Why Won't Developers Always Just Write Secure Open Source Software?

LISH
Laboratory for Innovation Science at Harvard

THE LINUX FOUNDATION

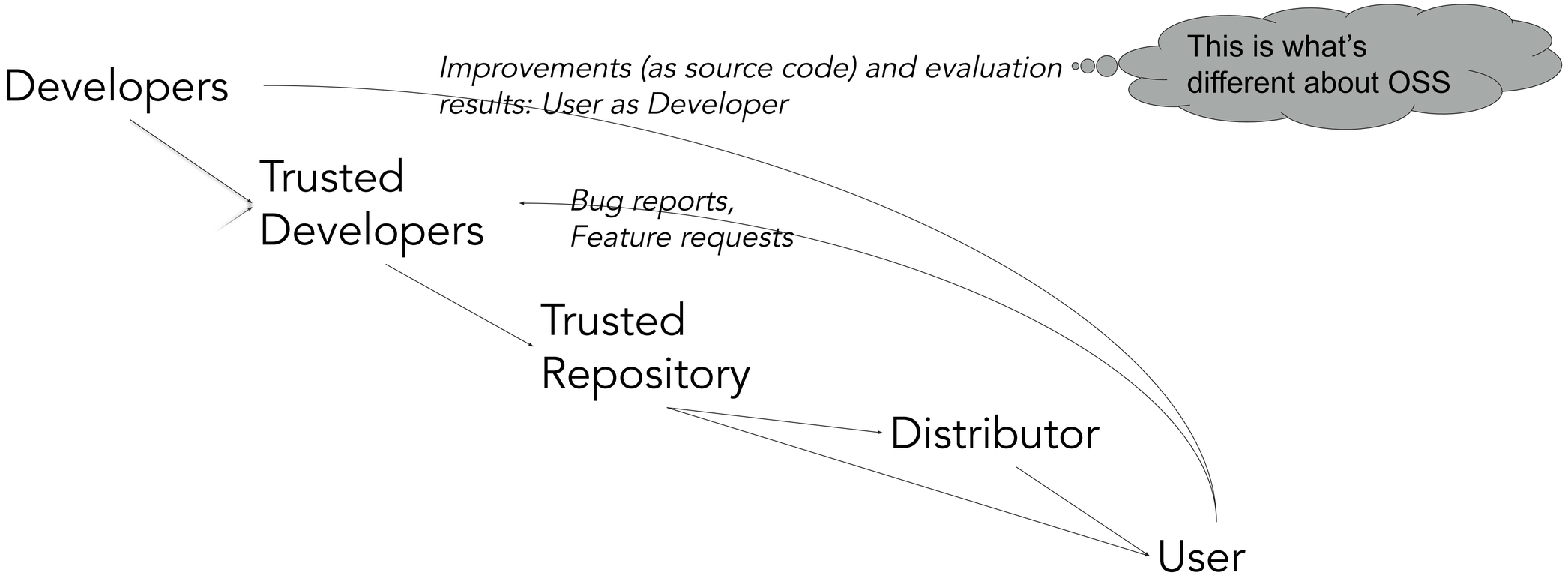
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

What is Open Source Software (OSS)?

- OSS: software licensed to users with these freedoms:
  - to *run* the program for any purpose,
  - to *study* and *modify* the program, and
  - to freely *redistribute* copies of original or modified program (without royalties, etc.)
- Details in "Open Source Definition" [Open Source Initiative]
  - Synonyms: Free sw (capital F), libre sw, free-libre sw, FOSS, FLOSS
  - Antonyms: proprietary, closed source
- Widely used; OSS #1 or #2 in many markets
  - 80-90% of typical applications are OSS [Sonatype 2016]
  - At least 3.26 million significant OSS projects [IDA 2017]
  - "[OSS] plays a more critical role in the DoD than [generally] recognized." [MITRE 2003]
- OSS is *commercial software* under US law & regulation (once released)
  - Commercial software includes software sold, leased, or *licensed* to the general public [41 USC 403, FAR 2.101, DFARS 212.212]

Sources:https://www.ida.org/research-and-publications/publications/all/c/co/core-infrastructure-initiative-cii-open-source-software-census-ii-strategy
https://www.sonatype.com/hubfs/SSC/Software_Supply_Chain_Inforgraphic.pdf?t=1468857601884
https://www.csiac.org/journal-article/open-source-software-is-commercial/

How is Open Source Software (OSS) Typically Developed?



- OSS licenses enable worldwide collaboration
- Well-run OSS projects seek to nurture this collaboration
- OSS isn't "no cost" but its cost-sharing & collaborative review often make it low cost

THE LINUX FOUNDATION
LISH Laboratory for Innovation Science at Harvard

Context

In 2014, the Heartbleed vulnerability in OpenSSL brought attention to the need for increased security

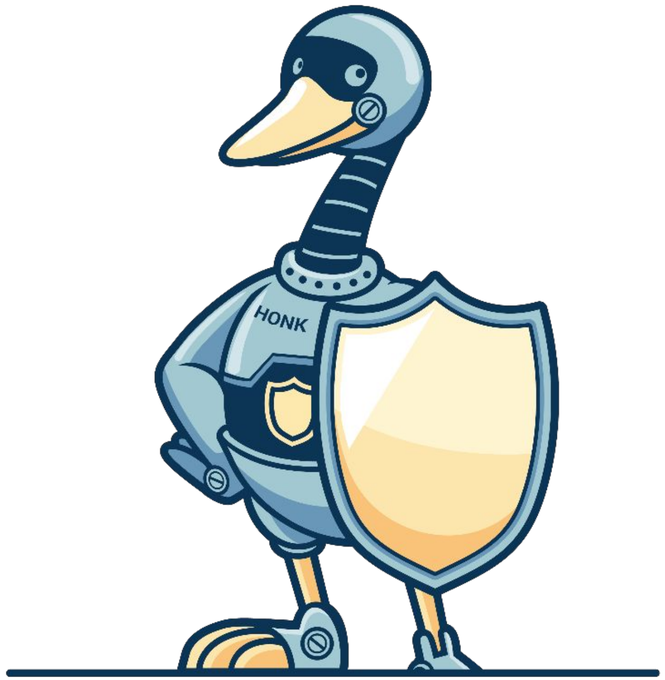
This led to formation of the Core Infrastructure Initiative (CII)

