
27 March 2026

# ***Authority is Not a Token***: *How Provenance Identity Continuity Rewrites the Ontology of Decentralized Finance*

***DeFi & Crypto @ SNS Pisa***

**Nicola Gallo**
Author

*Co-founder, Nitro Agility S.r.l.*

Co-Chair, Trusted AI Agents Working Group
Decentralized Identity Foundation (DIF)

*Formerly: JPMorgan, Citi, Société Générale*

**Stefano Silvestri**
Co-author

*Researcher at Institute for High Performance Computing and Networking of National Research Council of Italy (ICAR-CNR)*

When we make a payment or interact with a system, we typically connect, authenticate, and receive a access token or credential.

Today, I argue that possession-based mechanisms have worked, but they are a limiting factor for distributed and decentralized systems.

Smart contracts automate execution, but they do not remove the need to manage authority.

Proof of Possession comes with well-known categories of attacks.

The industry has continuously tried to mitigate them, but has never solved the problem at a structural level.

Is blockchain just a better mitigation or an actual structural solution?

# Examples of Possession-Based Authority: Known Attack Patterns

## Traditional Systems

- Confused Deputy: valid credentials, wrong intent
- Token leakage / reuse: stolen or misapplied authority
- Over-scoped permissions: authority exceeds original intent

## DeFi Systems

- Allowance abuse: approvals reused outside intent
- Composability exploits: unintended authority propagation via contract composition
- Flash-loan governance attacks: temporary possession = power
- Governance capture: authority equals token ownership
- MEV extraction: control by transient possession

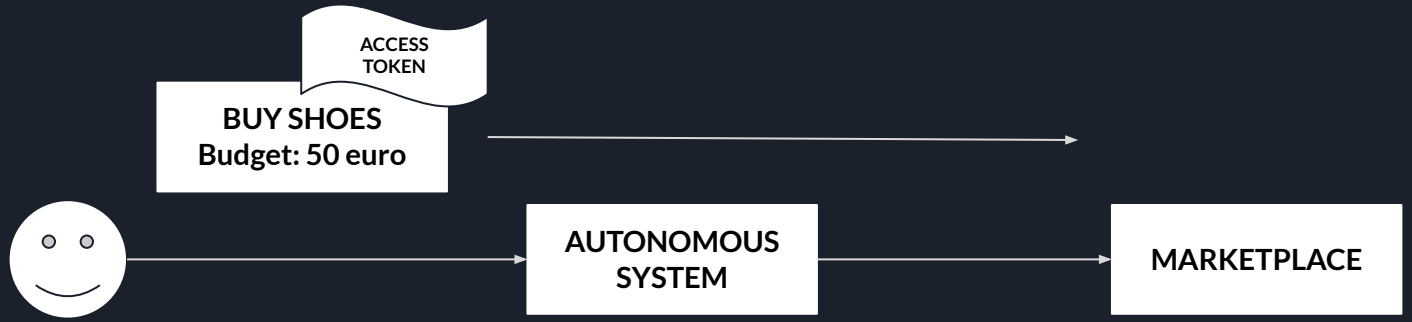
Proof of Possession is a mechanism.

What if it is actually a structural limitation for distributed and decentralized systems?

