



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



European Research Council
Established by the European Commission



A Security Analysis of Cross-Chain Bridges in Multi-Chain Architectures for Institutional Collaboration

DLT 2026 – 4-6 June – Pula, CA

Arianna Arruzzoli¹; Stefano Ferretti³; Mirko Zichichi⁴;
Ludovico Papalia^{1,2}; Chantal Bompreszi¹; Monica Palmirani¹

¹University of Bologna, ALMA-AI via Galliera 3, Bologna, 40121, Italy

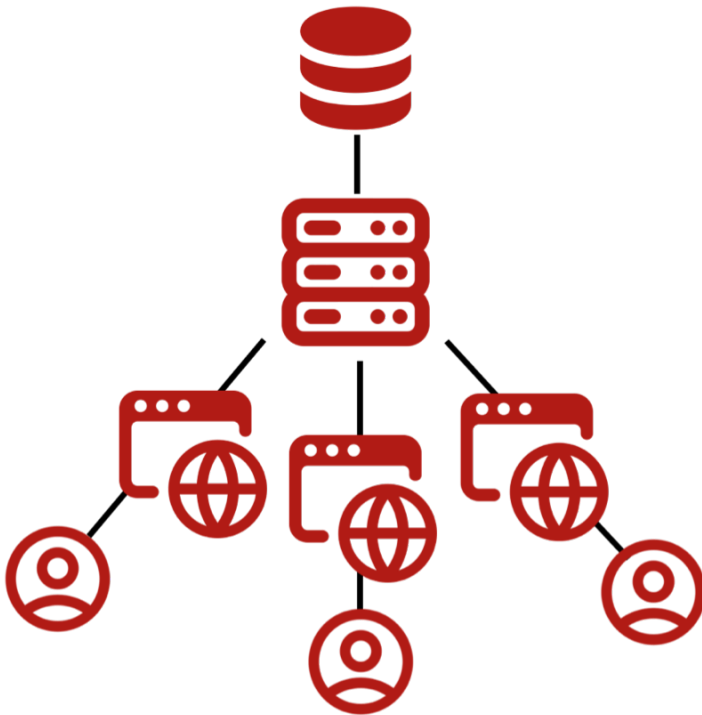
²University of Camerino, Piazza Cavour 19/f, 62032 Camerino, Italy

³University of Bologna, Department of Computer Science and Engineering, Bologna, Italy

⁴IOTA Foundation, Pappelallee 78/79, Berlin, 10437, Germany

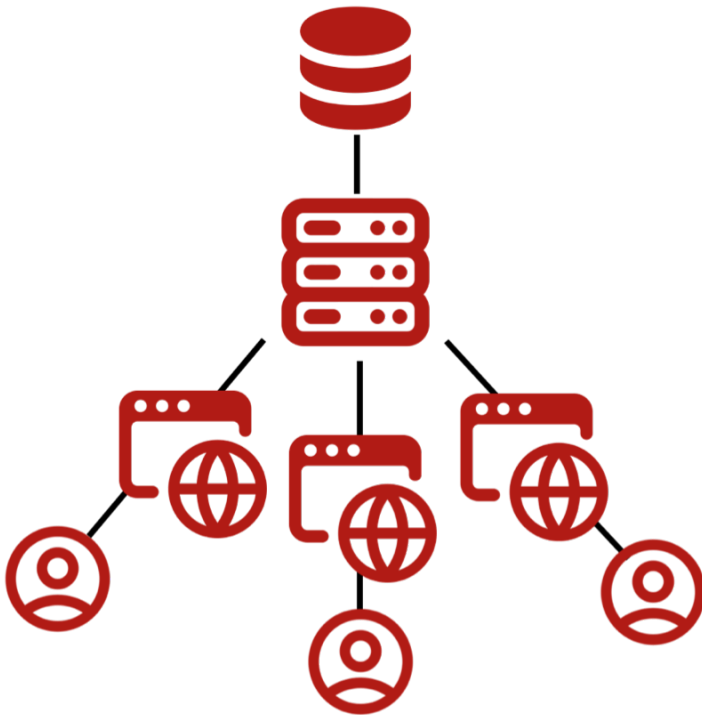
Security analysis in different architectures

