



# osql: The community oriented osquery fork

Stefano Bonicatti, Mark Mossberg  
QueryCon 2019



## Stefano Bonicatti

Software Engineer

---

`stefano.bonicatti@trailofbits.com`



## Mark Mossberg

Senior Security Engineer

---

`mark@trailofbits.com`

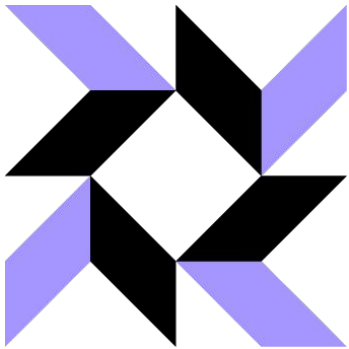
What is osql?

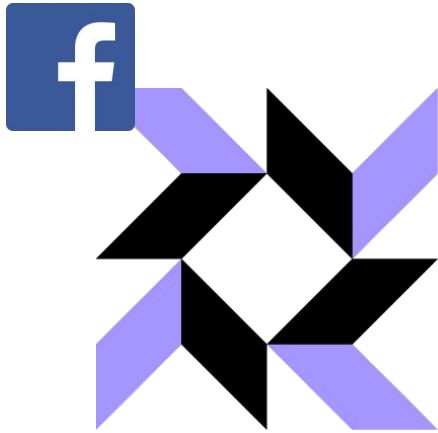
TRAIL  
OF  
BITS

**What is the relationship between  
osql and osquery?**

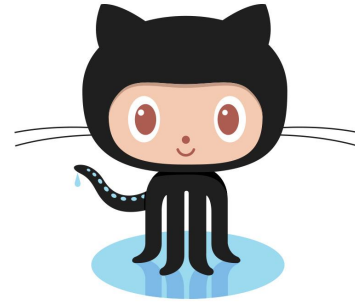
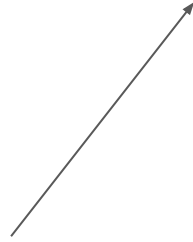
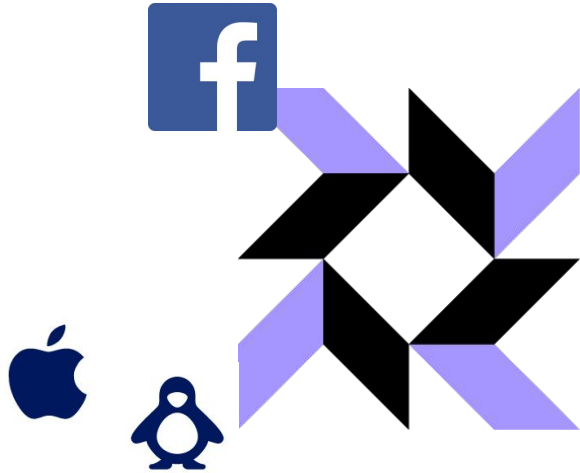
How is osql pronounced?

TRAIL  
OF  
BITS

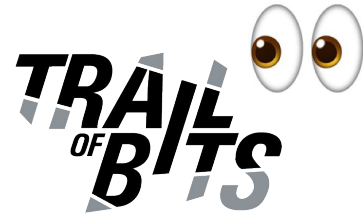
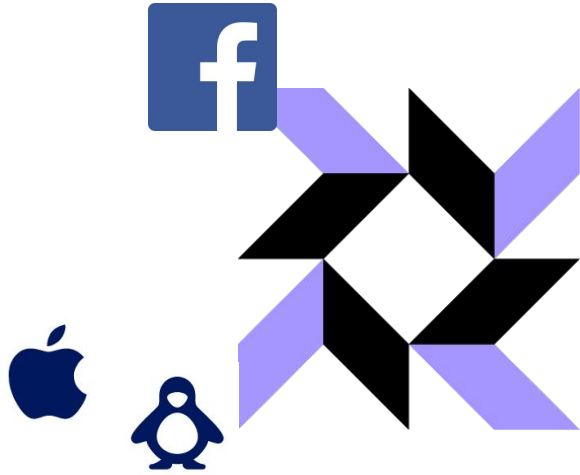


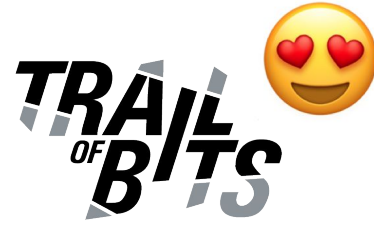
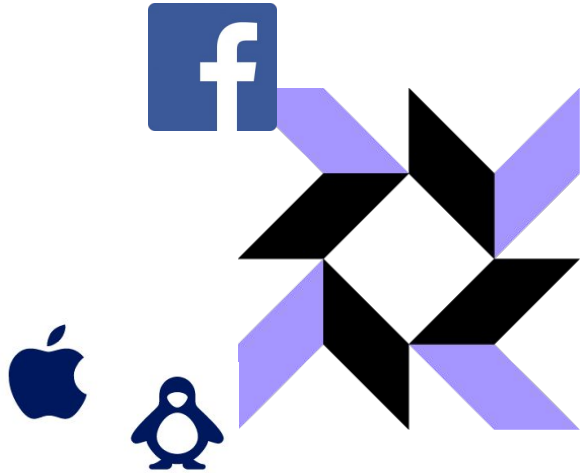


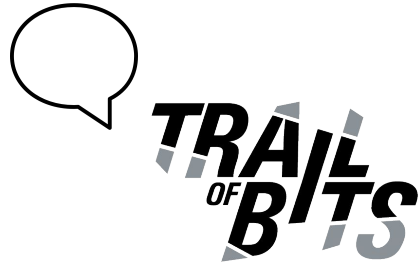
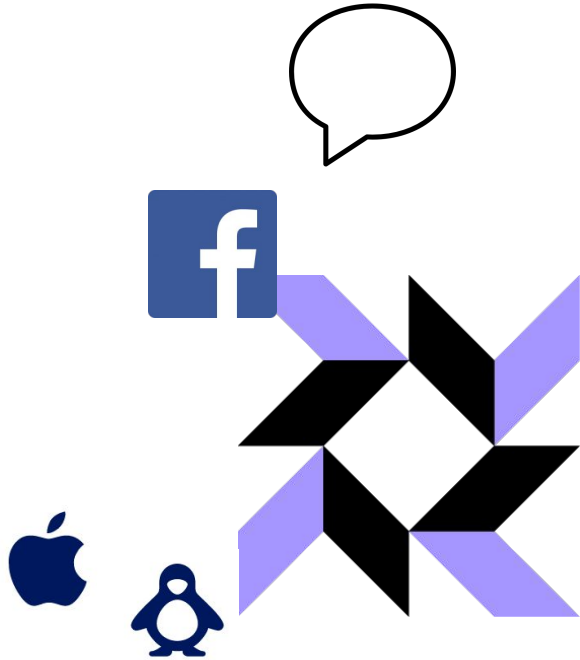
2014

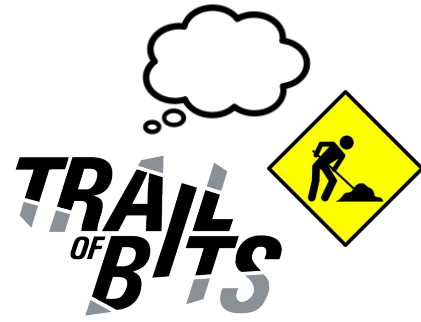
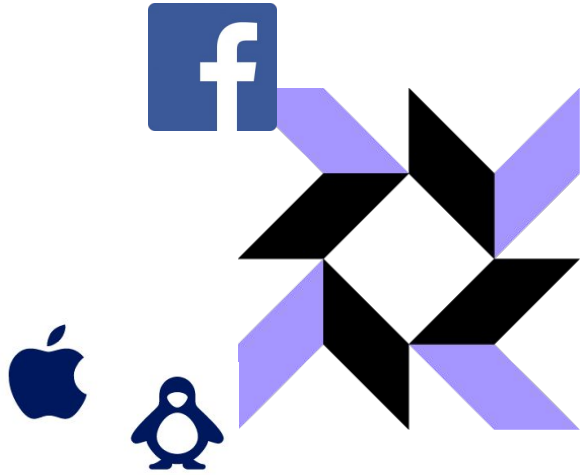




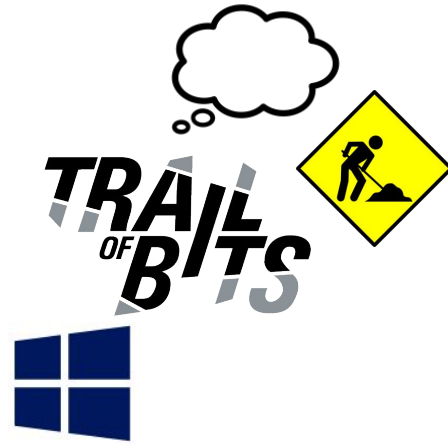
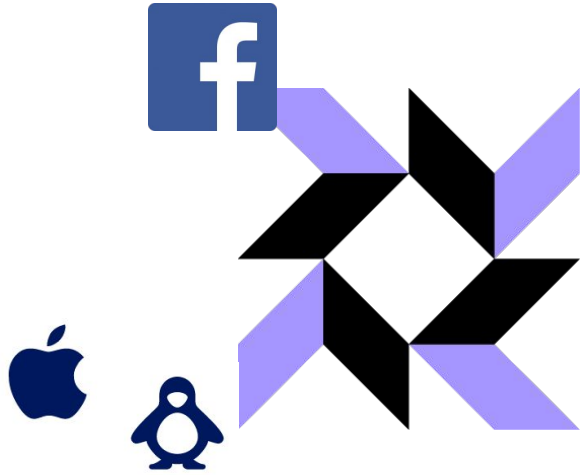


