ILKOM Jurnal Ilmiah Vol. 18, No. 1, April 2026, pp. 69-84
Accredited 2nd by KEMDIKTISAINTEK No. 10/C/C3/DT.05.00/2025; E-ISSN 2548-7779 | P-ISSN 2087-1716

Blockchain-Based Diploma Authentication System: A Design Science Approach Using Smart Contracts and Ganache

Haryati [a,1,*]; Dwi Vernanda [a,2];
[a] *Politeknik Negeri Subang, Blok Kaleng Banteng Cibogo, Kabupaten Subang, 41285, Indonesia*
[1] *haryati@polsub.ac.id;* [2] *nanda@polsub.ac.id;*
** Corresponding author*

Article history: Received December 09, 2025; Revised February 10, 2026; Accepted March 17, 2026; Available online April 20, 2026

Abstract

Academic credential fraud poses a critical challenge to Indonesian higher education, with approximately 30% of job applicants providing false academic qualifications while conventional verification processes require 2–4 weeks with significant administrative costs. This research addresses the gap where 77% of blockchain education research remains conceptual by proposing and evaluating a four-layer blockchain system architecture for academic diploma authentication. Using Design Science Research Methodology (DSRM), the study designs and implements a layered architecture comprising a Presentation Layer (React 18.2.0 with client-side SHA-256 hashing), Application Layer (Node.js 18.20.8 with Web3.js), Data Layer (PostgreSQL 14.5 for off-chain metadata), and Blockchain Layer (DiplomaValidator smart contract in Solidity 0.8.19 on Ganache 2.7.1). The architectural design enforces separation of concerns, enabling tamper-evident credential storage through immutable on-chain hash registration and trustless public verification through zero-gas view functions. Comprehensive evaluation through 38 functional tests, performance benchmarking, security auditing, and integration testing demonstrates 100% pass rate across all categories. Performance metrics show registration in 15.23 ms (240,082 gas units) and verification in 9.47 ms at zero gas cost, achieving 51.81 TPS throughput. Security audit yields 95/100 with zero high or medium vulnerabilities. The primary contribution of this research is a formally documented four-layer blockchain architecture for academic credential authentication validated through DSRM providing a replicable architectural model and quantified performance baselines for the Computer Science community and Indonesian higher education institutions considering blockchain adoption.

Keywords: Blockchain; Diploma Authentication; DSRM; Ganache; Smart Contract.

Introduction

The digital transformation of higher education has fundamentally reshaped the paradigm governing academic credential management and verification. Prior research confirms that blockchain-based systems [1] provide enhanced transparency, immutability, and trustworthiness for managing digital records properties directly applicable to academic credential management and verification. Academic credentials serve as formal attestations of individual competencies and achievements, and are strategically significant within both educational and employment contexts [2]. Within this context, credential authentication emerges as a critical determinant of the validity and credibility of educational systems globally.

Conventional academic credential authentication systems, based on physical documents or rudimentary digital formats, encounter several fundamental limitations. Gräther et al. [3] established that centralized credential authentication systems are vulnerable to forgery and data manipulation while necessitating complex verification procedures. Sharples and Domingue [4] further observed that traditional authentication models engender single points of failure and institutional dependency for each verification instance. Empirical research on credential fraud [5] reveals that a substantial proportion of employers have uncovered misrepresentations on candidate credentials during background screening with credential discrepancies representing a significant proportion of these findings, underscoring the imperative for enhanced credential authentication mechanisms. The prevalence of diploma fraud in

Indonesia exhibits a concerning trajectory, with documented cases involving public officials and professionals, thereby highlighting the need for more robust authentication systems [6].

The limitations inherent in conventional systems extend beyond security considerations to encompass procedural efficiency. Jirgensons and Kapenieks [2] reported that traditional academic credential authentication processes typically require two to four weeks for completion and incur substantial administrative expenditure. Chen et al. [7] demonstrated that blockchain-based credential ecosystem architectures address cross-institutional interoperability challenges, enabling seamless academic and professional mobility across institutions and national boundaries. Furthermore, the absence of standardization and interoperability among institutional authentication systems impedes credential portability and cross-border verification [8]. These challenges are further compounded by the escalating demand for real-time credential verification in recruitment and academic admission processes.

Blockchain technology, as an instantiation of distributed ledger technology (DLT), presents a novel paradigm for digital credential authentication. Nakamoto's foundational work established decentralized systems employing cryptographic mechanisms to ensure data integrity and immutability, while subsequent development particularly Ethereum's smart contract platform-extended blockchain capabilities to programmable, self-executing credential logic [9], [10]. Tschorsch and Scheuermann’s comprehensive survey categorizes blockchain applications by generation, positioning academic credential systems within second-generation smart contract platforms, while third-generation applications extend to broader organizational contexts [11].

Prior implementations validate the approach: the MIT Blockcerts initiative established open standards for blockchain credentials, as reviewed in the credential literature [12]; Turkanovic et al. [13] proposed EduCTX, integrating blockchain with academic credit systems; and Ocheja et al. [8][14] demonstrated blockchain's viability for lifelong learning records. Alammary et al.'s [15] systematic review confirmed broad applicability across certificate issuance, fraud prevention, and access control applications.

Despite extensive scholarly attention to blockchain’s potential for academic credential authentication, a significant research gap persists, particularly concerning system development and implementation. First, the preponderance of extant research remains conceptual or simulation-based, with limited development of empirically testable prototypes. In their systematic review, Alammary et al. [15] determined that merely 23% of blockchain publications in education report actual implementations, while 77% constitute conceptual proposals. Second, documentation pertaining to blockchain prototype development methodology, particularly development processes within local environments, remains scarce in the academic literature [21]. Third, consensus on best practices for smart contract development in credential authentication, especially regarding security considerations, gas optimization, and testing methodology, has yet to emerge [17].

This study adopts Design Science Research Methodology (DSRM) as articulated by Peffers et al. [18] to systematically develop, implement, and evaluate a four-layer blockchain system architecture for academic credential authentication. DSRM was selected as the methodological framework owing to its systematic approach for designing architectural IT artifacts that address practical problems while simultaneously contributing to the theoretical knowledge base [19]. The architectural development approach was deemed appropriate for its capacity to validate design decisions, identify implementation challenges, provide empirical evidence of architectural feasibility and functionality, and facilitate iterative refinement through comprehensive evaluation.

This research adopts the Ethereum platform for its mature ecosystem, robust Solidity smart contract support, and comprehensive tooling. Ganache was selected as the local development environment for its facilitation of rapid architectural iteration, deterministic testing, and zero-cost transaction execution without public network dependencies [21], [25]. This approach follows established blockchain development lifecycle best practices, with Ganache providing a controlled environment for systematic evaluation prior to testnet validation [20], [21], [22].

