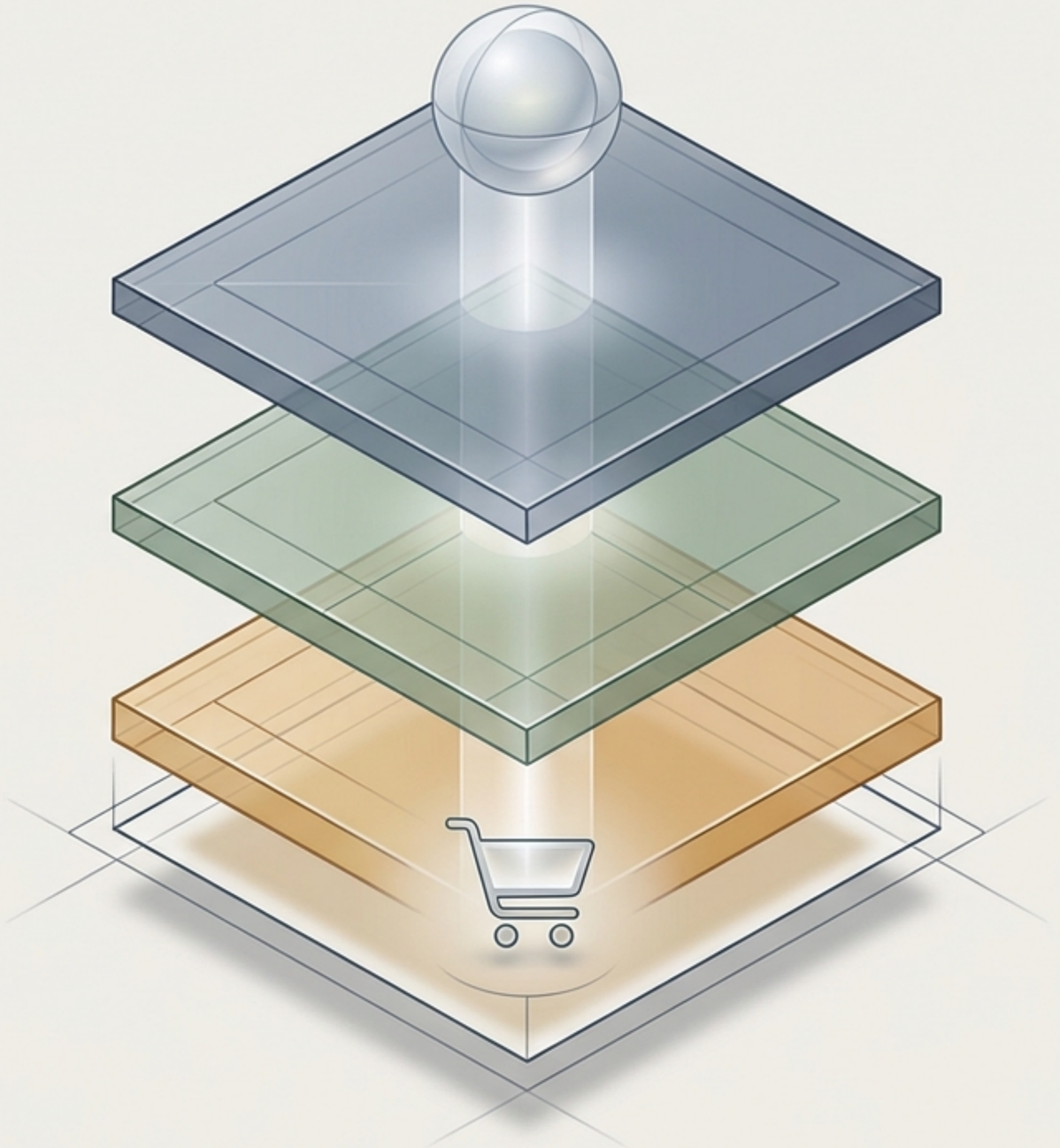
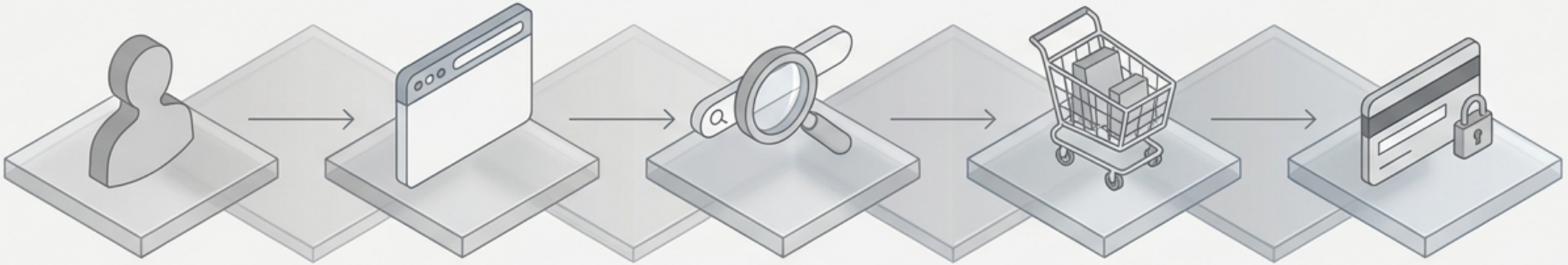
THE ARCHITECTURE OF AGENTIC COMMERCE

Decoding the Universal Commerce Protocol (UCP) and the new semantic substrate.

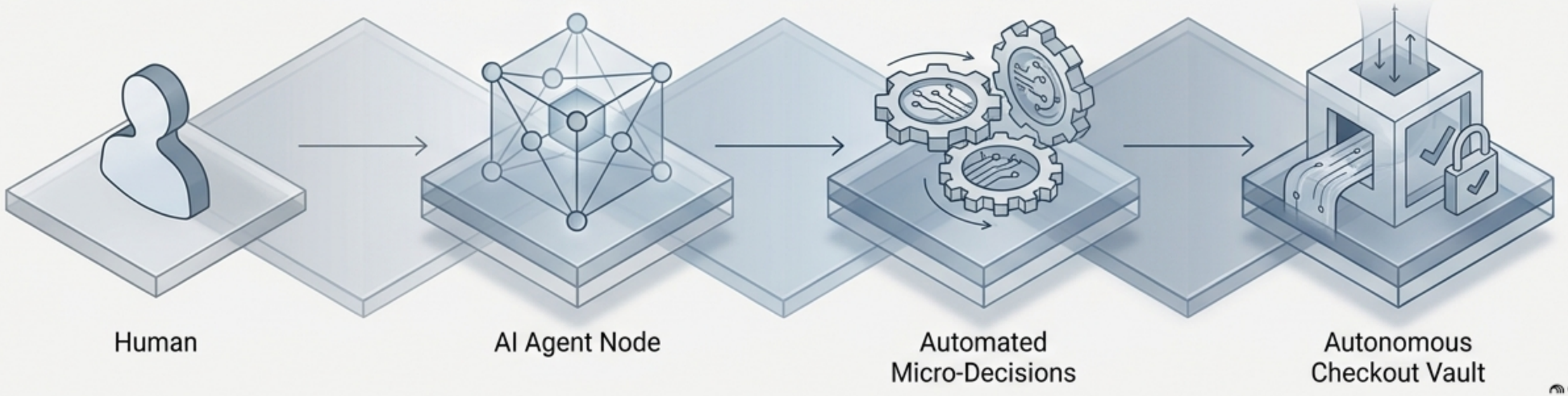


Gemini Notebook

The End of the UI-Mediated Purchase

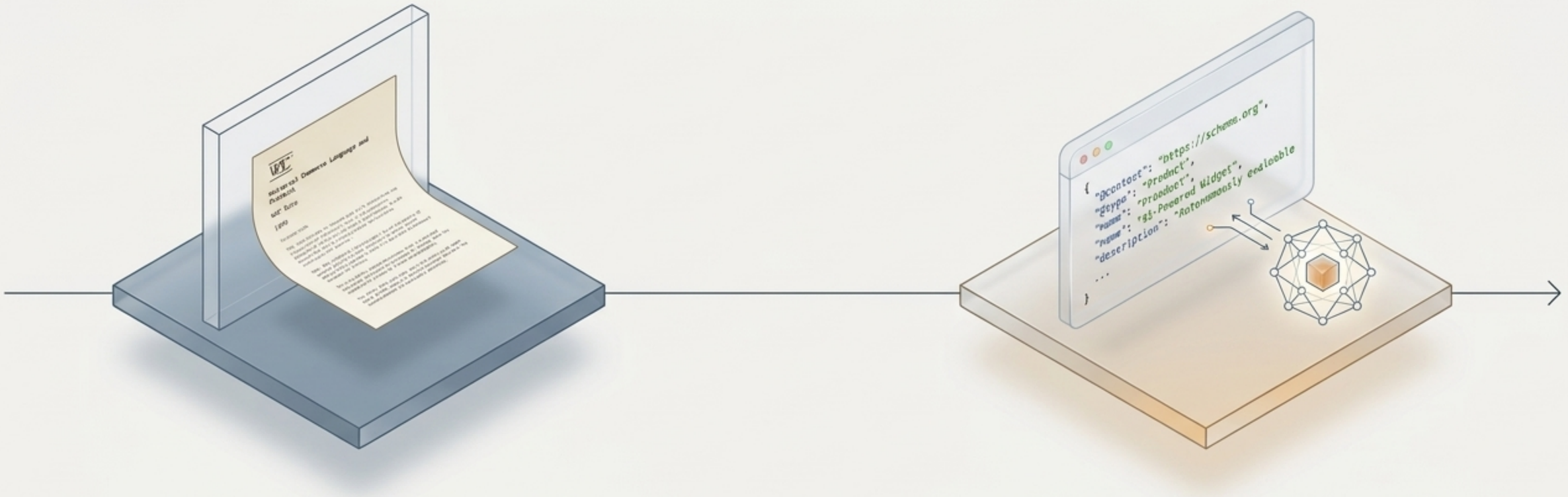


The conventional customer journey—characterized by conscious, manual decision points—is being replaced by continuous, automated micro-decisions executed by software agents interacting directly with merchant data.



Gemini Notebook

The 1999 Vision, Realized in 2026



January 1999: The W3C drafts the Universal Commerce Language and Protocol (UCLP) note, envisioning a web where data tags allow machines to independently evaluate products.

Today: Driven by Generative AI, LLMs, and the semantic web, the 25-year pursuit of machine-readable commerce is finally viable at scale.

