Administrative Workflows

Beyond the core submission-to-verification path, the implementation supports the administrative operations required to grow the network over time: the HEC dashboard allows new universities to be registered (Fig. 15) and their admin nodes created (Fig. 16), while each university admin dashboard allows further child nodes to be added to that institution's private group (Fig. 17), and exposes the pending-request and approval queues used in the certificate workflow described above.

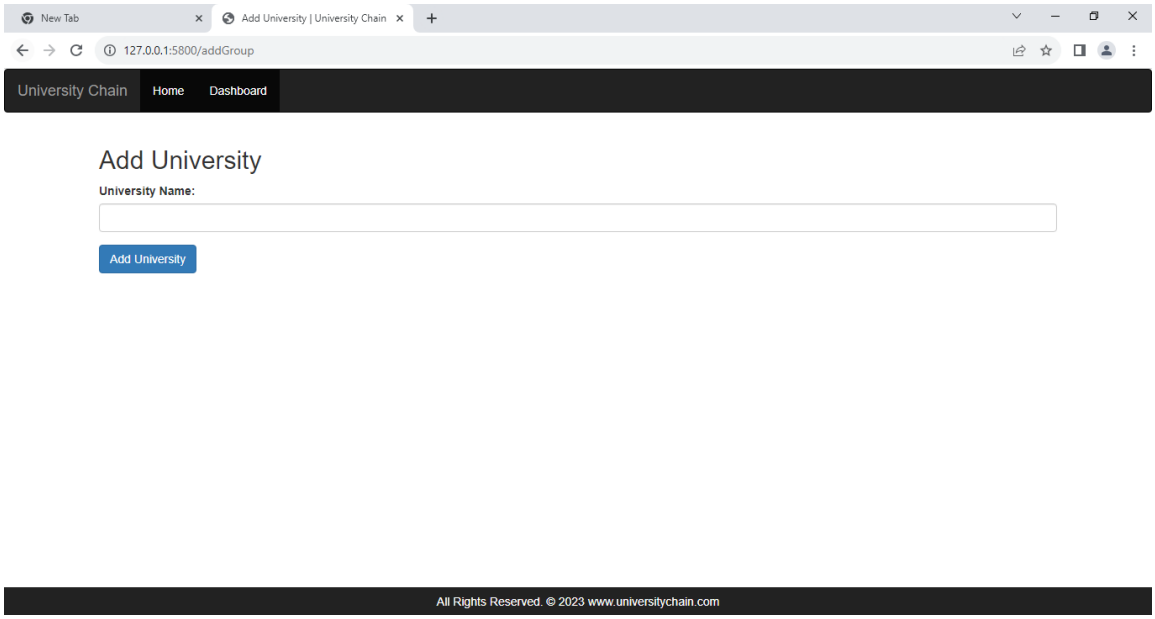


Fig. 15. HEC node registering a new university prior to admin-node creation.

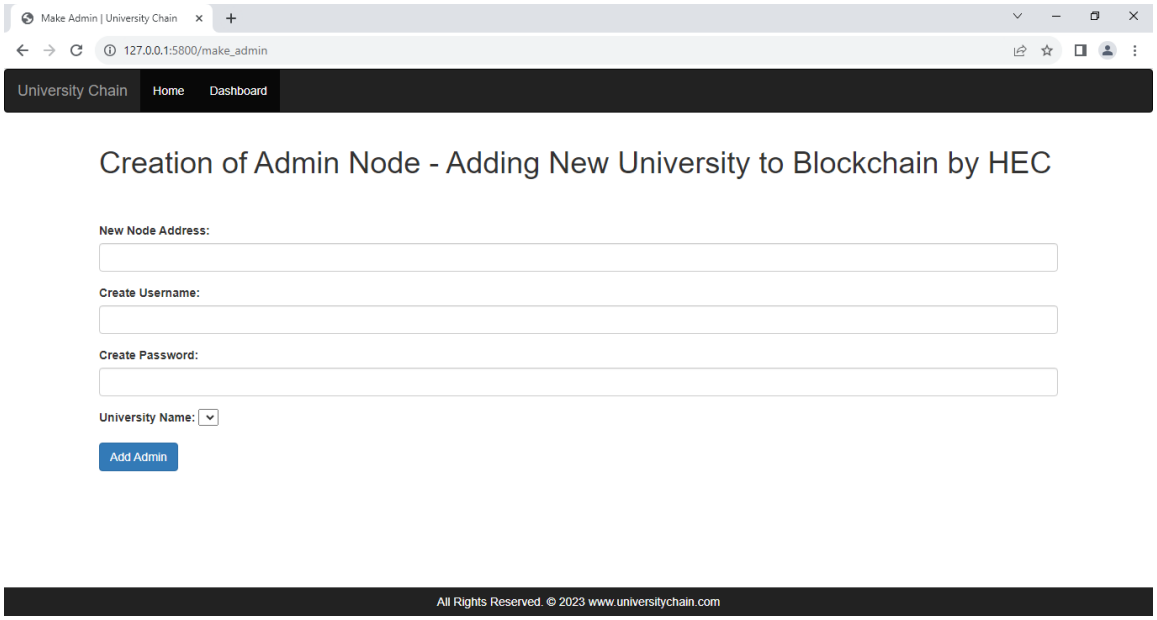


Fig. 16. HEC node creating the admin node for a newly registered university.