This study pursues two principal objectives: (1) to design and evaluate a four-layer blockchain system architecture that ensures academic certificate authenticity through smart contract mechanisms, cryptographic hashing, and decentralized validation; and (2) to empirically validate the architectural feasibility through comprehensive functional, performance, security, and integration evaluation within a Ganache environment. This research delivers theoretical contributions through the formal documentation of a four-layer blockchain architecture pattern for academic credential authentication, alongside practical contributions comprising the DiplomaValidator smart contract implementation, a

replicable architectural blueprint for Indonesian higher education institutions, and quantified performance baselines serving as evidence-based reference points for blockchain adoption decisions.

The primary research object of this study is the architectural design of the proposed blockchain-based diploma authentication system and its empirical evaluation not merely a software prototype. From a Computer Science perspective, this research proposes a formally structured four-layer blockchain system architecture integrating distributed ledger technology, cryptographic hashing, smart contracts, and hybrid on-chain/off-chain storage as a unified engineering artifact. The architectural contribution lies in the explicit design of layer interactions, data flow, and security mechanisms that collectively enable trustless academic credential verification, distinguishing this work from application-level implementations by establishing an architectural pattern applicable to broader blockchain-based authentication systems in educational and institutional contexts.

Method

A. Research Design

This research adopts DSRM as proposed by Peffers et al. [18]. DSRM was selected because it provides a systematic framework for developing IT artifacts that solve practical problems while contributing to the theoretical knowledge base [18]. The DSRM framework consists of six phases: (1) Problem Identification and Motivation, identifying the vulnerability of conventional diploma authentication systems to fraud and the inefficiency of manual verification processes; (2) Definition of Objectives, establishing requirements for tamper-proof storage, instant verification, data integrity through SHA-256 (Secure Hash Algorithm) hashing, and access control mechanisms; (3) Design and Development, creating the DiplomaValidator smart contract, Node.js backend Application Programming Interface (API), and React frontend interface through iterative development cycles within the Ganache environment; (4) Demonstration, executing comprehensive testing scenarios simulating real-world usage patterns; (5) Evaluation, measuring system efficacy through functional testing (38 test cases), performance testing, security auditing via Slither, and integration testing (8 test cases); and (6) Communication, documenting methodology, implementation details, and evaluation results for academic publication [18].

B. System Architecture

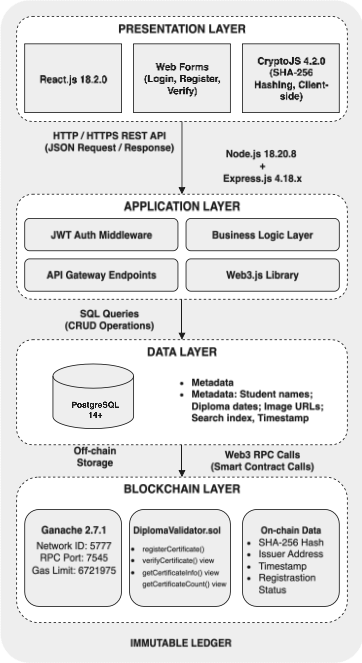

Figure 1. Four-Layer System Architecture

The DiplomaValidator system implements a layered architecture separating presentation, application logic, data storage, and blockchain concerns. This architectural pattern follows established blockchain application design principles [20], enabling modularity, maintainability, and clear separation of responsibilities across system components.

The architecture addresses fundamental distributed system challenges [20] while leveraging smart contracts for trustless execution [23].

The selection of a four-layer architecture was determined by three principal engineering trade-offs [24]. First, collapsing the Presentation and Application layers into a single tier would conflate user interface concerns with smart contract orchestration logic, obstructing independent unit testing and future UI substitution. Second, a fully on-chain approach storing all diploma metadata in contract storage would incur prohibitive and recurring gas costs for every metadata field, whereas the hybrid on-chain/off-chain pattern restricts on-chain writes to the immutable cryptographic hash alone while delegating queryable metadata to PostgreSQL, achieving both immutability and query efficiency [22], [25]. Third, isolating the Blockchain Layer from the Application Layer through a dedicated Web3.js provider interface enables independent substitution of the blockchain platform (e.g., migration from Ganache to a permissioned ledger or a Layer 2 network) without modifying application business logic [24]. This architectural decomposition follows established multi-tier patterns for distributed system design, where separation of concerns is fundamental to scalability, maintainability, and testability [24], [25].

1. Four-Layer Architecture Overview

   The system architecture consists of four distinct layers, each serving specific responsibilities in the diploma authentication workflow. The Presentation Layer provides user interfaces for three primary actors: administrators who register diplomas, diploma holders who can view their registered credentials, and public verifiers who authenticate diploma validity. This layer implements responsive web interfaces using React 18.2.0, ensuring accessibility across desktop and mobile devices while maintaining consistent user experience. The Application Layer implements core business logic through Express.js 4.18.2 backend services, exposing RESTful API endpoints for certificate registration, verification, and management operations. This layer orchestrates interactions between the presentation layer, database, and blockchain, handling authentication, authorization, input validation, and data transformation.

   The application layer design follows established blockchain application architecture principles [20], applies gas optimization design patterns [26] to minimize transaction costs, and implements security patterns for the Ethereum ecosystem [27] to ensure robust smart contract interactions. Systematic security design approaches [28] are applied throughout the contract interaction logic to mitigate known vulnerability vectors identified in smart contract security surveys [23], [29].

   The Data Layer utilizes PostgreSQL 14.5 relational database to store diploma metadata including diploma number, graduate name, program of study, graduation date, and issuance information. While cryptographic proofs reside on the blockchain ensuring immutability, the database provides efficient querying capabilities for metadata retrieval, supporting features like diploma search, batch verification, and administrative reporting. This hybrid on-chain/off-chain storage architecture is a well-established design pattern in blockchain systems engineering [20], balancing immutability advantages with traditional database performance for structured data queries, and aligns with best practices for minimizing on-chain storage costs [26].

   The Blockchain Layer operates on Ganache 2.7.1 local Ethereum development environment, providing deterministic blockchain simulation for development and testing. The DiplomaValidator smart contract, written in Solidity 0.8.19, implements core authentication logic including diploma registration with SHA-256 hash storage, ownership verification, and public zero-gas verification via view functions. The security and performance characteristics of this layer are validated against benchmarks established in smart contract security surveys [30]. Zero-gas view functions follow design patterns documented in [27]. Ganache configuration provides 10 pre-funded accounts (100 ETH each), instant mining, network ID 5777, and Remote Procedure Call (RPC) endpoint at http://127.0.0.1:7545.