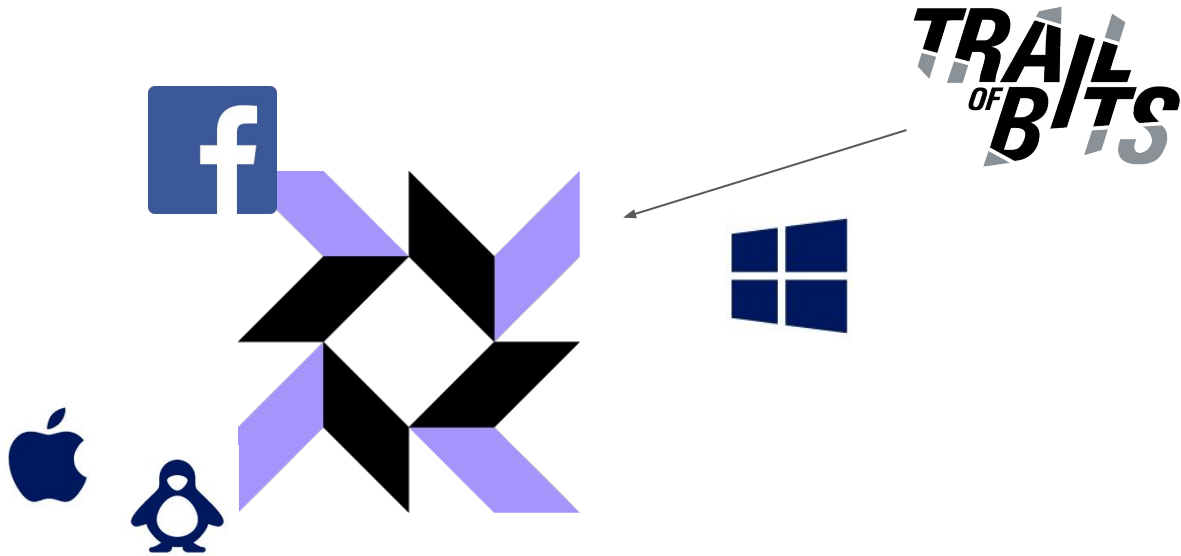


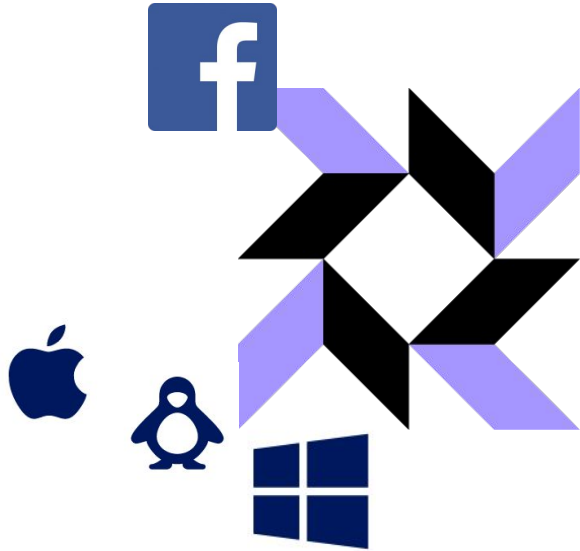




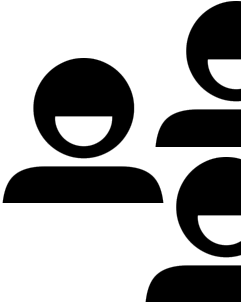
2016

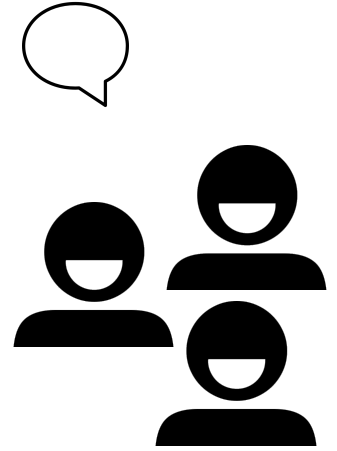
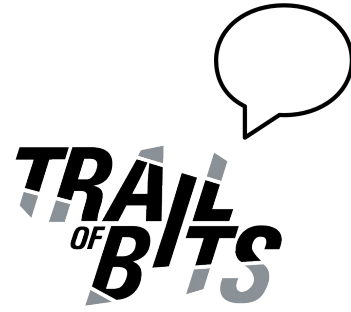
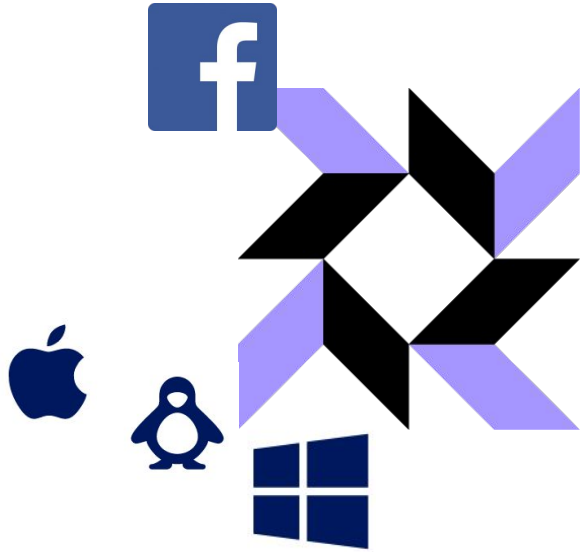




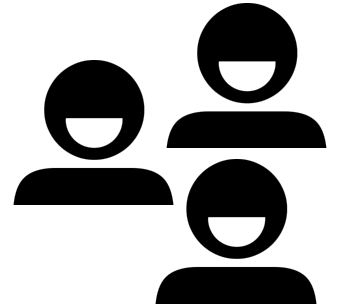
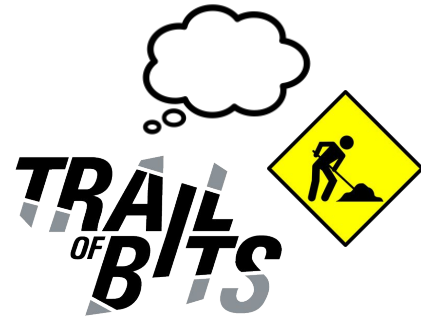
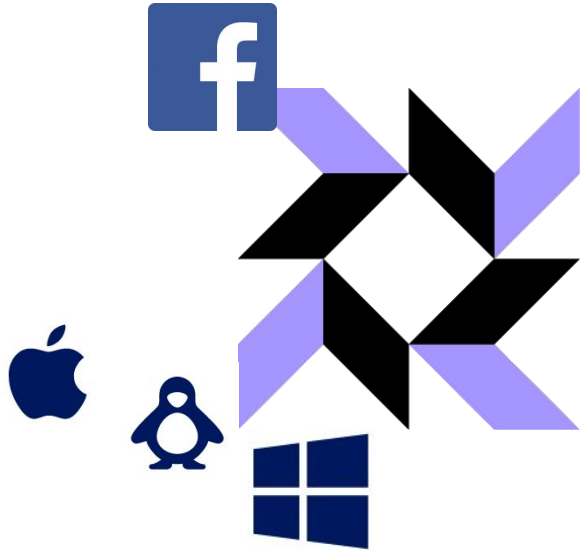


**TRAIL**  
*OF*  
**BITS**

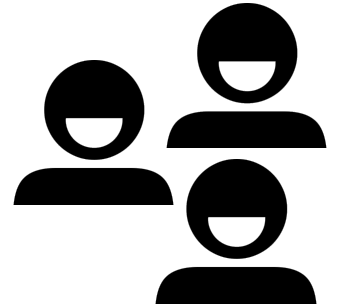
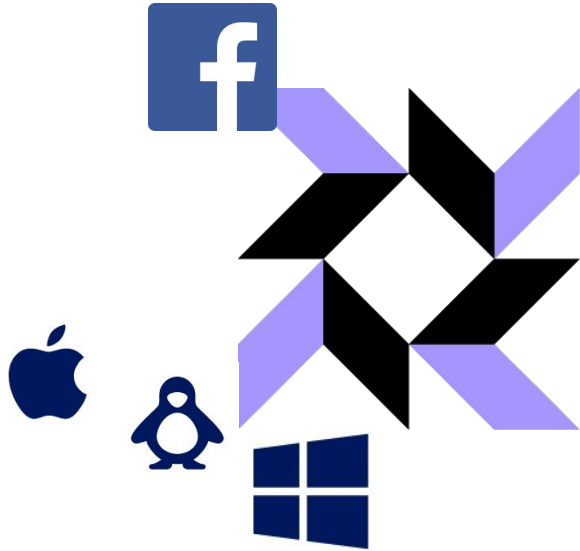


