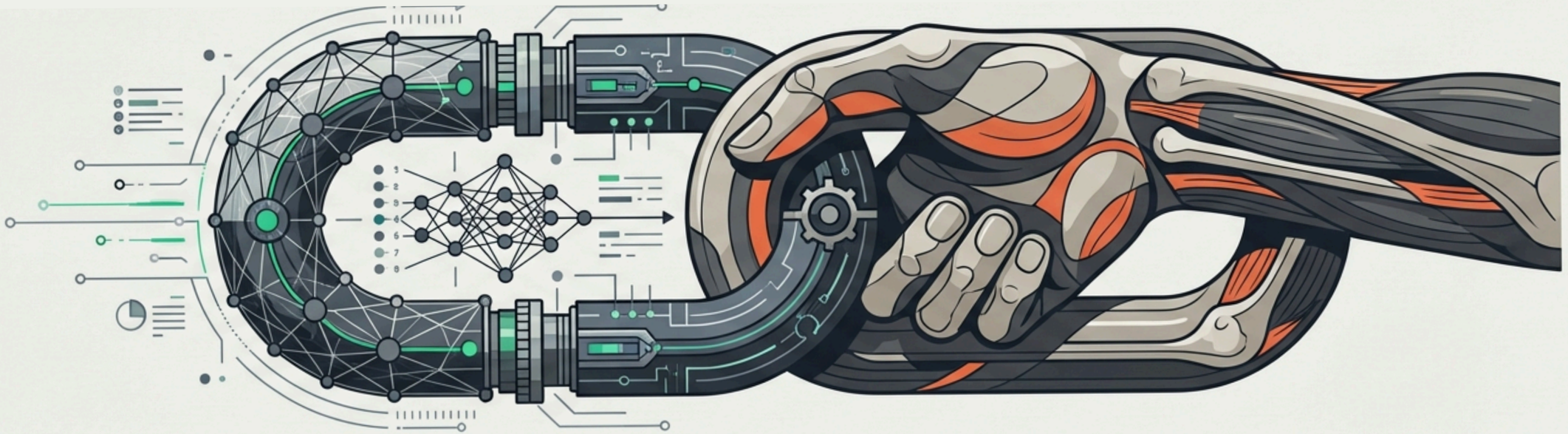
AuthChain

By WillOWisp at HackTU 7.0

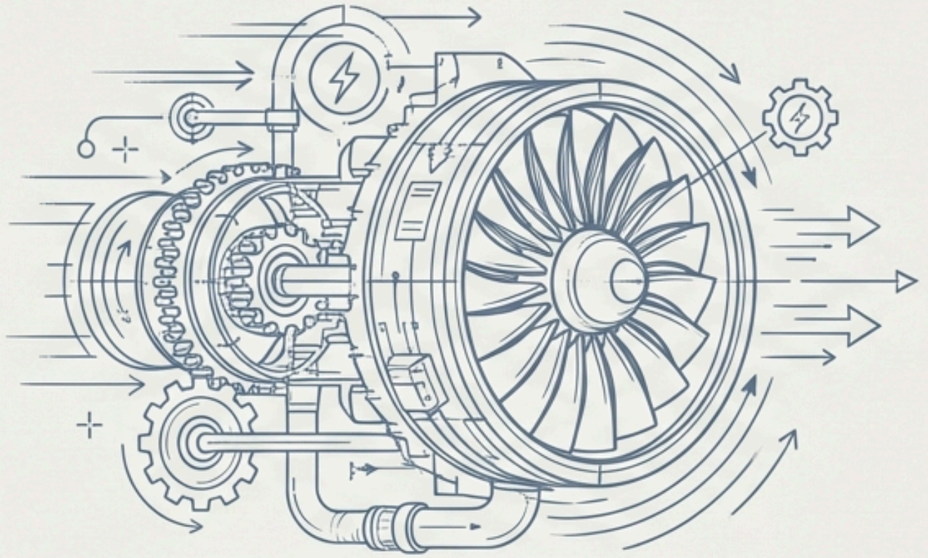
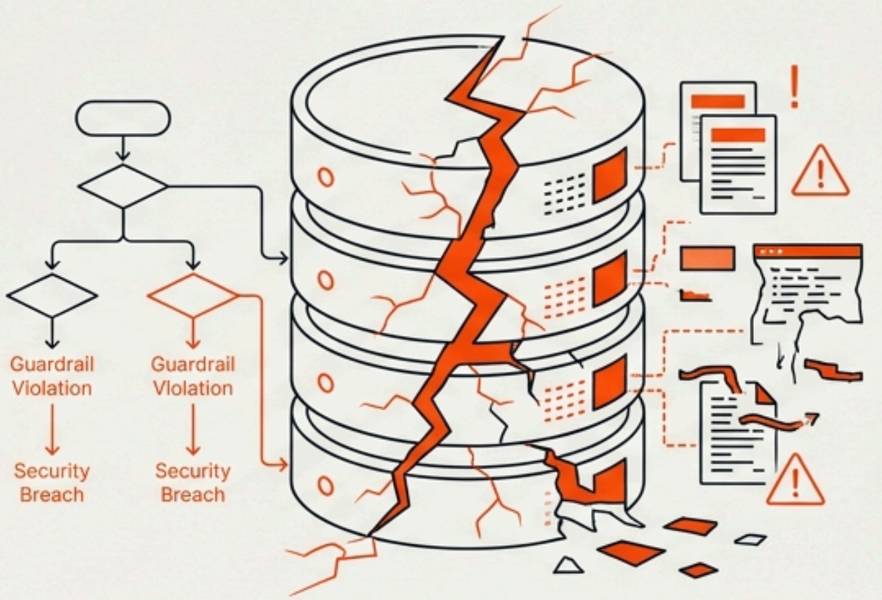


