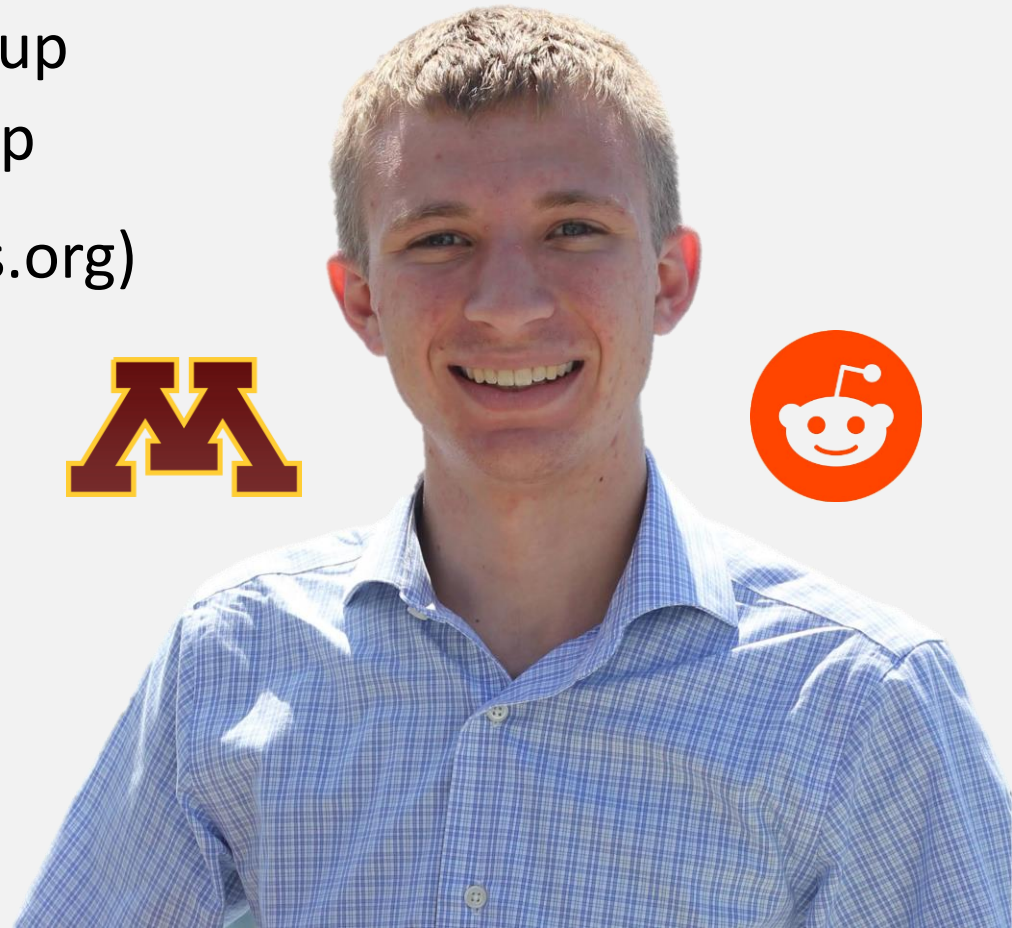

Privacy and Monero
MONERO

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 with 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

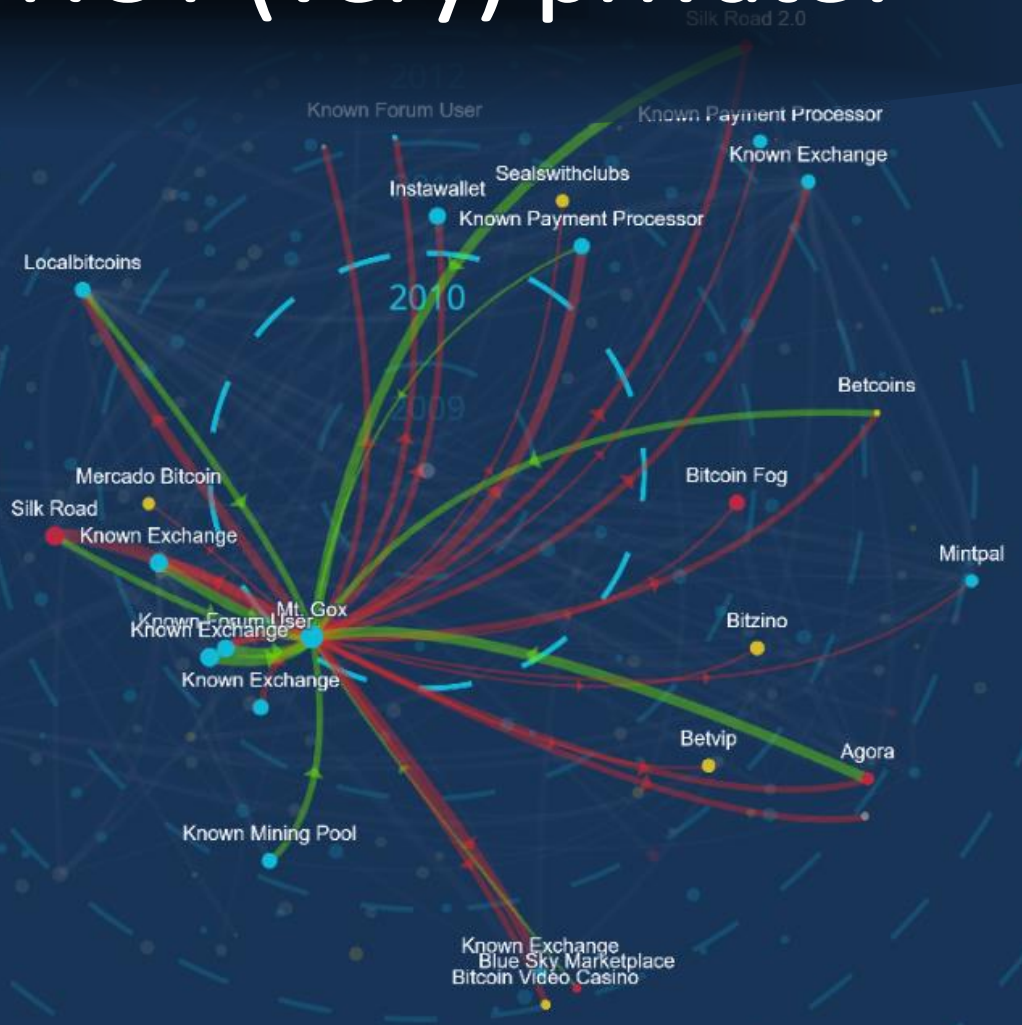
Privacy isn’t a thing that you achieve, it’s a constant cat-and-mouse battle.

