8TH DISTRIBUTED LEDGER TECHNOLOGY WORKSHOP

Pula · June 2026

Which Blockchain Technology Best Supports Self-Protecting Systems?

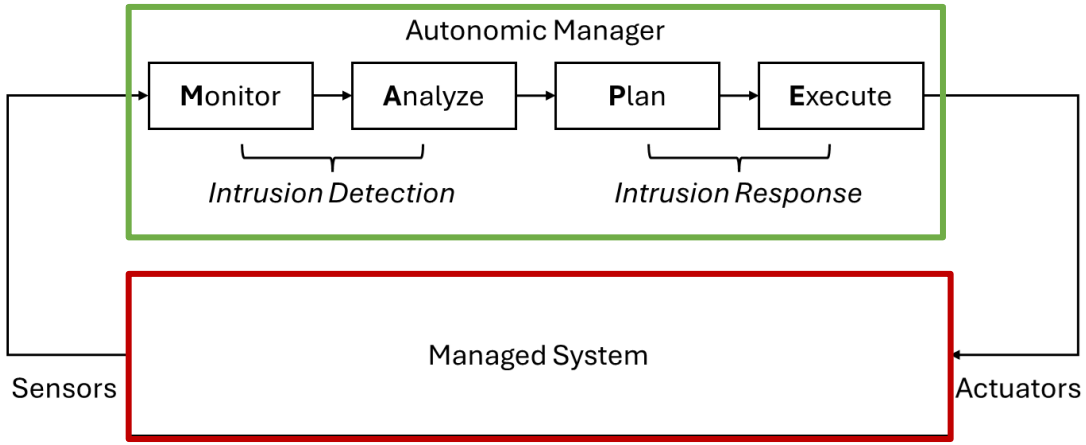
A comparison between Quorum and CometBFT

S. Albero · V. Tatti · D. Pennino · T. Caiazzi · S. Iannucci · M. Pizzonia

Roma Tre University · University of Tuscia

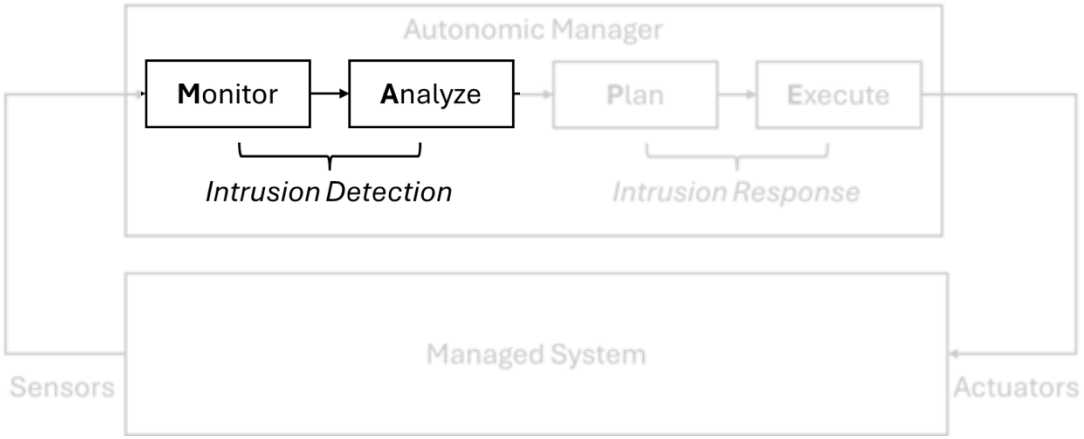
Research on SPS

- **Autonomic architecture and self-management frameworks**



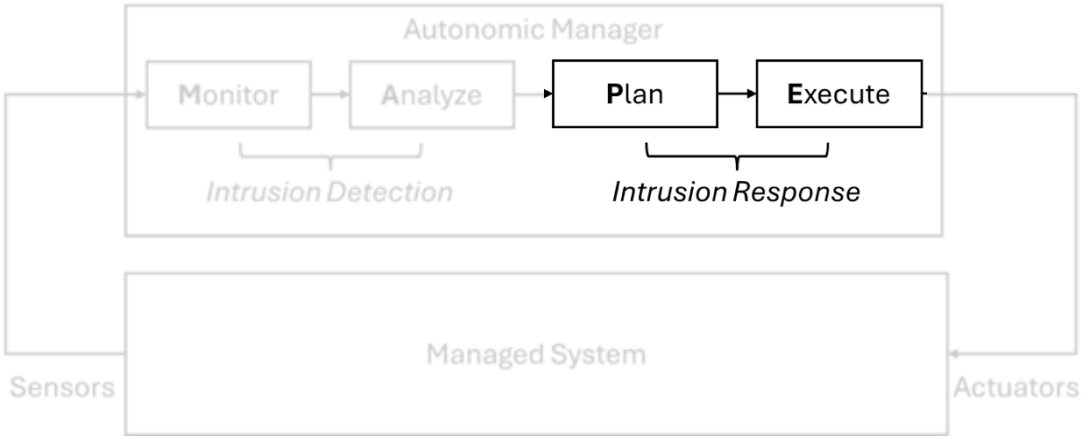
Research on SPS

- Autonomic architecture and self-management frameworks
- **Threat detection and anomaly identification**



Research on SPS

- Autonomic architecture and self-management frameworks
- Threat detection and anomaly identification
- **Autonomous response and recovery**

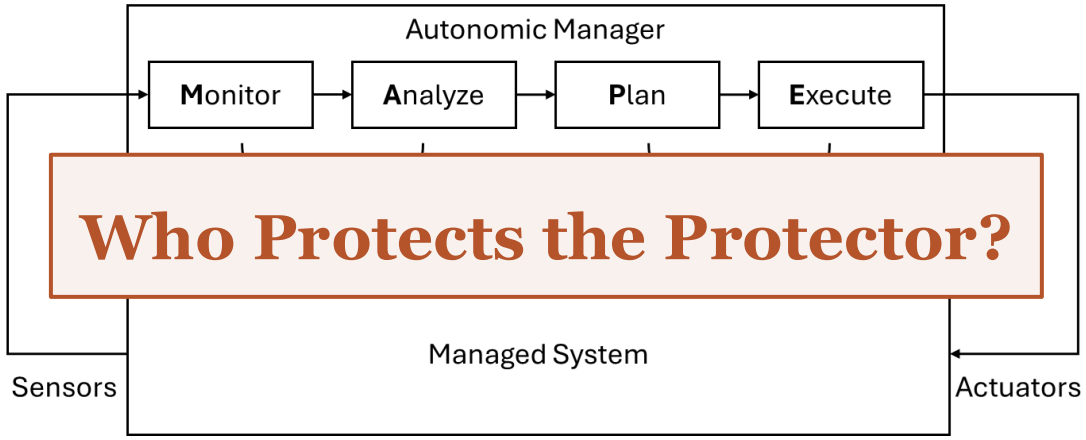


Research on SPS

- Autonomic architecture and self-management frameworks
- Threat detection and anomaly identification
- Autonomous response and recovery

… But what about attacks to the autonomic manager?

