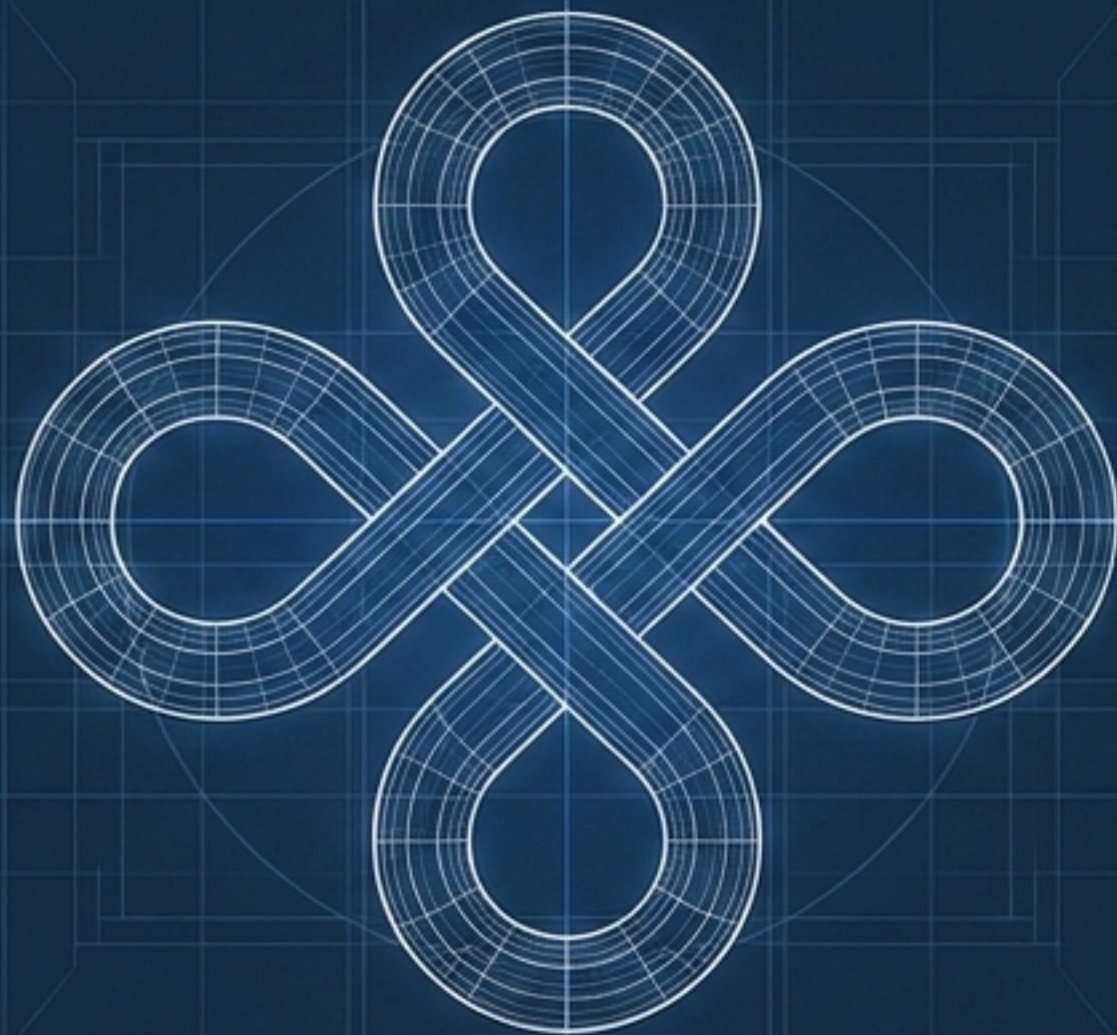


Executable Governance in the AI Era



Operationalizing ISO, NIST, and the EU AI Act as
Interoperable Class Architecture on SagaChain.