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

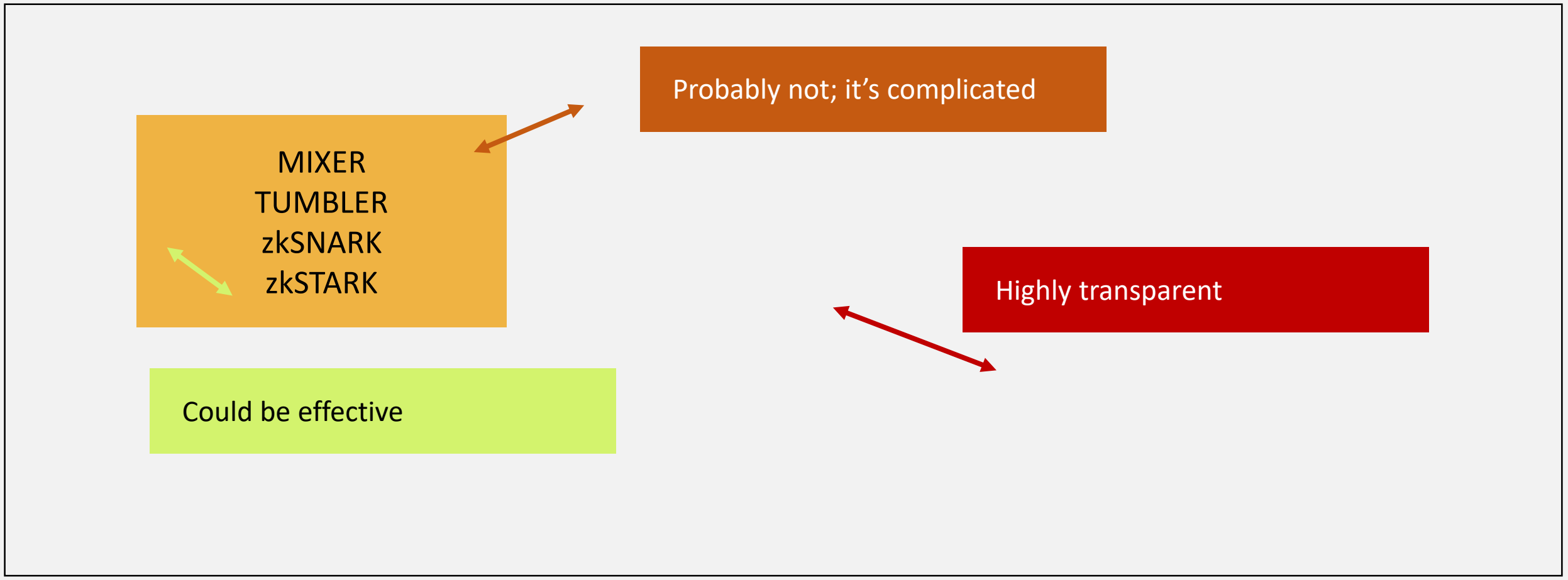
Expenses

- 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

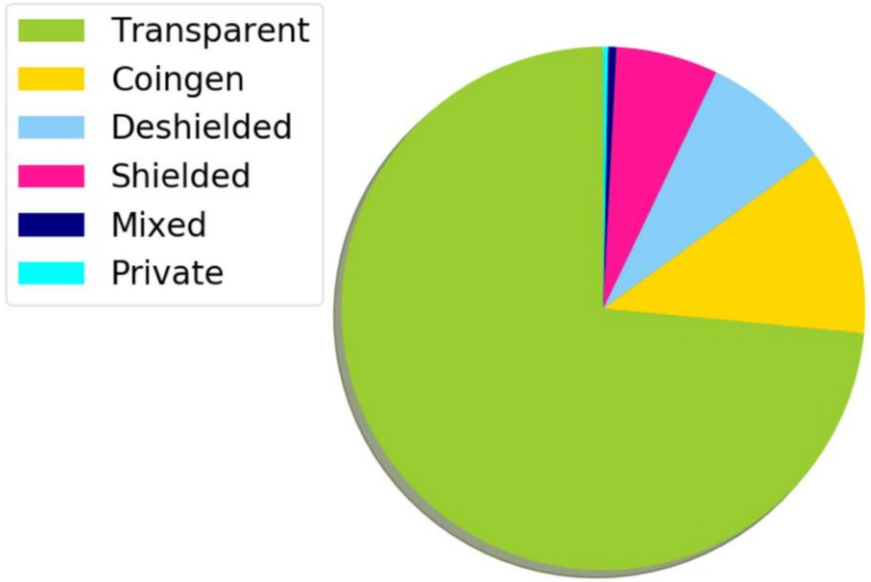
Tools Can Be Added to Transparent Systems. Their Effectiveness is Complicated