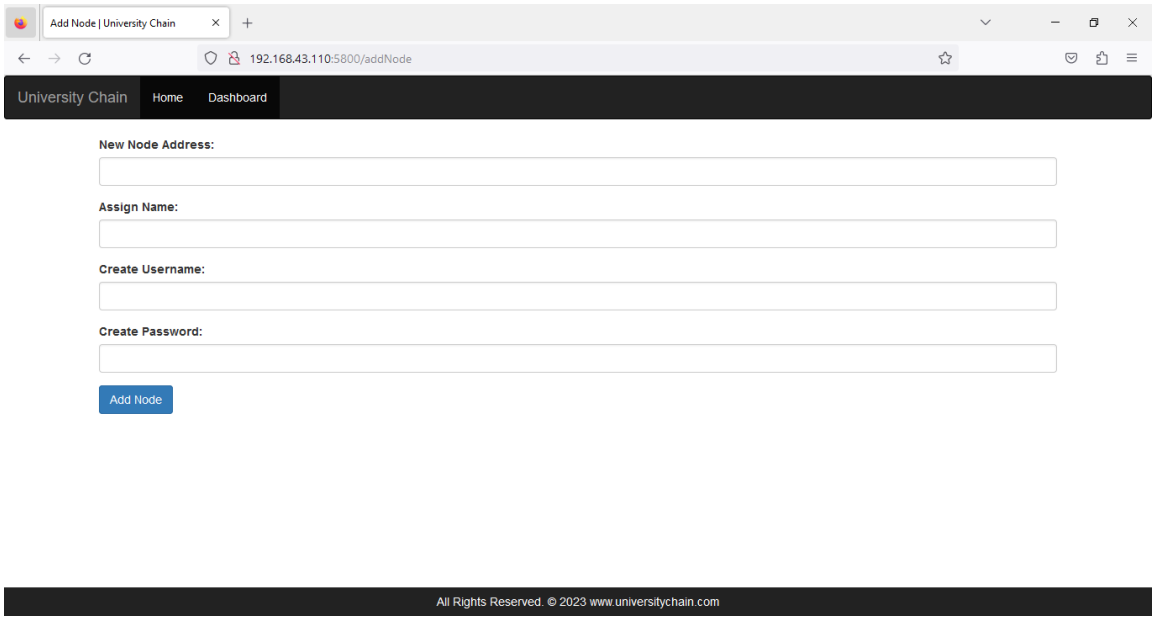


Fig. 17. University admin node adding a new child node to its private group.

5.6. Discussion of Results

Across the tested workflow, the system consistently enforced the intended invariants: no certificate became visible on the public portal without first clearing the 51% node-consensus threshold, and once committed, a certificate remained retrievable and displayed identically regardless of which node serviced the public query — confirming that the replicated ledger, rather than any single server, is the true source of truth. The separation between the ready-to-approve state and final commitment also proved useful in practice, giving the submitting node an explicit final checkpoint rather than an automatic, silent write the moment consensus was reached. These results support the core claim of this paper: that a hierarchical, consensus-gated blockchain architecture can prevent unilateral certificate forgery while still enabling fast, intermediary-free public verification.

6. Conclusion and Future Work

This paper presented a blockchain-based academic credential verification system that replaces signature-based physical attestation with a permissioned, hierarchical ledger rooted at a national regulatory authority and delegated down to individual universities and their departmental nodes. By requiring a 51% node-majority consensus before any certificate is committed to the chain, the system ensures that no single institutional actor can unilaterally issue or alter an academic record, directly addressing the collusion and forgery risks inherent in traditional attestation. The accompanying public verification portal allows any individual or organization, anywhere in the world, to confirm a certificate's authenticity in real time using only the holder's CNIC, eliminating the dependence on intermediaries or direct contact with the issuing institution that characterizes current verification practice. Implementation and testing using MultiChain, Python, and Flask confirmed that the system enforces its intended invariants end-to-end: certificates only become publicly visible after clearing node-level consensus, and once committed, they remain immutably and identically retrievable regardless of which node services the query.