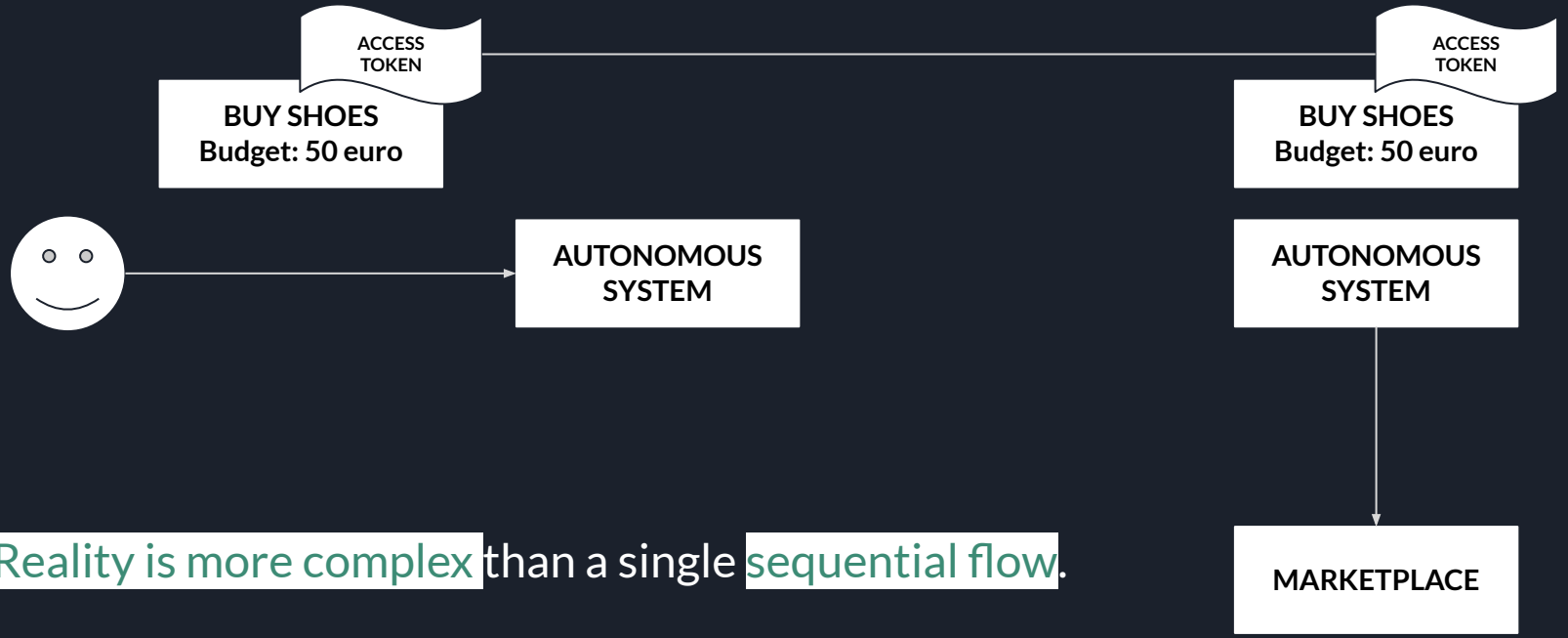
# A Simple Delegated Payment

Let’s start with something everyone understands: a simple delegated payment.

A user wants to buy a pair of shoes and delegates the execution to an autonomous system.

