A Blockchain Based Hybrid ZKP-Merkle Tree Framework for Secure and Regulation-Compliant E-Governance Identity Verification

Archy Renaldy Pratama Nugraha
School of Data Science, Mathematics, and Informatics, IPB University, Bogor, Indonesia | Informatics Study Program, International Women University, Bandung, Indonesia
archyrenaldy@apps.ipb.ac.id (corresponding author)

Yandra Arkeman
Department of Agro-Industrial Technology, IPB University, Bogor, Indonesia
yandra@apps.ipb.ac.id

Irman Hermadi
School of Data Science, Mathematics, and Informatics, IPB University, Bogor, Indonesia
irmanhermadi@apps.ipb.ac.id

Yani Nurhadryani
School of Data Science, Mathematics, and Informatics, IPB University, Bogor, Indonesia
yani_nurhadryani@apps.ipb.ac.id

Received: 23 January 2026 | Revised: 4 March 2026 | Accepted: 19 March 2026

 DOI: https://doi.org/10.48084/etasr.17425

ABSTRACT

Digital identity verification in e-governance faces a trilemma between security, scalability, and regulatory compliance with Indonesia's Personal Data Protection Law (UU PDP). To resolve this, in this paper, we propose the ZMC-Framework, a blockchain-based hybrid architecture integrating Zero-Knowledge Proofs (ZKPs) for privacy-preserving verification and Merkle Trees for efficient, scalable data integrity on-chain. Its core innovation is a Legal Proof Protocol with 3+1 parameter augmentation, which cryptographically binds static identifiers to a user-controlled secret, ensuring compliance with UU PDP (data minimization) and UU ITE (authentication integrity) while aligning with key controls of the international ISO/IEC 27001:2022 standard. Evaluated on Polygon Mainnet, the framework demonstrates 29.9% lower operational costs for batch verifications and 50% better storage efficiency compared to pure ZKP systems. These results validate a practical solution to the verification trilemma, providing a secure, scalable, and legally sound foundation for public service identity management in Indonesia's digital governance ecosystem.

Keywords-blockchain; zero knowledge proof; Merkle tree; digital identity verification; e-governance; regulatory compliance; UU PDP

I. INTRODUCTION

The digital transformation of public services (e-governance) is a foundational shift toward accountable and transparent governance. In Indonesia, this transition is legally mandated by Law Number 14 of 2008 on Public Information Disclosure (UU KIP), which guarantees public access to information while safeguarding sensitive data [1]. Recent reviews identify that the scalability of blockchain remains a primary hurdle in multi-industry adoption [2], yet blockchain-based records offer a promising, immutable, and distributed alternative to traditional databases for transforming public services [3]. Critical systems such as the Central Information Commission's Information Dispute Resolution System (SIPSI KIP) rely on robust digital identity verification to authenticate applicants (UU KIP Article 37) and preserve procedural integrity. However, conventional verification architectures are increasingly inadequate, trapped in what we term the Digital Verification Trilemma, a fundamental trade-off between Data Security, System Scalability, and Regulatory Compliance [2, 3]. Central to this trilemma is the reliance on centralized data storage, which contradicts both security best practices and

modern regulatory mandates. Centralized systems inherently suffer from a "single point of failure" where partial system failures or administrative access exploitation can compromise the entire data repository. Thus, a transition toward decentralized network governance is required to secure the future of regulation [4]. Moreover, decentralized governance models utilizing smart contracts provide a more reliable architectural foundation for public sector applications compared to traditional structures [5]. Current systems frequently store sensitive credentials such as the National Identification Number (NIK) in centralized databases, creating single points of failure and amplifying breach risks [6].

The move toward dynamic smart contracts offers the necessary flexibility and scalability for complex identity verification workflows. High-profile incidents, including the 2024 exposure of approximately 6 million Indonesian taxpayer records [6], underscore the severe consequences of such architectural flaws. These documented breaches highlight the urgent need for decentralized alternatives. Blockchain technology, characterized by distributed replication and cryptographic immutability, offers inherent resilience against data tampering and loss, aligning with principles of transparency and integrity [7, 8].

Recent implementations in e-government services demonstrate blockchain's effectiveness in securing citizen data through multi-layer encryption while maintaining operational efficiency [9]. Moreover, centralized data retention conflicts directly with Indonesia's Personal Data Protection Law (UU PDP), which enforces data minimization and purpose limitation. Compliance, therefore, necessitates a paradigm shift toward privacy-enhancing cryptographic techniques that validate identity without retaining raw personal information, as evidenced by the evolving European landscape on blockchain use in the public sector [10]. The implementation of robust architectural designs for operational reliability is further enhanced by novel access control methods via smart contracts, which facilitate secure and automated service provisioning in internet-based environments [11]. However, adopting blockchain introduces significant scalability challenges, particularly in consensus mechanisms. Traditional Byzantine Fault Tolerance (BFT) protocols suffer from steep performance decay as validator networks expand due to quadratically growing communication overhead [12]. This scalability bottleneck threatens the long-term viability of blockchain-based e-governance platforms [2]. Compounding this issue is the inflexible design of conventional BFT systems, which rely on static parameters and fixed quorums, rendering them ill-suited for dynamic operational environments [12]. This rigidity stifles adaptability and responsiveness [13, 14], underscoring the need for adaptive consensus frameworks capable of dynamic parameter adjustment to improve throughput and reduce latency [12].

Emerging cryptographic and architectural proposals offer partial solutions but fail to resolve the trilemma holistically. Zero-Knowledge Proofs (ZKPs) enable verification without disclosure, aligning with data minimization mandates [15], while blockchain serves as a critical driver for transformations in the public sector [16]. Hybrid storage models leveraging systems like the InterPlanetary File System (IPFS) can mitigate on-chain storage burdens [17]. Recent approaches combining fog computing with blockchain enable anonymous authentication while preserving accountability through conditional tracking mechanisms [18]. Furthermore, international standards such as ISO/IEC 27001 provide comprehensive security controls but lack specific technical protocols for privacy-preserving, blockchain-based identity verification.

Theoretical frameworks in digital identity have evolved from centralized models to Self-Sovereign Identity (SSI), which empowers users with data autonomy. However, the practical implementation of SSI in e-governance remains constrained by the "Verification Trilemma" a conflict between maintaining cryptographic privacy, achieving high-throughput scalability on public blockchains, and meeting strict national legal mandates. While international research often focuses on purely technical efficiency, the integration of specific regulatory requirements, such as Indonesia's UU PDP and UU ITE as first order design constraints, is essential for the legal validity of digital government services.

