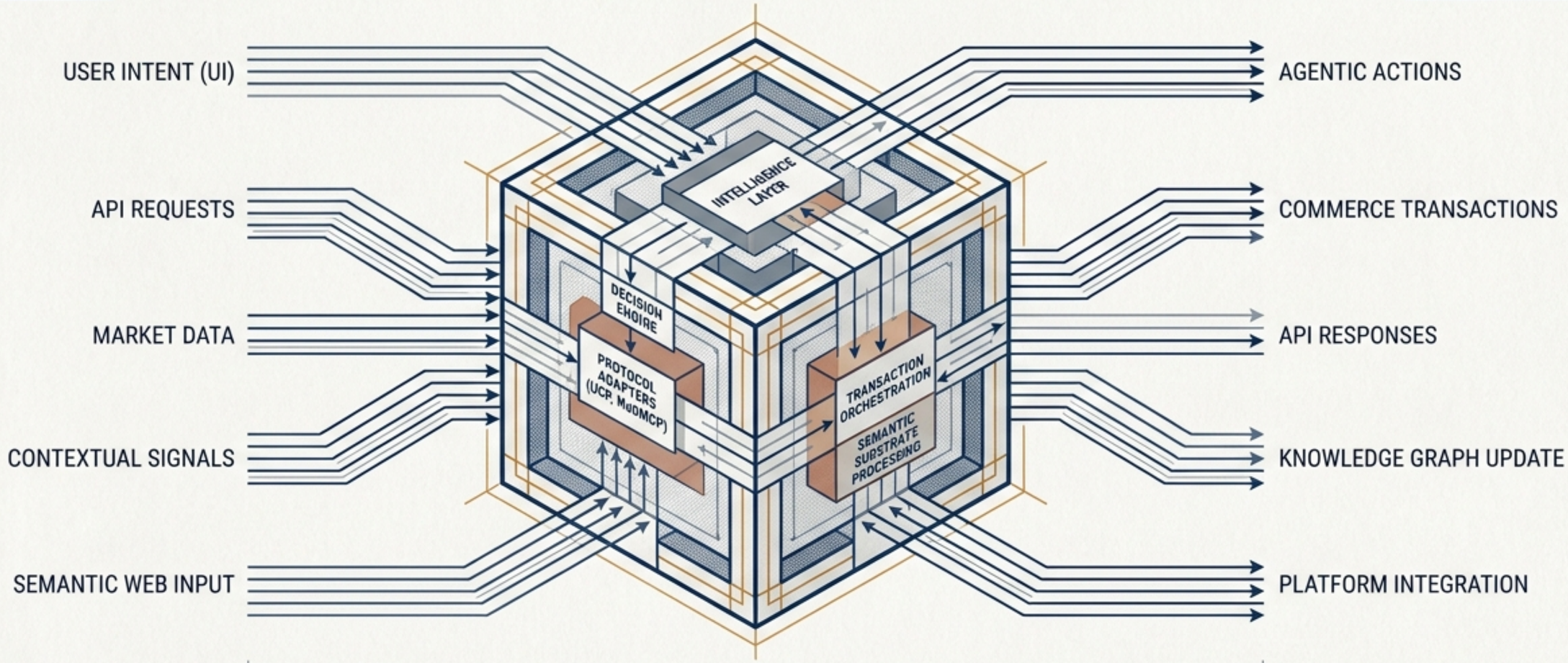
# The Architecture of Agentic Commerce

## From UI to API: Navigating UCP, WebMCP, and the New Semantic Substrate

SCHEMATIC OVERVIEW

SCALE: NOT TO SCALE



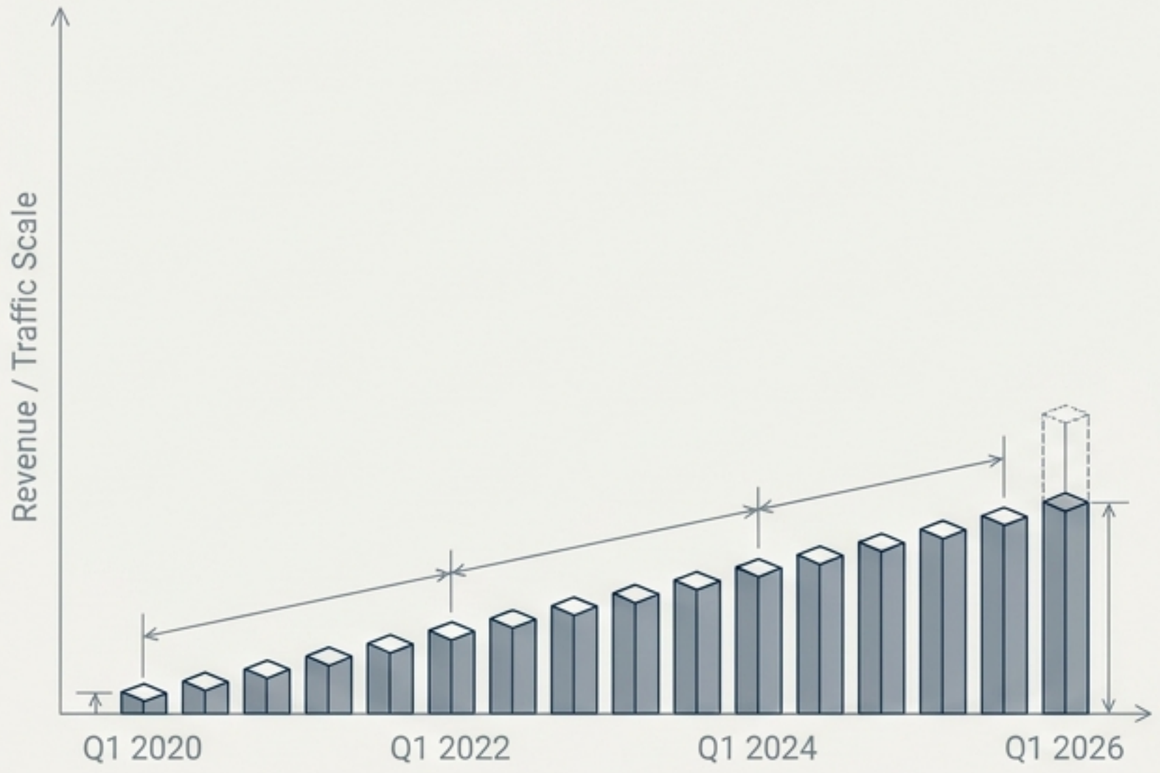

SCALE: NOT TO SCALE

SYSTEM ARCHITECTURE v1.2

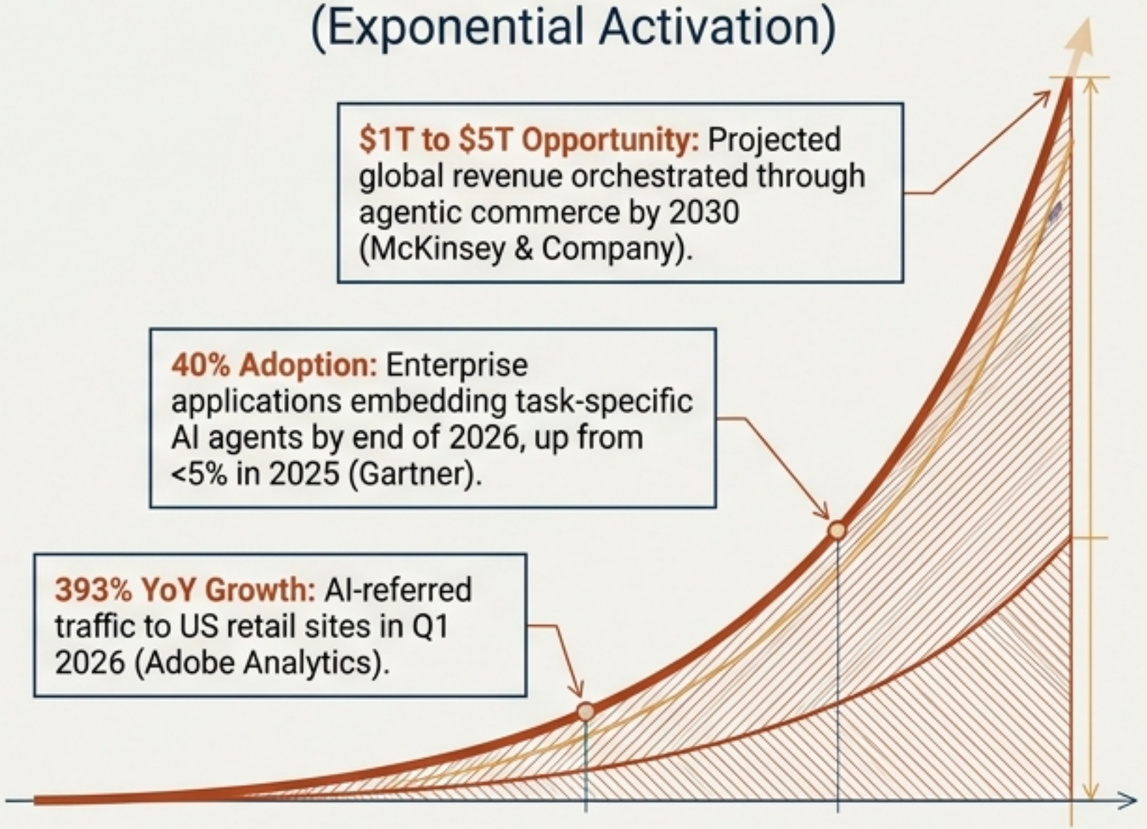
Gemini Notebook

# THE $5 TRILLION PARADIGM SHIFT

## TRADITIONAL E-COMMERCE
(Incremental Growth)




## AGENTIC COMMERCE EXPLOSION
(Exponential Activation)



**$1T to $5T Opportunity:** Projected global revenue orchestrated through agentic commerce by 2030 (McKinsey & Company).

**40% Adoption:** Enterprise applications embedding task-specific AI agents by end of 2026, up from <5% in 2025 (Gartner).

