Zero : Jurnal Sains, Matematika, dan Terapan
E-ISSN : 2580-5754; P-ISSN : 2580-569X
Volume 10, Number 1, 2026
DOI: 10.30829/zero.v10i1.27710
Page: 144-156

A Conceptual Consortium Blockchain Model to Enhance Integrity and Auditability in Indonesia's Election Result Recapitulation

[1]M. Hadi Pranowo
IPB University, Bogor, 16680, Indonesia

[2]Yani Nurhadryani
IPB University, Bogor, 16680, Indonesia

[3]Irman Hermadi
IPB University, Bogor, 16680, Indonesia

Article Info

Article history:

Accepted 25 March 2026

Keywords:

Blockchain;
Election;
Hyperledger Fabric;
Smart Contract.

ABSTRACT

Election results recapitulation requires stakeholder participation, data integrity, and auditability. However, electronic systems remain largely centralized and provide limited support for multi-stakeholder involvement, traceable audit trails, and verifiable record integrity. This study formalizes the recapitulation process as a rule-based state-transition model and proposes a consortium Blockchain architecture as a parallel recapitulation channel. Built on Hyperledger Fabric, the network comprises peer nodes representing election officials, supervisors, and witnesses, and is governed by smart contracts with policy-driven endorsement. The model encodes stakeholder roles, cryptographic document binding through IPFS content identifiers and hash verification, and rule-based state validation, with emphasis on arithmetic consistency and plenary time-window constraints. The artifact is evaluated through regulatory compliance mapping and computational testing. The results show that the model enables multiparty verification, preserves auditable transaction history, and maintains verifiable linkage between recapitulation records and supporting documents, while constraining accepted state transitions to defined arithmetic and procedural rules.

Corresponding Author:

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

1. INTRODUCTION

Vote counting and results recapitulation are critical stages in Indonesia's General Elections (Pemilu) [1]. Under Indonesian election law, election results are certified through tiered plenary recapitulation [2], [3], [4] However, this process creates a heavy administrative burden, increases the risk of human error, and may take up to 35 days [5], [6]. To address these limitations, the General Election Commission (KPU) introduced the Vote Counting Information System (Situng) in 2014 and used it widely in the 2019 General Election, before developing the Recapitulation Information System (Sirekap) for the 2024 election [7], [8], [9], [10]. Both systems were intended to improve transparency. Yet Situng recorded at least 7,300 data-entry errors caused by officer negligence [11]. Similar problems reappeared in Sirekap during the 2024 election, when errors in reading scanned official documents produced anomalous data in 24.2% of the initial incoming votes and required corrections in 154,541 polling stations (TPS) [12]. These recurring failures shifted public concern from technical

error to data integrity, suspicions of structured electoral fraud, and declining trust in the legitimacy of election results [11], [13].

Accordingly, this study adopts a consortium Blockchain approach using Hyperledger Fabric, a permissioned framework suited to multi-stakeholder electoral recapitulation through controlled access, confidentiality, and distributed governance [14], [15]. Conventional electronic systems remain vulnerable because they depend on a central authority and thus create a single point of failure [16], [17]. In electoral recapitulation, Blockchain mitigates this risk by distributing authority across the KPU, Bawaslu, and election witnesses [18], [19], [20]. Access is controlled through cryptographic identities and membership policies managed by the Membership Service Provider (MSP), while stakeholder participation is operationalized through Hyperledger Fabric's execute-order-validate architecture: endorsing peers simulate and endorse proposals [21], ordering service nodes sequence transactions into blocks [21], [22], and peers validate them before commitment to the ledger. Data integrity and auditability are supported by Blockchain's immutable ledger structure [23], in which vote records are stored in blocks linked by cryptographic hash functions [24]. Any unauthorized modification changes the block hash and breaks its consistency with the subsequent block [16], making the recapitulation record tamper resistant and auditable [25]. Because storing large files directly on-chain is inefficient and creates scalability risks [26], scanned C.Hasil documents are stored off-chain in the InterPlanetary File System (IPFS), which generates a unique hash-based Content Identifier (CID) that is then recorded on the Blockchain [19], [27]. Statutory rules and recapitulation procedures are enforced through smart contracts as a computational validation mechanism [28], including checks on vote aggregation results and procedural constraints to reduce human error and help constrain fraud [25].

A consortium Blockchain is intended not to replace the legally mandated hierarchical manual recapitulation, but to complement existing manual and electronic mechanisms as a parallel channel [29]. Most prior studies have examined the use of Blockchain in e-voting, whereas studies specifically focusing on Blockchain-based vote recapitulation remain very limited [19], [20]. Therefore, this study proposes a Hyperledger Fabric-based conceptual Blockchain model that represents the institutional roles of the General Election Commission (KPU), the Election Supervisory Board (Bawaslu), and election witnesses, while translating the rules of tiered recapitulation into a rule-based computational validation mechanism. This approach is expected to strengthen e-government principles emphasizing transparency, accountability, and public participation in the digital governance of elections [30].

2. RESEARCH METHOD

The Design Science Research Methodology (DSRM) is adopted to design and evaluate an artifact in the form of a conceptual Blockchain-based election results recapitulation model [31], [32], [33]. In the context and requirements analysis stages, a qualitative descriptive approach is used through regulatory review, literature review, and stakeholder-oriented requirement elicitation [34].

2.1 Problem Identification and Context Analysis through Regulatory Review

This stage analyzes the tiered vote recapitulation workflow to identify procedural constraints in the solution design. It also maps stakeholder roles and key recapitulation documents as the basis for formulating system requirements [35], [36]. The analysis refers to Law No. 7 of 2017, KPU Regulation No. 25 of 2023, and KPU Regulation No. 5 of 2024. The output is a mapping of actors, documents, decision points, and initial requirements for artifact design.

2.2 Solution Objectives and Requirements Formulation Based on Literature Review and FGD

Key issues in electronic recapitulation are identified to derive functional requirements and solution mechanisms for a consortium Blockchain model based on Hyperledger Fabric. These requirements are then reviewed and refined through a focus group discussion (FGD) involving representatives from the Bogor City KPU and Bawaslu, the Chair of the Bogor City DPRD representing the perspective of political party witnesses, the Executive Director of Perludem, and three researchers as facilitators. Participants examine the proposed model, discuss operational challenges, and assess its alignment with current recapitulation practices and the applicable regulatory framework in Indonesia. The output is the refinement of solution objectives and system requirements [37], [38], [39].

2.3 Formulation of the Blockchain Conceptual Model for Election Results Recapitulation

The proposed model is formalized as a rule-based state transition model [40], [41]. The tiered recapitulation workflow is modeled in accordance with applicable legal provisions to define actors, documents, decision points, and state transitions across levels, while stakeholder roles and institutional relations are represented in a structured interaction model. A consortium Blockchain architecture based on Hyperledger Fabric [21], [42] is designed with organizational peer nodes, Membership Service Providers (MSPs), endorsement policies, and off-chain IPFS integration for documentary evidence. Regulatory requirements are encoded in rule-based chaincode. To strengthen the computational framing of the artifact, the methodology is complemented by a simplified

interpretation of transaction-growth scalability across recapitulation tiers and the validation complexity of the chaincode logic. A proof-of-concept prototype is then developed to demonstrate feasibility.