Centralized Architecture

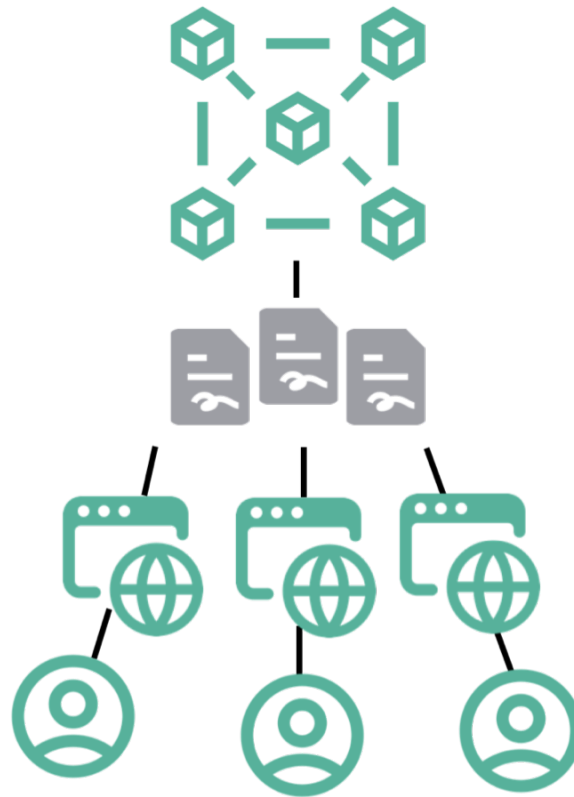


Security analysis in different architectures

**Centralized
Architecture**

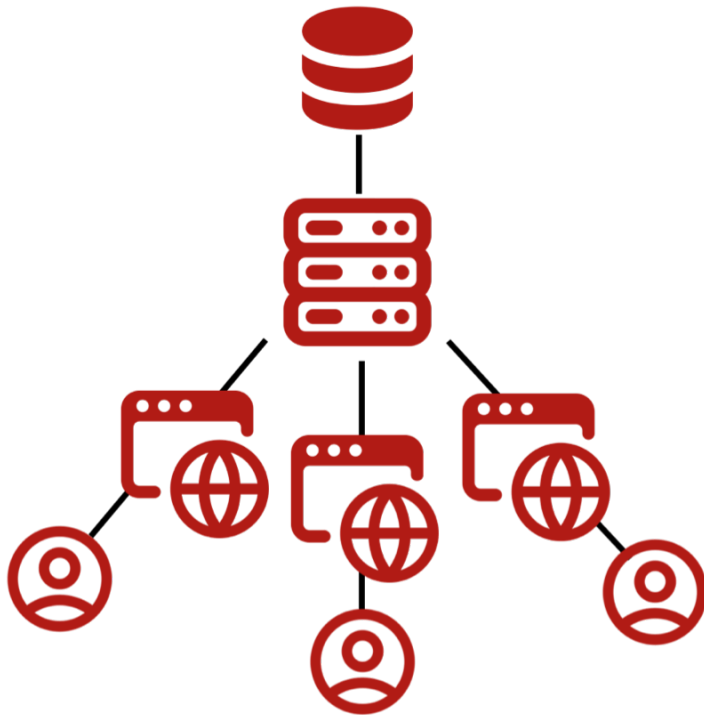


**Current DApps
Architecture**

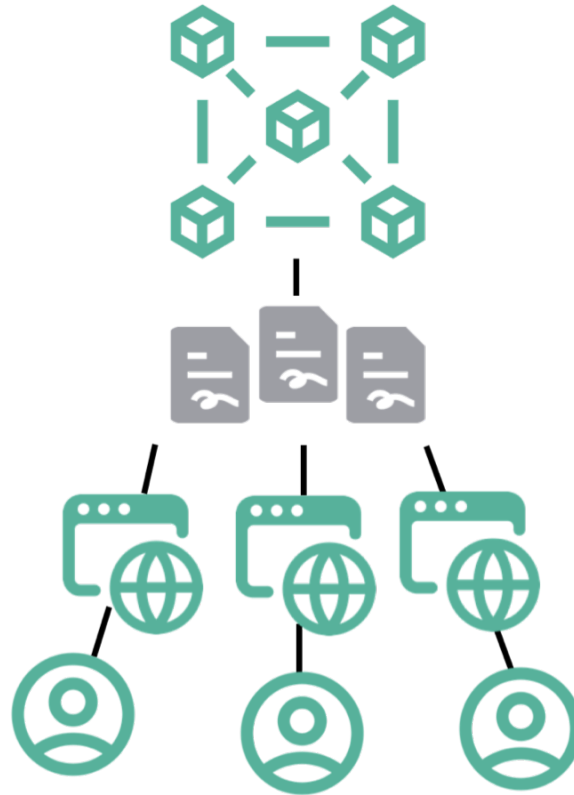


Security analysis in different architectures

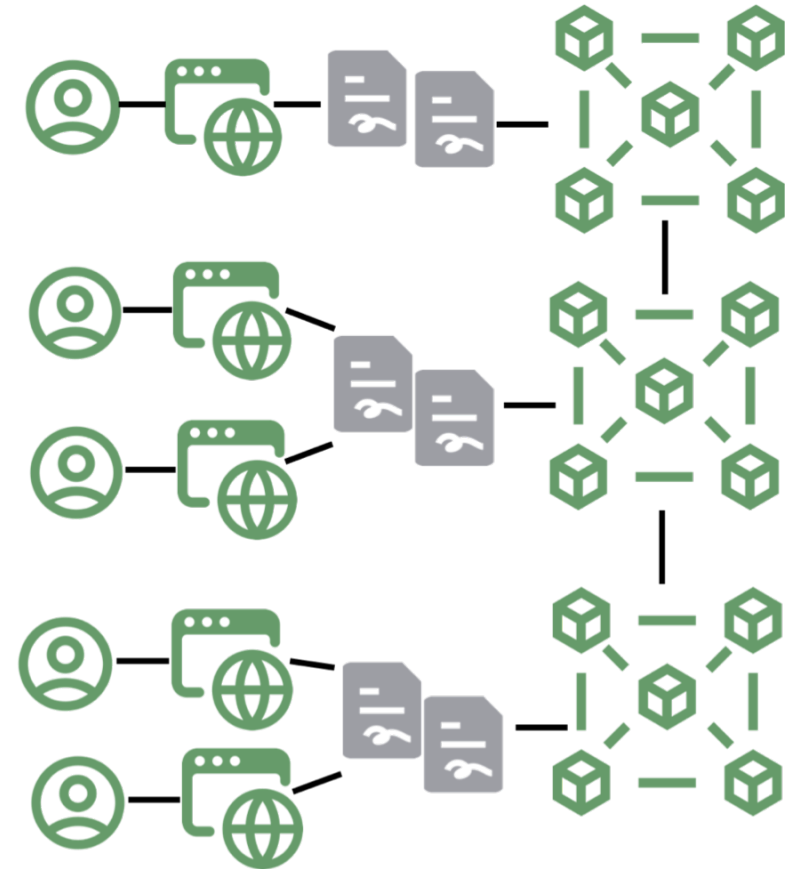
**Centralized
Architecture**



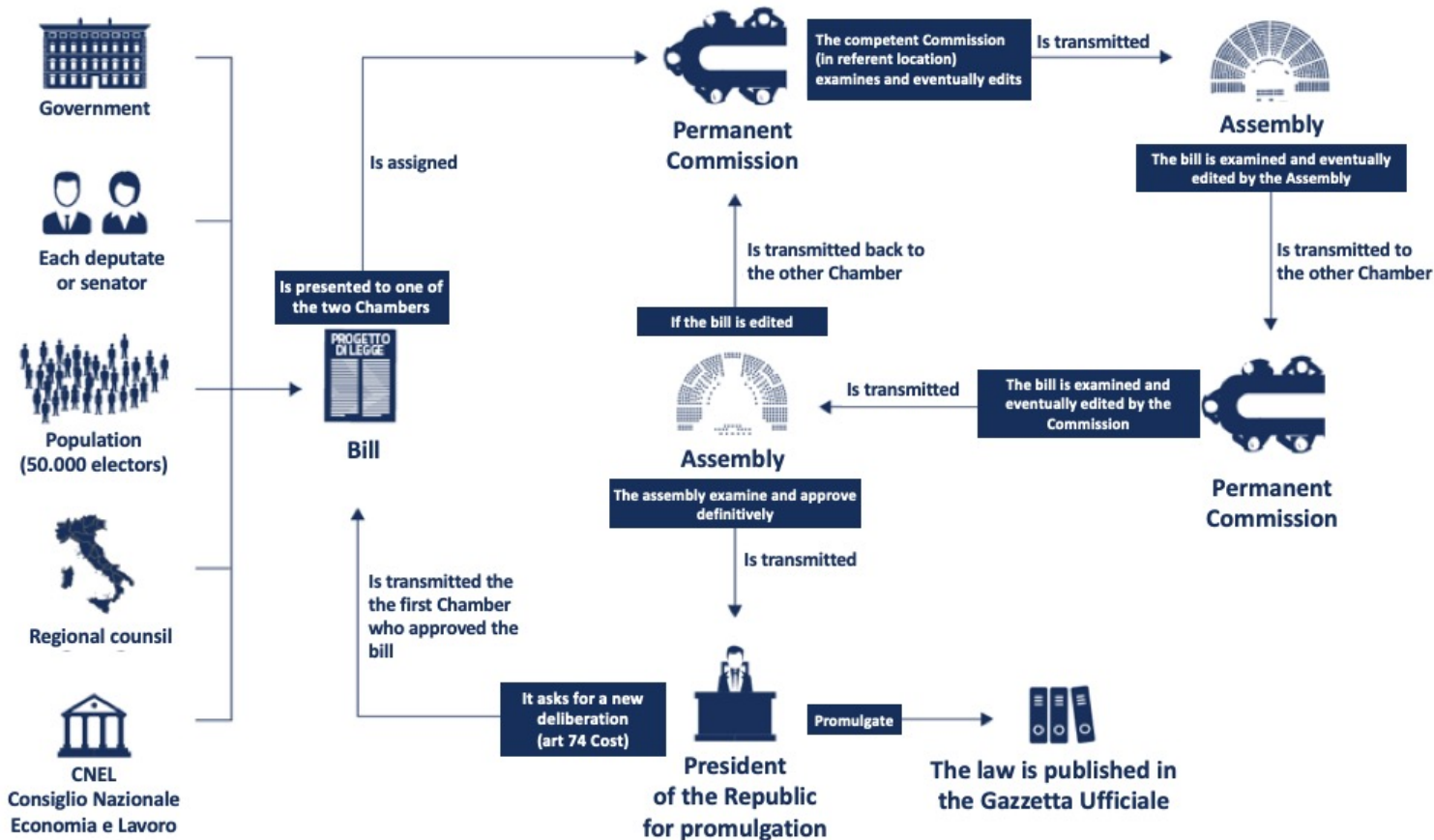
