



Cake Wallet

cakewallet.io

and



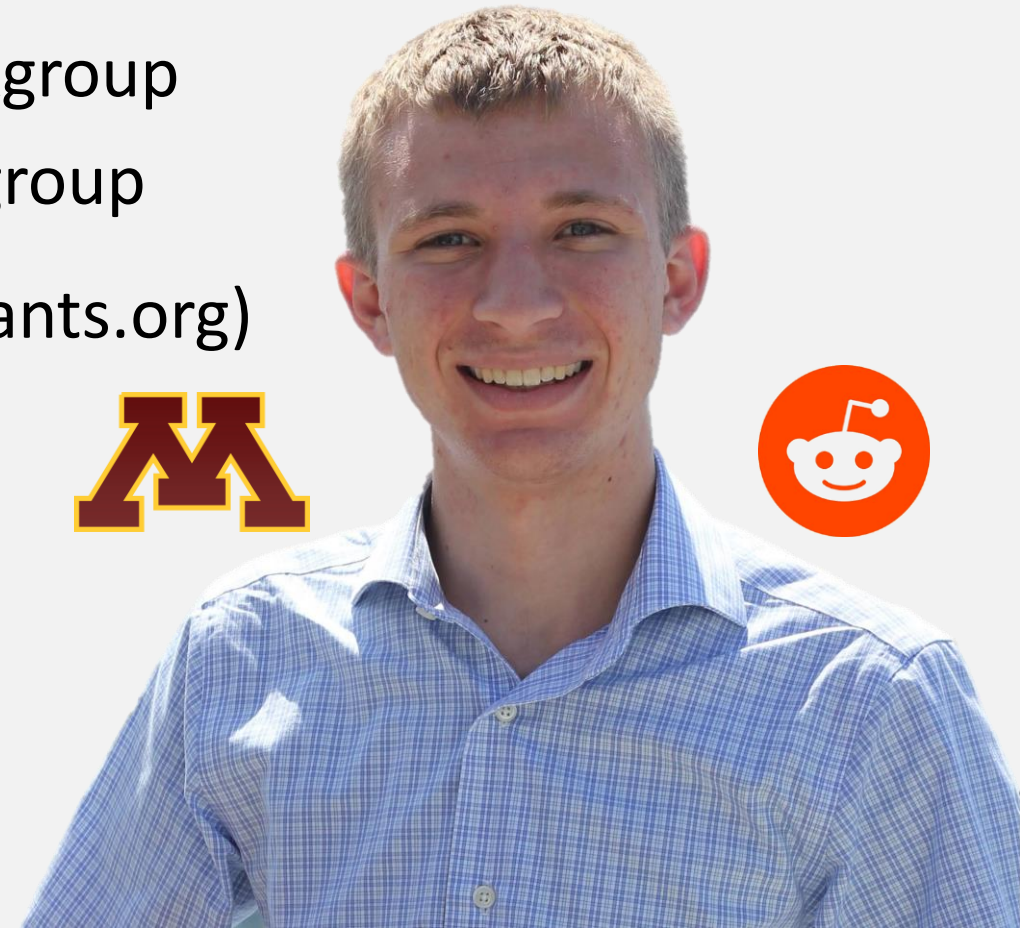
monerotalk.live

Welcome You!

Who Am I?

Justin Ehrenhofer

- Organizer of the Monero Community Workgroup and the Monero Malware Response Workgroup
- Board Member of MAGIC (<https://magicgrants.org>)
- Senior moderator of r/CryptoCurrency
- Host of Breaking Monero
- Publisher of Mastering Monero



Privacy Isn't Binary

What most people think privacy is:



Privacy Isn't Binary

What privacy actually is:



Perfect Privacy

Perfect Transparency

It All Comes Back to a Threat Model



Bitcoin is NOT (very) private!



Transparency Has Implications on People and Business



Sources

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



Expenses

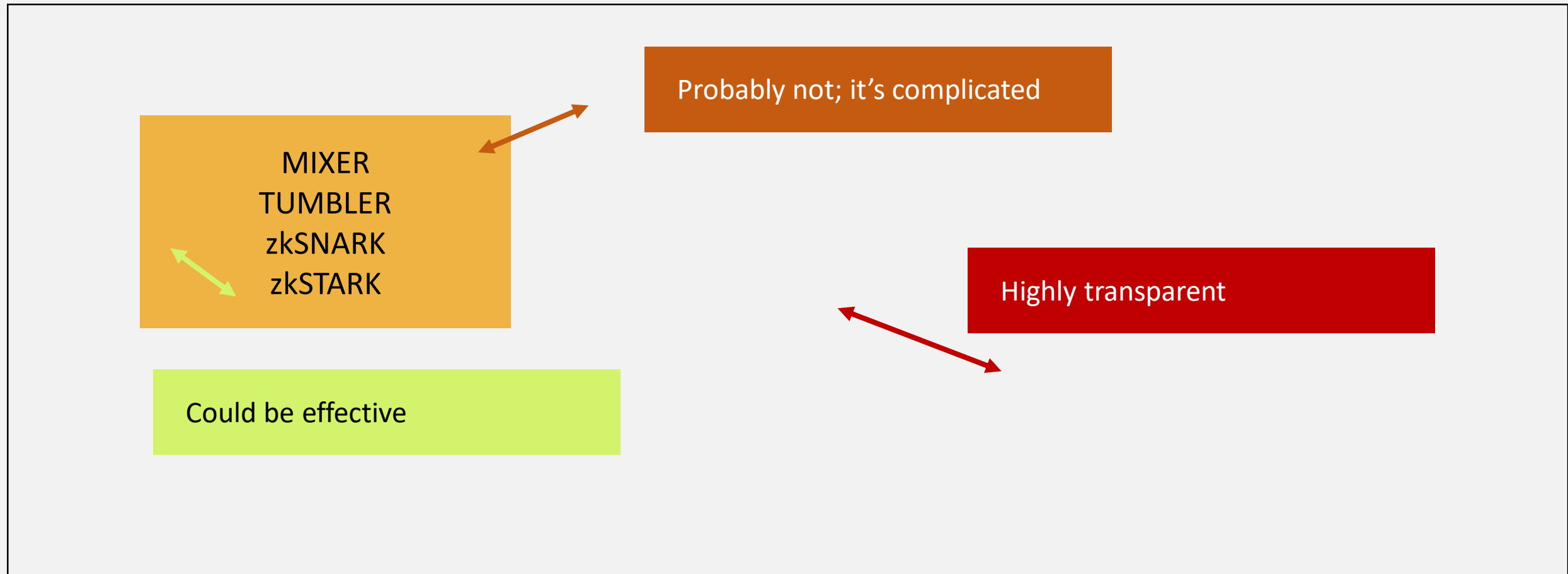
- Political and religious affiliations
- Health data and doctors
- Customers and downstream business connections
- Everyday purchasing habits
- Employees



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



Transparency Is Important...

For the Right People



Sender:

Receiver:

Amount:



Transparency Is Important...

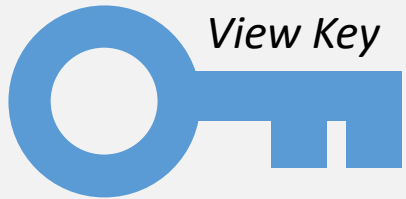
For the Right People



Sender:
Bob
Receiver:
Alice
Amount:
5



Transparency Is Important... For the Right People



Sender:
Bob
Receiver:

Amount:

Sender:

Receiver:

Amount:



Transparency Is Important... For the Right People



View Key + key image

Sender:

Bob

Receiver:

Alice

Amount:

5

Sender:

Receiver:

Amount:



