



Introduction to Monero

And a lesson in privacy and coin equality

Justin Ehrenhofer

Organizer, Monero Community Workgroup

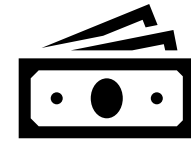
Compliance Analyst, DV Chain



a community-
driven,



open source
project that



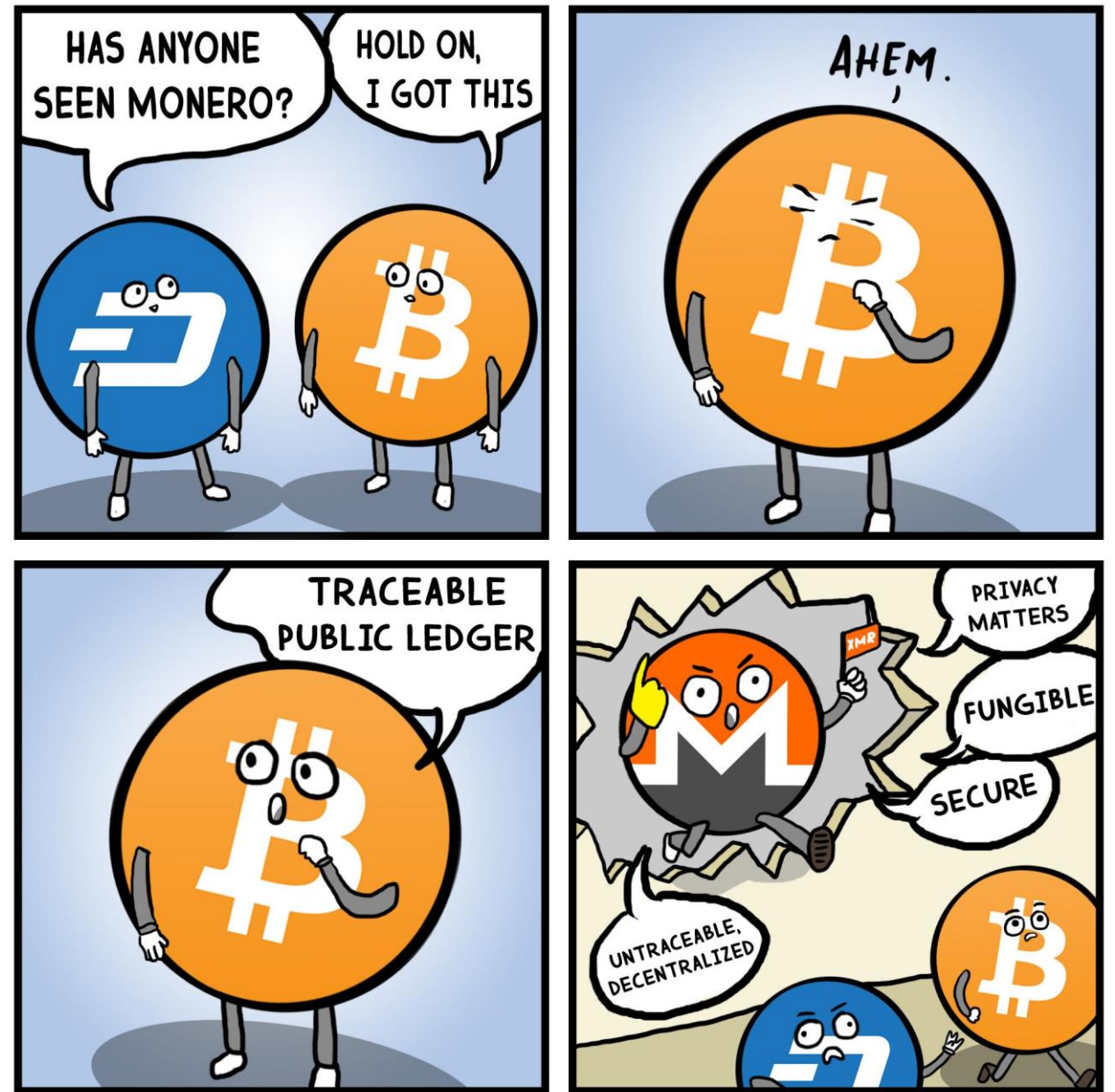
makes safe
digital cash



and owns up
to its
shortcomings

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

(We can't help it)



Real Problems Monero Addresses



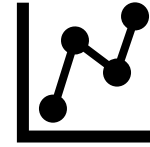
Strong,
ubiquitous
privacy



Coin equality
(fungibility)



Accessible
PoW mining
(**RandomX**)



Adaptive
block size and
fees

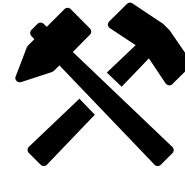
Real Problems Monero Addresses



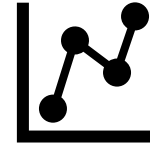
Strong,
ubiquitous
privacy



Coin equality
(fungibility)



Accessible
PoW mining
(**RandomX**)