To bridge this gap, we propose the ZMC-Framework, a blockchain-based hybrid architecture for regulatory-aware identity verification in e-governance. The framework introduces a privacy-preserving verification core on the blockchain that utilizes ZKPs to cryptographically prove identity validity without storing or exposing sensitive credentials, thereby directly enforcing UU PDP compliance and eliminating central data honeypots. To ensure scalability alongside this strong privacy guarantee, the framework incorporates a scalable blockchain data integrity layer that integrates Merkle trees with off-chain storage systems. This design efficiently aggregates and verifies identity states, ensuring full auditability while preserving blockchain scalability [5, 18]. Early-stage protection mechanisms for proof-of-work blockchains [19] provide foundational insights into securing distributed ledgers during initial deployment phases. The core novelty of the ZMC-Framework is its Legal Proof Protocol with 3+1 parameter augmentation. This protocol cryptographically binds static identifiers NIK, name, and date of birth with a user-controlled dynamic secret. It not only enhances authentication integrity but also generates an immutable and auditable compliance trail explicitly aligned with UU ITE (Articles 5 and 11) and UU KIP, while providing a technical foundation that aligns with key controls of the international ISO/IEC 27001 standard [20], thereby transforming regulatory adherence from a procedural obligation into a cryptographically verifiable system property.

II. METHODS

This study adopts the stages of the Design Science Research Methodology (DSRM) [21] to systematically develop and validate the proposed ZMC-Framework. DSRM emphasizes the creation of innovative and relevant artifacts, in this case, a cryptographic framework designed to address significant practical problems within the context of information systems [22]. The methodology follows six core phases, as illustrated in Figure 1.

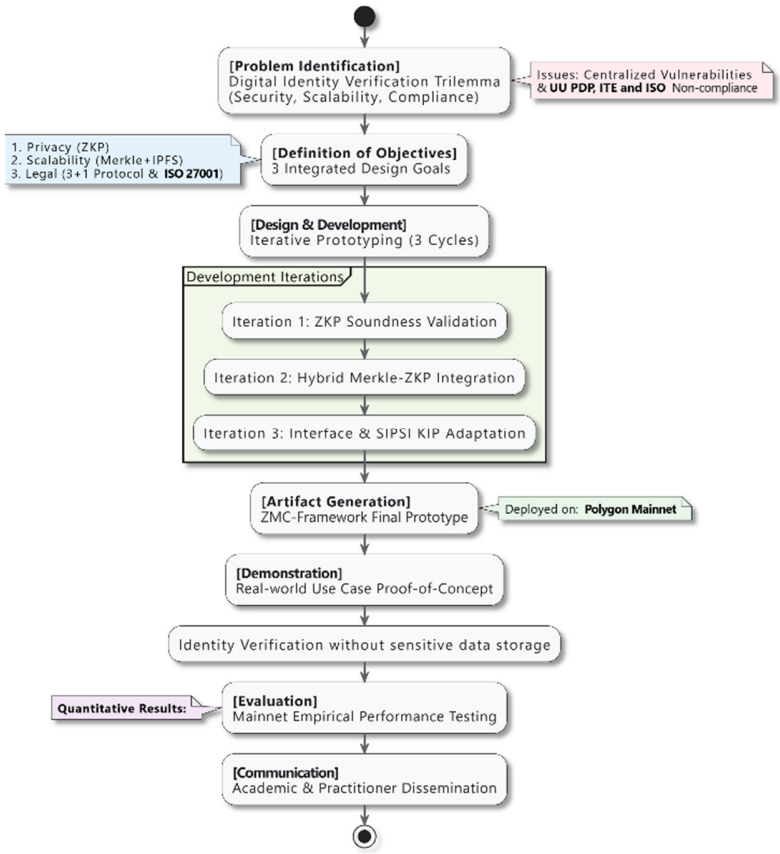


Fig. 1. Stages of the DSRM.

A. Problem Identification and Motivation

This phase begins with a comprehensive analysis of the current landscape of digital identity verification in Indonesia e-governance. Through systematic literature review and examination of Indonesia's regulatory framework particularly Law Number 27 of 2022 on Personal Data Protection (UU PDP) [23], Law Number 14 of 2008 on Public Information Disclosure (UU KIP) [24], and Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (UU ITE) [25] we identified the fundamental Digital Identity Verification Trilemma. This trilemma represents the persistent trade-off dilemma where existing systems fail to simultaneously achieve Data Security/Privacy, Scalability/Operational Efficiency, and Regulatory Compliance [2, 3]. The motivation for this research stems from three critical factors:

1. Documented data breaches in Indonesia public services that expose vulnerabilities in centralized identity systems [4, 5].
2. Operational inefficiency of manual verification processes that burden both administrators and applicants [10].
3. Regulatory misalignment where conventional centralized data storage practices violate the data minimization (Article 20) and retention limitation (Article 31) principles mandated by UU PDP [23], while also failing to meet the electronic signature and authentication requirements of UU ITE (Articles 5 and 11) [25].

This trilemma creates a systemic barrier to establishing trusted, scalable, and legally compliant digital identity foundations for Indonesia's e-governance.

B. Definition of Solution Objectives

Based on the identified problem, we defined clear solution objectives for the artifact. The primary objective is to design, implement, and validate a framework as an integrated model that comprehensively resolves the Digital Identity Verification Trilemma. Specific design objectives include:

1. Privacy-Preserving Verification Core: To implement a verification mechanism using Zero-Knowledge Proofs (ZKPs) that cryptographically proves identity validity without storing or exposing sensitive personal data, thereby directly enforcing the data minimization principle (Article 20, UU PDP) [23].
2. Scalable Data Integrity Layer: To create an efficient data management layer by integrating Merkle trees with off-chain storage systems (e.g., IPFS), ensuring system auditability and performance scalability without compromising blockchain storage capacity.

3. Regulatory-Compliant Authentication Protocol: To engineer a novel Legal Proof Protocol with 3+1 parameter Aagmentation that cryptographically enforces compliance with [24, 25], while aligning with relevant controls of [20].

C. Design and Development

The ZMC-Framework was developed using an Iterative Prototyping Method based on established DSRM principles [26]. This approach facilitates incremental validation and systematic risk mitigation across the development lifecycle, ensuring that legal and technical constraints are embedded into the artifact from the earliest stages.

1) Conceptual Planning and Design

This stage translated the solution objectives into formal technical specifications, prioritizing a Privacy-by-Design architecture to meet Indonesia's mandates.