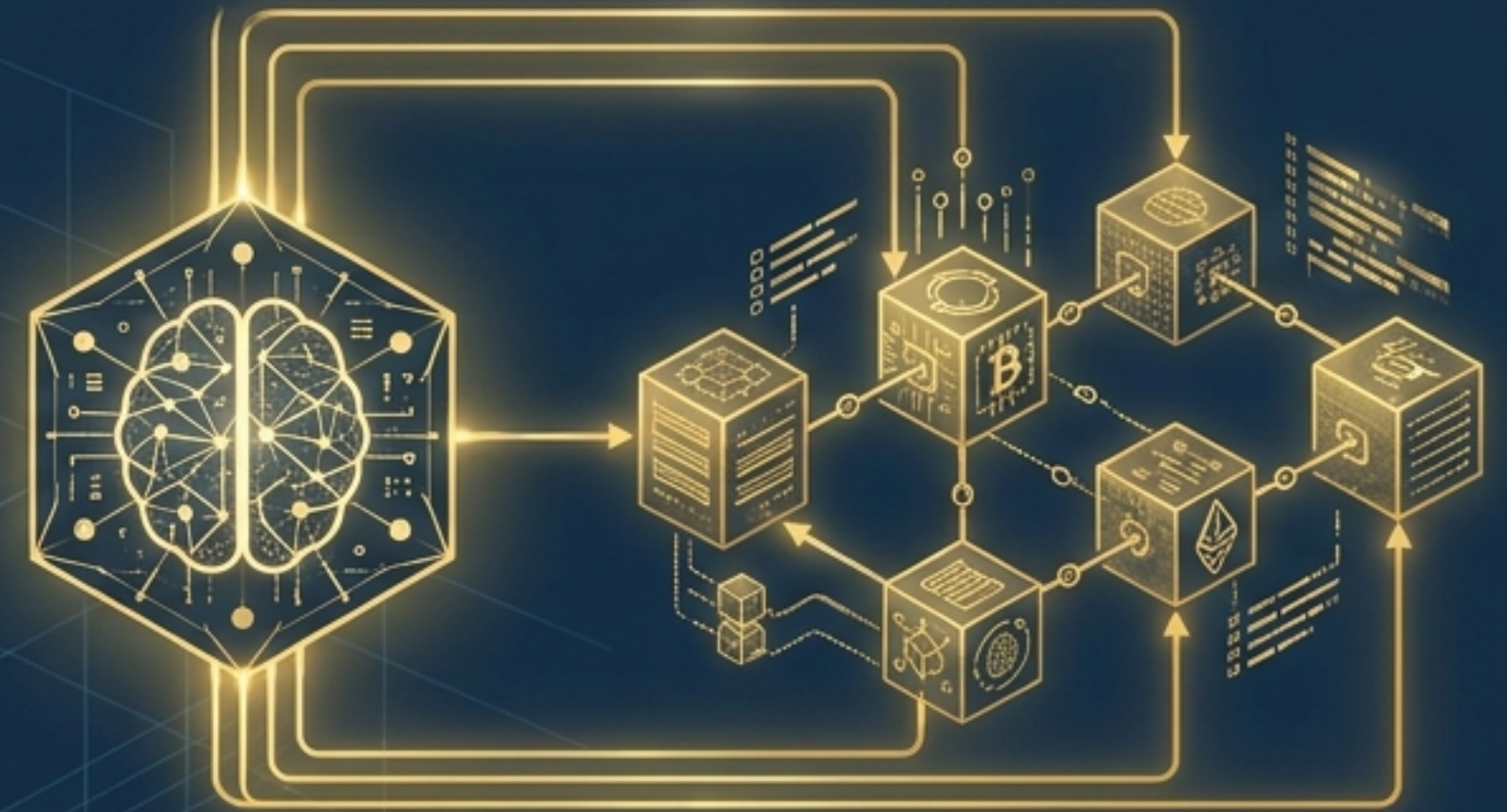
Powered by Persistent State-Augmented Generation (PSAG)

Narrative Governance



Documents, policies, and episodic audits.
Reconstructed, disputable, and structurally
disconnected from system runtime behavior.

Executable Governance



Deterministic, stateful, and non-bypassable.
Governance artifacts persist as runtime-bound
objects anchored to system execution.

Standards define **WHAT** must be governed. The structural gap is **HOW** governance persists as non-disputable state.

DIRECT PROTOCOLS (A2A/MCP)