2.4 Evaluating the Conceptual Model through Compliance Mapping and Testing

The evaluation assesses the extent to which the proposed artifact addresses vote recapitulation challenges, particularly stakeholder involvement, data consistency, and auditability, through regulatory compliance mapping [36] and stakeholder feedback obtained via the FGD. In addition, grey-box testing is conducted by combining observation of system behavior with inspection of internal outputs such as validation results, world-state records, and ledger transaction history [43]. Auditability is evaluated through audit trail and immutability testing on the distributed ledger, while data integrity is examined through arithmetic validation, plenary time-window enforcement in the chaincode, and tamper-resistance testing using world-state manipulation scenarios to assess consistency against ledger transaction history.

3. RESULT AND ANALYSIS

3.1 Regulatory Review of the Election Recapitulation Process in Indonesia

The election results recapitulation process in Indonesia begins at the TPS level and continues through the sub-district, regency or city, provincial, and national levels [2], [3], [4]. Each stage is conducted in an open plenary meeting involving election management bodies, supervisory bodies, and election witnesses. The main documents analyzed in this study are Form C.Hasil and C.Kejadian Khusus dan/atau Keberatan Saksi-KPU at the TPS level, and the corresponding D.Hasil and D.Kejadian Khusus dan/atau Keberatan Saksi-KPU forms at higher recapitulation levels.

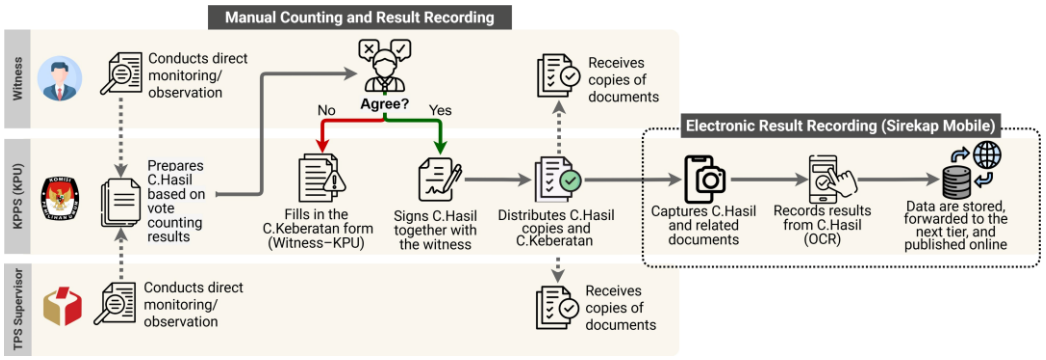

Figure 1. Vote Counting and Documentation Process at the Polling Station (TPS) Level.

At the polling station level, Sirekap digitizes the physical C.Hasil document and extracts election result data [8] through OCR and OMR. The document is signed by KPPS officers and election witnesses as verification of the polling station vote count. However, the upload to Sirekap is carried out only by KPPS officers on behalf of the KPU, with no direct real-time participation of witnesses in the system's data submission and validation process. This shows that the digital mechanism remains centralized under the KPU and limits multi-stakeholder participation in data submission and validation. Any witness objections or special incidents are therefore still recorded manually in the C.Kejadian Khusus dan/atau Keberatan Saksi-KPU form without interrupting the recapitulation process (Figure 1).

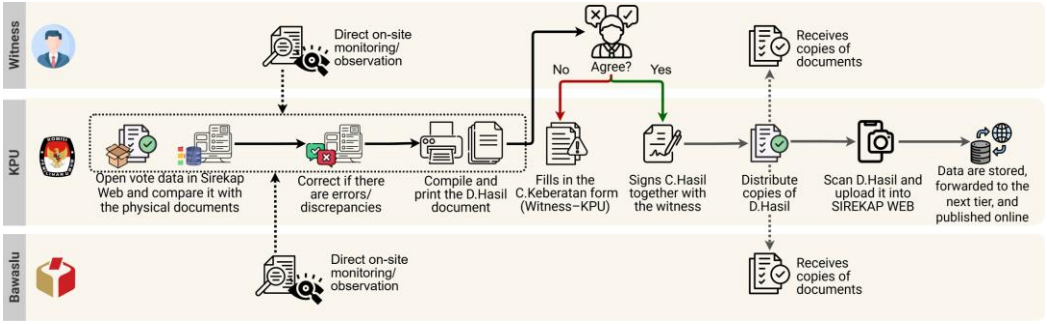

Figure 2. Tiered Vote Recapitulation Process from the Subdistrict to the National Level.

At the subdistrict, regency or city, provincial, and national levels, recapitulation generally follows a uniform workflow (Figure 2). Although Sirekap functions as a supporting system rather than the basis for the official determination of results, its role in practice remains significant. It is used to display results from the lower tier, support comparison and correction against physical documents, print official recapitulation documents, and archive validated C.Hasil/D.Hasil forms in digital form. The physical D.Hasil document signed and approved in the plenary meeting serves as the basis for the official determination of election results.

3.2 Formulation of System Requirements from Literature Review and FGD Findings

Table 1 presents a synthesis of the main issues, associated challenges, and proposed solution directions identified from the literature review. These findings are used as the analytical foundation for formulating the system requirements of the proposed election result recapitulation system.

Table 1. Literature Review (LR) on Key Issues, Challenges, and Solutions in Election Recapitulation

No.	Main issue	Findings on key challenges	Findings on proposed solutions
1	Centralized data governance and limited involvement of stakeholders	Data management remains centralized, raising suspicion of possible data changes. Real-time oversight by witnesses, supervisors, observers, and the public remains limited [1], [19].	Promoting more distributed governance to reduce dependence on a single authority [19], [20]. Expanding real-time monitoring access for stakeholders and the public [1], [13], [19]
2	Vulnerability of data integrity to input errors, document handling problems, and cyber threats	Data are vulnerable to anomalies from writing errors, misuploads, input errors, and incorrect document cropping [9], [12], [13]. Cyber threats and sabotage may compromise data integrity [9], [29].	Strengthening layered validation and rechecking before data are finalized [9], [12]. Adding logical controls to reject unreasonable or inconsistent inputs [6].
3	Limited auditability and traceability of data changes throughout the recapitulation process	The long, multi-layered recapitulation process makes data changes difficult to trace[1], [5], [6]. Fragmented or non-integrated systems make input, correction, and publication histories difficult to audit [9], [44]. Gaps between scanned results, manual entries, and source documents complicate auditing [6], [9]	Establishing parallel verification and backup mechanisms to facilitate cross-checking [9], [29]. Integrating data flows so that the history of changes is more consistent and traceable [44]. Leveraging technologies with tamper-resistant, real-time auditable records, such as Blockchain and IPFS [19], [20].

The analysis of the FGD in Table 2 identifies five core issues consistently raised by participants from KPU, Bawaslu, election witnesses, Perludem, and academia. The findings indicate that challenges in electronic recapitulation are not merely technical in nature, but relate to governance structures, stakeholder roles, auditability, and trust formation.

Table 2. Key Issues Identified from the Focus Group Discussion (FGD)

No	Issues	Description of findings
1	Centralization of Digital Recapitulation	Digital recapitulation processes remain centralized under a single authority, with data entry, validation, and correction conducted exclusively by election administrators.
2	Limited Stakeholder Involvement	Election witnesses and supervisors have restricted roles in digital systems and are unable to directly validate, approve, or formally object within the same platform.
3	Weak Audit Trails and Traceability	Existing systems do not provide clear digital records of who performed data changes, when they occurred, and the procedural basis for such actions.
4	Procedural Integrity and Rule Enforcement	The system does not explicitly enforce plenary time windows and vote aggregation logic, increasing the risk of procedural inconsistency.
5	Trust Deficit in Electronic Recapitulation	Trust in electronic recapitulation is perceived as dependent on transparency, auditability, and inclusiveness, alongside operational efficiency.

