A Self-orchestration Model for Business Collaborations with Verifiable Credentials

Imre Kocsis, Martin Farkas, Bertalan Zoltán Péter

kocsis.imre@vik.bme.hu

IFIP WG 10.4 meeting research report, 2026.06.27, Charlotte, NC

BME | FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS | Department of Artificial Intelligence and Systems Engineering | ftsrg Critical Systems Research Group

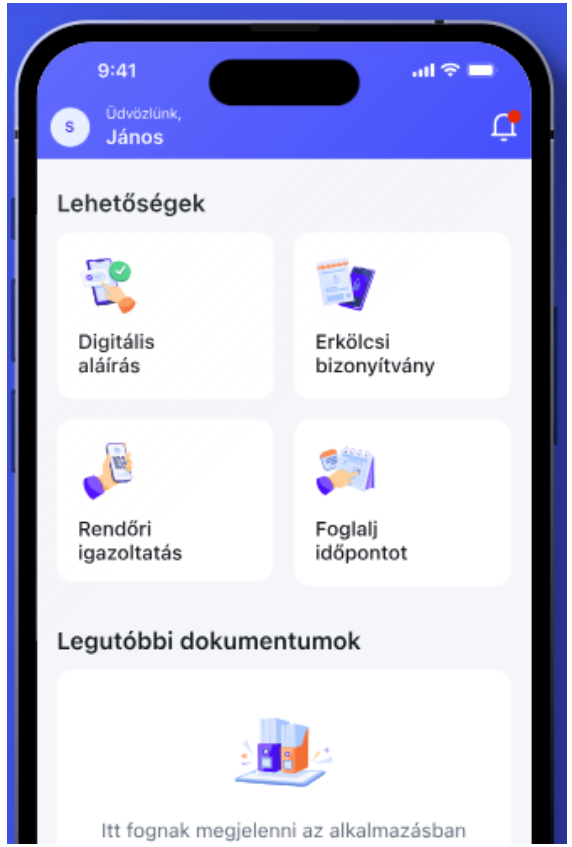
Prelude: Verifiable Credentials

- From the Self-Sovereign Identity movement, the W3C def

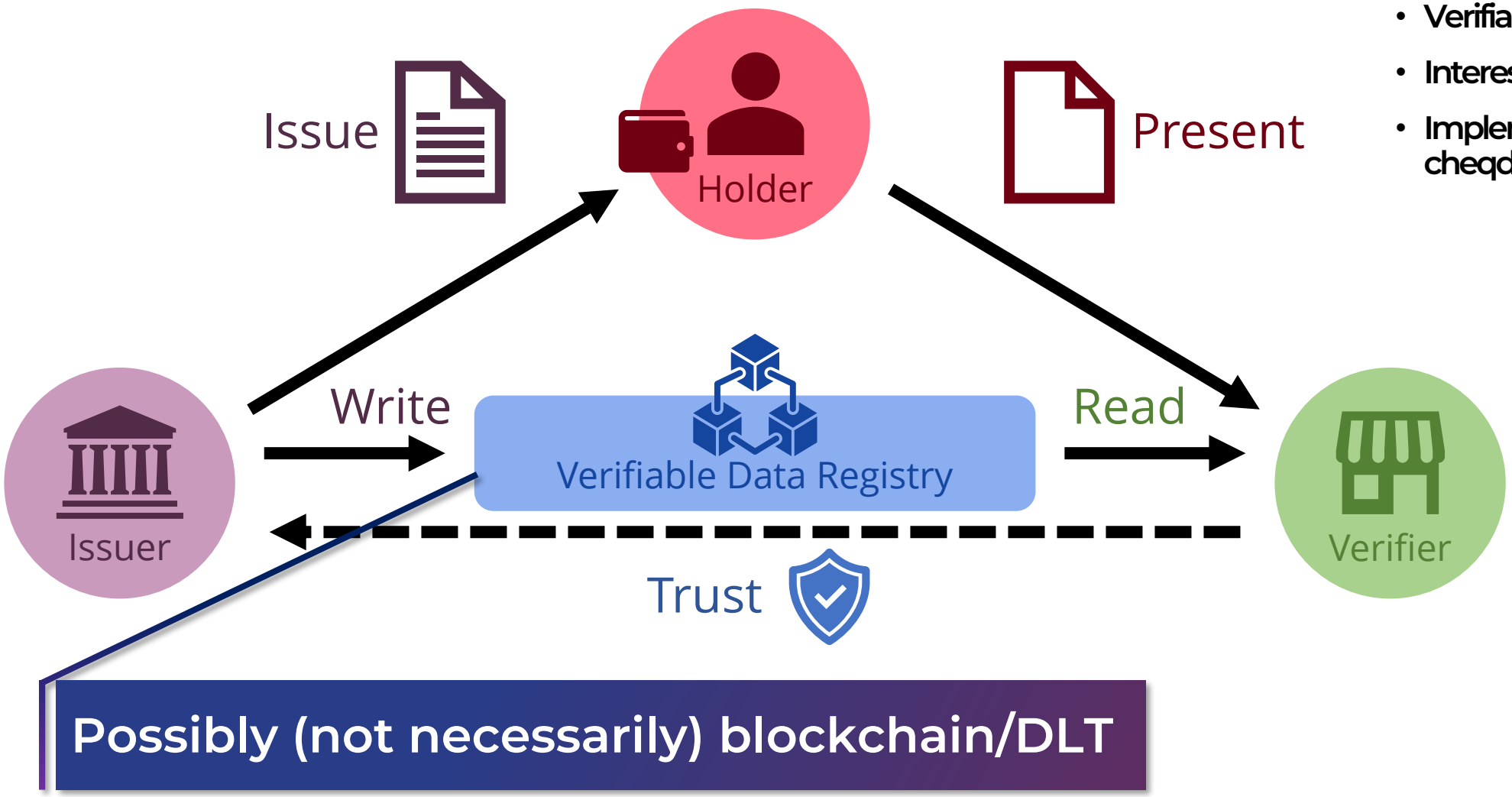
- Credential
  - Set of claims made by an issuer
  - Claims are assertions about a subject

