

Privacy Adoption: The **Collision** of Theory and Practice



Justin Ehrenhofer
Organizer, Monero Space

This isn't another talk in support of privacy.

It's about why projects need to take responsibility for privacy tech being adopted.

Agenda

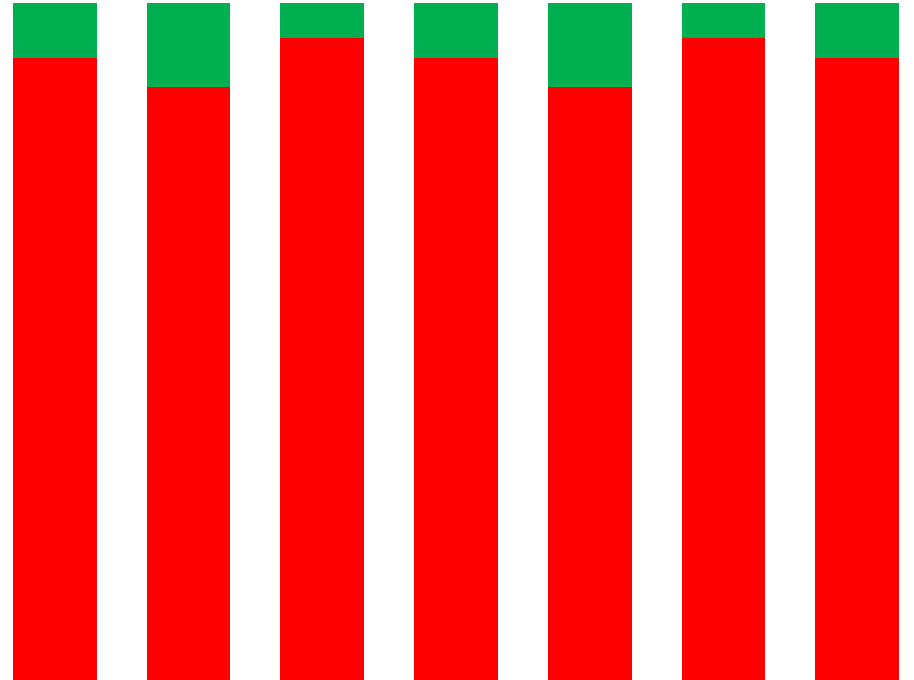
- Privacy theory vs practice
- Privacy vs coin equality (fungibility)
- Defense in numbers
- Results speak for themselves
- Hard truths
- Conclusion

Cool



Buy the blue sticker at Cypher Market
\$0.50 from each purchase to MRL

Not Cool



Theory or Practice?

Example - A perfectly private donation

On the other hand, here is an example of somebody using bitcoin to make a donation that is completely anonymous.