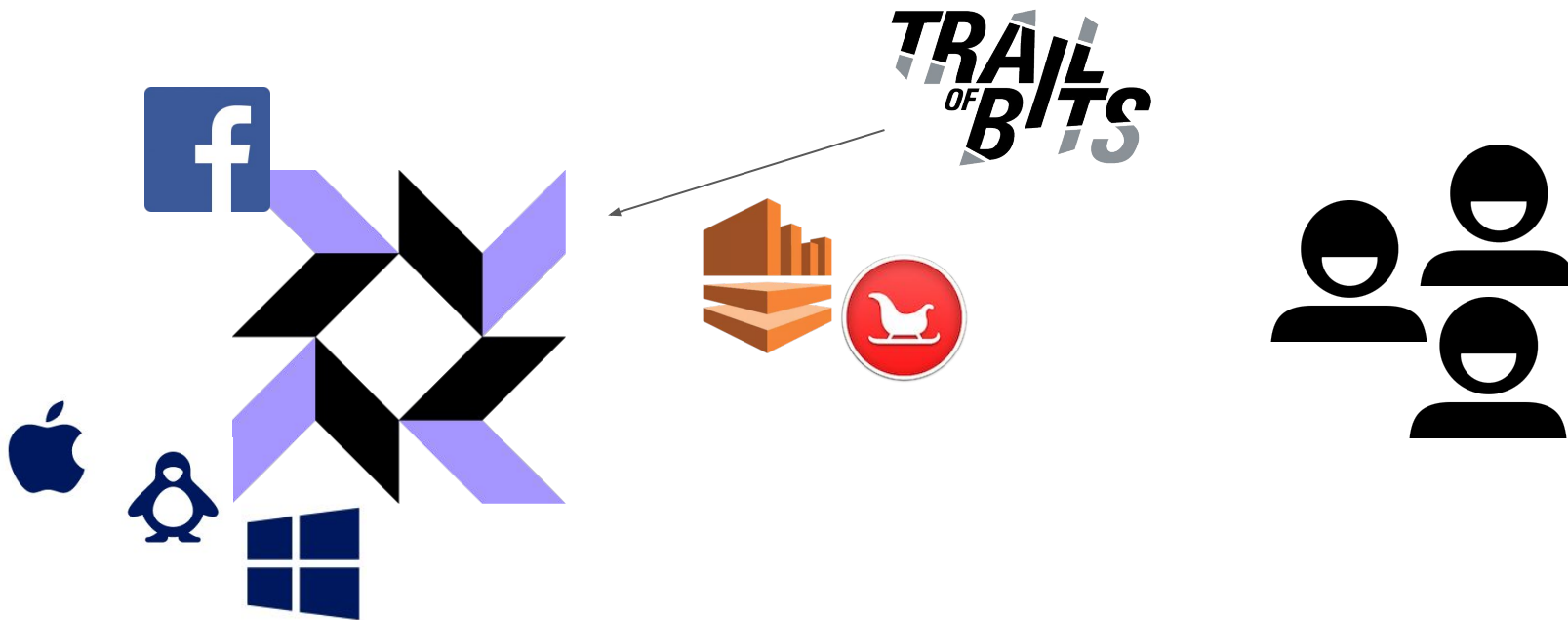


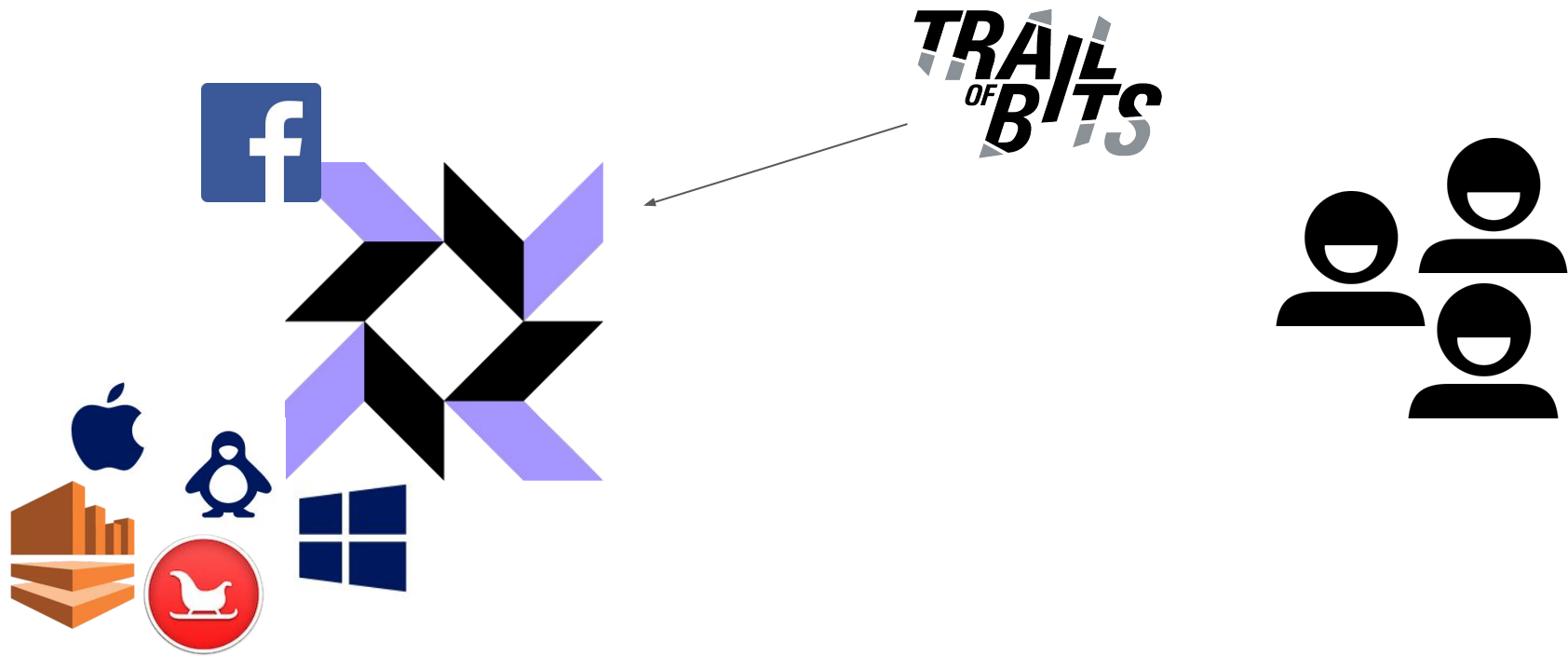


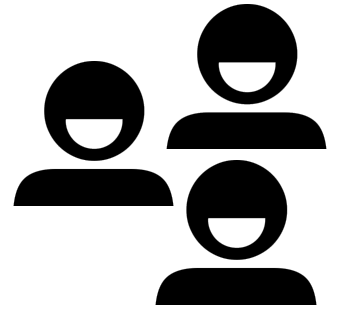
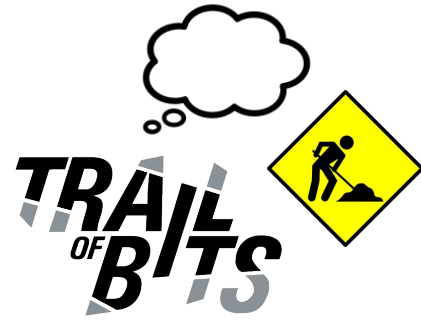


