

Best Practices for Starting an Open Source Program/Project

Lessons learned from Kubernetes/CNCF + TODO Group + LF

Chris Aniszczyk ([@cra](#))

May 13, 2020

Hi, I'm Chris Aniszczyk (@cra)

- › CTO/COO, Cloud Native Computing Foundation (CNCF)
- › Executive Director, Open Container Initiative (OCI)
- › VP, Developer Relations, Linux Foundation (LF)



› In a previous life...

- › Head of Open Source (@Twitter) / Sr. Eng Manager
- › Co-Founder of the TODO Group
- › Co-Founder of EclipseSource (via Code9)
- › Open Source Committer (Gentoo, Fedora, etc)
- › Principal Software Engineer, Red Hat
- › Senior Software Engineer, IBM

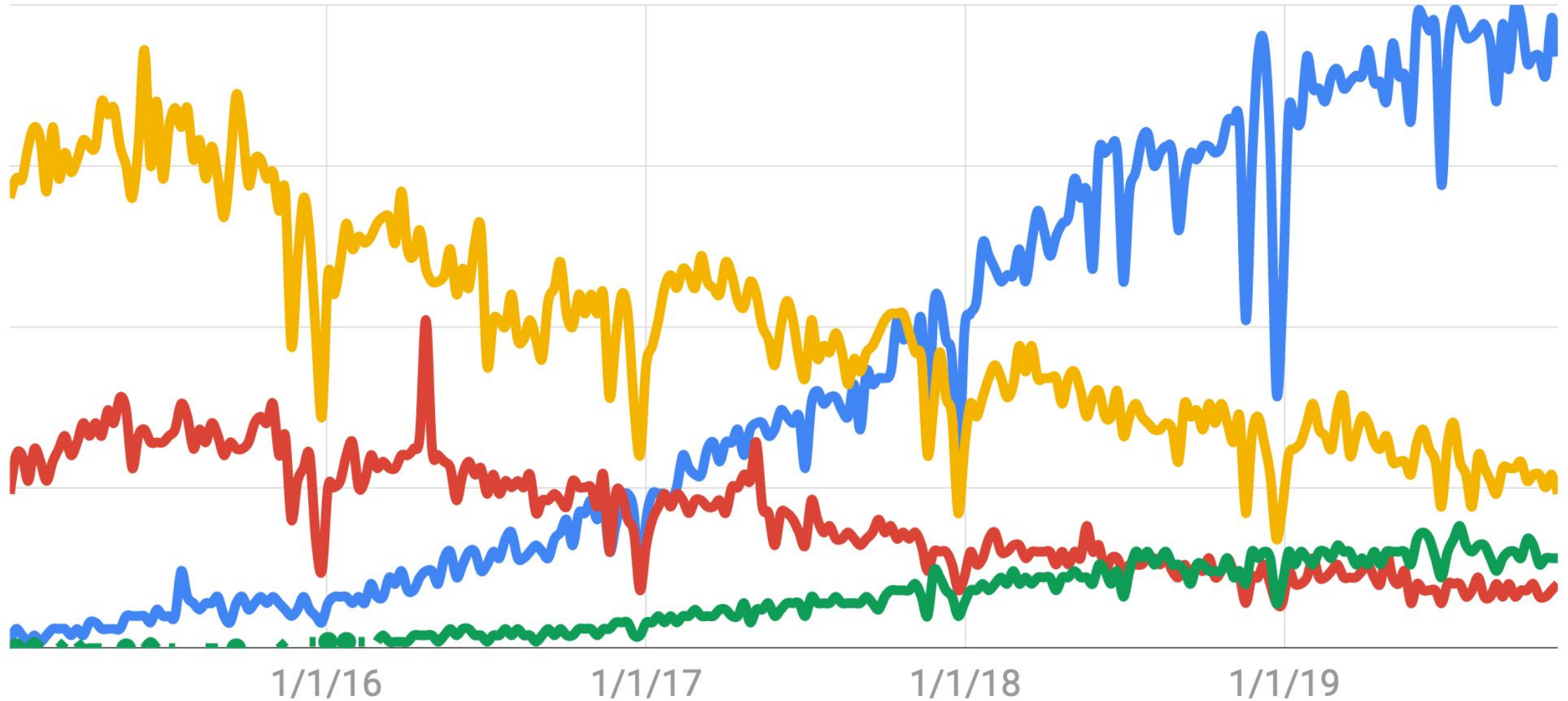


MESOS



eclipse

Life has been crazy the last ~5 years...



Open Source is Growing and Changing...

Trend: Open Source in the Enterprise (becoming default)

Open Source Use is Commonplace in the Enterprise

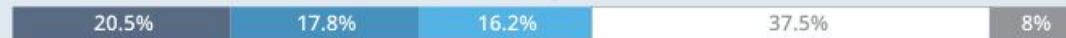
Use open source code for noncommercial or internal reasons



Use open source code in commercial products



Recruit and hire developers to work on open source projects



Attend and speak at open source events or conferences



Contribute code upstream



Create its own open source projects



Train developers to contribute to open source projects



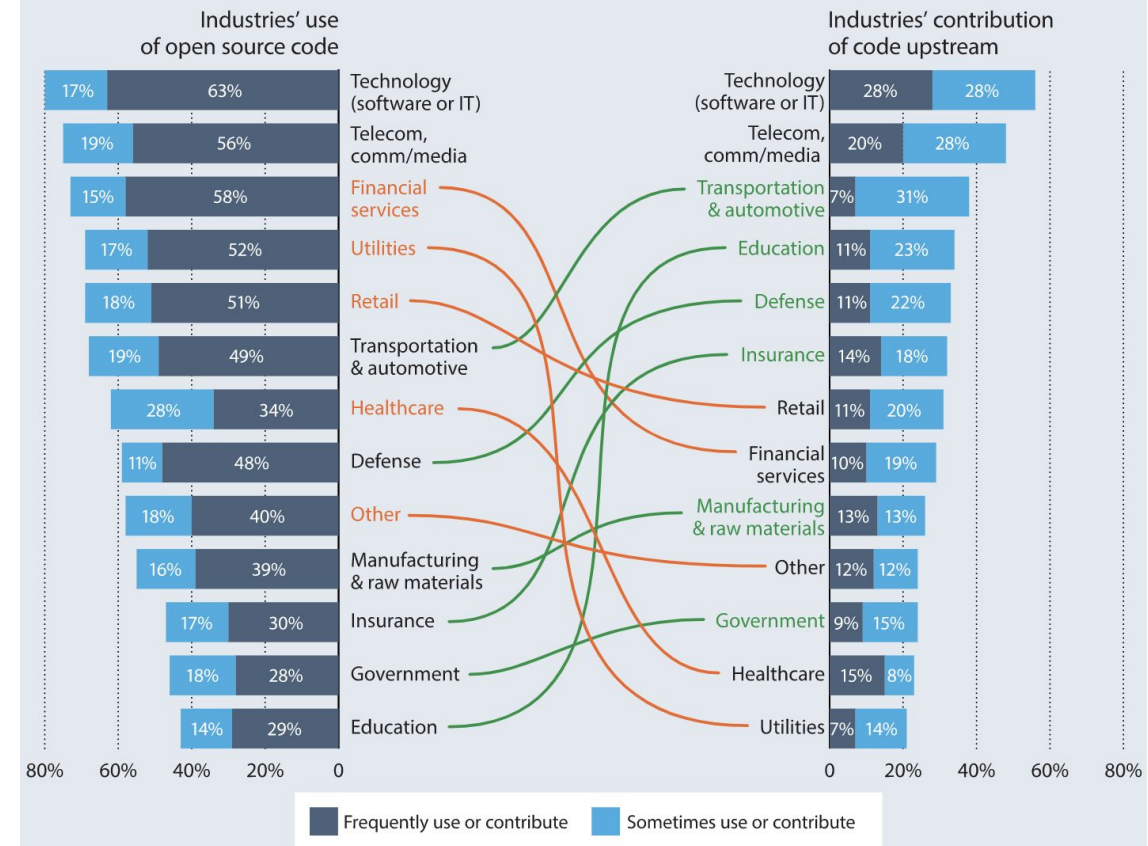
Frequently Sometimes Rarely Never Don't Know

Source: "Open Source Programs in the Enterprise - 2019" Survey. Q: How often does your company do the following activities? n=2652.



<https://github.com/todogroup/survey/tree/master/2019>

Financial, Utilities, Retail, Healthcare Use Open Source Code in Commercial Products, But Less Likely to Contribute Upstream