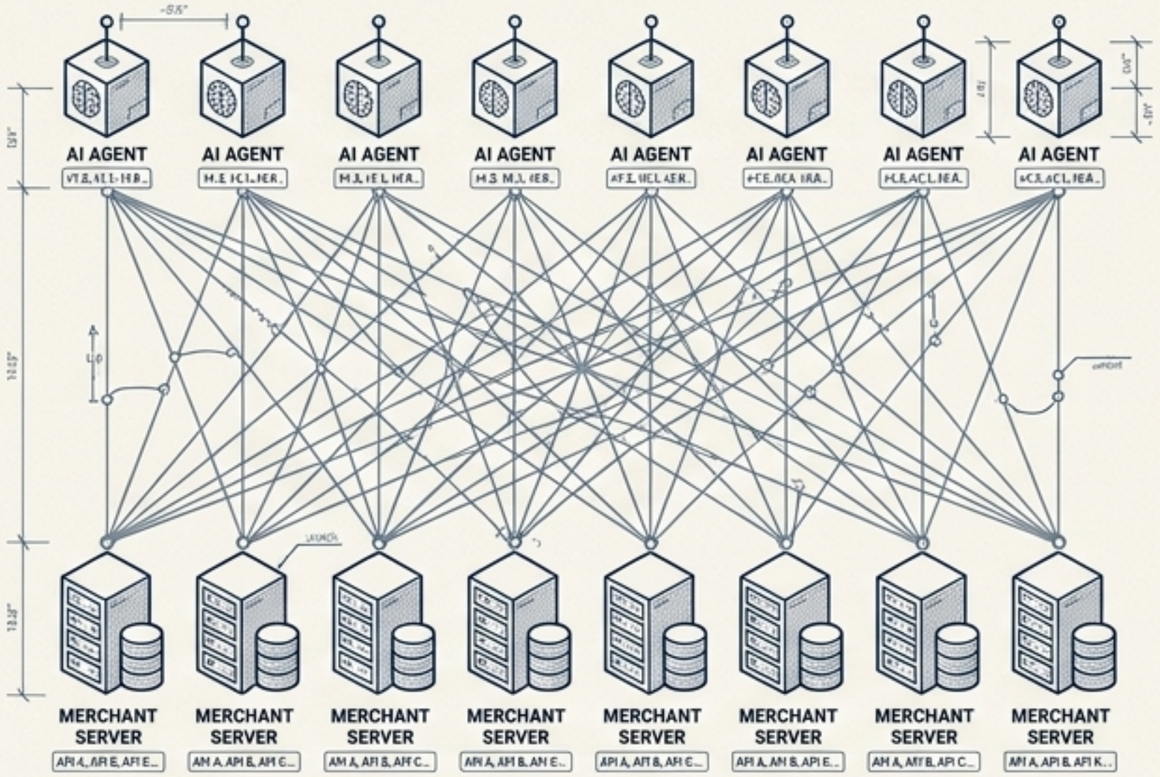
**393% YoY Growth:** AI-referred traffic to US retail sites in Q1 2026 (Adobe Analytics).

The conventional customer journey, characterized by conscious human decision points, is being replaced by continuous, automated micro-decisions performed by software agents.

Gemini Notebook

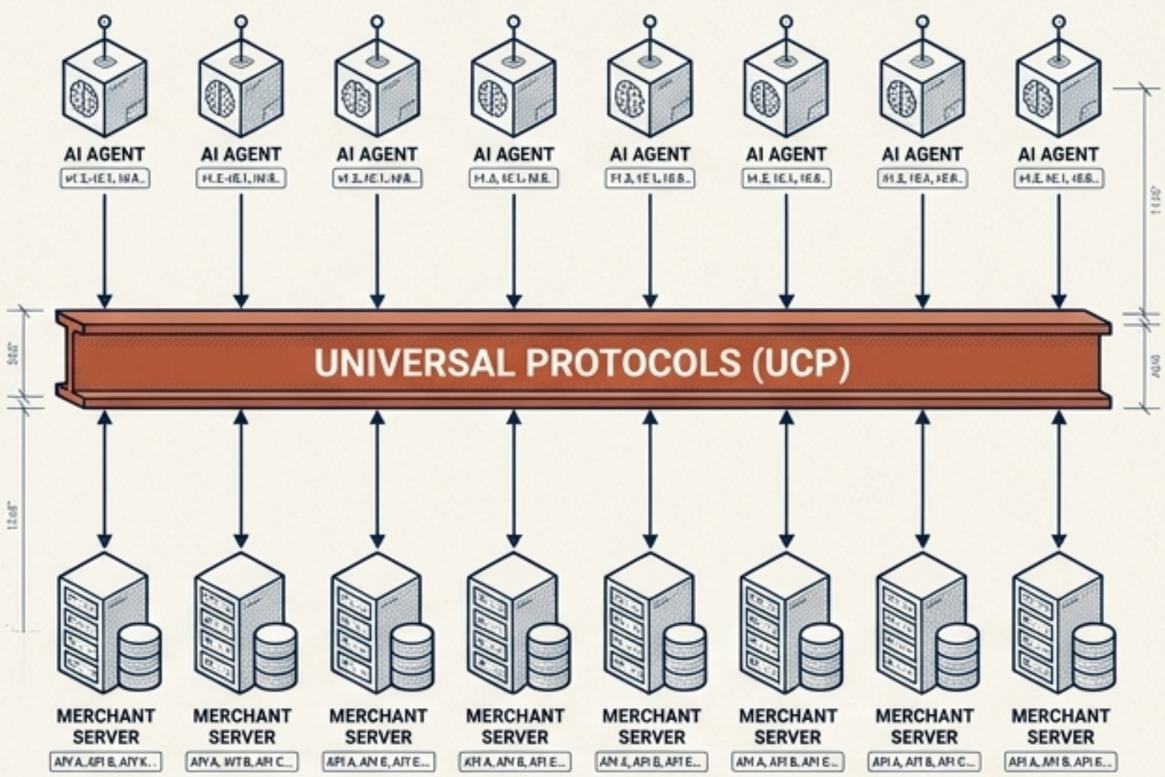
# The N by N Integration Bottleneck

## The Chaos




**Bespoke Connections:** Fragile, expensive, unscalable.

## The Standard




**Universal Protocols (UCP):** Implement once, transact anywhere.

Without a standard, every AI platform requires a bespoke connection to every merchant backend.
**Protocols collapse this into a single shared language.**

Gemini Notebook

# The Engine of the Agentic Web: Nouns vs. Verbs

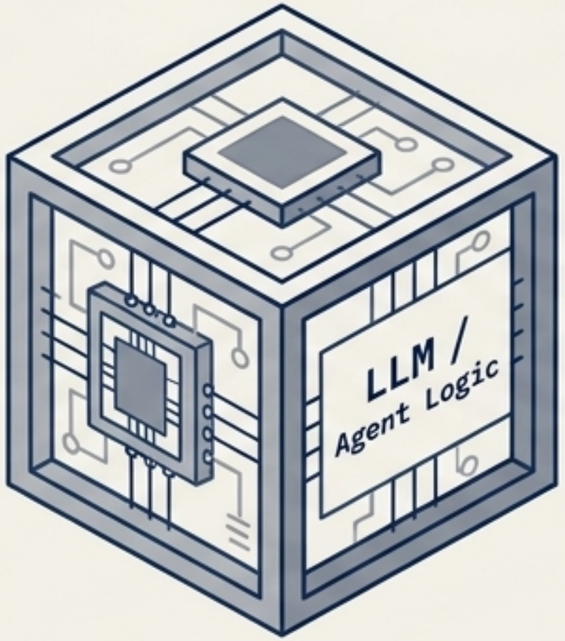
## The Fuel – Nouns

Schema.org /
Internal Knowledge Graphs



Describes what things ARE (Products, Offers, Policies).

