

SECURE. PRIVATE. UNTRACEABLE.



MONERO

Wroclaw, Poland



Welcome

Justin Ehrenhofer

Finance
Management Information Systems

/u/SamsungGalaxyPlayer or sgp_



UNIVERSITY OF MINNESOTA
Driven to DiscoverSM



CryptoUMN.com

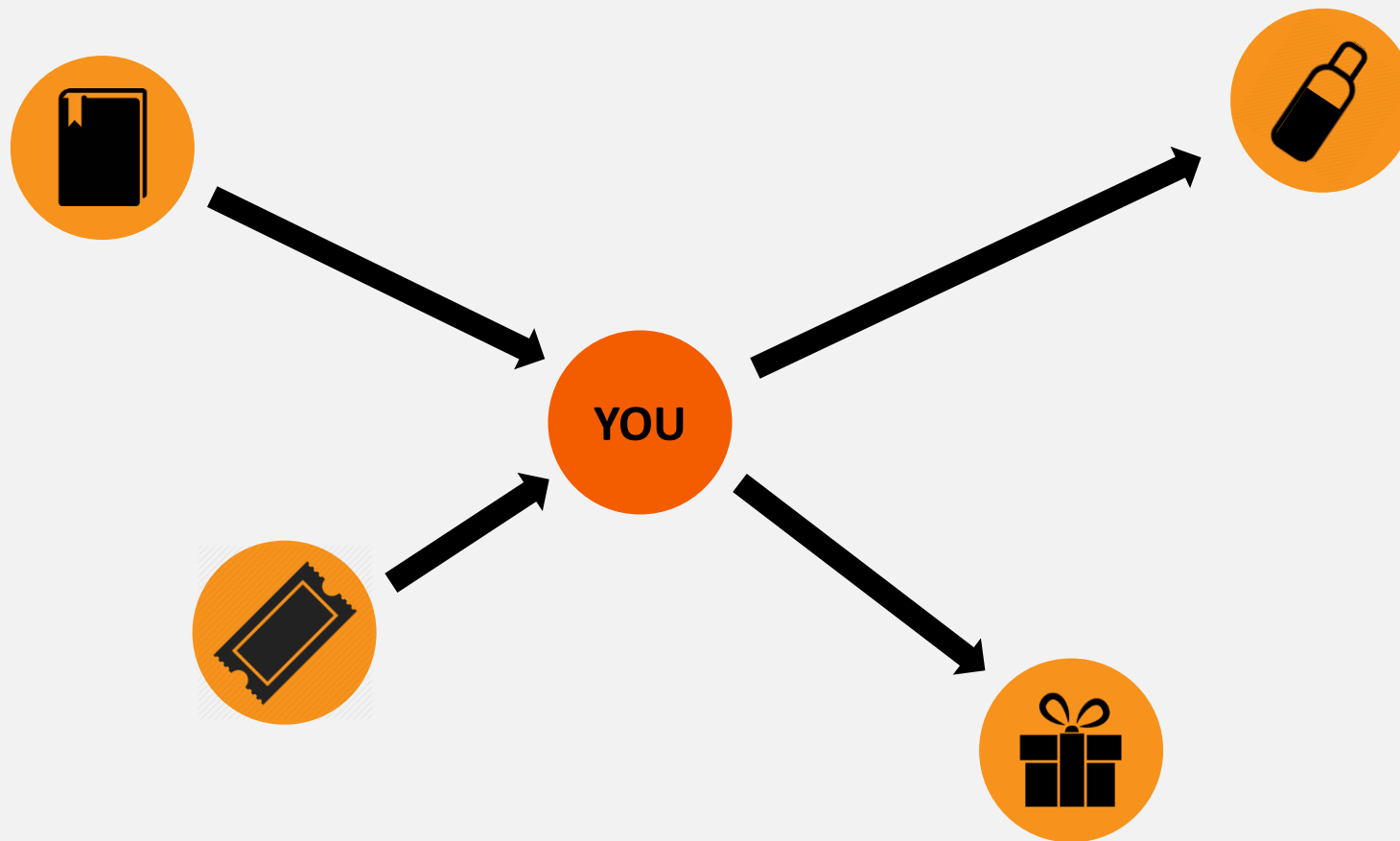
Fungibility



=

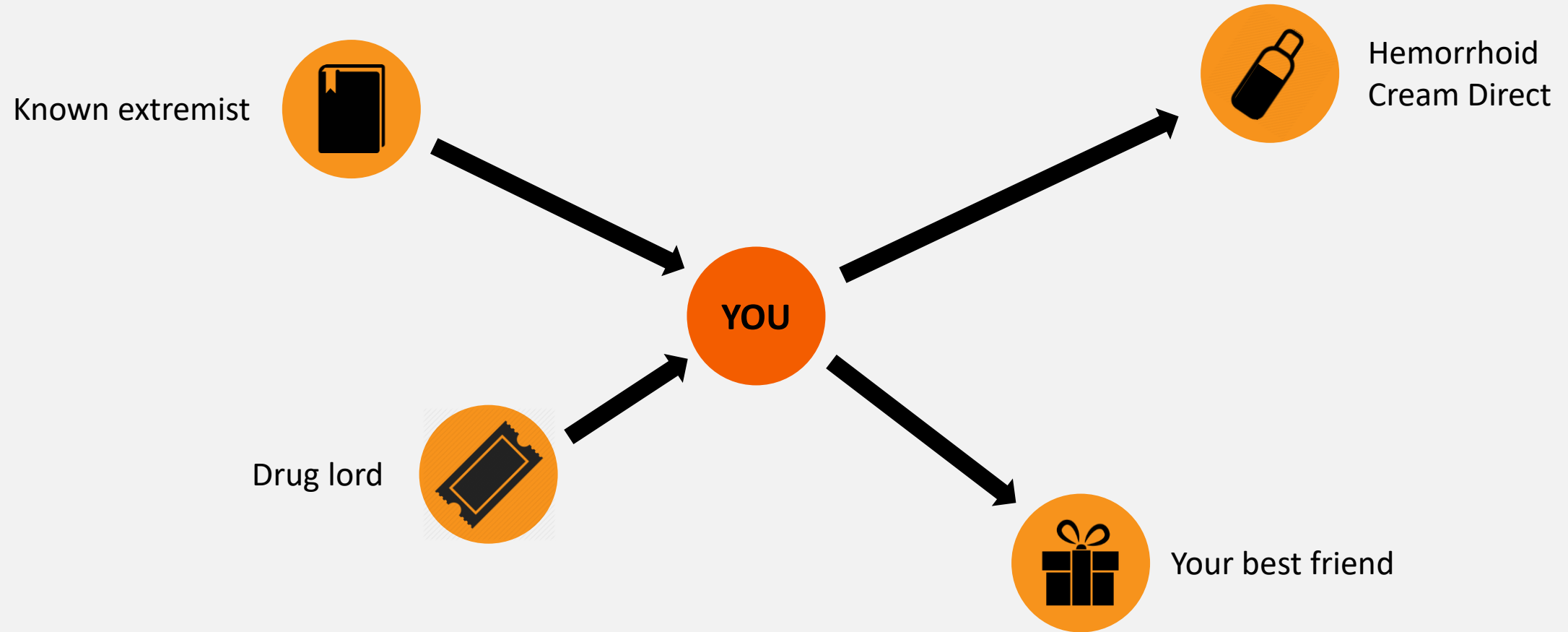


