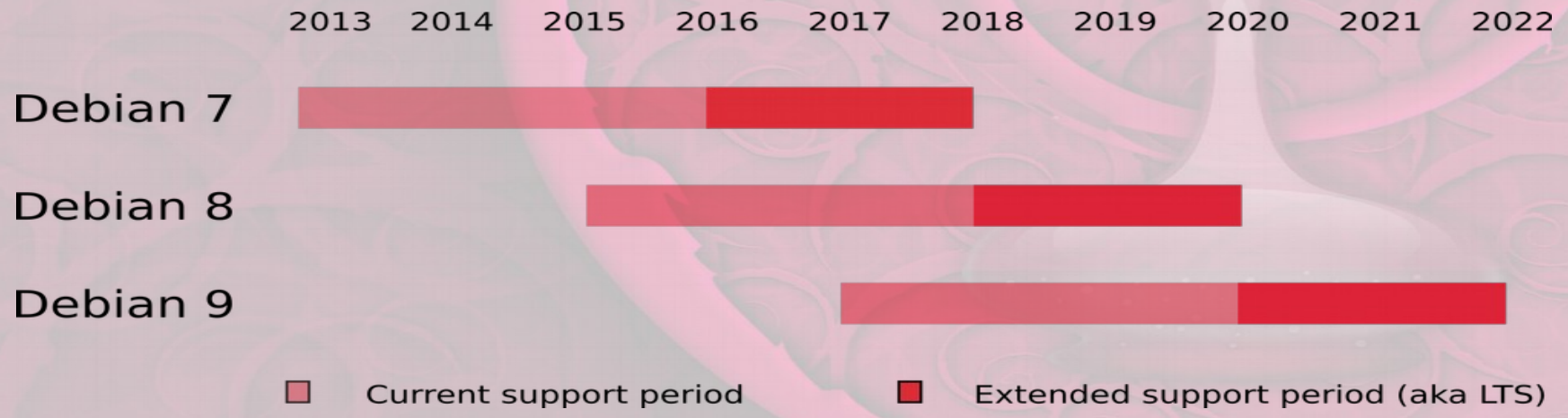
5 Years of Debian LTS Funding, What's Next ?

By Raphaël Hertzog <hertzog@debian.org>

MiniDebConf / Marseille / 2019-05-25

What is Debian LTS about ?

- Providing 5 years of security support
- Thus allowing users to skip a release



How did Debian LTS start ?

- A few Debian developers were doing long term security support of specific packages within their own company
  - Decided to try to work together and share their work
- Public call for others to join
  - Either by allocating time to their employees to contribute
  - Or by paying to fund the work of Debian contributors
    - https://wiki.debian.org/LTS/Funding
    - In practice, most of the (wanting to be) paid contributors joined forces behind a single offer managed by Freexian SARL : https://www.freexian.com/services/debian-lts.html

Freexian's intermediary role

Sponsors

Contributors

1. Collect money
2. Dispatch work hours
3. Work on Debian LTS
4. Collect/publish reports
5. Pay contributors

How it evolved ?

- More architectures supported
  - i386/amd64 → i386/amd64/armel/armhf
  - arm64 likely for stretch
- More packages supported
  - a subset → almost all packages
  - some are supported by third parties
    - Freexian pays Credativ to support Xen

How it evolved ?

- Almost all LTS security updates are now provided by contributors paid by Freexian
  - Paid contributors react more quickly than employees allowed to work on LTS
  - Package maintainers are no longer sollicited to provide updates. There are enough sponsors to cover the full workload.
  - There are exceptions: PostgreSQL by Credativ, and a few package maintainers that are very reactive.

