

*The Unbearable  
Vulnerability of  
Open Source*

**Hello!**  
**I'm Eileen M.**  
**Uchitelle**



**You can find  
me online  
@eileencodes**



I'm a *Systems*  
Engineer @  
**GitHub**



I'm on the



Core Team




*The Unbearable  
Vulnerability of  
Open Source*

What is  
*vulnerability*?

2012

My first PR


 **gerrit / radiant-sibling\_tags-extension**  
forked from nelstrom/radiant-sibling-tags-extension Watch 1

[Code](#) [Pull requests 0](#) [Projects 0](#) [Insights](#)



## Update README.md #1



**Closed** eileencodes wants to merge 1 commit into `gerrit:gerrit` from `eileencodes:patch-1`

[Conversation 0](#) [Commits 1](#) [Files changed 1](#)

 eileencodes commented on Aug 30, 2012

Fixed type in the name of the gem was radiant-sibling-tags-extension, but should be radiant-sibling\_tags-extension

  Update README.md ... 843bdba

  eileencodes closed this on Nov 6, 2014



2013

My first  
accepted PR


MiniProfiler / rack-mini-profiler Watch 54

[Code](#) [Issues 42](#) [Pull requests 3](#) [Projects 0](#) [Insights](#)

## Remove rendering whitespace, issue 12 #15

**Merged** SamSaffron merged 1 commit into MiniProfiler:master from eileencodes:remove-rendering-whitespace on Oct 2

[Conversation 1](#) [Commits 1](#) [Files changed 1](#)

 eileencodes commented on Oct 21, 2013 Contributor

The profile\_handler js file had a unicode character, U+FEFF, which is ZERO WIDTH NO-BREAK SPACE. It represents UTF-16 and not UTF-8. This unicode character is deprecated and causes the issues seen where there is annoying whitespace above the script when it is appended to the body by Rack::Response.

reference: [http://en.wikipedia.org/wiki/Byte\\_order\\_mark](http://en.wikipedia.org/wiki/Byte_order_mark)

# 2014

## My first Rails PR

The screenshot shows a GitHub pull request for the Rails project. The title is "Fix delete all to not produce sql in statement #14546". It is marked as "Merged" and was merged by "tenderlove" on March 31, 2014. The pull request includes 3 commits and 3 files changed. A comment from the owner, "eileencodes", is visible, describing the issue with SQL production during a delete\_all operation and providing the corrected SQL query.

rails / rails

Watch 2,459 Star 36,934 Fork 15,102

Code Issues 424 Pull requests 728 Projects 0 Insights

### Fix delete all to not produce sql in statement #14546

New Issue

Merged tenderlove merged 3 commits into rails:master from eileencodes:fix\_delete\_all\_to\_not\_use\_IN\_statement on Mar 31, 2014

Conversation 15 Commits 3 Files changed 3 +23 -2

eileencodes commented on Mar 31, 2014 Owner

When delete\_all is run on a CollectionProxy and has a dependency of delete\_all the SQL that is produced has an IN statement.

```
DELETE FROM associated_model where associated_model . parent_id = 1 AND associated_model . id IN (1, 2, 3...)
```

This is only happening if the association is not loaded — both loaded and non-loaded delete\_all should behave the same. This is a problem when it comes to deleting many records because the query becomes very slow. Instead the SQL produced should be:

```
DELETE FROM associated_model where associated_model . parent_model_id =1
```

I fixed this by making sure the check for loaded and destroy also makes sure that the dependent is not delete\_all, so the conditional goes to the else and deletes the records directly without the IN statement.

Thanks to @tenderlove for pairing with me to figure out exactly what was causing this issue

Reviewers: No reviews

Assignees: No one assigned

Labels: None yet

Projects: None yet

Milestone: No milestone





# 2016

# System Tests

The screenshot shows a GitHub pull request page for the Rails repository. The title is "WIP: Capybara Integration with Rails (AKA System Tests) #26703". It is a merged pull request from the "eileencodes" branch to the "rails:master" branch, merged on February 20. The pull request has 156 conversations, 37 commits, and 35 files changed. A comment from the owner, eileencodes, dated October 4, 2016, provides an update on the PR's progress and goals. The comment includes a list of reviewers: jnicklas, matthewd, dhh, fnando, twalpole, rafaelfranca, bf4, kaspth, jonathanhefner, maclover7, and alexcameron89.

rails / rails

Watch 2,459 Star 36,934 Fork 15,102

Code Issues 424 Pull requests 728 Projects 0 Insights

## WIP: Capybara Integration with Rails (AKA System Tests) #26703

New Issue

Merged eileencodes merged 37 commits into rails:master from eileencodes:rails\_system\_tests on Feb 20

Conversation 156 Commits 37 Files changed 35 +686 -5

eileencodes commented on Oct 4, 2016 • edited Owner

Update: This PR changed a lot over the course of being open. Please refer to the documentation or code in master / 5-1-stable to use system tests

I'm really excited to open this initial PR for bringing system/acceptance test support to Rails through Capybara.

The goal of this PR is for Rails to take on all the setup that is needed in applications to allow Capybara and make system testing default in Rails applications.

**Why is the name Rails::SystemTestCase?**

~~I chose this name because this was the name DHH indicated he preferred in the Rails' Basecamp long ago. I'm totally open to changing the name but ultimately decided to put it in ActiveSupport with the Rails namespace so I could get onto writing code and stop worrying about the name 😊~~

The test framework has been moved to its own gem under the Rails name and is now ActionSystemTest

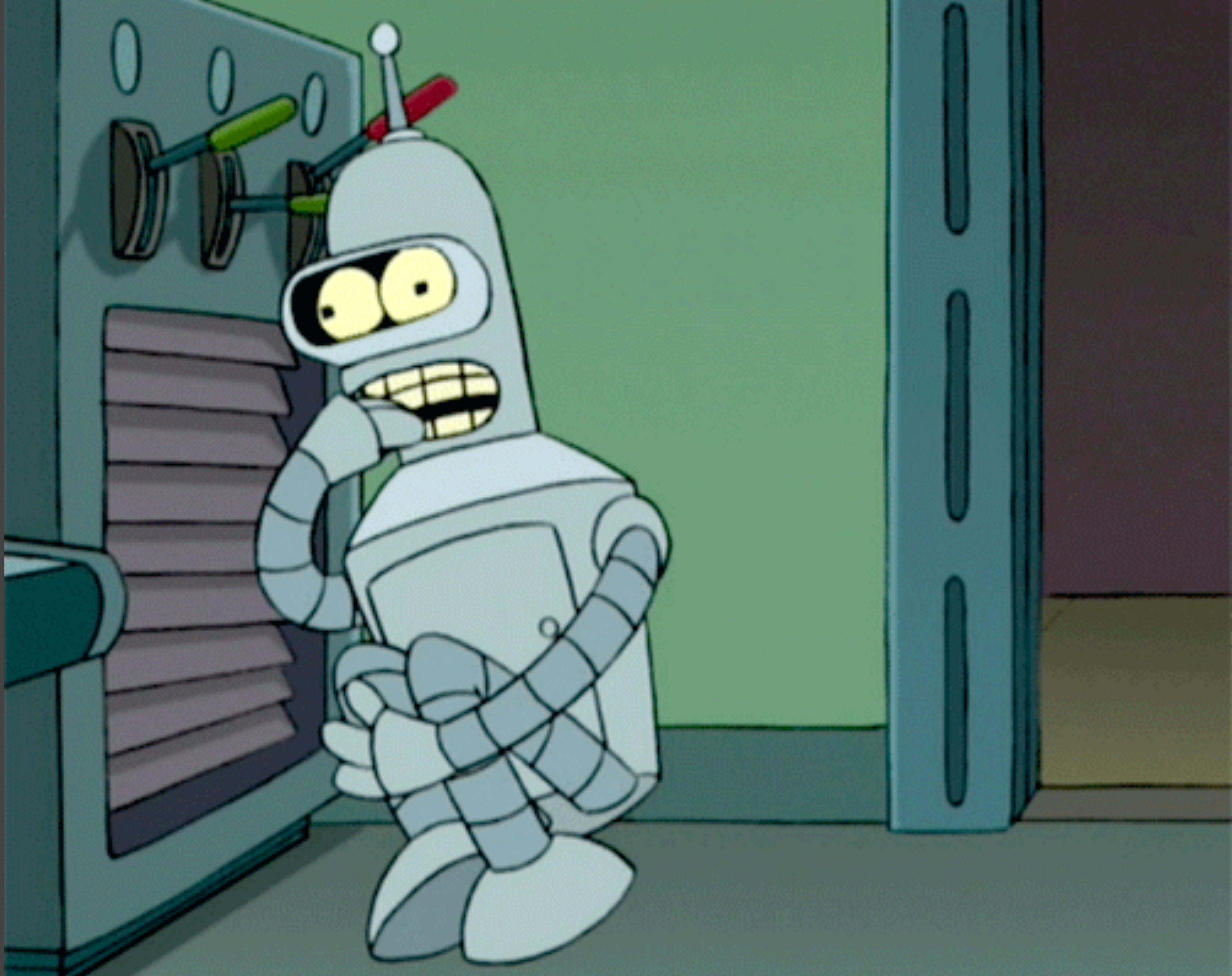
Reviewers

- jnicklas
- matthewd
- dhh
- fnando
- twalpole
- rafaelfranca
- bf4
- kaspth
- jonathanhefner
- maclover7
- alexcameron89

ORBO



PUSH



**If contributing to**



If contributing to  
*open source* was only

If contributing to  
*open source* was only  
about *writing code*

If contributing to  
*open source* was only  
about *writing code*  
it would be *easy*

*Open Source* is really

*Open Source* is really  
about *people*

And *people*

And *people*  
make us feel *vulnerable*

[NEWS](#)[GEMS](#)[GUIDES](#)[CONTRIBUTE](#)[SIGN IN](#)[SIGN UP](#)

# arya *0.0.1*

Arya is a gem that provides you with pictures of the best dog ever. You can find her at [@aryadog](#) on twitter.

## VERSIONS:

**0.0.1** - Sept 13, 2017 (249 KB)

[Show all versions \(70 total\) →](#)

## DEVELOPMENT DEPENDENCIES (4):

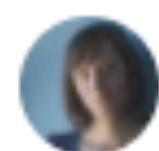
**minitest** ~> 5.0

**rake** >= 0

## AUTHORS:

Eileen Uchitelle

## OWNERS:




## TOTAL DOWNLOADS

**0**

## FOR THIS VERSION

**0**

## GEMFILE:

```
gem 'arya', '~> 0.0' 
```

## INSTALL:

```
gem install arya 
```

## LICENSE:

**MIT**





Search Gems...



NEWS

GEMS

GUIDES

CONTRIBUTE

SIGN IN

SIGN UP

# arya *0.0.1*

Arya is a gem that provides you with pictures of the best dog ever. You can find her at @aryadog on twitter.