Zero-Knowledge Does Not Mean Perfect

Monero

Ring signatures are not perfect

Zcash

Turnstile migration process is difficult, likely impossible

Sapling introduces more output metadata

Both

Some output metadata

Timing attacks

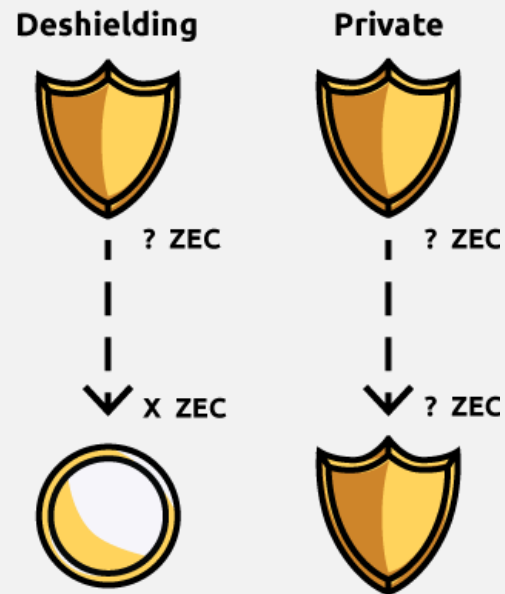
Privacy Solutions to Consider



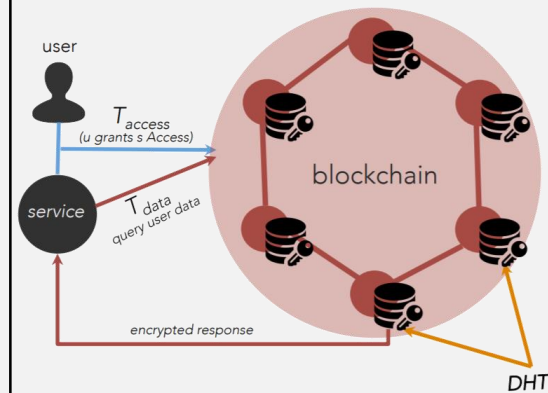
Ring signatures

RingCT

Stealth addressess



zkSNARKs



File encryption on
central server

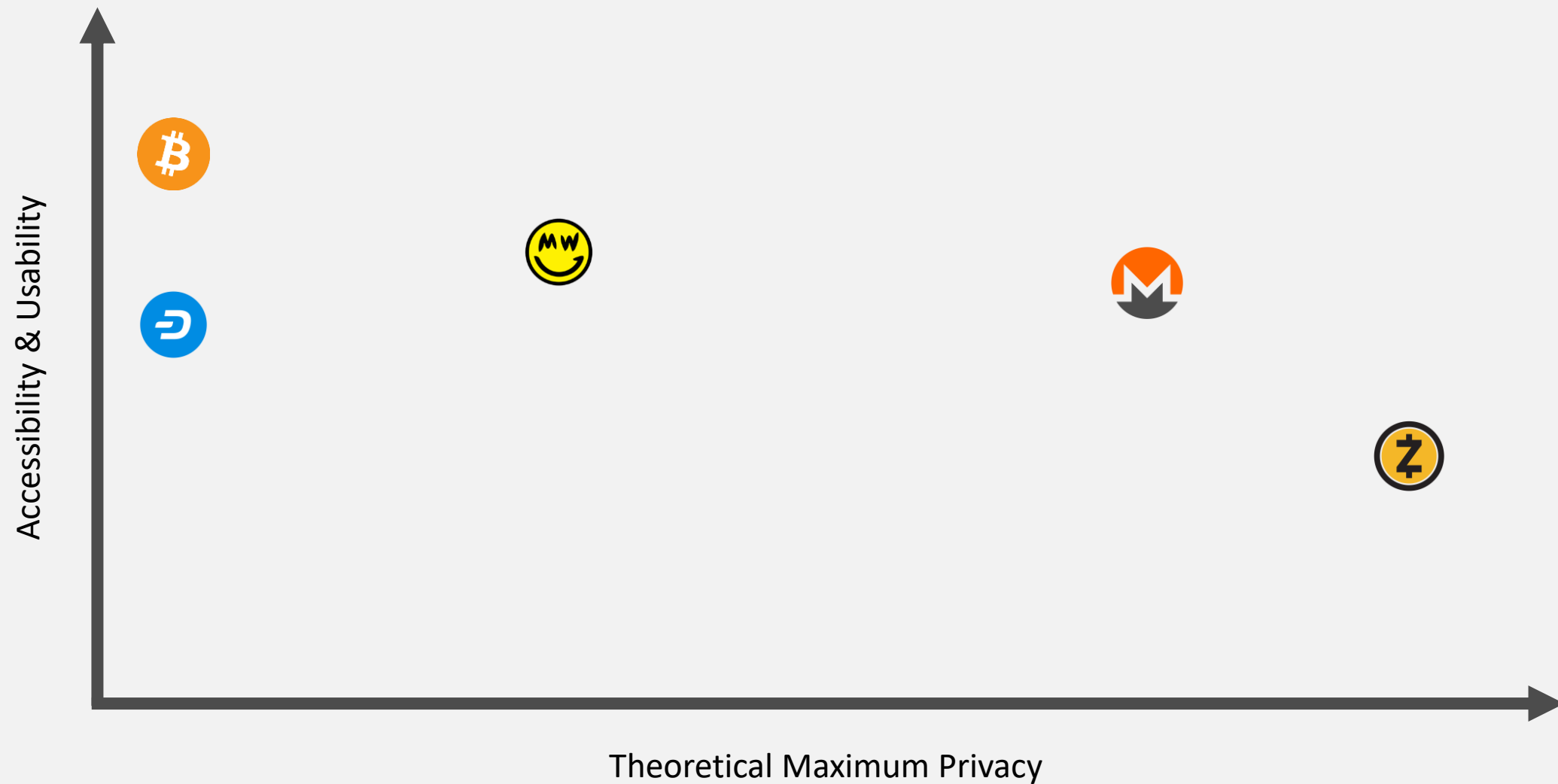
Hash stored on
blockchain













































Coming Soon™

zkSTARKs

Privacy Matrix
















































A Quick Note About Comparison Charts

Bulwark vs Others							
The next generation privacy cryptocurrency							
	 CASH	 PIVX <small>PRIVATE INSTANT VERIFIED TRANSACTIONS</small>	 MONERO	 BULWARK <small>CRYPTOCURRENCY</small>	 DASH	 VERGE	 ZCOIN
Consensus Algorithm	PoW	PoS 3.0	PoW	PoW + PoS 3.0	PoW	PoW	PoW
Masternodes		 +5.78% ROI		 +228.26% ROI	 +7.55% ROI		 +38.83% ROI
Premine Supply	10%	0%	0%	1.8%	25%	0%	10%
ASIC Resistant							
Untraceable / Mixing							
Wallets	Linux, Trezor	Windows, Linux, Mac, Android, Nano S	Windows, Linux, Mac, Web	Windows, Linux, Mac, Android, iOS, Paper, Pi, Web	Windows, Linux, Mac, Android, Trezor, Nano S, KeepKey, Paper	Windows, Linux, Mac, Android, Pi, Paper, Web, Docker	Windows, Linux, Mac
Staking Rewards							
Secure Home Node							
Big Exchanges	Huobi, Bittrex, Poloniex, Binance, Upbit, OKEx, Bithumb, Bitfinex, Kraken	Bittrex, Upbit, Binance	Bittrex, Poloniex, Binance, Upbit, OKEx, Bithumb, Bitfinex, Kraken	Coming Soon	Huobi, Bittrex, Poloniex, Binance, Upbit, OKEx, Bithumb, Bitfinex, Kraken	Bittrex, Binance, Upbit	Bittrex, Binance, Upbit

A Quick Note About Comparison Charts

Crypto Comparison Chart		
Features!	 CASH	
Optional Privacy!		
Zero Knowledge Proofs!		
zkSNARKS technology, which Ethereum wants to adopt!		
Trusted Setup, verified by Bitcoin developer Peter Todd!		
Based on Bitcoin codebase!		
Endorsed by Edward Snowden!		
Funds developers with 20% of mined coins, instead of just giving them to greedy miners!		

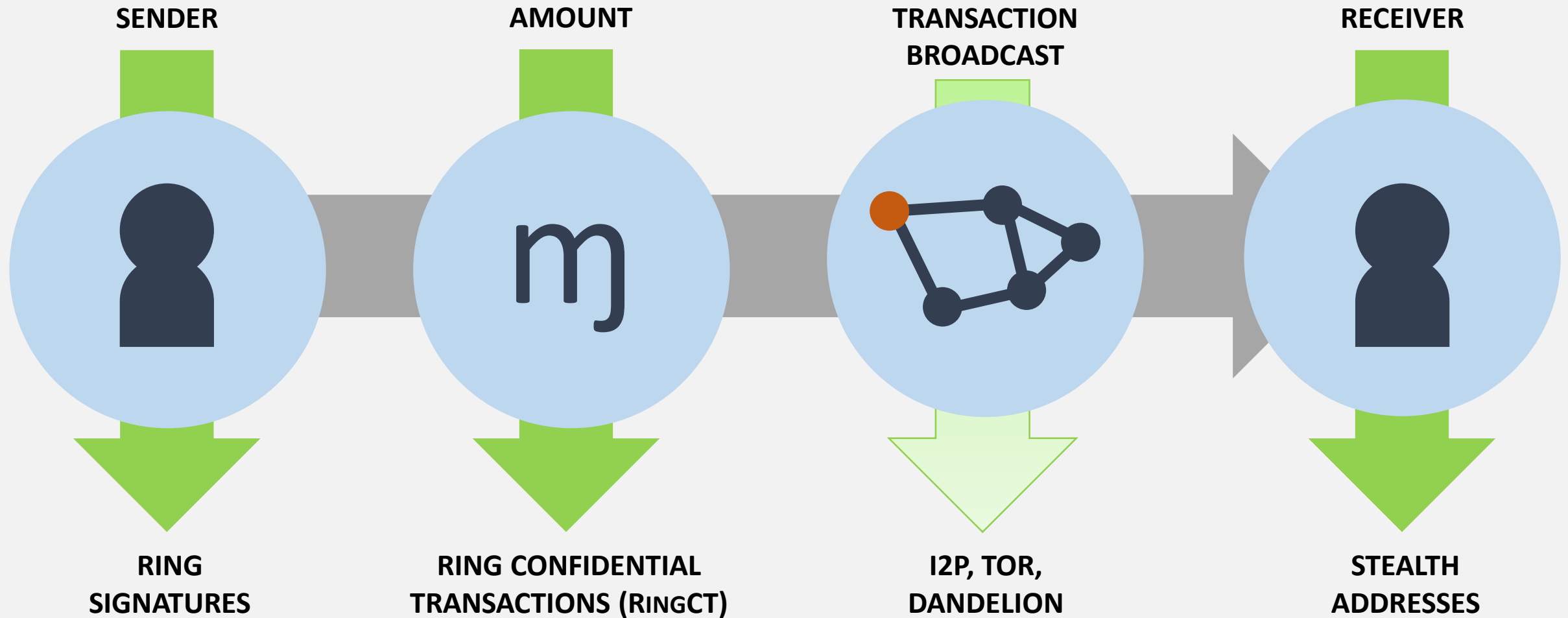
COMPARING PRIVACY PROTOCOLS HOW DAPS IS DIFFERENT					
					
	DAPS	VERGE	MONERO	ZCASH	DASH
SUPPLY	SWAP+10B	17B	INFINITE	INFINITE	18.9M
BLOCK TIME	1 MIN	30 SEC (2 MIN AVERAGE)	2 MIN	2 MIN 30 SEC	2 MIN 30 SEC
MINIMAL FEES					
MASTERNODES					
TOR/OBFS4 RELAY					
STEALTH ADDRESSES					
MANDATORY STEALTH					
ZK-SNARKS					
RING CT					
POS V3					
TIME WARP ATTACK	IMPOSSIBLE	VULNERABLE	POSSIBLE	VULNERABLE	POSSIBLE
TRUSTLESS	YES	YES	YES	NO	NO
ATOMIC SWAPS	PLANNED	PLANNED	NO	YES	YES

Privacy Solutions to Consider



Source of Funds	Decent Protection	Not Protected	Protected	Protected if Shielded
Receiver	Protected	Not Protected	Protected	Not Protected*
Amount	Protected	Not Protected	Protected	Mostly Not Protected
Transaction Size	~1.9kB	~0.3kB	~1kB	~20kB*
Verification Time	Milliseconds	Milliseconds	Milliseconds	Not Sure
Signing Time	Milliseconds	Milliseconds	~2.3 seconds	~10 seconds

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)

