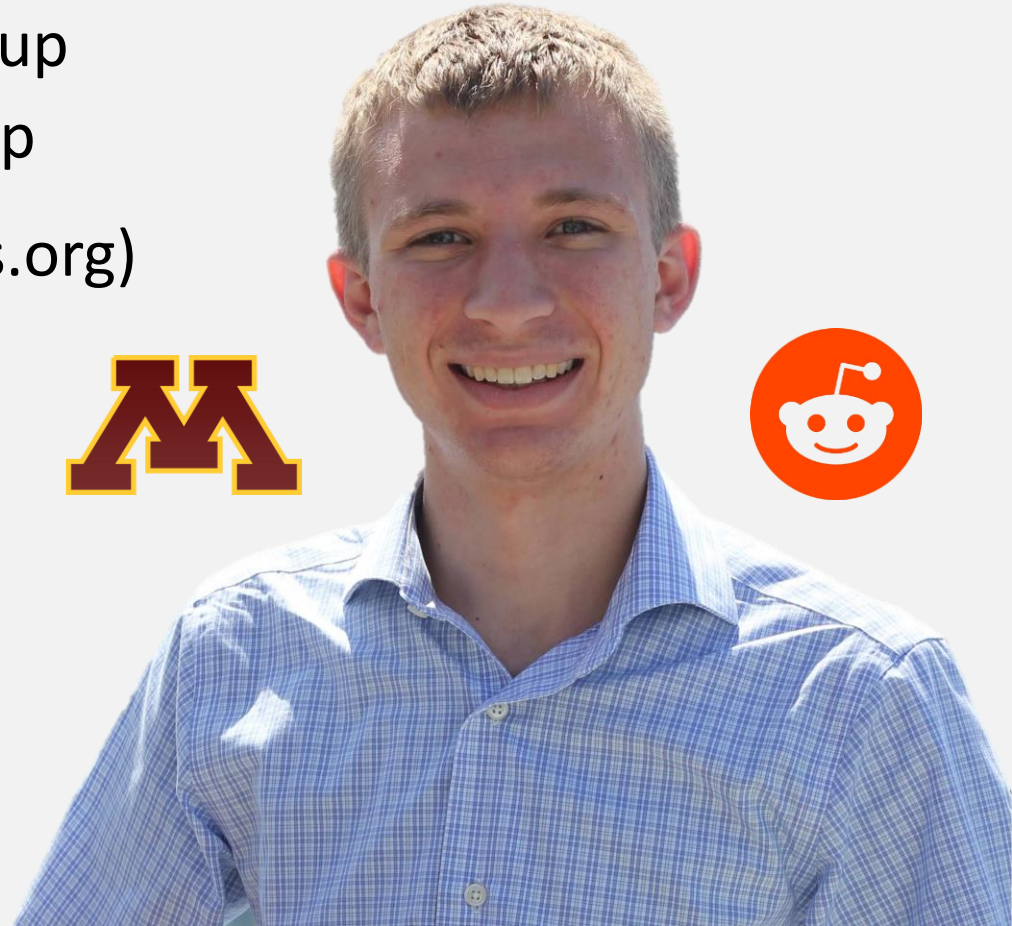

Importance of Privacy in
Distributed Systems

Who Am I?

Justin Ehrenhofer

- Organizer of the Monero Community Workgroup and the Monero Malware Response Workgroup
- Board Member of MAGIC (https://magicgrants.org)
- Previous experience in cybersecurity
- Interested in distributed privacy systems
- Senior moderator of r/CryptoCurrency with over 700,000 subscribers



Privacy Isn’t Binary

What most people think privacy is:

Privacy Isn’t Binary

What privacy actually is:

