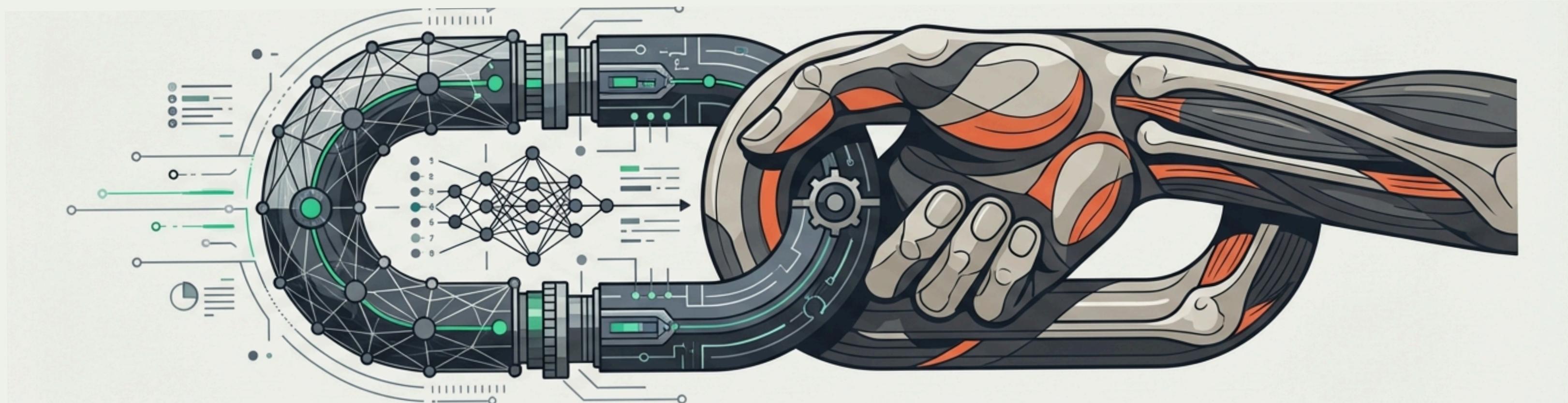


# AuthChain

By Willowisp at HackTU 7.0

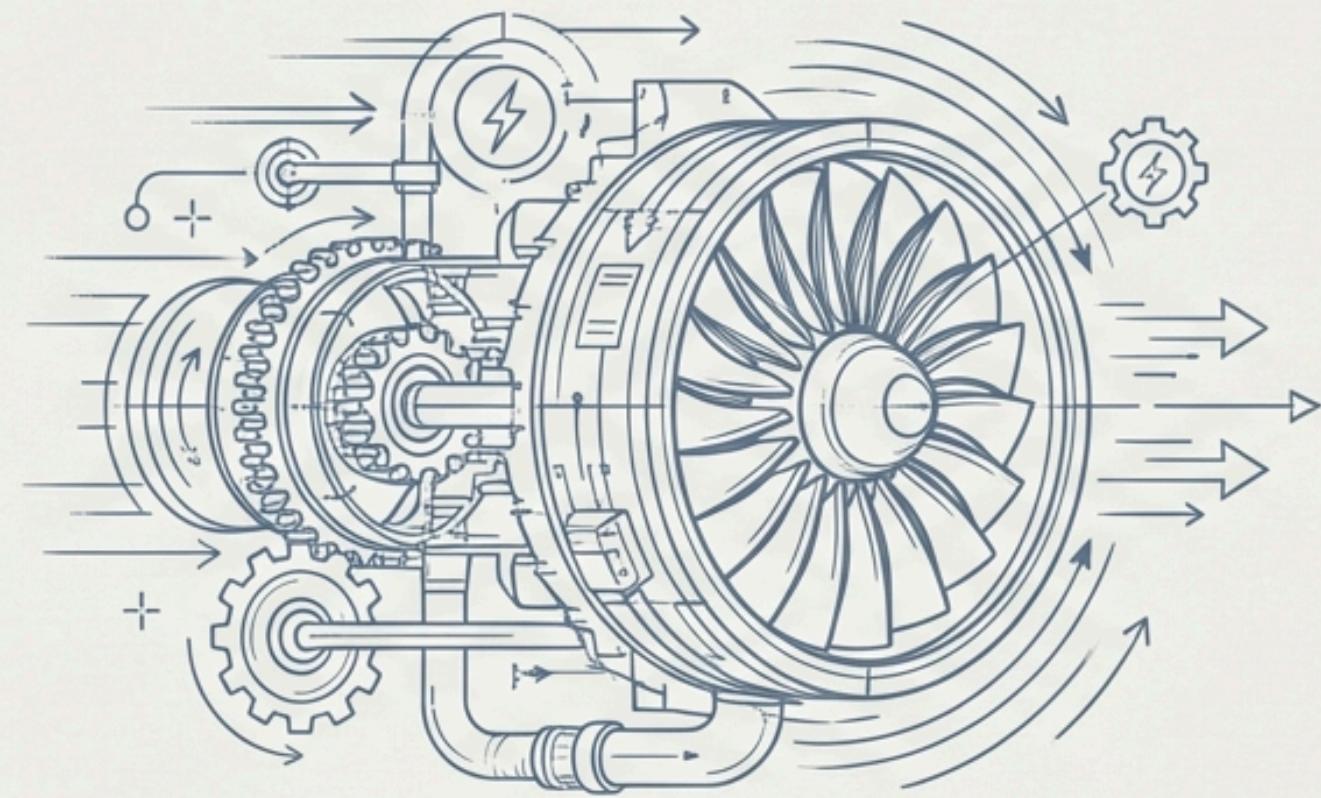


## Immutable Governance for Autonomous AI Systems

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

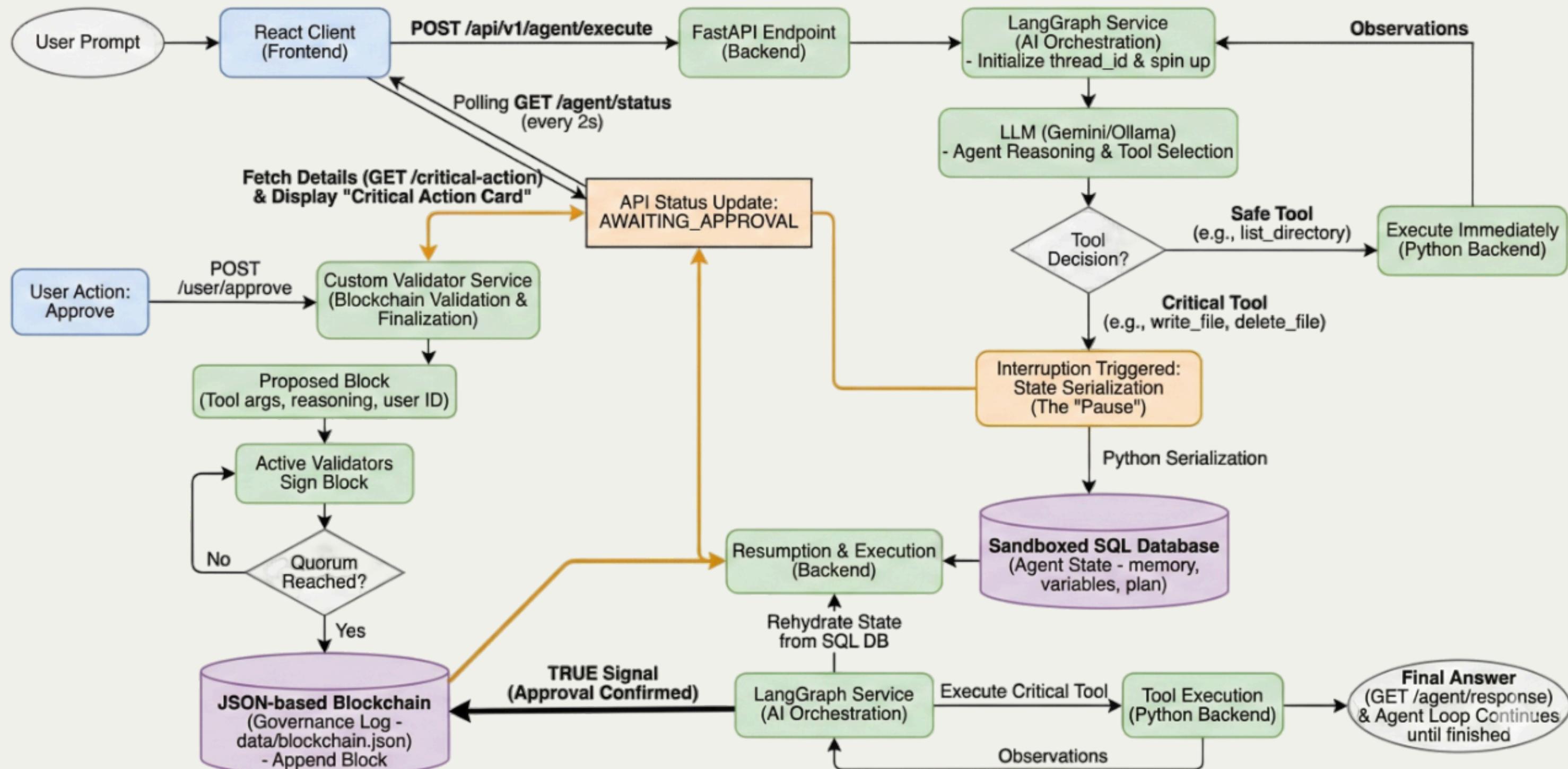
Contributors: Arnab Mandal, Suryansh Rohil, Shresth Tiwari

# The Conflict: Autonomy vs. Control

High-Frequency Utility	Probabilistic Failure
	 Flowchart illustrating the process of probabilistic failure: <pre>graph TD; Start(( )) --&gt; Decision1{ }; Decision1 --&gt; GuardrailViolation1[Guardrail Violation]; GuardrailViolation1 --&gt; SecurityBreach1[Security Breach]; Decision1 --&gt; GuardrailViolation2[Guardrail Violation]; GuardrailViolation2 --&gt; SecurityBreach2[Security Breach];</pre>
<p>AI excels at rapidly conducting low-complexity tasks. It provides speed and automation scale.</p>	<p>LLMs are probabilistic, not deterministic. This allows them to bypass prompt guardrails and execute tasks that violate security and privacy of data.</p>
<p>We need the automation of the agent, but the immutability of a blockchain log for sensitive actions.</p>	