2017-2018





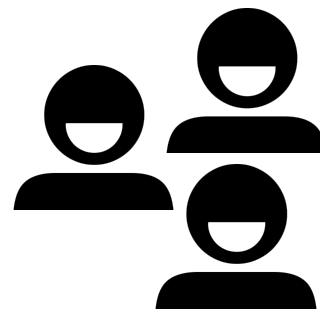


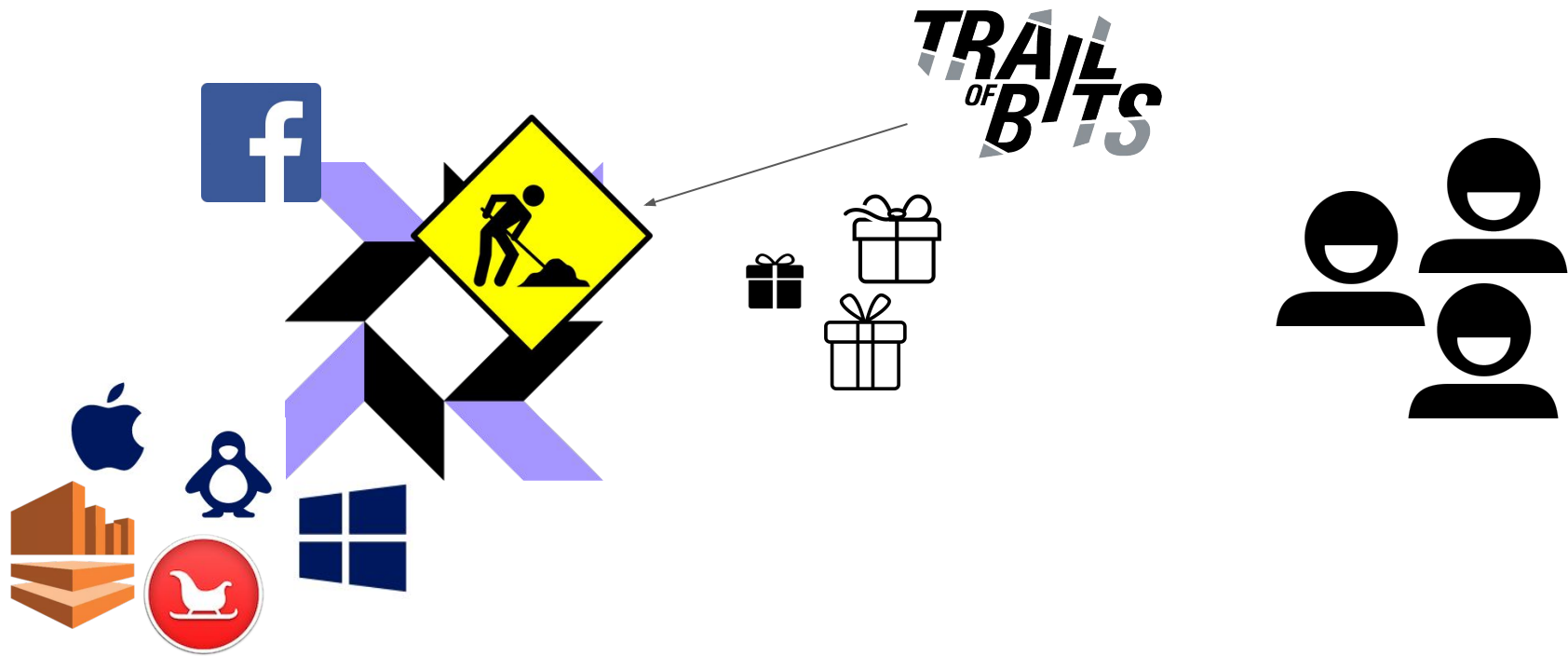


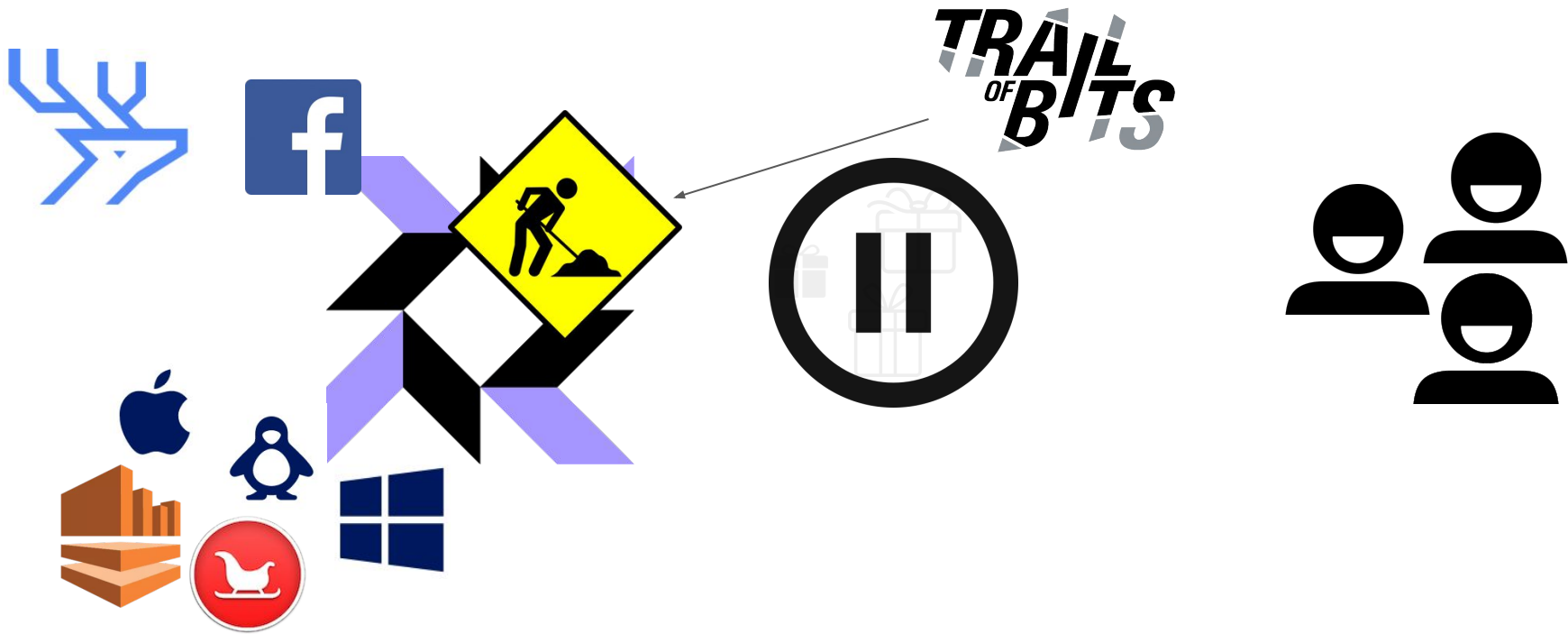
late 2018



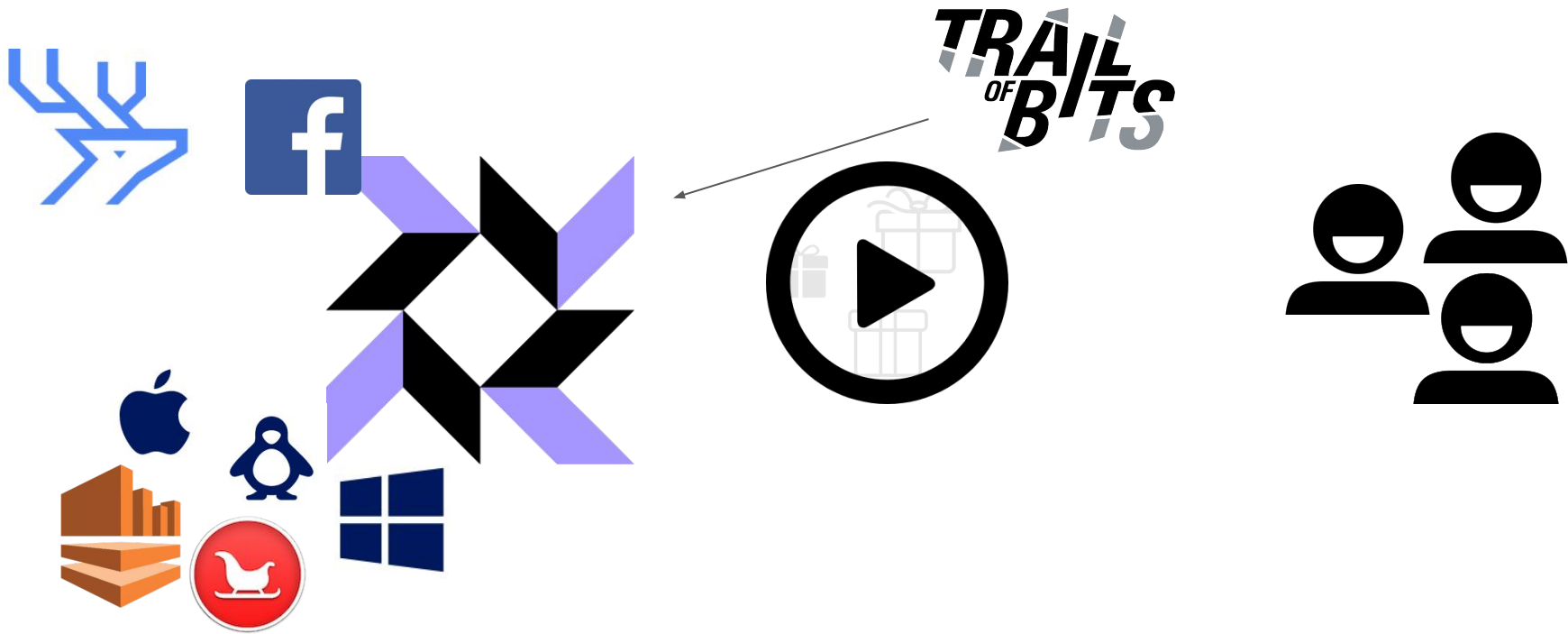
**TRAIL**  
*OF*  
**BITS**



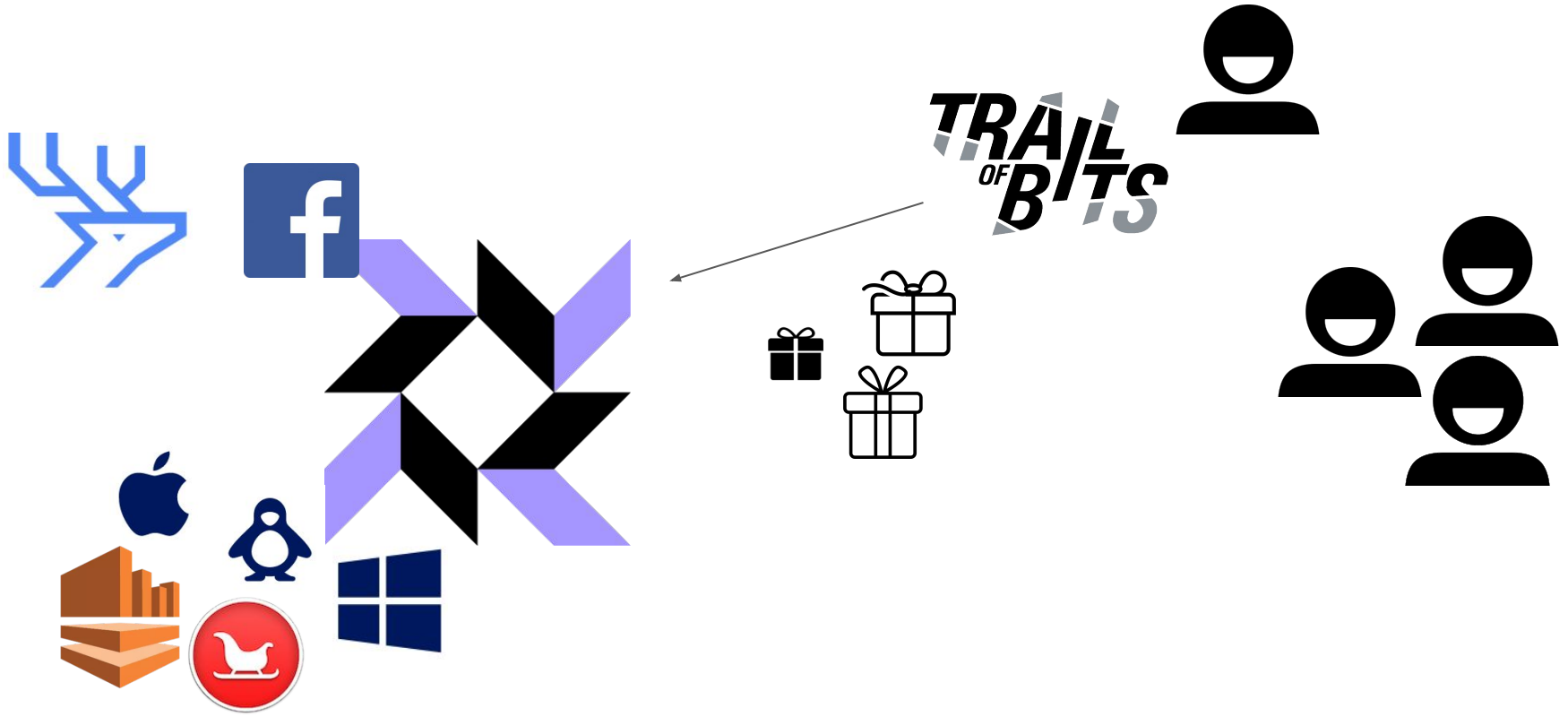


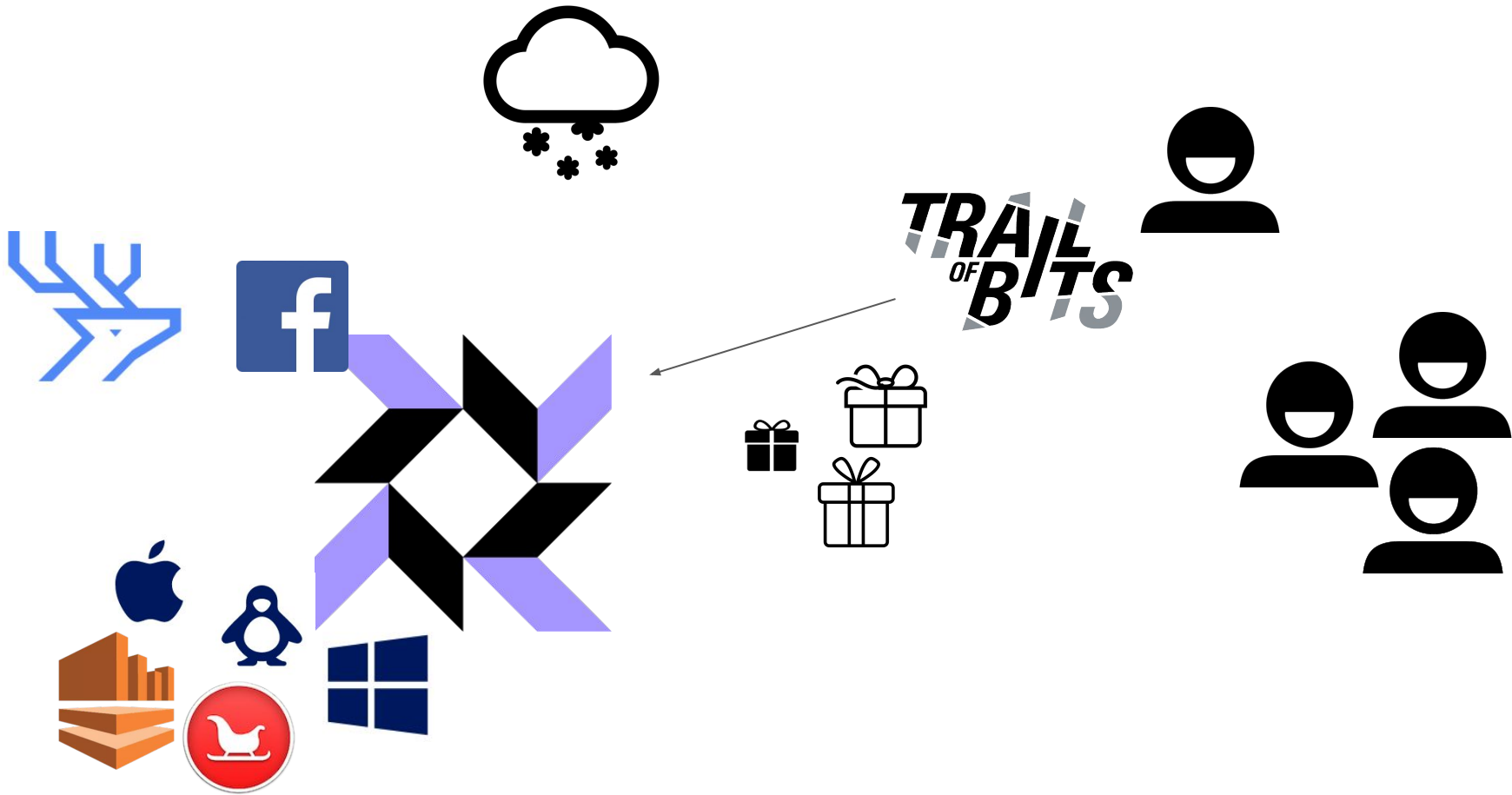


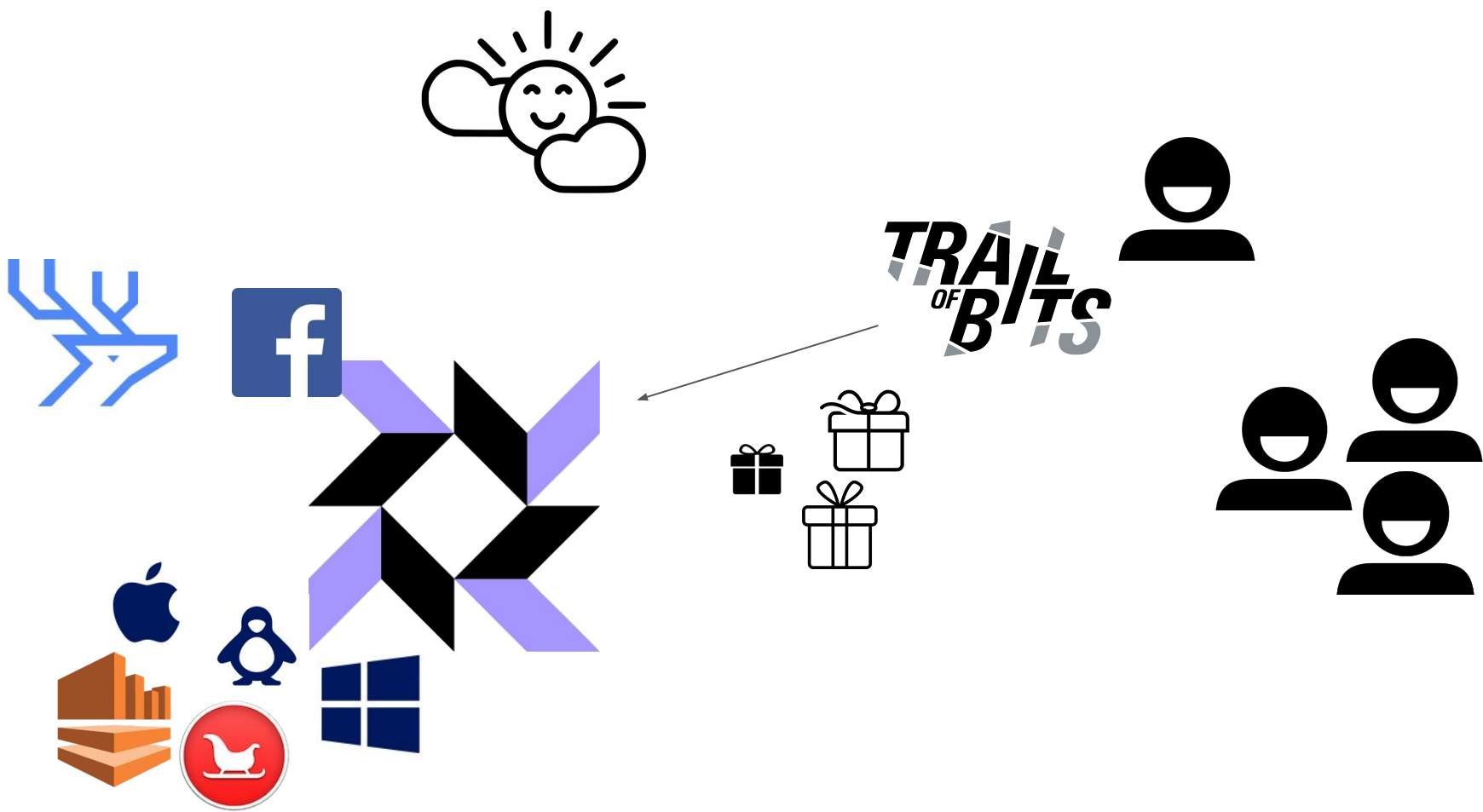