Why Fungibility Matters

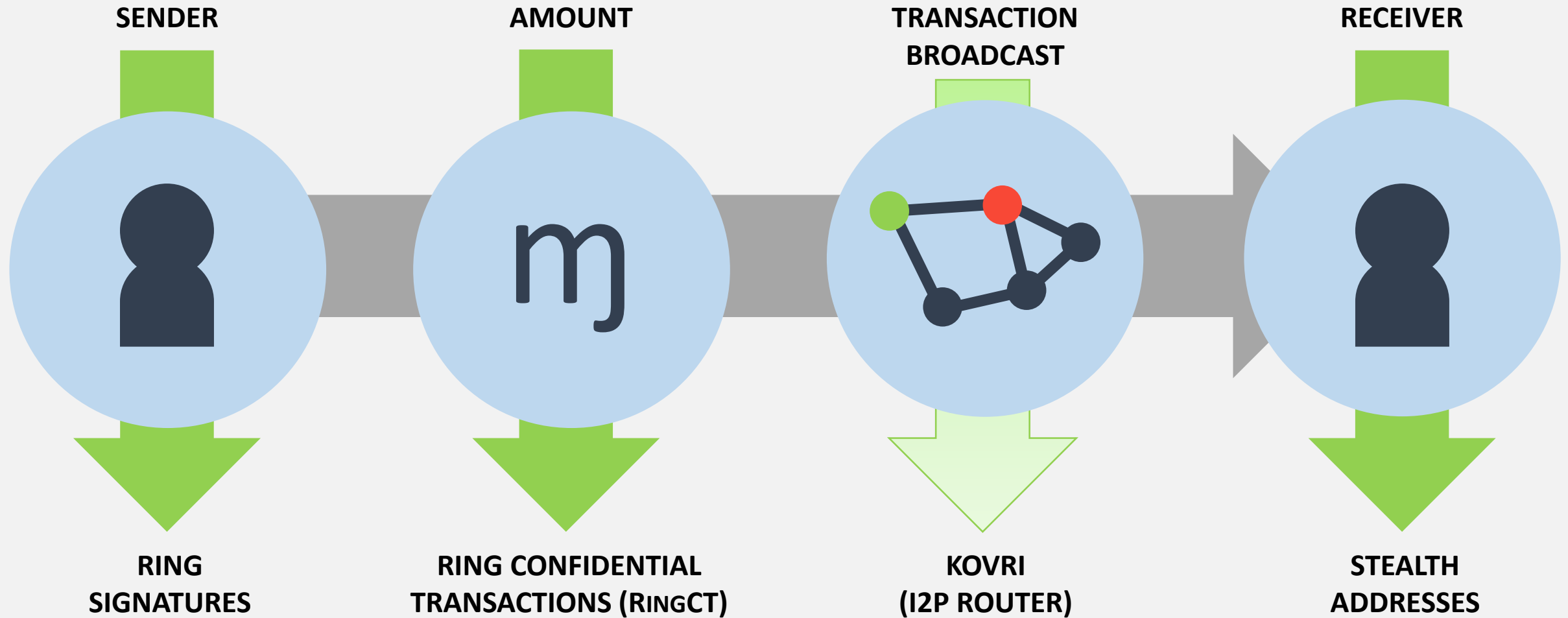


Adapted from Keybase.io

Why Fungibility Matters



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)