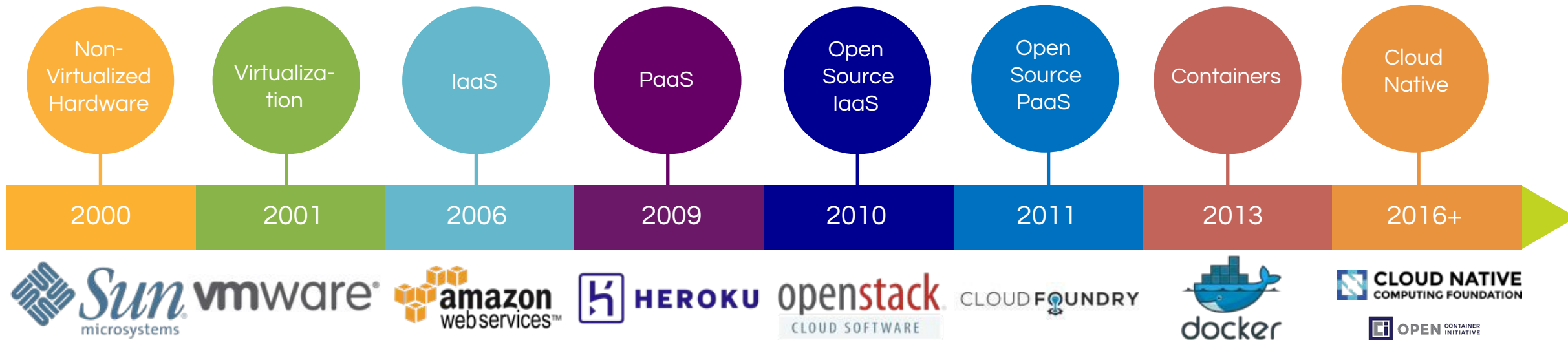


Trend: Web Scale Companies Open Up and Share

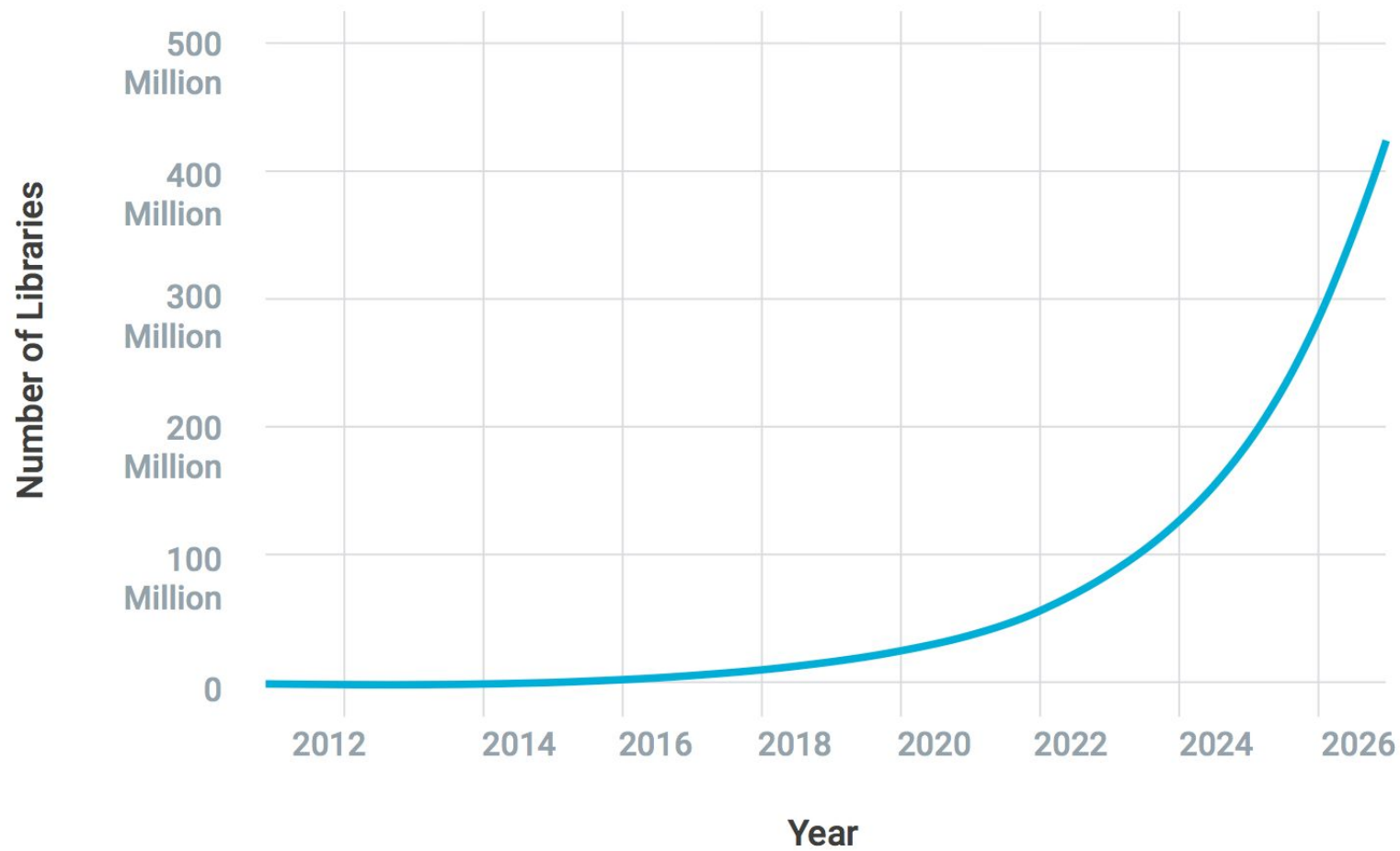
- › Software is a means to an end for internet/web scale companies
 - › Google: [Kubernetes](#), [Tensorflow](#)
 - › Facebook: [OpenCompute](#), HHVM, [OpenCellular](#), React, GraphQL
 - › Twitter: [Mesos](#)/Aurora/Parquet/[Heron](#)
 - › AWS: [FirecrackerVM](#)
 - › LinkedIn: [Kafka](#)
 - › Netflix: NetflixOSS <https://netflix.github.io>
 - › Uber: [Horovod](#), Pinot
 - › Lyft: [Envoy](#)
 - › Spotify: [Backstage.io](#)

Trend: Closed to Open Ecosystems

- › Over time, infrastructure has moved from single-vendor closed ecosystems to multiple cross-vendor open ecosystems
- › Infra is one example, happening in other areas (see RISC-V, FINOS)!



Trend: Open Source Isn't Slowing Down Any Time Soon!



[:] SourceClear

Rise of Open Source Programs (OSPOs)

Trend: Web Scale Companies + Open Source Programs

The internet scale companies pioneered the creation of open source programs:

- › Google: <https://developers.google.com/open-source/>
 - › *“...tasked with maintaining a healthy relationship with the open source software development community”*
- › Facebook: <https://code.facebook.com/opensource>
 - › “...we’re keen users and publishers of open software. We’ll keep you up-to-date with our new projects...”
- › Twitter: <http://todogroup.org/blog/why-we-run-an-open-source-program-twitter/>
- › Netflix: <https://netflix.github.io>

Trend: Traditional Companies + Open Source Programs

Traditional companies have begun creating open source programs too!

› Autodesk

› <https://github.com/todogroup/guides/blob/master/casestudies/autodesk.md>

› Comcast

› <https://github.com/todogroup/guides/blob/master/casestudies/comcast.md>

› Intel: <https://01.org> (*“...international team dedicated to working within open communities.”*)

› Salesforce

› <https://github.com/todogroup/guides/blob/master/casestudies/salesforce.md>

› Samsung: <http://commit101.org>

› *“The Open Source Group was formed in 2013 to do the following: Help guide the company in effective consumption, collaboration, and development of open source software. Provide advocacy on behalf of Samsung in external open source communities....*

Trend: Startups* + Open Source Programs

Forward looking startups also created open source programs in their earlier days

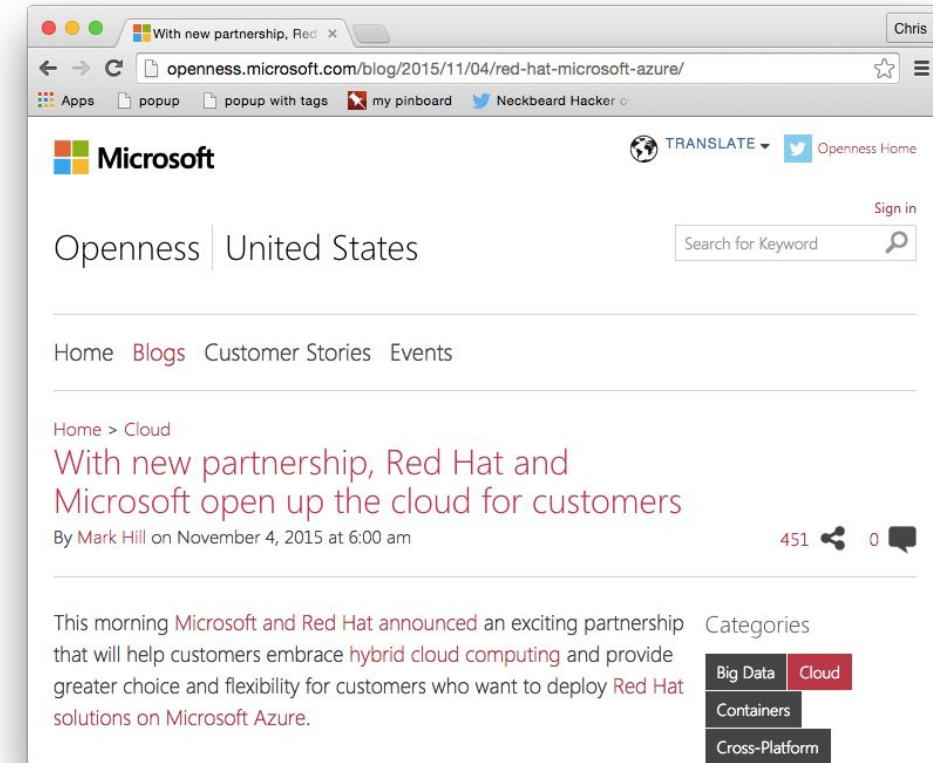
- › Box: <http://opensource.box.com>
 - › <http://todogroup.org/blog/creating-an-open-source-office-box/>
 - › “we give back to the open source community whenever possible, by contributing code to outside projects and sharing projects that we've developed internally”
- › Dropbox: <https://opensource.dropbox.com>
 - › “Dropbox loves open source! We participate in the open source community by using open source software internally and open sourcing our own projects”
- › Uber: <https://uber.github.io>
 - › “Uber loves open source and contributing to the open source community”

Trend: Open Source Program... even Microsoft!

<https://microsoft.com/opensource>

- ▶ *"Microsoft's commitment to openness and collaboration is ingrained... These collaborations have enabled new scenarios for customers and partners to take open source software and integrate it with a Microsoft platform."*
- ▶ <http://todogroup.org/blog/why-we-run-an-open-source-program-microsoft>

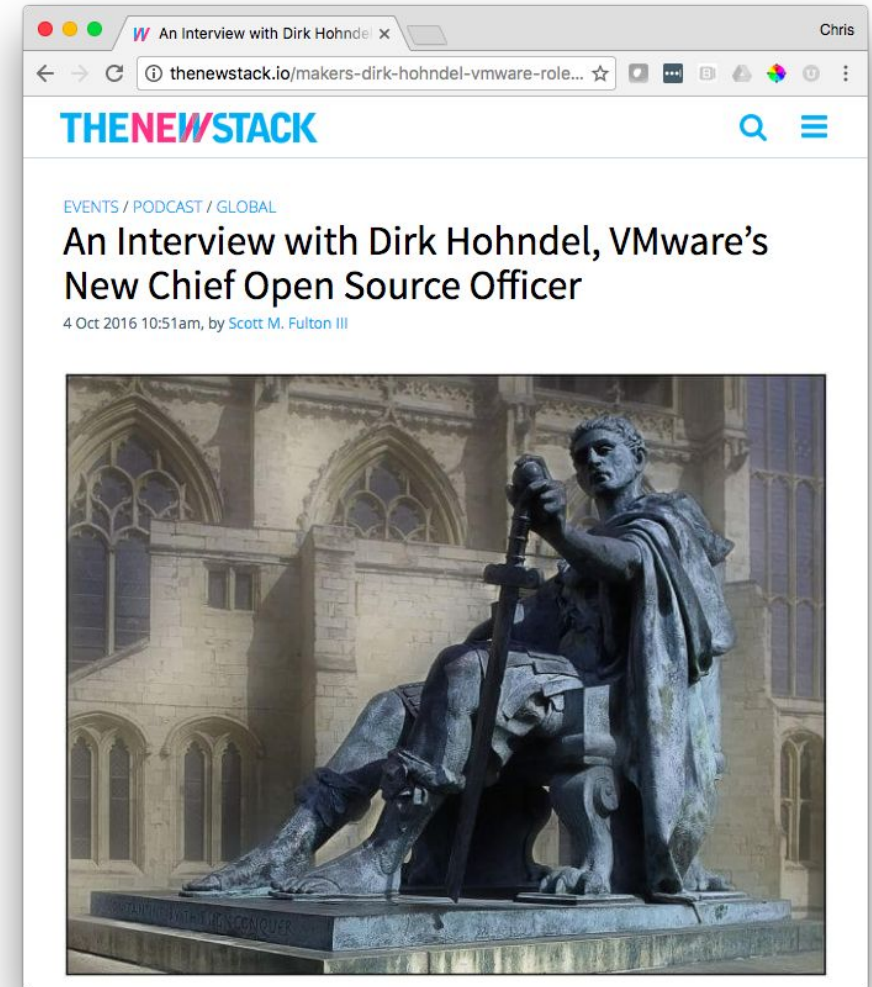
Hell they even bought GitHub!



Trend: Chief “Open Source” Officer

Companies are hiring executive open source leads...