**Current DApps
Architecture**



**Multi-Chain
Architecture**



Use Case: Italian legislative process

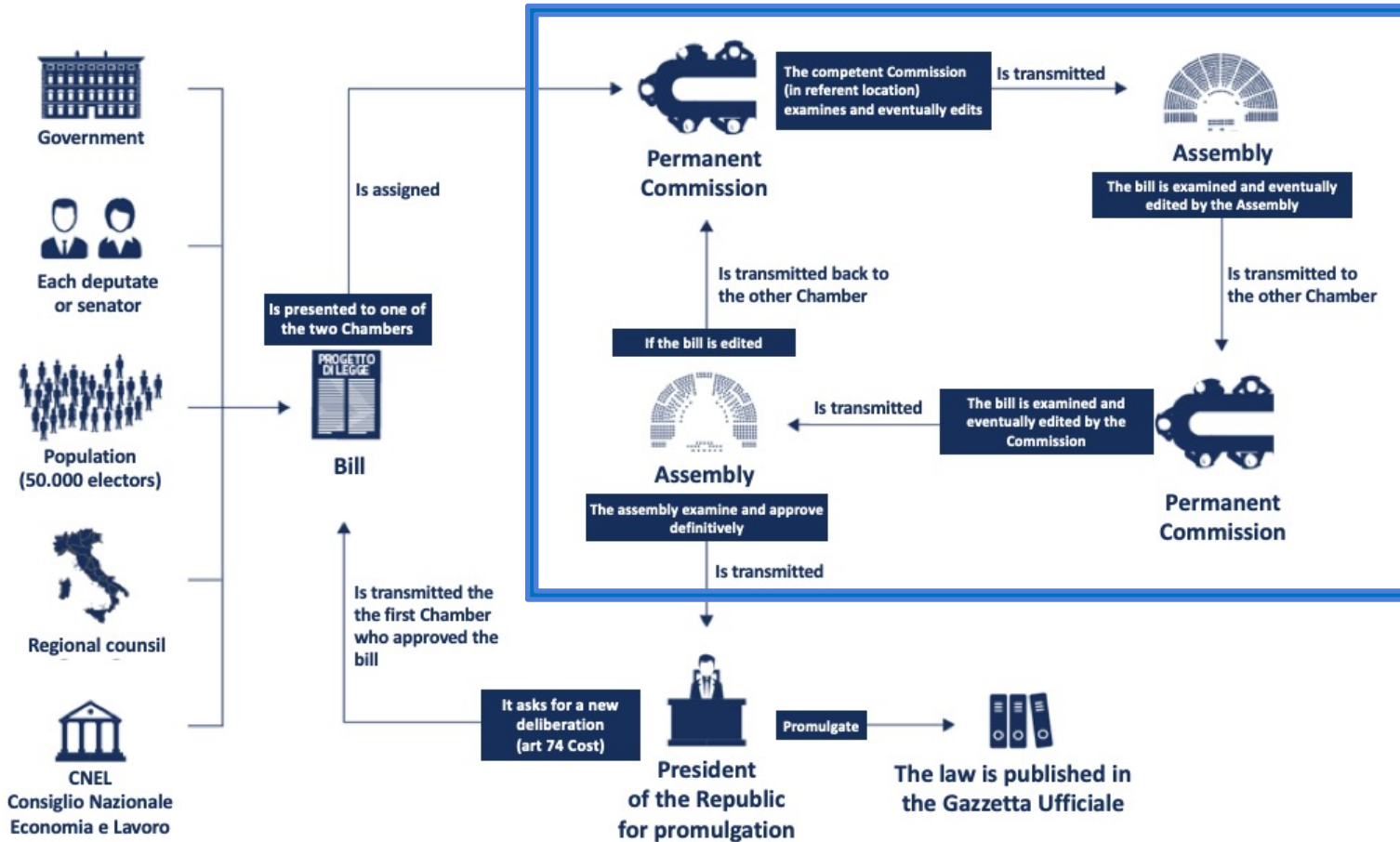


Institutional and governmental context

- Separation of Powers
- Institutional Autonomy
- Transparency

Use Case: Italian legislative process

legislative shuttle



WHY Separation of Powers Is a Design Constraint

The Constitutional Mandate:

