Journal of Soft Computing Exploration
Homepage: htttps://shmpublisher.com/index.php/joscex
p-ISSN: 2746-7686
e-ISSN: 2746-0991

.

Integration of blockchain and cryptographic algorithms for education certification and verification: a systematic literature

Roy Mubarak[1,2], Imam Riadi[3], Tole Sutikno[4]
[1]Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department of Informatics, Universitas Mercu Buana, Jakarta, Indonesia
[3]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[4]Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received March 17, 2026
Revised Apr 4, 2026
Accepted Apr 5, 2026

Keywords:

Digital certification
Blockchain
Cryptography
Personal data protection
PRISMA

ABSTRACT

Personal data has become a highly valuable asset in the digital era. The background of this research is the urgent need to raise awareness in the digital era about the importance of protecting digital education certificate. The purpose of this research is to analyze the integration of blockchain technology with cryptographic algorithms for the secure storage and verification of digital education certificates. The methodology follows the Prisma framework, which is carried out through four systematic stages: formulating research question, preparation research protocol, identification of records from four major databases (Google Scholar, IEEE, Springer, and MDPI) published between 2023 and 2026, screening of titles and abstracts to eliminate duplicate and irrelevant studies, eligibility assessment through full-text review based on predetermined inclusion and exclusion criteria, data extraction and validation for qualitative synthesis, and finally of 21 papers for analysis result, conclusion, limitation of research, research gap and novelty. The findings demonstrate that storage efficiency, verification speed, encryption diversity, fraud prevention and identity standards. The conclusion of this study is that a collaborative framework integrating blockchain with cryptographic techniques for the security and verification of digital education certificates, with a robust process, can create a robust and adaptive system against certificate forgery. This study provides conceptual and practical knowledge for developing a more comprehensive education certificate security framework.

Corresponding Author:
Roy Mubarak,
Department of Informatics,
Universitas Ahmad Dahlan,
Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55191,
Email: 2537083002@webmail.uad.ac.id
https://doi.org/10.00000/joscex.0000.00.00.000

1. INTRODUCTION

In today's digital era, with almost everyone connected to the internet, there is a pressing need to ensure security. Internet user activity has increased year by year, impacting user behavior [1]. Various reports indicate that fraudsters continue to develop new methods to bypass security mechanisms, making traditional approaches increasingly inadequate for providing adequate protection [2]. Rosmiati et al. [3] explain that information security protects information from threats to maintain business continuity, reduce risks, and increase profits and opportunities, while R. Umar et al. [4] highlight that data protection and security are necessary to address threats such as damage, natural disasters, and cybercrime. According to R. Umar et al. [5], this is because life, in all its forms, has entered the digital age, and many activities are now conducted digitally. This concern includes the need to protect (not treat lightly) personal data, which involves more than just confidentiality; it also relates to the integrity and availability of data for its owners. Y. Farida et al. [6] explain that cryptographic methods also provide stronger security by verifying the authenticity and integrity of digital data. A digital signature is a unique cryptographic value for each document, derived from its content and an encryption key.

Meanwhile, international laws such as GDPR also mean systems need to be both secure and transparent in line with legal frameworks. Z. Munawar et al. and P. Verma et al. [7][8] explain that blockchain technology has emerged as an ideal candidate due to its promising characteristics of transparency, immutability, and decentralization which promise higher levels of encryption and data security to address internal, malicious, peripheral, and incidental threats. Blockchain has the capability to achieve these standards since it is a truly distributed technology. A. Fadlil et al. [9] also explained that blockchain is a technology that involves third parties in the process of exchanging information. Information on the Blockchain can be in the form of data entry in transaction form, assets, identities, and other information that is packaged in digital form. Therefore, research is also directed at developing hybrid blockchain systems with IPFS for off-chain storage. R. M. Gonçalves [10] also explained that blockchain demonstrates this architecture can satisfy user privacy rights, such as "The Right to Be Forgotten". I Riadi et al [11][12] [13] explained that blockchain is a technology that combines tools, methods, and configurations to address specific problems or use cases, differs from traditional centralized approaches by enabling secure on-chain data management across a distributed and interconnected network of nodes, uses a consensus mechanism that allows transaction data to be securely stored on the network after verification and validation, without third-party interference, combines several security concepts to ensure the confidentiality of information. R. Zhu et al [14] propose to ensure user control over their personal data, particularly that generated by web applications, drives protection mechanisms that combine blockchain with distributed hash tables and cryptography. B. Dwi et al [15] also agree that secure, encrypted and unalterable data recording technology provides transparency and trust throughout the production and distribution process.

One use of blockchain technology is in the security and verification process of digital certificates. Academic qualifications or certificates also form part of the educational context. Not only is it needed for the university's reputation, but on a practical level, attempts to verify degrees are typically bureaucratic, and the weaknesses of this system are preyed upon by actors in the educational ecosystem seeking to game it. Without strong validation, the educational ecosystem is open to data tampering at the expense of employers and students. As physical documents shift to digital assets, threats to the security of visual content increase, along with the increasing sophistication of forgery practices.

The objectives and findings of this study offer both academic and practical contributions. Academically, it serves as a source of literature on the security of digital academic certificates by integrating perspectives on blockchain technology and cryptography. Practically, the results can guide educational institutions and system developers in designing more adaptive, real-time, and transparent digital certificate security and verification strategies. The novelty of this study lies in its analytical focus on integrating blockchain technology with cryptographic techniques as a conceptual and implementation approach for more effective and sustainable digital certificate storage and verification systems.

2. METHOD

The research method adopted is the PRISMA Systematic Literature Review guidelines. In conducting this research, Systematic Literature Review (SLR) refers to a methodology that aims to find, analyze, and access the latest research literature relevant to a particular subject area. Figure 1 below shows the stages of the Systematic Literature Review (SLR) method consisting of: Preparation Stage, Initial Search and Selection, Advanced Selection and Analysis as shown in Figure 1. Systematic Literature Review (SLR) method. A comprehensive explanation of the process stages and details regarding the process can also be seen in more detail.

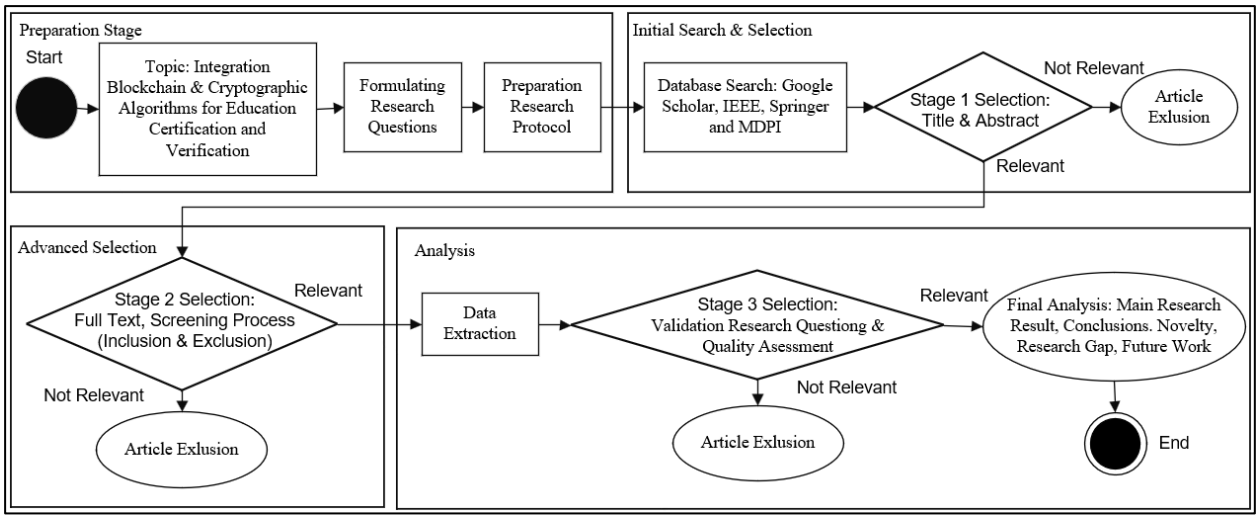

Figure 1. Systematic literature review (SLR) method

More detailed explanation of Figure 1 above is explained in the research design which consists of three stages, namely: Preparation Stage, Initial Stage & Selection and Advanced Selection & Analysis. Based on the framework presented in Figure 1, the literature search strategy was conducted through the following steps:

Preparation Stage

The preparation stage begins with the formulating research topic, developing research questions and developing a research protocol. The topic in this research is "Integration Blockchain & Cryptographic Algorithm for Education Certification and Verification". Formulating Research Questions, the researcher defined three research questions in the following Table 1. Research Questions bellow:

Table 1. Research questions

Code	Research Questions
Q1	Is the research objective in the paper focused on the blockchain security method integrated with cryptography or steganography algorithms?
Q2	Is the object of research in the paper a security issue: certificate or student certificate or graduation certificate or academic credential or digital diploma?
Q3	Can the results contribute to research?