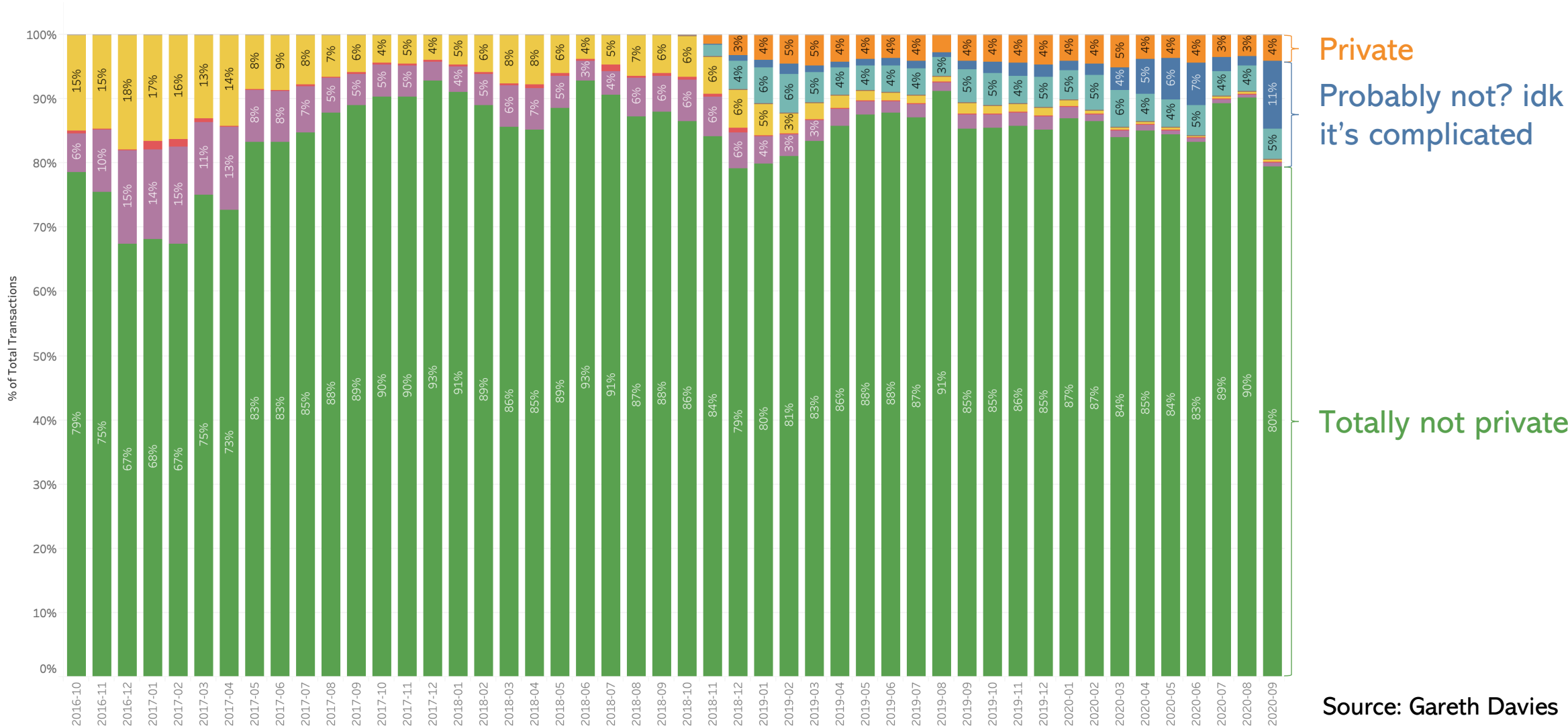
1. The aim is to donate to some organization that accepts bitcoin.
2. You run a Bitcoin Core wallet entirely through Tor.
3. Download some extra few hundred gigabytes of data over Tor so that the total download bandwidth isn't exactly blockchain-sized.
4. Solo-mine a block, and have the newly-mined coins sent to your wallet.
5. Send the entire balance to a donation address of that organization.
6. Finally you destroy the computer hardware used.

Theory or Practice?

- Any user who cares about privacy can:
 - Send a special private transaction
 - Download a special wallet
 - Spend more in fees
 - Wait longer
 - Remember to mix their change outputs
 - Build from source
 - Handle their own timing and denominations
 - Watch 100 hours of privacy videos

Theory or Practice?

Zcash Transaction % By Type



Privacy

Something that
allows users to hide

Effectiveness and
implementation of
privacy matters



Coin Equality (Fungibility)

Transaction and
output
indistinguishability

Implementation of
privacy matters
more

Privacy Requirements

- Tx graph
- Timing
- Networking
- Metadata
- Amount
- Other user behavior
- (etc)



Coin Equality (Fungibility) Requirements

- Good enough privacy
- Implemented everywhere

Results of a Coin Equality Exercise

Name to Alice

Alice to Bob ●

Bob to Charlie

Results of a Coin Equality 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 analysis software?

Name to Alice

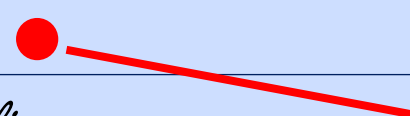
Alice to Bob ●

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> |
| | |
| | |



Defense in Numbers

Option 1

Thousands of people
who have basic
privacy protections
without caring too
much

Option 2

A handful of experts
who meticulously
seek ideal privacy

Defense in Numbers

Monero Way

Everyone has basic
protections; exact
protections are good
not perfect

Opt-In Way

Only 1% of people
have any privacy
protections at all

Defense in Numbers

Monero Users

- Privacy Fanatics
- Researchers
- Crypto nerds
- Speculators
- Miners
- Everyday users

