SINERGI Vol. 30, No. 3, October 2026: 961-980
http://publikasi.mercubuana.ac.id/index.php/sinergi
http://doi.org/10.22441/sinergi.2026.3.021

Designing the framework architecture of a blockchain-based cooperative oversight system in Indonesia: a Socio-Technical System (STS) approach

Agus Mulyanto[1], Riri Fitri Sari[2]*, Rachma Fitriati[3], Muhammad Firdaus Syawaludin Lubis[2]
[1]Department of Information System, Institut Teknologi PLN, Indonesia
[2]Department of Electrical Engineering, Universitas Indonesia, Indonesia
[3]Department of Business Administration, Universitas Indonesia, Indonesia

Abstract
Indonesia's cooperative sector plays a strategic role in inclusive economic development, yet persistent weaknesses in supervision continue to produce fragmented information, inconsistent data, and governance risks across administrative levels. These conditions motivate the design of an integrated e-government architecture for cooperative oversight. This study designs a framework architecture for a blockchain-based cooperative oversight system in Indonesia using a qualitative case study approach and Socio-Technical Systems (STS) theory to derive architectural requirements from institutional, regulatory, and organizational conditions. Data were collected through interviews and focus group discussions with 46 participants, as well as through the analysis of national regulations. The proposed framework specifies a six-layer e-government architecture aligned with ISO 23257:2022, comprising blockchain, service, access, application, security and privacy, and infrastructure layers. The architecture defines permissioned participation, role-based identity management, standardized oversight workflows, and hybrid on-chain and off-chain data management to support traceable and coordinated supervision across institutions. The designed framework provides an architectural foundation for strengthening cooperative oversight while accommodating heterogeneous institutional capacity, regulatory requirements, and uneven digital infrastructure in Indonesia.

Keywords:
Blockchain;
Cooperative oversight;
E-government;
ISO 23257:2022;
Socio-technical system;

Article History:
Received: November 10, 2025
Revised: February 7, 2026
Accepted: March 4, 2026
Published: October 2, 2026

Corresponding Author:
Riri Fitri Sari
Department of Electrical Engineering, Universitas Indonesia, Indonesia
Email: riri@ui.ac.id

INTRODUCTION

Cooperatives play a strategic role in socio-economic development by promoting financial inclusion, community welfare, and participatory governance [1]. International governance frameworks, particularly the principles of the International Cooperative Alliance (ICA) [2] and the International Labor Organization (ILO) Recommendation No. 193 [3], emphasize transparency, democratic control, accountability, and reliable financial reporting as essential foundations of effective cooperative supervision. These principles require oversight systems capable of ensuring verifiable records, consistent reporting, and coordinated monitoring among supervisory institutions [4].

Indonesia adopts these international cooperative principles within its national regulatory framework, yet the practical implementation of oversight remains fragmented. Law No. 25/1992 [5], Ministerial Regulation No. 09/2020 [6], and Law No. 4/2023 [7] establish formal supervisory obligations and reporting requirements for cooperatives. However, practical implementation remains fragmented due to decentralized authority, heterogeneous administrative capacity, and reliance on manual or siloed digital systems, resulting in delayed verification, inconsistent data, and weak transparency [8]. These weaknesses culminated in significant governance failures, exemplified by the 2023 collapse of eight major cooperatives with unpaid obligations of IDR 26 trillion [9]. This situation reflects systemic shortcomings in supervisory mechanisms that failed to enforce transparency and accountability in practice, underscoring the need for a more reliable and coordinated cooperative oversight architecture.

Against this backdrop, electronic governance technologies have been explored to strengthen public-sector accountability and interoperability. Centralized e-government architectures consolidate administrative control within a single institution, enabling efficiency but creating single points of failure and limiting auditability and cross-agency transparency [10]. Federated e-government architectures were subsequently proposed to improve interoperability by enabling inter-organizational data exchange while preserving institutional autonomy [11]. Nevertheless, federated systems continue to depend on inter-institutional trust and asynchronous data synchronization, constraining integrated auditability and timely supervisory intervention [12].

More recently, blockchain and distributed ledger technologies have been examined as a further evolution beyond federated architectures to address persistent challenges related to trust, auditability, and cross-agency data consistency through decentralized and verifiable recordkeeping [13, 14, 15, 16]. Researchers have applied blockchain to various public-sector functions such as digital identity digital identity [17], land registration [18][19], notarial services [20], supply chain governance [21][22], public finance [23][24], government management [25], health systems [26, 27, 28, 29], and auditing [30]. Governments in Estonia [31], the United Arab Emirates [32], China [33], Malaysia [34], Vietnam [35], and several European countries have piloted blockchain to improve data integrity, automate verification, and strengthen trust in administrative processes [36]. While blockchain enhances immutability and traceability, it does not inherently guarantee data accuracy at the point of entry. Erroneous or fraudulent inputs may become permanently recorded, making pre-entry validation, trusted data sources, and procedural controls essential components of blockchain-based governance systems.

Within the public sector, cooperative oversight represents a governance domain characterized by multi-level supervision, legally sensitive financial accountability, and inter-agency coordination. These characteristics align poorly with architectures that rely solely on administrative trust, such as centralized databases or federated systems, which cannot fully enforce shared-state consistency or end-to-end auditability across institutions [4, 10, 11]. In contrast, permissioned blockchain architectures embed protocol-level immutability, synchronized ledgers, and cryptographically verifiable audit trails [37][38], making them conceptually well-suited to fragmented, semi-trusted oversight environments such as Indonesia's cooperative supervision structure.

Despite growing interest in blockchain-based e-government, important gaps remain. Prior studies predominantly focus on transparency, immutability, and security properties, while data accuracy and cross-agency consistency are rarely treated as core architectural concerns [25][39]. Moreover, most implementations assume trustworthy data inputs and provide limited analysis of hybrid on-chain and off-chain architectures, despite their prevalence in real-world government systems [15][40]. Frameworks specifically tailored to cooperative oversight, characterized by multi-level supervision, financial accountability, and member-based governance, also remain scarce. In addition, existing studies seldom integrate socio-technical perspectives with international standards, such as ISO 23257:2022 [41], to guide the design of interoperable, auditable, and secure blockchain-based e-government.

Accordingly, this study proposes a socio-technical and ISO-aligned architectural framework for blockchain-based cooperative oversight in Indonesia. The contribution lies in systematically aligning regulatory requirements, organizational workflows, and technical components within a coherent e-government architecture, consistent with prior calls for standards-driven and context-aware blockchain adoption in the public sector [13, 16, 42]. Specifically, this study pursues three objectives: (1) identifying socio-technical factors influencing cooperative oversight digitalization; (2) designing an ISO-aligned blockchain-based e-government architecture; and (3) analyzing implementation challenges related to data accuracy, data consistency, and inter-agency coordination.

METHOD

Research Design

This study adopts a qualitative case study design to analyze the architecture of a blockchain-based cooperative oversight system in Indonesia, enabling in-depth examination of governance processes and exploratory theory building in emerging domains [43][44]. The study addresses persistent weaknesses in standardized digital procedures, reporting consistency, and system interoperability within Indonesia's cooperative oversight, as documented in official evaluations and supervisory reports issued by the Ministry of Cooperatives and SMEs and regional departments.

The study applies Socio-Technical Systems (STS) theory as the analytical foundation for the proposed architectural design [45]. Using the four core STS dimensions as an integrated design framework [46], the study examines interactions among institutional arrangements, regulatory structures, organizational practices, human actors, and technological infrastructures that shape system outcomes [47]. The people dimension analyses stakeholder roles, competencies, and accountability mechanisms in cooperative oversight. The structure dimension evaluates Indonesia's cooperative regulatory framework, including Law No. 25/1992 and related ministerial regulations, which reveal gaps in compliance, reporting, and institutional coordination [5]. The task dimension identifies oversight functions, audit workflows, and reporting processes that the proposed blockchain-based architecture must support. The technology dimension assesses infrastructure readiness, security requirements, and interoperability constraints within Indonesia's digital government environment.

Figure 1 illustrates how these STS dimensions jointly inform the architectural logic of the proposed blockchain-based cooperative oversight system and ensure coherent integration of social and technical components in the system design.

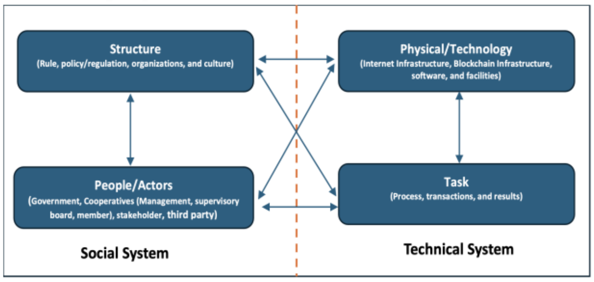

Figure 1. STS protocol for blockchain-based e-government framework design

Data Collection

The study employed primary and secondary data to support analytical triangulation. Primary data were collected through semi-structured interviews and focus group discussions conducted between September and November 2023, involving 46 participants across three stakeholder groups.

Government stakeholders comprised 12 participants representing three institutions, namely the Ministry of Cooperatives and SMEs (2 participants), BAPPENAS (4 participants), and cooperative supervisory offices at the provincial level in Lampung, West Java, and Jakarta (6 participants). Cooperative stakeholders consisted of 27 participants representing 27 cooperatives located in Lampung (2), Jakarta (4), West Java (20), and East Java (1). In addition, four professional practitioners participated. Technology experts included four participants specializing in blockchain engineering, network security, risk management, and IT security. All interview and FGD protocols followed socio-technical system dimensions and addressed regulatory compliance, process bottlenecks, identity management requirements, technological readiness, and stakeholder expectations.