- ▶ *“As VMware broadens its ecosystem from traditional engagements in the data center space to areas such as software-defined networking and Cloud Native and mobile app technologies, we have been releasing more and more of our new offerings as open source software,” said Ray O’Farrell, executive vice president and Chief Technology Officer, VMware. “Dirk brings a new level of leadership, best practices and creativity to help us drive these open source contributions and projects.”*
- ▶ <http://thenewstack.io/makers-dirk-hohndel-vmware-role-open-source-commercial-software/>



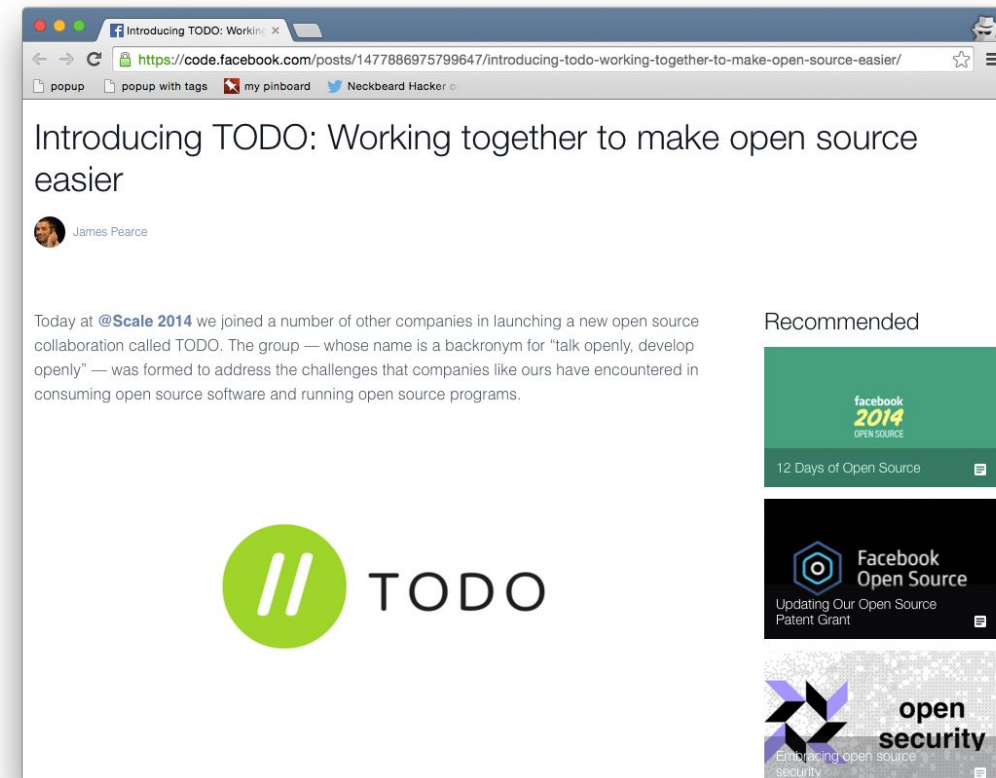
TODO Group



 THE **LINUX** FOUNDATION

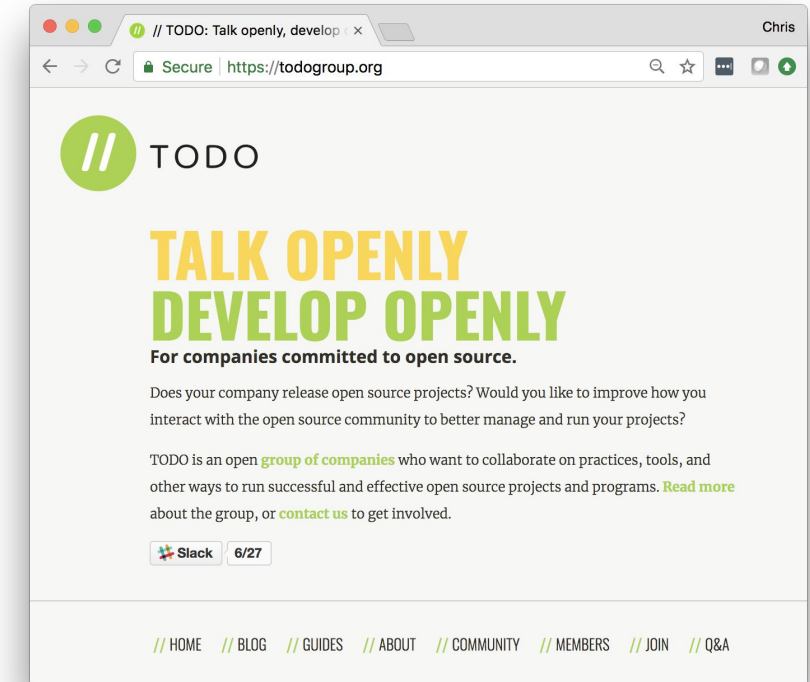
Origins of the TODO Group: todogroup.org

- ▶ Many of us who ran open source program offices shared a private mailing list to commiserate...
- ▶ It was an avenue to discuss issues in private and even find ways to collaborate on open source projects...
- ▶ Focused on Silicon Valley companies initially
- ▶ In 2014 we had an idea of scaling and opening up the the community more...
- ▶ Announced the TODO Group @Scale 2014 conference!
- ▶ [Moved to the Linux Foundation](#) in 2016!



What is the TODO Group?

- ▶ TODO Group is a group of companies who want to
 - collaborate on best practices on running open source programs
 - share open source policies and training material
 - codify quality criteria for well-run open source projects
 - build and share tools to maintain those quality standards
- As we scaled our open source programs, we realized we all built similar tools for the purposes of corporate scale open source...
- What is corporate scale open source?



FYI: Corporate Scale Open Source

- Corporate participants in open source have a number of unique concerns ranging from:
 - scale (i.e., Google and Microsoft have thousands of open source projects)
 - insights
 - cultural
 - legal / governance
- Companies doing open source generally want to be good community citizens, to be open and inclusive. They also need to run a business and be aware of responsibilities to their employees, shareholders and the broader community.

TODO Group + GitHub

- GitHub has won as the default host for open source projects but wasn't designed for corporate large scale open source so there are considerable feature gaps... the TODO Group is helping identify and fill those gaps (i.e., multiple org management, CLAs, community metrics)
- We also work with GitHub as a “product council” to help improve their platform that we continued to depend on (e.g., improved [org management](#) and required commit status features)
- See <https://github.com/todogroup/gh-issues>

TODO Group Members (50+ organizations)

Andrew Spyker (Netflix)

Christine Abernathy (Facebook)

Chris Aniszczyk (LF)

Gil Yehuda (Verizon)

Peter Giese (SAP)

Ian Varley (Salesforce)

Ibrahim Haddad (LF)

Jeff McAffer (GitHub)

Jeff Osier-Mixon (Intel)

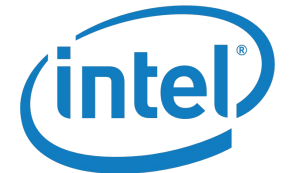
Dirk Hohndel (VMWare)

Nithya Ruff (Comcast)

Remy DeCausker (Spotify)

Stormy Peters (Microsoft)

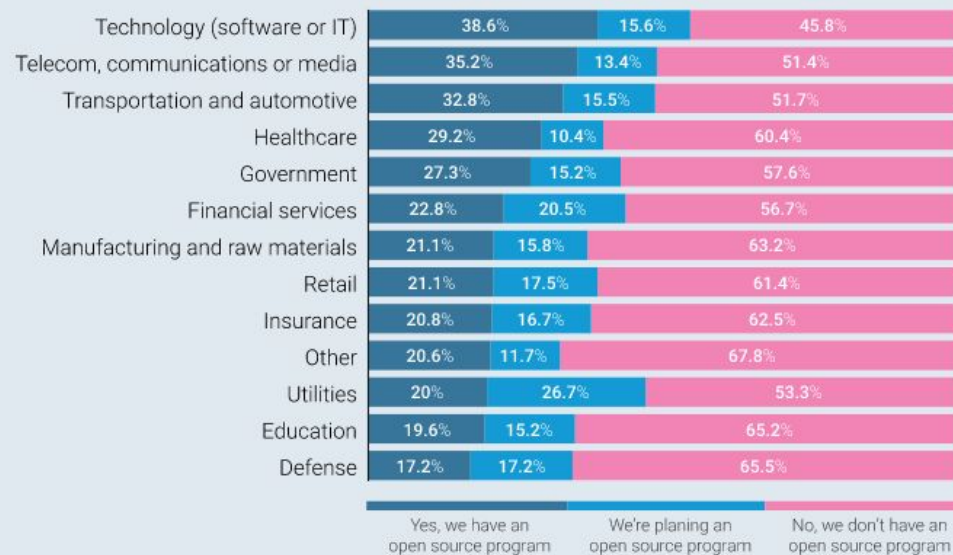
Will Norris (Google)



Annual Open Source Programs (OSPO) Survey

- <https://github.com/todogroup/survey>
 - 2020 is live! <https://www.surveymonkey.com/r/todo2020?ospo=todorepo>

Tech and Telecom Firms Most Likely to Have an OSS Program

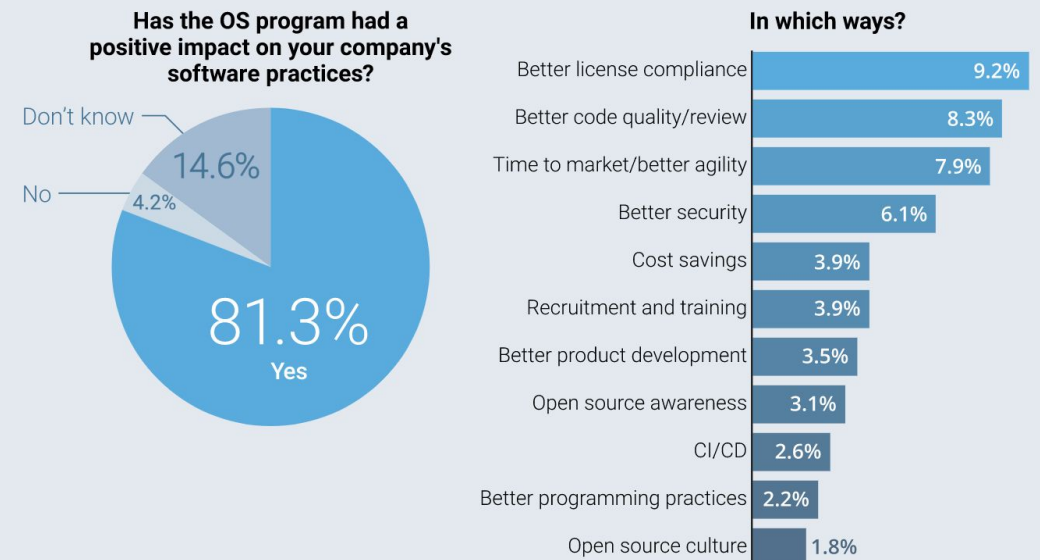


Source: "Open Source Programs in the Enterprise - 2019" Survey. Q. Does your company have an open source program (either formal or informal) or management initiative? Defense, n=29; Education, n=112; Financial services, n=127; Government, n=66; Healthcare, n=48; Insurance, n=24; Manufacturing and raw materials, n=38; Other, n=180; Retail, n=57; Technology (software or IT), n=712; Telecom, communications or media, n=142; Transportation and automotive, n=58; Utilities, n=30.



© 2019 THE NEW STACK

Open Source Programs are Overwhelmingly Beneficial



Source: "Open Source Programs in the Enterprise - 2019" Survey.
Q. Has the open source program had a positive impact on your company's software practices? n=576.
Q. If yes, please provide one or two specific examples. n=228.