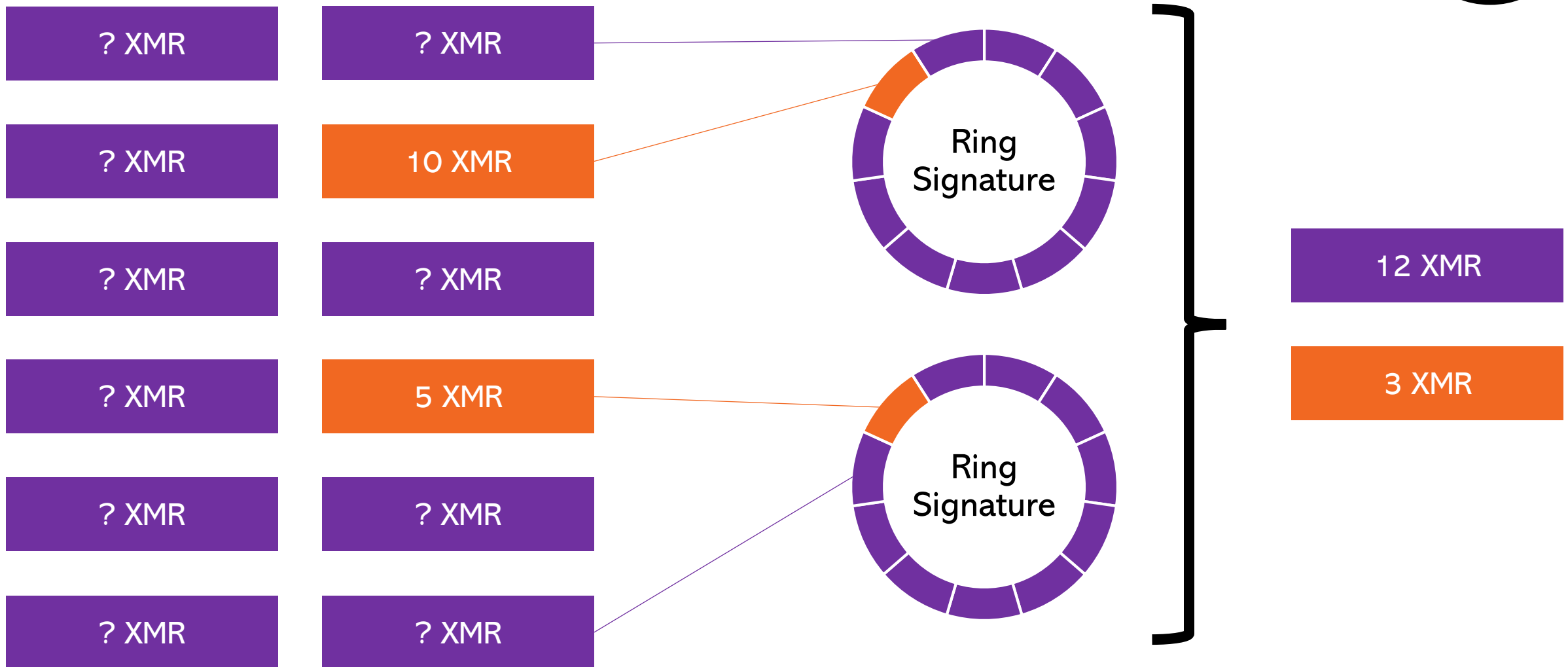


Adaptive
block size and
fees

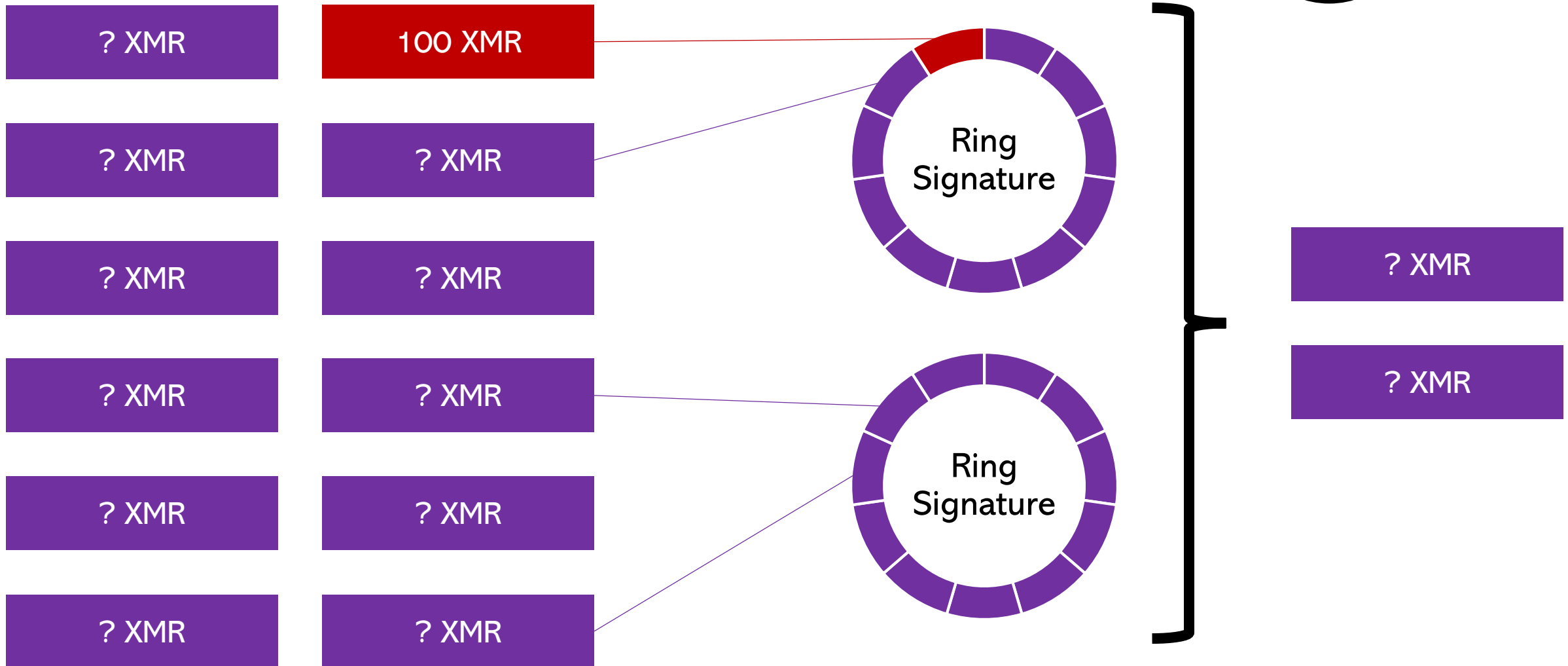
Cryptocurrency network privacy is less than the sum of its parts