Secondary data comprised key Indonesian regulatory instruments governing cooperative oversight and digital government. Law No. 25/1992 [5] establishes cooperative principles and governance, while Ministerial Regulations No. 09/2020 [6] and No. 19/2015 [48] define supervisory, audit, and members' meeting procedures. Presidential Regulation No. 95/2018 [49] sets national SPBE standards for interoperability, security, and data exchange. Law No. 4/2023 [7] further strengthens cooperative supervision through enhanced accountability, transparency, and reporting requirements, particularly for savings and loan cooperatives. Additional sources included supervisory and performance reports from the Ministry of Cooperatives and SMEs and provincial offices, which consistently indicate challenges related to compliance, reporting accuracy, data fragmentation, and oversight capacity. Collectively, these documents informed the regulatory and governance requirements underlying the proposed blockchain-based e-government architecture.

Data Analysis

The study employs thematic analysis that integrates STS-guided classification with the inductive identification of empirical patterns from interviews, focus group discussions, and documents. The analysis organizes qualitative evidence across people, structure, task, and technology dimensions and identifies key institutional and technical challenges in Indonesia's cooperative oversight system. These challenges are synthesized into analytical considerations that reflect organizational readiness and contextual constraints, thereby informing the architectural requirements of the proposed blockchain-based e-government framework and ensuring alignment with STS theory and the national regulatory context.

Design Architecture

This study designs the proposed blockchain-based cooperative oversight architecture by systematically aligning the four Socio-Technical Systems (STS) dimensions with the architectural principles defined in ISO 23257:2022 [41]. The STS analysis translates social, organizational, regulatory, and technical requirements into explicit architectural layers that structure the system design. The resulting architecture integrates governance and oversight modules, audit and reporting workflows, identity and access management, and core blockchain services to support verifiable audit trails, data integrity, and interoperable cross-agency reporting.

The architectural design prioritizes modularity, privacy protection, scalability, and regulatory compliance to ensure suitability for Indonesia's cooperative oversight environment.

Architecture Validation

This study employs a structured architectural validation procedure to assess whether the proposed framework adequately addresses the socio-technical challenges identified in the STS analysis. The validation comprises three stages that examine socio-technical alignment, technical adequacy, and institutional comparability.

The procedure maps STS-derived challenges to architectural components, evaluates the adequacy of core architectural mechanisms under regulated, multi-agency conditions, situates the design within international public-sector blockchain practices, and contrasts it with centralized and federated database alternatives across governance-relevant dimensions, including trust, coordination, auditability, data integrity, and scalability.

RESULTS

Cooperative Oversight in Indonesia

Indonesian cooperatives operate under a kinship-based governance model that emphasizes collective ownership, democratic participation, and seven cooperative principles [50]. Law No. 25/1992 provides the legal foundation for cooperative governance and defines internal and external oversight mechanisms. These principles are aligned with internationally recognized cooperative norms articulated by the ICA [2] and the ILO No. 193 [3], including voluntary and open membership, democratic member control, member economic participation, autonomy and independence, and education, training, and information. This alignment positions Indonesia's cooperative governance framework within the broader global context of cooperative values and standards.

Internal oversight relies on two governance bodies. The Annual Members Meeting (AMM) serves as the highest authority by reviewing financial reports, evaluating performance, approving plans and budgets, and electing board members. The Supervisory Board conducts continuous monitoring by examining financial records, ensuring regulatory compliance, and resolving internal disputes.

External oversight follows the regulatory mandates set in Ministerial Regulation No. 09/2020 [6], which defines procedures for cooperative monitoring and audit. Government Regulation No. 7/2021 [51] expands these requirements by establishing the national framework for cooperative development and supervision. Law No. 4/2023 [7] further strengthens oversight by imposing stricter accountability and transparency obligations, particularly for financial cooperatives. The Ministry of Cooperatives and SMEs (MCMSE) oversees inter-provincial cooperatives, Cooperative Provincial Agencies (CPA) oversee multi-district cooperatives, and Cooperative District or City Agencies (CDA) oversee local cooperatives through document verification, reporting reviews, on-site inspections, and sanctions such as warnings, operational restrictions, or revocation of cooperative status.

Oversight reports from national and regional agencies consistently identify recurring problems. Many cooperatives submit incomplete or inaccurate financial statements, often because of limited accounting capacity. Reporting formats also vary across districts, creating fragmented and inconsistent data. Provincial and district offices face capacity constraints, including shortages of trained personnel, uneven digital skills, and frequent staff rotation that undermines institutional continuity. Several cooperatives exploit regulatory gaps by engaging in practices such as shadow banking, inflating mandatory deposits, falsifying reports, and deliberately causing insolvency. These conditions indicate structural and operational weaknesses that undermine the effectiveness of the current oversight system.

Socio-Technical Issues and Requirements

Indonesia's cooperative oversight system faces persistent socio-technical issues that constrain accuracy, consistency, and accountability. Although regulations clearly define internal and external oversight roles, their implementation depends on fragmented organizational structures, heterogeneous procedures, and disconnected information systems across administrative levels.

Oversight authorities and cooperatives manage supervisory data through a combination of locally developed systems and centralized databases operating independently at district, provincial, and national levels. This arrangement impedes uniform data standards, consistent validation rules, and effective cross-jurisdictional reconciliation, resulting in incomplete, delayed, and inconsistent supervisory information.

The socio-economic nature of cooperatives further intensifies these challenges. Cooperatives emphasize member autonomy, collective decision-making, and data confidentiality, whereas oversight institutions require verifiable, comparable records. In the absence of integrated supervisory mechanisms, cooperatives retain primary control over membership data, Annual Members Meeting documentation, and financial records, thereby limiting external verification and increasing the risk of inaccurate reporting and selective data modification.

Oversight practices also rely heavily on manual documentation, non-standardized reporting formats, and localized verification procedures. Regional capacity disparities and frequent personnel rotation weaken institutional continuity, while existing digital authentication and reporting tools, where available, do not enforce common data structures or cross-institutional consistency.

These conditions indicate that current oversight limitations stem from socio-technical misalignment rather than regulatory absence. Fragmented authority, non-standardized processes, and disconnected data management practices collectively undermine reliable supervision. Table 1 synthesizes these issues using the STS framework and provides the basis for evaluating oversight requirements in the subsequent section.

Design of E-Government Framework

Building on the identified socio-technical constraints and architectural requirements, this study designs the architecture of a blockchain-based cooperative oversight system in Indonesia. The proposed architecture addresses persistent challenges in interoperability, accountability, and scalability arising from fragmented oversight processes and heterogeneous institutional capacities.

ISO 23257:2022(E) [41] provides an architectural reference by defining component organization, governance boundaries, identity management, interoperability mechanisms, and security controls for permissioned distributed ledger systems [53]. Alignment with these standards preserves cooperative data ownership and internal governance processes, while enabling traceable, verifiable, and secure oversight access across national, provincial, and district authorities. The proposed architecture consists of six modular layers that include the blockchain, service, access, application, security and privacy, and infra structure layers, as illustrated in Figure 2.

Blockchain Layer

This layer defines the blockchain platform, consensus mechanism, identity management, channel and ledger organization, smart contract logic, and document anchoring strategy to support accountable, reliable, and autonomy-preserving cooperation.

First, the architecture adopts a permissioned consortium blockchain based on Hyperledger Fabric to enable collaboration among semi-trusted organizations [54] while preserving cooperative autonomy. Fabric provides native support for permissioned participation, role-based access control, and Membership Service Provider (MSP)-based identity management using certificates issued by Certification Authorities (CA) [55]. Compared with other consortium-oriented platforms such as Quorum and Corda, which emphasize bilateral transaction coordination or application-level workflows, Fabric explicitly supports multi-party governance and a shared supervisory ledger required in hierarchical public-sector oversight settings [37].

Table 1. Social and technical dynamics of cooperative oversight systems in Indonesia.

Aspect	Challenges	Issues	Architecture Requirements
People	Resource inequality	Regional authorities operate with unequal human and financial resources, producing uneven supervisory capacity and inconsistent enforcement across administrative levels.	Uniform supervisory functionality operable under heterogeneous resource conditions
	Coordination problems	Weak coordination among district, provincial, and national offices delays audits, data verification, and enforcement actions.	Cross-level coordination and shared supervisory visibility
	Limited expertise	Cooperative managers and local officials lack sufficient expertise in digital reporting and data verification, increasing inaccurate or incomplete submissions.	Structured supervisory interactions that reduce dependence on individual technical expertise
Structure	Regulatory implementation	Existing cooperative oversight regulations do not enforce uniform national standards for reporting formats and data structures, resulting in region-specific practices that hinder data consolidation, delay verification, and weaken early detection of irregularities.	Uniform data structures and standardized reporting formats aligned with regulatory mandates
	Organizational readiness	Regions and cooperatives adopt digital oversight systems at different levels of readiness, producing uneven data quality and reporting practices.	Architectural tolerance for heterogeneous organizational readiness
	Acceptability	Cooperative autonomy and resistance to strict supervision reduce compliance with standardized reporting and documentation requirements.	Balanced accountability mechanisms that respect cooperative autonomy
Task	Process standardization	Oversight relies on manual records and heterogeneous workflows, generating inaccurate and inconsistent supervisory data.	Standardized oversight workflows across institutions
	Transaction scalability	Growing volumes of cooperative transactions and reports, generated by more than 130,354 active cooperatives and approximately 25 million members nationwide [52], strain existing oversight processes and reconciliation capacity across administrative levels.	Scalable handling of large volumes of supervisory data
	Operational complexity	Oversight tasks involve complex, repetitive, and largely manual data collection, verification, and reporting activities, increasing the risk of error and inconsistency.	Reduction of operational complexity and repetitive manual reconciliation
Technology	ICT Infrastructure	Uneven ICT infrastructure and limited institutional capacity prevent many cooperatives from adopting and maintaining digital systems for oversight.	Support for supervisory operations under uneven connectivity and infrastructure conditions
	Document storage and sharing	Cooperatives are required to share data with oversight authorities, but non-standardized formats and exchange mechanisms lead to inconsistent documentation and limited verification.	Consistent document management with traceable versioning and change histories
	Data security and privacy	Oversight systems protect data confidentiality unevenly, complicating secure data sharing while maintaining accountability.	Controlled, role-based access that preserves data confidentiality while enabling supervisory review
	Data fragmentation	Cooperative and regional data are stored in separate centralized or federated databases, preventing a consistent supervisory view.	Shared supervisory reference across distributed data sources
	Data integrity	Distributed storage enables modification, selective updating, or misreporting of membership records, AMM documentation, and financial statements.	Non-erasable and traceable change histories for supervisory data
	Data transparency	Fragmented systems prevent authorities from obtaining a complete and verifiable overview of cooperative conditions.	Comprehensive and verifiable supervisory visibility
	Interoperability	Oversight institutions lack shared data models and integration mechanisms, resulting in inconsistent representations across regions	Interoperable data models and cross-institutional integration