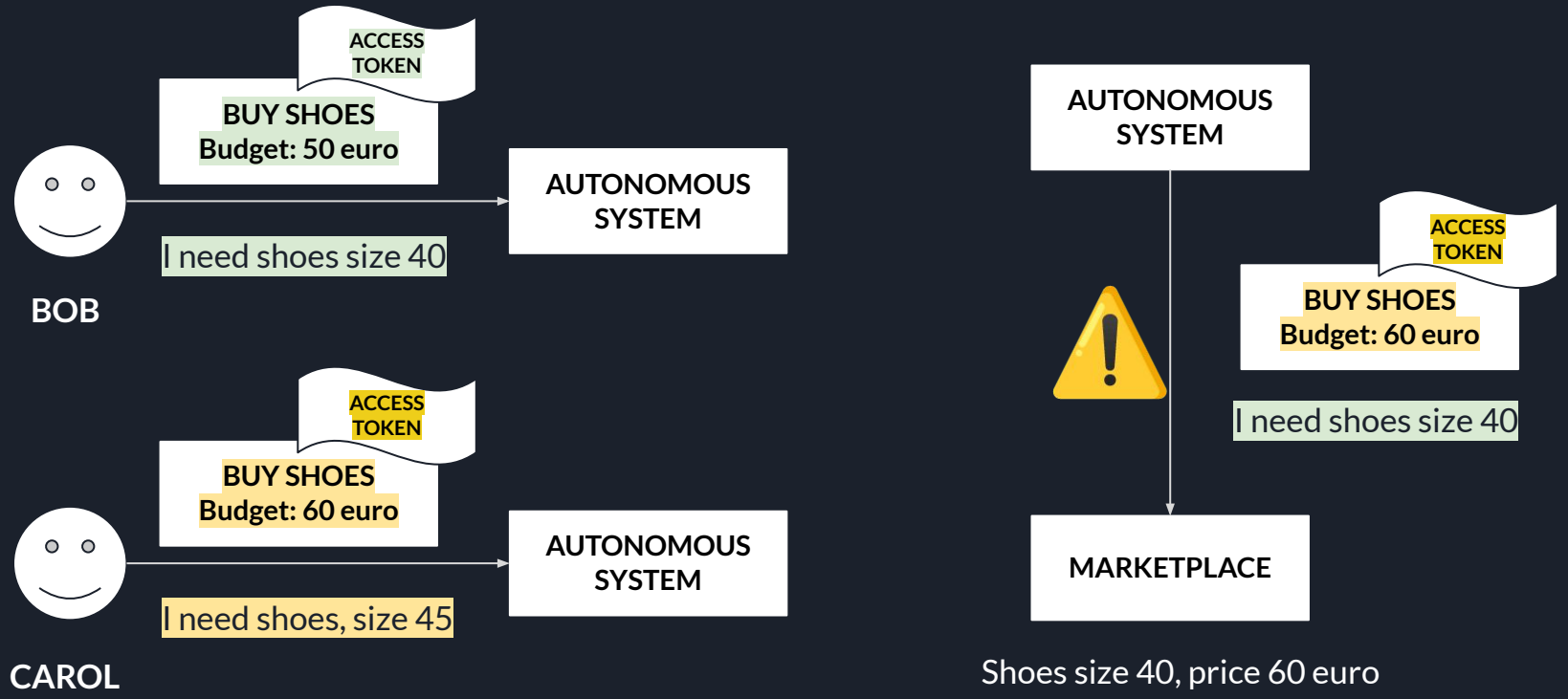


# A Simple Delegated Payment




Reality is more complex than a single sequential flow.

# A Simple (Confused) Delegated Payment



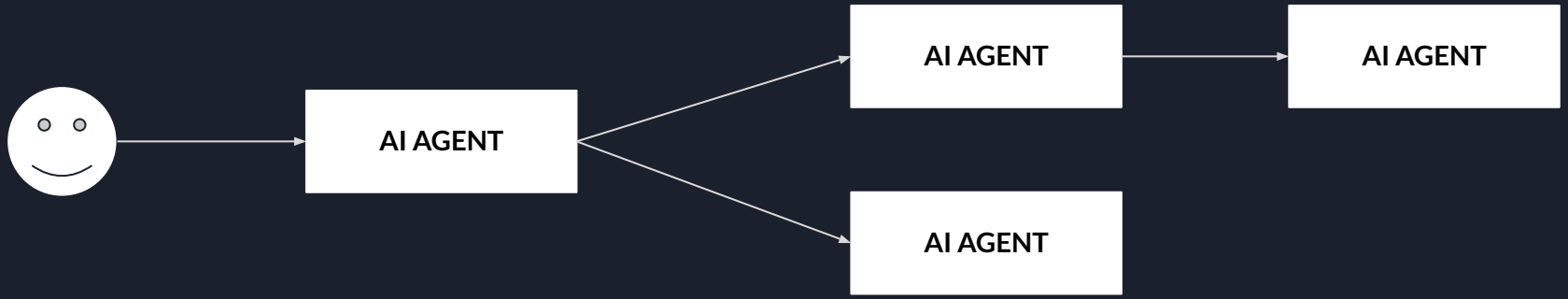
# Confused Deputy Problem

This is not a new bug.