	Monero		Zcash		Grin		Bitcoin	
	Novice	Expert	Novice	Expert	Novice	Expert	Novice	Expert
Amount	Green		Red	Green	Green		Red	Orange
Sender	Green		Red	Green	Orange	Yellow	Red	Yellow
Receiver	Green		Red	Green	Orange	Yellow	Red	Yellow
Tainted Coin and/or Suspicious Risk	Green		Red	Red	Yellow	Yellow	Red	Red

Transaction Structure and Tracing

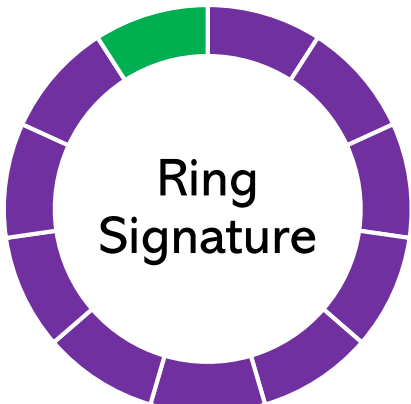
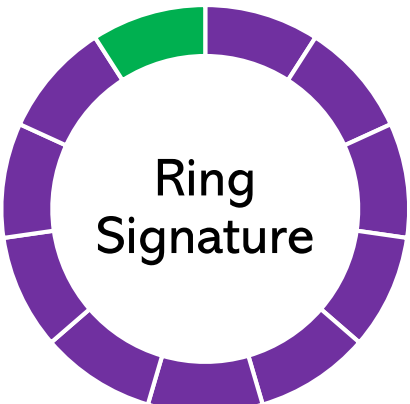
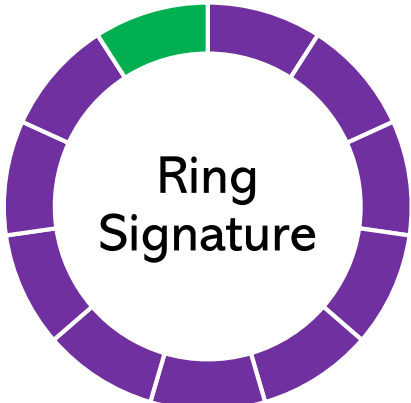
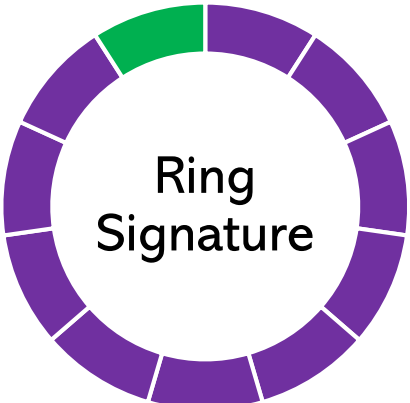
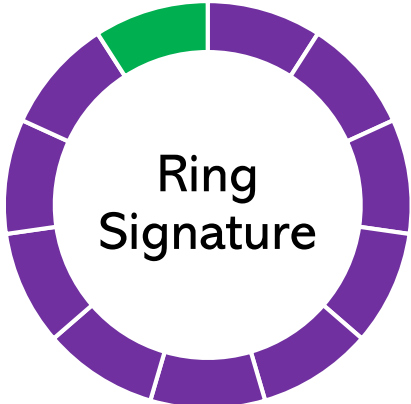
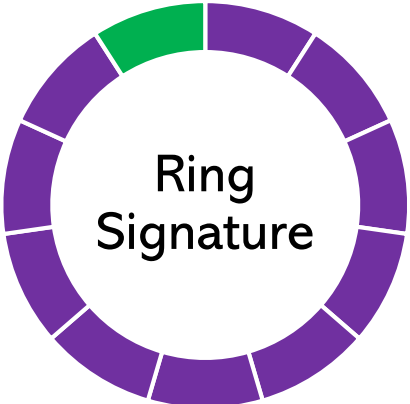


Transaction Structure and Tracing



Transaction Tracing

? XMR	? XMR
? XMR	? XMR
? XMR	? XMR
? XMR	? XMR
? XMR	? XMR
? XMR	? XMR



+

Monero has

REAL privacy, not
POTENTIAL privacy

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

Motivation

- **Keep Monero users safe**
- Inform best practices for users
- Inform best practices for software creators
- Design protocol that enforces best practices...
- ... by identifying and preventing anomalous behaviors



Community Crowdfunding Vulnerability

Get Started -

Downloads

Recent News -

Advisory note for users making use of subaddresses

Posted by: Justin Ehrenhofer / knaccc

October 18, 2019

Dear participants of the Monero ecosystem,

After some new limitations of subaddresses were found, this post should help clarify the use-cases of subaddresses and the privacy protections that they provide. Monero added subaddresses to its software to allow simpler OpSec management. For many users, subaddresses are a more elegant way to receive transactions than integrated addresses or main addresses. However, subaddresses are not as robust as using entirely different seeds for each desired disparate identity.

In summary, the below chart should help explain the relative privacy protections of different address behaviors. From a user experience perspective, subaddresses are far more user-friendly than using addresses from completely different seeds, while still providing a level of privacy protection that is sufficient for most use-cases.

MoneroKon 2019 - Visualizing Monero: A Figure is Worth a Thousand Logs

950 views • Jun 27, 2019

18 0 SHARE SAVE ...



Monero Community Workgroup
1.83K subscribers

SUBSCRIBE

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?