↑ *Don't leave him alone!*



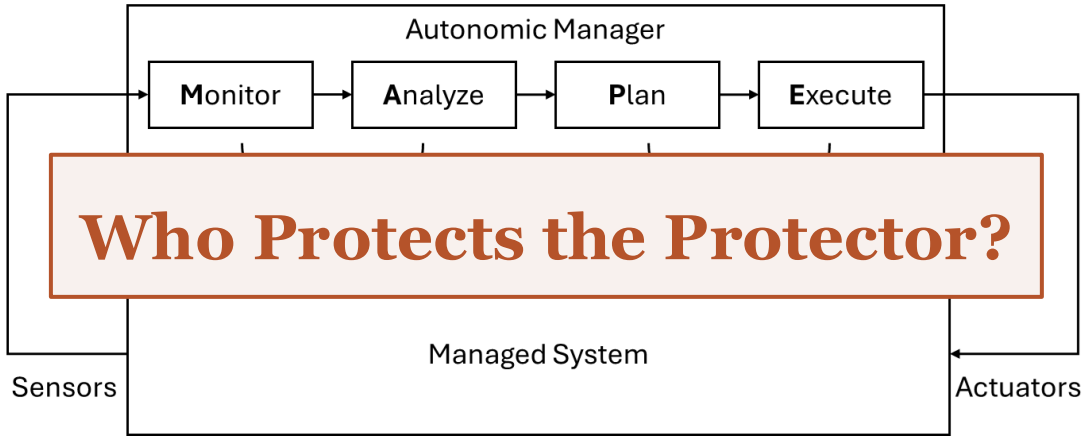
Can we design a Secure-by-Design SPS?

- **The structural weakness**

  Centralizing detection & response in one manager creates a single point of compromise

- **The consequence**

  If the manager is subverted, the whole system's security collapses



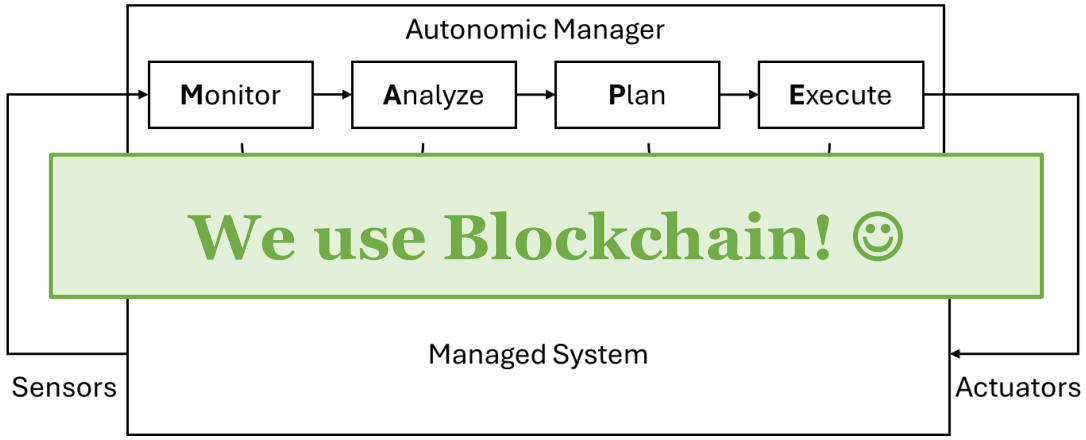
Can we design a Secure-by-Design SPS?

- **The structural weakness**

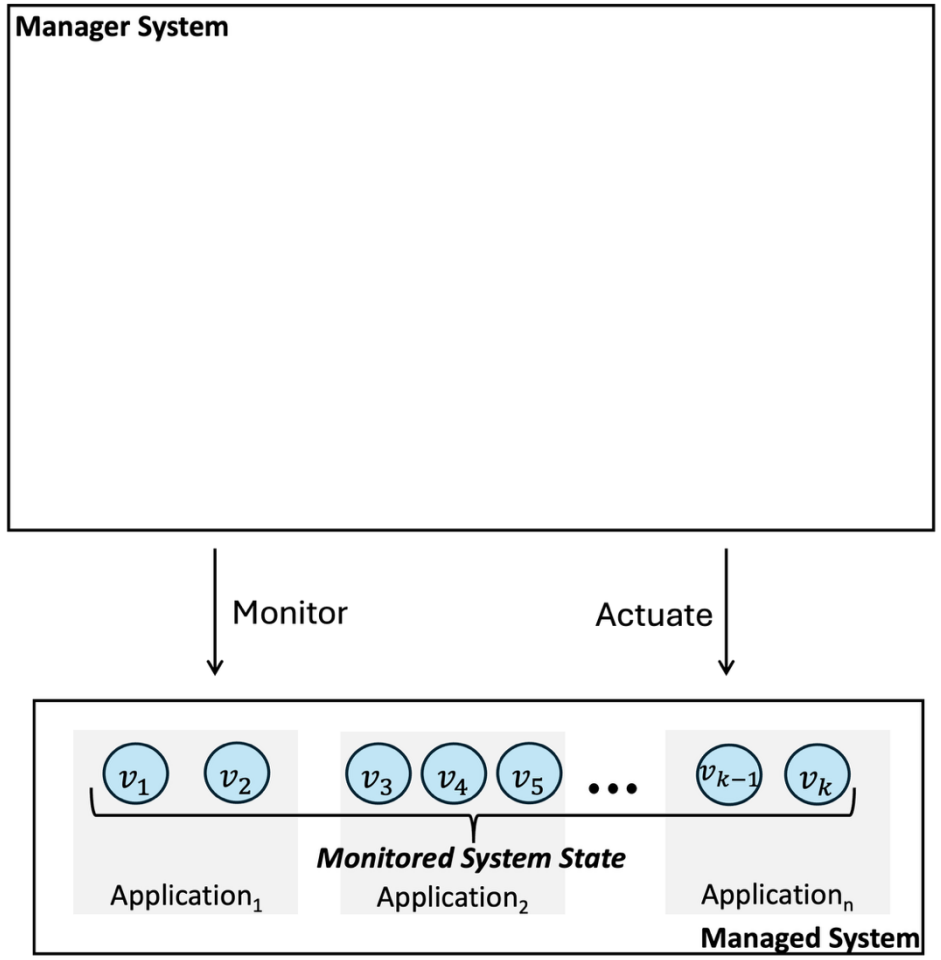
  Centralizing detection & response in one manager creates a single point of compromise