## VERSIONS:

**0.0.1** - Sept 13, 2017 (249 KB)

[Show all versions \(70 total\) →](#)

## DEVELOPMENT DEPENDENCIES (4):

**minitest** ~> 5.0

**rake** >= 0

## TOTAL DOWNLOADS

**0**

## FOR THIS VERSION

**0**

## GEMFILE:

```
gem 'arya', '~> 0.0
```



## INSTALL:

```
gem install arya
```



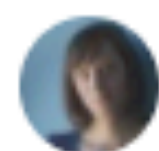
## LICENSE:

**MIT**

## AUTHORS:

Eileen Uchitelle

## OWNERS:



Filters ▾   🔍 is:pr is:open

Labels   Milestones

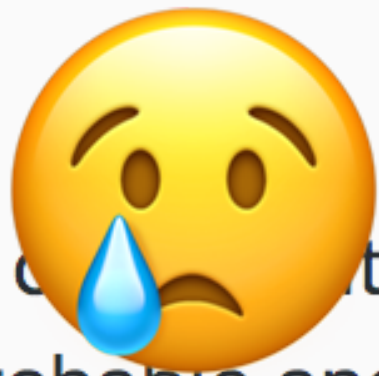
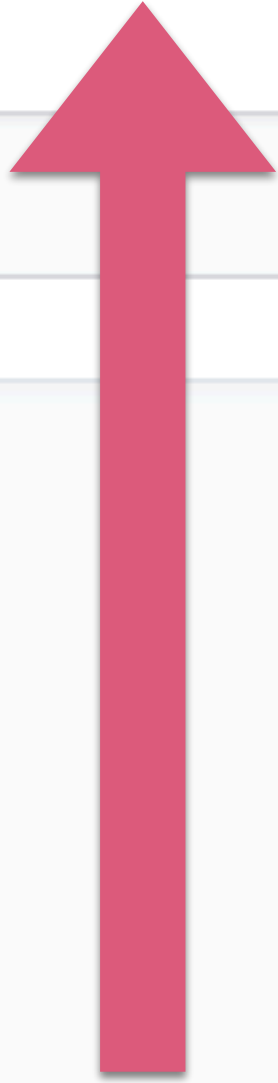
[New pull request](#)



## Welcome to Pull Requests!

Pull requests help you collaborate on code with other people. As pull requests are created, they'll appear here in a searchable and filterable list. To get started, you should [create a pull request](#).

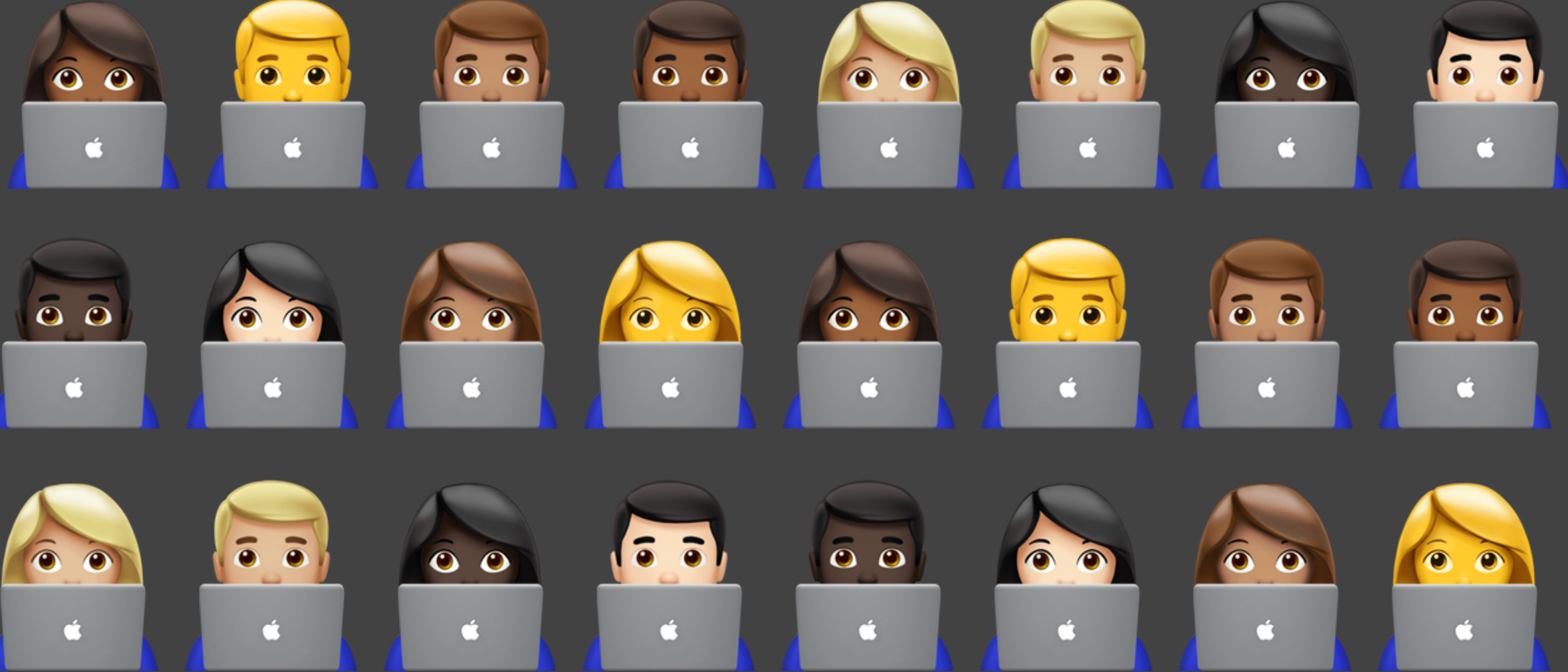
💡 **ProTip!** Filter pull requests by the default branch with [base:master](#)



### Welcome to Pull Requests!

Pull requests help you collaborate on code with other people. As pull requests are created, they'll appear here in a searchable and filterable list. To get started, you should [create a pull request](#).