The synthesis of the literature review and focus group discussion findings resulted in the formulation of system requirements aimed at enhancing auditability, ensuring data integrity, and facilitating stakeholder involvement, as presented in Table 3.

Table 3. Artifact Design Objectives, System Requirements, and Evaluation Criteria

No.	Solution Objectives	System requirement	Initial evaluation criteria	Source References
1	Reduce concentration of authority	Multi-party recording with verified organizational identities and policy-based endorsement	Transactions are recorded only when the approval policy is satisfied and approvers are verifiable	LR (1); FGD(2),(3)
2	Enable parallel record and verifiable transparency	Witnesses and supervisors can register linked parallel records and report discrepancies, while authorized stakeholders have controlled read access to records and evidence references	Official and parallel records can be compared, discrepancies can be traced, and records and evidence can be verified without modification rights	LR (1),(3); FGD(2),(3)
3	Ensure tamper-evident and accountable audit trails	Transactions and corrections are recorded sequentially as linked entries with actor, time, justification, and evidence information	Changes and corrections are chronologically traceable, attributable, and supported by justification and evidence	LR(2),(3); FGD(1),(3),(5)
4	Enforce procedural and arithmetic integrity	Stage rules, plenary time windows, aggregation logic, and input consistency are validated as system constraints to prevent inconsistent, duplicate, or unauthorized entries	Invalid stage, time, aggregation, duplicate, or unauthorized inputs are rejected and logged	LR(2); FGD(4),(5)

3.3 Blockchain Conceptual Model for Election Results Recapitulation

To represent stakeholder involvement within a consortium Blockchain network, the system provides role- and tier-specific dashboards for the KPU, Bawaslu, and election witnesses. At the TPS level, the KPU-side dashboard is used by KPPS, while at the sub-district and higher levels the corresponding dashboards are used by KPU officials according to their authority. Bawaslu and witness actors likewise access dashboards aligned with their respective roles and recapitulation tiers. Access to these applications and their permitted actions is governed by the Membership Service Provider (MSP), which authenticates organizational identity, and reinforced by chaincode-based authorization rules that determine who may perform which action at which recapitulation tier. The illustration is shown in Figure 3. KPPS completes the vote count, finalizes Form C.Hasil, then scans and uploads the physical document as a digital file.

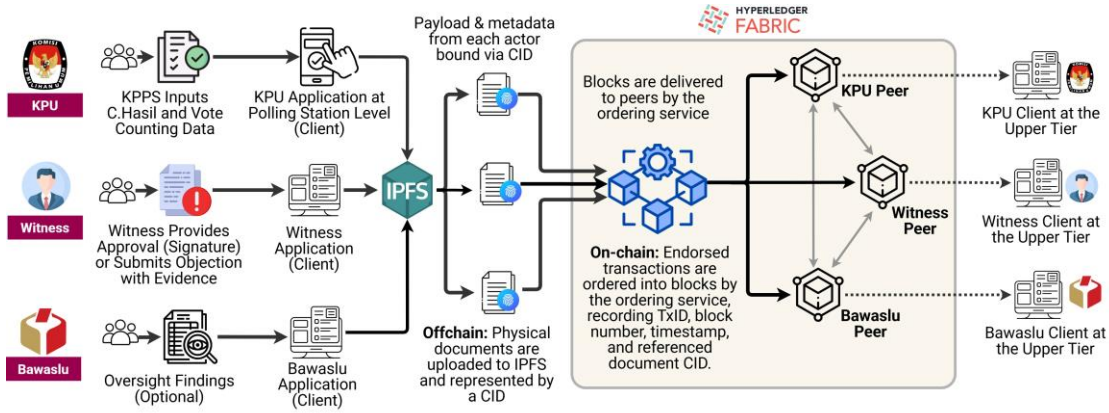

Figure 3. Stakeholder Involvement at the TPS Level in the Consortium Blockchain Model

The vote counting results (vote tallies, totals, and aggregated elements in Form C.Hasil) are recorded on chain as the transaction payload, while the scanned document is stored off chain on IPFS and linked through its Content Identifier (CID) and metadata, creating a cryptographic binding between the digital data and the physical evidence (Figure 4). Witnesses provide approval or submit objections through the system as a digital representation of Form C.Kejadian Khusus dan/atau Keberatan Saksi-KPU, while the formal determination remains based on the signed physical document, including supporting evidence also linked via CID. This linkage is reinforced through rule-based chaincode combined with hash and versioning controls to ensure consistent document binding, controlled updates, and the traceability and verifiability of each document version.

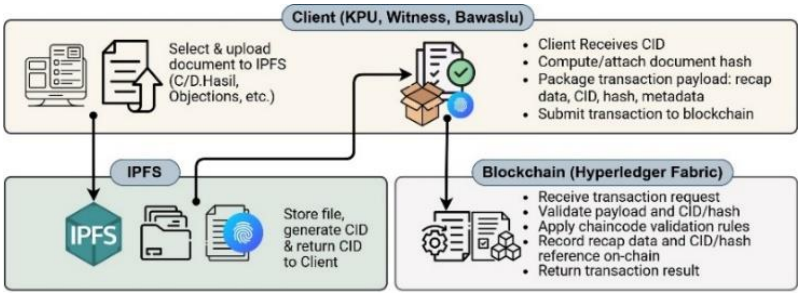

Figure 4. IPFS-Based Document Processing and On-Chain Referencing

Figure 5 represents the tiered recapitulation mechanism at the sub-district, regency or city, provincial, and national levels. At each tier, the client application connects to a trusted gateway peer within its organization to query committed results from the immediately lower tier. The retrieved results are then used as the basis for aggregation and verification, and are compared with the corresponding physical documents during the plenary meeting before any correction or transaction recording is performed. If any discrepancies are found, corrections are made according to the authority of the respective tier, while the manual oversight process by election administrators, supervisors, and witnesses continues in accordance with the applicable provisions. At this stage, witnesses may express approval or submit objections, which are recorded by the system together with the supporting evidence. This mechanism ensures that document copies and objection records are consistently treated within the system as an official reference for all stakeholders, thereby establishing a single source of truth. If discrepancies are found between the displayed data and the corresponding official documents, corrections are recorded as new justified transactions without overwriting prior records. Copies and objection records remain preserved on the replicated ledger and are used for further processing and tiered validation until formal endorsement at each level.