## The Processor




## The Exhaust – Verbs

UCP

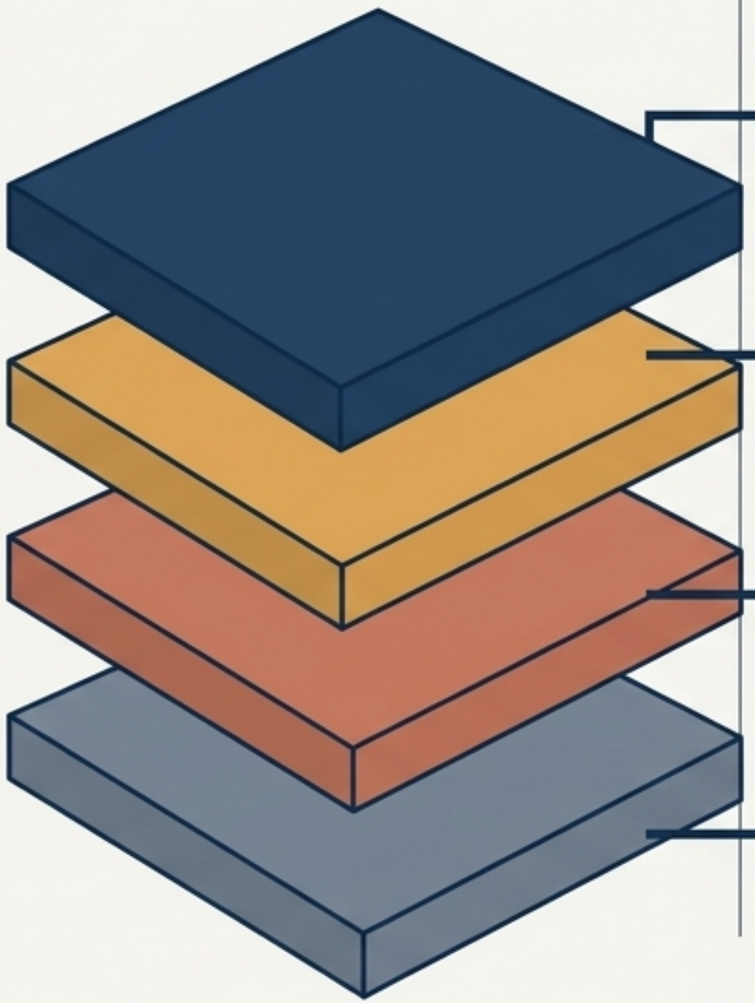
WebMCP

Describes what an agent can DO with them (Filter, Add to Cart, Checkout).

The verbs only work when the nouns are legible. An agent cannot confidently invoke a checkout verb if it cannot read the underlying product noun.

Gemini Notebook

# The 4-Layer Agentic Stack



### Layer 4: Governance

**Standards:** `OPA / Rego, W3C VC, Audit Logs`
**Function:** Expose, version, and control the rules.

### Layer 3: Transaction

**Standards:** `ACP, UCP, Visa Intelligent Commerce`
**Function:** Payment and identity for delegated buyers.

### Layer 2: Agent

**Standards:** `WebMCP, A2A, MCP`
**Function:** Open surfaces for agents to query and confirm.

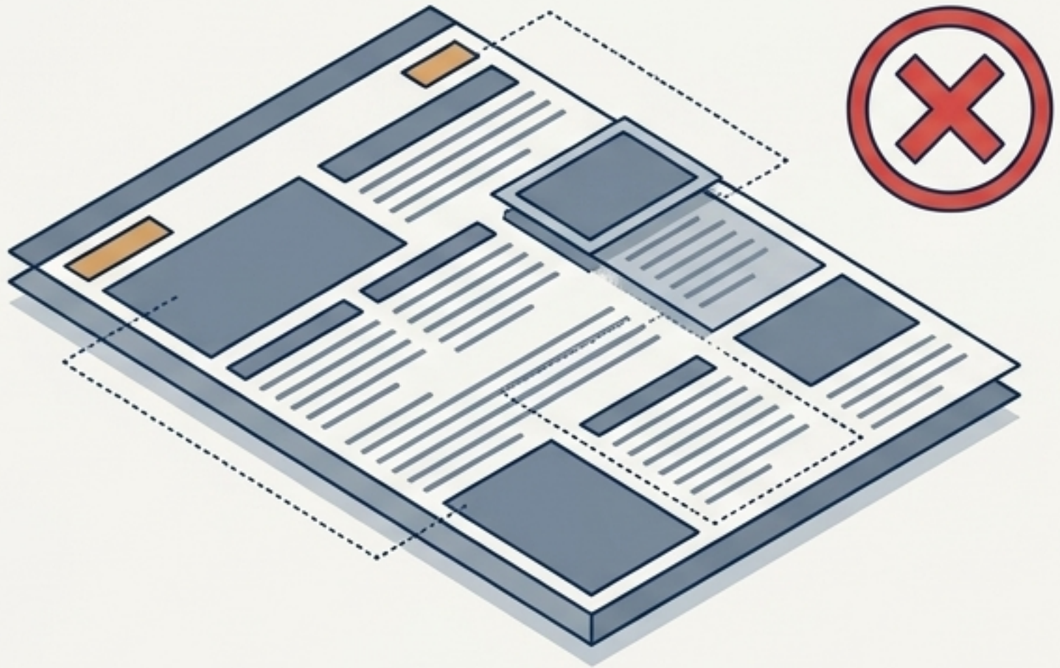
### Layer 1: Semantic

**Standards:** `Schema.org, GS1/GTIN, JSON-LD`
**Function:** Make the catalog machine-addressable.

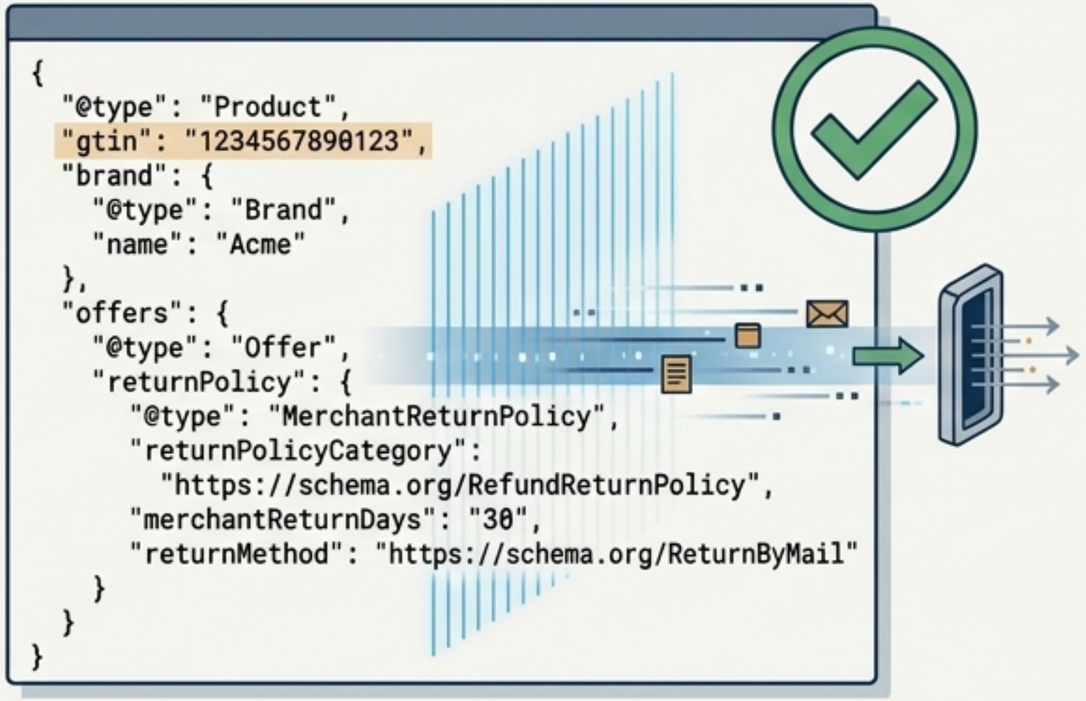
Gemini Notebook

# Layer 1: The Semantic Substrate

**Unstructured HTML** (Messy)



**Structured JSON-LD** (Clean)



```
{
  "@type": "Product",
  "gtin": "1234567890123",
  "brand": {
    "@type": "Brand",
    "name": "Acme"
  },
  "offers": {
    "@type": "Offer",
    "returnPolicy": {
      "@type": "MerchantReturnPolicy",
      "returnPolicyCategory":
        "https://schema.org/RefundReturnPolicy",
      "merchantReturnDays": "30",
      "returnMethod": "https://schema.org/ReturnByMail"
    }
  }
}
```

## UCP Readiness

1. Rate of product pages with GTIN, brand, canonical category.
2. Return policy and delivery time exposed in JSON-LD.
3. Consistency across Merchant feed, PIM, and HTML DOM.
4. Percentage of pages with enriched attributes (sizes, materials, compatibility).