The next process is preparation of the research protocol. The research protocol is a key aspect of any systematic literature review. The following processes are planned in the research protocol: (a) identification of studies, which includes selecting relevant databases to be surveyed, determining search strings, and the inclusion/exclusion process, (b) selection of relevant studies, and (c) the quality assessment process.

Eligibility and Quality Assessment Process is crucial to eliminate bias from the selected studies. The quality assessment criteria in Table 2 were used to ensure that all selected primary studies addressed the research question.

Table 2. Criteria for assessing eligibility and quality assessment

Code	Quality Assessment Factors
P1	Does the paper answer the research questions (Q1–Q3)?
P2	Does the paper comprehensively discuss the following: objectives, methods, tools and conclusions?
P3	Does the paper comprehensively discuss the following: implementation and the review process?
P4	Does the paper contain several significant points including: gap analysis, research contributions, novelty and future work?

Initial Search & Selection

The literature search was carried out using several reputable scientific databases as show in Table 3. Databases. These databases were selected due to their comprehensive coverage of internationally indexed articles relevant to Blockchain (BC) and Cryptographic Algorithm for Education Certification and Verification. The reviewed articles were limited to publications from 2023 to 2026

Table 3. Databases

No	Database	Website
1	Google Scholar	https://scholar.google.com/
2	IEEE	https://ieeexplore.ieee.org/Xplore/home.jsp
3	Springer	https://link.springer.com/
4	MDPI	https://www.mdpi.com/

The literature search employed combinations of search keywords using Boolean operators (AND, OR) as show in Table 4. Search Keywords below:

Table 4. Search keywords

No	Database	Search String	Filters on the website
1	Google Scholar	("Blockchain" OR "Smart Contract" OR "Distributed Ledger") AND (“Certificate” OR “Student Certificate” OR "Graduation Certificate" OR "Academic Credential" OR "Digital Diploma") AND (“Security” OR “authentication”) AND (“Cryptographic” OR “Steganography”)	- Article Period: 2023 – 2026 - Article Type: Research Article
2	IEEE	(Blockchain OR Smart Contract OR Distributed Ledger) AND (Certificate OR Student Certificate OR Graduation Certificate OR Academic Credential OR Digital Diploma) AND (Security OR Authentication) AND (Cryptographic or Steganography)	- Type: Journals - Access Provided by University - Year range: 2023 – 2026
3	Springer	(Blockchain OR Smart Contract OR Distributed Ledger) AND (Certificate OR Student Certificate OR Graduation Certificate OR Academic Credential OR Digital Diploma) AND (Security OR Authentication) AND (Cryptographic or Steganography)	- Content type: Article - Open Access - Date Published: Custom dates - Start Year: 2023, End Year: 2026 - Languages: English - Subject: Blockchain - Disciplines: Computer Science
4	MDPI	(Blockchain OR Smart Contract OR Distributed Ledger) AND (Certificate OR Student Certificate OR Graduation Certificate OR Academic Credential OR Digital Diploma) AND (Security OR Authentication) AND (Cryptographic or Steganography)	- Journal: All Journal - Article Types: Article - Filter Years: 2023 and 2026

The screening process uses all these keywords, so a search method is developed using a search string. The search string is designed using Boolean operators (AND, OR) that combine key terms and their synonyms [16]. The search string combination in the search method can be seen in Table 4 above. For the Google Scholar database, researchers only searched for Indonesian-language papers, while for English-language papers, researchers searched from IEEE, Springer, and MDPI. This was to prevent paper duplication, as many English-language papers found by researchers from Google Scholar were also found in IEEE, Springer, and MDPI. Through the use of this search string, the number of papers obtained was in Table 5. Search results according to the search string for each database below

Table 5. Search results according to the search string for each database

No	Database	Number of articles
1	Google Scholar	160
2	IEEE	189
3	Springer	178
4	MDPI	14

Advanced Selection

The advanced selection process began with the identification of 353 papers through an initial literature search as show in table 5. Then conducted a screening process using inclusion and exclusion criteria as table 6 below.

Table 6. Inclusion and exclusion criteria

No	Inclusion Criteria	Exclusion Criteria
1	Papers must be written in English and Indonesian.	Papers written in languages other than English and Indonesian
2	Papers must be published between 2023 and 2026.	Papers published before 2023
3	Paper type: journal	Papers outside the journal type, for example review papers or SLR Papers
4	Fundamental study: Blockchain research paper beyond the topic of security and personal data protection related to academic certificates with blockchain integrated with cryptography or steganography techniques	Blockchain research papers outside the topic of security and personal data Certificate or Student Certificate or Graduation Certificate or Academic Credential or Digital Diploma protection with blockchain.
5	The papers focus on blockchain implementation for security and protection of personal data especially academic certificates. The title and abstract must be relevant to studies on blockchain for personal data security and protection especially academic certificates.	Security implementations but not personal data protection, for example: network security, IoT security, and others. Personal data security, but not related to blockchain. Blockchain implementations but studies outside the field of informatics, for example, legal aspects, digital systems, e-commerce, and others Journal sources outside informatics journals

Inclusion criteria are conditions that must be met by the literature to be included, such as papers written in English or Indonesian, published between 2023 and 2026, journal papers, and focused on blockchain research for personal data education certificate protection and security, as well as discussing blockchain implementation in that context. Exclusion criteria are conditions that make the literature ineligible for inclusion, such as papers written in languages other than English or Indonesian, published before 2023, not journal papers, and discussions of blockchain outside the topic of personal data security and protection, such as network security or IoT security. In addition, papers discussing personal data security without any relation to blockchain, blockchain implementations outside the field of

informatics (e.g. law or e-commerce), as well as papers irrelevant to the field of informatics were also excluded. This process resulted in 52 relevant papers as show in Table 7 below.

Table 7. Search results after screening process

No	Database	Number of Journals
1	Google Scholar	29
2	IEEE	5
3	Springer	8
4	MDPI	10

Analysis

After the literature has been collected and selected, the next stage involves data analysis. This process aims to identify patterns, themes, and relationships among findings from relevant studies.

Data extraction

Data analysis was conducted by extracting key information into a structured Data Extraction Matrix (spreadsheet). This matrix includes: (1) author and year, (2) research objective, (3) object, (4) framework, (6) algorithm. The 52 selected articles were categorized based on these attributes to ensure consistent comparison.

Analysis method

Data were analysed using thematic content analysis. This process involved initial coding of findings from 52 articles, followed by grouping these codes into a central theme: Integration of Blockchain & Cryptographic Algorithms for Education Certification and Verification. Next, a thematic synthesis process was applied to integrate the findings across the studies.

Validity and reliability of the analysis

To ensure the validity and reliability of the analysis results, each included article was verified for relevance to the Research Questions and the Criteria for Assessing Eligibility and Quality Assessment.

3. RESULTS AND DISCUSSIONS

Characteristics of the Selected Studies

The literature selection process was conducted using a Systematic Literature Review (SLR) approach, focusing on articles published between 2023 and 2026 with the topic "Integration Blockchain & Cryptographic Algorithm for Education Certification and Verification". From searches across major databases including Google Scholar, IEEE, Springer and MDPI a total of 353 papers were identified. These studies were subsequently screened using predefined inclusion and exclusion criteria resulting in 52 papers. The next stage of the screening process involved validating research questions (Q1–Q3) and the assessment criteria (P1–P4) is shown in table 8 below.

Table 8. List of 52 papers for screening research questions criteria and assessment criteria

No	Main Author, Year	Explanation	RQ			Assessment			
			Q1	Q2	Q3	P1	P2	P3	P4
1	Said H. Said, 2025 [17]	**Purpose**: Holistic certificate management and one-stop verification. **Object**: Academic certificates from various levels/institutions. **Framework**: ElimuChain (DApp) with IPFS and Binance Smart Chain. **Algorithm**: Proof of Stake (BSC Consensus) and Smart Contracts		√	√				
2	Rojalina Priyadarshini, 2025 [18]	**Purpose**: Low-cost integrated solution for certificate and issuer validation. **Object**: Educational degree certificates. **Framework**: Ethereum-based decentralized network. **Algorithm**: Hash function mapping and hash-based searching methodology.		√	√				
3	Mohamed Fartitchou, 2025 [19]	**Purpose**: Automate issuance and secure management of digital credentials. **Object**: Moroccan higher education certificates. **Framework**: BlockMEDC using Ethereum Layer 2 (zk-Rollups) and IPFS. **Algorithm**: Zero-Knowledge Rollups (zk-Rollups) for transaction bundling.	√	√	√	√	√		√
4	Laltu Sardar, 2025 [20]	**Purpose**: Instant, cost-free global verification without blockchain overhead. **Object**: Digi-physical academic certificates. **Framework**: FastVer and SFastVer frameworks. **Algorithm**: IbSM tree (Interval-based Sparse Merkle tree) and Digital Signatures	√	√	√	√	√	√	√
5	Khoa Tan-Vo, 2024 [21]	**Purpose**: Optimize revocation performance and detect fraudulent transactions. **Object**: Academic credentials and revocation records. **Framework**: Layer-2 (Arbitrum) with Smart Contracts and ML integration. **Algorithm**: Optimistic Rollups and XGBoost for fraud detection.		√	√				
6	Sumathy Krishnan, 2025 [22]	**Purpose:** Mitigate credential fraud and automate equivalency estimation. **Object:** Degree details and equivalency certificates.		√	√				

