Zcash Governance

The Road Toward 2-of-2 Multisig

Josh Cincinnati @acityinohio
Executive Director, Zcash Foundation

Zcash Foundation

The Zcash Foundation's mission

A public charity dedicated to **building internet payment and privacy infrastructure for the public good**, primarily serving the users of the Zcash protocol and blockchain.

Zcash Foundation

...and that means being a check and balance on the Electric Coin Company's power

Zcash Foundation

A (very) brief history of Zcash

Zerocoin / Zerocash Papers

2013-2014

Zcash Co and Zcash 1.0.0

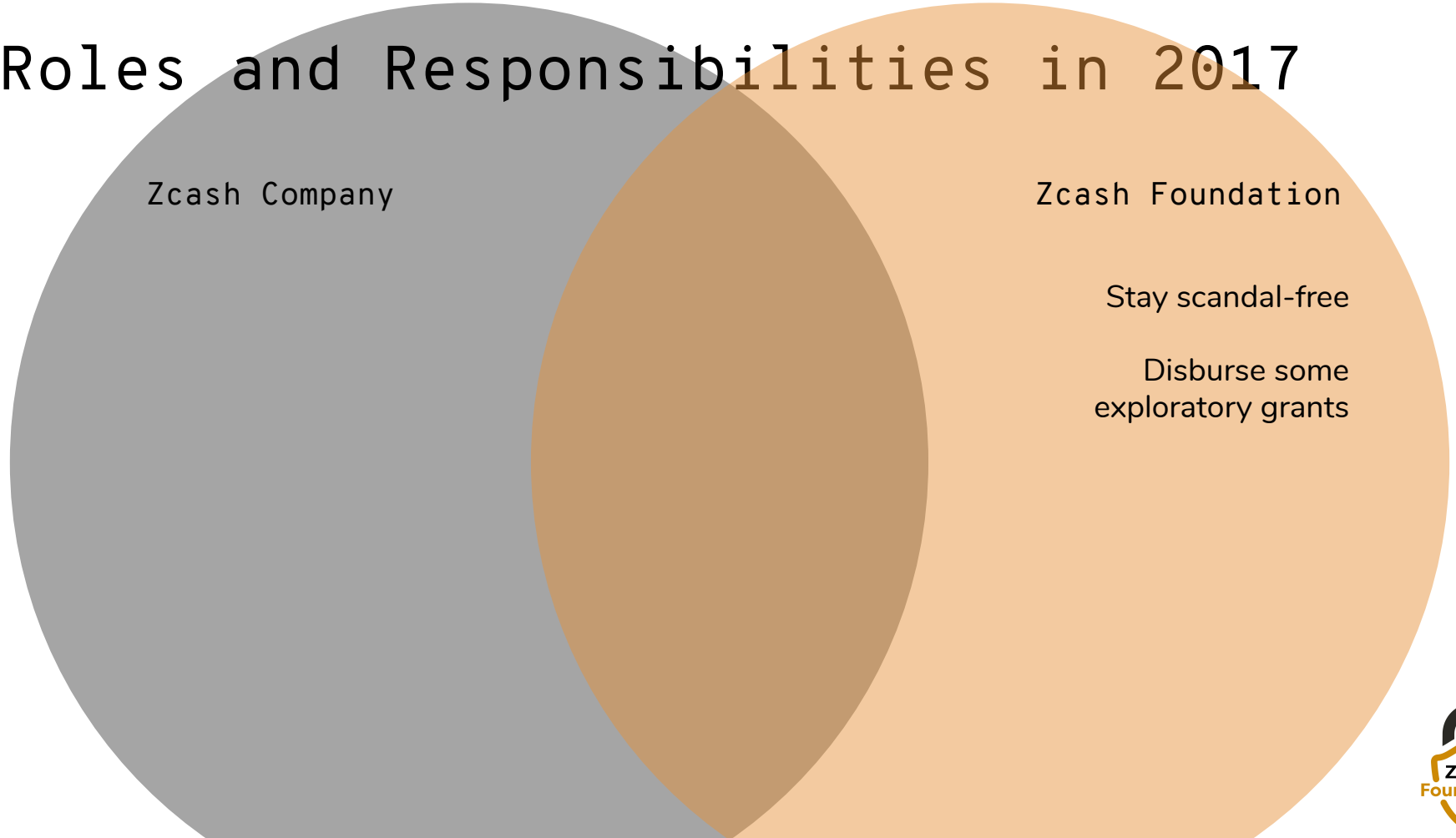