- **The consequence**

  If the manager is subverted, the whole system's security collapses



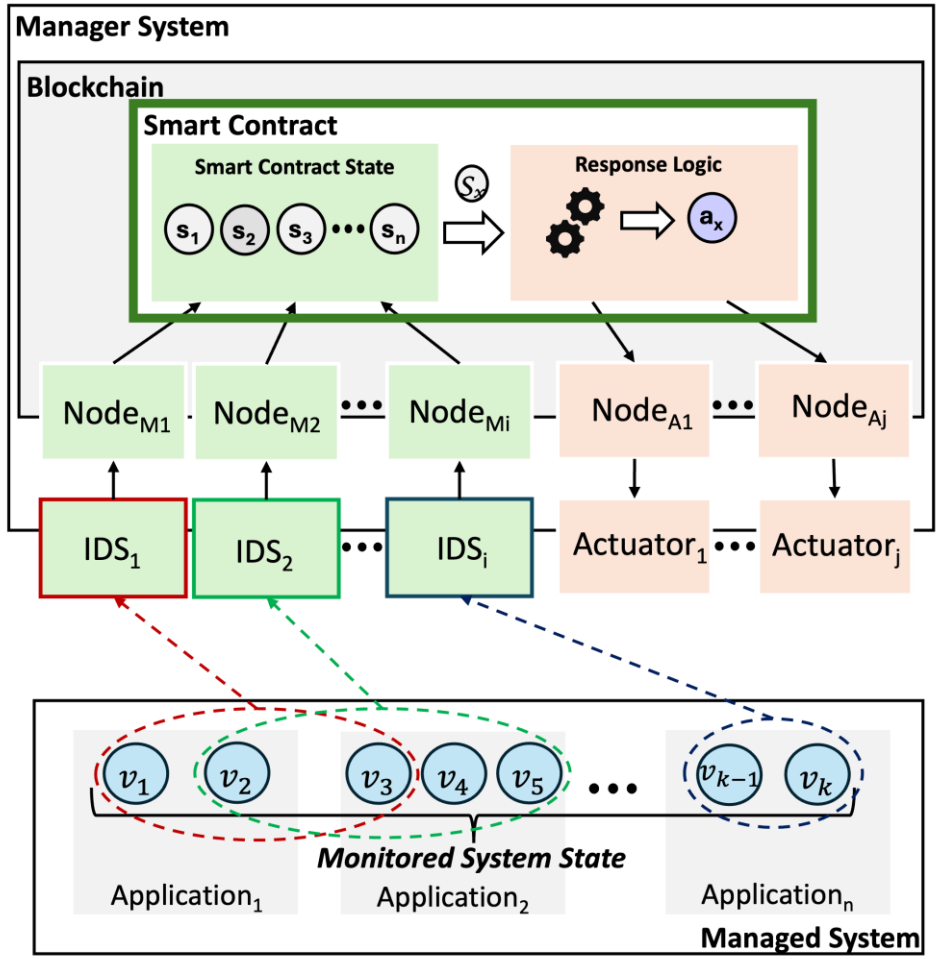
Reference from previous work



- **Manager and Managed System**

Caiazzi, et al. "A Novel Architecture for Cyber-Resilient Self-Protecting Systems Based on Blockchain." 2025

Reference from previous work

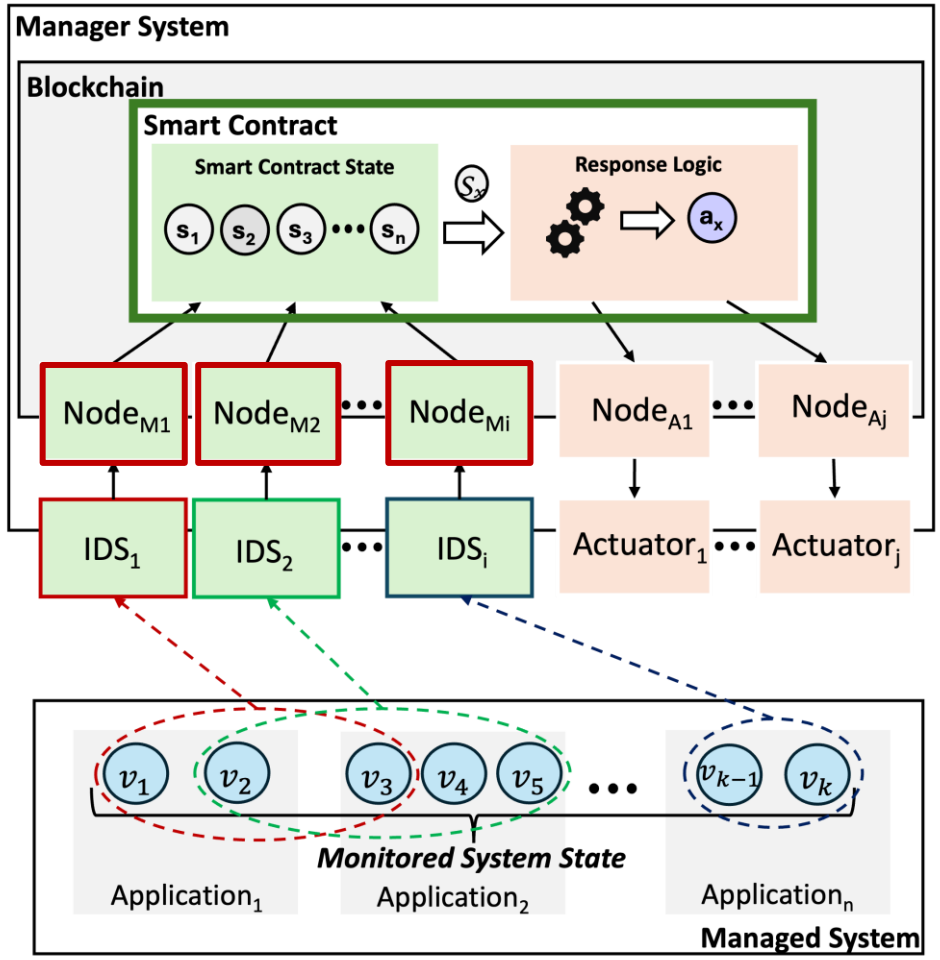


- **Manager and Managed System**
- **IDS alerts as transactions**

  Signed alerts are submitted to a shared smart-contract state.

Caiazzi, et al. "A Novel Architecture for Cyber-Resilient Self-Protecting Systems Based on Blockchain." 2025

Reference from previous work



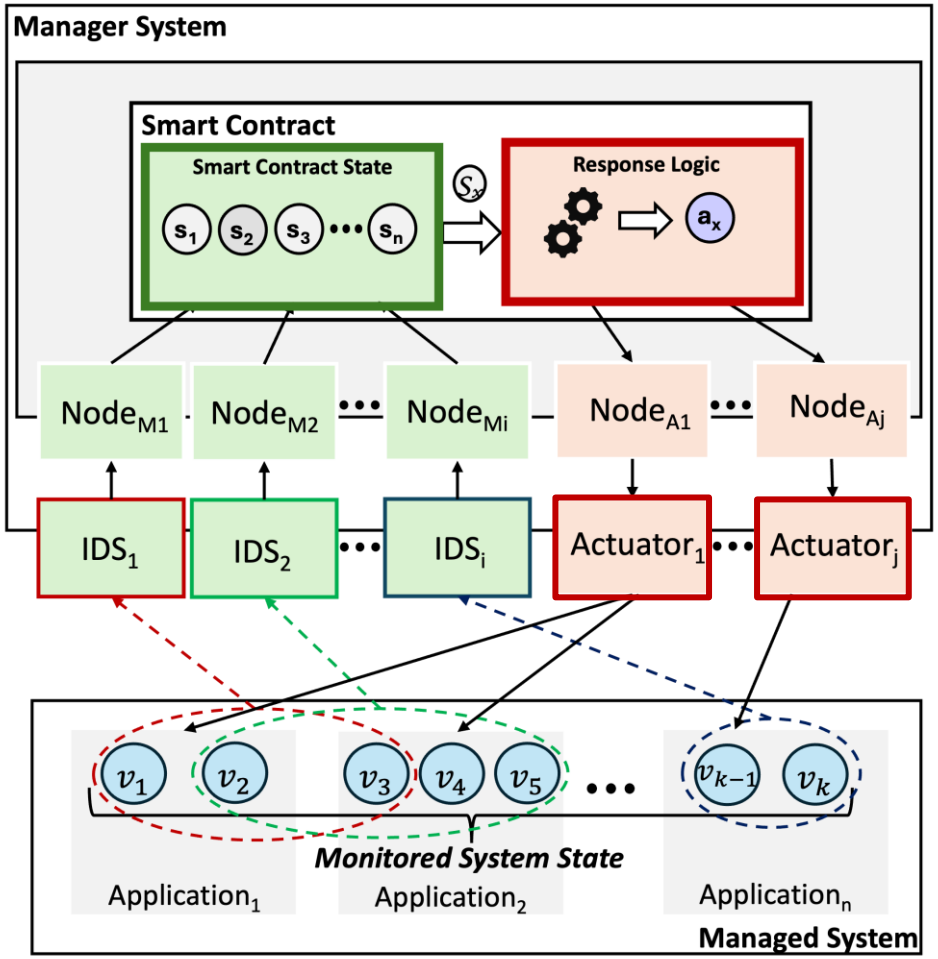
- **Manager and Managed System**
- **IDS alerts as transactions**

  Signed alerts are submitted to a shared smart-contract state.
- **Consensus tolerates compromise**

  BFT keeps the manager correct even if up to 1/3 of replicas are subverted.

