

Solving the Deployment Crisis with GNU Guix

Christopher Allan Webber & David Thompson

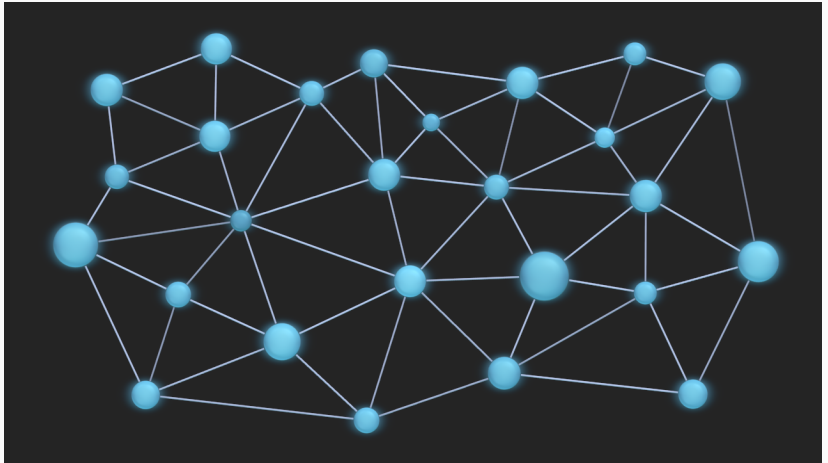
Saturday, March 19th, 2016

Setting the stage

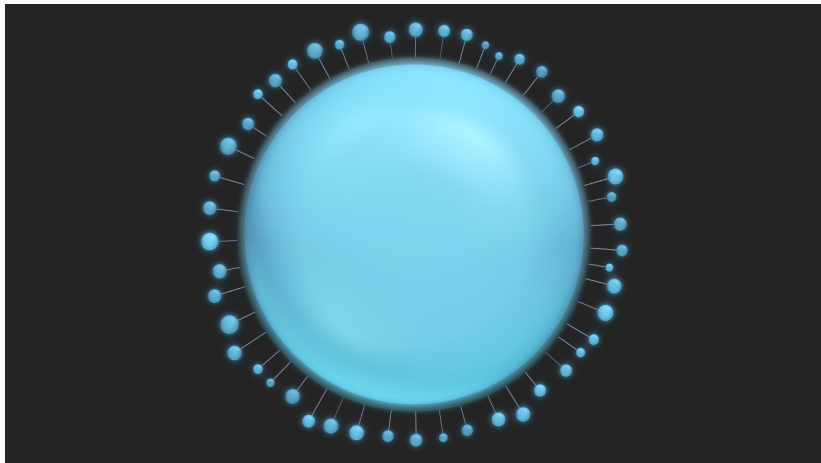
Who are we?

- Who is David Thompson?
- Who is Christopher Webber?