**ProTip!** Filter pull requests by the default branch with [base:master](#)



*Deterrents* can  
make contributors  
feel *vulnerable*

# Dismissing Concerns



**“This code  
sucks”**





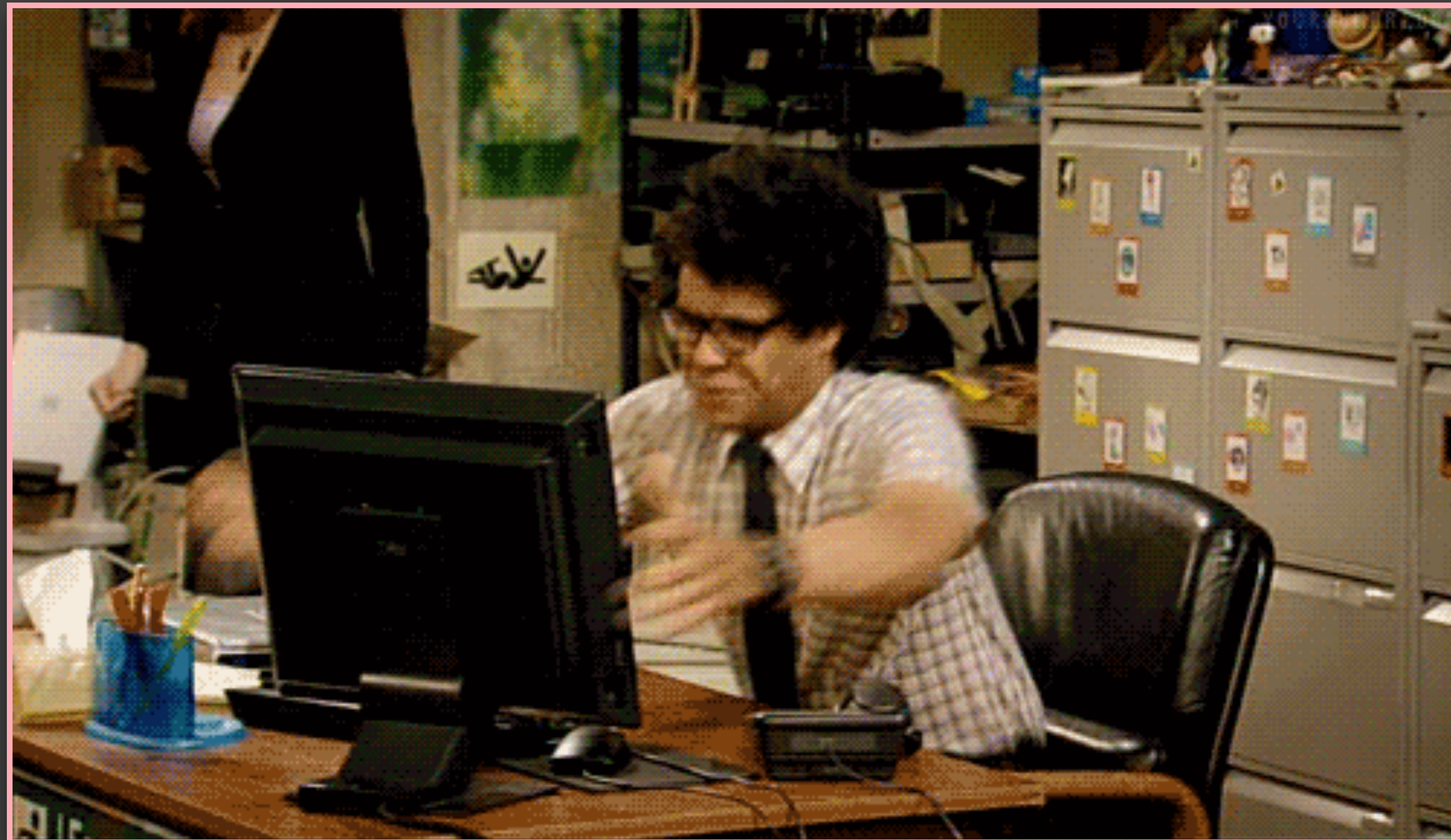
*Nadia Odunayo*

@nodunayo

**This Code Sucks: A Story  
About Non-violent  
Communication**



# Bad Actors





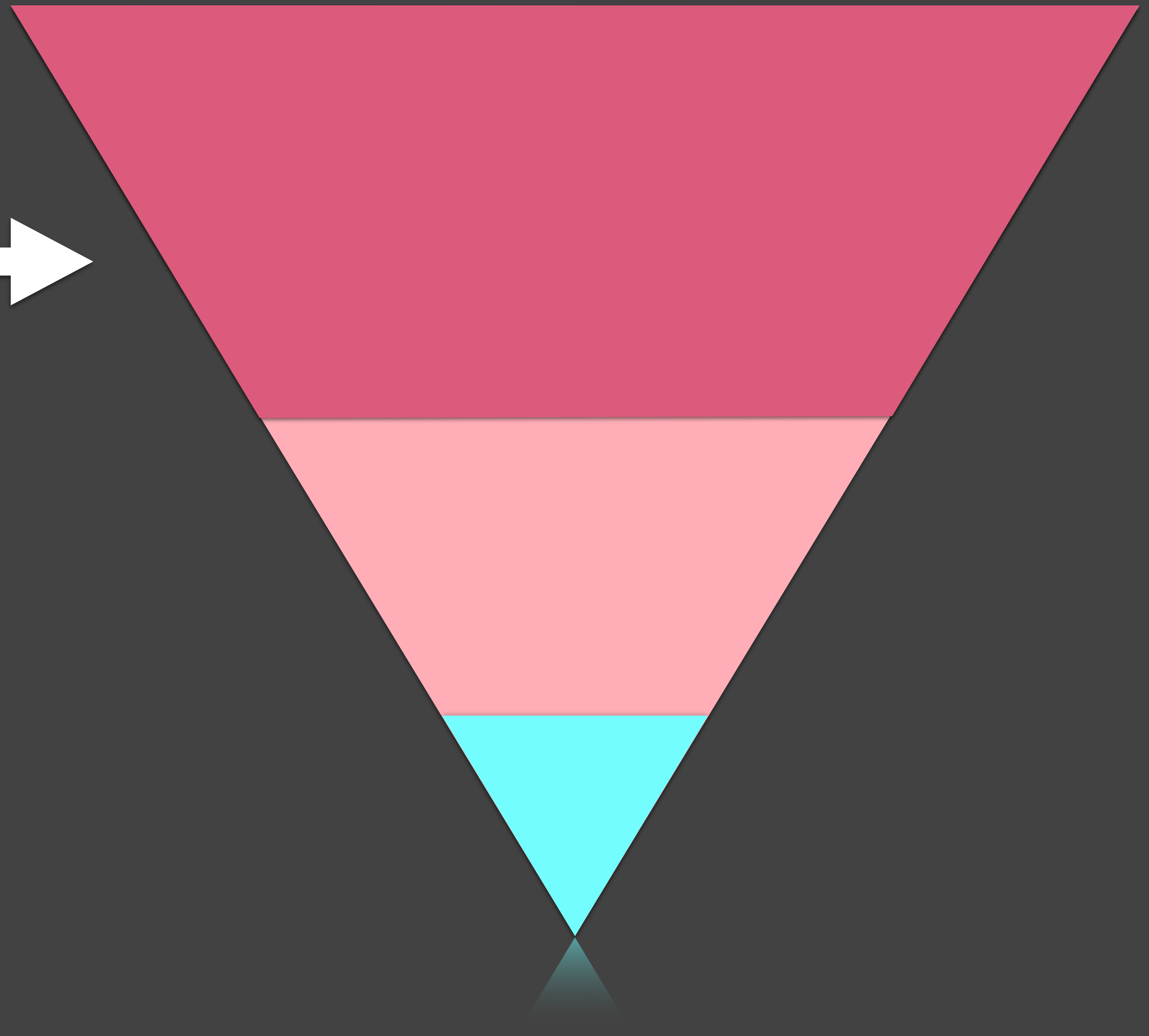


How can *vulnerability*  
be *harnessed* to  
*inspire* contributors?

Why is it *important*  
to create a *welcoming*  
& *supportive* open  
source *community*?