- Verifiable Credential
  - Tamper-evident credential
  - With cryptographically verifiable authorship

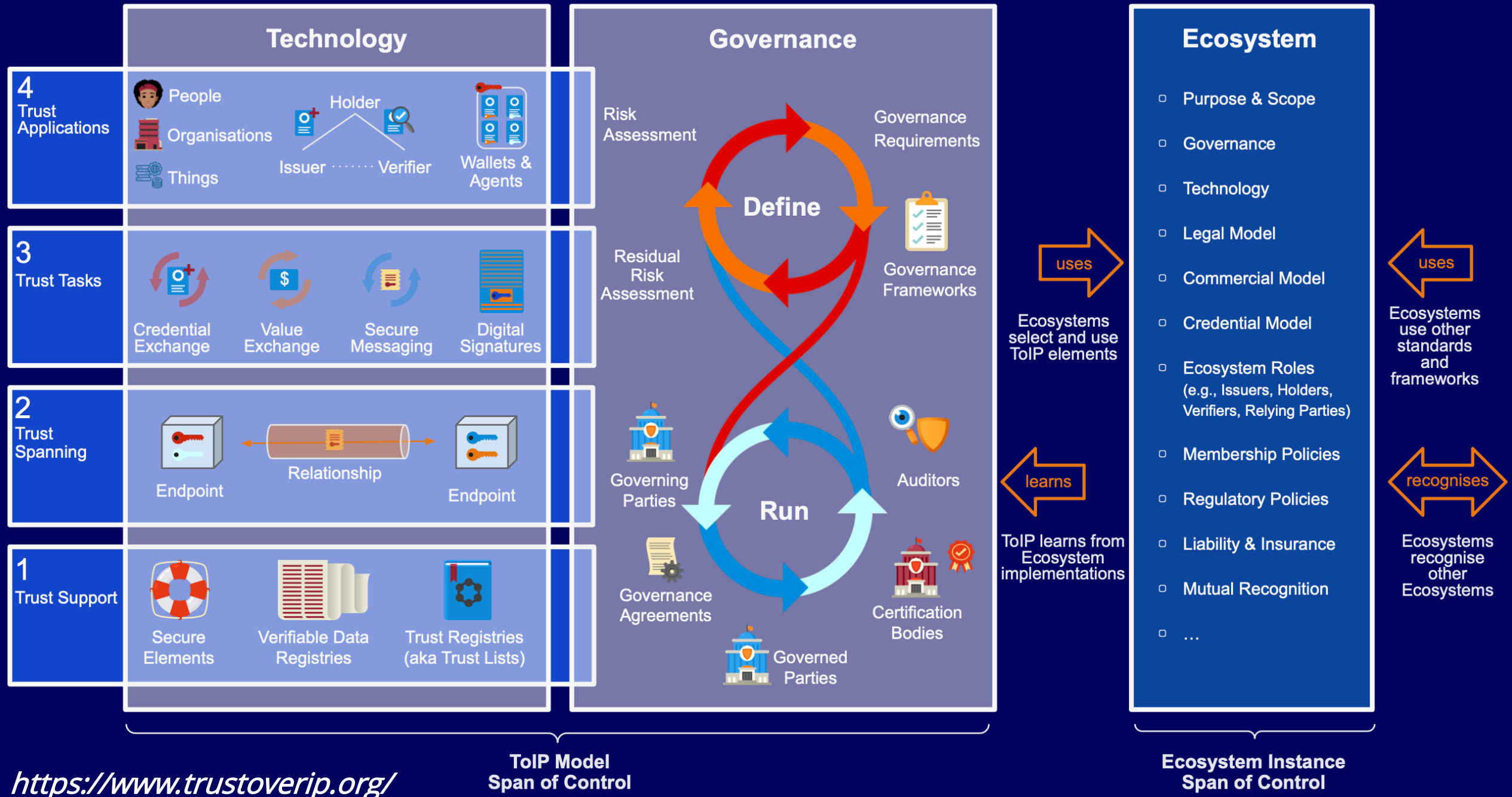
- Hedging comments
  - ~2023-: a veritable storm of formats, protocols, technologies, regulations, …
  - The EU is doing its own thing (eIDAS2, QEAA, EUDIW, …)
  - But this is coming in some way, shape or form for all of us



The W3C "trust triangle" model



- **Cryptographic guarantee of:**
  - Authenticity: *was issued by issuer*
  - Integrity: *was not tampered with*
  - Revocation status: *is/is not revoked*
- **Verifiable w/o asking the issuer**
- **Interesting SD/privacy options**
- **Implementation reality varied – cheqd…EntraID…EUDIW**



https://www.trustoverip.org/

Research direction

- We can use this for far more than “papers, please”
- VCs/VPs: carriers for DAGs of dependent claims
- *If* we have a VDR with (privacy-preserving) revocation
- Connected to ongoing research: decentralized process orchestration