If your Schema.org coverage is thin, the agent must infer the entity from the rendered DOM—the exact screen-scraping cost new protocols were designed to eliminate.

Gemini Notebook

# Layer 2: The Agent Surface (WebMCP)



## MCP (Anthropic)

Server-side, always reachable, durable backend.



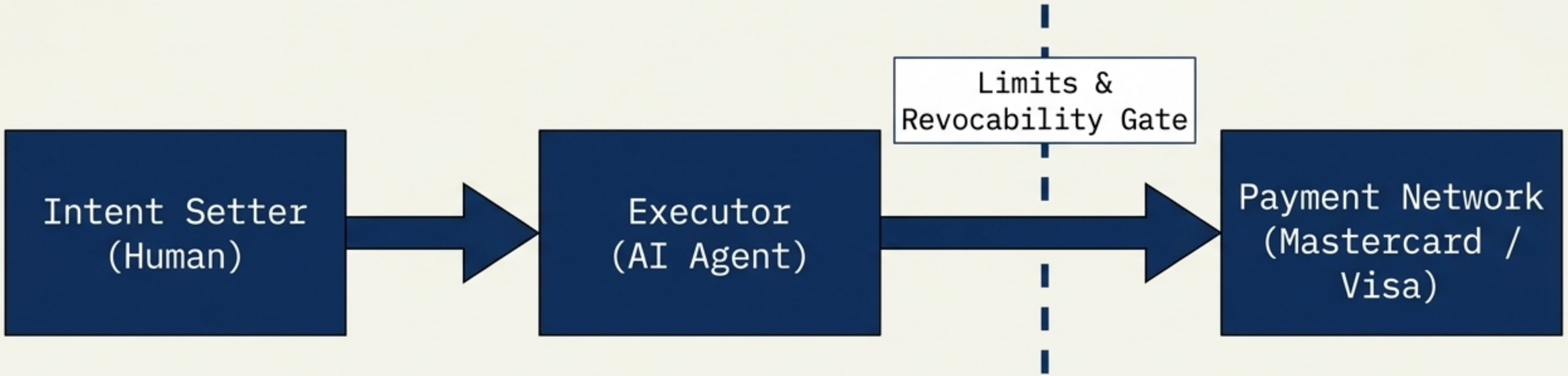
## WebMCP (W3C/Chrome)

In-tab, ephemeral, runs only while the tab is open with live user session.

**WebMCP** (previewed in `Chrome 146`) is a browser-native API. It lets a web page register its functions as structured, callable tools with `JSON-Schema-typed` parameters for AI agents to invoke directly without simulating clicks.

Gemini Notebook

# Layer 3: The Transaction Rail

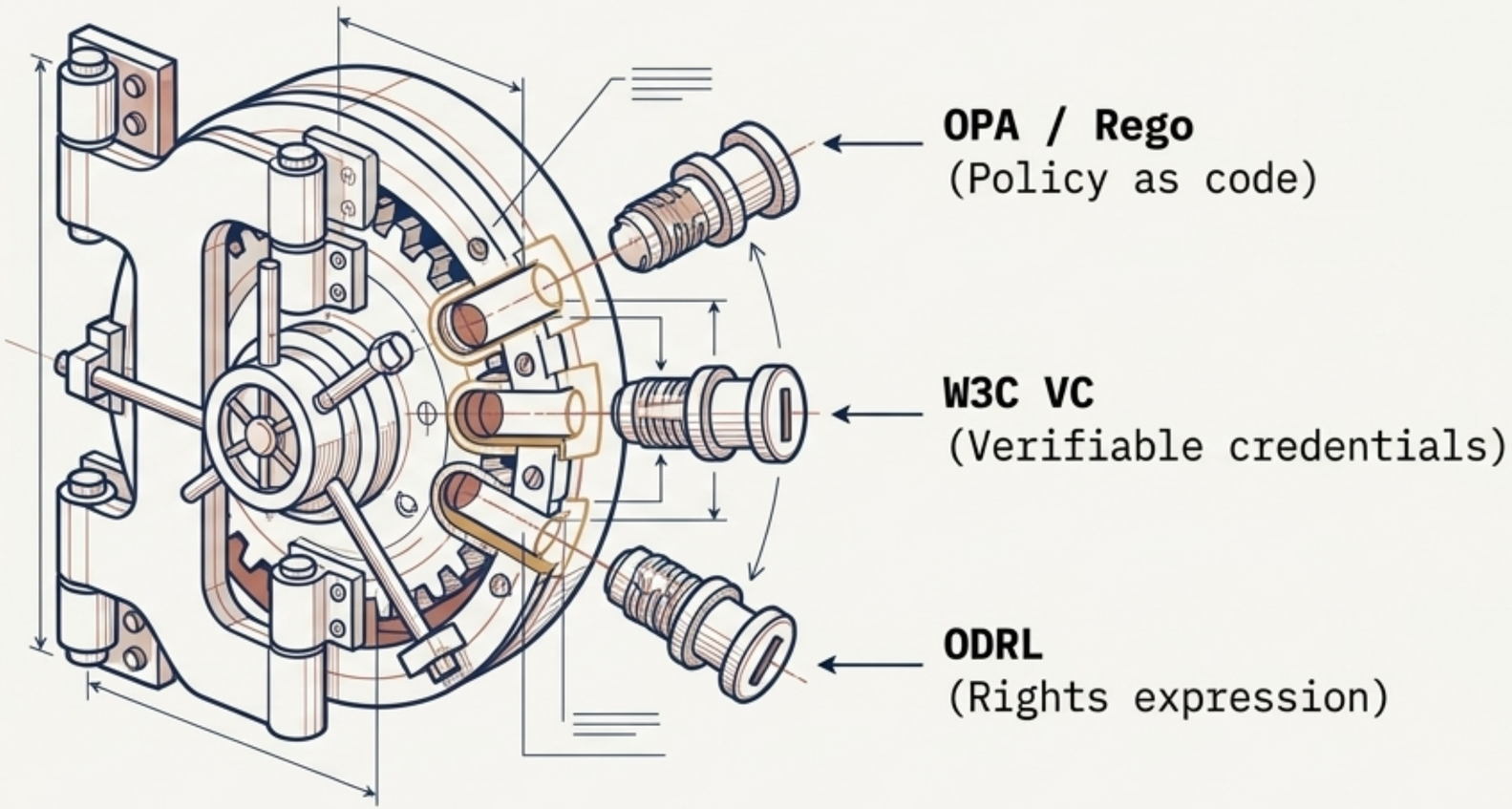



**Audit Checkpoints:**

1. Can a delegated payment execute within strict limits?
2. Is the agent identity traceable in standard accounting?
3. Are disputes accurately attributed to human vs. agent?
4. Does checkout remain deterministic under agentic constraints?