Opt-In Users

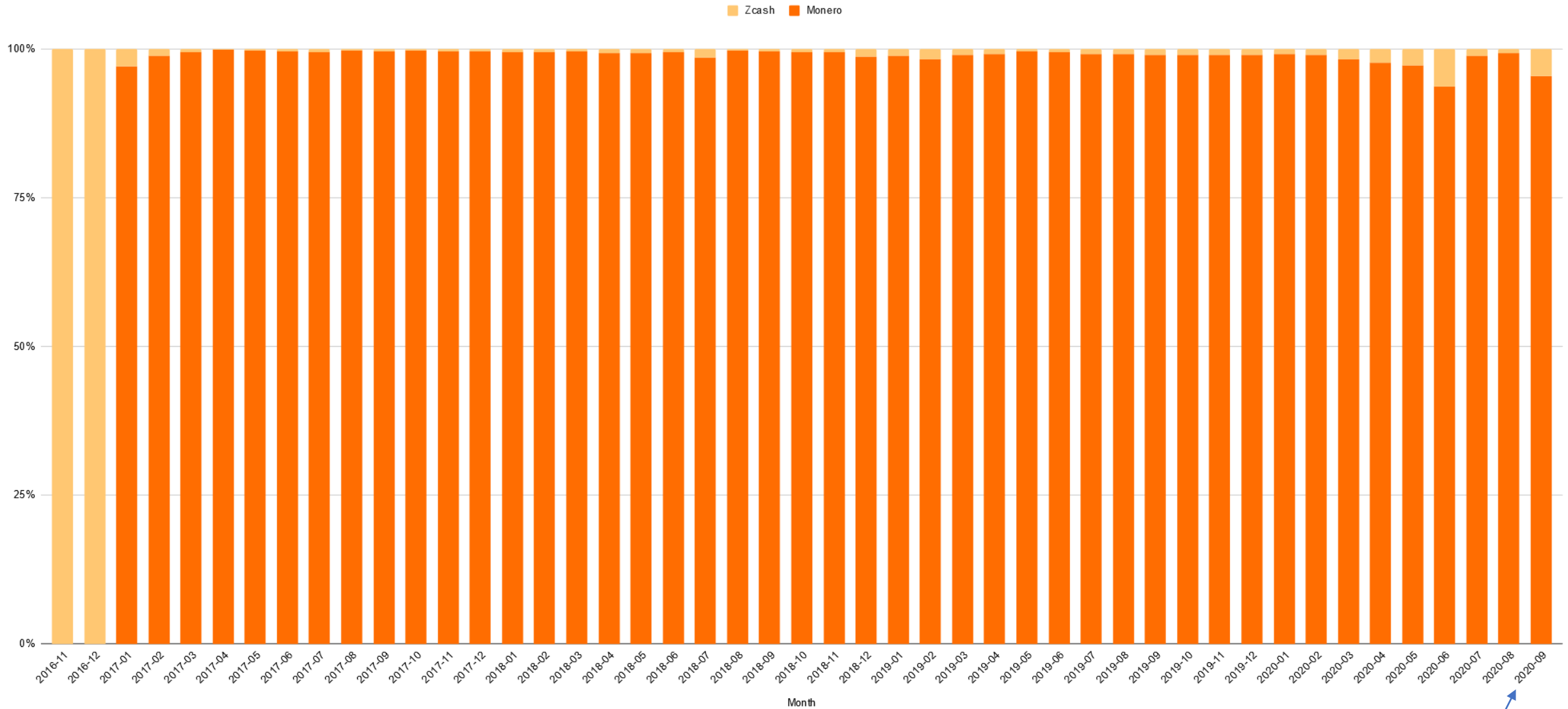
- Privacy Fanatics
- Researchers

Results of Defense in Numbers:

Monero provides **more
privacy to more users**
than any other
cryptocurrency project.

This benefits everyone, especially
those who need privacy the most
since **they need a crowd to hide in**

Comparative # of Transactions Hiding Sender, Receiver, Amount (XMR, ZEC)