Beyond academic credentials, the underlying architecture — a nationally rooted trust hierarchy combined with majority-consensus issuance — is directly extensible to other domains requiring tamper-proof, third-party-verifiable documentation, including professional licenses, government-issued identity documents, and employment records, and its adoption across these domains would further promote global mobility by allowing credentials to be recognized and verified across institutional and national borders without re-attestation. Several directions remain open for future work. Integrating zero-knowledge proofs would allow a verifier to confirm a certificate's authenticity without exposing the underlying record in full, addressing the transparency–privacy trade-off identified in Section II. Coupling the system with biometric authentication would strengthen the binding between a credential and the individual presenting it, reducing the risk of a valid certificate being misappropriated by another party. On the infrastructure side, migrating from MultiChain's default consensus and block parameters to a more throughput-optimized configuration would improve scalability as the number of participating institutions and issued certificates grows, and a formal pilot deployment within a live university registrar's office — rather than the controlled test environment used in this work — would be necessary to validate the system's usability and administrative overhead under real operating conditions. Pursuing these directions would move the system from a validated proof of concept toward a deployable, nationwide credential verification infrastructure.

Declaration of conflict of interest:

The author(s) declared no potential conflicts of interest(s) with respect to the research, authorship, and/or publication of this article.

Funding:

The author(s) received no financial support for the research, authorship and/or publication of this article.

Publisher's Note:

IDEA Publishers Group (NASIJ IDEA-PG) stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

References

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 30:1–30:15. https://doi.org/10.1145/3190508.3190538

Aponte-Novoa, F. A., Sandoval Orozco, A. L., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. *IEEE Access, 9*, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In M. Abadi & R. Kremer (Eds.), *Principles of security and trust* (Vol. 10204, pp. 164–186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8

Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system. *Sensors, 25*(11), 3450. https://doi.org/10.3390/s25113450

Buterin, V. (2014). *Ethereum: A next-generation smart contract and decentralized application platform*. Ethereum.

Cardenas-Quispe, M. A., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. *Scientific Reports, 15*, 9847. https://doi.org/10.1038/s41598-025-93913-6

Charitha, T. S., & Baba, K. A. (2022). A system for academic certificates verification using blockchain. *International Journal for Research in Applied Science & Engineering Technology, 10*(6), 3392–3397.

Dalal, J., Chaturvedi, M., Gandre, H., & Thombare, S. (2020). Verification of identity and educational certificates of students using blockchain. In *Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST)*. https://doi.org/10.2139/ssrn.3564638

Farabi, A., Khandaker, I., Ahsan, J., Shanto, I. K., Jahan, N., & Khan, M. J. (2025). *ShikkhaChain: A blockchain-powered academic credential verification system for Bangladesh* [Preprint]. arXiv. https://arxiv.org/abs/2508.05334

Fartitchou, M., Lamaakal, I., El Makkaoui, K., El Allali, Z., & Maleh, Y. (2024). *BlockMEDC: Blockchain smart contracts for securing Moroccan higher education digital certificates* [Preprint]. arXiv. https://arxiv.org/abs/2410.07258

Grech, A., & Camilleri, A. F. (2017). *Blockchain in education*. Publications Office of the European Union. https://doi.org/10.2760/60649

Greenspan, G. (2015). *MultiChain private blockchain—White paper*. Coin Sciences Ltd.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Nguyen, Q. K., & Dang, Q. V. (2018). Blockchain technology for the advancement of the future. In *Proceedings of the 4th International Conference on Green Technology and Sustainable Development (GTSD)* (pp. 483–486). IEEE. https://doi.org/10.1109/GTSD.2018.8595577

Nguyen, T., & Lin, X. (2023). EduLedger: Blockchain-based decentralized transcript management system. *Information Sciences, 644*, 119–138.

Pathak, S., Gupta, V., Malsa, N., Ghosh, A., & Shaw, R. N. (2022). Blockchain-based academic certificate verification system—A review. In *Advanced computing and intelligent technologies* (Lecture Notes in Electrical Engineering, Vol. 914). Springer. https://doi.org/10.1007/978-981-19-2980-9_42

Qu, C., Tao, M., Zhang, J., Hong, X., & Yuan, R. (2018). Blockchain based credibility verification method for IoT entities. *Security and Communication Networks, 2018*, 1–11. https://doi.org/10.1155/2018/7817614

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. *IEEE Access, 11*, 64679–64696. https://doi.org/10.1109/ACCESS.2023.3289598

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9*(9), 1788. https://doi.org/10.3390/app9091788

Sharples, M., & Domingue, J. (2016). The blockchain and Kudos: A distributed system for educational record, reputation and reward. In *Adaptive and adaptable learning* (pp. 490–496). Springer. https://doi.org/10.1007/978-3-319-45153-4_48

Tan-Vo, K., et al. (2024). Optimizing academic certificate management with blockchain and machine learning: A novel approach using optimistic rollups and fraud detection. *IEEE Access, 12*, 168135–168159.

University of Birmingham IT Innovation. (2019). *Blockchain-based academic certificate authentication system: Overview*. University of Birmingham.

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum Project.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials, 22*(2), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706

Yao, S., Chen, J., He, K., Du, R., Zhu, T., & Chen, X. (2019). PBCert: Privacy-preserving blockchain-based certificate status validation toward mass storage management. *IEEE Access, 7*, 6117–6128. https://doi.org/10.1109/ACCESS.2018.2889898

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW)* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27