It is a modern revision of the Confused Deputy problem, first described in 1988, and still unsolved.

# Confused Deputy Problem

AI agents are making these problems explicit.




Can I trust the configuration of something I don’t control, and don’t know who will physically operate, while it acts autonomously on my behalf?

Before building complex decentralized systems, we must first understand how authority works.

JOURNEY

# The journey starts with a simple question

What if possession is not a security primitive, but the problem itself?

# The Ontological Shift Begins Here

The journey started with a simple question:

we keep fixing problems caused by possession-based security, but what if possession itself is the structural flaw?

The unresolved Confused Deputy problem seems to be the evidence.

So this is what we need to solve.

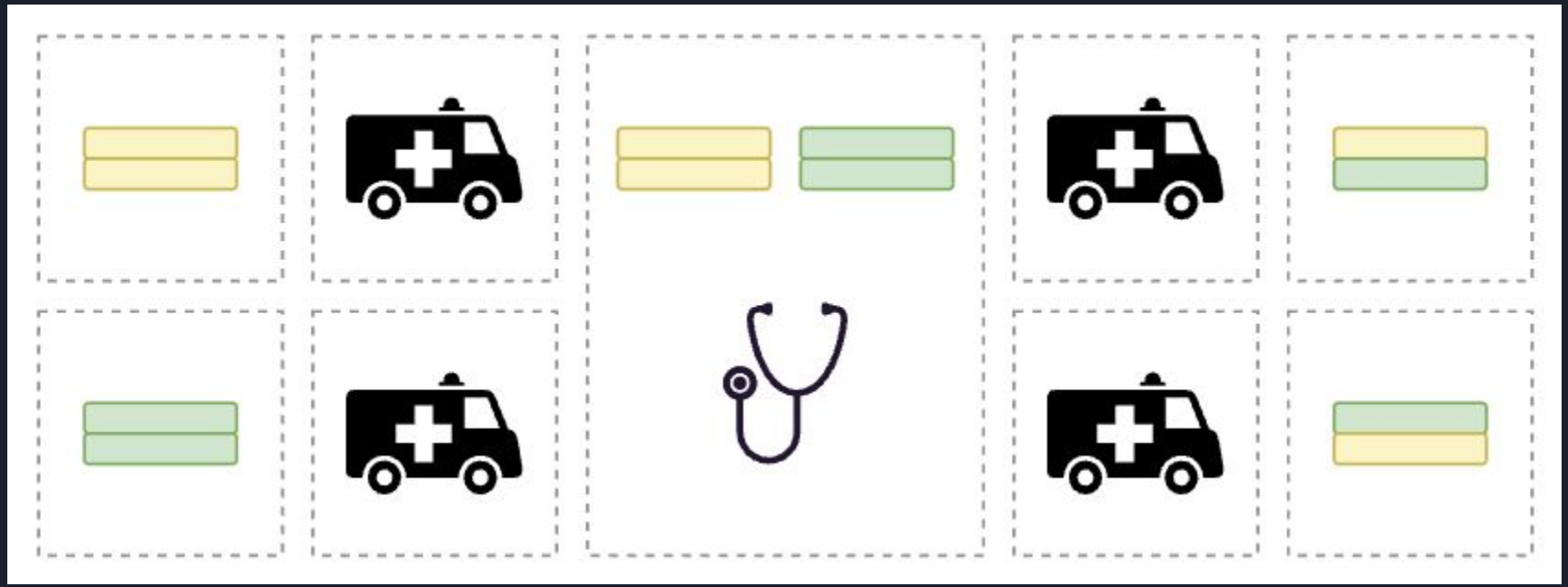
# The Research

This research led to the understanding that authority is a continuous system, in which every executor operates under the authority of the initiator.