		Framework: Cerberus++ network with Merkle Mountain Range (MMR). **Algorithm:** TCRN (Bi-GRU, DSC, BERT) and enhanced MD5 hash.								
7	Mariano A. Cardenas Quispe, 2025 [23]	**Purpose:** Guarantee authenticity and traceability of academic credentials. **Object:** Academic professional qualifications and degrees. **Framework:** Hybrid blockchain network with Docker nodes. **Algorithm:** Byzantine consensus and associative signature.		√	√					
8	Mohamed Al Hemairy, 2024 [24]	**urpose:** Achieve digital transformation in credential issuance and verify authenticity. **Object:** Academic certificates and institutional accreditation. **Framework:** Decentralized storage and Public Key Cryptography. **Algorithm:** ECDSA (Elliptic Curve Digital Signature Algorithm).	√	√	√	√	√	√	√	
9	Xibing Wang, 2025 [25]	**Purpose:** Address trust deficits and data confidentiality in identity management. **Object:** Student digital identity and learning records. **Framework:** BSIMS model within Personal Learning Environments (PLE). **Algorithm:** Smart contracts and private/public blockchain chains		√	√					
10	Sirapat Boonkrong, 2024 [26]	**Purpose:** Detect modifications and verify authenticity of digital documents. **Object:** Digital academic documents. **Framework:** Cryptographic hash-based verification system. **Algorithm:** Cryptographic hash functions.	√	√	√	√	√	√	√	
11	Avni Rustemi, 2024 [27]	**Purpose:** Enhance privacy, transparency, and digitization of diploma services. **Object:** Higher education academic diplomas. **Framework:** DIAR (Diploma Integrity Authentication Record) architecture. **Algorithm:** Standardized smart contracts.	√	√	√	√	√	√	√	
12	Rosa Pericàs-Gornals, 2024 [28]	**Purpose:** Manage non-transferable digital access credentials with explicit acceptance. **Object:** Digital identity and access credentials. **Framework:** RejSBTs (Rejectable Soulbound Tokens) system. **Algorithm:** Solidity smart contracts and RejSBTs logic		√	√					
13	Xiao Xu, 2024 [29]	**Purpose:** Verify disability status while preserving student privacy. **Object:** Disability management records and student identity. **Framework:** Blockchain-powered Zero-Knowledge Proofs (ZKPs). **Algorithm:** zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge).		√	√					
14	Mihai Caramihai, 2023 [30]	**Purpose:** Prevent diploma counterfeiting and automate verification. **Object:** University diplomas and academic credentials. **Framework:** Decentralized blockchain architecture for higher education. **Algorithm:** Not explicitly specified (General Blockchain distributed ledger).		√	√					
15	Juan A. Berrios Moya, 2025 [31]	**Purpose:** Secure, privacy-preserving academic credential verification. **Object:** Academic records and student identities. **Framework:** ZKBAR-V using dual-blockchain and zkEVM. **Algorithm:** Zero-Knowledge Proof (ZKP) and smart contracts.	√	√	√	√	√	√	√	
16	Bogdan Tiganoaia, 2023 [32]	**Purpose:** Support Sustainable Development Goals (SDGs) through secure crowdfunding. **Object:** Social and educational funding projects. **Framework:** Decentralized crowdfunding platform. **Algorithm:** Smart contract-based transaction processing.			√					
17	Ali Saleh Alammary, 2025 [33]	**Purpose:** Streamline and secure cross-institutional student enrollment. **Object:** Student enrollment data across multiple universities. **Framework:** BCHEEN (Cross-Institutional Blockchain Enrollment System). **Algorithm:** Hybrid blockchain architecture.		√	√					
18	Alvaro Gómez Vieites, 2025 [34]	**Purpose:** Achieve GDPR-compliant trusted digital academic certification. **Object:** Digital academic certificates. **Framework:** GAVIN Project (combining private blockchains and consortium nodes). **Algorithm:** HMAC-SHA encryption and smart contracts.	√		√					
19	Zainab Rasheed, 2024 [35]	**Purpose:** Evaluate social impact and improve graduation/verification processes. **Object:** University graduation systems and stakeholders. **Framework:** Social Impact Assessment (SIA) methodological model. **Algorithm:** Distributed Ledger Technology (DLT).		√	√					
20	Shaik Arshiya Sultana, 2023 [36]	**Purpose:** Reduce academic certificate fraud and ensure authenticity. **Object:** Academic certificates and verification data. **Framework:** Conceptual framework integrating IPFS and Blockchain. **Algorithm:** Ethereum-based Smart Contracts and IPFS hashing.	√	√	√	√	√	√	√	
21	Delgado-von-Eitzen, 2024 [37]	**Purpose:** Use NFTs for valid, GDPR-compliant academic accreditation. **Object:** Academic information, skills, and professional experience. **Framework:** Non-Fungible Token (NFT) based validation platform. **Algorithm:** Soulbound tokens/ERC-721 standards.	√	√	√	√	√	√	√	
22	Delgado-von-Eitzen, 2025 [38]	**Purpose:** Qualitative evaluation of GAVIN system adoption and GDPR compliance. **Object:** Academic credential verification			√					

		processes. **Framework:** GAVIN project (Blockchain-based educational management). **Algorithm:** Encryption keys and controlled private environments.								
23	Evrim Tan, 2023 [39]	**Purpose**: Leverage EBSI for cross-border public service verification. **Object**: Cross-border education credentials (Belgium-Italy case). **Framework**: EBSI (European Blockchain Services Infrastructure). **Algorithm**: Action Research methodology for blockchain implementation.		√	√					
24	Ifeyemi, T., 2024 [40]	**Objective**: Secure certificate verification.**Object**: Digital certificates in Nigeria. **Framework**: Celo Blockchain . **Algorithm**: QR Code and metadata hashing.	√	√	√	√	√	√	√	
25	Abdelmagid, R., 2024 [41]	**Objective**: Solve academic certificate fraud. **Object**: Student information and records. **Framework**: Hyperledger Fabric. **Algorithm**: Chaincode and permissioned nodes		√	√					
26	Said, S. H., 2023 [42]	**Objective**: Address manual verification issues **Object**: Certificates in Tanzania. **Framework**: Blockchain & IPFS. **Algorithm**: Smart contracts	√	√	√	√	√	√	√	
27	Harika, B., 2025 [43]	**Objective**: Secure issuance and storage. **Object**: Academic credentials. **Framework**: Blockchain & IPFS. **Algorithm**: ECC & AES encryption	√	√	√	√	√	√	√	
28	Saleh, O. S., 2023 [44]	**Objective**: Preserve identity privacy. **Object**: Diplomas and transcripts. **Framework**: Hyperledger Fabric . **Algorithm**: DCVPC protocol.		√	√					
29	Jayana Kaneriya, 2023 [45]	**Objective**: Ownership and minimal disclosure. **Object**: Educational digital credentials. **Framework**: Ethereum & IPFS. **Algorithm**: Smart contracts.	√	√	√	√	√		√	
30	S. Venkatramulu, 2024 [46]	**Objective**: Secure generation and sharing. **Object**: Academic certificates. **Framework**: Blockchain DApp. **Algorithm**: Selective disclosure.		√	√					
31	Yuhao Zhang, 2024 [47]	**Objective**: Automated certificate management. **Object**: Student credentials. **Framework**: Blockchain platform. **Algorithm**: Smart contracts.		√	√					
32	Onoshioze, 2025 [48]	**Objective**: Combat counterfeit degrees. **Object**: Degrees and diplomas. **Framework**: Ethereum. **Algorithm**: Solidity & NFT tokenization.		√	√					
33	Prof. Sayali Shivarkar, 2025 [49]	**Objective**: Reduce administrative overhead. **Object**: Educational qualifications. **Framework**: Decentralized Ledger. **Algorithm**: Smart contracts	√	√	√	√	√		√	
34	Soumen Mondal, 2023 [50]	**Purpose**: To overcome certificate counterfeiting in e-learning. **Object**: E-certificates/Academic credentials. **Framework**: Automated management system using blockchain. **Algorithm**: Blockchain-based digital certificate system.	√	√	√	√	√		√	
35	Smita Chaudhari, 2023 [51]	**Purpose**: To prevent forgery and manipulation of academic certificates. **Object**: Academic certificates and student records. **Framework**: Decentralized blockchain system. **Algorithm**: Smart contracts for verification and issuance.	√	√	√	√	√		√	
36	Md. Mijanur Rahman, 2023 [52]	**Purpose**: To ensure authenticity and enable secure correction of academic certificates. **Object**: Academic certificate authentication. **Framework**: Blockchain-based authentication system. **Algorithm**: Decentralized assertion and verification.	√	√	√	√	√	√	√	
37	Shivam Gangwar, 2024 [53]	**Purpose**: To address fake degree issues and reduce verification time. **Object**: Educational records and degrees. **Framework**: ReactJs front-end, Ethereum 2.0 back-end, and IPFS. **Algorithm**: Solidity smart contracts and QR code verification	√	√	√	√	√	√	√	
38	Kennedy C. Cuya, 2025 [54]	**Purpose**: To address academic document forgery and verification inefficiencies. **Object**: Academic credentials and records. **Framework**: Immutable and decentralized blockchain system. **Algorithm**: Blockchain-based record management and integrity checks.	√	√	√	√	√	√	√	
39	Md. Ahsan Habib, 2024 [55]	**Purpose**: To efficiently store, manage, and recover credentials without centralized authority. **Object**: University student credentials and results. **Framework**: Blockchain-based Secure Credential Management System (BCMS). **Algorithm**: Modified Two-Factor Encryption (m2FE) using RSA and DNA encoding.	√	√	√	√	√	√	√	
40	Umna Iftikhar, 2025 [56]	**Purpose**: To provide a standardized, cost-effective process for confirming certificate legitimacy. **Object**: Academic certifications and degrees. **Framework**: Decentralized architecture (CERTIFICATELY). **Algorithm**: Cryptographic hash functions and Zero-knowledge proof.	√	√	√	√	√	√	√	
41	Dr. Rashmi H C, 2025 [57]	**Purpose**: To improve security, transparency, and eliminate intermediaries in verification. **Object**: Academic certificates. **Framework**: Ethereum blockchain and React.js front-end. **Algorithm**: Smart contracts for issuance and verification	√	√	√	√	√	√	√	
42	Normi Sham Awang Abu Bakar, 2025 [58]	**Purpose**: To create a secure, unified verification system against counterfeit credentials. **Object**: Academic credentials and engineering degrees. **Framework**: Blockchain-based	√	√	√	√	√		√	

