This is the final peer-reviewed accepted manuscript of:

Implementing Role-Based Access Control through Multi-Layered Blockchain Solutions

Conference Proceedings: 2026 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), March 16-20, 2026, Pisa, Italy.

Author: Arianna Arruzzoli; Stefano Ferretti; Mirko Zichichi; Ludovico Papalia; Chantal Bomprezzi; Monica Palmirani

Publisher: IEEE

The final published version is available online at:
https://doi.org/10.1109/PerComWorkshops68308.2026.11585484

Rights / License:

© 2026 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website:

https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/author_version_faq.pdf

This item was downloaded from the author personal website (https://mirkozichichi.me)

When citing, please refer to the published version.

Implementing Role-Based Access Control through Multi-Layered Blockchain Solutions

Arianna Arruzzoli[1], Stefano Ferretti[2], Mirko Zichichi[3], Ludovico Papalia[4], Chantal Bomprezzi[4], Monica Palmirani[4]
[1]CIRSFID, University of Bologna, via Galliera 3, 40121 Bologna, Italy
[2]Department of Computer Science and Engineering, University of Bologna, Mura Anteo Zamboni 7, 40126 Bologna, Italy
[3]IOTA Foundation, Pappelallee 78/79, 10437 Berlin, Germany [4]ALMA-AI, University of Bologna, via Galliera 3, 40121 Bologna, Italy
{arianna.arruzzoli2, s.ferretti, ludovico.papalia2, chantal.bomprezzi, monica.palmirani}@unibo.it, mirko.zichichi@iota.org

***Abstract*—In recent years, a multitude of applications has emerged, each characterized by varying levels of privacy requirements and transparency management. To address these heterogeneous demands, multi-layered solutions leveraging blockchain technologies have been developed. Within these scenarios, data access management emerges as a critical concern. Solutions often incorporate access control lists and authorization mechanisms to regulate permissions, taking into account different roles and hierarchical structures. This results in a complex architecture, which in turn implies a challenging implementation process. Multi-layered solutions differ substantially from conventional decentralized applications (dApps), allowing for more granular control, modularity, and adaptability in systems where privacy, transparency, and role-based access are pivotal considerations. However, their implementation can be facilitated by the Move language and the diverse paradigms of alternative blockchain architectures. This paper presents a key example of how these technologies and architectural approaches can enhance security and access control over resources in sensitive contexts, such as legislative processes. Using the Italian Parliament as a case study, the paper outlines a multi-layered architecture designed in compliance with constitutional principles and ensuring the separation of powers. The architecture is implemented defining documents as the primary assets, employing the Akoma Ntoso XML standard for document identification and the IOTA Identity framework for decentralized access control.**

***Index Terms*—Multi-Layer Architecture, Access Control, Legislative Process**

I. Introduction

In the past decade, the adoption of blockchain technology has expanded considerably, leading to a diverse range of use cases. Its inherent properties and characteristics have been studied, enabling the development of numerous applications across the globe. Spreading from the finance sector to markets such as gaming, healthcare and public administration, blockchain technology has become increasingly well-understood and is being applied in a variety of contexts. A wide range of applications that leverage the unique properties of decentralized technologies has been developed, being commonly referred to as decentralized applications (dApps). DApps employ blockchain technology for data storage and processing, ensuring decentralization at their core, even though they are still functioning in ways that resemble traditional centralized applications. Recently, however, there has been a growing trend toward enhancing decentralization by using blockchain to develop multiple layers and modular components [1]–[3], enabling the implementation of specialized functions to address specific tasks. In this context, these advances place greater emphasis on resolving the challenges of data protection and access control. Different user hierarchies may require or be permitted to access distinct resources or modules, making the design of robust access control mechanisms that uphold both privacy and security a central concern in contemporary blockchain development.

This trend has aligned well with the emergence of innovative blockchain structures introduced in recent years on the market. These novel blockchains are diverging from the traditional blockchain architecture, as implemented in Ethereum or in Bitcoin. Considering the case of Sui, which employs an object-oriented structure [4], or the example of IOTA with its Tangle [5], we have the possibility to observe on the market different implementation of the same technologies, each exploring improved efficiency for distinct yet interrelated tasks. These innovative structures offer a range of novel technologies and mechanisms that can substantially enhance the design and implementation of access control policies for digital resources.