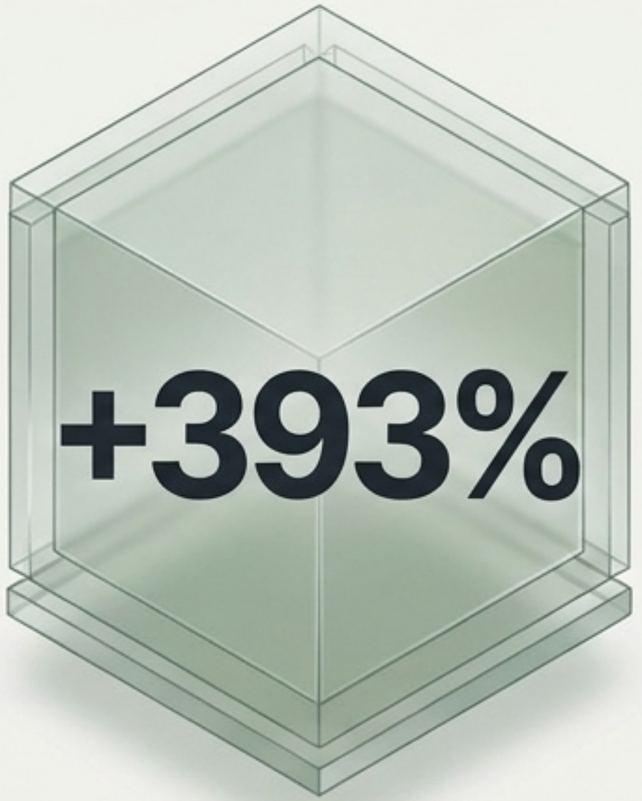
Gemini Notebook

The Trillion-Dollar Substrate



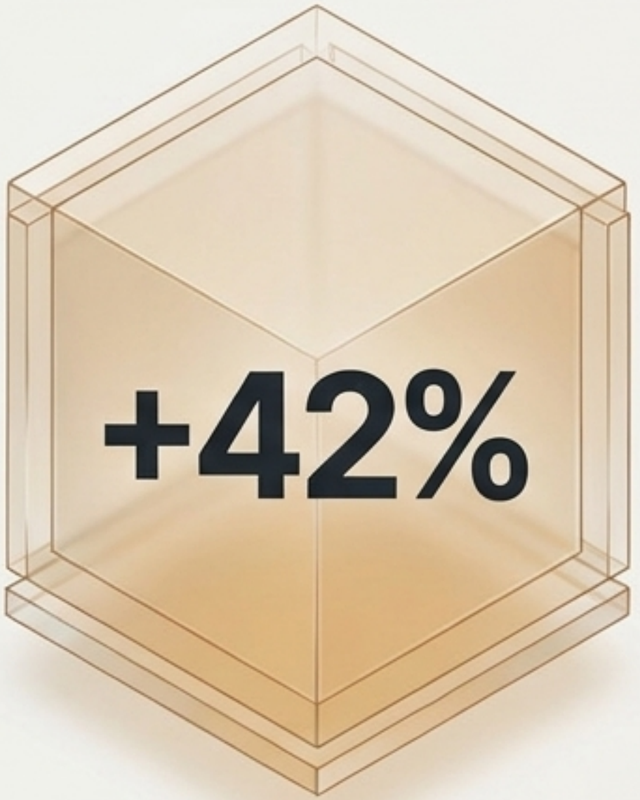
Projected agentic commerce revenue by 2030: up to $1T in US B2C, and $3T-$5T globally.

Source: McKinsey



YoY increase in AI-referred traffic to US retail sites in Q1 2026.

Source: Adobe Analytics

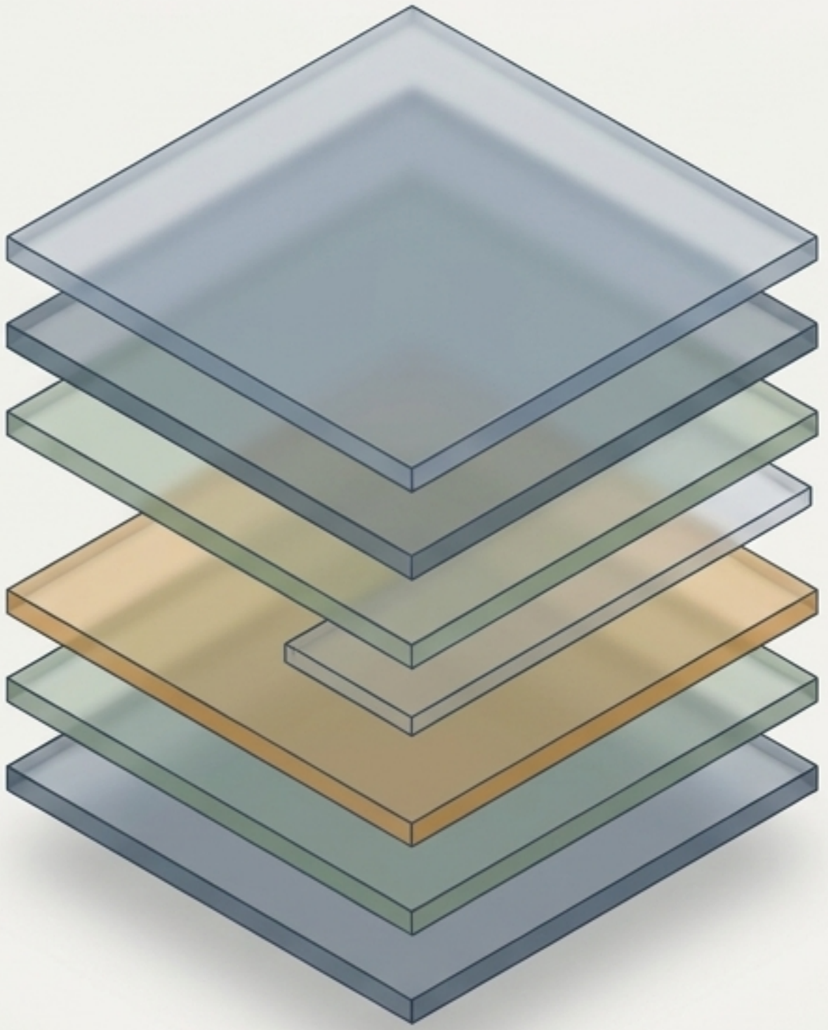


Higher conversion rate for AI-referred traffic compared to traditional channels.

Source: Adobe Analytics

Gemini Notebook

The Web is Growing a Second Addressability Layer



The Agentic Web

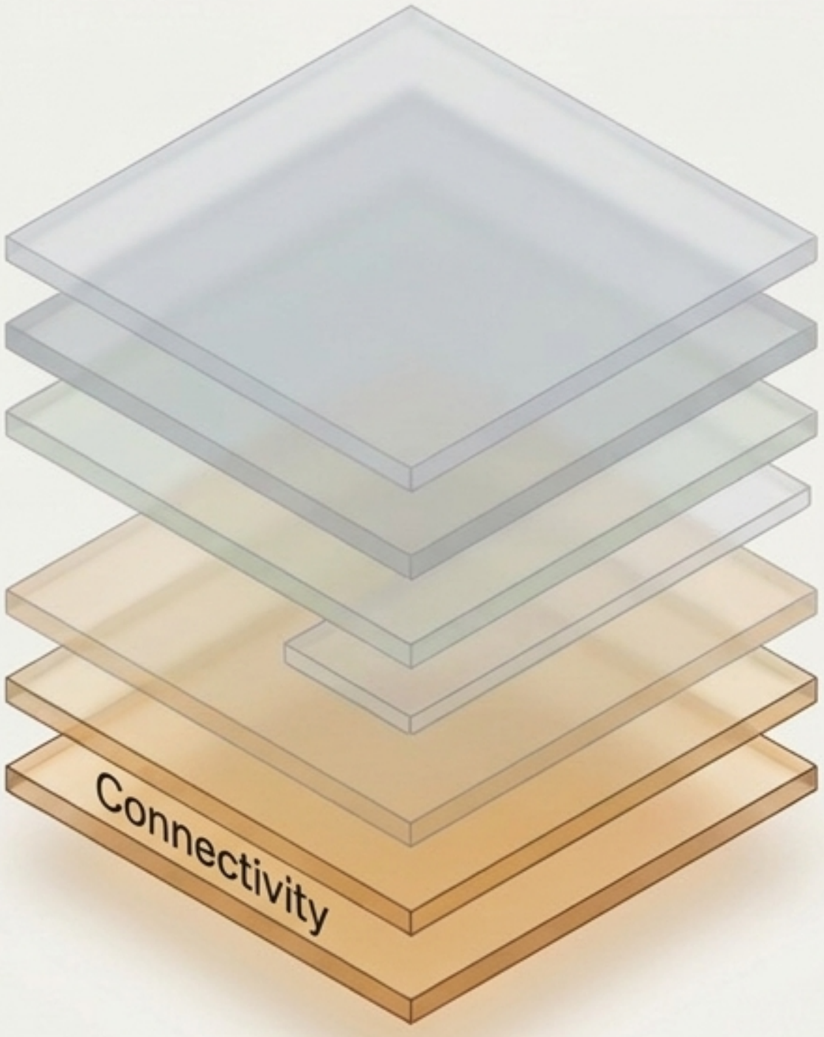
Key Insight:

The Agentic Web is not a single protocol. It is a constellation of complementary standards operating at different layers of the stack.

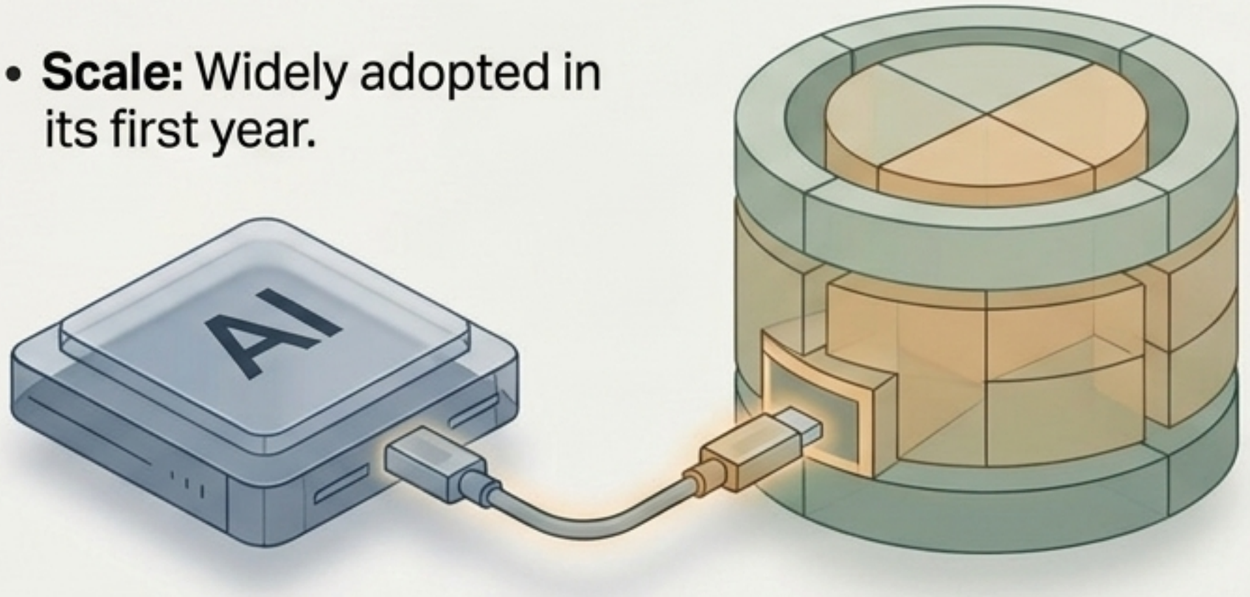
An agent must connect, negotiate, and transact—each requiring distinct rules.

