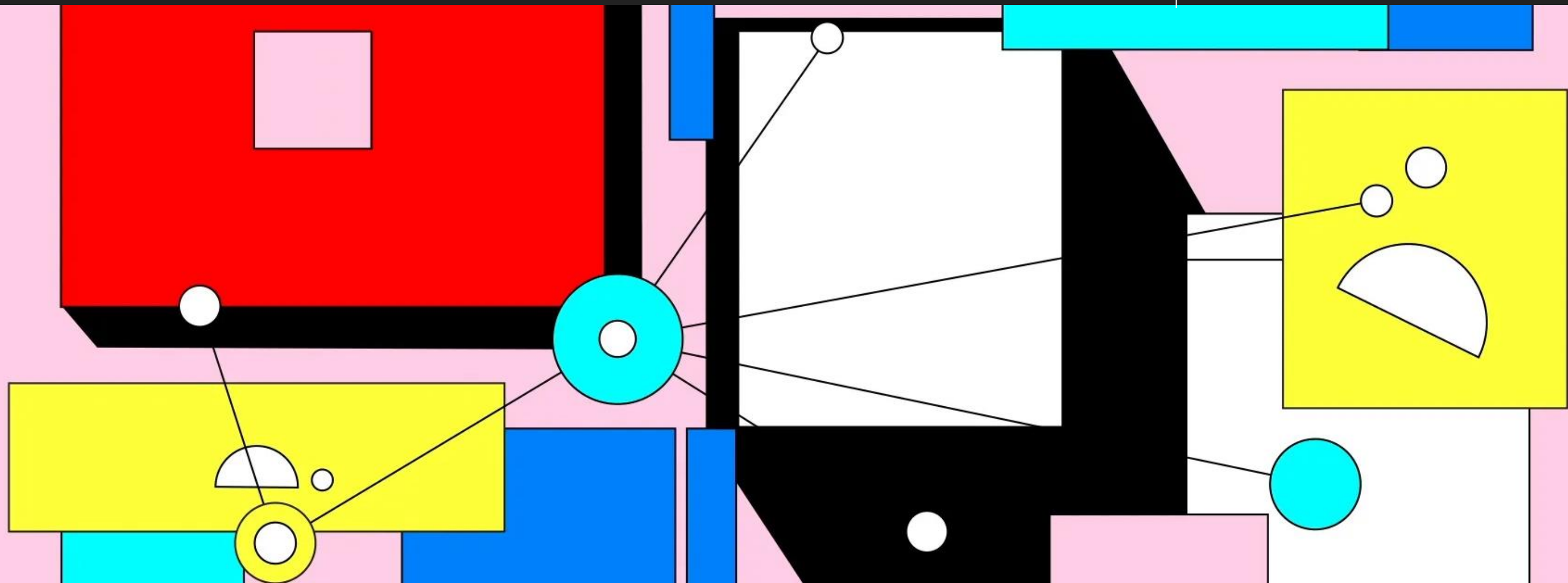


# Not as Simple as you may Think

Jacob Latonis



# whoami

---

Name: Jacob Latonis

What I do: Staff Software Engineer, Threat Research @ Proofpoint

Residing in: Boulder, CO

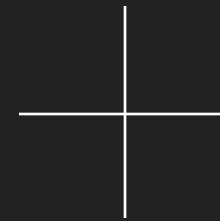
What I do for fun: cycling, running, reading, hiking, open source development



@jacoblatonis

# Contents

If it's online and available, it's  
free to use and modify, right?



- 01 - The origins of open-source
- 02 - Open-source communities
- 03 - Complexity in the community
- 04 - Leveraging open-source
- 05 - Contributing to open-source
- 06 - Modern open-source projects



before we dive in

---

who in the room has used open source software?

Literally all of you

# 01 - The origins of open-source technology

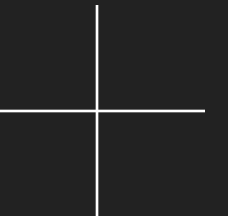


why work out in the open?

what're the benefits?

drawbacks?

the origins can be a bit murky as to the EXACT start, but there are some prominent characters and projects along the way

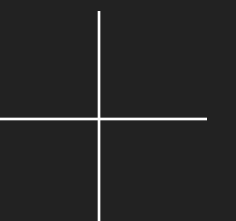




# How did it start?

## Richard Stallman

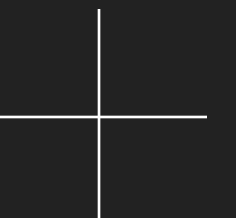
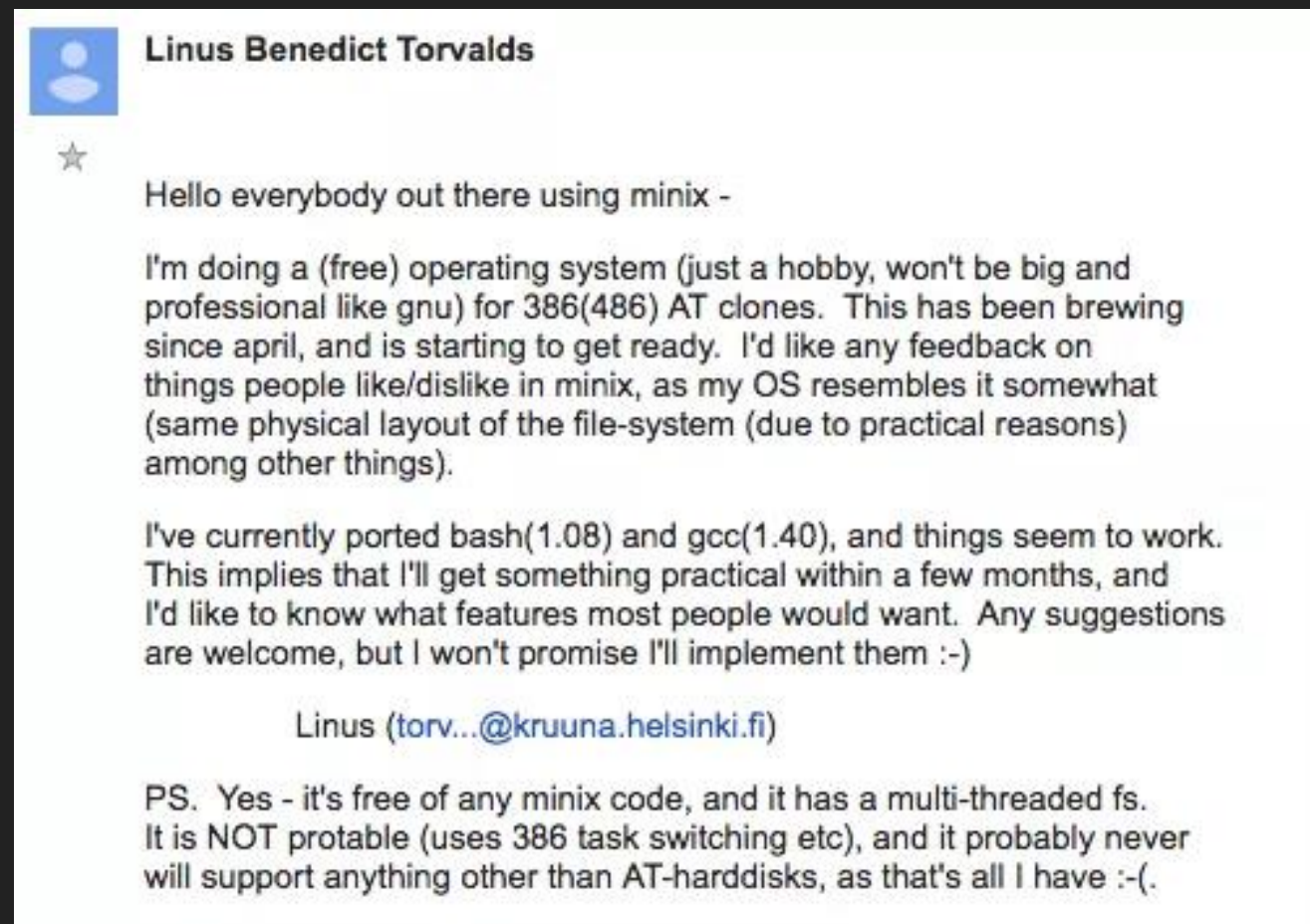
- released GNU on September 27, 1983
- GNU
- GNU Public License



# How did it start?

## Linus Torvalds

- released linux (sort-of) on August 25, 1991





# Two main modes of operation

## Cathedral

- Deeper level of knowledge needed
- Planning
- Reasoning
- Mostly the same ideals and techniques

## Bazaar

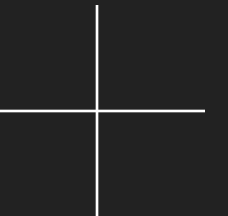
- Planning but not rigid
- Different folks, different strokes
- fast moving, many parts
- could be considered a bit messy

## 02 - Open-source communities



The word “community” in open source can mean a lot.

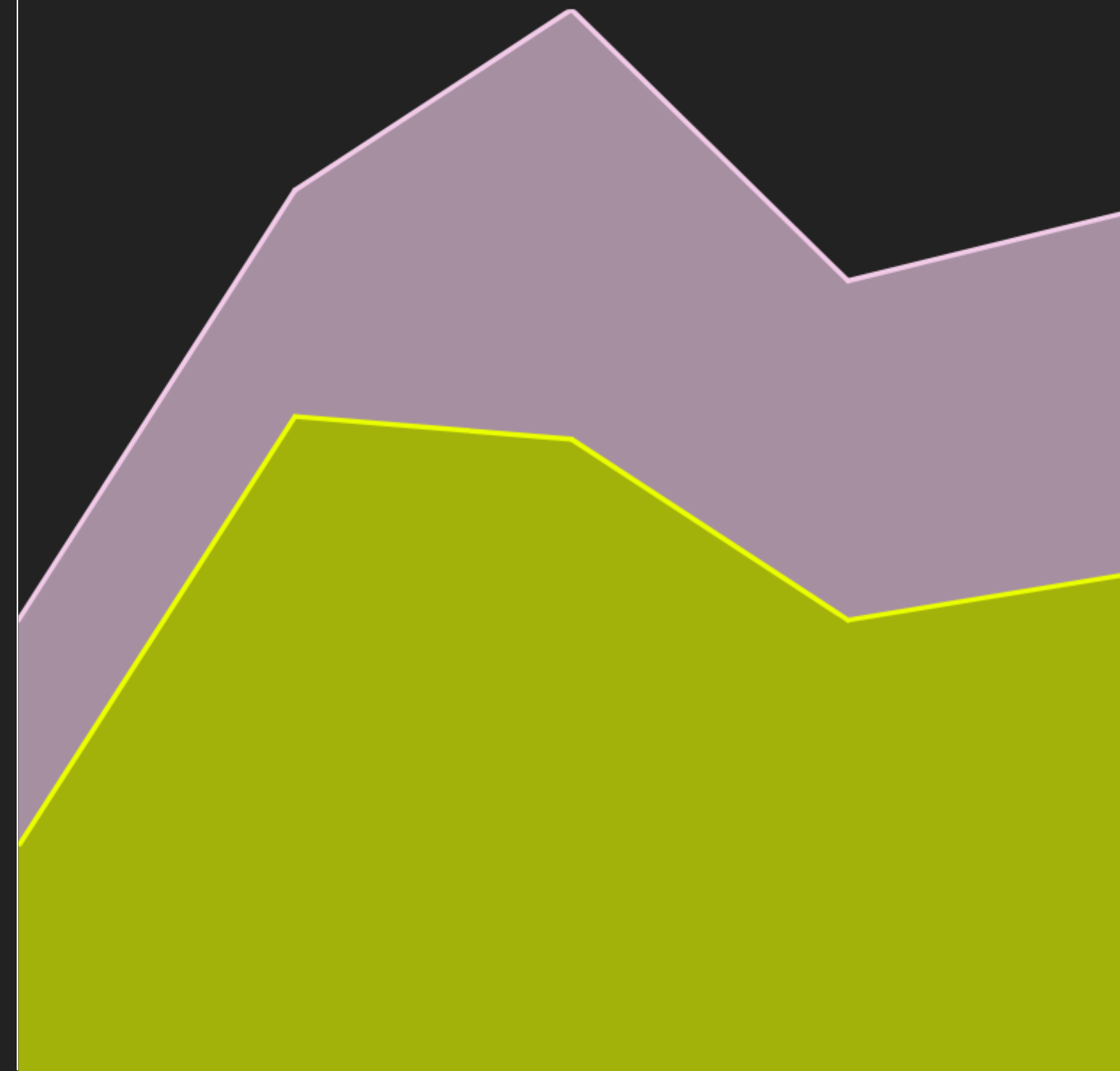
- user bases
- developers
- foundations
- the list goes on