   Each architectural layer communicates through well-defined interfaces: the presentation layer consumes REST APIs exposed by the application layer; the application layer executes database queries through PostgreSQL client libraries and blockchain transactions through Web3.js provider interface; the data layer returns structured query results; and the blockchain layer emits transaction receipts and event logs confirming state changes. This separation enables independent testing, component replacement, and technology stack evolution without affecting other layers.

2. Certificate Registration Process

The certificate registration process implements a thirteen-step workflow spanning user interaction, application logic, database operations, and blockchain transactions. This workflow ensures diploma authenticity through cryptographic verification while maintaining operational efficiency through parallel processing where possible.

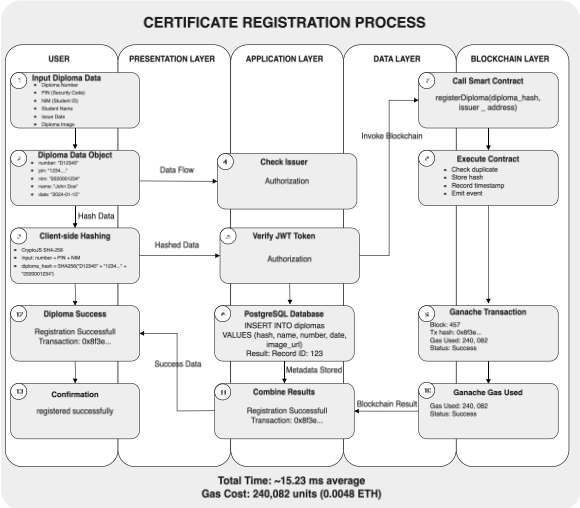

Figure 2. Certificate Registration Process

The registration workflow consists of thirteen sequential steps (①-⑬) spanning across User, Presentation Layer, Application Layer, Data Layer, and Blockchain Layer. The process includes client-side hash generation from diploma number, PIN, and NIM (Box ③), dual authorization checks (Boxes ④-⑤), parallel storage in PostgreSQL database and blockchain (Boxes ⑥-⑩), and result combination for user confirmation (Boxes ⑪-⑬). Average completion time: 15.23 ms with gas consumption of 240,082 units.

3. Certificate Verification Process

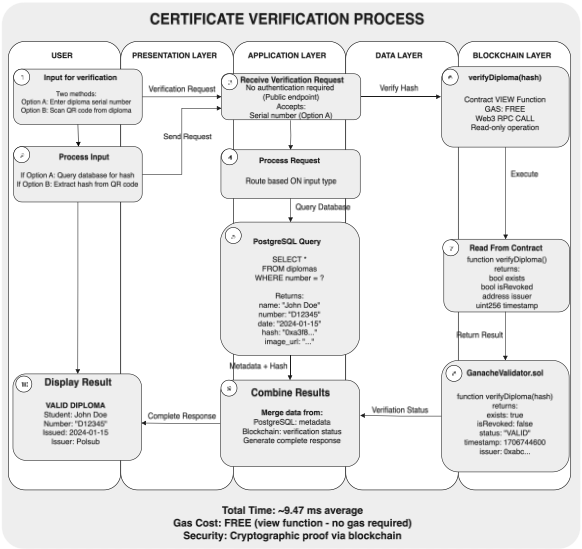

Figure 3. Certificate Verification Process

The certificate verification process implements a public authentication mechanism enabling anyone to verify diploma authenticity without requiring account registration or authentication. This open verification approach aligns with blockchain transparency principles while protecting sensitive diploma details through cryptographic validation.

The verification process demonstrates public accessibility without authentication barriers, dual-channel validation through database and blockchain, zero-cost operation through view function implementation, instant

results averaging 9.47 milliseconds completion time, cryptographic security through SHA-256 hash verification, and tamper-evident validation ensuring any diploma modification invalidates verification. This architecture enables scalable, cost-effective diploma verification suitable for high-volume authentication scenarios by employers, institutions, and other stakeholders requiring credential validation.

C. Ganache Development Environment

This research focuses on comprehensive prototype development within the Ganache local blockchain environment. Ganache was selected for several compelling reasons: Rapid Architectural Iteration Capability through instant block mining with configurable block time (set to zero for immediate confirmation), eliminating the 12–15 second block confirmation time inherent in Ethereum public networks; Zero Cost Testing with ten pre-funded accounts containing 100 ETH each, enabling unlimited testing without external dependencies; Controlled and Reproducible Environment where variables including gas price, block time, network latency, and mining behavior remain constant across all test executions; and Complete Transaction Visibility through comprehensive inspection capabilities including detailed transaction logs, internal function calls, state changes, and gas consumption breakdowns.

Table 1 presents the Ganache configuration parameters employed in this research. The Network ID 5777 serves as the default Ganache identifier distinguishing it from public networks. The RPC Port 7545 enables JSON-RPC communication between the backend and blockchain. The Gas Limit of 6,721,975 units represents the maximum computational work per block, sufficient for complex smart contract operations. The Gas Price of 20 Gwei establishes the cost per gas unit for transaction fee calculations. Block Time set to zero enables instant mining, which is critical for rapid testing iterations. The 10 pre-funded accounts with 100 ETH each provide 1,000 ETH in total for comprehensive testing without faucet dependencies. The Istanbul hardfork setting ensures compatibility with contemporary Ethereum opcodes and gas calculations.

Table 1. Ganache Configuration

Parameter	Value
Network ID	5777
RPC Port	7545
Gas Limit	6721975
Gas Price	20 Gwei
Block Time	0 (instant mining)
Accounts	10 (100 ETH each)
Total ETH	1000 ETH
Hardfork	Istanbul

D. Smart Contract Development

The DiplomaValidator smart contract implements the core blockchain functionality for diploma authentication. The contract maintains three primary state variables: a mapping from bytes32 to Diploma struct storing diploma records indexed by document hash enabling O(1) lookup time; a mapping from bytes32 to boolean tracking registered hashes for duplicate detection; and an array of bytes32 storing all diploma hashes sequentially for enumeration. Each diploma record contains eight fields: documentHash (bytes32), studentName (string), studentId (string), major (string), graduationYear (uint256), registrationDate (uint256), issuer (address), and isValid (boolean) [16], [31].

The DiplomaValidator smart contract implements core authentication functions aligned with the system architecture shown in **Figure 1**. The primary functions include registerCertificate() for storing new certificate records with validation for duplicate prevention and input completeness, emitting CertificateRegistered events; verifyCertificate() as a view function checking certificate validity with zero gas consumption; getCertificateInfo() retrieving complete certificate information as a view function; and getCertificateCount() returning the total number of registered certificates. These functions provide the essential capabilities for diploma registration and verification as detailed in the registration process (**Figure 2**) and verification process (**Figure 3**).