- Note: here we assume DIDs, AnonCreds and DIDComm
- …but that’s not the point

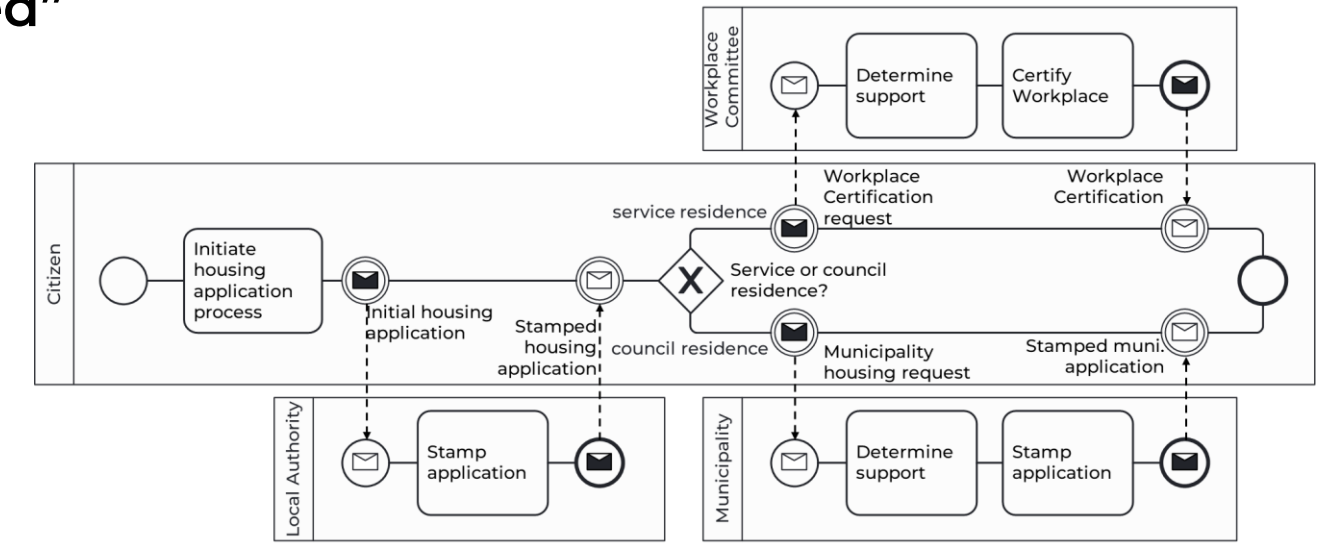
BPM 2025, BPM Forum, “A Self-orchestration Model for Business Collaborations with Verifiable Process History Credentials”, *https://doi.org/10.1007/978-3-032-02929-4*

Challenges in cross-org business process execution

- Ensuring that (partially) distrusting parties all “follow the process”
  - Enforcing control flow
  - Establishing irrepudiability
  - …

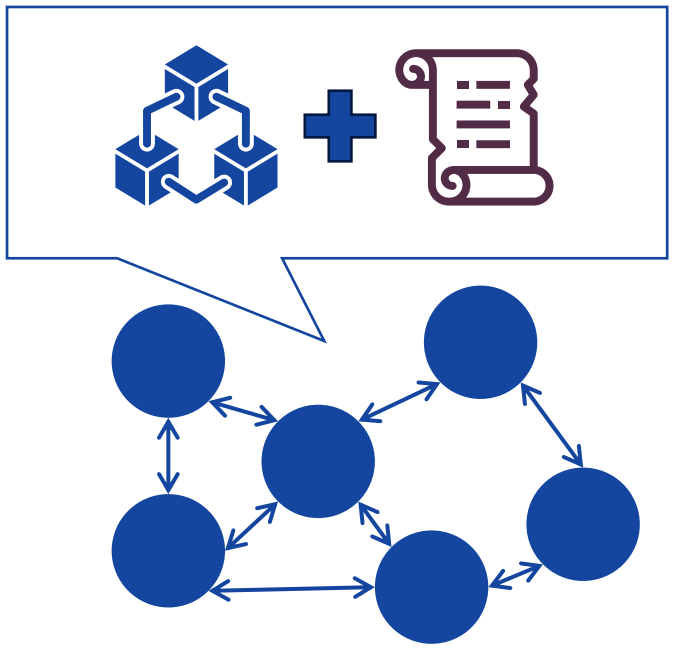
- Centralized orchestration/”federated” execution problematic

- Blockchain is the answer!
- …or is it?



