SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

A Review on Recent Advancements in Blockchain Technology for Secure Electronic Certificates

Nawal A.Alragwi * and Ammar T. Zahary

Department of Information Technology, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen

*Corresponding author:nawal.alragawi@su.edu.ye

Abstract

Blockchain technology is rapidly evolving, driving advancements in various sectors, most notably in securing academic credentials against forgery. Despite the critical need for tamper-proof certificates, consensus remains limited regarding the most secure, cost-effective, and scalable issuance models. To address this gap, a systematic literature review was conducted, meticulously analyzing 24 practical blockchain-based credentialing models published between 2018 and 2024. The quantitative analysis revealed a significant platform dichotomy: 50% of the reviewed models utilize Ethereum, while 25% rely on Hyperledger Fabric. These architectural split highlights a fundamental critical trade-off between the desire for absolute decentralization and Self-Sovereign Identity (SSI) and the necessity for high operational efficiency and low transaction costs. The review concludes that the primary methodological barrier to widespread institutional adoption is the critical absence of empirical quantitative performance data (such as throughput, latency, and actual operational costs) across the current literature. Consequently, the study advocates for future research to focus on developing Hybrid Architectures that can effectively reconcile the core principles of decentralized trust with the demanding efficiency requirements of large educational bodies.

Article Info

Keywords:
Blockchain Technology, Electronic Education, Electronic Certificate, Smart Contracts, LMS, Cryptographic.

Article History:
Received: 26-September-2025,
Revised: 24-October-2025,
Accepted: 5-November-2025,
Published: 28 February 2026.

1. INTRODUCTION

The landscape of global education is undergoing profound changes, largely fueled by rapid technological innovations and the expansion of online learning environments. Virtual classrooms and digital platforms are reshaping the way knowledge is delivered, resulting in more adaptive, accessible, and learner-centered educational experiences worldwide. A central component of this transformation is the Learning Management System (LMS), which consolidates instructional delivery, course organization, and learner assessment into a single platform. Although LMSs provide considerable advantages in terms of scalability and functionality, they are also susceptible to security risks, such as unauthorized data alteration, identity misuse, and limited transparency. These vulnerabilities threaten the credibility of academic records and may weaken confidence in digital learning infrastructure. In contrast, blockchain technology offers a decentralized and tamper-resistant framework capable of addressing many of these concerns through immutable record-keeping and verifiable transactions [1].

Current LMS ecosystems encompass a wide range of solutions, from open-source platforms such as Moodle, Open edX, Open LMS, and ILIAS to large-scale providers such as Udemy, Coursera, and edX, which connect educators with global audiences. These platforms not only support instructional content delivery, but also manage student information, monitor academic progress, and issue digital certificates, thus functioning as comprehensive digital learning environments. The ultimate objective of LMS adoption is to facilitate the acquisition of knowledge and skills by both students and professionals. Validation of such competencies often occurs through digital credentials certificates or badges that require reliable verification processes. As digital education relies heavily on trust, blockchain can serve as a foundation for secure and transparent credential validation protocols

[2].

Among open-source systems, Moodle has gained prominence in academic institutions because of its adaptability across pedagogical models, such as flipped learning, project-based approaches, online instruction, and distance education. Its versatile dashboards for educators, administrators, and learners enable full-scale educational management [3]. Although the integration of blockchain into education is still nascent, research has highlighted its capacity to improve diverse areas, including the management of student funds, academic credentialing, research data storage, and academic performance monitoring. Additionally, blockchain can enable tuition payments through cryptocurrencies, such as Bitcoin, offering reduced transaction costs compared to traditional methods [4].

From a technical perspective, a blockchain operates as a distributed ledger composed of cryptographically linked records known as blocks. Each block incorporates a hash value, timestamp, and transaction information, while referencing the block that precedes it. This architecture ensures chronological order and safeguards integrity, making blockchain particularly appropriate for managing digital credentials, which remain vulnerable to forgery in both physical and electronic formats [5]. Conventional certificate validation mechanisms, such as watermarks, QR codes, serial numbers, and barcode-based systems, are increasingly undermined by modern document-editing technologies, in addition to being costly, centralized, and time-consuming. However, blockchain introduces a decentralized, automated alternative that reduces the risk of falsification while significantly improving the efficiency of the verification process [6, 7].

Blockchain-based credentialing solutions typically store certificate data securely on distributed storage systems, such as the Interplanetary File System (IPFS), while recording corresponding hash values on the blockchain. This dual process ensures authenticity, preserves integrity, and limits unauthorized access [8]. The immutable and transparent nature of blockchain further ensures that academic credentials remain accessible and verifiable. In an increasingly competitive labor market, where educational achievements hold high economic and social value, fraudulent certificates pose serious challenges. Advances in scanning, editing, and printing technologies have made fake credentials more sophisticated and more difficult to detect. Consequently, rigorous and efficient verification mechanisms have become indispensable for employers and academic institutions [9].

This study contributes to the ongoing discussions on blockchain in education by synthesizing current research and identifying emerging interdisciplinary trends. By intersecting with complementary technologies, blockchain demonstrates the potential to establish secure, efficient, and transparent frameworks for educational processes, particularly for credentials. As technology continues to evolve, its influence is expected to extend beyond verification to broader aspects of digital learning ecosystems. This review provides updated insights into the integration of blockchain in educational research, emphasizing its role at the intersection of multiple fields and its capacity to redefine the future of teaching, learning, and academic trust.

2. RESEARCH OBJECTIVES AND CONTRIBUTION

This systematic review contributes significantly to the ongoing discourse on blockchain in education by synthesizing the current research and identifying emerging interdisciplinary trends in secure electronic certificates. This study aims to establish how blockchain, when integrated with complementary technologies, can create secure, efficient, and transparent frameworks for educational processes, particularly for credentials. Furthermore, it seeks to analyze the critical platform dichotomy observed in the literature, specifically the dominance of Ethereum and Hyperledger Fabric, which highlights the fundamental trade-off between the desire for absolute decentralization (SSI) and the institutional need for high operational efficiency and low costs. The primary contribution of this study is a rigorous, systematic analysis of 24 practical credentialing models, revealing that the main methodological barrier to widespread institutional adoption is the critical absence of quantitative empirical performance data (such as throughput and cost). By providing updated insights, this study redefines the future of academic trust and calls for future work to focus on hybrid architectures that balance decentralized trust with operational demands.

3. METHODOLOGY

This review employs a structured literature-based methodology designed to examine how blockchain technology is being applied to secure and verify academic certificates. The purpose of the methodology is to ensure a focused and systematic evaluation of recent advancements, addressing both theoretical models and practical implementation. Since the abstract highlights credential verification as the core theme, the review was specifically scoped to include works that discuss blockchain-enabled Academic Certificate Authenticity Systems, rather than broad or general explorations of blockchain in education.

The review process began with a comprehensive search across academic databases, including IEEE Xplore, SpringerLink, ScienceDirect, and the ACM Digital Library. To capture the most relevant and recent developments, the search strategy employed targeted keywords such as “blockchain for academic certificates,” “secure electronic credentials,” “tamper-proof certification,” and “certificate authenticity systems.” The timeframe was limited primarily to publications between 2020 and 2025, coinciding with the period of intensified interest in blockchain adoption for educational purposes.

