Aligning wishes of multiple orgs into an open source project

FOSS Backstage 2024

Nick Vidal
Thomas Steenbergen
Nick Vidal 👋

Community Manager at the Open Source Initiative

Projects: ClearlyDefined, Open Source AI, etc
ClearlyDefined’s mission is to crowdsource a **global database of licensing metadata** for every software component ever published for the benefit of all.

- Organizations are able to fetch a cached copy of licensing metadata for each component through a simple API.
- Organizations are able to contribute back with any missing or wrongly identified licensing metadata, helping to create a database that is as accurate as possible.
Thomas Steenbergen 👋

I help orgs manage open source in a strategic, safe and efficient manner that meets their business needs.

Former Head of OSPO at EPAM/HERE. Currently #OpenToWork

Maintainer / Contributor to:

- OSS Review Toolkit
- TODO
- SPDX
- OPENCHAIN

See also github.com/tsteenbe
OSS Review Toolkit Project

The OSS Review Toolkit (ORT) is a **FOSS policy automation and orchestration toolkit** which you can use to manage your (open source) software dependencies in a strategic, safe and efficient manner.

You can use it to:

- **Generate CycloneDX, SPDX SBOMs**, or custom FOSS attribution docs.
- **Automate your FOSS policy** using risk-based Policy as Code to do licensing, security vulnerability, InnerSource and engineering standards checks.
- **Create a source code archive** for your software project and its dependencies to comply with certain licenses or for business continuity.
- **Correct package metadata or license findings**, using InnerSource or with the help of the FOSS community.
Let's talk about roadmaps in a open source project...
A public and up-to-date roadmap for an open source project can:

- Encourage new contributors to join a project
- Guide the efforts of existing contributors
- Give confidence to adopters about the direction and sustainability of the project

“They Can Only Ever Guide:”
How an Open Source Software Community Uses Roadmaps to Coordinate Effort
https://dl.acm.org/doi/pdf/10.1145/3449232
Yet ORT, like many open source projects with a diverse community, struggles to maintain a roadmap due to:

- **Unclear market need**
  - Local value of current and future project’s capabilities is often unknown.
  - Limited to no insights into local decision makers or available resources across community.

- **Getting commitment to deliver is hard**
  - No top-down control.
  - Contributors / maintainers capacity is limited due to other obligations.
Tragedy of the Commons

- Overuse of common resource
- “Free rider” problem
- Someone else will tackle an issue / problem

- What incentives can we create so that we get a commitment from individuals and companies to tackle a problem?

https://en.wikipedia.org/wiki/Tragedy_of_the_commons
Commitment models

- Time / Money
- Donation / Sponsorship
- Bounties / Grants
- Crowdfunding
- Books / Merchandise
- Advertising
- Consulting / Paid support
- Venture capital
- SaaS / Open core
- Dual license
- Foundations / Consortiums

“Working in Public” Nadia Eghbal https://nadia.xyz/
Governance models

- Corporate-backed
  - Single vendor
- Foundation-backed
  - Linux Foundation
  - Apache Software Foundation
  - Eclipse Foundation
  - Python Software Foundation
Why upstream contributions?

- Reduce risks / Better security
- Maintainability / Compliance
- Shape roadmap / features
- Collaborate with other orgs
- Reduce costs / resources

xkcd.com/2347 (CC-BY-NC-2.5)
How can contributors commit to a feature in a FOSS project?
#1: Informal agreements

Members of orgs agree to:
- collaborate to build a feature informally
- member usually commits their own time or people they control
#2: Steering Committee

Orgs pays to become **member of project steering committee** who then decides on open source **project feature enhancements**.
Can we just contribute to this large feature?
What happens if one of the orgs pulls out?
What if each party commits different things?

💵 or/and 🖥️
What about us (unpaid) maintainers?
How can multiple orgs commit to build together a feature in a FOSS project?
Commitments between parties are typically handled via contracts.
 Aren't open source licenses also contracts?

 ⏳️ it depends..
What if we made a contract for open source commitments?

contributor commitment agreement
Contributor Commitment Agreement

● Preconditions
  ○ Project has defined enhancement proposal for larger contributions with multiple parties
  ○ Maintainers are capable to commit to working on larger contributions
● Enhancement proposal agreed upon by signees (that includes project maintainers) => Link to GitHub issue or similar
● Break up obligations (think money for project)
● If one party prefers to stay anonymous the agreement can enforce this.
Balancing supply and demand is commonly done via marketplaces.
Marketplace CMS & CCA

- Collaboration Marketplace Specification (CMS)
- Contributor Commitment Agreement (CCA)

- Addresses the mismatch between open source communities and enterprise users via a marketplace and re-usable contract.
Collaboration Marketplace Specification

- Specification defining format for enhancements wishlist (list of issues), resources (💪 or 💰) and point of contact. Wishlists can be public or private (anonymous via deployment keys).
- Integrated with regular GitHub / GitLab issue workflow and permissions (low operating costs, GitHub actions?)
Wanna learn more about ClearlyDefined & ORT?

Join us tomorrow at the ORT Community Days
March 6 & 7
Berlin, Germany