

MONERO'S RELEASE SCHEDULE: WE CAN DO BETTER

JUSTIN EHRENHOFER

DV TRADING / DV CHAIN

COMMUNITY WORKGROUP ORGANIZER

HIGH-LEVEL TAKEAWAYS

Monero's release schedule is usually nothing short of chaos

Updates are fine, but we need to get our act together

Effort isn't typically the issue

We need to be better at communication



WHAT MONERO SUPPOSEDLY DOES

Taken from the 2015 Year in Review



MONERO'S RELEASE SCHEDULE: WE CAN
DO BETTER - JUSTIN EHRENHOFER



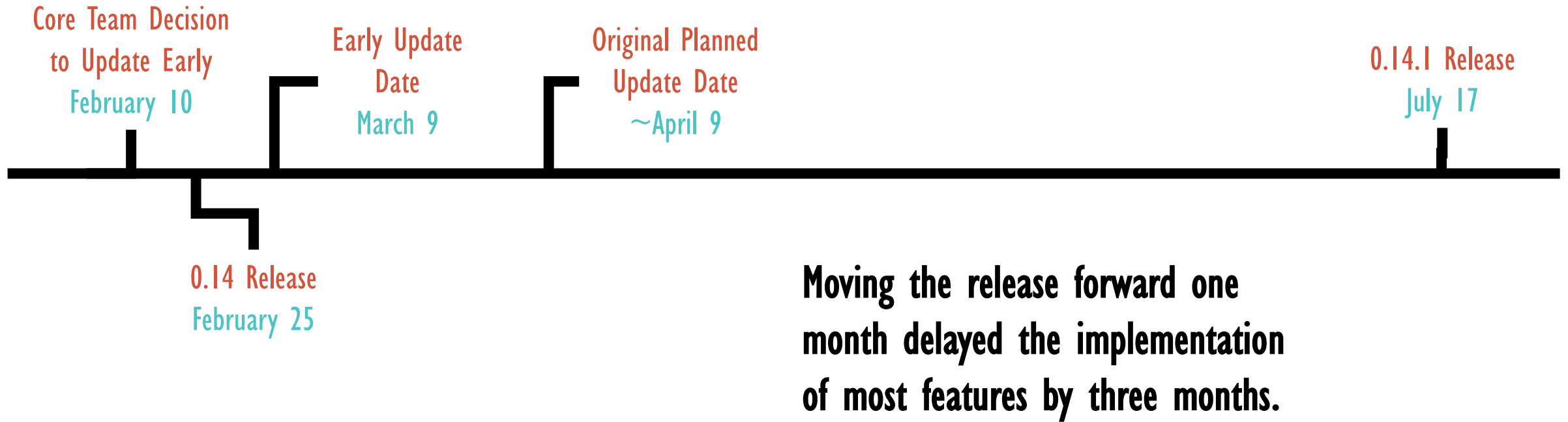
GOVERNANCE PROCESS



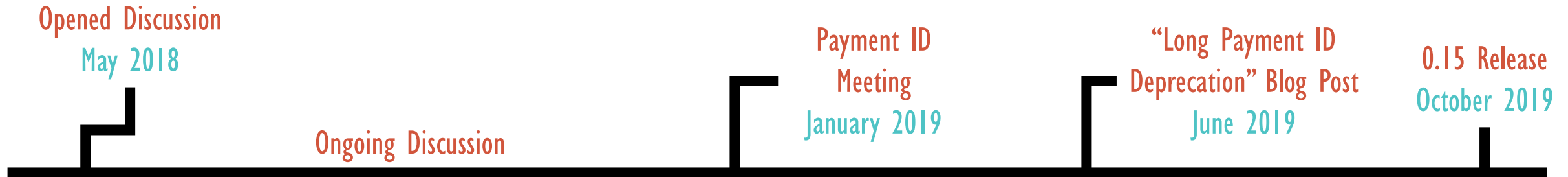
CASE STUDY I: SPRING 2019 UPDATE



CASE STUDY I: SPRING 2019 UPDATE



CASE STUDY II: PAYMENT IDs



CASE STUDY II: PAYMENT IDs

Everyone agreed that using long payment IDs is bad

Only some people argued for the removal of short payment IDs

No one agreed on what “deprecation” meant — wallet or consensus?