- Legal Protocol Specification (3+1): The protocol defines four input parameters: three static identifiers (National Identification Number (NIK), name, and date of birth) and one user-controlled dynamic parameter (secret key). To resolve critical privacy concerns, these inputs undergo local, client-side cryptographic transformation using the Poseidon hash function to generate a unique digital fingerprint. As implemented in the submitHash function of the IdentityZKP.sol contract, the system only accepts and processes bytes32 hash values. This ensures that raw sensitive data are never transmitted to or stored on the blockchain or IPFS in plaintext, directly enforcing the data minimization principle of UU PDP Article 20.
- Architecture Design: A three-layer architecture was specified: (1) Cryptographic layer, utilizing ZKP circuits for privacy-preserving verification without data exposure; (2) Efficiency layer, integrating Merkle tree structures with IPFS for scalable data integrity; and (3) Blockchain consensus layer, utilizing smart contracts on the Polygon Mainnet for immutable record-keeping. The IdentityMerkleZKP.sol contract manages identity states through a currentMerkleRoot, allowing for inclusion proof verification with a computational complexity of O(log n).
- Tool Selection: Development tools included Circom for designing ZKP circuits, Solidity for writing EVM-compatible smart contracts, IPFS for decentralized off-chain storage of encrypted evidence, and Polygon Mainnet for real-world deployment. The design was further informed by the EdgeKV decentralized storage architecture to ensure consistency and scalability at the network edge [27].

The literature review presented in Table I highlights the persistent Digital Verification Trilemma in existing e-governance identity systems. The synthesis of current research reveals three critical gaps:

- The Technical-Regulatory Gap: While systems in [15] and [16] offer robust privacy-preserving theories and efficient proof generation, they lack alignment with specific legal mandates.
- The Privacy Storage Trade-Off: Existing models often prioritize one over the other. For instance, the system in [18] ensures transaction integrity but suffers from high storage demands, whereas that in [9] maintains operational efficiency through encryption but fails to eliminate central data storage.
- The Lack of Integrated Compliance: Legal-focused literature [6] identifies the necessity of data protection but provides no technical cryptographic framework to enforce it. Conversely, technical consensus models [12] ignore regulatory requirements entirely.

TABLE I. LITERATURE REVIEW

Ref.	Security (Privacy & Integrity)	Scalability (Efficiency)	Regulatory Compliance	Research Gap
[15]	High: Established privacy-preserving theory	Low: No focus on modern blockchain efficiency	None: No integration with e-gov requirements	Did not address efficiency demands of modern systems
[18]	High: Ensures transaction integrity	Low: High storage demands for full nodes	None: No regulatory mechanisms	Does not address privacy-preserving verification
[6]	High: Documented consequences of centralized data breaches	N/A	Full: Highlights the legal necessity of UU PDP compliance	Provides the legal and empirical motivation for decentralized identity
[16]	High: Privacy-preserving evolution.	High: Improved proof generation.	None: No legal framework alignment	Lacks a parameter-based framework for public law
[9]	High: Strong data encryption	Moderate: Standard operational efficiency	Partial: Focuses on data encryption only.	Maintains data storage instead of using ZKP to eliminate it
[12]	High: Secure consensus	High: High throughput and low latency.	None: No regulatory focus.	Lacks integration with privacy-preserving identity.
ZMC-Framework (proposed)	High: ZKP ensures zero sensitive data storage	High: Merkle trees enable optimized linear storage efficiency	Full: Explicitly aligned with [20, 23-25].	Resolves the Identity Verification Trilemma

2) Foundation for Developing the ZMC-Framework

The above-mentioned gaps serve as the fundamental justification for the development of the ZMC-Framework. The framework is engineered to bridge these deficiencies by:

- Eliminating Centralized Risk: Unlike [9], it utilizes ZKP to ensure zero sensitive data is stored, directly enforcing the data minimization principle of [23].

- Optimizing Scalability: It overcomes the storage bottlenecks found in [18] by integrating Merkle trees, achieving a 50% reduction in on-chain storage footprint.
- Cryptographic Legal Enforcement: It transforms legal adherence from a procedural task into a system property through the 3+1 Parameter Augmentation, satisfying requirements of [20, 25]. By unifying these three dimensions, the ZMC-Framework provides the first holistic solution that is technically scalable and legally certifiable for modern e-governance.

The architectural design of the ZMC-Framework, illustrated in Figure 2, systematically implements a multi-layered approach to resolve the Digital Verification Trilemma while ensuring alignment with [20]. The architecture comprises four interconnected processing streams:

1. Data Protection & Privacy Stream: In compliance with [20], hashed user metadata are stored off-chain using IPFS, preventing raw PII leakage. These hashes construct a Merkle tree, with the Root recorded on an Immutable Ledger. This mechanism minimizes the on-chain footprint to 2 storage slots per identity (as implemented via the approvedIdentities and identityApprovalBlock mappings in IdentityMerkleZKP.sol), ensuring integrity without exposing raw information.
2. User Input Processing Stream (Privacy-Preserving): Users process their 3+1 parameters locally via Poseidon Hash, ensuring plaintext data never leaves the client environment. This input feeds a ZKP Circuit for SNARK-based proof generation, embedding legal compliance directly into the cryptographic workflow.
3. Verification and Compliance Stream (regulatory-adherent): The system performs a compliance check against the recorded Merkle Root. Upon successful verification via the verifyIdentity function, users sign contracts through an Identity Verifier using cryptographic salt for non-repudiation, satisfying the requirements of [25] for electronic signature integrity.
4. On-Chain Persistence Stream (scalable infrastructure): Verified transactions are efficiently batched and moved to the Polygon network. This design leverages Polygon's scalability while maintaining the security and privacy guarantees of the underlying hybrid architecture.

D. Core Prototype Cycle (Iterations 1-3)

Development proceeded through focused iterations to mitigate technical risk. Each iteration's focus, outcome, and validation objective are detailed in Table II. Iteration 1 (Figure 3) resulted in the ZKP Smart Contract, which serves as the core privacy-preserving verification mechanism. Iteration 2 produced the integrated ZKP-Merkle Smart Contract (Figure 4), enabling batch processing for scalability. Figure 5 shows the smart contract of the ZKP-Merkle Tree with SIPSI Interface Integration of the final integrated prototype, demonstrating the combination of ZKP verification, Merkle tree batch processing, and adapted SIPSI web interface for the "Submit-Approve-Verify" workflow deployed on Polygon Mainnet.