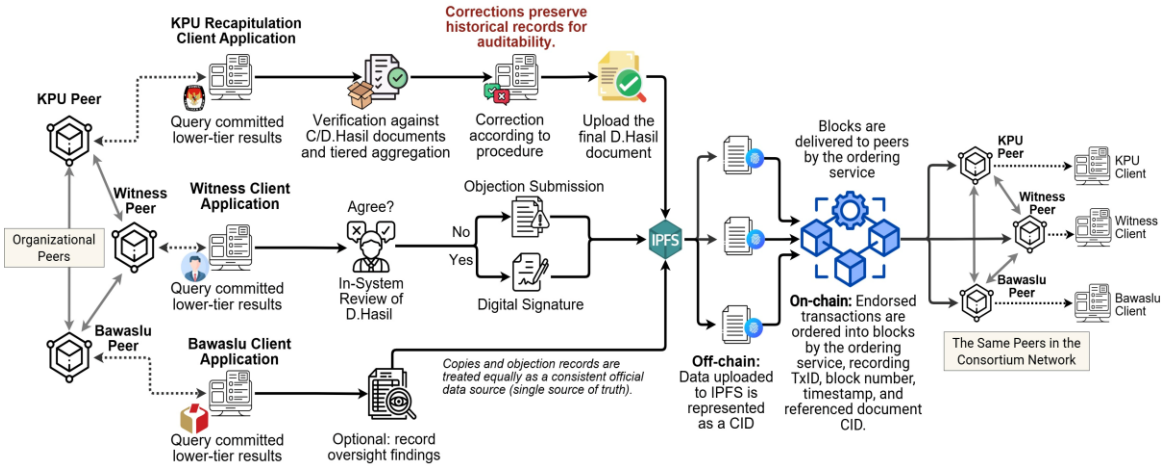

Figure 5. Consortium Blockchain Workflow for Tiered Election Recapitulation

Transaction processing follows the execute–order–validate (Figure 6) model of Hyperledger Fabric [21], [22], [45]. Transactions are endorsed, ordered, and validated before commitment to the ledger. During validation, MVCC filters out conflicts from concurrent updates, so only consistent records are committed and replicated across peer nodes for the next recapitulation tier.

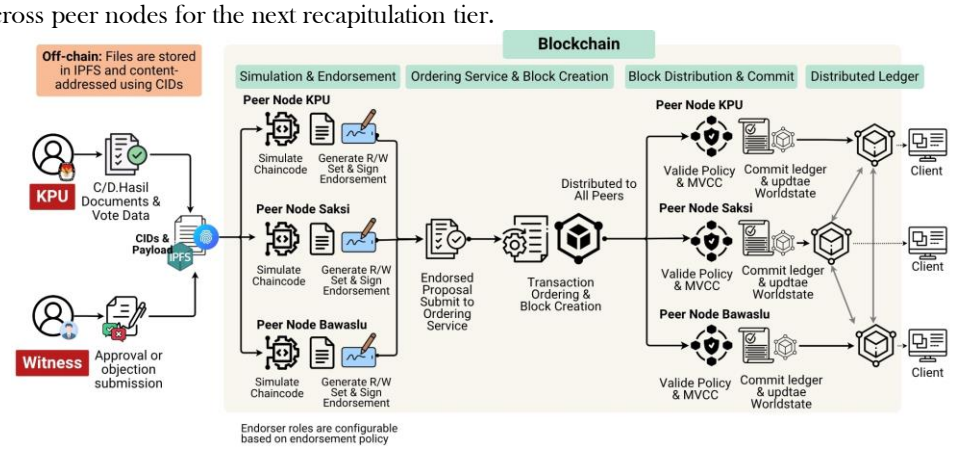

Figure 6. Transaction Flow in Consortium *Blockchain*-Based Election Recapitulation

The architecture separates user interaction (Figure 7), application orchestration, Blockchain execution, and storage functions in order to improve modularity, control, and traceability. Frontend applications are provided for each stakeholder role, but all requests are routed through the application gateway rather than being sent directly to the Blockchain network. This gateway layer centralizes authentication, authorization, input validation, and transaction routing, while also bridging interactions with distributed file storage.

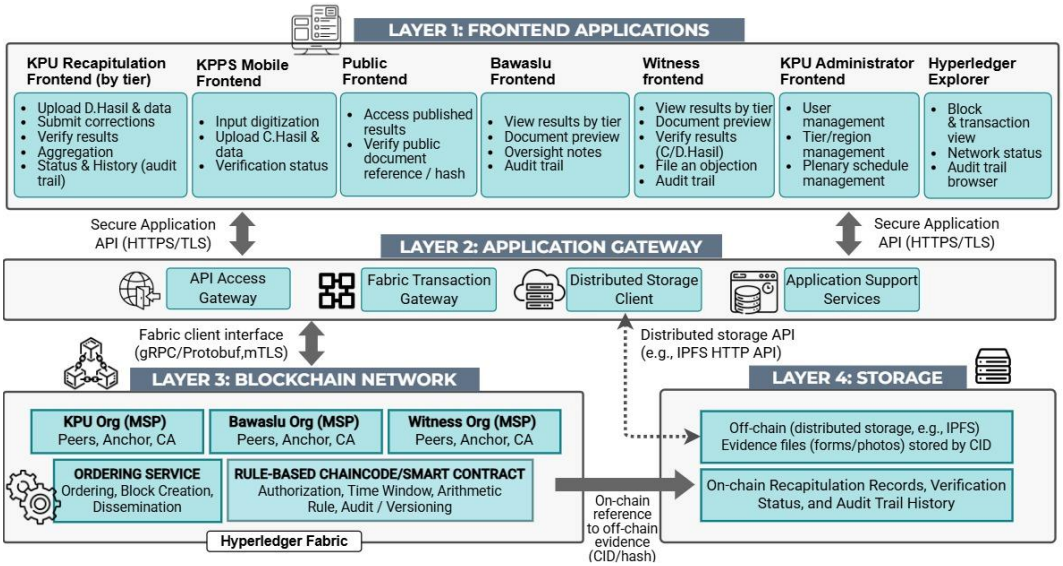

Figure 7. Proposed Consortium Blockchain Architecture for Tiered Election Result Recapitulation

At the network layer, the consortium Blockchain enforces rule-based validation through chaincode and records the recapitulation state, status changes, and audit trail on-chain across participating organizations. Off-chain storage is used for supporting evidence files, while cryptographic references to those files are maintained on-chain to preserve linkage, integrity, and verifiability. This layered design supports the main requirements of the model, namely multi-stakeholder participation, procedural rule enforcement, auditability, and document traceability [46].

3.4 Formalization of Rule-Based Chaincode for Strengthening Data Integrity through Plenary Time Window and Arithmetic Consistency Validation

To enhance data integrity through rule-based control, the proposed chaincode [28] formalizes two key validation constraints: plenary time window enforcement and arithmetic consistency validation. The plenary time constraint ensures that recapitulation can only be conducted within officially scheduled plenary sessions [2], [3], [4], thereby preventing unauthorized input or modification outside the formal process. The core chaincode rules are presented in the form of pseudocode algorithms.

Algorithm 1: Plenary Constraint Validation (Plenary Time/Status Control)

Input : action, scopeType, scopeId, txTime
Output: ACCEPT / REJECT

```
rule ← MapActionToPlenaryRule(action) // {requiresPlenary, phase}
if rule = NULL then return REJECT
if rule.requiresPlenary = FALSE then return ACCEPT
plenary ← GetPlenarySchedule(tier, unitId) // {status, submitStart, submitEnd, correctStart, correctEnd}
if plenary = NULL then return REJECT
if plenary.status ≠ "OPEN" then return REJECT
if rule.phase = "SUBMIT" then
window ← (plenary.submitStart , plenary.submitEnd)
else if rule.phase = "CORRECT" then
window ← (plenary.correctStart , plenary.correctEnd)
end if
if txTime < window.start OR txTime > window.end then
return REJECT // outside plenary window
end if
return ACCEPT
```

To help prevent numerical overstatement of votes before a transaction is committed to the ledger, the chaincode enforces arithmetic consistency checks on TPS recapitulation data. It verifies that the number of ballots used corresponds to total voter turnout, that total votes equal the sum of valid and invalid votes, and that turnout is consistent with the recorded vote totals. Any transaction that violates these constraints is rejected, while the remaining arithmetic rules are presented in Table 4.