Name to Alice

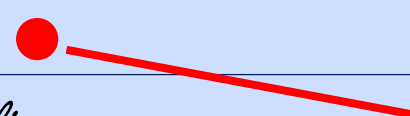
Alice to Bob ●

Bob to Charlie

Reality

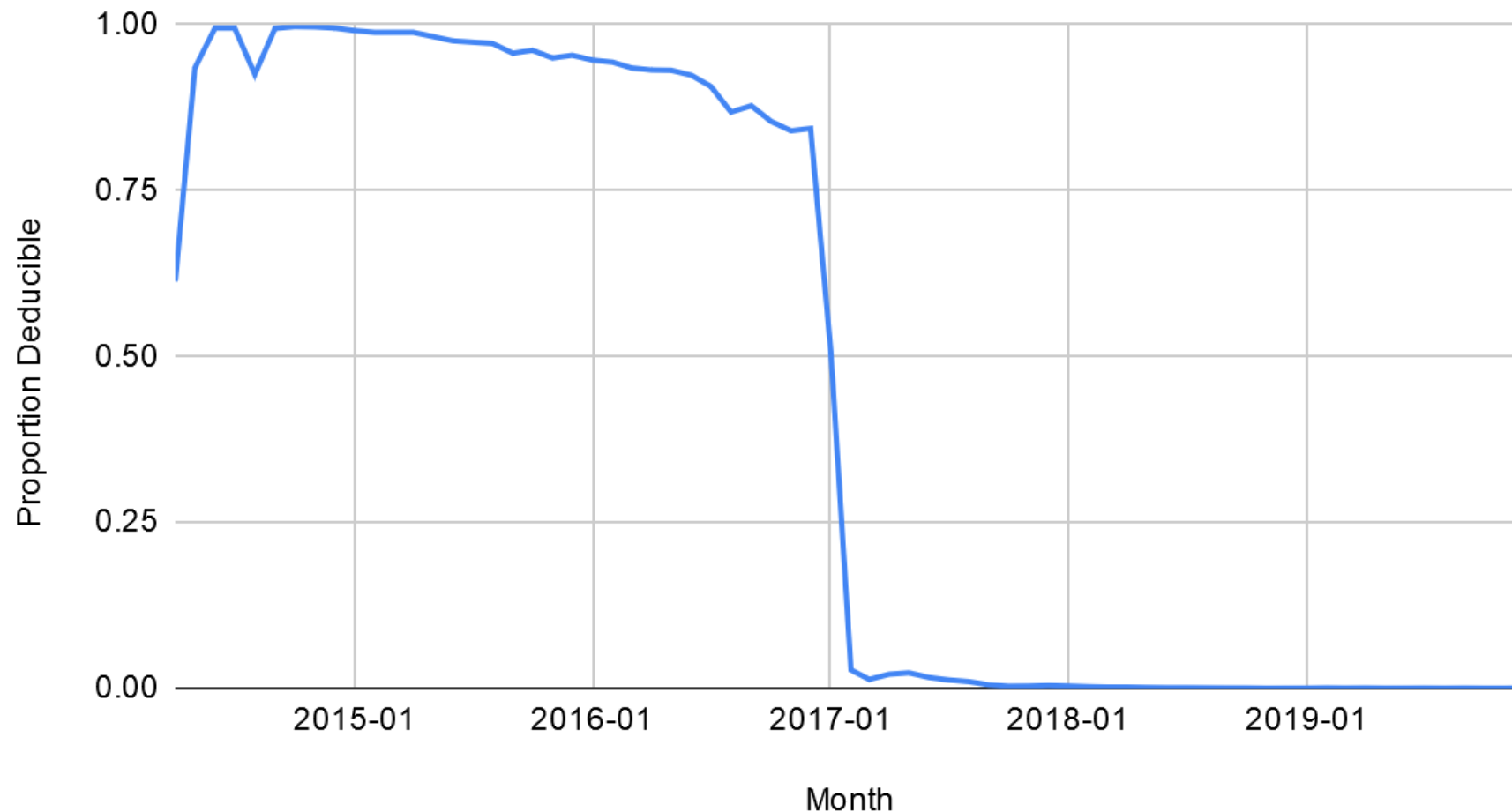
- Chain analysis companies will most likely mark the use of any optional privacy as higher risk (this is enforced by several tools)
- Mandatory mining to shielded doesn't fix
- Optional privacy often **harms** fungibility, not helps