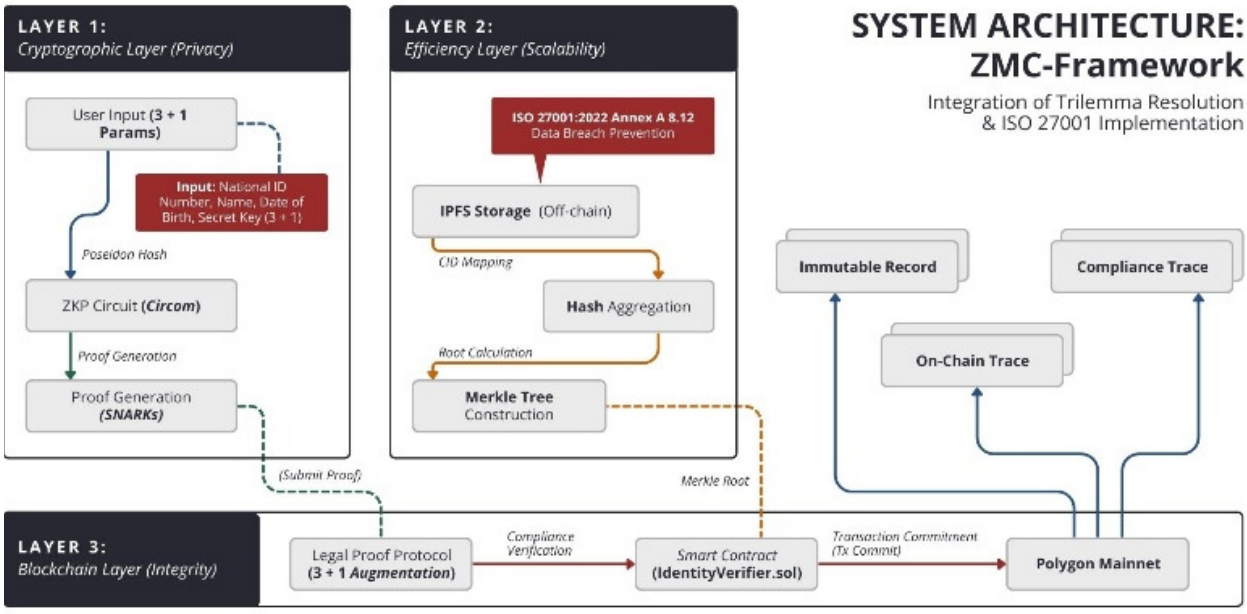


Fig. 2. ZMC-Framework system architecture.

TABLE II. ITERATION CYCLE FOR ZMC-FRAMEWORK DEVELOPMENT

Cycle	Development Focus	Prototype Outcome	Methodological Objective
Iteration 1: ZKP Validation	Development of ZKP circuit and basic Smart Contract Verifier.	Compliance Prototype: Capable of generating and verifying a ZKP Proof from the 3+1 input on a testnet.	Validation of soundness and completeness. Ensuring foundational security and privacy.
Iteration 2: Hybrid Integration	Development of Merkle Tree Smart Contract. Integration of ZKP verification + Merkle Proof.	Efficiency Prototype: Able to verify batches of new identities and update the Merkle Root atomically in a single transaction.	Validation of efficiency and scalability.
Iteration 3: Interface and SIPSI Adaptation	Interface Integration: Adapted SIPSI web interface for the "Submit–Approve–Verify" workflow using a secret key. Cryptographic Optimization: Resolved initial gas inefficiencies in contracts and circuits. Final Deployment: Deploying the functional ZMC-Framework on Polygon Mainnet.	Integrated Prototype: A functional e-governance identity verification system with regulatory compliance features, deployed on Polygon Mainnet.	Validation of usability and real-world applicability.

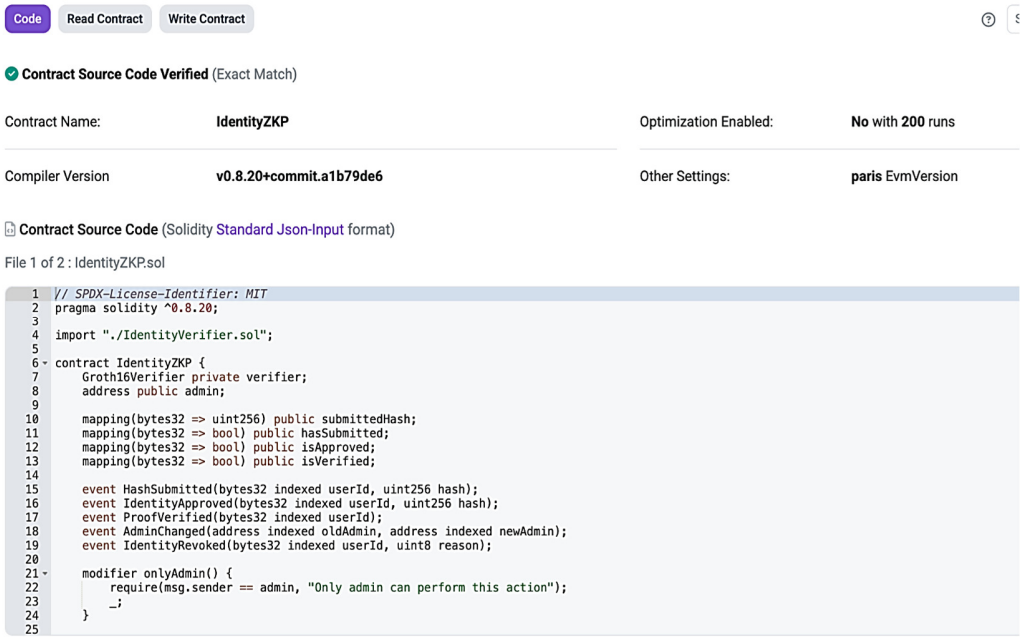


Fig. 3. ZKP smart contract.