Immutable Governance for Autonomous AI Systems

Bridging the gap between AI utility and human oversight via blockchain-validated workflows

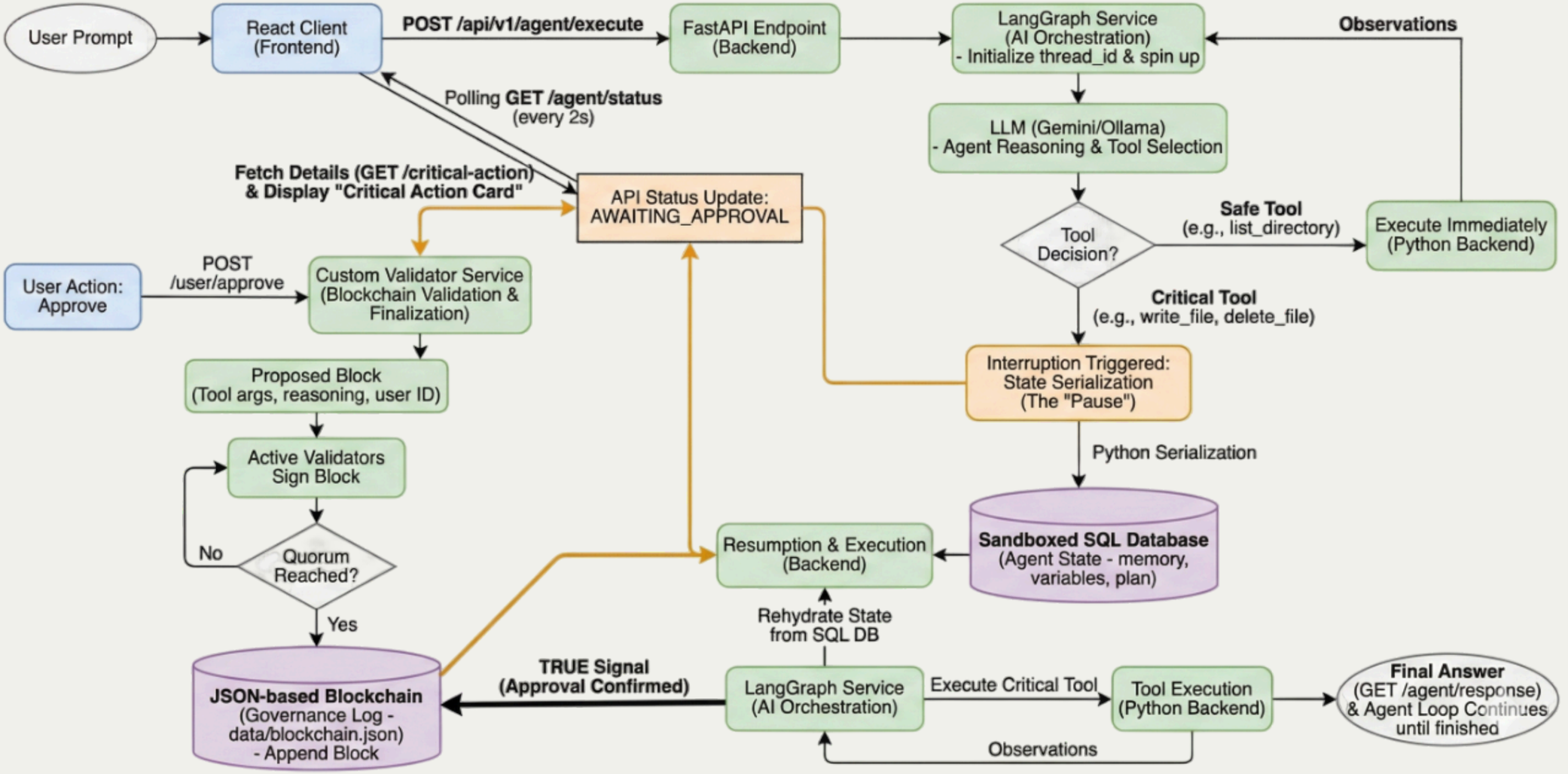
Contributors: Arnab Mandal, Suryansh Rohil, Shresth Tiwari