		verification system. **Algorithm**: Blockchain-enabled integrity and authentication protocols.								
43	Pooja M. Pondkule, 2025 [59]	**Purpose:** Enhance authenticity and transparency of academic records. **Object:** Higher education documents/transcripts. **Framework:** Decentralized blockchain framework. **Algorithm:** Smart contracts for automated verification.		√	√					
44	Awatef Salem Balobaid, 2023 [60]	**Purpose:** Securely store and share student records while ensuring confidentiality. **Object:** Student academic records. **Framework:** Private blockchain network using Merkle tree. **Algorithm:** Five-dimensional hyper chaos, dynamic DNA coding, and SHA-256.	√	√	√	√	√		√	
45	A. Janek, 2025 [61]	**Purpose**: To enhance efficiency, security, and global recognition of qualifications. **Object**: Digital diplomas and academic certificates. **Framework**: Decentralized database on Ethereum platform. **Algorithm**: Smart contracts for secure issuance and verification	√	√	√	√	√	√	√	
46	Padmala Harshavardhan, 2024 [62]	**Purpose:** Issue and verify academic certificates securely without compromising privacy. **Object:** Academic credentials/certificates. **Framework:** Permissioned blockchain. **Algorithm:** Merkle tree hashing and smart contracts.	√	√	√	√	√	√	√	
47	Aprianti Nanda Sari, 2025 [63]	**Purpose:** Preserve authenticity and prevent forgery of diplomas. **Object:** Diplomas and academic transcripts. **Framework:** Blockchain architecture integrated with SIVIL **Algorithm:** Not specified in abstract (focused on data integrity).	√	√	√	√	√	√	√	
48	Rashmika Boddupalli, 2024 [64]	**Purpose:** Automate certificate issuance with enhanced security and scalability. **Object:** Academic certificates (Honors & Merit). **Framework:** Django-based web platform with SQL. **Algorithm:** Encryption and Role-Based Access Control (RBAC).	√		√					
49	Shraddha H D, 2025 [65]	**Purpose:** Provide decentralized and immutable storage for certificate verification. **Object:** Academic certificate metadata and files. **Framework:** Ethereum blockchain integrated with IPFS. **Algorithm:** Ethereum Smart Contracts.	√	√	√	√	√	√	√	
50	Ahsan Farabi, 2025 [66]	**Purpose:** Securely issue, verify, and revoke academic credentials in a tamper-proof manner. **Object:** Academic credentials in Bangladesh. **Framework:** Ethereum blockchain with IPFS and React-based DApp. **Algorithm:** Ethereum Smart Contracts.	√	√	√	√	√	√	√	
51	Marian Ileana, 2024 [67]	**Purpose:** Validate and certify educational competencies through blockchain. **Object:** Competencies and educational certifications. **Framework:** Distributed web systems. **Algorithm:** Finite state machines and timed automata.		√	√					
52	Olaiya Samuel Oluwasey, 2024 [68]	**Purpose:** Create a tamper-proof digital certificate system to curb fraud**. Object:** University degree certificates and transcripts. **Framework:** Ethereum-based system with Ganache and Swarm. **Algorithm:** Smart contracts and Proof of Work/Stake consensus.	√	√	√	√	√		√	

Resulting in 21 final papers that met the methodological eligibility and topical relevance requirements. Mapping of Papers with Research Question Criteria and Assessment are show in table 9 below.

Table 9. List of 21 final papers

No	Author, Year	Objective	Novelty	Result & Limitation	Future Work
1	Laltu Sardar, 2025 [20]	Enable instant, global academic certificate verification without the high cost and complexity of blockchain	Proposes "FastVer," a non-blockchain framework using Merkle trees for membership proofs and IbSMT for efficient certificate revocation within a bottom-up trust model.	Result: Achieved verification times of just a few microseconds and successfully generated a Merkle tree for 1 million certificates in 4 seconds. Limitation: Assumes local authorities are "quasi-honest" and was tested only on a single-machine setup with simulated data.	Piloting with real government bodies, integrating AI for fraud detection, and exploring IoT-enabled verification points like smart gates.
2	Mohamed Al Hemairy, 2024 [24]	Create a secure blockchain framework for the issuance, storage, sharing, and equivalency of academic credentials	Integrates multi-party ECDSA signatures, AES encryption to protect sensitive on-chain data, and user-managed private keys.	Result: Developed using the MERN stack on the BSV Blockchain, achieving high scalability (50,000 TPS), low latency (1-3s), and extremely low transaction costs Limitation: Focuses on general adoption hurdles like regulatory compliance and ongoing privacy concerns rather than specific system flaws	Expanding the system to track professional achievements (e.g., experience letters) and integrating it with professional networks like LinkedIn
3	Sirapat Boonkrong, 2024 [26]	Detect academic document forgery using cryptographic hash functions rather	Completely avoids blockchain technology, relying solely on key-based HMAC-SHA512	Result: Achieved 100% detection accuracy with a rapid 0.352 ms verification speed, outperforming	Developing a mobile application for verification and extending the system