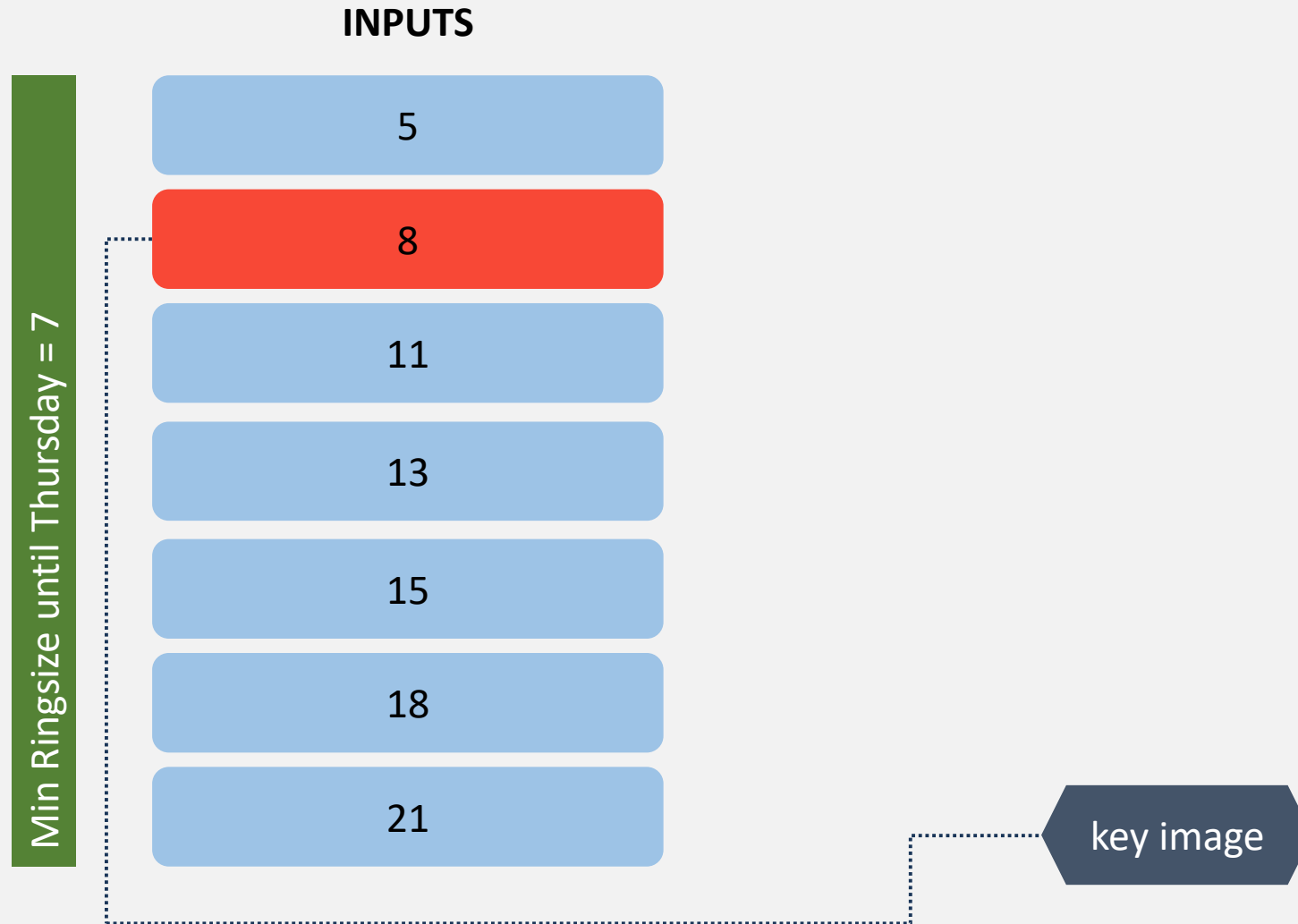
20 (Tx ID t4vn8lf8djer4)

7 (Tx ID e4bgn8flwwrj8)

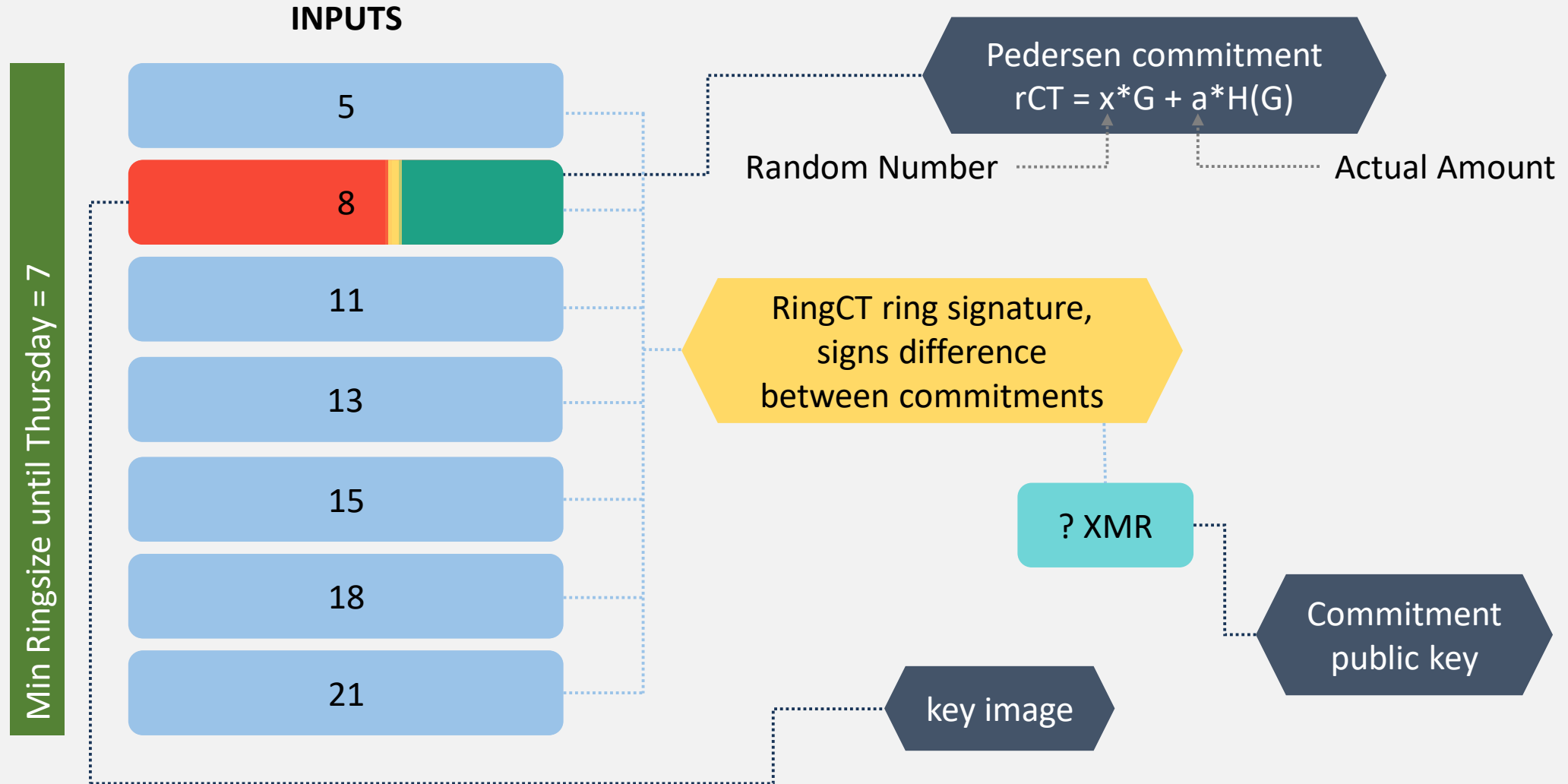
14 (Tx ID f8n8madkrjmd)

21 (Tx ID 4f5f8njdoam4)

Ring Signatures & RingCT



Ring Signatures & RingCT

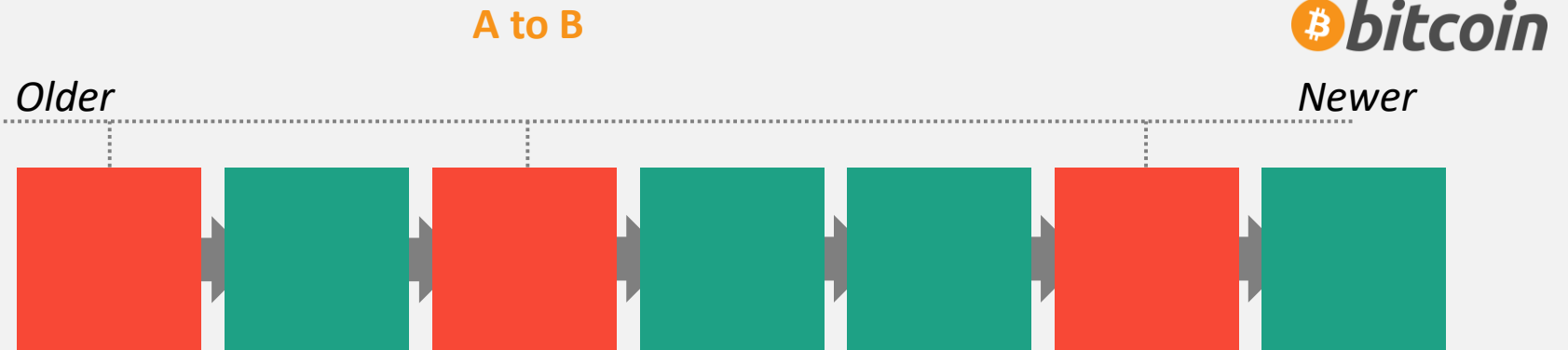
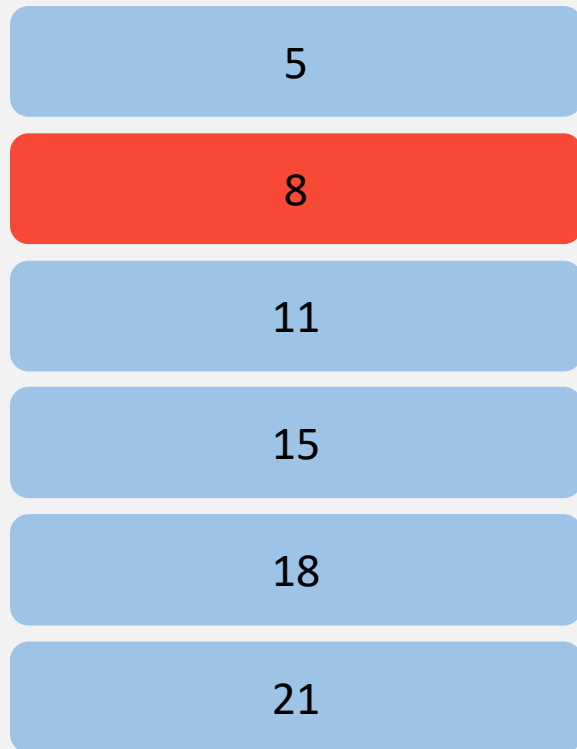