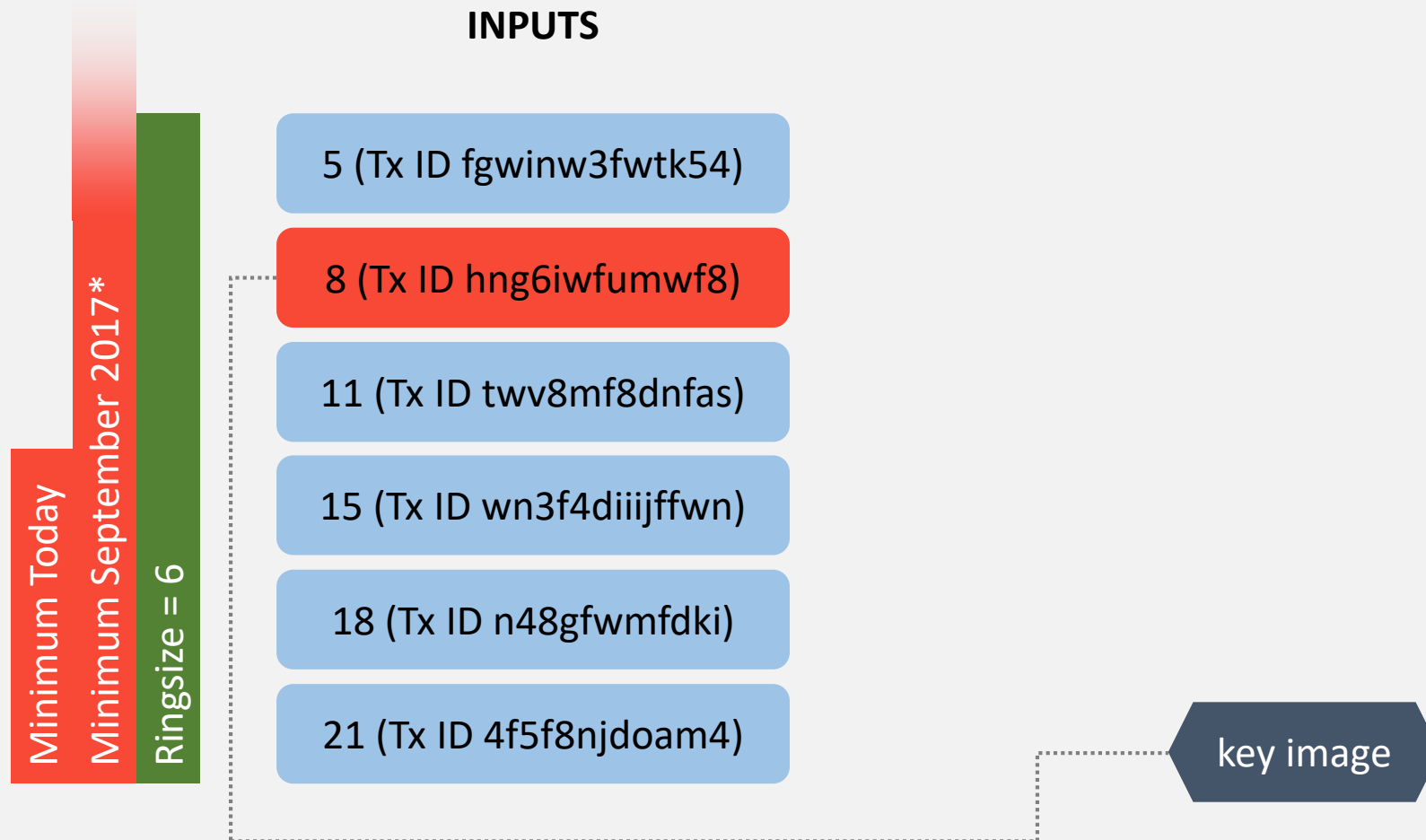
20 (Tx ID t4vn8lf8djer4)

7 (Tx ID e4bgn8flwwrj8)