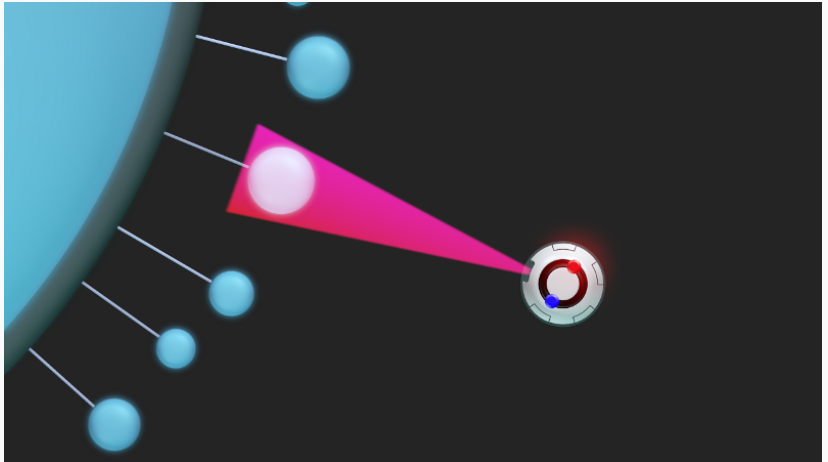
The web we want



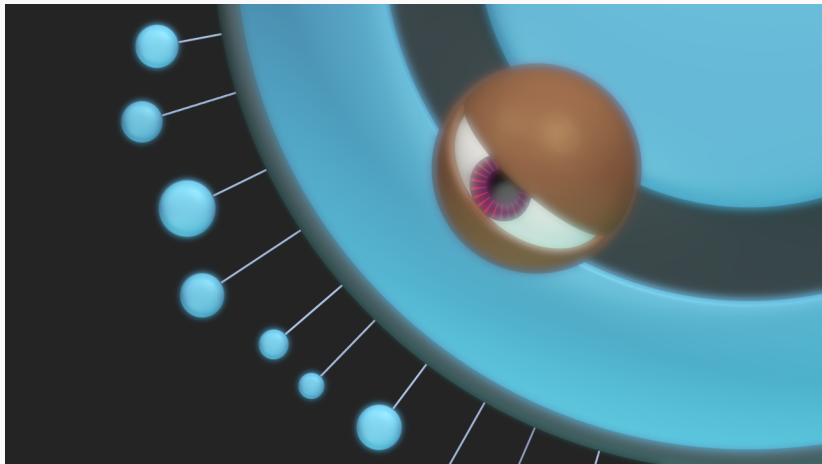
The sad reality (centralization)



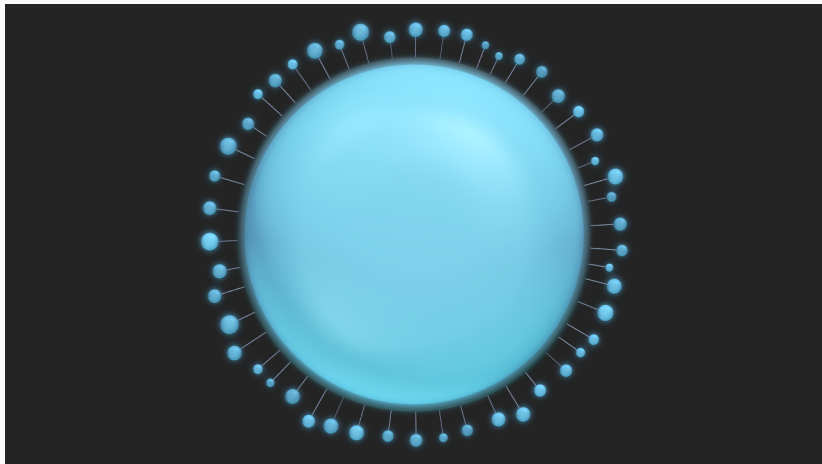
The sad reality (censorship)



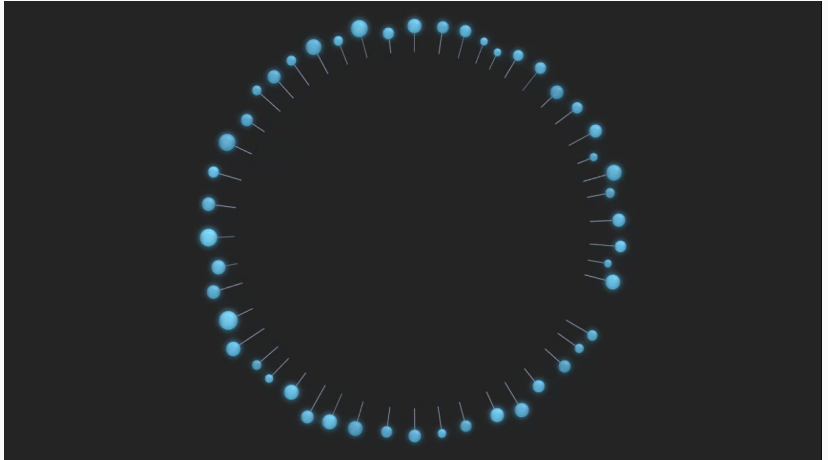
The sad reality (surveillance)