The purpose of this paper is to present and examine the implementation of a multi-layer architecture for the separation of powers in a legislative context, with the aim of highlighting the tools and design choices that ensure access control, transparency, and the effective separation of powers in a jurisdictional context.

The paper is structured as follows. It will first present the background in Section II and the use case of the proposed multi-layer architecture in Section III. Then, the implementation decisions made during development are examined in Section IV, addressing both the tools and design patterns adopted, and detailing the technologies employed throughout the process. Section V presents some results from a preliminary evaluation of the system prototype, while Section VI provides some concluding remarks.

II. Background

A. Move language for Security by Design

Move is a programming language designed specifically for use in blockchain environments. It employs a resource-oriented paradigm, which makes it particularly suitable for distributed ledger applications. Its design facilitates a natural and structured approach to managing state and behaviour associated with assets, users, and contracts, enabling intuitive modeling of complex data structures and interactions. Due to these characteristics, Move has been integrated into both the Sui and IOTA blockchains, where its design principles align well with the respective architectures and offer distinct advantages for their operational models.

The Move language derives its foundations from the Rust programming language. Therefore, it inherits a strong em-

phasis on safety and resource management. The language incorporates rigorous checks on the use of resources to prevent vulnerabilities arising from programming errors, ensuring a high degree of reliability and security in decentralized environments. The integration of Move into the Sui ecosystem has led to the development of Programmable Transaction Blocks (PTBs), which function as atomic transactions capable of encapsulating multiple operations within a single execution, providing better flexibility and a powerful tool for programmers [6]. Indeed, PTBs enable direct interaction with on-chain smart contracts and allow developers to design and implement complex yet economically efficient transactions to engage with the system.

B. Blockchain in the Legal Context

Blockchain technology is intrinsically linked to the legal context [1]. By definition, blockchain is a consensus-driven distributed ledger, as it contains immutable data approved by different actors before the information is recorded in the ledger. These properties have led to consider blockchain as a suitable technology within the legal context, used to secure and enforce digital agreements [7]. Relying on the technology's core features of security and immutability, blockchain applications aim to streamline dispute resolution. Furthermore, the transparency and integrity inherent in blockchain technology align conceptually with the need for democratically underpinned procedures as a basis for decision legitimacy.

C. Legal Foundation and Motivation for the Use-Case Study

Modern democracies are founded on three essential pillars: (i) the inclusive representation of diverse social interests; (ii) the separation of legislative, executive, and judicial powers; (iii) the active participation of citizens in public life. The latter principle, in particular, translates into the need to ensure transparency from the institutions. Transparency also serves to uphold the separation of powers, as it enables participation and oversight of governmental actions by the broad spectrum of actors involved, both institutional and non-institutional.

Current digital systems employed by public institutions do not fully operate in accordance with constitutional principles. Although these systems offer significant efficiency gains, they do not entirely meet the constitutional requirement of safeguarding institutional autonomy while ensuring inter-institutional coordination. The absence of unified document repositories, as mandated by regulatory requirements and constitutional frameworks, creates meaningful inefficiencies in legislative workflows [1]. Indeed, the decentralization measures adopted to preserve the separation of powers introduce significant challenges in achieving an appropriate balance between institutional autonomy and effective inter-institutional coordination. Consequently, digital legislative systems effectively address some procedural requirements while not fully satisfying others, creating a potential risk of misalignment with the constitutional foundations of the legislative process.

Within this context, the study focuses on the framework of Italy's legislative process. This choice is motivated by several methodological considerations; nonetheless, the design of the proposed architecture is modular and may be adapted with ease to other countries and institutional systems [8]. The Italian parliament is defined as perfect bicameralism, since the two chambers are endowed with the same functionality. This configuration offers a complex scenario and serves as a perfect test case for multi-institutional coordination. Furthermore, Italy's constitutional provisions regarding parliamentary procedures offer specific technical requirements regarding access control and privacy preservation.