- Art. 70 Cost.: both chambers must approve identical legislative text (perfect bicameralism)
- Art. 97 Cost.: transparency is an enforceable obligation, not a policy choice
- Corte Costituzionale n. 235/2015: consolidation of legislative data into a unified repository under any single institutional actor is **constitutionally prohibited**

The Structural Tension:

- Inter-institutional coordination is **mandatory** (navetta parlamentare)
- **Centralized** coordination is **forbidden** (CC 235/2015)
- Each chamber **must retain full autonomy** over its internal deliberative process

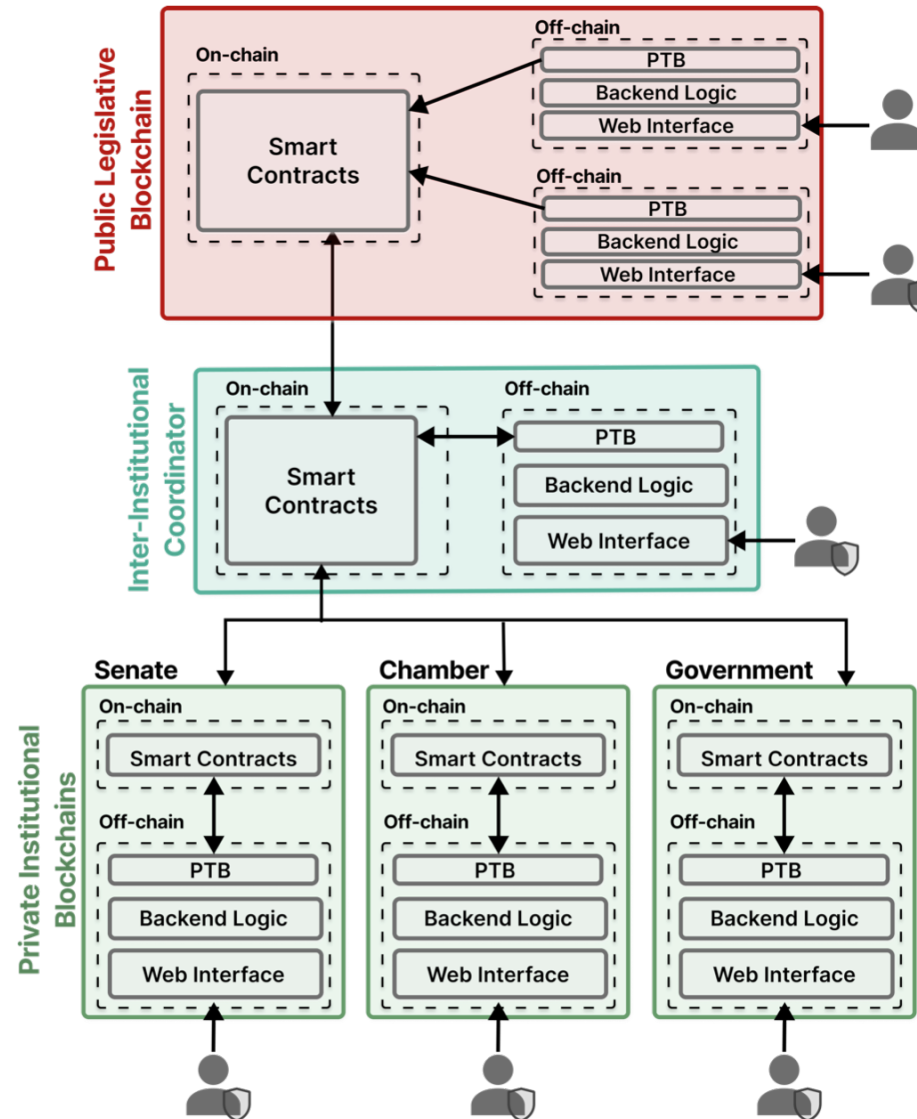
*The multi-chain architecture is **not** an engineering preference. It is the only **architectural model** that satisfies both constraints simultaneously.*

WHAT Should Be Shared

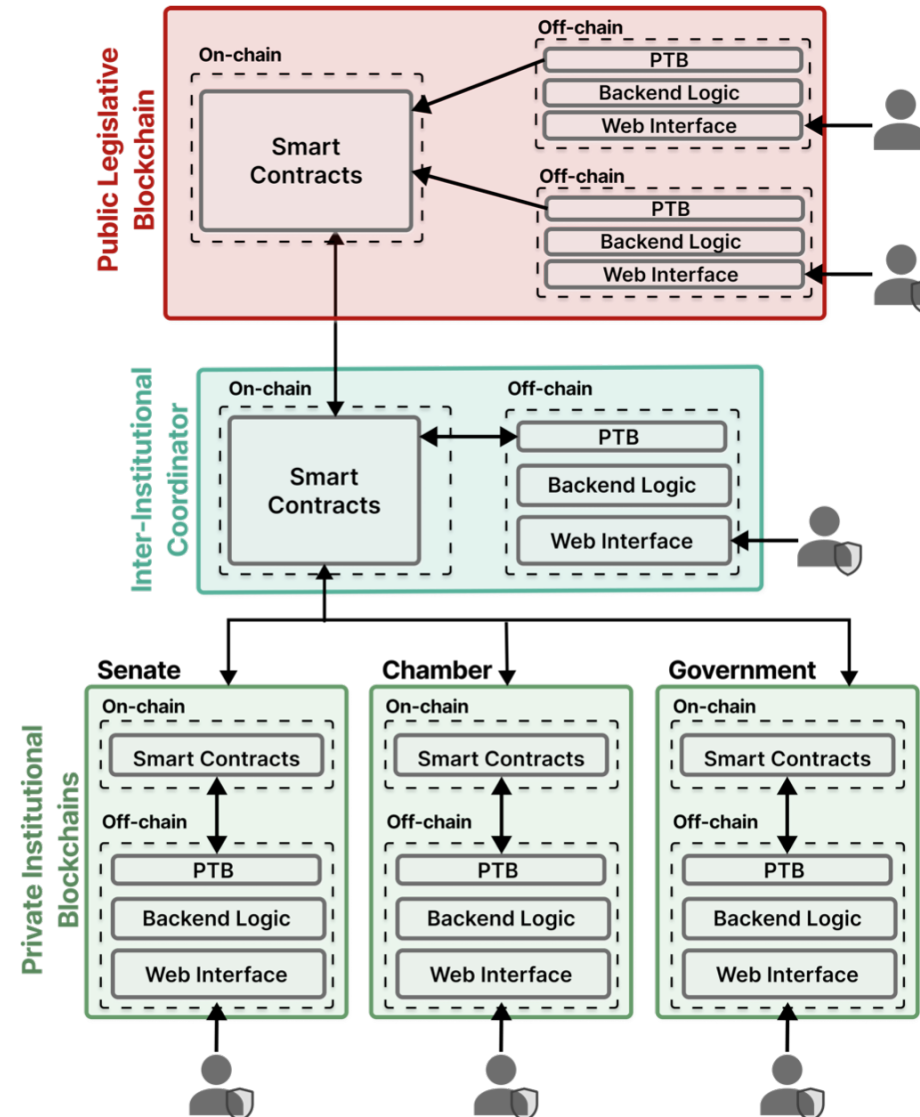
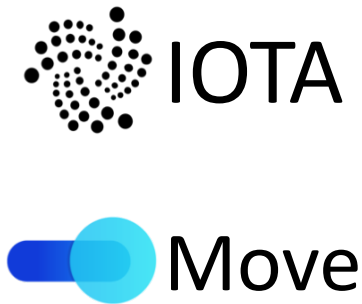
MUST be shared	MAY be shared	MUST NOT be shared
Presidential transmission message	Committee reports	Draft legislation
Consolidated approved text	Advisory opinions	Committee agendas
Technical report (Art. 17, L. 196/2009)	Technical dossiers	Confidential minutes
Legally mandated	Institutional practice, not enforceable	Protected deliberative sphere