# Federations


Federations can be defined as groups/projects with high contributor growth and high user growth. The number of users for the project is growing at a steady rate, and so is the number of contributions.

Contributors Users



# Examples of Federations

The most recent prominent example is probably the Rust foundation

 rust

Public

Watch 1.5k

Fork 12.5k

Star 96.5k


master

7 Branches

137 Tags

Go to file

Code

 bors

Auto merge of #129962 - pietroalbini:pa-cve-2...

4ac7bcb · 6 hours ago

265,029 Commits

.github	Update library/Cargo.toml in weekly job	2 weeks ago
LICENSES	Include REUSE.toml in REUSE.toml.	2 months ago
compiler	Auto merge of #129777 - nnethercote:unr...	2 days ago
library	More robust extension checking	yesterday
src	Auto merge of #129356 - nikic:llvm19-hos...	yesterday
tests	More robust extension checking	yesterday
.clang-format	Add .clang-format	3 months ago
.editorconfig	Only use max_line_length = 100 for *.rs	last year
.git-blame-ignore-revs	Exclude the copy blessing from git blame	2 weeks ago
.gitattributes	Rename config.toml.example to config.e...	last year
.gitignore	gitignore: ignore ICE reports regardless of ...	2 weeks ago
.gitmodules	Update to LLVM 19	2 months ago
.ignore	Add .ignore file to make config.toml sear...	3 months ago
.mailmap	Rollup merge of #129906 - BoxyUwU:boxy...	2 days ago
CODE_OF_CONDUCT.md	Remove the code of conduct; instead link ...	5 years ago
CONTRIBUTING.md	fix: Update CONTRIBUTING.md recomme...	10 months ago
COPYRIGHT	Update COPYRIGHT file	2 years ago
Cargo.lock	update object dependency to deduplicate...	3 days ago

About

Empowering everyone to build reliable and efficient software.

[www.rust-lang.org](http://www.rust-lang.org)

language

rust

compiler

hacktoberfest

Readme

Apache-2.0, MIT licenses found

Code of conduct

Security policy

Activity

Custom properties

96.5k stars

1.5k watching

12.5k forks

Report repository

Releases 128








Rust 1.80.0








Latest

on Jul 25

+ 127 releases

Contributors 5,000+







+ 5,065 contributors





# Examples of Federations (cont'd)


I also included Zig so I am not bullied after this talk by the 3 people in the room that like Zig

 **zig** Public

 Sponsor

 Watch 359

 Fork 2.5k

 Star 33.6k


master

29 Branches

19 Tags

Go to file

Code

 **kubkon**

Merge pull request #21305 from ziglang/elf-incr

7e31804 · 4 hours ago


30,931 Commits

github	Only set contents: read permission in GitHub Action	last week
ci	Dwarf: fix and test inline function bugs	last week
cmake	cmake: CLANG_LIBRARIES: find libclang-cpp.so.18.1	3 weeks ago
doc	langref: separate header for faulty default field values	5 days ago
lib	stdlib : base64 encode to writer (#20961)	16 hours ago
src	elf: fix 32bit build	10 hours ago
stage1	stage1: update zig1.wasm	last week
test	elf: fix emitting static lib when ZigObject is present	12 hours ago
tools	std: update std.builtin.Type fields to follow naming con...	last week
.gitattributes	Sync Aro sources (#19199)	6 months ago
.gitignore	update .gitignore to account for .zig-cache rename	4 months ago
.mailmap	update .mailmap	5 months ago
CMakeLists.txt	elf: add AtomList.zig to CMakeLists.txt	12 hours ago
LICENSE	LICENSE: copyright notices do not need years	last year
README.md	update readme	2 weeks ago
bootstrap.c	remove deprecated --mod CLI now that a zig1.wasm upda...	2 months ago
build.zig	loongarch: use medium code model for zig loongarch64 b...	4 days ago
build.zig.zon	Promote linker test cases to packages	5 months ago

README

Code of conduct

MIT license



General-purpose programming language and toolchain for maintaining robust, optimal, and reusable software.

[ziglang.org](https://ziglang.org)

language compiler zig

Readme

MIT license

Code of conduct

Activity

Custom properties

33.6k stars

359 watching

2.5k forks

Report repository


Releases 18

0.13.0 Latest

on Jun 7

+ 17 releases

Sponsor this project

 **ziglang** Zig Programming Language







Sponsor








Learn more about GitHub Sponsors

Packages

No packages published

Contributors 926





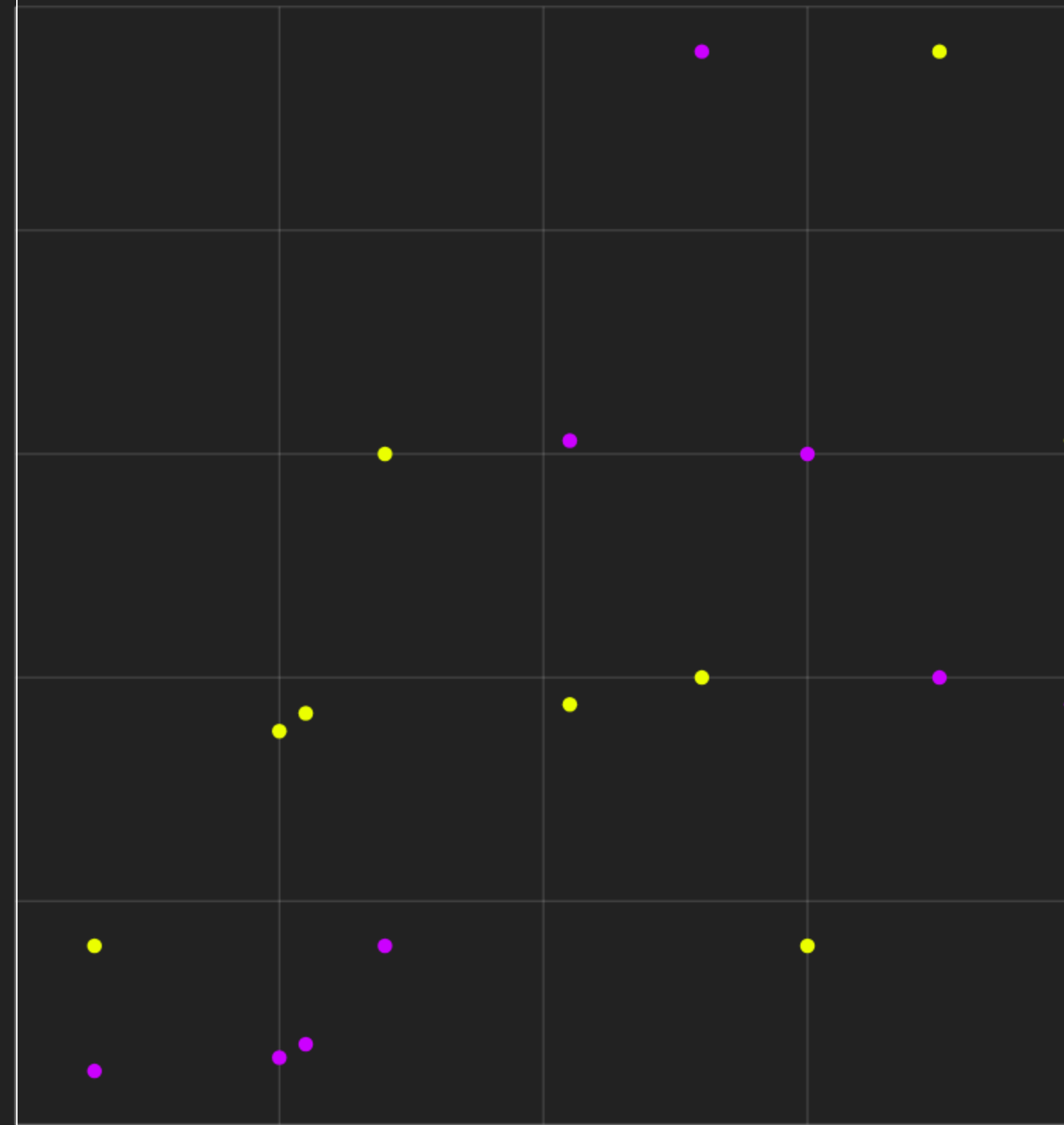
+ 912 contributors



# Clubs

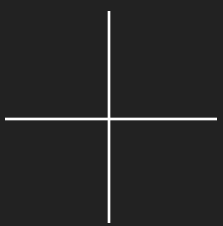
Clubs are usually niche communities in the open-source community where the user base doesn't quite grow at a steady rate, but many of the users present in the community are also contributors. This allows for a community that could be evenly numbered in contributor and user counts.

■ Contributors ■ Users




## Examples of Clubs

clubs usually revolve around niche interests where the projects arose for very specific use-cases or needs.

[illegible]

# Examples of Clubs (cont'd)

clubs usually revolve around niche interests where the projects arose for very specific use-cases or needs.