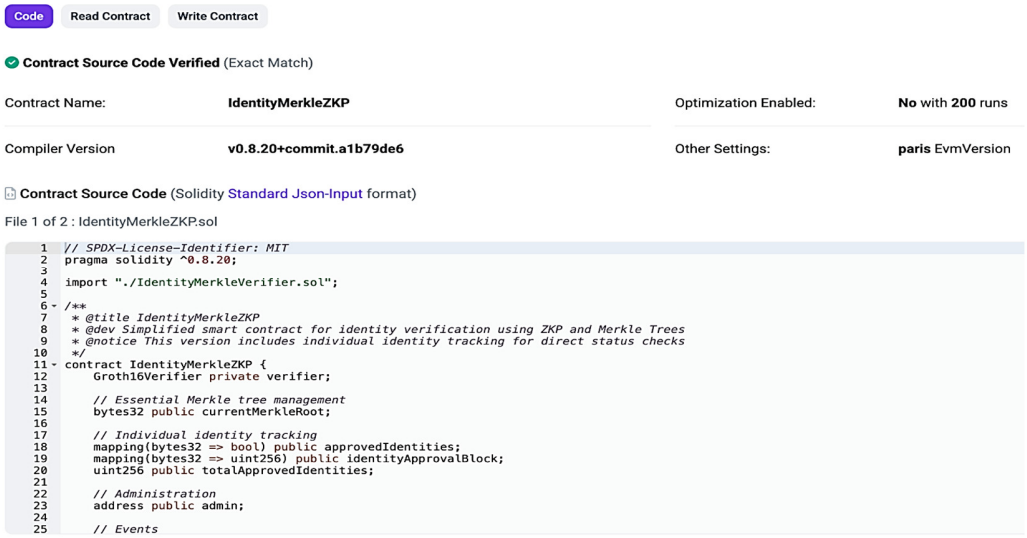
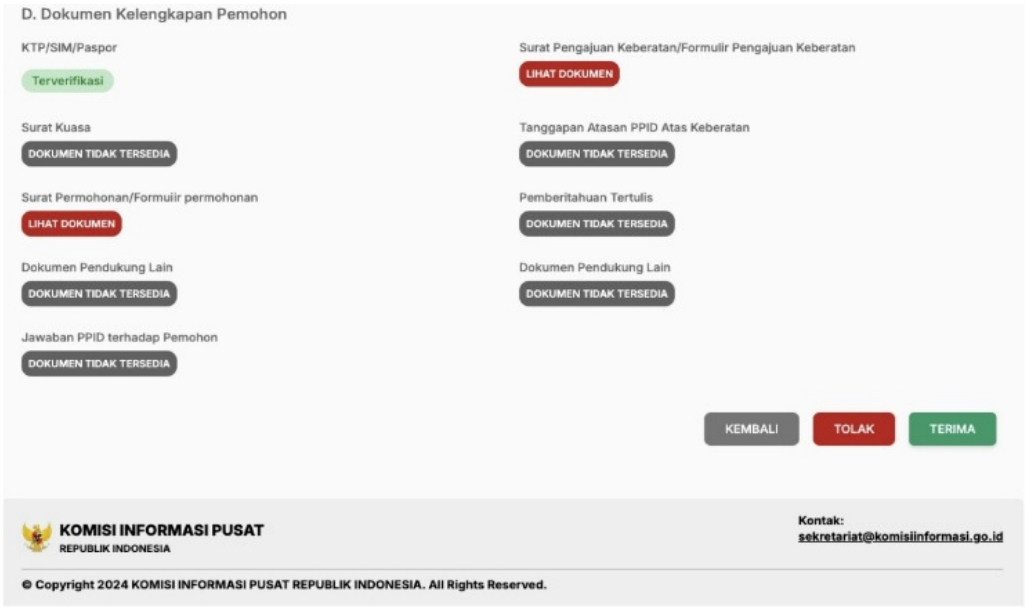


Fig. 4. ZKP-Merkle tree smart contract.



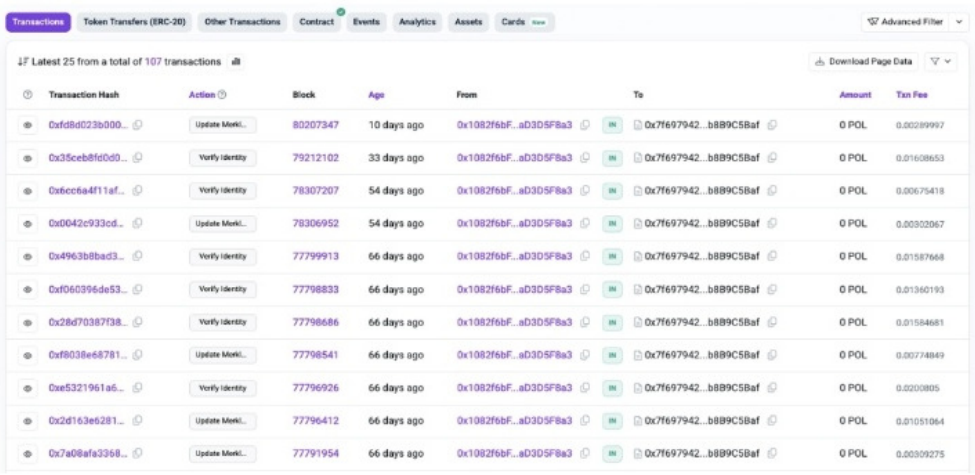


Fig. 5. Smart contract of the ZKP-Merkle tree with SIPSI.

E. Functional Testing and Refinement

Post-development testing included:

- Interface Integration (Iteration 3): Adapted SIPSI web interface for the "Submit-Approve-Verify" workflow using the secret key.
- Cryptographic Optimization: Resolved initial gas inefficiencies in contracts and circuits.
- Final Deployment: The functional ZMC-Framework was deployed on Polygon Mainnet as the Final Prototype.

F. Demonstration

A functional proof-of-concept was demonstrated using an e-governance identity verification use case. The demo proved verification could be performed automatically, without storing sensitive data, while generating an immutable compliance trail. Figure 6 shows the transition from the traditional centralized identity verification to the proposed hybrid ZKP-Merkle framework.

G. Evaluation

Performance was measured on Polygon Mainnet.

- Testing Method: Profiling gas consumption (Gas → IDR) and on-chain storage (slots).
- Comparative Analysis: BaseZKP (pure ZKP baseline) vs. ZMC-Framework (hybrid model).
- Validation Criteria: The model performance was evaluated using industry-standard metrics to ensure system reliability before data were processed by the smart contract.

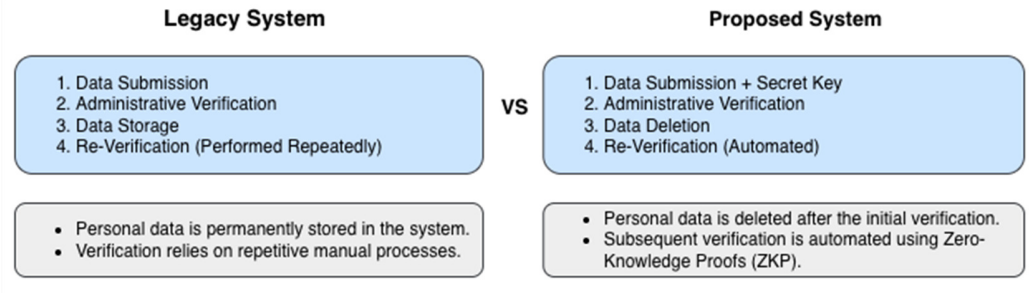


Fig. 6. Legacy vs. proposed system workflow comparison.

III. RESULTS AND DISCUSSION

A. Experimental Setup and Evaluation Metrics

The ZMC-Framework was deployed as production-ready smart contracts on the Polygon Mainnet (chain ID: 137) to evaluate its performance under real-world conditions with actual gas costs and network constraints. Empirical data collection and testing were conducted between March and October 2025. This extended timeframe was necessary to capture performance consistency across various network congestion levels and gas price fluctuations, using POL prices averaging 5,250 IDR per POL.