No one agreed on how to deprecate — permanent or temporary?



AREAS OF SUCCESS

Monero has a strong decentralized passion. It's unlikely that controversial changes can be implemented without significant prior discussion.

Monero has a huge community of people who genuinely care. They offer many perspectives with good intentions.

The Monero community continues to grow.



ROOM FOR IMPROVEMENT

Monero doesn't have enough code reviewers.

Monero Core Team is a bottleneck.

More formal proposal processes and distilled discussions are needed.

Better stakeholder notifications are essential for feedback and communicating timelines.

Monero needs to commit to many (not all) changes in advance.



WHAT ARE WE DOING?

Github issues and pull requests

Developer, Community, MRL meetings

Reddit discussions

IRC discussions



WHAT ARE WE DOING?

Github issues and pull requests

Developer, Community, MRL meetings

Reddit discussions

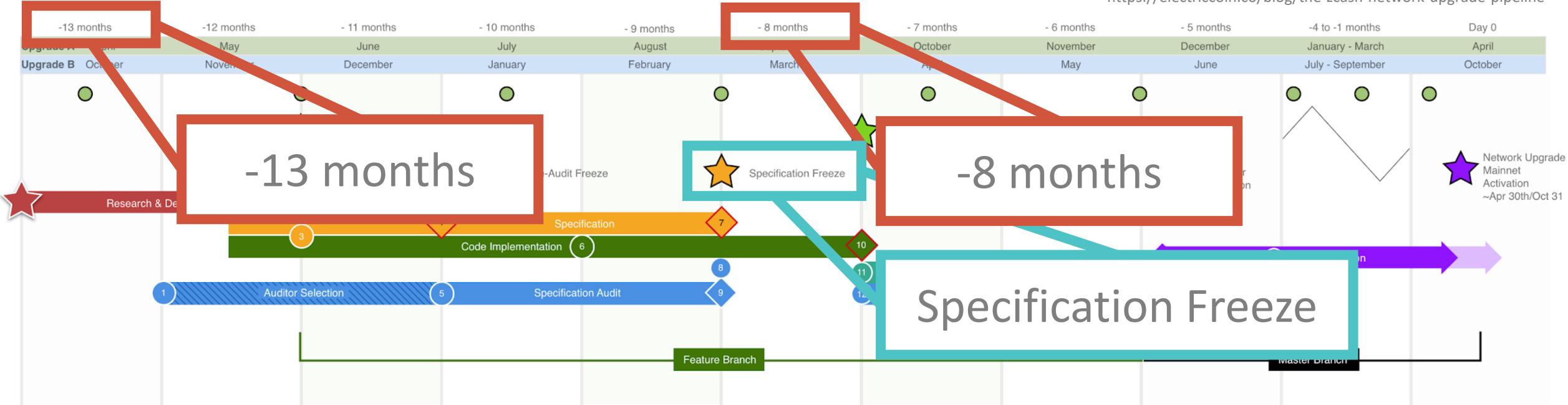
IRC discussions

**A chaotic, hands-off
decision-making process is
MORE centralized than a
clear, formal process**



WHAT ARE OTHERS DOING? - ZCASH

<https://electriccoin.co/blog/the-zcash-network-upgrade-pipeline>



R&D Begins

This should begin no later than 13 months before mainnet activation, but can be started earlier.



Minor Release



Auditor Selection Begins

Define scope based on specification information so far, find auditors, negotiate contracts.
Handoff from R&D Lead to Security Assessor



R&D Lead verifies that feature selection is complete and Specification Lead agrees to take on specification work



Specification Lead provides initial specifications to Implementation Lead and Implementation Lead agrees to take on work



All specifications for all features are complete. Specifications may only change after this point if anyone discovers a high priority issue.



All new or incomplete specifications after this point must go into the next activation, but work may continue to get them activation-ready for the next release.