- Fund & improve critical elements of open source including OpenSSL
- CII Best Practice Badging Program
- Two Project Censuses
- 2020 FOSS Contributor Survey

THE LINUX FOUNDATION

LISH Laboratory for Innovation Science at Harvard

Open Source Security Foundation (OpenSSF)



- Established August 3, 2020: https://openssf.org/
- Focused on improving the security of OSS, consolidates several different previous organizations

  Core Infrastructure Initiative (CII)
  Open Source Security Coalition
  Joint Open Source Software Initiative

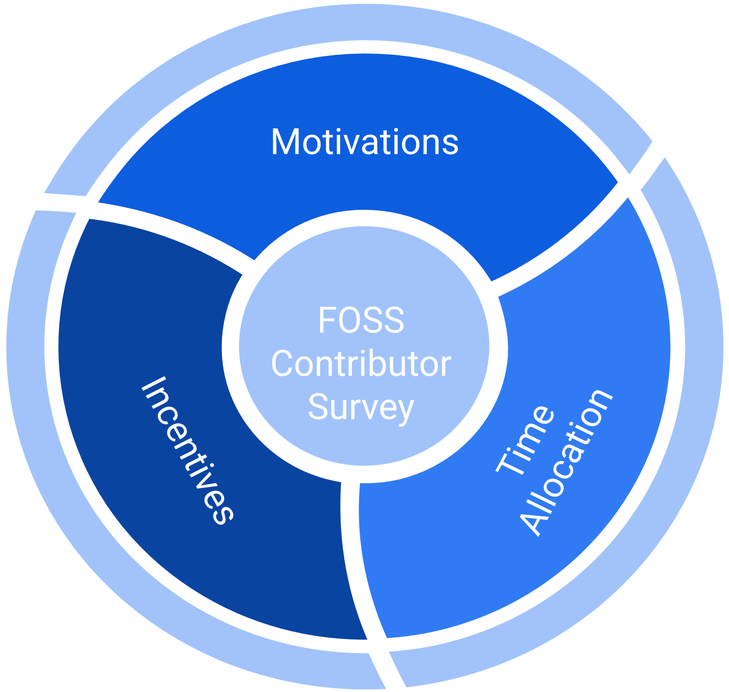
- Members include:

GitHub	Microsoft
Google	Red Hat
IBM	Uber
Intel	VMware

THE LINUX FOUNDATION
LISH Laboratory for Innovation Science at Harvard

Insights on Security from the 2020 FOSS Contributor Survey

Why won't developers always just write secure open source software?



Different people, different situations, e.g.:

- Paid maintainer
- Paid occasional contributor
- Unpaid maintainer

Survey Covered

- **Demographics**

  Who are FOSS contributors? In particular, what are their gender, employment, and geographic location?

- **Current FOSS Contributions**

  What kinds of security-related activities are already taking place in the FOSS projects represented by the respondents?

- **FOSS at Work**

  How many FOSS contributors are paid by their employers for their work on FOSS? How much of their contribution occur during work hours vs. free time?

- **Motivations**

  What are their reasons for starting, continuing, or stopping contributions to FOSS? How can projects keep contributors engaged, and do contributors feel that their employers or others value their work?

- **Time Allocation**

  How much time do contributors spend contributing to FOSS, and how would they like to spend it? Is there an interest in increasing time spent on security issues?

Definitions

"Maintainers" are package maintainers or software maintainers who are the final decision makers over all or portions of source code that goes into a build or release. Maintainers would likely also identify as a subset of core participants.

"Core participants" may have been involved in the project since inception, joined later, and regularly participated in major discussions about project direction, and have significant ongoing roles in the work, possibly including accepting patches to the code base. Core participants may be referred to as "Committers" in a project community.

"Occasional participants" would not normally participate in ongoing or weekly project discussions, but occasionally provide contributions over longer periods of time.

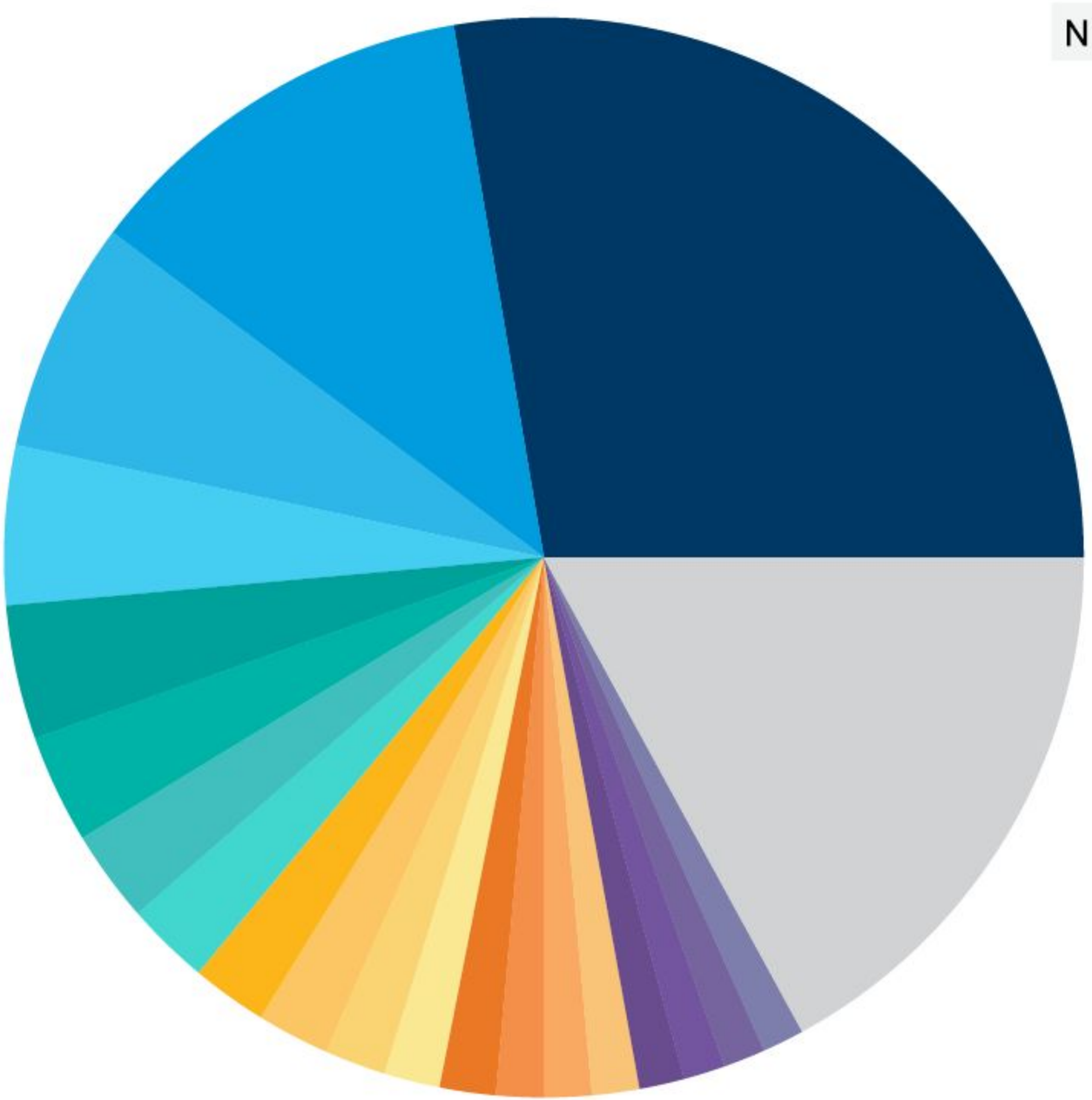
"One-time participant" is someone who provides a specific set of suggestions or contributions and then exits involvement once their work is done; these are sometimes called "drive-by commits."