Gemini Notebook

The Connectivity Substrate: MCP



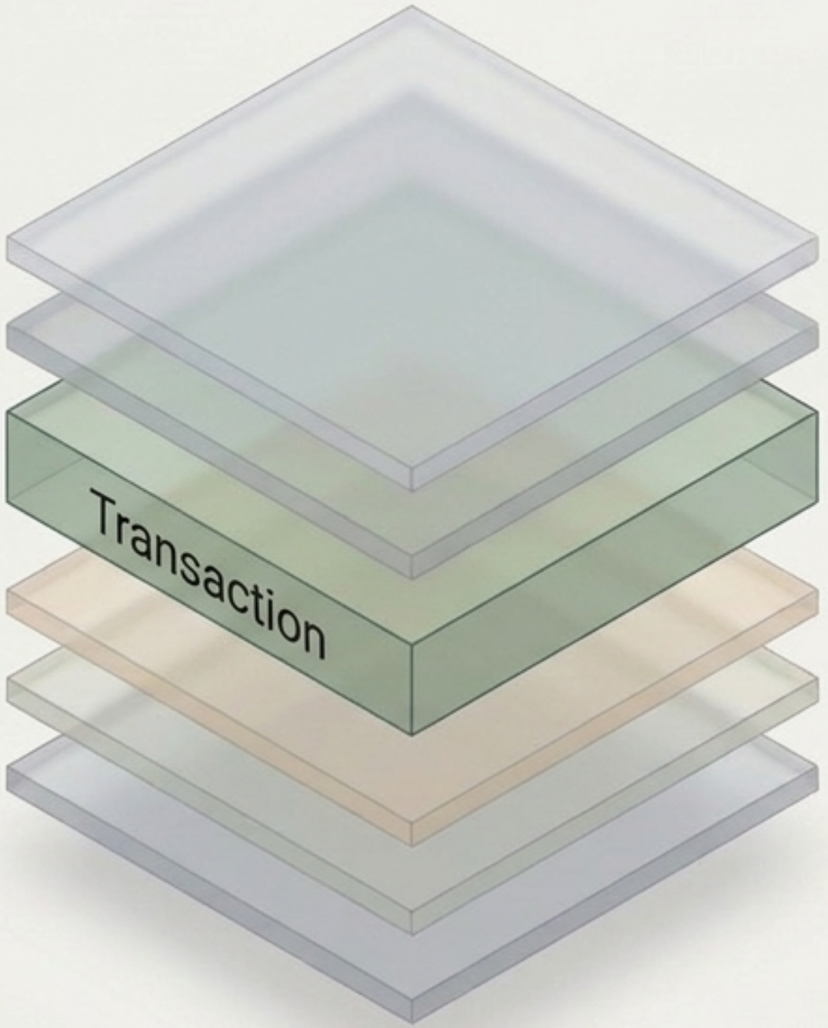
- **Definition:** The Model Context Protocol (governed by the Agentic AI Foundation).
- **Function:** It is not a commerce protocol. It is the open standard for connecting AI applications to external systems and data.
- **Scale:** Widely adopted in its first year.

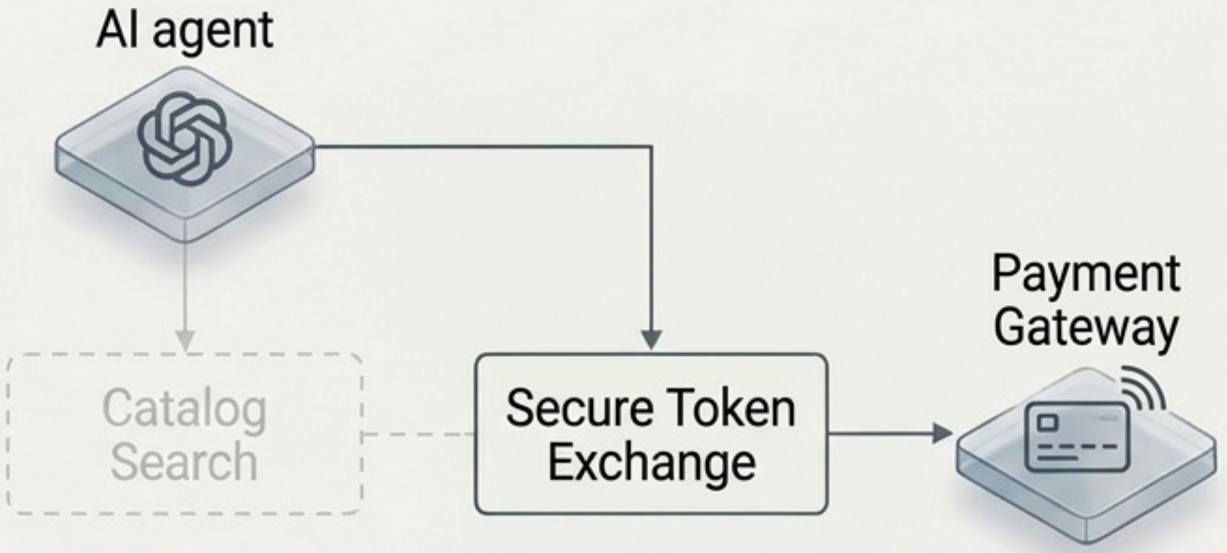


- **Scale:** Widely adopted baseline infrastructure—over 97 million SDK downloads and 10,000+ active servers in its first year.

Gemini Notebook

The Checkout Standard: ACP

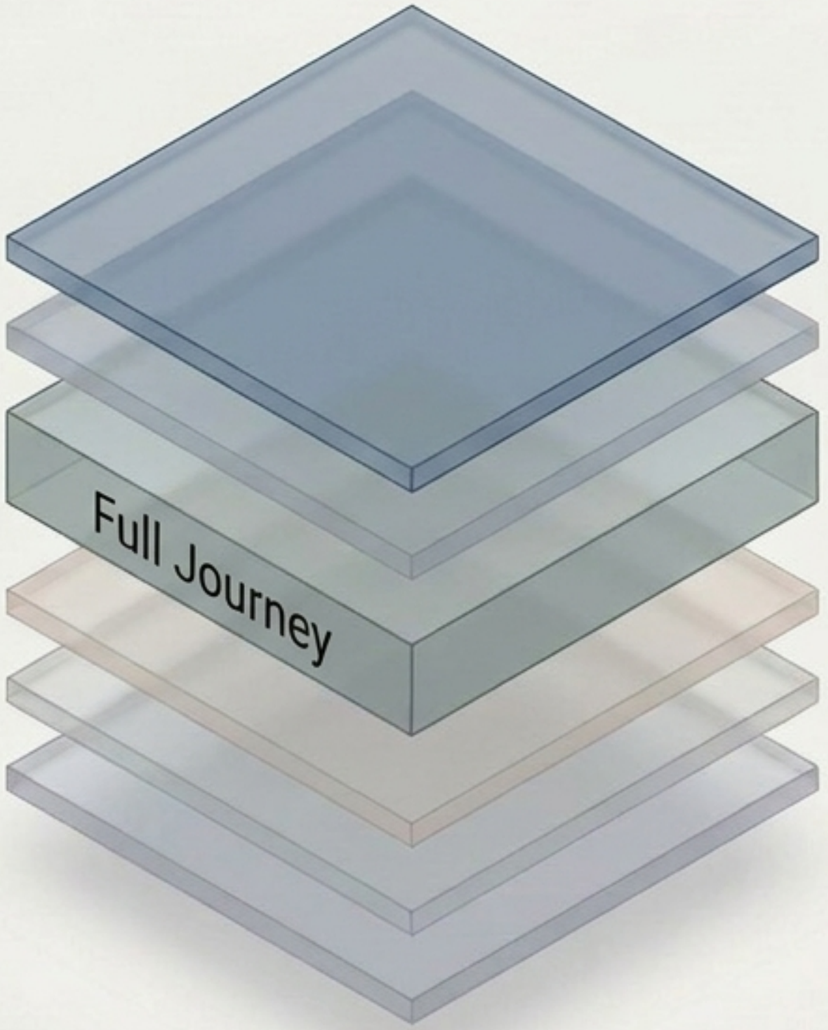


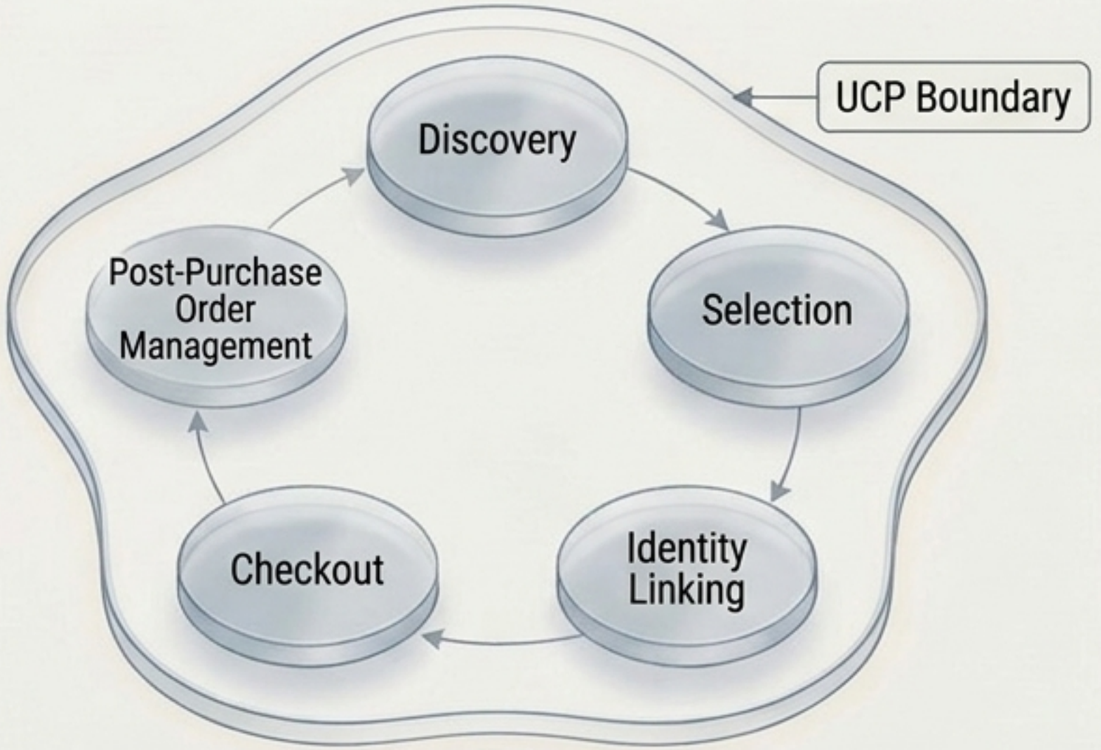


- **Definition:** The Agentic Commerce Protocol (OpenAI / Stripe).
- **Function:** A transaction-only open specification. It renders the checkout interface, manages checkout sessions via a merchant REST API, and relays credentials via delegated payment tokens.
- **Limitation:** It handles the end of the funnel. Discovery and product recommendations are outside its scope.

Gemini Notebook

The Full-Journey Standard: UCP





- **Definition:** The Universal Commerce Protocol (Google / Shopify / Retail Partners).
- **Function:** Standardizes the entire interaction between agents and merchants. It utilizes transport-agnostic capabilities (working over REST, MCP, or A2A) to govern everything from finding a product to post-purchase support.