Gemini Notebook

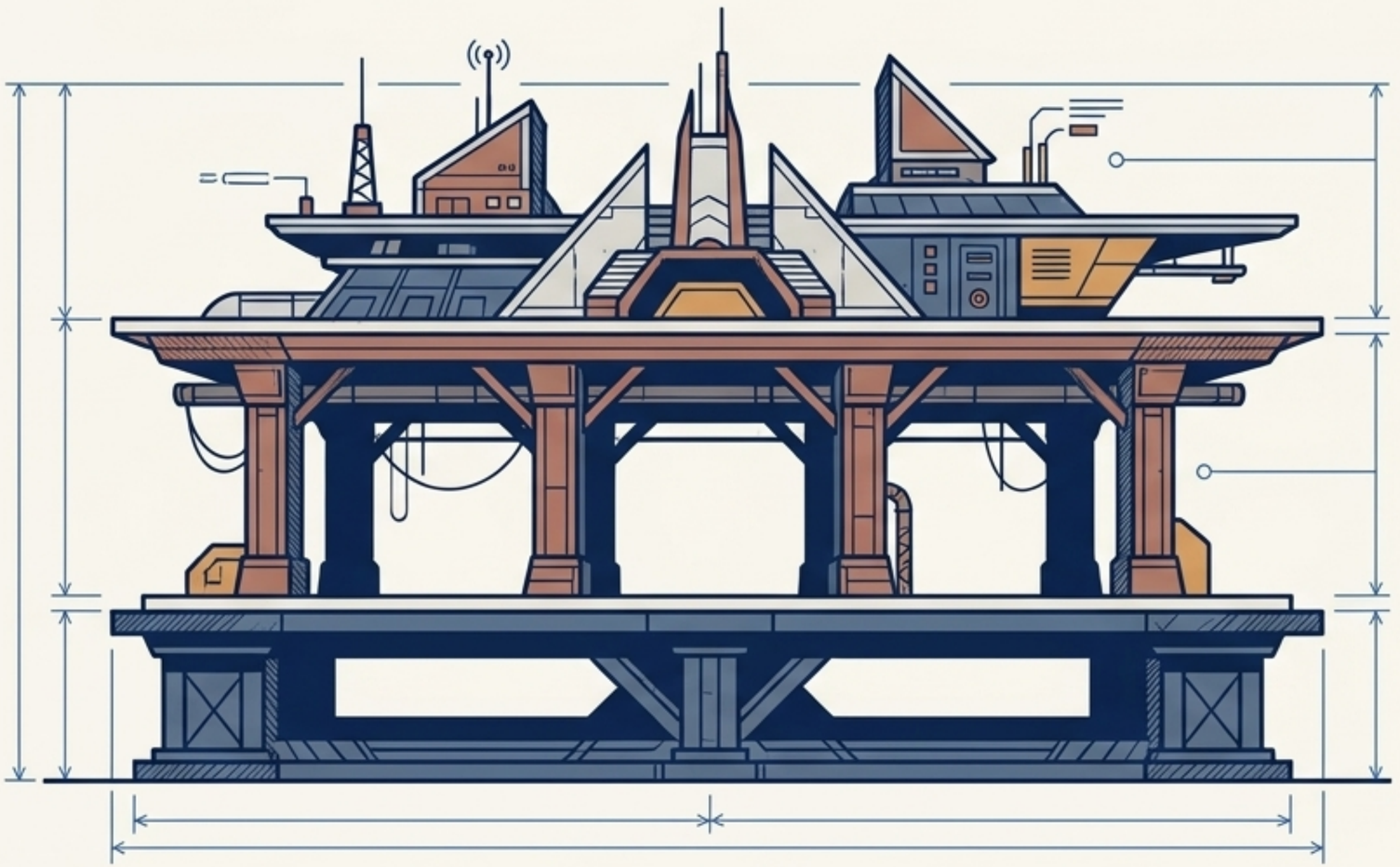
# Layer 4: Programmatic Governance




The governance layer ensures the merchant retains absolute control. It exposes pricing rules, territorial eligibility, and retention policies in machine-readable code, ensuring agents cannot bypass merchant logic or authorization scopes.

Gemini Notebook

# Decoding Universal Commerce Protocol (UCP)



### 3. Extensions

Domain-specific augmentations (e.g., `fulfillment`, `discount`, `subscription`).

### 2. Capabilities

Versioned functional areas (e.g., `dev.ucp.shopping.checkout`, `dev.ucp.shopping.catalog`).

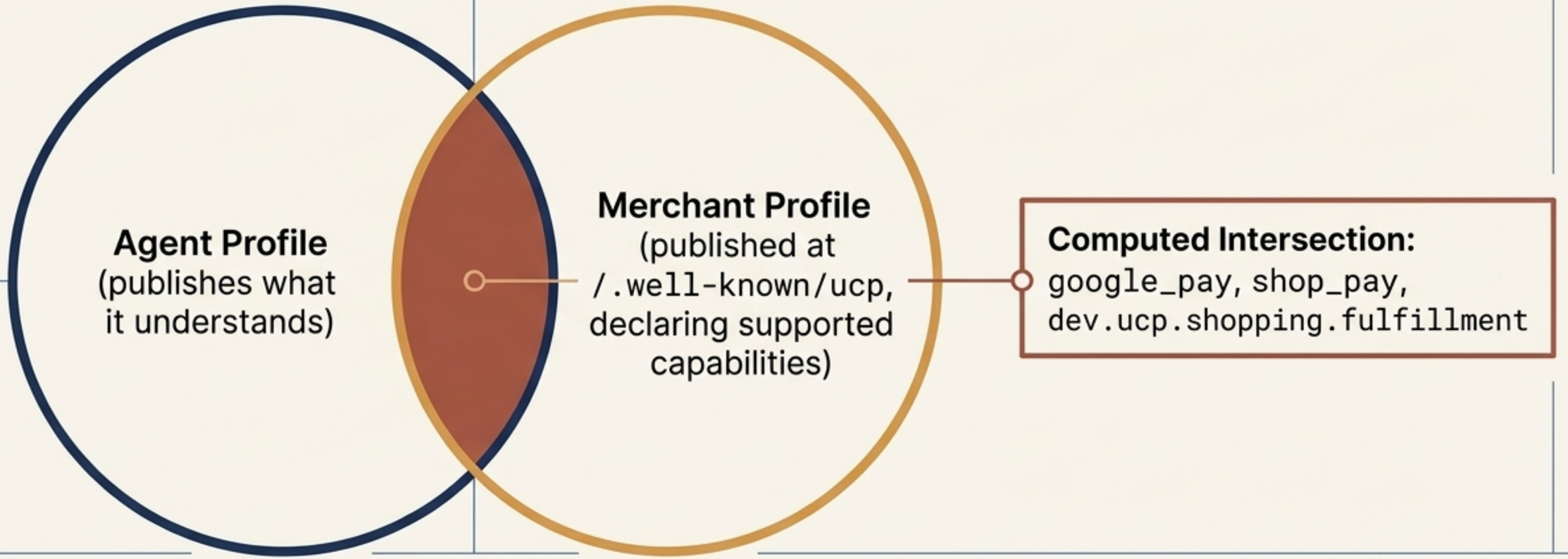
### 1. The Foundation (Shopping Service)

Core transaction primitives **(checkout session, line items, totals). Stable**, slow-changing.

**Co-developed by Google and Shopify (Jan 2026), UCP separates responsibilities. By using reverse-domain namespacing, merchants define custom extensions without waiting for committee approval.**

Gemini Notebook

# Capability Negotiation: Computing the Intersection




Rather than forcing a single rigid pathway, the agent and the merchant negotiate. They compare published JSON profiles and transact strictly within their mutually supported, overlapping capabilities.

Gemini Notebook

# The Handoff: Embedded Commerce Protocol (ECP)

**incomplete**

↓

Agent resolves via API.

**ready_for_complete**

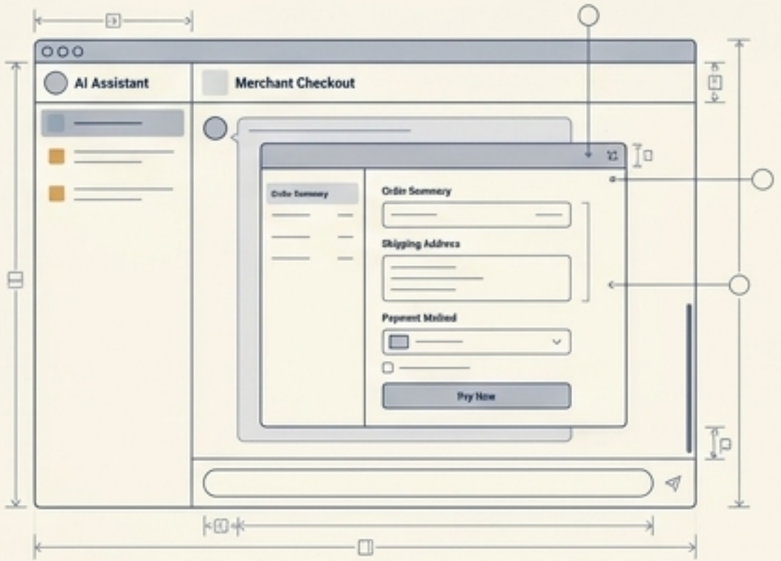
↓

Agent finalizes programmatically.

**requires_escalation**

↓

Agent loads continue_url -> Renders merchant's native checkout directly inside the AI chat interface via a JSON-RPC 2.0 channel.




Collaboration, not replacement. When an agent hits a capability gap or requires human input (like a complex B2B approval or specific delivery slot), it doesn't bounce the user to a new tab. It renders the merchant's real checkout inside the chat.