Definitions

"Paid contributor" is a contributor who is paid for at least one of the projects they work on

"Unpaid contributor" is a contributor who is not paid for any of their FOSS work

Geographic Location of Respondents by Country

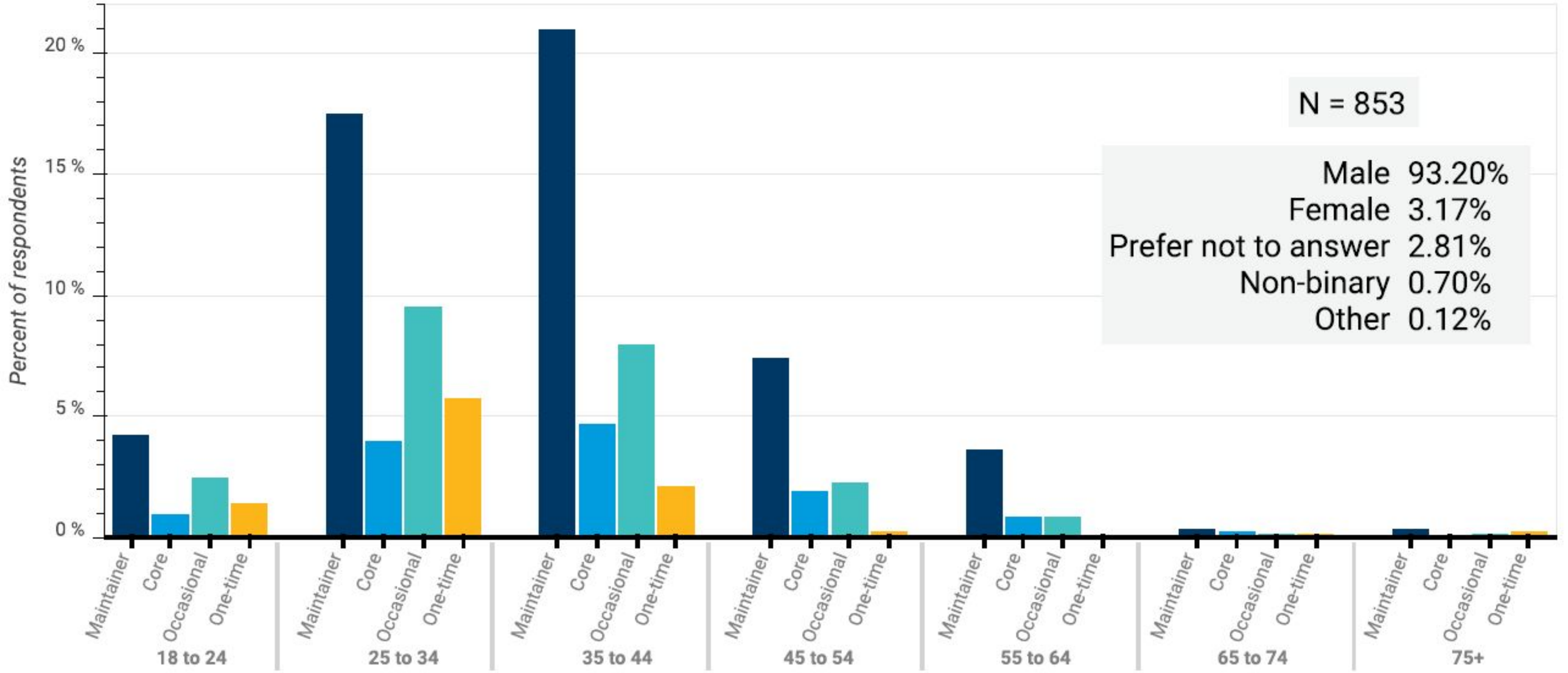


- United States of America: 28%
- Germany: 12%
- France: 7%
- United Kingdom: 5%
- India: 4%
- Canada: 3%
- Netherlands: 3%
- Russian Federation: 3%
- Czech Republic: 2%
- China: 2%
- Australia: 2%
- Japan: 2%
- Poland: 2%
- Switzerland: 1%
- Spain: 1%
- Brazil: 1%
- Sweden: 1%
- Israel: 1%
- Italy: 1%
- Austria: 1%
- Other: 17%