Perfect Privacy

Perfect Transparency

Riccardo “fluffypony” Spagni
Monero Core Team Member

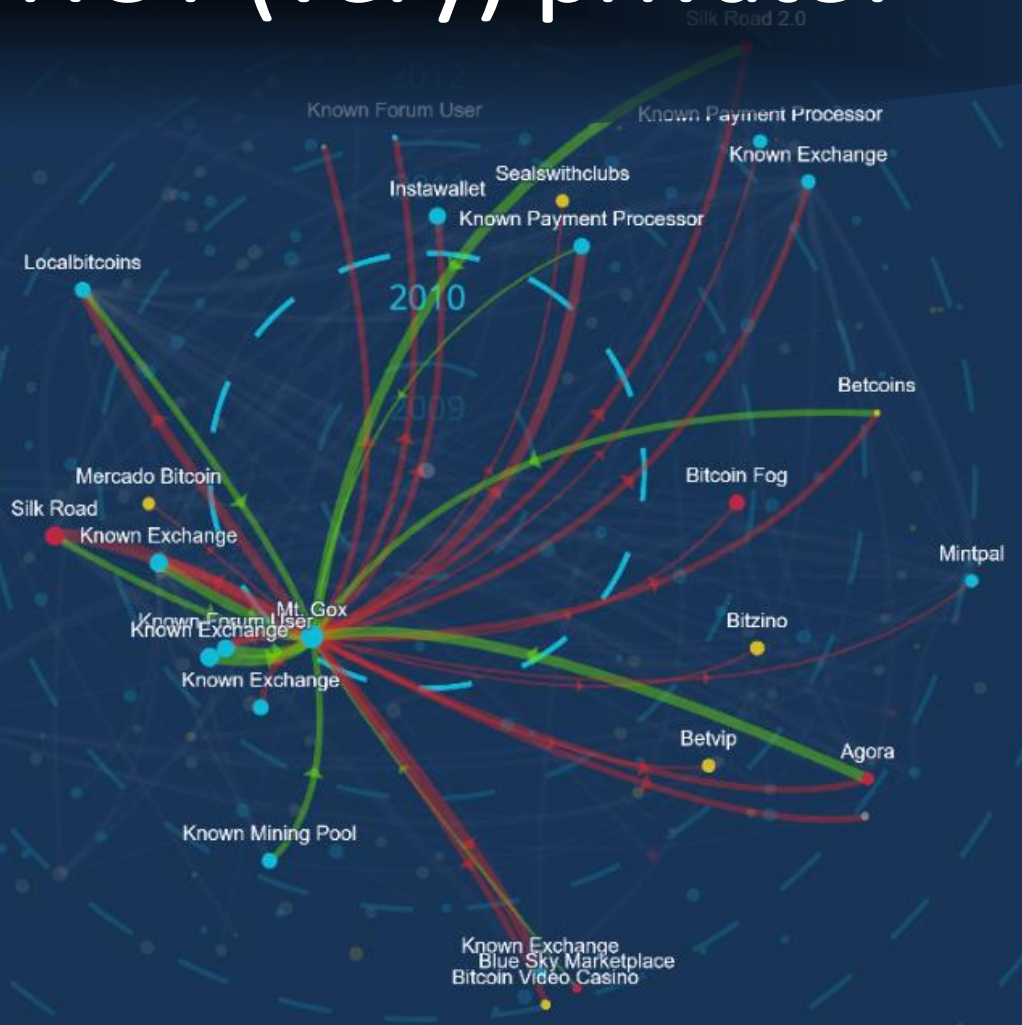
Privacy isn’t a thing that you achieve, it’s a constant cat-and-mouse battle.

It All Comes Back to a Threat Model

Image courtesy of EFF

THE BITCOIN
BIG BANG

Bitcoin is NOT (very) private!