 **astropy** Public

Sponsor

Watch 139

Fork 1.7k

Star 4.4k

main 24 Branches 160 Tags

Go to file

Code

pllim Merge pull request #16942 from neutrinos/table/bld/hotfix\_buil... 2b34397 · 4 hours ago 37,871 Commits

.circleci	DEP: update minimal recommendation for matplotlib (3.3....	3 months ago
.devcontainer	DOC: Fix broken links from dev docs re-organization	2 months ago
.github	MNT: ignore PTH linting ruleset by subpackage instead of...	yesterday
.pyinstaller	Ruff violation icn001 fix (#15899)	8 months ago
astropy	BLD: fix building against setuptools 68	6 hours ago
cextern	cfitsio: update script for 4.5.0	last week
docs	Merge pull request #16917 from neutrinos/mnt/ignore...	yesterday
examples	DOC: Move FITS example gallery to FAQ	6 months ago
licenses	DEPR: deprecate passing redshift (z) as a keyword argum...	2 months ago
.astropy-root	Don't rely on .git to enable auto-build when importing fro...	9 years ago
.flake8	Move setup.cfg to pyproject.toml (#15247)	last year
.git-blame-ignore-revs	Add f5a1738 to .git-blame-ignore-revs	last year
.gitattributes	Add canonical compressed data from FITS site	last year
.gitignore	DOC: Ignore sphinx-gallery generated file	9 months ago

About

Astronomy and astrophysics core library

[www.astropy.org](http://www.astropy.org)

python science astronomy

astrophysics astropy

Readme

BSD-3-Clause license

Code of conduct

Security policy

Cite this repository

Activity

Custom properties

4.4k stars

139 watching

1.7k forks

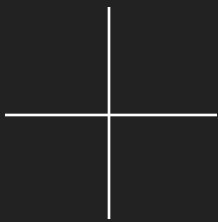
Report repository

Releases 29

v6.1.3 Latest

5 days ago

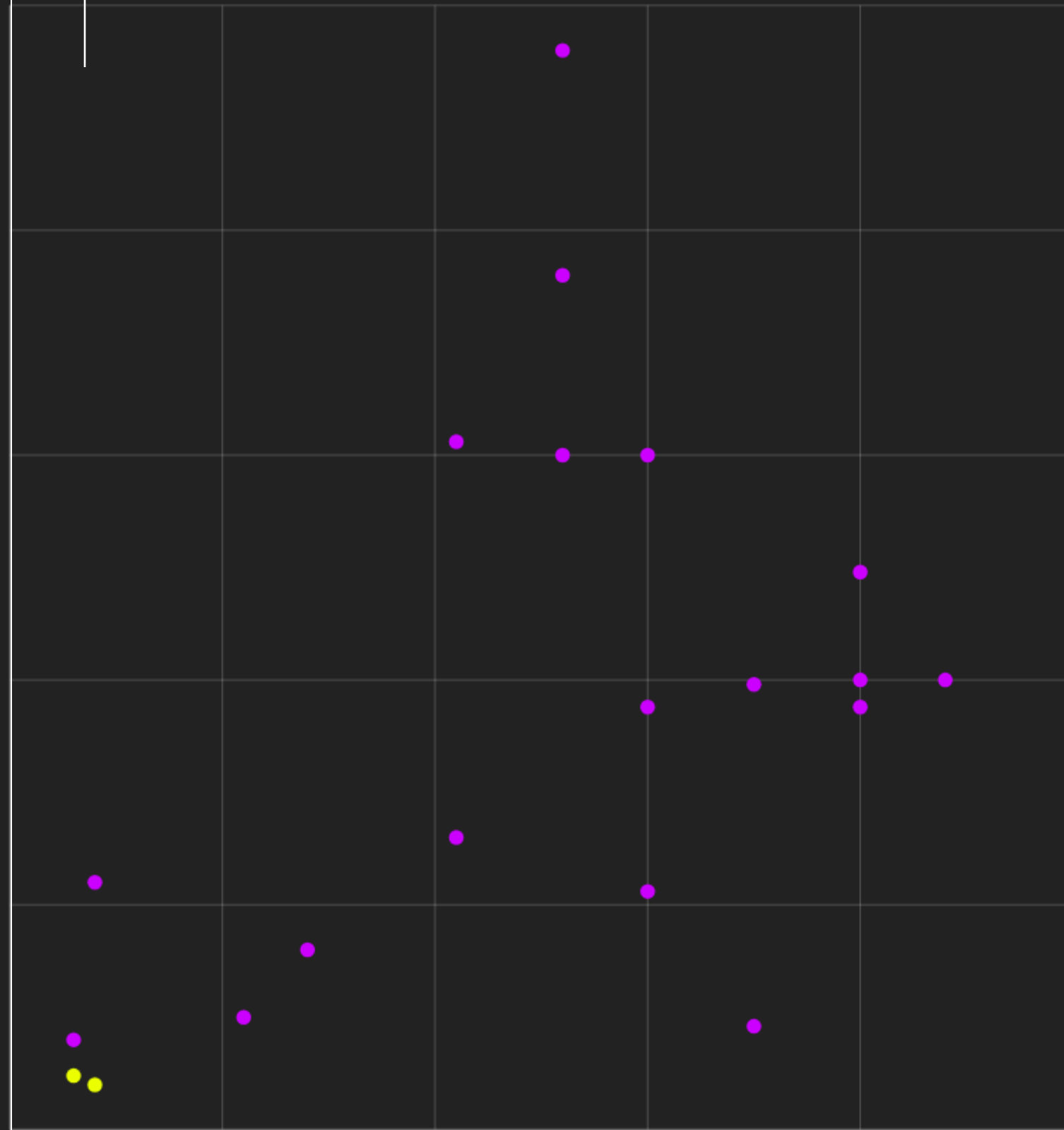
+ 28 releases



# Stadiums

Stadiums are communities that watch/rely on a very small subset of contributors to a project to keep it running, this can be due to a specialization of knowledge or due to the core maintainer working alone on purpose

Contributors Users



# Examples of Stadiums

Stadiums are generally widely-used projects that have a small, core subset of contributors over time.

The user-base generally grows much, much faster.

yara-x

Public

Watch

19

Fork

48

Star

609

main

3 Branches

16 Tags

Go to file

Code

plusvic

docs(cli): fix typo error in command documentation.

✓

b7c7080 · 2 hours ago

🕒 1,568 Commits

📁 .cargo	docs: fix typos.	last week
📁 .github/workflows	feat: add feature for compiling .proto files with protoc (#1...	17 hours ago
📁 capi	feat: expose compiler warnings in Golang and Python APIs.	last week
📁 cli	docs(cli): fix typo error in command documentation.	2 hours ago
📁 docs	docs: fix small error in Module Developer's Guide and refo...	2 weeks ago
📁 fmt	chore: rename yara-x-parser-ng to yara-x-parser	2 months ago
📁 go	feat: expose compiler warnings in Golang and Python APIs.	last week
📁 lib	feat: add feature for compiling .proto files with protoc (#1...	17 hours ago
📁 macros	refactor: large refactoring of how compilation errors are h...	last week
📁 parser	chore: revert rowan to version 0.15.15	last week
📁 proto-yaml	feat: add feature for compiling .proto files with protoc (#1...	17 hours ago
📁 proto	feat: control the name of the feature associated to each Y...	7 months ago
📁 py	chore: change homepage link and add some more metad...	last week
📁 site	feat(cli): implement the --ignore-module option.	4 days ago
📄 .gitattributes	chore: use LF line breaks for *.ir files	2 weeks ago
📄 .gitignore	docs: add project web page (#105)	4 months ago

About

A rewrite of YARA in Rust.

[virustotal.github.io/yara-x/](#)

Readme

BSD-3-Clause license

Activity

Custom properties

609 stars

19 watching

48 forks

Report repository

Releases

5

v0.7.0

Latest

last week

+ 4 releases

Packages

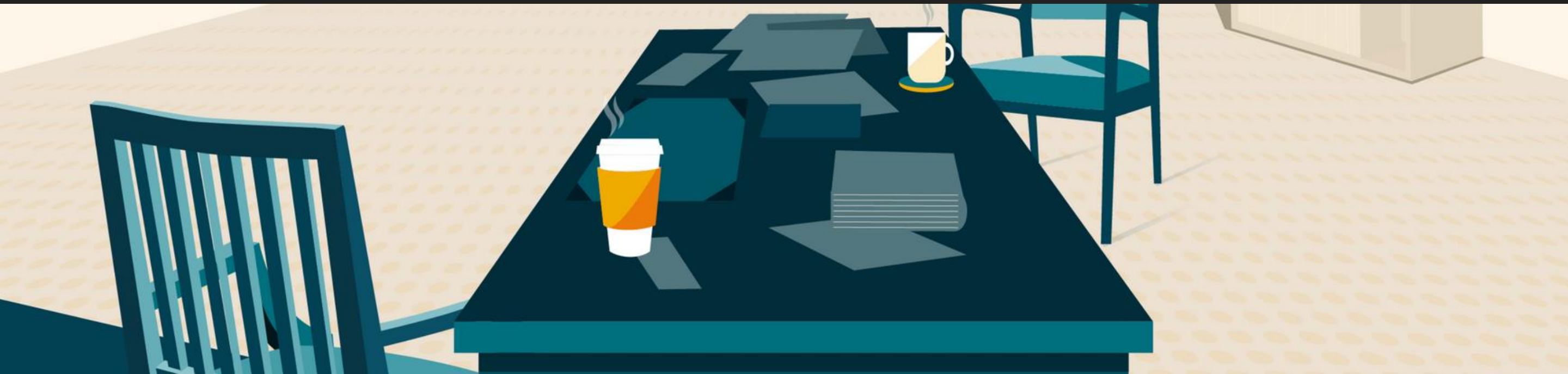
No packages published

Contributors

12



## 03 - Complexity in the community



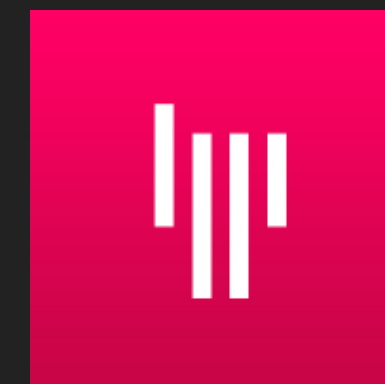
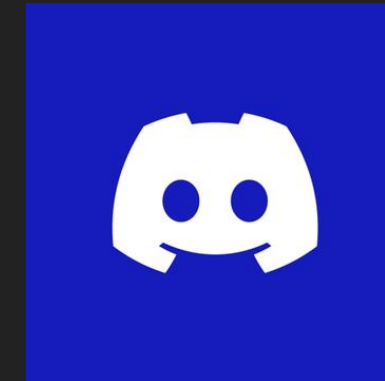
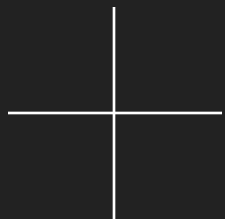
communities grow over time, and it almost always introduces complexity along the way.

