A Multi-Chain Approach to Transparent and Accountable Legislative Processes

Arianna Arruzzoli
University of Bologna
arianna.arruzzoli@studio.unibo.it

Mirko Zichichi
IOTA Foundation
mirko.zichichi@iota.org

Monica Palmirani
University of Bologna
monica.palmirani@unibo.it

Ludovico Papalia
University of Bologna
ludovico.papalia2@unibo.it

Chantal Bomprezzi
University of Bologna
chantal.bomprezzi@unibo.it

Stefano Ferretti
University of Bologna
s.ferretti@unibo.it

Abstract

This work proposes a multi-level blockchain architecture to support democratic principles in legislative processes. The system addresses three core requirements: separation of powers between legislative institutions, active stakeholder participation, and transparent decision-making. The architecture consists of three interconnected DLT levels: a Private Institutional Blockchain for internal operations, an Inter-Institutional Coordination Blockchain for cross-institutional communication, and a Public Legislative Blockchain for citizen transparency. The implementation utilizes Move language for smart contracts governing legislative procedures, Akoma Ntoso XML standard for document modeling and change tracking, and IOTA Identity framework for decentralized access control. The result is a system that balances institutional autonomy with public accountability in the legislative process.

Keywords: Deliberative Democracy, Multi-level DLT, Legislative Process

1. Introduction

Constitutional democratic governance is based on three fundamental principles: institutional separation of powers, representational inclusion of diverse societal voices, and promotion of civic engagement through governmental transparency [5]. The legislative process of democratic systems involves multiple institutions that operate under strict procedural frameworks while maintaining their independence. This requirement becomes increasingly complex when switching to digital systems [11].

Current digital legislative systems face a critical challenge: they typically operate within single institutions, failing to address the constitutional requirement for maintaining institutional autonomy while enabling inter-institutional coordination. Existing blockchain applications in governance focus primarily on individual institutions or general e-government services, overlooking the constitutional complexities inherent in multi-institutional legislative processes where separation of powers must be preserved.

The absence of unified document repositories, mandated by regulatory requirements and constitutional frameworks, creates significant inefficiencies in legislative workflows [3]. Manual document reconciliation across disparate platforms increases error rates, compromises traceability, and undermines transparency, which are fundamental democratic principles to guarantee. Italy's xLeges project [4], while innovative in its peer-to-peer approach using Certified Electronic Mail (PEC) and Uniform Resource Names (URN), demonstrates both the potential and limitations of current solutions.

This paper introduces the first multi-level blockchain architecture specifically designed to preserve separation of powers while digitalizing legislative processes. Our approach addresses the gap between constitutional requirements and technological implementation by proposing a three-tier system: a Private Institutional Blockchain for internal governance, an Inter-Institutional Coordination Blockchain for inter-agency procedures, and a Public Legislative Blockchain for citizen oversight [7]. Using Italy's constitutional framework as our primary case study, we demonstrate how distributed ledger technology can maintain institutional independence while enabling secure, transparent, and efficient legislative document management. While the Italian case study serves as a

URI: https://hdl.handle.net/10125/111662
978-0-9981331-9-5

representative example, we believe that the proposed solution can be readily applied to other countries and institutional governments.

The proposed architecture employs Move smart contracts [2] for encoding legislative protocols, Akoma Ntoso standards for structured legal document representation, and IOTA Identity framework for decentralized access control. This design ensures constitutional compliance, enhances democratic participation, and provides the foundation for more efficient legislative processes without compromising the fundamental principles of democratic governance.

The study reported in this paper tries to address the three critical research questions. **RQ1**: How can institutional autonomy be maintained within an integrated digital legislative system without compromising inter-institutional coordination requirements? **RQ2**: What mechanisms can ensure constitutional transparency obligations while preserving the confidentiality necessary for preliminary deliberative processes? **RQ3**: How can a (distributed) system architecture technically implement and enforce constitutional separation of powers principles?

Thus, our research contributions are threefold. First, we provide the first systematic analysis of constitutional requirements for digitalized legislative systems, mapping legal mandates to technical specifications. Second, we propose and implement a novel three-tier blockchain architecture that operationalizes separation of powers through technological design. Third, we demonstrate the practical applicability of our approach through a comprehensive case study of the Italian legislative framework, providing a replicable methodology for other constitutional democracies.