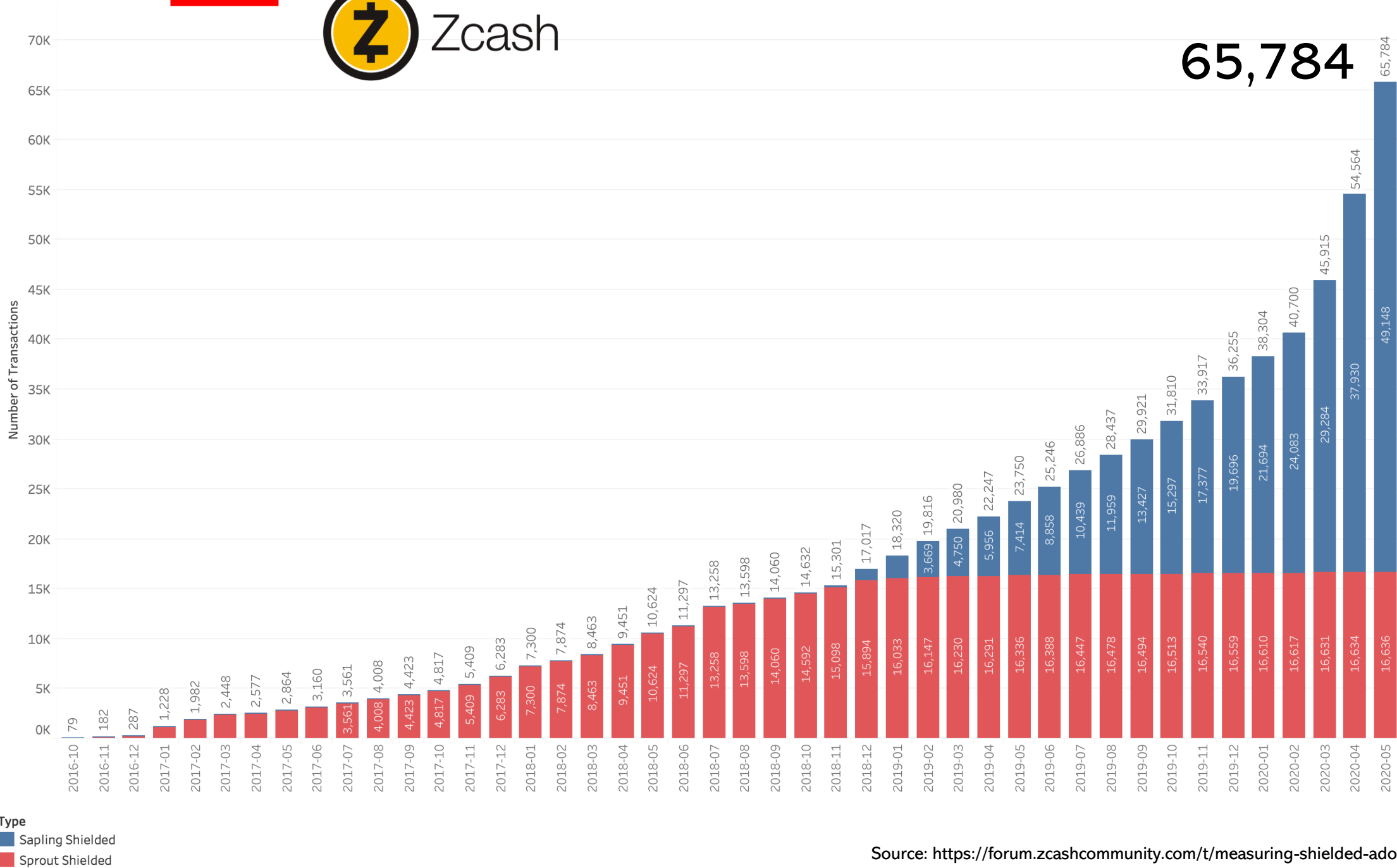
<i>Name to Alice</i>	<i>Mixers</i>
<i>Alice to Bob</i> ●	<i>Z-addresses</i>
<i>Bob to Charlie</i>	<i>PrivateSend</i>
	<i>Wasabi</i>
	<i>Samourai</i>



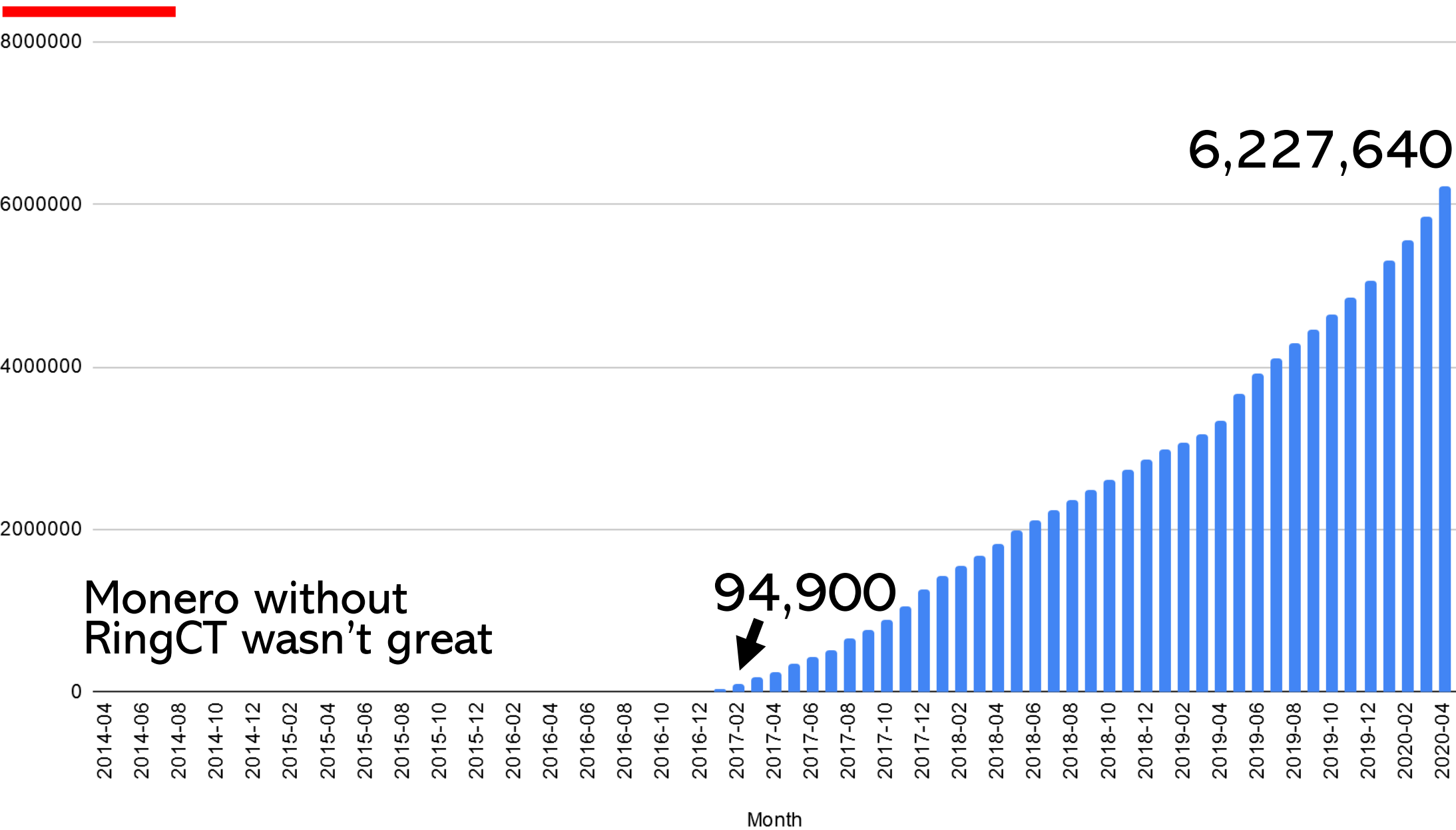
Privacy is hard. Coin equality is harder.