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

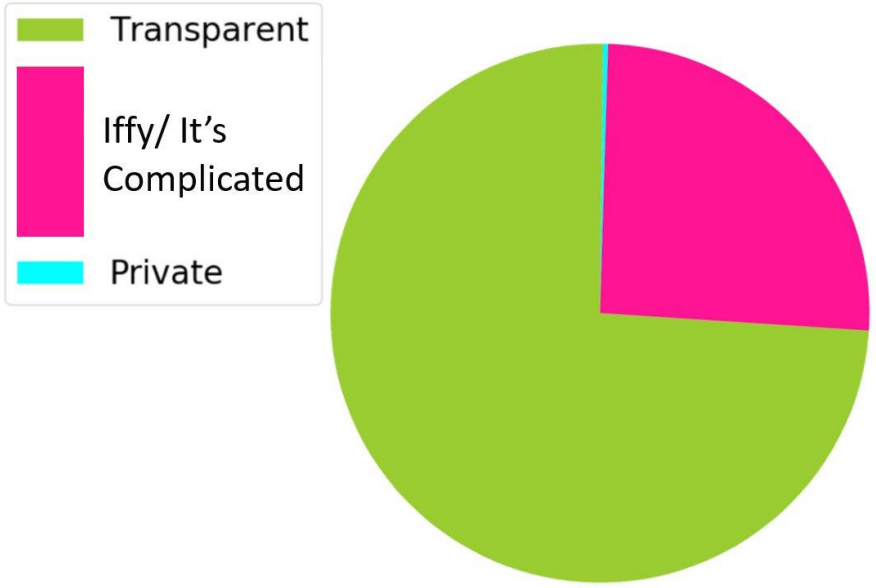
UCL

Interactions in Zcash

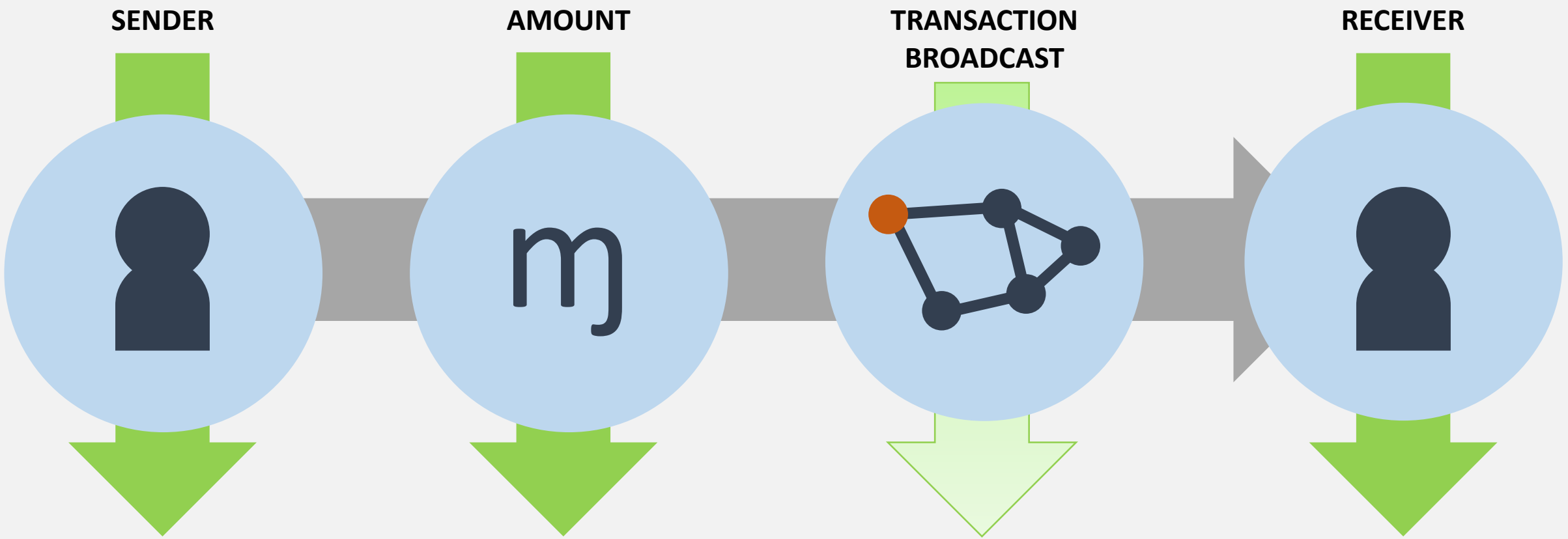


UCL

Interactions in Zcash



The Monero Difference

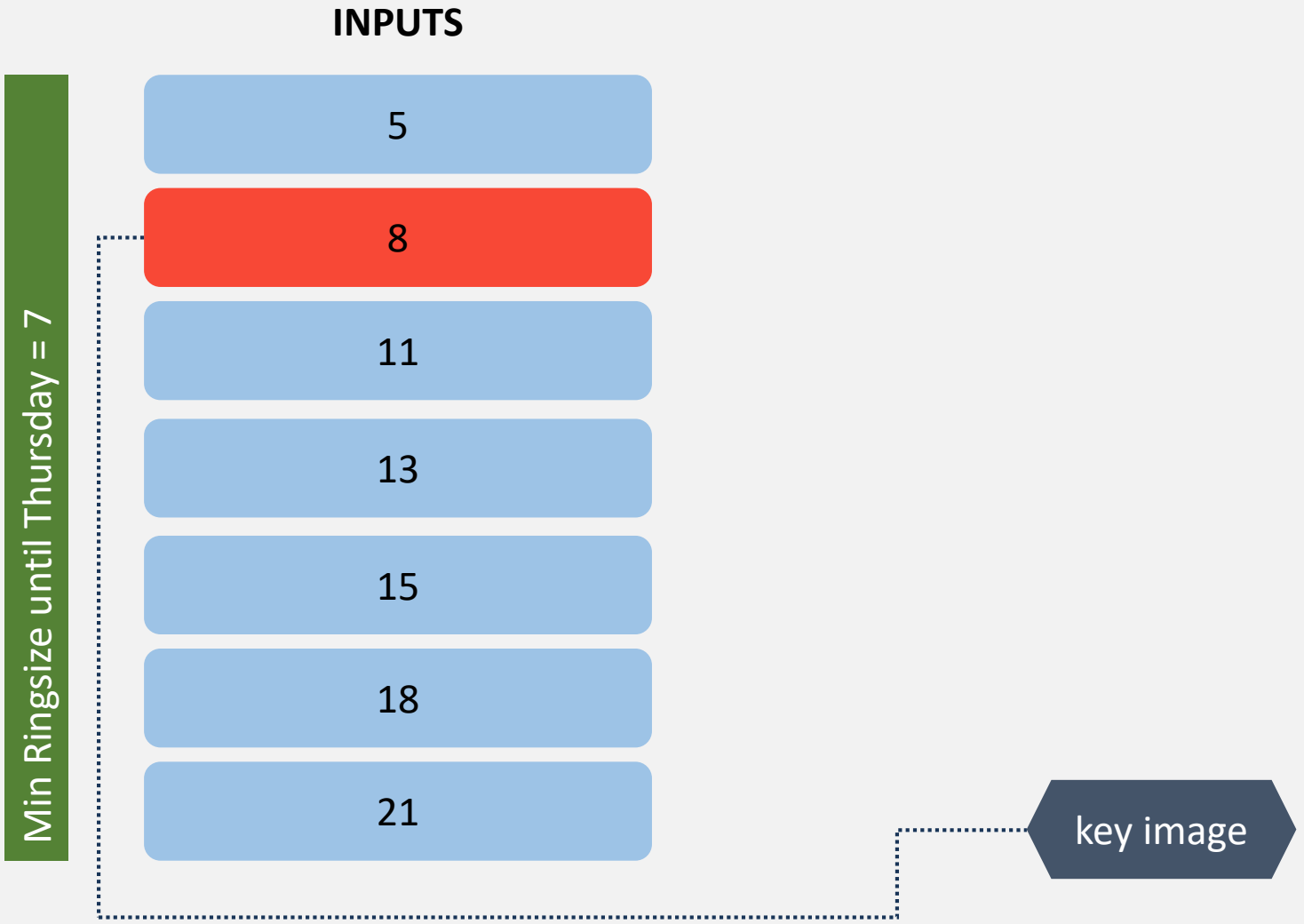


Ring Signatures & RingCT

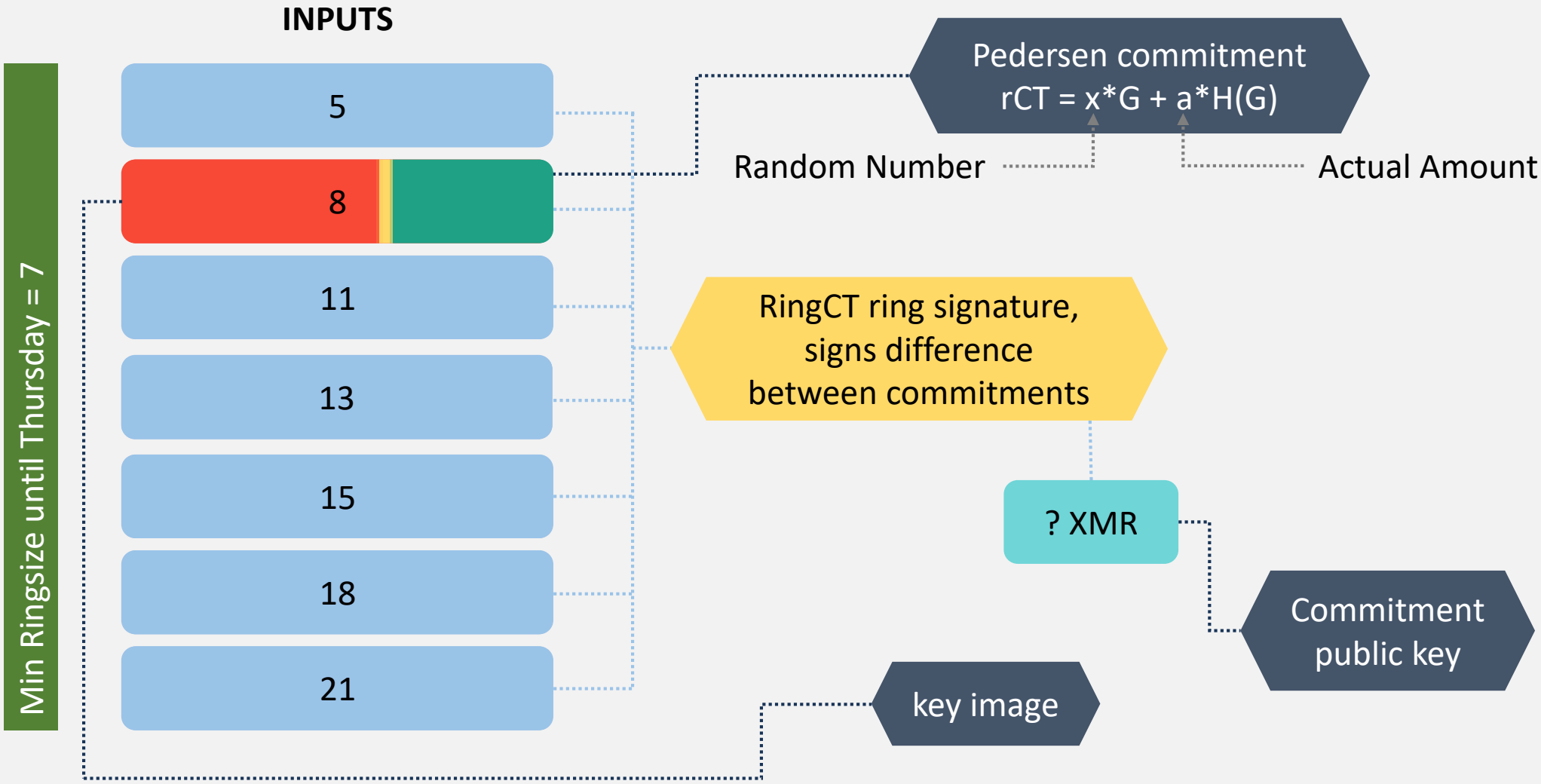
BLOCKCHAIN

1 (Tx ID e4hn4ifqyd5ed)	8 (Tx ID hng6iwfumwf8)	15 (Tx ID wn3f4diiijffwn)
2 (Tx ID eshgni5lsvnf74)	9 (Tx ID cb8vqfi8dfj65f)	16 (Tx ID 5 f8wnfdmmii)
3 (Tx ID wb4f5hdfdicnd)	10 (Tx ID fnidmfnu3dm8)	17 (Tx ID h8fn5mdfi4w)
4 (Tx ID nh5nogsefwjw)	11 (Tx ID twv8mf8dnfas)	18 (Tx ID n48gfwmfdki)
5 (Tx ID fgwinw3fwtk54)	12 (Tx ID h5o8mfdngkd)	19 (Tx ID fnidmnfdsam)
6 (Tx ID ybwnng8nengf)	13 (Tx ID 7nr8mrjffijdtm)	20 (Tx ID t4vn8lf8djer4)
7 (Tx ID e4bgn8flwwrj8)	14 (Tx ID f8n8madkrjmd)	21 (Tx ID 4f5f8njdoam4)