ELLIPTIC

Transparency Has Implications on People and Business

Sources

- Employer info
- Family and friend connections
- Business suppliers and upstream business connections
- Fungibility

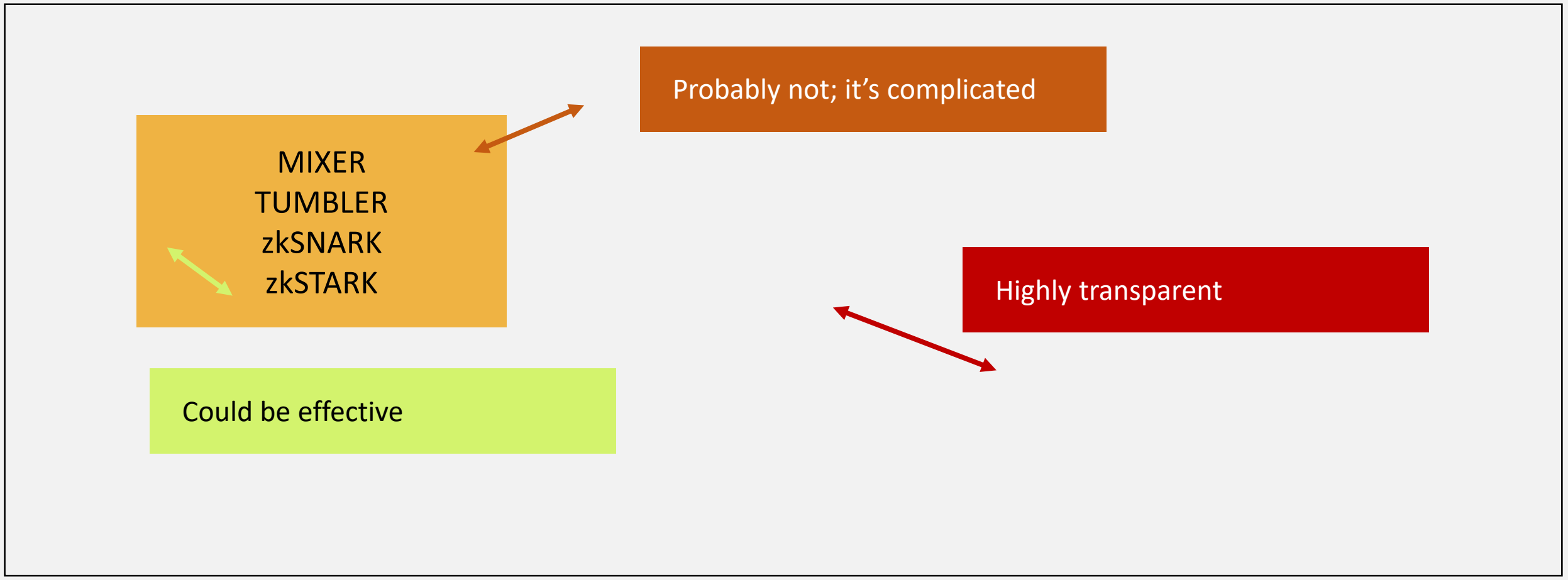
Expenses

- Political and religious affiliations
- Health data and doctors
- Customers and downstream business connections
- Everyday purchasing habits
- Employees