# *The Open Source Funnel*

**Users**

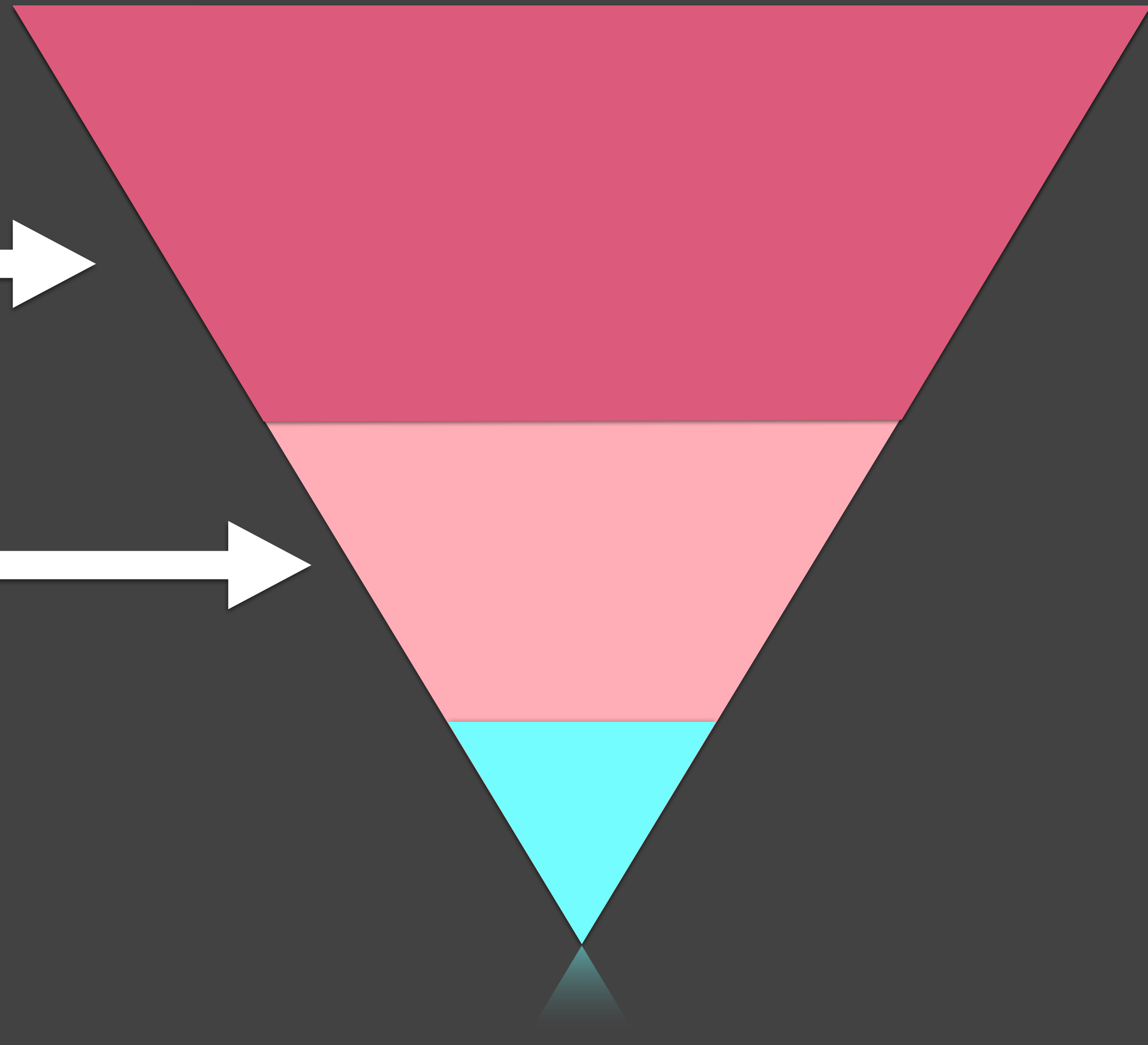


# *The Open Source Funnel*

**Users**



**Contributors**



# *The Open Source Funnel*

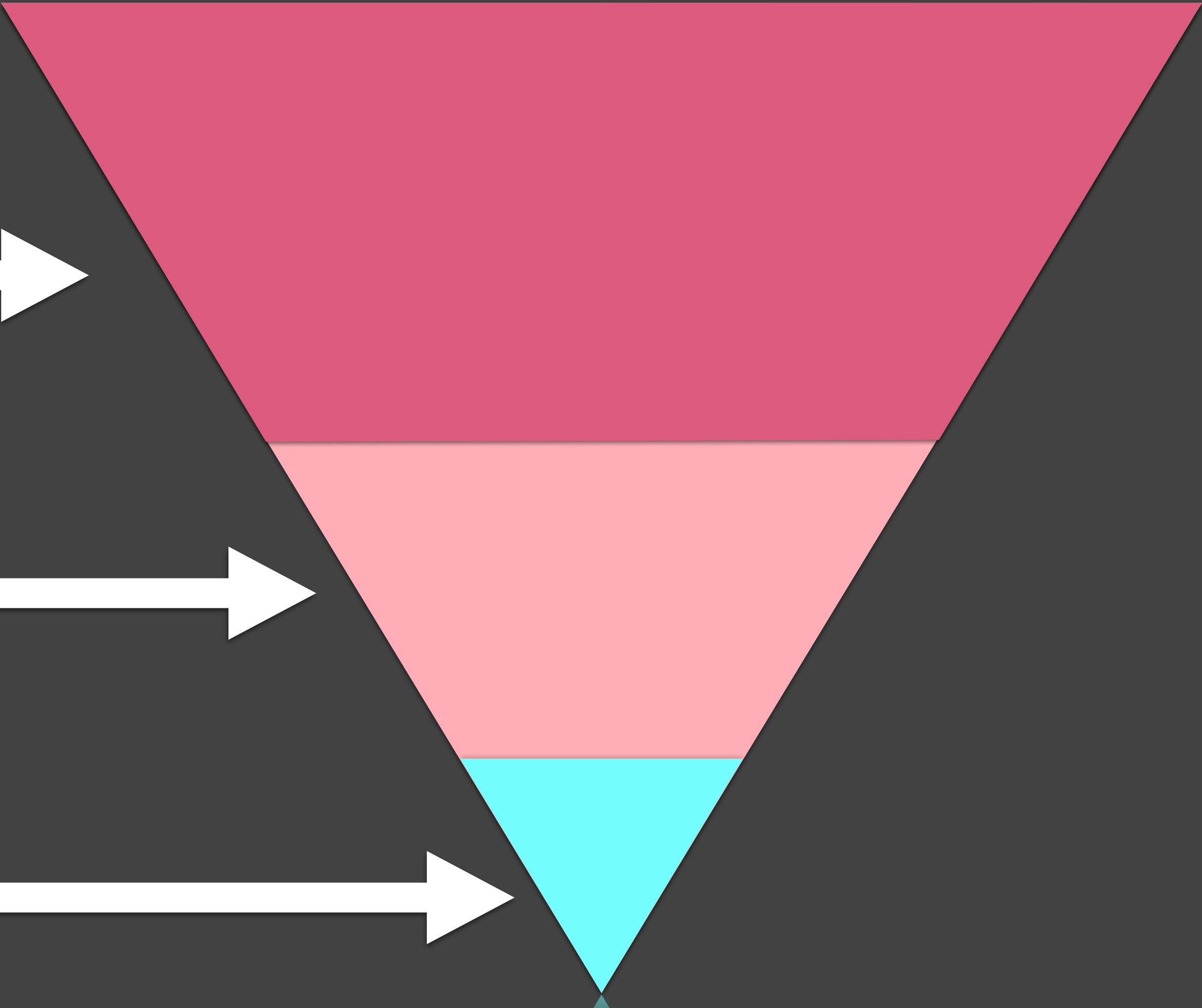
**Users**



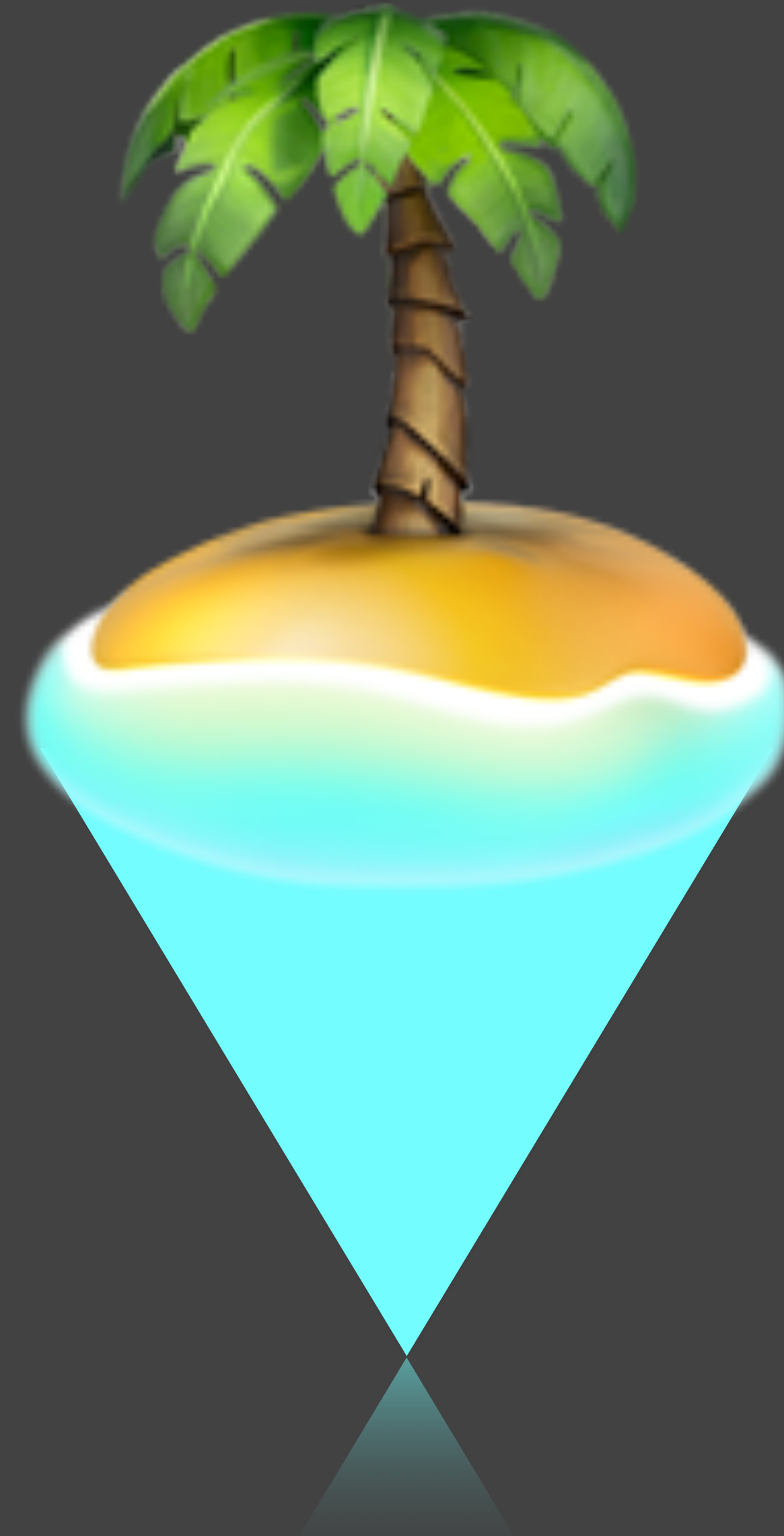
**Contributors**



**Maintainers**



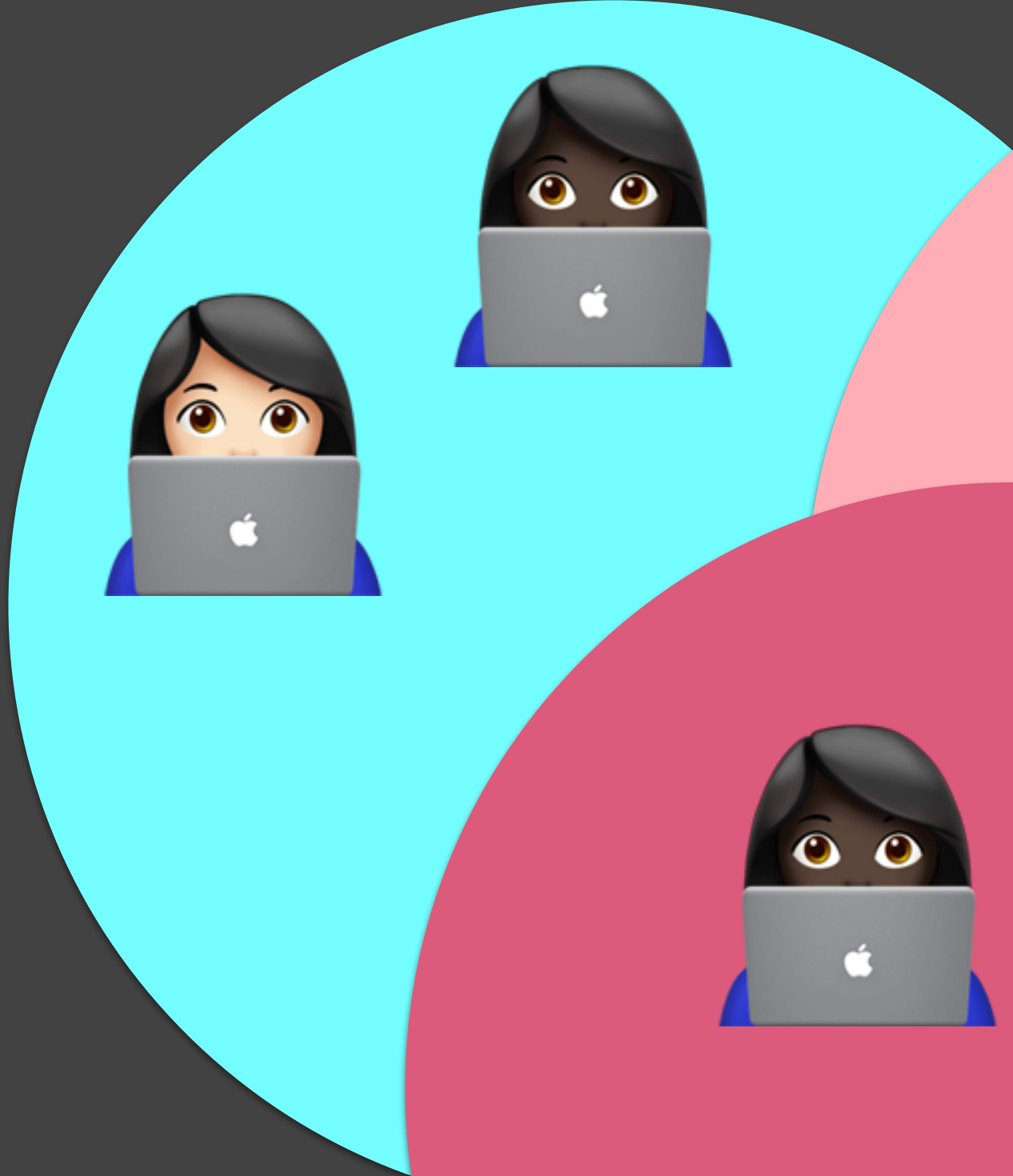




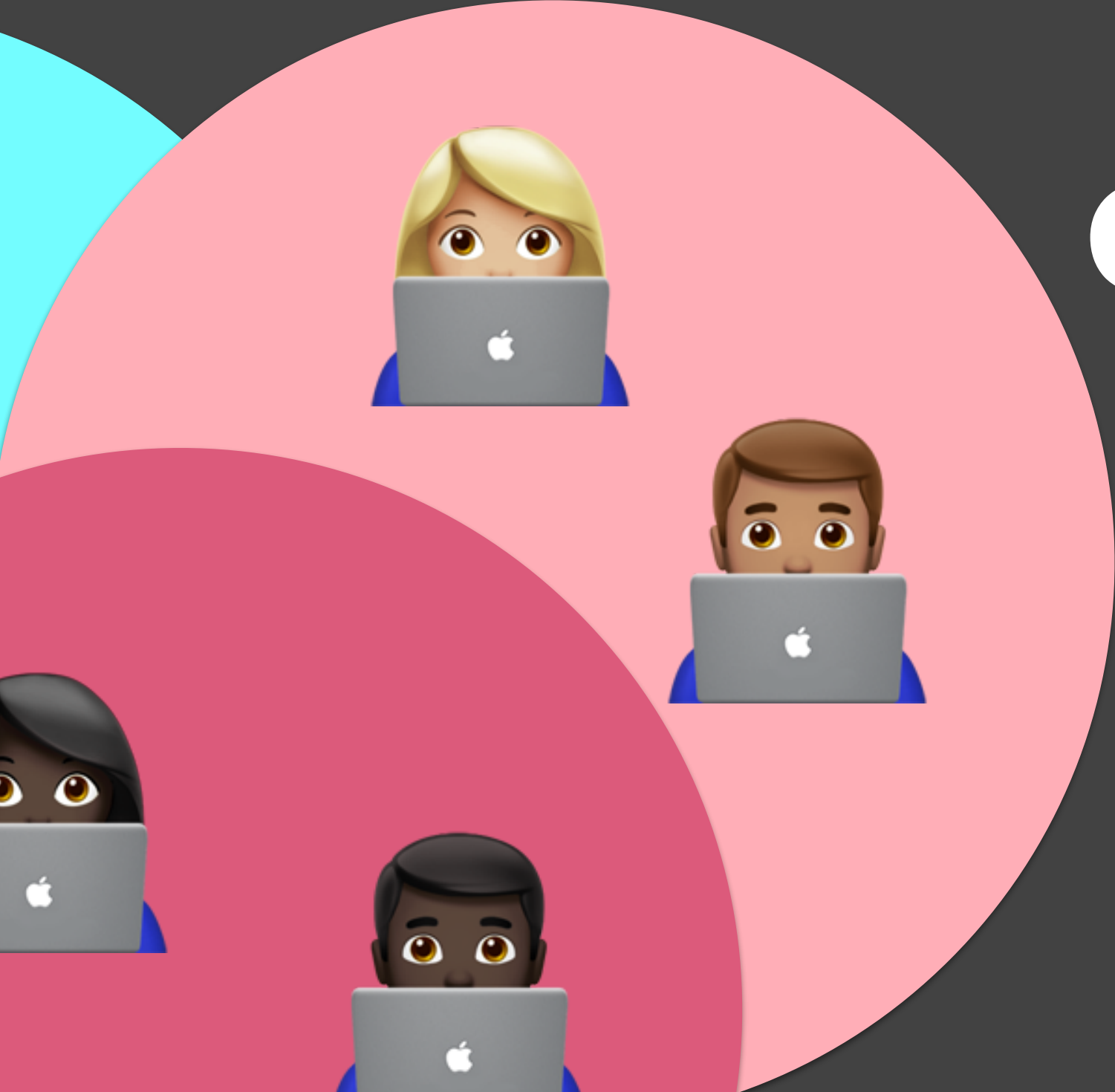


# *The Open Source Funnel*

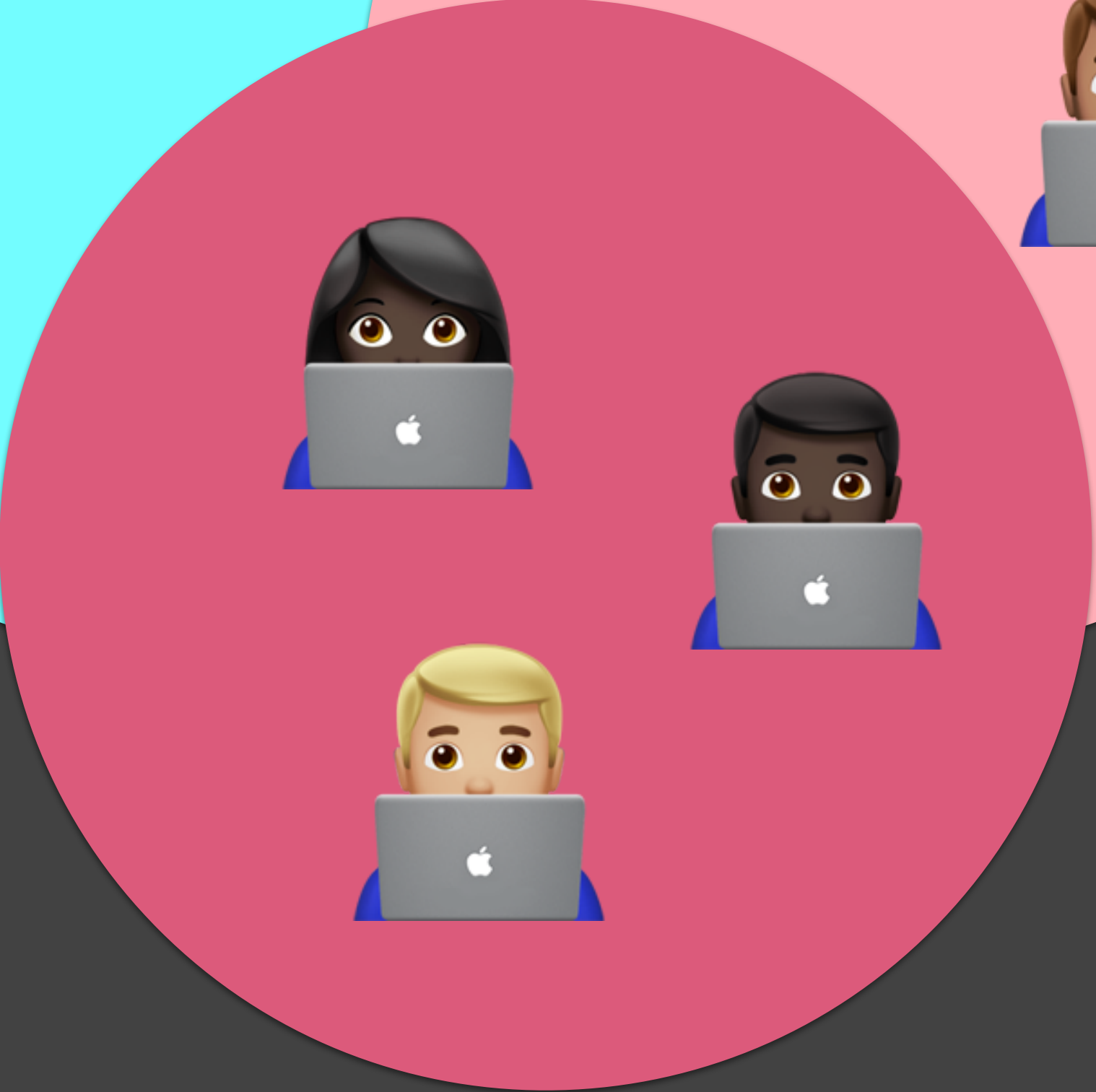
**Maintainers**



**Contributors**



**Users**



# *The Open Source Funnel*

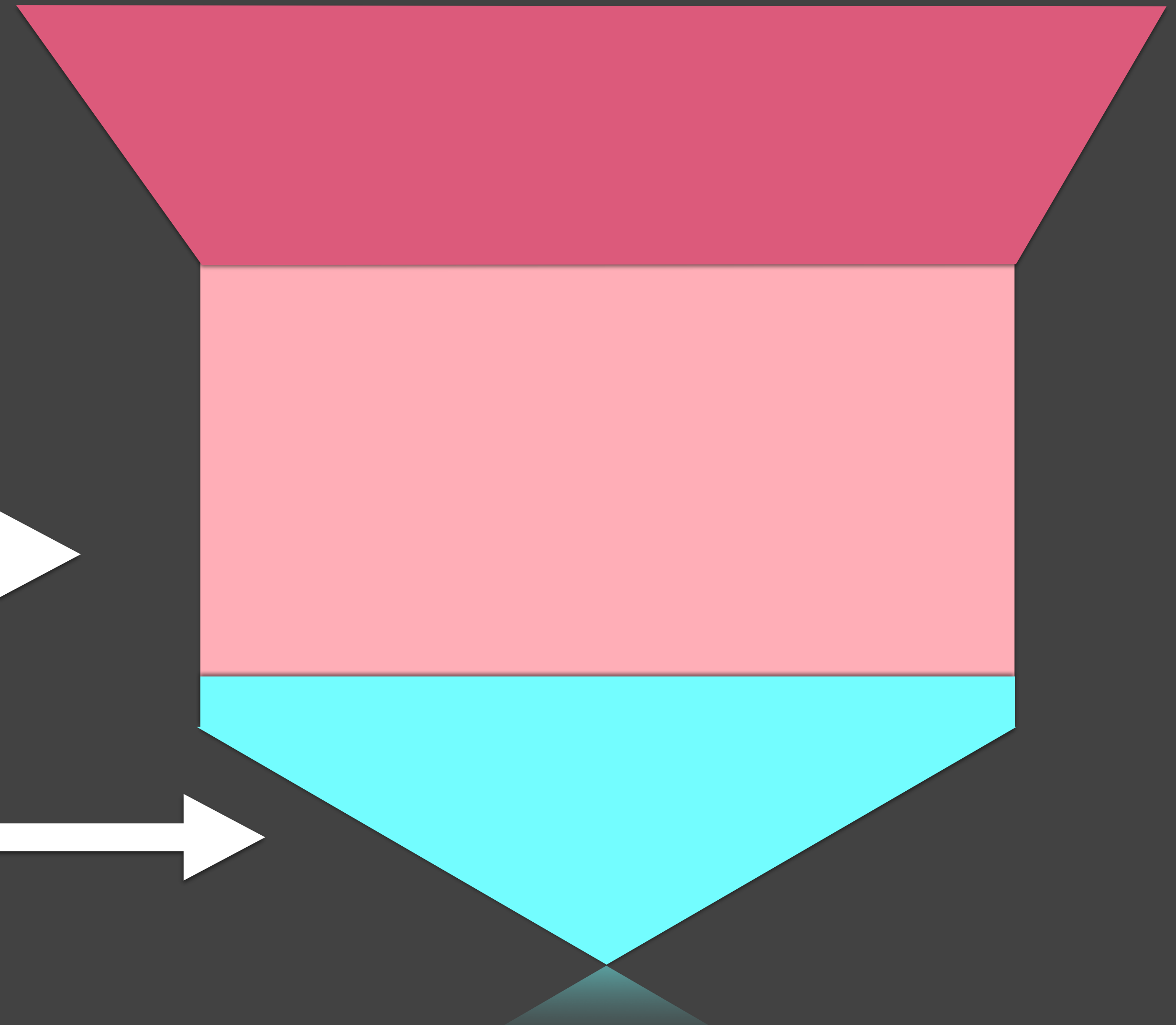
**Users**



**Contributors**



**Maintainers**



How can we create a  
*welcoming & supportive*  