© 2019 THE NEW STACK

Starting an Open Source Program

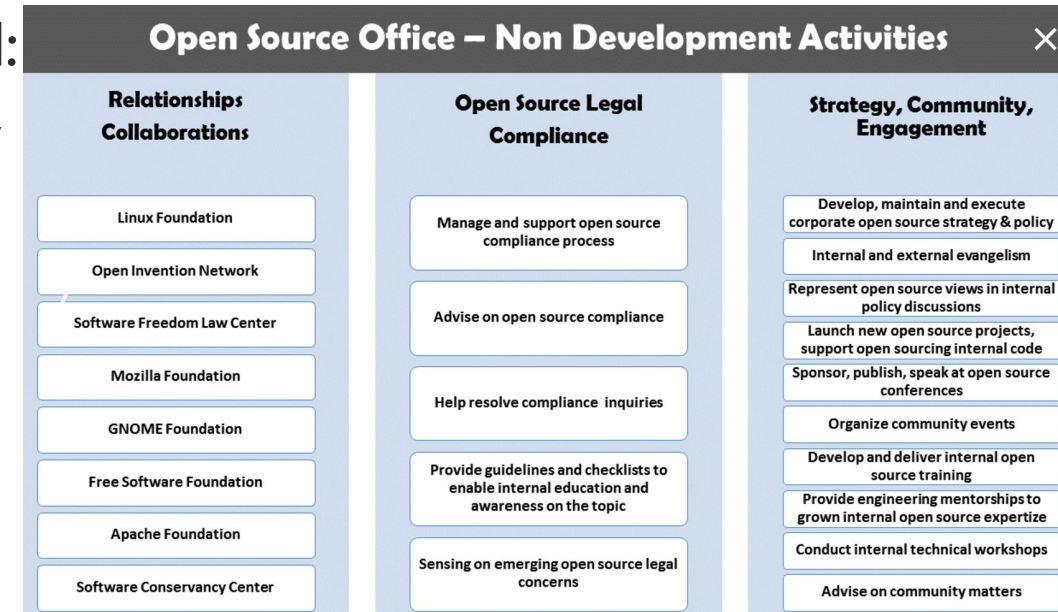
What is an Open Source Program/Office (OSPO)?

- By creating an open source program office, businesses can enable, streamline and organize the use of open source in ways that tie it directly to a company's long-term business plans. **An open source program is designed to be the center of the universe for a company's open source operations and structure, helping to bring all the needed components together.**
- **See official definition from TODO Group:**
 - <https://github.com/todogroup/ospodefinition.org>
 - <https://github.com/todogroup/guides/blob/master/creating-an-open-source-program.md>

Open Source Program Responsibilities

The responsibilities of a program office are varied:

- Clearly communicating the open source strategy within and outside the company
- Owning and overseeing the execution of the strategy
- Facilitating the effective use of open source in commercial products and services
- Ensuring high-quality and frequent releases of code to open source communities
- Engaging with developer communities and seeing ROI
- Fostering an open source culture within an organization
- Maintaining open source license compliance reviews and oversight



For every company, the role of the open source program office will likely be custom-configured based on its business, products, and goals. There is no broad template for building an open source program that applies across all industries

See TODO Group OSPO Awesome List For Ideas

› <https://github.com/todogroup/awesome-oss-mgmt>

Awesome OSS Management

This list identifies packages and projects that have been built by TODO Group members or found helpful for managing open source projects and offices.

Contents

- [Code Reviews](#)
- [Contributor License Agreements](#)
- [GitHub Metrics and Dashboards](#)
- [GitHub Management](#)
- [Project Quality](#)
- [Supply Chain Trust](#)
- [Licensing](#)
- [Localization and Internationalization](#)
- [Websites and Documentation](#)
- [License](#)
- [Security](#)

Code Reviews

- [mention-bot](#) - The mention bot will automatically mention potential reviewers on pull requests. It helps getting faster turnaround on pull requests by involving the right people early on.
- [PullApprove](#) - Allows for fancier rules on how pull requests are approved.
- [sentinel](#) - PR Test, review, and merge workflow bot
- [pull-review](#) - assign pull request reviewers intelligently, inspired by mention-bot
- [pull-request-size](#) - Automatically adds GitHub labels based on the size of a Pull Request.

Leverage Open Source Program Tooling To Scale*



REPO LINTER

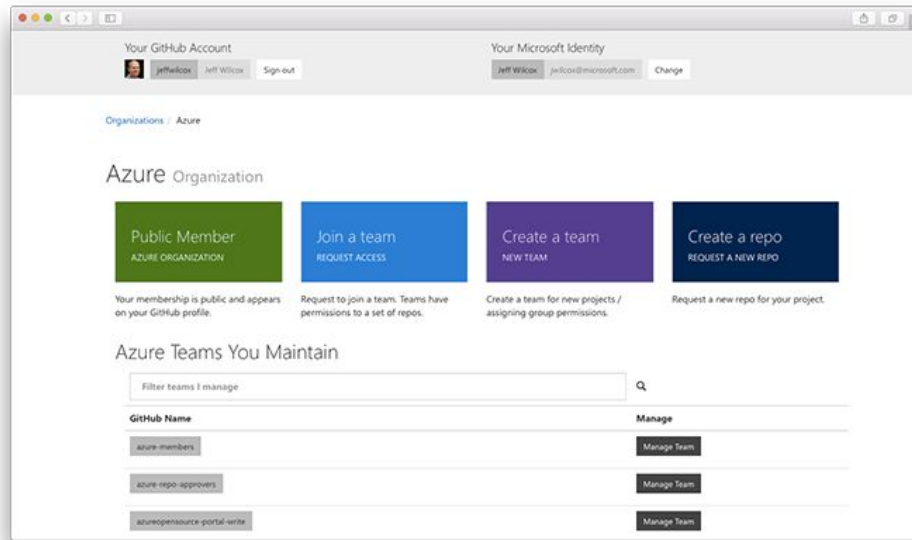
<https://github.com/todogroup/repolinter>



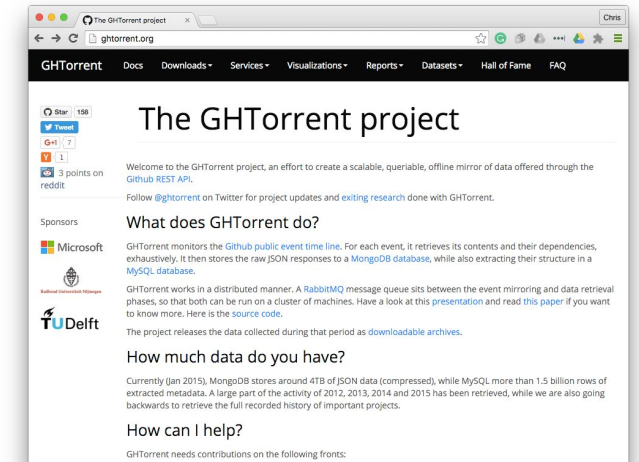
mention-bot commented 2 minutes ago

By analyzing the blame information on this pull request, we identified @vjeux to be a potential reviewer.

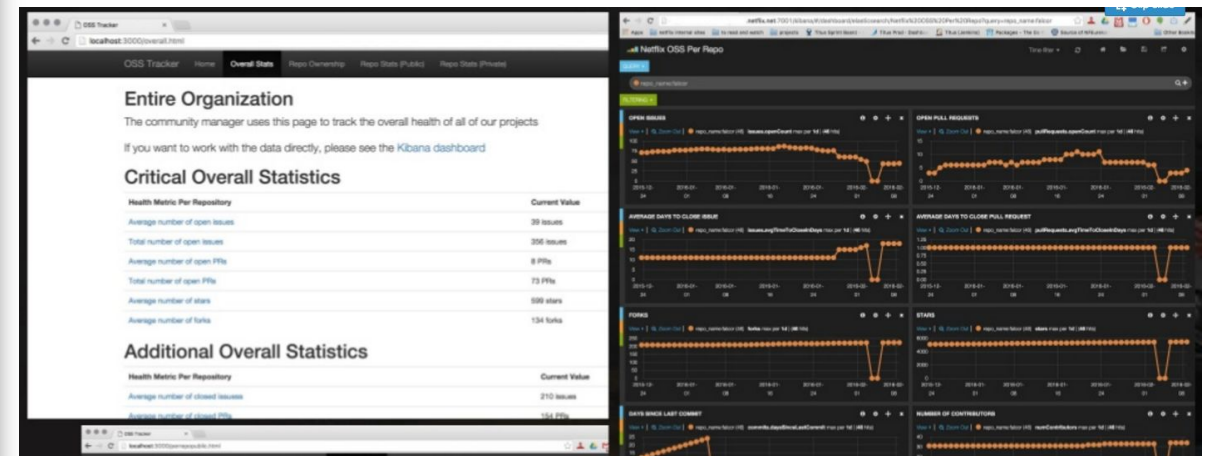
<https://github.com/facebook/mention-bot>



<https://github.com/Azure/azure-oss-portal>



<http://ghtorrent.org>



<https://github.com/Netflix/osstracker>

*<https://github.com/todogroup/guides/blob/master/tools-for-managing-open-source-programs.md>

Build Internal/External Open Source Tech Radar

- › Consider building an open source tech radar for your organization
- › <https://github.com/zalando/tech-radar>

Zalando Tech Radar — 2019.12

Frameworks

ADOPT

1. Akka (Scala)
2. Node.js
3. Play (Scala)
4. ReactJS
5. RxJava (Android)
6. scikit-learn
7. Spring

TRIAL

8. Akka-Http
9. Angular
10. AspectJ
11. Camel
12. Camunda
13. OpenNLP
14. TensorFlow
15. Thymeleaf

ASSESS

16. Aurelia
17. Ember.js
18. gRPC
19. Http4s
20. JOOQ
21. Redux
22. Vert.x
23. Vue.js

HOLD

24. Activiti
25. AngularJS 1.x
26. BackboneJS
27. Drools
28. Spray

Infrastructure

ADOPT

67. Docker
68. Hystrix
69. Kubernetes
70. Nginx
71. OpenTracing
72. Tomcat
73. ZMON

ASSESS

76. AWS Lambda

HOLD

77. STUPS

Data Management

ADOPT

29. AWS EMR
30. AWS S3
31. AWS SNS
32. AWS SQS
33. Cassandra
34. Elasticsearch
35. etcd
36. Kafka
37. Nakadi
38. PostgreSQL
39. Redis
40. Solr
41. Spark

TRIAL

42. Airflow
43. AWS Data Pipeline
44. AWS DynamoDB
45. Flink
46. Google BigQuery
47. HDFS
48. Presto
49. RabbitMQ

ASSESS

50. AWS Kinesis
51. Consul
52. Google Bigtable
53. Hadoop
54. RocksDB
55. YARN

HOLD

56. ActiveMQ
57. Aerospike
58. CouchBase
59. Esper
60. HBase
61. HornetQ
62. Memcached
63. MongoDB
64. MySQL
65. Oracle DB
66. ZooKeeper