Auditor Selection Complete



Prototype and Test Vectors Complete



All specifications are complete, including all changes as a result of the specification audit. Specification Lead certifies that all specifications are complete and Implementation Lead agrees to take on implementation completion



Security Assessor certifies that all specification audits are complete and all remediations have been completed. Implementation Lead agrees to take on implementation completion.



Specification Audit and Remediations Complete

All incompletely audited or remediated specifications after this point must go into the next activation, but work may continue on these incomplete specifications to get them activation-ready for the next release.



Code is Feature Complete



Code is complete except any fixes that arise in testing/implementation audit, including RPCs and wallet integration but not necessarily library updates. All features that are not code-complete must go into the next activation; work may continue on code to get it activation-ready for the next release.



Implementation Lead certifies that all coding is feature complete and Quality Assessor agrees to begin QA process.



Implementation Lead certifies all coding is complete and Security Assessor agrees to begin the implementation audit process.



All code has been completed, tested and audited. Library updates are completed



Testing and Remediations Complete

All features that are not fully tested with all issues remediated must go into the next activation, but work may continue on new specifications to get them activation-ready for the next release. Quality Assessor and Security Assessor certify that all testing and audit is complete and all remediations have been completed. Implementation lead agrees to merging and activation.



Mainnet Activation Commit

- 4 months (Dec 31/Jun 30)

WHAT ARE OTHERS DOING? - SIA

Sia Feature Roadmap



Public



Info



Welcome to the Sia Public Roadmap!
Click to learn more.

68 2

Sia Releases. Click for link.

3



Long Term



File sharing - share files with users who are not on Sia

295

Support for mobile wallets and other lite clients

140

Automatic host pricing

122

Ability to set price vs. performance preferences

65

Add proof-of-burn mechanic to hosts

44

Ability to see host uptime

41

Testnet for Sia

9

Medium Term



Simple file sharing - Share files with other Sia users

229

Support for tiny partial downloads. Instead of downloading 40 MiB at a time, download as little as 16 KiB at a time.

10

Relay Payments

SDK Library

Instant Boot

Continuous file backups

Local Language Support in the UI

Short Term



Video streaming - short load times

22

Improve memory usage for large uploads

Proper support for tiny files (reduce minimum file size from 40 MB to ~100kb)

192 1

Partial Uploads

2

Deletion of Data from Contracts

Renter Watch Dog

FUSE Binding

Support for file modification

1

Reset Wallet Password

Released Features



Scalability



Renter Actions



Host Actions



Wallet Features



UI Features



Troubleshooting Actions



Siacoin exchange options



1

Community Features



FORMALIZED PROCESSES \neq CENTRALIZATION

By adopting more formal processes, Monero can:

- Provide more clarity in the decision-making process
- Engage a wider set of stakeholders
- More clearly communicate changes in advance to important ecosystem components
- **Reduce** Core Team influence by giving others a clear platform
- Offer better, less chaotic release schedules

Agreeing to a sensible formal process increases decentralization overall and brings large benefits.



WHAT I DON'T PROPOSE

Voting for specific proposals — too easy to manipulate and subject to other issues

Delaying critical security patches

Upgrading at an unnecessarily high, burdensome frequency

Asking the Core Team to completely run this process

...but they need to be a part of it! Their buy-in is key!