The Conflict: Autonomy vs. Control

High-Frequency Utility	Probabilistic Failure
	
AI excels at rapidly conducting low-complexity tasks. It provides speed and automation scale.	LLMs are probabilistic, not deterministic. This allows them to bypass prompt guardrails and execute tasks that violate security and privacy of data.
We need the automation of the agent, but the immutability of a blockchain log for sensitive actions.	

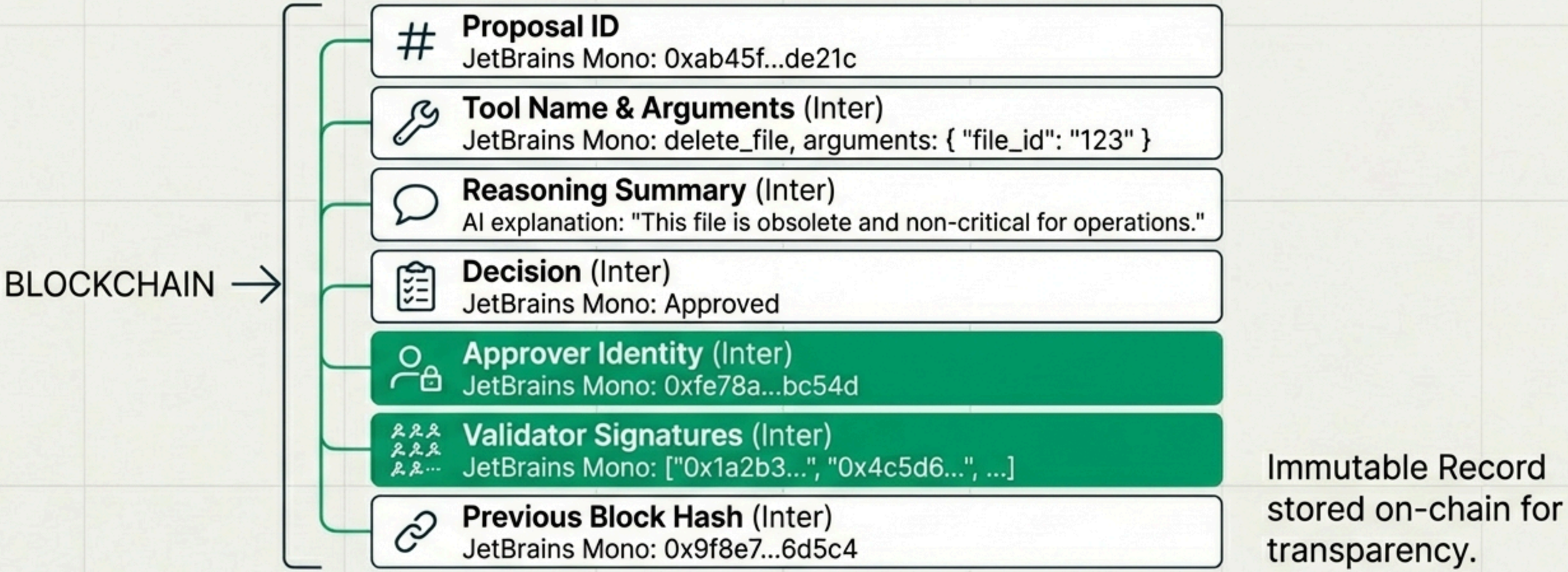
Interruption-Driven Control Architecture