open source *community*?

Creating a *sustainable*  
*community* through  
mentorship

# Mentoring



**Eileen M. Uchitelle** @eileencodes · 21 Mar 2014

@tenderlove thanks! Would love to chat sometime about active record. Just starting to understand its innards

2 1



**Eileen M. Uchitelle** @eileencodes · 22 Mar 2014

@tenderlove definitely! Will get in touch soon

2



**Aaron Patterson** ✓

@tenderlove

Following

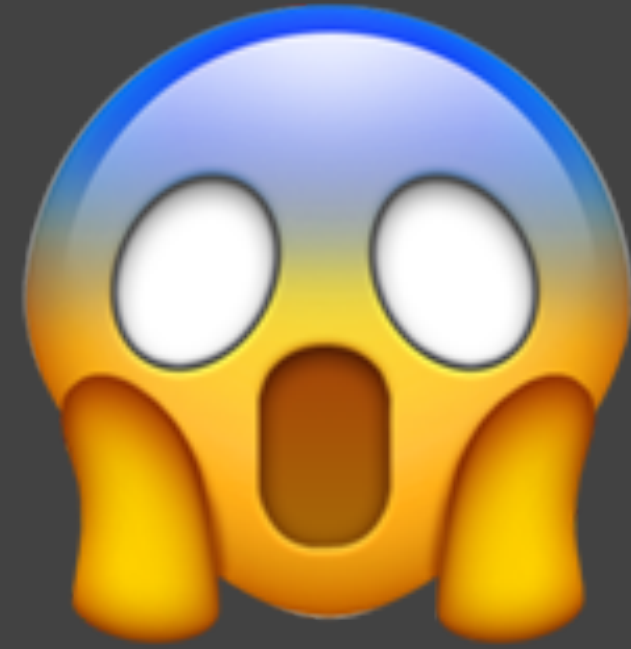
Replying to @eileencodes

@eileencodes ok! I have time to pair for a bit on Monday. Otherwise we can do something less real-time.

10:50 AM - 22 Mar 2014 from Salt Lake City, UT

1

**Mentoring**







# Mentoring

GOOD CODERS...