Languages

ADOPT

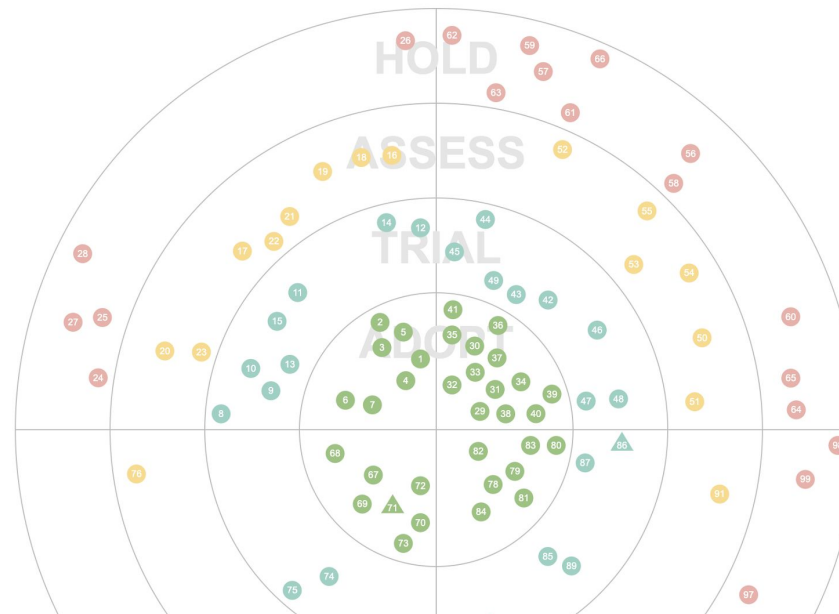
78. Go
79. Java
80. JavaScript
81. OpenAPI (Swagger)
82. Python
83. Scala
84. Swift

ASSESS

90. R
91. Rust

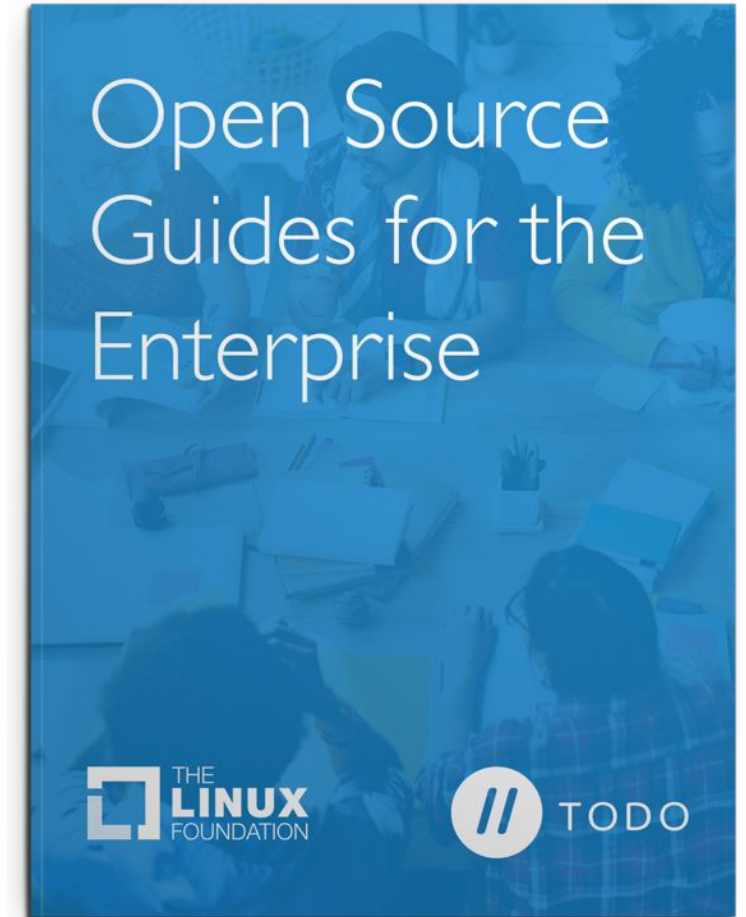
HOLD

92. .NET languages
93. C languages
94. CoffeeScript



Learn from Others: TODO Open Source Guides

- › Developed in collaboration with TODO Group
- › Leverage best practices to run or start an open source project within your organization
- › Topics include:
 - › Creating an Open Source Program
 - › Tools for Managing Open Source Programs
 - › Measuring Your Open Source Program's Success



English: <https://linuxfoundation.org/resources/open-source-guides>

Chinese: <https://linuxfoundation.cn/resources/open-source-guides>

Starting and Cultivating an Open Source Project?

Good Reasons to Start an Open Source Project

- › Undercut your competition!?
- › Shared R&D for costs with community on strategic efforts!
- › Commoditize a market! Reduce prices of non-strategic software dependencies (think IBM + Eclipse tooling)
- › Drive demand by building an ecosystem (think Kubernetes)
- › Partner and engage with customers; offer self-support; ability for users to adopt and adapt without waiting for you

Questions to Ask Before You Open Source!?


- › Is it possible to join an existing project or effort?
- › What constitutes success for the project? How to measure that?
- › Can we financially support and sustain the project?
- › Will the project attract outside interest from the start?
- › Is there enough interest to form an external developer community?
- › See: <https://todogroup.org/guides/starting/>

Best Practices and Lessons Learned for Open Source Projects

Please choose a standard + permissive license!

- › Otherwise it's not FOSS and can hamper adoption;
- › Permissive licensing better for adoption, Apache v2.0 (patent friendly)!

Branch: master ▾ facade / LICENSE Find file Copy path

 brianwarner/facade is licensed under the
Apache License 2.0
A permissive license whose main conditions require preservation of copyright and license notices. Contributors provide an express grant of patent rights. Licensed works, modifications, and larger works may be distributed under different terms and without source code.

Permissions	Limitations	Conditions
✓ Commercial use	✗ Trademark use	ⓘ License and copyright notice
✓ Modification	✗ Liability	ⓘ State changes
✓ Distribution	✗ Warranty	
✓ Patent use		
✓ Private use		

This is not legal advice. [Learn more about repository licenses.](#)



And please use an OSI-approved license
<https://opensource.org>



**CLOUD NATIVE
COMPUTING FOUNDATION**

<https://cncf.io/blog/2017/02/01/cncf-recommends-aslv2/>

Require CII Best Practices Badge (Checklist Manifesto)

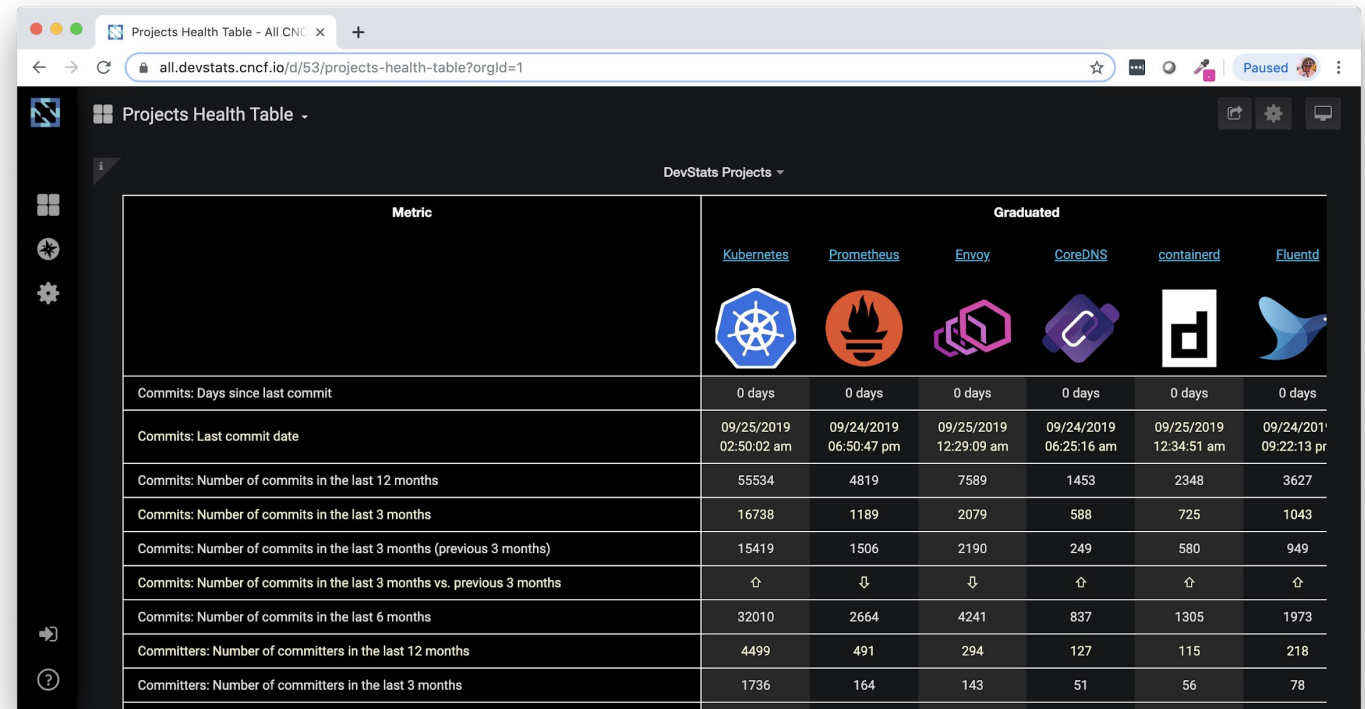
- › The open source checklist manifesto!
- › Initiative launched in May 2016 to raise awareness of development and governance steps for better security outcomes
- › The badge makes it easier for users of open source projects to see which projects take security seriously
 - › Not a “rubber stamp” process
- › 3,000+ projects registered for the badge
- › While only 10% of the projects successfully passed, every one of them made an improvement to achieve a badge



<https://www.coreinfrastructure.org>

DevStats: If You Can't Measure It, You Can't Improve It!

- › Public developer statistics help keep the community in check
- › Kubernetes + CNCF monitor project “health”
 - › <https://all.devstats.cncf.io/d/53/projects-health-table?orgId=1>
 - › See [CHAOSS Metrics](#)



The screenshot shows a web browser displaying the 'Projects Health Table' dashboard. The dashboard has a dark theme and a sidebar with navigation icons. The main content area is a table with columns for 'Metric' and 'Graduated' projects. The 'Graduated' column lists projects: Kubernetes, Prometheus, Envoy, CoreDNS, containerd, and Fluentd, each with its logo. The table contains various commit and committer statistics for these projects.

Metric	Kubernetes	Prometheus	Envoy	CoreDNS	containerd	Fluentd
Commits: Days since last commit	0 days	0 days	0 days	0 days	0 days	0 days
Commits: Last commit date	09/25/2019 02:50:02 am	09/24/2019 06:50:47 pm	09/25/2019 12:29:09 am	09/24/2019 06:25:16 am	09/25/2019 12:34:51 am	09/24/2019 09:22:13 pr
Commits: Number of commits in the last 12 months	55534	4819	7589	1453	2348	3627
Commits: Number of commits in the last 3 months	16738	1189	2079	588	725	1043
Commits: Number of commits in the last 3 months (previous 3 months)	15419	1506	2190	249	580	949
Commits: Number of commits in the last 3 months vs. previous 3 months	↑	↓	↓	↑	↑	↑
Commits: Number of commits in the last 6 months	32010	2664	4241	837	1305	1973
Committers: Number of committers in the last 12 months	4499	491	294	127	115	218
Committers: Number of committers in the last 3 months	1736	164	143	51	56	78

Open and Transparent Governance (opengovernance.dev)

- › The open governance of a project determines who has influence and control beyond what is legally required in an open source license. There are certain aspects of a projects ownership, from the copyright, trademarks, domains to even source control and build systems.
- › There is no one true way to do open governance, do what is best and optimized for your community
 - › <https://github.com/containerd/project/blob/master/GOVERNANCE.md>
 - › <https://github.com/envoyproxy/envoy/blob/master/GOVERNANCE.md>
 - › <https://github.com/helm/community/blob/master/governance/governance.md>
 - › <https://github.com/kubernetes/community/blob/master/governance.md>
 - › <https://github.com/nodejs/node/blob/master/GOVERNANCE.md>

Default to Open Communication (hard for newcomers)

- › Almost all communication should default to open, otherwise you run the risk of alienating newcomers
 - › Public meeting minutes
 - › Recorded meetings posted
 - › Open agendas
 - › Rotating meeting coordinators
- › See Kubernetes Community Meeting as a good example to follow:
 - › <https://github.com/kubernetes/community/blob/master/events/community-meeting.md>
- › **Note: include alternate meeting times for the whole world!**

Code of Conduct + Incident Response Training

- › A code of conduct is one ingredient in building an inclusive and welcoming community that can help you grow your project
- › **Don't reinvent the wheel**
 - › <https://github.com/cncf/foundation/blob/master/code-of-conduct.md>
 - › <https://www.contributor-covenant.org/>
- › For larger projects, consider a CoC Committee
 - › <https://github.com/kubernetes/community/tree/master/committee-code-of-conduct>
- › Consider Code of Conduct lessons+training:
 - › <https://otter.technology/code-of-conduct-training/>

Contributor Code of Conduct

As contributors and maintainers of this project, and in the interest of fostering an open and welcoming community, we pledge to respect all people who contribute through reporting issues, posting feature requests, updating documentation, submitting pull requests or patches, and other activities.