Caiazzi, et al. "A Novel Architecture for Cyber-Resilient Self-Protecting Systems Based on Blockchain." 2025

Reference from previous work



- **Manager and Managed System**
- **IDS alerts as transactions**

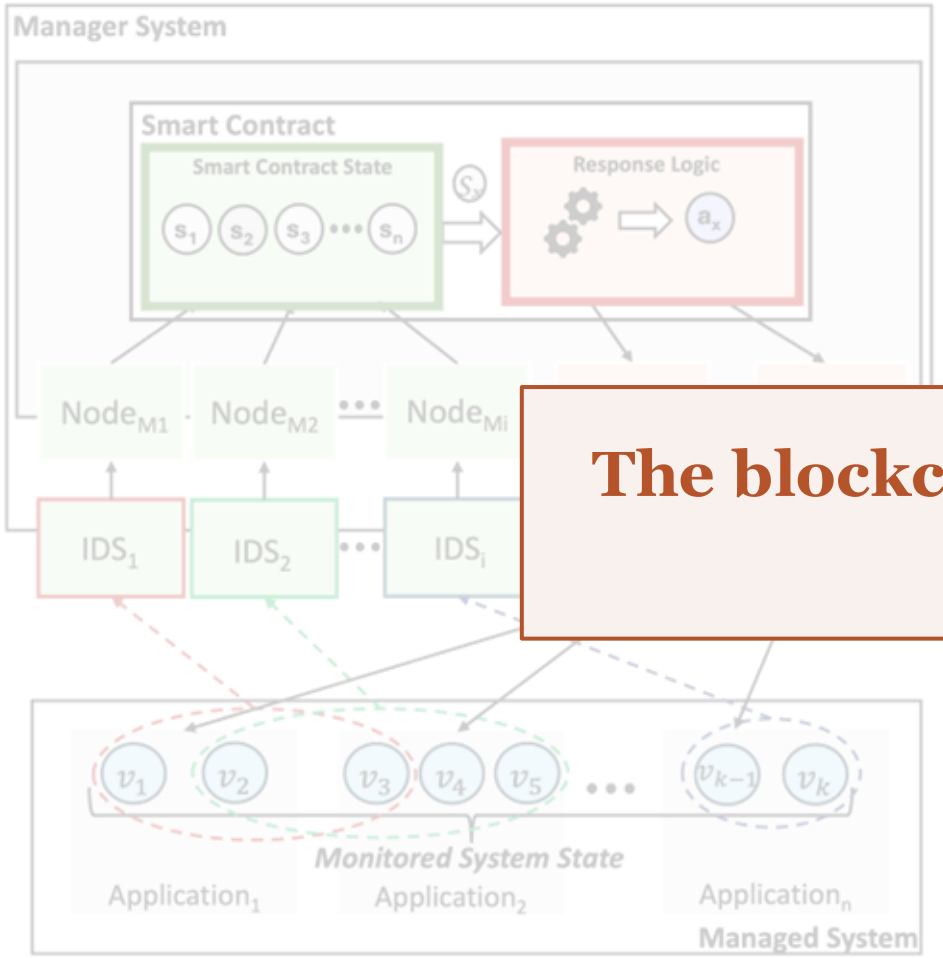
  Signed alerts are submitted to a shared smart-contract state
- **Consensus tolerates compromise**

  BFT keeps the manager correct even if up to 1/3 of replicas are subverted
- **Blind actuators**

  Actuators enforce countermeasures without reading the managed system

Caiazzi, et al. "A Novel Architecture for Cyber-Resilient Self-Protecting Systems Based on Blockchain." 2025

Reference from previous work



The blockchain layer was Quorum

But … ☹

- **Manager and Managed System**
- **IDS alerts as transactions**

  Signed alerts are submitted to a shared smart-contract state.
- **Consensus tolerates compromise**

  even if up to 1/3 of replicas

ures without reading the managed system.

The choice of platform is not neutral

The blockchain platform should follow from what it actually needs, not from what is popular by default. Three properties matter:

- **Minimal**
  Only a small, deterministic state machine, no general-purpose VM, no unused machinery
- **Deterministic & Byzantine-resilient**
  A single authoritative state that holds even if up to 1/3 of the nodes are compromised
- **No economic layer**
  Gas, fees and token incentives govern open networks. In a closed permissioned setting they are pure overhead

↑ *the SPS verdict on gas fees*

What an SPS needs from a blockchain

REQUIRED

BFT consensus + finality

Permissioned membership

Event-driven blocks

DESIRABLE

In-memory state

Low, predictable latency

Graceful scaling

Configurable audit

Push notifications

NOT NEEDED

Gas / fees

PoW / PoS

General-purpose VM

Fixed-interval blocks

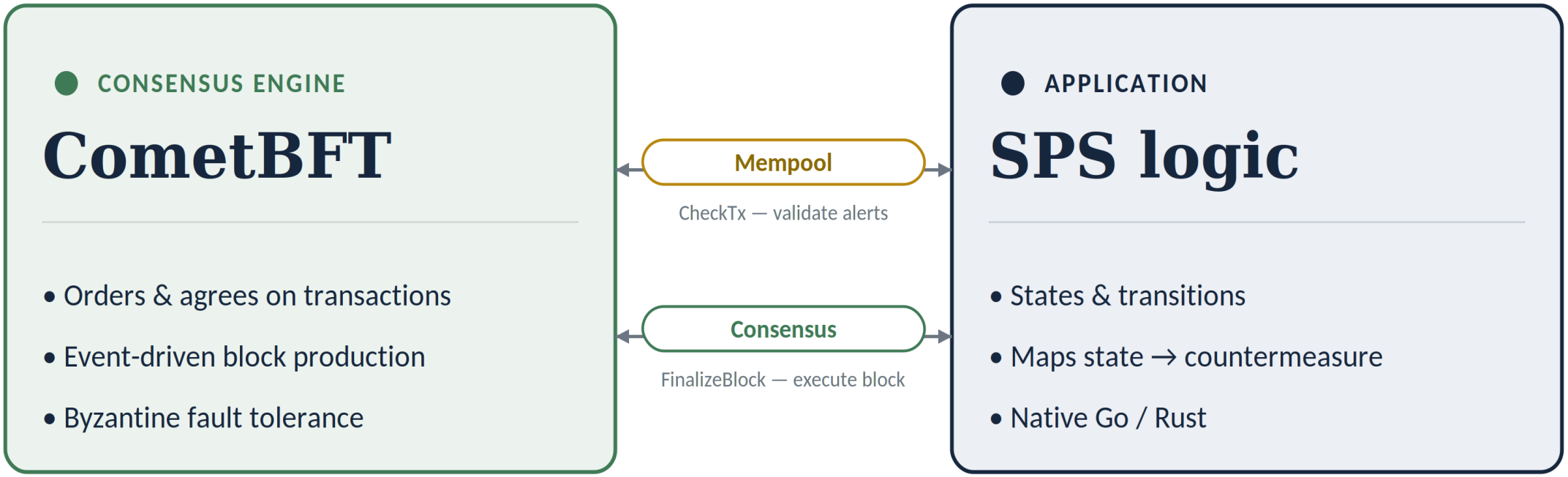
Token incentives

What an SPS needs from a blockchain

REQUIRED	DESIRABLE	NOT NEEDED
BFT consensus + finality	In-memory state	Gas / fees
Permissioned membershi		/ PoS
Event-driven blocks		ral-purpose VM
	Configurable audit	Fixed-interval blocks
	Push notifications	Token incentives

What architecture would meet these requirements?

