Introduction to Monero

And a lesson in privacy and coin equality

Justin Ehrenhofer
Organizer, Monero Community Workgroup
Compliance Analyst, DV Chain

MONERO is:

a community-driven,

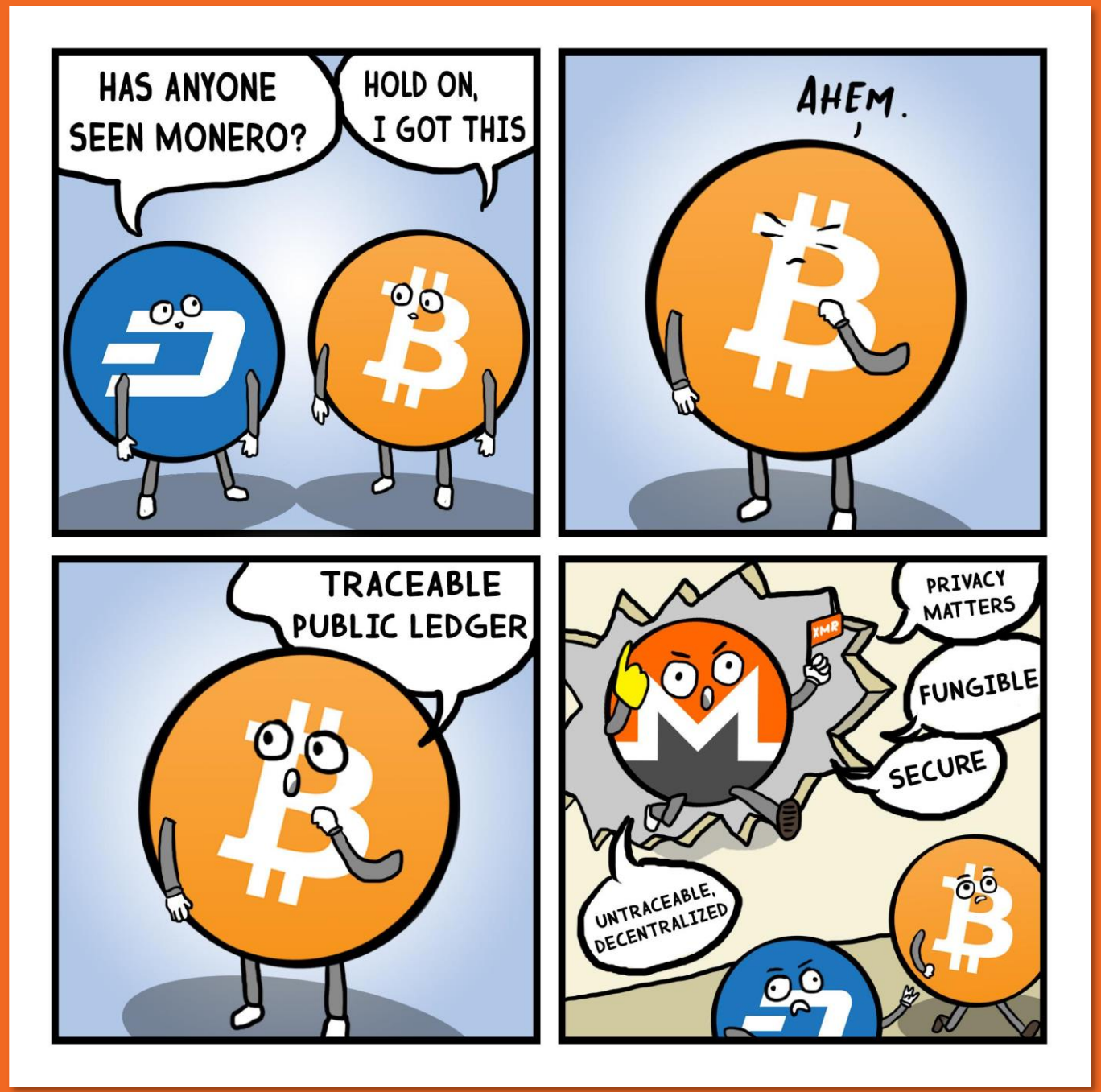
open source project that

makes safe digital cash

and owns up to its shortcomings

You may have met a Monero enthusiast in a situation like this:

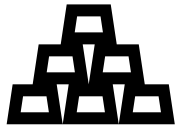
(We can't help it)



Source: https://www.reddit.com/r/moonero/comments/7h6ame/monero_in_da_house/

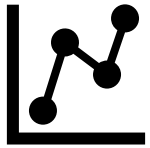
Real Problems Monero Addresses

Strong,
ubiquitous
privacy



Coin equality
(fungibility)

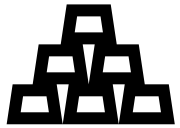
Accessible
PoW mining
(RandomX)



Adaptive
block size and
fees

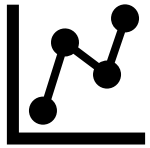
Real Problems Monero Addresses

Strong,
ubiquitous
privacy



Coin equality
(fungibility)

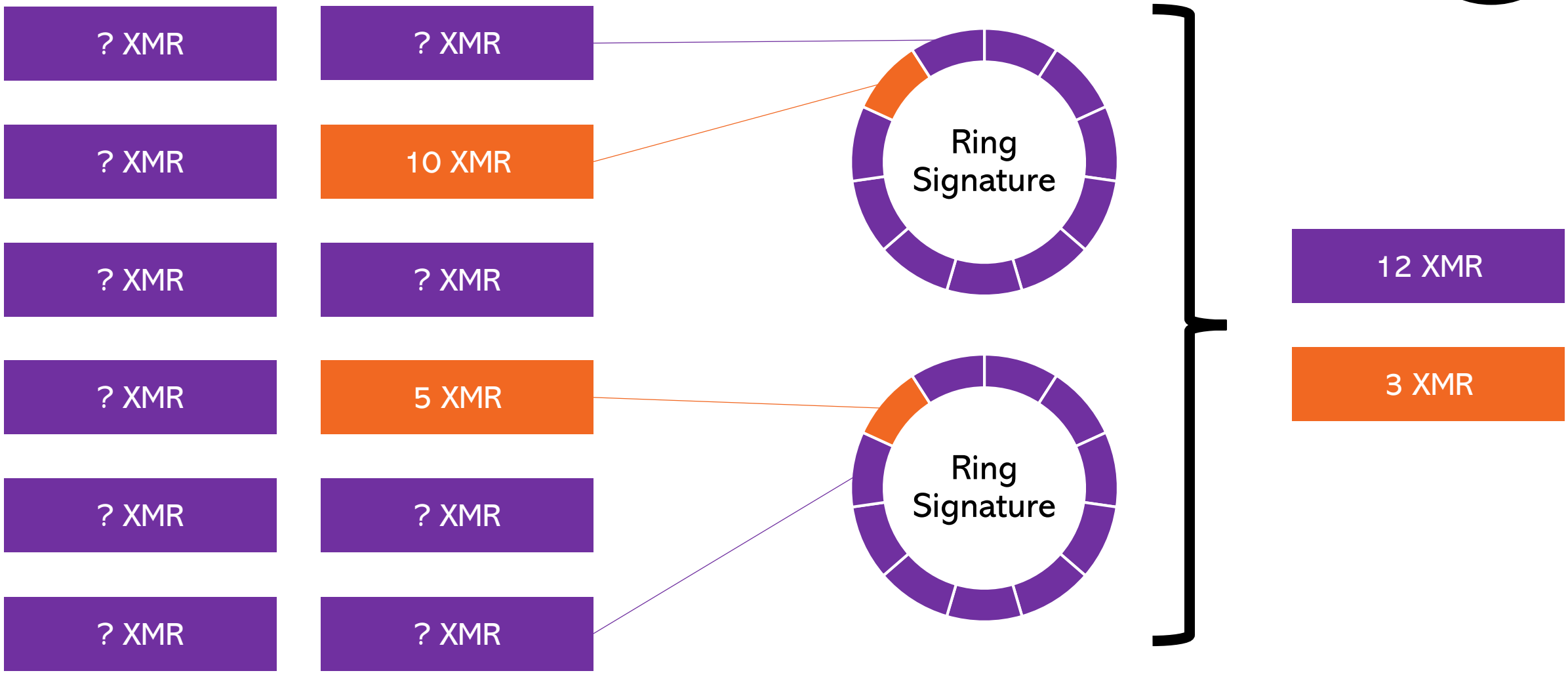
Accessible
PoW mining
(RandomX)