Gemini Notebook

# Bridging the Gap: The Proxy Adapter

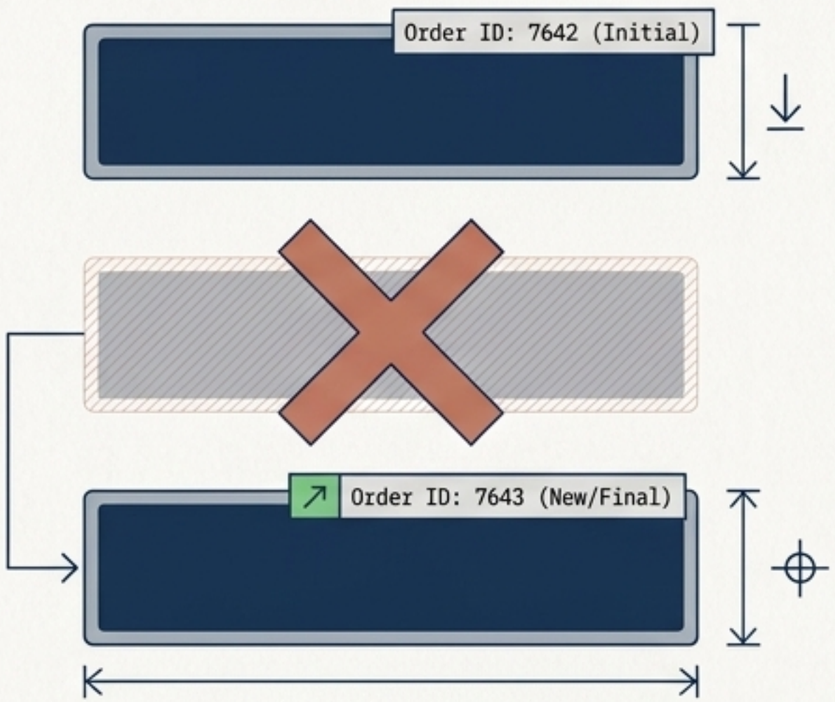



Legacy integration doesn't require a total rebuild. The Strabo model demonstrates how a Proxy Adapter acts as a translation layer, mapping declarative agent intents (**Langshaw protocols**) into standard **HTTP POST/PUT** requests for traditional merchants.

Gemini Notebook

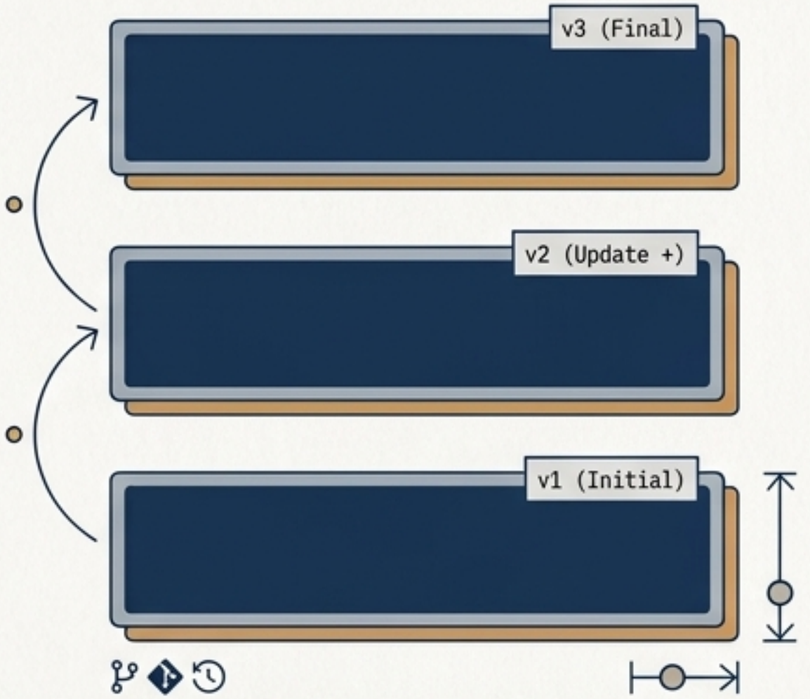
# Order Immutability: Atomic vs. Incremental

## Path A (Atomic)




**Cancel & Re-create loop:** Ensures absolute definitive state.

## Path B (Incremental)




**Versioned increments:** Supports multi-step update flows while preserving immutable history.

UCP avoids in-place overwrites. Agents update checkouts by appending new subenactments or recreating them entirely. This guarantees that human users and AI agents always share the exact same view of the transaction state.

Gemini Notebook

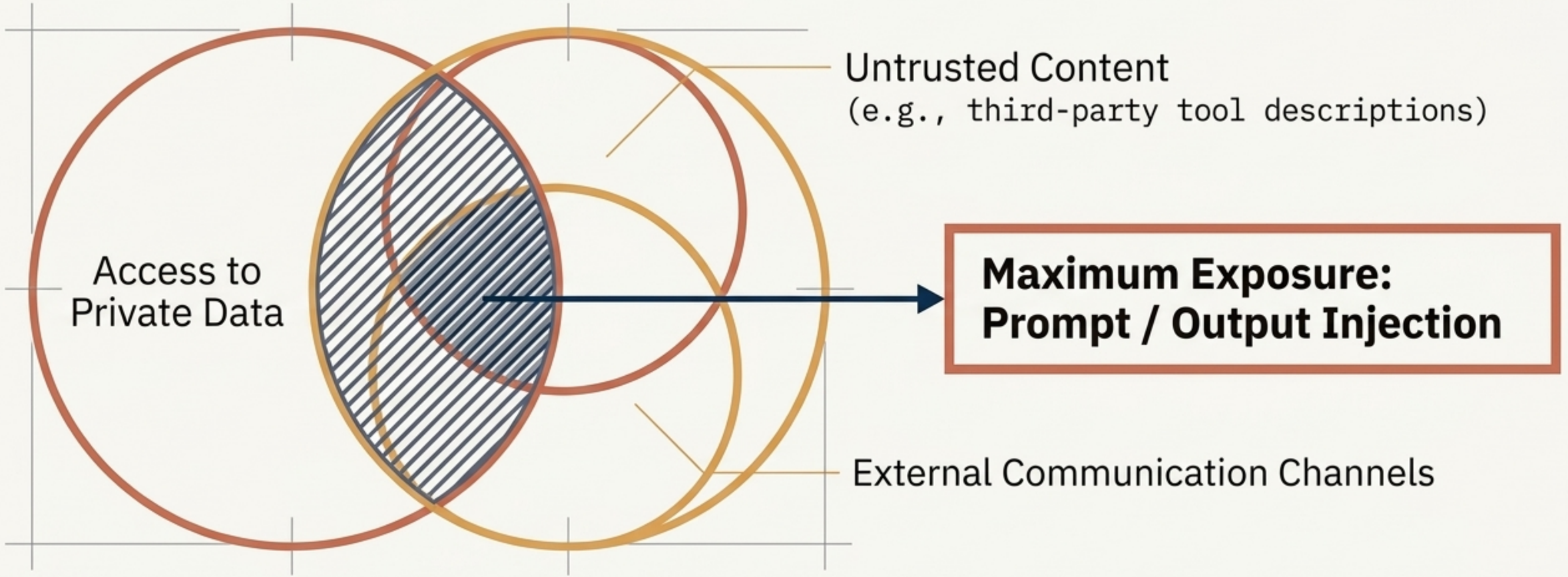
# The Protocol Landscape Matrix

| | UCP (Google/Shopify) | ACP (OpenAI/Stripe) | WebMCP (W3C/Chrome) |
|---|---|---|---|
| Scope | Full journey | Checkout only | In-tab interaction |
| Payment Flexibility | Any processor negotiated per transaction | Stripe-centric | N/A |
| Transports | REST / GraphQL / MCP | REST / MCP | Browser-native JS |
| Licensing | Apache 2.0 | Open Source | W3C Draft |

**Takeaway Bar:** Most serious merchants will ultimately support multiple protocols, decoupling discovery on one surface from transaction on another.

Gemini Notebook

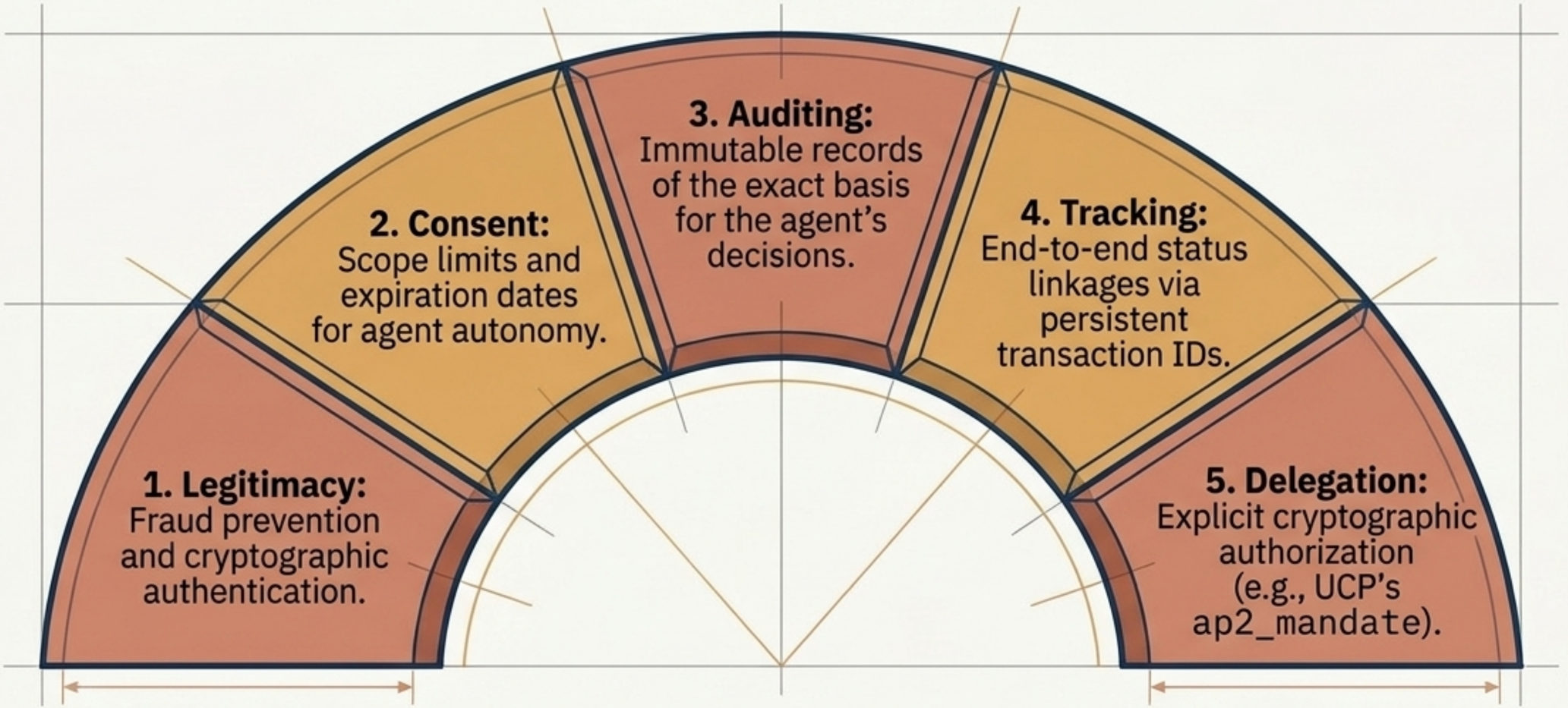
# The Lethal Trifecta of the Agentic Web