A closer look at CometBFT



- **One catch**

  Membership and audit must be coded; more flexibility, more work

Why CometBFT over Quorum?

QUORUM

✓ **Ready out of the box**
minimal config needed

✓ **Native BFT & permissioned**
IBFT2 consensus, on-chain membership

✗ **EVM & gas = unnecessary overhead**
Unused in closed SPS

✗ **Fixed-interval blocks**
Idle blocks waste resources

CometBFT

✓ **No gas overhead**
Minimal ABCI app

✓ **Event-driven block production**
Blocks only when transactions arrive

~ **Requires ABCI app development**
Membership, audit, logic must be coded

~ **More initial configuration**
No built-in smart-contract layer

Research Questions

Q1 End-to-end latency

What end-to-end latency does the SPS introduce under low traffic conditions?

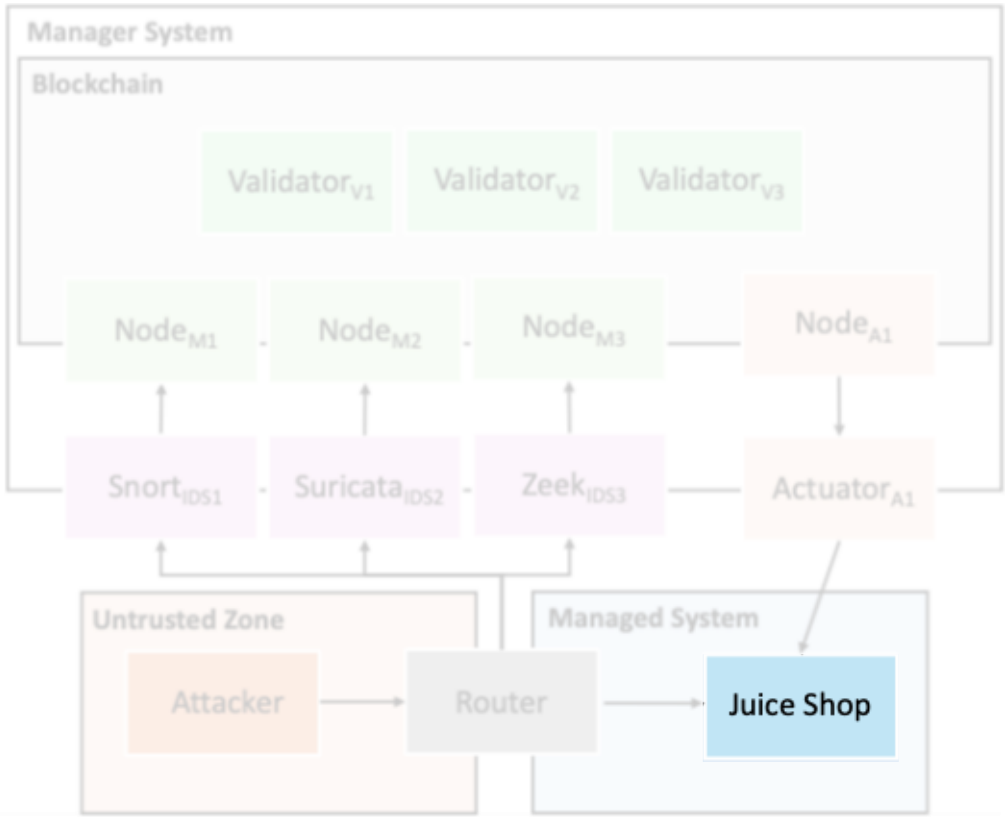
Q2 Transaction throughput

What transaction throughput can the SPS sustain under increasing input load?

Q3 Deduplication efficiency

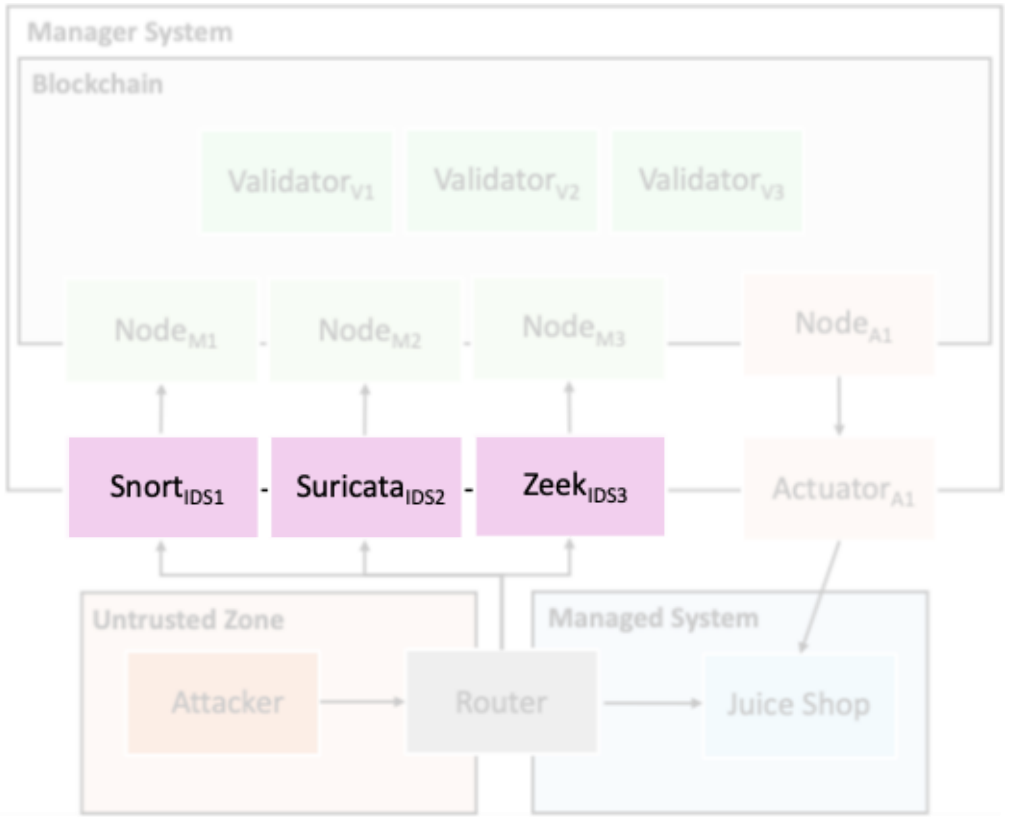
How does the deduplication mechanism reduce on-chain transaction load as the volume of a specific attack increases?