- technically complex
- bureaucratically complex
- just complex



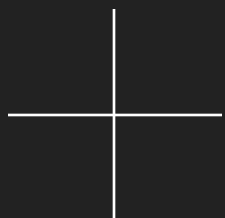
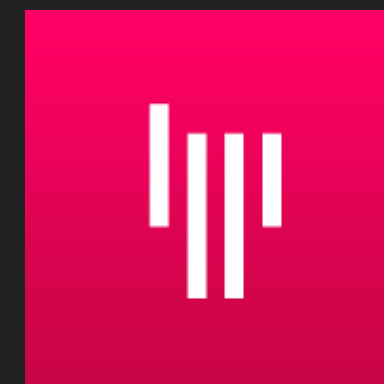
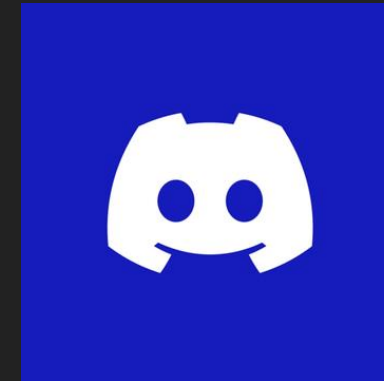
# Communicating in the community

Communicating and reporting issues, bugs, findings, use-cases, etc. is usually where the community first starts to find some complexity



# Communicating in the community (cont'd)

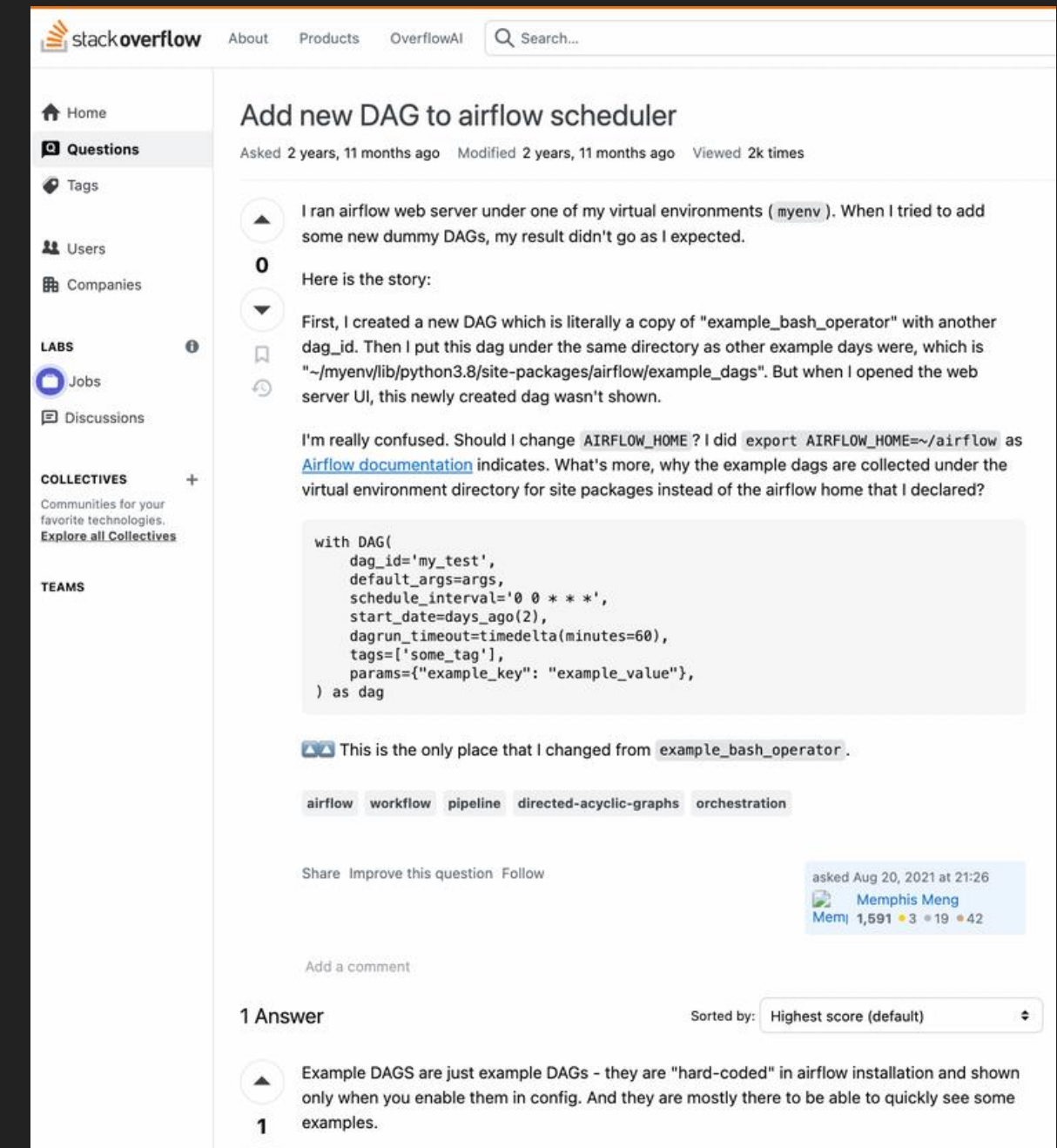
- where do i report this bug?
  - github
- how do i ask questions?
  - discord
  - stackoverflow
- is this expected behavior?
  - post in every channel that exists
    - yes, including that mailing list



# Documentation for the community

Where documentation lies can play a huge role in adoption and use

- do users need to navigate away from the website or repo?
- do users struggle with getting started with the project?



The screenshot shows a Stack Overflow page for a question titled "Add new DAG to airflow scheduler". The question is asked by Memphis Meng on August 20, 2021. The question text describes a user's attempt to add a new DAG to the Airflow scheduler by creating a copy of "example\_bash\_operator" and placing it in a specific directory. The user is confused about why the new DAG is not showing up in the web server UI. The question includes a code snippet for the DAG definition and a list of tags: airflow, workflow, pipeline, directed-acyclic-graphs, and orchestration. There is one answer provided, which states that example DAGs are "hard-coded" in the Airflow installation and are only shown when enabled in the config.

stackoverflow About Products OverflowAI Search...

Home Questions Tags Users Companies LABS Jobs Discussions COLLECTIVES TEAMS

### Add new DAG to airflow scheduler

Asked 2 years, 11 months ago Modified 2 years, 11 months ago Viewed 2k times

I ran airflow web server under one of my virtual environments (myenv). When I tried to add some new dummy DAGs, my result didn't go as I expected.

Here is the story:

First, I created a new DAG which is literally a copy of "example\_bash\_operator" with another dag\_id. Then I put this dag under the same directory as other example dags were, which is "~/myenv/lib/python3.8/site-packages/airflow/example\_dags". But when I opened the web server UI, this newly created dag wasn't shown.

I'm really confused. Should I change AIRFLOW\_HOME? I did export AIRFLOW\_HOME=~/.airflow as [Airflow documentation](#) indicates. What's more, why the example dags are collected under the virtual environment directory for site packages instead of the airflow home that I declared?

```
with DAG(
    dag_id='my_test',
    default_args=args,
    schedule_interval='0 0 * * *',
    start_date=days_ago(2),
    dagrun_timeout=timedelta(minutes=60),
    tags=['some_tag'],
    params={"example_key": "example_value"},
) as dag
```

This is the only place that I changed from example\_bash\_operator.

airflow workflow pipeline directed-acyclic-graphs orchestration

Share Improve this question Follow

asked Aug 20, 2021 at 21:26  
Memphis Meng  
1,591 3 19 42

Add a comment

1 Answer Sorted by: Highest score (default)

Example DAGS are just example DAGS - they are "hard-coded" in airflow installation and shown only when you enable them in config. And they are mostly there to be able to quickly see some examples.

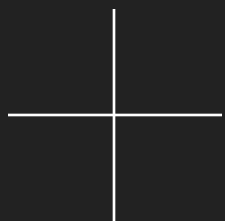
# Contributing to the community

Contributing can get messy at times

- resources exist to learn how to contribute, where to contribute, why to contribute, etc.
- It can be intimidating but it is not impossible

## Open Source Friday

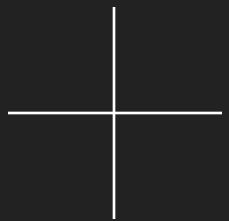
Open source is made by people just like you. This Friday, invest a few hours contributing to the software you use and love.





Does the community actually have a say?

The community doesn't always know what's best, or does it?



# Does the community actually have a say?

examples of this:

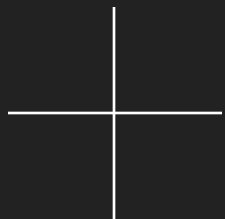
- license changes by the supporting org
- legal changes
- features/priorities against the status quo

▲ Rust Is Dead to Me (gavinhoward.com)

54 points by stargrave on April 12, 2023 | hide | past | favorite | 84 comments

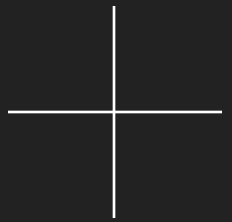
▲ echelon on April 12, 2023 | next [-]

The Rust Foundation is absolute bonkers and they don't deserve stewardship of the language.