D. State of the Art

The state of the art in Italy is represented by xLeges, a decentralized system developed via Web Services. The system relies on Certified Email (Posta Elettronica Certificata - PEC) to ensure accountability, and employs Uniform Resource Names (URNs) for traceability. Within the xLeges system, each institution functions as an autonomous node in the network. This design guarantees institutional autonomy, facilitating the necessary coordination through standardized document formats and communication protocols. Despite the decentralization achieved through these particular design and implementation choices, the system presents certain inefficiencies related to information consistency. The data are partitioned without the support of a unified repository for access, resulting in an inefficient process for retrieving information. In order to provide an alternative and innovative solution to these problems, a multi-layer approach has been applyed to design a novel system architecture, enabling secure data exchange between different legislative committees, facilitating institutional cooperation without compromising the autonomy required by constitutional principles.

III. Multi-Layer Architecture

Within the legislative context, the process of digitalization is particularly complex. This complexity arises not only from the need to ensure high standards of security and integrity but also from the requirement to incorporate, within the implementation criteria, fundamental legal principles derived from the respect for democratic governance. In order to respect the constitutional foundation within the legislative process, a multi-layered architecture has been designed, combining different types of blockchains to address distinct functionality and governance requirements.

The first layer consists of a **Private Institutional Blockchain**, where each institution owns an indipendent system, functioning as an isolated module, allowing commissions to deliberate privately before reaching a formal agreement on the drafting of the text. Within this context, the blockchain employed is a private permissioned, with a consensus mechanism restricted to the validator nodes specific to each institution. During the drafting of the text, not all members of the institution are permitted to access the same documents; therefore, a hierarchy of roles has been incorporated into the architecture. The implementation of these hierarchies through IOTA Identities makes it possible to define constraints and authorization

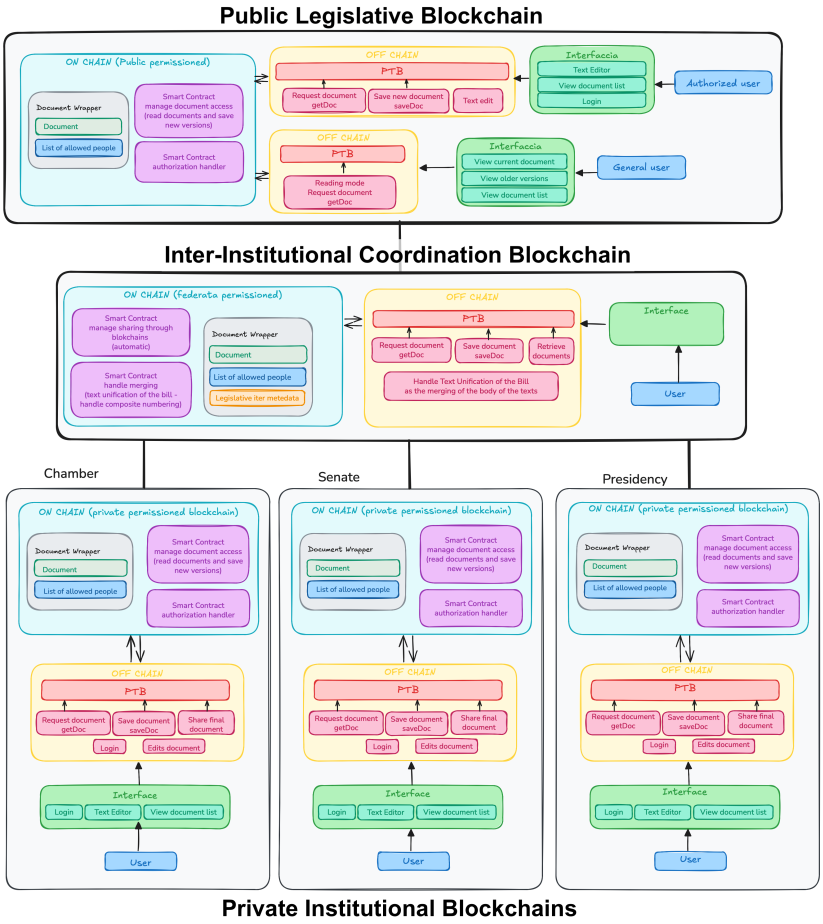


Fig. 1. Complete architecture design

policies that effectively leverage Move's resource-management logic. The details of this implementation are discussed further in Section IV-B.