Algorithm 2: Arithmetic Validation for Recapitulation (Core constraints shown; full set is provided in Table 4)

Input : voteData
Output: ACCEPT / REJECT

```
if voteData = NULL then return REJECT
if MissingRequiredFields(voteData) then return REJECT
if AnyValueNegative(voteData) then return REJECT
if voteData.ballotsUsed ≠ voteData.totalVoterTurnout then return REJECT
if voteData.totalVotes ≠ voteData.validVotes + voteData.invalidVotes then return REJECT
if voteData.totalVoterTurnout ≠ voteData.validVotes + voteData.invalidVotes then return REJECT
return ACCEPT
```

Table 4. Arithmetic Consistency Rules for Recapitulation (based on C.Hasil form)

No.	Description
1	Total registered voters (DPT) = male DPT + female DPT
2	Male voter turnout = male DPT turnout + male DPTb turnout + male DPK turnout
3	Female voter turnout = female DPT turnout + female DPTb turnout + female DPK turnout
4	Total voter turnout = male voter turnout + female voter turnout
5	Ballots used = total voter turnout
6	Total votes = valid votes + invalid votes
7	Total voter turnout = valid votes + invalid votes
8	Ballots received = ballots used + ballots returned + ballots remaining

The chaincode logic is designed in accordance with the architecture shown in Figure 7 as an integrated rule-based mechanism and a rule-based state transition system, rather than as a collection of isolated rules. In this system, each recapitulation record moves through defined states according to explicit rules that govern valid actions, transitions, and conditions at each stage. Its components work together to formalize actor governance by specifying permissible actions for each role, enforce plenary schedule compliance and tiered recapitulation logic to preserve procedural validity and data consistency, and support verification, objection handling, controlled correction, and document binding through CID and hash references to strengthen evidentiary integrity and auditability.

3.5 Demonstration of Key System Components

A demonstration of the system's key features is presented as a proof of concept to indicate that the proposed conceptual design is technically feasible in principle. Figure 8 shows that the application records timestamps and the actions of each stakeholder as a digital representation of witness signatures and formal objections. The input time restrictions embedded in the chaincode ensure compliance with the official recapitulation stages while enabling tamper-resistant verification and traceability.

Figure 8. Interface design of the election results entry application, illustrating witness involvement, input time constraints, and multi-level verification.

The mechanism for submitting witness objections and recording Bawaslu's oversight notes is illustrated in Figure 9. Objections, together with image-based evidence, are cryptographically bound to the blockchain record, allowing each objection to be verified and traced as part of the formal audit trail. To address human error without deleting previous records, the system provides a correction feature, as shown in Figure 10. Modified records are explicitly flagged, while prior records remain accessible, allowing changes to be traced in terms of the affected record, the responsible actor, and the stated reason. This supports transparency and strengthens confidence that data are not altered silently without legitimate justification. Each change is recorded as a new entry, so the original data, corrections, signatures, and objections remain preserved as part of the audit trail.

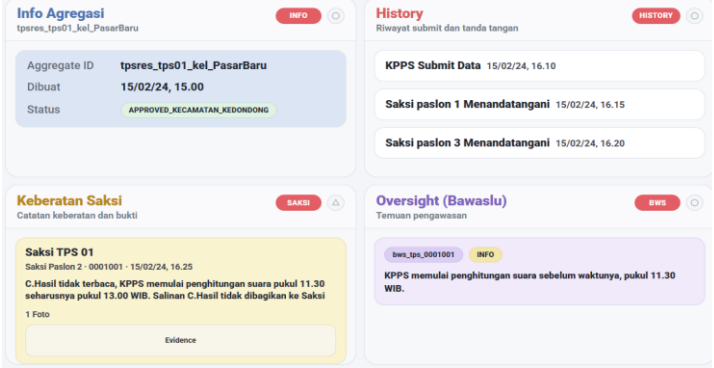

Figure 9. Interface of stakeholder engagement in the system through approval or objection submission.

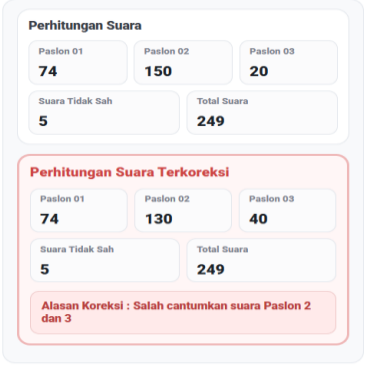

Figure 10. Corrected polling stations are marked, with history preserved.

3.6 Evaluation Result

Evaluation of the Conceptual Model

To validate the alignment between the purpose [31] of the conceptual design and the intended research objectives (Table 5), The evaluation uses two complementary instruments: one combines literature-based assessment and FGD input to examine the model's conceptual grounding and practical relevance, while the other assesses its alignment with the applicable electoral legal framework.

Table 5. Evaluation of Conceptual Design Responses Based on FGDs and Literature Findings

No.	Design objective	Identified problem	Proposed design elements	Evaluation outcome
1	Reduce concentration of authority	Digital recapitulation is perceived as centralized and opaque	Consortium-based network, distributed ledger, verified organizational identities, and policy-based endorsement	Recording authority is distributed across verified organizations, and transactions are accepted only when the endorsement policy is satisfied.
2	Enable parallel recording, oversight, and controlled transparency	Witnesses and supervisors have limited involvement in verification and discrepancy reporting	Linked parallel record registration, discrepancy reporting, and controlled read access for authorized stakeholders	Official and parallel records can be compared, discrepancies can be traced, and authorized stakeholders can verify records and evidence without write privileges.
3	Ensure tamper-evident and accountable audit trails	Data changes and corrections are difficult to trace and justify	Sequential transaction history, visible correction records, and CID- and hash-based evidence binding	Changes and corrections are chronologically traceable, attributable to specific actors, and linked to stated justification and evidence references.
4	Enforce procedural and arithmetic integrity	Recapitulation data may contain procedural violations, duplication, or inconsistent aggregation	Chaincode-enforced stage rules, plenary time windows, aggregation logic, and input consistency constraints within a rule-based state transition system	Invalid stage, time, aggregation, duplicate, or unauthorized inputs are rejected and logged before acceptance.

The subsequent evaluation focuses on regulatory compliance mapping. This evaluation is intended to assess the normative alignment and contextual consistency between the proposed conceptual design and the applicable legal provisions, as summarized in Table 6. It is not intended as a legal interpretation or juridical assessment, but as a structured mapping of the proposed Blockchain-based design to the core regulatory requirements of election result recapitulation.