2015-2016

~~Zcash Co~~ Electric Coin Company & Zcash Foundation

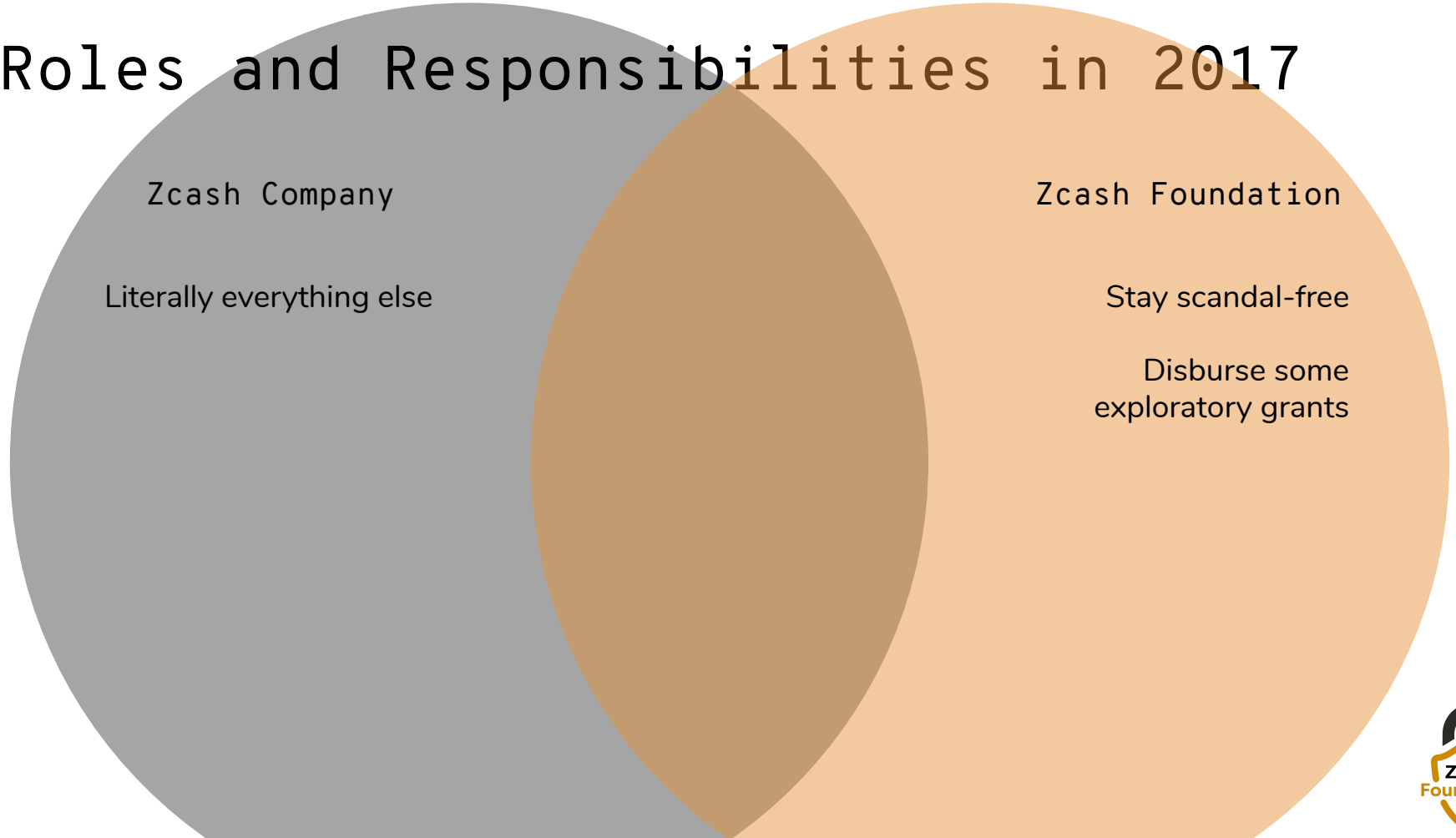
2017-the future

Zcash Foundation

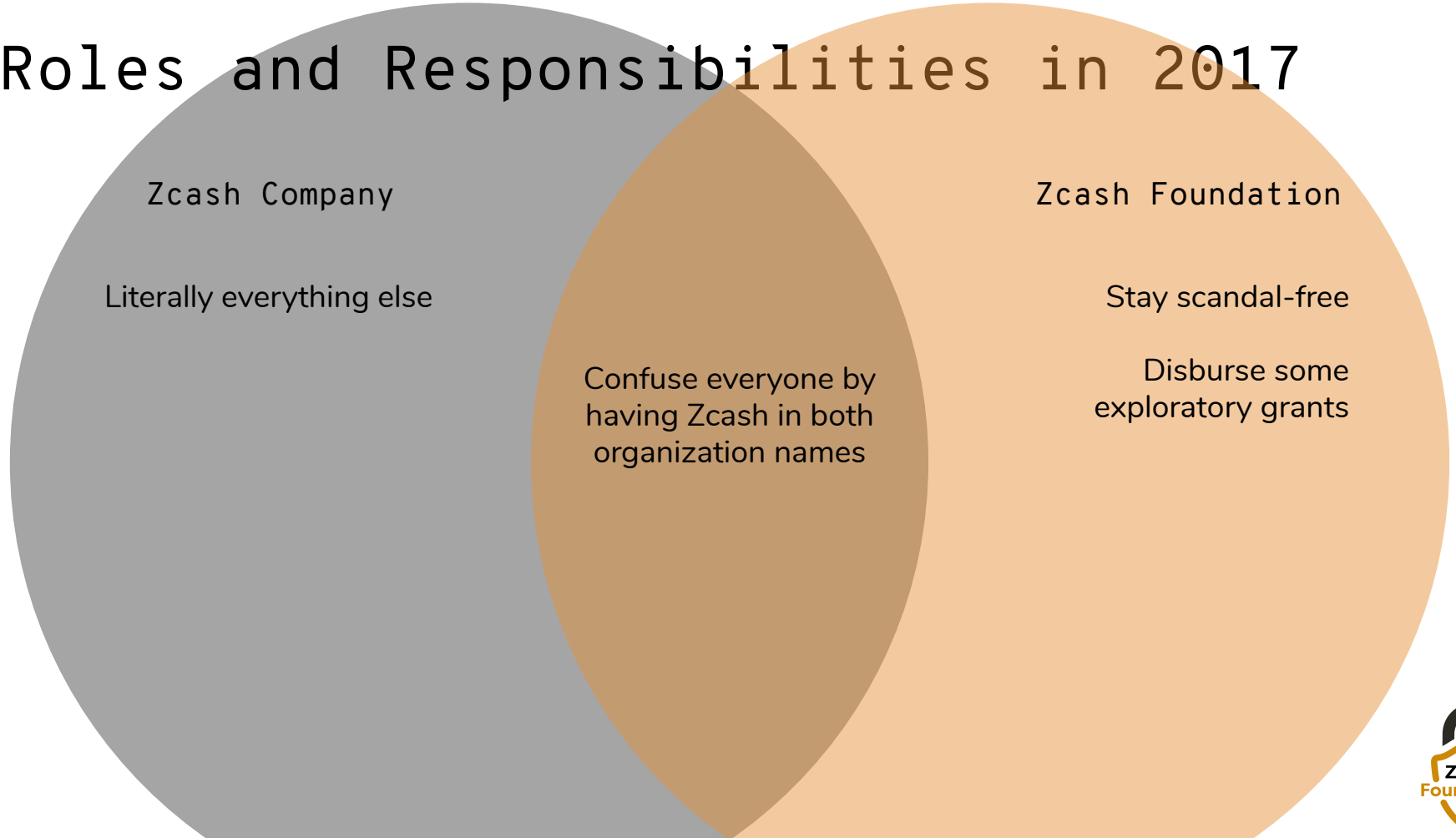
Roles and Responsibilities in 2017



Roles and Responsibilities in 2017



Roles and Responsibilities in 2017



Zcash Foundation

Roles and Responsibilities in 2019+

~~Zcash Company~~
Electric Coin Company

Continued maintenance of zcashd

Supermajority of protocol roadmap and feature development

Ecosystem development and partnerships

Build open source reference wallets and libraries around Zcash