... KNOW WHAT THEY'RE DOING

Creating a *sustainable*  
*community* with  
clear guidelines

# Guidelines

Branch: master ▾ rails / CONTRIBUTING.md Find

 **lostapathy** Remove html tag making markdown misrender [ci skip]

14 contributors 

50 lines (27 sloc) | 3.29 KB Raw Blame History

## How to contribute to Ruby on Rails

### Did you find a bug?

- Do not open up a GitHub issue if the bug is a security vulnerability in Rails, and instead to refer to our [policy](#).
- Ensure the bug was not already reported by searching on GitHub under [Issues](#).
- If you're unable to find an open issue addressing the problem, [open a new one](#). Be sure to include a **title** and **clear description**, as much relevant information as possible, and a **code sample** or an **executable test case** demonstrating the expected behavior that is not occurring.
- If possible, use the relevant bug report templates to create the issue. Simply copy the content of the appropriate template into a .rb file, make the necessary changes to demonstrate the issue, and **paste the content into the issue description**:

# Provide Scripts

```
1 # frozen_string_literal: true
2
3 begin
4   require "bundler/inline"
5 rescue LoadError => e
6   $stderr.puts "Bundler version 1.10 or later is required. Please update your Bundler"
7   raise e
8 end
9
10 gemfile(true) do
11   source "https://rubygems.org"
12
13   git_source(:github) { |repo| "https://github.com/#{repo}.git" }
14
15   # Activate the gem you are reporting the issue against.
16   gem "activesupport", "5.1.0"
17 end
18
19 require "active_support/core_ext/object/blank"
20 require "minitest/autorun"
21
22 # Ensure backward compatibility with Minitest 4
23 Minitest::Test = MiniTest::Unit::TestCase unless defined?(Minitest::Test)
24
25 class BugTest < Minitest::Test
26   def test_stuff
27     assert "zomg".present?
28     refute "".present?
29   end
30 end
```

# Use Bots

 rails-bot assigned eileencodes 3 hours ago



rails-bot commented 3 hours ago

Member

Thanks for the pull request, and welcome! The Rails team is excited to review your code. You should hear from @eileencodes (or someone else) soon.

If any changes to this PR are deemed necessary, please add them as extra commits so that the reviewer can see what has changed since they last reviewed the code. Due to how GitHub handles out-of-date commits, this should also make it reasonably obvious when changes haven't been addressed. Large or tricky changes may require several passes of review and changes.

This repository is being automatically checked for code quality issues using [Code Climate](#). You can see results for this analysis in the PR status below. Newly introduced issues should be addressed before a Pull Request is considered ready to review.

Please see [the contribution instructions](#) for more information.

# Don't Shame



Creating a *sustainable  
community* by  
asking for help



# Ask for help

## rack-mini-profiler needs your help

---

We have decided to restructure our repository so there is a central UI repo and have their own.

The new home for rack-mini-profiler is <https://github.com/MiniProfiler/rack-mini-profiler>

### WE NEED HELP.

- Setting up a build that reuses <https://github.com/MiniProfiler/ui>
- Migrating the internal data structures per spec at: <https://github.com/MiniProfiler/rack-mini-profiler>
- Cleaning up the horrendous class structure that using string as keys and constants at: [https://github.com/SamSaffron/MiniProfiler/blob/master/Ruby/lib/mini\\_profiler.rb](https://github.com/SamSaffron/MiniProfiler/blob/master/Ruby/lib/mini_profiler.rb)
- Add travis-ci testing at least MRI 1.9.3, JRuby and MRI 2.0

If you feel like taking on any of this start an issue and update us on your progress

# Build a core team



**David**  
Since 2003  
USA/Spain  
Commits



**Jeremy**  
Since 2005  
USA  
Commits



**Santiago**  
Since 2010  
Uruguay  
Commits



**Aaron**  
Since 2011  
USA  
Commits



**Xavier**  
Since 2011  
Spain  
Commits



**Rafael**  
Since 2012  
Brazil  
Commits



**Andrew**  
Since 2012  
UK  
Commits



**Guillermo**  
Since 2012  
USA/Colombia  
Commits



**Carlos**  
Since 2012  
Brazil  
Commits



**Matthew**  
Since 2015  
Australia  
Commits



**Kasper**  
Since 2016  
Denmark  
Commits

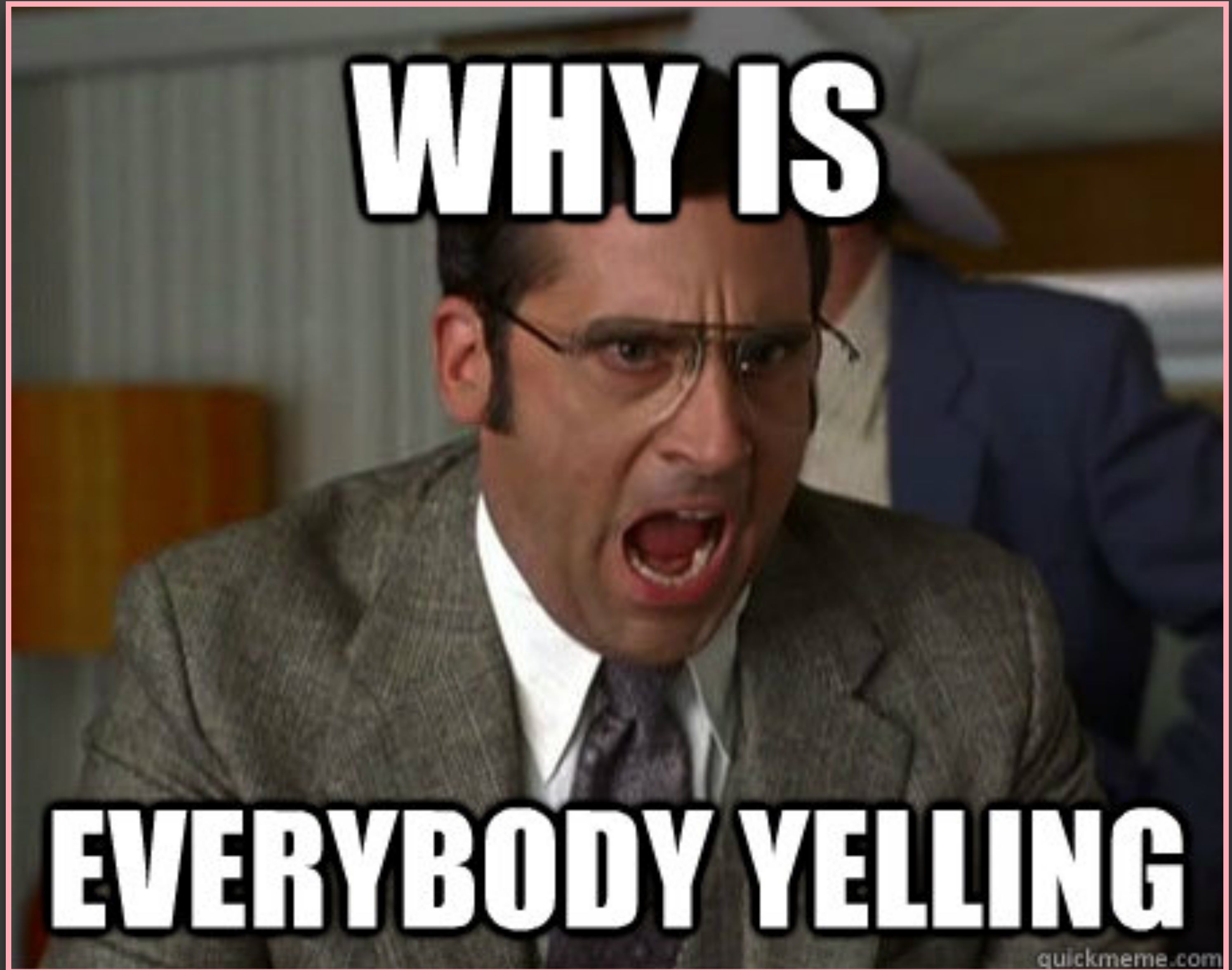


**Eileen**  
Since 2017  
USA  
Commits

Creating a *sustainable*  
*community* by  
respecting each other



**Respect**



# Add a CoC

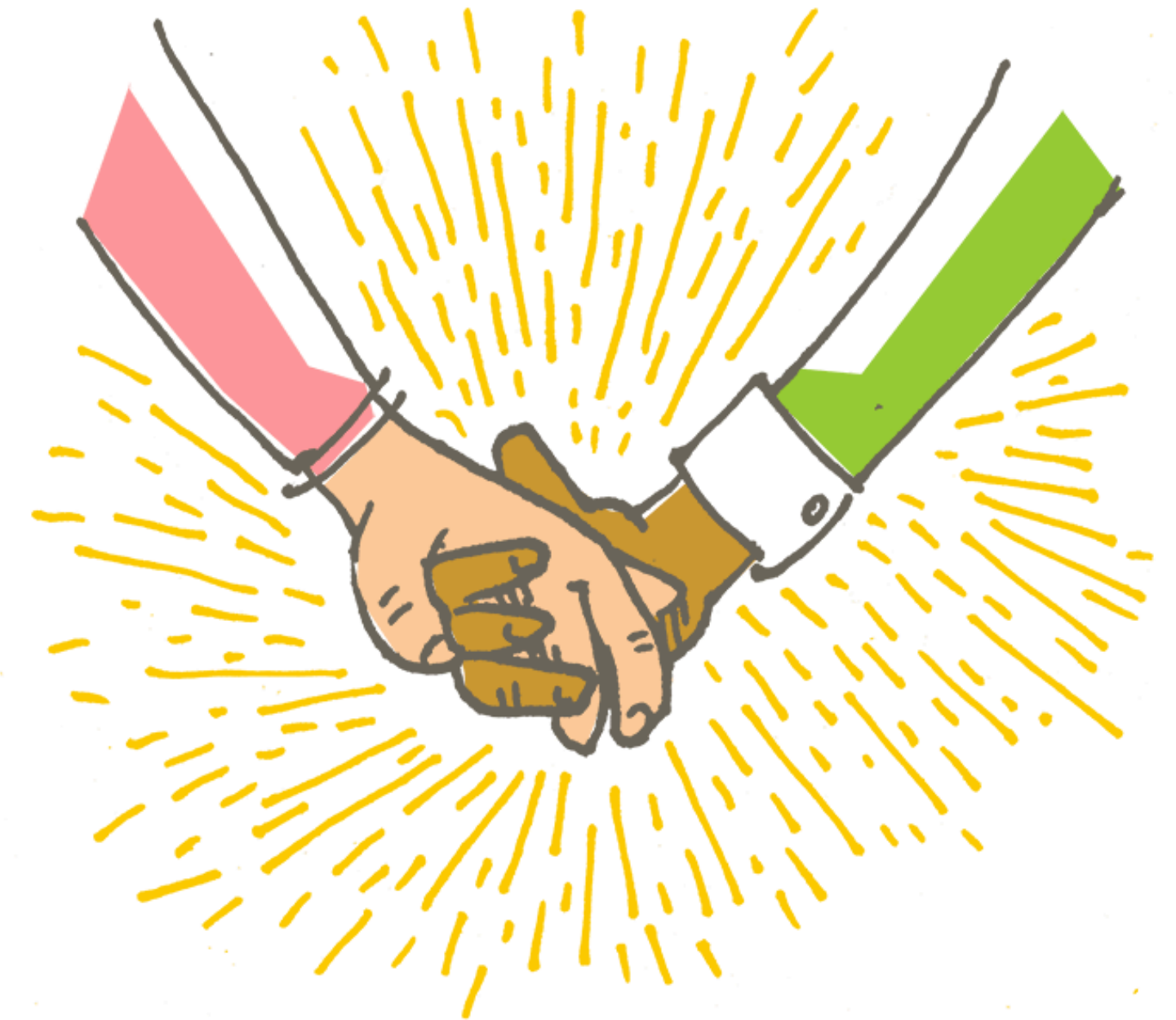


## Code of Conduct

Rails is committed to fostering a welcoming community. If you encounter any unacceptable behavior, follow these steps to report the issue to the **core team**. We are here to help.