*This **asymmetry** directly defines the bridge's **functional scope**:
 what **MUST be shared** should trigger automatic cross-chain transmission;
 what **MAY be shared** requires authorized user action;
 what **MUST NOT be shared** never traverses the bridge.*

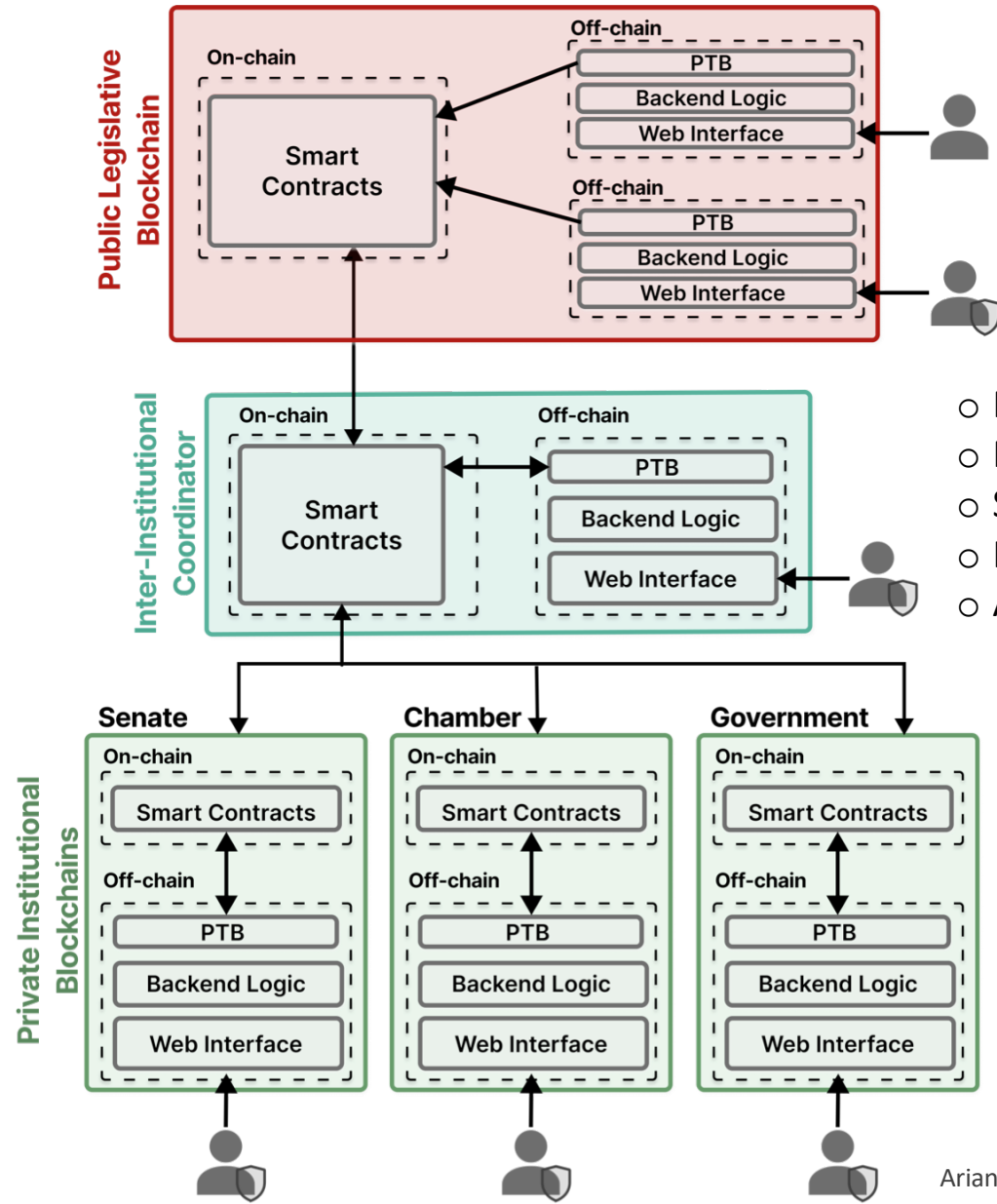
Our Multi-Chain Architecture



Our Multi-Chain Architecture



Our Multi-Chain Architecture



- Public Permissioned blockchain
- Support for Official Gazettes
- Compliant with constitutional principle of transparency
- Unified but decentralized repository
- Immutability of the documents

- Federated Permissioned blockchain
- Formally replicates institutional steps
- Smart contracts managing the unification process
- Immutable registry for institutional transactions
- Accountability

- Private Permissioned blockchain
- Independent and isolated system
- Compliant with constitutional requirements
- Confidentiality