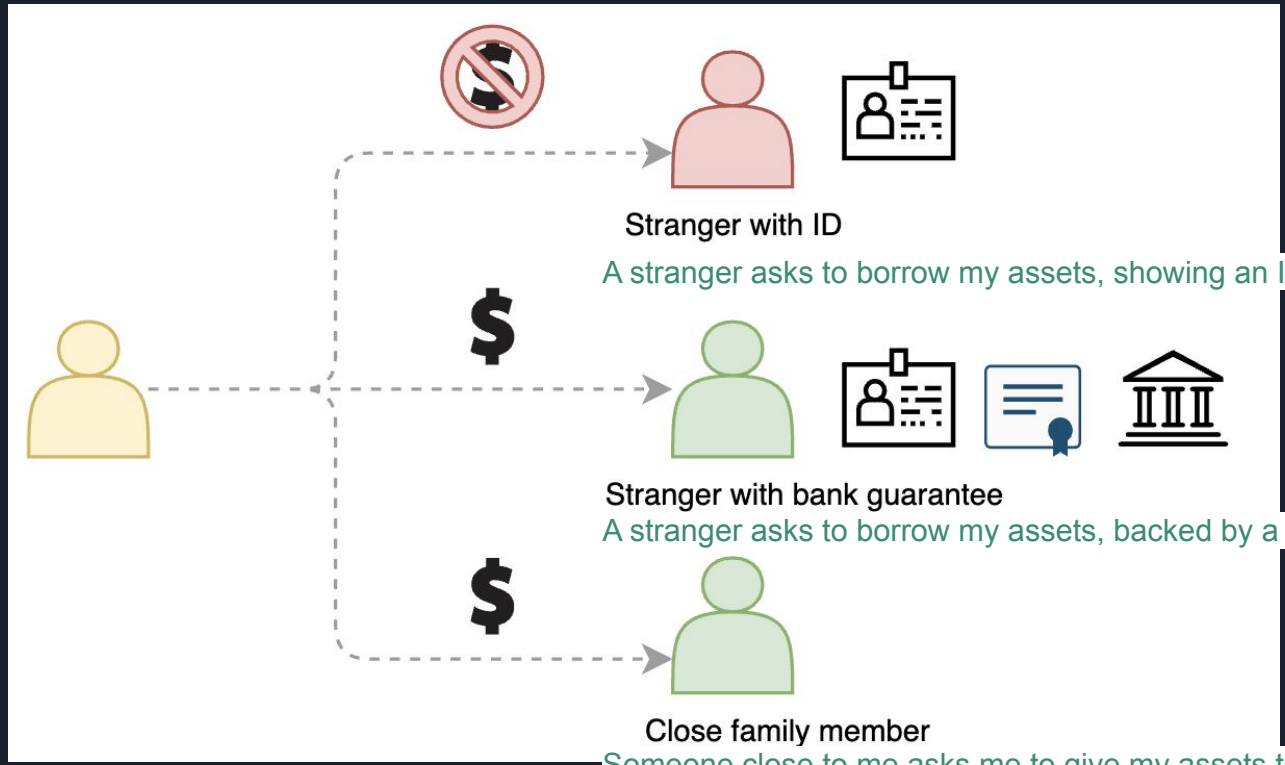
This naturally introduces a new primitive: Proof of Continuity.

To understand this, we can observe how humans already operate with authority at a social level.

# Authority & Supply Chain



# The Same Loan Request, Different Authority



Based on these examples, it should be clear that we can construct an authority model in which relationships are more fundamental than possession.

Authority is a continuous system. Each executor must be able to prove continuity through a Proof of Continuity.

Continuity is established through relationships, hence, a Proof of Relationship, not through possession.

This introduces a new ontology of authority, formally proven.

# The Authority Model

Authority is modeled as a sequence, not a permission.

Each step can only act within a subset of the original authority.