Ring Signatures & RingCT



Ring Signatures & RingCT

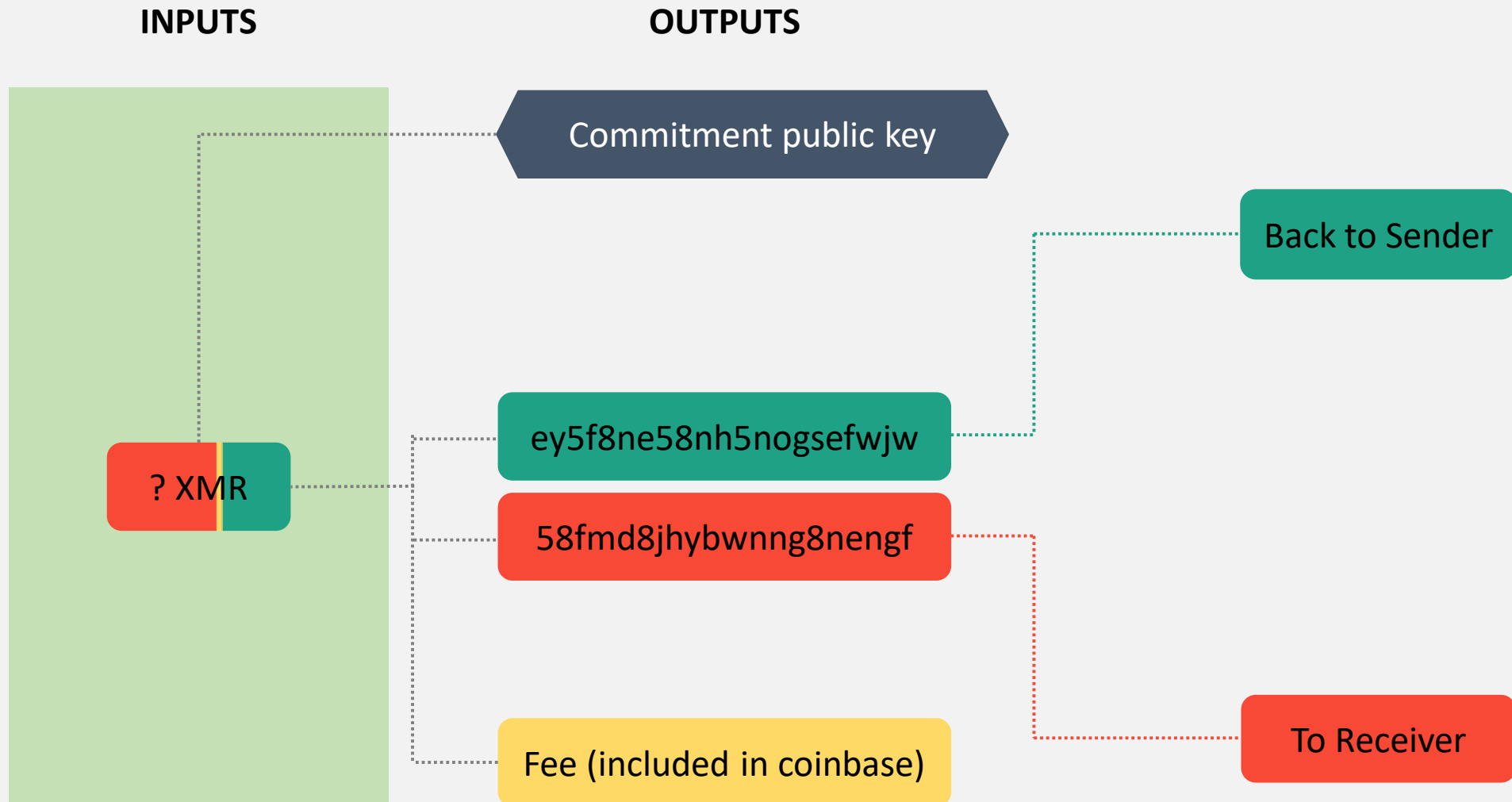
INPUTS



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

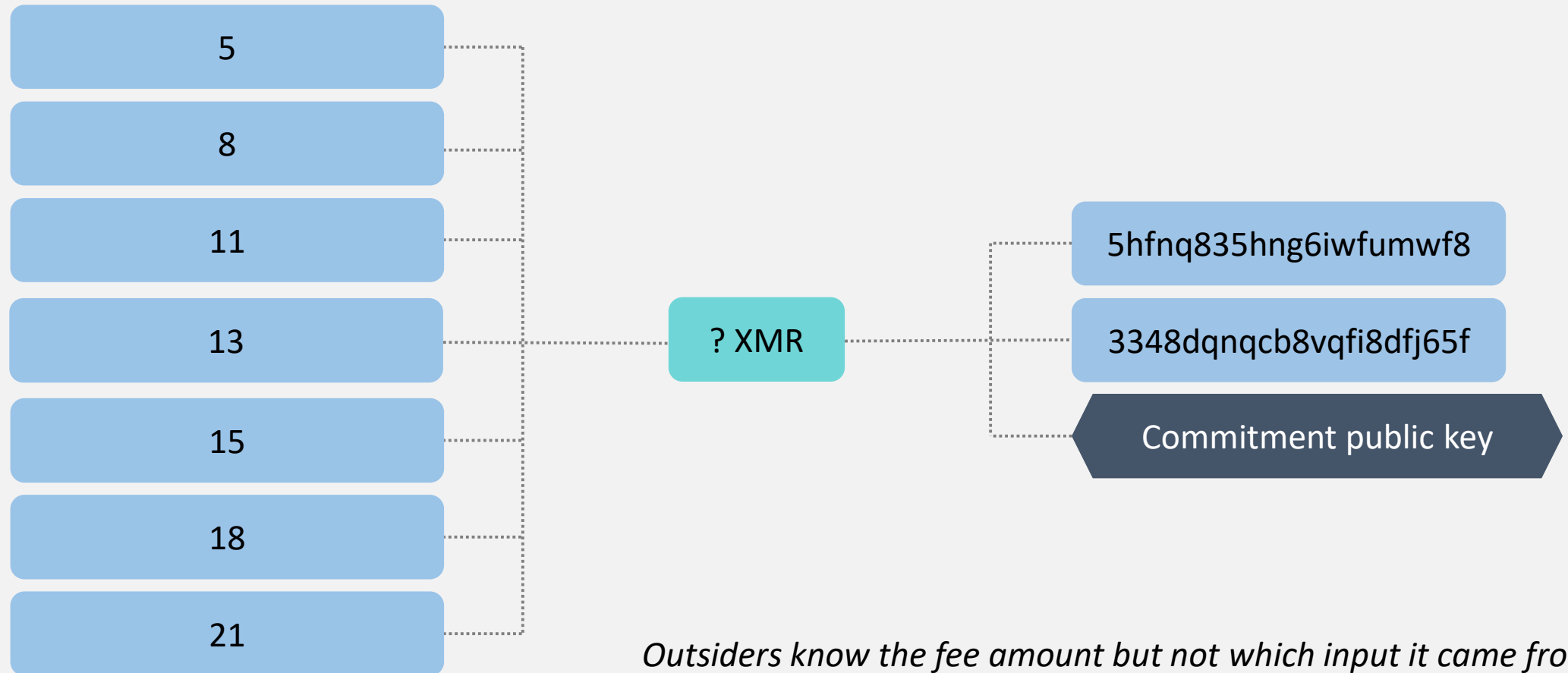


Stealth Addresses



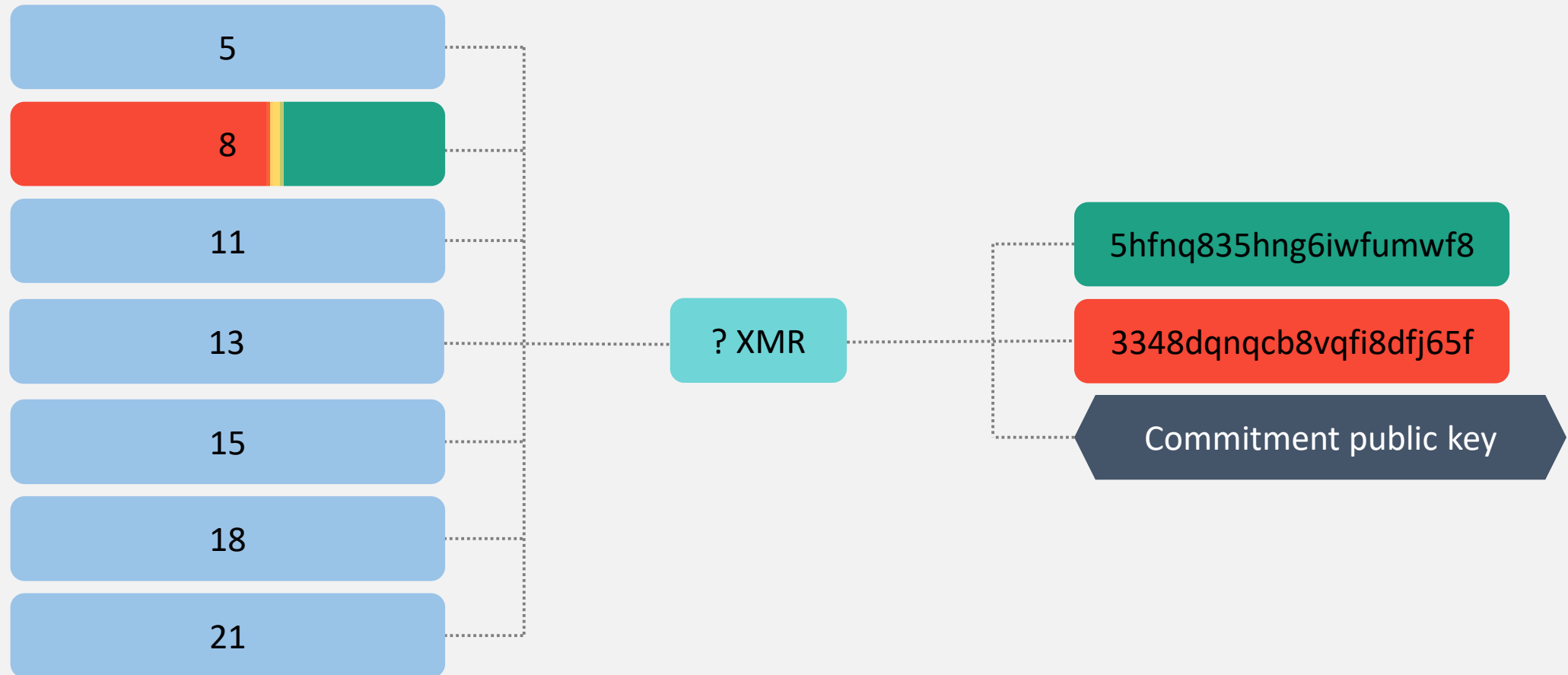
Summary

OUTSIDER VIEW

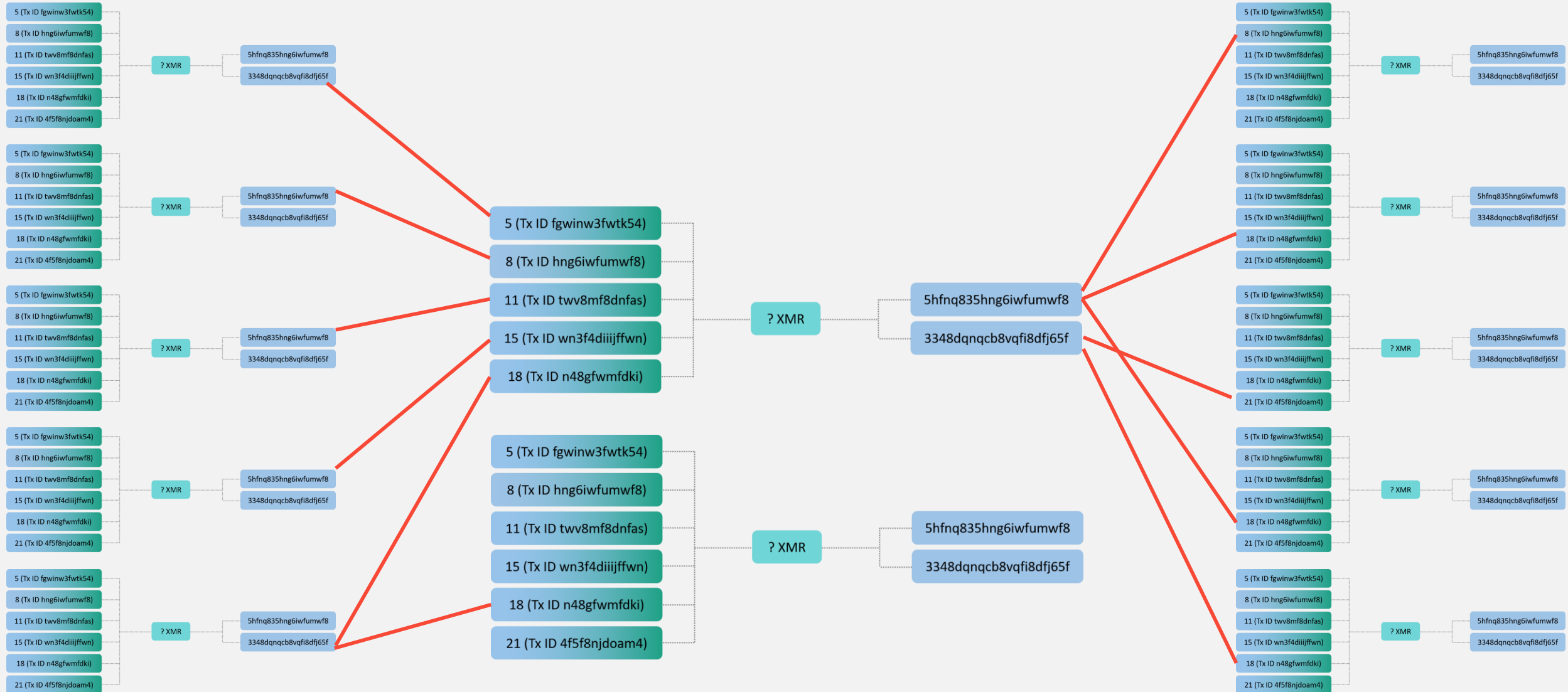