Traditional cross-chain bridges



Traditional cross-chain bridges

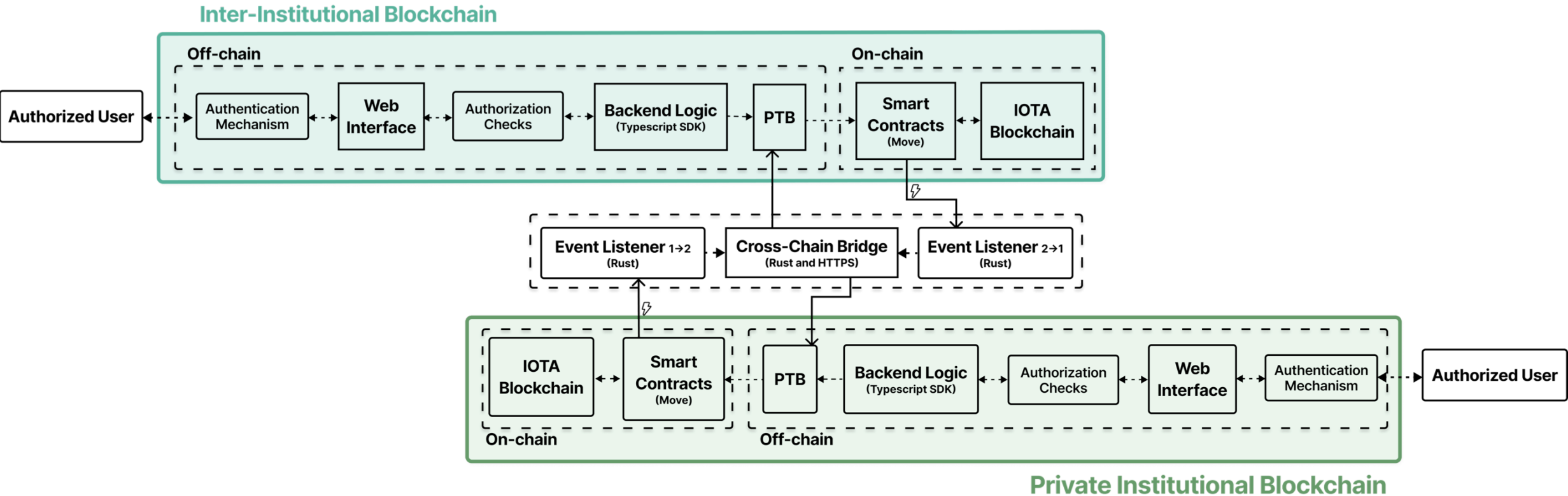


Problems found in existing literature solutions:

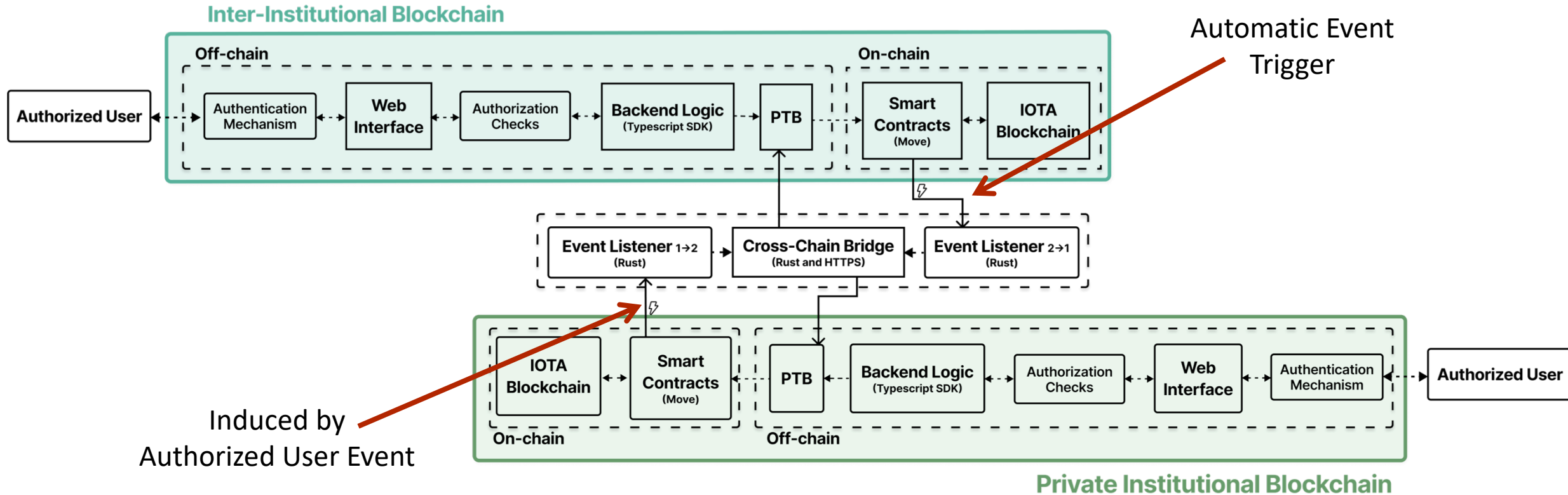
- Financial context
- Solidity-based smart contracts
- Need to focus on: **confidentiality, traceability, accountability and integrity**