We are committed to making participation in this project a harassment-free experience for everyone, regardless of level of experience, gender, gender identity and expression, sexual orientation, disability, personal appearance, body size, race, ethnicity, age, religion, or nationality.

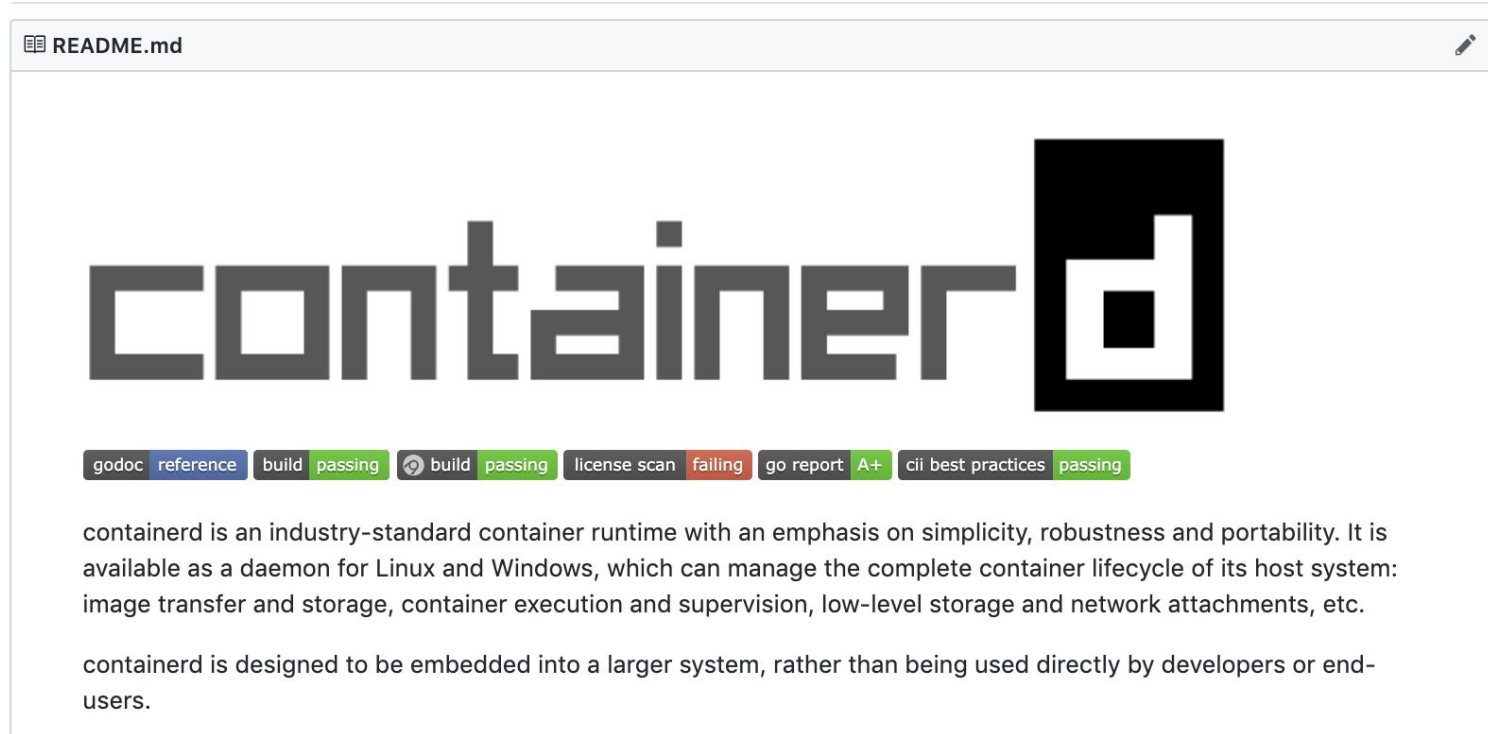
Examples of unacceptable behavior by participants include:

- The use of sexualized language or imagery
- Personal attacks
- Trolling or insulting/derogatory comments
- Public or private harassment
- Publishing other's private information, such as physical or electronic addresses, without explicit permission
- Other unethical or unprofessional conduct.

Project maintainers have the right and responsibility to remove, edit, or reject comments, commits, code, wiki edits, issues, and other contributions that are not aligned to this Code of Conduct. By adopting this Code of Conduct, project maintainers commit themselves to fairly and consistently applying these principles to every aspect of managing this project. Project maintainers who do not follow or enforce the Code of Conduct may be permanently removed from the project team.


Public and Community Driven CI/CD


- › Ensure that CI/CD is setup in a community shared responsibility fashion, no private single vendor build setups!
- › It is easier today with GitHub Actions, AZP, Circle CI etc




Acknowledge Contributors + Contributions!

- › Send contributors swag or acknowledge them in some fashion
- › Example: Kubernetes Contributor Patch For 1st Timers
 - › <https://store.cncf.io/products/copy-of-kubernetes-decal>


 **CLOUD NATIVE**
COMPUTING FOUNDATION

Search all products... 

 Cart


HOME CATALOG ABOUT US

Home > Contributor Patch



Contributor Patch
\$1,000⁰⁰

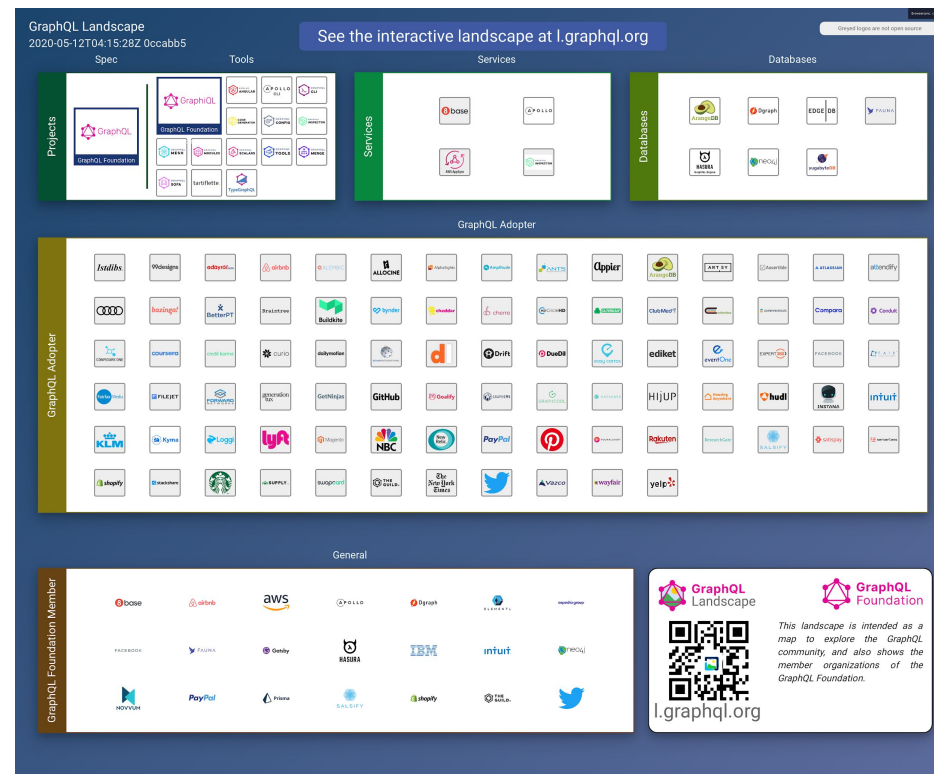
Quantity
- 1 +

 Add to Cart

This is an exclusive item only recognized contributors can earn. You must be awarded a purchase code to get this badge of honor.

Build a Landscape Around Your Project

- › An interactive landscape can help bring clarity to your project around adoption and also help you control the narrative around your ecosystem
- › See <https://landscape.graphql.org> and l.cncf.io as examples

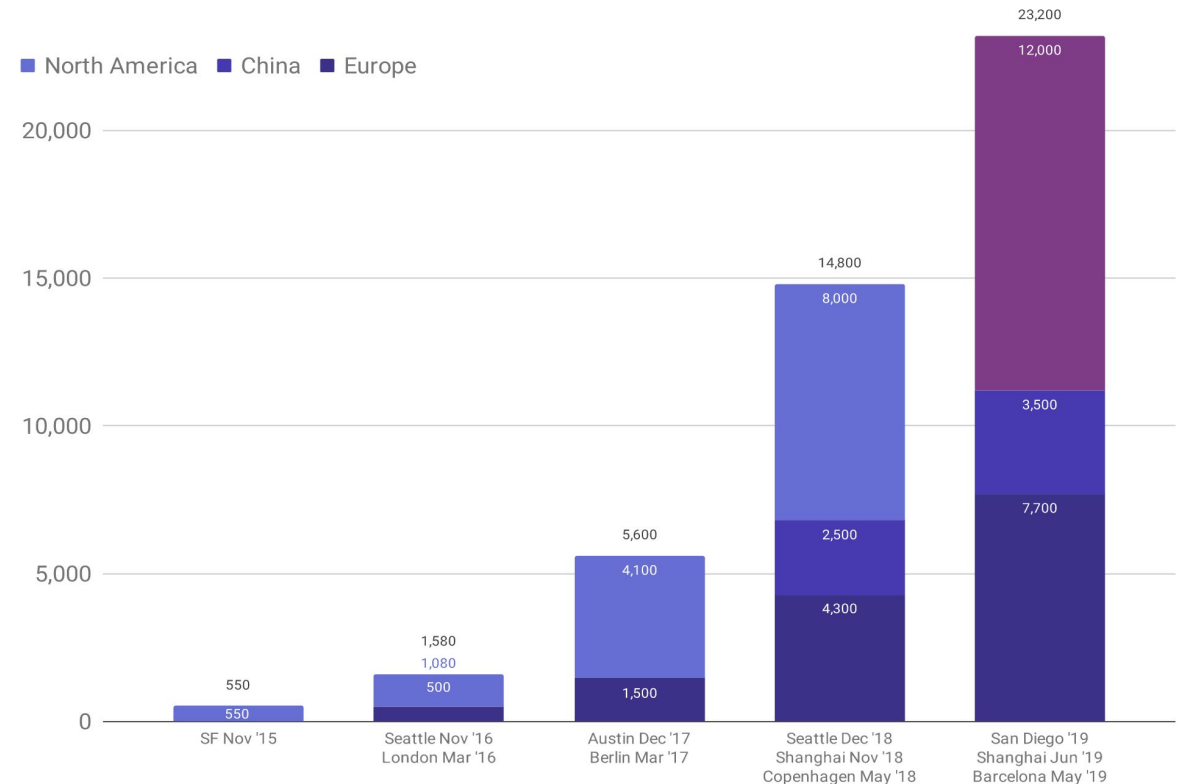


Events Build Community: Conferences + Meetups

› Open source communities should consider events for users as important as other developer activities