THE LINUX FOUNDATION

LISH Laboratory for Innovation Science at Harvard

Gender, Age & Contributor Status of Respondents



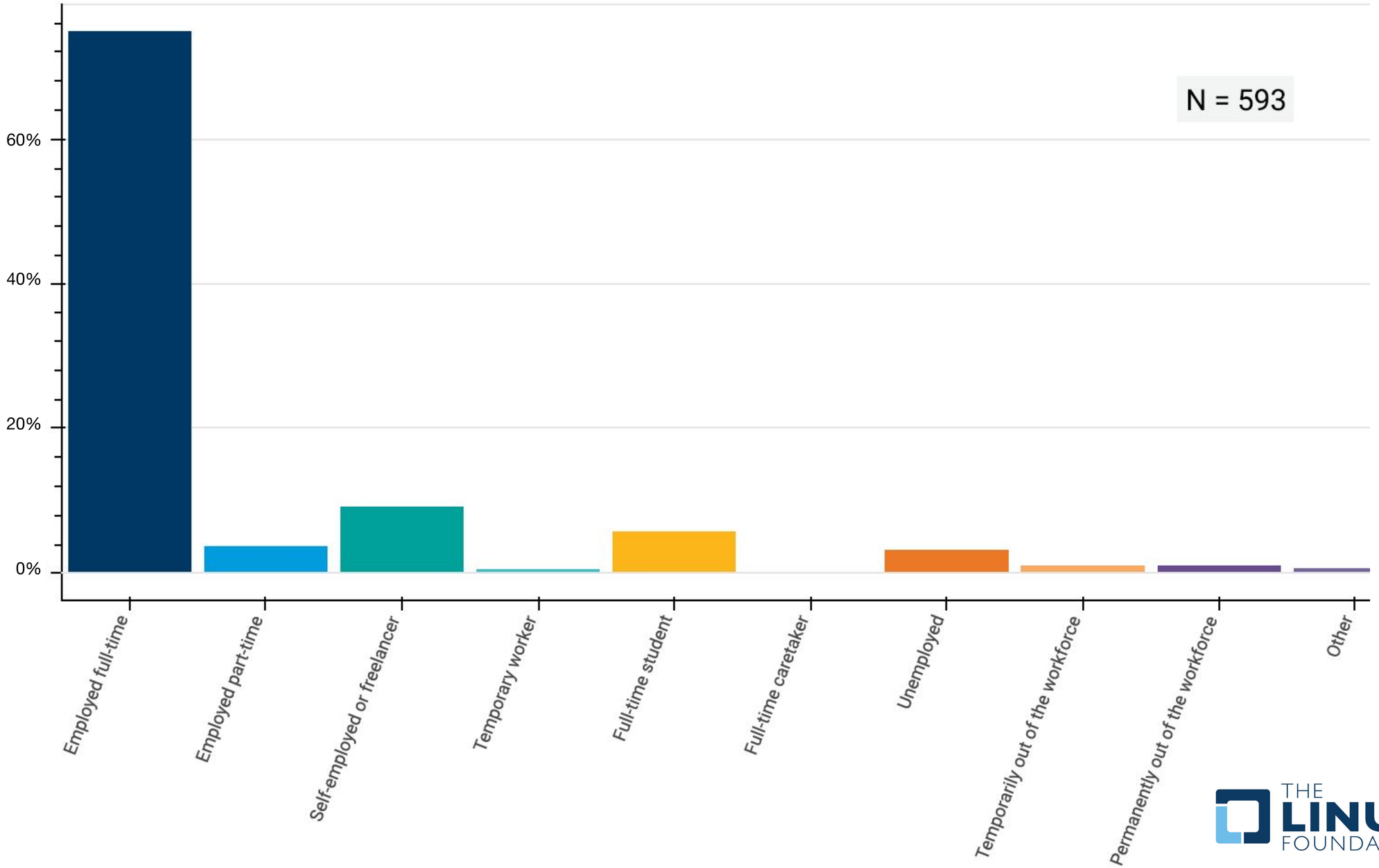
Paid Contributions

Over half (51.65%) of respondents reported that they receive payment for their FOSS contribution from either their employer or a third party.

Countries by Ratio of Paid Contributors to Total Respondents

Country	% of Respondents Paid for FOSS	Total Responses
United States of America	63.80%	174
Germany	58.70%	75
France	37.10%	35
United Kingdom	42.90%	28
Canada	57.10%	21
Netherlands	75.00%	20
India	15.80%	19
China	29.40%	17
Austria	63.40%	11
Brazil	45.50%	11
Japan	45.50%	11
Australia	30.00%	10
Other	43.50%	145