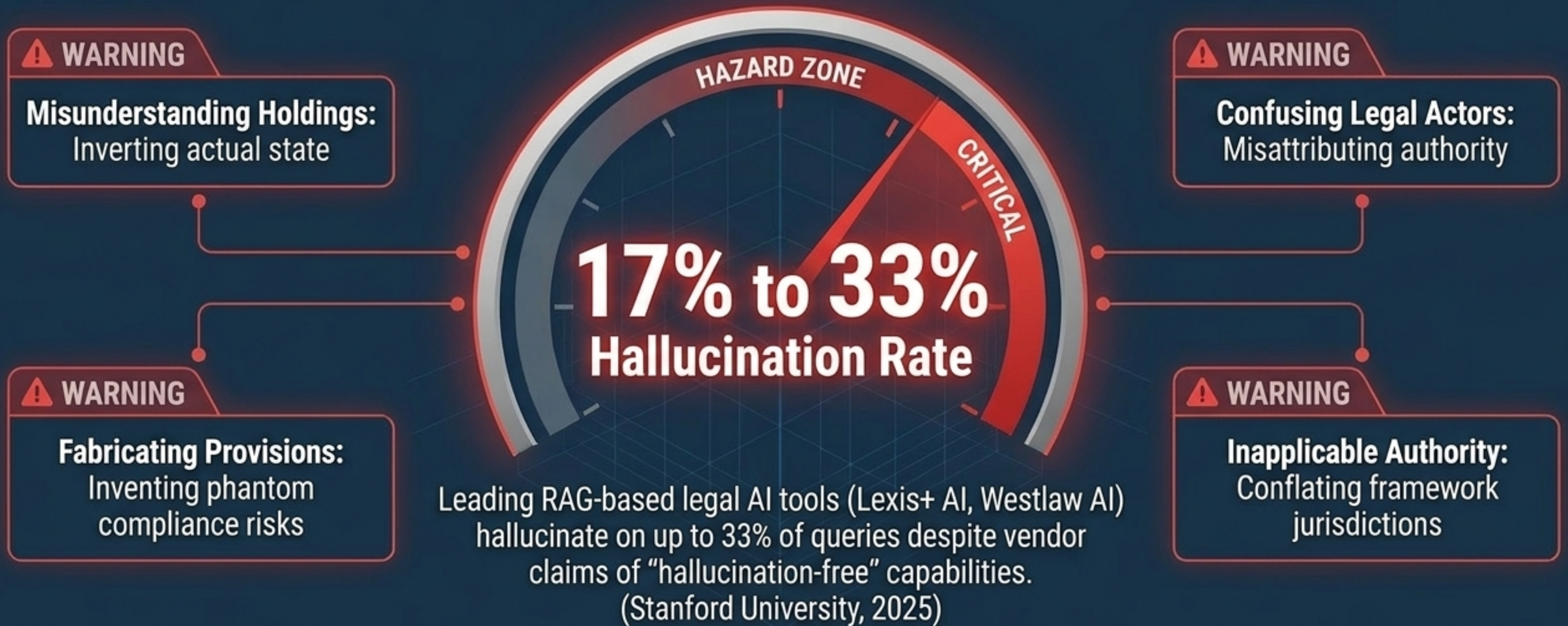
SAGACHAIN (BFT LEDGER)



Requirement	Direct Protocols (A2A/MCP)	SagaChain
Authorization	Satisfied	Satisfied
Authentication	Satisfied	Satisfied
Account Management	✗ Disputable	✓ Non-disputable (LOID-anchored)
Audit Logging	✗ Disputable	✓ Non-disputable (Immutable consensus)
Accountability	✗ Disputable	✓ Non-disputable (Observer notification)

A direct client-server architecture cannot act as its own arbiter. Account Management, Audit Logging, and Accountability remain permanently disputable without a shared, **BFT-mediated consensus record**.

The Hallucination Crisis in AI Governance



RAG is built for probabilistic retrieval of unstructured text. It is architecturally unsuited for deterministic governance state.

The Foundational Premise: Non-Bypassability



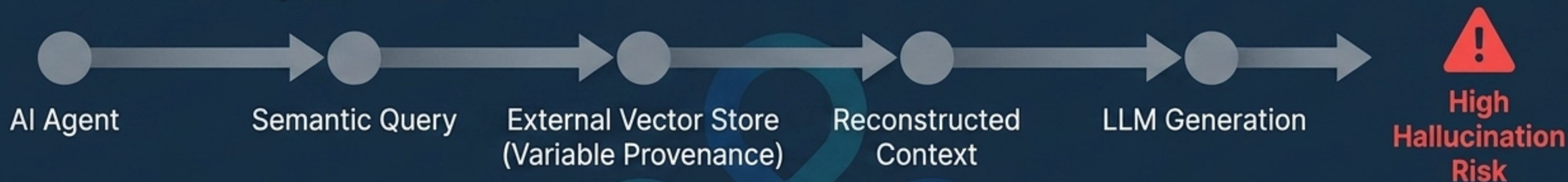
Definition: The architectural property by which no exchange between any two entities can circumvent a shared, independently verifiable record.

