

The Agent Web, Measured

A first-hand audit of the machine-facing web: every remote server in the official MCP registry, every paid endpoint in Coinbase's x402 Bazaar, and the crawlers that visit a live agent-facing storefront.

15,329 MCP registry URLs probed	140,284 tool descriptions read	14,820 x402 Bazaar endpoints probed
\$314 per day: the whole CDP-settled x402 market (upper bound)	60 named agent crawlers observed	0 of them that ever paid

Single-organisation licence. Every figure is recomputable from the data files listed in Appendix D. Corrections: support@fetchgate.dev · fetchgate.dev/research

Contents

1. Executive summary
2. How this was measured
3. Part I — The MCP registry
 1. Size, reachability and the two-operator problem
 2. Protocol versions and capabilities
 3. What 140,284 tools look like
 4. The `instructions` field
 5. Annotations: used, and self-reported
 6. Security: what is not there, and what is
 7. x402-gated MCP servers
4. Part II — The x402 Bazaar
 1. Demand: 289,401 calls, one median sale
 2. Revenue: the ceiling is \$314 a day
 3. Supply concentration and template farms
 4. Prices, networks, schemes
 5. Liveness and the signing-domain defect
 6. Facilitators
5. Part III — The agent crawler census
6. Synthesis: twelve conclusions
7. What we will re-measure, and when
8. Appendices: A. Concealment directives, verbatim (51) · B. Facilitator table · C. Method and limits · D. Data files

1. Executive summary

Three registries describe the "agent web" in 2026: the official Model Context Protocol registry, Coinbase's x402 Bazaar of machine-payable APIs, and the population of bots that crawl anything listed in either. All three are self-reported catalogues. This report is what you get when you stop reading the catalogue and ask every entry directly.

The MCP registry is about half as large as its headline, and a third of what works is two operators

Of 15,329 remote URLs listed across every version of every server, **8,235 (53.7%) returned a tool list** to an unauthenticated client. 3,617 (23.6%) demanded authentication first, and 3,477 (22.7%) were dead, broken, or not MCP endpoints at all — 609 hostnames no longer resolve. Two operators, `pipeworx.io` and `mcp.ai`, account for 2,357 of the live servers (28.6%) and 39.2% of all tools. Excluding them, the registry answers at **45.5%**, not 53.7%.

The textbook tool-poisoning attack has a base rate of zero; a quieter pattern is common

Across 140,284 live tool descriptions and 5,462 server-level `instructions` strings, the canonical "read `~/.ssh/id_rsa` and pass it as a parameter" payload appears **zero times**. What does appear: **47 hosts** whose descriptions tell the model what *not* to tell the user, 480 hosts (9.1% of live hosts) using model-directed language, and 406 hosts shipping a tool that claims precedence over every other tool in the session. The 51 concealment directives are reproduced verbatim in Appendix A.

The `instructions` field is an unreviewed system-prompt channel

66% of live servers return one; 114 are longer than 5,000 characters and 16 longer than 20,000. The longest is 68,669 characters — roughly 17,000 tokens injected into every conversation before a tool is called.

The x402 market is real, tiny, and concentrated

Coinbase's Bazaar lists 14,820 paid endpoints. Its own 30-day counters sum to **289,401 settled calls**; priced at each resource's minimum listed rate that is at most **\$9,416 for the month, \$314 a day**, for the entire CDP-facilitated market. The median resource sold once. 34 resources took 59.5% of all calls; the single busiest one is a Chainlink workflow with 36,335 calls from exactly one payer. 898 USDC-on-Base listings (1 in 16) declare an EIP-712 domain a stock client cannot sign for.

Discovery is solved. Demand is not.

A live, thirty-directory-listed x402 + MCP storefront received 60 named crawlers and 2,315 named-agent requests in 24 hours. 19 of the crawlers declare in their own User-Agent string that they never pay. None of the 60 has ever paid.

If you keep one number from each part: the registry answers at 45.5% once two fleets are removed; the whole x402 market clears under \$314 a day through its dominant facilitator; and 91% of named agent traffic to a paid endpoint is uptime monitors and index crawlers.

2. How this was measured

Three independent measurements, each first-hand, each reproducible from the files in Appendix D.

Measurement	Population	Window (UTC)	Probe
MCP registry audit	All 837 pages of <code>registry.modelcontextprotocol.io/v0/servers</code> : 83,603 version entries, 25,289 unique names, 15,329 unique remote URLs	Fetch 2026-08-27 22:31–23:02; probe 2026-08-27 23:03–00:18	One read-only MCP session per URL: <code>initialize</code> (2025-06-18) → <code>notifications/initialized</code> → <code>tools/list</code> . <code>tools/call</code> never sent . 10 s timeout, one transport-level retry, bodies capped at 4 MB, identifying User-Agent.
x402 Bazaar audit	All 149 pages of <code>api.cdp.coinbase.com/platform/v2/x402/discovery/resources</code> : 14,820 resources, 1,608 hosts, 789 domains	Fetch 2026-08-28 21:35; probe 2026-08-28 21:50	One <code>GET</code> per unique URL with no payment header, 10 s timeout. A 402 with a parseable x402 body (v1) or <code>PAYMENT-REQUIRED</code> header (v2) counts as live. Every USDC-on-Base option's EIP-712 domain checked. All 21 known facilitators asked <code>GET /supported</code> .
Agent crawler census	Every request to <code>fetchgate.dev</code> , a live x402 + MCP storefront listed in ~30 directories: 6,309 requests, 60 named agents	24 h ending 2026-08-27 20:30	Cloudflare zone analytics for traffic; the endpoint's own payment log (every verify/settle attempt at one choke point) for payments. Categories assigned from observed request paths, cross-checked against each agent's self-description.

Flags in Part I are pattern matches with documented false-positive profiles (Appendix C); the concealment directives in Appendix A were each read by a person. Nothing in this report required an account, a payment, or an authenticated request to any third party.

This is the free sample

You have read the cover, the contents, the executive summary and the method — the first 4 of 25 pages. The full edition continues with everything the summary only names.

- **Part I — the MCP registry** (7 sections, 13 figures): the reachability funnel and every failure mode, the two-operator split, protocol versions and capabilities, what 140,284 tools look like, the `instructions` field, annotations, the security findings table, and the x402-gated servers.
- **Part II — the x402 Bazaar** (6 sections, 8 figures): demand distribution, the ten busiest and ten highest-revenue resources named, supply concentration and the template farms, prices and networks, liveness, the EIP-712 signing-domain defect, and all 21 facilitators probed.
- **Part III — the crawler census**, with every self-declared non-payer quoted.
- **Twelve conclusions** and the re-measurement schedule.
- **Appendix A: all 51 concealment directives, verbatim**, with host, tool and field — the table nobody else has, because nobody else read 140,284 descriptions.
- **Appendices B–D**: the facilitator table, method limits, and every data file with its URL.

Get the full report: growthchief5.gumroad.com/l/agent-web-report — \$149, single-organisation licence, re-probe summaries and the 2026 Q4 edition included. Or pay in USDC over x402: `GET fetchgate.dev/v1/buy/agent-web-report-2026-q3`.

Every number in the sample is generated from the same files as the full edition and is checkable against the free CC BY 4.0 data at fetchgate.dev.