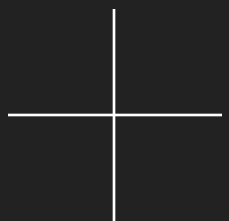
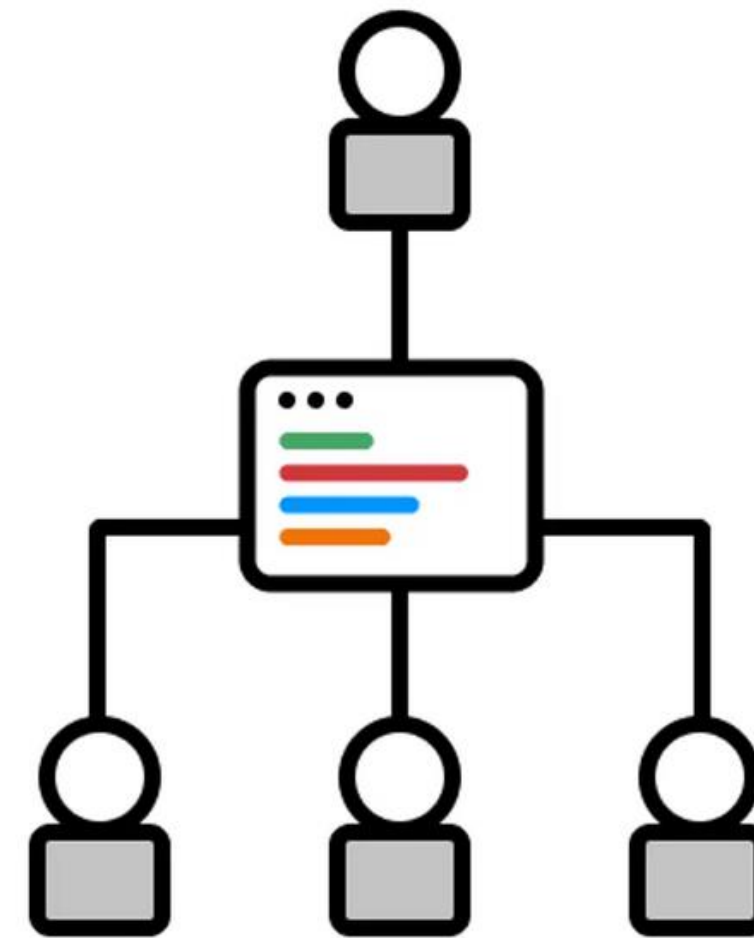
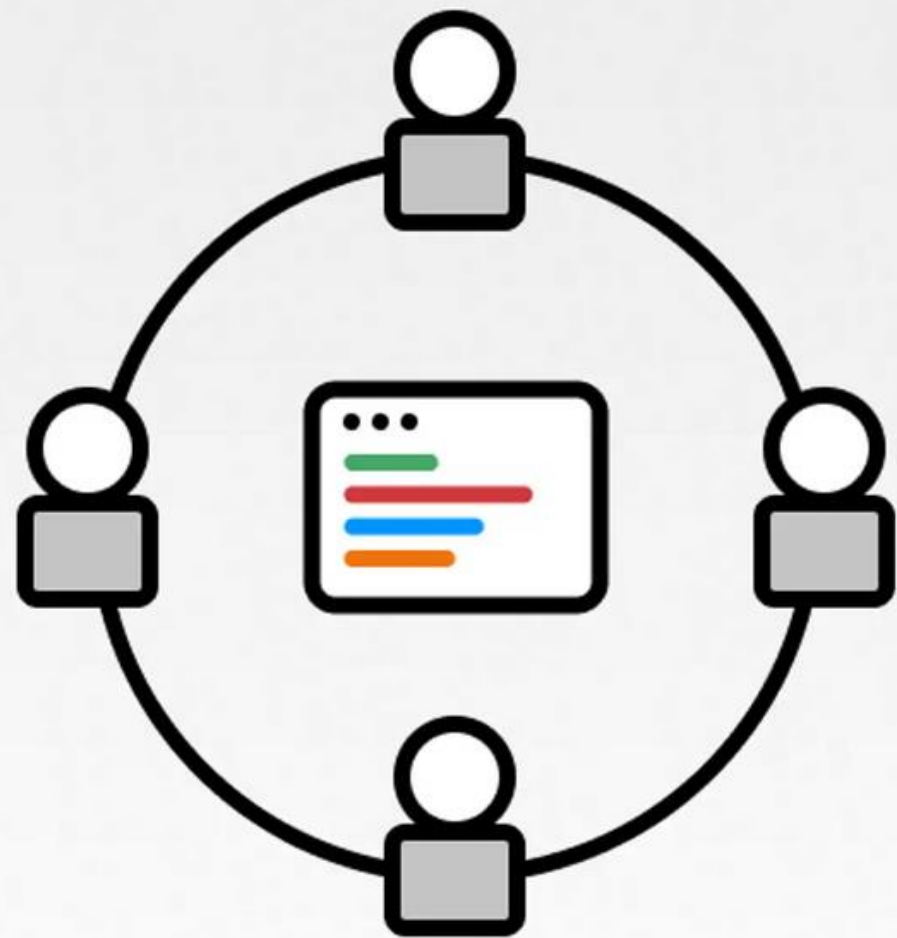




Who is this?



# Benevolent Dictator for Life (BDFL) Model



# Benevolent Dictator for Life Model

maybe

## Is BDFL a death sentence?

What happens when a Benevolent Dictator For Life moves on from an open source project?

### [python-committers] Transfer of power

Guido van Rossum | Thu, 12 Jul 2018 07:59:19 -0700

Now that PEP 572 is done, I don't ever want to have to fight so hard for a PEP and find that so many people despise my decisions.

I would like to remove myself entirely from the decision process. I'll still be there for a while as an ordinary core dev, and I'll still be available to mentor people -- possibly more available. But I'm basically giving myself a permanent vacation from being BDFL, and you all will be on your own.

no

yes



## PEP 572 – Assignment Expressions

**Author:** Chris Angelico <rosuav at gmail.com>, Tim Peters <tim.peters at gmail.com>, Guido van Rossum <guido at python.org>

**Status:** Final

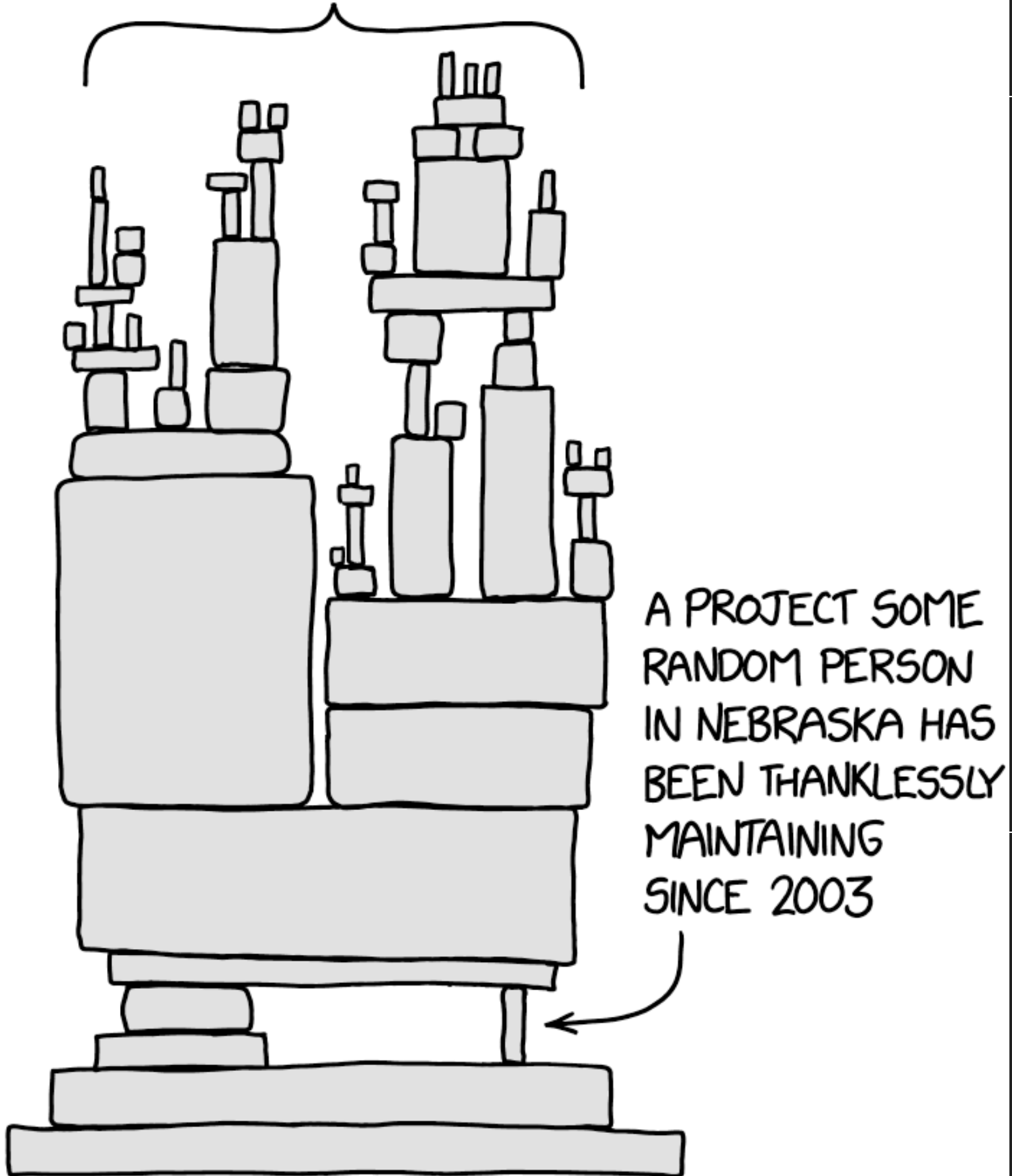
**Type:** Standards Track

**Created:** 28-Feb-2018

**Python-Version:** 3.8

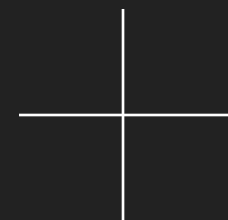
**Post-History:** 28-Feb-2018, 02-Mar-2018, 23-Mar-2018, 04-Apr-2018, 17-Apr-2018, 25-Apr-2018, 09-Jul-2018, 05-Aug-2019

ALL MODERN DIGITAL  
INFRASTRUCTURE



## 04 - Leveraging open-source

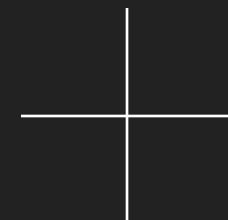
You plan to leverage some open-source technology? Do you know what you could possibly encounter?





## The security aspect

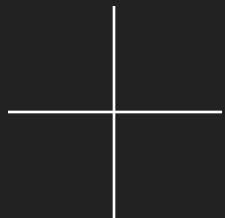
There's quite a few security aspects you need to consider with open-source. Open-source may have more eyes on the code base, but it doesn't mean it's inherently more secure.



vulnerabilities and mistakes happen in all software

# The security aspect

When you pull in an open-source library for your next project, are you really gonna read every single line of source code? any of it?



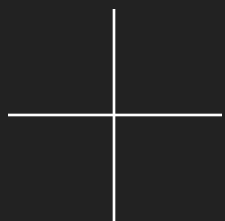
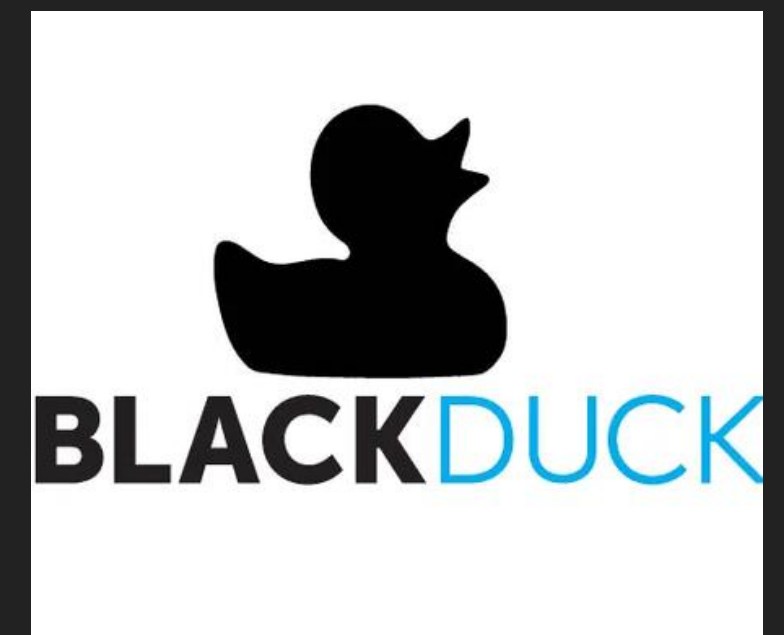
# The security aspect

There are things that can help with this:

- Snyc
- BlackDuck
- etc.

Do we trust these results?

- most of these are just CVE reports after the fact



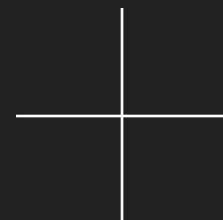




## The legal and compliance aspect

If you're using these projects for non-commercial or personal use, it's pretty easy.