Once a document is ready to be examined by the other chamber, individual institutions share their work to enable the assembly to review their actions and, if necessary, modify specific portions of the text. This is achieved through the second level: the **Inter-Institutional Coordination Blockchain**. This second level serves as the core of the architecture, as it formally replicates the institutional steps of the Italian legislative process, enabling the construction of a single, unified, and distributed ledger with immutable information via a federated permissioned blockchain.

A federated permissioned blockchain allows for the simultaneous utilization of features from both public and private blockchains, enabling read operations by many participants while restricting write operations to a limited number. Compared to the current state of the art, this level would replace the services currently offered and implemented by xLeges. Furthermore, this intermediate level functions as a central repository for potential legislative exchange of draft laws. Internal smart contracts manage the unification of document identifiers and the updating of metadata, while the off-chain logic is responsible for consolidating proposed texts and ensuring that any modifications result in a coherent and harmonized final document.

Upon the conclusion of the legislative deliberation by the chambers, the texts are submitted to the review of the President of the Republic for potential promulgation. Once promulgated, they are published in the Official Gazette. For the publication of these texts, the relevant information is transmitted to the third level, the **Public Legislative Blockchain**, which is built on a public-permissioned blockchain with institutional validator nodes and public read nodes. The use of a public blockchain embodies the constitutional principle of transparency of legislative acts.

Each layer is designed with respect to the Italian legislative iter, implementing the requirements specified by law via different types of blockchains. The primary assets on the blockchain are the documents produced and shared by each institution. These documents are governed by specific access policies that must be enforced. To manage such policies, a

hierarchical identity structure was implemented, allowing for the straightforward definition and application of differentiated authorization rules. PTBs are employed in the architecture to facilitate interaction between on-chain and off-chain logic, thereby enabling users to engage directly with the blockchain system. Moreover, they support interoperability between Private Institutional Blockchains and the Inter-Institutional Coordination Blockchain.

IV. Implementation

The architecture is designed to uphold constitutional principles while ensuring efficient and secure communication among the various components within each layer. The technologies have been selected in accordance with this architectural design, leveraging their specific characteristics to enhance security alongside a faster and more seamless user experience. The architecture has been developed using Move IOTA, which offers specific features that support the creation of a robust and well-structured framework.

The on-chain logic of the architecture has been developed using smart contracts in Move for access control and document storage. The Move programming language provides design patterns such as Wrapped Objects, which facilitate the incorporation of Security by Design principles into the system, hiding the objects from the blockchain.

A. Document and Document Wrapper

Documents constitute the core of the proposed architecture due to their central role throughout the entire legislative process. The Document entity is initially conceived as a legislative initiative, with the potential to evolve into a bill draft. However, given the intended use of blockchain technology, particularly for its traceability features, the Document entity has been abstracted to accommodate and encapsulate any type of document that can be described and defined through an Akoma Ntoso International Resource Identifier (IRI) [9].
In order to enhance security, the concept of Wrapper [10], as defined within the Move IOTA framework, has been employed to prevent the Document from being directly exposed on the blockchain. By definition, the Wrapper encapsulates the Document ID, such that the Document no longer exists independently on-chain. Ownership of the Document is thus transferred to the Wrapper, reinforcing the overall security of the system. Since access to the information is intended to be restricted solely to authorised individuals, this structure enables the integration of both the document and the list of permitted users into a single entity. Therefore, the Document Wrapper entity is introduced, enabling verification of the identity of the transaction sender and preventing any unauthorised access to non-public information. This is achieved by embedding multiple checks within each callable function, defining continuous validation of the sender's identity against the list of authorised entities, in accordance with the Zero Trust security paradigm. Some snippet of the code is provided in Figure 2. Through this pattern, the ownership of the Document is assigned to the DocumentWrapper, ensuring that all access to the Document is mediated through the smart contracts governing the DocumentWrapper. Through this mechanism, we can ensure that only the authorised people can operate on it via the smart contracts regulations.