		than complex infrastructures.	hashing for data tampering detection.	CNN, blockchain, and digital signature methods. Limitation: Requires access to the original document's hash value for comparison and places a secure key management burden on issuing institutions	to a wider range of document types
4	Avni Rustemi, 2024 [27]	Propose DIAR, a 7-layer blockchain framework for the secure generation, verification, and revocation of academic diplomas	Treats entire diplomas as unique non-fungible tokens (NFTs) rather than tokenizing individual credits , and integrates hybrid off-chain storage (IPFS) with advanced privacy protections like Zero-Knowledge Proofs.	Result: Successfully designed a comprehensive conceptual model, system architecture, and smart contract architecture to manage diploma lifecycle. Limitation: System remains in the conceptual and prototype phase and acknowledges inherent blockchain challenges such as slow transaction speeds and high maintenance costs	Developing the Solidity smart contracts, building user interfaces, deploying on the Ethereum Virtual Machine, and conducting empirical functionality testing.
5	Juan A. Berrios Moya, 2025 [31]	Develop ZKBAR-V, a privacy-preserving and secure academic credential verification system	Uniquely combines Zero-Knowledge Proofs (ZKPs), Decentralized Identifiers (DIDs), a dual-blockchain (public/private) architecture, and IPFS off-chain storage.	Result: Efficiently processed up to 280 concurrent requests , reduced transaction costs by ~94% using zkEVM Polygon, and achieved ~120x faster verification latency compared to standard EVM Limitation: System performance degrades past 280 concurrent requests ; lacks testing for real-time IPFS retrieval, multi-language support, and user accessibility.	Execution of large-scale pilot deployments, user studies, and performance benchmarking under varying network conditions
6	Shaik Arshiya Sultana, 2023 [36]	Create a secure, decentralized framework for academic certificates using blockchain and IPFS to reduce fraud.	Uses a unique lightweight homomorphic encryption algorithm (Tetrahedral and Penta tope keys) to secure data before storing identifiers on the blockchain.	Result: Demonstrated resistance to Brute force and Sybil attacks, with processing times that scale linearly with the number of certificates. Limitation: Potential for increased transaction latency and scalability issues when handling a very large volume of records.	Researching regulatory and legal compliance for broader adoption and addressing high-volume implementation challenges
7	Delgado-von-Eitzen, 2024 [37]	Introduce a GDPR-compliant NFT model for issuing and verifying academic credentials.	Uses dynamic token URIs to separate public on-chain data from private off-chain data, ensuring the data subject's control and the "right to be forgotten".	Result: Developed an Ethereum-based MVP proving that tamper-proof, verifiable digital diplomas can strictly align with European privacy regulations. Limitation: Requires some centralization for personal data storage and faces scalability constraints inherent in public blockchains like Ethereum.	Focusing on improving technical scalability via private blockchains and researching global interoperability frameworks.
8	Ifeyemi, T., 2024 [40]	Build a tamper-proof blockchain system for issuing and verifying digital academic certificates at Olabisi Onabanjo University	Uses the eco-friendly and lightweight Celo blockchain paired with MongoDB for data storage, featuring instant QR code verification	Result: Achieved high user ratings (82% for blockchain security, 78% for UI), proving it simplifies the verification process Limitation: Currently limited to one university and requires specialized Web3 knowledge to maintain	Enhancing security measures, expanding the system for use in other institutions and industries, and support additional document types
9	Said, S. H., 2023 [42]	Propose a blockchain conceptual model to solve educational certificate verification challenges in Tanzania..	Customized for Tanzania, it features regulatory management, handles foreign equivalent certificates, and utilizes off-chain IPFS storage	Result: Conceptually proved that the model resolves manual and centralized system flaws by enabling decentralized, independent verification. Limitation: It is strictly a conceptual design and lacks a full real-world implementation.	Build and evaluate a practical proof-of-concept on a smart-contract platform like Ethereum.
10	Harika, B., 2025 [43]	Develop a secure, decentralized academic certificate system using blockchain and IPFS to prevent forgery and data tampering	Integrates AES for certificate encryption, Elliptic Curve Cryptography (ECC) for key security, and off-chain IPFS storage to ensure privacy while minimizing on-chain data limits.	Result: Successfully tested on the Ethereum Spolia test net , featuring fast verification times (~100 ms) and cost-effective certificate issuance (0.0011-0.0013 ETH). Limitation: System performance is subject to network latency, causing slight delays during IPFS uploads (~1.2 seconds) and blockchain confirmations (10-15 seconds)	Paves the way for broader, real-world adoption of blockchain-based verification systems across the education sector and other industries
11	Md. Mijanur Rahman, 2023 [52]	Build a secure blockchain system that generates, authenticates, and corrects academic	Introduces a unique editing function utilizing a dual-chain architecture (a certificate chain and a correction chain) to fix generation errors, a	Result: The smart contract was successfully written, tested on the Remix IDE, deployed on the Gerritsen network, and connected to a frontend web application via a MetaMask wallet	The architecture can be expanded to handle professional degree management and National Identity Card

		certificates to eliminate forgery	feature absent in existing systems	Limitation: The paper does not explicitly state any technical limitations regarding its proposed framework	(NID) verification systems.
12	Shivam Gangwar, 2024 [53]	Build a blockchain-based DAPP with QR codes for fast, low-cost academic certificate verification.	Combines Ethereum 2.0, IPFS storage, and QR code scanning for instant, serverless credential authentication.	Result: Successfully tested on test networks (Ganache/Goerli), achieving extremely low transaction costs (under $1) and eliminating server maintenance fees. Limitation: Student details currently require manual data entry by the issuer	Automating data entry via cloud integration, adding automated email delivery for certificates, and expanding the system to government document verification.
13	Kennedy C. Cuya, 2025 [54]	Implement an effective anti-forgery mechanism for academic documents utilizing blockchain, IPFS, and hash functions.	Combines off-chain IPFS storage for large document files with on-chain blockchain storage for document hashes and UUIDs	Result: Successfully enabled real-time, tamper-proof document verification by cross-referencing user wallet addresses, UUIDs, and PDF files Limitation: Heavily reliant on digital infrastructure (internet access) and faces hurdles regarding public understanding and adoption of blockchain	Expanding the system to support diverse document formats and adding interactive features for broader industry adoption
14	Md. Ahsan Habib, 2024 [55]	Develop a distributed and tamper-proof blockchain-based secure credential management system (BCMS) for storing, managing, and recovering academic credentials without direct central authority involvement	Integrates a modified two-factor encryption (m2FE) using RSA and DNA encoding, and utilizes a Character to Integer (C2I) table instead of an ASCII table to reduce data size and conversion time.	Result: Successfully reduced overhead by up to 33%, achieved a lower cipher ratio (2.5), and demonstrated faster data retrieval performance compared to standard systems. Limitation: The processing time required for asymmetric key encryption (RSA) remains too high.	Suggests implementing symmetric key encryption methods to significantly reduce encryption and decryption times..
15	Umna Iftikhar, 2025 [56]	Develop a decentralized architecture to make the process of verifying digital credentials quicker, simpler, and more cost-effective.	The system combines real-time verification capabilities with zero-knowledge proof mechanisms through a web application called "Certificate", enabling users to retrieve certificates without paying gas fees.	Result: The platform demonstrated high scalability and achieved a 99.8% success rate for certificate retrieval. It also successfully eliminated intermediate agencies and reduced administrative expenses Limitation: Transaction processing times were longer than anticipated (approximately 5 minutes) due to the complexity of smart contract compilation and encryption measures.	The authors plan to adopt layer-2 solutions like Polygon to reduce gas fees, establish a worldwide database of approved institutions, and extend the platform to verify professional and vocational credentials.
16	Dr. Rashmi H C, 2025 [57]	Build a decentralized, blockchain-based system for issuing and verifying academic certificates to improve security and efficiency.	Combines Ethereum smart contracts, a React.js interface, and QR-coded digital and physical certificates for instant, intermediary-free validation.	Result: Achieved 100% data integrity and reduced verification time to 10 seconds, compared to 300 seconds for manual methods. Limitation: Faces scalability challenges and requires human intervention for evaluating subjective academic assessments.	Incorporating additional blockchain platforms like Hyperledger to improve system robustness and interoperability.
17	A. Janek, 2025 [61]	Build a decentralized Ethereum-based application for secure academic certificate issuance and verification.	Incorporates an ERC-20 tokenization mechanism to manage payments and redemption incentives for certificates	Result: Developed a functional DApp (using React.js, MetaMask, MongoDB, and Solidity) that enables tamper-proof, real-time certificate validation. Limitation**:** Faced Solidity stack limits (e.g., "Stack too deep" errors) requiring parameter reduction, and needs further real-world testing.	Integrating external data, optimizing Ethereum operational costs, improving the user experience, and ensuring data privacy compliance.
18	Padmala Harshavardhan, 2025 [62]	Create a decentralized, tamper-proof platform for secure academic certificate issuance and verification.	Implements a "selective disclosure" model using Merkle trees and dual QR codes to protect sensitive student data while allowing instant verification	Result: Developed an Ethereum-based prototype with role-specific dashboards (student, university, recruiter) that verifies credentials in real-time. Limitation: Primarily evaluated in local development environments (Ganache) and requires Ethereum-compatible infrastructure for real-world scaling.	Integrating Decentralized Identifiers (DIDs), multi-chain compatibility, and biometric authentication for enhanced security.
19	Aprianti Nanda Sari, 2025 [63]	Integrate blockchain for preserving diploma authenticity and	Ensures compliance with Indonesian Regulation 59/2018 by omitting	Result: Developed a Python prototype that successfully ensures data integrity, non-repudiation, and	Collaborating with universities for pilot testing and deploying

		resolving centralized storage risks in Indonesia.	physical QR codes on original documents and uses text-based storage to minimize memory usage.	traceability while detecting invalid blockchain states. Limitation: Currently in the prototype stage operating within a single-node environment.	across multiple nodes to evaluate scalability and fault tolerance.
20	Shraddha H D, 2025 [65]	Implement a secure, real-time, and decentralized academic certificate authentication framework.	Combines Ethereum smart contracts and IPFS with Firebase Authentication and an intuitive Stream lit dashboard for enhanced institutional usability.	Result: Successfully enabled tamper-proof storage and automated verification, significantly reducing administrative overhead and document forgery risks. Limitation: The system relies on a public blockchain and remains susceptible to errors during the initial manual data entry phase	Incorporating AI for automated data extraction, implementing Zero Knowledge Proofs (ZKP) for privacy, and exploring private blockchain alternatives like Hyperledger.
21	Ahsan Farabi, 2025 [66]	Create a decentralized, tamper-proof system for issuing, verifying, and revoking academic credentials in Bangladesh.	Features a four-tier role-aware governance model (government, regulator, institution, public) and integrates Ethereum with IPFS using on-chain CIDs for scalability.	Result: Developed a functional React-based DApp prototype that enables real-time QR and hash-based verification, reducing manual processing time. Limitation: Faces high gas costs and latency on the Ethereum main net, and metadata is currently exposed publicly once the CID is known.	Implementing Layer-2 scaling, Zero-Knowledge Proofs for privacy, and AI-driven anomaly detection to identify fraudulent patterns.

