

OPEN SOURCE COMMUNITY & ECOSYSTEM HEALTH

Open Source Has Been Here Before

Sustainability Lessons for Agentic AI

Katherine Druckman · Head of Community and Partnership Engagement, JetBrains

AGNTCon + MCPCon North America · 23 October 2026

2014

Two thousand dollars a year

\$2,000

a year of donations at OpenSSL, weeks after Heartbleed.

“There should be at least a half dozen full time OpenSSL team members, not just one.”

Steve Marquess, OpenSSL Software Foundation, 2014

Twelve years ago. Since, we diagnosed it, funded it, and built an institution for it.

And are we sustainable yet?

veridicalsystems.com, “Of Money, Responsibility, and Pride,” April 2014. OpenSSL also sold support contracts; the two thousand dollars is outright donations. OpenSSL Foundation FY2025 report: expenses exceeded revenue, and the gap was covered from reserves.

Nobody promised us forever.

“The idea that CNCF is a bulwark that’s just always going to be there, I think is actually a dangerous assumption.”

Luis Villa, co-founder of Tidelift, on my podcast in 2024

At any level. From a single maintainer all the way up to a giant foundation.

**“Human in the loop”
is not a safety feature.**

It’s a person.

And that person needs support and resources.

(That’s it. That’s the whole talk.)

2024

I gave a semi-related talk two years ago

Secure Consumption of Open Source Software. Grace Hopper, SOSS Day, and a few other stages in between.

Evaluating open source projects

1. Review basic health—Is it active?
2. Check governance—Is it defined?
3. Review maintenance & releases—Is there a cadence?
4. Explore the community—Are people engaged?
5. Bug reporting—Is there a documented process?

I still think that is the right checklist.

As long as someone owns the result.

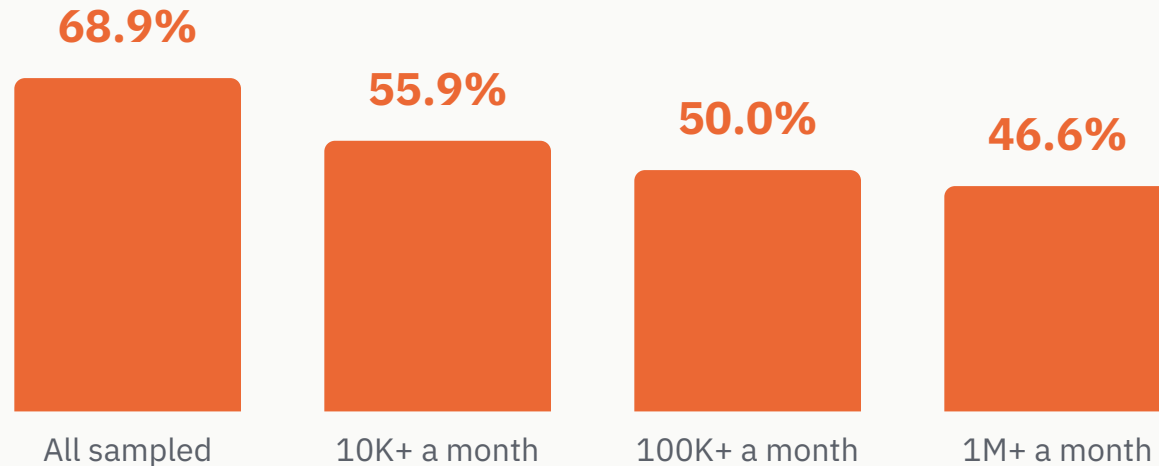
That assumption may be broken?

THE UPDATE

Did it take?

npm search API, sample collected October 18, 2026.