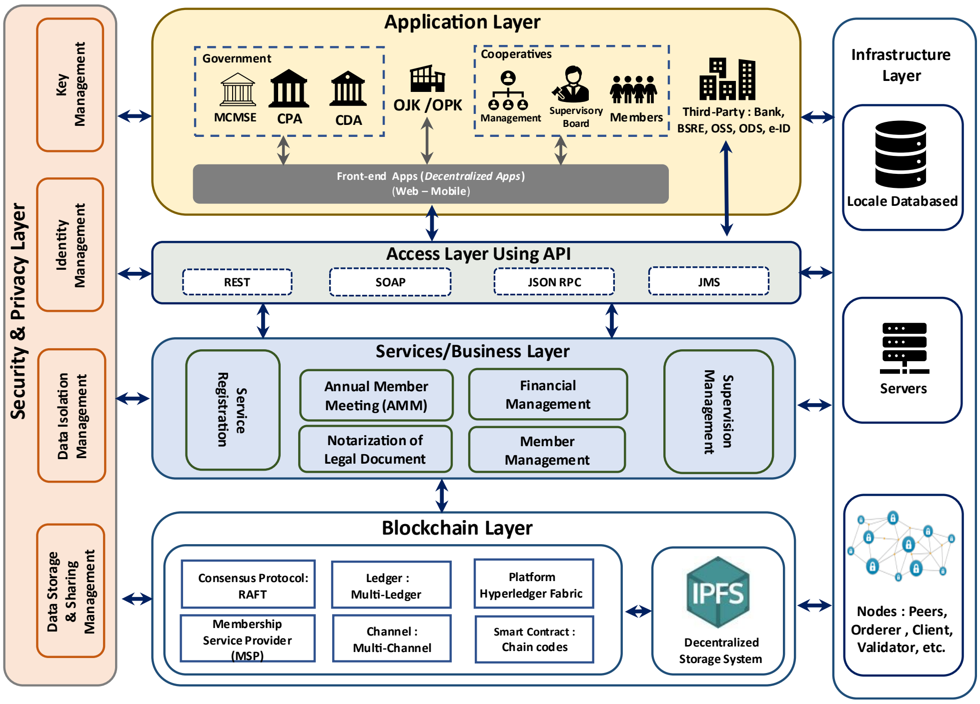

Figure 2. Proposed blockchain-based e-government framework

The proposed architecture adopts the RAFT consensus algorithm to efficiently replicate logs, maintain consistency, and achieve high performance in authenticated inter-agency environments [37][56] that handle large volumes of data. RAFT applies leader-based log replication and crash fault tolerance under trusted-participant assumptions, enabling stable coordination with lower coordination complexity than message-intensive consensus protocols such as PBFT, Kafka-based ordering services, and Paxos [37, 56, 57]. This trust model aligns with regulated cooperative oversight, in contrast to Proof-of-Work-based consensus, which targets permissionless environments and introduces probabilistic finality and high computational overhead [58].

Third, the blockchain layer specifies a multi-channel ledger structure [55] to isolate cooperative data while enabling authorized oversight access. Each channel corresponds to a defined stakeholder scope, including inter-agency coordination, government oversight levels, and cooperative entities, with independent ledgers accessible only to authorized participants. This structure preserves cooperative data ownership and internal governance processes, while supporting traceable and verifiable supervision consistent with ICA principles and ILO Recommendation No. 193.

Fourth, the architecture specifies the use of chaincode at the service and business logic layers to govern transaction validation and oversight rules. Chaincode defines structured data schemas, rule-based validation checks, and multi-level approval workflows aligned with existing oversight hierarchies, reducing the risk of erroneous or falsified records becoming immutable and addressing data accuracy concerns identified in the socio-technical analysis.

Finally, the architecture specifies off-chain document storage using IPFS [59] to support scalable document management under uneven ICT infrastructure conditions. The design anchors cryptographic hashes and metadata on the ledger, enabling integrity verification and auditability while avoiding ledger bloat and limiting exposure of sensitive cooperative data.

Service or Business Logic Layer

The service or business logic layer defines the procedural logic that governs validation, authorization, and preparation of cooperative data prior to ledger recording. This layer addresses process-level socio-technical constraints identified in the STS analysis, including dependence on manual verification, inconsistent reporting practices across administrative levels, and limited formalization of cross-level approval procedures.

The architecture incorporates pre-entry validation rules, role-based approval flows, and multi-level verification logic aligned with Indonesia's cooperative oversight hierarchy. Structured data schemas, rule-based validation logic, and supervisory checks operate within coordinated service workflows to improve data consistency and verification before records are written to immutable storage. This approach reduces variation in local practices and strengthens procedural consistency across institutions.

The service layer operates between application interfaces and the blockchain layer, integrating business rules with chaincode specifications within standardized workflows. This configuration enforces supervisory authority across cooperative, district, provincial, and national levels, supports traceable and verifiable oversight interactions, and preserves cooperative data ownership and internal governance processes in accordance with ICA principles and ILO Recommendation No. 193.

Figure 3 illustrates how the proposed service logic interacts with the underlying blockchain infrastructure through a multi-channel architecture. The figure depicts the separation of oversight scopes across channels and the controlled interaction between service workflows, access control mechanisms, and shared ledgers. This architectural arrangement positions channel structures as governance boundaries that support role-based supervision, data confidentiality, and cross-level coordination, rather than as purely technical ledger partitions.

The proposed service logic layer organizes six business modules that collectively support cooperative oversight functions.

(1) *Service Registration*

The Service Registration service defines a proposed architectural mechanism designed to facilitate the enrolment of organizations and users into the cooperative oversight network and to structure accountable participation within a permissioned governance environment. The proposed design is intended to accommodate participation from key institutions, including the Ministry of Cooperatives and SMEs, provincial and district supervisory authorities, financial regulators (OJK/OPK), and cooperatives, which submit registration requests through a designated government institution acting as the root of trust.

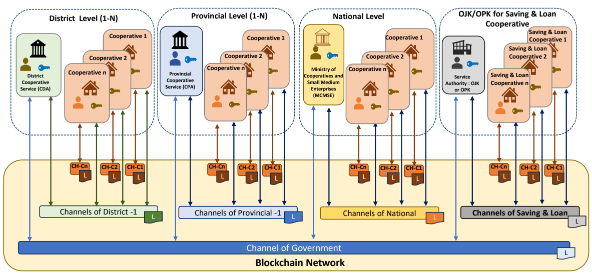

Figure 3. Multi-Channel Architecture of the Proposed E-Government Framework

Within the proposed architecture, CA issues X.509 certificates following organizational verification. At the same time, the MSP activates digital identities, assigns roles according to administrative level, and determines access privileges to relevant blockchain channels. The architecture records essential entity metadata through chaincode-defined transactions to support traceability and auditability, thereby establishing a controlled entry point that strengthens identity governance, access control, and accountability across heterogeneous institutions.

(2) *Service of Member Management*

The Member Management service governs cooperative membership data while preserving member-oriented governance principles, as shown in Figure 4. The architecture specifies an electronic Cooperative Digital Identity (e-CID) as a unified national identity to reduce redundancy and inconsistency in member records across cooperatives. Validation processes reference authoritative population administration data from DISDUKCAPIL to verify population registration numbers, addresses, and demographic attributes. Through this mechanism, individuals may participate in multiple cooperatives while maintaining a single verified identity. The architecture further defines an electronic Cooperative Member ID (e-CMID) for each cooperative membership, which generates credentials for accessing cooperative decentralized applications. This design supports data consistency, traceability, and accountability across cooperative entities without centralizing control over membership data.

(1) *Service of Annual Member Meeting (AMM)*

The AMM service structures both online and offline Annual Member Meeting processes within a verifiable governance framework, as illustrated in Figure 5.