Authority is monotonic, it can only decrease, never expand.

$$\pi = \langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$$

$$\pi = \langle (p_0, ops_0), (p_1, ops_1), \ldots, (p_n, ops_n) \rangle$$

$$ops_n \subseteq ops_0$$

monotonic

$$\forall i : \ \mathrm{ops}_{i+1} \subseteq \mathrm{ops}_i$$

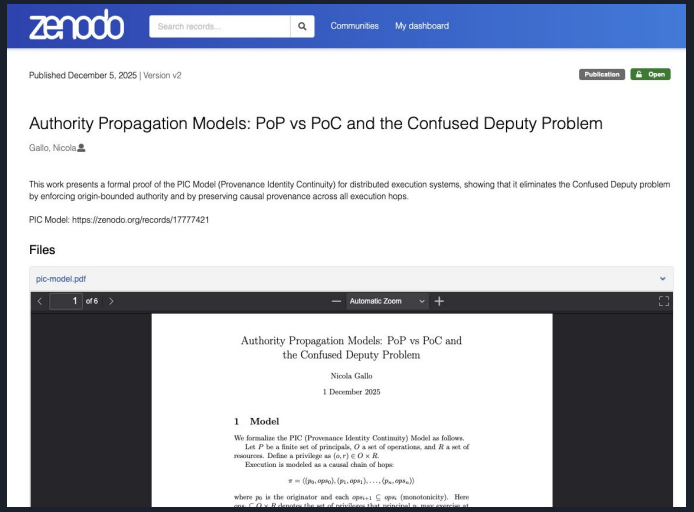
$$\forall i : \ p_0^{(i)} = p_0^{(0)}$$

Immutable origin

# The Authority Model

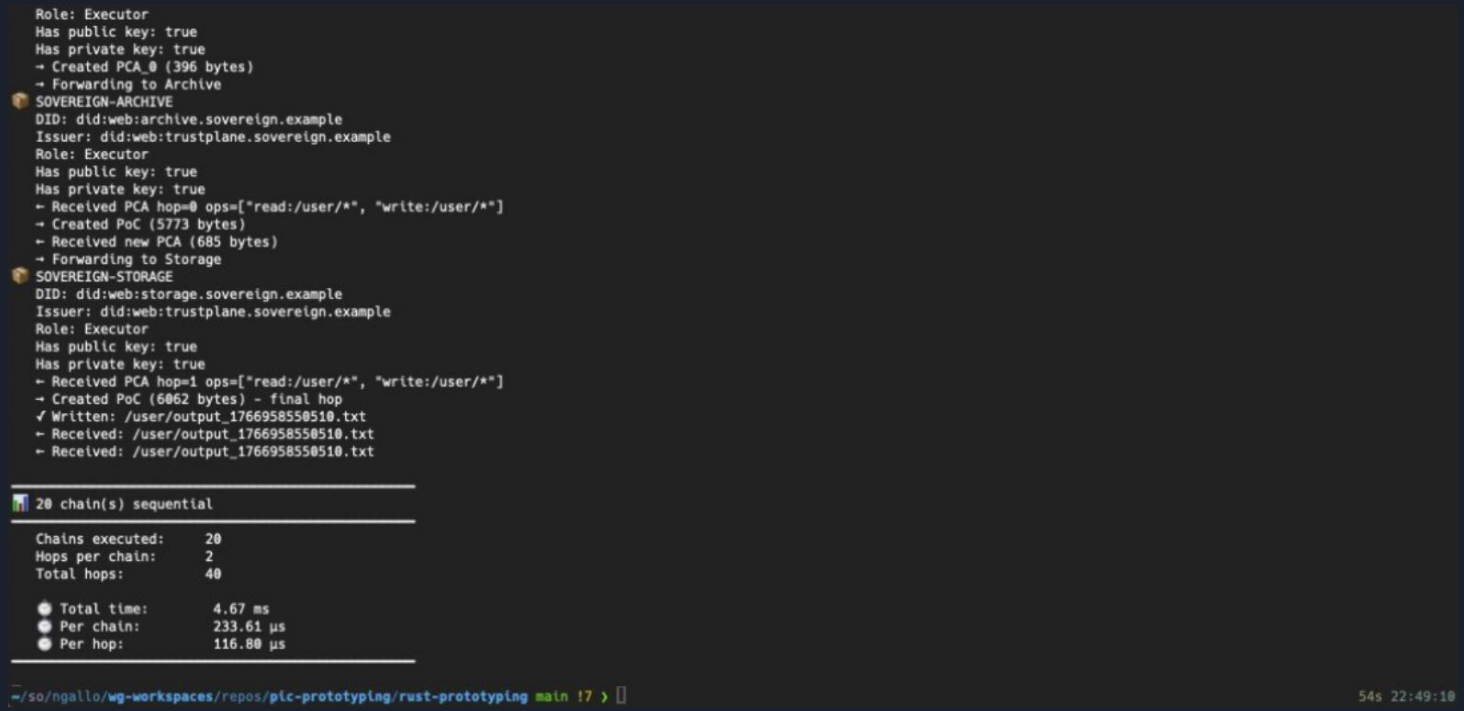
Under this model, certain attacks are not mitigated.