Experimental Topology



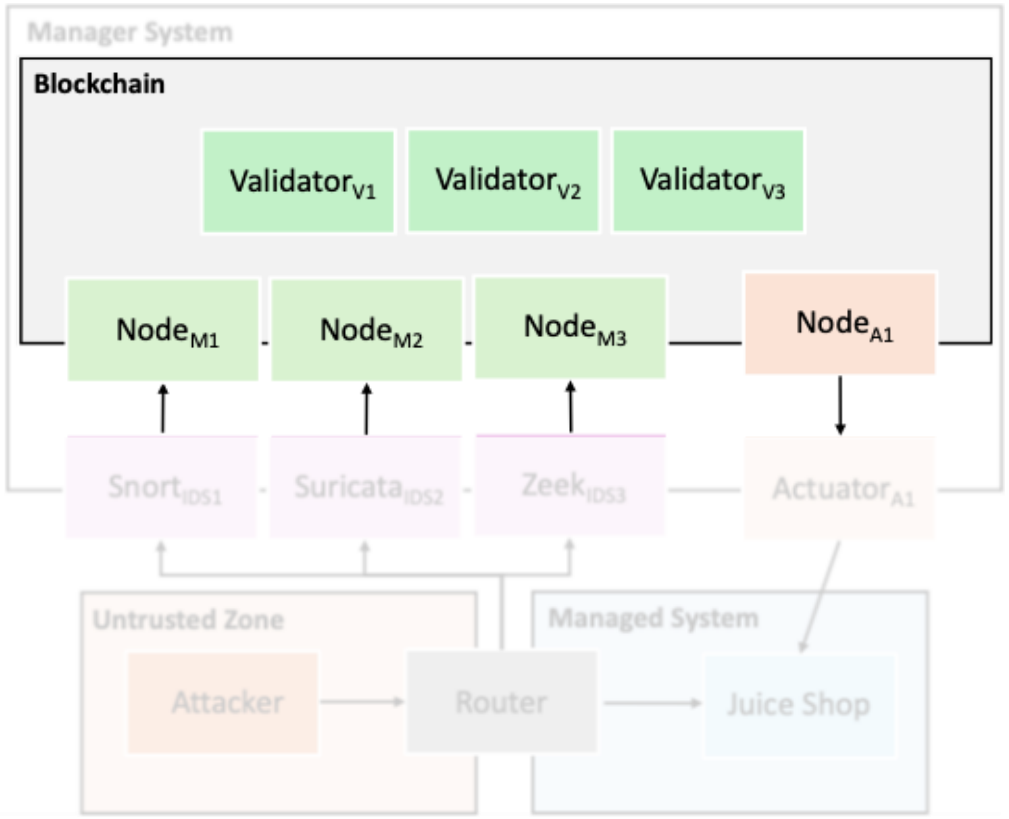
- **Target:** OWASP Juice Shop

Experimental Topology



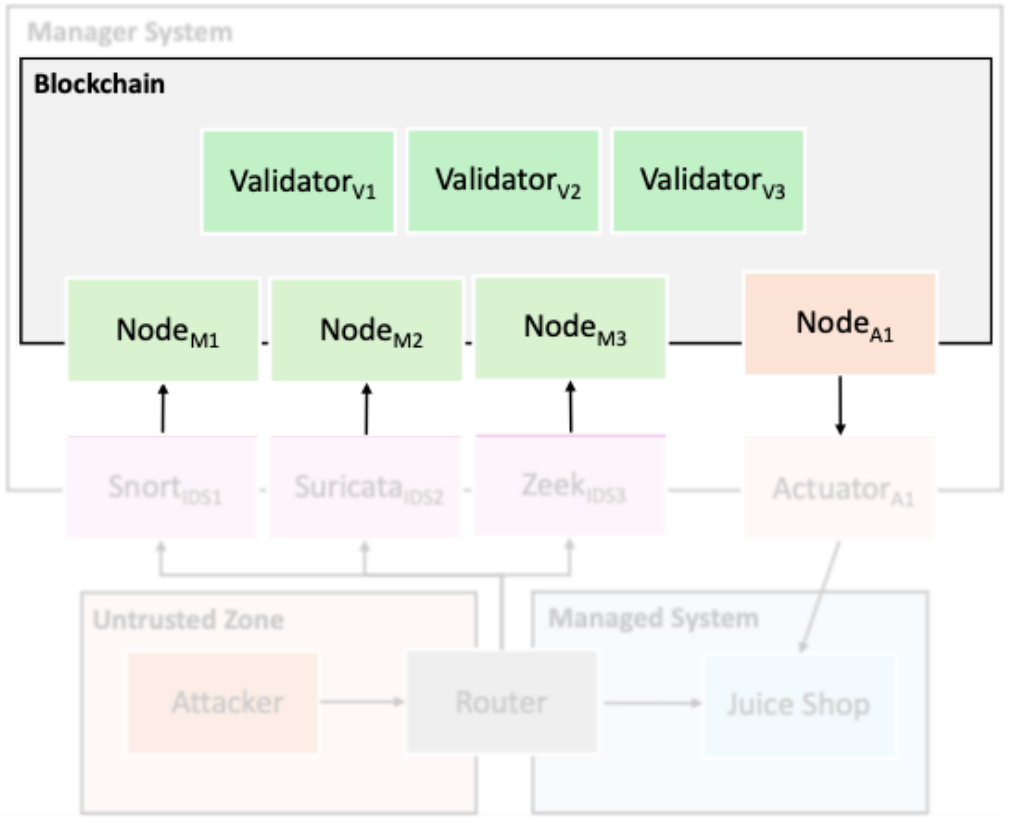
- **Target:** OWASP Juice Shop
- **3 heterogeneous IDSs:**
  - Snort
  - Suricata
  - Zeek

Experimental Topology



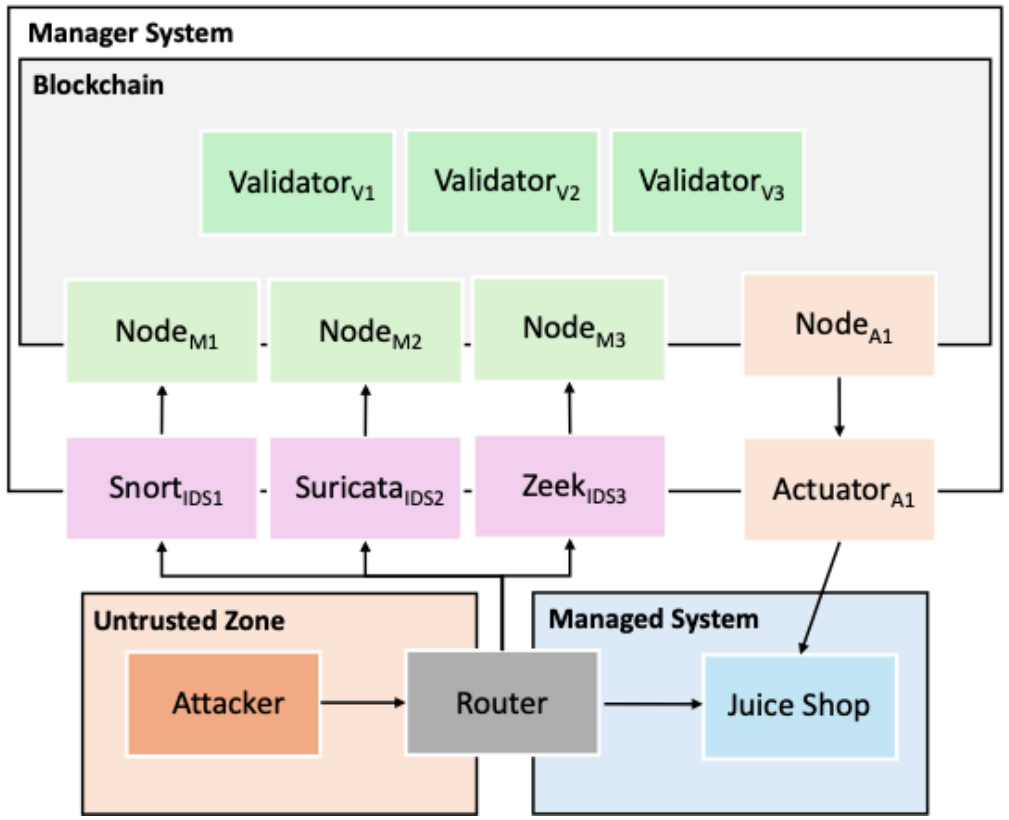
- **Target:** OWASP Juice Shop
- **3 heterogeneous IDSs:**
  - Snort
  - Suricata
  - Zeek
- **7 blockchain nodes:**
  - 3 validators
  - 3 nodes
  - 1 actuator