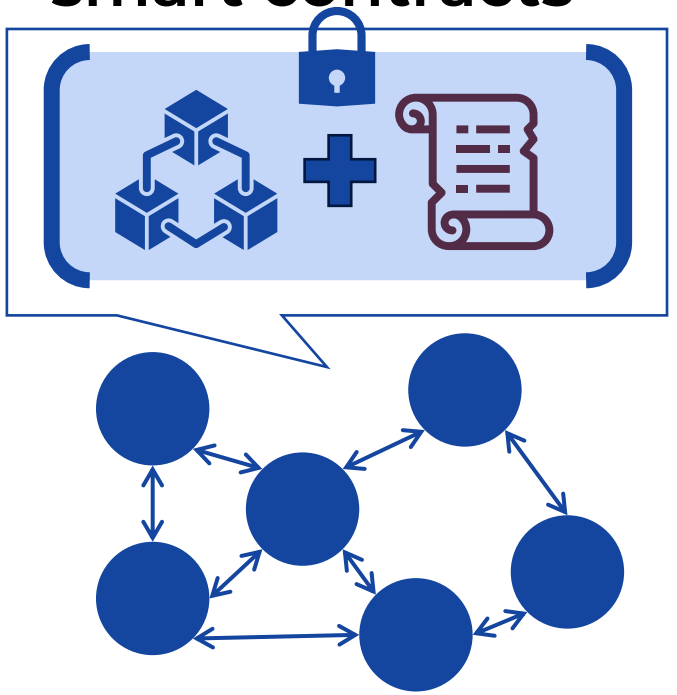
Decentralized “orchestration” approaches

State machine smart contracts



Significant body of work

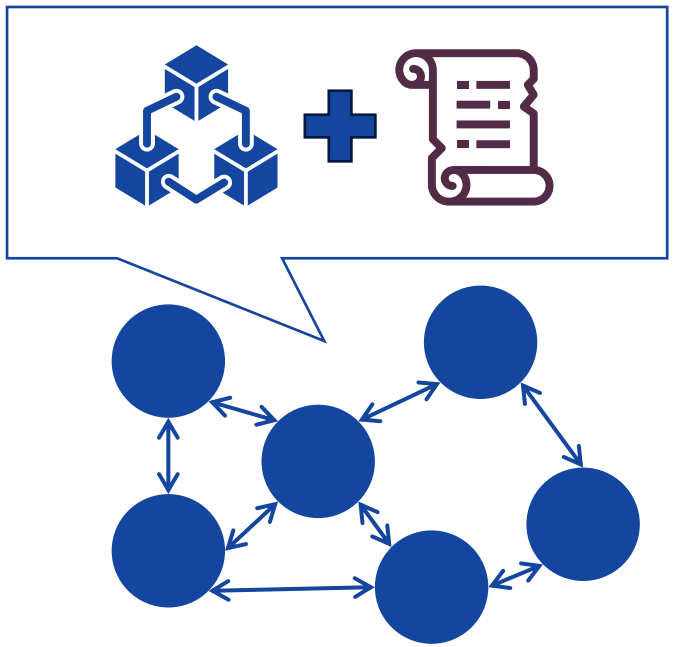
Commit & check ZKP smart contracts



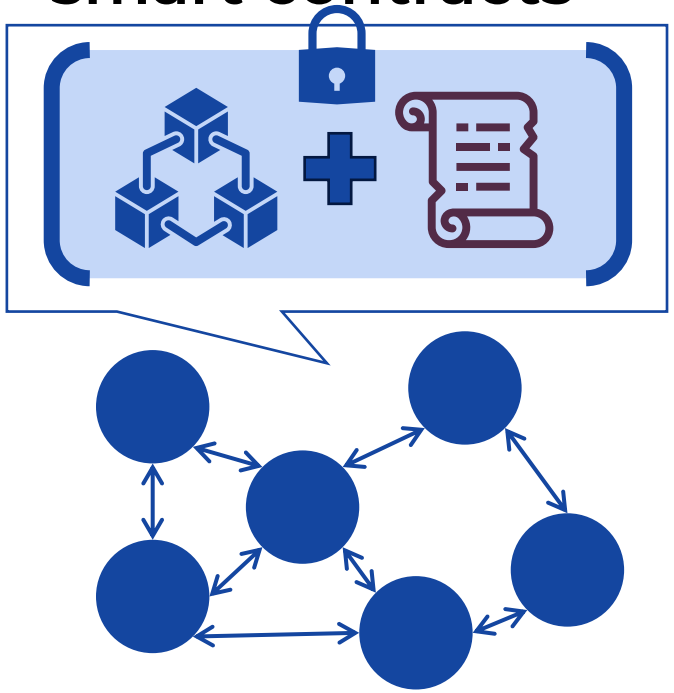
Petto et al.(BPM 2024)
Toldi, Kocsis (2023)
https://github.com/ftsrg/zkWF

The gap and our goal

State machine smart contracts



Commit & check ZKP smart contracts



Collaboration self-orchestration

Our Goal

An orchestration model with cryptographically verifiable execution
But peer-to-peer and confidentiality-preserving