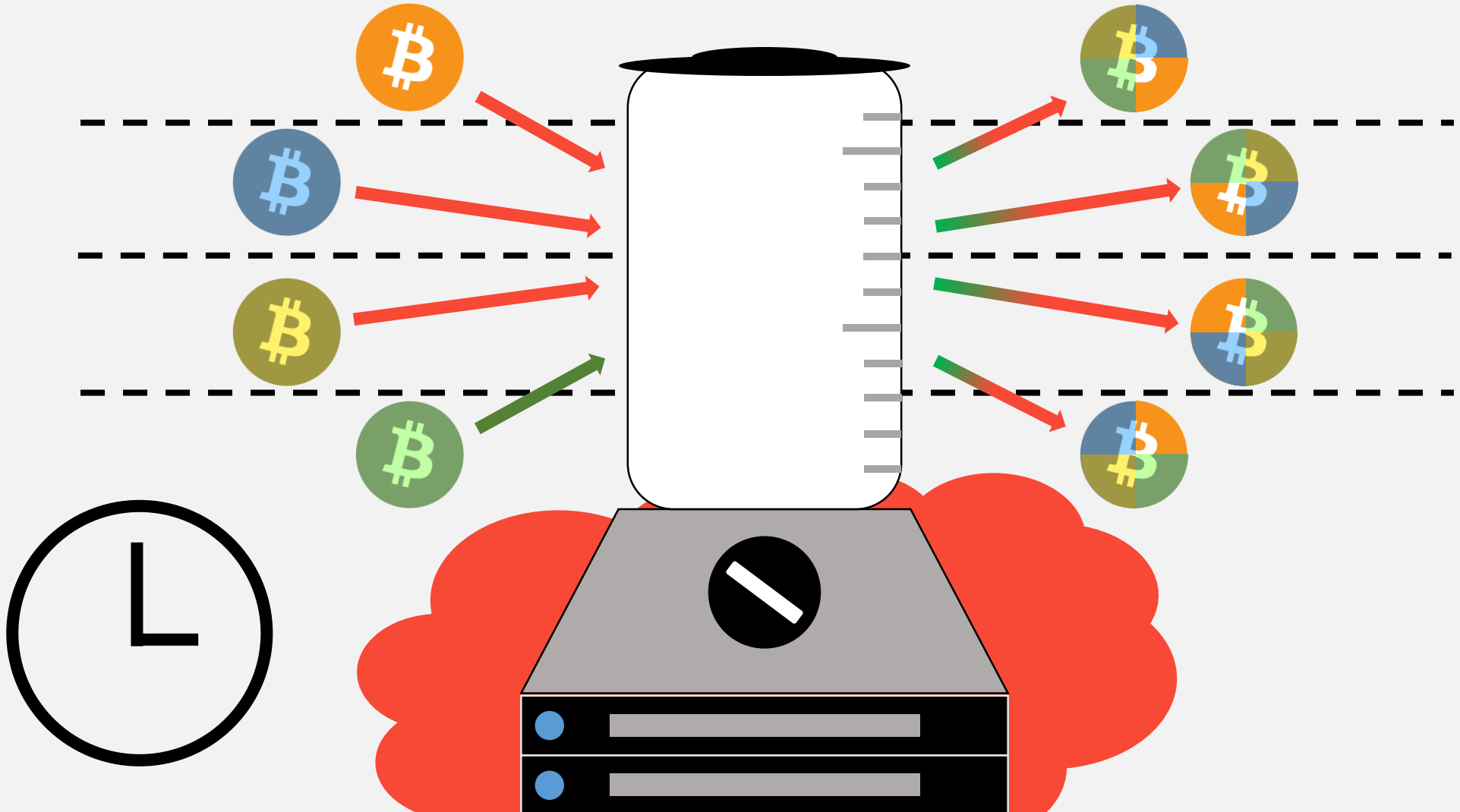
Balances

- How much money you have
- Targeted crime against wealthy individuals and companies, especially in cases of malware and robbery
- Willingness to pay suppliers and charge customers
- Willingness to pay employees