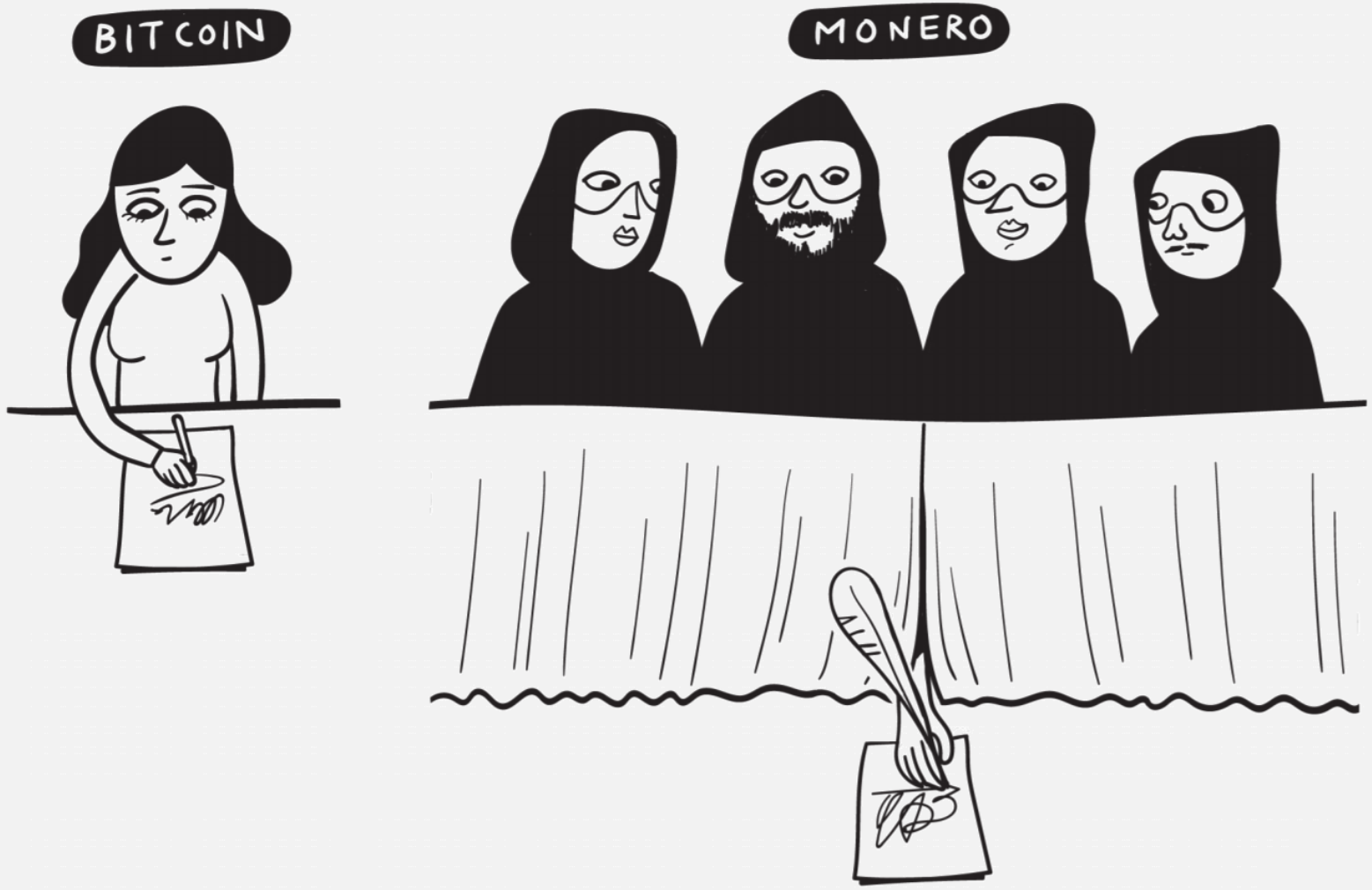
Ring Signatures & RingCT



Ring Signatures & RingCT

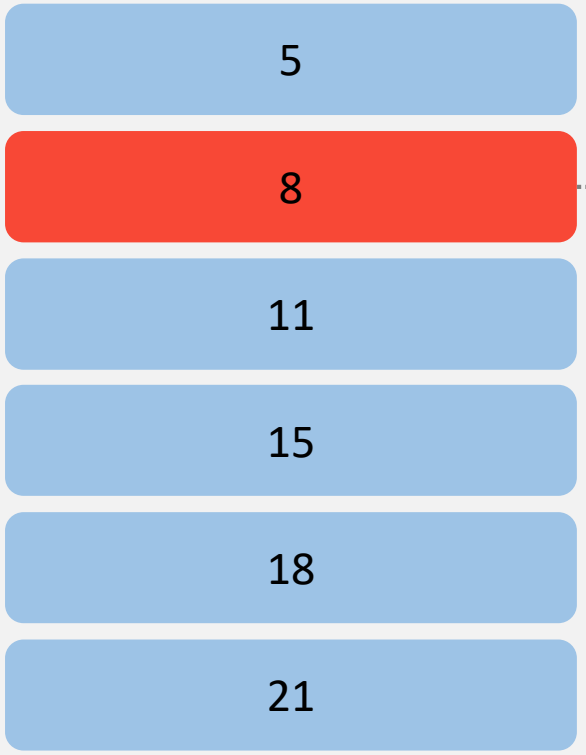


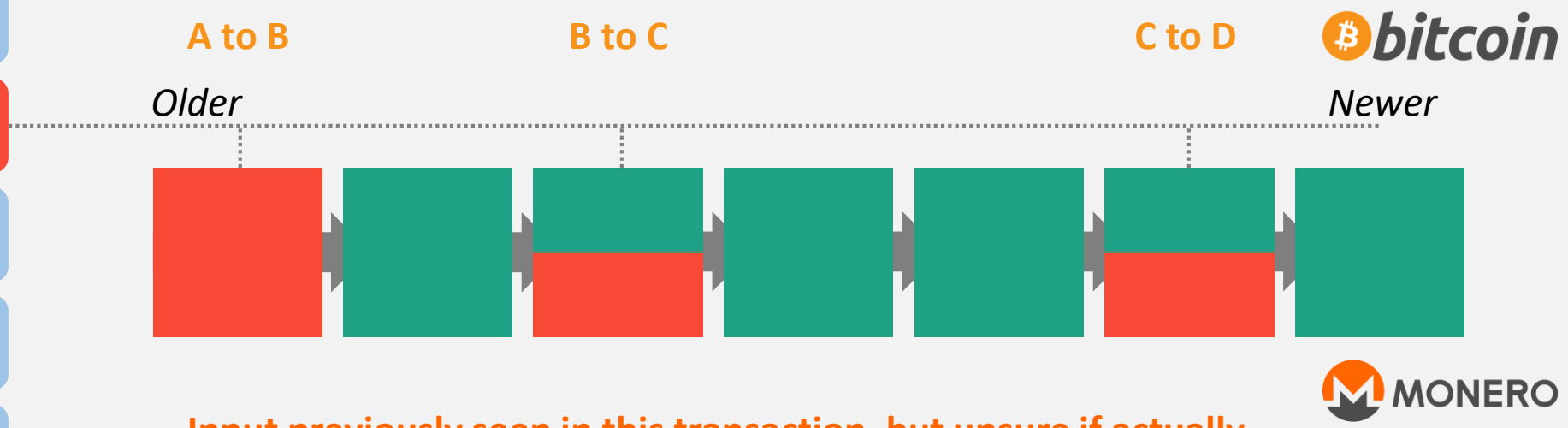
Ring Signatures & RingCT



Ring Signatures & RingCT