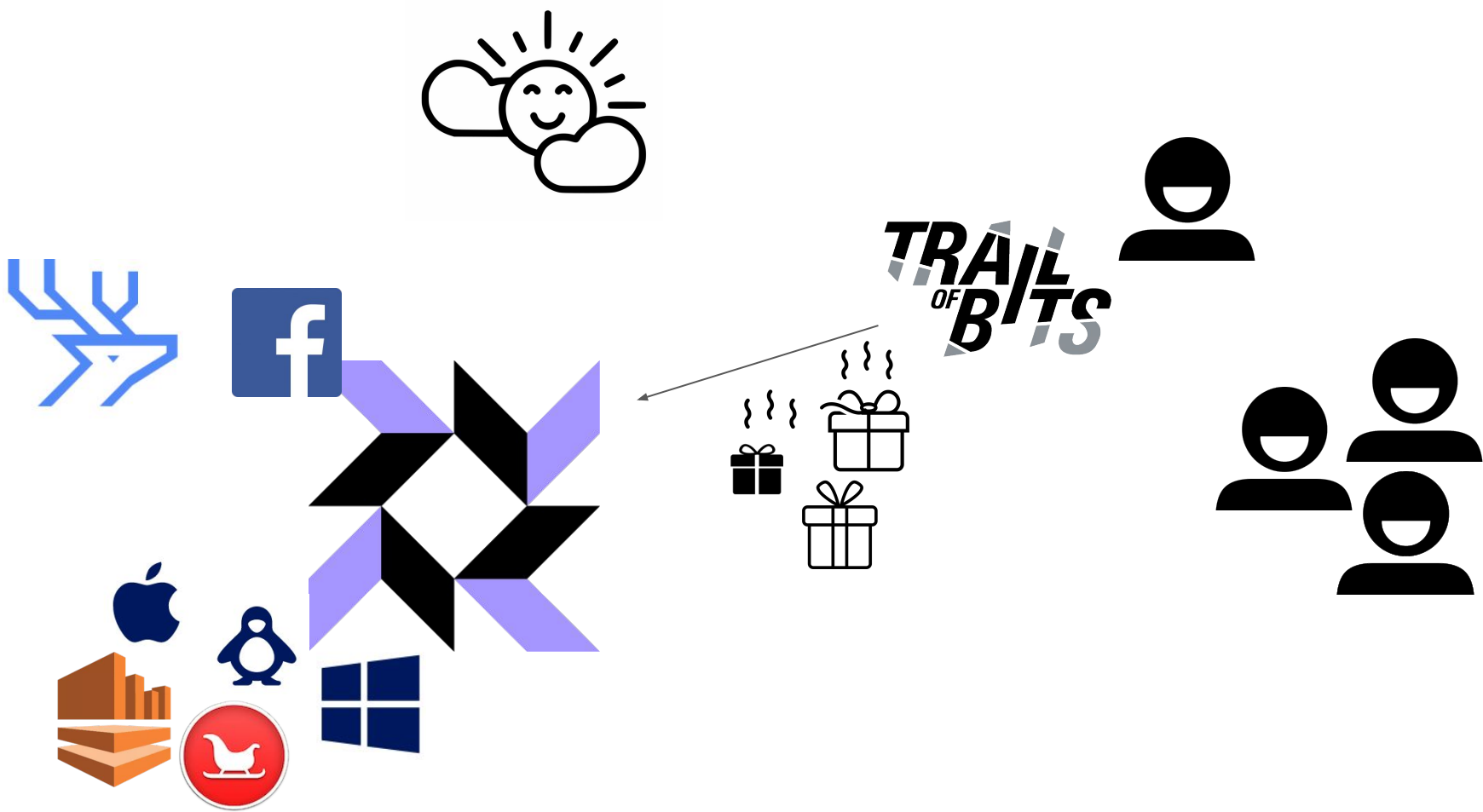


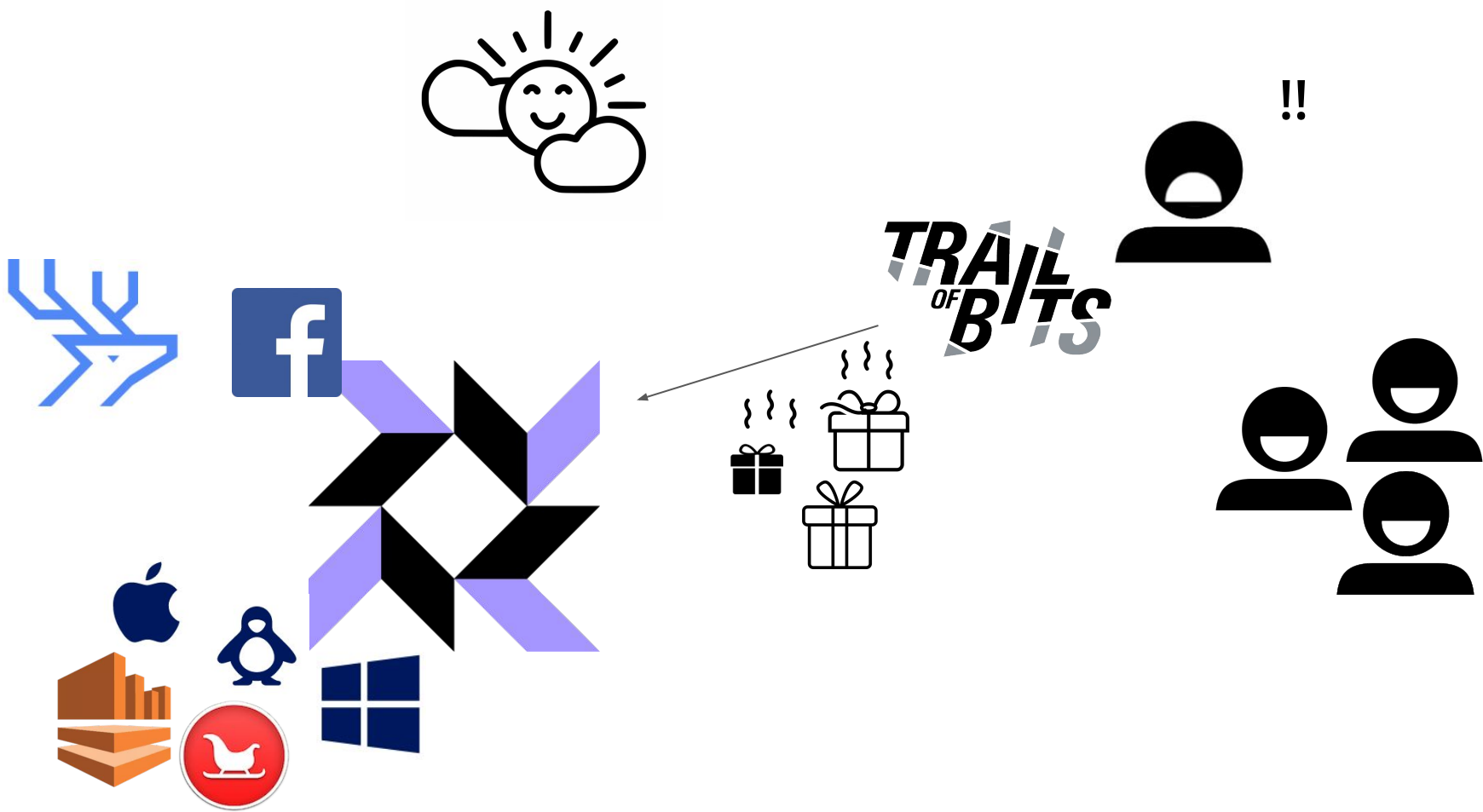


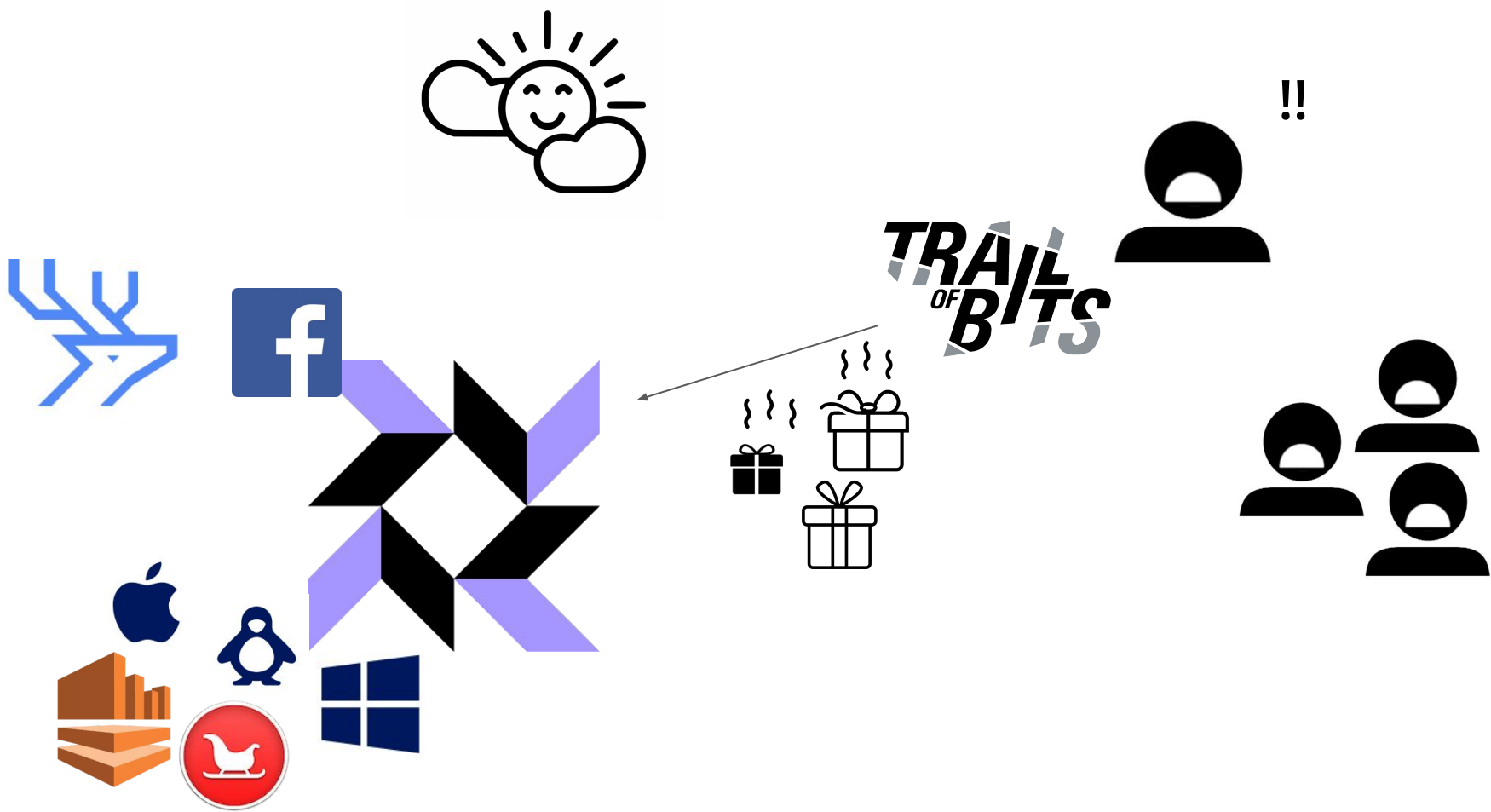
















# osql

 **Repositories** 8

 **People** 19

 **Teams** 2

 **Projects** 0

## Pinned repositories

 **osql**

SQL powered operating system instrumentation, monitoring, and analytics.