Articles were screened using explicit inclusion and exclusion criteria to maintain alignment with the study objectives. Studies were included if they (1) focused on blockchain-based models to verify academic credentials, (2) presented technical frameworks or implementation case studies, or (3) discussed practical challenges, such as scalability, cost, and interoperability. Conversely, papers that only provided generic overviews of blockchain technology without addressing academic certification or those that centered exclusively on unrelated domains such as finance, logistics, or healthcare were excluded unless they offered transferable insights into certificate verification.

This methodological approach ensures that the review does not merely summarize the existing literature, but also evaluates it critically to highlight both opportunities and limitations. The emphasis on authenticity, trust, and real-world applicability reflects the increasing urgency of combating certificate forgery in the higher education and professional certification contexts. By synthesizing insights from scholarly contributions and emerging implementations, this review offers a comprehensive foundation for understanding the role of blockchain in establishing secure, verifiable, and scalable systems for academic electronic certification.

4. BLOCKCHAIN TECHNOLOGY

Although blockchain technology is often linked to cryptocurrencies, its influence extends far beyond it, significantly affecting various domains of distributed applications. Key features, such as decentralized data storage across independent nodes and the use of consensus algorithms that ensure immutability and transparency, eliminate the need for a central authority, establishing blockchain as a reliable and trustworthy technology. These characteristics are closely related to the development of secure, transparent applications. Blockchain safeguards transaction data from tampering, offers a range of additional functionalities, and addresses systemic challenges. The following section provides an in-depth exploration of the fundamental concepts and nature of blockchain technology, based on a review of the existing literature. Blockchain is also known as distributed ledger technology (DLT), as the transactions among peers/nodes in a peer-to-peer network (P2P) are stored as a chain list of data structures known as blocks[68]. When a new transaction is generated, all nodes in the network participate in the block validation. A copy of this transaction at each instant is distributed, stored, and updated by each blockchain peer in the network. Altering any of the created blocks can be easily noticed by the other nodes in the network [10].

4.1. Concept, Definition

Blockchain technology was invented in 2008 and initially used to record Bitcoin transactions. It is now widely used in various nonfinancial applications [11]. Blockchain is essentially a digital ledger, often described as a "chain" of individual "blocks" of data. When new data is added to the network, a new "block" is created and connected to the chain. This necessitates all nodes to update their blockchain ledgers to be identical [12].

Table 1. Type of Blockchain technology

Aspect	Permissionless Blockchain	Permissioned Blockchain
Access Control	Open to anyone; no permission required	Restricted to authorized participants only
Transparency	Fully transparent; all data and transactions are publicly visible	Limited visibility; data is accessible only to permitted users
Consensus Mechanism	Typically uses Proof-of-Work (PoW) or Proof-of-Stake (PoS)	May use more efficient mechanisms like Practical Byzantine Fault Tolerance (PBFT)
Scalability	Generally lower due to decentralized consensus	Higher scalability due to fewer validators and optimized processes
Security Model	Relies on economic incentives and cryptography	Relies on trust between known participants and cryptographic techniques
Privacy	Low – all transactions are public	High – data can be kept private within a closed group
Typical Use Cases	Cryptocurrencies (e.g., Bitcoin, Ethereum)	Enterprise solutions (e.g., supply chain, banking, healthcare)

Blockchain technology organizes data into blocks that are secured using unique encryption algorithms to ensure privacy and security. These blocks are linked in a mesh topology to create a chain. Blockchain provides various services for managing credentials and ensures their issuance on blocks with the trust of all parties involved (institutions, learners, and third parties) [7]. Blockchain technology combines peer-to-peer protocols, hashing algorithms, and cryptographic primitives such as public-key cryptography and distributed consensus methods [13]. The blockchain architecture provides essential features such as consistency, speed, scalability, and verifiability to the sectors in which it is employed. However, significant challenges may arise, such as the complete replacement of outdated system infrastructure

[14]. Blockchain technology is an area of interest for several companies and institutions worldwide. Blockchain, a relatively new development in the field of computing, is a global, cross-industry, technological revolution that is expected to fuel worldwide economic growth in the future. It is widely used in education because it combines the advantages of a decentralized system with strong cryptography, allowing institutions to set up an architecture for archive maintenance in the form of diplomas and certificates [15].

coming years [16]. Show the evolution of blockchain technology across different time periods and versions.

4.2. Type of Blockchain Technology

Blockchain technology can be implemented in two main forms: permissionless or Permissioned [17, 18].

- **Permissionless Blockchain**
  Also known as a public or unpermissioned blockchain, this type allows anyone to participate in a network. Any user can create and validate blocks as well as read, write, and update the blockchain state through transactions. These blockchains are fully transparent, meaning that openness promotes decentralization and trust; however, it can raise privacy concerns in scenarios where sensitive data must be protected.
- **Permissioned Blockchain**
  This model restricts access to the network, which is also referred to as a private blockchain. Only authorized and trusted participants are allowed to engage in network activities such as validating transactions or accessing data. This controlled environment ensures greater privacy and data confidentiality, making it suitable for enterprise and institutional use cases. A comparison between permissioned and permissionless blockchains is presented in Tables 1 [17, 19–21].

4.3. Blockchain Components

The Blockchain functions as a distributed database that securely and immutably records transactions exchanged among participants. It operates as a peer-to-peer (P2P) network in which nodes (peers) collectively maintain the system by validating and exchanging blocks and transactions [22]. The key components of a blockchain network are as following Figure 1

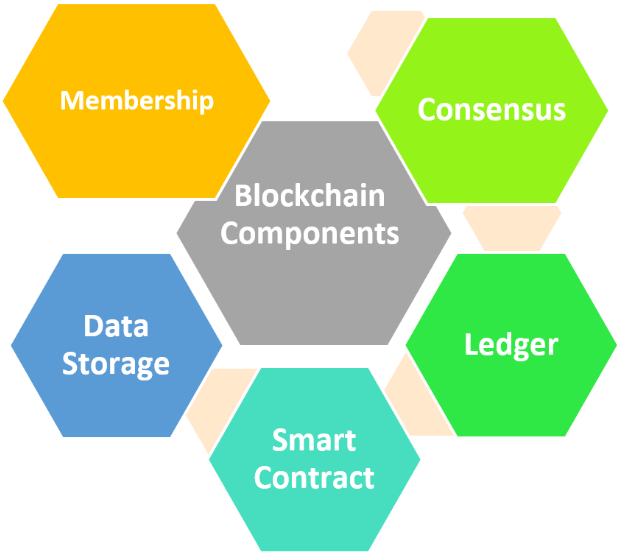

Figure 1. Blockchain Components

- Membership: Provides unique identities for the nodes participating in the network.
- Consensus: A fault-tolerant mechanism is employed in both computing and blockchain systems to establish an agreement on a single data value or the overall state of the network among distributed processes.
- Ledger: A sequential chain of blocks in which validated transaction details are recorded, ensuring transparency and integrity.
- Smart Contract: A self-executing code that enforces predefined rules and conditions between two or more parties. Events are embedded within the contract to capture the arguments stored in transaction logs. Communication: Refers to fork and read operations that enable information exchange among nodes within the network.
- Data Storage: A private storage area within the smart contract, accessible solely by the contract itself, which can read, write, modify, and delete data as required.