The remainder of this paper is organized as follows. In Section 2, we provide some background and motivation. Section 3 discusses the methodology we used to design our solution. Section 4 presents the multi-level system architecture. In Section 5, we focus on the implementation aspects related to the document management and access control policies. Section 6 reports on a qualitative evaluation and analysis of the implementation of the prototype system. Finally, Section 7 provides some conclusions and future works.

2. Background and Motivation

2.1. Blockchain in Democratic Governance

The application of blockchain technology to democratic governance has emerged as a significant research domain [12]. However, existing research predominantly focuses on single-institution implementations or general e-government applications, with limited attention to the constitutional complexities of multi-institutional legislative processes. Recent works explore blockchain applications in parliamentary contexts, focusing primarily on voting mechanisms and citizen engagement platforms [1].

The digitalization of governmental processes raises fundamental questions about how technological systems can preserve constitutional principles designed for analog institutional structures. Our approach is based on the idea of treating separation of powers as a foundational design requirement rather than an implementation detail. For this reason, the chosen approach is to develop a multi-tier architecture, which ensures the separation of document and information management in an independent and distinct manner, by design.

2.2. Technological Foundation and Security Considerations

The proposed multi-level blockchain architecture is built in the attempt to address the security and governance requirements of legislative processes, with the Italian Parliament as a use case example. The choice of Move used on top of the IOTA DLT, as the programming language for smart contract development, was driven by security and access control needs.

We claim that the use of a multi-tier blockchain approach offers significant advantages over alternative approaches to legislative digitalization [13]. A flat, single blockchain approach, while potentially simpler to implement, may compromise the principle of separation of powers, by creating metadata leakage through transaction visibility [6]. Even when robust encryption mechanisms are used to protect data content, all institutional actors can observe the transaction patterns, frequencies, and timing of legislative activities in different branches of government. This metadata exposure constitutes a form of information disclosure that can compromise the autonomy required for independent institutional operation, as it reveals operational patterns that could influence inter-institutional dynamics and compromise the deliberative process.

In contrast, the multi-tier architecture ensures complete transactional isolation between institutional layers while maintaining selective interoperability through controlled cross-chain communication protocols [10]. Although encryption is used at all levels for data protection, physical separation of permissioned blockchain networks prevents even metadata observation by unauthorized institutional actors. This approach preserves the constitutional requirement for institutional independence by ensuring that sensitive legislative processes remain completely opaque to external observers, including other government branches, except where constitutionally mandated disclosure is required.

Another possible solution is based on the use of a traditional encrypted database that, while offering simpler access management, introduces centralization in data control, creating potential points of failure and abuse. Moreover, centralized databases lack immutable audit trails and transparent verification mechanisms essential for democratic accountability.

2.3. Move Language: Enhanced Secure by Design Smart Contracts

Move is a (not so) novel programming language designed for blockchain environments, originally developed by the Diem (formerly Libra) project at Meta and subsequently adopted by various blockchain platforms including Sui, Aptos, Starcoin and IOTA.

Move language was designed to provide specific security controls not fully available in more traditional smart contract languages such as Solidity (security by design) [2]. The core philosophy of Move centers on the concept of ”resources”, rather than referring to the ”account-based model” typical of Solidity, for instance. Unlike conventional programming languages, where data structures can be freely copied, modified, or discarded, Move treats digital assets as linear resources that must follow strict ownership and lifecycle rules. This resource-oriented approach ensures that valuable digital assets (e.g., tokens or other valuable data) cannot accidentally be duplicated, lost, or destroyed due to programming errors The management of digital assets requires explicit authorization by data owners. This contrasts with Solidity, where assets are often represented as integers in mappings, making them susceptible to common vulnerabilities like accidental duplication, double-spending, or loss if not handled meticulously by the developer.

Moreover, Move has built-in mechanisms for managing resource ownership and access control. Modules in Move own their declared resource types, and only authorized code can manipulate specific assets. This limits potential attack vectors [9].

Move avoids the possibility of calling functions whose addresses are determined at run-time and restricts recursive external calls. This design choice significantly mitigates the risk of reentrancy attacks, a common and devastating vulnerability in Solidity.

These characteristics are particularly valuable in legislative contexts. The specific implementation of Move, used on top of IOTA blockchain technologies, enables native regulation of asset access, addressing the complex permission requirements inherent in legislative processes. Indeed, our approach makes use of document wrappers that create a structured environment where objects contained within wrappers are not directly accessible, enforcing object ownership policies at the protocol level.

This native access control mechanism is essential for maintaining the separation of powers principle, as it ensures that institutional actors can only access and modify documents and processes within their designated authority. Such a wrapper structure naturally implements the principle of least privilege, where each institutional actor has access only to the resources necessary for their specific legislative functions. More details are provided in the rest of the paper.