Tools Can Be Added to Transparent Systems. Their Effectiveness is Complicated



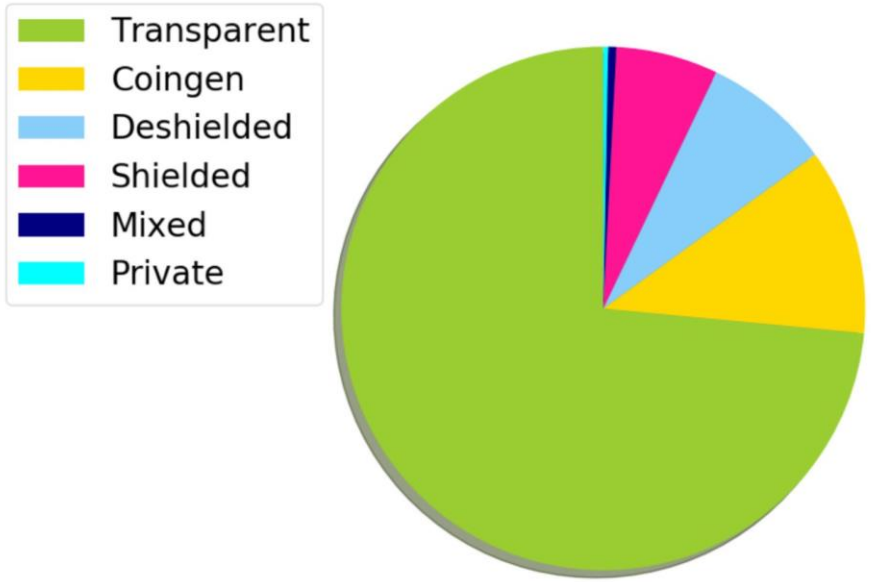
Mixing Isn't Very Effective



Effectiveness of Optional Extremely Private Systems is Complicated

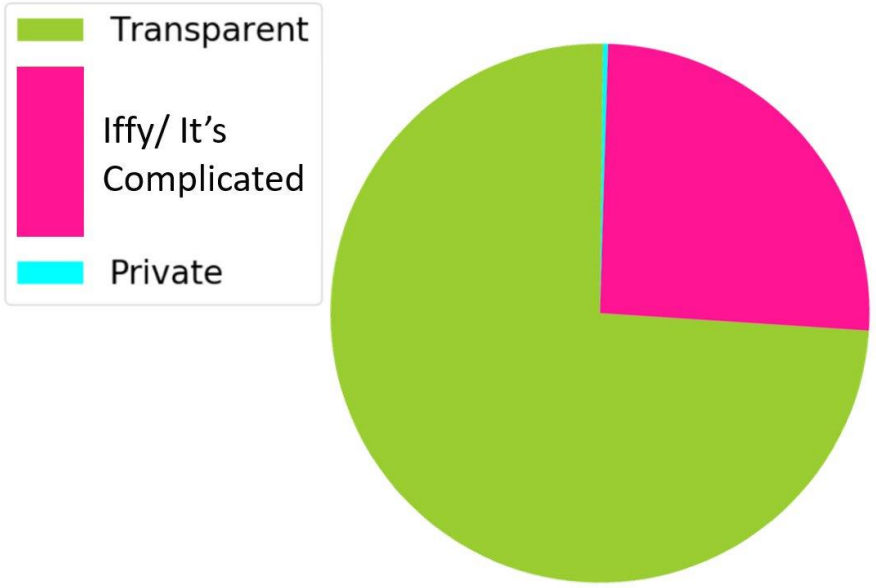
UCL

Interactions in Zcash



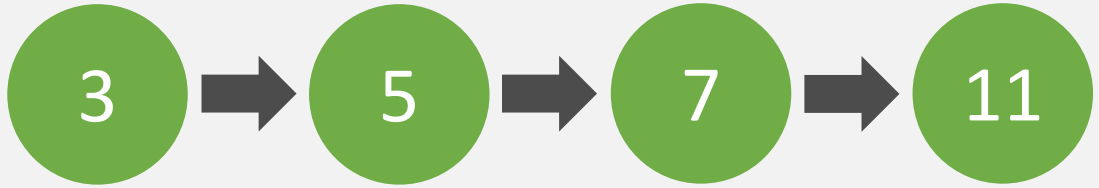