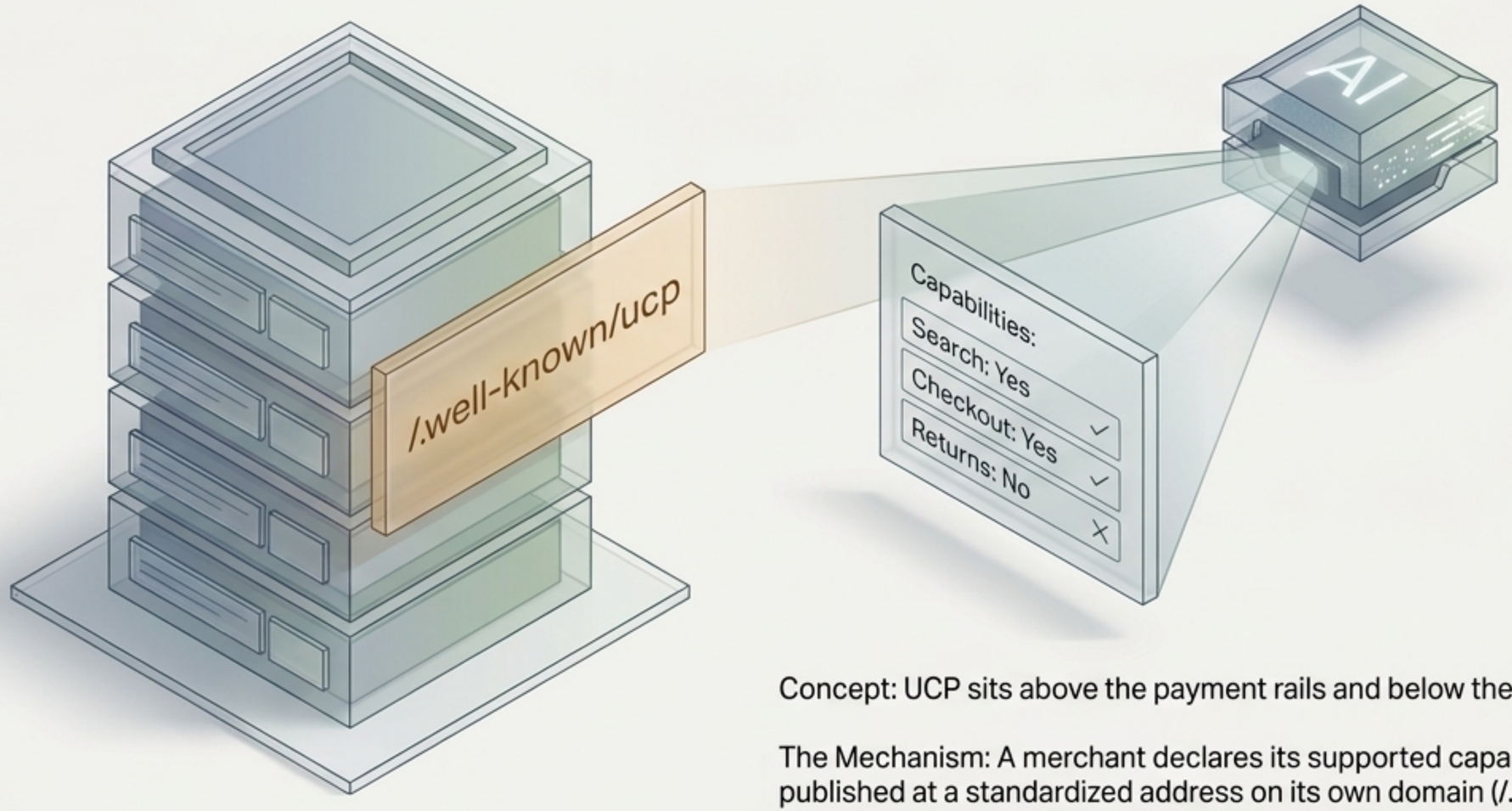
Gemini Notebook

The Definitive Protocol Matrix

	MCP (Connectivity)	ACP (Checkout)	UCP (Full Journey)
Creators	Anthropic / Linux Foundation	OpenAI & Stripe	Google, Shopify & Partners
Architecture	Client-Server tool exposure	REST API for checkout sessions	Composable capabilities via /.well-known/ucp
Key Function	Tool discovery & invocation	Structured payment handlers & tokens	Catalog search, identity linking, order management
Merchant Need	An MCP server exposing systems	Endpoints for payment token handling	Hosted UCP profile & live capability endpoints

Gemini Notebook

How UCP Actually Functions

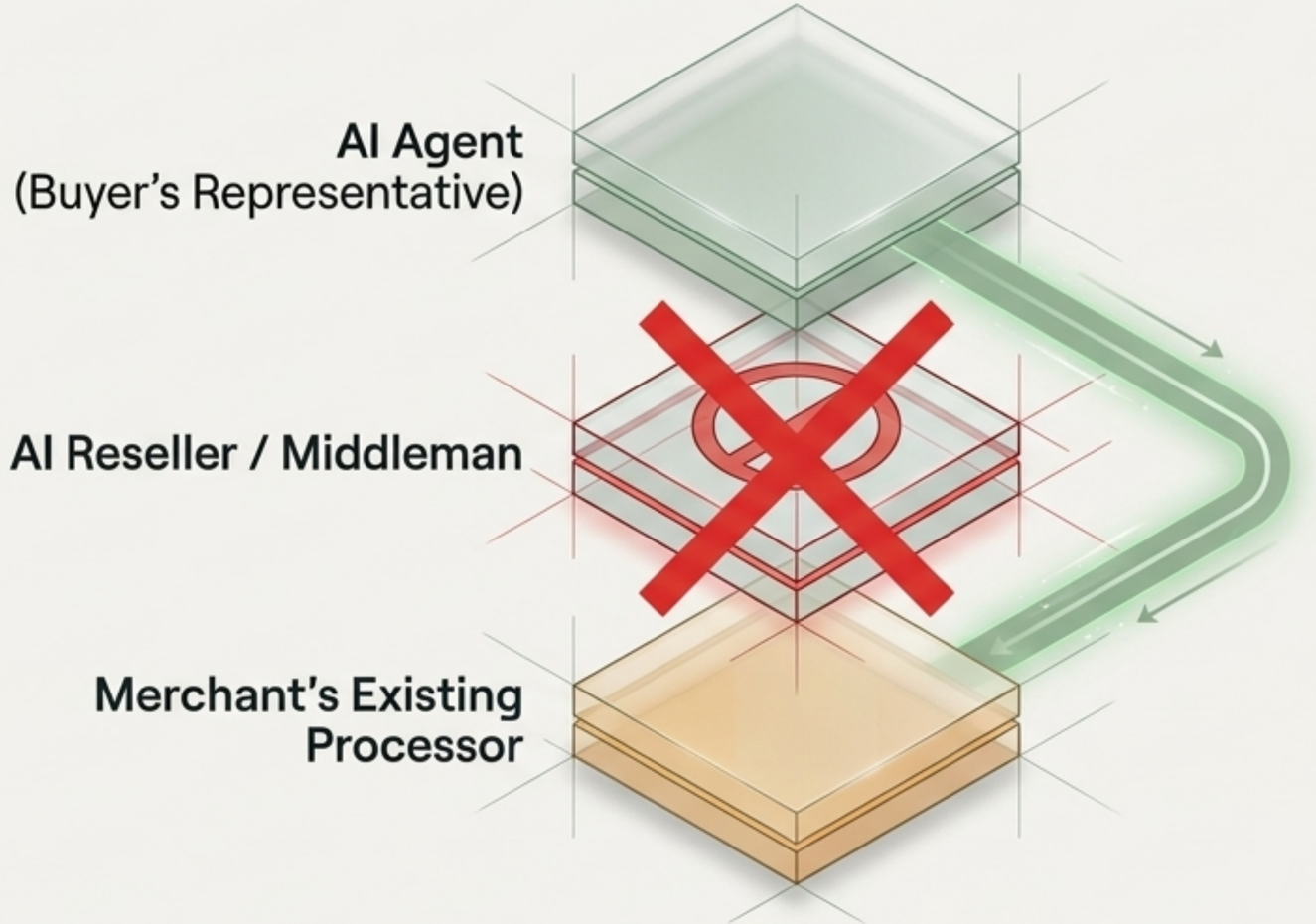


Concept: UCP sits above the payment rails and below the agent.

The Mechanism: A merchant declares its supported capabilities in a profile published at a standardized address on its own domain (/.well-known/ucp). Agents discover this profile and negotiate a session based on the exact intersection of what both the agent and the merchant support.

Gemini Notebook

The CMO’s Anxiety: Who is the Merchant of Record?

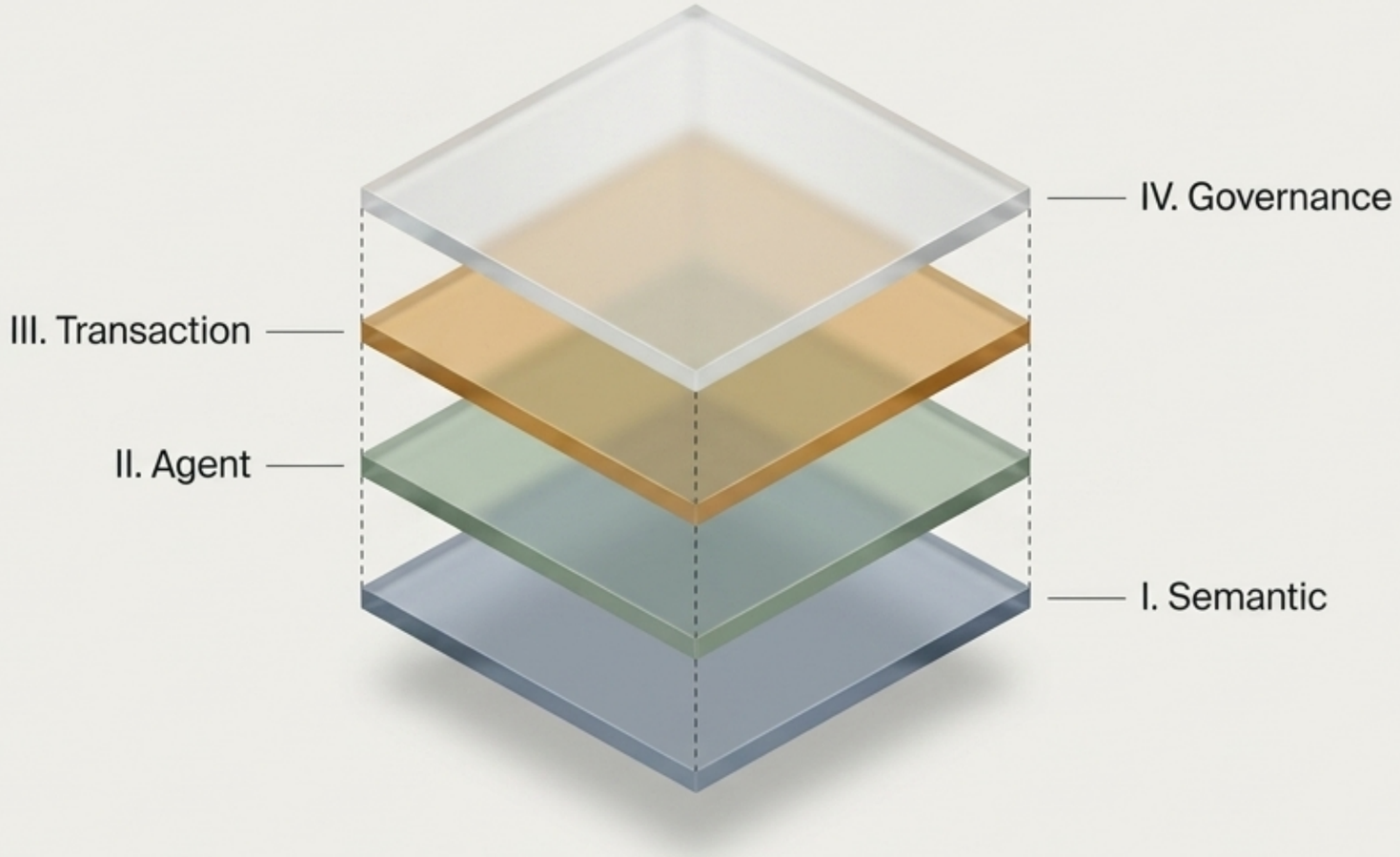


Key Insight: Under UCP, the merchant unequivocally remains the Merchant of Record.