Table 6. Regulatory Compliance Mapping for the Proposed Blockchain-Based Recapitulation Model

No	Regulatory Basis	Core Normative Requirement	Compliance Gap in Existing Electronic Recapitulation	Compliance-Oriented Blockchain Design Response
1	Law No. 7/2017 Articles 1, 12(a,c,g), 405(2), 388(2)–(3), 408(2)–(4), 409; PKPU No. 25/2023 Article 49(5), Articles 64–65; PKPU No. 5/2024 Articles 14(8), 19, 25, 47(8), 59, 64(8), 75, 80(8), 91; KKPU No. 115/2024.	Recapitulation remains under KPU authority, while witnesses and Bawaslu may attend, supervise, sign, file objections, and have their positions recorded.	Existing electronic recapitulation remains centralized, with limited system-based participation and weak linkage between stakeholder positions and recapitulation data.	A consortium ledger can record role-based participation, approvals, and objections as part of the recapitulation record.
2	PKPU No. 25/2023 Articles 56–61, 66; Law No. 7/2017 Article 390(2); PKPU No. 5/2024 Articles 16, 18–19, 48–51, 65–68, 84–86.	Recapitulation must be supported by official forms so that results, objections, and corrections remain traceable.	Data, supporting documents, and correction history are not yet fully traceable in an integrated manner.	Hash-linked document references and on-chain correction history can strengthen traceability and auditability
3	Law No. 7/2017 Articles 385(1), 386; PKPU No. 25/2023 Articles 26(2)–(4), 46, 51–54, 61, 64; PKPU No. 5/2024 Articles 10, 44, 61, 77.	Recapitulation must follow regulated plenary timing and maintain logical consistency of ballot and vote totals.	Existing electronic recapitulation does not automatically enforce timing rules or arithmetic consistency at the transaction level.	Rule-based chaincode can enforce plenary time windows and arithmetic validation before transactions are committed.
4	Law No. 7/2017 Articles 381(1)–(2), 405(7); PKPU No. 25/2023 Articles 59, 66(4); PKPU No. 5/2024 Articles 23, 55, 72, 90.	Election results must be publicly accessible and verifiable.	Transparency remains focused on result publication, while access to supporting records and objections is still limited.	A transparent access layer can support public verification of results, objections, and supporting records within the applicable disclosure scope.

Overall, the evaluation indicates that the proposed system is conceptually capable of addressing the key challenges identified through the literature review, FGDs, and regulatory assessment. While the conceptual design demonstrates adequacy in resolving these constraints at the design level, further work is required to strengthen the findings through technical testing and empirical validation in real or simulated operational settings.

System Testing and Results

To verify system behavior, this study employs automated grey-box testing [43], a testing method that evaluates the system through external interfaces while designing test scenarios based on partial knowledge of its internal logic and architecture. This approach is used to assess whether the proposed artifact can support vote recapitulation in a consistent, traceable manner and in accordance with the adopted procedural rules. The testing results are summarized in Table 7.

Table 7. Main Testing Results of the Proposed Blockchain-Based Vote Recapitulation System

No.	Test Category	Objective	Test Scenario	Expected Result	Result
1	Audit Trail	To verify that all recapitulation changes are permanently recorded and retrievable	An asset was created, updated, finalized, and queried through the history function	All prior states, timestamps, and transactions are retrievable in chronological order	PASS
2	Immutability	To verify that updates do not erase prior ledger records	The latest World State was compared with the on-chain asset history	The current state reflects only the latest record, while previous records remain preserved in the ledger	PASS
3	Time-Window Enforcement	To verify that submission and correction are restricted to the authorized plenary schedule	Transactions were tested before, during, and after the configured time window	Valid transactions are accepted, while out-of-window transactions are rejected	PASS
4	Arithmetic and Logical Validation	To verify the consistency of vote totals, ballot usage, and numeric constraints	Inputs with inconsistent totals, ballot mismatches, turnout anomalies, and negative values were submitted	Invalid numeric or logical inputs are rejected by the smart contract	PASS
5	Objection Recording	To verify that structured objection records can be stored and retrieved	A witness objection with narrative fields and evidence metadata was submitted and queried	The objection record is successfully stored and retrievable from the ledger	PASS
6	IPFS-based Evidence Auditability	To verify that digital evidence is stored in IPFS and retrievable through its CID	A document was uploaded through the front end, generating a CID, and later retrieved via the IPFS gateway	The upload returns a valid CID, and the same file is retrievable and verifiable through the gateway	PASS
7	Distributed Consensus and Tamper Resistance	To verify cross-organizational consistency and resistance to unauthorized state modification	A transaction was verified across peers, then one peer's World State was manually altered before resubmission	Legitimate data remain consistent across peers, and tampered state causes endorsement failure	PASS

Among the conducted tests, tamper resistance was particularly relevant to system integrity because it assessed whether unauthorized changes at the storage level could bypass consensus and endorsement. Direct manipulation of the World State on one peer, followed by an official update transaction, was rejected due to an endorsement mismatch across peers, showing that illegal changes could not be silently propagated to the ledger. In addition, the arithmetic consistency and plenary time-window tests confirmed that the chaincode could enforce core procedural rules by rejecting logically inconsistent vote data and transactions submitted outside the authorized plenary period. Taken together, these results indicate that the proposed system supports auditability and data integrity through immutable records, rule-based validation, and consistent peer behavior under the tested scenarios.

3.7 Discussion of Finding

Given the scale of Indonesia's 2024 election, spanning 38 provinces, 514 regencies or cities, 7,277 sub-districts, and 823,236 polling stations [8], [10], the proposed chaincode should also be examined in terms of scalability and computational complexity. Although full network-level performance testing is beyond the scope of this study, the volume of recapitulation units and transaction events motivates an assessment of whether the rule-based validation logic remains computationally manageable across tiers.

Scalability Model and Complexity Analysis

To assess scalability across recapitulation tiers, a simple transaction volume and validation complexity model is formulated. Let $J = \{\text{TPS}, \text{Kec}, \text{Kab}, \text{Prov}, \text{Nas}\}$ denote the set of recapitulation tiers, and let U_j denote the number of units at tier $j \in J$. For each tier j, let b_j, c_j, and o_j denote the baseline transaction volume, correction volume, and objection or additional verification volume per unit, respectively. The transaction volume at tier j is defined as $T_j = U_j(b_j + c_j + o_j)$, and the total transaction volume across all tiers is $T_{\text{total}} = \sum_{j \in J} T_j$. For the current rule set, local *chaincode* validation, particularly arithmetic consistency checking and plenary time-window enforcement, operates over a fixed number of fields and decision steps. Hence, the local computational cost per transaction can be approximated asymptotically as $C_{\text{cc}} = O(1)$. Accordingly, the total validation workload is $W_{\text{cc}} = T_{\text{total}} \cdot C_{\text{cc}} = O(T_{\text{total}})$. This formulation indicates that the proposed rule-based chaincode has constant local validation complexity, while the total validation workload grows linearly with transaction volume across recapitulation tiers. The complexity analysis in this subsection is based on the validation rules formalized in Algorithm 1 and Algorithm 2.

Consensus and Rule-based Endorsement Mechanism

In the current prototype, the ordering layer remains simplified [47], but a fuller inter-institutional deployment could strengthen it through a Raft-based ordering service [48], which typically requires at least three ordering nodes for reliable operation. However, transaction endorsement should not be interpreted as full multi-stakeholder approval, since recapitulation does not procedurally depend on witness or Bawaslu consent under the applicable legal framework [2], [3], [4]. A more realistic design therefore combines feasible organizational endorsement with rule-based chaincode to enforce plenary windows, arithmetic consistency, actor and tier scope, and document completeness in accordance with the governing regulations. This should be understood as a conceptual refinement of ordering and endorsement design rather than a formal optimization of consensus policies.

Limitations and Future Work.

The findings of this study should be understood within the scope of the current prototype environment. This study provides a formal contribution through rule-based state transition modeling of tiered recapitulation, the specification of arithmetic and plenary-window validation rules, and a simple interpretation of scalability and validation complexity. Although the model has been functionally evaluated through rule-based chaincode testing, the evaluation has not yet covered large-scale operational conditions, such as nationwide transaction volume, dense transaction traffic, heterogeneous deployment settings, and probabilistic failure scenarios across participating nodes and organizations. Accordingly, future research should focus on strengthening the mathematical and quantitative aspects of the model, including formalization of the core chaincode logic, more rigorous scalability and validation complexity analysis, and evaluation of system robustness under more realistic operating conditions. Future development may also examine more reliable consensus and ordering configurations, including Raft-based deployment, as well as formal verification of core chaincode rules [40], [49], particularly those related to plenary time compliance, arithmetic consistency, and status locking after finalization.