Summary

INSIDER VIEW

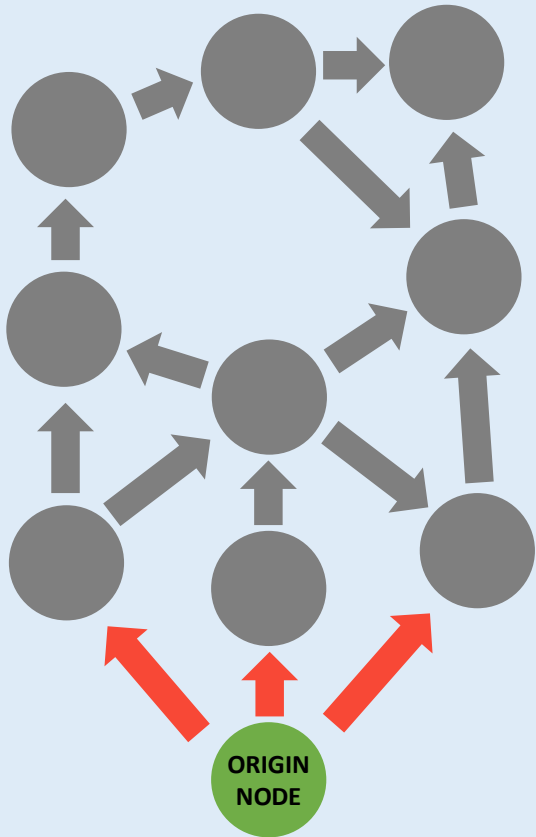


Things Get Complicated Quickly

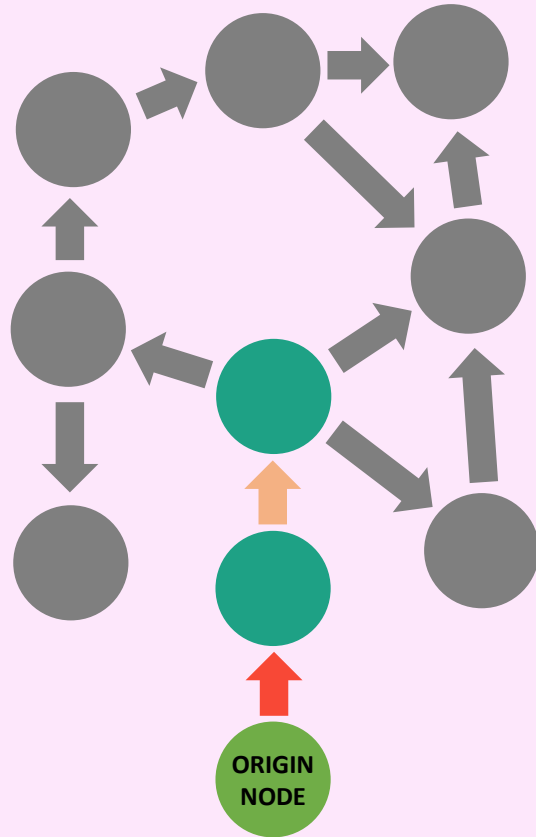


Network Metadata

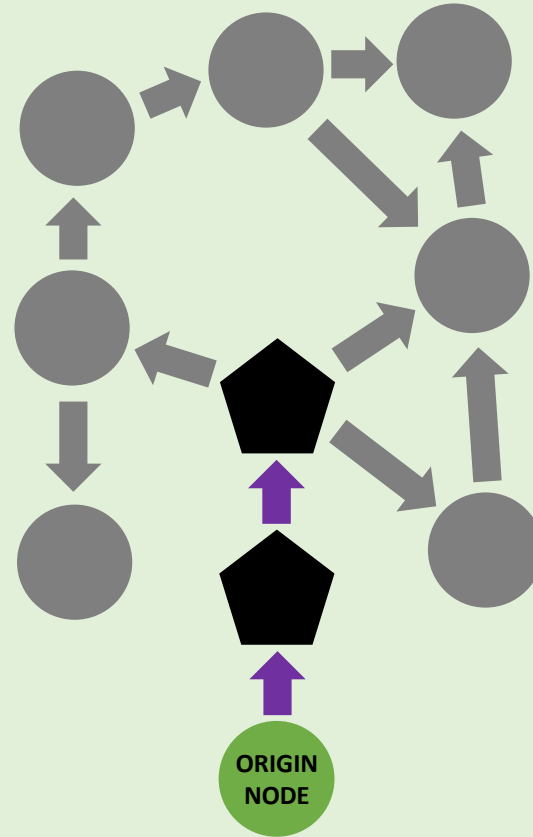
Clearnet (No Dandelion)



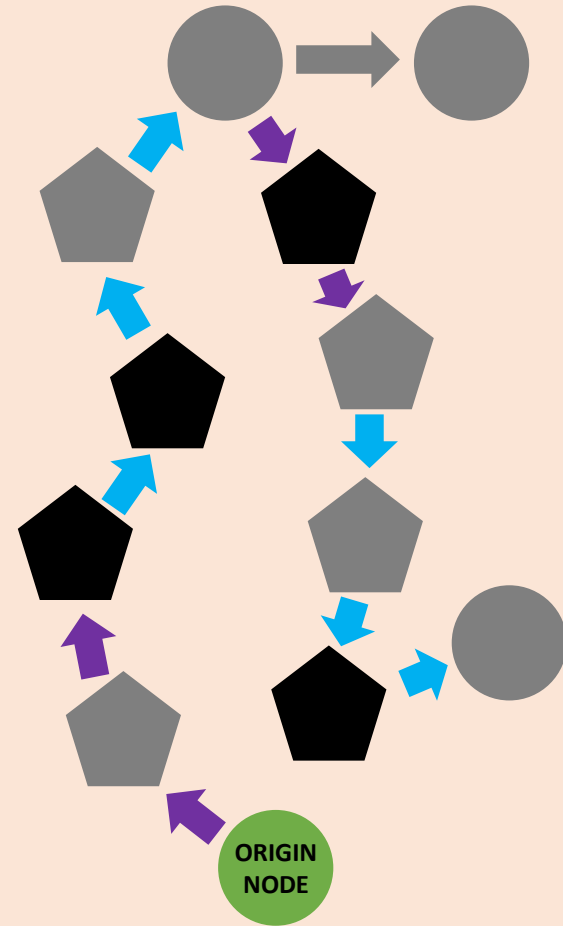
Clearnet (Dandelion++)