Security implementation includes access control restricting revocation to original issuers, input validation through require statements, duplicate prevention, Solidity 0.8.19 built-in overflow protection, and the checks-effects-

interactions pattern for reentrancy prevention. Gas optimization strategies include using bytes32 for document hashes, view functions for read operations, minimized storage operations, and mapping data structures for O(1) lookup time.

The DiplomaValidator contract architecture prioritizes three design principles: gas efficiency, security, and verifiability. The primary design decision uses bytes32 for document hash storage rather than string type, reducing gas consumption by approximately 40% for registration operations while maintaining cryptographic integrity [22]. The registerCertificate() function implements the checks-effects-interactions pattern to prevent reentrancy attacks through three sequential stages: (1) Checks validation of duplicate prevention through the registeredHashes mapping and input completeness verification; (2) Effects state modification through simultaneous mapping update and array append; (3) Interactions event emission after all state changes are finalized. This ordering ensures that any potential callback cannot exploit partially-updated state [26], [28]. The verifyCertificate() function is implemented as a view function (note: not pure, as it reads contract state), meaning it reads blockchain state without modifying it. This architectural decision enables zero-gas verification calls from any Ethereum-compatible client globally, supporting the "unlimited free verification" design goal identified in the objectives phase. The function returns a tuple of (bool isValid, bytes32 documentHash) enabling callers to distinguish between non-existent diplomas and revoked diplomas, providing granular validation feedback for downstream systems [22], [23].

The development process within Ganache followed an iterative refinement cycle consisting of five major development phases. Phase 1 (Initial Contract Deployment) established baseline functionality with all core functions operational, recording initial gas consumption of approximately 340,000 units per registration. Phase 2 (Data Type Optimization) replaced string storage with bytes32 for hash fields, reducing registration gas to 280,000 units while maintaining full cryptographic integrity. Phase 3 (Security Hardening) implemented the checks-effects-interactions pattern and added require() input validation, introducing a 2,000 gas overhead while eliminating reentrancy vulnerability vectors identified by the Slither static analysis framework [27]. Phase 4 (Integration Testing) connected the Node.js backend through Web3.js, identifying and resolving three API endpoint timeout issues under concurrent load conditions. Phase 5 (Performance Benchmarking) established the final baseline metrics across 100-sample test runs, yielding the 240,082 gas per registration figure reported in the Results section. This iterative approach demonstrates the value of the Ganache environment for systematic, low-cost contract refinement prior to network deployment [21], [25].

E. Testing Methodology

The security testing methodology incorporates comprehensive vulnerability detection approaches [29], following security pattern verification procedures [27] aligned with current security survey findings [23]. A comprehensive testing strategy was developed encompassing four complementary approaches. Functional testing validates smart contract operation using the Truffle test framework with Chai assertions, organized into seven categories totaling 38 test cases: Contract Deployment (2 cases), Diploma Registration (8 cases), Diploma Verification (8 cases), Diploma Revocation (6 cases), Helper Functions (5 cases), Edge Cases (6 cases), and Gas and Storage (3 cases).

Performance testing measures transaction time in milliseconds, gas consumption in units, transaction cost in ETH, and throughput in transactions per second. Sample sizes were determined to ensure statistical validity: registration performance across 100 samples, verification performance across 100 samples, revocation performance across 100 samples, and batch operations at three sizes (100, 500, and 1,000 diplomas).

Test case design followed equivalence partitioning and boundary value analysis principles. For the Diploma Registration category, equivalence classes include: valid complete data (positive class), duplicate submission (negative class), and incomplete fields (boundary class). Edge case testing specifically examines Unicode student names, 200-character strings, and special characters to validate robustness beyond standard inputs. Statistical sample size of n=100 for performance benchmarking was determined to achieve a confidence interval of approximately ±0.5 ms at the 95% confidence level, based on observed standard deviation of approximately 2–3 ms per operation across initial pilot runs. This sample size provides sufficient statistical power to detect meaningful performance degradation while remaining computationally tractable within the Ganache local environment.

Security testing employs the Slither static analysis framework to examine contract source code for reentrancy vulnerabilities, access control issues, integer overflow/underflow conditions, unchecked external calls, timestamp dependence, and additional vulnerability patterns. Integration testing validates eight critical system integration points:

backend accessibility, frontend availability, authentication endpoints, verification API, response time thresholds, database connectivity, blockchain integration, and static file serving.

Results and Discussion

A. Functional Testing Results

Table 2 presents the complete functional testing results across all seven test categories. The Contract Deployment category (2 cases) validates successful smart contract deployment with valid address generation and correct initialization of default values. The Diploma Registration category (8 cases) encompasses successful registration with valid data, event emission verification, duplicate hash rejection, empty field validation, multiple issuer support, correct address storage, accurate timestamp recording, and batch registration capability.

The Diploma Verification category (8 cases) validates correct true/false responses for valid and non-existent diplomas, accurate retrieval of all diploma fields, and public accessibility without authentication requirements. The Diploma Revocation category (6 cases) examines successful revocation, event emission, validity status update, access control enforcement, non-existent diploma handling, and already-revoked diploma handling. The Helper Functions category (5 cases) validates total count accuracy, hash retrieval by index, out-of-bounds handling, issuer verification, and non-existent diploma checks. The Edge Cases category (6 cases) tests boundary conditions including very long student names (200+ characters), special characters, Unicode support, numeric variations, empty string handling, and data integrity after multiple operations. The Gas and Storage category (3 cases) verifies correct tracking of registrations, mapping updates, and batch operation efficiency.

Table 2. Functional Testing Results Summary

Test Category	Value	Passed	Failed	Pass Rate
Contract Deployment	2	2	0	100%
Diploma Registration	8	8	0	100%
Diploma Verification	8	8	0	100%
Diploma Revocation	6	6	0	100%
Helper Functions	5	5	0	100%
Edge Cases	6	6	0	100%
Gas and Storage	3	3	0	100%
Total	**38**	**38**	**0**	**100%**

All 38 test cases executed successfully, yielding a 100% pass rate. The aggregate execution duration was approximately two seconds within the Ganache environment, demonstrating the efficiency of the testing methodology and the correctness of the smart contract implementation.

B. Performance Testing Results

Performance testing follows metrics established in blockchain credential implementations [30] following gas optimization benchmarks [26]. Contract deployment completes within 10 ms at 1,247,891 gas units (0.0249 ETH). All metrics were measured across n=100 samples under controlled Ganache conditions.