In an agentic web, malicious copy hidden in a **tool's description** can **hijack** an agent's next move. Prototyping should be restricted to read-only canonical tools (price lookups, FAQs) before authorizing state-modifying transactional flows.

Gemini Notebook

# The 5 Pillars of Digital Trust

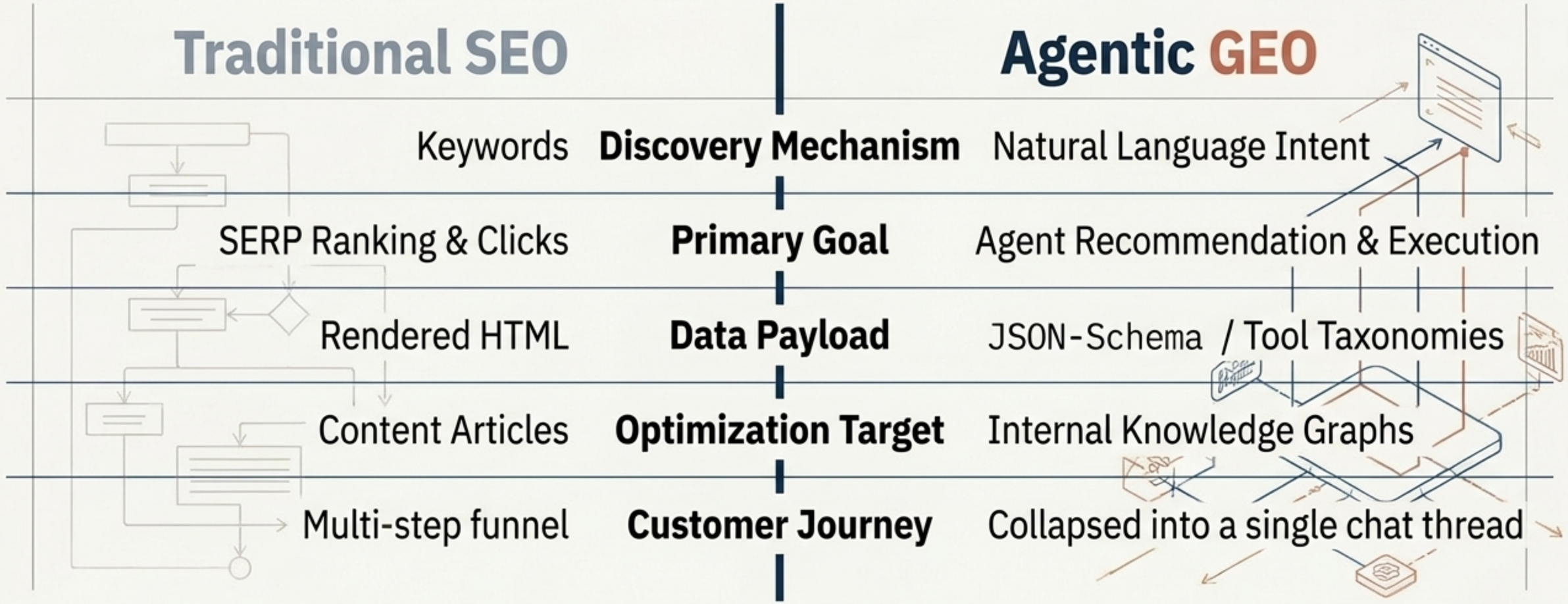



In the agentic era, transactions rely on infrastructure that verifiably records **WHO** authorized an agent, **HOW MUCH** authority it has, and **WHY** it made a decision.

Gemini Notebook

# Paradigm Shift: Traditional SEO vs. Agentic GEO

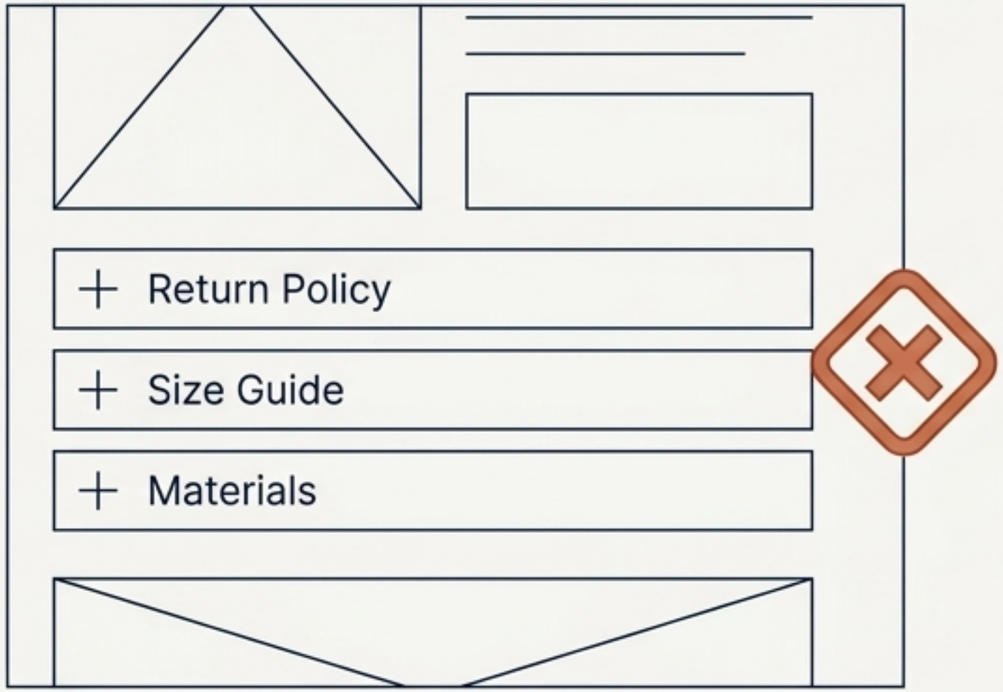
| Traditional SEO | | Agentic GEO |
| --- | --- | --- |
| Keywords | **Discovery Mechanism** | Natural Language Intent |
| SERP Ranking & Clicks | **Primary Goal** | Agent Recommendation & Execution |
| Rendered HTML | **Data Payload** | JSON-Schema / Tool Taxonomies |
| Content Articles | **Optimization Target** | Internal Knowledge Graphs |
| Multi-step funnel | **Customer Journey** | Collapsed into a single chat thread |



**Generative Engine Optimization (GEO)** rewards factual completeness. Where SEO rewarded keyword coverage, **agentic discovery** rewards **machine-readable semantic exactness**.

Gemini Notebook

# The Accordion Problem




Agents parsing the initial DOM often miss data hidden behind UI clicks.