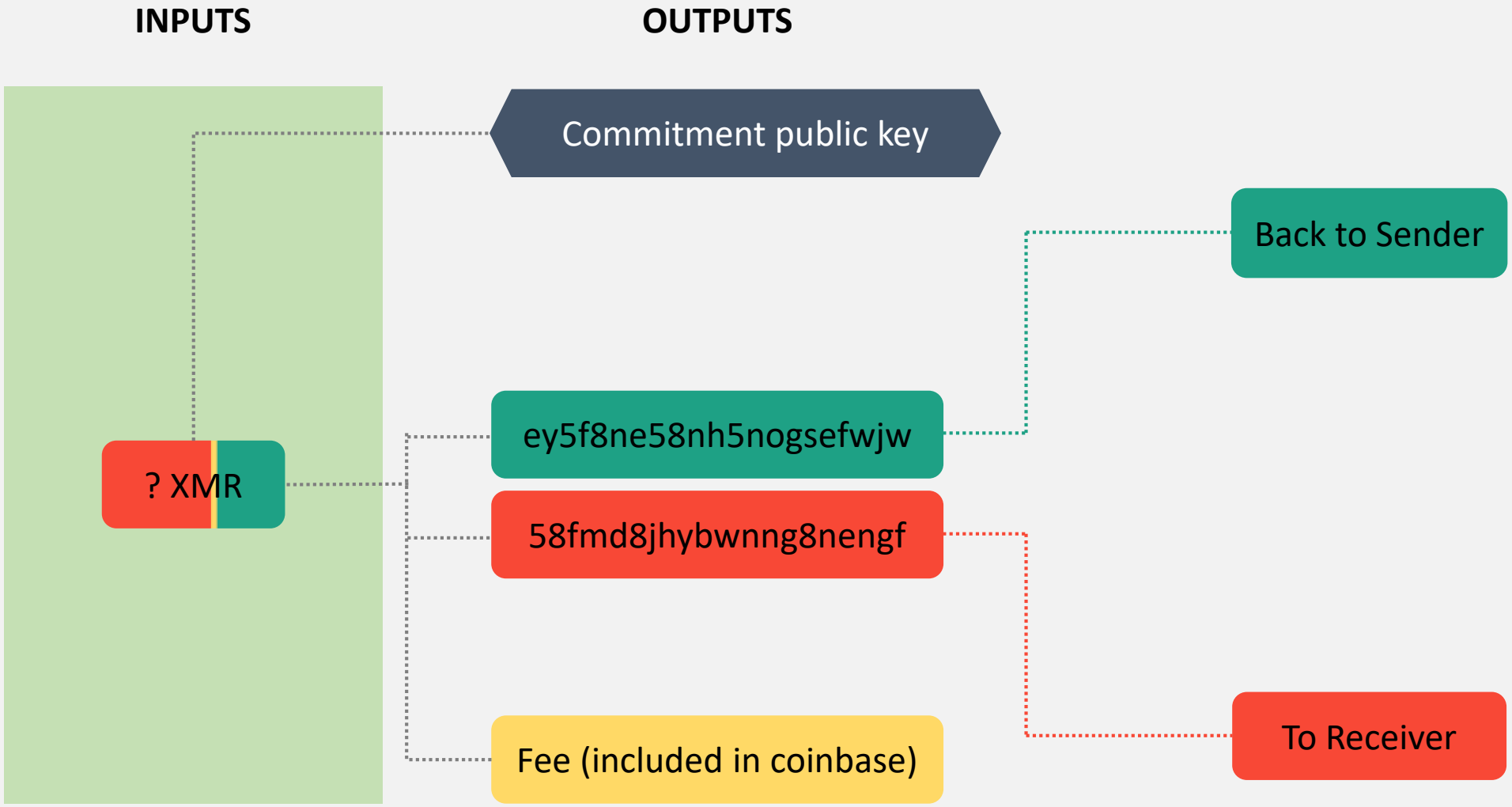
INPUTS





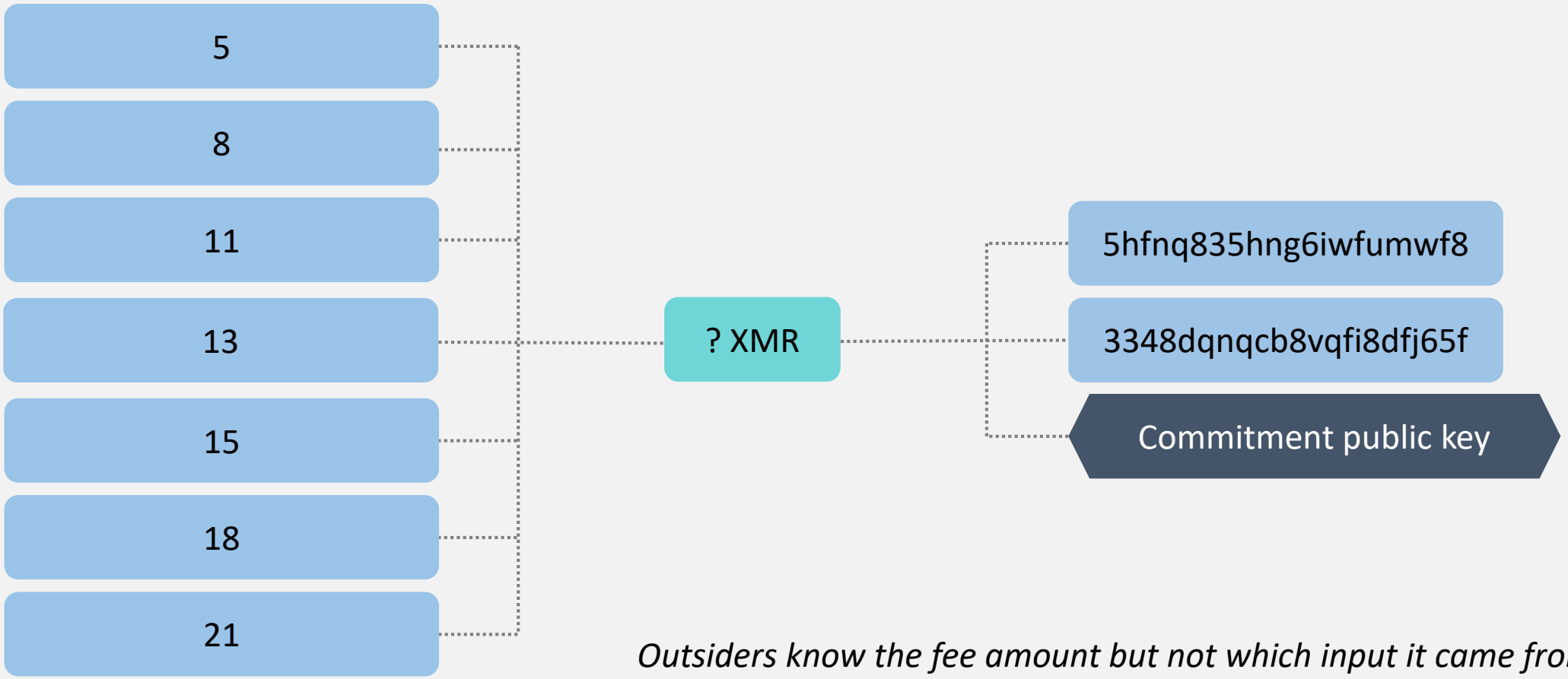
Input previously seen in this transaction, but unsure if actually used to send money or if used as a decoy in a ring signature.