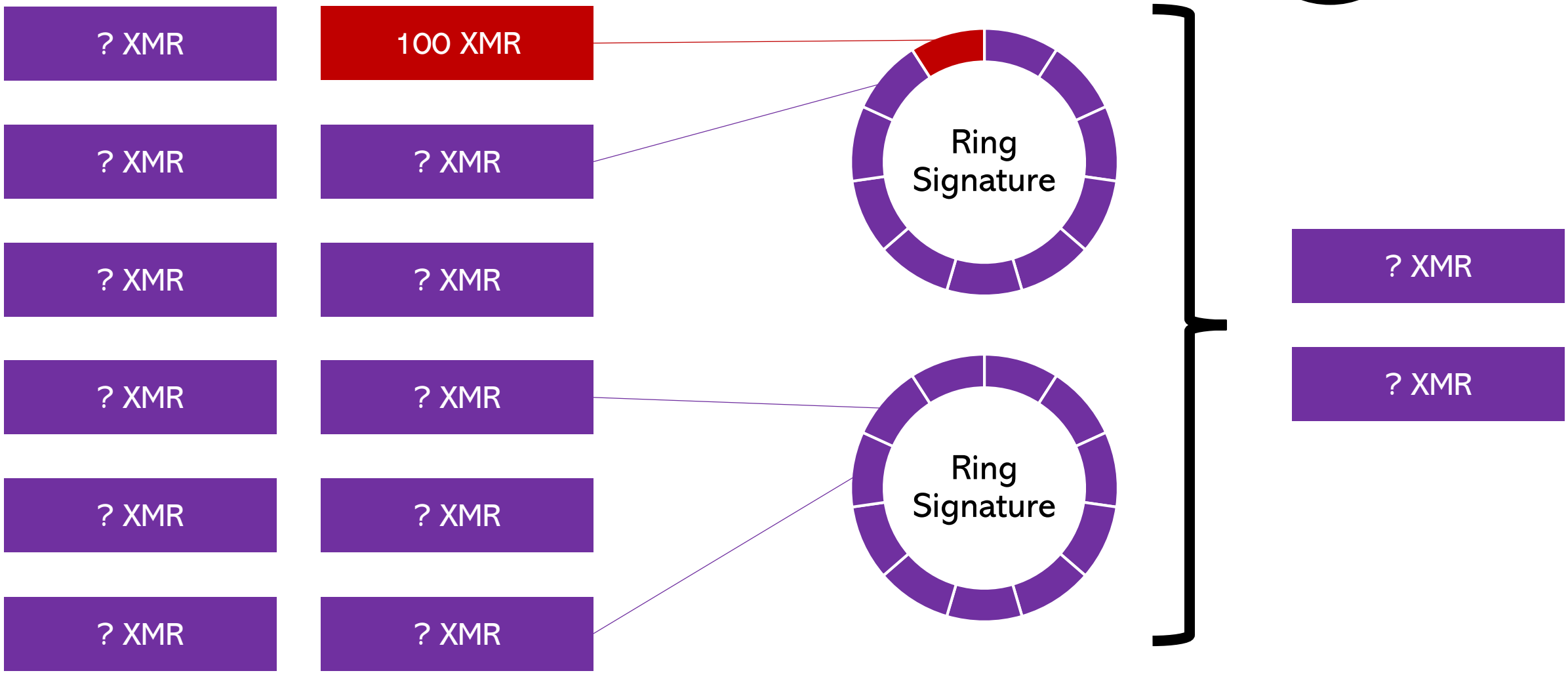
Adaptive
block size and
fees

Cryptocurrency network privacy is less than the sum of its parts

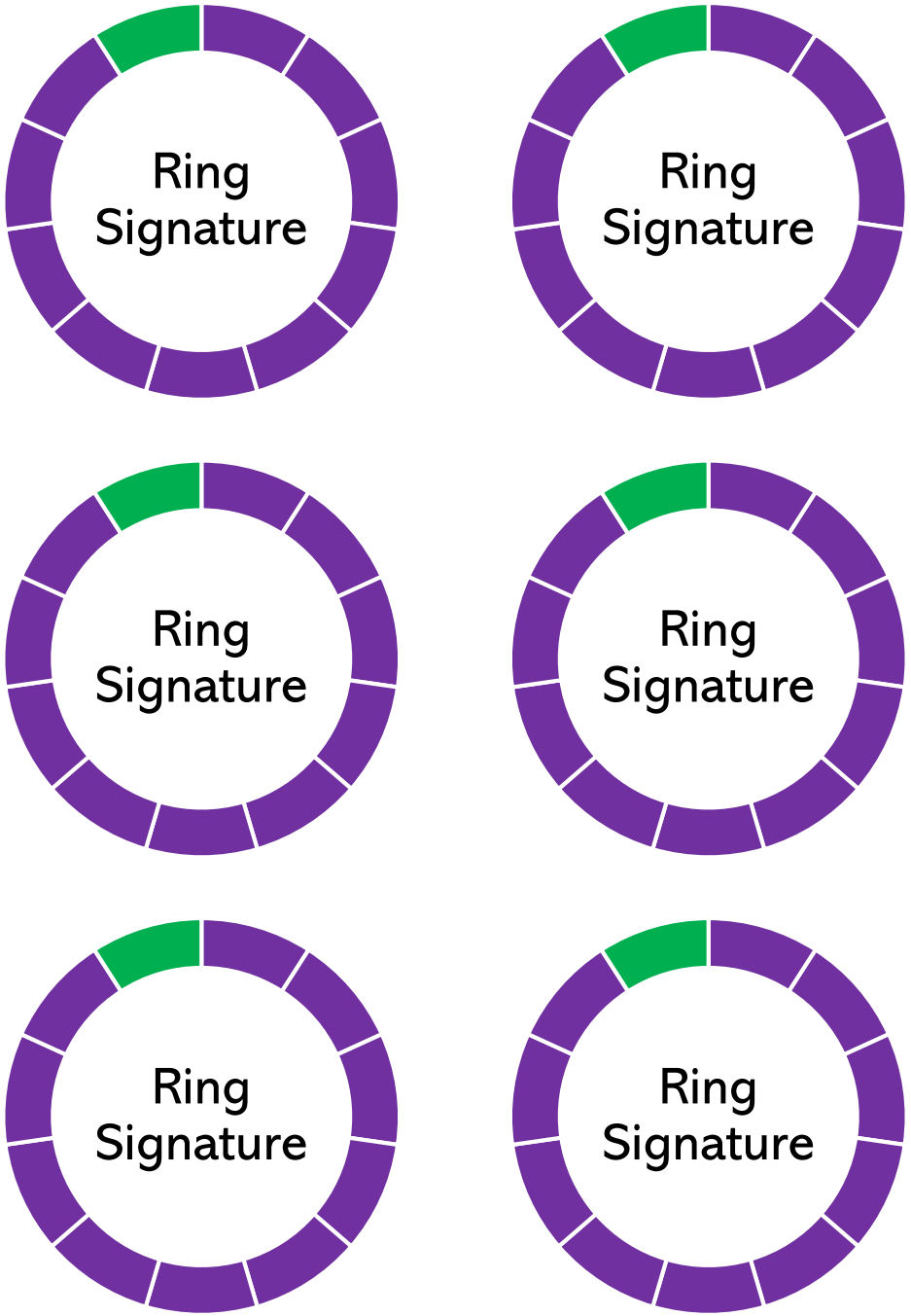
Transaction Structure and Tracing



Transaction Structure and Tracing