Finally, one of the main advantages of using a blockchain system based on Move, compared to ”classic” Solidity smart contracts architectures, is based on the use of Programmable Transaction Blocks (PTBs). A PTB is a temporary sequence of operations, orchestrated and executed atomically in a single transaction, which can be built dynamically on the client side, without the need to write and deploy a dedicated smart contract. A PTB can also interact with existing smart contracts, enabling the creation of complex orchestrations across multiple modules. Thus, functionally, the use of PTBs allows to build an interface that acts as a document editor, where modifiable legislative documents are managed in accordance with the specifications outlined herein.

3. Methodology

3.1. Research Process

Our research process for the design and implementation of the proposed system follows the methodology outlined in this section.

Step 1 - Problem Identification: Through an analysis of current digital legislative systems and constitutional requirements, we identified the fundamental tension between institutional integration and separation of powers in digital governance contexts.

Step 2 - Solution Objectives: We defined three primary objectives: (1) preserve constitutional separation of powers, (2) enable transparent democratic processes, and (3) facilitate efficient inter-institutional coordination.

Step 3 - Design: We designed a three-tier blockchain architecture utilizing Move smart contracts, Akoma Ntoso standards, and IOTA Identity framework, with each design decision validated against constitutional requirements.

Step 4 - Development and Demonstration: We implemented a functional prototype and demonstrated its application to Italian legislative procedures, showing how constitutional mandates translate into technical implementation.

Step 5 - Evaluation: We evaluated the architecture against constitutional compliance criteria, validating both legal and technological adequacy. At this level, the evaluation was primarily qualitative, using the experience of authors with a legal background. We plan to conduct a quantitative evaluation of the developed system in future work. The criteria for our evaluation are the following.

- Constitutional Compliance: The system must preserve separation-of-powers principles, while enabling necessary inter-institutional coordination.
- Technical Adequacy: The implementation must provide adequate security, performance, and reliability for real-world legislative applications.
- Transparency Enhancement: The system must improve citizen access to legislative information while respecting constitutional confidentiality.
- Practical Feasibility: The solution must be implementable within existing institutional constraints and technological capabilities.

3.2. Case Study Selection

We selected the Italian constitutional system as our primary case study for several methodological reasons. First, Italy's bicameral system with perfect symmetry between chambers provides a complex test case for multi-institutional coordination. Second, Italy's detailed constitutional provisions regarding parliamentary procedures offer specific technical requirements for privacy preservation. Third, Italy's existing xLeges initiative provides a baseline for comparison and demonstrates practitioner awareness of digitalization challenges.

The Italian case serves as an ”exemplar” to demonstrate the viability and generalizability of our approach, while providing specific implementation details necessary for validation and replication.

4. System Architecture

The architectural design leverages a multi-level approach to enable secure data exchange between different legislative bodies and committees, facilitating institutional cooperation without compromising the autonomy required by democratic governance principles. In particular, we employ three distinct yet interconnected blockchain layers, each designed to address specific constitutional and operational requirements of democratic legislative processes. A sketch of the system architecture is shown in Figure 1, where the three tiers of blockchains are shown.

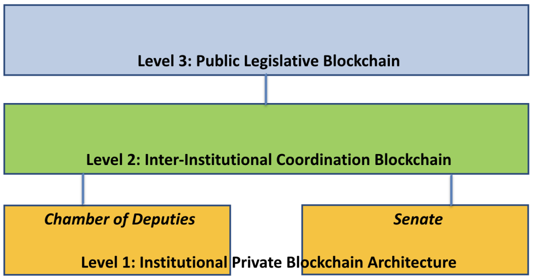
Level 3: Public Legislative Blockchain
Level 2: Inter-Institutional Coordination Blockchain
Chamber of Deputies
Senate
Level 1: Institutional Private Blockchain Architecture

Figure 1. System architecture.

4.1. Level 1: Private Institutional Blockchains

Each legislative institution operates within its dedicated, permissioned blockchain environment, ensuring complete autonomy over internal deliberative processes. Parliamentary committees, ministries, and specialized legislative offices maintain independent blockchain networks characterized by:

- **Governance Model:** Proof of Authority consensus mechanism with validator nodes exclusively managed by the respective institution, ensuring complete control over internal operations.
- **Content Management:** Comprehensive handling of working documents including draft legislation, preparatory reports, committee agendas, proposed amendments, and confidential meeting minutes. All documents are structured using Akoma Ntoso XML standard for semantic consistency and interoperability.
- **Access Control:** Strict restriction to authorized institutional members through the implementation of the IOTA Identity Framework, providing decentralized authentication while maintaining institutional boundaries.
- **Functional Purpose:** Support for internal deliberative workflows through Move smart contracts, enabling automated procedural compliance while preserving the confidentiality essential for preliminary legislative discussions.