Extended LTS

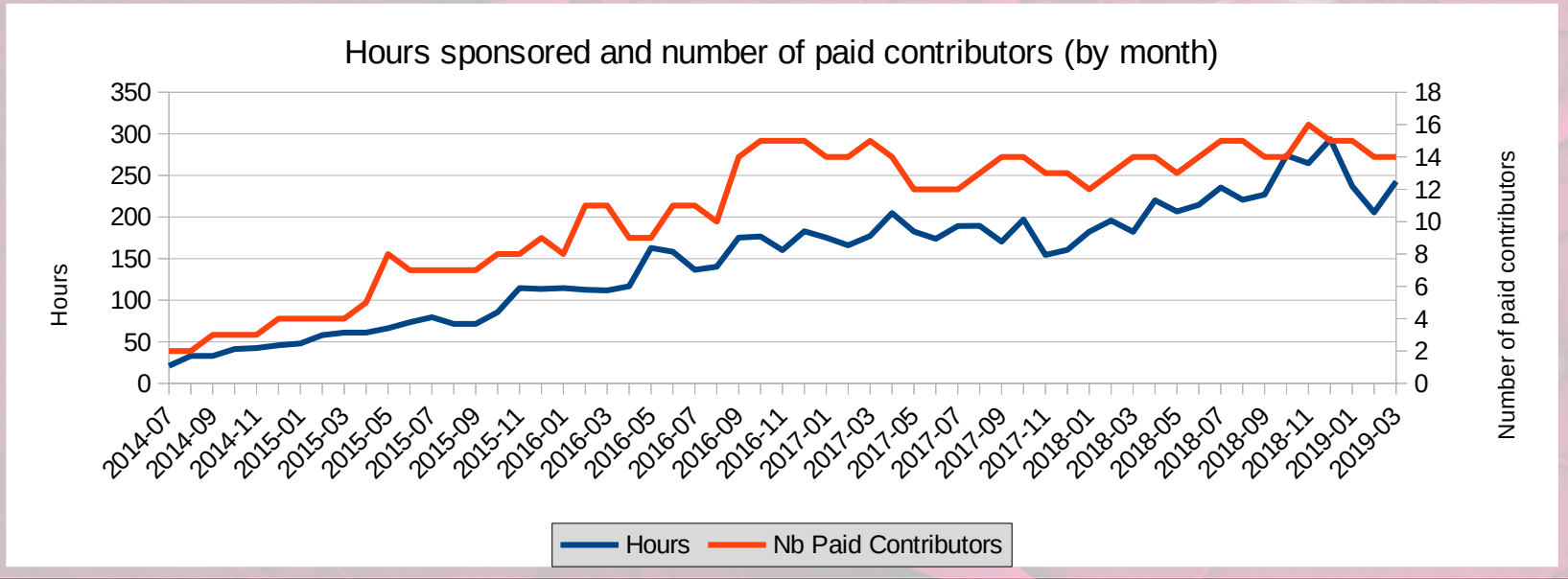
- Some sponsors wanted more than 5 years
- New offer :
  - Only their packages are supported
  - amd64 and i386 only
  - Cost is determined based on package list
  - Cost is evaluated each quarter
    - split among all sponsors (up to 8000 EUR/quarter)
    - goes up when sponsors stop

Wheezy Extended LTS

- First try with Extended LTS
- Will likely last until December 2019
  - i.e. 5 years + 19 months
- https://deb.freexian.com/extended-lts/