5. USING BLOCKCHAIN IN CERTIFICATES

A certificate is an official document that provides a verified statement that validates a claim. In education, these documents are crucial, serving as proof of learning achievements, teacher qualifications, or a learner's progress. The entire process of issuing a certificate to validate such claims is known as certification [19]. Given its potential, researchers have thoroughly investigated the blockchain technology to assess its value and applicability in education. The primary goal of these studies is to answer the fundamental question: Why integrate blockchain into educational systems? The justification for its adoption usually centers on solving various existing institutional challenges. These issues include the difficulty of verifying physical credentials, dependence on centralized systems (which are vulnerable to single points of failure), the need for more secure storage and exchange of academic data, and the widespread problem of academic fraud [20, 21].

5.1. Key Benefits and Rationale for Blockchain Adoption

The rationale for integrating blockchain technology into educational systems is primarily framed by the need to overcome several persistent **institutional challenges** faced by current academic credentials. These challenges justify the adoption of technology [22, 23].

- **Prevention of Forgery and Tampering.**
  Traditional papers and unsecured digital certificates are susceptible to fraud. Blockchain ensures immutability. Once a certificate has been issued, it cannot be altered or forged.
- **Instant and Independent Verification**
  Through smart contracts, any third party (e.g., an employer) can verify the authenticity of a certificate in real time using a unique student and certificate ID without needing to contact the issuing institution.
- **Elimination of Third-Party Dependency**
  The system eliminates the need for intermediaries in the verification process and reduces administrative effort and time.
- **Enhanced Transparency and Trust**
  Every action (issuance, verification, sharing) is permanently recorded on the blockchain ledger, which increases confidence in the authenticity of academic credentials.

5.2. Security Themes for Educational Certificates on Blockchain

To ensure trust, integrity, and authenticity, educational certificates stored on a blockchain must adhere to several fundamental security principles [6, 20].

1. **Authentication**
   Blockchain systems must verify the identities of all participants, including students, academic institutions, and employers. User authentication is typically achieved through usernames and passwords and, in some cases, is enhanced by multi-factor authentication methods such as biometrics. For instance, an employer wishing to verify a certificate must first join the blockchain network and the certificate owner (student) must authorize access.
2. **Authorization**
   Authorization defines the user permissions for executing transactions within the blockchain. For example, a student can choose to share their certificate with an employer. Once the certificate is issued, the issuer grants the student full control of it. All operations must be governed by explicit authorization rules embedded within the system.
3. **Confidentiality**
   Confidentiality involves safeguarding the student's personal and academic data. This responsibility is shared between the issuing institution and student. The student retains control over when and how to disclose their certificate to third parties such as employers during the verification process.
4. **Ownership**
   Digital certificates stored in the blockchain are fully owned by the recipient. Ownership is maintained through the use of public and private cryptographic keys that allow the user to control access and verify the identity of the blockchain.
5. **Privacy**
   Public keys are handled in a manner that maintains user anonymity. The system employs cryptographic algorithms and hash functions to protect user identities and data, thereby ensuring the integrity and privacy of the certificate.

5.3. Key Technical Mechanisms for Electronic Certificates

The following components are instrumental in the secure operation of blockchain-based certificate systems.

- **Hash Functions:** Cryptographic hash functions (e.g., SHA-256) generate a unique, fixed-size message digest for a certificate file [24]. This digest is the data stored on the blockchain, serving as a tamper-proof digital fingerprint that proves the integrity of the certificate.
- **Smart Contracts:** These self-executing codes that automatically enforce predefined rules and conditions [25]. In educational contexts, smart contracts automate secure issuance and verification processes without the need for manual intervention, thus streamlining the management of academic credentials.
- **Digital Signatures:** Using public-key cryptography, the issuing authority digitally signs certificate data [16]. This signature acts as undeniable proof of the issuer's identity and confirms that the certificate content has remained unaltered.

- **Consensus Algorithms**
  Consensus algorithms are essential for ensuring that all nodes in a blockchain network, whether honest or malicious, agree with the current state of the distributed ledger. The most common mechanisms include Proof of Work (PoW), where miners solve complex mathematical puzzles that require significant computational resources to validate transactions and secure the network, thus preventing attacks such as double-spending [26]; Proof of Stake (PoS), which selects block validators based on the amount of cryptocurrency they have staked, discouraging dishonest actions through potential financial penalties [2]; and Byzantine Fault Tolerance (BFT), which enables the system to function correctly even if some nodes fail or

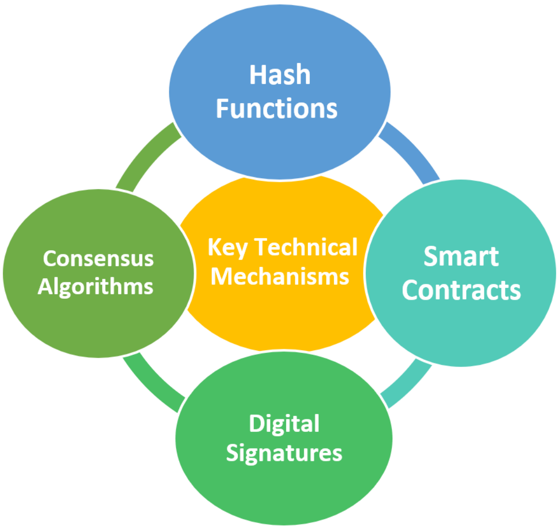

Figure 2. Key Technical Mechanisms

act maliciously, addressing the challenge of achieving consensus in unreliable environments [27].

6. ANALYSIS OF REVIEW FINDINGS AND DISCUSSION

Recent studies have increasingly examined the role of blockchain technology in transforming educational systems, particularly concerning secure academic credentialing. A systematic review was conducted to rigorously analyze existing models and identify their strengths, weaknesses, and key architectural choices. The following sections present the detailed methodology, quantitative assessment of the platform trends, and critical analysis of the core trade-offs observed in the reviewed literature.

6.1. Review Methodology and Scope

The methodology for this systematic literature review was meticulously designed to identify and analyze recent scholarly work focusing on the practical application of blockchain technology for secure academic credentialing.

- **Search Strategy and Scope**
  The search was conducted across leading academic databases including IEEE Xplore, Scopus, ScienceDirect, and Google Scholar. The primary search strategy utilized combinations of keywords such as: "Blockchain" AND ("Academic Certificates" OR "Credentials" OR "Transcript") AND ("Consensus Algorithms" OR "Smart Contracts"). The scope was limited to papers published between 2018 and 2024, reflecting the timeframe of significant practical model development in this area.
- **Inclusion and Exclusion Criteria**
  Specific criteria were applied to ensure the relevance and technical depth of the reviewed studies.
  - **Inclusion Criteria:** Papers must propose a practical model or application for a blockchain-based credentialing system, include clear analysis of the technical mechanisms (e.g., consensus, platform), and be published in peer-reviewed journals or conferences.
  - **Exclusion Criteria:** General literature reviews without a proposed model, papers focusing solely on theoretical or legal aspects without technical implementation details, and articles not written in English (or in the primary research language) were excluded.
  - **Screening Process (PRISMA)**
    The selection process followed a multi-stage screening method inspired by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure a rigorous selection of the final corpus of studies. This process involves three main stages.

    1 **Identification:** Initial collection of all papers resulting from the keyword searches.
    2 **Screening:** Removal of duplicates and assessment of titles and abstracts for relevance.
    3 **Eligibility:** Full-text reading of the remaining papers to rigorously apply the inclusion and exclusion criteria resulted in a final selection of 24 studies for in-depth analysis.