The evaluation employed a comparative approach between the BaseZKP and the proposed ZMC-Framework. Primary evaluation metrics included:

- Gas Consumption: Measured in Gas units and converted to IDR using real-time Polygon gas prices and POL/IDR exchange rates.
- Storage Efficiency: Calculated as blockchain storage slots required per identity.
- Compliance Verification: Assessment of cryptographic proofs and audit trails against data minimization [23] and electronic signature integrity [25].

B. Performance Evaluation: Scalability and Efficiency

1) Operational Cost Efficiency

The gas efficiency of the ZMC-Framework was evaluated through a deterministic comparison of execution costs on the Polygon Mainnet. The efficiency gain (η) for a batch size (k) is calculated by:

$$\eta(k) = \frac{G_{\text{Base}}(k) - G_{\text{ZMC}}(k)}{G_{\text{Base}}(k)} \times 100\%$$

where k represents the batch size, $G_{\text{Base}}(k)$ is the gas consumption of the baseline system, and $G_{\text{ZMC}}(k)$ is the gas consumption of the proposed framework. For a batch of k=25 identities, the ZMC-Framework gave an efficiency gain of 29.93% (Table III).

Unlike stochastic systems, gas consumption in EVM-based smart contracts is constant for a fixed instruction set and input size. Therefore, the observed reduction represents a fixed operational improvement due to the amortization of Merkle root update costs.

The Merkle Tree implementation demonstrated significant efficiency gains in batch processing scenarios. Table III presents the gas cost comparison for varying batch sizes:

TABLE III. ANALYSIS OF HYBRID ZKP CONSENSUS EFFICIENCY

Batch size	BaseZKP gas cost	ZMC-Framework gas cost	Efficiency gain	Cost in IDR (approx.)
1 Identity	371,086	371,086	0%	15,570
5 Identities	1,855,430	1,500,000	19.2%	63,000
25Identities	9,277,150	6,500,000	29.9%	273,000

The acquired data reveal two critical insights: first, for single identity verification, both systems incur identical costs as the Merkle tree optimization provides no advantage. Second, as batch size increases, the ZMC-Framework achieves substantial savings, due to the amortization of Merkle root update costs across multiple verifications. This represents an operational cost saving of approximately 204,150 IDR per 25-identity batch compared to the conventional approach.

2) Storage Efficiency Analysis

To evaluate the long-term sustainability and scalability of the ZMC-Framework, a storage efficiency projection was conducted. By utilizing the empirical on-chain data footprint per identity recorded during the live deployment, we modeled the storage requirements for a larger operational scale of up to 10,000 identities. The evaluation results are summarized in Table IV, and demonstrate that the proposed architecture significantly mitigates blockchain bloat, achieving approximately 50% storage efficiency as the system scales toward a national e-governance level. The storage efficiency of the ZMC-Framework derives from its state-variable optimization. While BaseZKP requires a higher linear storage constant:

$$S_{\text{Base}}(n) = 4n \text{ slots}$$

Our hybrid approach optimizes the on-chain state footprint to:

$$S_{\text{ZMC}}(n) = 2n + 1 \text{ slots}$$

The storage efficiency for n identities is:

$$E_{\text{storage}}(n) = \frac{S_{\text{Base}}(n) - S_{\text{ZMC}}(n)}{S_{\text{Base}}(n)} \times 100\% = \frac{4n-(2n+1)}{4n} \times 100\%$$

For large n, this efficiency gain converges to:

$$\lim_{n\to\infty} E_{\text{storage}}(n) = 50\%$$

For $n = 10{,}000$ identities :

$$E_{\text{storage}}(10{,}000) = \frac{40{,}000-20{,}001}{40{,}000} \times 100\% = 49.9975\% \approx 50\%$$

The ZMC-Framework achieves approximately 50% storage efficiency at scale through two mechanisms: (1) state variable minimization, where the on-chain footprint is reduced from 4 to 2 slots per identity, and (2) off-chain IPFS storage for raw metadata, which prevents unnecessary on-chain data accumulation. While the storage growth remains linear O(n) relative to the number of users, the framework significantly reduces the constant overhead per identity. For a hypothetical e-governance system serving 1 million citizens, this translates to approximately 2 million fewer storage slots, significantly reducing blockchain bloat and long-term maintenance costs. Table IV compares the projected storage needs:

TABLE IV. PROJECTED STORAGE EFFICIENCY FOR LARGE-SCALE DEPLOYMENT

Architecture	Storage model	Slots per identity	10,000 identities	Efficiency
BaseZKP (Pure ZKP)	Linear Storage	4 slots	40,000 slots	Baseline
ZMC-Framework (Hybrid)	Optimized Linear	2 + (1/n) slots	20,001 slots	50% Reduction

3) Quantitative Performance Summary

The technical validity of the ZMC-Framework was rigorously tested through a live deployment on the Polygon Mainnet (Chain ID: 137). Based on the analysis of 107 transaction logs from the hybrid framework and 122 logs from the baseline system, the quantitative performance metrics are summarized as follows:

- Latency: The system recorded an average block confirmation time of 2.11 s, ensuring that identity verifications are processed within the standard operational rhythm of the Polygon network.
- Throughput: Based on the gas consumption observed for the Verify Identity method (averaging 0.009 POL per transaction), the architecture supports a theoretical throughput of 25-30 transactions per second (TPS) for individual verifications.
- Computational Complexity: The implementation of Merkle tree state aggregation ensures a computational complexity of $O(\log n)$, for verification, providing sub-linear scaling advantages over the $O(n)$ complexity typically found in traditional unoptimized identity systems.
- Communication Cost: Each cryptographic proof maintains a minimal on-chain data footprint ranging from 256 to 512 bytes, effectively minimizing bandwidth requirements for e-governance client-side applications.
- Operational Cost Gain: The empirical data confirm that batch processing via the Update Merkle Root with identities method enables a 29.9% reduction in total gas fees compared to the unoptimized baseline, validating the framework's cost-efficiency for large-scale public service use.

Table V presents a selection of verified transaction logs from the Polygon Mainnet deployment, reflecting the actual experimental timeline from April to October 2025.