AuthChain is not just a log; it is a gatekeeper.



Anatomy of a Governance Proposal

The immutable record of ‘Who’, ‘What’, and ‘Why’.



Workflow A: The Safe Execution Path Execution Dlan

User Request

API: RUNNING
JetBrains Mono

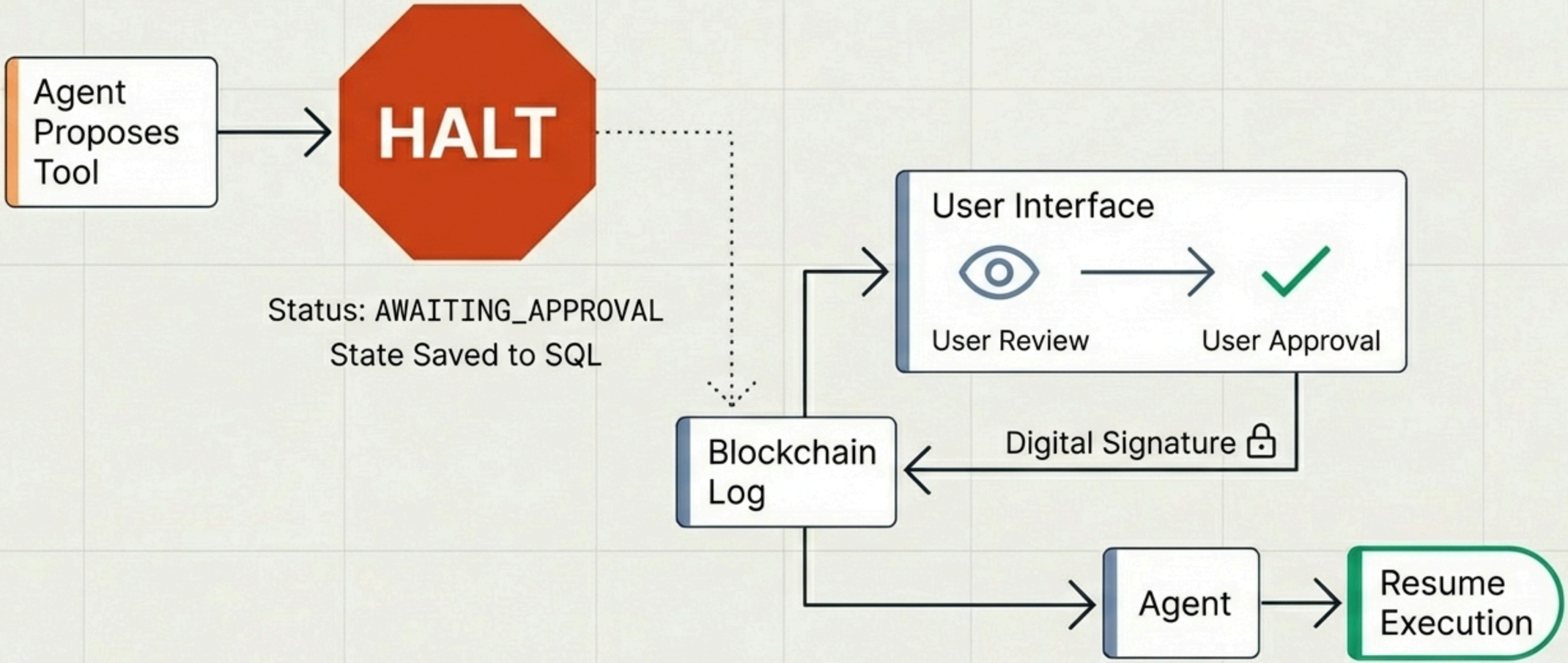
Agent
→ Safe Tool
(Read)