- **Data Extraction and Analysis**
  To facilitate the critical comparative analysis, data were extracted from the final 24 studies and categorized into four core elements: (1) the utilized technical platform (e.g., Ethereum, Hyperledger), (2) the adopted consensus mechanism, (3) the model's key features or strengths, and (4) the limitations or weaknesses acknowledged by the authors. The extracted data formed the basis for the descriptive, quantitative, and critical comparative analyses presented in Sections 5.2 and 5.3 respectively.

6.2. Descriptive Findings of the Literature Review

The 24 studies identified through the systematic review process are summarized in this section. Table 2 provides an overview of the proposed solutions and their respective limitations (drawbacks), and Table 3 presents a technical summary. The subsequent paragraphs briefly introduce the key models before the quantitative and critical analyses in Sections 5.3.

Cheriguene et al. [1] examined how blockchain technology can enhance online education, and proposed a framework that prioritizes both security and reliability. The model ensures that academic standards are met by maintaining fairness in assessment and adherence to class timetables. Additionally, the reward features associated with blockchain serve as motivational drivers, encouraging teachers and students to maintain consistent engagement even within distance-learning environments. Similarly, Purnama et al. [28] designed a cooperative education management system by incorporating e-portfolios into a cloud infrastructure underpinned by blockchain. Their results highlight that the student-centered learning blockchain (SCi-B) environment not only strengthens institutional capacity, but also promotes digital skills. Importantly, the SCi-B framework ensures the authenticity of student assessment records by employing blockchain-based hashing, while simultaneously offering a flexible learning process unconstrained by geographic or temporal barriers. Complementing this work, In the study of Rahardja et al. [29], the researchers combined data collection with a review of relevant scholarship to assess blockchain's contribution to education. These findings underscore the potential of blockchain to simplify access to learning resources, regardless of location or time. By removing such barriers, technology fosters efficiency and encourages learners to broaden their educational engagement, resulting in improved academic performance. Likewise, In their research, Asaad et al. [4] proposed strategies for applying blockchain to protect sensitive educational information. Utilizing blockchain's immutability, they demonstrated how online education can benefit from enhanced confidentiality and resistance to tampering. Examples discussed include securing academic credentials and validating student participation records.

Building on these perspectives, According to Lutfiani et al. [30], counterfeit academic certificates undermine both institutional credibility and employment quality. To mitigate this issue, the authors proposed blockchain-based verification systems that incorporate digital signature schemes and time-based authentication. These methods ensure the authenticity of credentials and prevent fraudulent practices. From another perspective, Harthy et al. [31] stressed the novelty of blockchain in distributed computing and its role in decentralized applications. Their literature-based analysis identified blockchain as a highly secure method for transmitting information in LMS environments, noting its relevance as an evolving trend in the education sector. Extending this discussion

In their study, Abdelsalam et al. [2] introduced an extension for Moodle that employs blockchain to secure examination processes. Their approach stores both exam content and responses immutably in blockchain networks, thereby preventing data manipulation and reinforcing academic integrity. Furthermore, Aliane et al. [27] showed that merging Education 4.0 principles with blockchain produces student-centered educational experiences. Their study emphasized improvements in academic record management, fraud prevention, and institutional transparency while also providing broader implications for higher education policies and practices.

Addressing Challenges

According to Rustemi et al. [26], a major issue in higher education is credential falsification. Their research proposed blockchain-based solutions for diploma verification, outlining general models applicable across various institutions to form collective defense against fraud. Empirical validation was also provided by Vipie et al. [12], who defined blockchain in general and educational terms and tested hypotheses using student surveys. The findings confirmed all assumptions, illustrating blockchain's applicability to learning environments. In addition, Khan et al. [32] introduced BLMS, a secure and decentralized learning platform built on a blockchain. The authors argue that decentralization not only resolves reliability issues but also strengthens data integrity and lowers operational expenditure. Beyond education, Youssef et al. [33] proposed a blockchain-enabled EMC framework that connects patient medical records with clinical decision making. The system guarantees privacy and accelerates healthcare delivery using time-stamped and immutable data blocks.

Recently, Noorhizam et al. [8] proposed securing doctoral certificates using blockchain-enabled QR codes. Implemented with Solidity, PHP, HTML/CSS, and MetaMask, the model ensures authenticity by requiring private-key authorization from issuing institutions. Collectively, these studies underscore the multifaceted potential of blockchain to enhance security, credibility, efficiency, and personalization within education, while also extending its applications to adjacent sectors, such as healthcare and certification management.

P. Ocheja et al, [34] One of the studies recommends different Learning Management Systems (LMS), Learning Record Stores (LRS), and a blockchain-based approach for connecting learning data between institutions and organizations. Thus, we attempted to take advantage of blockchain technology's ability to provide consistency.

E . KARATAŞ et al, [35] This study aims to verify digital certificates given to the participants at the Turkish stage of the International Informatics and Computational Thinking event by using an Ethereum Blockchain smart contract. The tasks in the event were transmitted to students in Turkey using the exam module of the Moodle Learning Management System. For this study, first, a smart contract was developed in which the certificate information could be stored on the Ethereum blockchain and checked for control purposes if necessary.

M .Khan et al.[5] emphasized database distribution and security issues in learning management systems to identify the security parameters, which are significant in providing a secure database application in the learning management system and its usage. The researcher used blockchain methodology to provide highly secure data in database distribution concerning certificates in case of loss, re-issues, global authentication for the learning management system, and secure online tutorials. According to Lutfiani et al. [36], a review of existing scholarly works highlights how integrating blockchain technologies into the framework of Education 4.0 can generate significant benefits. This discussion particularly underscores its potential in areas such as digital record management, instructional activities, and credential verification. This study concludes that blockchain may function as an enabler for the ongoing advancement of educational quality by bridging technological progress with the dynamic requirements of academic institutions.

O.SALEH et al. [6] aimed to enhance the document verification process using blockchain technology. In this study, the authors identified the security themes required for document verification in the blockchain. This study also identifies gaps and loopholes in current blockchain-based educational certificate verification solutions. Finally, a blockchain-based framework for verifying educational certificates focusing on themes including authentication, authorization, confidentiality, privacy, and ownership is proposed using the Hyperledger Fabric Framework.

Latha et al.[37] proposed that the government use the proposed system to construct a decentralized network to store and maintain records. This is also the best way to ensure that documents exist in the state of their creation and that they are not tampered with by anyone. Motivated by this, we propose the development of a decentralized blockchain system using Ethereum, which will serve as an application to authenticate documents.

6.3. Quantitative Analysis of Platform and Consensus Trends

To provide a quantitative overview of the current research trends, the 24 studies analyzed in Table 3 were assessed based on the adopted blockchain platforms and consensus mechanisms.

1. Blockchain Platforms Adoption Trends
   The analysis of platform usage demonstrated clear preferences among the reviewed literature:
   - Ethereum (50%, 12 studies): Ethereum emerged as the most predominantly utilized platform, accounting for exactly half of the reviewed models.
   - Hyperledger Fabric (25% / 6 studies): Solutions based on Hyperledger Fabric followed, representing a quarter of the documented studies.
   - Other Technologies (25%): The remaining 25% were distributed among various other technologies, including decentralized file systems and databases, such as IPFS and BigchainDB.
2. Consensus Mechanism Trends
   The analysis revealed a corresponding variation in the consensus mechanism choices tailored to the platform type.
   - Ethereum-based Models: These systems utilize the Proof of Stake (PoS) algorithm (or Proof of Work (PoW) in earlier studies before Ethereum's transition), or modified permissioned variants such as proof of authority (PoA) within test environments.
   - Hyperledger-Based Models: These predominantly rely on algorithms optimized for permissioned environments, such as Practical Byzantine Fault Tolerance (PBFT) or Raft, focusing on the high speed and instant finality of consensus among known nodes.