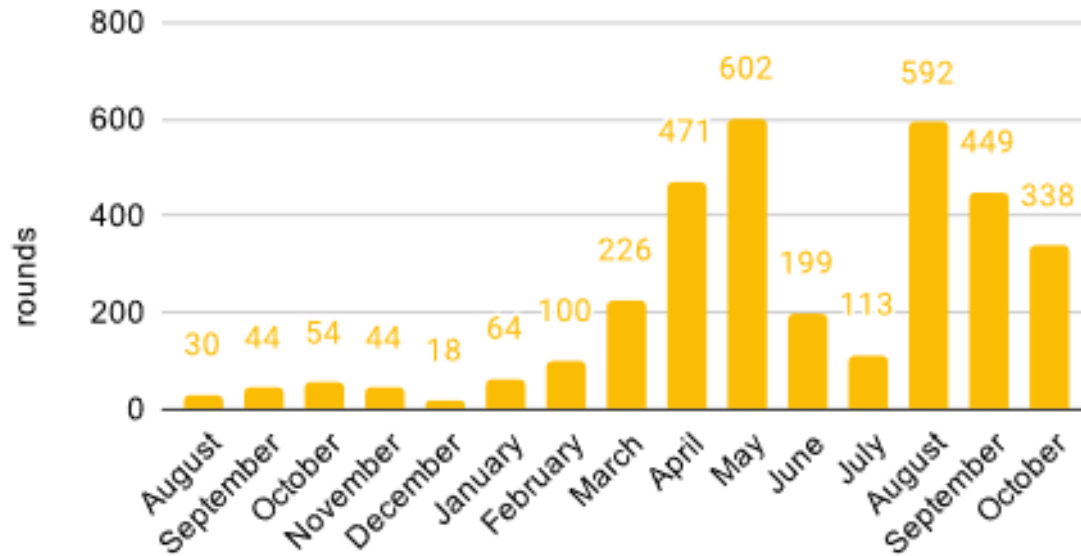


Sources: Sarang Noether, Ph.D.; CoinMetrics; Gareth Davies

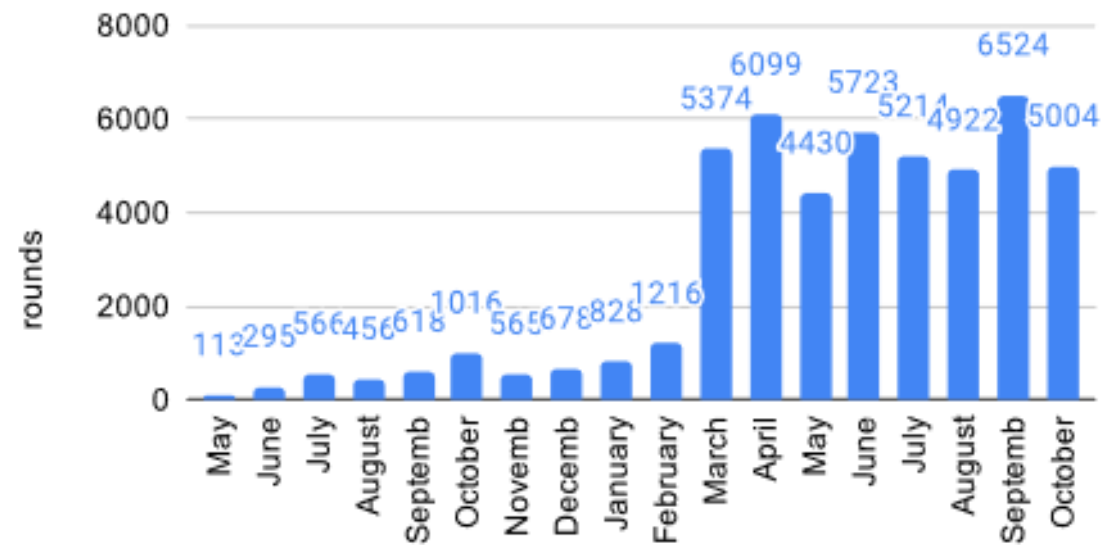
Monero has **20x** the number of tx that hide basic info

Reader beware: No direct comparison between the # of Samurai mixing rounds and the # of Monero transactions