Respondents' Employment Status

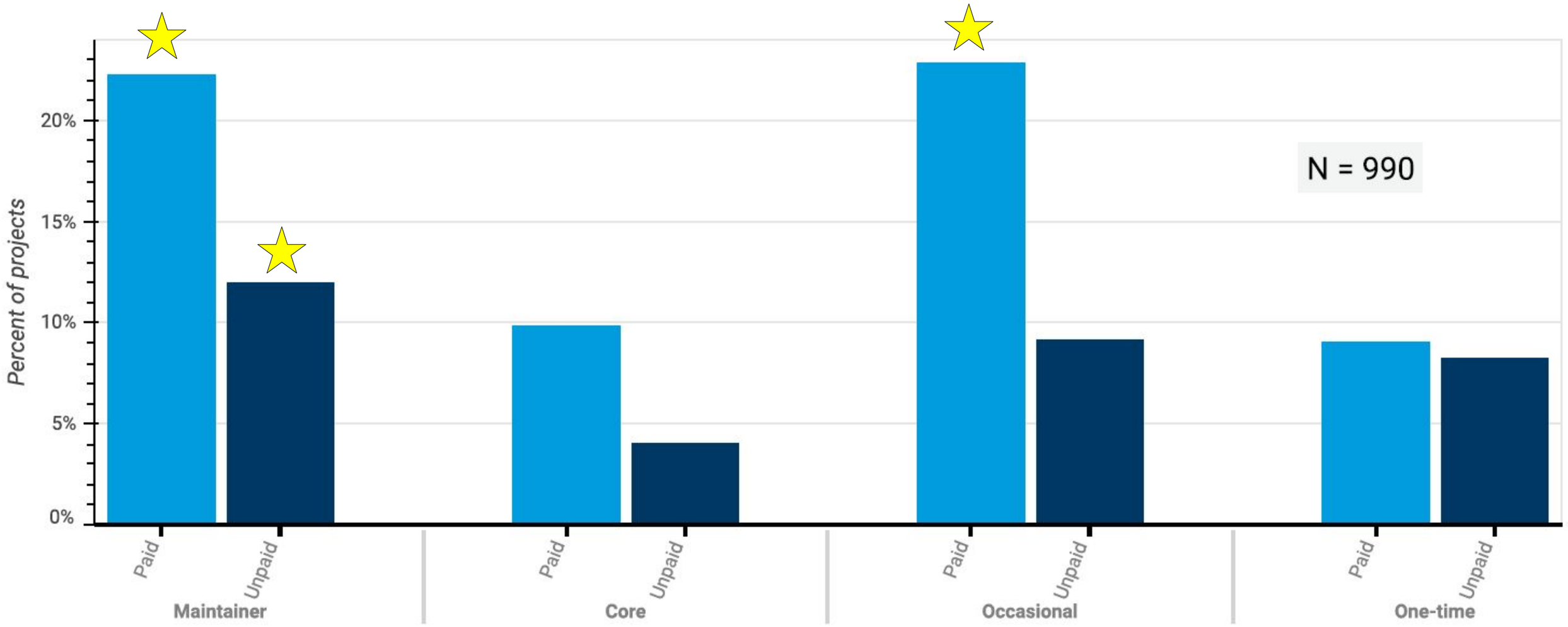


- Overwhelming majority are employed full-time
- Skills necessary to contribute to FOSS are highly valued in today's job market
- Despite the economic downturn due to COVID-19 pandemic, very few respondents were out of the workforce

THE LINUX FOUNDATION

LISH Laboratory for Innovation Science at Harvard

Contributors Receiving Payment by Contributor Status per Project

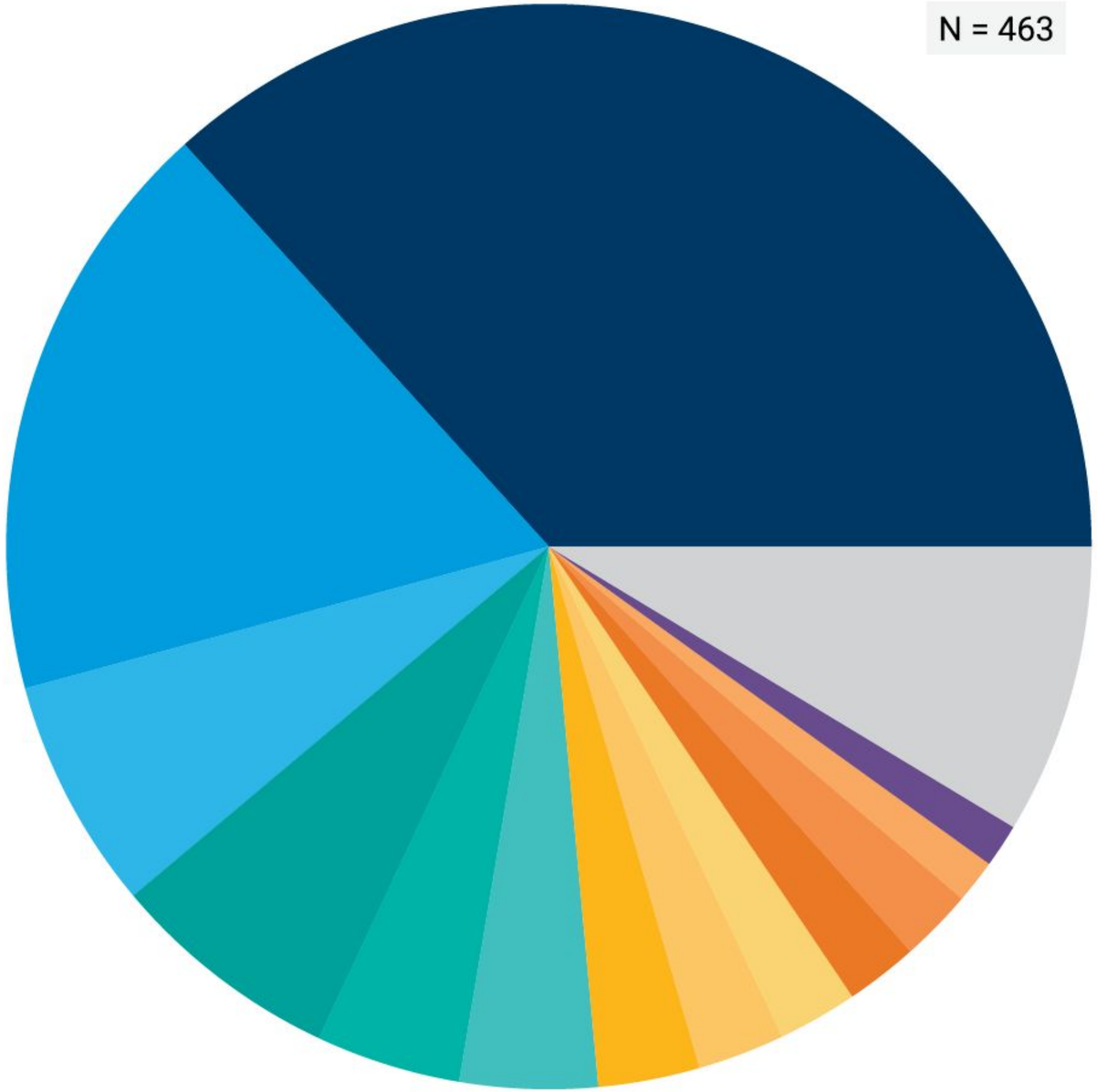


Stars identify the 3 most common groups & roughly correspond to the examples listed earlier.