UCL

Interactions in Zcash



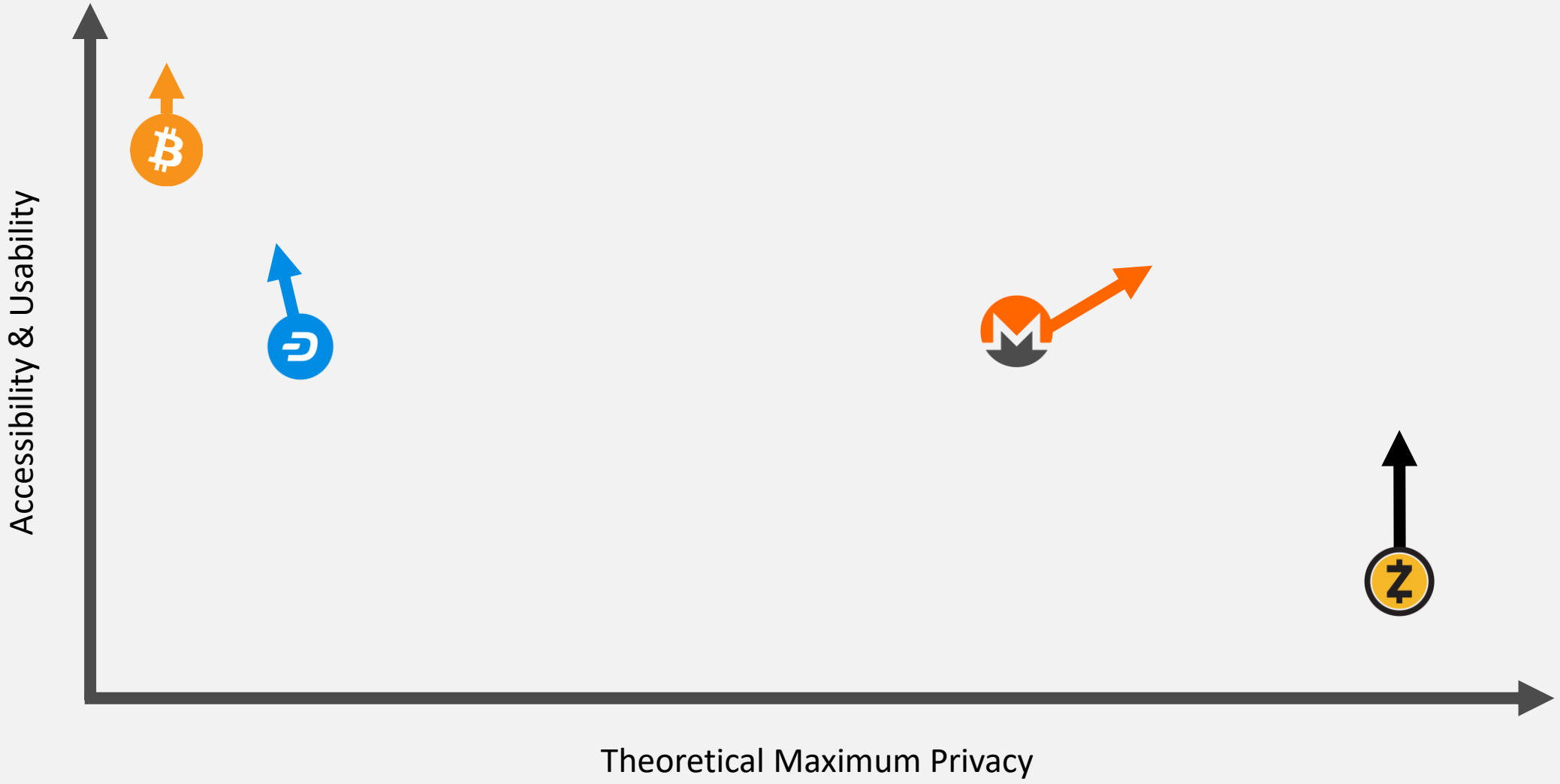
Even Mandatory Privacy Isn’t Perfect

Some things Monero has done to increase its privacy in the last few months:

- Increase ringsize from 

- Mandatory ringsizes
- Better remote node metadata protection
- Blackball tool
- Churning recommendations