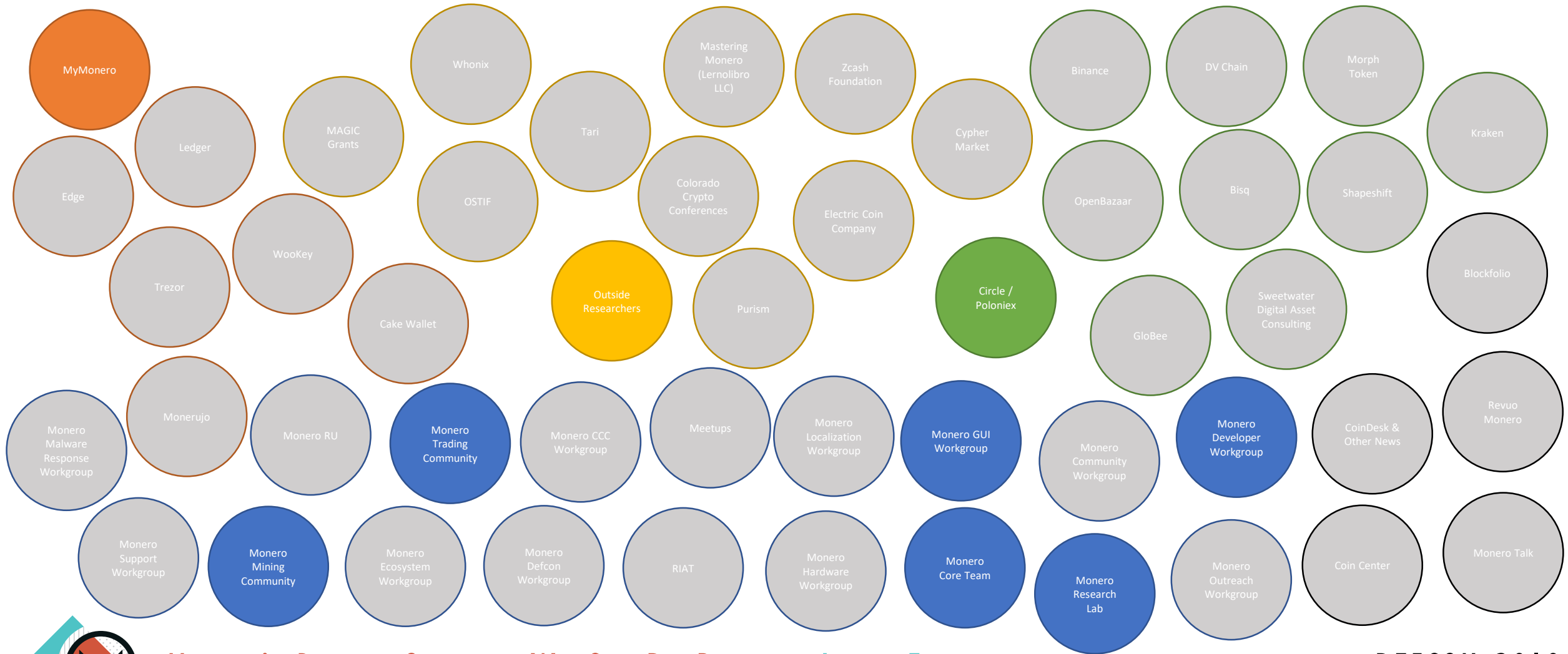
THE MONERO ECOSYSTEM GROWS IN COMPLEXITY



MONERO'S RELEASE SCHEDULE: WE CAN DO BETTER - JUSTIN EHRENHOFER

DEFCON 2019

THE MONERO ECOSYSTEM GROWS IN COMPLEXITY



MONERO'S RELEASE SCHEDULE: WE CAN DO BETTER - JUSTIN EHRENHOFER

DEFCON 2019

THE MONERO ECOSYSTEM GROWS IN COMPLEXITY

With such a diverse set of stakeholders, the Core Team & community need to embrace formalization

There is no way to keep track of thousands of conversations and dozens of workgroups

Delegate this task as needed to other workgroups sensibly

Some bureaucracy is good if it gets everyone on the same page

Core Team needs to embrace responsibilities or delegate/abdicate

Smart communication is key



SPECIFIC BABY STEPS

Commit to code freezes one full month before

Decide on the main features about 6 months before scheduled upgrades

More frequent and scheduled minor, feature updates (reproduceable builds, yay!)

Create timelines for major features

Have formal feedback submission procedures for large changes and open conversations to discuss these

Set and adhere to reasonable deadlines, and only adjust if the situation changes



SPECIFIC BABY STEPS

Commit to code freezes one full month before

Decide on the main features about 6 months before scheduled upgrades

More frequent and scheduled minor, feature updates (reproduceable builds, yay!)

Create timelines for major features

Have formal feedback submission procedures for large changes and open conversations to discuss these

Set and adhere to reasonable deadlines, and only adjust if the situation changes

Plans may change, but we need to make them and communicate them clearly



THANK YOU

justin@ehrenhofer.org