Source Structured Data

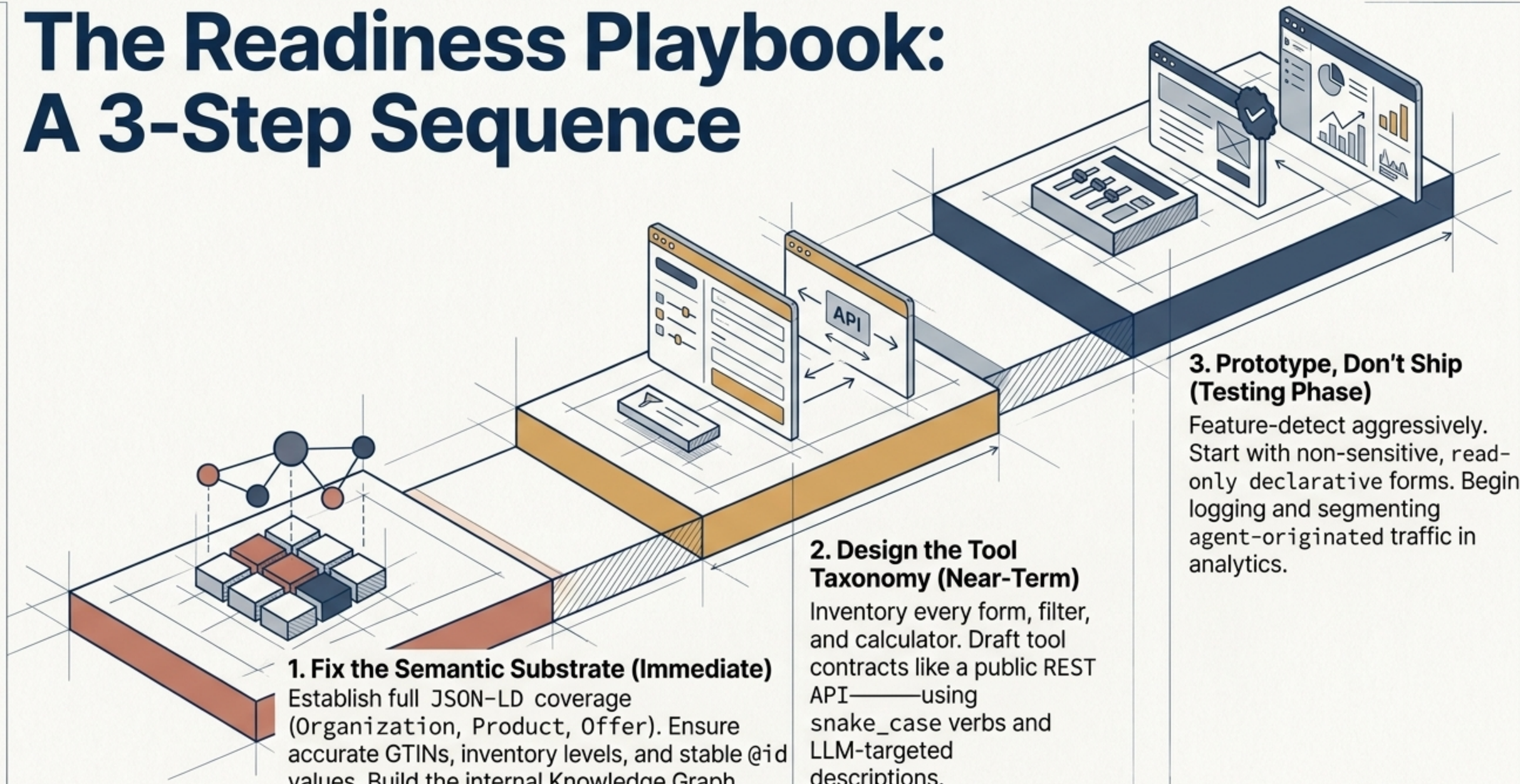
```
{
  "@context": "https://schema.org/",
  "@type": "Product",
  "name": "Example Product",
  "description": "...",
  "offers": { … },
  "additionalProperty": [
    {
      "@type": "PropertyValue",
      "name": "Return Policy",
      "value": "30-day free returns..."
    },
    { "@type": "PropertyValue",
      "name": "Size Guide",
      "value": "Fit runs true to size..."
    },
    { "@type": "PropertyValue",
      "name": "Materials",
      "value": "100% Organic Cotton..."
    }
```

Immediate machine readability ensures agents can confidently parse the data.

Anything load-bearing for a purchase decision must exist in the page source and in structured data, not only rendered behind a client-side JavaScript click. Agents are unforgiving about ambiguity.

Gemini Notebook

# The Readiness Playbook: A 3-Step Sequence



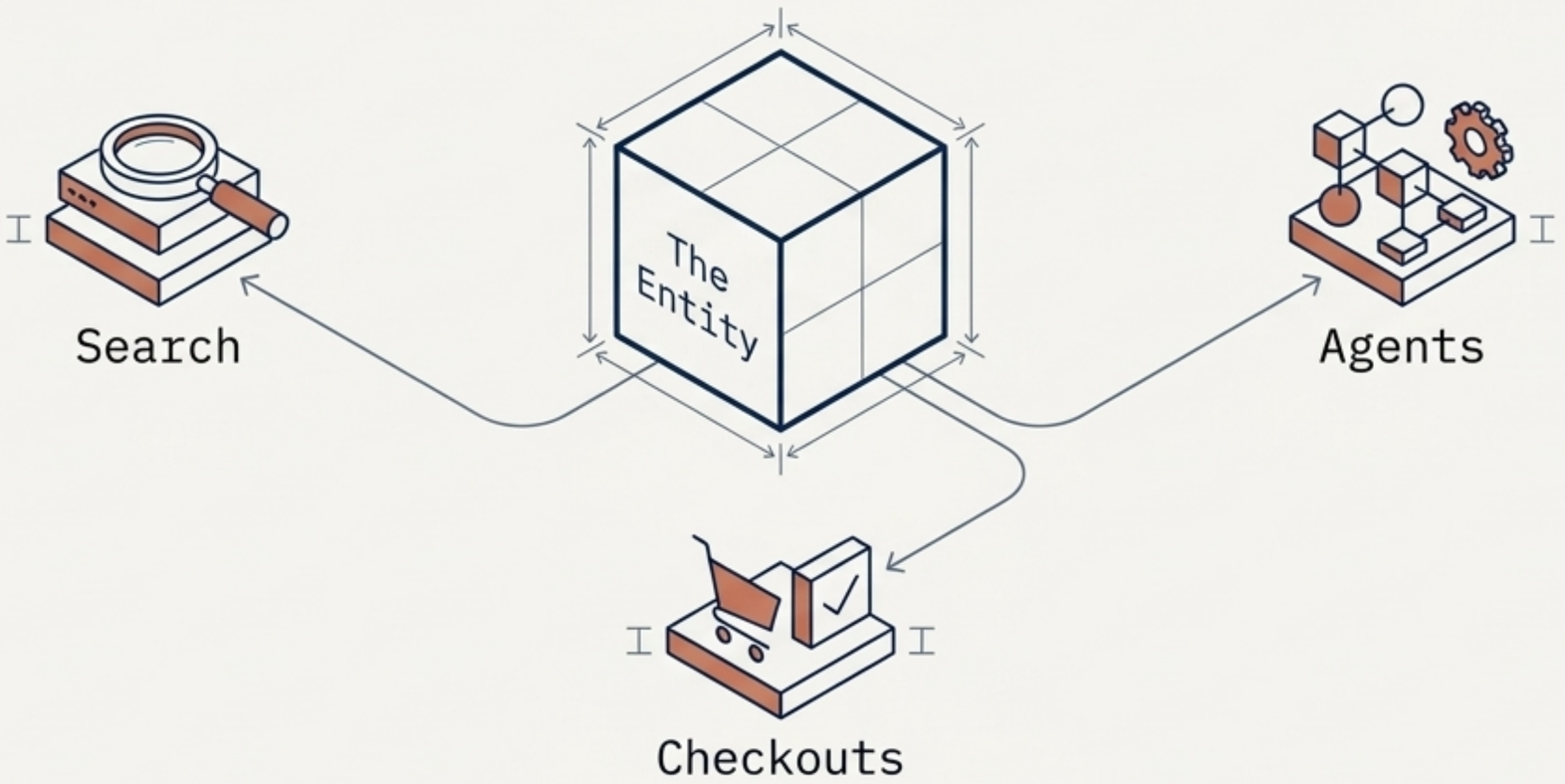

**1. Fix the Semantic Substrate (Immediate)**
Establish full `JSON-LD` coverage (`Organization`, `Product`, `Offer`). Ensure accurate GTINs, inventory levels, and stable `@id` values. Build the internal Knowledge Graph.

**2. Design the Tool Taxonomy (Near-Term)**
Inventory every form, filter, and calculator. Draft tool contracts like a public REST API———using `snake_case` verbs and LLM-targeted descriptions.

**3. Prototype, Don't Ship (Testing Phase)**
Feature-detect aggressively. Start with non-sensitive, `read-only` `declarative` forms. Begin logging and segmenting `agent-originated` traffic in analytics.

Gemini Notebook

# The Architecture of Authority




The teams that already think in entities and structured relationships will adapt naturally to the agentic web. The interface is shifting from screens to APIs, but the underlying currency of commerce remains the same: complete, accurate, and structured data.

**Prepare your nouns. The verbs are already here.**

Gemini Notebook