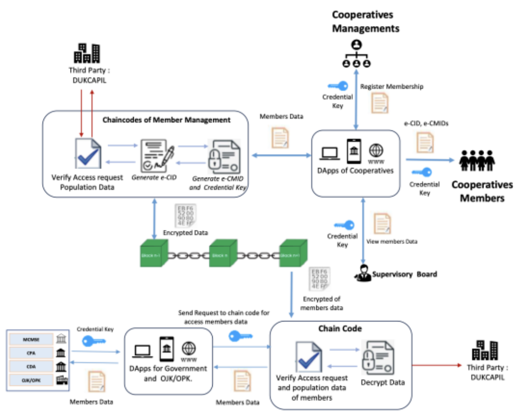

Figure 4. Business logic of the oversight mechanism for cooperative members

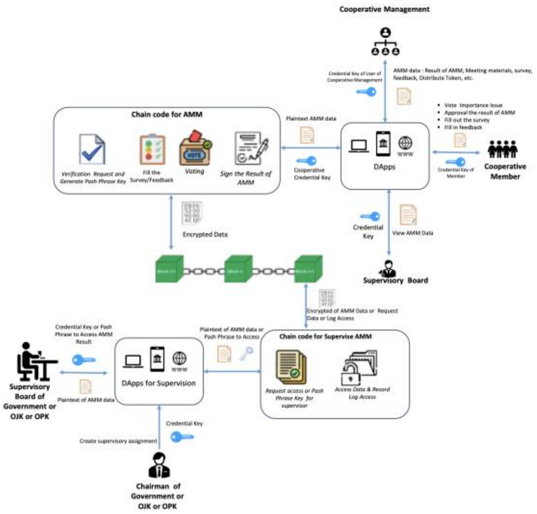

Figure 5. The proposed AMM oversight mechanisms

The proposed architecture incorporates three functional components: a token-based voting mechanism that operationalizes the one-member–one-vote principle [60]. Chaincode-based validation and digital endorsement that constrain post-meeting alteration or selective disclosure while maintaining controlled access for authorized stakeholders; and digital feedback and survey mechanisms whose outcomes form traceable, non-erasable records. Collectively, these components support democratic member control, transparency, accountability, and data integrity in cooperative decision-making and reduce reliance on manual AMM procedures.

(2) *Service of financial management*

The financial management service structures the recording and supervision of cooperative financial activities, including income, expenses, investments, capital, and assets, as illustrated in Figure 6. The proposed architecture defines standardized financial data structures and validation rules that reduce reporting inconsistency and limit opportunities for misstatement or selective disclosure.

The design supports controlled interaction with external systems, such as banking and taxation authorities, to enhance transparency and regulatory compliance while preserving cooperative autonomy. Predefined access and approval rules govern the visibility and verification of financial records across supervisory levels, ensuring that authorized actors, including OJK or OPK, internal auditors, and cooperative members, can verify records consistently while maintaining traceability and accountability in financial oversight.

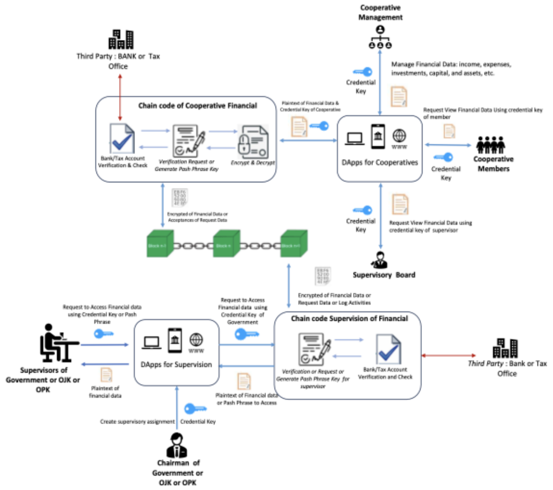

Figure 6. The proposed mechanisms for financial oversight

(3) *Legal Document Notarization and Sharing.*

The legal document notarization and sharing service structures the management of cooperative governance documents, including deeds, eligibility certificates, legal records, member agreements, and regulatory amendments. The architecture specifies blockchain-based notarization using digital seals or signatures to establish authenticity, prevent unauthorized modification, and reduce risks of falsification. Standardized registration and traceable version histories support transparent verification by authorized stakeholders while preserving data confidentiality.

This service reduces administrative fragmentation and supports consistent legal oversight compliance, as illustrated in Figure 7.

(4) *Service of Oversight Management*

The oversight management service defines how government authorities exercise supervisory functions over cooperatives in a structured and accountable manner. The architecture specifies controlled supervisory access to governance data, financial records, cooperative capital, and identified risk indicators, in accordance with Ministerial Regulation No. 9 of 2020 on Cooperative Oversight.

Access scopes and oversight permissions follow predefined authorization rules aligned with administrative hierarchies, ensuring that supervisory actions remain traceable, auditable, and proportionate. This design addresses socio-technical issues related to fragmented authority, inconsistent enforcement, and data manipulation by enabling consistent cross-level oversight while preserving cooperative data ownership and internal governance autonomy.

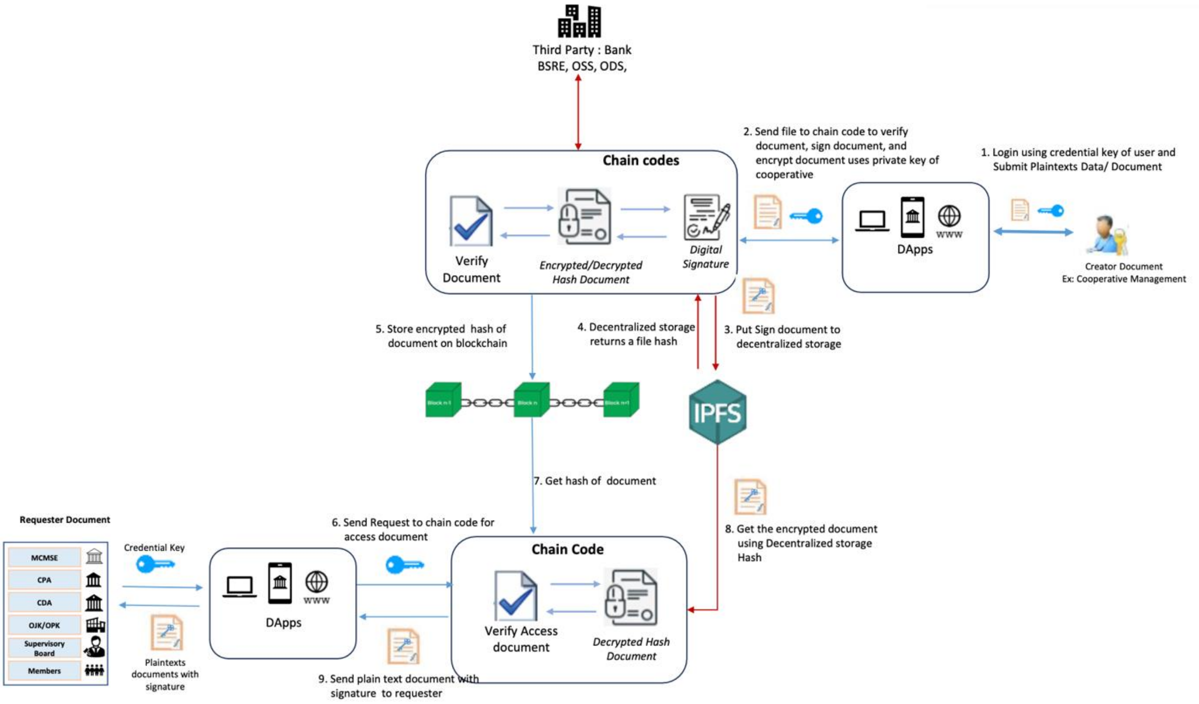

Figure 7. Decentralized legal document notarization and sharing mechanism

Access Layers

The access layer is designed to define standardized interfaces that connect the service logic layer with applications used by cooperatives, oversight authorities, and authorized third-party institutions. The architecture specifies protocol-based Application Programming Interfaces (APIs) to enable controlled and consistent data exchange across heterogeneous e-government environments, addressing fragmentation and cross-agency data inconsistency.

The design supports REST, SOAP, JSON-RPC, and message-oriented interfaces, enabling government dashboards, cooperative platforms, and third-party systems, such as banking and taxation services, to access blockchain services in a uniform and traceable manner. This architectural approach supports coordinated supervision while preserving cooperative autonomy and accountability.

Application Layer

The application layer defines the architectural space for developing user-facing applications that interact with blockchain services through the standardized API infrastructure provided by the access layer. This layer specifies how authorized users access, manage, and monitor cooperative data and oversight services in accordance with assigned roles, access rights, and supervisory responsibilities defined at the architectural level.

The architecture supports the development of web, mobile, and desktop applications tailored to the operational, governance, and supervisory needs of different stakeholders. Government oversight authorities, cooperatives, and approved third-party service providers may develop and deploy applications within this layer, subject to predefined authorization and access control policies. This design enables functional flexibility and innovation while preserving consistency with standardized workflows, data governance rules, and institutional accountability mechanisms.

Security Layer

The security layer defines how the proposed architecture protects data confidentiality, integrity, and access control within a permissioned blockchain network. The design specifies data visibility boundaries that regulate which records are shared across nodes and which remain restricted within designated channels. This layer design comprises four core security functions: data isolation, key management, secure data storage and sharing, and identity management.

The architecture specifies a hybrid encryption design that combines symmetric encryption for secure data processing and asymmetric encryption for key exchange, with AES-256 and RSA algorithms [61].