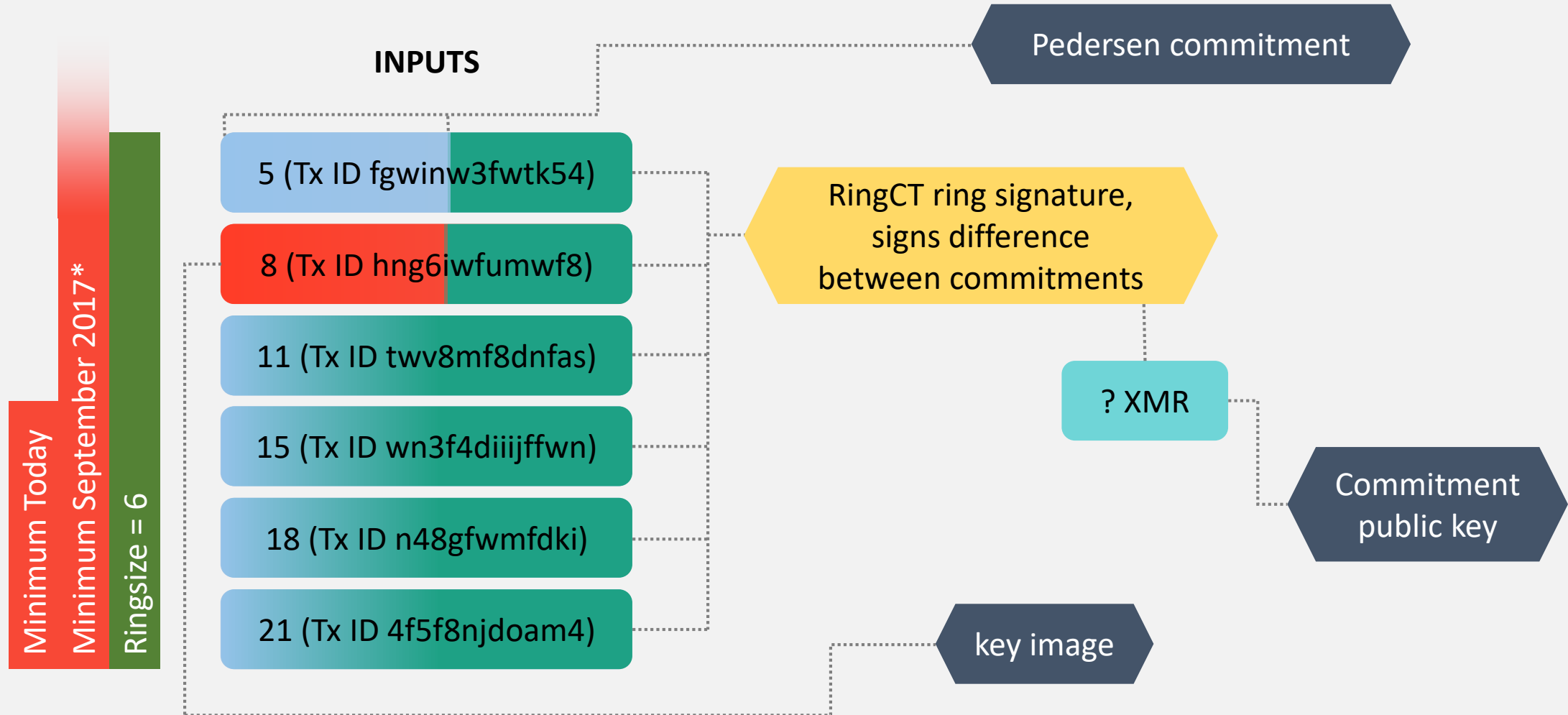
14 (Tx ID f8n8madkrjmd)

21 (Tx ID 4f5f8njdoam4)