Protocol and feature development

Zcash Foundation

Disburse grants and coordinate crowdfunding

Experiment with governance structures (see our advisory vote process)

Host Zcon\d*

Research speculative cryptography

Zcash Foundation

But what *incentives* generate these delineations?

Zcash Foundation

Incentives

~~Zcash Company~~
Electric Coin Company

Fiduciary duty to shareholders as for-profit

Advance privacy everywhere

Maintain and grow Zcash

Zcash Foundation

Duty of care as non-profit

Public support test for public charities

Zcash Foundation

Why have a 501(c)3 Public Charity?

Long legal tradition removes (some) ambiguity

Conflict of Interest policies are legally binding

Plenty of history of successful software- and protocol-focused 501(c)3s

Norms for nonprofit pay

Meeting public support test means you collect lots of donations from like-minded, ideologically aligned public and orgs, while you must make less from investment and income. Wide distribution of funding is a Good Thing.™

Zcash Foundation

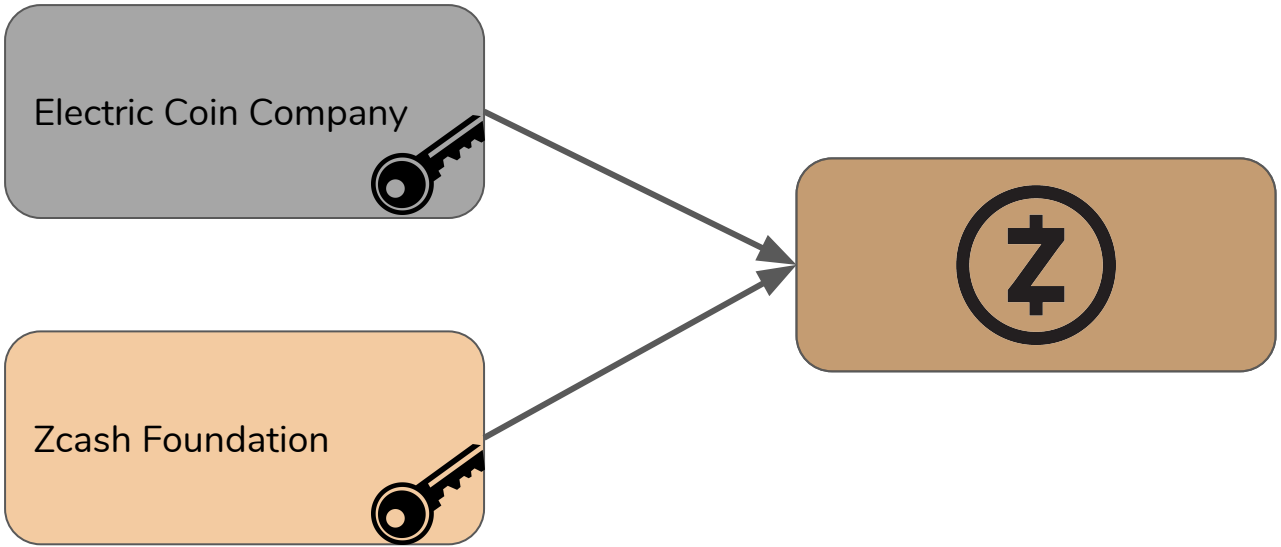
Bimodal political power distributions are *powerful* in systems *designed for gridlock*