Result Analysis

The analysis of the literature review findings is systematically organized using the following assessment criteria: trends and research, technology and innovation, further research opportunities, comparative analysis, performance evaluation, and security vs. scalability.

Trends and research

The research focus demonstrates a strong transition from theoretical experiments (Proof of Concept) to architectural implementation. The majority of research focuses on the development of decentralized identity and the implementation of Self-Sovereign Identity (SSI). A paradigm shift is underway from a system in which institutions retain full control over data to one in which students have absolute ownership and autonomy over their credentials.

Technology trends and innovations

The most prominent innovation is the adoption of a hybrid storage architecture. This system no longer burdens the blockchain with large documents; instead, the Interplanetary File System (IPFS) is used for off-chain storage, while the blockchain stores only cryptographic hash trails via Smart Contracts. Other key innovations include the integration of Zero-Knowledge Proofs (ZKP) to maintain privacy during verification, the use of Soulbound Tokens (SBT), non-transferable NFT-derived tokens (such as those based on the ERC-5484 standard), to represent permanent academic achievement, and the use of advanced encryption techniques such as DNA Encoding for additional data abstraction.

Comparative analysis

The analysed literature consistently compares three major infrastructure models. Centralized systems (such as traditional ministry databases) excel in ease of operation but are vulnerable to single points of failure and internal manipulation. Public blockchains (e.g., Ethereum) offer absolute invulnerability and full transparency but are hampered by volatile gas fees. As a counterbalance, consortium/permissioned blockchains (such as Hyperledger) are increasingly dominating proposed architectures for university networks, as they can restrict read-write access to authorized institutions while keeping transaction costs manageable.

Performance evaluation

The key performance parameters evaluated focus on reduced verification time and computational efficiency. Decentralized Application (DApp)-based interfaces combined with QR code scanning have been empirically proven to reduce authentication time from several weeks to mere milliseconds. In terms of accuracy, the avalanche effect mechanism in hash functions (such as SHA-256) demonstrates a 100% success rate in detecting even the slightest anomalies in counterfeit digital documents.

Security vs Scalability

Current academic credential architectures grapple with the Blockchain Trilemma. Storing raw academic data within the blockchain maximizes cryptographic security, but also leads to ledger bloat, an anomaly that hampers scalability. Maintaining document integrity and security with standard encryption (RSA/ECC) requires a permanent audit trail, ultimately leading to ledger bloat as the number of graduates increases. Current approaches address this scalability barrier through Layer-2 Scalability implementations (such as Polygon) that process large transaction volumes off-blockchain, maintaining network security without sacrificing national-scale processing speeds.

Gap and challenge analysis

Based on a systematic review of 21 existing literature, although blockchain-based academic credential verification technology has reached the prototype and early implementation stages, several critical gaps remain unresolved:

The privacy-immutability paradox

The biggest challenge consistently emerging in the literature (such as in studies addressing GDPR compliance) is the clash between the fundamental nature of blockchain and modern privacy laws. Blockchains guarantee immutability (data cannot be changed/deleted), while data protection regulations such as the Personal Data Protection Act (PDP) in Indonesia or the GDPR in Europe guarantee the "Right to be Forgotten." Current systems using hybrid storage architectures (IPFS) still struggle to design a mechanism by which physical diploma data can be deleted off-chain without compromising the integrity of the on-chain hash tree (Merkle Tree).

Vulnerabilities of classical cryptographic infrastructure

The majority of the systems proposed in the 21 documents (including implementations on Ethereum, Celo, or Hyperledger) still rely heavily on classical cryptographic algorithms, such as the Elliptic Curve Digital Signature Algorithm (ECDSA) and RSA. The fundamental gap here is the lack of anticipation of future computational threats. These algorithms are vulnerable to quantum decryption, which could undermine the entire foundation of digital certificate security in the next few years.

Fragmentation and lack of cross-chain interoperability

The literature shows many successful local platform developments (such as in Bangladesh, Tanzania, or the United Arab Emirates). However, this creates a siloed architecture. There is no standard cross-chain communication protocol that would allow immigration authorities or companies on one continent to directly and seamlessly verify diplomas issued by smart contracts on another continent.

Scalability vs. Transaction costs (the blockchain trilemma)

Although Layer 2 has been proposed, existing research still faces challenges in balancing the security of decentralization with low operating costs. Fluctuating gas fees on public networks make mass institutional adoption for millions of diploma documents economically inefficient.

Recommendations For The Future Research

Following are some recommendations for future research that would provide significant novelty to the academic literature.

Transition toward post-quantum cryptography (PQC)

Future research should explore integrating post-quantum cryptographic algorithms into blockchain architectures for diploma verification systems. The implementation of hash-based signature schemes (such as SPHINCS+) is highly recommended to standardize the security of digital certificates.

Exploration of advanced hybrid encryption algorithms

Future studies should design more complex security layers. Integrating algorithms such as Chaotic DNA-Quantum Walk could be a highly innovative research avenue. This approach offers a dynamic, high-level method of data randomization and encryption, creating a double defense far superior to the conventional SHA-256 hash function.

Regulatory compliance governance design **(PDP/GDPR Laws)**

Combining the privacy advantages of Zero-Knowledge Proofs (ZKP) with the ability to execute data erasure. The goal is to create a smart contract design that allows for legitimate state modification, or "unlinking," between on-chain identities and off-chain documents, enabling institutions to fully comply with national and international personal data protection regulations.

Strengthening methodological evaluation

Future research should utilize international reporting standards. During data extraction and synthesis, research findings will remain objective, transparent, and recognized as valid by national and international scientific journals.

4. CONCLUSION

Research on academic credentials from 2023 to 2026 indicates a shift from centralized databases to decentralized frameworks powered by blockchain technology. To address the inherent "blockchain trilemma" of balancing scalability, security, and transaction costs, contemporary research largely advocates hybrid storage architectures that combine on-chain cryptographic hashing with off-chain storage via the Interplanetary File System (IPFS). This paradigm not only reduces verification latency and maintains complete fraud detection accuracy but also increasingly integrates advanced privacy mechanisms. Innovations such as Zero-Knowledge Proofs (ZKP) and Soul bound Tokens (ERC-5484) can give students full control over their digital identities while securely and selectively

enabling student documentation. Despite these significant technological advances, widespread adoption of blockchain-based verification systems at institutions remains hampered by regulatory and critical infrastructure barriers. The fundamental immutability of distributed ledgers inherently conflicts with modern data protection regulations, such as the "Right to Be Forgotten" in the GDPR, necessitating the development of new, legally compliant off-chain data management protocols. Furthermore, current implementations are often fragmented into institutional silos, lack the cross-chain interoperability necessary for seamless credential verification, and rely heavily on classical cryptography, which is vulnerable to future quantum computing threats. Future research should prioritize addressing these infrastructure and regulatory gaps to build a truly secure and universally trusted ecosystem for academic records. Research should focus heavily on integrating Post-Quantum Cryptography (PQC), such as hash-based signature schemes, to protect digital certificates from next-generation computational attacks. Furthermore, future research should explore standardized, globally interoperable protocols (cross-chain bridges) to enable seamless verification, while investigating AI-based data extraction and advanced Layer-2 scaling solutions to eliminate manual entry errors and efficiently manage national-level credential volumes.

REFERENCES

[1] M. Zulfadhilah, Y. Prayudi, dan I. Riadi, "Cyber Profiling using Log Analysis and K-Means Clustering A Case Study Higher Education in Indonesia," *IJACSA - Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, hal. 430–435, 2016, doi: https://doi.org/10.14569/IJACSA.2016.070759.

[2] A. F. Islami dan M. A. I. Palereng, "Literature analysis on the role of artificial intelligence in addressing fraud in digital financial services," *J. Soft Comput. Explor.*, vol. 6, no. 4, hal. 295–302, 2026, doi: https://doi.org/10.52465/joscex.v6i4.637.

[3] Rosmiati, I. Riadi, dan Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," *Int. J. Comput. Appl.*, vol. 141, no. 8, hal. 1–6, 2016, doi: https://doi.org/10.5120/IJCA2016907930.

[4] R. Umar, I. Riadi, dan R. S. Kusuma, "Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method," *IJID (International J. Informatics Dev.*, vol. 10, no. 1, hal. 53–61, 2021, doi: https://doi.org/10.14421/ijid.2021.2423.

[5] R. Umar, I. Riadi, M. Ihya, dan A. Elfatiha, "Security analysis of web-based academic information system using OWASP framework," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 4, 2024, doi: https://doi.org/10.22219/kinetik.v9i4.2015.

[6] Y. Farida, A. D. Azzahra, A. A. Lestari, S. Siswantyo, A. D. Handayani, dan D. F. Priambodo, "A Security Enhancement To The Secure Mutual Authentication Protocol For Fog/Edge," *Janapati*, vol. 14, no. 1, hal. 73–80, 2025, doi: https://doi.org/10.23887/janapati.v14i1.84725.