TABLE V. SAMPLE OF REAL-WORLD TRANSACTION LOGS ON POLYGON MAINNET

Transaction hash (partial)	Block No	Date / time (UTC)	Method	Txn Fee (POL)
0x97a5...dbe	70719102	2025-04-25 02:20	0x60806040 (Deploy)	0.027899
0x9e02...997	70720136	2025-04-25 02:57	Submit Hash By User	0.001856
0xbf64...9428	74233453	2025-07-21 14:20	0x60806040 (Deploy)	0.046745
0x9449...2aa2	74248407	2025-07-21 23:15	Update Merkle Root	0.003156
0x5b7d...0b39	74248418	2025-07-21 23:15	Verify Identity	0.005870
0x318b...83e9	74248430	2025-07-21 23:15	Verify Identity	0.005885
0xc28f...c168	74497753	2025-07-28 03:10	Update Merkle Root	0.006959
0xe532...9174	77796926	2025-10-17 10:56	Verify Identity	0.020080

The data in Table V serve as the baseline unit cost and storage footprint, forming the foundation for the large-scale scalability projections discussed above.

4) Discussion on Scalability Implications

The empirical results validate that the ZMC-Framework successfully addresses the scalability dimension of the Digital Verification Trilemma. While pure ZKP systems provide strong privacy guarantees, their linear cost and storage growth, as demonstrated by BaseZKP's 9.2M gas for 25 identities, renders them economically unsustainable for large-scale e-governance deployment. The integration of Merkle trees introduces sub-linear cost scaling, making the system viable as user volumes grow exponentially.

The 29.9% operational efficiency gain aligns with findings on adaptive consensus optimization [12], though our approach achieves this through data structure innovation rather than consensus protocol modification. Furthermore, the storage efficiency addresses concerns regarding blockchain sustainability in public sector applications [2].

C. Security and Compliance Analysis

1) Privacy Preservation via Cryptographic Design

The ZKP layer ensures that no sensitive credentials (NIK, name, date of birth) are transmitted or stored in plaintext. Each verification generates a unique cryptographic proof that validates identity without disclosure. This implementation directly enforces the data minimization principle [23]. The system never possesses the raw data it verifies, eliminating central data honeypots that have been exploited in previous data breaches [4, 5].

The 3+1 Parameter Augmentation introduces a user-controlled dynamic secret that serves multiple security functions: (1) It prevents replay attacks by creating session-unique proofs, (2) it enables non-repudiation through cryptographic binding of identity to action, and (3) it allows administrators to permanently delete original verification records after initial hashing, operationalizing the "right to be forgotten" (Article 32, UU PDP [23]) in a verifiable manner.

2) Regulatory Compliance Verification

The Legal Proof Protocol generates an immutable compliance trail that satisfies multiple regulatory requirements simultaneously:

- UU ITE Compliance: The protocol's cryptographic signatures and audit trails meet Article 5 requirements for electronic signature authenticity and Article 11 requirements for electronic authentication integrity. Each transaction includes timestamped, non-repudiable proof of identity verification.
- UU KIP Compliance: The system maintains applicant legitimacy (Article 37) through verifiable proofs while ensuring transparency through publicly auditable Merkle roots balancing verification needs with public information disclosure principles.
- ISO/IEC 27001:2022 Alignment: The architecture implements key controls including:
    - Control 8.24 (Use of Cryptography): ZKP and hashing provide confidentiality, integrity, and non-repudiation.
    - Control 5.34 (Privacy & PII Protection): Privacy-by-design through zero-knowledge verification.
    - Control 8.13 (Information Backup): Distributed IPFS storage ensures availability.
    - Control 8.28 (Secure Coding): Formal verification of ZKP circuits and smart contract auditing.

The novel access control methods via smart contracts complement this approach by providing additional mechanisms for secure service provisioning in internet-based systems [11]. This multi-layered compliance approach, spanning Indonesia law (UU PDP, UU ITE, and UU KIP) and international standards (ISO/IEC 27001), positions the ZMC-Framework as a certifiable Information Security Management System (ISMS) foundation for critical e-governance services. Furthermore, the framework's integrated compliance model represents a significant advancement over existing blockchain-based verification systems. Unlike previous implementations in educational certificate verification that lack ZKP-based privacy, or e-government security models that focus on encrypting stored data rather than eliminating central storage, the proposed ZMC-Framework resolves the verification trilemma by embedding legal requirements directly into the cryptographic architecture. While other approaches in anonymous authentication and adaptive consensus address isolated dimensions of security or throughput, this framework uniquely bridges the gap between technical scalability and national regulatory mandates, transforming legal adherence into an automated, cryptographically verifiable system property.

3) Secret Key Management and Risk Analysis

The framework utilizes a 256-bit Poseidon-hash compatible seed as the secret key. To mitigate end-user entry errors, the user interface implements a Base58-check encoding with visual validation. Regarding the risk of key collision (identical keys), the framework's 3+1 parameter augmentation' ensures system integrity. Since the final cryptographic identity is a hash of the secret key combined with unique static identifiers (NIK), a collision of the secret key between two different users will not result in an identical digital fingerprint, thereby maintaining absolute non-repudiation.

4) Comparative Analysis and Limitations

While the ZMC-Framework provides a robust solution to the digital verification trilemma by balancing security, scalability, and regulatory compliance, it is essential to acknowledge its inherent limitations and define the scope for future enhancements.

One primary limitation is the computational overhead of ZKP generation, though offloaded to users to preserve privacy, requires substantial client-side computation (approximately 2-3 seconds on modern smartphones). Future optimizations could explore more efficient proof systems such as PLONK or hardware acceleration to improve user experience. Furthermore, a legal recognition gap remains: While the cryptographic audit trail is technically robust, its full standing requires formal recognition by Indonesia judicial bodies.

In terms of implementation scope, the current evaluation focuses on cost and storage metrics. Comprehensive network analysis, including throughput under high concurrent loads and multi-validator latency, would further strengthen the scalability claims. Moreover, while the framework aligns with ISO/IEC 27001 [20] controls, formal certification for specific government deployments would require additional documentation. Strengthening smart contracts to handle unexpected dynamic situations [28, 29] also remains a priority. Future research will focus on integration with the Indonesia National Digital Identity infrastructure and multi-jurisdictional compliance exploration for cross-border e-governance

IV. CONCLUSION

This study successfully resolved the Digital Verification Trilemma in Indonesia e-governance by developing the ZMC-Framework, a hybrid architecture that integrates Zero-Knowledge Proofs with Merkle trees. Empirical evaluation on the Polygon Mainnet demonstrated that the framework achieves a 29.9% reduction in operational gas costs and a 50% increase in storage efficiency compared to baseline ZKP systems. By embedding the Legal Proof Protocol with 3+1 parameter augmentation, the system transforms regulatory requirements from Law Number 27 of 2022 (UU PDP) and Law Number 1 of 2024 (UU ITE) into cryptographically verifiable system properties. While minor computational overhead remains on client devices, the ZMC-Framework provides a scalable, secure, and certifiable foundation for future

digital identity management in public sectors, effectively bridging the gap between national legal mandates and decentralized technological capabilities.