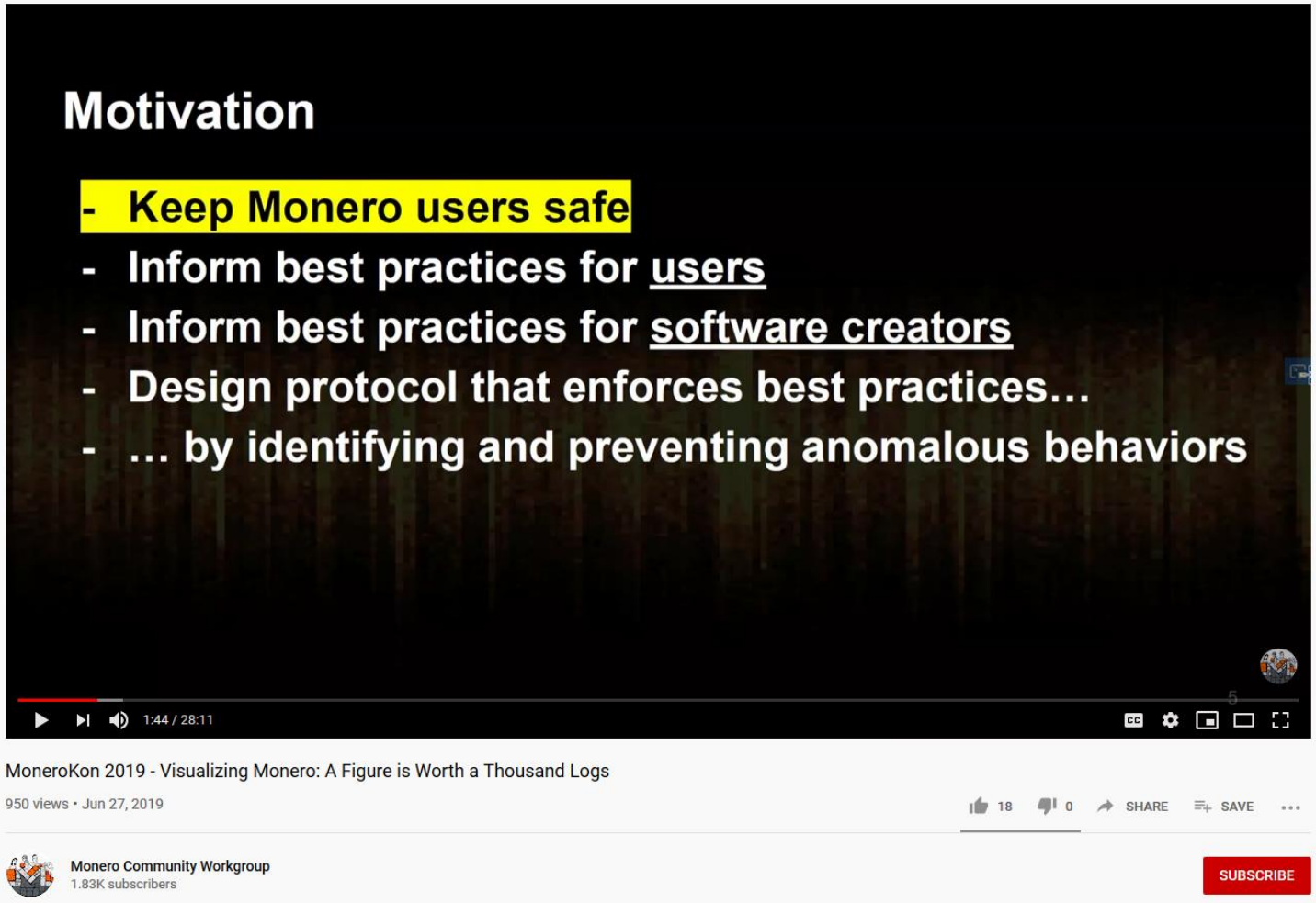
Transaction Tracing

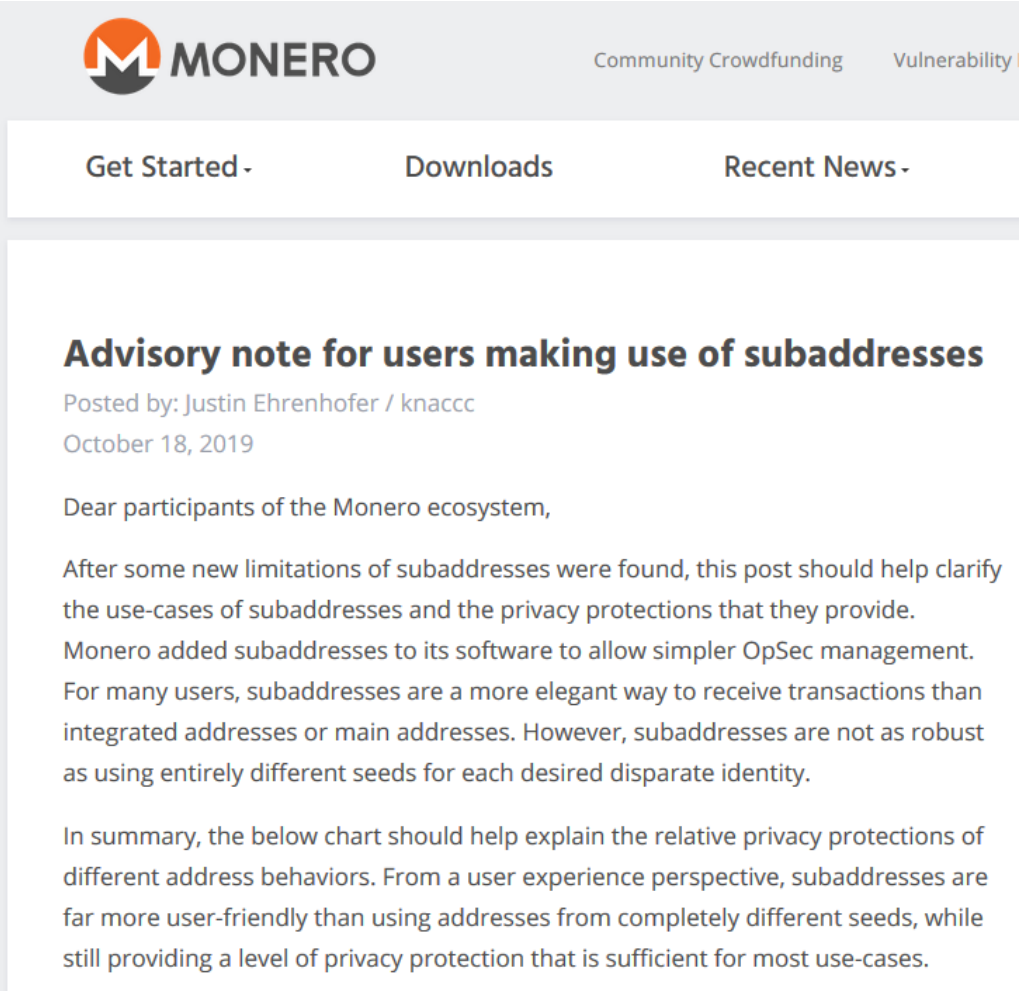


+

Monero has
REAL privacy, not
POTENTIAL privacy

If there are issues with privacy, we discuss and patch them openly, not blame users