[7] Z. Munawar, N. Indah Putri, I. Iswanto, dan D. Widhiantoro, "Analisis Keamanan Pada Teknologi Blockchain," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 8, no. 2, hal. 67–79, 2023, doi: https://doi.org/10.32897/infotronik.2023.8.2.2062.

[8] P. Verma dan B. Ram, "Application of blockchain technology in data security," *IP Indian J. Libr. Sci. Inf. Technol.*, vol. 29, no. 1, hal. 51–55, 2024, doi: https://doi.org/10.18231/j.ijlsit.2024.008.

[9] A. Fadlil, I. Riadi, dan A. Nugrahantoro, "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification," *J. Hari. Reg.*, vol. 11, no. 3, hal. 155–166, 2020, doi: https://doi.org/10.24843/LKJITI.2020.v11.i03.p04.

[10] R. M. Gonçalves, M. M. da Silva, dan P. R. da Cunha, "Olympus: a GDPR compliant blockchain system," *Int. J. Inf. Secur.*, vol. 23, no. 2, hal. 1021–1036, 2024, doi: https://doi.org/10.1007/s10207-023-00782-z.

[11] I. Riadi, A. Z. Ifani, dan R. S. Kusuma, "Optimization and Evaluation of Authentication System using Blockchain Technology," *Emerg. Sci. J.*, vol. 4, no. February, hal. 225–240, 2022, doi: http://dx.doi.org/10.28991/esj-2021-SP1-015.

[12] I. Riadi, T. Ahmad, R. Sarno, P. Purwono, dan A. Ma, "Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study : COVID-19 Data)," *Emerg. Sci. J. Vol.*, vol. 4, no. February, hal. 190–206, 2022, doi: http://dx.doi.org/10.28991/esj-2021-SP1-013.

[13] I. Riadi, R. Umar, I. Busthomi, dan A. Wirawan, "Block-hash of blockchain framework against man-in-the- middle attacks," *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 8, no. 1, hal. 1–9, 2022, doi: https://doi.org/10.26594/register.v8i1.2190.

[14] R. Zhu, M. Wang, X. Zhang, dan X. Peng, "Investigation of personal data protection mechanism based on blockchain technology," *Sci. Rep.*, vol. 13, no. 1, hal. 1–18, 2023, doi: https://doi.org/10.1038/s41598-023-48661-w.

[15] B. Dwi *et al.*, "Evaluating The Acceptance of Blockchain Technology In The Supply Chain of Lombok Traditional Weaving Industry Using Extended Technology Acceptance Model," *Janapati*, vol. 14, no. 2, hal. 408–420, 2025, doi: https://doi.org/10.23887/janapati.v14i2.92595.

[16] B. Alamri, K. Crowley, dan I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," *IEEE Access*, vol. 10, hal. 59612–59629, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3180367.

[17] S. H. Said, R. S. Sinde, E. M. Kosia, dan M. A. Dida, "A Comprehensive Blockchain-Based System for Educational Qualifications Management and Verification to Counter Forgery," *IEEE Access*, vol. 13, no. February, hal. 31562–31589, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3542545.

[18] R. Priyadarshini *et al.*, "A Faster , Integrated , and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," *IEEE Access*, vol. 13, no. January, hal. 27037–27049, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3539180.

[19] M. Fartitchou, I. Lamaakal, K. El Makkaoui, dan Y. Maleh, "BlockMEDC : Blockchain Smart Contracts System for Securing Moroccan Higher Education Digital Certificates," *IEEE Access*, vol. 13, no. March, hal. 39152–39175, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3546177.

[20] L. Sardar, "Fake Me If You Can : Unforgeable Digi-Physical Academic Certificates With Instant Verifiability," *IEEE Access*, vol. 13, no. June, hal. 118334–118353, 2025, doi: https://doi.org/10.1109/ACCESS.2025.3583184.

[21] K. Tan-vo *et al.*, "Optimizing Academic Certificate Management With Blockchain and Machine Learning : A Novel Approach Using Optimistic Rollups and Fraud Detection," *IEEE Access*, no. August, hal. 168135–168159, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3486029.

[22] S. Krishnan, S. Rajendran, dan M. Zakariah, "A secured accreditation and equivalency certification using Merkle mountain range and transformer based deep learning model for the education ecosystem," *Sci. Rep.*, vol. 15, no. 22511 |, hal. 1–21, 2025, doi: https://doi.org/10.1038/s41598-025-06789-x.

[23] M. A. Cardenas-Quispe dan A. Pacheco, "Blockchain ensuring academic integrity with a degree verification prototype," *Sci. Rep.*, vol. 15, no. 1, hal. 9281, 2025, doi: https://doi.org/10.1038/s41598-025-93913-6.

[24] M. Al Hemairy, M. A. Talib, A. Khalil, A. Zulfiqar, dan T. Mohamed, "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022),"