Proportion of transactions w/ 1+ deducible ring over time

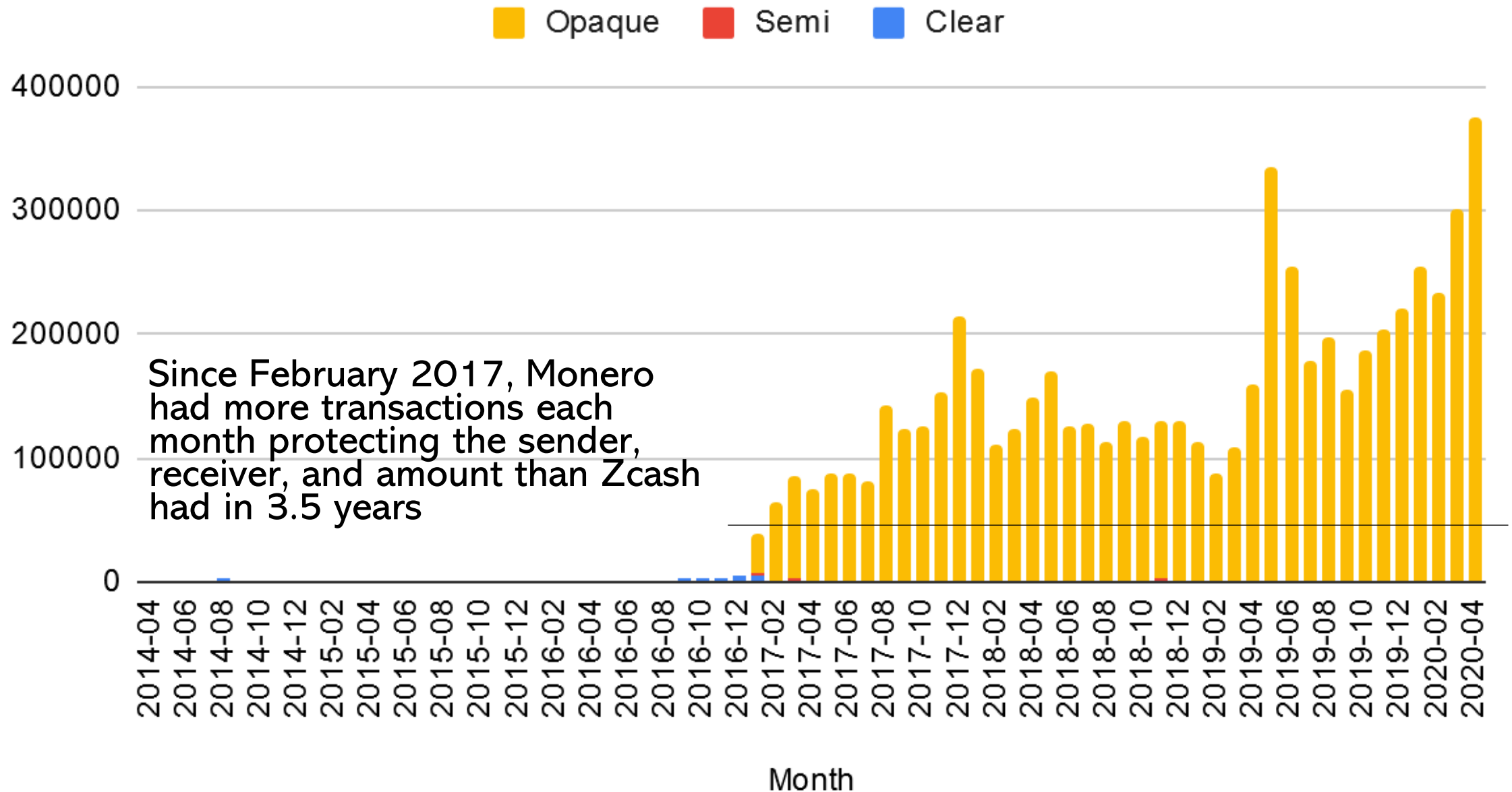




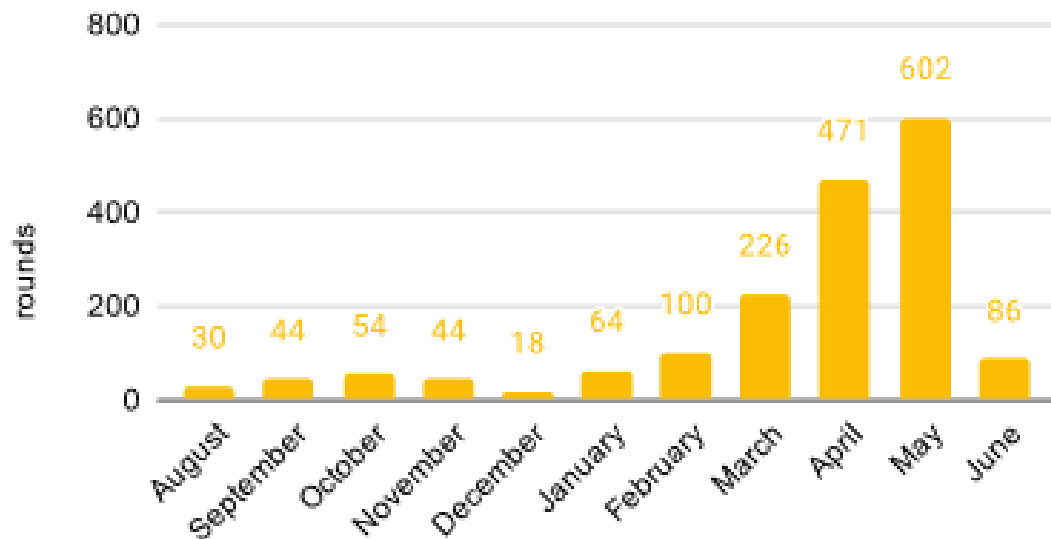
Cumulative transactions w/o deducible ring and hidden amount