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

    // Zero Trust Policy: Verify 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)
}
```

Fig. 2. Simplified code snippet of the function to access the document.

B. IOTA Identities

IOTA Identities consist of Decentralised Identifiers (DIDs), which adhere to the W3C specification, and Verifiable Credentials. DIDs enable any entity to possess a unique identifier for which they can prove ownership. Through the development of the DID document, IOTA focuses on implementing mechanisms that ensure identity holders maintain control over the selective disclosure of their information. Verifiable Credentials, on the other hand, are digitally signed assertions issued by trusted third parties regarding a specific identity; they serve to verify identity claims and ensure that the published data is controlled and trustworthy. When combined altogether, these components provide an efficient and robust implementation for verifiability. IOTA Identities are implemented as Move shared objects. Due to its nature as an object, it is possible to implement hierarchical structures that define who holds authority over the identity, while preserving the privacy of the indented users.

C. Programmable Transaction Blocks (PTBs)

The Sui network introduced Programmable Transaction Blocks (PTBs), incorporating them as foundational components, considering all transactions natively defined as PTBs. This implementation provides developers a versatile tool that improves both scalability and composability [11]. As previously introduced, PTBs are commands that allow the execution of multiple actions within a single event. This capability of executing multiple transactions, within the same request, enhances efficiency and reduces gas fees compared to processing individual transactions. Indeed, PTBs can perform up to 1,024 unique operations in one execution, instead of typically requiring 1,024 individual executions on traditional blockchains [12].

The PTB executes actions sequentially, and through the use of nested transactions, results from previous actions can be employed as parameters in subsequent operations. As highlighted in [13], nested transactions constitute a fundamental

primitive required for the correct and composable execution of blockchain transactions.

Finally, the effects of the actions are applied atomically, thus preventing inconsistent states and partial failures in blockchain transactions.

PTBs offer significant advantages for blockchain development, enabling developers to implement complex interactions and, consequently, to encapsulate certain aspects of smart contract logic within the PTB. Furthermore, the execution of multiple operations within a single PTB generally results in lower gas fees compared to executing the same operations through individual transactions. Indeed, the primary advantage is the amortization of transaction fees, which, although seemingly modest, follows a linear distribution and consequently exerts a cumulative effect over the long term. PTBs can offer more stable and predictable costs for publishing on the network. In Ethereum, the base fee is influenced by network congestion, which is a consequence of its underlying structure and consensus mechanism, resulting in a more volatile fee moving over a wide range. In contrast, Sui and IOTA exhibit highly predictable transaction costs when PTBs are employed, as their fees are based on the computational resources required and take into account a storage refund when storage space is released [14], [15].

Although they constitute highly useful and efficient tools, their implementation remains in an early stage of adoption. Their current implementation is relatively rudimentary, as they operate exclusively with primitive data types. Consequently, the primary challenges associated with their integration involve adapting the technology to support more complex structures that are represented on-chain. The fundamental structure of PTBs consists of inputs and commands. Inputs refer to raw values or objects, whereas commands involve different actions among invoking various modules within the same transaction. These modules enable the use of different user-defined functions and allow complex objects to be employed as arguments.

Within the proposed architecture, PTBs play a significant role. They function as the primary conduit through which each layer communicates with its own on-chain module, allowing the system to translate user intent into structured, verifiable actions. Through PTBs, complex transactions can be composed and executed, enabling users and system components alike to engage in intricate operations. At the architectural level, PTBs also serve as the bridge that share information securely and consistently across layers, ensuring that documents are conveyed with integrity. Thus, PTBs become the mechanism that maintains both the structural coherence and the communication throughout the system.

In particular, in our implementation we employed two specific PTBs already defined by Sui and IOTA versions of their integration of Move language within their blockchains. The designed PTB is a sequence of nested transactions that involve two main commands, i.e., *MoveCall* and *MakeMoveVec* [12]. The *MoveCall* command allows the execution of user-defined functions already published inside the blockchain. *MakeMoveVec* creates a vector of Move values, used to construct vectors of Move values as arguments for MoveCall. Such PTB thus allows to store and update complex documents into an atomic transaction. Figure 3 shows a simplified PTB that invokes the update function to grant access to a document (here referred as *@0xddd*) for two different identities (formally *@0xaaa* and *@0xbbb*).

