

The **economics** of package management

CJ Silverio

@ceejibot

you are in this story

a story about

money

a story about

power

remember **Yahoo?**
ypm was its package manager

JSConfEU 2009

node.js announced

**early node had
package managers plural**

one got official status

Joyent **bought** node

Joyent did **not** buy
node's package manager

open-source doesn't mean
open ownership or **control**

node grows through 2013

success is a catastrophe
you need to survive

the package registry
is centralized

centralization has advantages

centralization has been the trend

centralization of costs

servers cost money
who pays for them?

donations work when you're small

success is expensive
(for centralized services)

npm needed money

this is not a novel **problem**

founding a company
was a novel choice

the node project decided this was fine

you decided this was fine

not everybody thought it was fine

money changes everything

I decided this was fine

I was employee number two

**those large numbers
sure are large**

let's talk about money

**open source generates
a lot of value**

capitalism does not reward
open source authors

most of us give away source code
not expecting money

open source vs free software

capitalism loves open source

**one person in this story
didn't give his stuff away**

javascript's commons

**commons: the resources
available to everybody**

the language spec

all our shared code

**our common registry of shared code
is owned by a private company**

Ryan Dahl was here again last year

It's unfortunate that there is a centralized (privately controlled even) repository for modules. --Ryan Dahl

**what are the consequences
of private control?**

no input into registry policies

no input into registry features

the **registry** is what matters
not the clients

**the management of our commons
is opaque to us**

**there is no trust
without accountability**

**you had no way to
hold **me** accountable**

so is npm evil?

mu. ask a different question.

npm is a financial instrument

financial instruments

are monetary contracts

**npm Inc is a means for turning
some money into more money**

companies don't love you
not even ones that make things you like

npm does not love you

nobody believes it anymore

how did the fall happen?

**It's 2018. Packages
flow like water.**

**packages cost money even if
you're not paying for them**

VCs want to go big or go home

**npm is obligated to
its **owners** not us**

make money or raise money

by telling a story about spending money to make money

in some kind of money-ception. you can't fool me; it's money all the way down

**they hired a CEO who made
some, um, interesting moves**

the centralized registry is expensive

**the situation today is uneasy
& probably short-lived**

this was not the only option

what are we going to do about it?

do nothing?

**imagine npm run by a
non-benevolent entity**

**maybe we'll be saved by
some large company**

I agree with **Ryan Dahl**

do you think that's impossible?

I believe in giving source code away

**Chris Dickinson @isntitvacant
& I have an announcement**

entropic: a federated package manager

<https://www.entropic.dev>

Apache 2.0 licensed
entirely open source (sorry RMS)

new cli & new api
decentralized: many registries

no, don't use entropic yet



but we do want **your help**
github/entropic-dev

entropic's goals

first, prove we have power

second, share our expertise

third, promote federation

take back the commons

go do something amazing



from ceej & chris