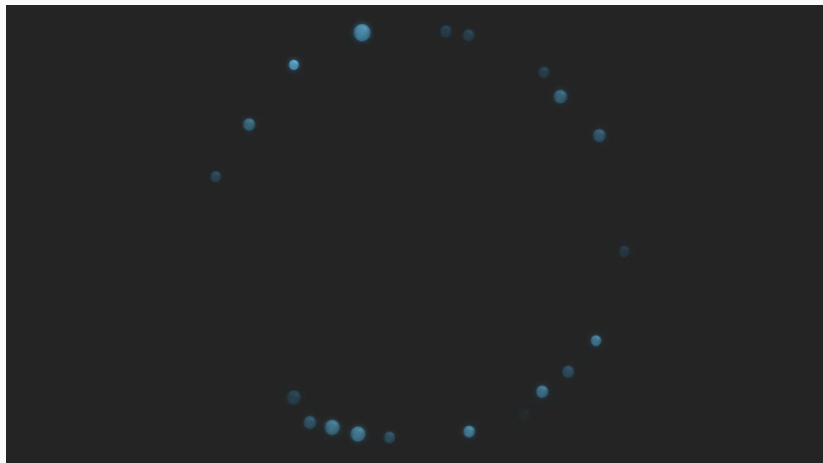
The sad reality (fragility)



The sad reality (fragility)



The sad reality (fragility)



The sad reality (fragility)



4) Bring MediaGoblin to the people!



Dependent on phase of the moon



One Language Package Manager Per Child

```
INSTALL.SH  
#!/bin/bash  
  
pip install "$1" &  
easy_install "$1" &  
brew install "$1" &  
npm install "$1" &  
yum install "$1" & dnf install "$1" &  
docker run "$1" &  
pkg install "$1" &  
apt-get install "$1" &  
sudo apt-get install "$1" &  
steamcmd +app_update "$1" validate &  
git clone https://github.com/"$1"/"$1" &  
cd "$1";./configure;make;make install &  
curl "$1" | bash &
```

Have fun managing configuration



So... docker??? (Or something like it?)

```

--
  __|II|
    __|II|II|__  ,.
--|II|II|II|II|___/  __/  -'-.-'-.-'-
----- |      [Docker]      / -----
----- :                      / -----
----- \____, o                ,' -----
----- '---,-----, ' -----
```

Easy for users! “I already built this for you, just pull it down and use it!”

Maybe not :(



Distro-sized static compiling considered hazardous

- Extremely heavy: throws away dynamic linking
- Hard to introspect, rebuild
- Analysis of Docker Hub: over 70% have medium vulnerabilities, 30-40% high (shellshock, heartbleed) vulnerabilities ¹
- Reproducible? Not in the sense of <https://reproducible-builds.org/>
- Docker's DSL is not expressive
- Still dependent on “phase of the moon” of distributions!

¹<http://www.banyanops.com/blog/analyzing-docker-hub/>

Unfortunately, it's not just Docker

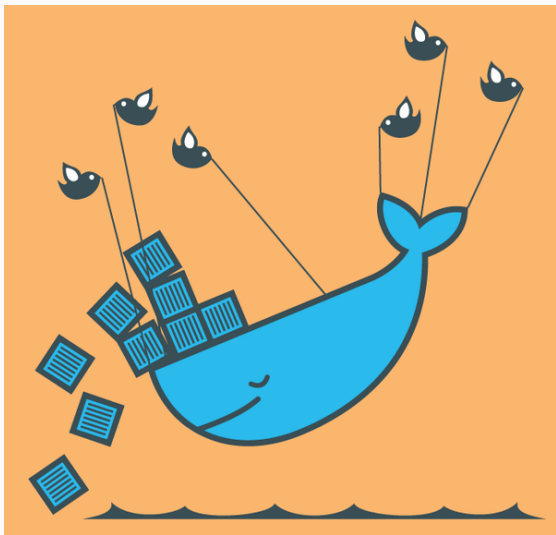
- CoreOS
- xdg-app
- Qubes
- Snappy
- egads!

We are losing the ability to reason about free software!

A policy issue disguised as a technical issue?

If it's too hard to build, run and modify software, what does this mean for user freedom?