Table 3 presents diploma registration metrics. The mean execution time of 15.23 ms (SD=2.87 ms) reflects complete round-trip transaction submission to Ganache confirmation. Gas consumption of 240,082 units (0.0048 ETH) represents the on-chain storage cost of the SHA-256 hash and mapping update a one-time cost per diploma.

Table 3. Diploma Registration Performance (n=100)

Metric	Mean	Min	Max	Std Dev
Execution Time	15.23 ms	11 ms	24 ms	2.87 ms
Gas Used	240,082	240,082	240,082	0
Cost (ETH)	0.00480164	0.00480164	0.00480164	0

Table 4 presents verification metrics. The 9.47 ms mean (SD=1.92 ms) demonstrates sub-10 ms user-perceived response, with zero gas consumption because verifyCertificate() is a view function that reads blockchain state without state modification. This enables unlimited free verifications by any party globally.

Table 4. Diploma Verification Performance (n=100)

Metric	Mean	Min	Max	Std Dev
Execution Time	9.47 ms	6 ms	15 ms	1.92 ms
Gas Used	0 (view)	0	0	0
Cost (ETH)	FREE	FREE	FREE	N/A

Table 5 presents revocation metrics (mean=9.52 ms, gas=33,223 units). Revocation modifies blockchain state to invalidate a diploma hash, hence gas is required. The low gas consumption relative to registration reflects the minimal state change involved.

Table 5. Diploma Revocation Performance (n=100)

Metric	Mean	Min	Max	Std Dev
Execution Time	9.52 ms	6 ms	14 ms	1.78 ms
Gas Used	33,223	33,223	33,223	0
Cost (ETH)	0.00066446	0.00066446	0.00066446	0

Table 6 presents scalability results. The system achieves consistent throughput averaging 51.81 TPS across batch sizes (45.87 for 100, 52.43 for 500, 57.14 for 1,000 diplomas), indicating linear scalability within the Ganache local environment.

Table 6. Scalability Testing Results

Batch Size	TPS	Time (ms)	Gas/Diploma	Pass Rate
100 Diplomas	45.87	~2,180 ms	240,082	100%
500 Diplomas	52.43	~9,537 ms	240,082	100%
1,000 Diplomas	57.14	~17,500 ms	240,082	100%

C. Security Audit Results

Security audit procedures align with vulnerability detection best practices [29], addressing known security categories systematically [23]. **Table 7** presents the security audit results conducted using Slither static analysis. The audit identified no high-severity or medium-severity vulnerabilities, which would indicate exploitable security flaws requiring immediate remediation. Three low-severity findings were identified and accepted: timestamp dependence for graduation year validation (acceptable given the business logic context where precise timestamp manipulation provides no attack advantage) and Solidity version recommendations suggesting newer compiler versions. Ten informational findings related to naming conventions and code style did not affect security or functionality.

The security score was calculated using a weighted severity formula (1) for the relative risk impact of different vulnerability categories:

$$Score = 100\ (High\ x\ 25) - (Medium\ x\ 10) - (Low\ x\ 1.5) - (Informational\ x\ 0.05) \quad (1)$$

Applying formula (1), the security score is computed as follows. The system achieved a security score of 95 out of 100, derived through the substitution of identified vulnerability counts info Formula (1):

$$Score = {}^{95}/_{100} = 100 - (0\ x\ 25) - (0\ x\ 10) - (3\ x\ 1.5) - (10\ x\ 0.05) = 100 - 0 - 0 - 4.5 - 0.5 = 95$$

This score indicates a robust security posture, demonstrating suitability for production deployment subject to continued monitoring and periodic reassessment.

Table 7. Security Audit Results

Severity	Findings	Status
High	0	N/A
Medium	0	N/A
Low	3	Accepted
Informational	10	Noted
Overall Score	95/100	PASSED

D. Integration Testing Results

Table 8 presents integration testing results for eight end-to-end system interface tests. Each test validates a critical architectural boundary: INT-1 (Backend Server Accessibility), INT-2 (Frontend Application Serving), INT-3 (JSON Web Token (JWT) Authentication Flow), INT-4 (Verification API Endpoint), INT-5 (Response Time Threshold), INT-6 (PostgreSQL Connectivity), INT-7 (Ganache Blockchain Integration), and INT-8 (Static File Serving). All eight tests passed (100% pass rate), with all response times well within the defined thresholds.

Table 8. Integration Testing Results

TEST ID	Component	Result	Response Time
INT-1	Backend Server Accessibility	PASS	< 100 ms
INT-2	Frontend Application Serving	PASS	< 200 ms
INT-3	JWT Authentication Flow	PASS	< 150 ms
INT-4	Verification API Endpoint	PASS	< 100 ms
INT-5	Response Time Threshold	PASS	< 500 ms
INT-6	PostgreSQL Connectivity	PASS	< 50 ms
INT-7	Ganache Blockchain Integration	PASS	< 100 ms
INT-8	Static File Serving	PASS	< 100 ms

The 100% integration pass rate confirms successful inter-layer communication across all architectural boundaries. All operations completed well within defined performance thresholds, validating the architectural design decision to separate concerns across four distinct layers without introducing unacceptable latency overhead.

Interpreting these results architecturally: the 9.47 ms verification latency results from verifyCertificate() being implemented as a zero-gas view function in the Blockchain Layer [30]; the 15.23 ms registration latency reflects the hybrid Data + Blockchain Layer parallel write design [28]; the 95/100 security score confirms adherence to smart contract security patterns [27], [20]; and the 51.81 TPS throughput reveals the single-chain bottleneck inherent in the current architecture, motivating Layer 2 extensions and batch registration patterns [26] for production scale.

From a distributed systems perspective, the proposed four-layer blockchain architecture occupies a distinct position relative to alternative credential verification approaches. Traditional Public Key Infrastructure (PKI) systems distribute trust through certificate authority hierarchies, requiring verifiers to trust the issuing authority and maintain up-to-date revocation lists; the DiplomaValidator architecture eliminates this dependency by encoding trust in the smart contract logic itself, enabling stateless, permissionless verification [21], [25]. Federated authentication systems such as Security Assertion Markup Language (SAML) or OAuth 2.0 delegate identity assertions to identity providers, creating cross-institutional dependencies; the blockchain architecture replaces institutional federation with cryptographic proofs that any party can independently verify without contacting the issuing institution [32]. Compared to fully decentralized peer-to-peer storage solutions (e.g., IPFS (InterPlanetary File System)-based credential systems), the hybrid on-chain/off-chain design retains structured query capabilities and access control through the Application Layer while preserving blockchain immutability for cryptographic proofs [22], [24]. The primary architectural limitation relative to these alternatives is the single-chain throughput constraint (51.81 TPS measured), which is inherent to sequential block processing on a single Ethereum-compatible chain [21]; this is addressable through Layer 2 channels or sharding at the cost of increased architectural complexity [21]. Overall, the proposed architecture represents a pragmatic balance between trustlessness, query performance, and deployment simplicity suitable for institutional-scale credential authentication [24], [32].