WHAT I MEASURED LAST MONTH



Share with exactly one listed maintainer account

WHAT I SHOWED IN 2024

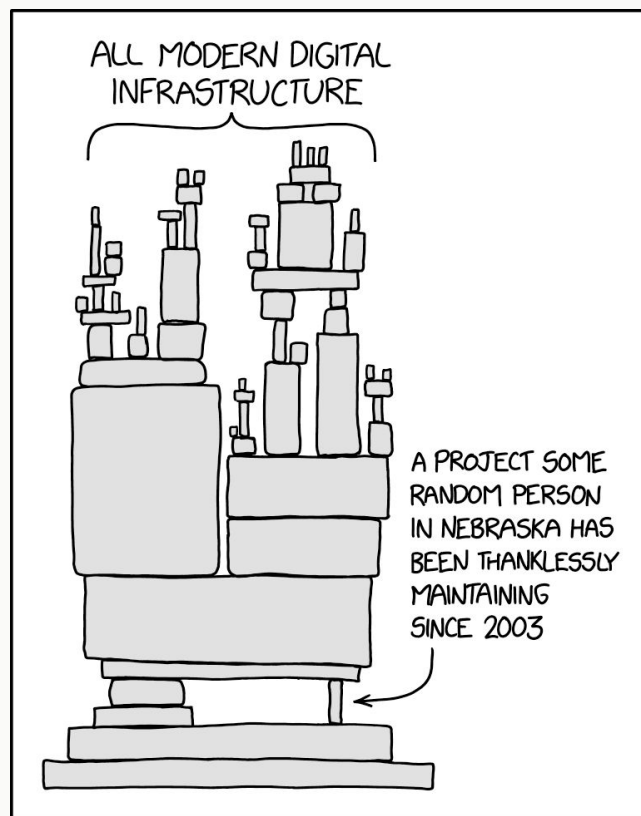


Josh Bressers' data, 2023. He counted releases, not packages.

Popularity does not buy you a second maintainer.

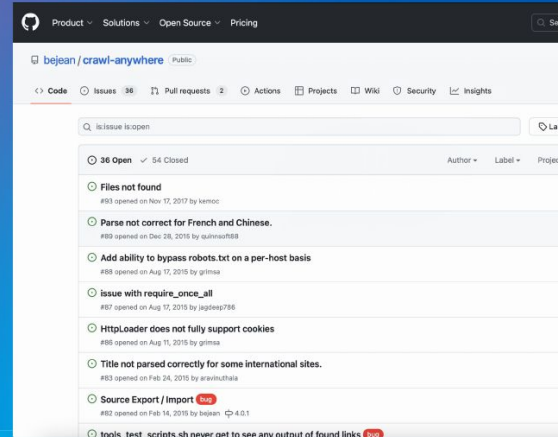
A listed account is a publishing credential, not a count of humans.

You know the cartoon.



1. Evaluating software: Basic health

- Does the project even have a maintainer anymore?
- When was the last commit?
- Look at the issue queue
 - How active is it?
 - When was the last post?
 - When was the last response to an issue?



“Is there a second person who can ship a fix?”

-Alyssa Wright

Mine asks whether anybody is there. Hers asks whether anybody else is.

github.com/aboutcode-org/healthycode

Daniel Stenberg, who maintains curl

Jul 2025	About 20% of submissions were AI slop. The valid rate had “decreased significantly.”
Jan 2026	Ends the bug bounty, to remove the incentive for submitting made-up lies.
Apr 2026	“The slop situation is not a problem anymore.” Confirmed rate back to 15–16%. Volume at a record.
May 2026	Four to five times the 2024 volume, mostly high quality. Says he might have to cut his hours.
Oct 2026	A year of AI-assisted collaboration produces 35 CVEs, more than any group has found in curl before.

The slop stopped and the pressure went up.

Better reports still overwhelmed the team's capacity.

AT SCALE

Not just curl

Anthropic's own vulnerability disclosure pipeline, as of 2 October 2026

6,157

disclosed to maintainers

5,103

acknowledged by a maintainer

516 patched upstream so far

“...since the process of independent human triage and review is the rate limiting step.”

Anthropic, on its own dashboard, describing the triage step inside its own pipeline. Finding more does not reduce the need for someone to review it.

red.anthropic.com/2026/cvd, as of 2 October 2026, covering findings discovered 1 November 2025 onward. Anthropic notes patches are a lagging indicator because patches take a long time to create, so the bottom bar understates eventual fixes. 92.7% of 6,123 firm-reviewed findings were confirmed real; 4,824 disclosures went direct without independent triage and may contain false positives.

Code was never
the contribution.

Philippe Ensarguet of Orange at Open Source Summit in Prague.

Making a patch got cheap. Reviewing it didn't.

CHEAP NOW

Producing a patch

Writing code, running tests, opening a pull request.



STILL EXPENSIVE

Accepting a change

Understanding it, deciding whether it belongs, maintaining it.

DEPENDENCIES YOU TAKE ON

Your agent can choose what your software uses

WHEN WRITING CODE

Which package to add

WHEN CARRYING OUT A TASK

Which available tool to call, and what arguments to pass

Your agent doesn't answer for it at three in the morning. You do.

We learned to ask what's in our software.