Mechanism: Client and server entities never connect directly. Interactions are mediated via SagaChain transactions subject to 4-gate Byzantine Fault Tolerant (BFT) consensus.

Result: The append-only consensus log becomes the single source of truth—mathematically non-disputable.

The Augmentation Paradigm Shift: PSAG

RAG (Retrieval-Augmented Generation)



PSAG (Persistent State-Augmented Generation)



Core Distinction: RAG retrieves unstructured document fragments probabilistically. PSAG executes deterministic reads against a globally consistent, on-chain persistent state (SagaChain LOIDs).

Governance Implication: For state queries ('What is the current risk classification?'), PSAG eliminates hallucination entirely. The answer is the cryptographically verifiable on-chain state itself.

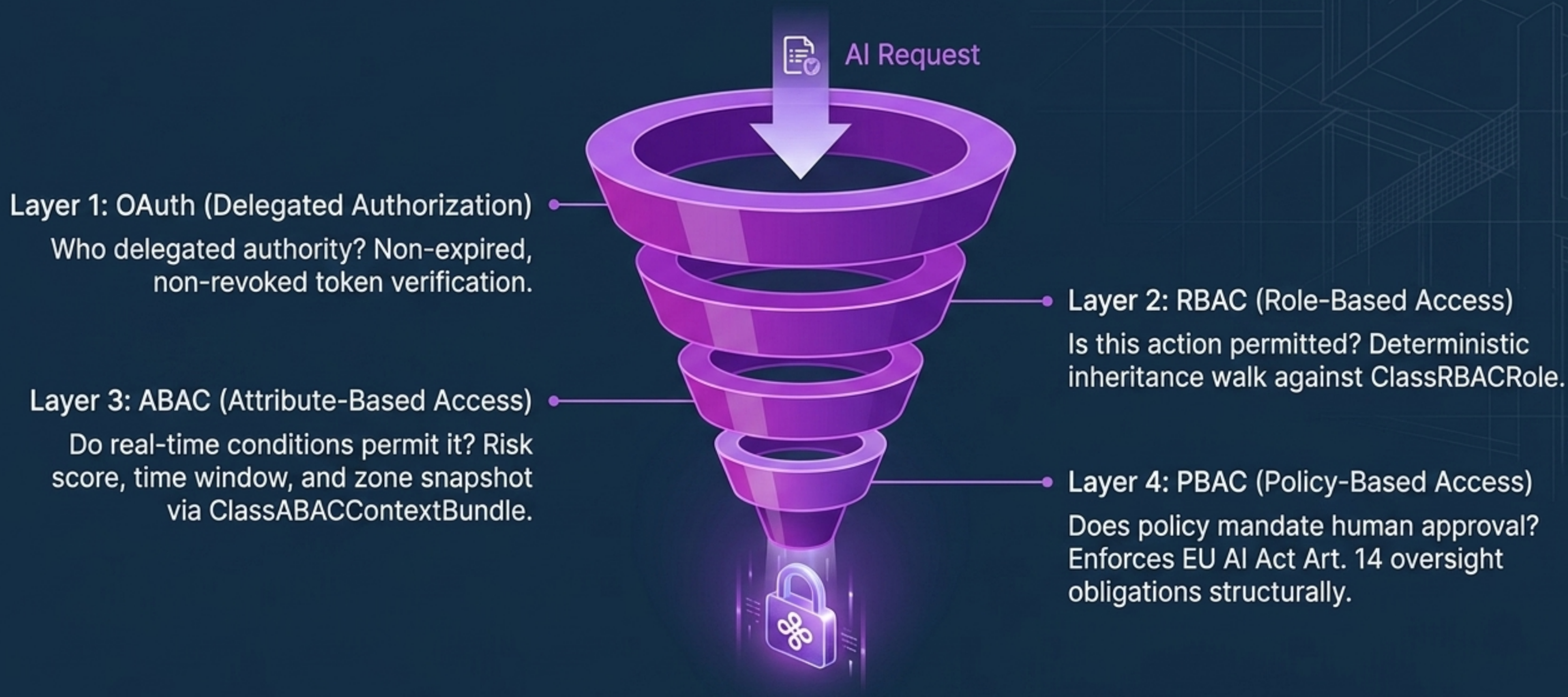
SagaAI: Bounded Runtime Guard Architecture

Evaluating function calls against structured governance objects prior to state mutation.