Stealth Addresses



Summary

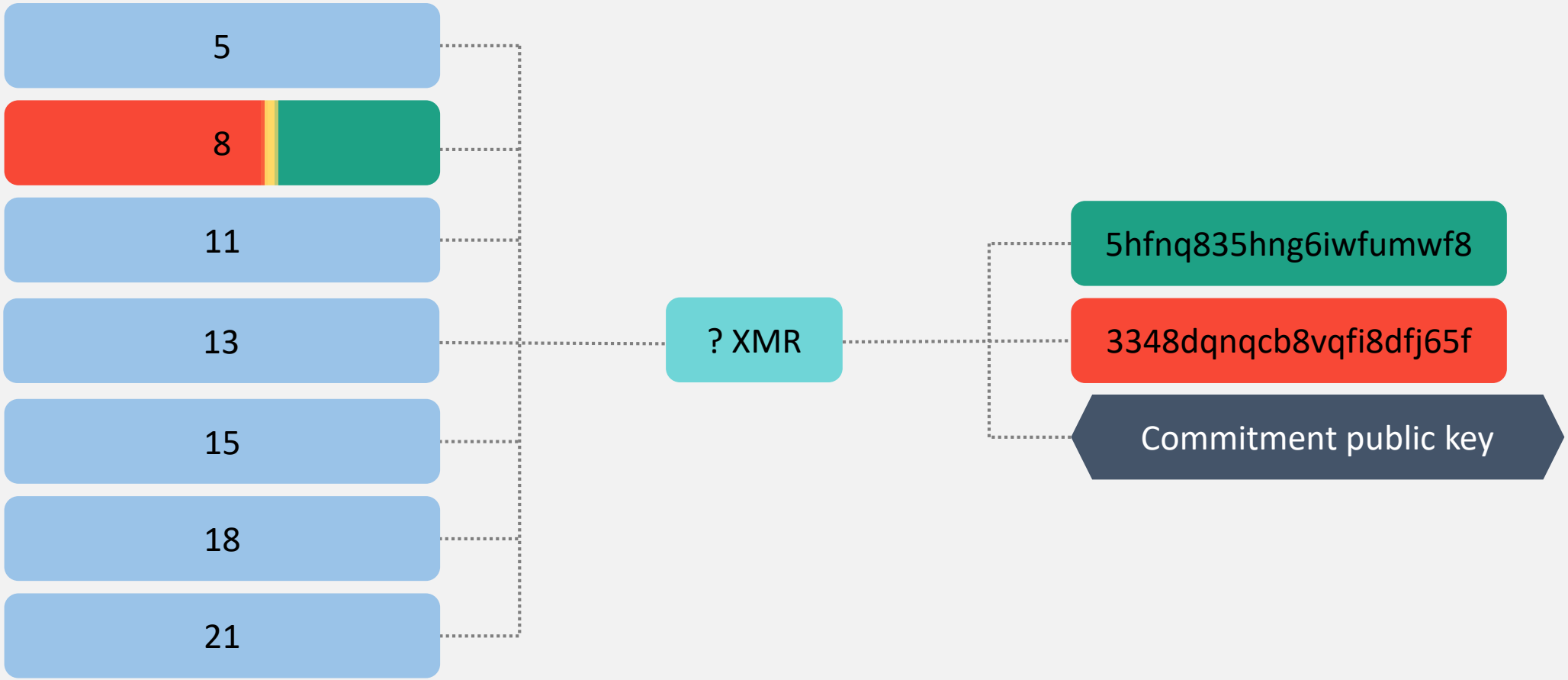
OUTSIDER VIEW



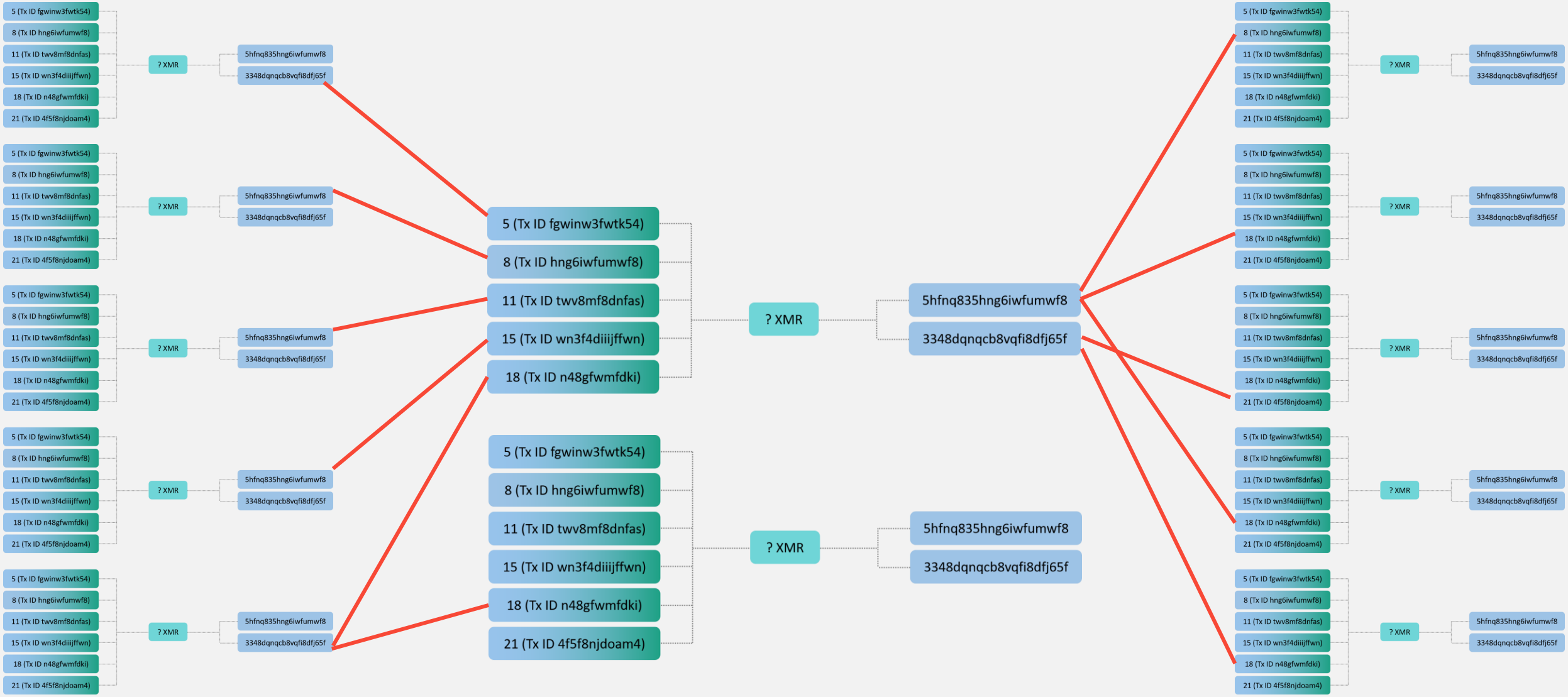
Outsiders know the fee amount but not which input it came from