This architecture preserves the fundamental deliberative autonomy of parliamentary democracy.

Constitutional scholars emphasize that legislative committees require confidential spaces for preliminary discussions, enabling a comprehensive debate of controversial proposals before they mature sufficiently for public consideration.

In Figure 1, we take the Italian Parliament as an example and show two blockchains as representatives of the Italian Chamber of Deputies and the Senate. This is a simplified view of a solution that takes into account the two main Parliamentary chambers, only. However, more sophisticated designs are possible in which multiple chains and tiers are used to handle the activities of internal committees and other representative bodies.

4.2. Level 2: Inter-Institutional Coordination Blockchain

The coordination layer implements a federated blockchain infrastructure managing formal document transmission and procedural coordination between distinct legislative institutions:

- **Governance Model:** Federated permissioned consensus with validator nodes distributed proportionally among participating institutions, ensuring that no single entity controls inter-institutional communications.
- **Content Management:** Official documents exchanged between institutions, including comprehensive metadata tracking the progress of legislative processes, verification of procedural compliance, and validation of constitutional checkpoints. Smart contracts manage the integration of document metadata and version control, specifically handling the integration of unique document identifiers and procedural timestamps. This on-chain metadata management ensures cryptographic verification of document authenticity and legislative progression tracking, while actual document text integration is handled off-chain to optimize costs and maintain system interoperability across different institutional platforms.
- **Access Control:** Participation limited to institutions with constitutional roles in the legislative process, with access permissions encoded in Move smart contracts reflecting legal mandates.
- **Functional Purpose:** Creation of immutable audit trails for formal inter-institutional exchanges, including transfers between legislative chambers, committee assignments, and executive communications.

This intermediate layer replicates the formal institutional procedures mandated by constitutional frameworks such as, for instance, Italy's bicameral system. Each transfer between the Chamber of Deputies and Senate, committee assignment, or governmental transmission creates permanent, verifiable records of institutional compliance with procedural requirements.

4.3. Level 3: Public Legislative Blockchain

The public layer serves as the authoritative repository for legislative acts requiring constitutional transparency and democratic accountability.

- **Governance Model:** Public-permissioned architecture with institutional validator nodes maintaining write authority while providing unrestricted public read access, ensuring transparency without compromising document integrity.
- **Content Management:** Definitive versions of promulgated legislative acts, official legal texts, and constitutionally mandated public documents, all structured according to Akoma Ntoso standards for semantic clarity and legal reference consistency.
- **Access Control:** Universal public read access with write permissions restricted to constitutionally authorized institutions, potentially automated through smart contract triggers upon official promulgation.
- **Functional Purpose:** Technological implementation of constitutional transparency requirements, providing citizens with immutable access to authoritative legislative texts while maintaining document authenticity.

This public blockchain embodies the constitutional principle of legislative transparency, serving as the digital equivalent of official government gazettes. The selective publication mechanism ensures that only documents meeting constitutional requirements for public disclosure are included, maintaining the balance between transparency and necessary institutional confidentiality.

4.4. Integration and Interoperability

The three-tier architecture leverages Move IOTA's native interoperability features to ensure seamless, yet controlled, interaction between layers. Cross-layer communication is governed by constitutional constraints encoded in smart contracts, preventing unauthorized access while enabling necessary institutional coordination. The wrapper-based object model ensures that sensitive institutional data remain protected, while allowing for the controlled sharing of information required for legislative processes.

This architectural approach addresses the fundamental challenge of digitizing legislative processes while maintaining constitutional separation of powers, ensuring that technological implementation reinforces rather than undermines democratic governance principles.

5. A Focus on the Access Control Implementation

In this Section, we will give some details on the implementation aspects of our solution, with emphasis on the document management and access control. Indeed, we think these are crucial issues that lead to the adoption of a Move on top of IOTA technological solution. In particular, our prototype implementation is based on the use of Document Wrappers and PTBs.