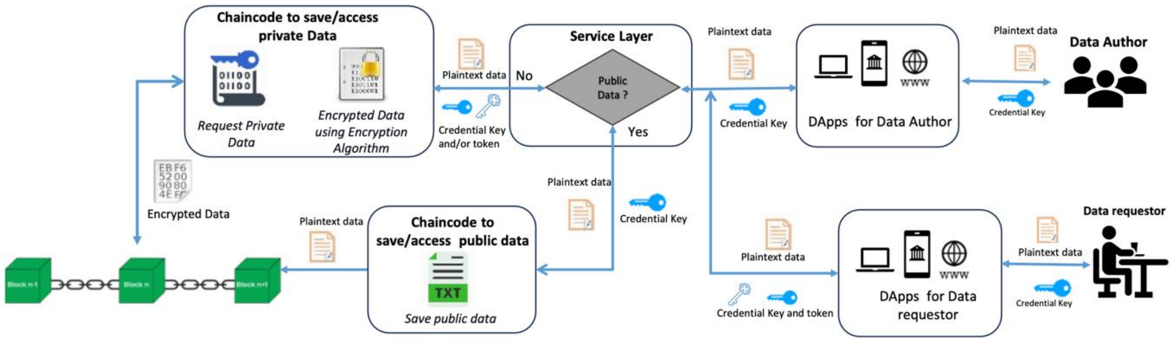

Figure 8. The data isolation technique assures data integrity before it is stored on a block

As illustrated in Figure 8, the design defines a secure workflow in which documents are encrypted, hashed, stored in distributed repositories, and accessed only through key-based verification.

Key management governs the lifecycle of cryptographic credentials, while identity management establishes certificate-based trust through MSP and CA. Together, these design choices mitigate the risks of unauthorized access and data manipulation while preserving cooperative autonomy and supervisory accountability.

Infrastructure Layer

The infrastructure layer defines the proposed technical foundation of the blockchain-based cooperative oversight architecture under uneven ICT conditions in Indonesia. The design addresses socio-technical constraints identified in the STS analysis, including regional disparities in infrastructure capacity, intermittent connectivity, and the need to support scalable supervision across heterogeneous cooperative environments.

The proposed architecture adopts a distributed deployment model that combines servers, peer nodes, and local data storage across administrative levels. Government institutions, supervisory authorities, and cooperatives host peer nodes according to institutional roles, while provincial-level nodes provide shared infrastructure support for smaller cooperatives operating under limited bandwidth conditions. Channel allocation and access privileges follow chaincode-defined rules, which preserve cooperative data autonomy while enabling authorized supervisory access, thereby balancing decentralized participation with coordinated oversight.

ANALYSIS AND DISCUSSION

Analysis

This section evaluates whether the proposed framework architecture adequately addresses the socio-technical challenges identified in Indonesia's cooperative oversight system. The analysis applies three sequential validation stages, namely socio-technical alignment validation, technical adequacy validation, and comparative institutional validation. These validation stages examine the coherence, suitability, and institutional fit of the architectural design with respect to governance requirements, data quality concerns, and inter-agency coordination constraints.

Socio-Technical Alignment Validation

This validation stage examines the alignment between the proposed framework architecture and the socio-technical challenges identified through the STS assessment. The proposed architecture design distributes responsibilities across blockchain, service, access, security, infrastructure, and application layers.

This distribution enables coordination across administrative levels, accommodates heterogeneous institutional readiness, and supports standardized oversight workflows without enforcing centralized operational control. Table 2 summarizes the correspondence between identified socio-technical challenges and the architectural mechanisms that address them.

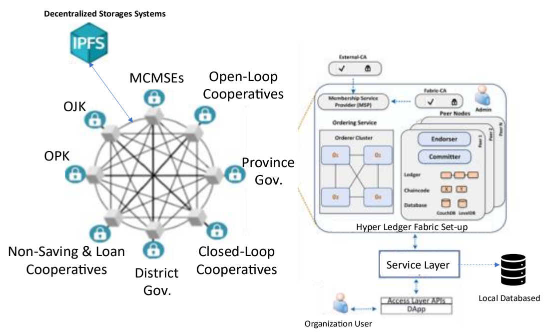

Figure 9. Proposed e-government infrastructure design using Hyperledger Fabric

Table 2. Mapping Socio-Technical Challenges to Architectural Features

STS Aspect	Socio-Technical Issue	Architecture Layer(s)	Architectural Framework Design Features
People	Resource inequality	Infrastructure Layer	Distributed peer nodes at cooperative, provincial, and national levels combined with off-chain document storage and asynchronous on-chain submission enable supervisory participation despite uneven ICT capacity and intermittent connectivity.
	Coordination problems	Blockchain, Service, Access Layers	A permissioned multi-channel ledger provides a shared supervisory reference, while MSP–CA–based role assignment and standardized APIs synchronize oversight actions across administrative levels.
	Limited expertise	Service Layer	Chaincode-defined workflows and rule-based pre-ledger validation embed procedural knowledge into services, reducing dependence on local technical expertise during reporting and verification.
Structure	Regulatory implementation	Blockchain, Security Layers	Regulatory data schemas and validation rules encoded in chaincode enforce uniform interpretation of cooperative regulations before records become immutable.
	Organizational readiness	Infrastructure, Service Layers	Modular Hyperledger Fabric deployment with layered service abstraction supports gradual institutional integration without disrupting national supervisory consistency
	Acceptability	Blockchain Layer	Permissioned consortium governance and channel separation preserve cooperative data ownership while enabling traceable and authorized supervisory access.
Task	Process standardization	Service Layer	Dedicated service modules for registration, AMM, financial reporting, legal documentation, and oversight management enforce standardized supervisory workflows across institutions.
	Transaction scalability	Blockchain, Infrastructure Layers	RAFT consensus combined with multi-channel ledger organization ensures deterministic ordering and scalable supervisory transactions without overloading resource-constrained nodes.
	Operational complexity	Service Layer	Automated validation, approval workflows, and audit-trail generation through chaincode reduce repetitive manual reconciliation and procedural errors.
Technology	Uneven ICT infrastructure	Infrastructure Layer	Hybrid deployment with provincial peer nodes and off-chain storage sustains supervisory operations under heterogeneous connectivity conditions.
	Document storage and sharing	Blockchain, Security Layers	IPFS-based off-chain document storage with cryptographic hash anchoring on the ledger enables traceable versioning and integrity verification without ledger bloat.
	Data security and privacy	Security Layer	MSP–CA–based identities, X.509 certificates, and AES-256/RSA encryption enforce role-bound access and confidentiality across cooperative and supervisory domains.
	Data fragmentation	Blockchain, Access Layers	Shared supervisory reference specified through channel-based ledgers, standardized data models, controlled integration interfaces, and encrypted external document storage
	Data integrity	Blockchain Layer	Non-erasable and traceable change histories defined through immutable ledger records, cryptographic hash anchoring of off-chain documents, identity-bound transactions (e-CID/e-CMID), and deterministic transaction finality.
	Data transparency	Blockchain, Access Layers	Verifiable supervisory visibility specified through multi-channel ledger organization, role-based access control, chaincode-defined validation rules, and immutable audit records.
	Smart contracts	Blockchain Layer	Chaincode enforces compliance rules and multi-level approval logic prior to ledger commitment, reducing discretionary manipulation.
	Interoperability	Access Layer	Protocol-based REST, SOAP, and JSON-RPC APIs enable consistent cross-institutional data exchange across heterogeneous e-government systems.

Collectively, the mappings in Table 2 demonstrate that the proposed framework architecture translates socio-technical challenges into concrete architectural features. The layered allocation of governance, validation, and coordination functions addresses structural fragmentation, heterogeneous institutional capacity, and data governance constraints without imposing centralized operational control. Coordination, traceability, and supervisory visibility emerge from the architectural configuration as an integrated system, while responsibility for data correctness remains embedded in pre-ledger institutional processes.

Technical Adequacy Validation

This validation stage evaluates the technical adequacy of the proposed framework architecture. It examines whether its core architectural components provide reliable, scalable, and accountable support for cooperative oversight under regulated, multi-agency conditions. The analysis focuses on core blockchain mechanisms and complementary architectural components that directly affect auditability, consistency, access control, and data protection. Validation draws on empirical and analytical evidence from prior studies to assess how these features perform in permissioned governance environments and to clarify their technical boundaries and trade-offs. This evaluation positions blockchain as an infrastructural component embedded within institutional oversight processes and coordinated data governance arrangements. Table 3 summarizes the technical validation of these core architectural components.

Overall, the technical validation indicates that the proposed framework architecture employs established architectural components whose operational properties have been examined in prior studies and shown to support auditability, consistency, and controlled access in permissioned governance environments. The combination of deterministic consensus, channel-based ledger organization, certificate-bound identities, smart contract validation, cryptographic protection, and hybrid data storage defines clear technical boundaries for supervisory operations. These features provide a stable foundation for accountable cooperative oversight while remaining dependent on institutional governance for identity assurance, key management, and exception handling. The validation thus confirms that the architecture's technical design is sufficient for its intended governance role and provides a basis for comparative positioning against alternative oversight architectures in the subsequent validation stage.