Optional
CoinJoin
zkSNARKs
Lelantus
CoinSwap
PerfectlyPrivate™

is a bad solution for the wrong problem

Results of a fungibility exercise

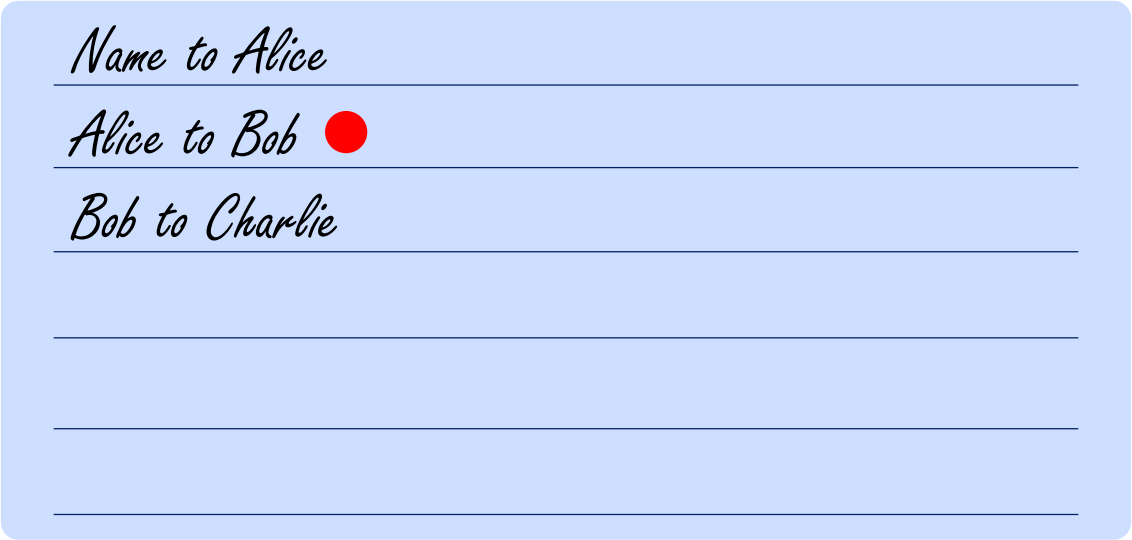
Name to Alice

Alice to Bob

Bob to Charlie

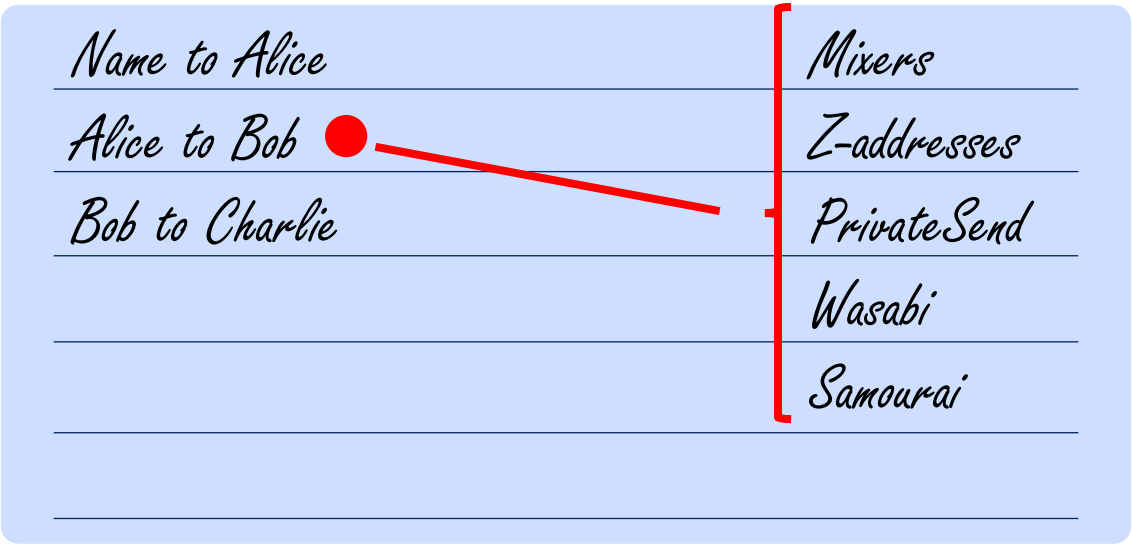
Results of a fungibility exercise

- People avoided the tainted cards
- Some would only accept tainted for “something extra”
- Most people would pay more for “fresh cards”
- In reality, who among the attendees pays for Chainalysis?