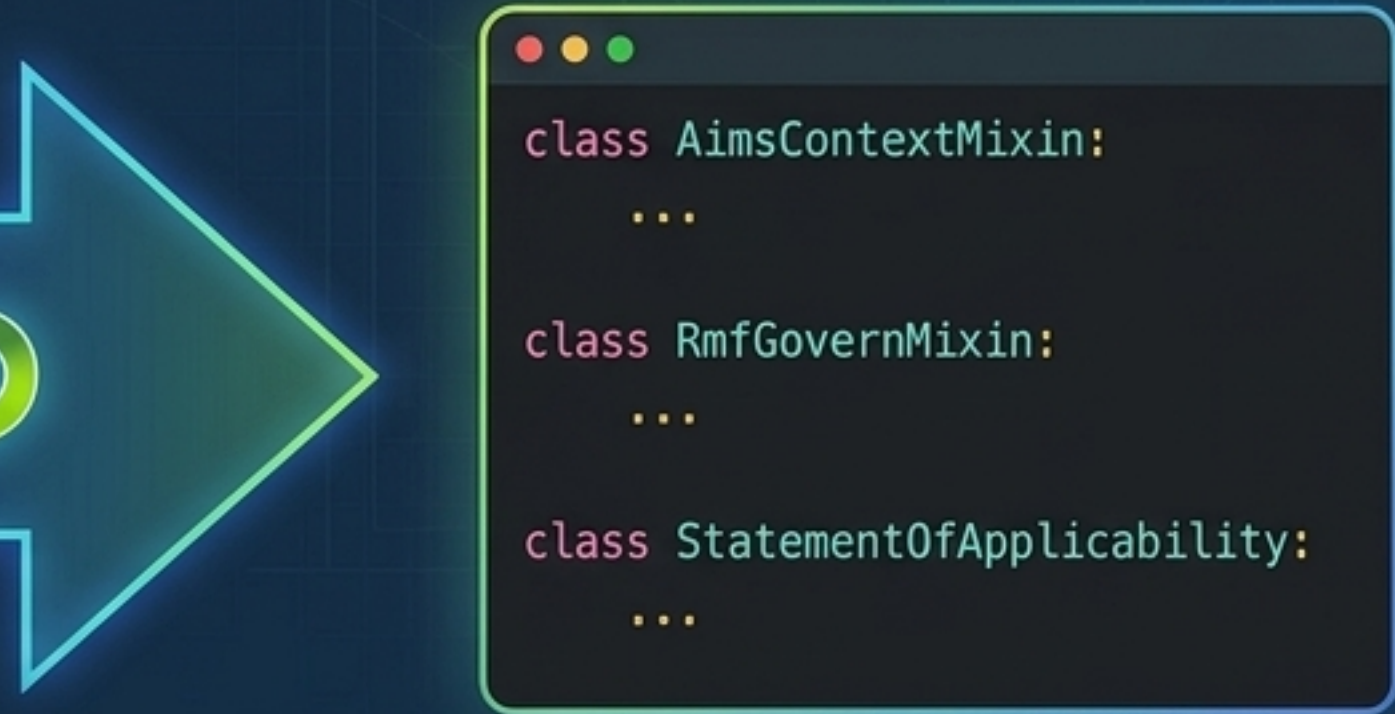
Every guard evaluation is recorded as a SagaChain transaction.
Self-evidencing compliance that cannot be bypassed.

The 4-Layer Access-Control Stack



Takeaway: No AI acts without delegated authority. Evaluation failure at any layer deterministically terminates the pipeline.

Mapping Global Standards to Executable Code



ISO 42001 Mapping: Clauses 4-10 operationalized as composable mixins (e.g., AimsContextMixin, AimsOperationMixin). Annex A controls become structurally linked ClassStatementOfApplicability objects.

NIST AI RMF 1.0 Mapping: Govern, Map, Measure, and Manage encoded via examples.saga_ai.nist_rmf.

The Concept: Semantic governance (SagaStandards) controls class architecture; persistent state (SagaChain) records the objects. Standards are no longer static policies—they are multi-inheritable **Programmable Smart Assets** (SagaPSAs).

EU AI Act Parity Modeling

EU AI Act Statutory Obligation	SagaChain Executable Mechanism
Art. 9 (Risk Management)	ClassAIIA + RmfMapMixin (Lifecycle risk objects on chain)
Art. 10 (Data Governance)	ISO Annex A.6 Mixins (Control declarations recorded immutably)
Art. 12 (Logging)	SagaChain Consensus Record (Direct, architectural satisfaction via append-only ledger)
Art. 13 (Transparency)	ClassEUAIActInstructions (Structured, linked governance artifacts)
Art. 14 (Human Oversight)	PBAC require_human_approval + Cryptographic Institutional Auth

We encode statutory obligations as structured governance objects, natively satisfying EU requirements without displacing regulatory authority.