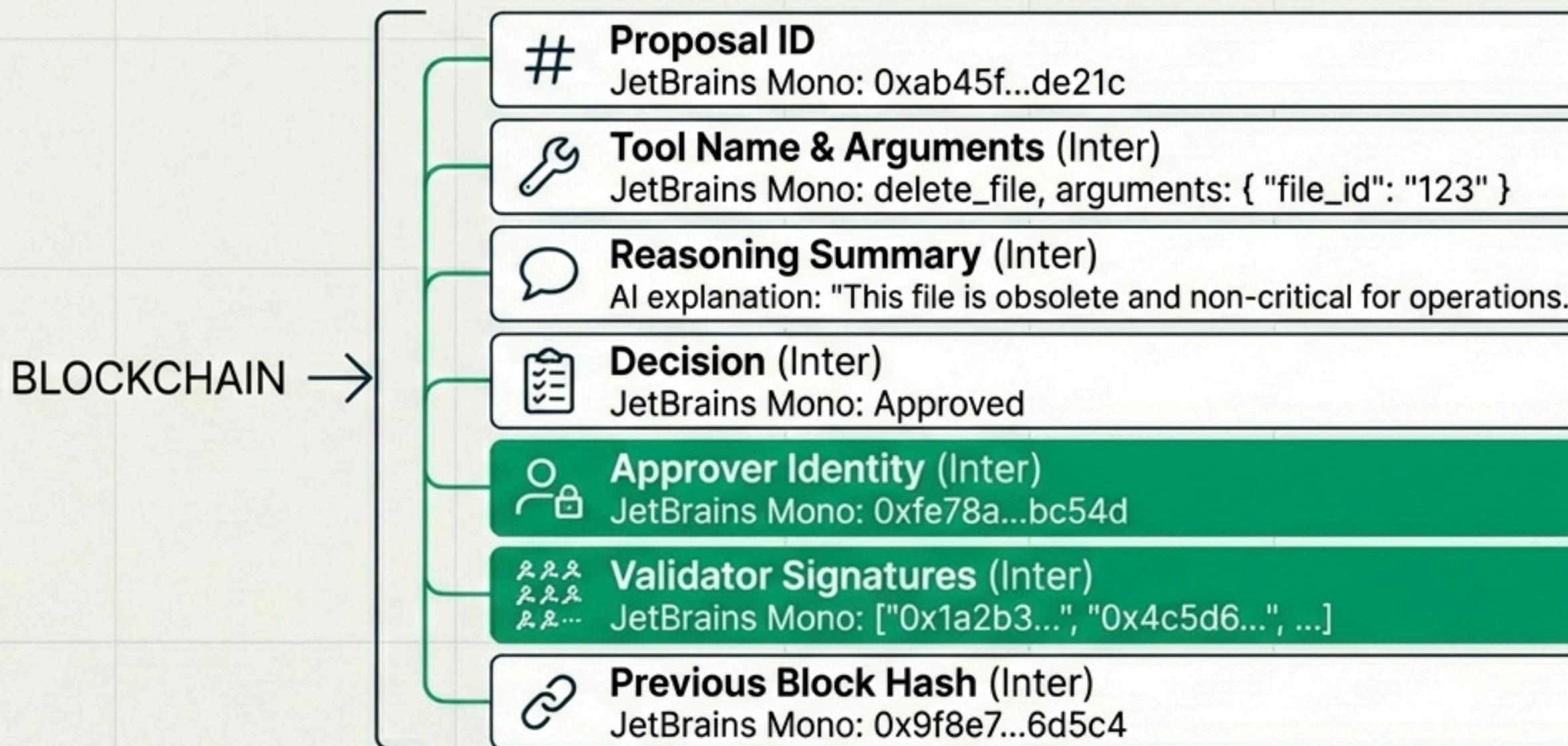
# Interruption-Driven Control Architecture

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



# Anatomy of a Governance Proposal

The immutable record of 'Who', 'What', and 'Why'.



Immutable Record  
stored on-chain for  
transparency.