And so here we are

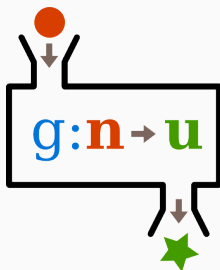


Enter Guix & GuixSD!



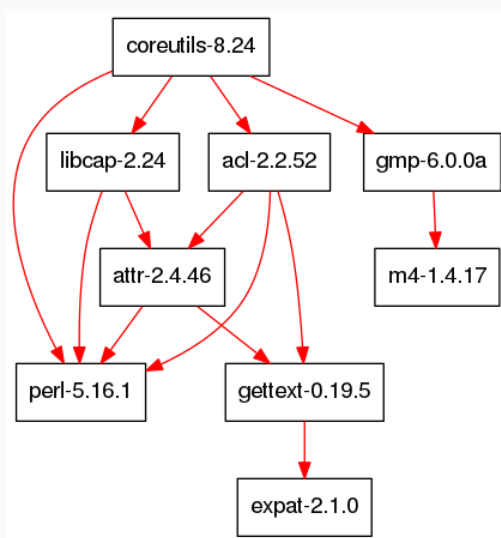
GuixSD

Functional package management



- Precisely specified dependencies
- Reproducible builds (same input, same output)
- Built packages are immutable
- Unprivileged package management
- Atomic upgrades and roll backs

Packages capture the **full** dependency graph



Your profile, my profile

- Unprivileged package management (no root privileges needed!)
- Each user may install software **without conflicting** with other users or the system
- Each user may have **many** profiles

Guix gives users **practical freedom** to use different sets of packages for different tasks.

Transactional upgrades and rollbacks

Bad upgrade? No problem!

```
guix package --roll-back
```

Congratulations, you are now a time wizard!



Like Git, for your operating system!

```
cwebber@oolong:~$ ls -l ~/.guix-profile/bin
total 1612
lrwxrwxrwx 3 root guixbuild 65 Dec 31 1969 2to3 -> /gnu/store/xw8ikmsj7b62aimwyd9kxwvygxm78h1-python-3.4.3/bin/2to3
lrwxrwxrwx 3 root guixbuild 69 Dec 31 1969 2to3-3.4 -> /gnu/store/xw8ikmsj7b62aimwyd9kxwvygxm78h1-python-3.4.3/bin/2to3-3.4
lrwxrwxrwx 16 root guixbuild 66 Dec 31 1969 abbaye -> /gnu/store/9qr1p42rsjz0cpk7q7qza4g15g5pibi-abbaye-1.13/bin/abbaye
lrwxrwxrwx 3 root guixbuild 69 Dec 31 1969 aclocal -> /gnu/store/rr3wsxa5q53hkvw9q8kmm114clrv7rdk-automake-1.15/bin/aclocal
lrwxrwxrwx 3 root guixbuild 74 Dec 31 1969 aclocal-1.15 -> /gnu/store/rr3wsxa5q53hkvw9q8kmm114clrv7rdk-automake-1.15/bin/aclocal-1.15
lrwxrwxrwx 22 root 1001 73 Dec 31 1969 aconnect -> /gnu/store/1jqsldmm16j0hbw12mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/aconnect
lrwxrwxrwx 3 root guixbuild 71 Dec 31 1969 acyclic -> /gnu/store/4g4gq0dny1capi0fa0idf248ys7cx2mv-graphviz-2.38.0/bin/acyclic
lrwxrwxrwx 22 root 1001 77 Dec 31 1969 addr2line -> /gnu/store/7m8s5qm2xyz30lwzxhaccqh7i4kpkyl8i-gcc-toolchain-5.3.0/bin/addr2line
lrwxrwxrwx 22 root 1001 73 Dec 31 1969 alsaloop -> /gnu/store/1jqsldmm16j0hbw12mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/alsaloop
lrwxrwxrwx 22 root 1001 74 Dec 31 1969 alsamixer -> /gnu/store/1jqsldmm16j0hbw12mjhkylz7zb0ip75-alsa-utils-1.1.0/bin/als

cwebber@oolong:~$ ls /gnu/store | head
0001mfr72xdjw284dm1dw067zzy1f2p0-grep-2.21.drv
0004fhpfzncal119v7zaa4p7rj31bz7f-redland-1.0.17-guile-builder
00267biy0d5f8gh66scnj8bjz44n567d-other.drv
002111ka4a8v87d0ikrn543b10wd6a7z-guile-static-stripped-2.0.11.drv
0030hbba317r4kqsq1b459h3jsl57fki-libspectre-0.2.7.drv
004ib0h788s3bcjm26q7szvk1k8qsqzd-git-manpages-2.6.3.tar.xz.drv
004pk19mwih54mvfrid8363pmh2glvbz-unzip-6.0.drv
005z52jrc8yrr8z205gpc5ml33i3qpqf-python-2.7.10.drv
009903g12bx1pny50a8cqc9yiw9bbniz-libxshmfence-1.1.tar.bz2.drv
00c6nc4n4a66ji9k04ngvf9xyw6vmmn-shared-mime-info-1.2.tar.xz.drv
cwebber@oolong:~$
```