The Cybersecurity Overlay: NIST IR 8596

AI requires specific adversarial defenses. The executable architecture implements the NIST Cyber AI Profile as an active, versioned overlay.



High-priority cyber designations trigger enhanced runtime validations. All cybersecurity guard evaluations and anomaly events are non-bypassable and permanently logged on SagaChain.

The Unified Governance Graph

Core Insight: Interoperability without conflation. SagaChain's multi-inheritable object model allows a single AI function to be simultaneously evaluated against financial, legal, regulatory, and operational class hierarchies.



ISO AIMS
Context



NIST Risk
Profile

Conclusion: The governance graph is complete, referentially closed, and entirely auditable.



EU AI Act
Classification

ClassMCPAIFunction

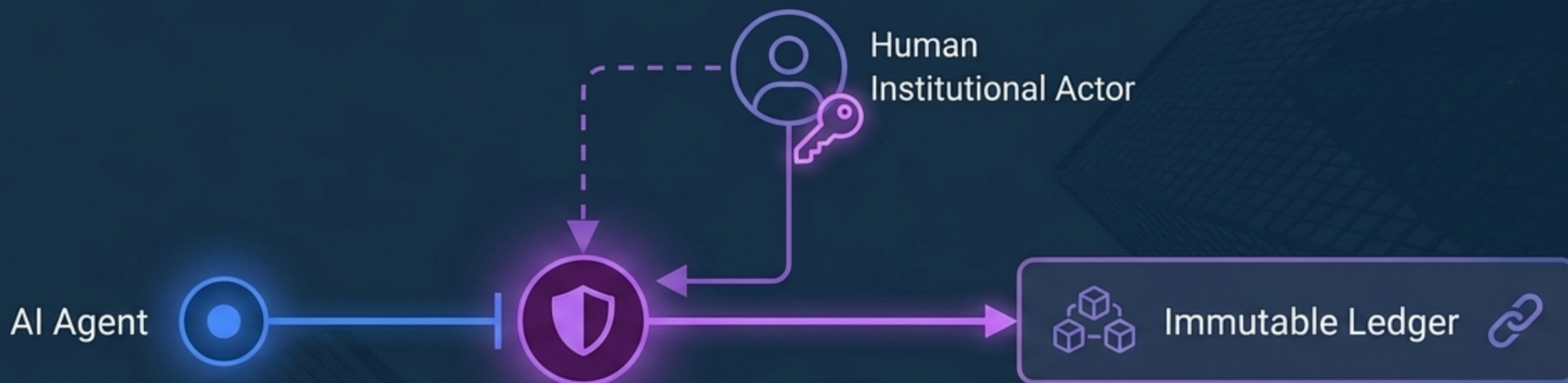
PSAG Integration: PSAG provides AI agents with deterministic traversal of this exact graph, with every data access event recorded on-chain.



Human Oversight
Quorum

Authority Preservation: The Human in the Loop

$\text{Commit}(F) \Rightarrow \text{Authorized}(\text{InstitutionalActor}) \text{ AND } \text{StructurallyValid}(F) \text{ AND } \text{NonBypassable}(F)$



Mechanism: SagaAI enforces structural governance sufficiency; it does not replace human judgment. All state transitions remain subject to explicit cryptographic authorization by designated institutional actors.

The Result: The system records decisions immutably but does not originate authority. Regulators and executives retain full statutory and operational control.

Stakeholder Impact: A Structural Transformation



Enterprise AI Operators

Governance is structurally integrated into operational workflows. No post-hoc document chasing. You cannot dispute what governance state was in effect—and neither can any counterparty.



Regulators & Auditors

Reconstructive, disputable
Reconstructive, disputable
auditing is replaced by
deterministic object lineage
inspection on an immutable
ledger.



AI Platform Hosts

Multi-agent interactions (A2A,
Multi-agent interactions (A2A,
MCP) are fully auditable without
requiring inherent trust between
agents. The shared SagaChain
record supersedes isolated logs.



The Epistemic Shift

We are moving from a documentary paradigm—where truth is reconstructed and debated—to an infrastructural paradigm where governance is continuous, structured, and mathematically non-disputable.

Executable AI governance is no longer theoretical. It is here.