6.4. Critical Comparative Analysis of Credentialing Models

A critical review of the 24 analyzed frameworks, particularly considering the platform choices detailed in Section 5.3, reveals a core methodological split in addressing academic credentialing. While all studies seek to solve the fundamental problem of trust and forgery, they diverge significantly in their approach to tackling the major technical trade-offs of decentralization versus operational efficiency.

1- The Core Trade-Off: Public vs. Permissioned

The quantitative results underscore a conflict in priorities between the most adopted platforms:

- Ethereum-Based Models (50%): Studies favoring Ethereum (e.g., [8, 35, 37]) prioritize absolute decentralization and the concept of Self-Sovereign Identity (SSI). Their primary strength lies in offering a censorship-resistant and globally verifiable system in which the student maintains the ultimate ownership of their credentials, independent of any single university or government authority.
- Hyperledger Fabric-Based Models (25%): Conversely, solutions utilizing Hyperledger Fabric (e.g., [6, 19, 38, 39]) focus on operational efficiency and governance. Their strength is their ability to deliver high transaction throughput and low (or zero) transaction costs, making them structurally superior for large educational institutions that must process millions of records quickly and affordably.

2- Analysis of Key Technical Challenges and Drawbacks

The choice of platform necessitates accepting specific drawbacks, which have been frequently noted as limitations in the reviewed literature (see Table 2):

1. Cost and Scalability: The reliance on Ethereum's public network introduces critical issues regarding Gas Fees and limited scalability under high transaction loads. The literature often fails to pro-

vide a sustainable cost model for mass institutional adoption within Ethereum's structure. In contrast, Hyperledger Fabric's permissioned architecture, leveraging consensus mechanisms such as PBFT or Raft, intrinsically overcomes these issues by operating in a closed environment of trusted nodes, ensuring high speed and low cost.

2. Governance and Control: The drawback of Hyperledger lies in its limited decentralization. Because control rests with a consortium (e.g., a group of universities), the system is viewed as less trustless than a public chain. This raises academic questions regarding whether the system truly empowers the student (SSI) or merely shifts centralized control from a single entity to a small consortium.

3- Future Direction: The Necessity of Hybrid Architectures

This critical analysis concludes that no single platform offers a perfect solution that satisfies both the educational sector's operational demands and blockchain's core principles. A future direction suggested by this analysis is the development of Hybrid Architectures. These solutions must combine the trust and immutability of a public chain (e.g., Ethereum's ability to anchor a student's sovereign identity) with the efficiency and cost-effectiveness of a permissioned framework (e.g., hyperledger for high-volume internal record management). Achieving this balance is the key methodological gap that future research must address to create a truly viable and globally scalable reality.

6.5. Discussion of Identified Challenges and Methodological Gaps

Despite clear progress in the proposed models for blockchain-based academic credentialing, the critical analysis in the preceding sections reveals that the current literature suffers from major challenges and methodological gaps that prevent the widespread adoption of this technology in large educational institutions.

1. The Critical Absence of Quantitative Performance Data

This represents the most significant methodological gap in the present study. While many studies have proposed a framework to solve the forgery problem (e.g., [1, 4, 30]), few have provided Empirical Quantitative Data regarding system performance. Most studies lack the fundamental metrics necessary for assessing practical viability, such as

- **Transaction Throughput:** The number of certificates the system can process per second.
- **Latency:** The time required for certificate confirmation.
- **Operational Costs:** The actual cost (Gas Fees) incurred by the institution or student.

This absence of quantitative data (as noted in the limitations of [2, 34]) makes objective comparison of platform effectiveness difficult, particularly between Ethereum, which faces gas fees and scalability challenges [8, 35], and Hyperledger Fabric, which promises higher efficiency [6, 38].

2. Theoretical Focus and Lack of Large-Scale Pilot Projects (Conceptual Focus)

A substantial portion of the literature focuses on the theoretical or Conceptual aspects of technology. Several studies, such as [26, 27, 31, 36], are essentially literature reviews or framework proposals that lack a complete practical implementation at the institutional level (proof of concept) or are limited to testing in restricted environments (testbed). This indicates a significant gap between theoretical potential and real-world implementation challenges, where educational systems require compatibility with existing Learning Management Systems (LMS), as noted in [35].

3. The Unresolved Governance Dilemma and Student Sovereignty

As discussed in Section 5.3, disparity persists in the preferred governance model:

- **The Public Model (Ethereum):** Guarantees absolute decentralization and **Student Self-Sovereign Identity (SSI)** but comes with the technical challenges noted above.
- **The Permissioned Model (Hyperledger):** Offers efficiency and speed, but requires a high level of complexity and specialized infrastructure [6], placing ultimate control in the hands of a university Consortium, which limits the desired decentralization.

This split means the research community has yet to agree on an architecture that balances individual student privacy protection with educational institution operational requirements, posing a major methodological challenge for global adoption plans.In conclusion, the identified methodological gaps and challenges indicate that future research must move beyond theoretical proposals and descriptive analyses.

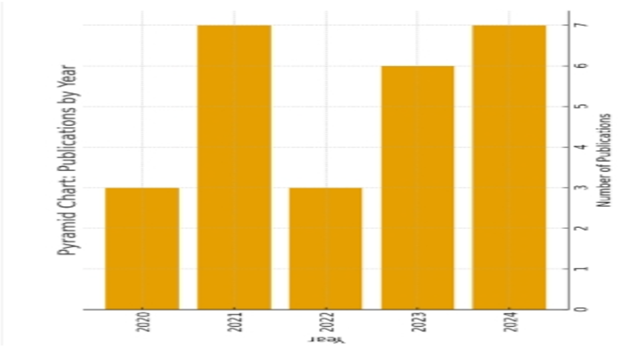

Figure 3. numbers of publication for studies.

Table 2. Solutions and Drawbacks of Blockchain for Secure Electronic Certificates

Ref	Blockchain Solution	Drawbacks
[34]	Proposed blockchain-based approach for connecting learning data across institutions and organizations through LMS/LRS.	Interoperability across diverse institutions is complex; scalability challenges.
[35]	Verified digital certificates using Ethereum smart contracts integrated with Moodle LMS.	Ethereum gas fees; limited scalability for mass adoption.
[5]	Addressed database distribution & security issues in LMS; used blockchain for secure certificates, global authentication, and reissuance.	Blockchain deployment complexity; high energy/cost overhead.
[36]	Informed opportunities of blockchain in Education 4.0 (archiving, learning, certification).	Conceptual focus; lacks real-world implementation/testing.
[1]	Proposed blockchain-based online learning framework ensuring fairness in assessment and secured teaching standards.	Implementation at scale remains untested; adoption barriers.
[28]	Designed cooperative education management with Blockchain-based E-Portfolio (SCi-B).	Dependence on cloud infrastructure; technical integration issues.
[29]	Highlighted efficiency and accessibility of blockchain for learning systems.	Generalized study; lacks security depth and technical prototype.
[4]	Secured educational data from hacking, theft, modification using blockchain (degrees, attendance).	High implementation cost; requires strong infrastructure.
[30]	Prevent falsification of educational documents using blockchain verification with digital signatures and timestamps.	Limited scalability; requires institutional collaboration.
[31]	Explored decentralized LMS data handling with blockchain security.	Only literature-based; no practical implementation.
[2]	Developed blockchain-based online exam storage integrated with Moodle for tamper-proof results.	System performance compared to centralized storage may slow down at scale.
[27]	Integrated Blockchain with Education 4.0 for data management and preventing transcript fraud.	Theoretical focus; lacks practical framework.
[26]	Proposed blockchain-based diploma management model to prevent forgery.	Remains conceptual; adoption across institutions is challenging.
[12]	Case study validating hypotheses about blockchain's role in education.	Small-scale; student perception focused, not technical depth.
[32]	Proposed Blockchain-based LMS (BLMS) to overcome single point of failure and reduce cost.	Implementation cost vs. benefit balance unclear.
[33]	Used blockchain for managing electronic medical certifications linked with patient records.	Focused on medical domain, not directly education; privacy concerns.
[8]	Verified PhD certificates using Ethereum + QR codes; ensured tamper-proof certificates.	Ethereum limitations (cost, scalability); dependence on external tools like MetaMask.
[6]	Proposed blockchain framework for certificate verification using Hyperledger Fabric (authentication, privacy, ownership).	Framework complexity; requires technical expertise and infrastructure.
[37]	Proposed decentralized blockchain system (Ethereum) for government document authentication.	Dependence on local apps; scalability & user adoption issues.