The wrapper-based access control mechanism inherent in Move IOTA provides selective visibility across the three-tier architecture. This ensures that sensitive institutional processes, such as those protected under Article 82 of the Italian Constitution regarding parliamentary immunity and confidential proceedings, remain appropriately restricted within their designated blockchain layer. Simultaneously, constitutionally mandated public acts maintain the necessary transparency and immutability through controlled publication on the public blockchain layer.

Move's resource-oriented programming model naturally supports hierarchical scalability. Documents are managed through controlled wrappers on appropriate tiers, reducing the risk of compromising official legislative records. The native access policies enforce that only authorized institutional actors can modify documents within their constitutional mandate, aligning with cyber-security best practices while preserving both integrity and confidentiality of legislative data.

5.1. Document Structure and Access Control

The system implements a layered document structure utilizing Move's wrapper pattern to encapsulate legislative documents within access-controlled containers. The core architecture separates document content from access permissions through the `DocumentWrapper` abstraction. Figure 2 shows a code snippet of the `request_doc()` function. It shows how a zero-trust security model can be implemented in Move through explicit authorization verification (`assert!` statement). The wrapper ensures that sensitive legislative documents remain inaccessible to unauthorized institutional actors, even within the same blockchain network.

```
pub fun request_doc(
    docWrapper: &mut DocumentWrapper,
    ctx: &mut TxContext ): VisibleDoc
{
    let sender = tx_context::sender(ctx);

    // Zero Trust Policy: Verify requestor
    // authorization. Execution aborts if
    // access is not allowed.
    assert!(manage_docs::is_allowed(
                docWrapper, &sender),
            EAccessNotAllowed);

    // If authorized, return document.
    manage_docs::get_visible(docWrapper)
}
```

Figure 2. Simplified code snippet of the `request_doc()` function.

5.2. Document Creation and Akoma Ntoso Integration

The document creation process integrates Akoma Ntoso ontological standards through structured metadata management. Each legislative document incorporates semantic identifiers that maintain legal traceability across institutional boundaries. Figure 3 shows a simplified related code snippet. The semantic structure distinguishes between the conceptual work (the legislative act itself) and its various expressions (different versions, languages, or amendments), ensuring that document relationships remain traceable throughout the legislative process while maintaining version integrity.

```
// Create a unique work IRI using Akoma Ntoso
// ontology standards. Combines country, document
// type, and timestamp for identification
let workIRI = akn_ontology::work::new(
    country_name, type_of_doc,
    clock.timestamp_ms()
);

// Generate expression IRI to track document
// versions. Links to the work IRI and indicates
// if this is the current version
let expressionIRI =
    akn_ontology::expression::new(
        is_current_version
    );

// Create the document object with all required
// metadata. Binds together identification,
// content hash, and Akoma Ntoso IRIs
let doc = manage_docs::doc::new(
    ctx, identifier, document_hash,
    workIRI, expressionIRI
);
```

Figure 3. Simplified code snippet for the initialization of a document ('doc') and creation of its associated IRI.

The integration of the Akoma Ntoso standard [8] with Move's type system creates a robust framework for maintaining semantic clarity between authoritative legislative texts and interpretive metadata. Move's resource model ensures that legal content and annotations remain structurally distinct within the blockchain architecture, preventing unauthorized modifications to official legislative documents while enabling controlled access to supplementary information.

This separation proves essential for upholding constitutional separation of powers, as Move's ownership policies automatically enforce the neutrality of legislative texts. Annotations and interpretive content, which may reflect subjective institutional perspectives, are managed through separate wrapper structures that prevent interference with the authoritative legal corpus. The smart contract implementation in Move ensures that only constitutionally authorized institutions can modify specific document components, maintaining the impartiality required by democratic legislative processes.

5.3. Version Control and Legislative Continuity

The system implements version control mechanisms that preserve legislative document lineage while enabling institutional modifications. The `save_new_version` function, shown in Figure 4, demonstrates how constitutional procedures are encoded into the smart contract logic. This approach ensures that only constitutionally authorized institutions can modify legislative documents while maintaining an immutable audit trail of all changes. The wrapper-based access control prevents unauthorized modifications while enabling legitimate institutional collaboration.