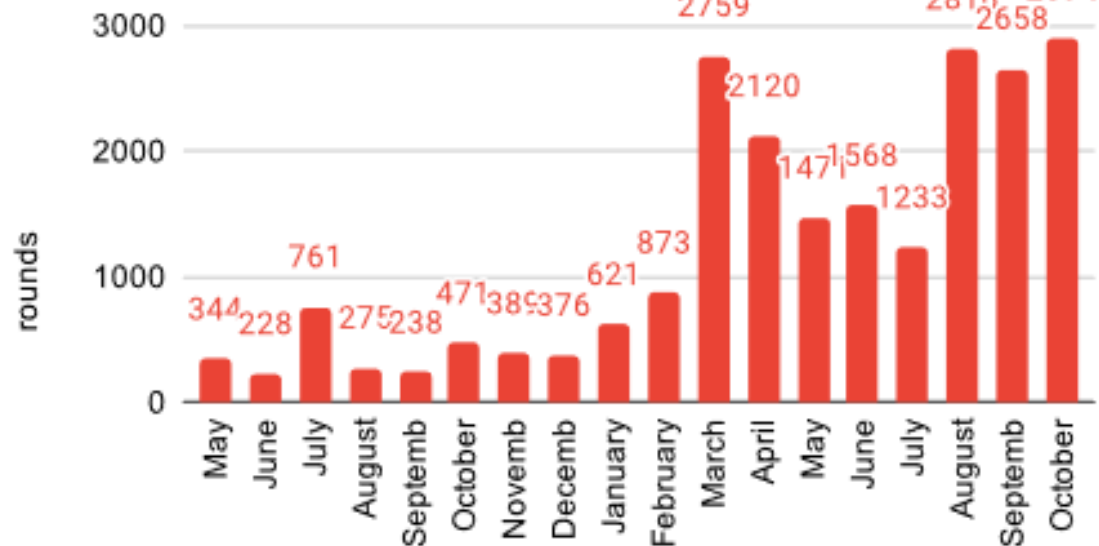
50M sat pool rounds per month



1M sat pool rounds per month



5M sat pool rounds per month



Maximum: **9,631** rounds per month

Monero had 450,000 transactions protected with ring signatures in October, or **>45x Samurai's best**

Again, these #s are not directly comparable (rings vs. outputs?)

Changing of Priorities

- Focus on improving the base-level privacy achieved; focus less on the maximum potential privacy someone can have
- Think: “how can someone fuck this up?” Start with the obvious.
- Privacy will come to those who need it from the larger pool of users engaging with privacy functionality
- Power users gain more flexibility and volume to play with for greater privacy results
- Far more users get the basic privacy protections they need
- This gives us the “easy” win of coin equality (fungibility) first

Hard Truths: Transparent Amounts = Bad

- It's effectively impossible to build a fungible and private asset where the base asset has transparent amounts.
- Amount transacted is a critical piece of metadata that's effectively impossible to work around

Example for Zcash: “Just the Tip” Pool Use
Actually: Quesnelle Analysis



Hard Truths: Users Are Humans

- Your implementation needs to honor that users are not experts
- Don't blame users for not getting it
- Basic privacy protections should be achievable by newcomers, not only reserved for enthusiasts
- We can't dismiss education entirely (since advanced users will always need it for the bleeding edge of attacks), but it's not the solution for >99% of people

Theory and
implementation
are identical...
in theory

Hard Truths: Can't Protect Against It All

- Not every threat model is solvable
- There will always be limitations as attackers get stronger over time
- Don't ignore the broader threats in pursuit of the niche ones
- Design and build against risks that are most likely to affect the most people (build protections up from the bottom)
- Clearly communicate this strategy and the known limitations

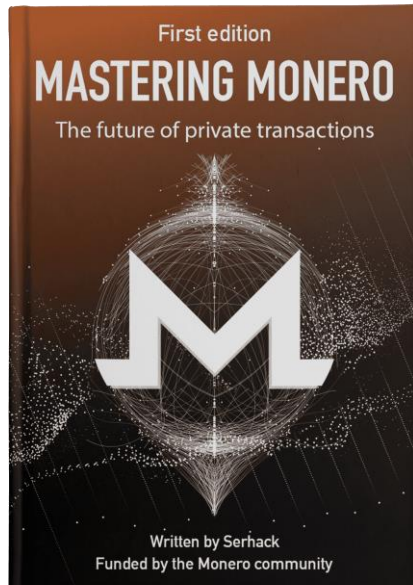


Conclusion

- Monero offers far more privacy than any other cryptocurrency project by focusing on implementation
- Monero focuses on the goals of coin equality (fungibility) and privacy for the masses
- Privacy is a never-ending battle; those who take responsibility for delivering privacy will be best-prepared to win this battle
- Privacy is all about accommodating for user behavior, not making an isolated experiment in a lab

Questions?

justin@monero.space
@JEhrenhofer



Get educated

masteringmonero.com
moneromeans.money



Get started

cakewallet.com
getmonero.org



Join the community

monero.space
communityworkgroup.org

Acknowledgements

- Sarang Noether, Ph.D. for their similar MCCVR 2020 talk
- CypherMarket (MRL sticker design)
- The Monero Project getmonero.org
- MrMonOcle (CLSAG logo)
- CoinMetrics
- Gareth Davies