› Meetup Pro or Bevy to run communities at scale:

<https://meetup.com/pro/cncf> +
<https://www.bevyhq.com/>



Internationalization (i18n) + Localization (l10n)

- › Ensuring that your project is open to i18n and l10n can enable a new community of contributors and expand the reach of your project
- › Kubernetes contributions increase since we enabled translations for documentation!
 - › <https://kubernetes.io/docs/contribute/localization/>
- › Also an option to use community translation tools
 - › <http://zanata.org/>
 - › <https://github.com/mozilla/pontoon/>

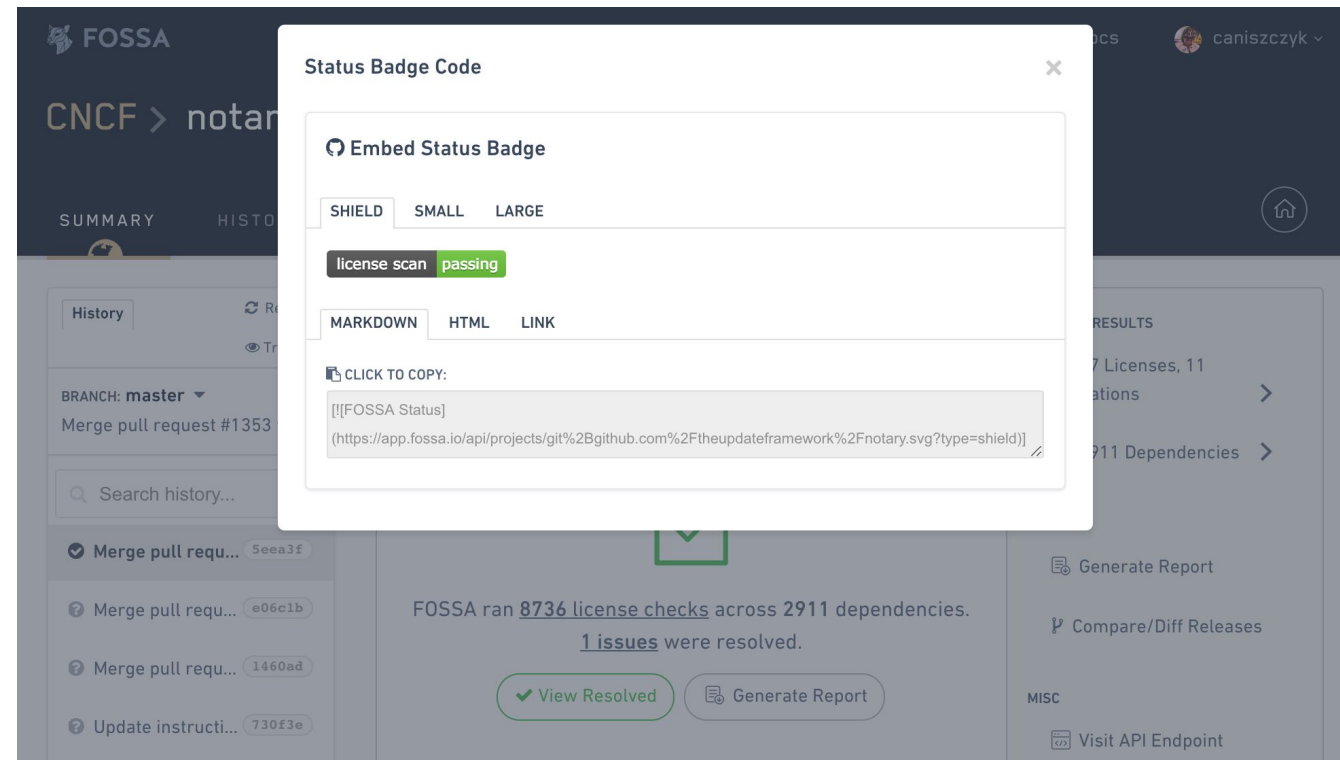
Internships: SoC + CommunityBridge (Free* Labor)

- › Internships help build and sustain community
 - › Diversify contributors! Interns become maintainers + get jobs!
 - › Teach senior contributors value of mentoring!
- › <https://www.cncf.io/blog/2019/08/22/cncf-hosts-three-student-internships-for-kubernetes-and-coredns-projects-through-linux-foundations-communitybridge/>
- › <https://www.cncf.io/blog/2019/08/23/cncf-joins-google-summer-of-code-2019-with-17-interns-projects-for-containerd-coredns-kubernetes-opa-prometheus-rook-and-more/>
- › <https://people.communitybridge.org/>
- › <https://summerofcode.withgoogle.com> + <https://developers.google.com/season-of-docs>



Legal: Automate License Scanning (FOSSA / Fossology)

- › License scanning with FOSSA.io / [Fossology](https://Fossology.com) can help your developers ensure they aren't bringing in code out of IP Policy
- › Shift left license scanning!

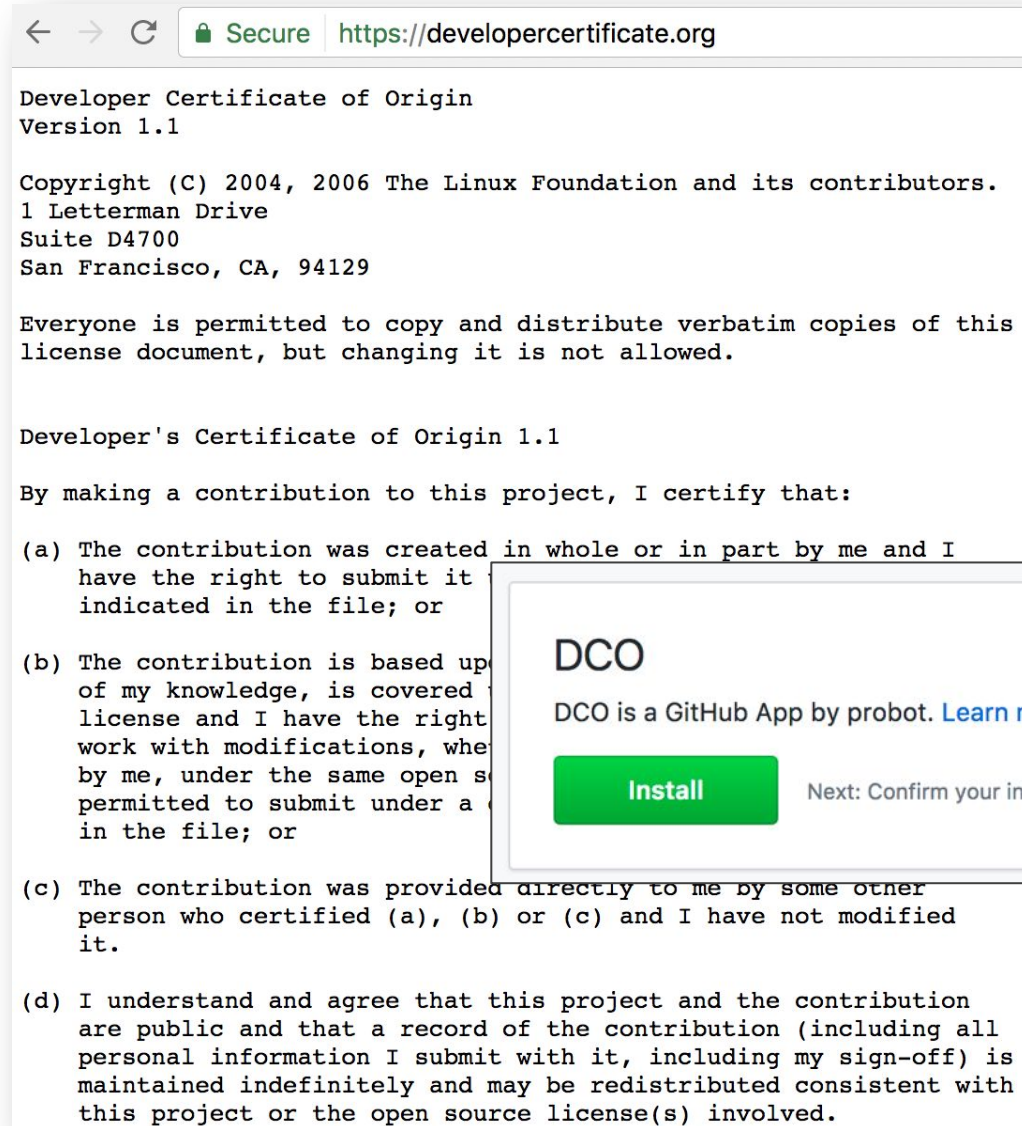


Legal: DCO (over CLA if you can)

The DCO captures code provenance at time of submitting a pull request, on every contribution. **Lower barrier to entry than CLA.**

The Linux Foundation worked with GitHub to make it easy to implement “DCO required” in any project.

<https://github.com/apps/dco>



The screenshot shows a web browser window at <https://developercertificate.org>. The page displays the text of the Developer Certificate of Origin (Version 1.1), including copyright information for The Linux Foundation and its contributors, and a list of four conditions (a, b, c, d) that a contributor must certify. Overlaid on the bottom right of the browser window is a GitHub DCO app installation card. The card has a title 'DCO', a description 'DCO is a GitHub App by probot. [Learn more...](#)', a green 'Install' button, and a note 'Next: Confirm your installation location.' with a small robot icon.

Developer Certificate of Origin
Version 1.1

Copyright (C) 2004, 2006 The Linux Foundation and its contributors.
1 Letterman Drive
Suite D4700
San Francisco, CA, 94129

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Developer's Certificate of Origin 1.1

By making a contribution to this project, I certify that:

- (a) The contribution was created in whole or in part by me and I have the right to submit it indicated in the file; or
- (b) The contribution is based upon previous work that, to the best of my knowledge, is covered by an existing open source license and I have the right to reuse that work with modifications, whether made by me, under the same open source license(s) that I am permitted to submit under a previous license, or in the file; or
- (c) The contribution was provided directly to me by some other person who certified (a), (b) or (c) and I have not modified it.
- (d) I understand and agree that this project and the contribution are public and that a record of the contribution (including all personal information I submit with it, including my sign-off) is maintained indefinitely and may be redistributed consistent with this project or the open source license(s) involved.

DCO
DCO is a GitHub App by probot. [Learn more...](#)

Install Next: Confirm your installation location.

Security: Public/Private Disclosure Process

› Consider formulating a security disclosure process or use a tool like HackerOne to help you with security issues!

› <https://github.com/envoyproxy/envoy/blob/master/SECURITY.md>

› GitHub [Supports Security Advisories](#) Now

Security Release Process

Envoy is a large growing community of volunteers, users, and vendors. The Envoy community has adopted this security disclosures and response policy to ensure we responsibly handle critical issues.