Zcash Foundation

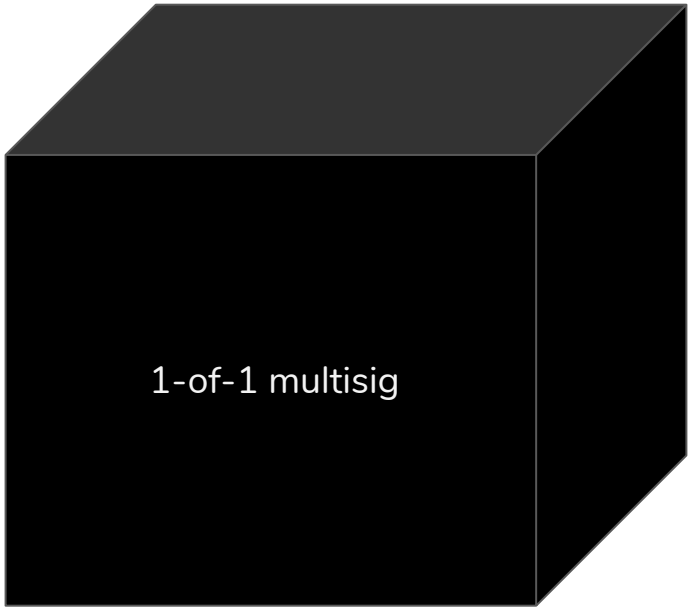
Bimodal political power distributions are *powerful* in systems *designed for gridlock*

Zcash Foundation

...or perhaps by more familiar analogy



Zcash Protocol Governance to date



this was by design, but not suitable for long-term protocol sustainability
***there was/is long-term incentive alignment between ECC and Zcash protocol development!*

Zcash Foundation

It’s up to us — and the broader Zcash community — to build multisig governance

Parity partnership for independent, consensus-compatible Zcash node

Future trademark agreement

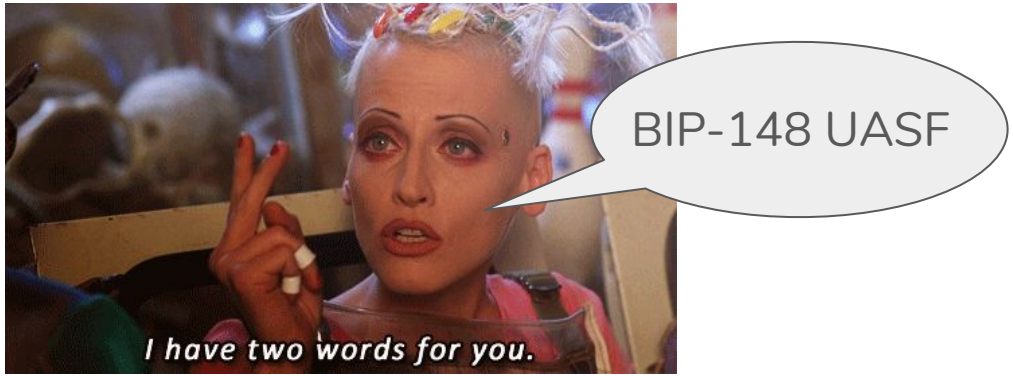
Zcash Foundation grant platform

ZIP improvements

Zcash Foundation governance panel experiment

Zcash Foundation

`Alternative consensus-compatible node`



Plausible threats of intentional chainsplit dynamics matter...though there are trade-offs with multiple implementations

`Trademark Agreement`

Legal equivalent of “plausible threat of intentional chainsplit”

Zcash Foundation

ZF Grant Program

ZFGrants

ZIP Process

```
ZIP: 0
Title: ZIP Process
Champions: Daira Hopwood
           Josh Cincinnati
Status: Draft
Type: Process
Created: 2019-02-16
License: BSD-2-Clause
```