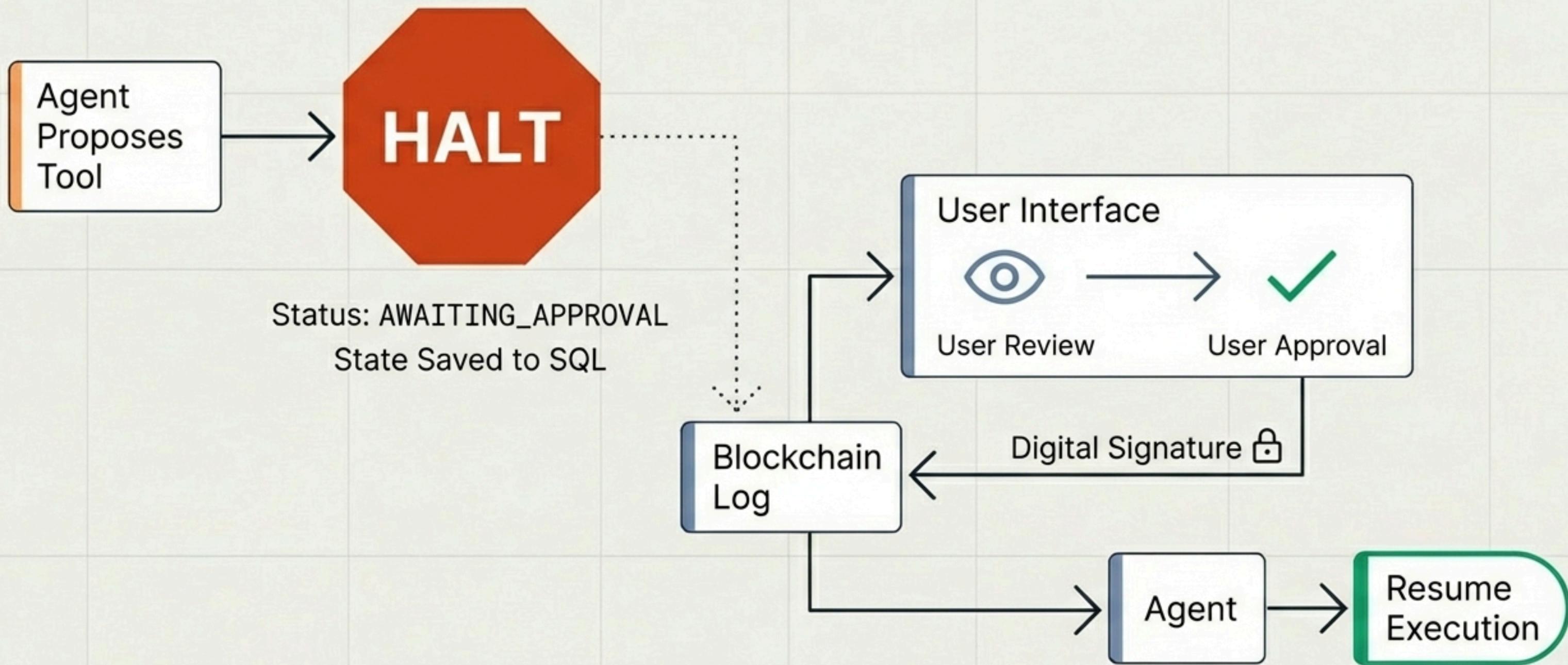
# Workflow A: The Safe Execution Path

## Execution Plan



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

# Workflow B: The Critical Execution Path



# The Human-in-the-Loop Interface

A screenshot of a web-based Human-in-the-Loop interface. At the top left is a 'Back to Home' button with a left arrow icon. At the top right is a blue button labeled 'Delete the database.' Below these, a large central box contains the following information:

**Authorization Required**  
This operation exceeds autonomous execution limits and requires explicit approval.

**Operation**  
`delete_file`

This action will permanently delete the `task_tracker.db` file. The agent needs to do this to ensure a clean slate for the new task tracking system. The expected outcome is that the old database will no longer exist, allowing the agent to create and populate a new one.