Ring Signatures & RingCT

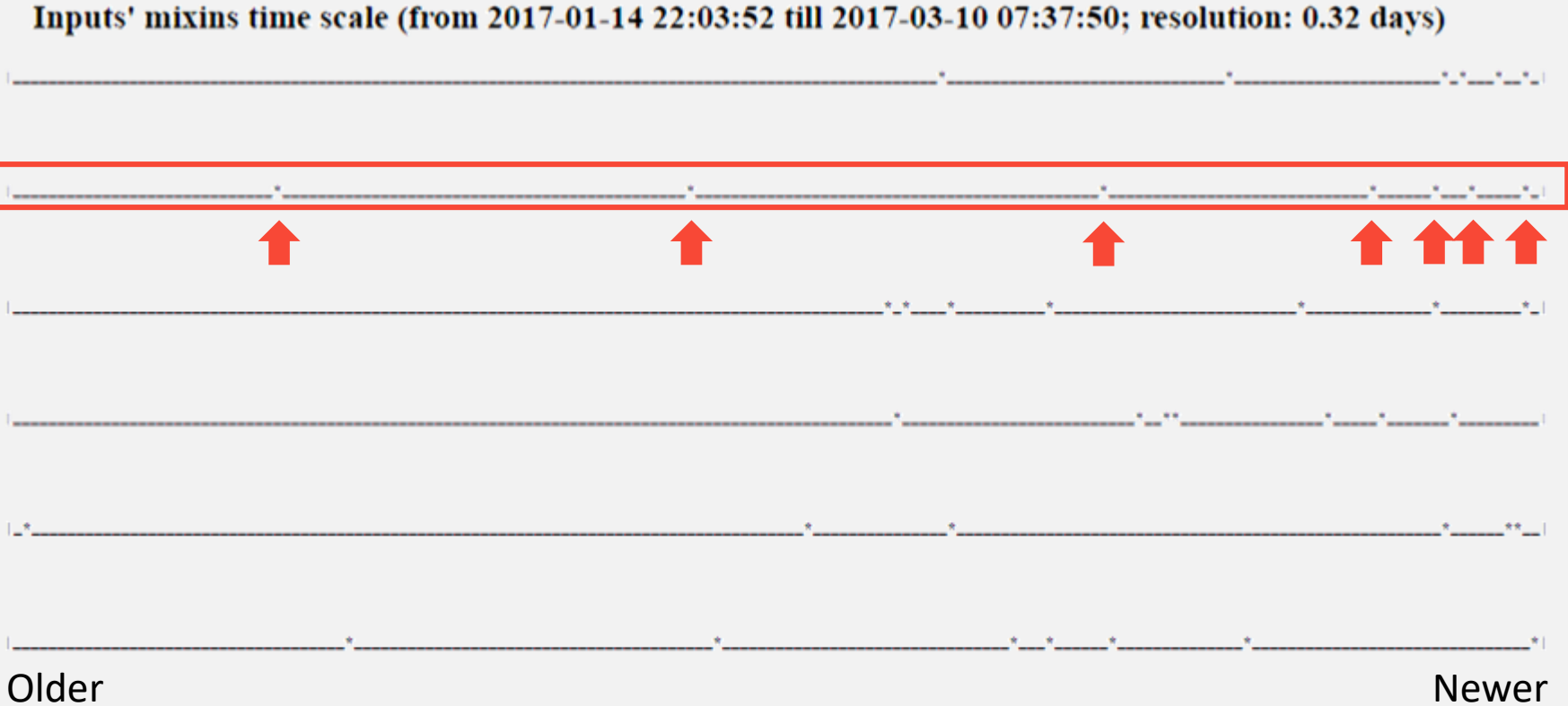
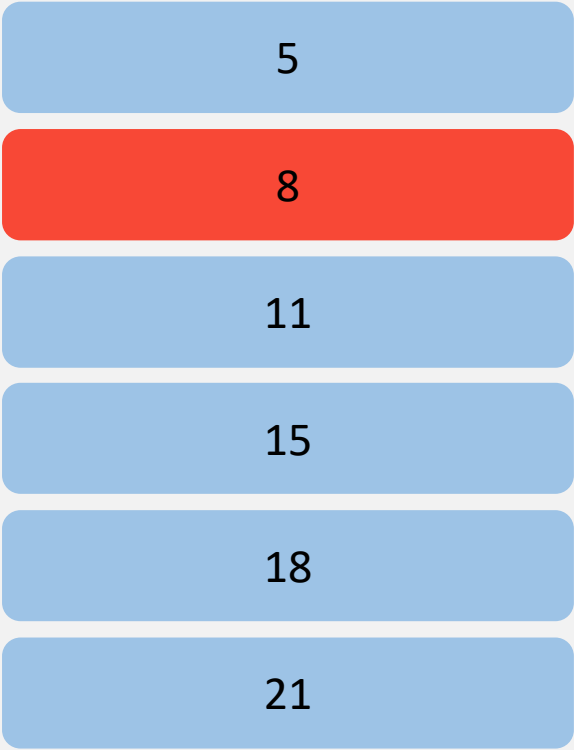