Table 3. Summary of papers related to the development of blockchain in Electronic certificates

Year	**Title**	**Keyword**	**Journal/Conference**	**Type of Research**
2020[40],	"verification and validation of certificate using blockchain"	"Blockchain, Digital Certificate"	"Turkish Journal of Computer and Mathematics Education"	Article
November, 2020[41]	"bcert–a decentralized academic certificate system distribution using blockchain technology"	"blockchain, certificates, smart contracts, solidity, AES, IPFS"	"International Journal on Information Technologies & Security"	Article

September 2020[42]	"Authenticity of a Diploma Using the Blockchain Approach"	"Blockchain, Counterfeiting, Authenticity, Diploma."	"International Journal of Advanced Trends in Computer Science and Engineering"	Article
February, 2021[43]	"Development and Evaluation of Blockchain-based Secure Application for Verification and Validation of Academic Certificates"	"Blockchain; Ethereum; Smart Contract; Test Environment; Verification Application"	"Annals of Emerging Technologies in Computing (AETiC)"	Review Article
April, 2021[44]	"Digital Certificate Authority with Blockchain Cybersecurity in Education"	"Digital Certificate, Blockchain, Cybersecurity, Education"	"International Journal of Cyber and IT Service Management (IJCITSM)"	Article
April, 2021[45]	"A Blockchain-based framework for secure Educational Credentials"	"Blockchain, Education, Digital Certificate, Educational Credential, Security, Privacy"	"Turkish Journal of Computer and Mathematics Education"	Article
2021[46]	"Higher Education's Certificates Model Based on Blockchain Technology"	"Blockchain Applications, Consensus, Automated Certificate Educational Systems, University Digital Certificate."	"Ibn Al-Haitham International Conference for Pure and Applied Sciences (IHICPS)"	Article
June 2021[47]	"Blockchain Technology and Academic Certificate Authenticity-Review"	"Blockchain Technology; Digital certificates; Blockchain in Education; Technical Challenges"	"ResearchGate"	Review
October, 2021[48]	"Verification of University Student and Graduate Data using Blockchain Technology"	"Blockchain, smart contract, academic records, verification"	"International journal of computers, communications & control"	Article
October, 2021[49]	"A survey on blockchain-based student certificate management system"	"blockchain, digital certification, academics, educational projects"	"International Conference on Theory and Practice of Electronic Governance (ICEGOV)"	survey
May 2022[50]	"Blockchain-based Documents Verification for Smart Learning Management System"	"Blockchain, SHA-256, QR code, Document Forgery, Smartphones"	"International Journal of Advances in Engineering and Management (IJAEM)"	Article
April, 2022[38]	"Blockchain-based student certificate management and system sharing using Hyperledger fabric platform"	"Computer Network, Distributed Systems, Blockchain, Hyperledger Fabric, Data Sharing, Student Certification"	"Periodicals of Engineering and Natural Sciences"	Article
December 2022[51]	"The application of blockchain algorithms to the management of education certificates"	"Blockchain, Cryptographic algorithms, Technology, Digital certificates, Cybersecurity"	Evolutionary Intelligence	special issue
January 2023[52]	"Educational Certificate Verification System Using Blockchain"	"Blockchain, Digital Certificate, Distributed Ledger, Hashing, Ethereum, Cryptography, Counterfeit"	International Journal of Scientific & Technology Research · January 2023	Article

June 2023[53]	"A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification"	"Blockchain platforms, smart contracts, academic certificate verification, systematic literature review, security and transparency, fraud prevention, Ethereum, automatic certificate generation"	IEEE Access	Topical Review
March 2023[54]	"Review: verification process of academic certificates using blockchain technology"	"Blockchain; Academic certificate; Smart contract; Decentralization; Verification."	Kirkuk University Journal-Scientific Studies	review:
March 2023[55]	Blockchain-Based Certificate Authentication System with Enabling Correction"	"Blockchain, Certificate Authentication, Certificate Correction, Secure Certification, Eliminate Forging"	Journal of Computer and Communications	Article
November 2023[19]	"A blockchain-based Certificate Management System using the Hyperledger Fabric Platform"	"Blockchain, Hyperledger Fabric, Educational Certificate, Verifica. tion, Permissioned Blockchain."	Mathematics Subject Classification	Article
May 2024[56]	"Blockchain in education: potentials and challenges in academic records and certifications"	"Blockchain, Education, Potential, Challenges, Academic Record, Certification".	International Journal of Teaching and Learning (INJOTEL)	Article
March 2024[57]	"Educational Certificate Verification System: Enhancing Security and Authenticity using Ethereum Blockchain and IPFS"	"Blockchain technology, Educational certificate verification, Ethereum blockchain, Interplanetary File System (IPFS), Decentralized architecture, Certificate counterfeiting, Ropsten test network".	Al-Mustansiriyah Journal of Science	Article
March 2023[58]	"Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022)"	"Academic Credentials· Authenticity· Blockchain· Certificates· Degrees· Digital Signatures· Institute Accreditation· Verification· Validation"	Education and Information Technologies	Article
March 2024[59]	"A Secure Blockchain-Based Student Certificate Generation and Sharing System"	"Data sharing; distributed systems; computer network; certificate blockchain; Ethereum"	Journal of Sensors, IoT & Health Sciences	Article
March 2024[39]	"Educert-chain: a secure and notarized educational certificate authentication and verification system using permissioned blockchain"	"Blockchain Educational Certificates Elliptic Curve Algorithm Hyperledger Fabric Raft Algorithm Smart Contract Validation Verification"	Cluster Computing, Springer.	Article
2024[60]	"An Empirical Review of Security Models used for Issuing Tamper-Proof Certificates for Authentic Credentials"	"Tamper-Proof Certificates, Authentic Credentials, Security Models."	"International Conference on Intelligent Data Communication Technologies and Internet of Things"	Review

7. CONCLUSION

This systematic review concludes that integrating blockchain technology into academic credential management is a promising solution for combating forgery and enhancing transparency in education. By applying quantitative and critical analysis to the 24 models reviewed, the study confirms a fundamental architectural dichotomy in the research community: 50% of studies favor Ethereum, focusing on absolute decentralization and Self-Sovereign Identity (SSI), while 25% rely on Hyperledger Fabric to achieve high operational efficiency and low costs for processing large institutional records. This inherent trade-off forms the basis of the methodological gaps identified, as the critical analysis revealed a critical absence of empirical quantitative data (such as throughput and cost) in the majority of research. This lack of data prevents objective comparisons of system effectiveness, and is the single largest obstacle to widespread institutional adoption. Consequently, future research must move beyond theoretical proposals for large-scale empirical applications. The focus must shift to developing Hybrid Architectures that effectively combine decentralized trust with operational efficiency, committing to the provision of standardized and comparable quantitative performance metrics, and prioritizing institutional compatibility with existing Learning Management Systems (LMS), thereby making the resolution of these gaps a decisive step in transforming blockchain-based academic credentialing into a globally viable operational reality.