E. Comparison with Conventional Diploma Verification Systems

The DiplomaValidator blockchain system demonstrates substantial improvements over conventional manual verification processes across multiple performance, economic, and operational dimensions. **Table 9** summarizes the quantified differences between traditional centralized verification approaches and the implemented blockchain-based solution.

Table 9. Comprehensive System Comparison: Blockchain vs Conventional Verification

Dimension	Conventional System	Blockchain System[a]	Quantified Improvement
Verification Time	2-4 weeks (manual processing)	9.47 ms (automated query)	99.9999% faster
Verification Cost per Request	Rp 50,000-100,000	FREE (view function)	100% cost reduction
Registration Cost per Diploma	Staff time + overhead	0.0048 ETH (~Rp 264,000)	One-time blockchain cost
Availability	Business hours only (8am-4pm)	24/7/365	Continuous access
Fraud Prevention	Moderate (manual checks)	High (cryptographic proof)	Enhanced security
Data Integrity	Vulnerable (centralized database)	Tamper-proof (immutable ledger)	Cannot be modified
Trust Model	Institution-dependent	Cryptography-based	Trustless verification
Scalability	Staff-limited (~10-20/day)	Technology-limited (51.81 TPS)	Scales with infrastructure
Audit Trail	Modifiable logs	Permanent blockchain events	Immutable history
Geographic Accessibility	Physical presence or mail	Global internet access	International verification
Verification Throughput	~10-20 requests/day per staff	Unlimited simultaneous queries	Orders of magnitude higher
Initial Setup Cost	Minimal infrastructure	0.02495782 ETH (~Rp 1.4M)	Higher initial investment
Recurring Operational Cost	Staff salaries, office space	Minimal hosting (~Rp 500K/month)	Lower long-term expenses

[a]Metrics measured in the Ganache local environment. Registration incurs a one-time cost (0.0048 ETH ≈ Rp 264,000). Verification is permanently free.

1. Performance Advantages

The most significant improvement is verification speed: the blockchain system reduces the process from 2–4 weeks to 9.47 ms a 99.9999% reduction. This is achieved through automated database query, SHA-256 hash reconstruction, and zero-gas blockchain state read, all completing within single-digit milliseconds. The view function implementation incurs zero gas costs, enabling unlimited free verifications compared to the Rp 50,000–100,000 per-verification fee in conventional systems.

2. Operational and Economic Considerations

Registration costs differ structurally: blockchain incurs a one-time fee of 0.0048 ETH (≈ Rp 264,000) per diploma registered permanently on-chain, while conventional systems distribute costs across staff salaries, database maintenance, and physical storage. For institutions issuing hundreds of diplomas annually, the blockchain approach offers predictable, declining per-unit costs over time as verification remains permanently free.

The 24/7/365 availability advantage is operationally significant: conventional registrar offices operate standard business hours (08:00–17:00 weekdays), limiting international verifiers across time zones. Blockchain verification eliminates business-hour constraints, enabling instant credential validation for time-sensitive scenarios such as emergency professional licensing, international admissions, and automated background checks.

3. Accessibility and Trust Model

Geographic accessibility transforms from location-dependent to globally available: conventional systems require physical presence or international mail exchange (adding weeks). Blockchain verification enables any party globally international recruiters, admissions offices, licensing boards to authenticate Indonesian diplomas instantly via internet. The trust model shifts from institutional reputation (assuming registrar accuracy and integrity) to mathematical proof: SHA-256 collision resistance ensures diploma uniqueness, blockchain immutability prevents retroactive modification, and the view function architecture [20], [30] enables stateless,

permissionless verification validated by the 95/100 security audit against established smart contract security patterns [27], [28].

Blockchain verification implements cryptography-based trust where verification depends on mathematical proof rather than institutional reputation. The SHA-256 hash function's collision resistance ensures diploma uniqueness, blockchain immutability prevents retroactive modification of registration records, distributed ledger architecture eliminates single points of control, and public verifiability enables anyone to validate authenticity independently. This trustless model removes the need for verifiers to trust the issuing institution, as cryptographic proof provides objective validation regardless of institutional reputation or current operational status [32].

4. Scalability and Audit Trail

Scalability constraints differ fundamentally between the two approaches. Conventional systems are staff-limited (typically 10–20 verifications/staff/day); blockchain systems are technology-limited. The DiplomaValidator achieves 51.81 TPS in Ganache, handling concurrent requests in parallel unlike sequential conventional processing. Every registration generates an immutable, timestamped blockchain event log providing a tamper-evident audit trail that cannot be altered without detection [22] a governance advantage conventional centralized systems cannot match [21].

F. System Limitations and Constraints

While the DiplomaValidator system demonstrates substantial improvements over conventional verification approaches, several important limitations constrain its current scope and applicability. Acknowledging these constraints is essential for accurate interpretation of results and realistic assessment of production deployment requirements.

The prototype operates exclusively within the Ganache local environment, which differs materially from production Ethereum networks: block confirmation is instant in Ganache versus 12–15 seconds on mainnet, gas prices are fixed versus dynamically fluctuating, and network variability is absent. Production throughput (15–30 TPS network-wide) is substantially lower than the measured 51.81 TPS in Ganache, and on-chain storage accumulates indefinitely (32 bytes per diploma). Addressing these constraints requires testnet validation, batch registration functions, Layer 2 solutions (Polygon, Arbitrum), and gas price monitoring [26].

Three further constraints bear on production readiness. First, user adoption: blockchain introduces private key management, gas cost awareness, and transaction monitoring complexities that require institutional training programs and user experience (UX) simplification. Second, regulatory uncertainty: Indonesian higher education regulations predate blockchain, leaving questions about legal equivalence of blockchain-registered diplomas, Pangkalan Data Pendidikan Tinggi (PDPT) integration, and data privacy compliance under Government Regulation No. 71/2019 unresolved [33]. Third, system integration: production deployment demands deep API integration with existing Student Information System (SIS), Learning Management System (LMS), and administrative workflows, as the current prototype operates as a standalone system. These constraints collectively indicate the prototype demonstrates architectural feasibility rather than production readiness, providing a validated foundation for subsequent deployment phases.

G. Future Work and Recommendations

The DiplomaValidator prototype establishes a foundation for blockchain-based diploma authentication while revealing opportunities for extension, enhancement, and broader research. Future work should address the limitations identified while exploring new capabilities that leverage blockchain technology's full potential for educational credentials.