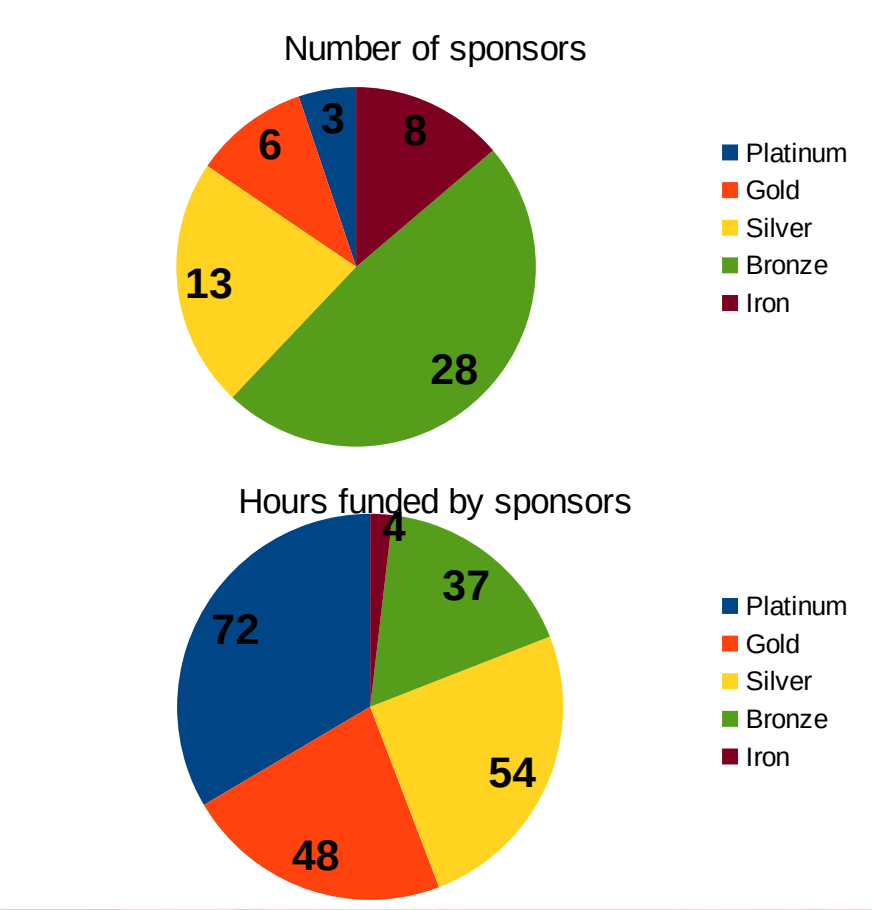
Some figures

- 5 years already! (June 2014)
- 24 contributors got paid, 14 currently
- 215 hours funded per month



Some figures about sponsors

- 58 sponsors (215 hours/ month)
  - 3 platinum (72 h)
  - 6 gold (48 h)
  - 13 silver (54 h)
  - 28 bronze (37 h)
  - 8 iron (4 h)



$erious mon€y

- Over 5 years:
  - 592,800 € paid to Debian LTS contributors
  - 81,450 € paid to the most active contributor
- 31,050 € paid to the former Debian Project Leader during his 2 years of leadership

Clear rules to prevent problems

- Rules for:
  - Who can join
  - How hours are split among contributors
  - What must be done on paid time
  - What else can be done on paid time
  - Who decides in case of problems
- Expectations are clearly documented

Open rules to join the set of paid contributors

- Documented on Freexian's website (from the start), no arbitrary selection:
  - Debian Developer or Debian Maintainer
  - Prior experience with security updates
  - Good programming skills (multiple languages)
  - Can emit invoices to Freexian
  - Accept the rules
    - Privacy of customer data
    - Public monthly report
    - Debian code of conduct, obligation to respond to queries
    - Best effort to meet high quality standards of security team

Hours allocation rules

- **Available hours split evenly across all contributors** (in the limit they fix for themselves)
- Never assign less than 8 hours per contributor. If we had to, we would organize a rotation to ensure this.
- Few hours per contributor → resilient team

What must be done on paid time ?

- CVE triaging (week of frontdesk duty)
- Prepare and publish security updates for the LTS release
- Respond to queries of other Debian contributors
- Public monthly report
- All this while respecting the Debian Code of Conduct

What can be done on paid time ?

- Write the patch if upstream hasn’t done so
- Prepare security updates for stable and unstable in some cases
- Work on the security infrastructure (security tracker mainly)
- Work on improving packages from a security perspective
  - Enabling hardening flags
  - Adding DEP-8 tests (autopkgtest) → easier to test a security update

Who decides in case of problems ?

- Freexian, as the trusted intermediary, thus me.
  - Currently delegating the day-to-day management to Holger Levsen.
- That said decisions are usually taken by consensus among all the paid contributors.