They become non-formulable.




Gallo, N. (2025). Authority Propagation Models: PoP vs PoC and the Confused Deputy Problem. Zenodo. https://doi.org/10.5281/zenodo.17833000

When an idea stops being theory and starts matching reality, including at scale and speed it deserves to be shared.



# Provenance Identity Continuity (PIC) Model


## Provenance

*The causal chain is always traceable and auditable. From Origin to end, unbroken. If it breaks, it stops.*

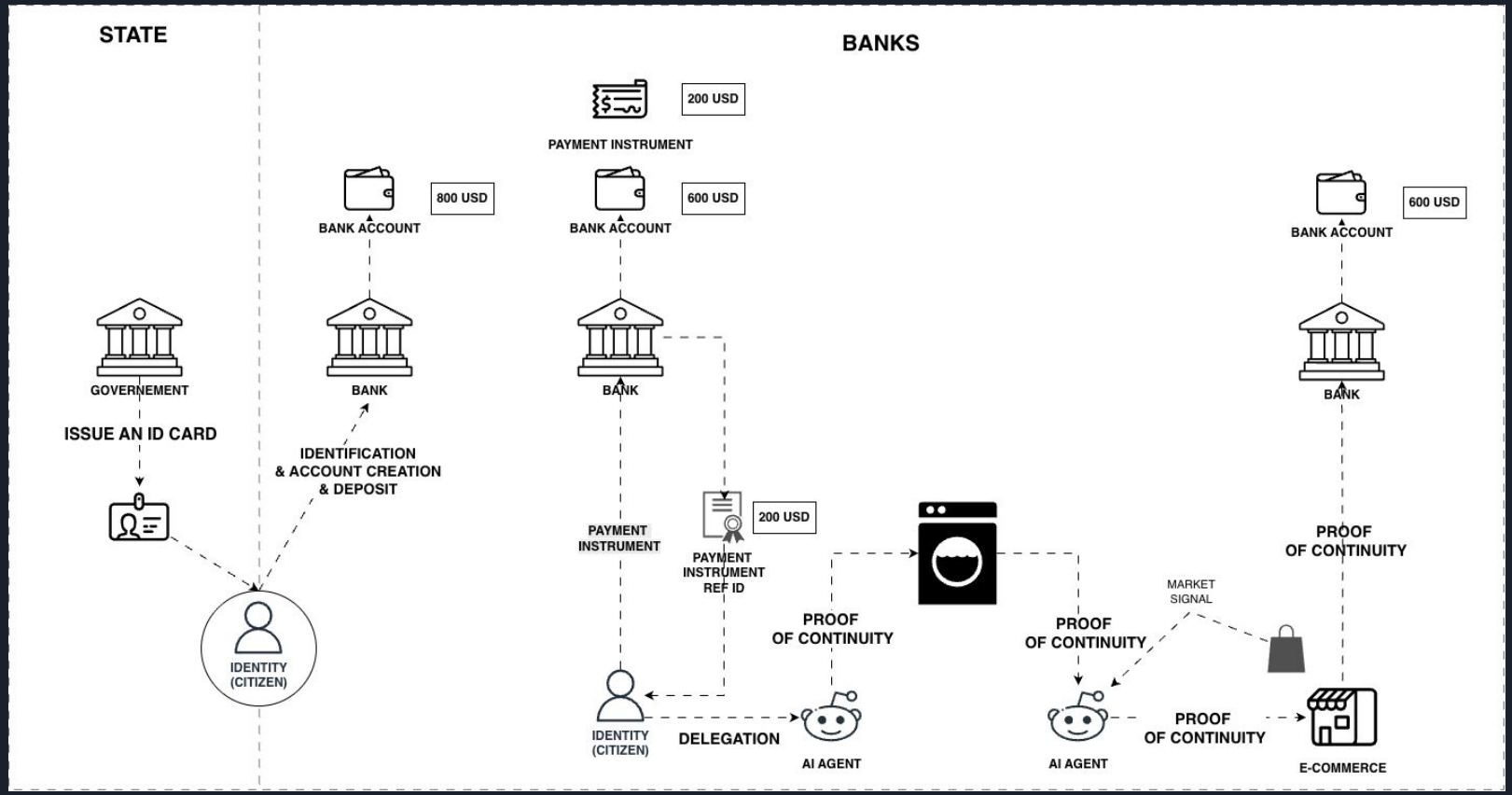
## Identity

*The origin identity is immutable. It generates authority. It cannot change throughout the chain.*

## Continuity

*Continuity is proven at every step. Proof of Continuity replaces Proof of Possession. Authority can only shrink.*

# A payment example with PIC



## If banks execute on blockchain with PIC

Assume a realistic scenario:

Banks:

- use blockchain as a settlement layer
- retain backend systems and regulatory compliance

PIC:

- guarantees authority, continuity, and accountability
- enables secure execution without parasitic MEV

Result:

- faster payments
- lower costs
- clear responsibility
- no unnecessary intermediaries

- If banks execute on blockchain with PIC, most retail DeFi use cases lose their advantage.

- What survives is only DeFi with a structural reason to exist: permissionless access, global neutrality, and autonomous agents.

- PIC does not replace DeFi—it filters it, removing speculative layers and exposing real infrastructure value.

# One possible outcome…

Bitcoin vs Ethereum under Institutional Execution