Keep the history until you don't need it

```
"Guix Generation List: guix-profile"
-----
N.  Current  Time          File name
*  212 (current) 2016-03-03 17:12:31 /var/guix/profiles/per-user/cwebber/guix-profile-212-link
  211          2016-03-03 13:49:49 /var/guix/profiles/per-user/cwebber/guix-profile-211-link
*  210          2016-03-03 10:16:30 /var/guix/profiles/per-user/cwebber/guix-profile-210-link
  209          2016-03-02 08:23:37 /var/guix/profiles/per-user/cwebber/guix-profile-209-link
  208          2016-03-02 07:40:41 /var/guix/profiles/per-user/cwebber/guix-profile-208-link
  207          2016-03-02 07:35:21 /var/guix/profiles/per-user/cwebber/guix-profile-207-link
  206          2016-03-02 07:35:02 /var/guix/profiles/per-user/cwebber/guix-profile-206-link
  205          2016-03-02 07:34:24 /var/guix/profiles/per-user/cwebber/guix-profile-205-link
  204          2016-03-02 07:33:51 /var/guix/profiles/per-user/cwebber/guix-profile-204-link
  203          2016-03-01 19:18:01 /var/guix/profiles/per-user/cwebber/guix-profile-203-link
  202          2016-03-01 15:03:39 /var/guix/profiles/per-user/cwebber/guix-profile-202-link
  201          2016-03-01 14:27:47 /var/guix/profiles/per-user/cwebber/guix-profile-201-link
  200          2016-03-01 12:25:25 /var/guix/profiles/per-user/cwebber/guix-profile-200-link
  199          2016-03-01 12:23:29 /var/guix/profiles/per-user/cwebber/guix-profile-199-link
  198          2016-03-01 12:03:22 /var/guix/profiles/per-user/cwebber/guix-profile-198-link
[Ins,Mod,RO] *Guix Generation List: guix-profile* ( 3, 0) [Guix-Generation-List] -----
diff -u --label '\<buffer\ \*Guix\ guix-profile:\ generation\ 210\>' --label '\<buffer\ \*Guix\ guix-profile\
s:\ generation\ 212\>' /tmp/buffer-content-664-e1 /tmp/buffer-content-664woE
--- #<buffer *Guix guix-profile: generation 210*>
+++ #<buffer *Guix guix-profile: generation 212*>
@@ -1,40 +1,40 @@
  abbaye-1.13.out /gnu/store/9qr1p42rsjzp0cpk7q7qza4g15g5pibi-abbaye-1.13
  alsa-utils-1.1.0.out /gnu/store/1jqslldmml6j0hbw12mjhkylz7zb0ip75-alsa-utils-1.1.0
  -aspell-0.60.6.1.out /gnu/store/d6y35430s9sagx0csc1yfbz5j92w91x0a-aspell-0.60.6.1
  +aspell-0.60.6.1.out /gnu/store/dhj0k9sk83479x1259nql8p5ikk48cg6-aspell-0.60.6.1
  aspell-dict-en-2016.01.19-0.out /gnu/store/ci352syqq8w1qlpvw16iqzc83jhazsm-aspell-dict-en-2016.01.19-0
  -assword-0.8.out /gnu/store/4h145h9myqwgqd2kvs1jghx4pz1wb6s-assword-0.8
  +autoconf-2.69.out /gnu/store/bj59z4kp62ksmmwvns53d2pi9dsw7kp-autoconf-2.69
  -automake-1.15.out /gnu/store/3cq8rzbypnfbcvrpx8xpw98vmd7yyhcf-automake-1.15
  +assword-0.8.out /gnu/store/qkvv8zd03zd24vzs4g8d0rlayvrgpzd-assword-0.8
  +autoconf-2.69.out /gnu/store/mbr57wg24dlrqqkzsa5szyhss2a47b5q4-autoconf-2.69
  +automake-1.15.out /gnu/store/rr3wsxa5q53hkvw9q8kmm114clrv7rdk-automake-1.15
[Ins,Mod,RO] *Diff* ( 2, 0) [Diff]
```