4. CONCLUSION

This study concludes that the proposed Blockchain-based election results recapitulation model provides a structured mechanism for addressing key challenges in electronic recapitulation, particularly centralization, data integrity, and auditability. By adopting a consortium Blockchain architecture, the model reduces reliance on a single authority through multiparty participation involving KPU, Bawaslu, and election witnesses. Data integrity is supported through immutable records, resistance to unauthorized modification, and rule-based enforcement of procedural controls, including plenary time-window constraints and arithmetic validation. Auditability is strengthened through audit trails, timestamps, traceable histories, and the cryptographic linkage of digital evidence to recapitulation transactions, enabling transparent and verifiable review. Future research should extend the model through scalability testing, denser transaction simulations, evaluation in more realistic operational environments, and interface improvements to better translate engineered trust into experienced trust [50], [51].

ACKNOWLEDGEMENT

This research was supported by the Ministry of Higher Education, Science, and Technology of Indonesia through the Penelitian Tesis Magister scheme under the Basis Informasi Penelitian dan Pengabdian kepada Masyarakat (BIMA) funding platform, under Main Contract No. 006/C3/DT.05.00/PL/2025 and Derivative Contract No. 23359/IT3.D10/PT.01.03/P/B/2025.

5. REFERENCES

[1] M. Habibi, A. Mahadika, and W. Astuti, "Digital dilemma: technology in the vote counting process for general elections and local head elections in Indonesia," *Otoritas: Jurnal Ilmu Pemerintahan*, vol. 13, no. 3, pp. 377–389, Dec. 2023, doi: 10.26618/OJIP.V13I3.12729.

[2] Pemerintah Republik Indonesia , *Undang-undang Nomor 7 Tahun 2017 tentang Pemilihan Umum*. 2017.

[3] Komisi Pemilihan Umum, "Peraturan Komisi Pemilihan Umum Nomor 25 Tahun 2023 tentang Pemungutan dan Penghitungan Suara dalam Pemilihan Umum," 2023.

[4] Komisi Pemilihan Umum, "Peraturan Komisi Pemilihan Umum Nomor 5 Tahun 2024 tentang Rekapitulasi Hasil Penghitungan Perolehan Suara dan Penetapan Hasil Pemilihan Umum," 2024.

[5] R. Azzahri, "Tinjauan Kritis terhadap Penggunaan Aplikasi Sirekap dalam Proses Pemilihan Umum Presiden Tahun 2024," *Iapa Proceedings Conference*, p. 398, 2024, doi: 10.30589/proceedings.2024.1067.

[6] S. Zuhri, "Urgensi pemanfaatan teknologi informasi dalam penghitungan dan rekapitulasi suara," *Electoral Research*, no. 29, pp. 1–17, 2019.

[7] H. M. Pratama and N. A. Salabi, *Adoption of Voting Technology: A Guide for Electoral Stakeholders in Indonesia*. International IDEA and Perludem, 2020. doi: 10.31752/idea.2020.26.

[8] A. I. Patiroi, A. G. Karim, and B. Setiawan, *Storytelling Data Pemilu 2024*. Jakarta: Komisi Pemilihan Umum Republik Indonesia, 2024.

[9] M. A. Pramessella, N. A. Ramadhani, R. Misbah, F. N. Fakih, A. A. Viqri, and A. S. Azmy, "Analisis Peran Komisi Pemilihan Umum Dalam Mewujudkan Pelaksanaan Demokrasi Substantif Pada Pemilihan Umum: Studi Kasus Manipulasi Data Dalam Sirekap Pada Pilpres 2024," *Mandub : Jurnal Politik, Sosial, Hukum dan Humaniora*, vol. 2, no. 4, pp. 278–304, 2024, doi: 10.59059/mandub.v2i4.1877.

[10] H. Husein, *Perjalanan Data Pemilih Pemilu 2024*. Jakarta: Komisi Pemilihan Umum Republik Indonesia, 2024.

[11] Mahpudin, "Pemanfaatan Teknologi Pemilu Di Tengah Era Post Truth: Antara Efisiensi dan Kepercayaan," *Jurnal PolGov*, vol. 1, no. 2, pp. 157–197, Oct. 2019, doi: 10.22146/POLGOV.V1I2.55886.

[12] A. D. K. Amrynudin, "Data Anomali dalam Sistem Informasi Rekapitulasi pada Pemilu 2024," Mar. 2024, *Jakarta*. Accessed: Feb. 16, 2026. [Online]. Available: https://berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XVI-5-I-P3DI-Maret-2024-2014.pdf

[13] A. N. Azzahra, Y. Janwari, and L. F. Rizal, "Implikasi Konflik Penggelembungan Suara Sirekap Terhadap Demokrasi yang Jurdil dalam Pemilu 2024 Perspektif Siyasah Dusturiyah," *UNES Law Review*, vol. 6, no. 4, pp. 11818–11832, Jul. 2024, doi: 10.31933/UNESREV.V6I4.2193.

[14] O. Dib, K.-L. Brousmiche, A. Durand, E. E. Thea, and B. Hamida, "Consortium Blockchains: Overview, Applications and Challenges," *International Journal on Advances in Telecommunications.*, vol. 11(1 & 2), pp. 51–63, 2018.

[15] Y. Bai, Q. Hu, S. H. Seo, K. Kang, and J. J. Lee, "Public Participation Consortium Blockchain for Smart City Governance," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2094–2108, Feb. 2022, doi: 10.1109/JIOT.2021.3091151.

[16] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," *Sensors 2022, Vol. 22, Page 7585*, vol. 22, no. 19, p. 7585, Oct. 2022, doi: 10.3390/S22197585.

[17] C. C. Z. Wei and C. C. Wen, "Blockchain-Based Electronic Voting Protocol," *JOIV : International Journal on Informatics Visualization*, vol. 2, no. 4–2, pp. 336–341, Sep. 2018, doi: 10.30630/joiv.2.4-2.174.

[18] M. M. Merlec, M. M. Islam, Y. K. Lee, and H. P. In, "A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme," *Sensors 2022, Vol. 22, Page 1271*, vol. 22, no. 3, p. 1271, Feb. 2022, doi: 10.3390/S22031271.

[19] S. Lie, A. Wicaksana, and M. Widjaja, "A Blockchain-Based E-Recapitulation System for Indonesia'S Presidential Election," *Journal of Logistics, Informatics and Service Science*, vol. 11, no. 4, pp. 313–329, 2024, doi: 10.33168/JLISS.2024.0419.

[20] C. G. Pakpahan and T. Q. Al-Fahd, "Manifestasi Negara Indonesia Sebagai Negara Kesejahteraan (Welfare State): Penerapan Sistem Electronic Recap (E-Recap) Berbasis Teknologi Blockchain Dalam Pemilu Serentak Indonesia," *Jurnal Hukum dan HAM Wara Sains*, vol. 2, no. 08, pp. 622–630, Aug. 2023, doi: 10.58812/JHHWS.V2I08.513.

[21] E. Androulaki, A. De Caro, M. Neugschwandtner, and A. Sorniotti, "Endorsement in hyperledger fabric," *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, pp. 510–519, Jul. 2019, doi: 10.1109/Blockchain.2019.00077.