## Our Pledge

In the interest of fostering an open and welcoming environment, we as contributors and maintainers pledge to making participation in our project and our community a harassment-free experience



# Creating a *welcoming community* using the GitHub tools

# GitHub Tools

otea commented 3 minutes ago

First-time contributor

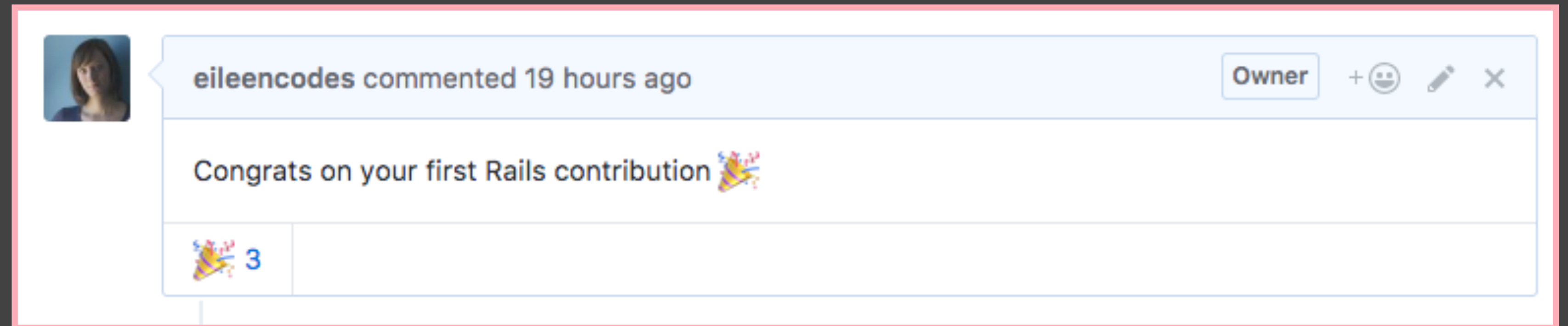


re some changes that I believe will be helpful.





# GitHub Tools



A screenshot of a GitHub comment interface. On the left is a small profile picture of a woman. To its right, a light blue header bar contains the text "eileencodes commented 19 hours ago" and a "Owner" label with a plus icon, a smiley face icon, a pencil icon, and a close icon. Below this is the comment text: "Congrats on your first Rails contribution 🎉". At the bottom left of the comment box, there is a reaction count: a 🎉 emoji followed by the number "3".

# GitHub Tools

The screenshot shows the GitHub repository page for rails/rails. The repository is currently on the master branch. A dropdown menu is open, highlighting the 'Community' option with a red arrow. The repository statistics show 64,852 commits, 30 branches, 337 releases, and 3,381 contributors. The latest commit is bd2542b 4. The repository is currently on the master branch. The repository is currently on the master branch.

rails / rails

Unwatch 2,465 Unstar 37,121

Code Issues 434 Pull requests 753 Projects 0 Settings Insights

Ruby on Rails <http://rubyonrails.org>

rails mvc html activerecord activejob ruby Manage topics

64,852 commits 30 branches 337 releases 3,381 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

eileencodes Merge pull request #30744 from eileencodes/early-hints Latest commit bd2542b 4

.github	Limit stale checks to issues	6 m
actioncable	Fix quotes [ci skip]	10
actionmailer	Cleanup CHANGELOGs [ci skip]	19
actionpack	Implement H2 Early Hints for Rails	4
actionview	Implement H2 Early Hints for Rails	4
activejob	Update activejob doc [ci skip]	a
activemodel	Clarify intentions around method redefinitions	a
activerecord	Cleanup CHANGELOGs [ci skip]	19

# GitHub Tools

## Community profile

---

Here's how this project compares to [recommended community standards](#).

### Checklist

✓ Description
✓ <a href="#">README</a>
✓ <a href="#">Code of conduct</a>
✓ <a href="#">Contributing</a>
✓ <a href="#">License</a>
✓ <a href="#">Issue template</a> and <a href="#">pull request template</a>

What is [the community profile?](#)

How can *contributors*  
find *communities*?

*Contribute* to  
*projects* you use

Finding a *welcoming*  
*community* by  
observing behavior

# Observing behavior

The screenshot shows the GitHub repository page for 'activejob'. At the top, there are navigation tabs for 'activejob' and 'ruby', along with a 'Manage topics' link. Below this, repository statistics are displayed: '0 branches', '336 releases', '3,379 contributors', and 'MIT' license. A navigation bar contains buttons for 'Create new file', 'Upload files', 'Find file', and 'Clone or download'. The commit history table below shows the following entries:

Commit Message	Time Ago
able secret_key_base.	Latest commit f60bf5a 3 hours ago
Limit stale checks to issues	6 hours ago
Fix quotes [ci skip]	8 days ago
Update Action Mailer doc [ci skip]	27 days ago
Fix cookies/session tests broken after merging key rotation.	5 hours ago
Fix `test_should_sanitize_illegal_style_properties` failure	1 day ago
Update activejob doc [ci skip]	27 days ago
Clarify intentions around method redefinitions	25 days ago
Merge pull request #30705 from frodsan/use-digest-thread-safe	4 hours ago

A red arrow points to the '3 hours ago' timestamp of the latest commit.

# Observing behavior

The screenshot shows a GitHub pull request interface. A red arrow points to the text "Show all checks" in the top right corner of the pull request content area. Below this, the text "the base branch" is visible. Further down, there is a link that says "View this in GitHub Desktop or view command line instructions." Below the main content area is a toolbar with various icons for formatting and actions. On the right side of the interface, there are sections for "Projects" (None yet), "Milestone" (No milestone), "Notifications" (with a "Subscribe" button), and "2 participants" (with two profile pictures).





Learning to  
*accept* rejection

Once you *find* a  
*community* be respectful

## Resources

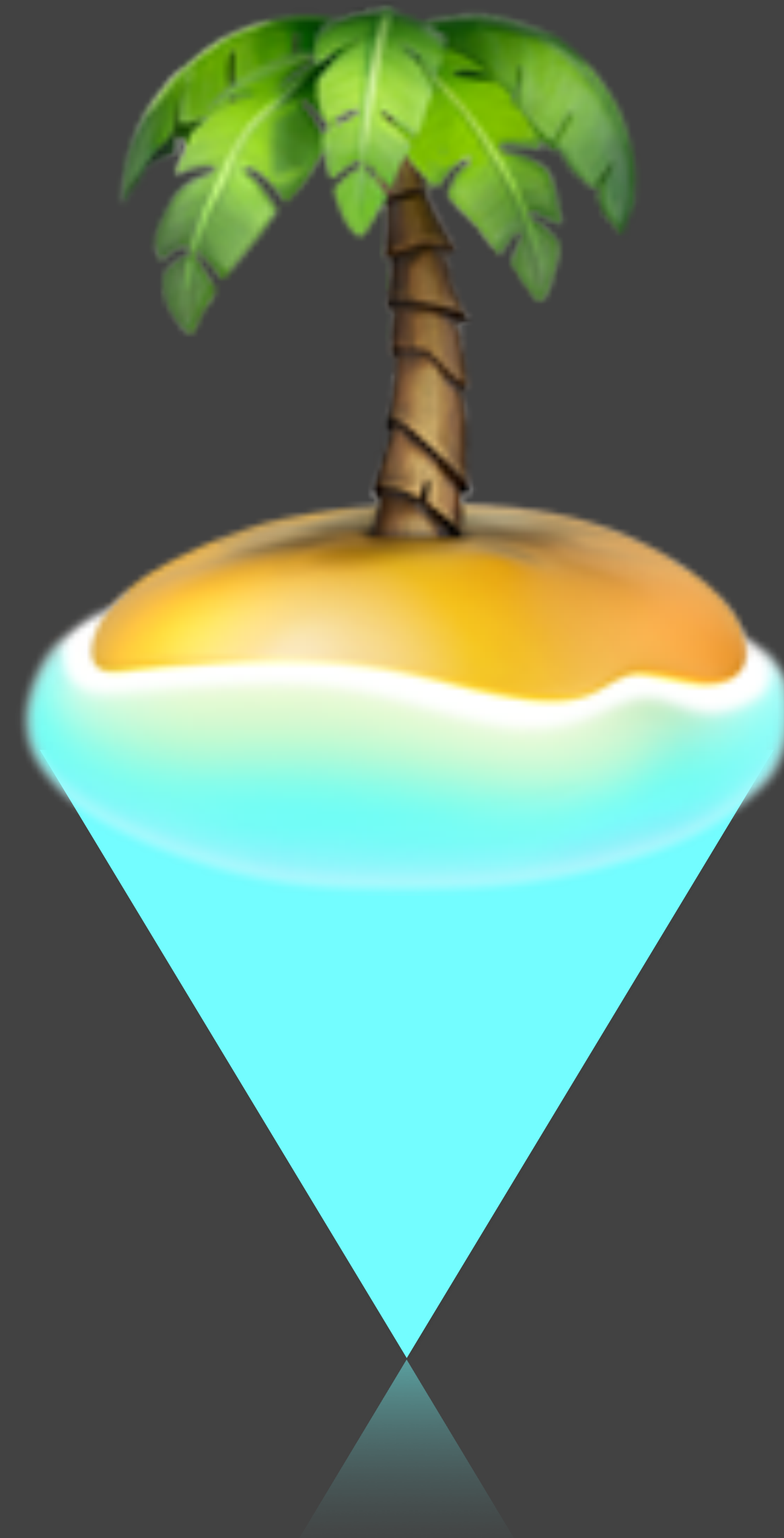
- [www.firsttimersonly.com](http://www.firsttimersonly.com)
- [www.yourfirstpr.github.io](http://www.yourfirstpr.github.io)
- [www.codetriage.com](http://www.codetriage.com)
- [www.opensource.guide](http://www.opensource.guide)

