Pre Commit Verification for AI Operations

Sofian Mousa · Apodictic Systems · Extracted from 983 Production Businesses (Rasmi)

01 Origin Insight: Authorized Writes Break Ledgers

Across 983 Egyptian businesses using Rasmi to validate 900,000+ statutory invoices under Egypt ETA Resolution 281, our hardest failures were not malicious cyberattacks. Multi-branch retailers connecting AI automation scripts to Odoo v18 and PostgreSQL caused failures using valid credentials: cross-branch discounts, imbalanced account.move postings, and soft-deletes that severed SHA-256 tax receipt chains.

983	14 Blocked	4 Chains	21.4 ms
Rasmi Businesses	Destructive AI Writes	$490/mo Enterprise	6-Subsystem Harness
900,000+ validated docs	12-branch chain (30 days)	Odoo & Postgres guarded	Z3 5.4.1 verified run

02 Why Sandboxes & Prompt Filters Miss the Bug

Container sandboxes restrict OS syscalls; prompt guardrails inspect natural language. Neither proves whether a valid SQL or Odoo mutation preserves accounting invariants. Apodictic inserts a formal verifier directly at the transaction boundary.

Stage 1 · SYM_* Privacy Proxy

Strips IBANs, tax IDs, emails, and secrets locally in RAM (<=1.4ms) before cloud reasoning calls.

Stage 2 · Z3 SMT State Proving

Tests post-write cash floors, double-entry parity, T2/T1 compound VAT, and halala UBL rounding (<2.5ms).

Stage 3 · 2-Phase Reversal & Outbox

Staged Postgres SAVEPOINTs and Odoo account.move.reversal run locally (<38ms); external wires require sign-off.

Stage 4 · Privacy-Preserving Distillation

Recurring safe patterns compile into local <2ms Python AST rules via federated invariants with zero raw PII retention.

03 Production Evidence & 30 Day Intercept Breakdown

On our highest-volume paying deployment (a 12-branch retail and pharmacy group processing ~1,400 governed ledger writes per week at $490/month), Apodictic intercepted 14 consequential AI-proposed mutations over 30 days:

- 3 Cross-Branch Pricing Errors: Agents attempted store-wide 22% promotional overrides without branch scoping or CFO approval.
- 7 Imbalanced Journal Entries: Proposed Odoo account.move drafts failed Debit == Credit parity or applied flat VAT over compound T2/T1 tax.
- 4 Hash-Chain Soft-Deletes: Automated cleanup scripts attempted direct SQL unlinks that would have broken sequential ETA UUID receipt links.

04 Privacy Preserving Telemetry Without Data Exposure

Regulated finance teams forbid training shared models on raw invoices. Apodictic separates data custody from structural learning: (1) sensitive literals remain masked behind tenant-local SYM_* vaults, (2) structural accounting rules compile locally into deterministic Python ASTs, and (3) only anonymized invariant templates improve cross-deployment coverage.

External Research Baseline Cited: Kim et al., Google Research & MIT (arXiv:2512.08296) on multi-agent error amplification; Veracode GenAI Security Report (2026).