THE LINUX FOUNDATION

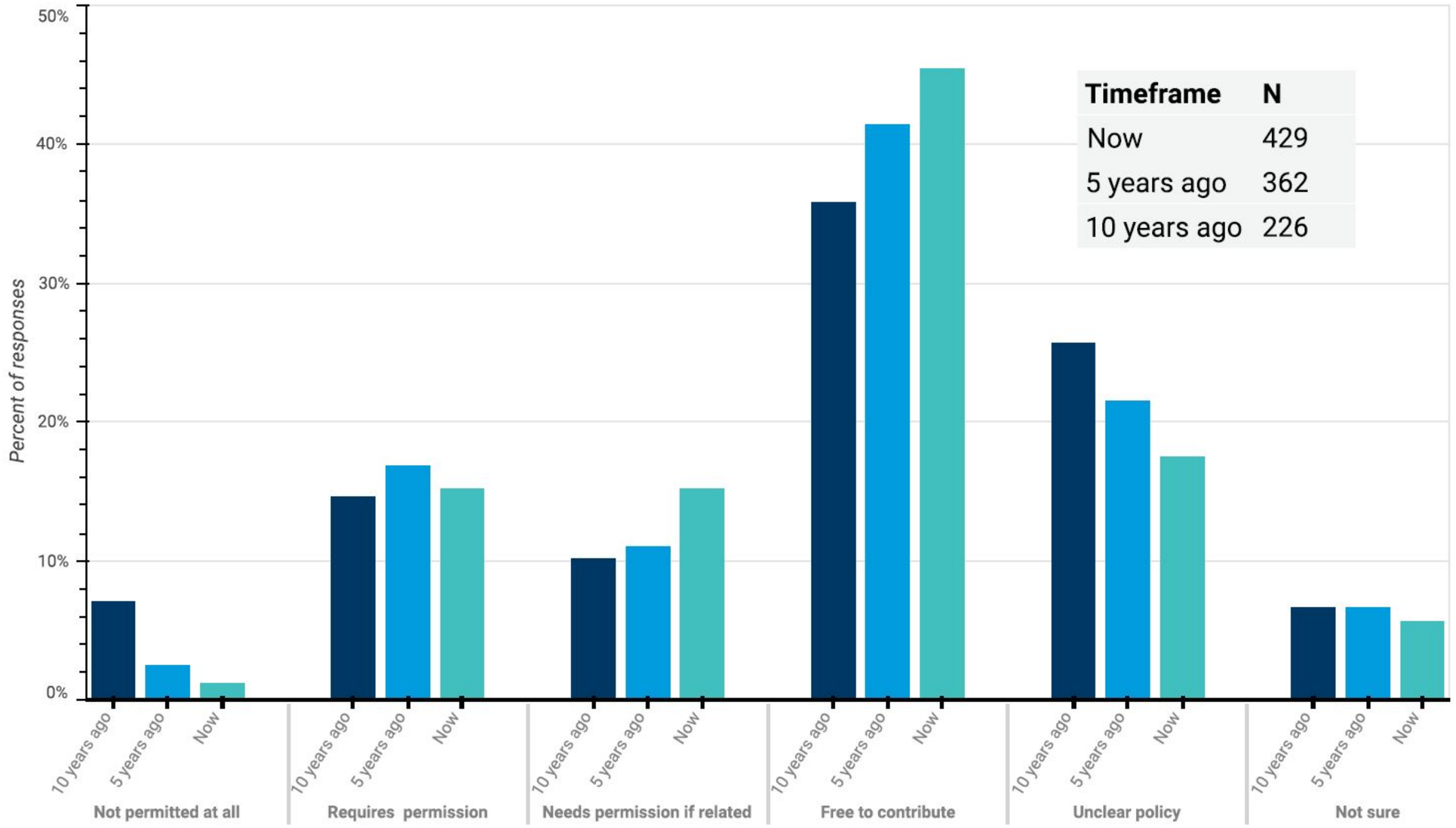
LISH Laboratory for Innovation Science at Harvard

Respondents' Employer by Sector



- Software Development: 37%
- IT Services: 17%
- Technology Hardware: 7%
- Finance and Insurance: 7%
- Telecommunications: 4%
- Educational Services: 4%
- Professional, Scientific, and Technical Services: 3%
- Health Care and Social Assistance: 3%
- Manufacturing: 2%
- Retail/Consumer Goods: 2%
- Non-profit: 2%
- Media: 1%
- Transportation and Warehousing: 1%
- Other: 9%

Employer's IP Policy Related to FOSS Contributions During Free Time



Timeframe	N
Now	429
5 years ago	362
10 years ago	226

THE LINUX FOUNDATION

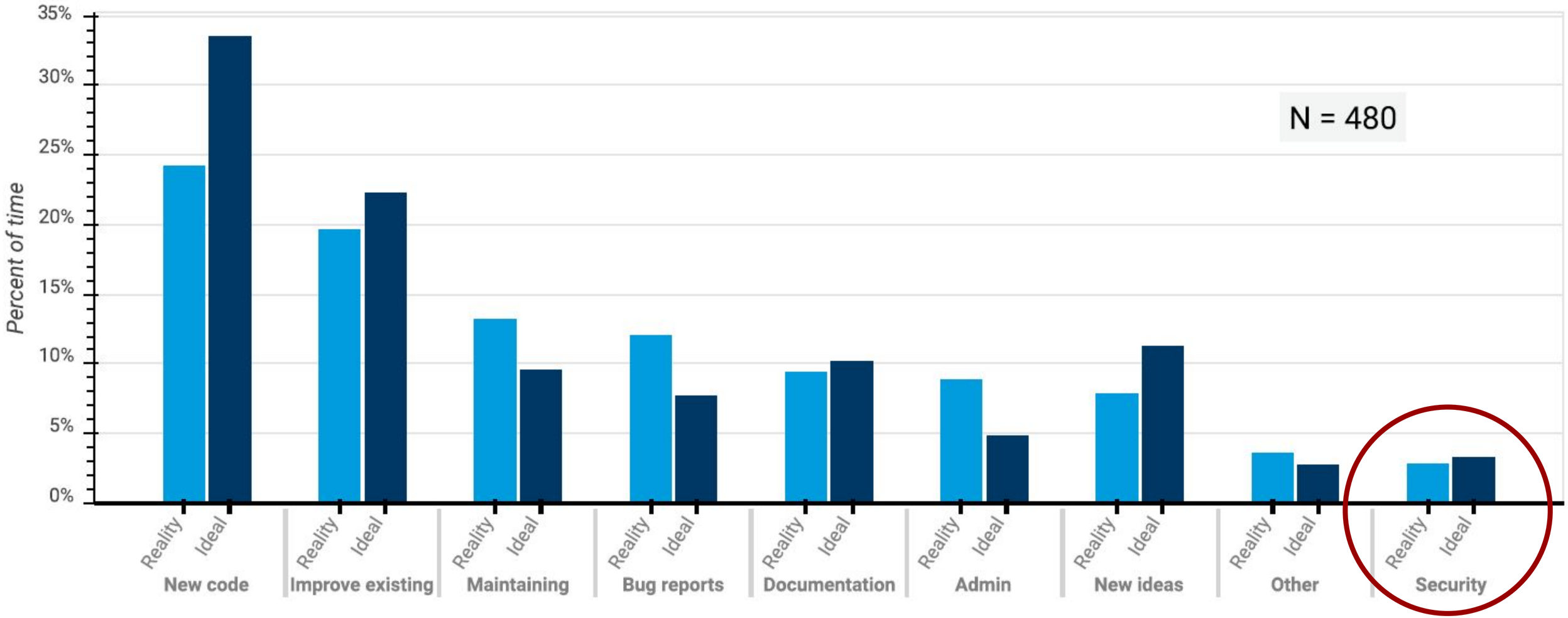
LISH Laboratory for Innovation Science at Harvard