Educ. Inf. Technol., vol. 29, no. 14, hal. 18203–18232, 2024, doi: https://doi.org/10.1007/s10639-024-12493-6.
[25] X. Wang, X. Xu, V. Ngan, L. Lei, dan S. Hao, "Conceptual design of the Blockchain - based Student Identity Management System (BSIMS) model for higher education personal learning environments," *Discov. Comput.*, vol. 28, no. 1, hal. 42, 2025, doi: https://doi.org/10.1007/s10791-025-09545-x.
[26] S. Boonkrong, "Design of an academic document forgery detection system," *Int. J. Inf. Technol.*, vol. 17, no. 9, hal. 5175–5187, 2025, doi: https://doi.org/10.1007/s41870-024-02006-6.
[27] A. Rustemi, F. Dalipi, V. Atanasovski, dan A. Risteski, "DIAR : a blockchain - based system for generation and verification of academic diplomas," *Discov. Appl. Sci.*, vol. 6, no. 6, hal. 297, 2024, doi: https://doi.org/10.1007/s42452-024-05984-1.
[28] R. P. Macià, M. M. M. P. Miquel, dan J. Ramis-bibiloni, "Digital credentials management system using rejectable soulbound tokens," *Ann. Telecommun.*, vol. 79, no. 11, hal. 843–855, 2024, doi: https://doi.org/10.1007/s12243-024-01032-6.
[29] X. Xu, "Zero - knowledge proofs in education : a pathway to disability inclusion and equitable learning opportunities," *Smart Learn. Environ.*, vol. 11, no. 1, hal. 7, 2024, doi: https://doi.org/10.1186/s40561-024-00294-w.
[30] M. Caramihai dan I. Severin, "A Blockchain-Based Solution for Diploma Management in Universities," *MDPI*, vol. 15, no. 20, hal. 1–22, 2023, doi: https://doi.org/10.3390/su152015169.
[31] J. A. B. Moya, J. Ayoade, dan M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," *MDPI*, vol. 25, no. 11, hal. 1–24, 2025, doi: https://doi.org/10.3390/s25113450.
[32] B. Tiganoaia dan G.-M. Alexandru, "Building a Blockchain-Based Decentralized Crowdfunding Platform for Social and Educational Causes in the Context of Sustainable Development," *MDPI*, vol. 15, no. 23, hal. 1–19, 2023, doi: https://doi.org/10.3390/su152316205.
[33] C. Enrollment dan A. S. Alammary, "Building a Sustainable Digital Infrastructure for Higher Education : A Blockchain-Based Solution for," *MDPI*, vol. 17, no. 1, hal. 194, 2025, doi: https://doi.org/10.3390/su17010194.
[34] A. G. Vieites, C. Delgado-von-eitzen, dan D. E. Garcia, "GDPR-Compliant Academic Certification via Blockchain : Legal and Technical Validation of the GAVIN Project," *MDPI*, vol. 15, no. 9191, hal. 1–34, 2025, doi: https://doi.org/10.3390/app15169191.
[35] Z. Rasheed, "Integrating Blockchain Technology into a University Graduation System," *MDPI*, vol. 2, no. 3, hal. 514–525, 2023, doi: https://doi.org/10.3390/higheredu2030031.
[36] S. A. Sultana, C. Rupa, R. P. Malleswari, dan T. R. Gadekallu, "IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field," *MDPI*, vol. 14, no. 8, hal. 1–19, 2023, doi: https://doi.org/10.3390/info14080446.
[37] C. Delgado-von-eitzen, L. Anido-rif, dan M. J. Fernández-Iglesias, "NFTs for the Issuance and Validation of Academic Information That Complies with the GDPR," *MDPI*, vol. 14, no. 2, hal. 706, 2024, doi: https://doi.org/10.3390/app14020706.
[38] C. Delgado-von-Eitzen, L. Anido-Rifón, M. J. Fernández-Iglesias, dan M. Ruiz-Molina, "Qualitative Analysis of a Blockchain-Based System Adoption for Academic Credentials Verification That Complies with the GDPR : GAVIN Project," *MDPI*, vol. 15, no. 22, hal. 1–31, 2025, doi: https://doi.org/10.3390/app152211958.
[39] E. Tan, E. Lerouge, J. Du Caju, dan D. Du Seuil, "Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy," *MDPI*, vol. 7, no. 79, hal. 1–20, 2023, doi: https://doi.org/10.3390/bdcc7020079.
[40] T. Ifeyemi, A. Oyedeji, dan F. Adebiyi, "A Blockchain-Based Digital Educational Certificate Verification System," *J. Eng. Technol. Ind. Appl.*, vol. 10, no. 49, hal. 35–41, 2024, doi: https://doi.org/10.5935/jetia.v10i49.1145.
[41] R. Abdelmagid, M. Abdelsalam, dan F. K. Alsheref, "A Blockchain Framework for Academic Certificates Authentication," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, hal. 297–305, 2024, doi: http://dx.doi.org/10.14569/IJACSA.2024.0150729.
[42] S. H. Said, M. A. Dida, E. M. Kosia, dan R. S. Sinde, "A Blockchain-based Conceptual Model to Address Educational Certificate Verification Challenges in Tanzania," *Eng. Technol. Appl. Sci. Res.*, vol. 13, no. 5, hal. 11691–11704, 2023, doi: https://doi.org/10.48084/etasr.6170.
[43] B. Harika, C. Sidhardha, dan K. Manikanta, "A Decentralized Approach to Academic Certificate Management Using Blockchain and IPFS," *Int. J. Sci. Res. Eng. Manag.*, vol. 9, no. 5, hal. 1–7, 2025, doi: https://doi.org/10.55041/IJSREM47151.
[44] O. S. Saleh, O. Ghazali, dan N. B. Idris, "A New Privacy-Preserving Protocol for Academic Certificates on Hyperledger Fabric," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 2, hal. 595–609, 2023, doi: http://dx.doi.org/10.14569/IJACSA.2023.0140271.
[45] J. Kaneriya dan H. Patel, "A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology," *Int. J. Inf. Educ. Technol.*, vol. 13, no. 8, hal. 1251–1260, 2023, doi: https://doi.org/10.18178/ijiet.2023.13.8.1927.
[46] S. Venkatramulu *et al.*, "A Secure Blockchain Based Student Certificate Generation and Sharing System," *J. Sensors, IoT Heal. Sci.*, vol. 02, no. 01, hal. 17–27, 2024, doi: https://doi.org/10.69996/jsihs.2024003.
[47] Y. Zhang, J. Wu, H. Yi, H. Zhou, dan W. Deng, "A Smart Contract Based Academic Certificate System," *ACM Digit. Libr.*, no. September 2024, hal. 426–433, 2025, doi: https://doi.org/10.1145/3689236.3689325.
[48] Onoshooze, Ahubele, dan Obahiagbon, "Academic Certificate Verification Framework Using Blockchain Technology," *BIU J. Basic Appl. Sci.*, vol. 10, no. 1, hal. 42–55, 2025, doi: https://oer.biu.edu.ng/2025/05/13/biujbas-101_4/.
[49] S. Shivarkar, S. Atram, T. Devare, N. Kore, dan T. Labhade, "Academic Certificate Verification Using Decentralized Digital Certification," *Int. J. Sci. Res. Eng. Manag.*, vol. 9, no. 2, hal. 1–5, 2025, doi: https://doi.org/10.55041/IJSREM41735.
[50] S. Mondal, A. Panja, dan S. Karforma, "An efficient e-certificate management system in e-learning using blockchain," *Sci. Cult.*, vol. 89, no. 3–4, hal. 120–124, 2023, doi: https://doi.org/10.36094/sc.v89.2023.An_Efficient_E-certificate_Management_System.Mondal.120.
[51] S. Chaudhari, S. Mohite, S. Kumbhakarn, V. Rathod, dan S. Khairnar, "Blockchain based solution for academic certificate management system using smart contract," *Int. J. Sci. Res. Arch.*, vol. 08, no. 01, hal. 291–297, 2023, doi: https://doi.org/10.30574/ijsra.2023.8.1.0037.
[52] M. Rahman, S. R. Shihab, T. K. Tonmoy, dan R. Farhana, "Blockchain-based certificate authentication system with enabling correction," *J. Comput. Commun.*, vol. 11, no. 3, hal. 73–82, 2023, doi: https://doi.org/10.4236/jcc.2023.113006.
[53] S. Gangwar dan A. Chaurasia, "Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications," *Int. J. ofComputer Appl.*, vol. 186, no. 26, hal. 1–10, 2024, doi: 10.5120/ijca2024923722.
[54] K. C. Cuya dan T. D. Palaoag, "Blockchain in Higher Education : Advancing Security , Verification , and Trust in Academic Credentials," *Nanotechnol. Perceptions*, vol. 20, no. S3, hal. 373–386, 2024, doi: https://doi.org/10.62441/nano-ntp.v20iS3.596.
[55] A. Habib, M. Rahman, dan N. H. Neom, "CredSec : A Blockchain-based Secure Credential Management System for University Adoption," *arXivLabs*, hal. 10, 2024, doi: https://doi.org/10.48550/arXiv.2406.05151.
[56] U. Iftikhar, H. M. Attaullah, I. U. Khan, M. M. Alam, M. M. Su'ud, dan A. Sajid, "Cryptographically secure digital certificates on a distributed ledger," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 40, no. 1, hal. 236–262, 2025, doi: http://doi.org/10.11591/ijeecs.v40.i1.pp236-262.
[57] D. R. H. C, P. B. S, R. T. L, R. T. L, dan V. K. T, "Decentralized Academic Certificate Issuance and Verification Using Blockchain Technology," *Int. J. Sci. Res. Eng. Manag.*, vol. 9, no. 6, hal. 1–10, 2025, doi: https://doi.org/10.55041/IJSREM50735.
[58] N. S. A. A. Bakar, N. Yahya, N. B. Idris, Z. Zakaria, dan M. A. M. Nordin, "Enhancing Academic Credential Integrity Through Blockchain-Based Verification Systems," *IOS Press*, vol. 0, hal. 55–67, 2025, doi: https://doi.org/10.3233/FAIA250509.
[59] P. M. Pondkule dan S. Kothari, "Implementation of blockchain-based document management system for higher education organizations," *Int. J. Smart Sens. Intell. Syst.*, vol. 18, no. 1, hal. 1–11, 2025, doi: https://doi.org/10.2478/ijssis-2025-0001.
[60] A. Salem, Y. Hamza, A. Hussein, dan J. N. Hasoon, "Modeling of blockchain with encryption based secure education record management

system," *Egypt. Informatics J.*, vol. 24, no. 4, hal. 100411, 2023, doi: https://doi.org/10.1016/j.eij.2023.100411.

[61] A. Janek dan P. P. Urbanovich, "Digital Certificate System In Education Based On The Ethereum Blockchain Platform," *Comput. Sci. Eng. Sci.*, vol. 2, no. 296, hal. 48–57, 2025, doi: https://elib.belstu.by/handle/123456789/71733.

[62] P. Harshavardhan, M. Sharath, dan S. Rajyalaxmi, "Privacy Protected Blockchain based Sharing and Verification of Student's Credentials," *TechRxiv*, 2025, doi: https://doi.org/10.36227/techrxiv.176049826.69897193/v1.

[63] A. N. Sari dan T. Gelar, "Prototype of Blockchain-Based Diploma Transcript Authentication Method," *J. Comput. Eng. Electron. Inf. Technol.*, vol. 4, no. 2, hal. 91–102, 2025, doi: https://doi.org/10.17509/coelite.v4i2.86050.

[64] R. Boddupalli, K. Malika, R. M. Harshita, dan K. V. Sharma, "QuickCert - A Scalable Web-Based Certificate Management System for Academic Institutions with Enhanced Security and Real-Time Automation," *Synthesis (Stuttg).*, vol. 2, no. 3, hal. 1–10, 2024, doi: https://doi.org/10.70162/smrj/2024/v2/i3/v2i301.

[65] S. H. D dan S. N, "Secure Academic Certificate Authentication Using Blockchain Technology," *SSRN Electron. J.*, hal. 6, 2025, doi: http://dx.doi.org/10.2139/ssrn.5375293.

[66] A. Farabi, I. Khandaker, J. Ahsan, I. K. Shanto, N. Jahan, dan M. J. Khan, "ShikkhaChain : A Blockchain-Powered Academic Credential Verification System for Bangladesh," *Arxiv*, 2025, doi: https://doi.org/10.48550/arXiv.2508.05334.

[67] M. Ileana dan A. Popgeorgiev, "The Use of Blockchain Technology for the Validation and Certification of Competencies in Education," *ACM Digit. Libr.*, vol. 2024, no. June 2024, 2025, doi: https://doi.org/10.1145/3674912.3674933.

[68] O. S. Oluwaseyi dan R. O. Akinyede, "Utilizing Blockchain Technology for University Certificate Verification System," *Int. J. Appl. Inf. Syst.* –, vol. 12, no. 45, hal. 23–40, 2024, doi: https://doi.org/10.5120/ijais2024451977.