*Open Source* isn't about  
writing *code*

*Open Source* is really  
about *people*

Build a

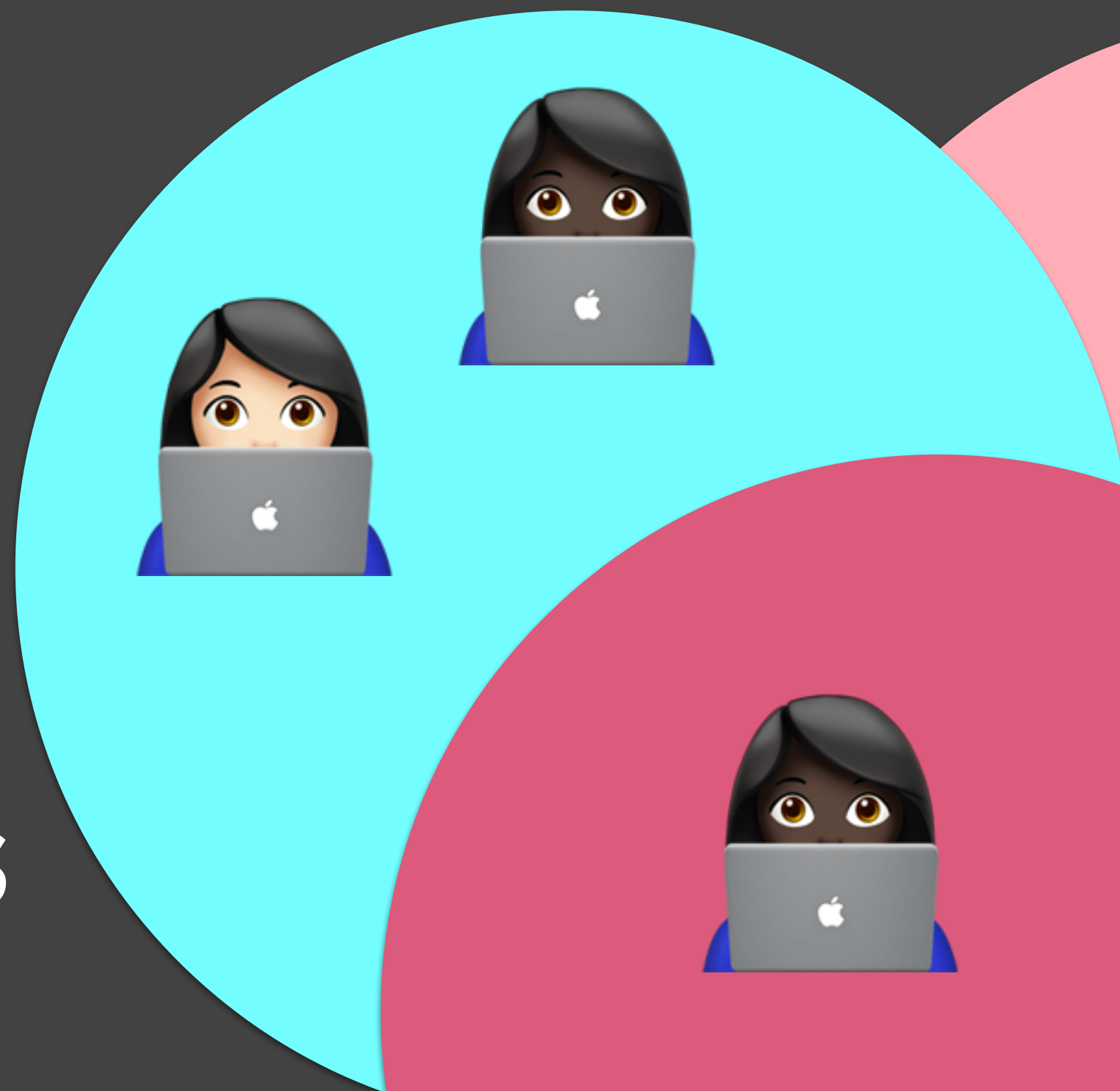
*welcoming & supportive*  
open source *community*



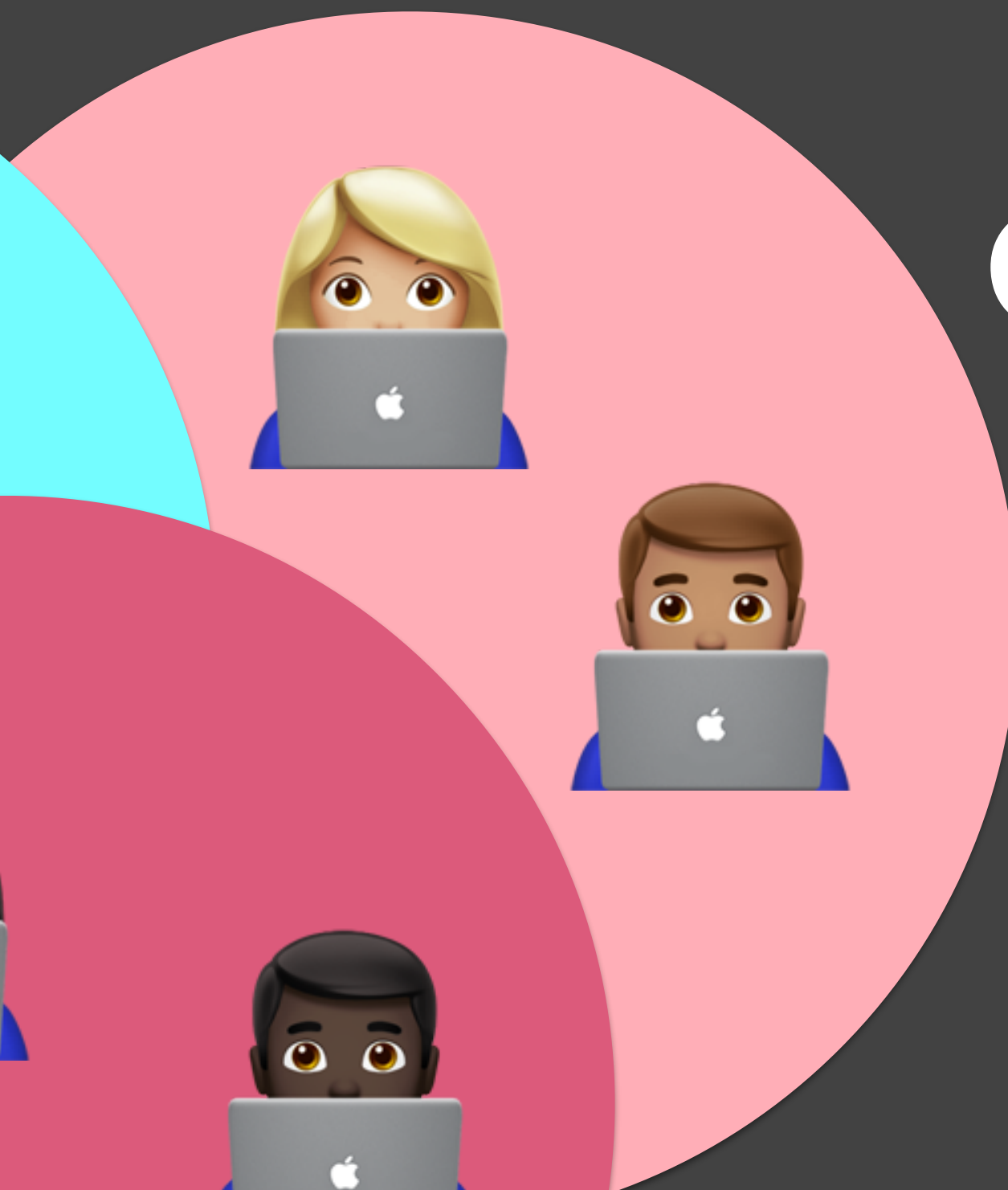




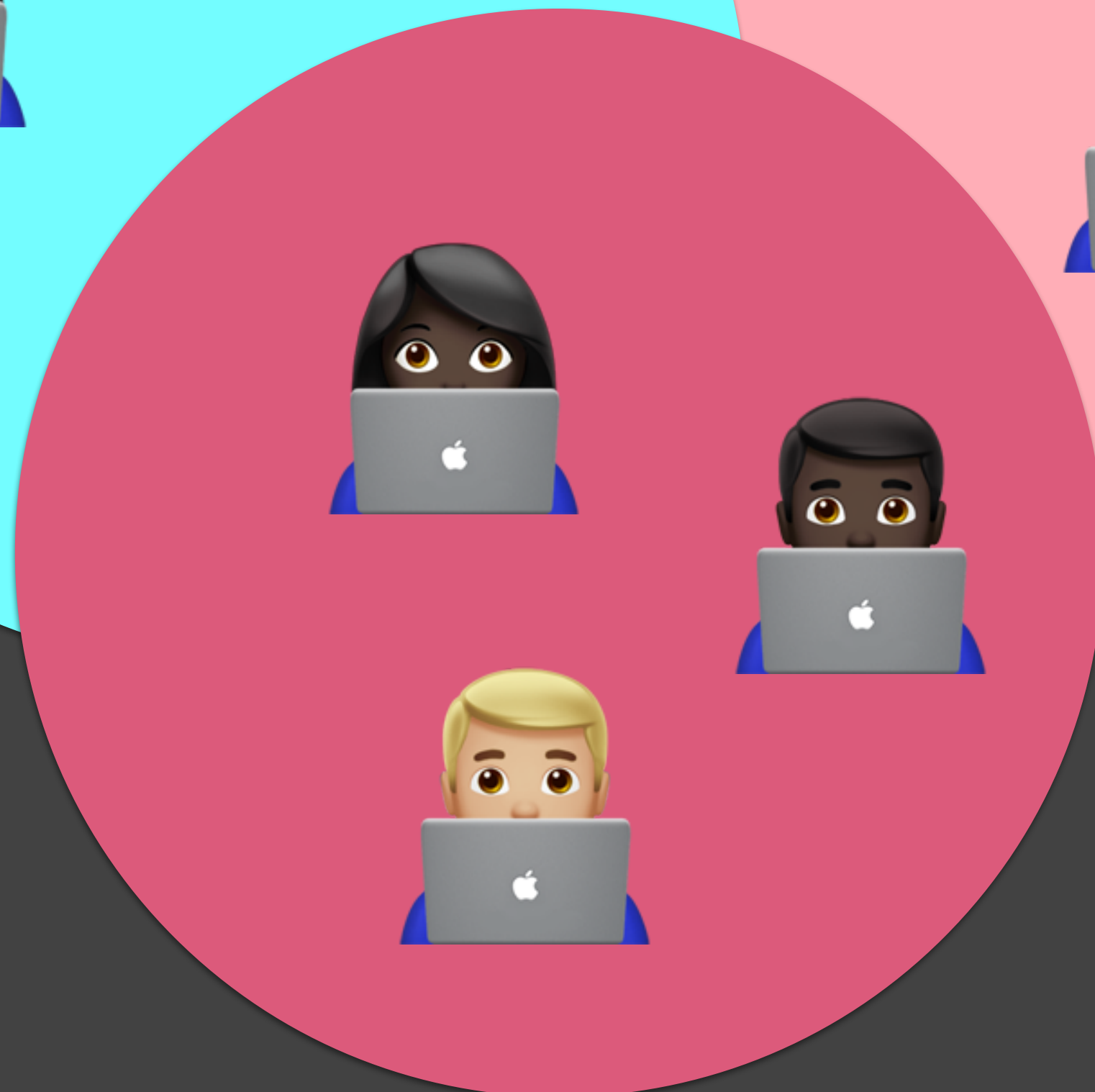
**Maintainers**



**Contributors**



**Users**







The *future*  
of *open source*  
depends on *all of us*

*Together* we can  
make *vulnerability*  
*bearable*

**Thank you  
RubyConf!**





# Eileen Uchitelle

@eileencodes

Senior Systems Engineer

**GitHub**