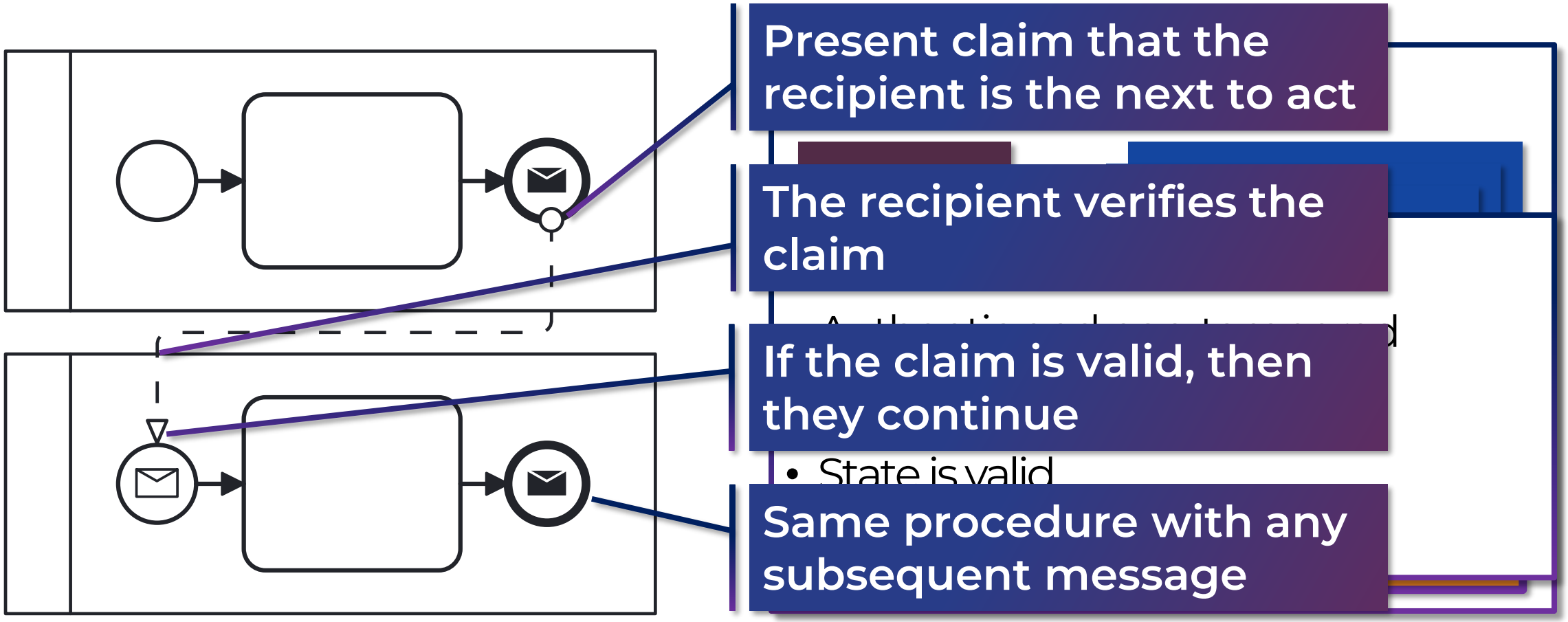
Novel concept: self-orchestration

Each participant carries the process state forward by presenting a cryptographically verifiable process history to the subsequent party.

- Physically AND logically distributed global state
- Shift trust to only the party who has to be trusted
  i.e. the one who actually claims something about the state

- *Provenance* of process steps/traces – message passing
- Fine-grained tradeoff b/w confidentiality and integrity
- (For now) worked out for **BPMN collaborations**

Bird's eye view



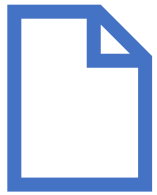
Core idea

Each pool is its own orchestrator. Collaboration "emerges" from verifiable process histories passed directly between parties.

Key constructs

Verifiable process history Credentials
VphCs

- Claim of what happened
  - Pool-internal process trace, etc.
  - VphCs recieved for each message recieve event
- Issued
  - When transition takes place
  - By the last actor
  - To the next actor



Non-invoked Transition Credentials
NiTCs

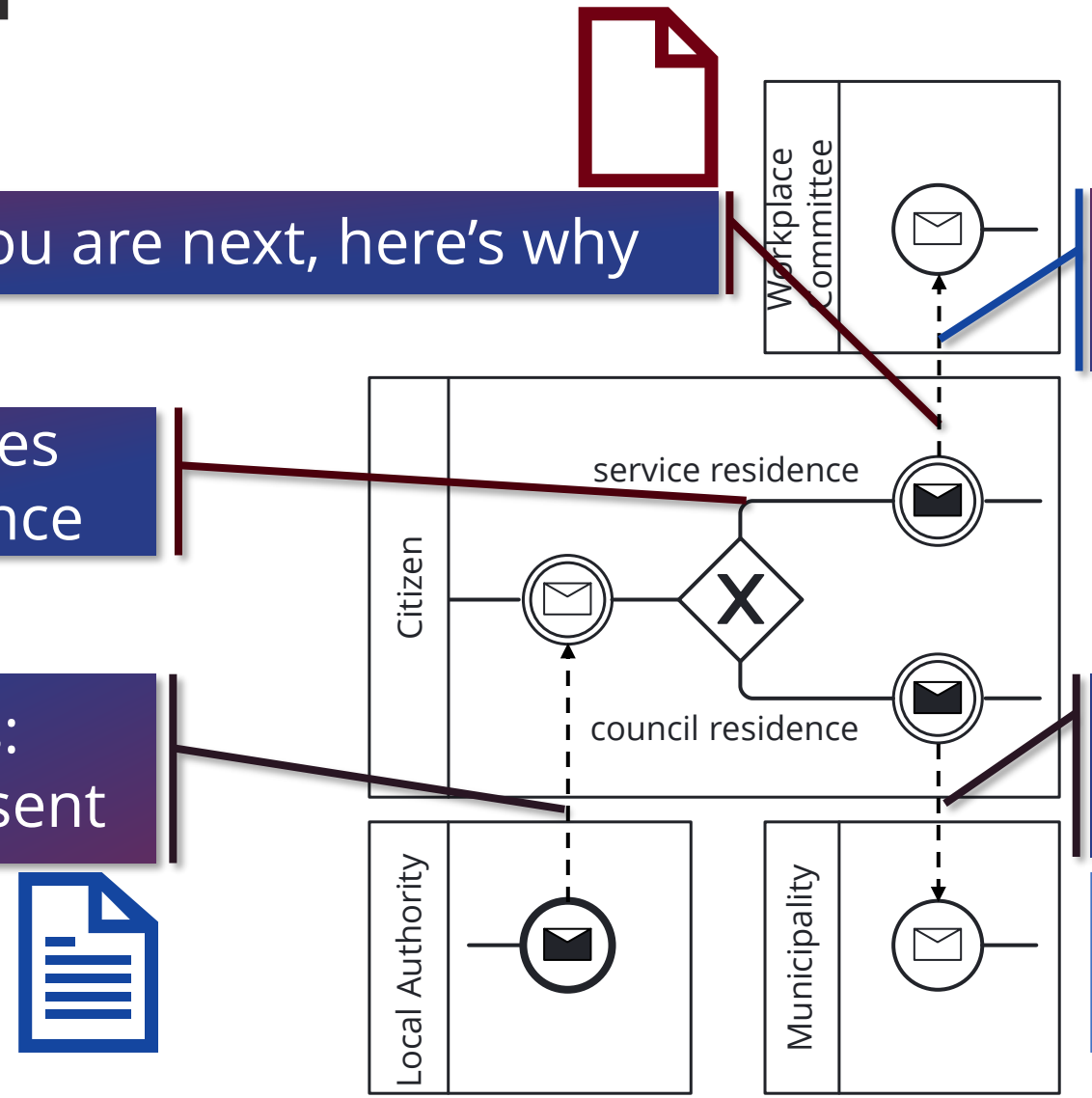
- Claim of what *didn't* happen
  - Revoked if path is taken
- Issued
  - Before transition takes place
  - By the target
  - To the initiator