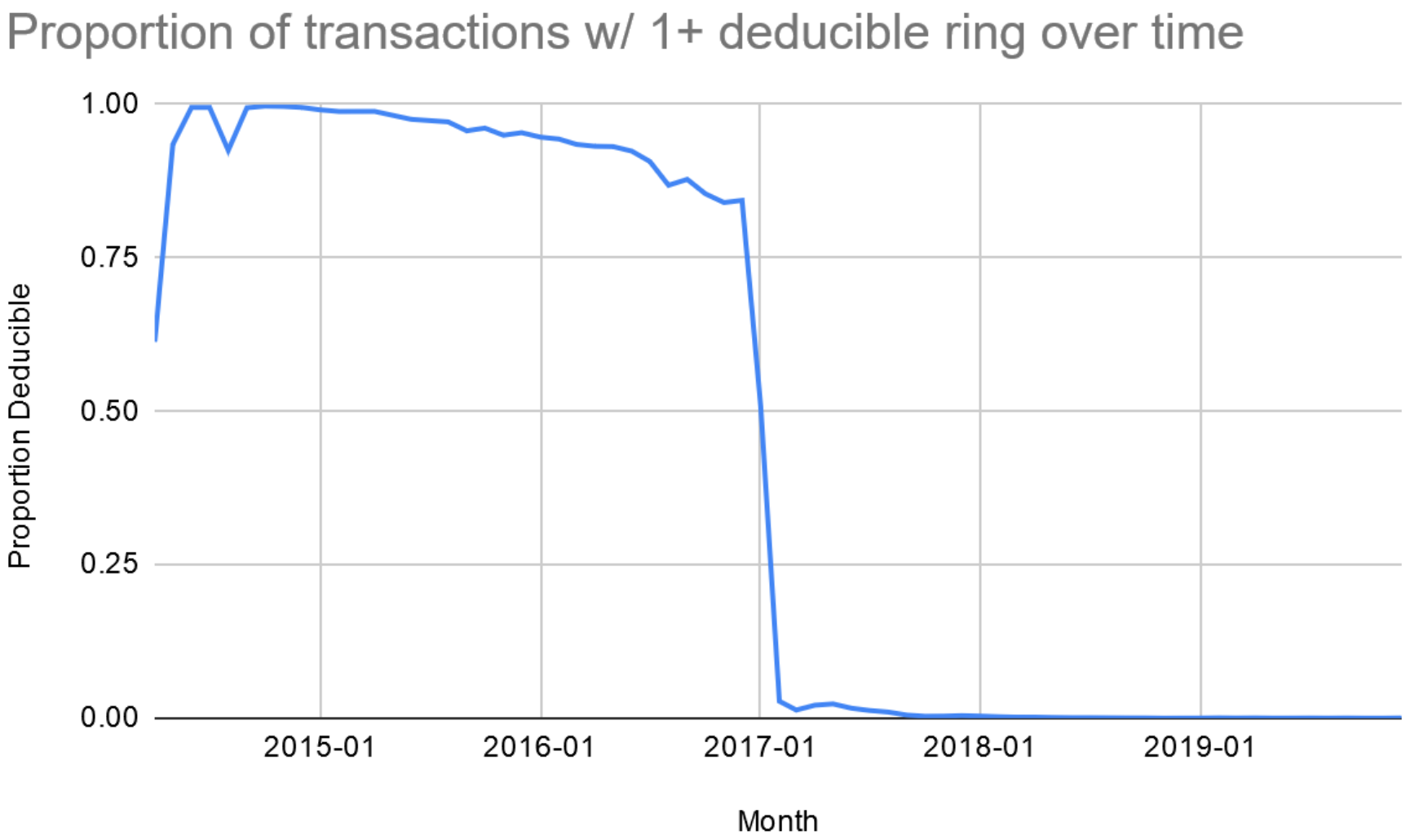


Reality

- Chain analysis companies will most likely mark the use of any optional privacy as higher risk (this is enforced by several tools)
- Mandatory mining to shielded doesn't fix
- Optional privacy often harms fungibility, not helps

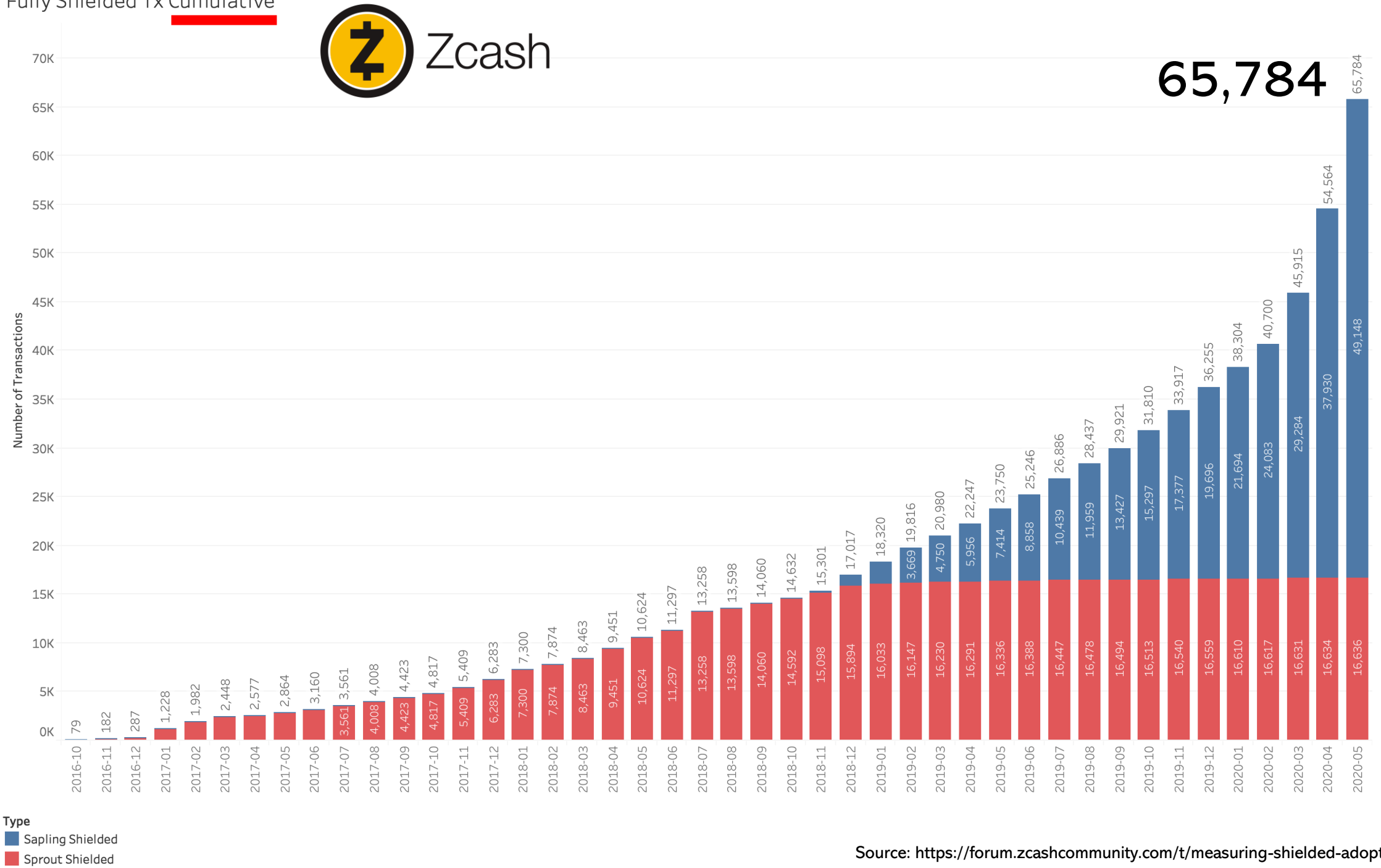


Privacy is hard. Coin equality is harder.