5.4. Identity-Based Authorization

The system integrates decentralized identity management, through the `intelligible_identity` module, enabling institutional actors to maintain autonomous control over their document access policies. The identity-based authorization is currently implemented via the IOTA Identity framework, and it ensures that access permissions reflect constitutional mandates rather than arbitrary administrative decisions. This solution allows for a separation of powers by making unauthorized access computationally impossible, rather than merely administratively restricted.

```
// Creates a new version of an existing
// document with proper authorization
// checks. Maintains version history
// and links to the parent document
pub fun save_new_version(
    parent_doc: &mut DocumentWrapper,
    ctx: &mut TxContext,
    people: vector<Identity>,
    document_hash: vector<u8>,
    // ... additional parameters
)
{
    // Extract the transaction sender for
    // authorization
    let sender = tx_context::sender(ctx);
    // Zero Trust Policy: Verify caller
    // authorization. Execution aborts if
    // access is not allowed.
    assert!(
        manage_docs::is_allowed(
            parent_doc, &sender),
        EAccessNotAllowed
    );

    // Get reference to the current document
    // version.This will become the parent
    // of the new version
    let old_doc = parent_doc.get_doc();

    // Create new document version with
    // version chain linkage
    // Inherits work IRI but gets new
    // expression IRI for versioning
    let new_doc =
        manage_docs::doc::new_version(
           ctx, identifier, document_hash,
           workIRI, expressionIRI, old_doc
    );
}
```

Figure 4. The `save_new_version` function handles the creation of a new document version. It enforces a "Zero Trust" policy to ensure the sender's authorization before creating the new version.

Currently, documents are stored on-chain in a format where the Akoma Ntoso IRI are integrated with the blockchain address identifiers. Moreover, the code structure has been designed to allow for future integration with the Intelligible Decentralized Identity system developed in [**zichichi2022**].

6. System Validation and Discussion

6.1. Constitutional Compliance Assessment

We evaluated our architecture against key constitutional principles using a systematic compliance framework developed through legal analysis. Table 1 presents an assessment of constitutional compliance with key democratic principles. Each row identifies a specific principle (derived from the Italian Constitution) and maps it to a corresponding technical implementation within the multi-layered system. The architecture is designed in three layers, each serving a specific constitutional function. Layer 1 ensures Institutional Autonomy by deploying private blockchains governed independently by each institution. Layer

2 facilitates Inter-institutional Coordination through a federated blockchain model that respects proportional representation and collaborative governance. Layer 3 guarantees Public Transparency via a public blockchain with universal read access, enabling citizens and external stakeholders to audit institutional actions. Additional mechanisms, such as wrapper-based access control and smart contract encoding of constitutional procedures, address Institutional Confidentiality and Procedure Compliance, respectively.

The system is designed to accommodate potential regulatory changes through a flexible integration of structured legal standards and programmable logic. In particular, the use of the Akoma Ntoso XML format facilitates the identification and modeling of normative updates, while the architecture supports the translation of such changes into procedural logic. In the case of IOTA Move, smart contracts can be upgraded by maintaining the previous version on-chain (as it remains immutable) and updating the references so that they point to a new version of the code. Institutional users can adopt the updated version in an opt-in manner, either by upgrading their own smart contracts or by adapting their off-chain software accordingly.

In addition, the framework is extensible, making it feasible to accommodate structural modifications, such as changes in the number of committees or the organization of legislative offices.

6.2. Cost Efficiency Considerations

Legislative digitalization efforts often suffer from fragmented systems, lack of interoperability, redundant data entry, limited process oversight, and exposure to cybersecurity threats, all of which contribute to significant operational costs. The proposed multi-tier architecture addresses these inefficiencies by introducing a unified framework for document management, procedural automation, and secure access control. While a detailed cost analysis is beyond the scope of this study, the system is designed to reduce the cumulative burden associated with legislative production through improved coordination, traceability, and resilience.

6.3. Threat Model and Security Risk Analysis

We used a systematic threat modeling specifically adapted for governmental blockchain systems, considering the unique security requirements of legislative processes. We identified three primary threats to constitutional integrity and institutional trust:

1. **External adversaries** seeking to compromise legislative integrity.
2. **Malicious insiders** attempting to exceed their constitutional authority.
3. **Institutional actors** aiming to violate the principle of separation of powers.

These threats are systematically addressed through a layered security risk analysis, as summarized below. Each identified risk corresponds to one or more of the above threats and is mitigated through targeted technical mechanisms embedded in the system design.