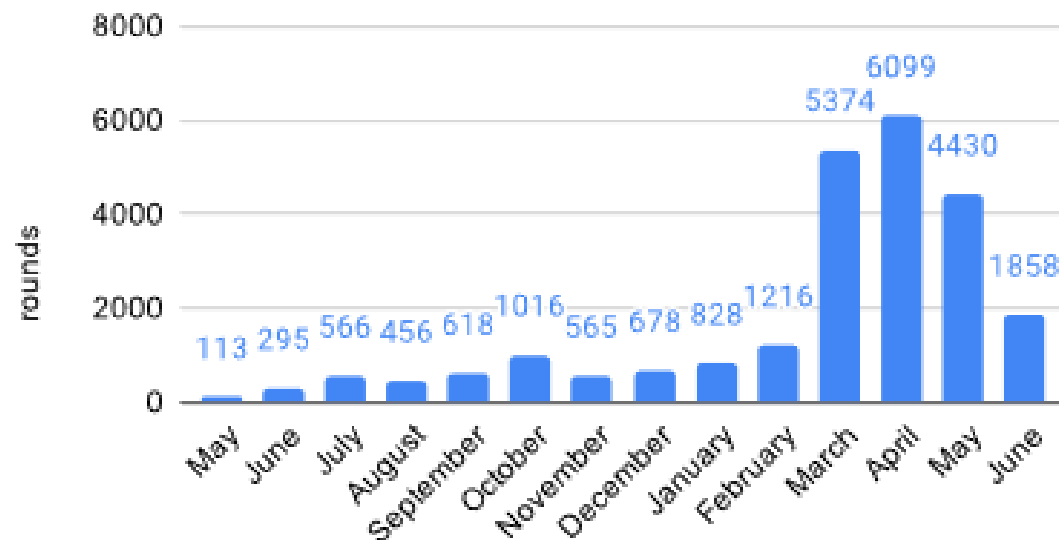
Transactions w/o deducible ring



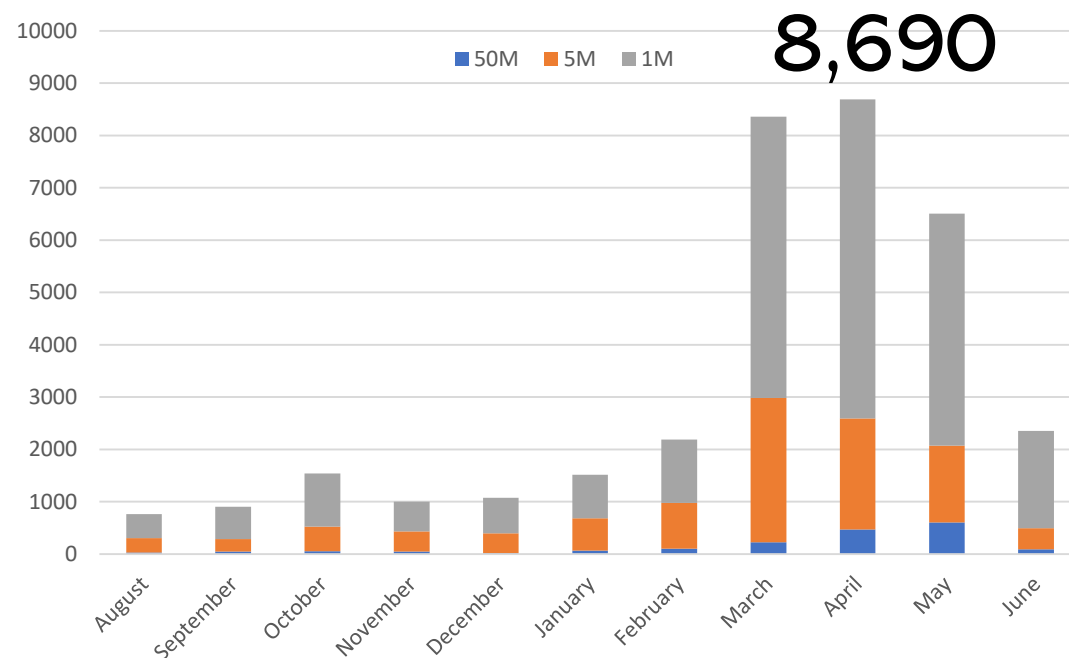
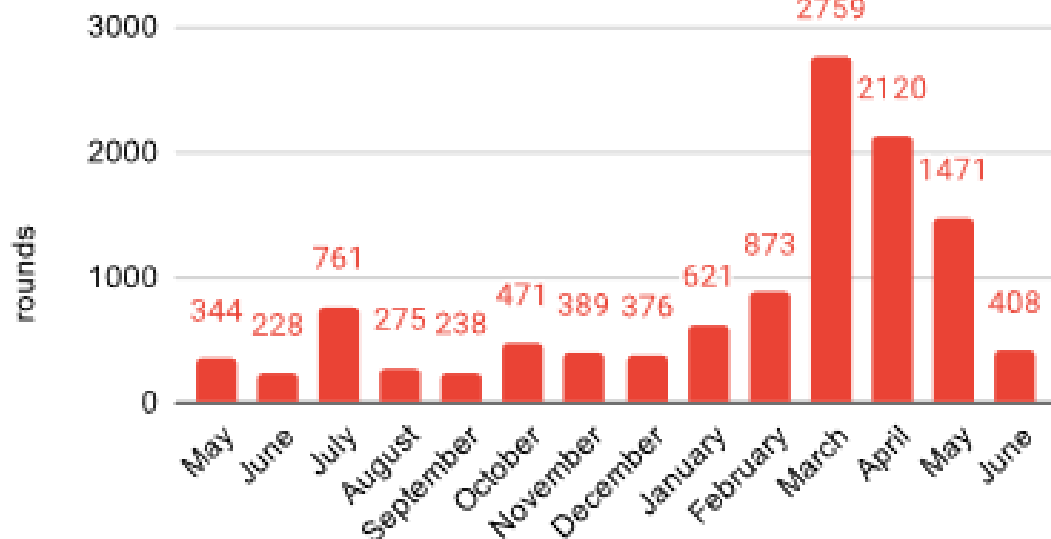
50M sat pool rounds per month