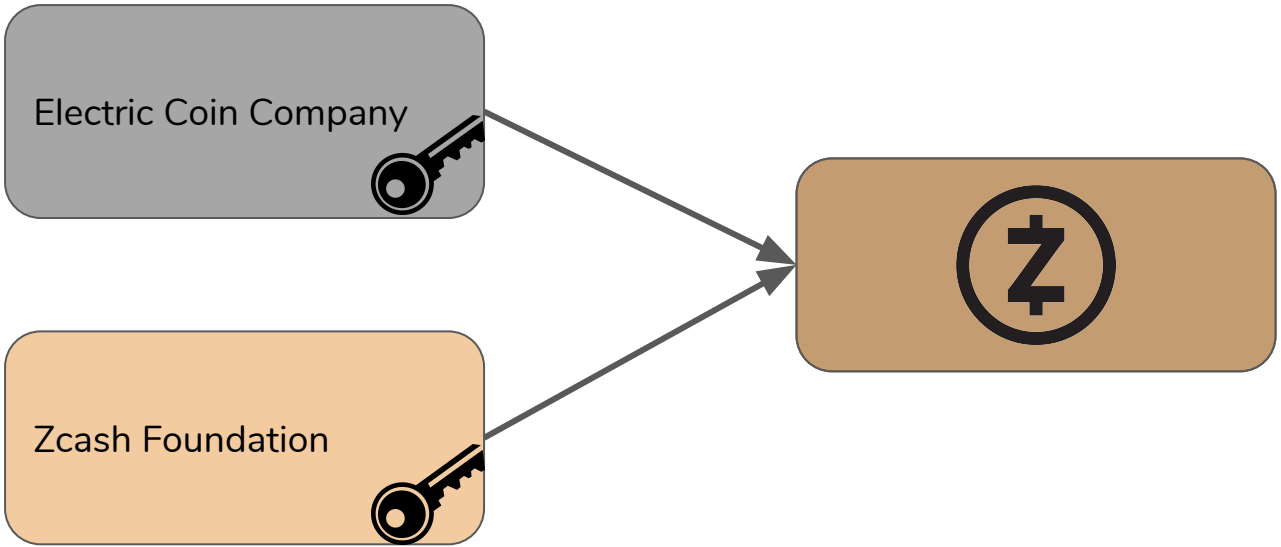
Governance Panel Experiment

Zcash Foundation Governance Process Results

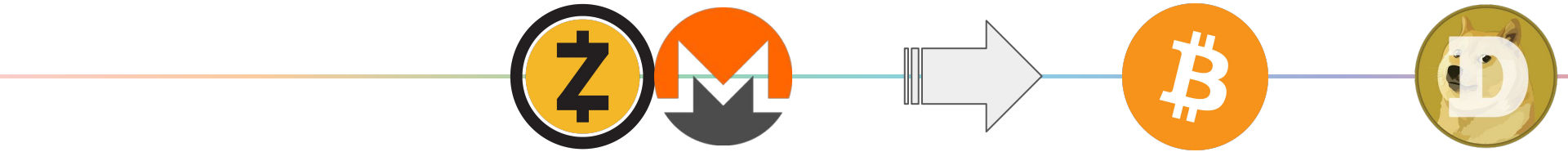
BY ZCASH FOUNDATION JULY 03, 2018

Throughout June, the Zcash Foundation carried out an experimental governance process. We first announced it back in April and recently shared the results at Zcon0 on June 28.

Zcash Foundation


Electric Coin Company
Zcash Foundation

...bimodal power distribution is not the end goal



Concentrated Power

Distributed Power

Zcash Foundation

Ultimately we are one of many governance experiments, for one of many privacy experiments.
And that’s a very Good Thing™.

Zcash Foundation

Before Q&A

Josh Cincinnati
@acityinohio

You can simultaneously believe:
- Grin/Beam/MW is super cool
- So are many other privacy approaches in cryptocurrency (Zcash, Monero, etc.)
- ...but not others (Dash, Verge, etc)
- Bitcoin will remain a dominant SoV cryptocurrency (and once Lightning matures, an awesome MoE too)

2:14 PM - 18 Jan 2019

62 Retweets **365** Likes

28 62 365

Zcash Foundation

Thank you and Q&A!

@acityinohio
@ZcashFoundation
zfnd.org/zcon

Zcash Foundation