- **Cross-chain privacy breaches:** This risk, primarily associated with external adversaries, involves the potential exposure of sensitive institutional data across blockchain boundaries. It is mitigated through wrapper isolation and metadata separation at the protocol level.
- **Institutional authority escalation:** Linked to malicious insiders, this risk concerns actors exploiting the system to exceed their constitutional powers. It is prevented through the Move language's resource ownership model and the encoding of constitutional constraints directly into smart contracts.
- **Document integrity attacks:** Relevant to both external adversaries and insiders, this risk involves unauthorized modification or corruption of legislative documents. It is eliminated through cryptographic integrity verification and immutable audit trails.
- **Unauthorized access attempts:** This risk, tied to both external and internal threats, targets confidential legislative proceedings. It is blocked through the integration of the IOTA Identity framework, which enforces role-based permissions aligned with constitutional roles.
- **Metadata inference attacks:** This risk involves deriving sensitive information from transaction patterns. It is addressed through the physical separation of blockchain networks and encrypted inter-chain communication.

6.4. Validation and Compliance Testing

We tested our smart contract implementation to validate constitutional compliance and system behavior. The testing suite included unit tests for individual smart contract functions, integration tests for cross-chain communication protocols, and end-to-end workflow tests that simulate complete legislative procedures. All tests confirmed that the system behaves according to constitutional requirements and prevents unauthorized operations.

To assess the viability of our implementation,

Table 1. Constitutional Compliance Assessment Matrix

Constitutional Principle	Technical Implementation	Compliance Status
Institutional Autonomy	Private institutional blockchains with independent governance (Layer 1)	✓ Fully Compliant
Inter-institutional Coordination	Federated coordination blockchain with proportional representation (Layer 2)	✓ Fully Compliant
Institutional Confidentiality	Wrapper-based access control preventing external observation	✓ Fully Compliant
Public Transparency	Public blockchain with universal read access (Layer 3)	✓ Fully Compliant
Constitutional Procedure Compliance	Smart contract encoding of constitutional procedures	✓ Fully Compliant
Regulatory Adaptability	Integration of structured legal standards (Akoma Ntoso) and support for smart contract upgrades via IOTA Move, enabling opt-in adoption of updated procedural logic	○ Practicably Compliant

Cost Component	Create New Document	Save New Version	Request Document
Storage Cost	0.0058412	0.005092	0
Computation Cost	0.001	0.001	0.001
Total Gas Fee	**0.0068412**	**0.006092**	**0.001**

Table 2. Transaction gas costs expressed in IOTA tokens (0.001 is the minumum network computation cost).

we conducted performance testing focusing on gas consumption for the three primary functions that interact with the off-chain and interface layers. Table 2 presents the results for three core operations, i.e., creating new documents, saving document versions, and requesting document access. The performance testing scenario involved documents with nine authorized identities (representing institutional actors with access rights), legislative text of 129 words processed through SHA-256 hashing to produce a 256-byte vector, and complete Akoma Ntoso IRI metadata components. This configuration represents a realistic legislative document scenario with multiple stakeholders and comprehensive semantic markup. The cost structure is as follows. *Storage Cost* represents the expense of writing or updating data on the blockchain, constituting the primary cost component for document creation and modification operations. *Computation Cost* reflects the computational resources required to execute smart contract logic, remaining constant at 0.001 IOTA across all operations. *Computation Cost Burned* represents anti-spam protection mechanisms, permanently removing tokens from circulation to prevent network abuse. *Storage Rebate* provides cost recovery when transactions complete successfully, significantly reducing the net cost of read operations. *Non-refundable Storage Fee* covers permanent network storage costs, appearing as zero in our test scenarios.

The results demonstrate that computational costs remain fixed at minimal levels (0.001 IOTA), indicating that the Move smart contract logic for constitutional compliance checking and procedural validation imposes negligible overhead. As expected, storage costs represent the primary variable expense, reflecting the blockchain's resource allocation for permanent document storage. Performance characteristics validate the economic feasibility of the proposed architecture for real-world legislative applications. The low transaction costs allow frequent document access without prohibitive expenses, while the storage cost structure appropriately reflects the permanent archival nature of legislative records. These results support the system's scalability for institutional deployment, particularly considering that legislative document volumes, while constitutionally significant, remain manageable compared to high-throughput commercial blockchain applications.

7. Conclusions

This paper presented a novel multi-level blockchain architecture designed to digitale legislative processes while preserving the constitutional principle of separation of powers. Our three-tier system demonstrates how distributed ledger technologies can be of help in order to solve the trade-off between the demand of institutional autonomy, on one side, and inter-institutional coordination in democratic governance, on the other side. Our work is based on the integration of Move smart contracts, Akoma Ntoso standards, and IOTA Identity framework. In the paper, we focus on a case study implementation, based on the Italy's legislative context, that validates the practical applicability of our approach. The system offers a secure, transparent, and constitutionally compliant foundation for legislative digitalization. The proposed model bridges the gap between constitutional mandates and technical implementation, offering a replicable framework for digital governance in multi-institutional contexts. The Italian case study serves as a representative exemplar, illustrating both the feasibility and generalizability of our approach.