Privacy Matrix



Privacy Solutions to Consider

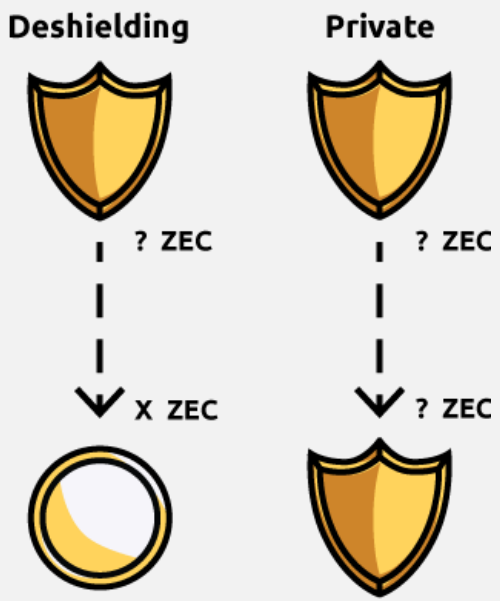
MONERO

Ring signatures

RingCT

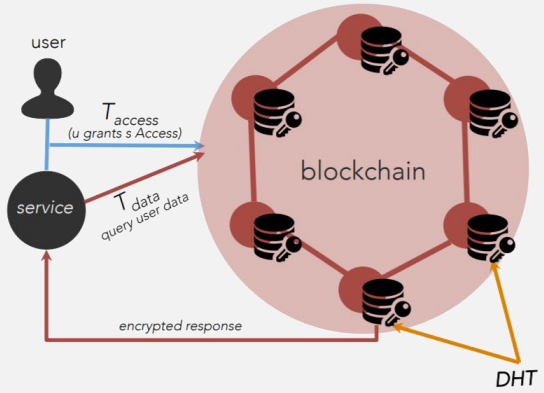
Stealth addressess

Zcash



zkSNARKs

enigma



File encryption on server

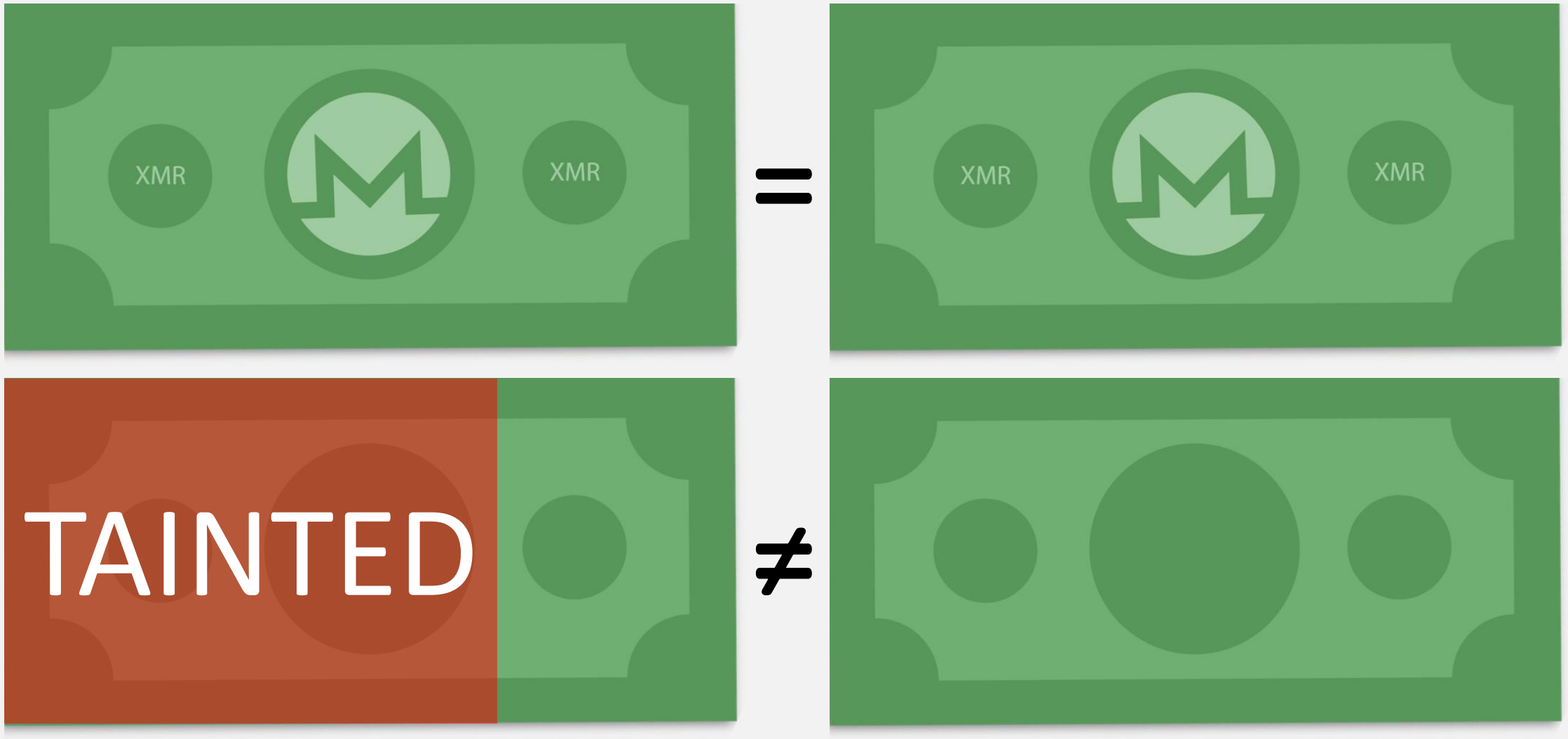