- Bitcoin benefits from scarcity. Its value proposition is monetary and largely independent from execution quality.
- Ethereum benefits from better execution. Its value grows as execution becomes safer, more accountable, and institution-ready.
- With PIC, Ethereum evolves into institutional infrastructure. Execution quality improves → trust increases → real adoption → value is captured at the base layer.

By now, it should be clear that authority is foundational.

It is not a side effect of execution, nor the same as possession.

Changing how we understand authority changes what systems we can build.

Clear boundaries—what belongs on-chain, inside transactions, and outside both—are essential.

Only with this clarity can distributed systems, AI agents, and DeFi reach real-world adoption.

## What contract law discovered socially, PIC captures structurally.

Three actors:

- A = debtor
- B = creditor
- C = guarantor

The guarantor doesn't replace A—they bind themselves to cover if A defaults.

PIC representation:

ops_0 (A → obligation X owed to B) → ops_1 (C guarantees X to B if condition Y)

Key properties:

- Immutable origin → obligation starts from A
- Causal continuity → C's commitment ties to the same obligation
- Monotonicity → no new control rights, only additional liable parties
- Non-fusion → C cannot alter the original obligation

The guarantor attaches to an existing chain with a liability clause—no new authority created.

PIC

Not a Policy.
Not a Token.
An *Ontological Shift*
Proven Mathematically.

*JOIN THE PIC SLACK CHANNEL*

www.pic-protocol.org

Thank you!