Motivations for Contributing

Rank your primary motivations for contributing to the FOSS project you spend the most time on. *(#1 indicates the most important, #10 is the least important)*

- I enjoy learning
- I am paid to develop FOSS
- I value the recognition of my peers
- Contributing allows me to fulfill a need for creative, challenging, and/or enjoyable work
- I use this piece of FOSS and needed the specific features/fixes I added
- Since I use FOSS, I feel I should contribute back to it
- I believe in the mission of FOSS or the particular area I contribute to (e.g., privacy software)
- I expect my contributions will help me advance my career
- I enjoy working with my peers and my community
- I enjoy helping others

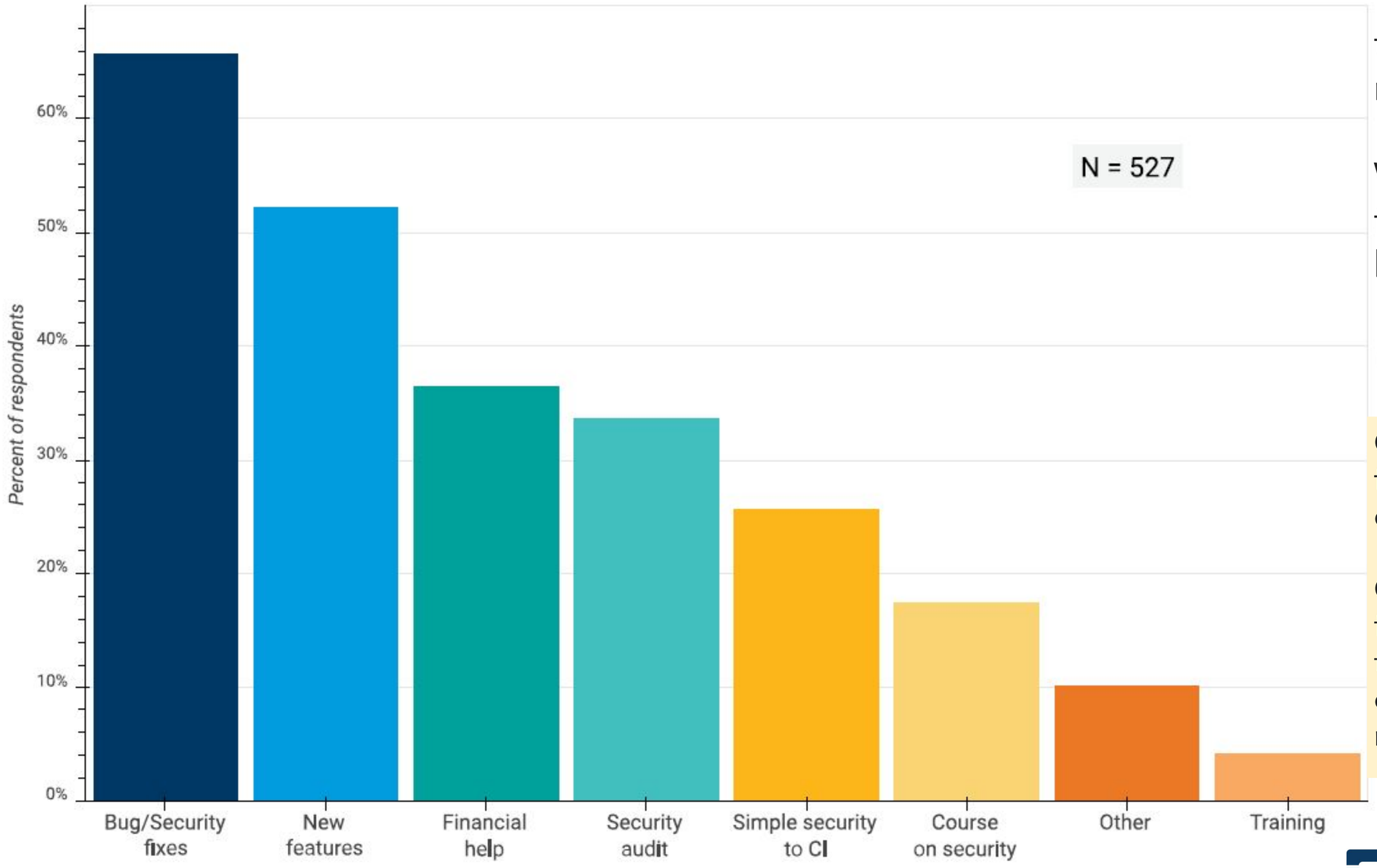
FOSS Time Allocation: Actual vs. Ideal



THE LINUX FOUNDATION

LISH Laboratory for Innovation Science at Harvard

Value of Contributions from External Sources



Think of the FOSS project to which you contribute that needs the most assistance.

What type of contribution from external sources would be most beneficial?

(Please select all that apply.)

Only 39% said that they received formal training in secure software development earlier in the survey.

Options like bug/security fixes, free security audits, simplified ways to add security tools, and a course on security rated high in the responses

THE LINUX FOUNDATION

LISH Laboratory for Innovation Science at Harvard

Summary & Suggested Actions

74.9%

of respondents are employed full-time

Leverage the top **3** motivations for contributing (all non-monetary)

1. Desire to learn
2. Need for features/fixes
3. Need for creative work

- Recognize value of skills gained from FOSS contributions
- Support learning process for new contributors
- Balance creative & mundane tasks for all contributors
- Consider other financial support (e.g., security audits, travel, etc.)