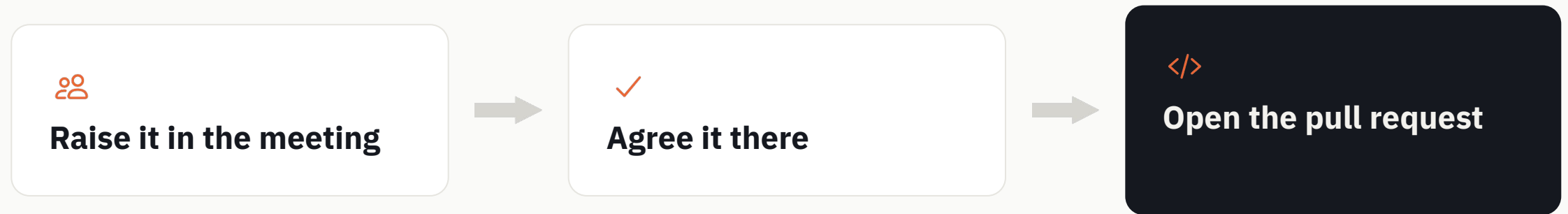
Can we explain how an agent chose it?

What did it choose? Who approved it?

WHAT WE DID ABOUT IT

We faced it too

The drive-bys found us as soon as our repositories went public. Some of our most dedicated contributors wrote the policy, fast.



Agree on the contribution before reviewing the pull request.

CONTRIBUTING.md in the AAIF taxonomy workstream, rewritten 29 September 2026.

We already have reasons to support the people, not just the code

2014

Heartbleed

A critical vulnerability exposed OpenSSL's funding and staffing needs.

2018

event-stream

A maintainer hands the keys to a stranger who asked nicely.

2021

Log4Shell

A small volunteer team, over a holiday week.

2024

xz-utils

Two years of patient social engineering against one exhausted person.

We are not early to the risk. We can apply those lessons to agents now.

“You ingest it, you own it.”

I was saying that in 2024. Even when an agent picks it, you still own it.

A licence is not a support agreement.

Installing a package does not, by itself, buy you a support commitment. If your business needs a four-hour response, that is yours to arrange: pay for support, staff it yourself, or choose a dependency whose support meets your needs.

Nobody is behind

- A maintainer ends his bug bounty, then welcomes an AI-assisted collaboration that finds more CVEs in his project than anyone before.
- 281 projects have written an AI contribution policy. About half ask you to disclose. The rest don't. No common convention has emerged.
- A group of volunteers writes one in a week rather than wait for a policy from above.

Every one of those is a competent team making its tradeoffs in public, under conditions nobody designed for.

We are all in the first draft.

Policy figures: arXiv 2609.07542, a preprint posted 7 September 2026, surveying 281 open source AI contribution policies; 83.3% permit or encourage AI for code and 48.8% require disclosure.

What I'd ask of the community

1

Fund review and mentoring.

Budget for the people needed for sustainability.

2

Give critical dependencies an owner.

Someone on your team who knows the support arrangements and fallback plan.

3

Help finish the work.

Use AI to ease the burden on both sides, and not just generation.

4

Keep contribution policies clear

Protect reviewers while allowing people to participate effectively.

“Human in the loop” is not a safety feature. It’s a person.

Pick one thing your agent depends on. Find out who keeps it running, and what happens to you if they stop.

“We are up for a bumpy ride.”

Daniel Stenberg, closing a post called High-Quality Chaos, April 2026

Thank you

Katherine Druckman

Community strategy, JetBrains

Questions, arguments and corrections all welcome.



[linkedin.com/in/katherinedruckman](https://www.linkedin.com/in/katherinedruckman)

Sources

Everything here is a public document, a talk I sat in, or a measurement you can re-run

What	Where
curl, July 2025 – October 2026	daniel.haxx.se
OpenSSL funding at Heartbleed	veridicalsystems.com · OpenSSL Foundation FY2025 report
My 2024 talk, Secure Consumption of Open Source Software	Grace Hopper · OpenSSF SOSS Day NA
The npm measurement, script and raw sample	One endpoint, no API key, about five minutes. Ask me.
Josh Bressers, Open Source is one person	opensourcesecurity.io, 28 Aug 2025 · ecosyste.ms
Ruth Suehle, Alyssa Wright, Philippe Ensarguet	Open Source Summit, October 2026
Anthropic vulnerability disclosure dashboard	red.anthropic.com/2026/cvd, read 2 Oct 2026
AAIF working group contribution policy	CONTRIBUTING.md, aaif taxonomy workstream, 29 Sep 2026
MCP python-sdk · goose contribution gates	github.com/modelcontextprotocol · github.com/block/goose