Table 3. Technical validation of architectural components

Component	Functional Adequacy
RAFT Consensus	RAFT implements leader-based log replication with crash fault tolerance [56], providing deterministic transaction ordering and immediate finality under authenticated participation. Empirical evaluations report commits latencies in the order of hundreds of milliseconds in permissioned deployments [37], supporting predictable audit trails required for supervisory systems. These features help mitigate the effects of uneven ICT infrastructure by tolerating node downtime and reducing coordination delays across supervisory units operating under variable network reliability.
Multi-Channel Ledger Structure	Channel-based ledger isolation separates state and transaction histories across oversight scopes, enabling parallel transaction processing and reducing cross-domain interference [55], Prior studies show that channelization improves scalability and administrative separation, while introducing governance overhead associated with channel lifecycle management. In cooperative oversight, channel-based isolation limits data exposure across supervisory domains, supporting confidentiality requirements of cooperatives, while requiring coordinated governance of channel membership and lifecycle across institutions with differing administrative capacity
Identity Management (MSP–CA, e-CID/e-CMID)	Certificate-based identities bind transactions to verifiable organizational and individual roles, strengthening authentication, authorization, and non-repudiation [62]. This mechanism supports role-based access control across cooperative and supervisory domains, while identity assurance depends on certificate issuance, revocation, and lifecycle governance.
Smart Contracts (Chaincode)	Chaincode executes deterministic validation and approval logic that enforces predefined data schemas and regulatory rules prior to ledger commitment [20]. This mechanism constrains discretionary modification of supervisory data and standardizes oversight procedures, while exceptional cases remain subject to institutional resolution.
Hybrid data storage IPFS with Hash Anchoring	Hybrid data storage employs IPFS for off-chain content-addressed storage, with cryptographic hash anchoring used to record corresponding on-chain references for integrity verification and auditability, as reported in prior studies [63]. Cryptographic hash preserves integrity verification and auditability on-chain, while data availability and confidentiality depend on external storage configuration and access control. In cooperative oversight, this design accommodates large volumes of finance, AMM, and legal records across regions with uneven ICT capacity, where direct on-chain storage would be impractical.
Cryptographic Protection	Symmetric encryption (AES-256) protects data confidentiality [38], while asymmetric encryption (RSA) supports secure key exchange and identity binding [61]. Cryptographic hashing links on-chain references to off-chain records, and role-bound authentication tokens enforce authorized access, which is relevant for protecting sensitive cooperative financial, membership, and governance data across multiple supervisory authorities, with effectiveness dependent on secure key and token lifecycle management.
Layered Architectural Separation	Layered separation enhances modularity, maintainability, and fault isolation, consistent with ISO 23257:2022 principles and validated across distributed government systems [41]. In cooperative oversight, this structure mitigates fragmented institutional coordination and uneven digital readiness by isolating governance logic from application and infrastructure changes, enabling incremental integration across administrative levels.

Comparative Institutional Validation

This section assesses the institutional plausibility of the proposed framework architecture through comparative and counterfactual analysis. The evaluation examines whether the architectural features align with governance patterns observed in established public-sector institutions blockchain initiatives and whether the proposed design addresses socio-technical challenges inherent in multi-level cooperative oversight. International implementations serve as reference cases to assess architectural feasibility and governance alignment rather than as models for replication. Table 4 presents the comparative validation results.

As summarized in Table 4, the proposed architecture aligns with governance-oriented features widely adopted in public-sector blockchain systems, including permissioned participation, role-bound identity management, standardized supervisory workflows, and cryptographically verifiable records. Prior studies on Estonia's e-government infrastructure emphasize certificate-based digital identity, controlled access, and tamper-evident records as foundational mechanisms for accountable public administration [64][65]. Similar governance patterns appear in the United Arab Emirates, where permissioned blockchain platforms support standardized workflows and controlled inter-agency data sharing in public services [32]. China's Blockchain Service Network further demonstrates the feasibility of multi-tier node deployment for nationwide supervision across heterogeneous ICT environments [33]. These documented practices correspond with the proposed use of MSP–CA–based identity governance, chaincode-enforced validation logic, multi-channel ledger separation, and provincially distributed peer nodes within the framework.

This comparative alignment becomes clearer when contrasted with non-blockchain alternatives.

Table 4. Comparative Validation with International Implementations

Oversight Problem	Estonia [64][65]	UAE [32]	China [33]	Malaysia [34]	Vietnam [35]	Proposed Architecture
Fragmented identity and weak accountability	National digital ID and PKI bind public transactions to legal identity	Permissioned blockchain with role-based identity	State-managed identity within BSN	Government-controlled permissioned identity	Blockchain-supported identity for document authentication	MSP–CA–based identity governance; e-CID for unique member identity; e-CMID for cooperative-membership traceability
Inconsistent membership and participation records	Centralized population registries reused across services	Unified identity across government platforms	Integrated identity under national systems	Registry-based membership records	Digital identity for authenticated records	e-CID as unified member identity; e-CMID to link individuals to multiple cooperatives without centralizing control
Inconsistent reporting and manual workflows	Standardized e-services and once-only principle	Automated government service workflows	Unified blockchain infrastructure	Blockchain-supported reporting workflows	Structured digital verification	Chaincode-enforced validation rules; standardized service workflows for AMM, finance, legal, and oversight
Limited cross-agency coordination	X-Road enables secure data exchange	Cross-agency permissioned blockchain	BSN connects multi-level nodes	National blockchain platforms	Blockchain-enabled inter-organizational verification	Multi-channel ledger supporting shared supervisory reference across oversight levels
Data integrity and risk of record manipulation	KSI Blockchain ensures immutable logs	Immutable public-service records	Blockchain transaction verification	Blockchain notarization	Hash-based document authentication	Immutable ledger records; cryptographic hash anchoring of off-chain documents
Confidentiality concerns and institutional autonomy	Citizen-controlled data access transparency	Controlled access in permissioned networks	Permissioned state governance	Permissioned government blockchain	Restricted access blockchain systems	Channel-based data isolation; role-based access control preserving cooperative autonomy
Uneven ICT infrastructure capacity	Secure centralized infrastructure	Central government platforms	Provincially distributed BSN nodes	National shared infrastructure	Lightweight blockchain deployments	Distributed peer nodes; provincial nodes; hybrid on-chain/off-chain storage

Centralized oversight databases consolidate authority and simplify system administration but concentrate trust within a single institution, thereby limiting transparency and weakening cross-level accountability in multi-tier governance settings [34][41]. Federated database architectures preserve organizational autonomy but rely on bilateral coordination and administrative enforcement to maintain data consistency, making them susceptible to fragmented validation rules, delayed reconciliation, and selective data modification across jurisdictions [20][57]. In contrast, permissioned blockchain architectures establish a shared supervisory state with protocol-enforced immutability, deterministic consistency, and identity-bound non-repudiation once records are validated and committed, as documented in prior government blockchain evaluations [9][37]. These properties constrain post-verification alteration without displacing institutional oversight roles, addressing coordination and accountability limitations identified in cooperative supervision.

The comparison also highlights cooperative-specific architectural extensions introduced by the proposed framework. The e-CID and e-CMID mechanisms adapt digital identity practices observed in national e-government systems to cooperative governance by enabling consistent membership traceability across multiple cooperatives without centralizing control, consistent with principles of autonomy and democratic governance [2][3]. Multi-channel ledger organization and role-based access control directly address data confidentiality concerns frequently reported in cooperative oversight contexts. At the same time, hybrid on-chain and off-chain data management reflects scalable approaches to document handling reported in blockchain-based registries and document authentication systems in Malaysia and Vietnam [34][35]. Collectively, the comparative and counterfactual analysis indicates that the proposed architecture integrates established public-sector blockchain practices with design responses tailored to Indonesia's cooperative oversight challenges, supporting its institutional plausibility beyond purely technical considerations.

Discussion

The findings indicate that the limitations of Indonesia’s cooperative oversight system are primarily institutional and socio-technical rather than purely technological. Fragmented authority, heterogeneous reporting practices, and limited interagency coordination weaken the effectiveness of supervision even in the presence of existing digital systems. Within this context, the proposed framework illustrates how blockchain can serve as a governance-enabling infrastructure that strengthens accountability and interoperability when embedded within appropriate institutional arrangements. The discussion therefore focuses on the theoretical, practical, and policy implications of these findings, as well as the conditions required for effective adoption.

Theoretical Contribution

This study contributes to the literature on blockchain-enabled e-government by demonstrating how the STS perspective can be operationalized as an architectural design logic rather than applied solely as an analytical lens. By integrating people, structure, task, and technology into a coherent framework, the findings confirm that blockchain adoption in public governance depends on institutional alignment, regulatory clarity, and organizational capacity, not on technological sophistication alone.

Importantly, the discussion clarifies that core governance challenges, such as data accuracy and consistency, are not intrinsic properties of distributed ledgers. Blockchain immutability preserves verified records, but the correctness and coherence of those records emerge from socio-technical governance mechanisms that operate before and around ledger commitment. This interpretation addresses a critical gap in prior e-government studies that emphasize transparency and security while overlooking data quality as an architectural concern. The findings therefore reinforce the view that effective digital governance innovation arises from harmonizing technological affordances with institutional norms, procedural discipline, and accountability structures, particularly in developing-country contexts and cooperative governance settings, where unified oversight models remain limited.

Practical Contribution

From a practical perspective, the discussion highlights how the proposed architecture translates socio-technical requirements into implementable governance mechanisms suited to Indonesia's multi-level oversight environment. Role-based validation, standardized reporting workflows, multi-channel ledger organization, and hybrid on-chain and off-chain integration collectively support more reliable verification of cooperative data while reducing reliance on manual reconciliation. The framework embeds pre-entry validation, structured approval processes, and traceable accountability, thereby mitigating the risk that inaccurate or manipulated data become permanently recorded.

The findings also indicate that successful implementation depends critically on organizational readiness and technical capacity. Uneven preparedness across government levels and limited digital expertise among cooperative actors remain significant constraints. Accordingly, blockchain adoption should be approached as an institutional transformation process rather than a standalone information technology project. Capacity building aligned with stakeholder roles is essential to ensure the system's meaningful use and to prevent governance asymmetries from being reproduced in digital form. International experiences demonstrate that structured training and certification programs, supported by collaboration with universities, research institutions, and industry partners, can strengthen institutional competence and trust, thereby enhancing long-term sustainability.

Infrastructure readiness further conditions feasibility. Although national indicators show progress in e-government development, regional disparities continue to limit the applicability of advanced digital architectures, particularly in rural cooperatives. The discussion therefore underscores the need for incremental deployment supported by digital readiness assessments, targeted infrastructure investment, and controlled pilot implementation. Regulatory sandboxes and proof-of-concept initiatives enable learning and adaptation while managing operational and legal uncertainty across heterogeneous regions.