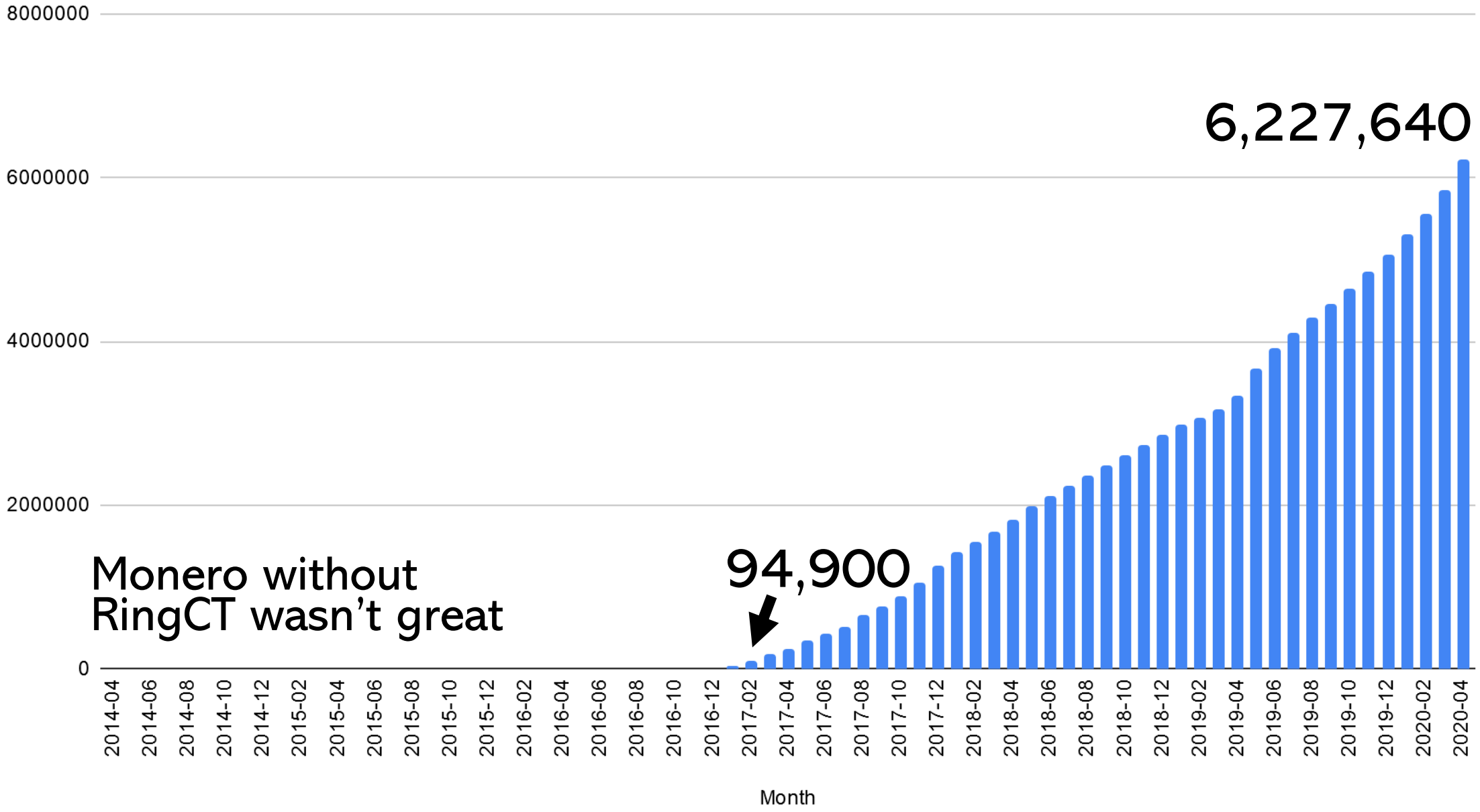
Source: Sarang Noether of Monero Research Lab using blockchain data

Fully Shielded Tx Cumulative



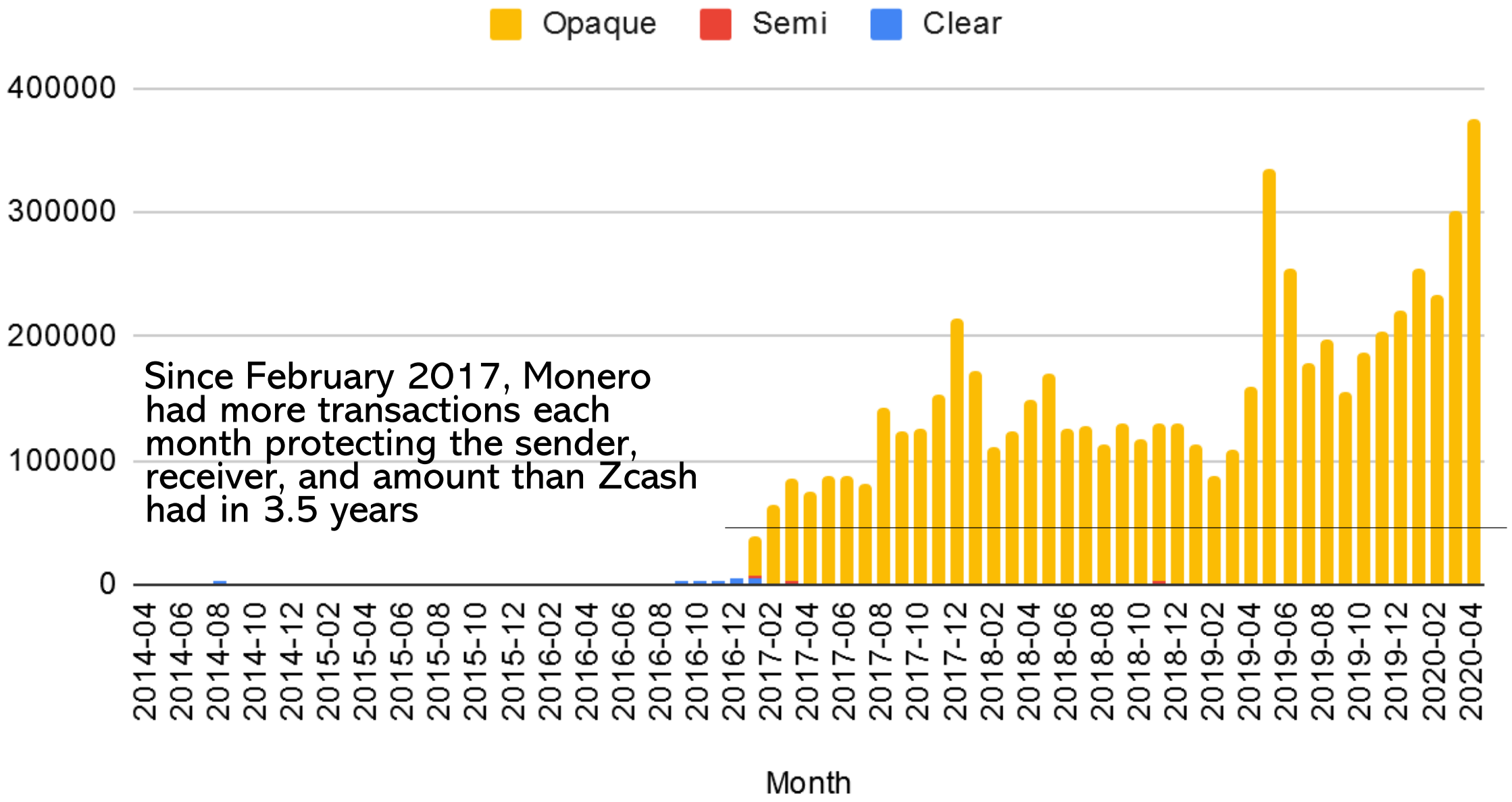
Source: https://forum.zcashcommunity.com/t/measuring-shielded-adoption/35022