The Reality: The agent orchestrates, but the brand owns the transaction, the customer relationship, the fulfillment, and the margin. Payments flow directly through the merchant’s existing processors.

Gemini Notebook

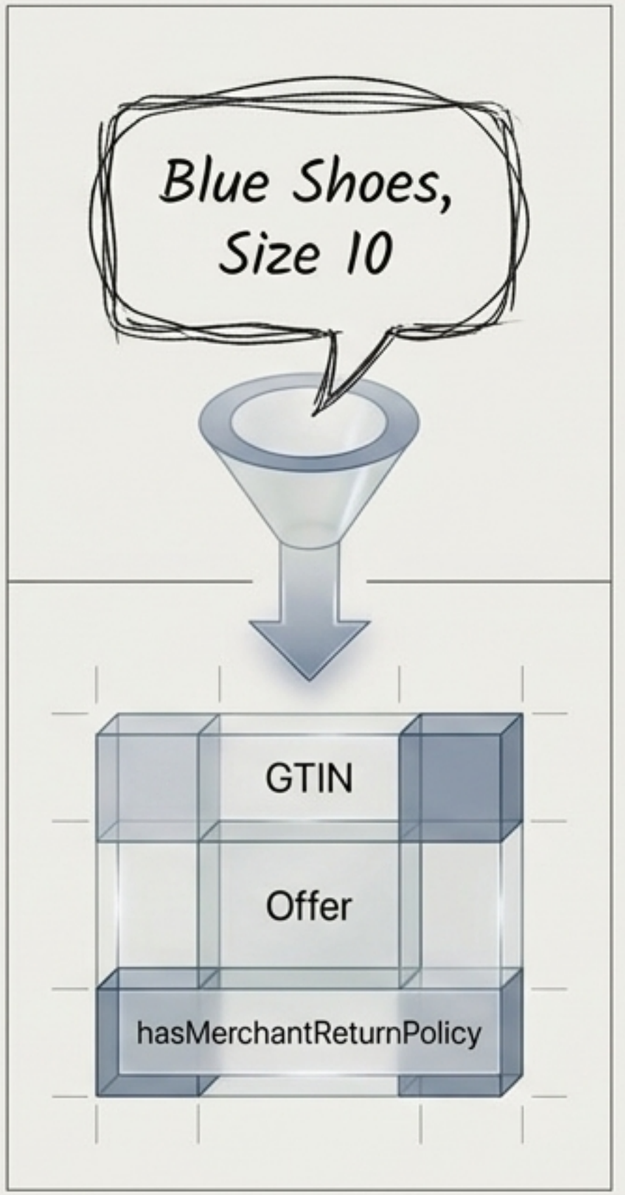
The UCP Framework: Four Mappable Layers



A merchant is UCP-ready when an agent can read its offer (I), interact without ambiguity (II), pay under control (III), and the merchant can audit every decision (IV).

Gemini Notebook





Layer I: The Semantic Layer

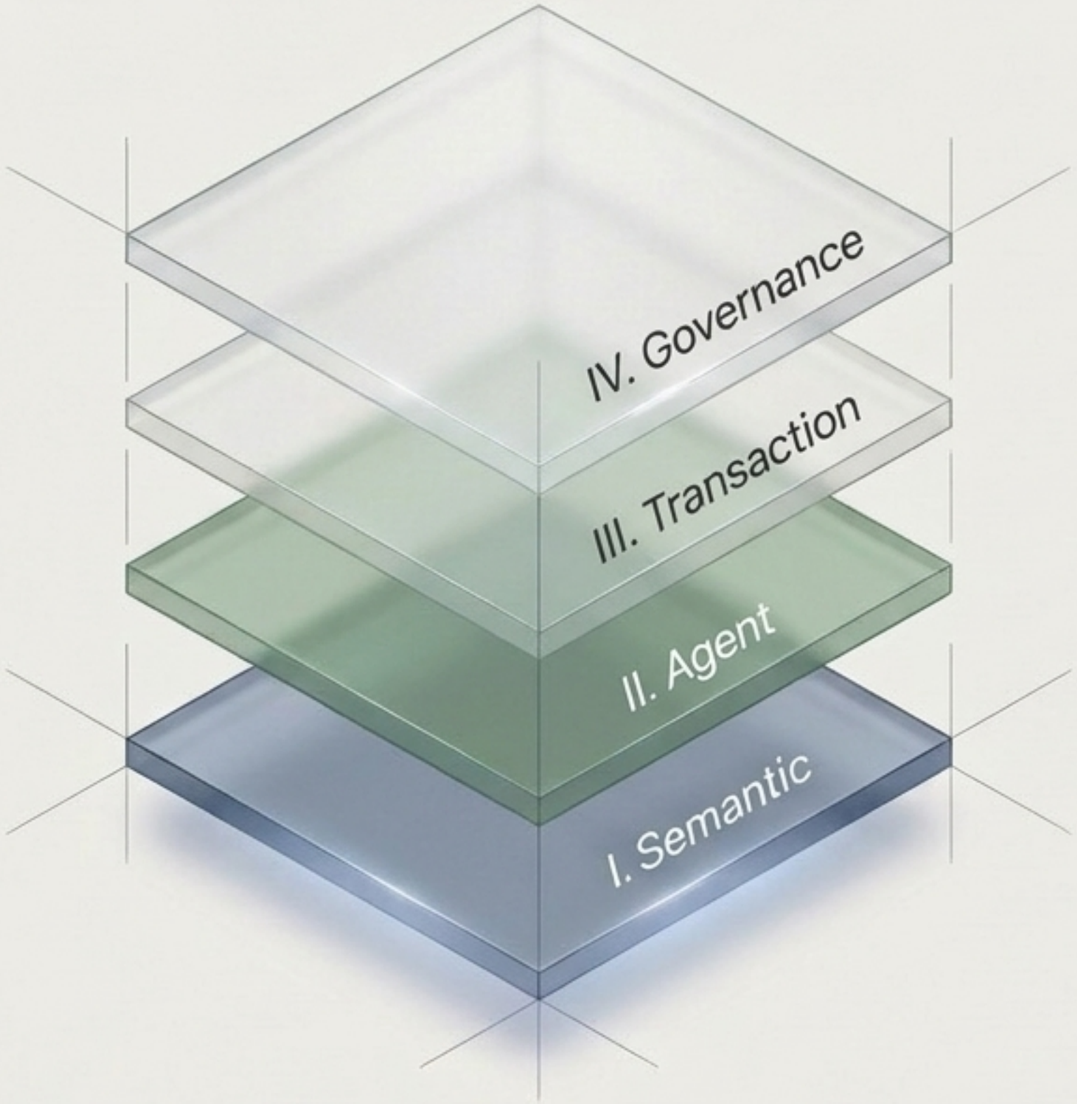
Objective: Making the catalog machine-addressable.

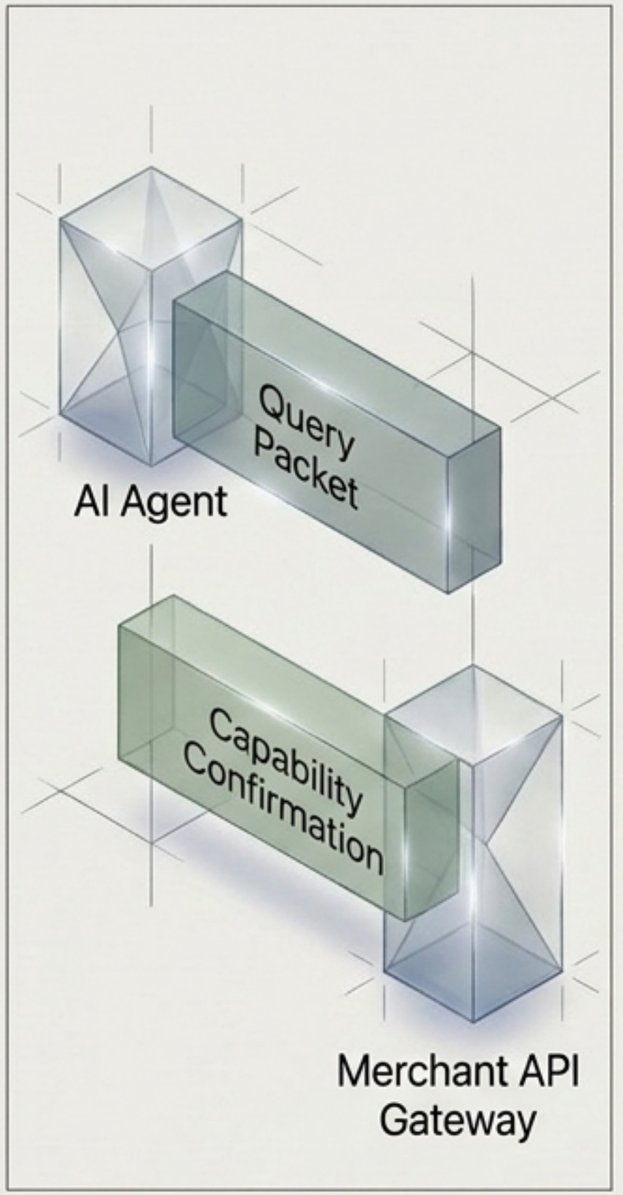
Key Objects: Product, Offer, Policy, Availability.

Standards: Schema.org, GS1 / GTIN, JSON-LD.

Readiness Audit: Do 100% of your product pages have canonical GTINs? Are return policies and delivery times explicitly exposed in JSON-LD?