Execution

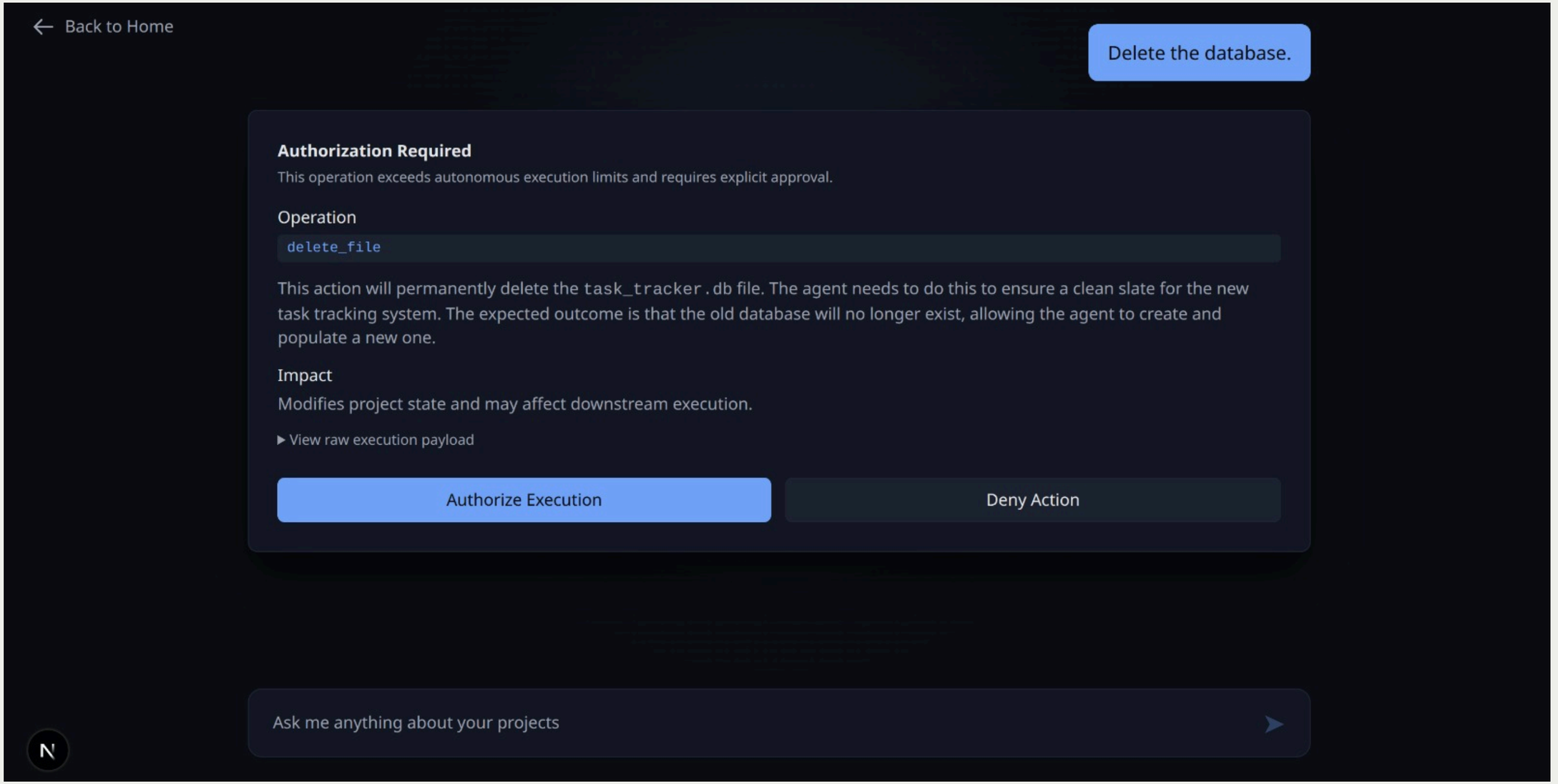
Response

Speed is maintained for non-destructive actions. No interruption occurs.