Cumulative transactions w/o deducible ring and hidden amount

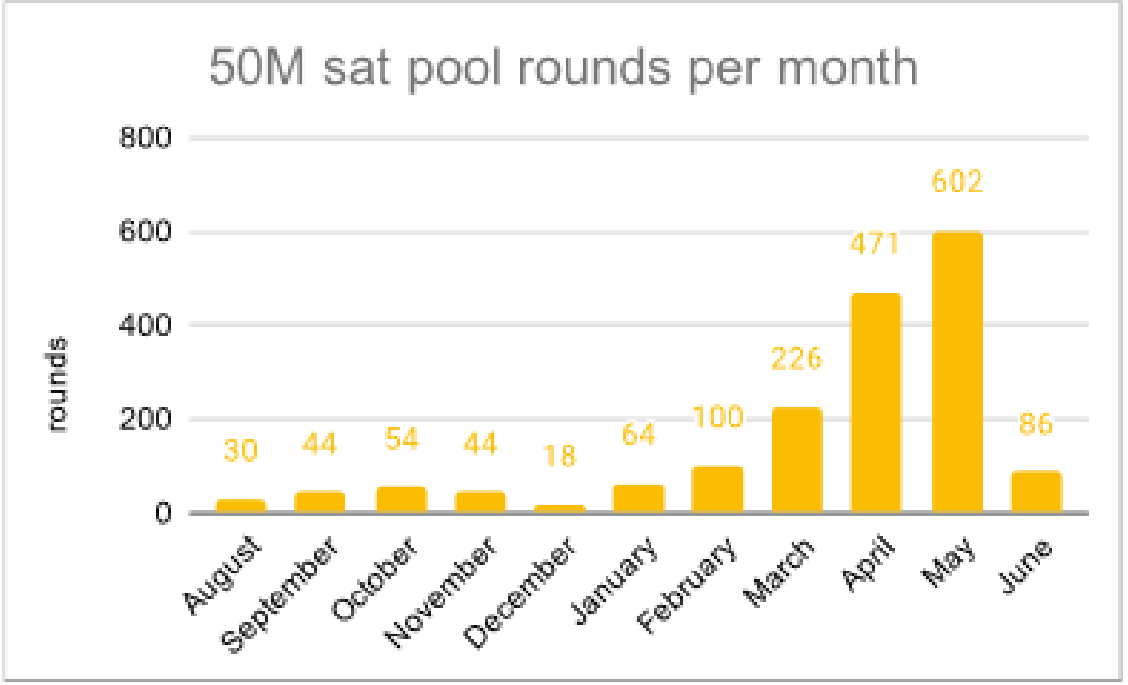


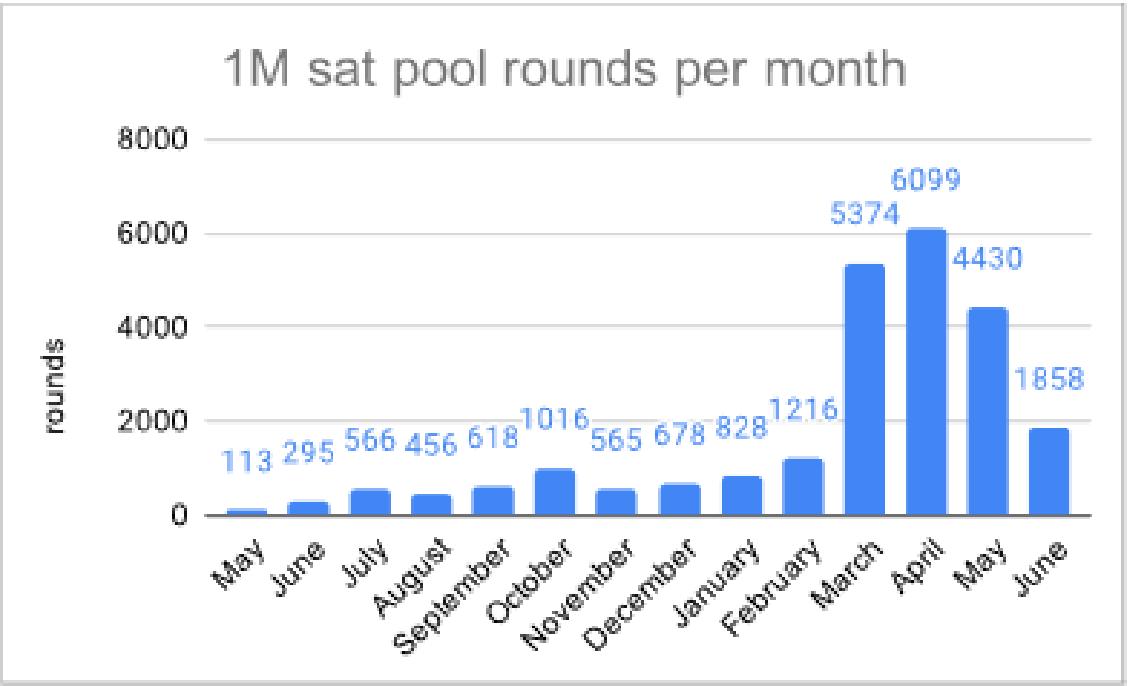
Source: blockchain data from Sarang Noether of Monero Research Lab