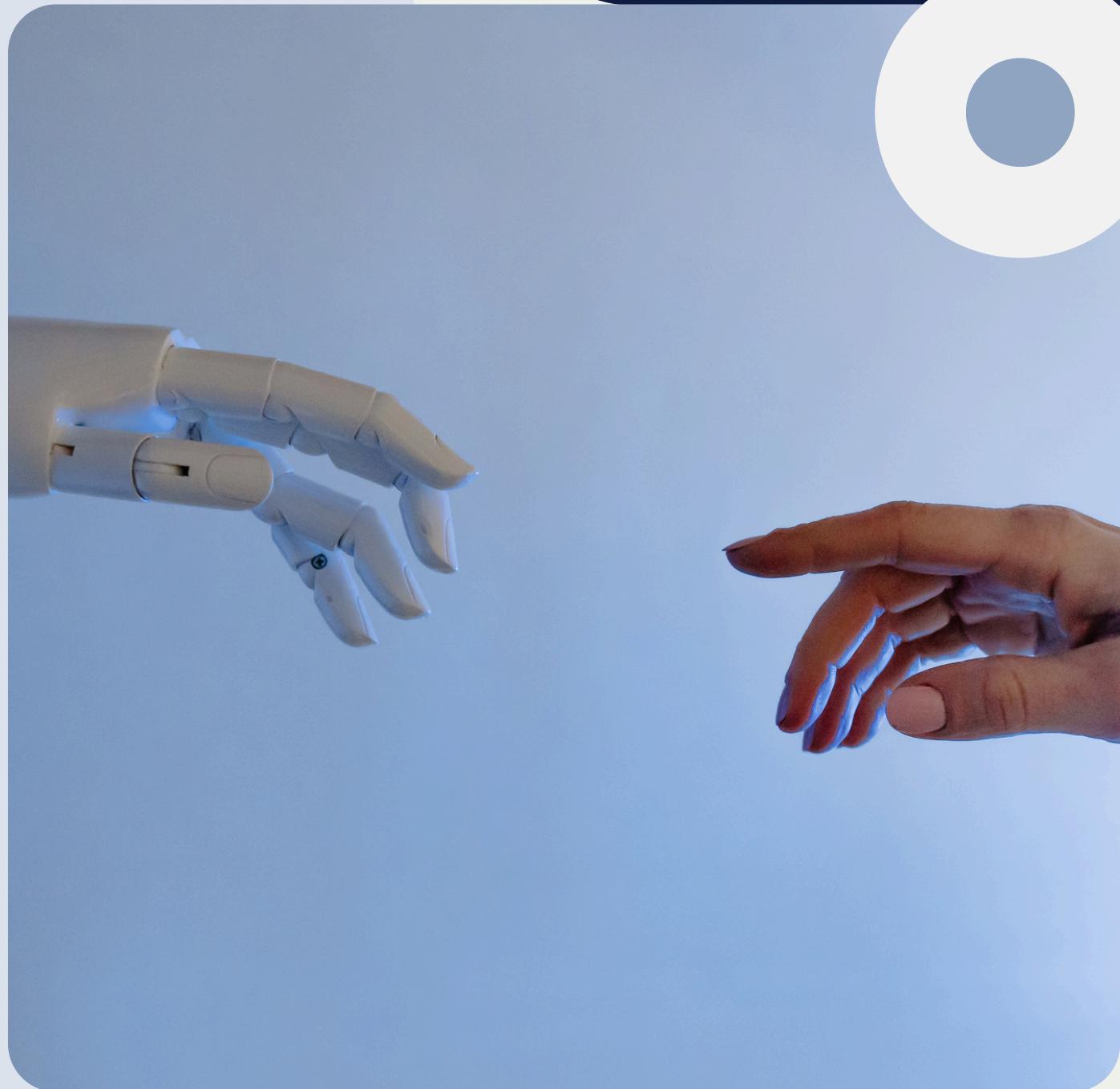
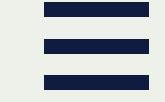
**Impact**  
Modifies project state and may affect downstream execution.

▶ View raw execution payload

At the bottom of the central box are two buttons: a blue 'Authorize Execution' button on the left and a dark green 'Deny Action' button on the right.

At the very bottom of the page is a dark footer bar containing the text 'Ask me anything about your projects' next to a right-pointing arrow, and a small circular icon with a white letter 'N' in the bottom-left corner.

# 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.



[Github](#)

# AuthChain

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

[Enter Execution Console >](#)

Because True AI autonomy requires immutable governance