What happens with these things make it into a product? Is it used to create a commercial product? Are you aware of the licenses used/accepted?

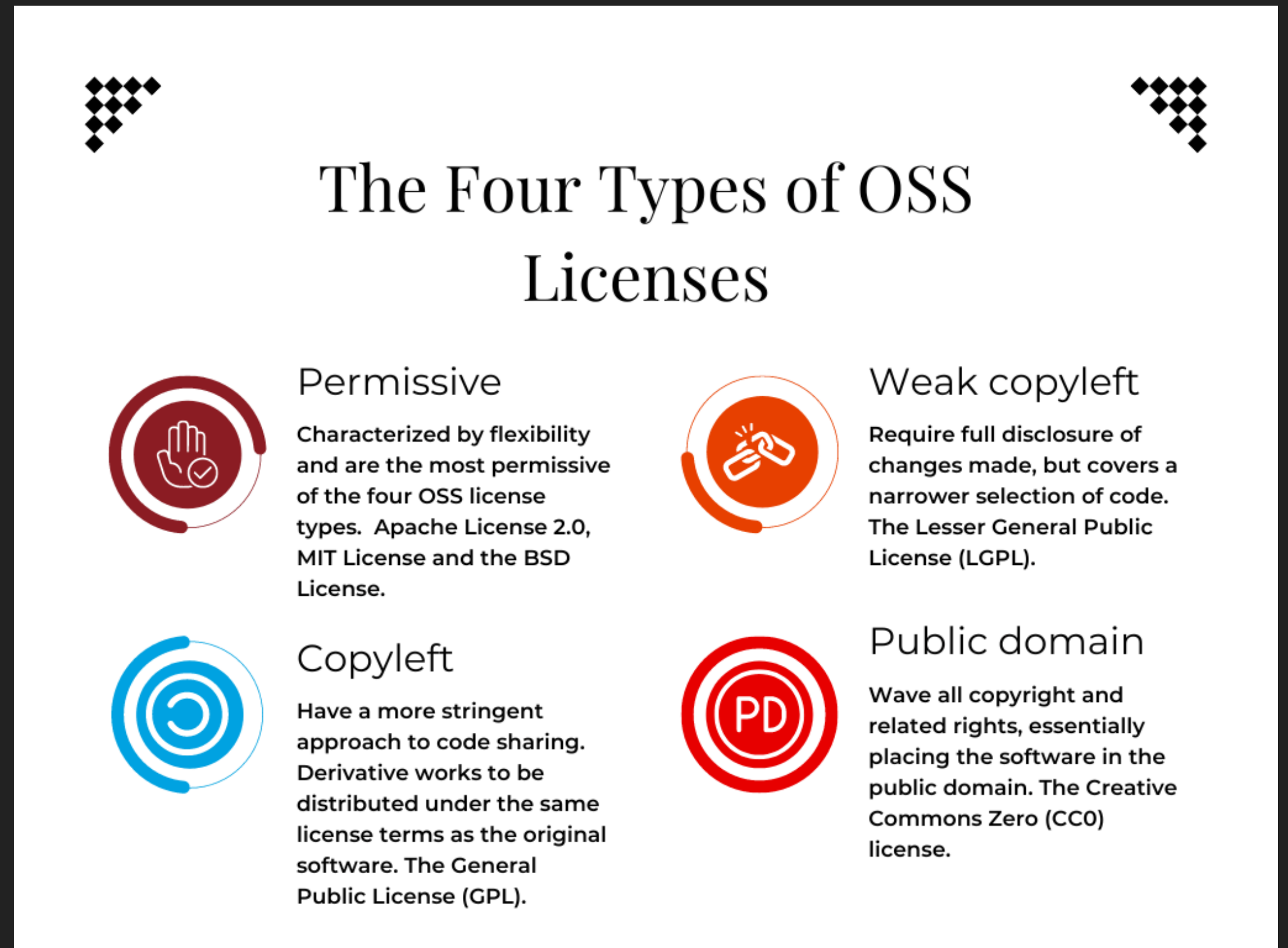


is there any risk from using OSS in my product?

# The legal and compliance aspect

licenses galore

- tools can help here

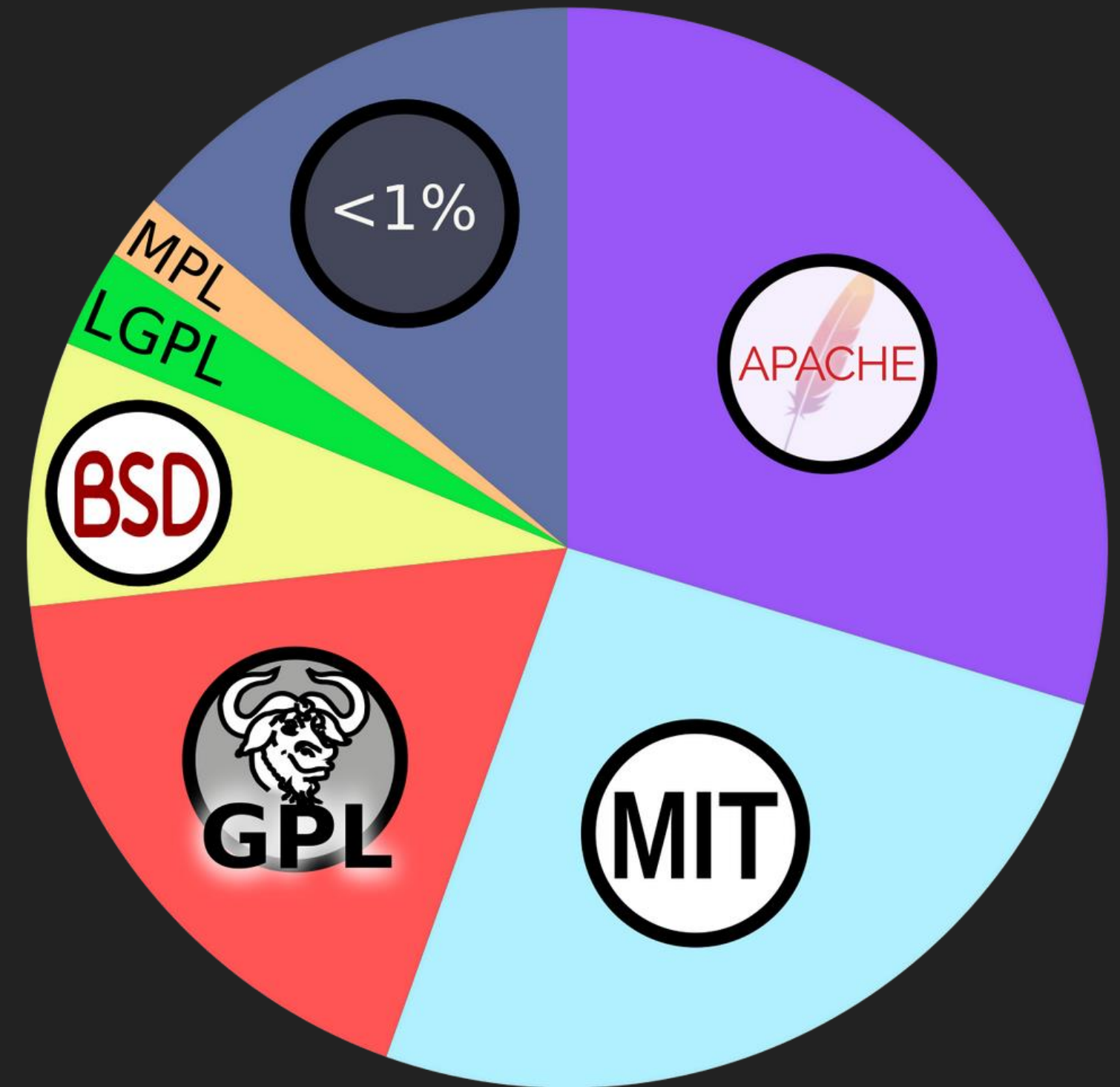


# Diving into the licenses...

There's at least 3 of them:

- GPL
- Beerware
- WTFPL

```
/*
 * -----
 * "THE BEER-WARE LICENSE" (Revision 42):
 * <phk@FreeBSD.ORG> wrote this file.  As long as you retain
 * this notice you
 * can do whatever you want with this stuff.  If we meet some
 * day, and you think
 * this stuff is worth it, you can buy me a beer in return.
 * Poul-Henning Kamp
 * -----
 */
```





## The maintenance aspect

maybe you've found a project your company can use both legally and the security risks have been accepted: how do you make sure it remains supported for years to come?

if it becomes abandoned, are you or your company prepared to support it?

why did they stop developing that project? why was it archived?

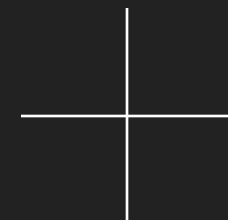




## The longevity aspect

some open-source projects have been around a while, some are fresh and new

do we inherently trust older projects more?

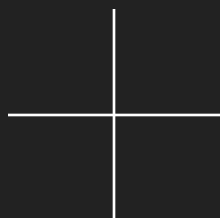


this project is only a few weeks old...

who knows what CVE this is?