We are aware of various practical challenges that may hinder the effective implementation of the proposed system in real-world institutional settings. Potential barriers to adoption include institutional inertia, the need for specialized training, and integration with legacy systems. While many legislative institutions still rely on paper-based or fragmented digital systems, the proposed architecture is designed to support (gradual) migration toward a unified digital framework. The use of Akoma Ntoso standards enables semantic modeling of legacy documents, facilitating their integration into the blockchain-based system. Moreover, the modular and layered design allows institutions to adopt the system incrementally, if needed, minimizing disruption and enabling tailored migration strategies based on institutional readiness.

In future work, we will conduct a performance evaluation to assess the system's scalability, reliability, and latency characteristics under realistic legislative workloads. Additional work may include expanding the framework, investigating advanced privacy-preserving mechanisms for sensitive legislative documents.

8. Acknowledgments

This project is conducted with the support of the European Commission funds within ERC HyperModeLex. Grant agreement ID: 101055185.

References

[1] Patricia Baudier et al. "Peace engineering: The contribution of blockchain systems to the e-voting process". In: *Technological Forecasting and Social Change* 162 (2021), p. 120397. DOI: https://doi.org/10.1016/j.techfore.2020.120397.

[2] Sam Blackshear et al. *Move: A language with programmable resources*. 2019.

[3] Primavera De Filippi, Morshed Mannan, and Wessel Reijers. "The alegality of blockchain technology". In: *Policy and Society* 41.3 (Feb. 2022), pp. 358–372.

[4] Luca De Santis et al. "The x-leges system: peer-to-peer for legislative document exchange". In: *Proc. of the 5th International Conference on Electronic Government*. EGOV'06. Kraków, Poland: Springer-Verlag, 2006, pp. 231–242. DOI: 10.1007/11823100_21.

[5] Oonagh Gay and et.al. "Watchdogs of the Constitution - the Biters Bit?" In: *Constitutional Futures Revisited: Britain's Constitution to 2020*. London: Palgrave, 2008, pp. 197–214. DOI: 10.1057/9780230595088_12.

[6] Stefano Loss, Nelio Cacho, and Frederico Lopes. "Blockchain Strategy for Multi-level Interoperability in Public Safety Scenario". In: *Proc. of Cyber-Physical Systems and Internet of Things Week 2023*. CPS-IoT Week '23. New York, NY, USA: ACM, 2023, pp. 307–312. DOI: 10.1145/3576914.3588020.

[7] Monica Palmirani et al. "Multi-level Architecture for Separation of Powers in Legislative Process". In: *Proc. of the 7th Distributed Ledger Technology Workshop (DLT 2025)*. CEUR WS Proc. Pizzo, Italy, June 2025.

[8] Vitali Fabio Palmirani Monica. "Akoma-Ntoso for Legal Documents". In: *Legislative XML for the Semantic Web: Principles, Models, Standards for Document Management*. Dordrecht: Springer, 2011, pp. 75–100. DOI: 10.1007/978-94-007-1887-6_6.

[9] R. E. Spiridonov. "Restricted Move – a Smart Contract Description Language to Create and Control Finance Instruments on DFinance Blockchain Platform". In: *Journal of Physics: Conf. Series* 1864.1 (May 2021), p. 012109. DOI: 10.1088/1742-6596/1864/1/012109.

[10] Qaiser Abbas Tahir Alyas. "Multi blockchain architecture for judicial case management using smart contracts". In: *Sci Rep 15* (2025). DOI: https://doi.org/10.1038/s41598-025-92842-8.

[11] Wim Voermans, Hans-Martien ten Napel, and Reijer Passchier and. "Combining efficiency and transparency in legislative processes". In: *The Theory and Practice of Legislation* 3.3 (2015), pp. 279–294. DOI: 10.1080/20508840.2015.1133398.

[12] Lu Zhang and et el. "A Systematic Review of Blockchain Technology for Government Information Sharing". In: *Computers, Materials and Continua* 74.1 (2022), pp. 1161–1181. ISSN: 1546-2218.

[13] Mirko Zichichi et al. "Data governance through a multi-DLT architecture in view of the GDPR". In: *Cluster Computing* 25.6 (Dec. 2022), pp. 4515–4542. DOI: 10.1007/s10586-022-03691-3.