Gemini Notebook





Layer II: The Agent Layer

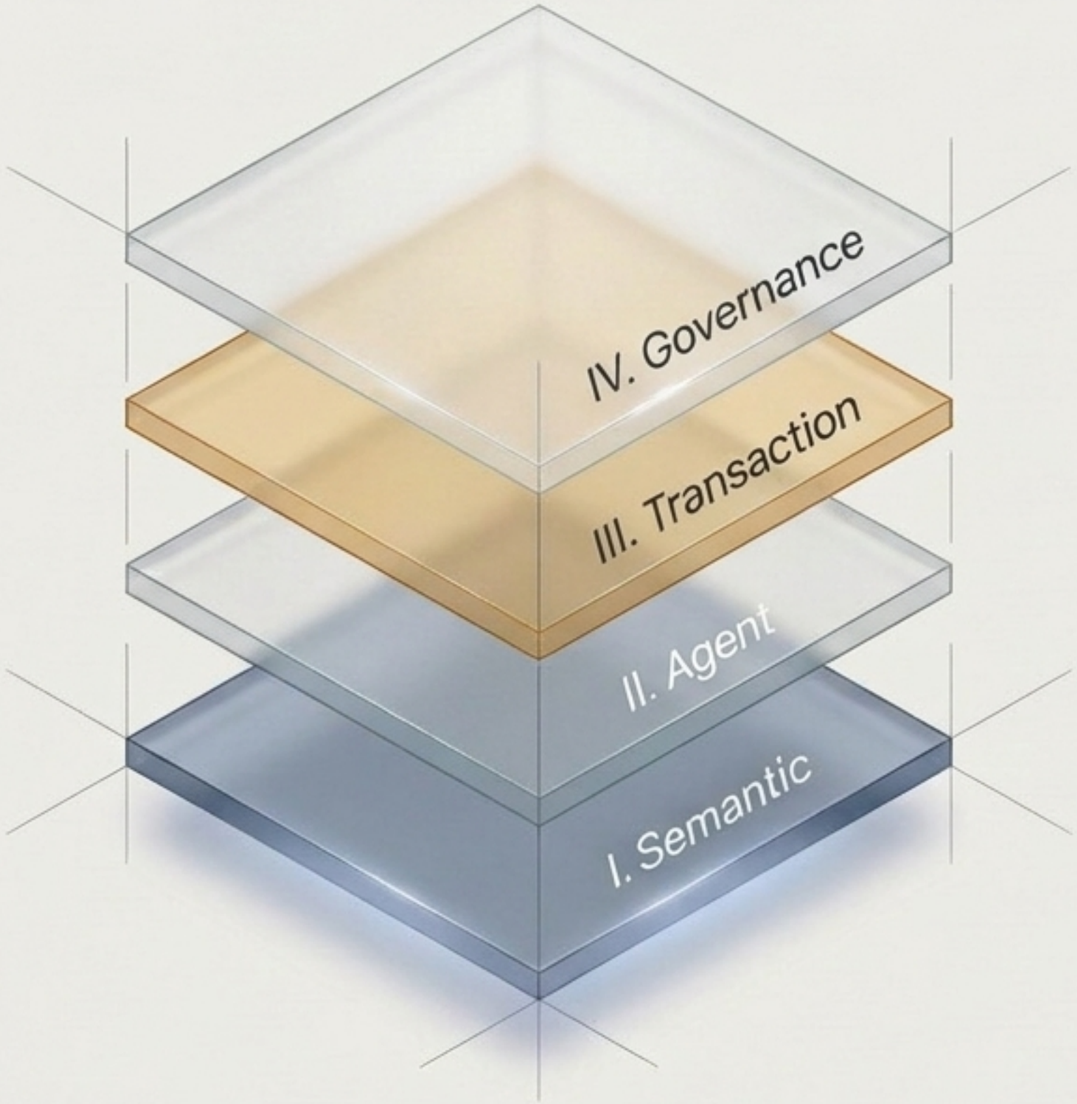
Objective: Opening surfaces that agents can query, propose to, and confirm through.

Key Objects: Tools, Resources, Prompts, Capabilities.

Standards: MCP, A2A (Agent-to-Agent).

Readiness Audit: Does a typed entry point exist for querying the catalog? Are your tools discoverable via a registry? Is end-to-end agent response latency optimized?

Gemini Notebook





Layer III: The Transaction Layer

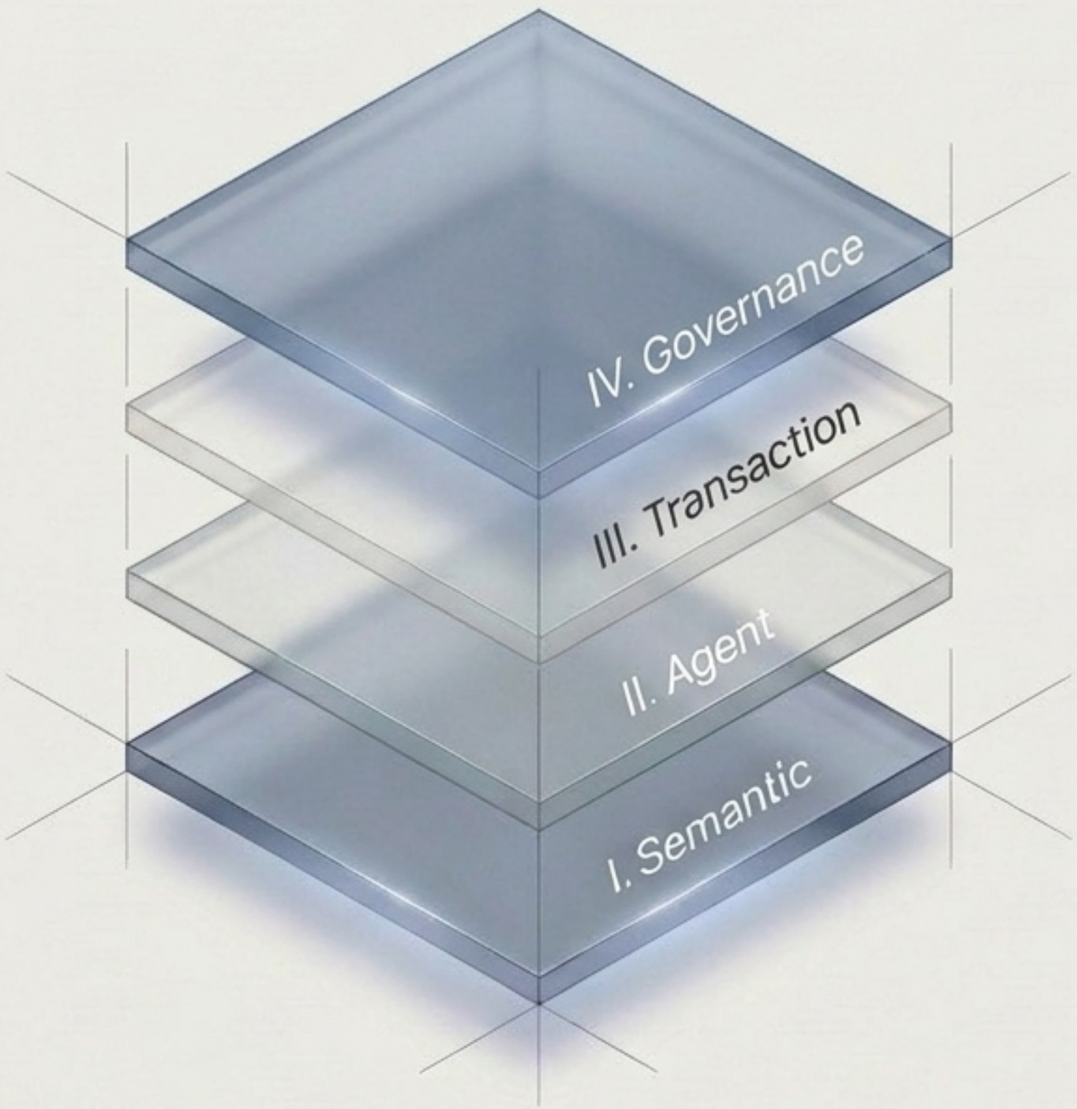
Objective: Making payment and identity compatible with a delegated buyer.

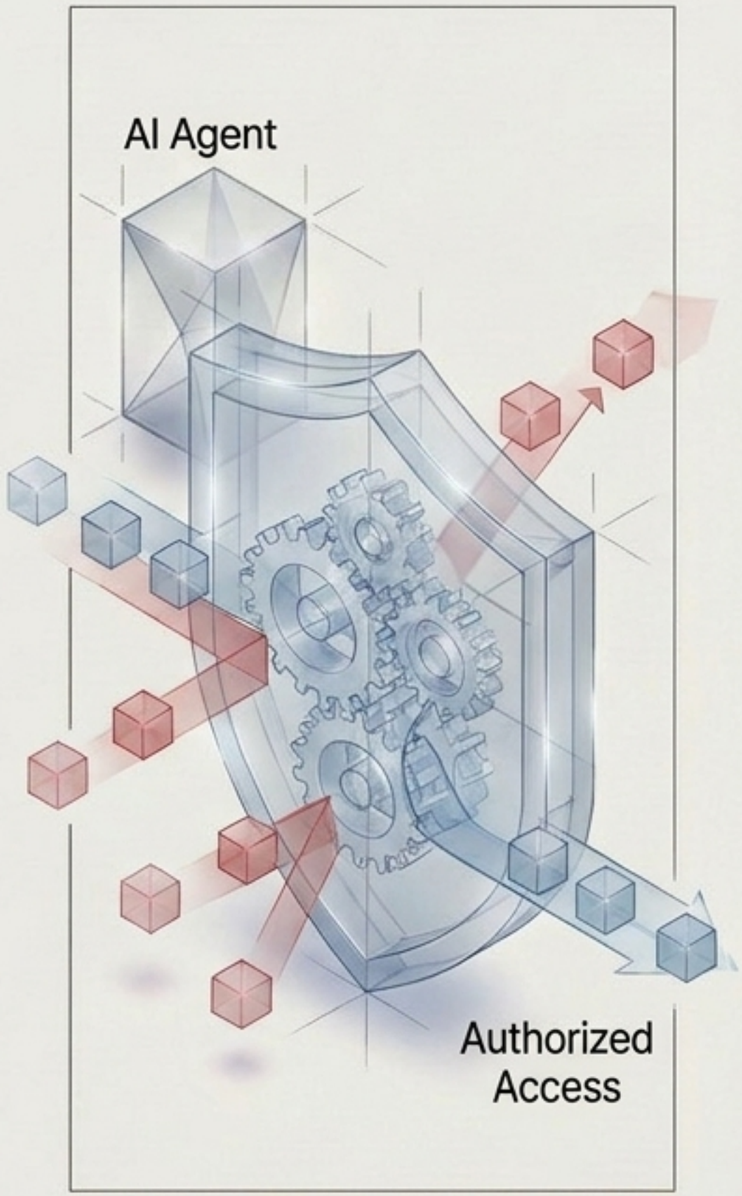
Key Objects: Intent, Credential, Spend Limit, Dispute.

Standards: AP2 (Agent Payments Protocol via FIDO), ACP.

Readiness Audit: Can a delegated payment process with strict, revocable limits? Are disputes accurately attributed to the human vs. the agent?

Gemini Notebook





Layer IV: The Governance Layer

Objective: Exposing, versioning, and controlling the rules that govern the offer.

Key Objects: Pricing rules, Eligibility, Territory, Audit logs.

Standards: OPA (Open Policy Agent), W3C Verifiable Credentials.

Readiness Audit: Can you opt-out a specific category of agents for a specific product line? Does a versioned log of automated governance decisions exist?