Summary

INSIDER VIEW



Things Get Complicated Quickly

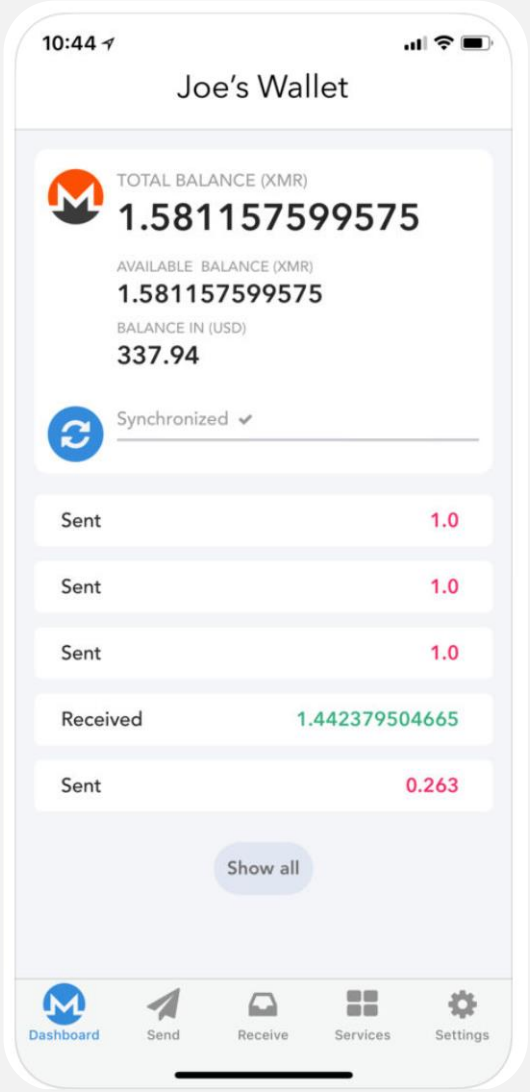


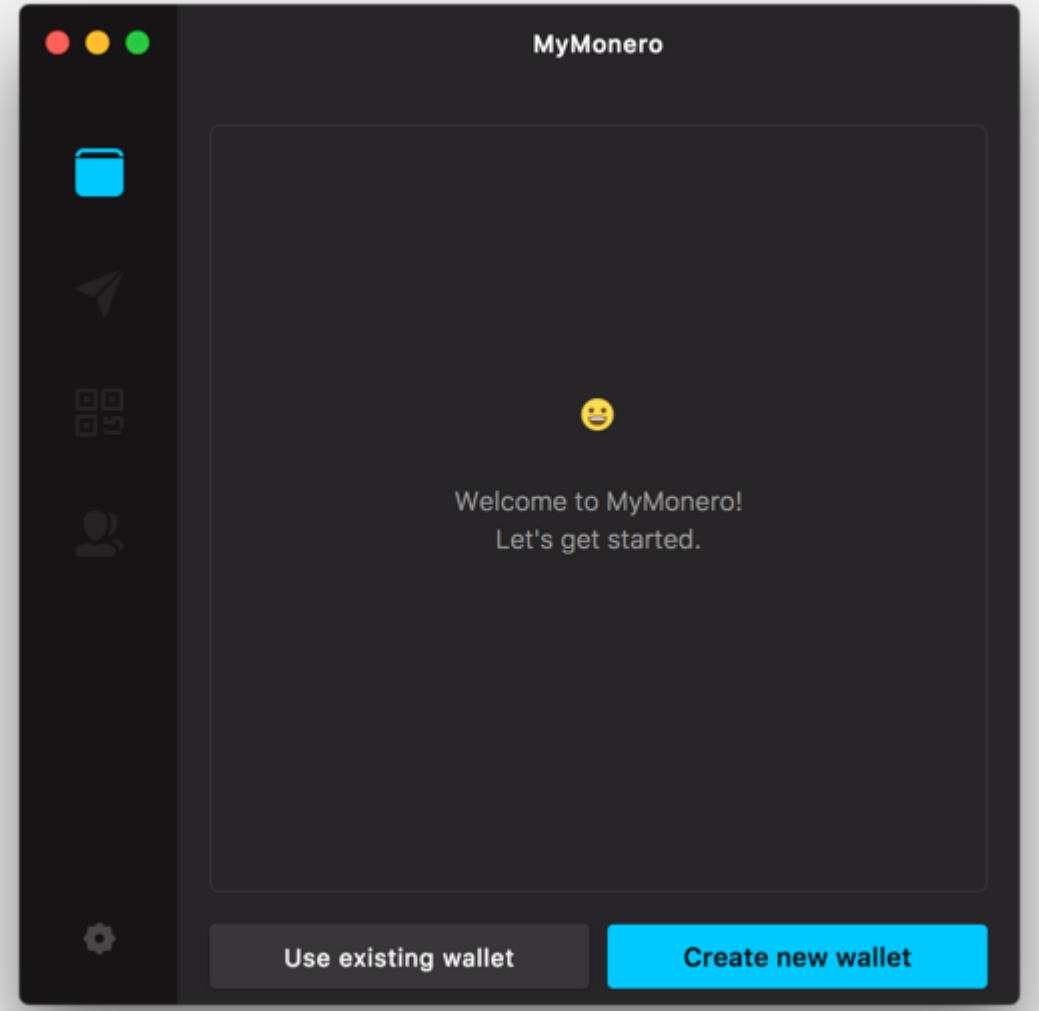
Even Mandatory Privacy Isn’t Perfect

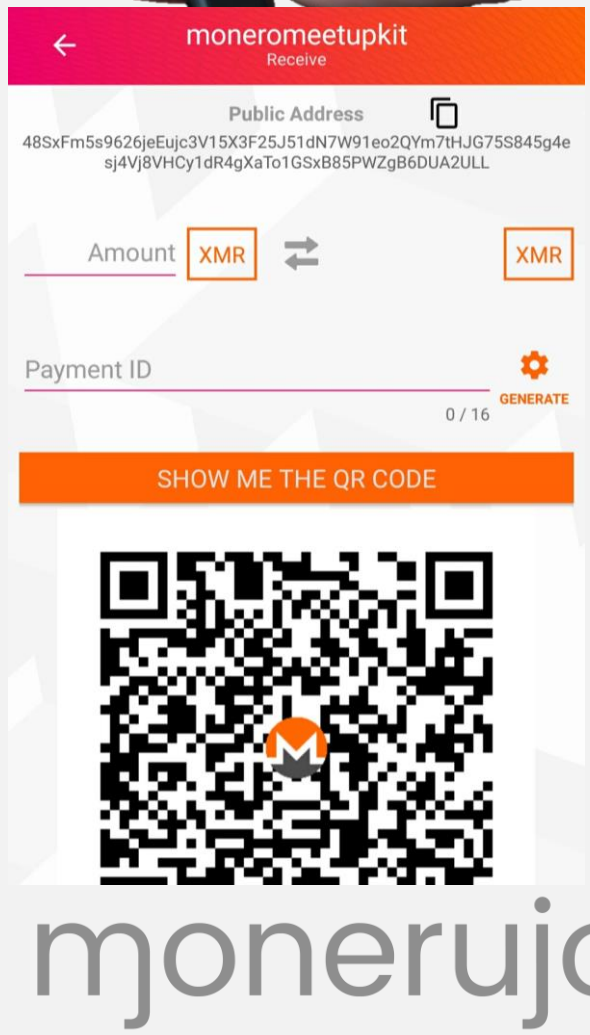
Some things Monero has done to increase its privacy in the last few months:

- Increase ringsize from 3 to 5, 5 to 7, 7 to 11
- Mandatory ringsizes
- Better remote node metadata protection
- Blackball tool
- Churning recommendations

Available Wallets







monerujo

What's Next? Addressing Transaction Size

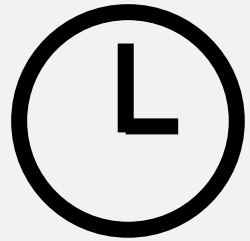
bitcoin ~250B

MONERO ~13.2kB

with single-output bulletproofs (~2.5kB)

with multiple-output bulletproofs (~2.2kB)

Lower Fees
(<80%)