Happy path

Present VCs: You are next, here's why

Citizen chooses service residence

VphC claims: message was sent



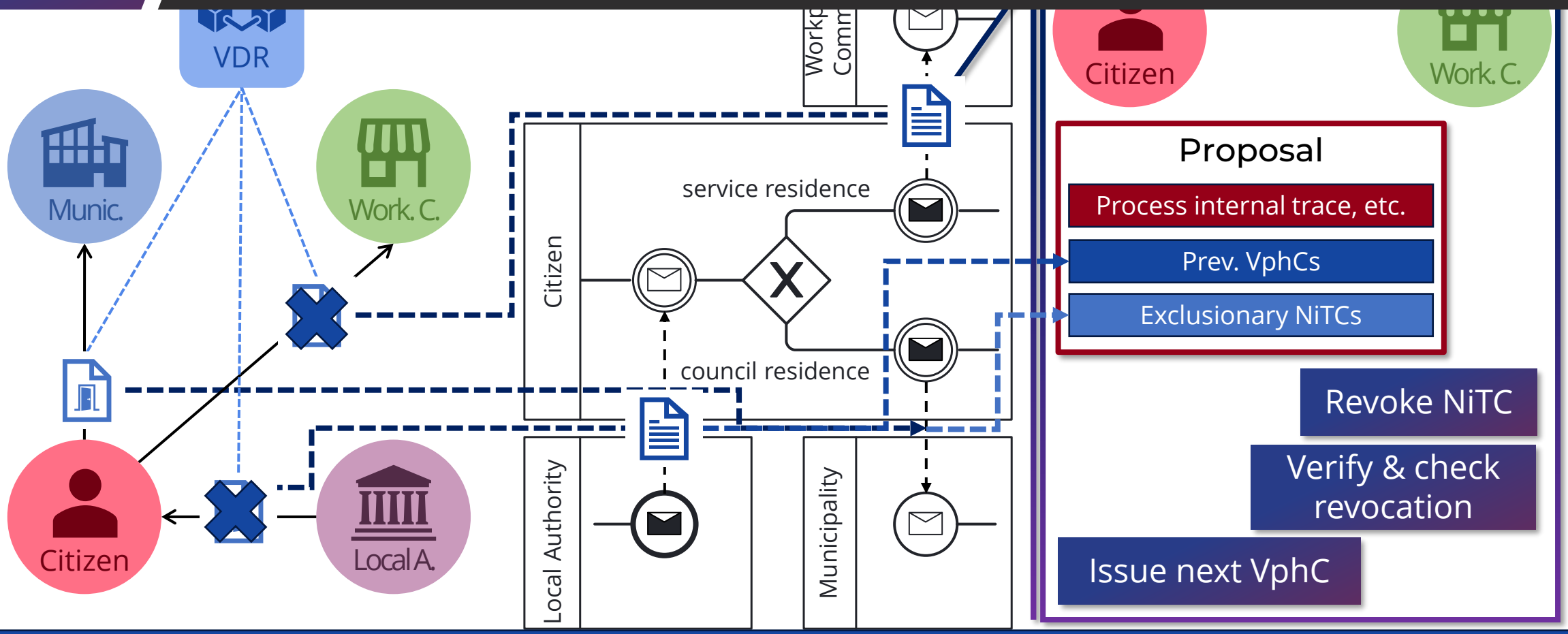
If ok, issue next VphC and continue

NiTC claims: message still may be sent

Avoiding ~~double spend~~ split brain problem

Problem

How can the Citizen convince the Committee that they did not take another invalid path (XOR-split)?