```
iota client ptb
  --make-move-vec "<address>" "[@0xaaa, @0xbbb]"
  --assign vec_identities
  --move-call "<PackageName>::manage_documents::save_new_version"
  @0xddd
  vec_identities
```

Fig. 3. Simplified code snippet of a PTB that creates the identites vector and update the *@0xddd* document to grant them access

D. Security Context and Anticipated Threat Scenarios

Given the sensitivity of the data involved in the use case and the high level of confidentiality required by the operational context, the multi-layer architecture has been conceived with the explicit assumption that malicious actors and hostile actions may arise. This assumption shaped the overall design process and directed the integration of security mechanisms from the very beginning.

Among the risks identified, particular concern is devoted to threats that may undermine constitutional integrity and institutional trust, being the core assets that the architecture is, by design, intended to safeguard. The primary threats identified concern external adversaries attempting to compromise legislative integrity, malicious insiders seeking to act beyond their constitutional authority, and institutional actors whose actions may jeopardize the separation of powers.

To establish an initial layer of defense against these threats, the system integrates a range of technical mechanisms within its architectural design. To prevent unauthorized exposure, each document is encapsulated within a wrapper that enforces authorization and access control at the protocol level. Privilege escalation is mitigated through the resource ownership policy natively defined in the Move language and enforced via hierarchical identity structures, translating constitutional constraints within the smart contracts. The IOTA Identities offer an appropriate framework for enforcing role-based permissions that align with constitutionally defined roles, thereby providing protection against unauthorized access attempts. Furthermore, the inherent separation between the blockchain networks and their encrypted inter-chain communication channels reduces the risks associated with sniffing attacks.

V. System Evaluation

In order to assess the technical feasibility and the scalability of the proposed architecture, smart contracts have been tested via the use of PTBs. The first prototype implemented smart contracts for the Private Institutional Blockchains. Consequently, the main functions tested concerned the creation, retrieval, and updating of documents, while also enforcing the access control and authorization policies required by the

identity hierarchies. Since the PTBs are transactions, the main measures evaluated regarded the computational cost and complexity of the operations implemented.

TABLE I
TRANSACTION GAS COSTS EXPRESSED IN IOTA TOKENS

Cost Component	Create New Document	Update Document	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**

*0.001 is the minumum network computation cost

As reported in Table I, costs are fixed at the minimal levels (0.001 IOTA) indicating that the logic implemented via Move's smart contracts for constitutional compliance and procedural validation imposes negligible overhead. The testing scenario considered a setting in which the documents involved were associated with nine identities, serving as an emulation of authorized institutional actors. The documents included a legislative text of 129 words processed through a SHA-256 hashing procedure, as well as a complete Akoma Ntoso IRI together with its corresponding metadata components. Overall, the most expensive measured component in the transactions is the *Storage Cost*, which represents the total cost of writing or updating data on the blockchain. Nevertheless, the gas required to complete the operations remains relatively low, even in scenarios involving document overwriting after saving a new version.

These findings enable inferences regarding the scalability potential of the system for institutional deployment and confirm the validity of the proposed implementation.

VI. CONCLUSIONS

This study has demonstrated how emerging blockchain technologies, combined with advanced programming paradigms such as the Move language, can facilitate the implementation of secure and transparent multi-layered architectures, specifically in sensitive institutional contexts.