Hash stored on blockchain

STARKWARE

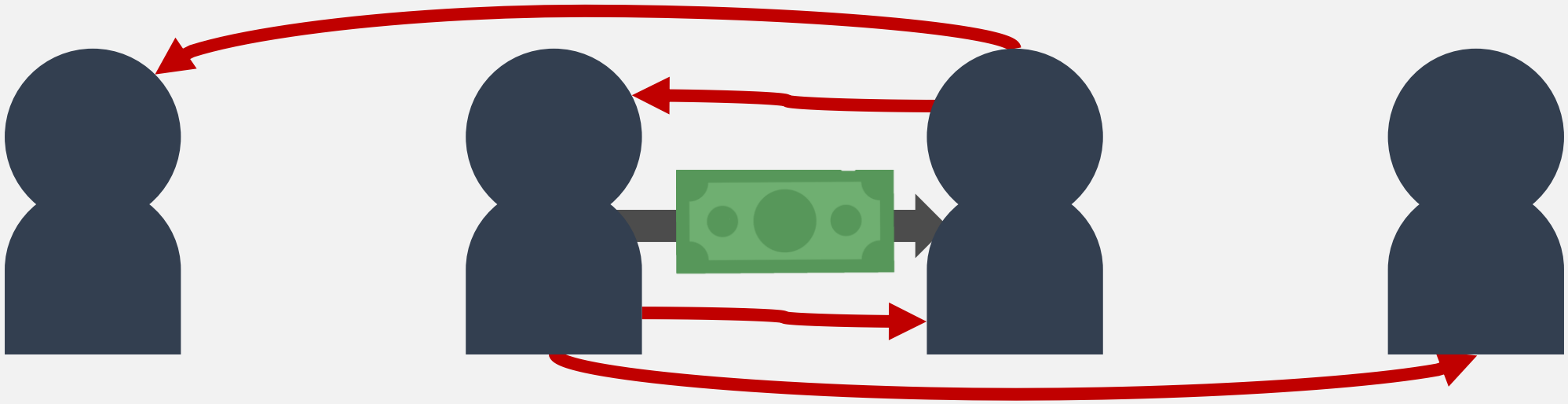
Coming Soon™

zkSTARKs

Fungibility



Fungibility



Summary

Thank You!

MAGICgrants.org

u/SamsungGalaxyPlayer

@JEhrenhofer

justin@ehrenhofer.org

`5137 9F1B A7FC 2D05`