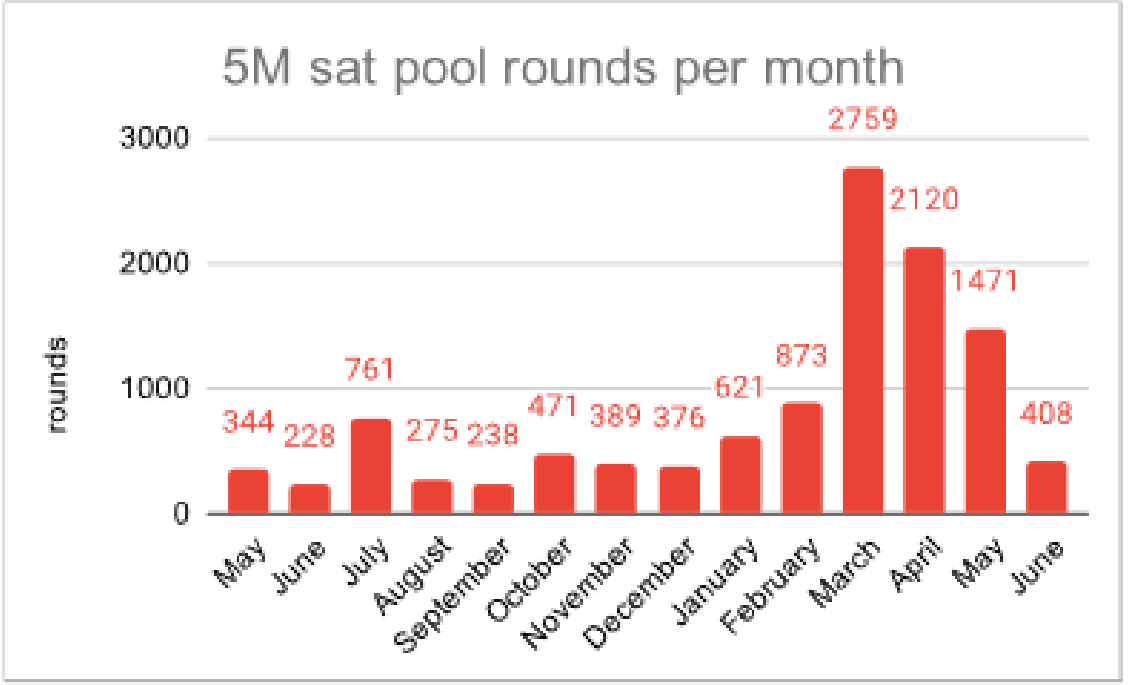
Transactions w/o deducible ring

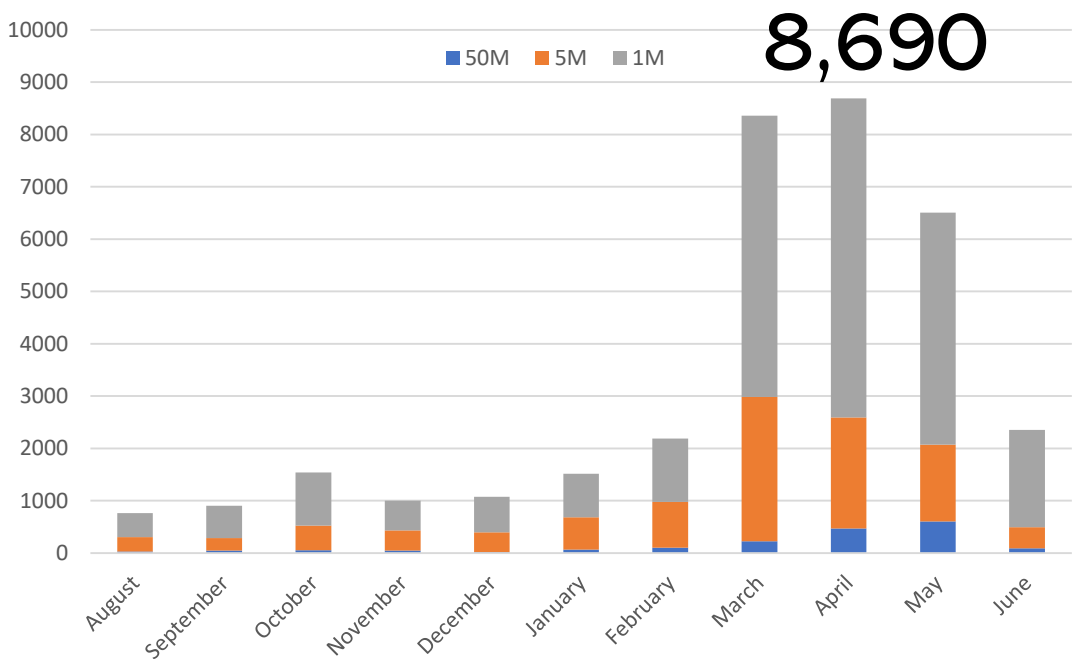


Source: blockchain data from Sarang Noether of Monero Research Lab









Source: https://mattodell.keybase.pub/whirlpoolstats.pdf

What's next?

Today

<6 months

~12-18 months

Image credit
Edge Wallet

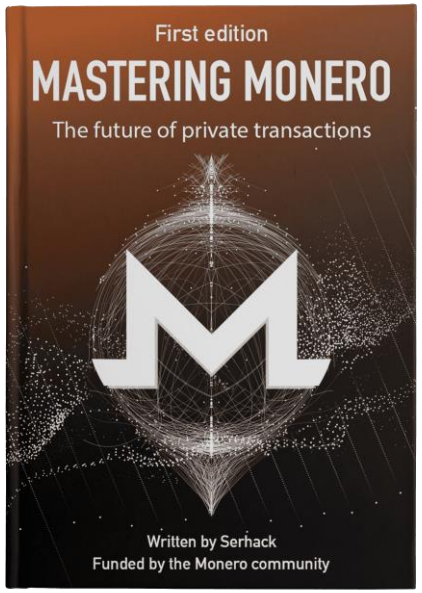
CLSAG

More efficient transactions

Arcturus, Triptych

Larger ringsizes 128-256

How YOU should participate



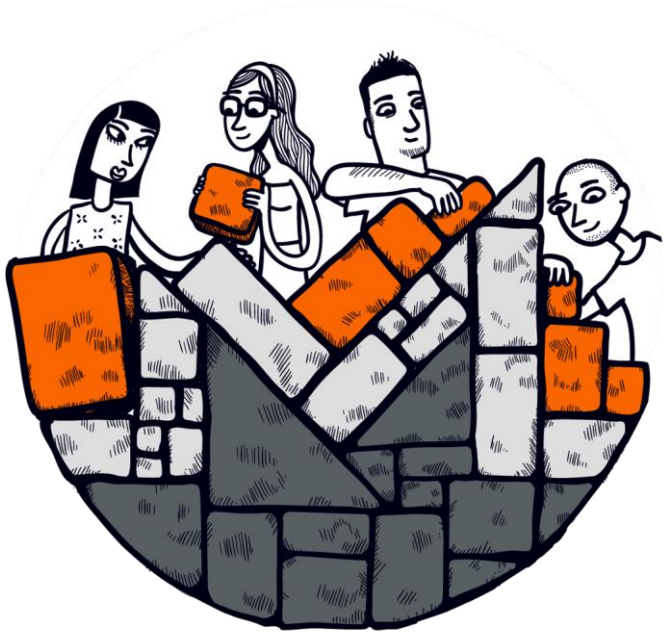
Get educated

masteringmonero.com

moneromeans.money

Get started

cakewallet.com



Join the community

communityworkgroup.org

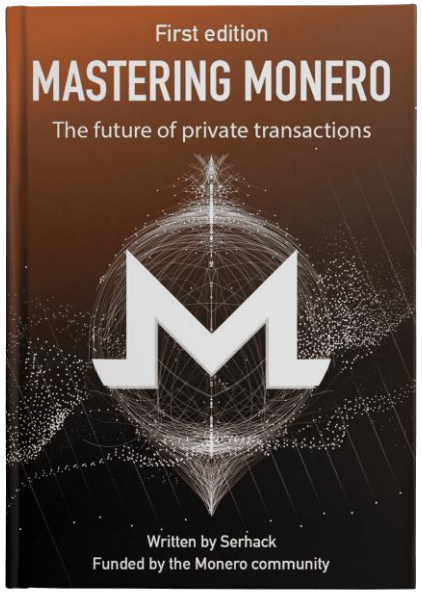
Cake Wallet sponsored this meetup. Mastering Monero provided 3 free books for a giveaway.

Conclusion

- Monero transactions use ring signatures and stealth addresses
- Monero beginners have reasonably strong privacy by default
- Privacy needs to be thought of on a network implementation basis, not on a single-user basis
- Monero is the only network that seems to care about real privacy
- Monero is the only network that prevents mass surveillance
- Watch for more efficient transactions soon, and much larger ringsizes in the medium-term future

Questions?

justin@ehrenhofer.org
@JEhrenhofer



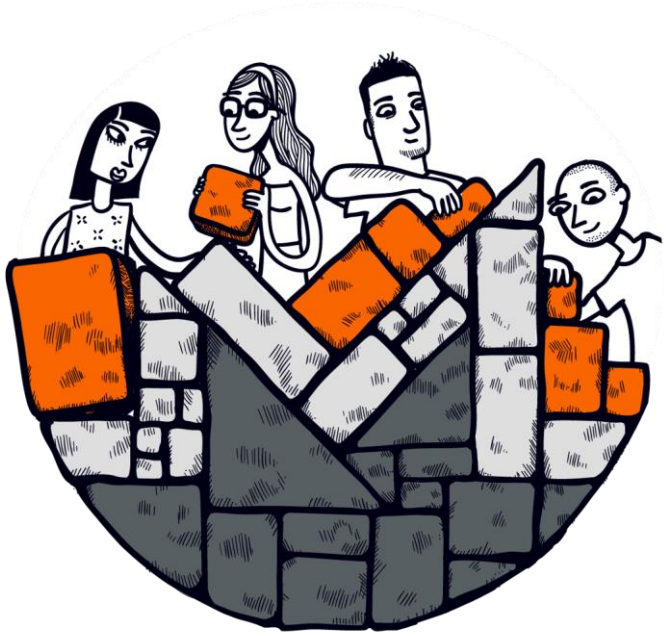
Get educated

masteringmonero.com

moneromeans.money

Get started

cakewallet.com



Join the community

communityworkgroup.org