[22] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, vol. 2018-January, Apr. 2018, doi: 10.1145/3190508.3190538.

[23] S. R. Aji and W. T. H. Putri, "Implementasi Teknologi Blockchain dalam Aplikasi E-Voting Berbasis Mobile," *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi*, vol. 14, no. 2, pp. 219–231, 2023, doi: 10.31849/digitalzone.v14i2.16682.

[24] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 70746–70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[25] J. Sarker, "Blockchain Technology in Accounting and Auditing: Benefits, Challenges, and Emerging Practices," *South Asian Res J Bus Manag*, vol. 7, no. 6, pp. 517–526, 2025, doi: 10.36346/sarjbm.2025.v07i06.005.

[26] C. Antal, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Distributed ledger technology review and decentralized applications development guidelines," *Future Internet*, vol. 13, no. 3, pp. 1–32, Mar. 2021, doi: 10.3390/FI13030062.

[27] N. Sangeeta, S. Y. Nam, N. Sangeeta, and S. Y. Nam, "Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability," *Electronics 2023, Vol. 12,* vol. 12, no. 7, Mar. 2023, doi: 10.3390/ELECTRONICS12071545.
[28] H. Taherdoost and H. Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review," *Information 2023, Vol. 14,* vol. 14, no. 2, Feb. 2023, doi: 10.3390/INFO14020117.
[29] R. McDermott, V. Prochko, and T. Chaudhary, "Briefing Paper: Cybersecurity of Election Results Management Systems," 2022. Accessed: Jan. 18, 2026. [Online]. Available: https://www.ifes.org/sites/default/files/2023-06/Briefing_paper_2_Election_Results_Management.pdf
[30] H. Y. Novita, Y. Nurhadryani, S. Wahjuni, D. I. Komputer, F. Mipa, and P. Bogor, "Analisis Penerapan Teknologi Informasi dalam Mendukung Pengembangan Local E-Government," *Jurnal Penelitian Pos dan Informatika*, vol. 11, no. 1, pp. 1–19, Nov. 2021, doi: 10.17933/JPPI.V11I1.265.
[31] S. Kroop, "Artifact Validity in Design Science Research (DSR): A Comparative Analysis of Three Influential Frameworks," *Lecture Notes in Computer Science*, vol. 15703 LNCS, pp. 199–215, Feb. 2025, doi: 10.1007/978-3-031-93976-1_13.
[32] 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, doi: 10.2753/MIS0742-1222240302.
[33] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," 2004.
[34] H. Kim, J. S. Sefcik, and C. Bradway, "Characteristics of Qualitative Descriptive Studies: A Systematic Review," *Res. Nurs. Health*, vol. 40, no. 1, p. 23, Feb. 2016, doi: 10.1002/NUR.21768.
[35] A. Zasada, M. Hashmi, M. Fellmann, and D. Knuplesch, "Evaluation of Compliance Rule Languages for Modelling Regulatory Compliance Requirements," *Software*, vol. 2, no. 1, pp. 71–120, Jan. 2023, doi: 10.3390/software2010004.
[36] S. Ingolfo, A. Siena, and J. Mylopoulos, "Establishing regulatory compliance for software requirements," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6998 LNCS, pp. 47–61, 2011, doi: 10.1007/978-3-642-24606-7_5.
[37] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, Nov. 2019, doi: 10.1016/J.JBUSRES.2019.07.039.
[38] N. K. Bachtiar, M. Fariz, and M. S. Arif, "Conducting a Focus Group Discussion in Qualitative Research," *Innovation, Technology, and Entrepreneurship Journal*, vol. 1, no. 2, pp. 94–101, Aug. 2024, doi: 10.31603/ITEJ.11466.
[39] C. Farinha, M. M. da Silva, C. Farinha, and M. M. da Silva, "Focus Groups For Eliciting Requirements In Information Systems Development," *UK Academy for Information Systems Conference Proceedings 2009*, Mar. 2009, Accessed: Mar. 03, 2026. [Online]. Available: https://aisel.aisnet.org/ukais2009/26
[40] P. Tolmach, Y. Li, S. W. Lin, Y. Liu, and Z. Li, "A Survey of Smart Contract Formal Specification and Verification," *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, Jul. 2021, doi: 10.1145/3464421.
[41] A. Mavridou, A. Laszka, E. Stachtiari, and A. Dubey, "VeriSolid: Correct-by-Design Smart Contracts for Ethereum," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11598 LNCS, pp. 446–465, 2019, doi: 10.1007/978-3-030-32101-7_27.
[42] X. Chen, S. He, L. Sun, Y. Zheng, and C. Q. Wu, "A Survey of Consortium Blockchain and Its Applications," *Cryptography 2024, Vol. 8, Page 12*, vol. 8, no. 2, p. 12, Mar. 2024, doi: 10.3390/CRYPTOGRAPHY8020012.
[43] M. Ehmer and F. Khan, "A Comparative Study of White Box, Black Box and Grey Box Testing Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 6, 2012, doi: 10.14569/IJACSA.2012.030603.
[44] D. Ajeng, I. Pusparini, E. Raharjo, and S. Lestari, "PENERAPAN APLIKASI KEPEMILUAN KPU DI TINGKAT KABUPATEN/KOTA: HAMBATAN DAN SOLUSI," *Electoral Governance Jurnal Tata Kelola Pemilu Indonesia*, vol. 3, no. 2, pp. 138–160, Nov. 2022, doi: 10.46874/tkp.v3i2.651.
[45] P. Jangid, N. B. Badhe, N. Giri, and V. Ashok Bharadi, "Comparative Analysis Of Hyperledger Fabric Performance Across Various Ordering Service," *Int. J. Appl. Math. (Sofia).*, vol. 38, no. 2s, pp. 1367–1385, Oct. 2025, doi: 10.12732/IJAM.V38I2S.728.
[46] A. Barlianto, I. Hermadi, and S. Wahjuni, "Pengembangan Prototipe Aplikasi Berbasis Blockchain dan QR Code dengan Metode ABCDE untuk Rantai Pasok Beras," *Jurnal Ilmu Komputer dan Agri-Informatika*, vol. 11, no. 2, pp. 205–215, Nov. 2024, doi: 10.29244/JIKA.11.2.205-215.
[47] C. Wang, X. Chu, and S. Member, "Stochastic Performance Analysis of Phase Decomposition in Hyperledger Fabric," 2023, Accessed: Dec. 09, 2025. [Online]. Available: https://arxiv.org/pdf/2309.09547
[48] D. Ongaro and J. Ousterhout, "In Search of an Understandable Consensus Algorithm," in *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, Philadelpia: USENIX Association, Jun. 2014, p. 305. [Online]. Available: https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro
[49] S. Kalra, S. Goel, M. Dhawan, and S. Sharma, "ZEUS: Analyzing Safety of Smart Contracts", doi: 10.14722/ndss.2018.23082.
[50] A. T. Polcumpally, K. K. Pandey, A. Kumar, and A. Samadhiya, "Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions," *Heliyon*, vol. 10, no. 12, p. e32975, Jun. 2024, doi: 10.1016/J.HELIYON.2024.E32975.
[51] S. Keaney, P. Berthon, S. Keaney, and P. Berthon, "The Blockchain Trust Paradox: Engineered Trust vs. Experienced Trust in Decentralized Systems," *Information 2025, Vol. 16,* vol. 16, no. 9, Sep. 2025, doi: 10.3390/INFO16090801.