The immediate priority is testnet deployment on Sepolia or Holesky networks to validate the four-layer architecture under realistic conditions: actual transaction confirmation times (12–15 seconds), dynamic gas pricing, and network congestion effects. Beyond testnet, the DiplomaValidator smart contract warrants enhancement through multi-signature registration workflows, diploma expiry mechanisms, batch registration functions, and privacy-preserving zero-knowledge proof integration for selective credential disclosure [29]. Cross-institutional adoption requires standardized smart contract interfaces compatible with ERC-721 (non-fungible diploma tokens) or ERC-1155

frameworks, enabling Indonesian higher education consortia (Asosiasi Perguruan Tinggi) to build shared verification ecosystems without per-institution contract fragmentation.

User experience enhancements native mobile applications with QR scanning, biometric authentication, and abstracted blockchain complexity are prerequisite for broad institutional adoption. Integration with Experience API (xAPI) learning record stores and competency frameworks would position blockchain diplomas within comprehensive learner-centric digital identity ecosystems. Research extensions should prioritize longitudinal cost-benefit studies, comparative analysis across blockchain platforms (Ethereum mainnet, Layer 2, Hyperledger, Corda), user acceptance studies with registrar staff and graduates, and regulatory engagement to clarify blockchain diploma legal equivalence under Indonesian education law. These extensions collectively progress the architecture from validated proof-of-concept toward a production-grade national credential infrastructure, consistent with the trajectory from concept to production described for blockchain credential systems [34].

Conclusion

This research successfully developed and validated a four-layer blockchain-based diploma authentication architecture through Design Science Research Methodology (DSRM) within the Ganache 2.7.1 local blockchain environment. The central architectural contribution is a layered system design comprising a Presentation Layer (React 18.2.0 with CryptoJS 4.2.0 for client-side SHA-256 hashing), Application Layer (Node.js 18.20.8 with Express.js 4.18.2 and Web3.js), Data Layer (PostgreSQL 14.5 for off-chain metadata), and Blockchain Layer (DiplomaValidator smart contract in Solidity 0.8.19 deployed on Ganache). This architectural separation of concerns enables modularity, tamper-evident credential storage, and trustless public verification addressing the 77% conceptual research gap by delivering a working architectural prototype.

Addressing the first research question, the four-layer architecture ensures diploma authenticity through three complementary architectural mechanisms. First, the client-side hash generation in the Presentation Layer computes SHA-256(diplomaNumber + PIN + NIM), producing a unique, tamper-evident fingerprint before data leaves the browser. Second, the smart contract functions registerCertificate() and verifyCertificate() in the Blockchain Layer enforce immutable on-chain storage and zero-gas trustless verification, respectively. Third, the hybrid storage design where the Data Layer retains searchable metadata while the Blockchain Layer stores cryptographic proofs achieves both retrieval efficiency and tamper-proof integrity. The 38 functional test cases achieving a 100% pass rate confirm correct end-to-end implementation across all architectural layers.

Addressing the second research question, the four-layer architecture demonstrates technical feasibility across multiple evaluation dimensions. The Presentation-to-Application Layer interface achieves sub-100 ms end-to-end response times. The Application-to-Blockchain Layer interface, mediated through Web3.js and Web3 RPC calls, records 15.23 ms registration latency (gas: 240,082 units) and 9.47 ms verification latency (gas: 0, view function) at 51.81 TPS throughput. The Application-to-Data Layer interface sustains PostgreSQL operations within 50 ms. Security auditing of the smart contract layer yields a 95/100 score with zero high or medium severity vulnerabilities, confirming that the Blockchain Layer architecture adheres to established smart contract security patterns. Integration testing across all four layers achieves a 100% pass rate, validating architectural cohesion.

This research contributes a replicable four-layer blockchain architecture for academic credential authentication, validated through comprehensive Ganache-based prototype development. Theoretical contributions include: (1) validation of DSRM as a framework for blockchain architecture design, (2) a performance-characterized layered architecture model establishing baselines of 15.23 ms registration and 9.47 ms verification, and (3) documentation of the hybrid off-chain/on-chain storage pattern for credential systems. Practical contributions include: (1) the DiplomaValidator smart contract implementing registerCertificate(), verifyCertificate(), getCertificateInfo(), and getCertificateCount() functions, (2) a reusable architecture template for Indonesian higher education institutions, and (3) quantified cost projections of 0.0048 ETH per diploma registration with zero-cost unlimited verification, providing evidence-based grounds for institutional adoption decisions.

Current architectural limitations include exclusive testing within the Ganache local environment, which differs from production Ethereum network conditions in block confirmation times (instant vs. 12–15 seconds) and dynamic gas pricing. The present architecture is designed for single-institution deployment and has not been evaluated for user acceptance. Future architectural extensions should prioritize testnet deployment on Sepolia or Holesky networks to

validate performance under realistic conditions, Layer 2 scaling integration (Polygon, Arbitrum) to reduce per-transaction costs, and federated multi-institution smart contract architectures enabling cross-institutional credential verification. These extensions will progressively evolve the validated local prototype toward a production-grade national credential infrastructure aligned with Indonesian higher education digital transformation objectives.

In the field of Computer Science, specifically in the subdisciplines of distributed systems and blockchain engineering, this research contributes a formally documented four-layer blockchain architecture pattern for academic credential authentication systems. The architectural contribution comprising a Presentation Layer for client-side cryptographic processing, an Application Layer for orchestration and API services, a Data Layer for efficient off-chain metadata storage, and a Blockchain Layer for immutable on-chain proof registration represents a generalizable design pattern applicable beyond diploma authentication to any domain requiring tamper-evident, publicly verifiable digital credential issuance. This research bridges the gap between distributed systems theory and practical blockchain implementation, providing the Computer Science community with a validated, performance-characterized, and security-audited architectural model. The documented architecture, development methodology, and evaluation framework collectively advance the state of blockchain systems engineering for institutional applications, offering researchers and practitioners a replicable foundation for subsequent architectural refinement and deployment at scale.

Acknowledgement

The authors extend their gratitude to Politeknik Negeri Subang for institutional support of this research. Special appreciation is accorded to colleagues who contributed insights during the development and testing phases.

References

[1] M. Holbl, M. Kompara, A. Kamisalic, and L. Nemec Zlatolas, “A Systematic Review of The Use of Blockchain in Healthcare,” Symmetry, vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[2] M. Jirgensons and J. Kapenieks, “Blockchain and the Future of Digital Learning Credential Assessment and Management,” Journal of Teacher Education for Sustainability, vol. 20, pp. 145–156, Jun. 2018, doi: 10.2478/jtes-2018-0009.