REFERENCES

[1] A. Cheriguene, T. Kabache, A. Adnane, C. A. Kerrache, and F. Ahmad, "On the use of blockchain technology for education during pandemics," *IT Prof.*, vol. 24, no. 2, pp. 52–61, 2022. DOI: 10.1109/MITP.2021.3066252.

[2] M. Abdelsalam, M. Shokry, and A. M. Idrees, "002-a proposed model for improving the reliability of online exam results using blockchain," *IEEE Access*, vol. 12, pp. 7719–7733, 2024. DOI: 10.1109/ACCESS.2023.3304995.

[3] J. Park, "03-promises and challenges of blockchain in education," *Smart Learn. Environ.*, vol. 8, no. 1, Dec. 2021. DOI: 10.1186/s40561-021-00179-2.

[4] A. M. Saad, S. M. Elatawy, M. S. Elbelkasy, and D. M. Hawa, "Proposed model for using blockchain to secure the university management system in online education," *Webology*, vol. 19, no. 1, pp. 729–748, Jan. 2022. DOI: 10.14704/web/v19i1/web19052.

[5] M. Khan, T. Naz, and K. Mahmood, "Using blockchain to resolve database distribution and security issues in the learning management systems (lms)," 2019.

[6] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain-based framework for educational certificates verification," Innovare Academics Sciences Pvt. Ltd., 2020. DOI: 10.31838/jcr.07.03.13.

[7] "2019 4th mec international conference on big data and smart city (icbdsc)," IEEE, 2019.

[8] N. K. Noorhizam, Z. Abdullah, S. Kasim, I. Rahmi, A. Hamid, and M. Anuar, "Verification of ph.d. certificate using qr code on blockchain ethereum," *JOIV*, 2023. [Online]. Available: https://www.joiv.org/index.php/joiv.

[9] R. S. Lamkoti, D. Maji, A. B. Gondhalekar, and H. Shetty, "Certificate verification using blockchain and generation of transcript," 2021. [Online]. Available: https://www.ijert.org.

[10] S. Abed, R. Jaffal, and B. J. Mohd, "A review on blockchain and iot integration from energy, security and hardware perspectives," Apr. 2023. DOI: 10.1007/s11277-023-10226-5.

[11] U. Rahardja, Q. Aini, M. A. Ngadi, M. Hardini, and F. P. Oganda, "The blockchain manifesto," in *2020 2nd International Conference on Cybernetics and Intelligent Systems (ICORIS)*, IEEE, Oct. 2020. DOI: 10.1109/ICORIS50180.2020.9320798.

[12] C.-M. Vipie, A.-D. Afumatu, and M. Caramihai, *016-blockchain-based educational certificates: A proposal*, 2023. [Online]. Available: https://www.intechopen.com.

[13] S. Perera, S. Nanayakkara, M. N. N. Rodrigo, S. Senaratne, and R. Weinand, "Blockchain technology: Is it hype or real in the construction industry?," Mar. 2020. DOI: 10.1016/j.jii.2020.100125.

[14] *Blockchain technology: Application, benefits, and challenges*, IEEE, 2019.

[15] L. K. Choi, P. A. Sunarya, and M. Fakhrezzy, "Blockchain technology as an authenticated system for smart universities," *IAIC Trans. on Sustain. Digit. Innov. (ITSDI)*, vol. 4, no. 1, pp. 57–61, Sep. 2022. DOI: 10.34306/itsdi.v4i1.570.

[16] V. G. Martínez, L. Hernández-Álvarez, and L. H. Encinas, "Analysis of the cryptographic tools for blockchain and bitcoin," Jan. 2020. DOI: 10.3390/math8010131.

[17] Z. Benetti and F. Piazza, *Decentralised finance: A categorisation of smart contracts*, 2024. [Online]. Available: https://www.esma.europa.eu.

[18] E. A. Abdullah, A. Shamiri, and A. Khulaidi, "A hybrid model for using cloud computing and blockchain technologies to protect hospital records," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 1, no. 2, pp. 131–146, 2023.

[19] Q. Duy, T. Trong, and M. Hoang, *A blockchain-based certificate management system using the hyperledger fabric platform*, 2023.

[20] M. S. Al and M. Alalyan, *Blockchain technology adoption in saudi arabia's higher education sector certificate of original authorship*, 2023.

[21] R. N. Mir, A. Hussain, R. Nazir, Z. A. Shah Syed, and M. A. Wani, "Blockchain-based academic credit verification system," *Int. J. Eng. Res. Comput. Sci. Eng. (IJERCSE)*, vol. 9, 2022. [Online]. Available: https://www.researchgate.net/publication/369912496.

[22] S. I. Mouno, T. Rahman, A. M. Raatul, and N. Mansoor, "Blockchain-enhanced academic certificate verification: A decentralized and trustworthy framework," in *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)*, IEEE, 2024. DOI: 10.1109/iCACCESS61735.2024.10499524.

[23] S. Al Ahmed, R. Al Mamun Rudro, A. J. Prity, S. Saha, N. Mansoor, and K. Nur, "Credchain: Academic and professional certificate verification system using blockchain," in *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)*, IEEE, 2024. DOI: 10.1109/iCACCESS61735.2024.10499520.

[24] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Tech. Rep., Jun. 2019. DOI: 10.6028/NIST.IR.8202.

[25] A. Z. Huang, "Blockchain performance optimization using cloud technology," 2023. DOI: 10.25959/25792590.

[26] A. Rustemi, V. Atanasovski, A. Risteski, and P. Latkoski, "Challenges of blockchain in higher education institutions for protection against diploma forgery," in *2023 International Balkan Conference on Communications and Networking (BalkanCom)*, IEEE, 2023. DOI: 10.1109/BalkanCom58402.2023.10167986.

[27] N. Aliane and A. S. Salim, "Revolutionising higher education: Case studies on education 4.0 integration and blockchain-enhanced education management," *Eurasian J. Educ. Res.*, vol. 2023, no. 105, pp. 217–235, 2023. DOI: 10.14689/ejer.2023.105.013.

[28] S. Purnama, Q. Aini, U. Rahardja, N. Puji, L. Santoso, and S. Millah, "Design of educational learning management cloud process with blockchain 4.0-based e-portfolio," *J. Educ. Technol.*, vol. 5, no. 4, pp. 628–635, 2021. DOI: 10.23887/jet.v5i4.4.

[29] U. Rahardja, Q. Aini, A. Khairunisa, and S. Millah, "Implementation of blockchain technology in learning management system (lms)," *APTISI Trans. on Manag. (ATM)*, vol. 6, no. 2, pp. 112–120, Dec. 2021. DOI: 10.33050/atm.v6i2.1396.