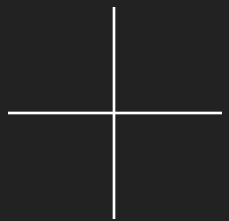
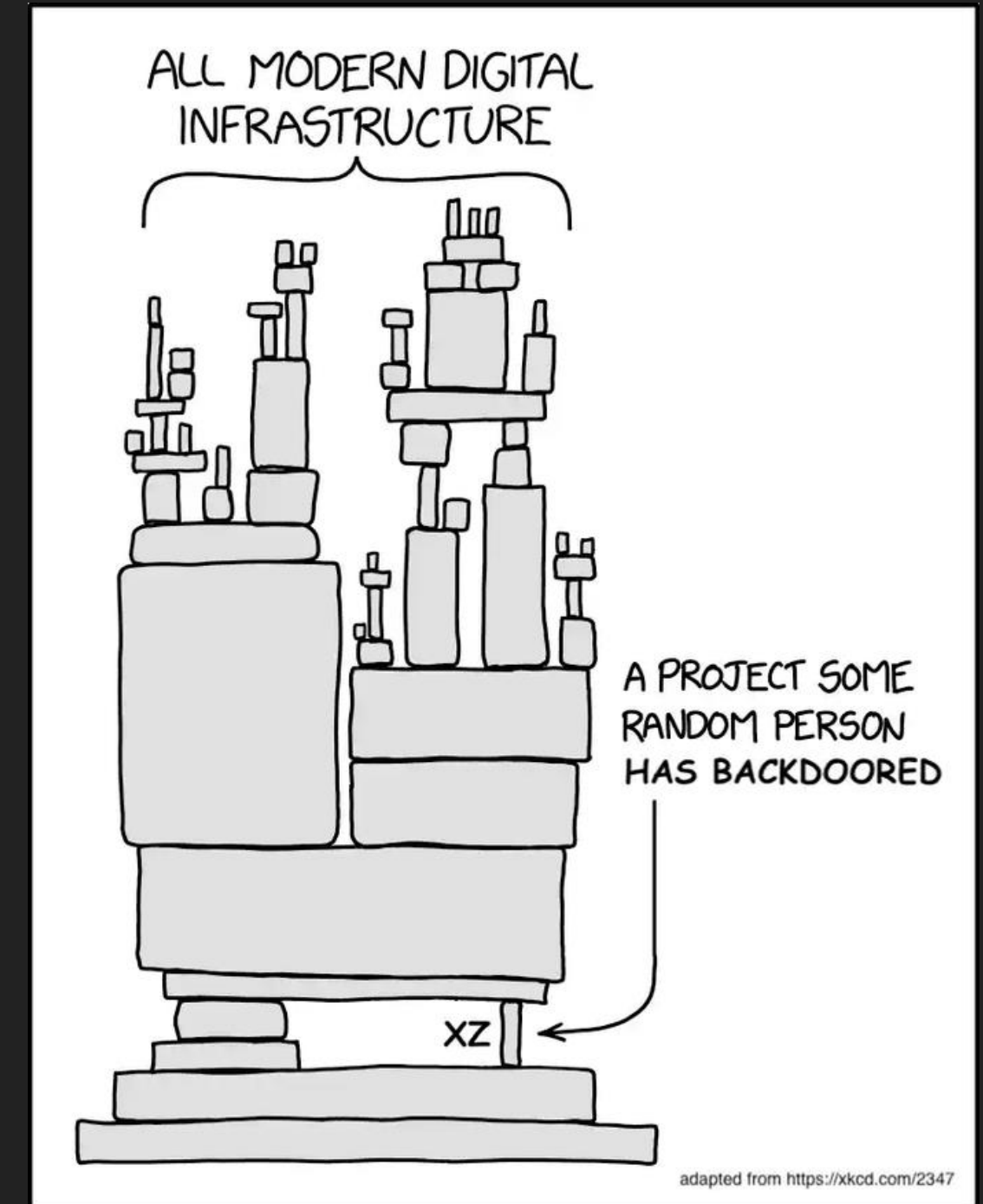
---

CVE-2024-3094



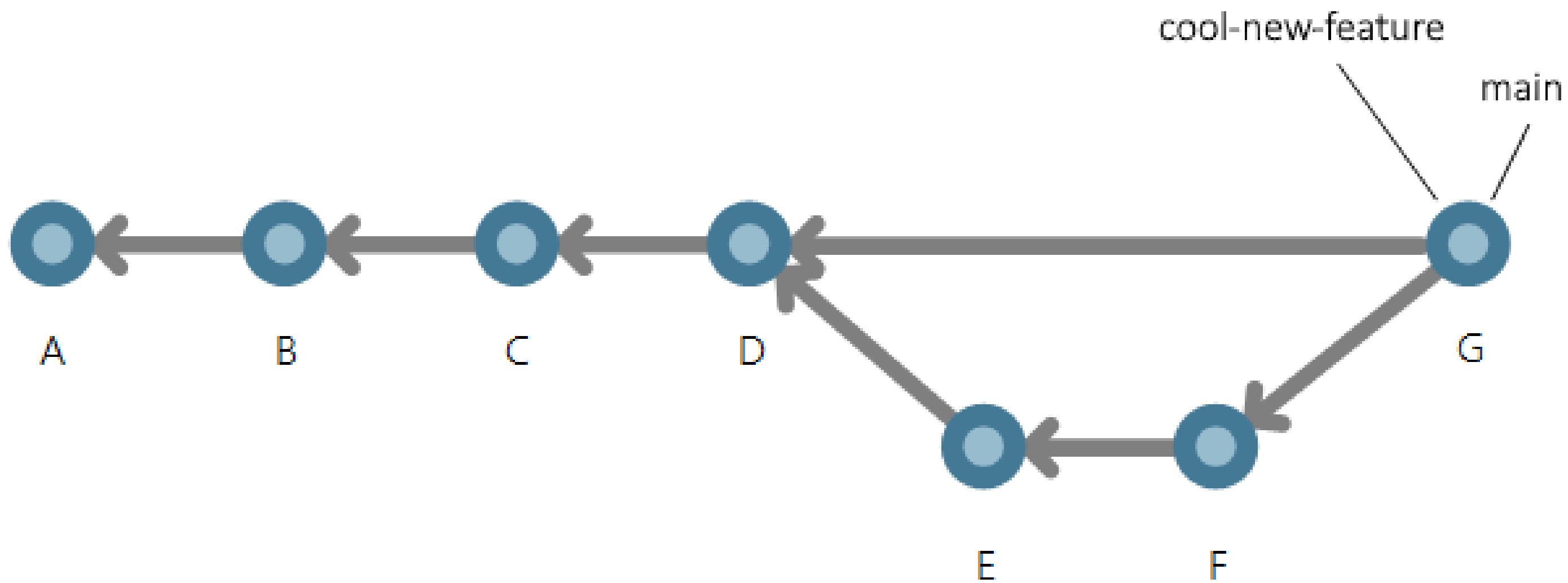
# xz vulnerability

jia tan took advantage of everyone's trust for a well established, long existing open-source project and repository

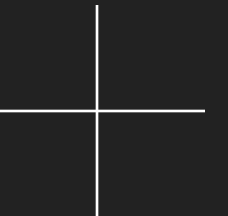


## 05 - Contributing to open-source

why contribute?



because you should!

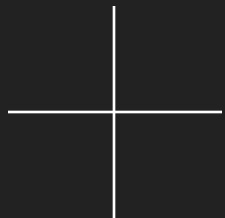




# Contribution Guidelines

---

- `contributing.md`
  - Look for it in the repo
- If there isn't one, you can still contribute
  - Try to match the style guide already in the code base
  - Don't reformat the entire codebase just for your PR



# Contribution Guidelines

target / strelka

<> Code

Issues 8

Pull requests 7

Discussions

Actions

Projects

Security

Insights

master

strelka / CONTRIBUTING.md

Go to file

t

ryanohoro

Update CONTRIBUTING.md with style automation, development environment

6b290f5 · last year

189 lines (150 loc) · 6.5 KB

Preview

Code

Blame

Raw

Contributing to Strelka

Thank you so much for your interest in contributing to Strelka! This document contains guidelines to follow when contributing to the project.

Code of Conduct

# Contributing via Code

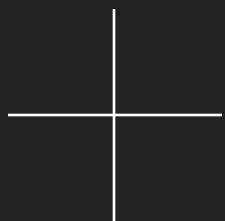
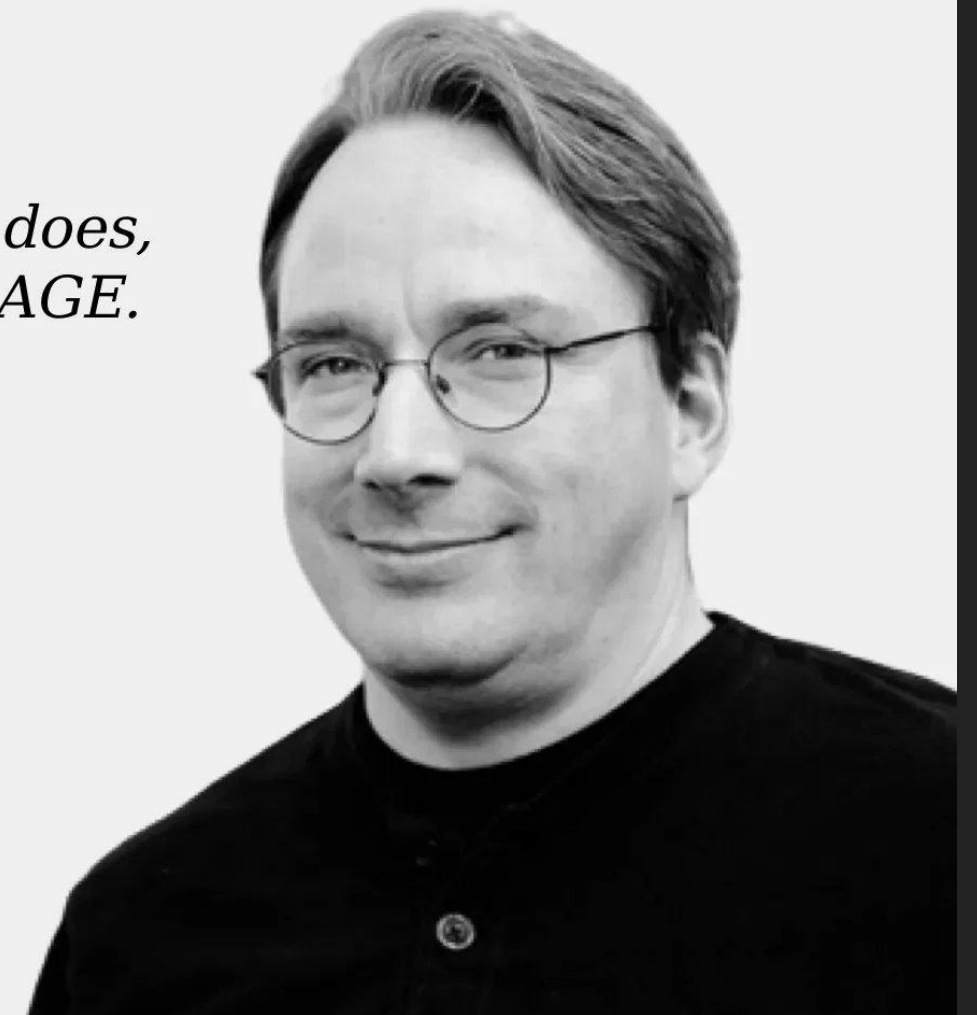
What do contributions look like?