 C++  11  6

 **osql-experimental**

A community-oriented fork of osquery with support for cmake, public CI testing, and regular releases

 CMake  65  2



osql

Repositories 8

People 19

Teams 2

Projects 0

Original osql

### Pinned repositories

osql

SQL powered operating system instrumentation, monitoring, and analytics.

C++ ★ 11 🍴 6

osql-experimental

A community-oriented fork of osquery with support for cmake, public CI testing, and regular releases

CMake ★ 65 🍴 2

- Public continuous integration & testing
- Standard build system (CMake)
- Regular releases, including community-reviewed PRs

Hard-fork osquery



# Anti-Goals


Hard-fork osquery







# “soft fork”

● CMake 99.6%

Branch: master ▾    New pull request

 **Smjert** Update Azure Pipelines to use osql-experimental Docker re

 <a href="#">cmake</a>	Do not require the source
 <a href="#">osquery-src @ c55eb57</a>	Sync with experimental c
 <a href="#">osquery</a>	Sync with experimental c
 <a href="#">plugins</a>	Shorten a target name to


# “soft fork”





The screenshot shows a GitHub repository interface. At the top, there is a progress bar for 'CMake 99.6%'. Below it, there are two buttons: 'Branch: master' and 'New pull request'. The main content area shows a list of pull requests. The second pull request, titled 'osquery-src @ c55eb57', is highlighted with an orange rounded rectangle. To the left of the pull request list, there is a small red robot icon and the text 'Smjert Update Azure Pipelines to use osql-experimental Docker re'. The pull request list has the following items:



Folder Name	Description
<a href="#">cmake</a>	Do not require the source
<a href="#">osquery-src @ c55eb57</a>	Sync with experimental c
<a href="#">osquery</a>	Sync with experimental c
<a href="#">plugins</a>	Shorten a target name to

● CMake 99.6%

Branch: master ▾    New pull request

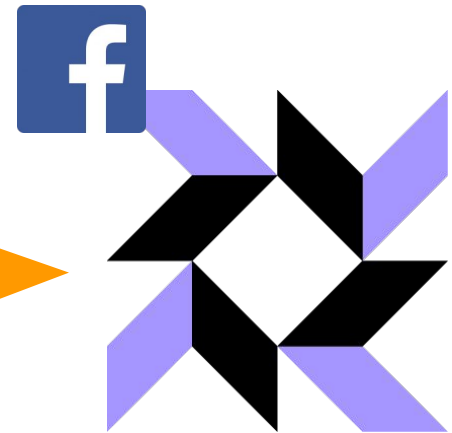
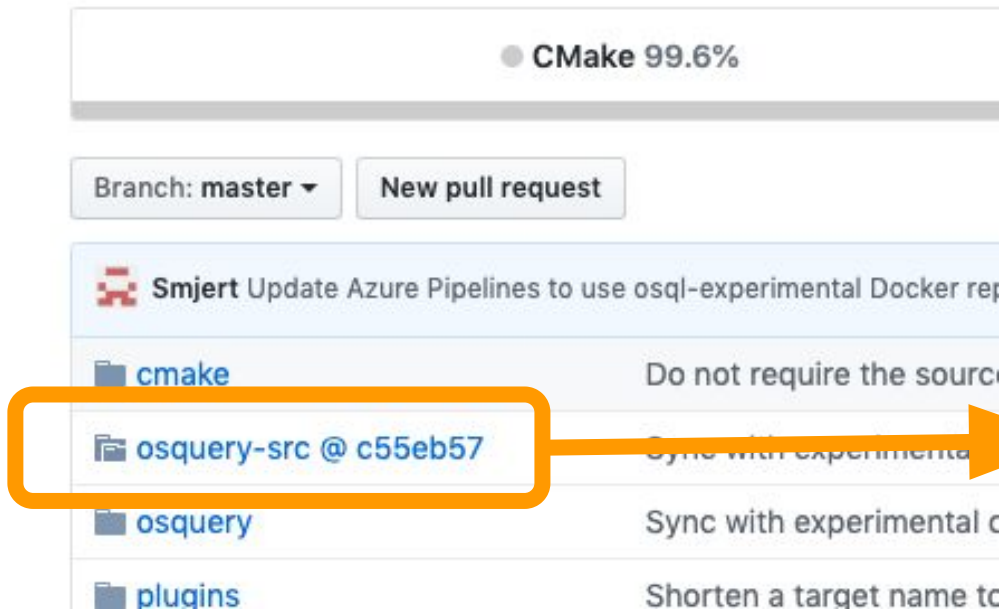
 Smjert Update Azure Pipelines to use osql-experimental Docker re

 <a href="#">cmake</a>	Do not require the source
 <a href="#">osquery-src @ c55eb57</a>	Sync with experimental
 <a href="#">osquery</a>	Sync with experimental c
 <a href="#">plugins</a>	Shorten a target name to

An orange box highlights the `osquery-src @ c55eb57` entry, with an orange arrow pointing from it to the Docker logo.





upstream/experimental

A community-oriented fork of osquery with support for CI

osquery

security

monitoring

intrusion-detection

sql

● CMake 99.6%

Branch: master ▾

New pull request



Smjert Update Azure Pipelines to use osql-experimental Docker rep

📁 [cmake](#)

Do not require the source

📁 [osquery-src @ c55eb57](#)

Sync with experimental c

📁 [osquery](#)

Sync with experimental c

📁 [plugins](#)