The `guix environment` tool can be used to quickly create development environments.

Like Python's `virtualenv`, but for **anything**.

Development environments

```
$ which irb
which: no irb in (/run/current-system/profile/bin)
$ guix environment --ad-hoc ruby ruby-nokogiri
$ which irb
/gnu/store/q2ldaivsnfdmvlxnc7hlw5skc9f9xw5g-profile/bin/irb
$ irb
irb(main):001:0> require 'nokogiri'
=> true
irb(main):002:0> Nokogiri
=> Nokogiri
```

Guix is written in Scheme

```
grep.scm
(define-public grep
  (package
    (name "grep")
    (version "2.21")
    (source
      (origin
        (method url-fetch)
        (uri (string-append "mirror://gnu/grep/grep-"
                             version ".tar.xz"))
        (sha256
          (base32
            "1pp5n15qwxrw1pibwjhhgsiby5cafhamf8lwzjygs6y00fa2i2j")))
        (patches (list (search-patch "grep-CVE-2015-1345.patch")))))
    (build-system gnu-build-system)
    (synopsis "Print lines matching a pattern")
    (description
      "grep is a tool for finding text inside files. Text is found by
      matcing a pattern provided by the user in one or many files. The pattern
      may e provided as a basic or extended regular expression, or as fixed
      strigs. By default, the matching text is simply printed to the screen,
      however the output can be greatly customized to include, for example, line
      numbrs. GNU grep offers many extensions over the standard utility,
      inclding, for example, recursive directory searching.")
    (license gpl3+)
    (home-page "http://www.gnu.org/software/grep/")))

[Ins] grep.scm (26, 0) [Scheme] Git-master
```


Guix is a library

All data structures, procedures, etc. are exposed as Guile APIs.

Using these APIs, we've implemented:

- Declarative config management (Puppet, Chef, Salt, Ansible, etc.)
- Universal language packaging (PyPI, RubyGems, ELPA, CRAN, etc.)
- Local dev environments (virtualenv, rvm, rbenv, nvm, etc.)
- Local VM creation (Vagrant)
- Linux containers (Docker, rkt, lxc, etc.)

The world is yours to hack!

Full system configuration management

```
(operating-system
  (host-name "izanagi")
  (timezone "America/New_York")
  (locale "en_US.UTF-8")
  (bootloader (grub-configuration (device "/dev/sda")))
  (file-systems (cons (file-system
    (device "root")
    (title 'label)
    (mount-point "/")
    (type "ext4"))
    %base-file-systems))
  (users (list (user-account
    (name "dave")
    (comment "David Thompson")
    (group "users")
    (supplementary-groups '("wheel" "netdev" "audio"
      "video" "cdrom"))
    (home-directory "/home/dave"))))
  (packages (cons* adwaita-icon-theme avahi gnome-terminal
    htop less man-db ncurses nss-certs
    openssh wicd unzip rsync xfce
    %base-packages))
  (services %desktop-services)
  (name-service-switch %mdns-host-lookup-nss))
```

```
U:@--- izanagi.scm Bot (52,0) Git:master (Scheme Guix Guile/A Paredit Proj
```