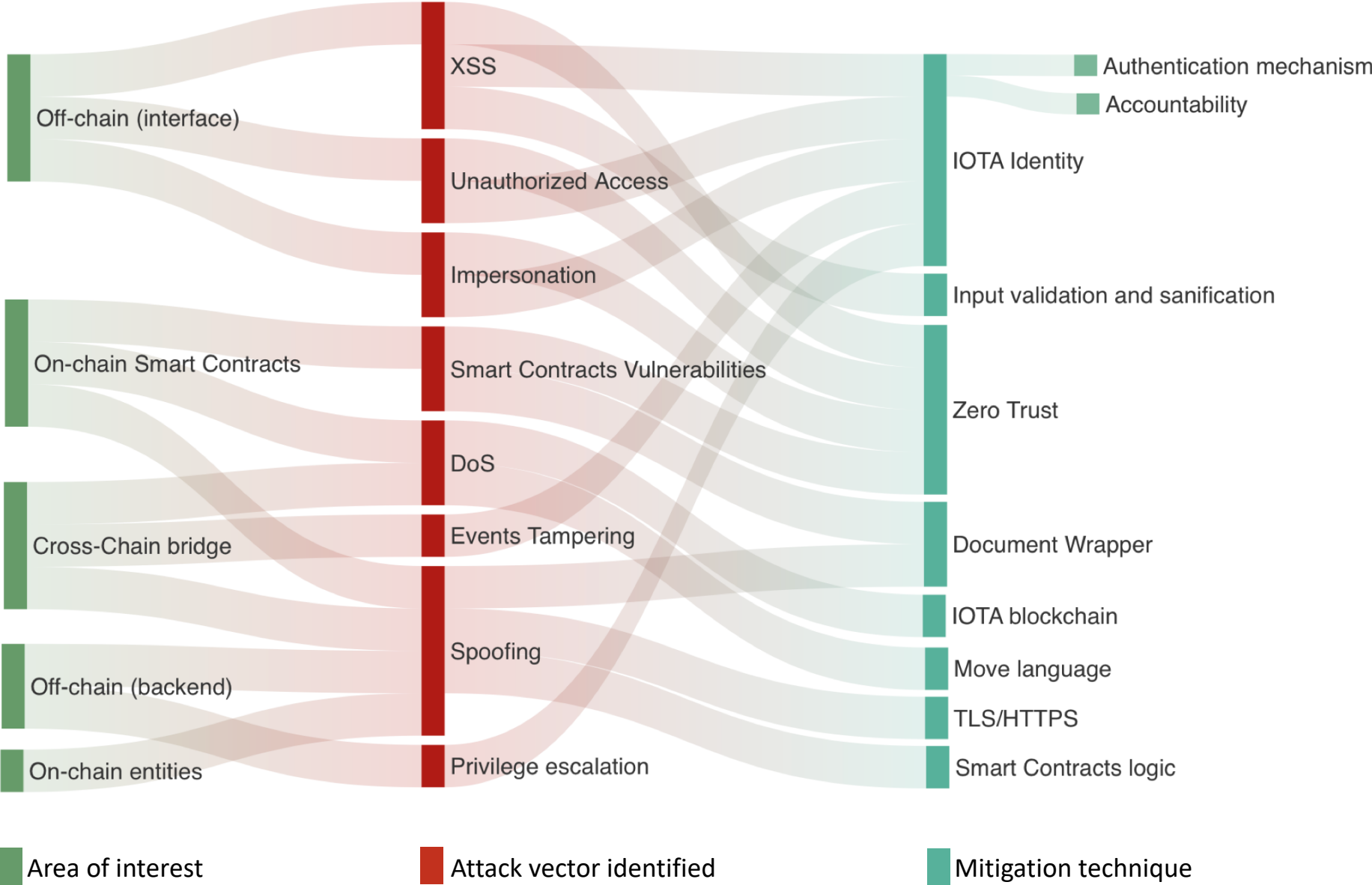
Cross-Chain bridge



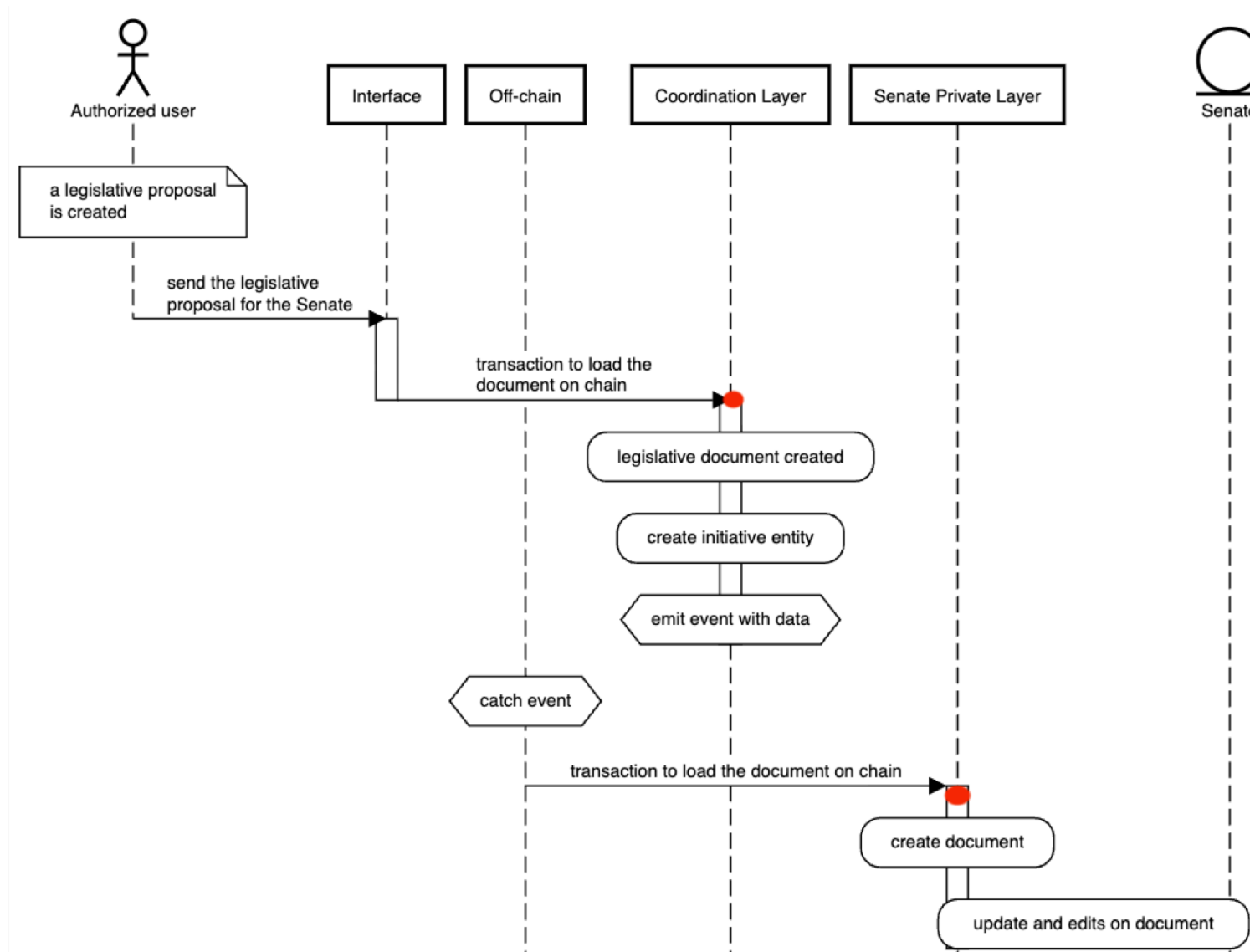
Cross-Chain bridge



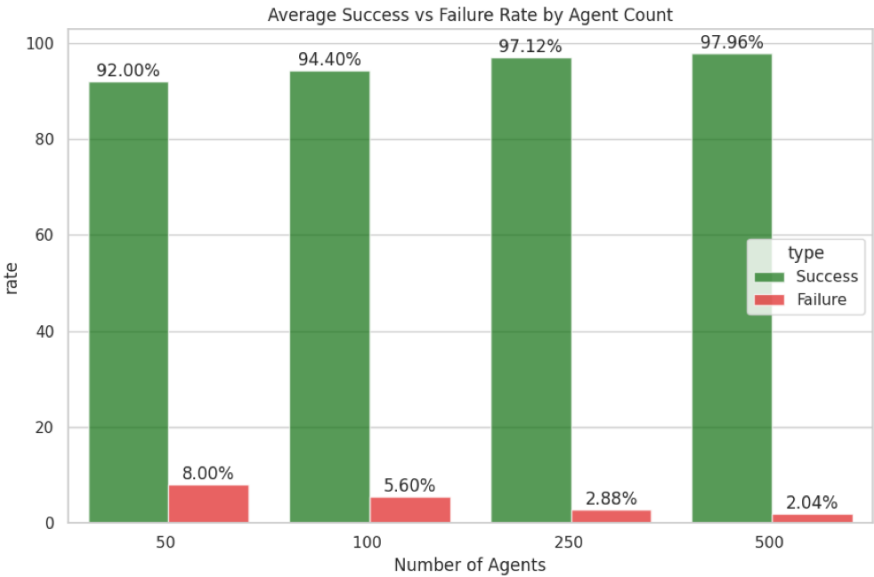
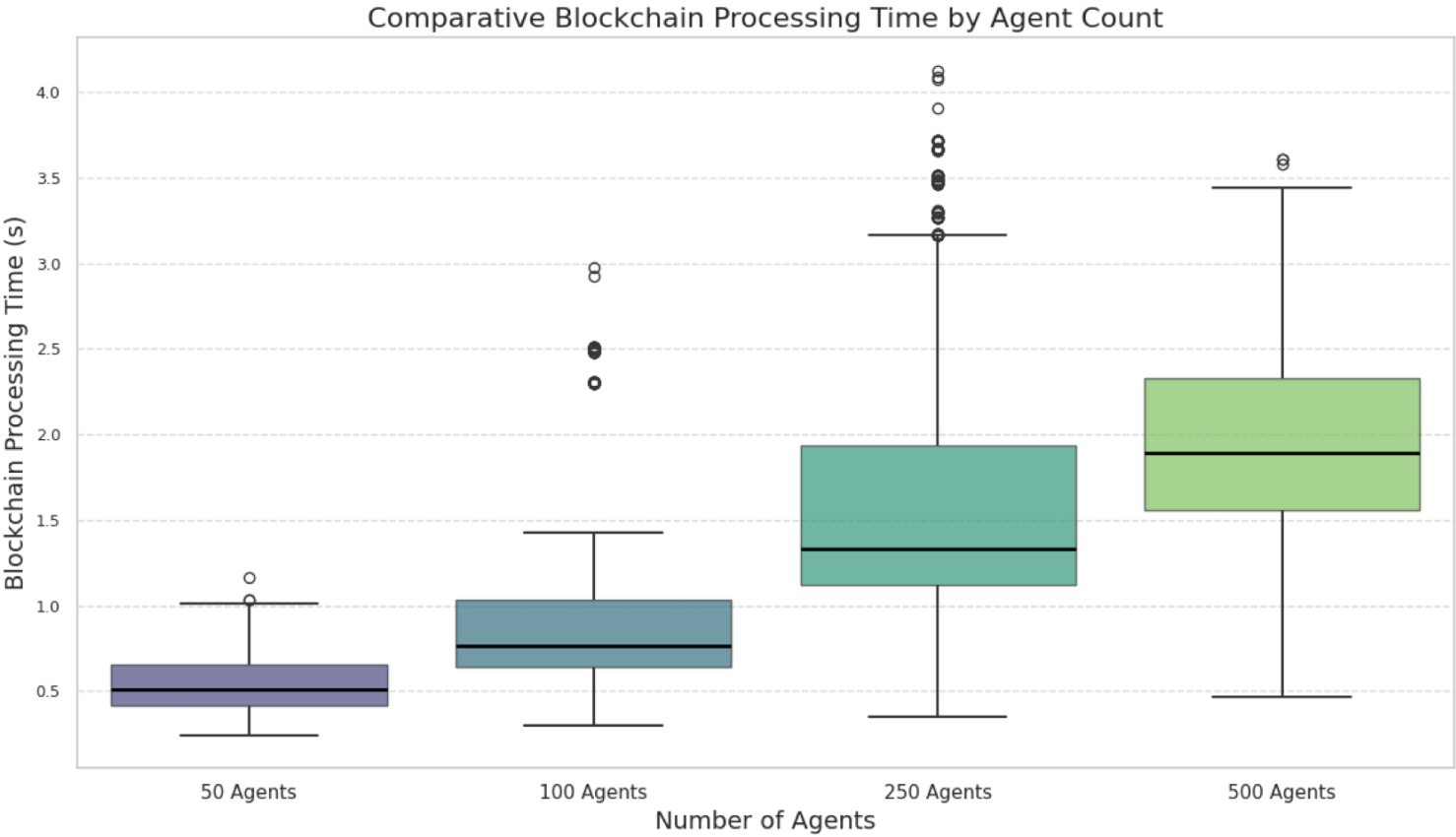
Threat model



Performance Evaluation



Results



Wrapping up

- Multi-chain architectures can support institutional collaboration without sacrificing decentralization, security, or constitutional guarantees.
- Bridges can constitute exposed attack surfaces, but a robust architecture can be developed considering not only financial applications.
- The security measures implemented leveraging the technologies properties and specific design patterns improved the security of the overall system without interfering on its performances.



Wrapping up

- Multi-chain architectures can support institutional collaboration without sacrificing decentralization, security, or constitutional guarantees.
- Bridges can constitute exposed attack surfaces, but a robust architecture can be developed considering not only financial applications.
- The security measures implemented leveraging the technologies properties and specific design patterns improved the security of the overall system without interfering on its performances.



Open challenges

- **Technical:** Accountability mechanisms and transaction signing responsibilities
- **Legal:** existing parliamentary regulations do not address algorithmically generated institutional attestations



Thank you for your attention

Arianna Arruzzoli

arianna.arruzzoli2@unibo.it

Ludovico Papalia

ludovico.papalia2@unibo.it



European Research Council
Established by the European Commission

HyperModeLex

Grant agreement ID: 101055185



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

www.unibo.it