Gemini Notebook

The Nouns vs. Verbs Paradigm

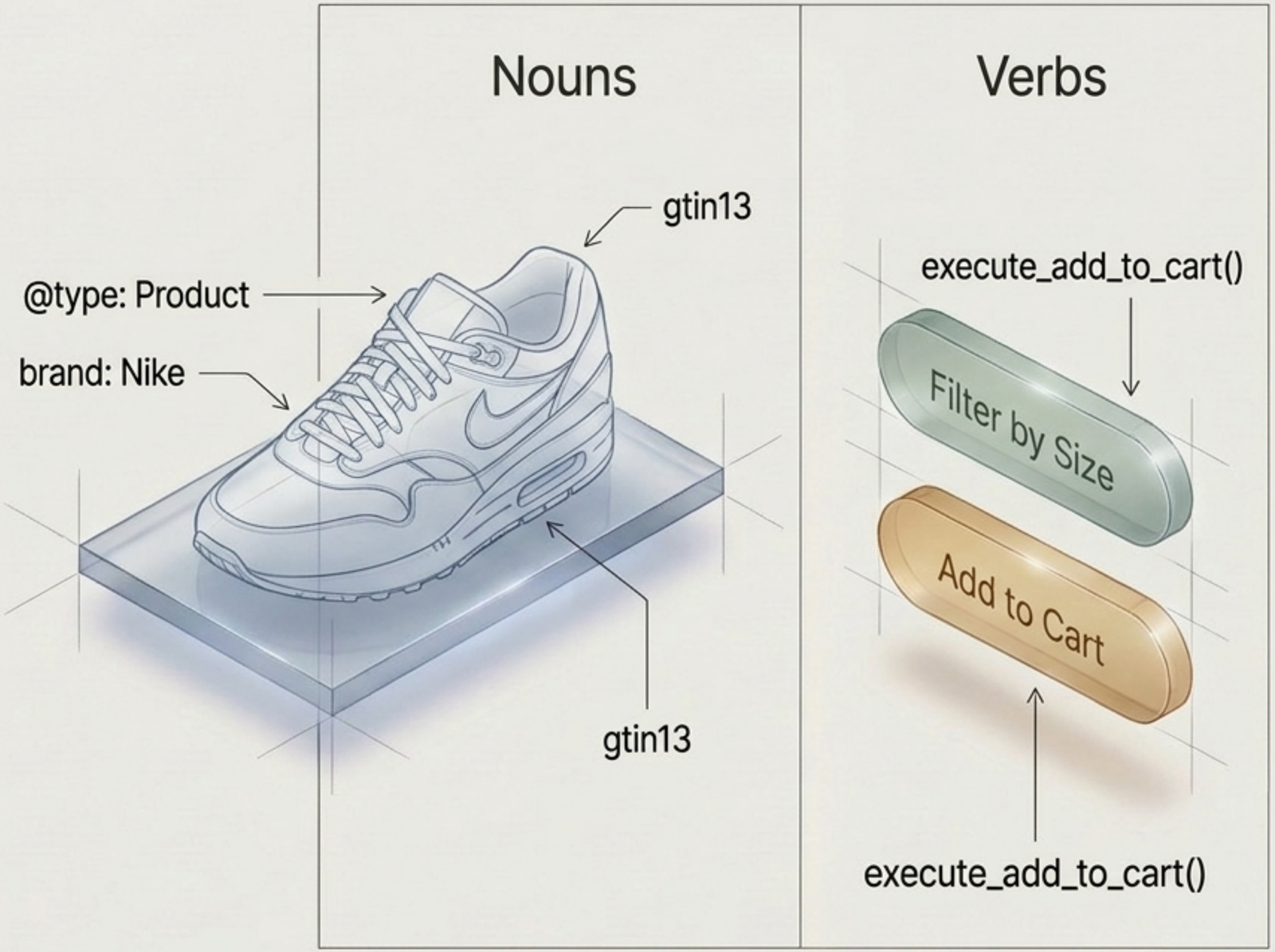
Key Insight: The illusion of Agent Readiness.

You cannot have Verbs without Nouns.

UCP and WebMCP describe what an agent can do (the Verbs).

Schema.org describes what the things are (the Nouns).

If product data is incomplete, agents will fail to execute verbs. Protocols only move data; they do not fix it.

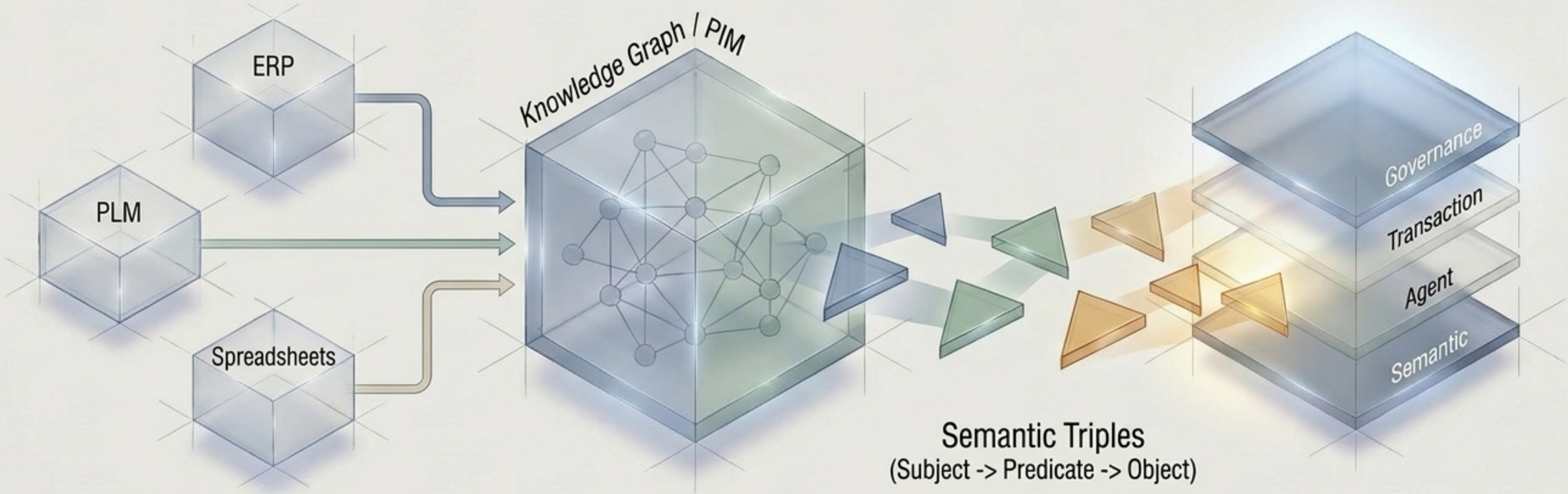


Gemini Notebook

The True Substrate: Internal Knowledge Graphs

The Reality: When an agent calls **getProductDetails()**, it does not want rendered HTML; it wants the structured object the page was rendered from.

The Discipline: Designing UCP tool responses requires modeling entities as semantic triples (**Subject —> Predicate —> Object**). A well-formed tool output is just a **serialized subgraph** from your PIM.

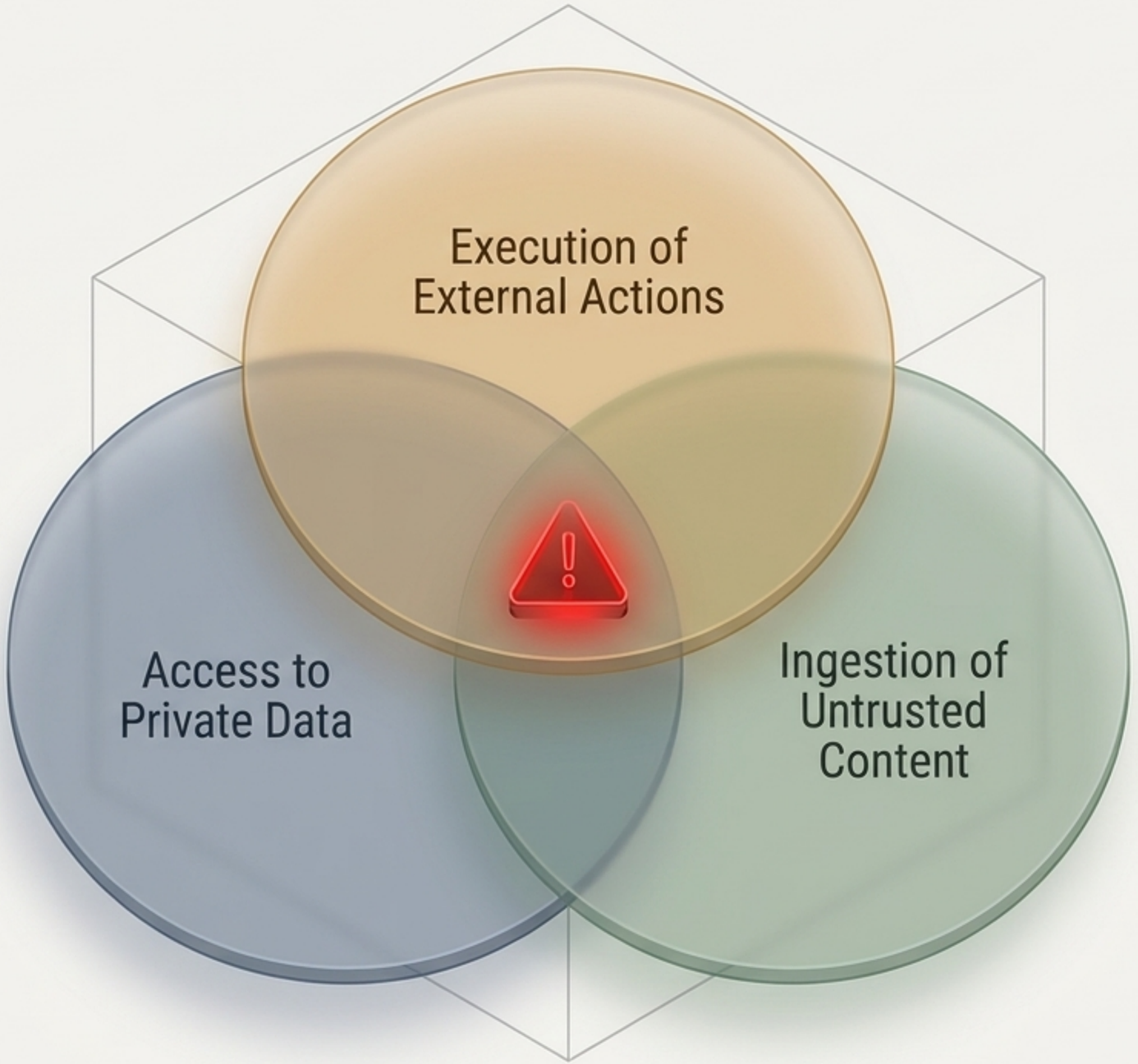


Gemini Notebook

Security and The Lethal Trifecta

Key Risks:

1. Prompt Injection: Malicious copy hidden in a product review steering the agent's behavior.
2. Output Injection: Tool returns containing instructions that hijack the agent's next planned move.
3. Deceptive Descriptions: An agent misinterpreting an add_to_cart tool as a harmless query, accidentally initiating a purchase.