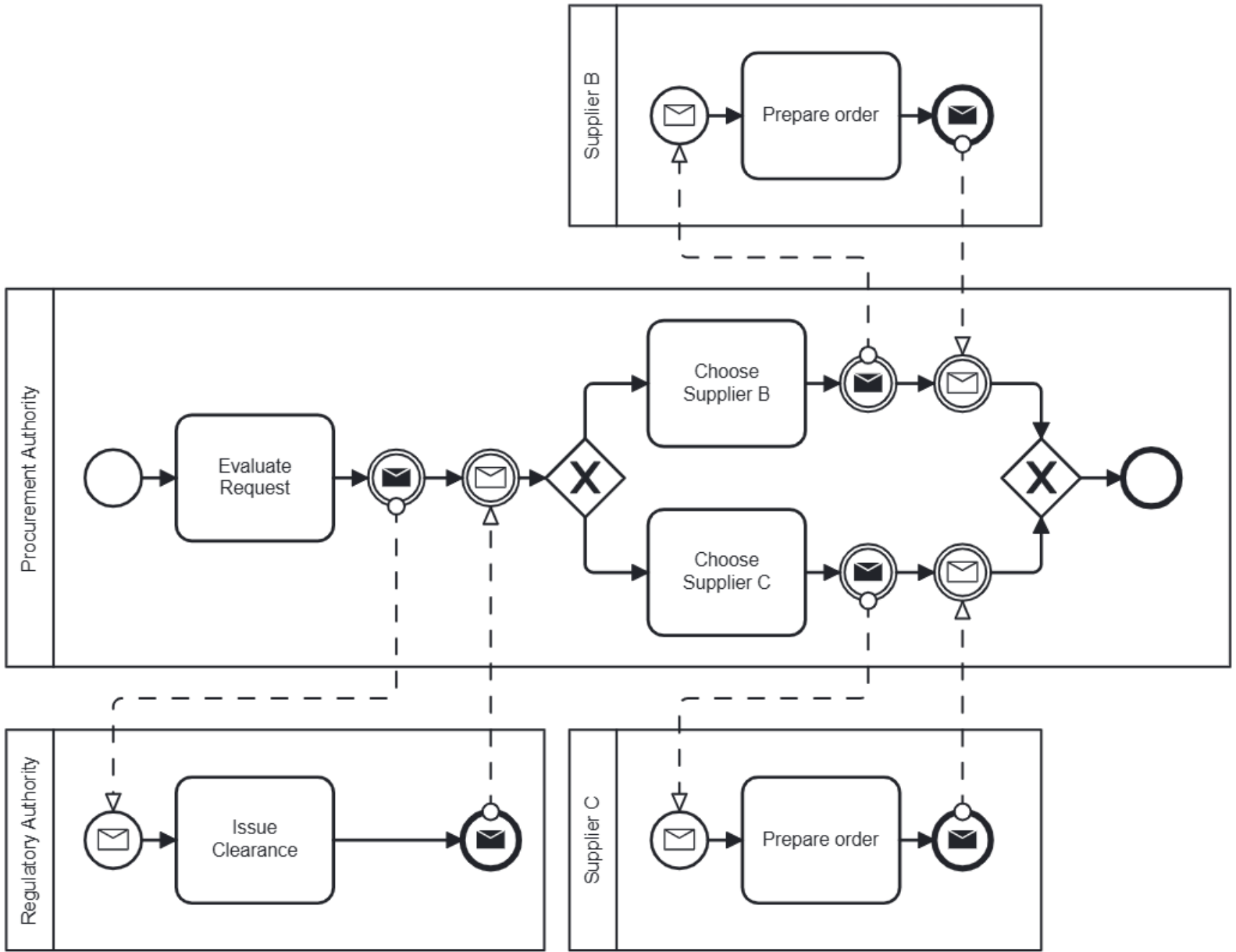
Details (and safety) a bit involved.
For (serious) liveness, needs a (linearizable) VDR with atomic revocation check + revoke (wip)

What this buys us – and what it does not

- Positives
  - Process orchestration without third party, smart contract, blockchain
  - All you need is a *process-oblivious* VDR
  - Privacy-preserving (modulo tx pattern analysis)
  - Existing representational/carrier standards
  - Small step to semantic interpretation (VCs/VPs are knowledge graphs)

- Current downsides
  - Guarantees meaningfully weaker than smart contracts
  - E.g., malicious recipients
  - “Straightforward” only for single malicious actors (multiparty collusion proofs: wip)
  - VDR with atomic test and set necessary for strong safety + liveness?
  - Protocol finalization in progress
  - Optics: it’s just stateless blockchain/Canton/… (it isn’t)