Lessons learned

- It's possible to pay Debian contributors without disrupting the entire community
- Care must be taken at many levels:
  - To work transparently and in an inclusive way
  - To avoid someone getting locked in a paid position
  - To have fair criteria to use the money or at least a fair chance of being paid
- You must be aware that it will have consequences
  - Change of priorities for some volunteers

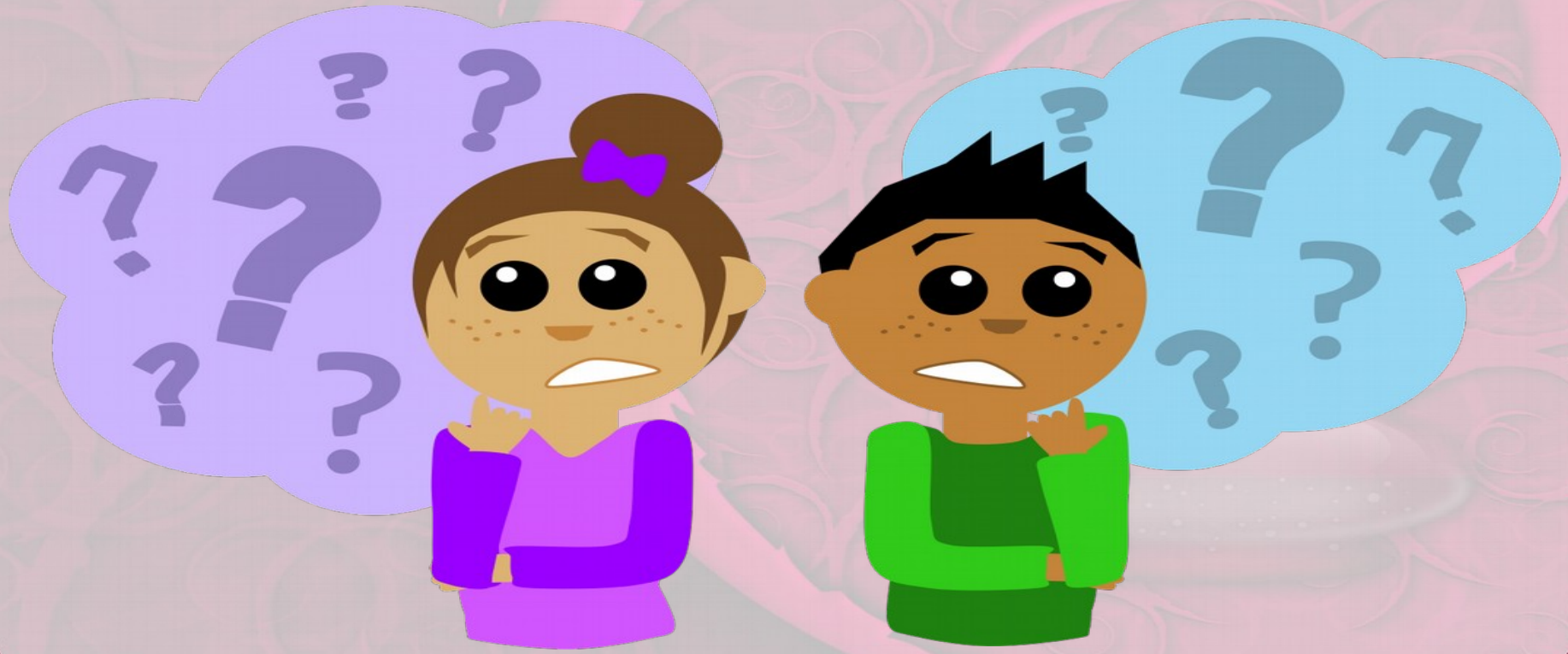
What else could be funded ?

- Package maintenance
  - Orphaned packages, new packages
  - Monitoring of important packages
  - Ex: tryton (paid by Freexian)
- New infrastructure
  - PPA (Personal Package Archive)
  - Wishlist bugs on tracker.debian.org
  - ...

What else could be funded ?

- Repetitive / thankless tasks
  - NEW review
  - review of unblock requests during freeze
  - Creation of debian/copyright for complex packages ?
- Leadership roles ?
  - Molly de blanc: http://deblanc.net/blog/2019/05/21/remuneration/

Questions ?



Credits & License

- Content by Raphaël Hertzog
  http://raphaelhertzog.com
  License: GPL-2+
- Cliparts from https://openclipart.org
  License: Public domain
- OpenOffice.org template by Raphaël Hertzog
  http://raphaelhertzog.com/go/ooo-template
  License: GPL-2+
- Background image by Alexis Younes “ayo”
  http://www.73lab.com
  License: GPL-2+