Product Security Team (PST)

Security vulnerabilities should be handled quickly and sometimes privately. The primary goal of this process is to reduce the total time users are vulnerable to publicly known exploits.

The Product Security Team (PST) is responsible for organizing the entire response including internal communication and external disclosure but will need help from relevant developers to successfully run this process.

The initial Product Security Team will consist of all [maintainers](#) in the private [envoy-security](#) list. In the future we may decide to have a subset of maintainers work on security response given that this process is time consuming.

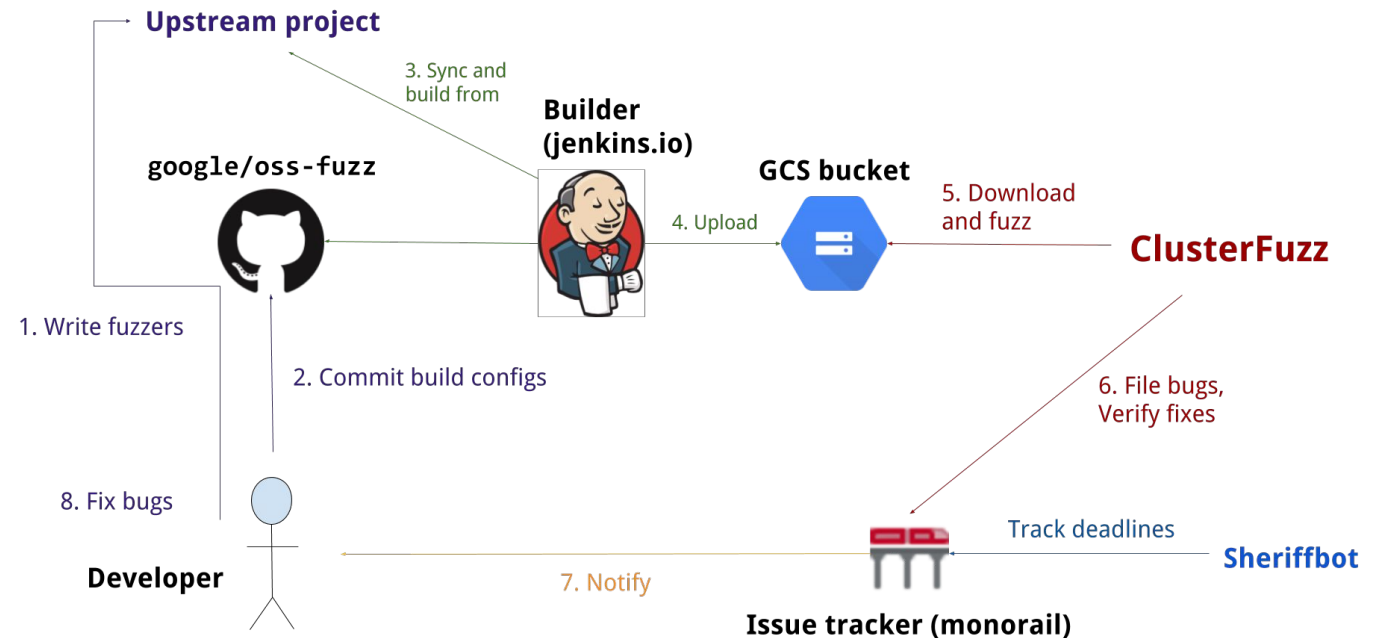
Disclosures

Private Disclosure Processes

The Envoy community asks that all suspected vulnerabilities be privately and responsibly disclosed via the [reporting policy](#).

Security: Scanning Tools, Shift Left Everything!

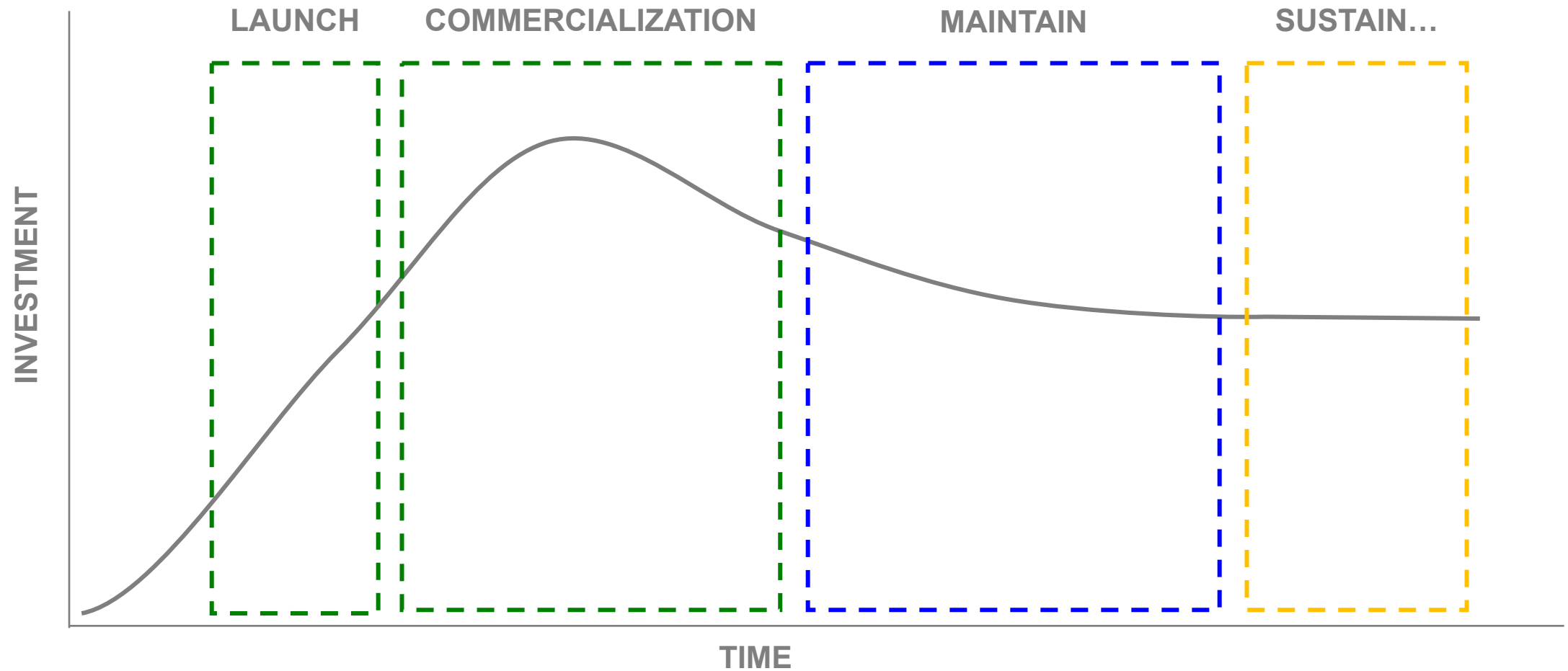
- › Use security scanning tools during build (shift left)
 - › Snyk.io, FOSSA, WhiteSource, etc
 - › Fuzzers: FuzzIt.Dev, <https://github.com/google/oss-fuzz>



Open Source Security Audits

- › Mature projects should have a battle tested security process
- › Doing a security audit and open sourcing the results helps
 - › <https://www.cncf.io/blog/2019/08/06/open-sourcing-the-kubernetes-security-audit/>
- › I recommend Cure53 and Trail of Bits as security audit vendors who are comfortable working with open source communities
 - › See [OSTIF.org](https://www.ostif.org/) and [MOSS](https://www.moss.usgoc.gov/) audits for good example audits/firms

Remember: projects have life cycles like products...



Summary and Final Thoughts...

- › There is NO ONE SIZE FITS ALL approach to guaranteeing open source project success and building a community, each project is different
- › More companies will act like software companies
 - › They will also act more like internet-scale companies like Google, Facebook, Netflix
 - › They will establish open source programs and hire open source leads
- › **Contribution brings influence and is the currency in open source... contribute or lose relevance!** <https://todogroup.org/join/>
- › **Read:** <https://github.com/todogroup/guides>

Thank You!

Q&A

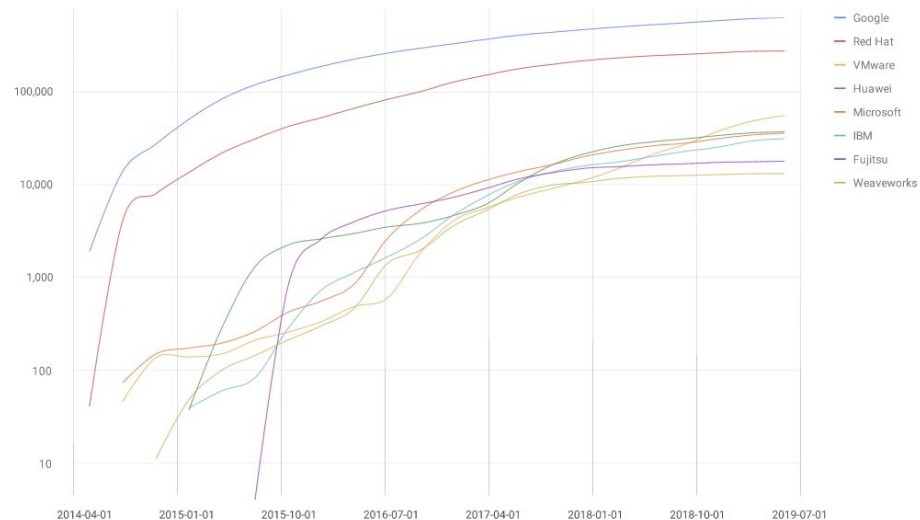
todogroup.org/guides

caniszczyk@linuxfoundation.org

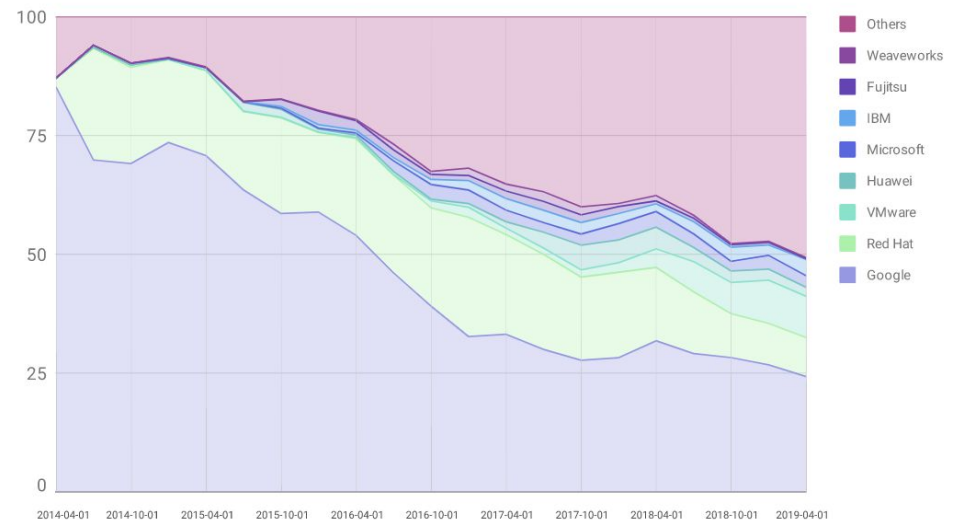
 THE **LINUX** FOUNDATION

All Happy Open Source Projects Are All Alike...

› <https://www.cncf.io/cncf-kubernetes-project-journey/>



Cumulative volume of contributions by company since Kubernetes project launch



Percentage breakdown of contributions by company since Kubernetes project launch