Experimental Topology



- **Target:** OWASP Juice Shop
- **3 heterogeneous IDSs:**
  - Snort
  - Suricata
  - Zeek
- **7 blockchain nodes:**
  - 3 validators
  - 3 nodes
  - 1 actuator
- **Deduplication Mechanism**
  Same attack -> 1 transaction

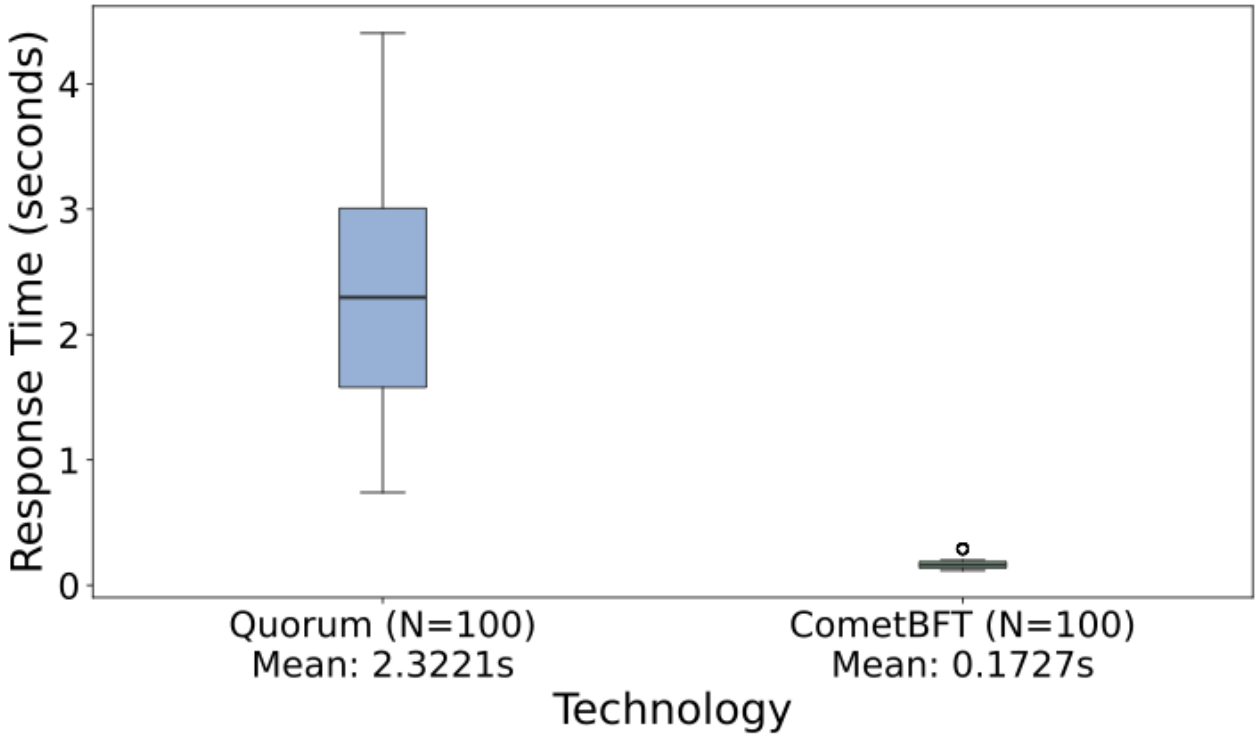
Experimental Topology



How do we do this?

Q1: End-to-end latency under low traffic?

Answer. *CometBFT responds ≈13× faster;*
0.17 s vs 2.32 s mean with a tighter, more stable spread