Faster
Verification Time

Quarkslab
SECURING EVERY BIT OF YOUR DATA

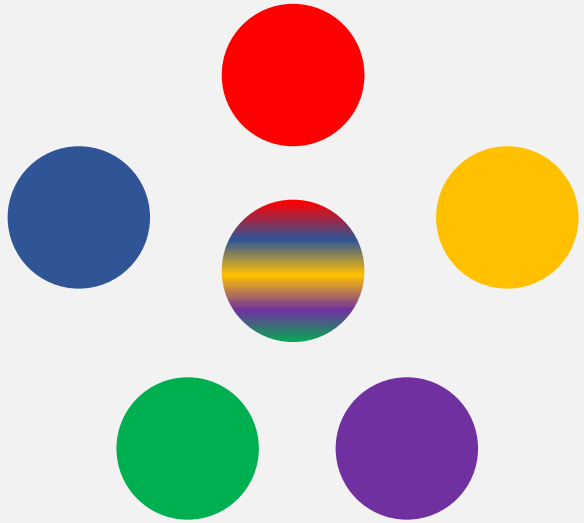
KUDELSKI SECURITY

What’s Next? Addressing Blockchain Bloat

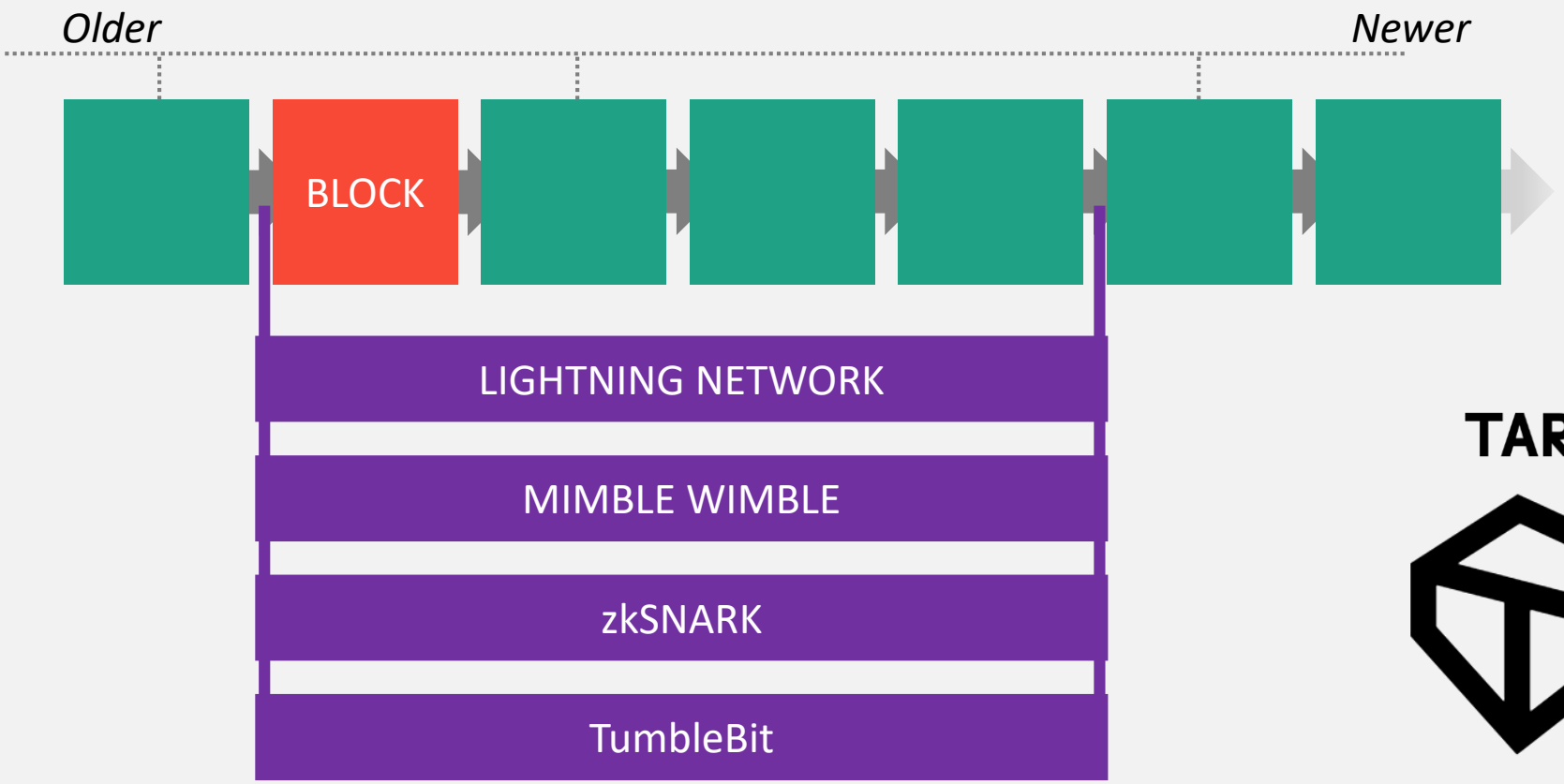
PRUNING

2/3 pruned
in testing

SHARDING

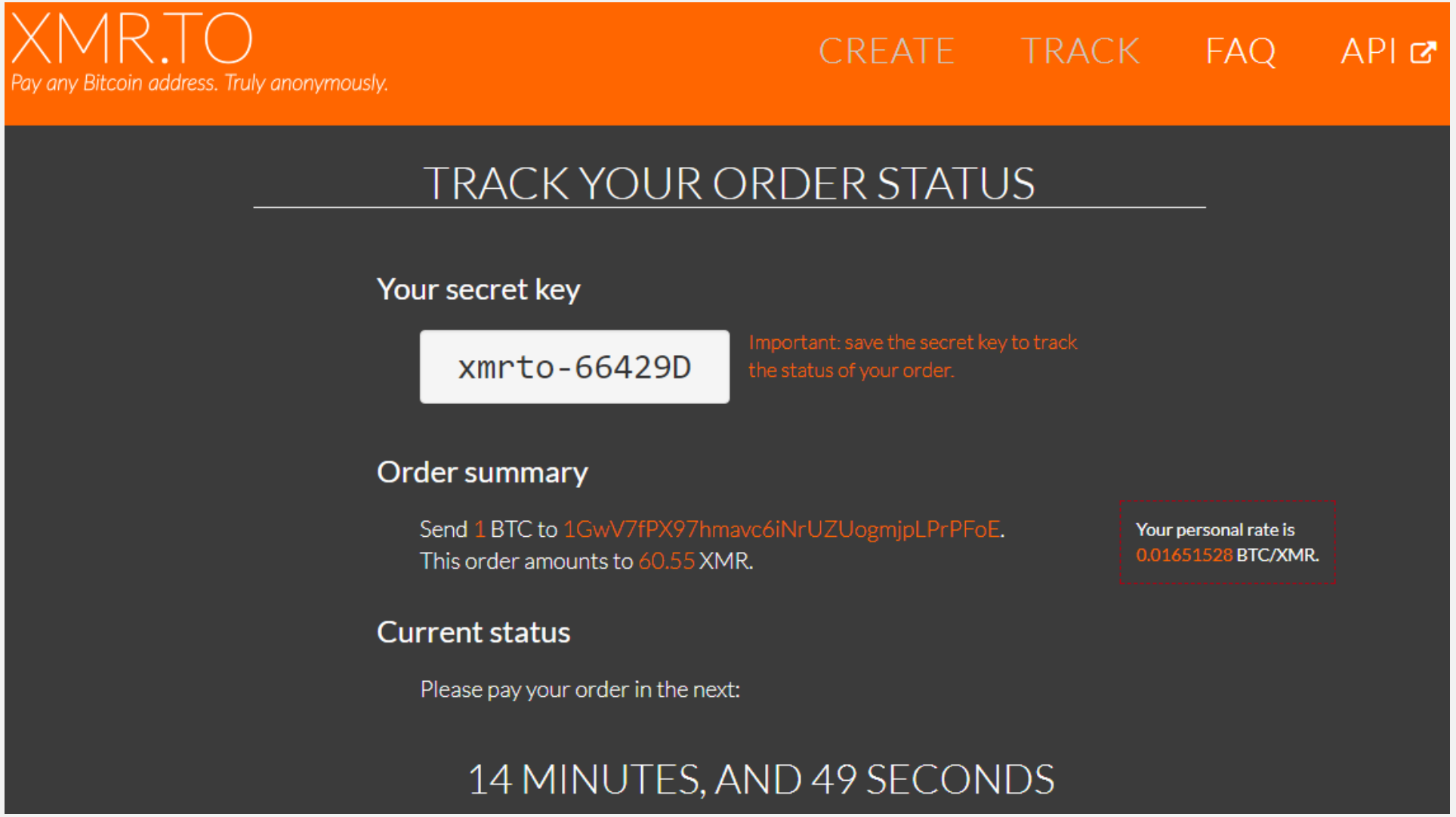


What's Next? Side Chains



TARI

XMR.TO – Pay Bitcoin Addresses with Monero



Why Monero?

Thank You!

getmonero.org

/r/Monero

monero.stackexchange.com

justin@ehrenhofer.org