1M sat pool rounds per month



5M sat pool rounds per month

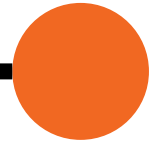
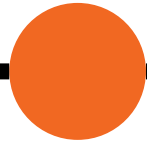
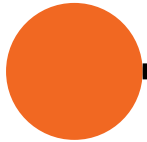


What's next?

Today

<6 months

~12-18 months



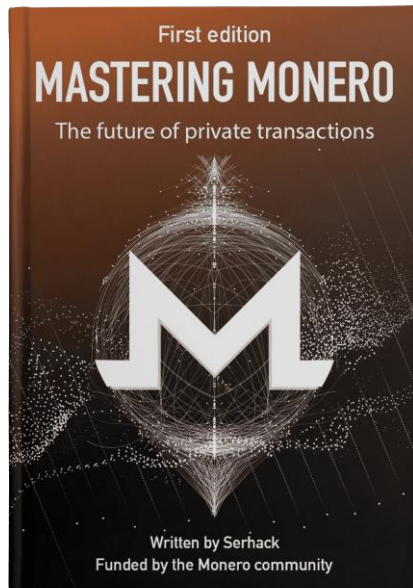
CLSAG

More efficient
transactions

Arcturus, Triptych

Larger ringsizes
128-256

How YOU should participate



Get educated

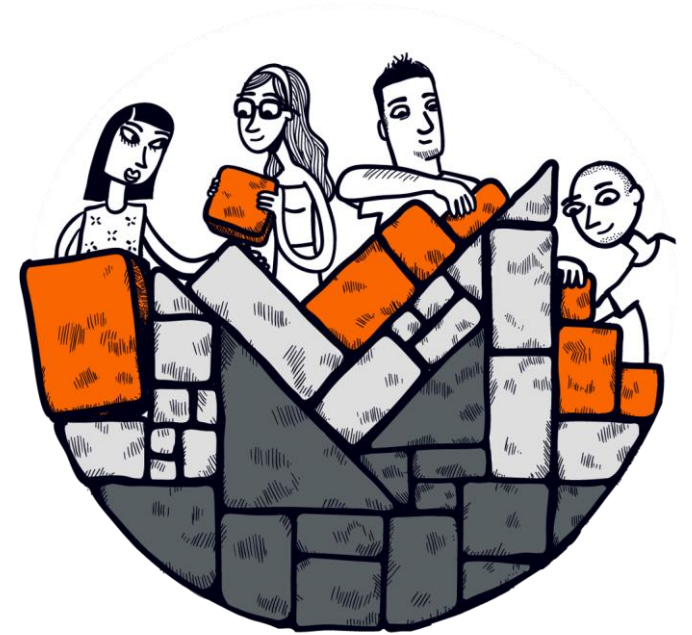
masteringmonero.com

moneromeans.money



Get started

cakewallet.com



Join the community

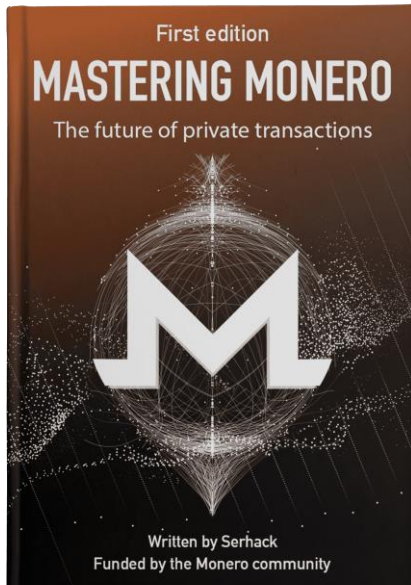
communityworkgroup.org

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

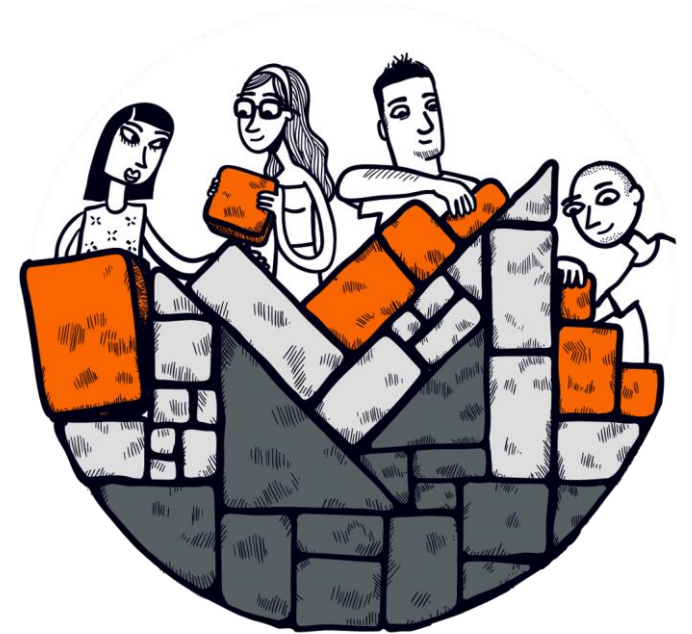
masteringmonero.com

moneromeans.money



Get started

cakewallet.com



Join the community

communityworkgroup.org