Shorten a target name to

upstream/experimental

Release plan

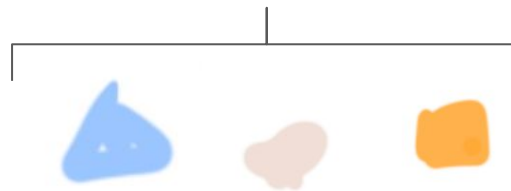


upstream/experimental

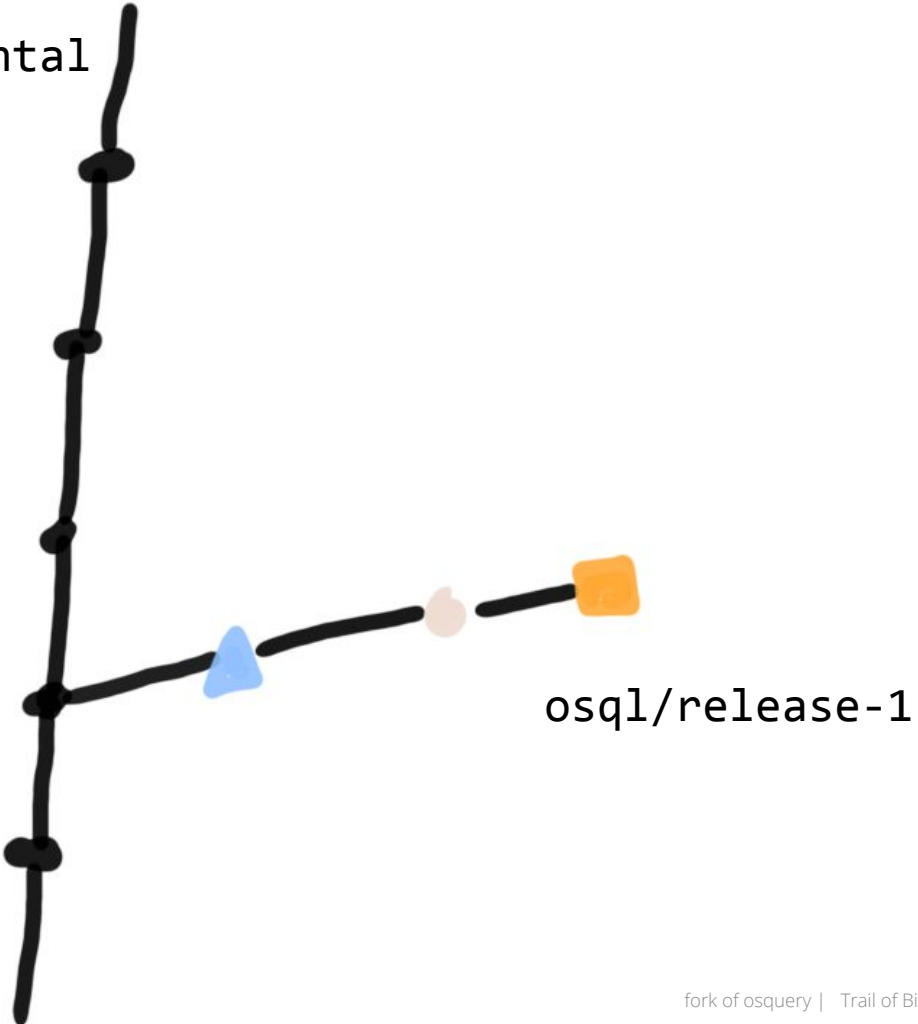


Release plan

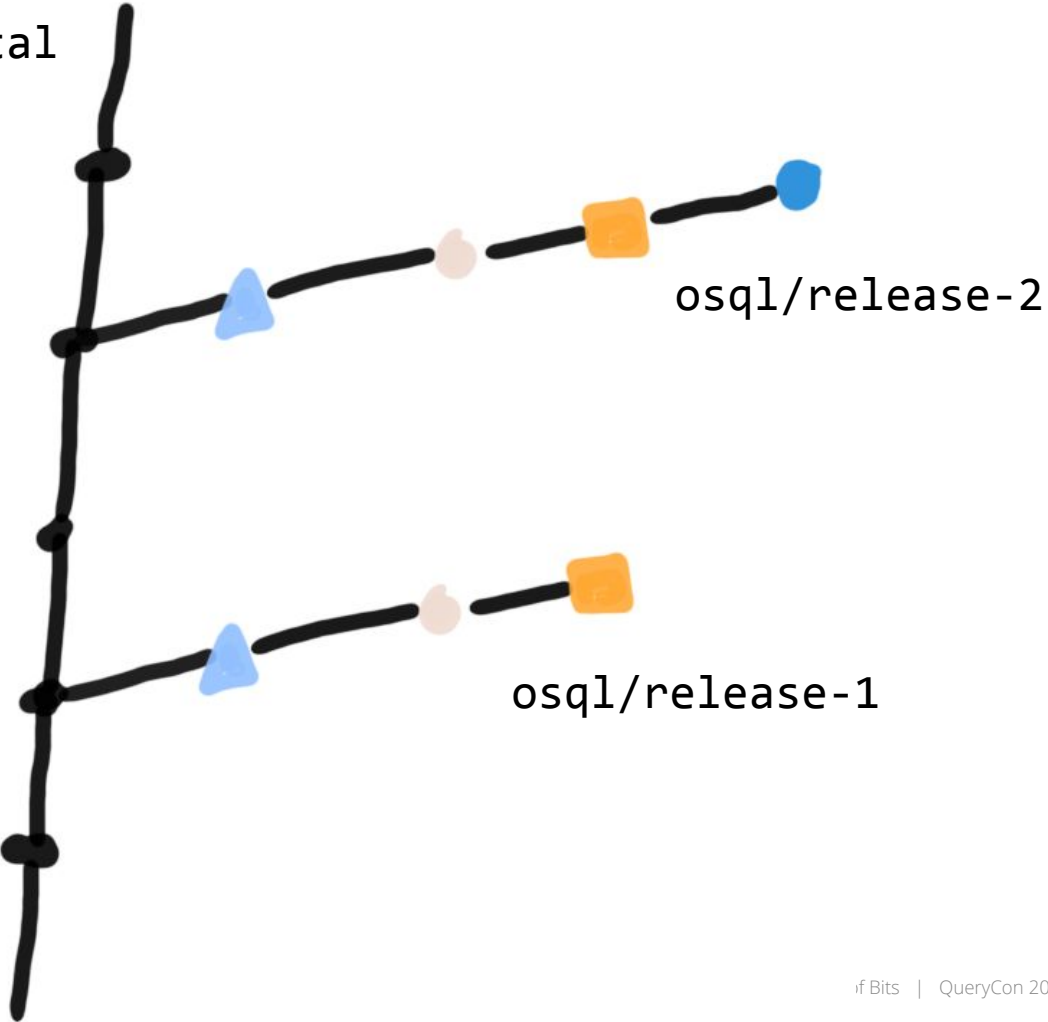
Community Pull Requests



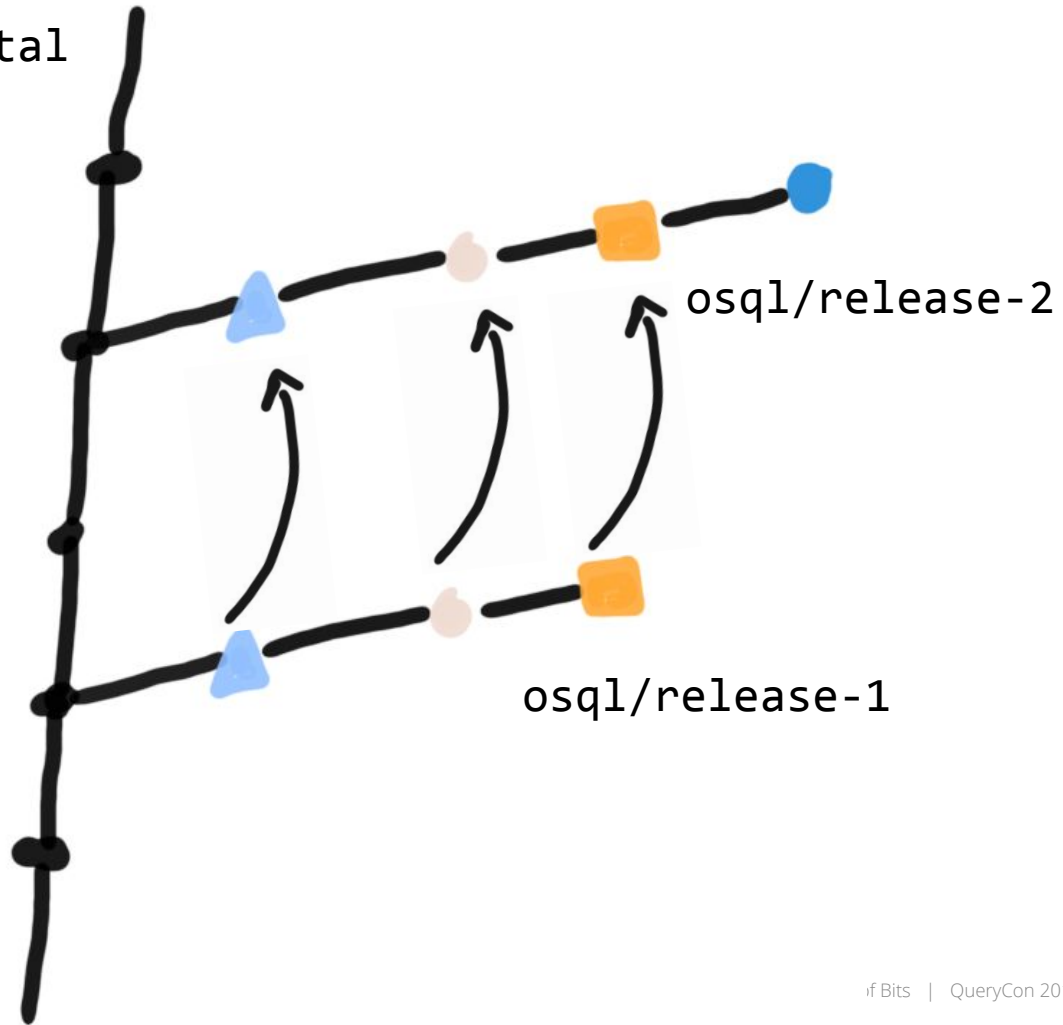
upstream/experimental



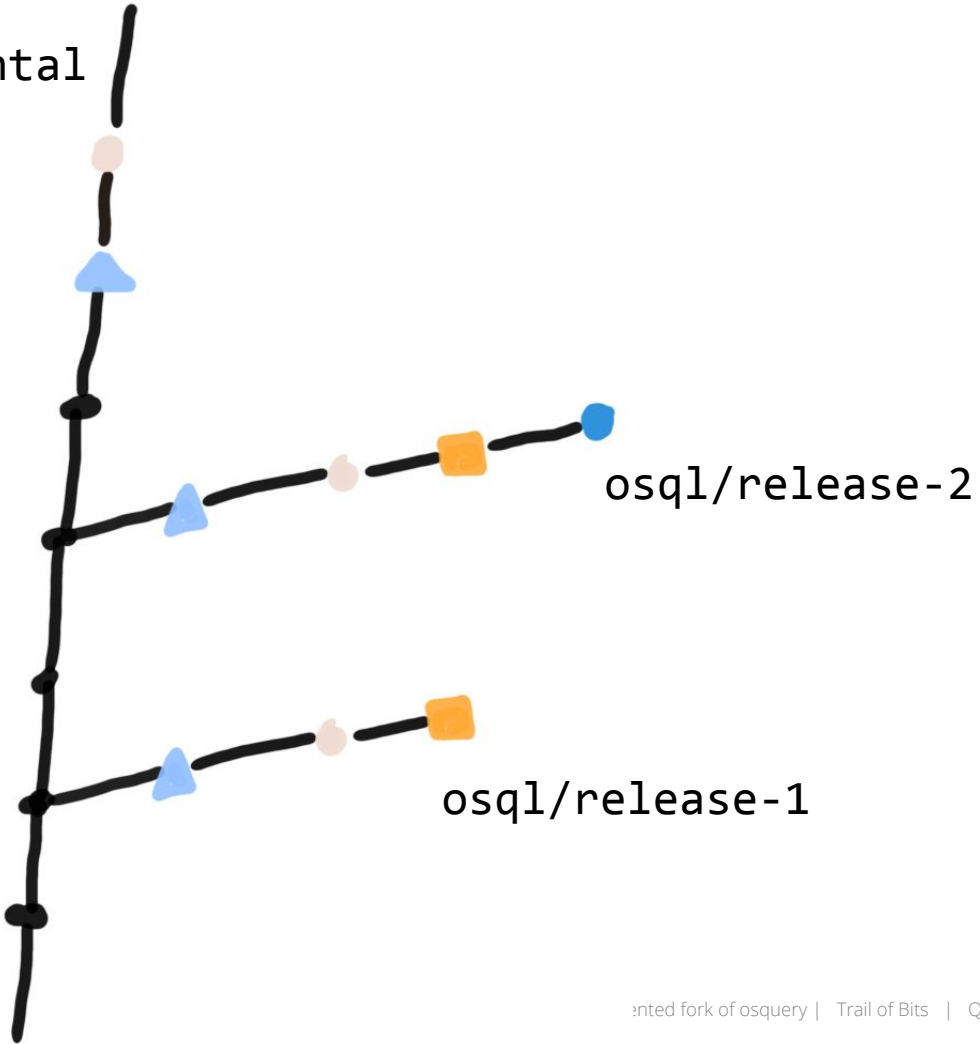
upstream/experimental



upstream/experimental

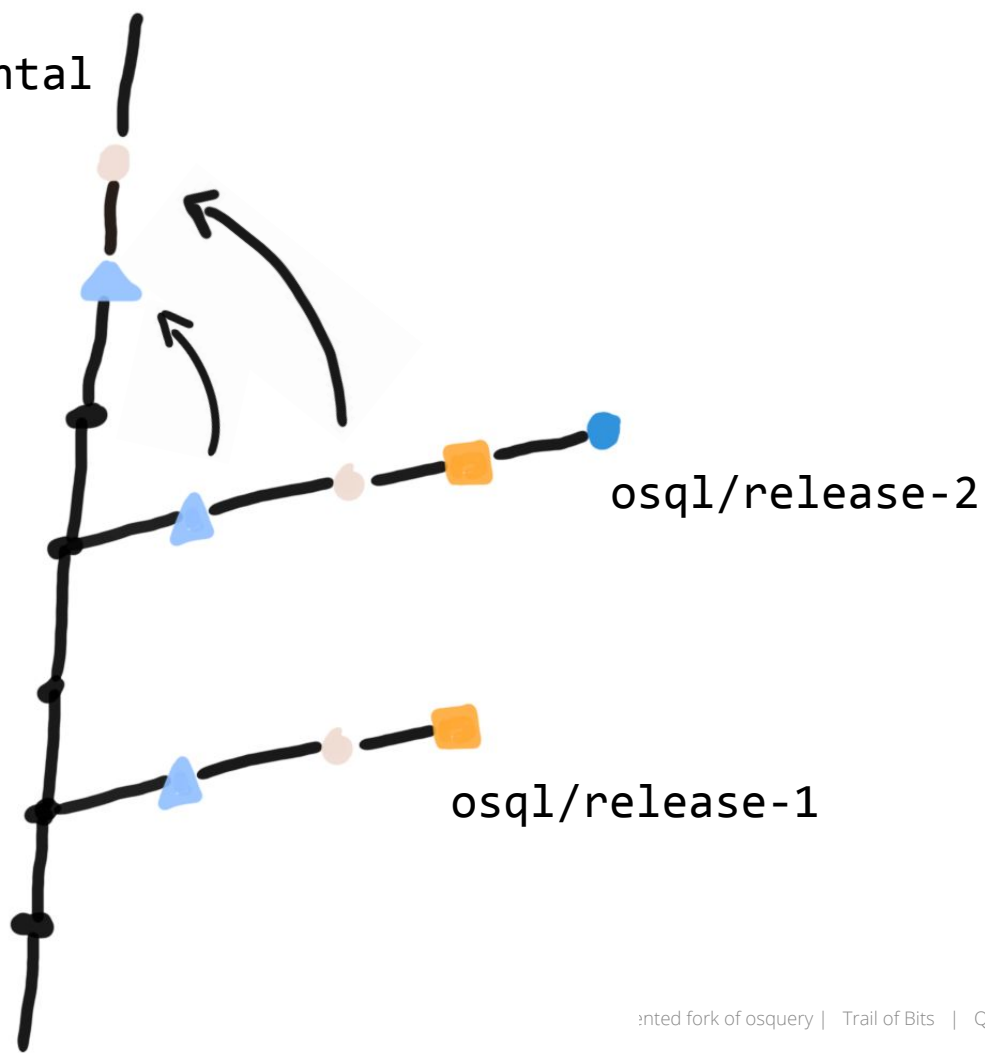


upstream/experimental

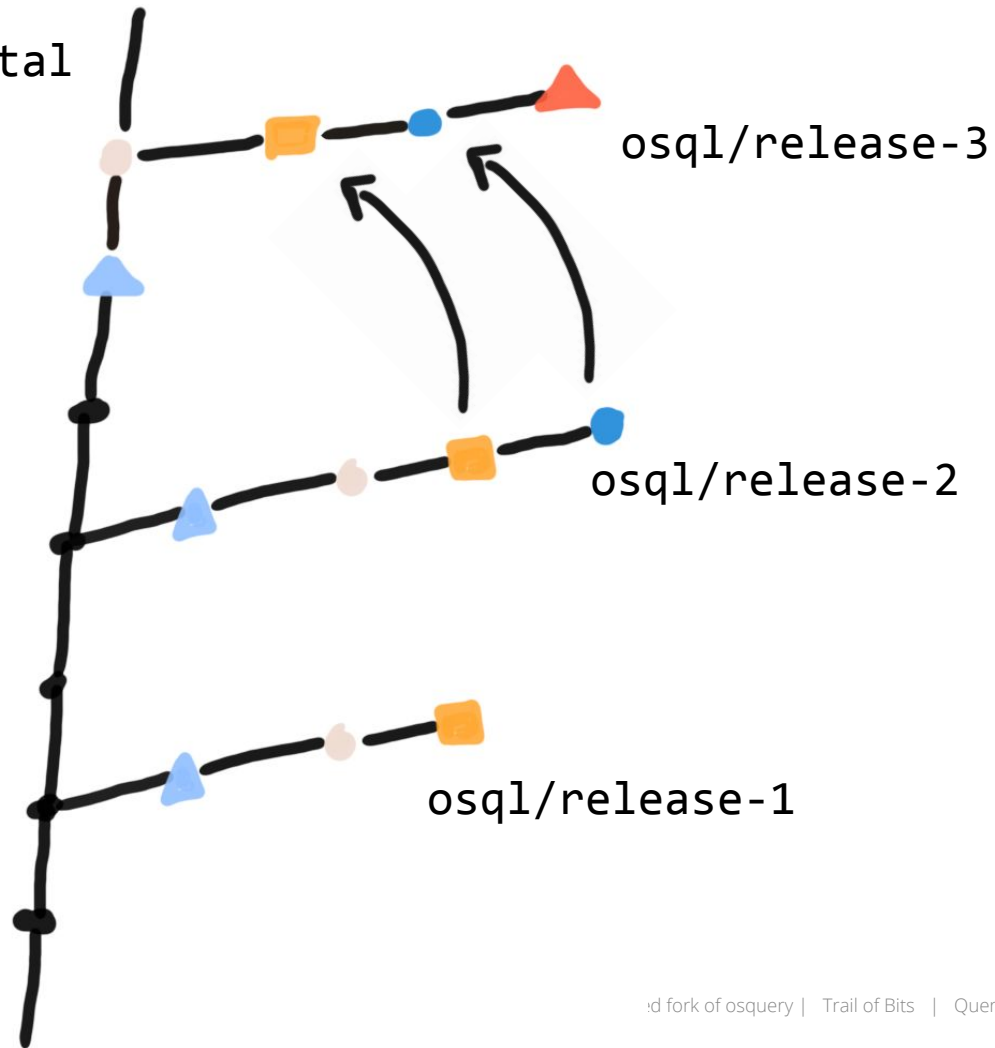




upstream/experimental



upstream/experimental



- 
- ✓ Stay in sync with upstream
  - ✓ Ship releases with community PRs

# upstream/experimental

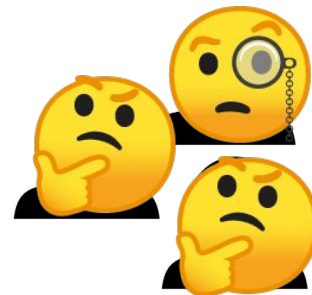


Uncertain future:

- Stability issues
- Unclear roadmap
- PRs merged rarely

## Uncertain future:

- Stability issues
- Unclear roadmap
- PRs merged rarely





# osql

 **Repositories** 8

 **People** 19

 **Teams** 2

 **Projects** 0

## Pinned repositories

 **osql**

SQL powered operating system instrumentation, monitoring, and analytics.

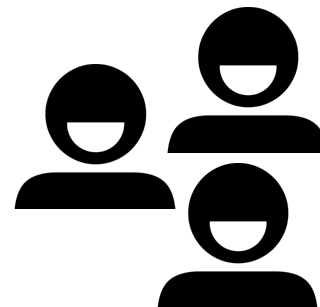
 C++  11  6

 **osql-experimental**







A community-oriented fork of osquery with support for cmake, public CI testing, and regular releases

 CMake  65  2

- “Hard fork” of upstream/master
- Fixes build & restores public CI
- Suitable place to continue osquery development
  - Stable branch
  - Clear roadmap
  - Community PR reviews



The tools make low-level operating system analytics and monitoring both performant and intuitive.

Platform	Build status		
MacOS 10.15		Homepage:	<a href="https://osquery.io">https://osquery.io</a>
CentOS 7		Downloads:	<a href="https://osquery.io/downloads">https://osquery.io/downloads</a>
CentOS 8		Schemas:	<a href="https://osquery.io/schema">https://osquery.io/schema</a>
Ubuntu 16.04		Packs:	<a href="https://osquery.io/packs">https://osquery.io/packs</a>
Windows 2016		Guide:	<a href="https://osquery.readthedocs.org">https://osquery.readthedocs.org</a>
Windows 10	N/A		<a href="https://osquery-slack.herokuapp.com">https://osquery-slack.herokuapp.com</a>
FreeBSD 11	N/A		



🔗 17 Open ✓ 4 Closed

Author ▾

Labels ▾

Projects ▾

Milestones ▾

🔗 **replacing sync calls by async ones and some cleanup** ✓

#69 opened yesterday by uptycs-nishant • Review required

🔗 **check\_output should have .decode(utf-8) in python3** ✓

#65 opened 7 days ago by packetzero • Review required

🔗 **Change windows deployment location to the Program Files directory** ✓

#64 opened 8 days ago by GarretReece • Review required

🐛 17 Open ▾ 🐛 replacing :  
#69 opened y 🐛 check\_out  
#65 opened 7

- 🐛 **53 spec missing index** ✓  
#54 opened 12 days ago by packetzero • Review required