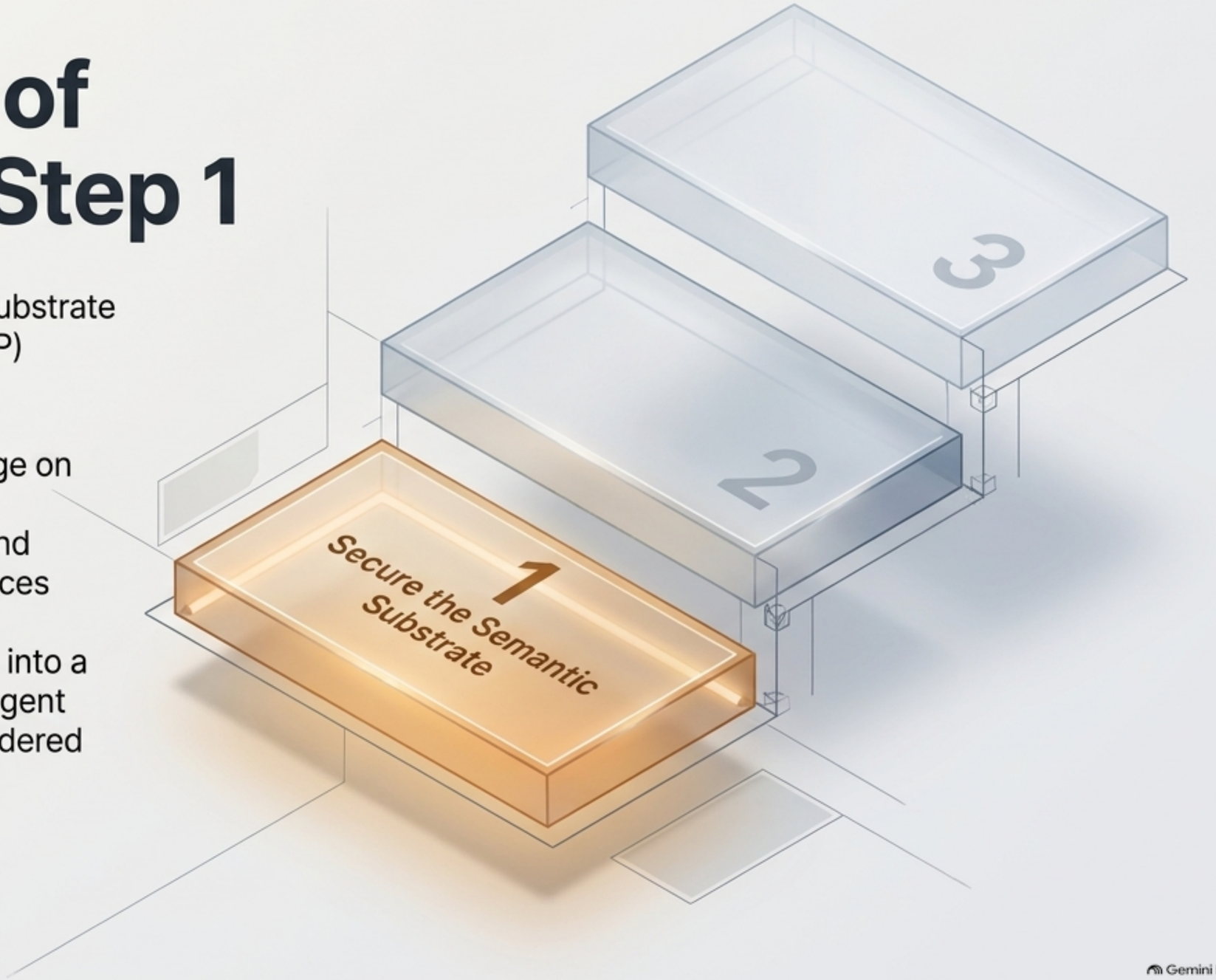


Gemini Notebook

Sequence of Priorities: Step 1

Action: Secure the Semantic Substrate (Do this regardless of UCP/MCP)

Details:
- Achieve full JSON-LD coverage on every primary entity.
- Establish stable @id values and sameAs links to canonical sources (Wikidata, manufacturer sites).
- Consolidate fragmented data into a unified PIM system to ensure agent responses perfectly match rendered HTML.

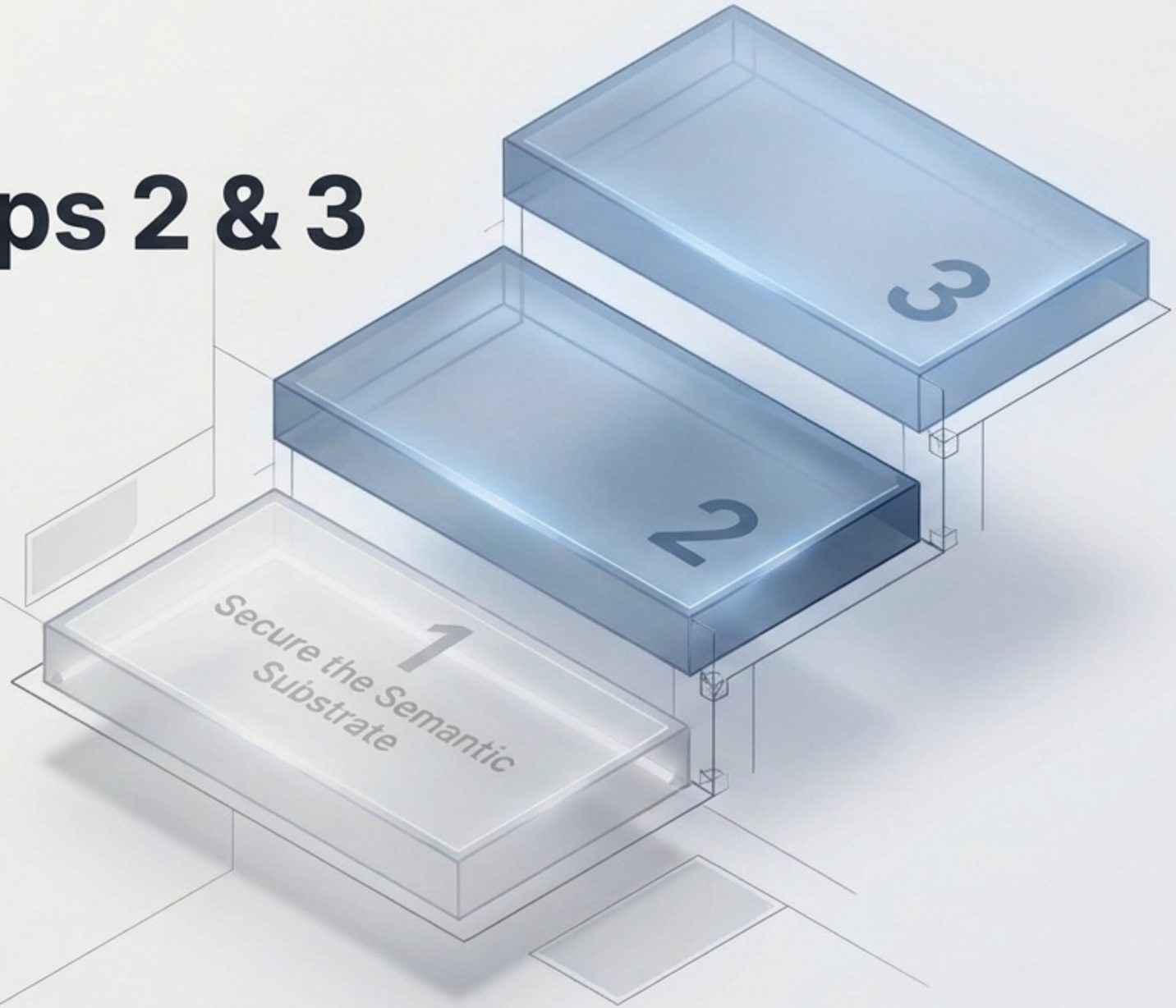


Gemini Notebook

Sequence of Priorities: Steps 2 & 3

Step 2: Design the Tool Taxonomy
- Inventory every form, filter, and calculator on your site.
- Draft tool contracts like a public REST API: snake_case action verbs and 1-sentence descriptions written for LLM comprehension.

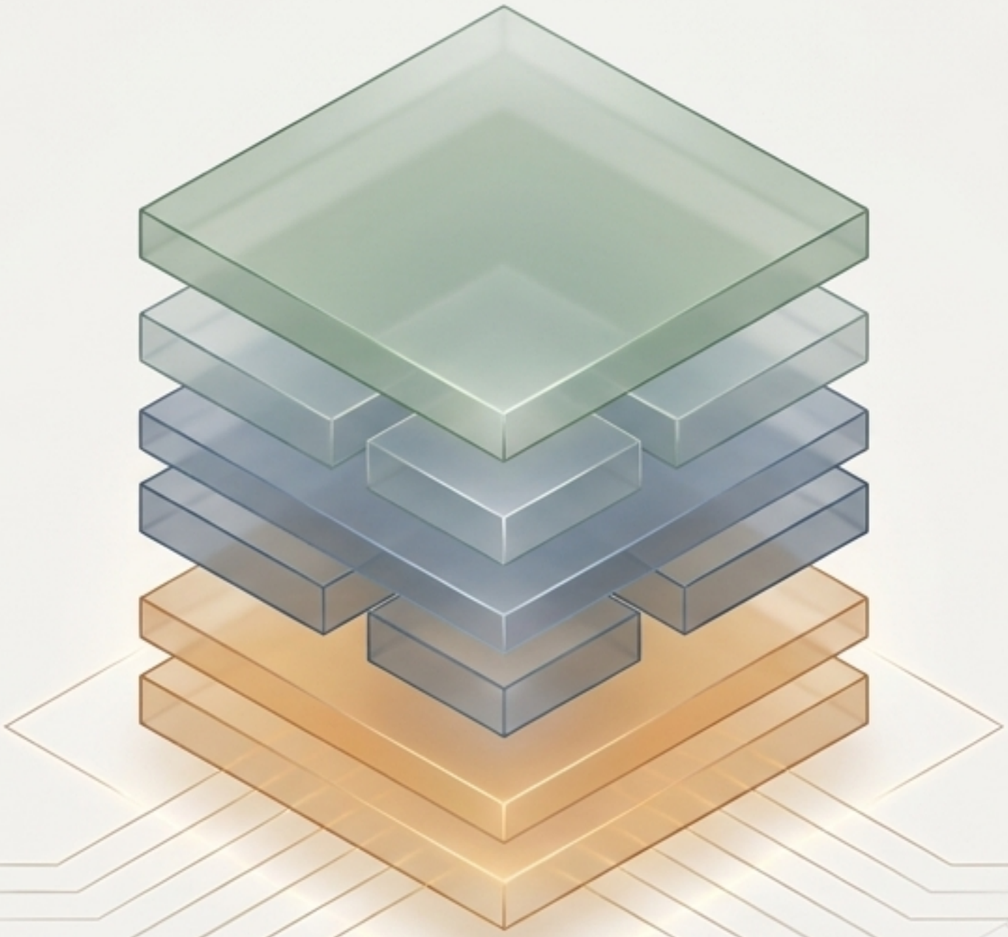
Step 3: Prototype, Do Not Ship
- Test on read-only, non-sensitive canonical tools first (e.g., price lookups, shipping estimates).
- Never expose payment fields or PII forms to agents until the security model matures.



Gemini Notebook

The Agentic Visibility Imperative

Closing Insight: Every time the web has added a new machine-readable layer—robots.txt, XML sitemaps, Schema.org—the sites that structured their data early compounded a decade of advantage. The web is growing its second addressability layer right now.



The Question: As UI-mediated purchases decline, are you becoming easier or harder for machines to discover?

Gemini Notebook