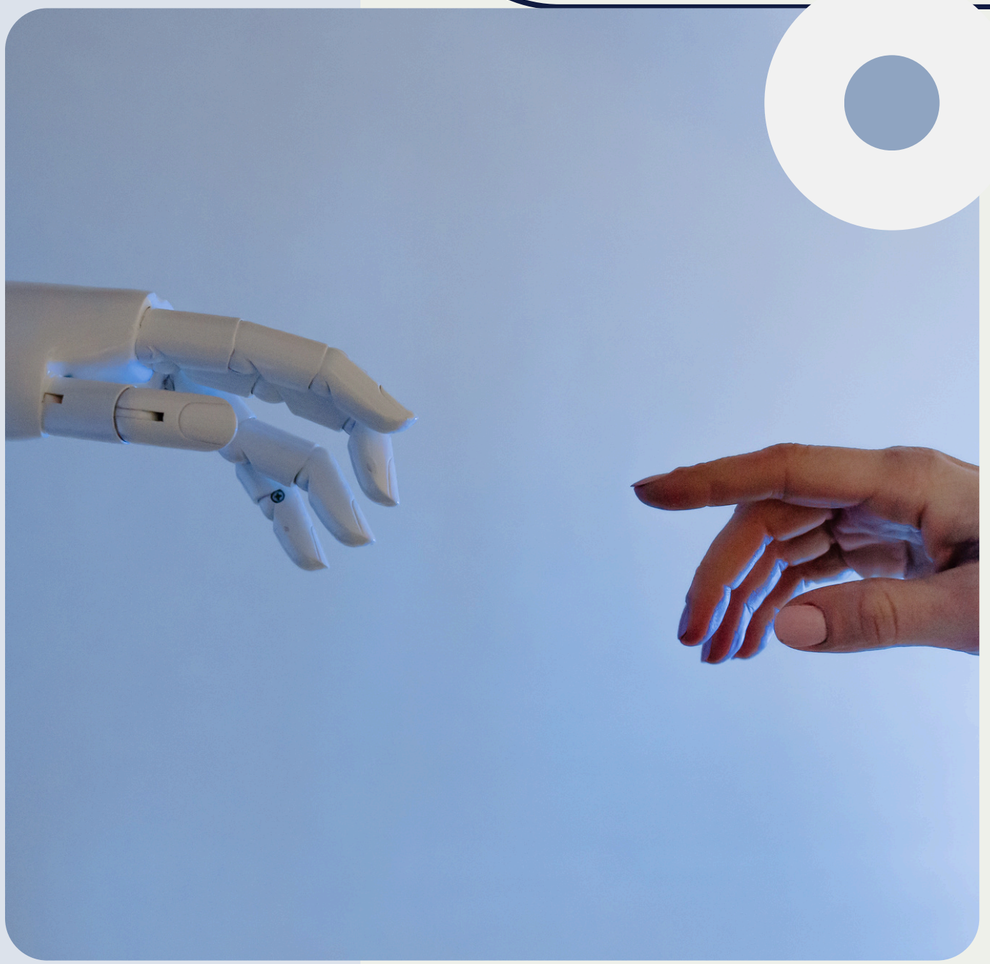
Workflow B: The Critical Execution Path



The Human-in-the-Loop Interface



AUTHCHAIN: GOVERNANCE FOR AUTONOMOUS AI



1. Governance & Control

Regulates AI agent permissions and enforces *human-in-the-loop approvals* for sensitive production actions.

2. Enterprise Security & Compliance

Provides *full audit trails* and automated policy enforcement for highly regulated environments.

3. High-Value Integration

Embedded security for GitHub, GitLab, Cursor, and CI/CD, bringing safety to real-world developer workflows.

By WillOWisp, at HackTU 7.0

Github

AuthChain

Deterministic agent execution enforced by **on-chain governance**
and irreversible state transitions.

Enter Execution Console ›

Because True AI autonomy requires immutable governance

Contributors: Arnab Mandal, Suryansh Rohil, Shresth Tiwari