- 🐛 **Fix and re-enable OsVersion.test\_sanity** ✓  
#52 opened 12 days ago by Smjert • Review required
- 🐛 **Various Boost fixes (1.66 to 1.69 upgrade)** ✗  
#44 opened 19 days ago by alessandrogario • Review required
- 🐛 **Fix for #5379, only use index if implemented** ✓  
#12 opened 23 days ago by packetzero • Review required
- 🐛 **Fix readthedocs docs generation** ✓  
#10 opened 29 days ago by Smjert • Review required
- 🐛 **windows/certificates: Fix enumeration bugs, add columns** ✗
- 🐛 **Change windows deployment location to the Program Files directory** ✓  
#64 opened 8 days ago by GarretReece • Review required

<> Code

! Issue

 **53 spec missing index** ✓

#54 opened 12 days ago by packetzero • Review required

 **windows/certificates: Fix enumeration bugs, add columns** ✗

#9 opened on May 20 by mossberg • Review required  osql first release

 **Implement process\_memory\_map.filetype column for windows, linux** ✓

#6 opened on May 17 by packetzero • Review required

 **port fix for #4810 - syslog pipe hang** ✓

#5 opened on May 17 by packetzero • Review required

 **Add cached\_logger with aws\_kinesis implementation.** ✓

#4 opened on May 17 by packetzero • Review required

 **port processes table without wmi, filter by pid** ✓

#3 opened on May 17 by packetzero • Review required

1s ✗

 **Fix #4280: windows named pipes issues** ✓

#2 opened on May 17 by packetzero • Review required

**The future of osquery = community**

**TRAIL  
OF  
BITS**

# The Linux Foundation Announces Intent to Form New Foundation to Support osquery Community

By The Linux Foundation | June 18, 2019

---

*Engineers and developers from Facebook, Google, Trail of Bits and more to help*

**Let's use osql as a starting point!**

**TRAIL  
OF  
BITS**

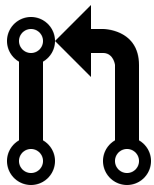


Governance





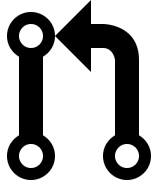
Governance



Development  
Process



Governance

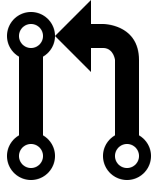


Development  
Process

Funding & Support

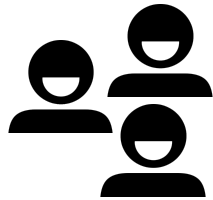


Governance



Development  
Process

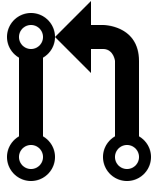
Funding & Support



Community  
Management

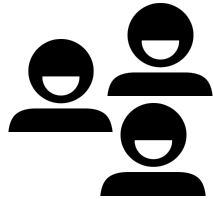


Governance

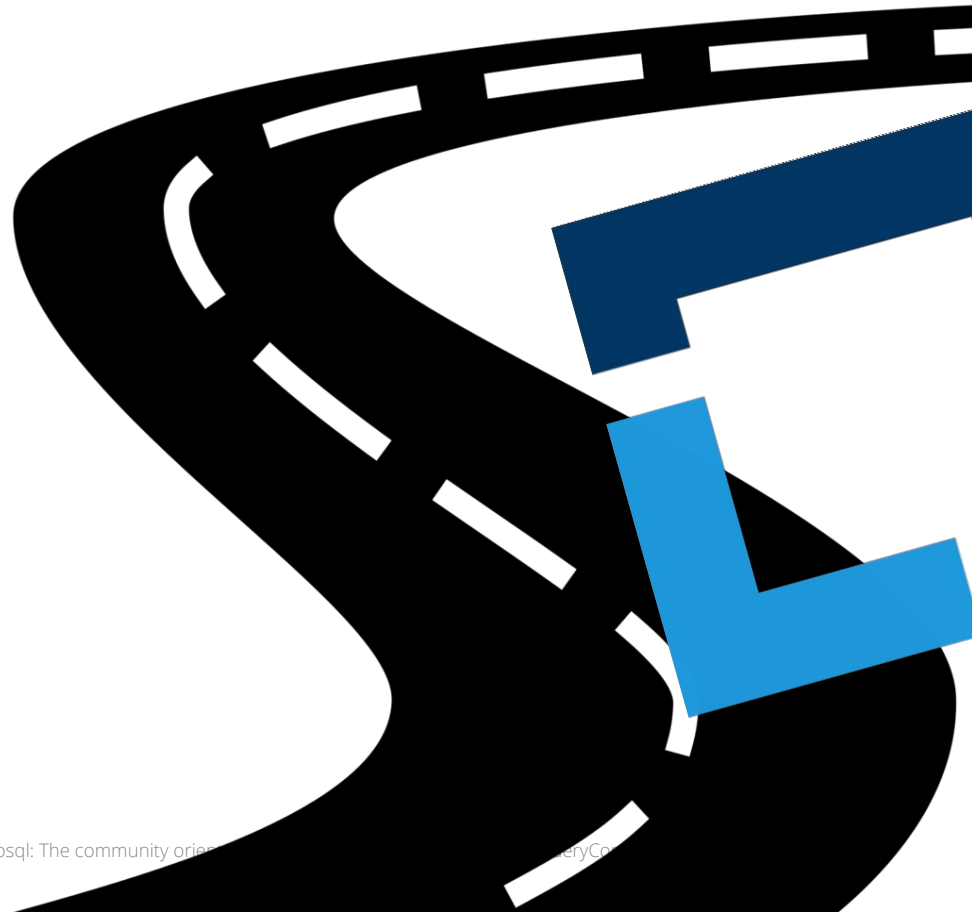


Development  
Process

Funding & Support



Community  
Management





osql

Repositories

Pinned repositories

osql

SQL powered operating system instrumentation, monitoring, and analytics.

C++ ★ 11 🍴 6

osql-experimental

A community-oriented fork of osquery with support for cmake, public CI testing, and regular releases

CMake ★ 65 🍴 2

## Get involved with osql!

<http://github.com/osql>  
#osql @ osquery Slack