OpenSSL CONFERENCE

git revert: review of an OpenSSL fork

Rich Salz, Akamai Technologies

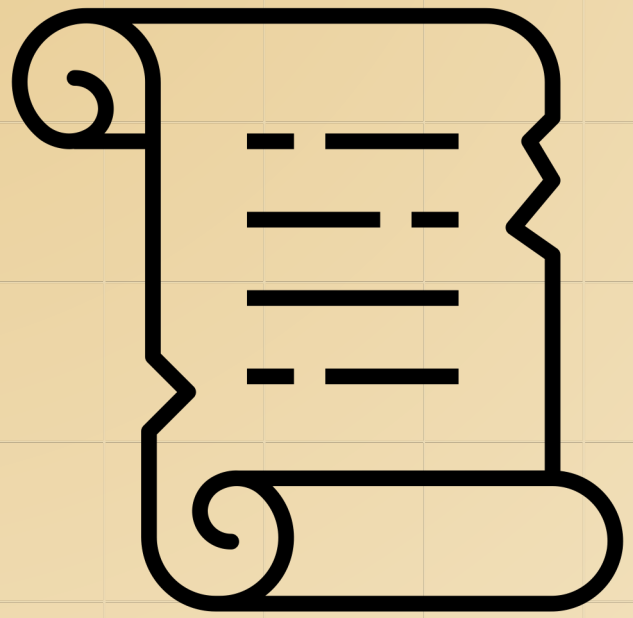
§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

20.10.2026

My background

Who, what, and why?

What happened?



Hofstadter's Law:

It always takes longer than you expect even when you take into account Hofstadter's law.

Why did they do that?

First regrouping

Second regrouping

What we accomplished

OpenSSL CONFERENCE

- Shrink down Perl use (the templating library; if all you have is a knife)
  - Add six simple programs
- Moved to modern C, Posix, etc.
- Remove a bunch of old platforms
  - VMS: 184 files, 6500 deletions
- Removed a bunch of old config options (nextprotoneg) TLS 1.3 is mandatory
- Converted to Cmake
- Reported all fixes “upstream“ to OpenSSL

We did not succeed

THE ASF

"Communit
y over
code"

Why?

- A few stellar volunteers
- Nobody really interested in rebasing their upstream
- And most important:
  - We (mostly) ported QUIC to the OpenSSL API

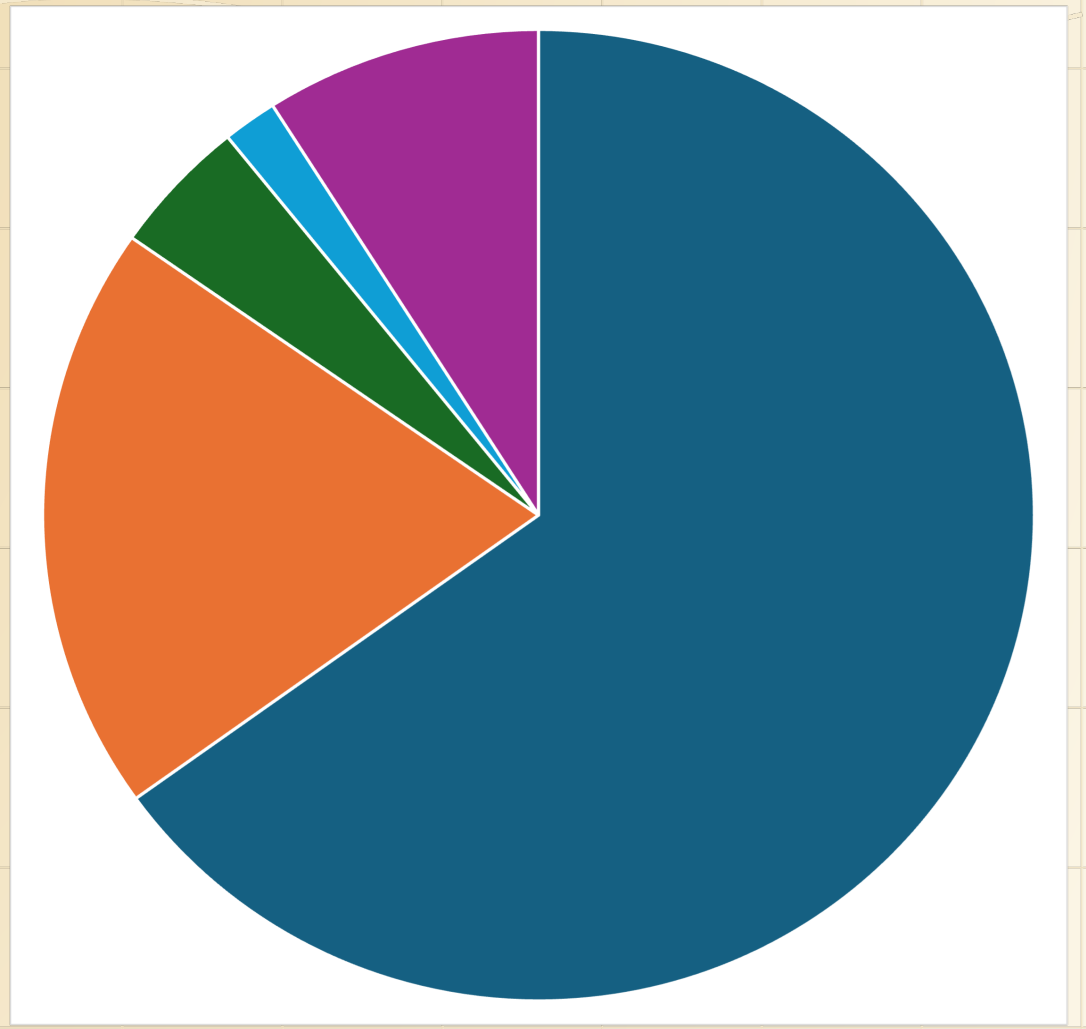
Lessons for upstream

OpenSSL CONFERENCE

- OpenSSL is a small software company
- Give up on QUIC, it's a resource-sink
  - Nobody wants a unified programming model
- Do you want to build a community?

In nine months...

- January – September, 2026
- There were 2,3696 commits
- 1538 were by paid staff
- 463 external committers
- 107 by the public
- 42 by someone using Claude Opus
- 213 by public with fewer than 11 commits



It‘s always technical debt

- There are 546 open PR‘s
  - Oldest non-WIP is from 2021
- There are over 1,000 issues
  - Oldest is from 2018
- Do you want to build a community?