An illustrative instance of these multi-layered architectures has been provided in conjunction with the technologies adopted throughout the development process. Within the proposed architecture, both the properties of the technologies employed and the specific programming patterns of Move language have guided the implementation of access-control policies. Each module of the architecture implements distinct authorization mechanisms designed to uphold the levels of confidentiality and transparency prescribed by fundamental constitutional principles.

Furthermore, the tests performed on the core functionalities of the architectures provided sufficient data to substantiate the efficiency of the implemented smart contracts and to draw informed conclusions regarding system scalability. The resulting implementation confirms to assess constitutional compliance with key democratic principles, respecting institutional confidentiality while providing public transparency for external stakeholders. Future work will concentrate on enhancing the interoperability between the different layers, assessing both the security and performance of inter-layer communications, evaluating reliability and latency under conditions that emulate real-world scenarios.

REFERENCES

[1] M. Palmirani, L. Papalia, C. Bomprezzi, A. Arruzzoli, M. Zichichi, and S. Ferretti, "A multi-chain approach to transparent and accountable legislative processes," June 2025.

[2] C. Pungila and V. Negru, "A multi-layered programmable blockchain approach to digital currency for high-volume transactions in e-commerce systems," *Online] Avaialble: https://abey. com/whitepaper/aBey-Whitepaper*, vol. 3.

[3] A. Iaria, S. Ferretti, M. Zichichi, and V. Ghini, "Towards next generation domain services: A committee based privacy scheme leveraging move on iota," in *Proceedings of the 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. Zurich, Switzerland: IEEE, Nov. 2025.

[4] The MystenLabs Team, "The sui smart contracts platform," 2023. [Online]. Available: https://docs.sui.io/paper/sui.pdf

[5] S. Popov, O. Saa, and P. Finardi, "Equilibria in the tangle," *Computers & Industrial Engineering*, vol. 136, pp. 160–172, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360835219304164

[6] Harvey, "Discover programmable transaction blocks on sui move," Aug 2023, accessed: 2025-11-24. [Online]. Available: https://suipiens.com/blog/discover-programmable-transaction-blocks-on-sui-move/

[7] W. Voermans, H.-M. ten Napel, and R. Passchier, "Combining efficiency and transparency in legislative processes," *The Theory and Practice of Legislation*, vol. 3, no. 3, pp. 279–294, 2015. [Online]. Available: https://doi.org/10.1080/20508840.2015.1133398

[8] M. Palmirani, L. Papalia, C. Bomprezzi, M. Zichichi, A. Arruzzoli, and S. Ferretti, "Multi-level architecture for separation of powers in legislative process," in *Proceedings of the 7th Distributed Ledger Technology Workshop (DLT 2025)*, ser. CEUR Workshop Proceedings. Pizzo, Italy: CEUR-WS.org, June 2025.

[9] M. Palmirani, R. Sperberg, G. Vergottini, and F. Vitali, "Akoma ntoso version 1.0," Aug. 2018. [Online]. Available: http://docs.oasis-open.org/legaldocml/akn-core/v1.0/os/part1-vocabulary/akn-core-v1.0-os-part1-vocabulary.html

[10] IOTA Stiftung, "Move - wrapped objects references," accessed: 2025-06-28. [Online]. Available: https://docs.iota.org/developer/iota-101/objects/object-ownership/wrapped

[11] Sui Foundation, "Sui move intro course - programmable transaction block (ptb)." [Online]. Available: https://intro.sui-book.com/unit-five/lessons/1_programmable_transaction_block.html

[12] Sui Documentation, "Programmable transaction blocks – executing a transaction command," https://docs.sui.io/concepts/transactions/prog-txn-blocks, accessed: 2025-11-24.

[13] N. Korchiev, A. Pateria, V. Samatova, S. Mansouri, and K. Anyanwu, "Taming the beast of user-programmed transactions on blockchains: A declarative transaction approach," 2024. [Online]. Available: https://arxiv.org/abs/2411.02597

[14] IOTA Stiftung, "Transaction pricing," https://docs.iota.org/about-iota/tokenomics/gas-in-iota, accessed: 2025-11-25.

[15] Sui Foundation, "Gas fees," accessed: 2025-11-25. [Online]. Available: https://docs.sui.io/concepts/tokenomics/gas-in-sui

[16] W. Yan, N. Zhang, L. L. Njilla, and X. Zhang, "Pcbchain: Lightweight reconfigurable blockchain primitives for secure iot applications," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 10, pp. 2196–2209, 2020.

[17] S. Tanwar, *Basics of Cryptographic Primitives for Blockchain Development*. Singapore: Springer Nature Singapore, 2022, pp. 83–111. [Online]. Available: https://doi.org/10.1007/978-981-19-1488-1_4

ACKNOWLEDGEMENT

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