Tor

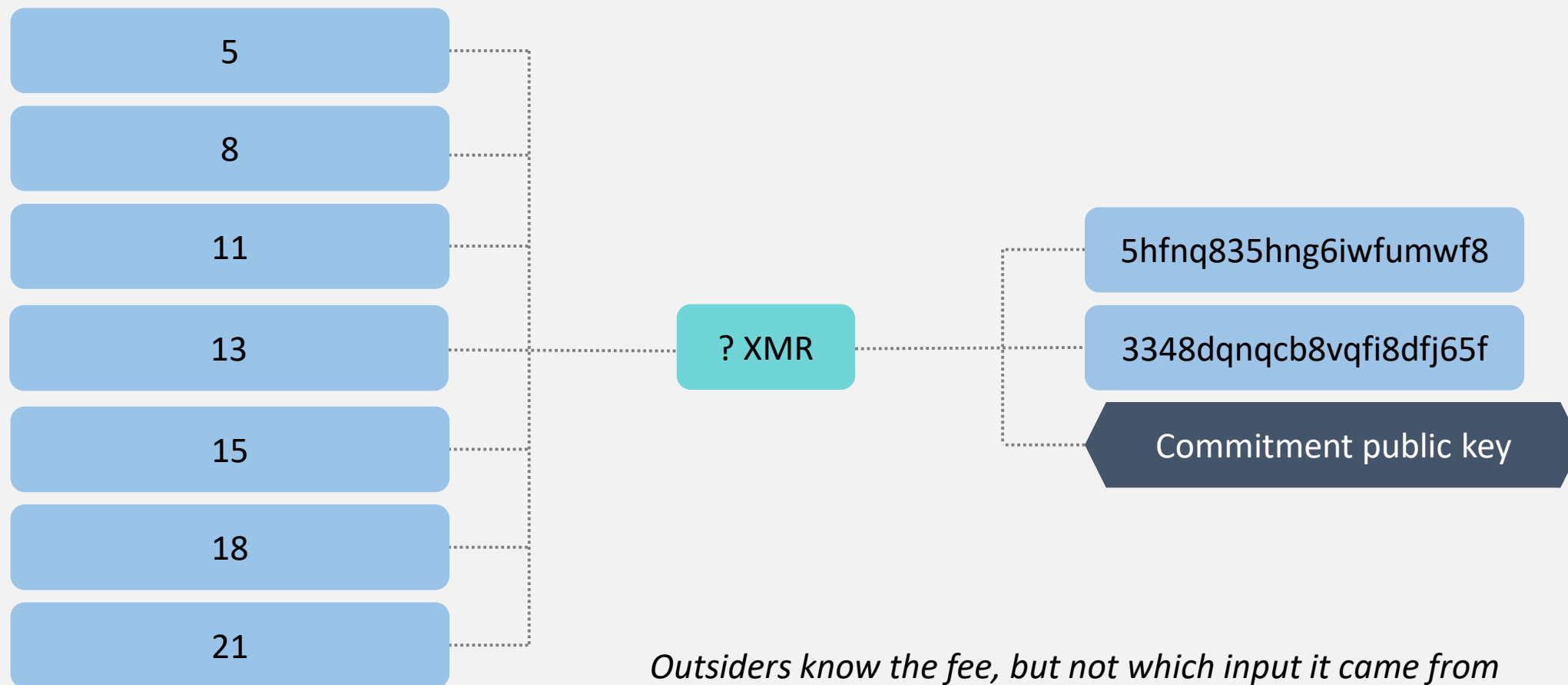


i2p



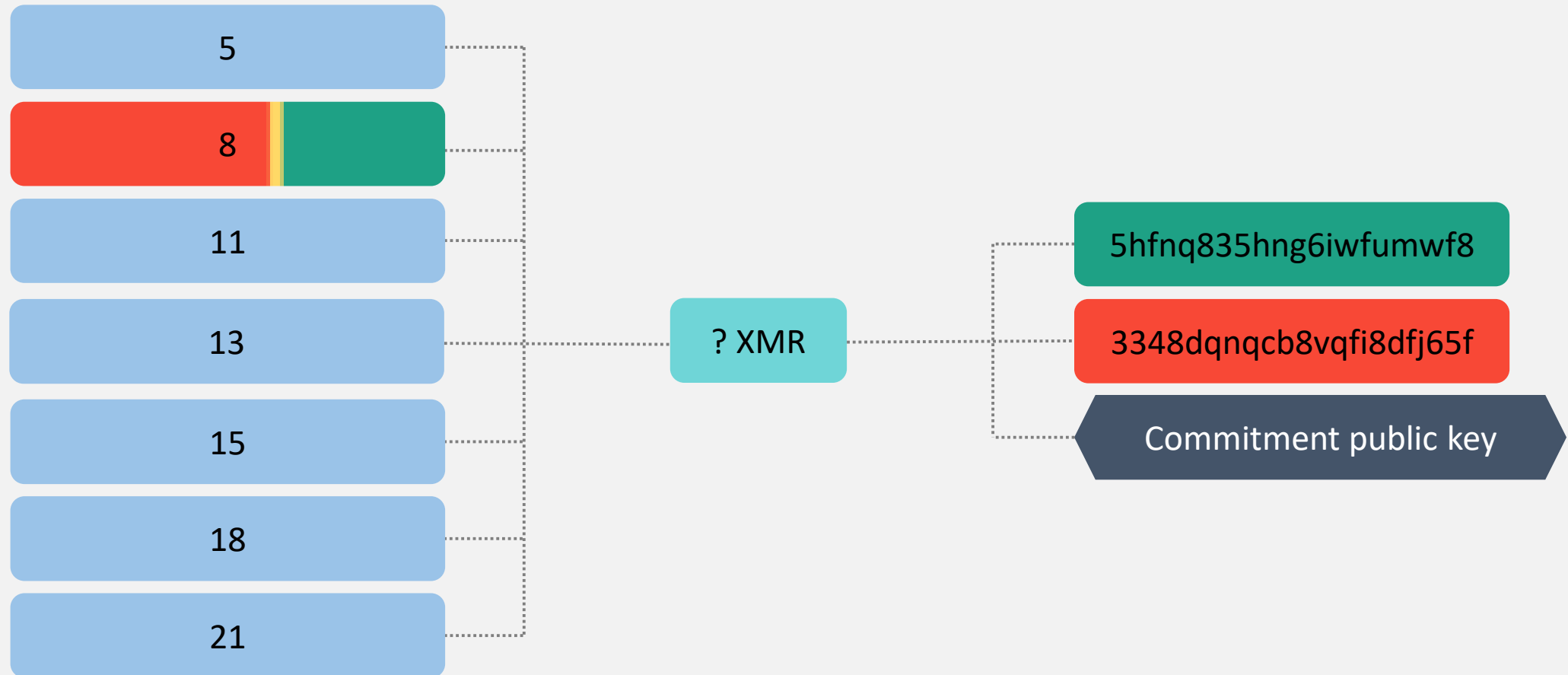
Summary

OUTSIDER VIEW

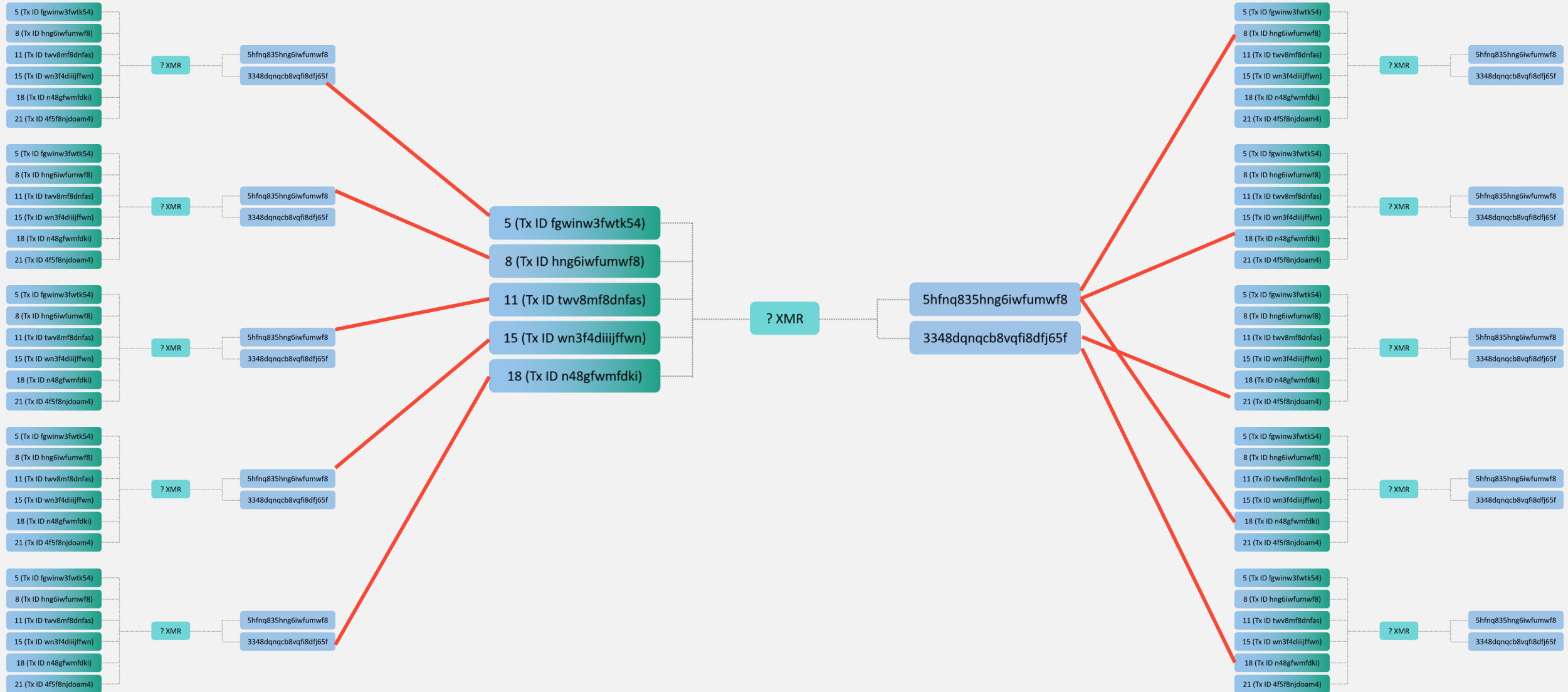