Policy Contribution

This study emphasizes that effective blockchain adoption in public administration requires clear and coherent regulatory frameworks [66]. Regulations governing data ownership, access rights, interoperability standards, and the legal recognition of automated verification mechanisms directly shape institutional participation, accountability, and trust [67]. Ambiguous or fragmented regulatory arrangements risk reproducing existing governance silos rather than resolving them, even when advanced digital technologies are introduced.

The proposed framework highlights the importance of policies that standardize data structures, clarify institutional responsibilities for data governance, and formally recognize digitally enforced verification and audit mechanisms. Such policy alignment enables blockchain-based systems to support coordinated supervision while maintaining legal certainty, institutional accountability, and data protection across administrative levels.

The framework also informs policymakers by articulating governance structures, validation models, and coordination mechanisms required for responsible blockchain-enabled public-sector innovation. Explicit alignment with the ICA principles and ILO Recommendation No. 193 positions the proposed architecture within internationally recognized cooperative governance norms, demonstrating how blockchain-based e-government can reinforce transparency, accountability, democratic member control, and institutional autonomy rather than undermine them.

CONCLUSION

This study designs a framework architecture for a blockchain-based cooperative oversight system in Indonesia using a socio-technical approach. The design integrates institutional arrangements, governance processes, and technical components into a coherent architectural model grounded in STS analysis and aligned with ISO 23257:2022. The results demonstrate that effective cooperative oversight does not depend on blockchain technology alone, but on the alignment between governance structures, standardized workflows, and institutional coordination across national, provincial, and district levels.

The proposed permissioned blockchain architecture, supported by multi-channel ledger separation, smart contract- or chaincode-based workflow enforcement, and hybrid document management, structurally addresses long-standing oversight challenges, including fragmented reporting, weak inter-agency coordination, limited transparency, and uneven ICT capacity. Within this framework, blockchain functions as an integrity-preserving and coordination-enabling layer. At the same time, data accuracy and consistency emerge from socio-technical governance mechanisms such as pre-entry validation, institutional approval, and standardized reporting processes rather than from ledger immutability alone.

Successful adoption of the proposed architecture depends on a phased, policy-driven strategy that balances cooperative autonomy with supervisory accountability and is supported by regulatory harmonization and institutional capacity building. Future work should validate the framework through pilot deployments in digitally ready regions and empirical evaluations of governance effectiveness, interoperability, and system performance, including comparisons with database-based oversight solutions, to refine and strengthen the proposed architectural design.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all stakeholders who supported the data acquisition process, particularly Bank Indonesia for providing the Research Grant Bank Indonesia (RGBI) 2023 under Contract No. 25/12/PKS/BINS/2023. Appreciation is also extended to the Faculty of Engineering, Universitas Indonesia; the Faculty of Administrative Science, Universitas Indonesia; and the Faculty of Telematics Energy, Institut Teknologi PLN, for their valuable institutional support. The authors are also deeply thankful to all informants who contributed to and supported this research project.

REFERENCES

[1] F. O. Wanyama, “Cooperatives and the Sustainable Development Goals Resilience in a downturn : The power of financial cooperatives,” *International Labour Organization*, 2015.
[2] ICA, "Guidance Notes to the Cooperative Principles," *International Cooperative Alliance*, 2013.
[3] ILO, "Promotion of Cooperatives Recommendation No. 193," *International Labor Organization*, pp. 1–10, 2002.
[4] D. Meira, A. M. Bandeira, and M. Santos, “Accountability and Transparency in Cooperatives: A Comparative Analysis between Portugal and Germany,” *REVESCO Rev. Estud. Coop.*, vol. 142, no. 142, pp. 1–20, 2022, doi: 10.5209/reve.83721.
[5] President of The Republic of Indonesia, “Law No. 25 about Cooperatives,” *Indonesia*, 1992.
[6] MCMSE, “Regulation No. 9 Year 2020,” *Indonesia*, 2020, pp. 1–53.
[7] President of The Republic of Indonesia, “LAW No. 4/2023,” *Indonesia*, 2023.
[8] E. Kusmiati, D. Masyita, E. Febrian, and M. F. Cahyandito, “A study on the determinants of successful performance of Indonesian cooperatives,” *International Journal of Social Economics*, vol. 50, no. 9, pp. 1285–1301, 2023, doi: 10.1108/IJSE-02-2022-0078.
[9] Tempo.co, “Eight Troubled Cooperatives Default on IDR 26 Trillion, Says Ministry of Cooperatives and SMEs: Only IDR 3.4 Trillion Has Been Paid,” *Tempo,* Accessed: Jan. 22, 2026. [Online]. Available: https://www.tempo.co/ekonomi/8-koperasi-bermasalah-gagal-bayar-rp26-triliun-kemenkop-ukm-baru-dibayar-rp-3-4-triliun-34173
[10] P. Mishra and R. Ganesan, “Securing E-governance: a blockchain-based framework for tamper-proof PDF document exchange,” *Front. Blockchain*, vol. 8, pp. 1–20, December 2025, doi: 10.3389/fbloc.2025.1699773.
[11] T. Freeman, F. Baum, S. Javanparast, A. Ziersch, T. Mackean, and A. Windle, “Challenges facing primary health care in federated government systems: Implementation of Primary Health Networks in Australian states and territories,” *Health Policy (New. York).*, vol. 125, no. 4, pp. 495–503, Apr. 2021, doi: 10.1016/j.healthpol.2021.02.002.
[12] M. Defriani and M. G. Resmi, "E-Government Architectural Planning Using Federal Enterprise Architecture Framework in Purwakarta District Government," *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, 2019, doi: 10.1109/ICIC47613.2019.8985819.
[13] G. Mustafa, W. Rafiq, N. Jhamat, Z. Arshad, and F. A. Rana, “Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations,” *Int. J. Law Manag.*, 2024, doi: 10.1108/IJLMA-08-2023-0172.
[14] M. Atzori, “Blockchain technology and decentralized governance: Is the state still necessary?,” *J. Gov. Regul.*, vol. 6, no. 1, pp. 45–62, 2017, doi: 10.22495/jgr_v6_i1_p5.
[15] K. Gai, J. Guo, L. Zhu, and S. Yu, “Blockchain Meets Cloud Computing: A Survey,” *IEEE* Commun. Surv. Tutorials, vol. 22, no. 3, pp. 2009–2030, 2020, doi: 10.1109/COMST.2020.2989392.
[16] D. Cagigas, J. Clifton, D. Diaz-fuentes, and M. Fernández-gutiérrez, “Blockchain for Public Services : A Systematic Literature Review,” vol. 9, 2021, doi: 10.1109/ACCESS.2021.3052019.
[17] C. S. Sung and J. Y. Park, “Understanding of blockchain-based identity management system adoption in the public sector,” *J. Enterp. Inf. Manag.*, vol. 34, no. 5, pp. 1481–1505, 2021, doi: 10.1108/JEIM-12-2020-0532.
[18] I. Racetin, J. Kilić Pamuković, M. Zrinjski, and M. Peko, “Blockchain-Based Land Management for Sustainable Development,” *Sustain.*, vol. 14, no. 17, 2022, doi: 10.3390/su141710649.
[19] K. M. Alam, J. M. Ashfiqur Rahman, A. Tasnim, and A. Akther, “A Blockchain-based

Land Title Management System for Bangladesh," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3096–3110, 2022, doi: 10.1016/j.jksuci.2020.10.011.

[20] Y. Gao, Q. Pan, Y. Liu, H. Lin, Y. Chen, and Q. Wen, "The Notarial Office in E-government : A Blockchain-Based Solution," *IEEE Access*, vol. 9, pp. 44411-44425, 2021, doi: 10.1109/ACCESS.2021.3066184.

[21] L. Jimenez-Castillo, J. Sarkis, S. Saberi, and T. Yao, "Blockchain-based governance implications for ecologically sustainable supply chain management," *J. Enterp. Inf. Manag.*, vol. 37, no. 1, pp. 76–99, 2024, doi: 10.1108/JEIM-02-2022-0055.

[22] R. Manzoor, B. S. Sahay, and S. K. Singh, "Examining the Factors That Facilitate or Hinder the Use of Blockchain Technology to Enhance the Resilience of Supply Chains," *IEEE Trans. Eng. Manag.*, vol. 71, pp. 10626–10649, 2024, doi: 10.1109/TEM.2024.3358722.

[23] B. Sriman and S. G. Kumar, "Decentralized finance (DeFi): The Future of Finance and Defi Application for Ethereum blockchain based Finance Market," *Proc. - IEEE Int. Conf. Adv. Comput. Commun. Appl. Informatics, ACCAI 2022*, pp. 1–9, 2022, doi: 10.1109/ACCAI53970.2022.9752657.

[24] L. Gudgeon, S. Werner, D. Perez, and W. J. Knottenbelt, "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency," *AFT 2020 - Proc. 2nd ACM Conf. Adv. Financ. Technol.*, pp. 92–112, 2020, doi: 10.1145/3419614.3423254.

[25] N. Elisa, L. Yang, F. Chao, N. Naik, and T. Boongoen, "A Secure and Privacy-Preserving E-Government Framework using Blockchain and Artificial Immunity," *IEEE Access*, vol. 11, no. November 2022, pp. 1–1, 2023, doi: 10.1109/access.2023.3239814.

[26] S. Sharaf and N. F. Shilbayeh, "A Secure G-Cloud-Based Framework for Government Healthcare Services," *IEEE Access*, vol. 7, pp. 37876–37882, 2019, doi: 10.1109/ACCESS.2019.2906131.