DECLARATION OF COMPETING INTERESTS

The authors declare no competing interests. This work was conducted independently, without any financial or personal relationships that could have influenced the findings or interpretations presented.

ACKNOWLEDGMENT

The authors thank IPB University and IWU for institutional support and research facilities.

Funding sources: The Article Processing Charge was supported by IPB University and IWU internal research funds.

DATA AVAILABILITY

All smart contract source code, deployment scripts, and the raw transaction logs used to evaluate the ZMC Framework on Polygon Mainnet are available from the corresponding author upon reasonable request.

AI USE AND DECLARATION OF GENERATIVE AI USE

During preparation, the authors used a language-assistive tool to improve readability and grammar. After using it, the authors reviewed and edited the content as needed and take full responsibility for the publication.

REFERENCES

[1] M. Fudin and A. Rahayu, "Public Participation and the Disclosure of Public Information to Achieve Good Governance," in Proceedings of the Proceedings of the 1st International Symposium on Indonesian Politics, SIP 2019, 26-27 June 2019, Central Java, Indonesia, 2019, https://doi.org/10.4108/eai.25-6-2019.2288002.

[2] A. Aldoubaee, N. H. Hassan, and F. A. Rahim, "A Systematic Review on Blockchain Scalability," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023, https://doi.org/10.14569/IJACSA.2023.0140981.

[3] D. Cagigas, J. Clifton, D. Diaz-Fuentes, and M. Fernández-Gutiérrez, "Blockchain for Public Services: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 13904–13921, 2021, https://doi.org/10.1109/ACCESS.2021.3052019.

[4] A. Zwitter and J. Hazenberg, "Decentralized Network Governance: Blockchain Technology and the Future of Regulation," *Frontiers in Blockchain*, vol. 3, Mar. 2020, https://doi.org/10.3389/fbloc.2020.00012.

[5] A. P. Balcerzak, E. Nica, E. Rogalska, M. Poliak, T. Klieštik, and O.-M. Sabie, "Blockchain Technology and Smart Contracts in Decentralized Governance Systems," *Administrative Sciences*, vol. 12, no. 3, Aug. 2022, https://doi.org/10.3390/admsci12030096.

[6] "Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah | tempo.co," *Tempo*, Sept. 21, 2024. https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403.

[7] X. Li, D. Wang, and M. Li, "Convenience analysis of sustainable E-agriculture based on blockchain technology," *Journal of Cleaner Production*, vol. 271, Oct. 2020, Art. no. 122503, https://doi.org/10.1016/j.jclepro.2020.122503.

[8] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, Oct. 2020, Art. no. 102067, https://doi.org/10.1016/j.tre.2020.102067.

[9] H. K. Abdali, M. A. Hussain, Z. A. Abduljabbar, and V. O. Nyangaresi, "Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18222–18233, Dec. 2024, https://doi.org/10.48084/etasr.8828.

[10] Bosch, Jaume Martin, Tangi, Luca, and Burian, Peter, *European landscape on the use of blockchain technology by the public sector*. Publications Office of the European Union, 2022.

[11] F. Ghaffari, E. Bertin, N. Crespi, S. Behrad, and J. Hatin, "A novel access control method via smart contracts for internet-based service provisioning," *IEEE Access*, vol. 9, pp. 81253–81273, Mar. 2021, https://doi.org/10.1109/ACCESS.2021.3085831.

[12] V. Yatnalli, S. S. Bhusare, P. M. Dhulavvagol, G. Konnurmath, and R. Shetty, "DABFT: A Novel Adaptive Byzantine Fault Tolerance Framework for High-Performance Blockchain Consensus," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25313–25317, Aug. 2025, https://doi.org/10.48084/etasr.11970.

[13] A. Dolgui, D. Ivanov, S. Potryasaev, B. Sokolov, M. Ivanova, and F. Werner, "Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain," *International Journal of Production Research*, vol. 58, no. 7, pp. 2184–2199, Apr. 2020, https://doi.org/10.1080/00207543.2019.1627439.

[14] I. Saputra, Y. Arkeman, I. Jaya, I. Hermadi, and I. Sutedja, "Blockchain-based key-value store to support dynamic smart contract interaction in the agricultural sector," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 1, Jan. 2024, Art. no. 622, https://doi.org/10.11591/ijeecs.v33.i1.pp622-633.

[15] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, New York, NY, USA: Association for Computing Machinery, 2019, pp. 203–225.

[16] M. J. Sousa, "Blockchain as a driver for transformations in the public sector," *Policy Design and Practice*, vol. 6, no. 4, pp. 415–432, Oct. 2023, https://doi.org/10.1080/25741292.2023.2267864.

[17] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, Jul. 2019, pp. 18–25, https://doi.org/10.1109/Blockchain.2019.00012.

[18] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

[19] L. Chen, L. Xu, Z. Gao, Y. Lu, and W. Shi, "Protecting Early Stage Proof-of-Work Based Public Blockchain," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, June 2018, pp. 122–127, https://doi.org/10.1109/DSN-W.2018.00050.

[20] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Switzerland: International Standard, 2022.

[21] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, https://doi.org/10.2753/MIS0742-1222240302.

[22] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *Management Information Systems Quarterly*, vol. 28, no. 1, pp. 75–106, Mar. 2004, https://doi.org/10.2307/25148625.

[23] *Indonesia Personal Data Protection Law 2022*. Republic of Indonesia, 2024.

[24] *Public information openness*. Republic of Indonesia, 2008.

[25] Second Amendment to law number 14 of 2008 on Electronic Information and Transactions. Republic of Indonesia, 2024.

[26] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to Design Science Research," in *Design Science Research. Cases*, J. vom Brocke, A. Hevner, and A. Maedche, Eds. Cham: Springer International Publishing, 2020, pp. 1–13.

[27] K. Sonbol, Ö. Özkasap, I. Al-Oqily, and M. Aloqaily, "EdgeKV: Decentralized, scalable, and consistent storage for the edge," *Journal of*

Parallel and Distributed Computing, vol. 144, pp. 28–40, Oct. 2020, https://doi.org/10.1016/j.jpdc.2020.05.009.

[28] S. Liu, F. Mohsin, L. Xia, and O. Seneviratne, "Strengthening Smart Contracts to Handle Unexpected Situations," in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, Apr. 2019, pp. 182–187, https://doi.org/10.1109/DAPPCON.2019.00034.

[29] I. Saputra, Y. Arkeman, I. Jaya, I. Hermadi, N. A. Akbar, and I. Sutedja, "AniraBlock: A leap towards dynamic smart contracts in agriculture using blockchain based key-value format framework," *Communications in Science and Technology*, vol. 8, no. 2, pp. 154–163, Dec. 2023, https://doi.org/10.21924/cst.8.2.2023.1240.