2.8%

of total reported contribution time is spent on security issues

There is a clear need to increase security efforts, while limiting the burden on contributors

- Fund security audits for critical FOSS projects
- Prioritize secure software development (SSD) best practices
- Make SSD training required for paid FOSS developers
- Incorporate security tools & automated tests into CI pipeline

48.7%

of respondents are paid by their employer to contribute to FOSS

As more contributors are paid by their employers, Stakeholders need to balance corporate and project interests

- Allay concerns over corporate involvement in FOSS through greater transparency & clear commitments
- Incentive paid contributors to dedicate time to mentoring new volunteer contributors
- Transfer FOSS projects to foundations w/ neutral governance

17.5%

of respondents reported that their employer had unclear FOSS policies

Despite companies' increasing openness towards their employees' involvement in FOSS, many still do not have clear FOSS policies.

- Clarify policies on when & how employees can contribute to FOSS
- Promote contributions to FOSS projects' security improvements - through individual employee's or collaborative efforts (e.g., OpenSSF)

THE LINUX FOUNDATION
LISH Laboratory for Innovation Science at Harvard

Open Source Developer Sample Personas

Enterprise Developer

- Full-time job at a company, works on OSS as part of their job working on some solution for their company
- Motivation: ensure the OSS works for the solution they are responsible for
- Security Training: formally trained in secure open source methods, but the focus is on the company's solutions, which may overlap with their OSS project or not.
- Some are full time maintainers on critical projects; many others touch multiple (5+) open source projects they rely on for their solution
- "Plate's full": their job security depends on meeting company's goals, not general security ideals

Contract Developer

- Freelance developer who often is closely associated with an OSS project and gets contracts to support various companies solutions using that OSS
- Motivation: has a connection to the OSS project
- Security Training: informal experience, not a proactive focus, but will respond to bugs
- Part time on everything, split many ways across contracts
- 150% overcommitted already, your secure OSS ideals are nice, but send me the patches because I don't have the time

Community Maintainer

- Unpaid maintainer
- Motivation: cares about OSS and this capability
- Security training: Typically none, as this is uncommon in universities & many developers don't get SW-related degrees
- Unpaid, so limited time
- Focused on what interests them, which is often not security
- "Send me the patches"

These sample personas are based on our direct experiences & consistent with the survey results

What can be done to improve OSS security?

- Efforts to dramatically increase the time contributors spend on security are unlikely to be welcomed
  a. “I find the enterprise of security a soul-withering chore and a subject best left for the lawyers and process freaks. I am an application developer.”
  b. “I find security an insufferably boring procedural hindrance.”

- Improve security practices while limiting the burden on contributors
  a. ID vulnerabilities in existing code (e.g., using audits and tools) & propose fixes
  b. Help modify CI pipelines to add problem-detecting tools (style, vulnerability detection)
  c. Audit critical OSS projects & develop patches
  d. Rewrite portions/components prone to vulnerabilities (e.g., for memory safety)
  e. Contribute hardening measures
  f. Require secure dev training for paid OSS developers (see free OpenSSF course)
  g. Use badging programs for secure dev practices (e.g., CII Best Practices badge)
  h. Ask influential OSS contributors to stress security
  i. Partner with mentoring programs to incorporate security best practices
  j. Simplify incorporating tools into CI pipelines

It IS possible to improve OSS security

- OpenSSL post-Heartbleed: LF CII founded & invested in OpenSSL, dramatically improved
  - Proactively looked for & fixed vulnerabilities, added hardening
  - Restructured & reformatted code
  - Earned CII Best Practices badge
  - Moved to common OSS license
- LF / CII audits - funded many (human) security audits to proactively find/fix problems
- OSS-Fuzz / Fuzz onboarding - contractors fuzz OSS, report vulnerabilities to OSS projects
- Google/LF underwriting some Linux kernel security development efforts
  - Triaging and fixing all warnings/bugs found with Clang/LLVM compilers
  - Eliminating several classes of buffer overflows by transforming all instances of zero-length and one-element arrays into flexible-array members (less error-prone approach)
  - Prevent whole vulnerability classes - Kernel Self Protection Project (KSPP)

Secure OSS by getting involved or paying someone to be involved

Sources: "The Impact of a Major Security Event on an Open Source Project: The Case of OpenSSL" by James Walden; CII Audit program; https://www.coreinfrastructure.org/programs/audit-program/ ; https://www.linuxfoundation.org/en/press-release/google-funds-linux-kernel-developers-to-focus-exclusively-on-security/

Ideas for US Government (1)

1. Identify OSS critical to US government & US critical infrastructure, and *invest*:
   - Identify which critical OSS need help (low resource & security concerns)
     - Analyze (fuzzing, static analysis, audit, etc.), help fix or replace, help improve their CI pipeline, help earn badges (e.g., CII Best Practices badge), constantly monitor
   - Identify common tools/libraries that are hard to use securely - help make security default
   - Help harden the OSS supply chain: counter typosquatting, malicious code insertion, stolen passwords, and non-reproducible build processes
   - Get involved with other organizations working on this (e.g., OpenSSF, Harvard/Linux)

2. Require developers of US government custom software to know how to develop secure software
   - OpenSSF has released free courses: https://openssf.org/edx-courses/
   - Those custom software developers (gov't & contractor) will also eventually write OSS

Ideas for US Government (2)

1. Encourage maturing & use of Software Bill of Materials (SBOM)
   - See National Telecommunications and Information Administration (NTIA)'s SBOM work

2. Update/eliminate the Vulnerabilities Equities Process (VEP)
   - Make process & charter public, Dept. of Commerce chairs, consider public impact (including critical infra) before withholding, disclose by default, require quarterly public stats showing timely disclosure

3. Ask NIST to formally define reproducible builds, move to requiring for high-criticality software
   - Could establish lab(s) to verify reproducible builds for OSS ("this reproduces" or "it doesn't, here's what it produces & a diffoscope comparison")

4. Require US ISPs to secure infrastructure (e.g., require RPKI to protect BGP: isbgpsafeyet.com)
   - OSS development *depends* on secured Internet infrastructure, yet US doesn't require it

5. Fund NVD/CVE proactively track vulns (↑complete),id project for automation

Question & Answer

Thank you!

Full report:
https://www.linuxfoundation.org/blog/2020/12/download-the-report-on-the-2020-foss-contributor-survey/

Interested in participating next year?
https://bit.ly/2021-FOSS-Survey

Questions: lish@harvard.edu

THE LINUX FOUNDATION

LISH Laboratory for Innovation Science at Harvard