Package importers

```
$ guix import pypi pyglet
(package
  (name "python-pyglet")
  (version "1.2.4")
  (source
    (origin
      (method url-fetch)
      (uri (pypi-uri "pyglet" version))
      (sha256
        (base32
          "0i9la03pm51swv2z8f17bx7qz2yjfxfg6hn7i9c42s81bryxzyqlz"))))
  (build-system python-build-system)
  (inputs
    `(("python-setuptools" ,python-setuptools)))
  (home-page
    "http://pyglet.readthedocs.org/en/pyglet-1.2-maintenance/")
  (synopsis
    "Cross-platform windowing and multimedia library")
  (description
    "Cross-platform windowing and multimedia library")
  (license bsd-3))
```

What's in (/gnu/)store?

- Remote cluster management tool
- Provision bare metal, VMs, containers
- Complete replacement for Chef, Puppet, Ansible, Salt, etc.

Recipe based deployments? With a GUI?

- Select pre-built recipes for MediaGoblin, Wordpress, etc.
- “Don’t repeat yourself“ configuration
- Could we make a simple web interface for this?

- Why should Solitaire have access to your GPG/SSH keys?
- Limit web browser's access to your home directory

- Graphical distro installer
- Graphical interface for:
 - system configuration
 - user-specific packaging
 - easy roll-backs

Support for difficult languages that web developers use

NodeJS, we're looking at you! ²

Also, Java. ³

Send help.

²<http://dustycloud.org/blog/javascript-packaging-dystopia/>

³<http://lists.gnu.org/archive/html/guix-devel/2016-02/msg01396.html>

Wrapping up

- “It’s still beta!”
- But probably more stable than most devops stuff
- A delight to run (we use it!)
- Easy to develop and get involved in
- ≈ 3350 packages
- $\approx 20-30$ contributors per month and increasing

There's more to do (and you can help!)

- Test drive Guix or GuixSD and send feedback
- Write GuixSD system services
- Improve documentation
- Improve containers, add packages, add importers, ...

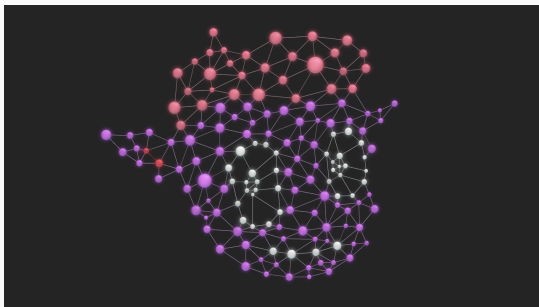
Talk with the developers via IRC at #guix on Freenode or via email at guix-devel@gnu.org or help-guix@gnu.org

A short story



- Moon image from *Le Voyage dans la lune* (A Trip to the Moon), public domain. Retrieved from:
https://en.wikipedia.org/wiki/A_Trip_to_the_Moon#/media/File:Le_Voyage_dans_la_lune.jpg
- Tar pit image by Ray Bouknight, CC BY 2.0:
<https://www.flickr.com/photos/raybouk/8341369957>
- Rena runs aground (container fail image), CC BY 2.0 <https://www.flickr.com/photos/nzdefenceforce/6386334175/>

- Caminandes video screenshot by Blender Institute, CC BY 4.0
<http://www.caminandes.com/>
- Chemical warehouse image from Pixabay, CC0 <https://pixabay.com/en/warehouse-chemistry-industry-629641/>
- GuixSD logos by Luis Felipe López Acevedo, CC BY-SA 4.0
<http://www.gnu.org/software/guix/graphics/>
- Docker + Twitter image by Karen Rustad
- Slight snippet from Guix (grep package), GPLv3 or later



© 2016 Christopher Allan Webber <cwebber@dustycloud.org>

© 2016 David Thompson <davet@gnu.org>

This presentation is licensed under the Creative Commons Attribution Share-Alike 4.0 International license.

More on Guix: <https://gnu.org/software/guix>