Summary

INSIDER VIEW

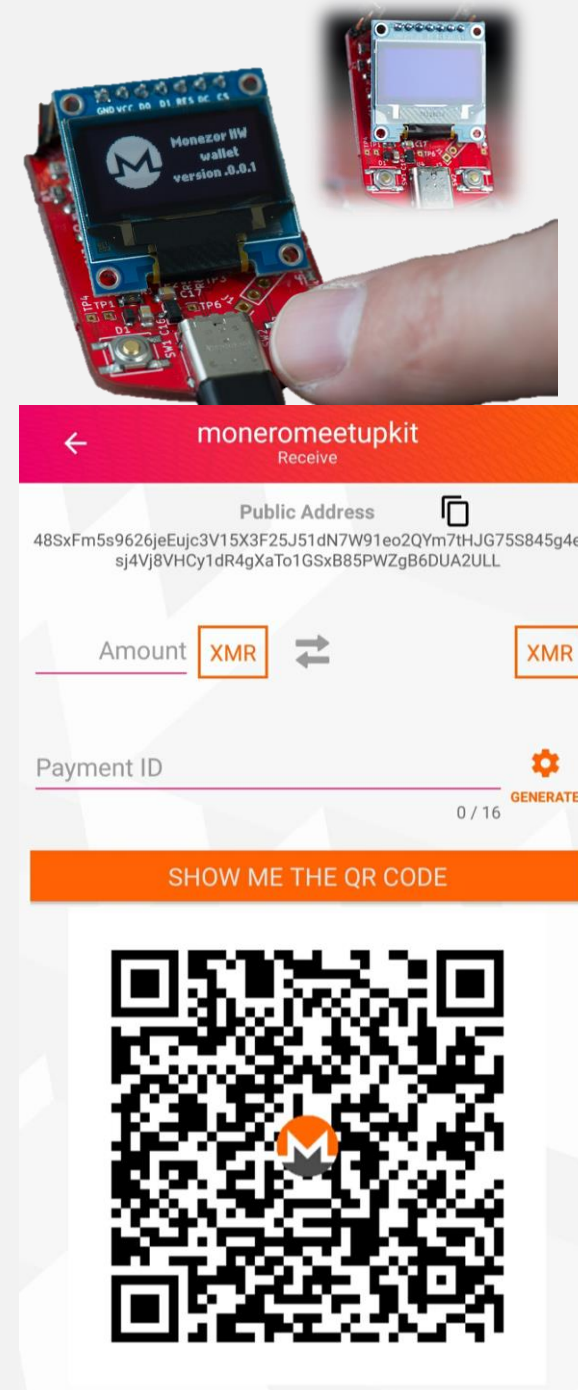
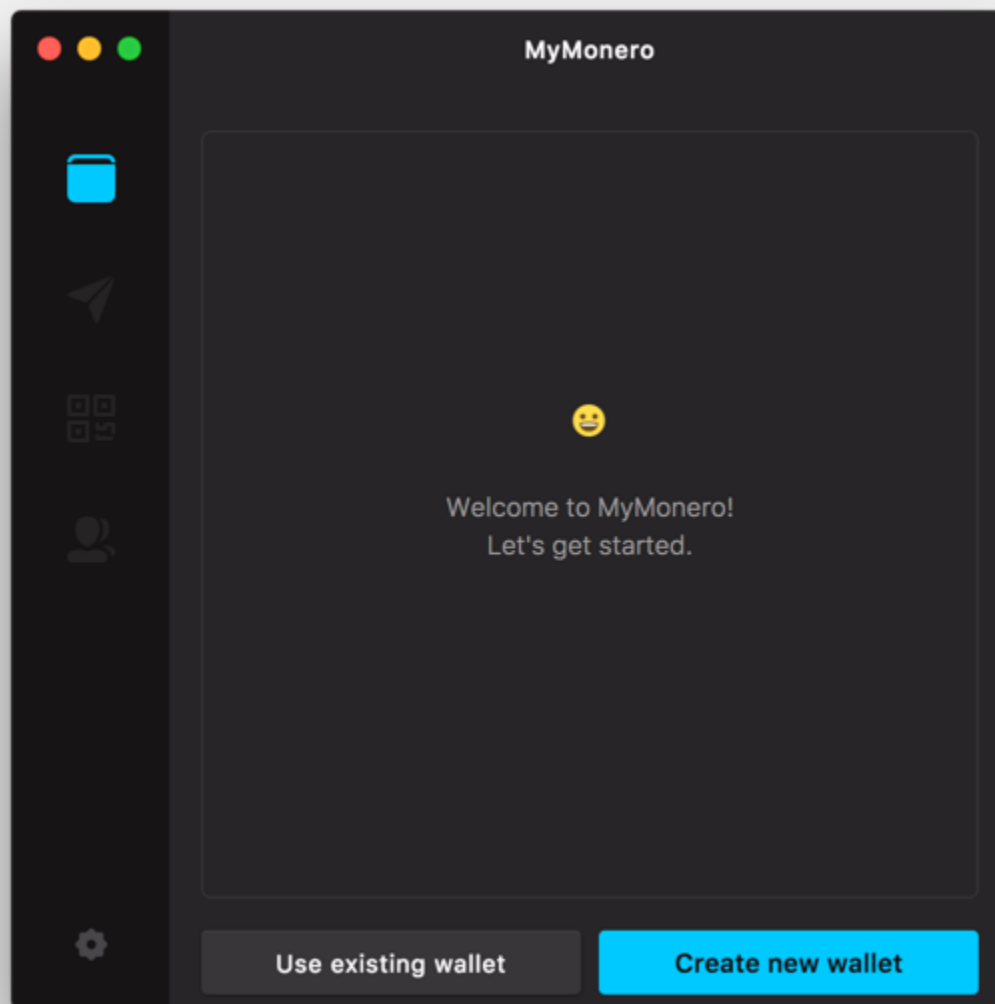
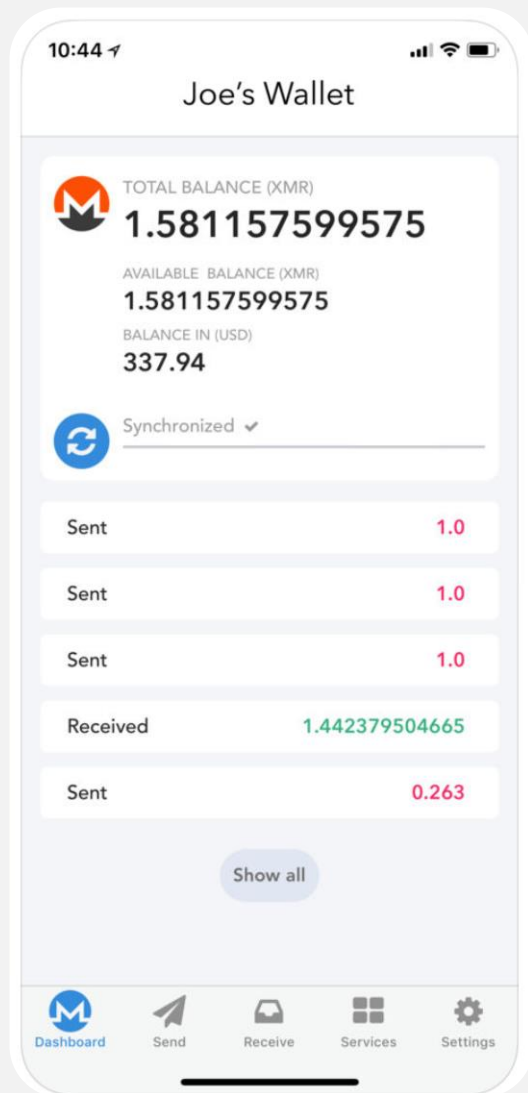