[30] N. Lutfiani, D. Apriani, E. Ayu Nabila, and H. Lutfilah Juniar, "Blockchain frontier technology (b-front) academic certificate fraud detection system framework using blockchain technology," *B-Front*, no. 40, 2022. [Online]. Available: https://journal.pandawan.id/b-front/article/view/37.

[31] A. Harthy, *The upcoming blockchain adoption in higher education: Requirements and process*, IEEE, 2019.

[32] M. Khan and T. Naz, "Smart contracts based on blockchain for decentralized learning management system," *SN Comput. Sci.*, vol. 2, no. 4, Jul. 2021. DOI: 10.1007/s42979-021-00661-1.

[33] K. Youssef, T. Amer, Y. Ibrahim, and F. Thabit, *Implementing blockchain for secure electronic medical certifications: An analytical study*, 2024. [Online]. Available: https://ssrn.com/abstract=4714110.

[34] P. Ocheja, B. Flanagan, and H. Ogata, "Connecting decentralized learning records: A blockchain-based learning analytics platform," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Mar. 2018, pp. 265–269. DOI: 10.1145/3170358.3170365.

[35] E. KARATAS, "Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System," *BiliSim Teknolojileri Dergisi*, vol. 11, no. 4, pp. 399–406, Oct. 2018. DOI: 10.17671/gazibtd.452686.

[36] N. Lutfiani, Q. Aini, U. Rahardja, L. Wijayanti, E. A. Nabila, and M. I. Ali, "Transformation of blockchain and opportunities for education 4.0," *Int. J. Educ. Learn.*, vol. 3, no. 3, pp. 222–231, Dec. 2021. DOI: 10.31763/ijele.v3i3.283.

[37] S. S. Latha, N. Priya, and A. Shettar, "Blockchain-based framework for document verification," in *2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP)*, IEEE, 2022. DOI: 10.1109/AISP53593.2022.9760651.

[38] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri, "Blockchain-based student certificate management and system sharing using hyperledger fabric platform," *Period. Eng. Nat. Sci.*, vol. 10, no. 2, pp. 207–218, Apr. 2022. DOI: 10.21533/pen.v10i2.2839.

[39] P. Rani, R. K. Sachan, and S. Kukreja, "Educert-chain: A secure and notarized educational certificate authentication and verification system using permissioned blockchain," *Clust. Comput.*, vol. 27, no. 7, pp. 10 169–10 196, Oct. 2024. DOI: 10.1007/s10586-024-04469-5.

[40] M. Chandra Rao et al., *Verification and validation of certificate using blockchain*, 2020.

[41] E. Leka, B. Selimi, and N. Macedonia, "Bcert-a decentralized academic certificate system distribution using blockchain technology," 2020. [Online]. Available: https://www.researchgate.net/publication/346487511.

[42] "Authenticity of a diploma using the blockchain approach," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1.2, pp. 250–256, Apr. 2020. DOI: 10.30534/ijatcse/2020/3791.22020.

[43] E. Leka and B. Selimi, "Development and evaluation of blockchain-based secure application for verification and validation of academic certificates," *Ann. Emerg. Technol. Comput.*, vol. 5, no. 2, pp. 22–36, 2021. DOI: 10.33166/AETiC.2021.02.003.

[44] G. Maulani, G. Gunawan, L. Leli, E. Ayu Nabila, and W. Y. Sari, "Digital certificate authority with blockchain cybersecurity in education," *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 1, pp. 136–150, May 2021. DOI: 10.34306/ijcitsm.v1i1.40.

[45] S. A. et al., "A blockchain-based framework for secure educational credentials," *Turkish J. Comput. Math. Educ. (TURCOMAT)*, vol. 12, no. 10, pp. 5157–5167, Apr. 2021. DOI: 10.17762/turcomat.v12i10.5298.

[46] M. A. Ali and W. S. Bhaya, "Higher education's certificates model based on blockchain technology," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, May 2021. DOI: 10.1088/1742-6596/1879/2/022091.

[47] K. Kumutha and S. Jayalakshmi, *Blockchain technology and academic certificate authenticity-review*, 2021.

[48] Y. Shakan, B. Kumalakov, G. Mutanov, Z. Mamykova, and Y. Kistaubayev, "Verification of university student and graduate data using blockchain technology," *Int. J. Comput. Commun. Control.*, vol. 16, no. 5, pp. 1–16, 2021. DOI: 10.15837/ijccc.2021.5.4266.

[49] S. Murugesan and M. B. Lakshminarasaiah, "A survey on blockchain-based student certificate management system," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Oct. 2021, pp. 44–50. DOI: 10.1145/3494193.3494199.

[50] Y. Dharmik, S. Gaikwad, H. Patil, P. Gujar, and A. Domkundwar, "Blockchain-based documents verification for smart learning management system," *Int. J. Adv. Eng. Manag. (IJAEM)*, vol. 4, p. 1634, 2022. DOI: 10.35629/5252-040516341638.

[51] R. J. Maestre, J. B. Higuera, N. G. Gómez, J. R. B. Higuera, J. A. S. Montalvo, and L. O. Palma, "The application of blockchain algorithms to the management of education certificates," *Evol. Intell.*, vol. 16, no. 6, pp. 1967–1984, Dec. 2023. DOI: 10.1007/s12065-022-00812-0.

[52] D. K. Kumar and M. D. Kumar, "Educational certificate verification system using blockchain," *Int. J. Sci. & Technol. Res.*, 2023. [Online]. Available: https://www.ijstr.org.

[53] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A systematic literature review on blockchain-based systems for academic certificate verification," 2023. DOI: 10.1109/ACCESS.2023.3289598.

[54] A. Kareem and A. C. Shakir, "Review: Verification process of academic certificates using blockchain technology," *Kirkuk Univ. Journal-Scientific Stud.*, vol. 18, no. 1, pp. 62–75, Mar. 2023. DOI: 10.32894/kujss.2023.135876.1072.

[55] M. M. Rahman, M. T. K. Tonmoy, S. R. Shihab, and R. Farhana, "Blockchain-based certificate authentication system with enabling correction," *J. Comput. Commun.*, vol. 11, no. 03, pp. 73–82, 2023. DOI: 10.4236/jcc.2023.113006.

[56] E. Widyasari, A. Muhibbin, and I. A. Al-Shreifeen, "Blockchain in education: Potentials and challenges in academic records and certifications," *Int. J. Teach. Learn. (INJOTEL)*, vol. 2, no. 5, 2024.

[57] R. A. Jaafar, S. N. Alsaad, and M. N. Al-Kabi, “Educational certificate verification system: Enhancing security and authenticity using ethereum blockchain and ipfs,” *Al-Mustansiriyah J. Sci.*, vol. 35, no. 1, pp. 78–87, Mar. 2024. DOI: 10.23851/mjs.v35i1.1461.

[58] M. Al Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, “Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution’s accreditation: Uae case study and system performance,” *Educ. Inf. Technol.*, Oct. 2024. DOI: 10.1007/s10639-024-12493-6.

[59] S. Venkatramulu et al., *A secure blockchain-based student certificate generation and sharing system*, 2024.

[60] S. Dhote, P. Maidamwar, and S. Thakur, “An empirical review of security models used for issuing tamper-proof certificates for authentic credentials,” in *2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, IEEE, 2024, pp. 486–492. DOI: 10.1109/IDCIoT59759.2024.10467298.