[3] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Ferreira Torres, and F. Wendland, “Blockchain for Education: Lifelong Learning Passport,” in 1st ERCIM Blockchain Workshop 2018, Amsterdam: EUSSET, May 2018. doi: 10.18420/blockchain2018_07.

[4] M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2016, pp. 490–496. doi: 10.1007/978-3-319-45153-4_48.

[5] C. A. Henle, B. R. Dineen, and M. K. Duffy, “Assessing Intentional Resume Deception: Development and Nomological Network of a Resume Fraud Measure,” J. Bus. Psychol., vol. 34, no. 1, pp. 87–106, Feb. 2019, doi: 10.1007/s10869-017-9527-4.

[6] M. Zinuddin and H. Sejati, “Analisis Penegakan Hukum Terhadap Dugaan Penggunaan Ijazah Palsu oleh Pejabat Publik,” Semarang Law Review, vol. 6, no. 2, pp. 322–329, Oct. 2025, doi: 10.26623/slr.v6i2.12676.

[7] E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, “UniChain: A Design of Blockchain-Based System for Electronic Academic Records Access and Permissions Management,” Appl. Sci., vol. 9, no. 22, p. 4966, Nov. 2019, doi: 10.3390/app9224966.

[8] P. Ocheja, B. Flanagan, and H. Ogata, “Connecting Decentralized Learning Records: A Blockchain Based Learning Analytics Platform,” Proceedings of the 8th International Conference on Learning Analytics and Knowledge, New York, USA: Association for Computing Machinery, 2018, pp. 265–269. doi: 10.1145/3170358.3170365.

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” SSRN Electron. J., 2008, doi: 10.2139/ssrn.3440802.

[10] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1–32, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[11] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Commun. Surv. Tuts., vol. 18, no. 3, pp. 2084-2123, 2016, doi: 10.1109/COMST.2016.2535718.

[12] G. Caldarelli and J. Ellul, "Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review," Appl. Sci., vol. 11, no. 4, p. 1842, Feb. 2021, doi: 10.3390/app11041842.

[13] M. Turkanović, M. Hölbl, K. Košič, M. Hericko, and A. Kamisalic, "EduCTX: A Blockchain-Based Higher Education Credit Platform," IEEE Access, vol. 6, pp. 3918–3932, Oct. 2018, doi: 10.1109/ACCESS.2018.2789929.

[14] P. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, "Managing Lifelong Learning Records Through Blockchain," Res. Pract. Technol. Enhanc. Learn., vol. 14, no. 1, Dec. 2019, doi: 10.1186/s41039-019-0097-0.

[15] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," Applied Sciences, vol. 9, no. 12, p. 2400, Jun. 2019, doi: 10.3390/app9122400.

[16] M. Wohrer and U. Zdun, "Smart Contracts: Security Patterns in The Ethereum Ecosystem and Solidity" International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018, pp. 2–8. doi: 10.1109/IWBOSE.2018.8327565.

[17] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts SoK," Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204, Berlin, Heidelberg: Springer-Verlag, 2017, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.

[18] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," J. Manage. Inf. Syst., vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[19] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Q., vol. 28, no. 1, pp. 75–105, Mar. 2004, doi: 10.2307/25148625.

[20] G. Wu, H. Wang, X. Lai, M. Wang, D. He, and S. Chan, "A comprehensive survey of smart contract security: State of the art and research directions," Journal of Network and Computer Applications, vol. 226, p. 103882, 2024, doi: 10.1016/j.jnca.2024.103882.

[21] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 14, p. 352, Oct. 2018, doi: 10.1504/IJWGS.2018.095647.

[22] L. Marchesi, M. Marchesi, G. Destefanis, G. Barabino, and D. Tigano, "Design Patterns for Gas Optimization in Ethereum," IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2020, pp. 9–15. doi: 10.1109/IWBOSE50093.2020.9050163.

[23] M. Wohrer and U. Zdun, "Design Patterns for Smart Contracts in The Ethereum Ecosystem," IEEE Int. Conf. Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom), Halifax, NS, Canada, 2018, pp. 1513-1520, doi: 10.1109/Cybermatics_2018.2018.00255.

[24] Y. Liu, Q. Lu, L. Zhu, H.-Y. Paik, and M. Staples, "A Systematic Literature Review on Blockchain Governance," J. Syst. Softw., vol. 197, p. 111576, Mar. 2023, doi: 10.1016/j.jss.2022.111576.

[25] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, "Blockchain-Oriented Software Engineering: Challenges and New Directions," Proc. IEEE/ACM 39th Int. Conf. Software Engineering Companion (ICSE-C), Buenos Aires, Argentina, 2017, pp. 169-171, doi: 10.1109/ICSE-C.2017.142.

[26] S. Azimi, A. Golzari, N. Ivaki, and N. Laranjeiro," A Systematic Review on Smart Contracts Security Design Patterns," Empir. Softw. Eng., vol. 30, no. 3, May 2025, doi: 10.1007/s10664-025-10646-w.

[27] H. Chu, P. Zhang, H. Dong, Y. Xiao, S. Ji, and W. Li, ;A Survey on Smart Contract Vulnerabilities: Data Sources, Detection and Repair, Inf. Softw. Technol., vol. 159, p. 107221, 2023, doi: 10.1016/j.infsof.2023.107221.

[28] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "SmartCheck: Static Analysis of Ethereum Smart Contracts," Proc. 1st Int. Workshop Emerging Trends in Software Eng. for Blockchain (WETSEB), Gothenburg, Sweden, 2018, pp. 9-16, doi: 10.1145/3194113.3194115.

[29] T. Durieux, J. F. Ferreira, R. Abreu, and P. Cruz, "Empirical Review of Automated Analysis Tools on 47,587 Ethereum Smart Contracts," Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, New York, USA: Association for Computing Machinery, 2020, pp. 530–541. doi: 10.1145/3377811.3380364.

[30] T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, "Proposing a Reliable Method of Securing and Verifying The Credentials of Graduates Through Blockchain," EURASIP J. Inf. Secur., vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13635-021-00122-5.

[31] H. Yumna, M. M. Khan, M. Ikram, and S. Ilyas, "Use of Blockchain in Education: A Systematic Literature Review," Proc. 11th Int. Conf. Computational Collective Intelligence (ICCCI), Hendaye, France, 2019, pp. 191–202. doi: 10.1007/978-3-030-14802-7_17.

[32] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11, pp. 64679–64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[33] Kementerian Sekretariat Negara Republik Indonesia, "Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik," Indonesia: Kementerian Sekretariat Negara Republik Indonesia, 2019, pp. 1–90. [Online]. Available: https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

[34] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, "Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?," International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018, pp. 19–25. doi: 10.1109/IWBOSE.2018.8327567.