From “we need proofs” to a grave realization



Observation: BPMN’s standard operational semantics treats attacks as nonexistent

Thesis: collaboration logics need internal threat analysis

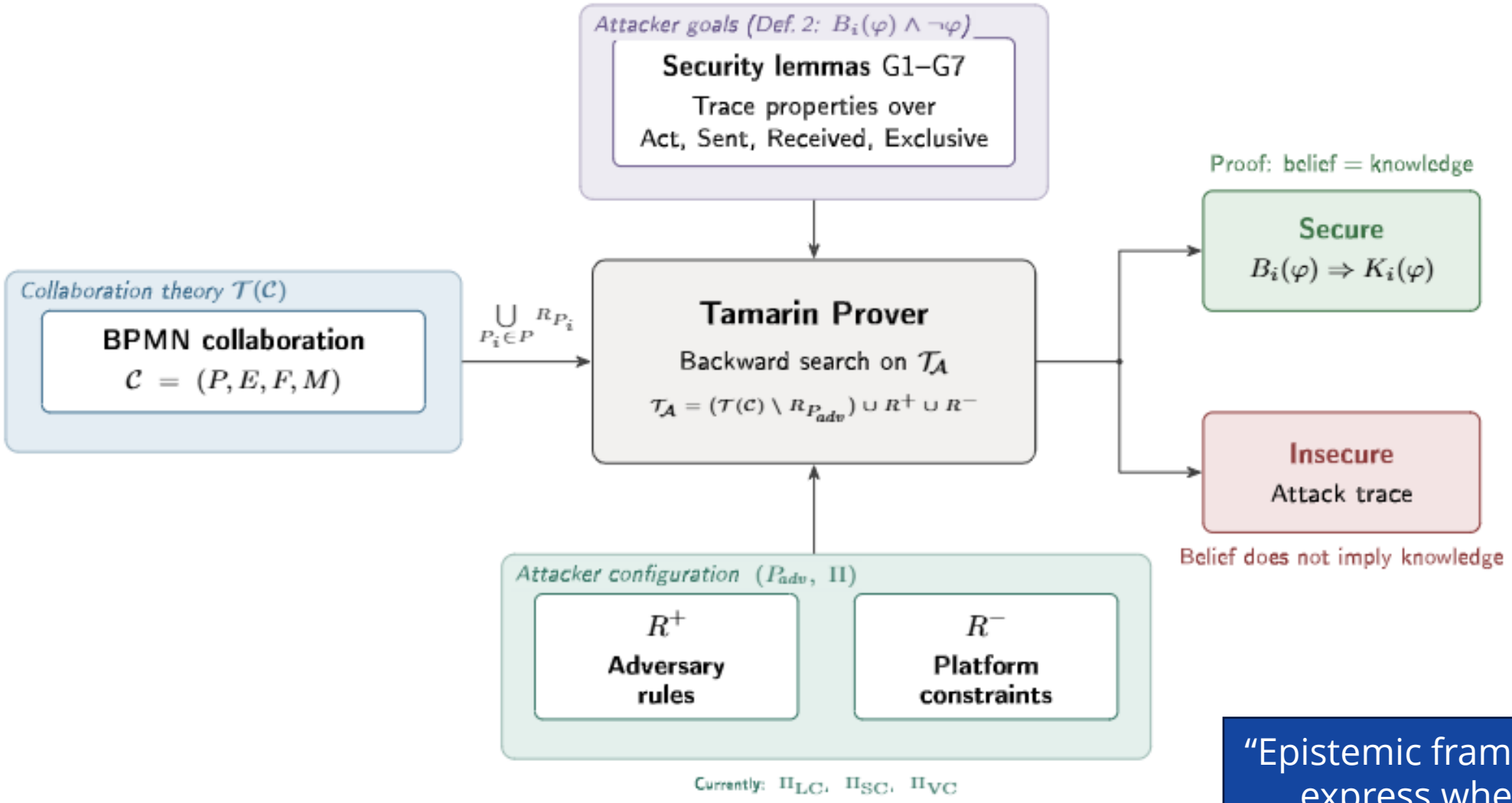
Approach:
Epistemic framing
Co-modeling of
logic + platform + attack primitives

Tool: Tamarin prover (multiset-rewriting + trace property formulas)

Accepted for BPM 2026 Foundations Track, “Trust No Pool: Formal Security Analysis of BPMN Collaborations”

ftsrg

A collaboration logic *is* a security protocol



"Epistemic framing": Tamarin theories express whether agents can be coerced (Byzantinely) to believe "not true" statements about process state

Definition 2 (Secure and Insecure Execution States). *Given epistemic execution model $\mathcal{M}$ and security properties $\Phi = \{\varphi_1, \ldots, \varphi_k\}$, a world $w \in W$ is secure iff for every honest participant i and every $\varphi_j \in \Phi$: if $B_i(\varphi_j)$ holds in w, then φ_j holds in w. A world is insecure if some honest participant holds a false security-relevant belief.*

Goal	Property	Π_{LC}	Π_{SC}	Π_{VC} (atomic)	Π_{VC} (non-at.)
G1	No-bifurcation	×	✓	✓	$\times^{\dagger}$
G2	Non-repudiation	✓	✓	✓	✓
G3	Faithful history	×	✓	✓	×
G4	Auth. progression	✓	✓	✓	✓
G5	Process progress	B^{a}	B^{a}	B^{a}	B^{a}
G6a	Value secrecy	×	×	✓	✓
G6b	Structural secrecy	$\times^{\text{a}}$	—	$\times^{\text{a}}$	$\times^{\text{a}}$
G7	Instance isolation	×	✓	✓	✓

Comparing loose coupling, orchestrator smart contracts, VCs-with-atomic-test-and-set-VDR, VCs-with-standard-VDR

Ongoing work

- Final protocol spec + properties + application-independent proofs
- Privacy-preserving, atomic test-and-set VDRs (scroll.io and Fabric)
- SDK & wallet framework

- Application for agentic collaborations (“data veracity” in EU data spaces)
- Epistemic (epistemic-alethic?) false claim impact analysis in VC lattices
- Claim risk mitigation strategies (Laprie et al. transfers – to an extent)