[27] A. H. Mayer, V. F. Rodrigues, C. A. Da Costa, R. Da Rosa Righi, A. Roehrs, and R. S. Antunes, "FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records," *IEEE Access*, vol. 9, pp. 122723–122737, 2021, doi: 10.1109/ACCESS.2021. 3109822.

[28] S. Tanwar, "Blockchain for 5G Healthcare Applications: Security and privacy solutions," *The Institution of Engineering and Technology,* 2021, doi: 10.1049/pbhe035e.

[29] M. Hegde and R. R. Rao, "DDMIA : Distributed Dynamic Mutual Identity Authentication for Referrals in Blockchain-Based Health Care Networks," *IEEE Access*, vol. 10, no. July, pp. 78557–78575, 2022, doi: 10.1109/ACCESS.2022.3193238.

[30] N. Fikri, M. Rida, N. Abghour, K. Moussaid, A. El Omri, and M. Myara, "A blockchain architecture for trusted sub-ledger operations and financial audit using decentralized microservices," *IEEE Access*, vol. 10, no. August, pp. 90873–90886, 2022, doi: 10.1109/ACCESS.2022.3201885.

[31] RIA, "Cybersecurity Competence Center Signs Cooperation Agreement with Estonian Government," https://www.ria.ee. Accessed: May 20, 2025. [Online]. Available: https://www.ria.ee/en/news/cybersecurity-competence-centre-signs-cooperation-agreement-estonian-government

[32] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services-Use cases, security benefits and challenges," in *2018 15th Learning and Technology Conference, L and T 2018*, IEEE, 2018, pp. 112–119. doi: 10.1109/LT.2018.8368494.

[33] N. Stockton, "China Takes Blockchain National," *IEEE Spectrum*, vol. 57, IEEE, pp. 11–12, 2020. doi: 10.1109/MSPEC.2020. 9055903.

[34] MOSTI, *National Blockchain Roadmap 2021-2025,* 2021.

[35] L. T. Nguyen, D. T. Nguyen, K. N. N. Ngoc, and D. T. V. Duc, "Blockchain adoption in logistics companies in Ho Chi Minh City, Vietnam," *Cogent Bus. Manag.*, vol. 10, no. 2, 2023, doi: 10.1080/23311975.2023.2216436.

[36] S. Saxena, D. Shao, A. Nikiforova, and R. Thapliyal, "Invoking blockchain technology in e-government services: a cybernetic perspective," *Digit. Policy, Regul. Gov.*, vol. 24, no. 3, pp. 246–258, 2022, doi: 10.1108/DPRG-10-2021-0128.

[37] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proc. 13th EuroSys Conf. EuroSys 2018*, vol. 2018–January, 2018, doi: 10.1145/3190508. 3190538.

[38] J. Zhou, Y. Feng, Z. Wang, and D. Guo, "Using secure multi-party computation to protect privacy on a permissioned blockchain," *Sensors*, vol. 21, no. 4, pp. 1–17, 2021, doi: 10.3390/s21041540.

[39] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Gov. Inf. Q.*, vol. 34,

no. 3, pp. 355–364, 2017, doi: 10.1016/j.giq.2017.09.007.

[40] V. Venkatesh, J. Y. L. Thong, F. K. Y. Chan, and P. J. H. Hu, “Managing citizens’ uncertainty in e-government services: The mediating and moderating roles of transparency and trust,” *Inf. Syst. Res.*, vol. 27, no. 1, pp. 87–111, 2016, doi: 10.1287/isre.2015.0612.

[41] ISO, “ISO 23257:2022 (E) Blockchain and distributed ledger technologies — Reference architecture,” International Organization for Standardization. Accessed: Oct. 31, 2023. [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso:23257:ed-1:v1:en

[42] Y. Yang, Y. Shi, and T. Wang, “Blockchain Technology Application Maturity Assessment Model for Digital Government Public Service Projects,” *International Journal of Crowd Science*, vol. 6, no. 4, pp. 184-194, November 2022, doi: 10.26599/IJCS.2022.9100025..

[43] R. K. Yin, *Case Study Research and Applications: Design and Methods, 6th Edition*, Third Edit. London: SAGE Publications, Inc, 2017.

[44] A. Chaudhuri, M. S. Bhatia, N. Subramanian, Y. Kayikci, and M. Dora, “Socio-technical capabilities for blockchain implementation by service providers: multiple case study of projects with transaction time reduction and quality improvement objectives,” *Prod. Plan. Control*, vol. 0, no. 0, pp. 1–14, 2022, doi: 10.1080/09537287.2022.2128865.

[45] R. P. Bostrom and J. S. Heinen, “STS Perspective MIS Problems and Failures : A Socio- Technical Perspective PART I : THE CAUSES By : Robert P . Bostrom,” *MIS Q.*, vol. 1, no. 3, pp. 17–32, 1977.

[46] G. Baxter and I. Sommerville, “Socio-technical systems: From design methods to systems engineering,” *Interact. Comput.*, vol. 23, no. 1, pp. 4–17, 2011, doi: 10.1016/j.intcom.2010.07.003.

[47] D. Shin and M. Ibahrine, “The socio-technical assemblages of blockchain system: how blockchains are framed and how the framing reflects societal contexts,” *Digit. Policy, Regul. Gov.*, vol. 22, no. 3, pp. 245–263, 2020, doi: 10.1108/DPRG-11-2019-0095.

[48] MCMSE, “*Regulation Number 19/Per/M.KUKM/IX/2015*,” *Indonesia*, 2015.

[49] President of the Republic of Indonesia, “Government Regulation Number 95 of 2018 concerning the Electronic-Based Government System,” *Indonesia*, 2018, p. 110.

[50] A. H. Firdaus and I. Gusti Bagus Baskara Nugraha, "Saving and Loan Transaction System in Cooperative Using Blockchain," *2019 International Conference on ICT for Smart Society (ICISS)*, Bandung, Indonesia, 2019, pp. 1-4, doi: 10.1109/ICISS48059.2019.8969847.

[51] President of The Republic of Indonesia, “Government Regulation Number 7 of 2021,” *Indonesia*, 2021.

[52] N. Muhamad, “The number of cooperatives in Indonesia increased in 2024,” *Katadata*, Accessed: Jan. 22, 2026. [Online]. Available: https://databoks.katadata.co.id /ekonomi-makro/statistik/67c574cf2d55b /jumlah-koperasi-di-indonesia-bertambah-pada-2024

[53] F. Alzhrani and K. Saeedi, "Applied Sciences Architectural Patterns for Blockchain Systems and Application Design," *Appl. Sci.*, vol. 13, 2023, doi: 10.3390/app132011533.

[54] P. Pandey and R. Litoriya, “Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain,” *Wirel. Pers. Commun.*, vol. 117, no. 1, pp. 7–25, 2021, doi: 10.1007/s11277-020-07041-7.

[55] Á. Díaz and H. Kaschel, “Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric,” *Systems*, vol. 11, no. 7, 2023, doi: 10.3390/systems11070346.

[56] L. Ismail and H. Materwala, “A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions,” *Symmetry (Basel).*, vol. 11, no. 10, 2019, doi: 10.3390/sym11101198.

[57] H. Mao, T. Nie, H. A. O. Sun, and D. Shen, "A Survey on Cross-Chain Technology: Challenges, Development, and Prospect," *IEEE Access*, no. December 2022, pp. 45527–45546, 2023, doi: 10.1109/ACCESS.2022.3228535.

[58] V. Mardiansyah and R. F. Sari, "Implementation of Proof-of-Work Concept Algorithm using SimBlock Simulator," *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2021, pp. 1-6, doi: 10.1109/NTMS49979.2021.9432645.

[59] J. Benet, “IPFS - Content Addressed, Versioned, P2P File System,” 2014, [Online]. Available: http://arxiv.org/abs/1407.3561

[60] W. Ding *et al.*, “DeSci Based on Web3 and DAO: A Comprehensive Overview and Reference Model,” *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 5, pp. 1563–1573, 2022, doi: 10.1109/tcss.2022.3204745.

[61] S. Rehman, N. Talat Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "Hybrid AES-ECC model for the security of data over cloud storage," *Electron.*, vol. 10, no. 21, pp. 1–20, 2021, doi: 10.3390/electronics10212673.

[62] B. Alamri, K. Crowley, and I. Richardson, “Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT,” *Sensors*, vol. 23, no. 1, pp. 1–38, 2023, doi: 10.3390/s23010218.

[63] B. Alamri, K. Crowley, and I. Richardson, “Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review,” *IEEE Access*, vol. 10, pp. 59612–59629, 2022, doi: 10.1109/ACCESS.2022. 3180367.

[64] _, "Estonia: E-Governance,” Estonia, Accessed: Jun. 05, 2023. [Online]. Available: https://e-estonia.com/solutions/e-governance/government-cloud/

[65] S. Semenzin, D. Rozas, and S. Hassan, “Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia,” *Policy Soc.*, vol. 41, no. 3, pp. 386–401, 2022, doi: 10.1093/polsoc/puac014.

[66] D. J. Daluwathumullagamage and A. Sims, “Blockchain-enabled corporate governance and regulation,” *Int. J. Financ. Stud.*, vol. 8, no. 2, pp. 1–41, 2020, doi: 10.3390/ijfs8020036.

[67] M. D. Lytras and A. C. Şerban, “E-Government Insights to Smart Cities Research: European Union (EU) Study and the Role of Regulations,” *IEEE Access*, vol. 8, pp. 65313–65326, 2020, doi: 10.1109/ACCESS.2020.2982737.