Things Get Complicated Quickly

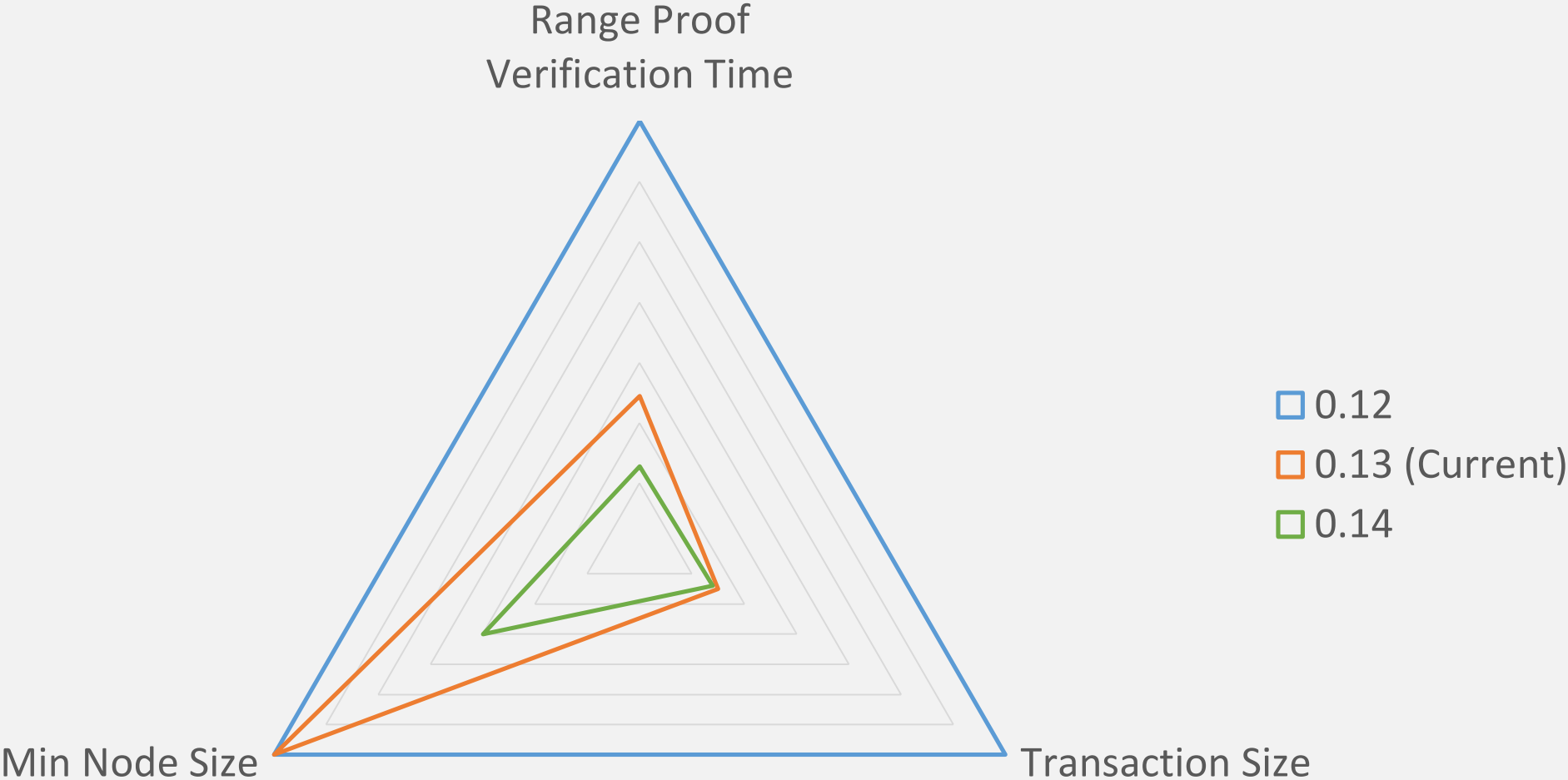


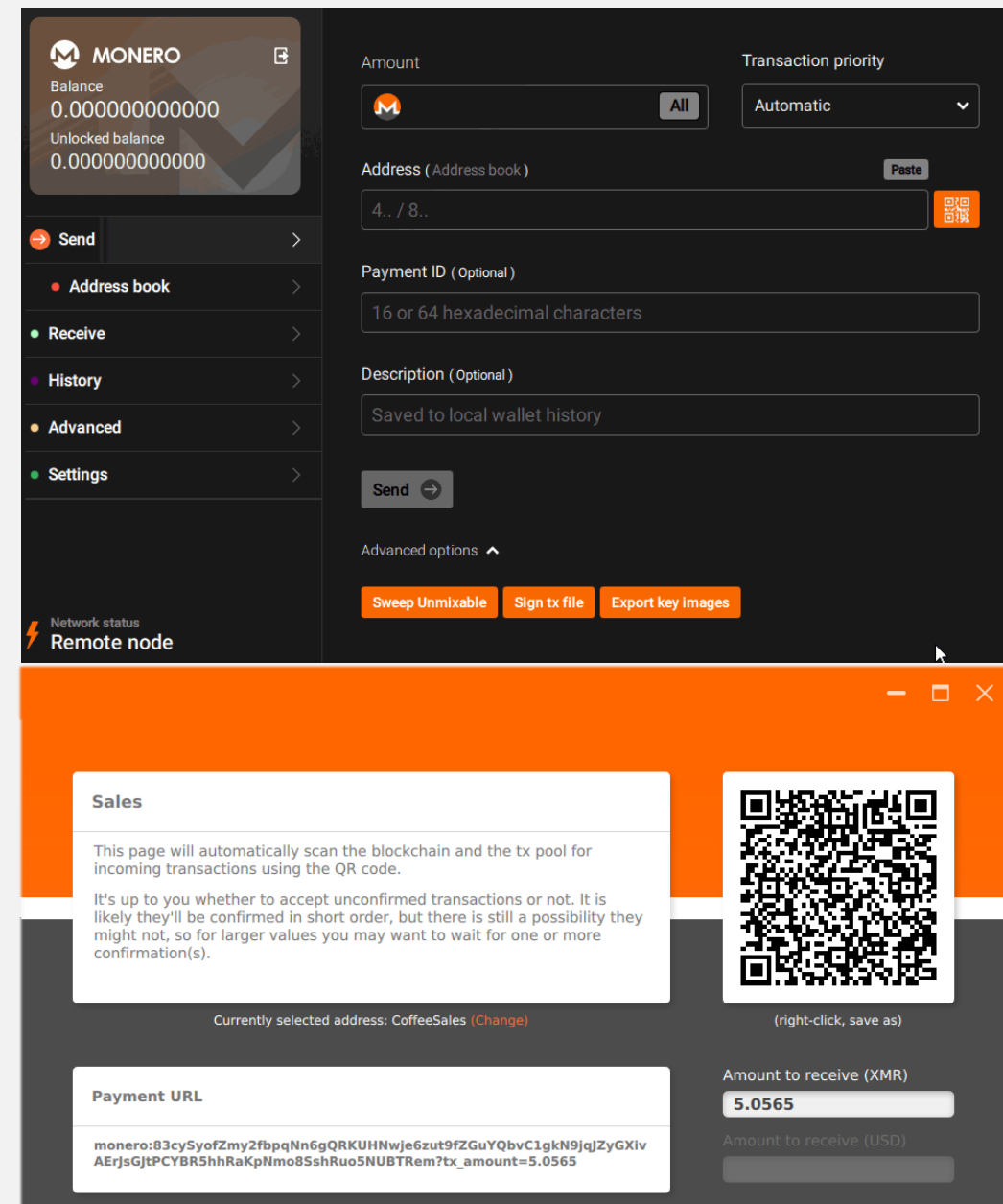
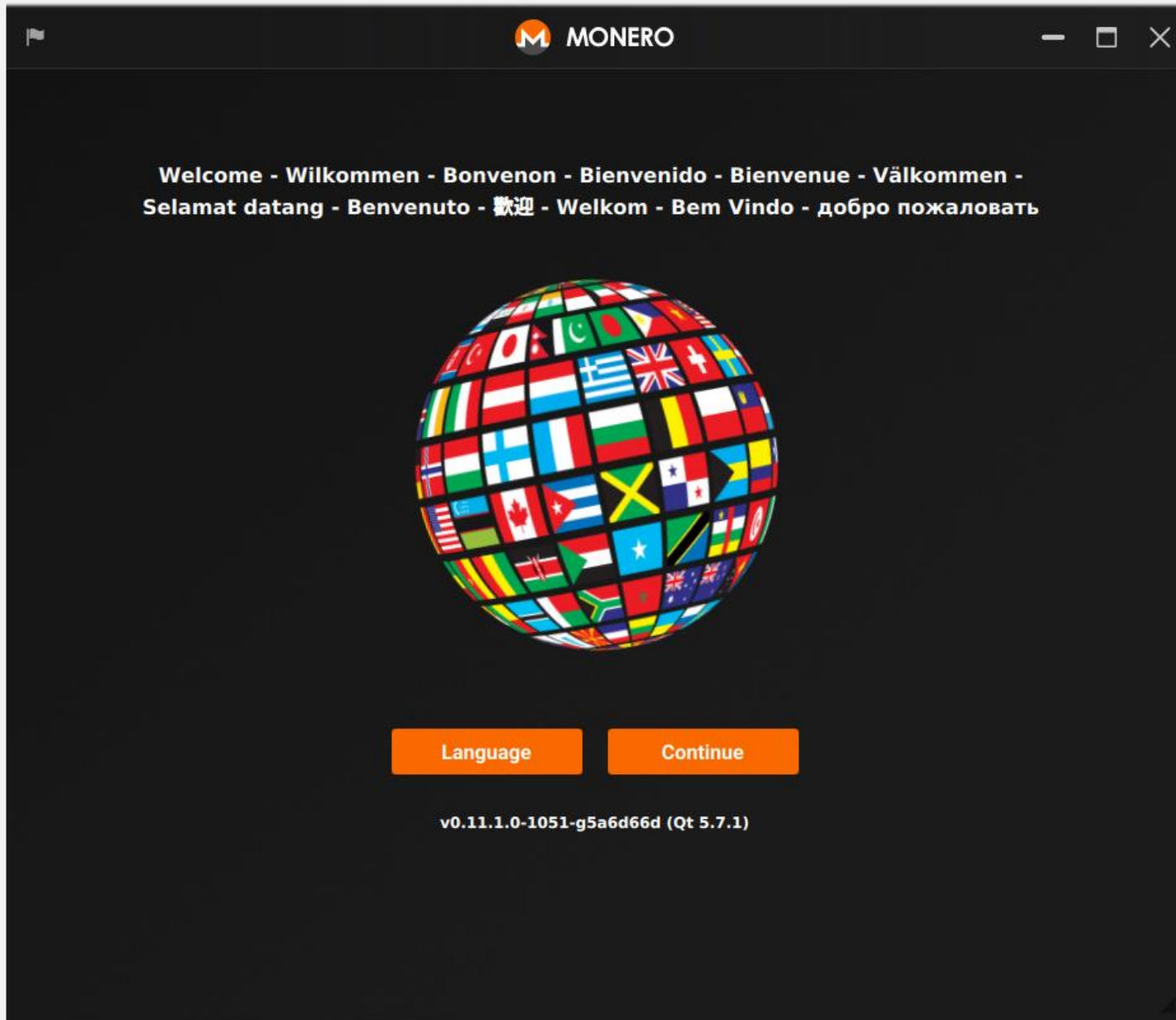


Available Wallets



Efficiency Efficiency Efficiency







Payment IDs Are Terrible

Instant Rate 1 BTC = 330.05076175 XMR

Deposit Min
0.00011854 BTC

Deposit Max
2.49292688 BTC

Liquidity
●●●●○

 → 

Your Monero Address (destination address)

Your Bitcoin Refund Address

Payment Id

☒ I agree to terms

Miner Fee: 0.02 XMR

Start Transaction

Confirm Monero Withdrawal

WITHDRAWAL MONERO

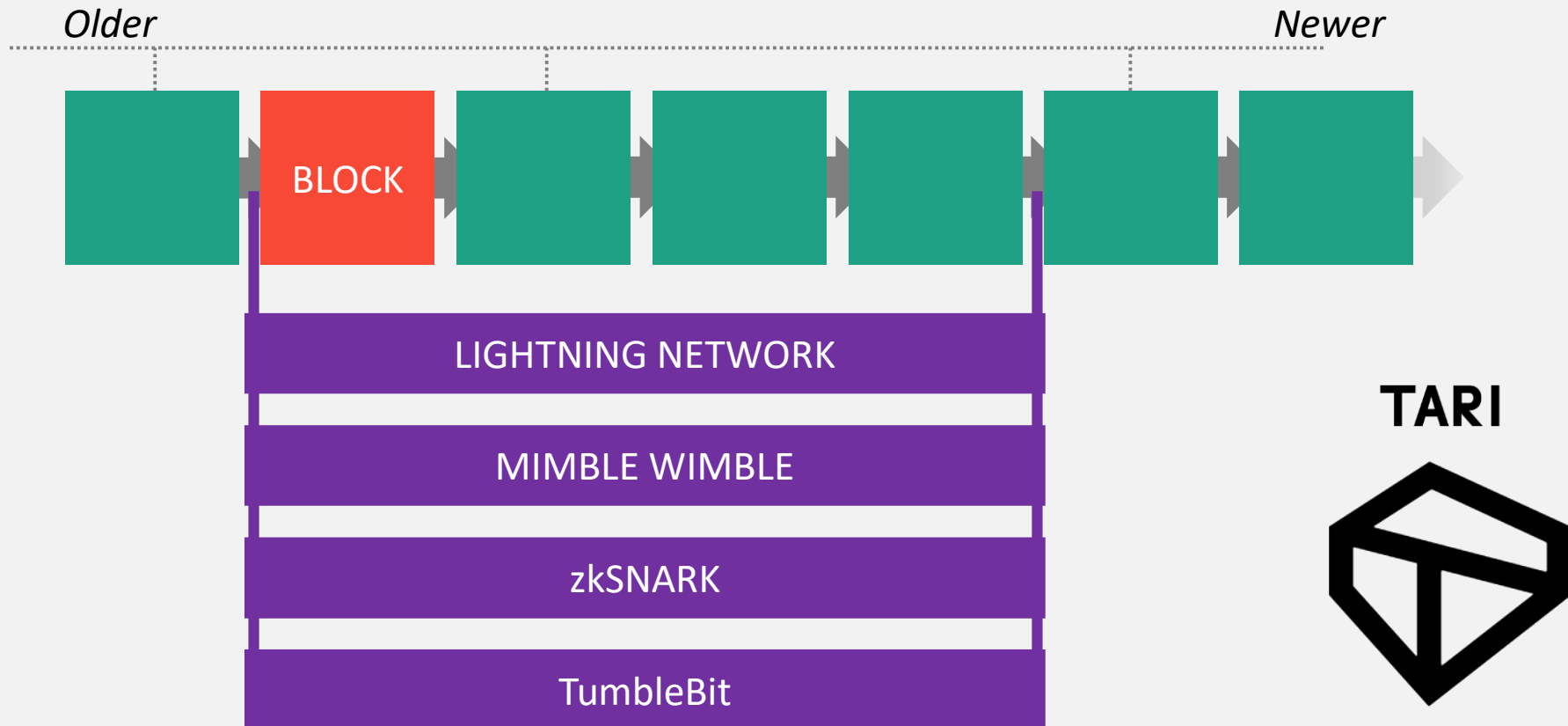
CURRENTLY AVAILABLE: 52.68180402 XMR

Payment_Id	<input type="text"/>	ID
Base Address	<input type="text"/>	ADDR
Quantity	<input type="text" value="0"/>	XMR
Tx Fee	<input type="text" value="0.04000000"/>	XMR
Withdrawal	<input type="text" value="-0.04000000"/>	XMR

Please verify your withdrawal address. We cannot refund an incorrect withdrawal.

Do not withdrawal directly to a crowdfund or ICO. We will not credit your account with tokens from that sale.

Side Chains



Community Crowdfunding System (CCS)

Monero is a decentralized community-driven project, and the CCS is a way for members to get involved and proposals to be funded. To learn more about what it is and what the rules are, [click here](#). To see how to submit your own proposal or idea, [click here](#).



Ideas

If you have an idea for a feature, task, or service, this is the place to pitch it for discussion.



Funding Required

Once a pitched and approved idea has been picked up by a developer or team it goes here for community fundraising.



Work in Progress

Approved ideas that have been picked up and successfully funded are moved here so their progress can be monitored.



Completed Tasks

Once an item has been completed, all milestones met, and all funds paid out, the thread moves here.

XMR.TO – Pay Bitcoin Addresses with Monero

XMR.TO
Pay any Bitcoin address. Truly anonymously.

CREATETRACKFAQAPI

TRACK YOUR ORDER STATUS

Your secret key

xmrto-66429D

Important: save the secret key to track the status of your order.

Order summary

Send 1 BTC to 1GwV7fPX97hmaxc6iNrUZUogmjprLPFoE.
This order amounts to 60.55 XMR.

Your personal rate is
0.01651528 BTC/XMR.

Current status

Please pay your order in the next:

14 MINUTES, AND 49 SECONDS

Why Monero?



Thank You!



getmonero.org



[/r/Monero](https://www.reddit.com/r/Monero)



monero.stackexchange.com



justin@ehrenhofer.org