- Doc fixes (typos or new/better documentation)
- Bug fixes
- New features

*You copied that function without understanding why it does what it does, and as a result your code IS GARBAGE.*

*AGAIN.*

*- Linus Torvalds*



# Funding Guidelines

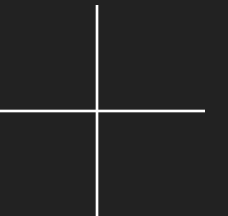
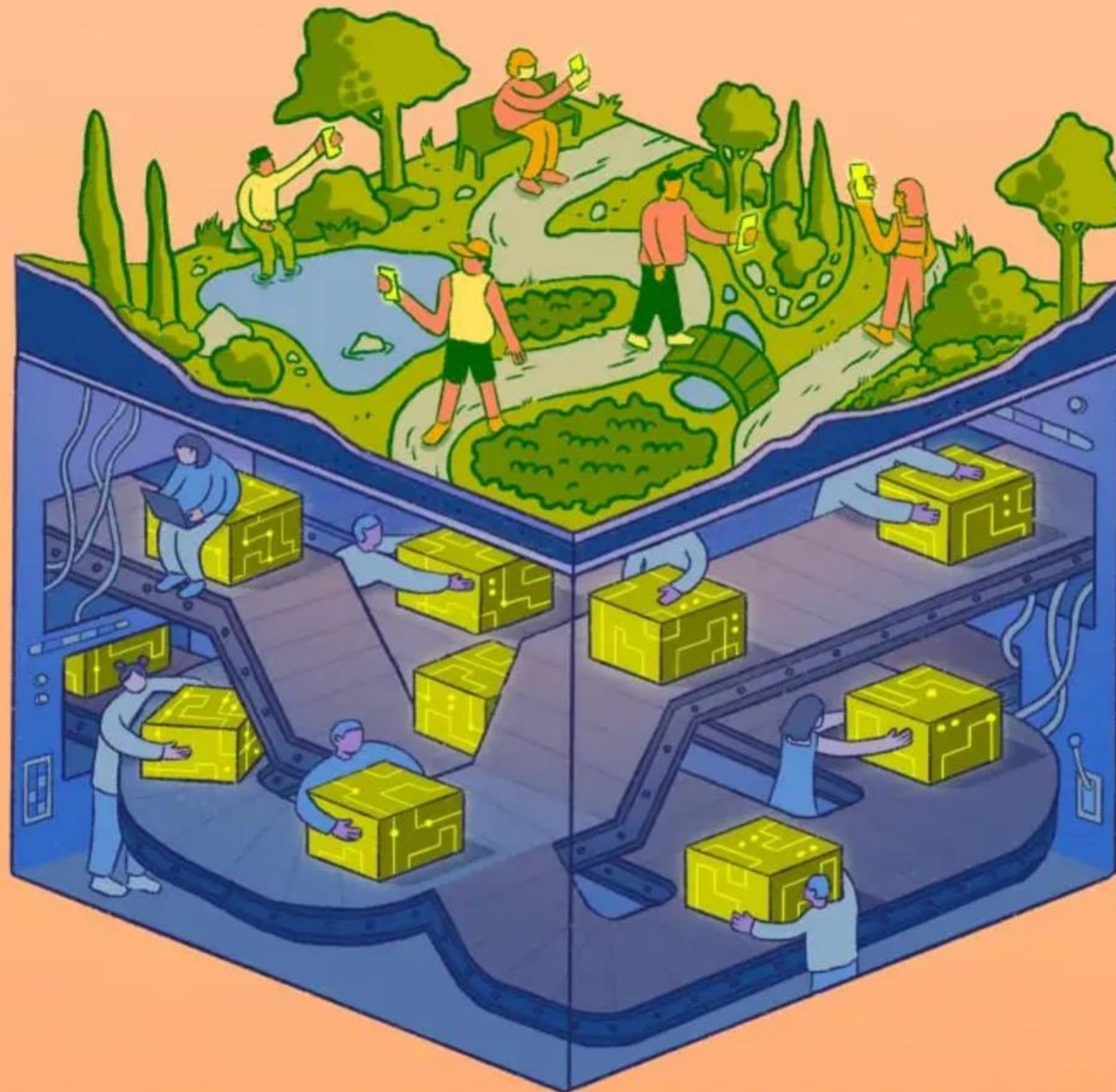
---

- Funded purely via community support
- Funded via organization donations
- Support does not always need to be monetary
  - Helping document issues
  - Answering those beginner questions
  - Letting the developers develop





## 06 - Modern open-source projects



# Server Side Public License

- based on AGPL
- NOT considered open-source by the open source initiative
  - why is this?
- drama, mostly



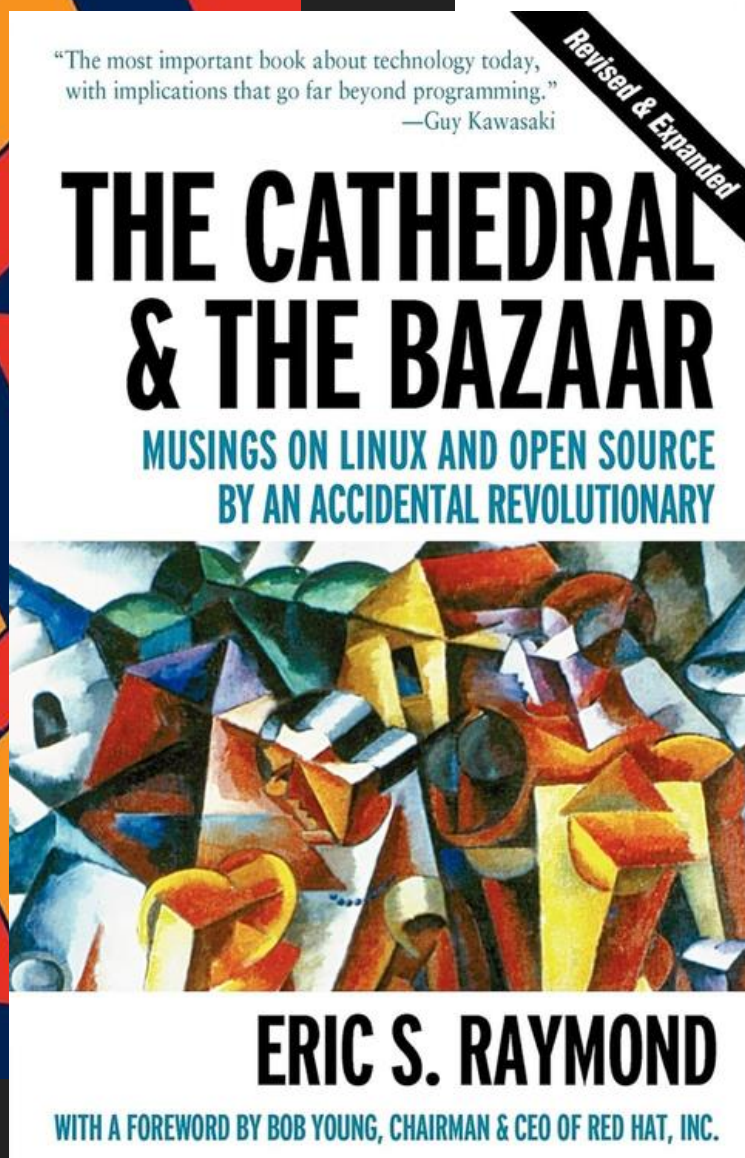
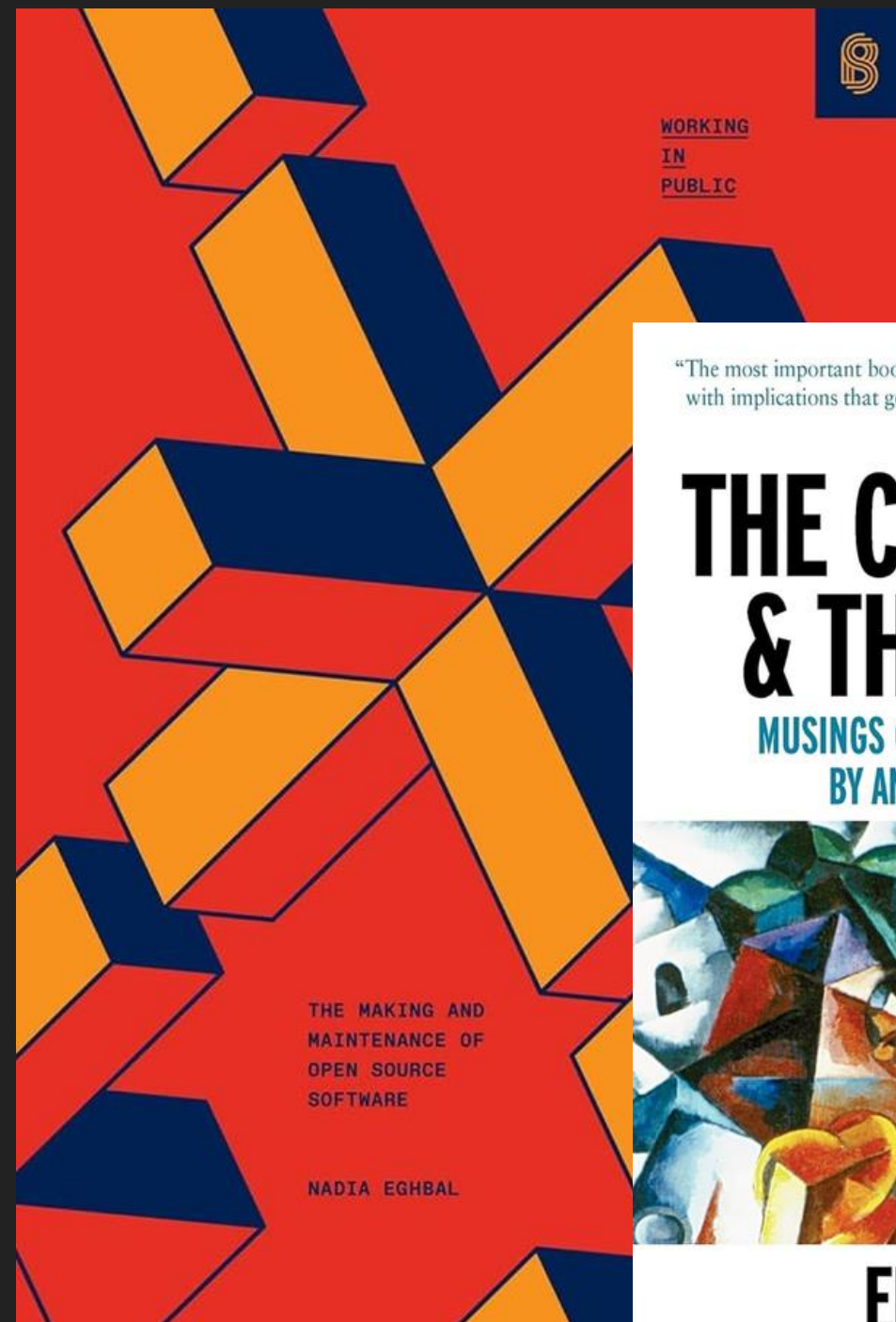
# Why does SSPL actually matter?

- Prohibitive
- Control
- Competition





# Dive Deep into Open Source



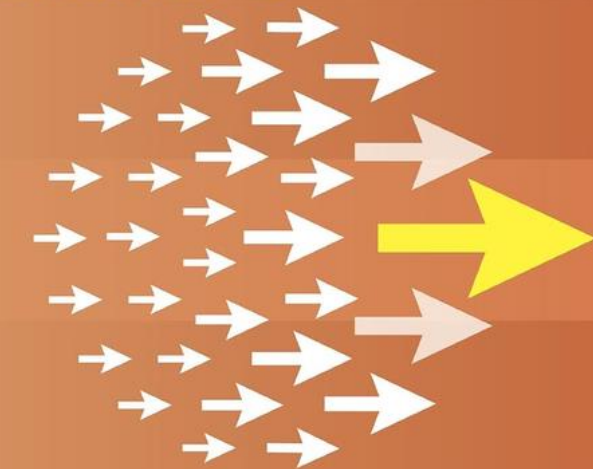
Free Software, Free Society:  
Selected Essays of Richard M. Stallman



Introduction by Lawrence Lessig  
Edited by Joshua Gay

producing  
open source  
software

Karl Fogel



HOW TO RUN A SUCCESSFUL FREE SOFTWARE PROJECT

O'REILLY®

# 0x00

Jacob Latonis