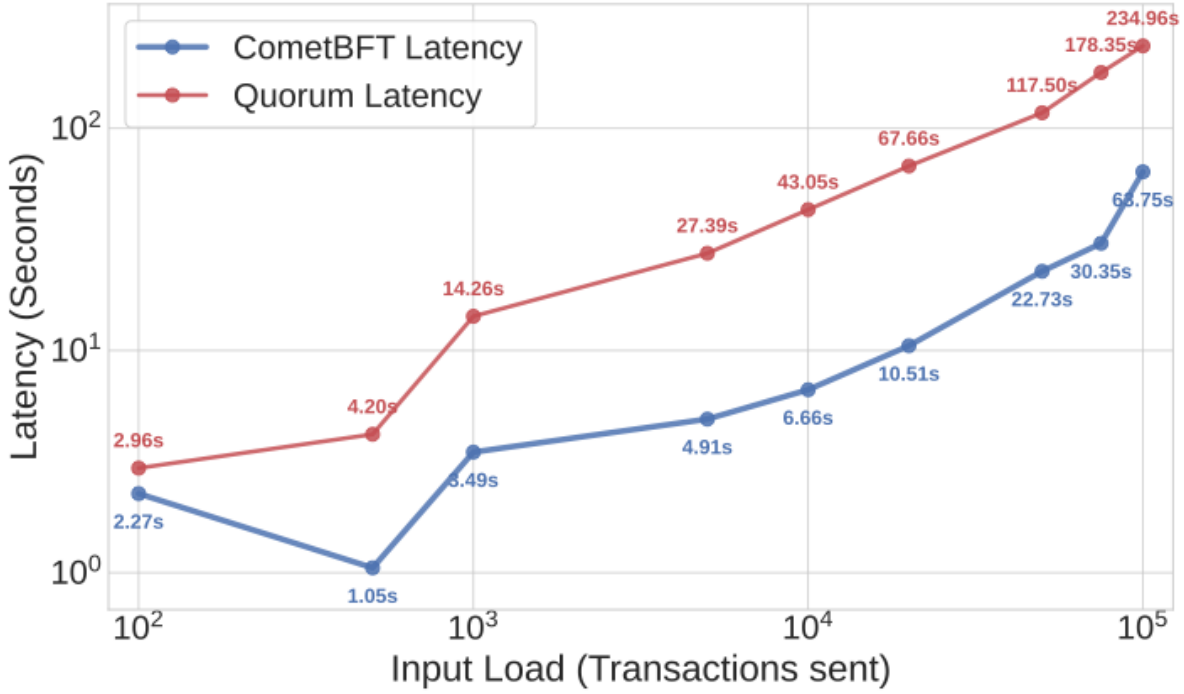
13×

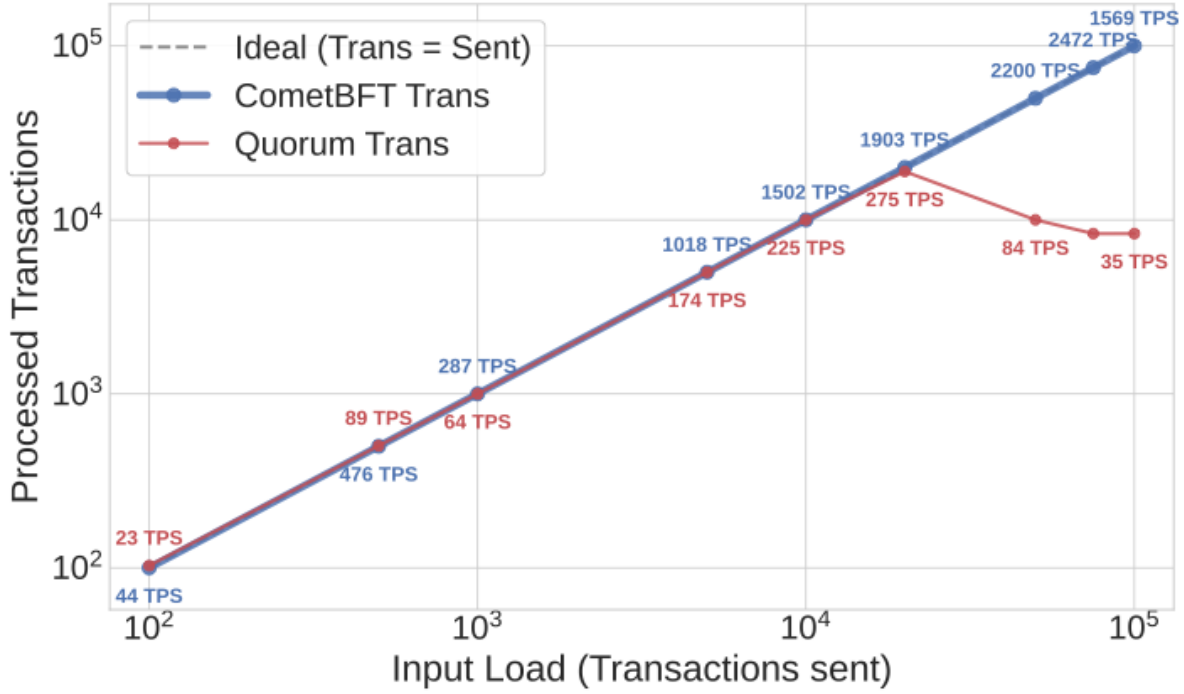
lower mean latency with CometBFT

0.17 s vs 2.32 s

Q2: Throughput under increasing load?

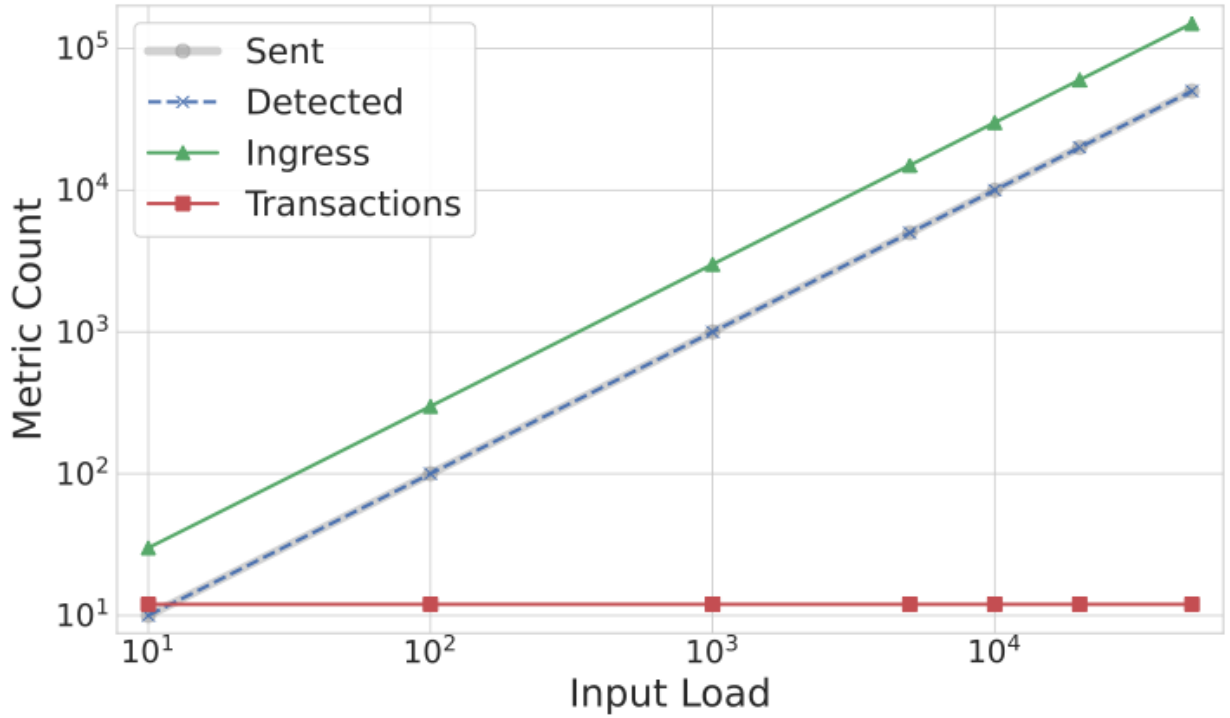
Answer. *CometBFT scales to ≈2.5K TPS with zero loss;*
GoQuorum peaks ≈275 TPS then collapses to ~10% executed.





Does deduplication cut on-chain load?

Answer. *While alerts grow ×10,000, on-chain transactions stay flat*



flat

on-chain tx stays constant
while attacks grow ×10^4

Conclusion

The blockchain backend is a decisive design choice.

- **Requirement-driven, not default**
  SPS needs minimality, determinism and BFT resilience.
- **CometBFT fits better**
  A broader set of requirements satisfied with substantially lower execution overhead.
- **Validated empirically**
  Same SPS, only the ledger swapped: lower latency, higher throughput, no loss.

Conclusion

The blockchain backend is a decisive design choice.

- **Requirement-driven, not default**
  SPS needs minimality, determinism and BFT resilience.
- **CometBFT fits better**
  A broader set of requirements satisfied with substantially lower execution overhead.
- **Validated empirically**
  Same SPS, only the ledger swapped: lower latency, higher throughput, no loss.

FUTURE WORK

Programmable membership & audit

Committee-based validator scaling

Larger attack-and-defense scenarios

8TH DISTRIBUTED LEDGER TECHNOLOGY WORKSHOP

Pula · June 2026

Code HERE!

Which Blockchain Technology Best Supports Self-Protecting Systems?

A comparison between Quorum and CometBFT

S. Albero · V. Tatti · D. Pennino · T. Caiazzi · S. Iannucci · M. Pizzonia

Roma Tre University · University of Tuscia

UNIVERSITÀ DEGLI STUDI DELLA TUSCIA

Roma Tre