Ring Signatures & RingCT



Ring Signatures & RingCT

INPUTS

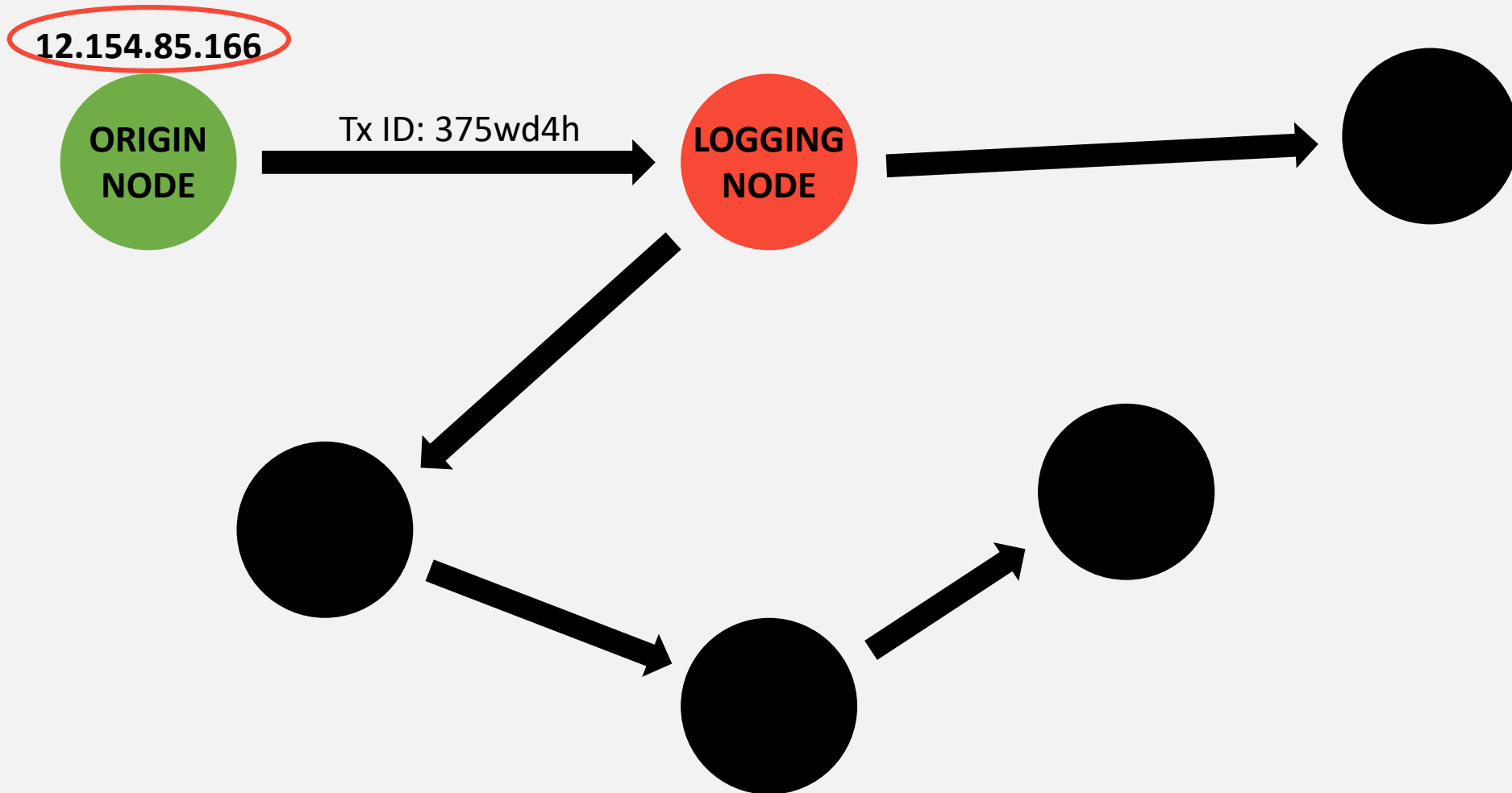


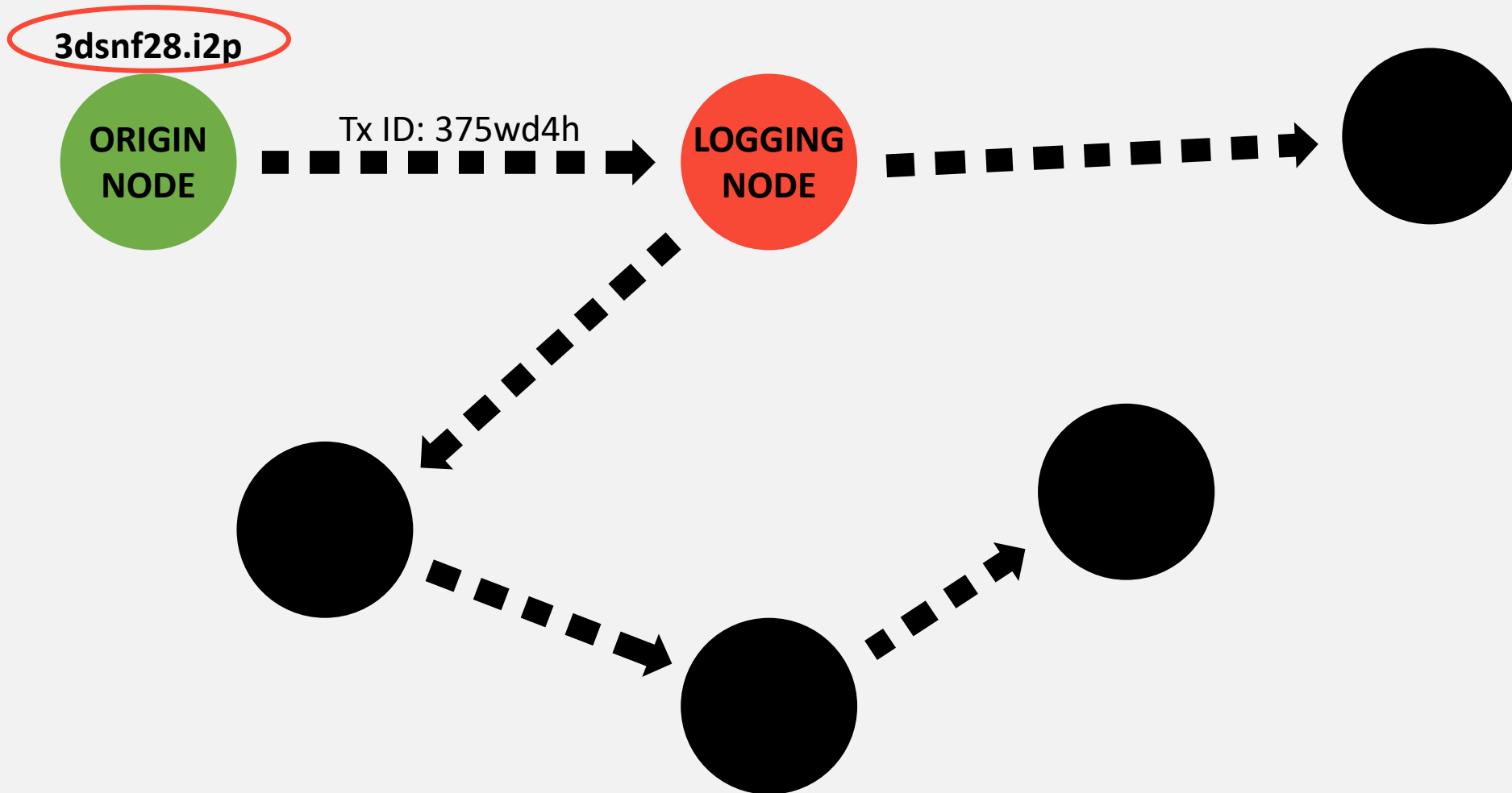
Ring Signatures & RingCT

date	non ringct	ringct	ratio
2017-03-06	0	1944	100%
2017-03-05	0	2065	100%
2017-03-04	1	1859	99.95%
2017-03-03	2	2634	99.92%
2017-03-02	0	2579	100%
2017-03-01	0	2643	100%
2017-02-28	0	2446	100%
2017-02-27	1	2507	99.96%

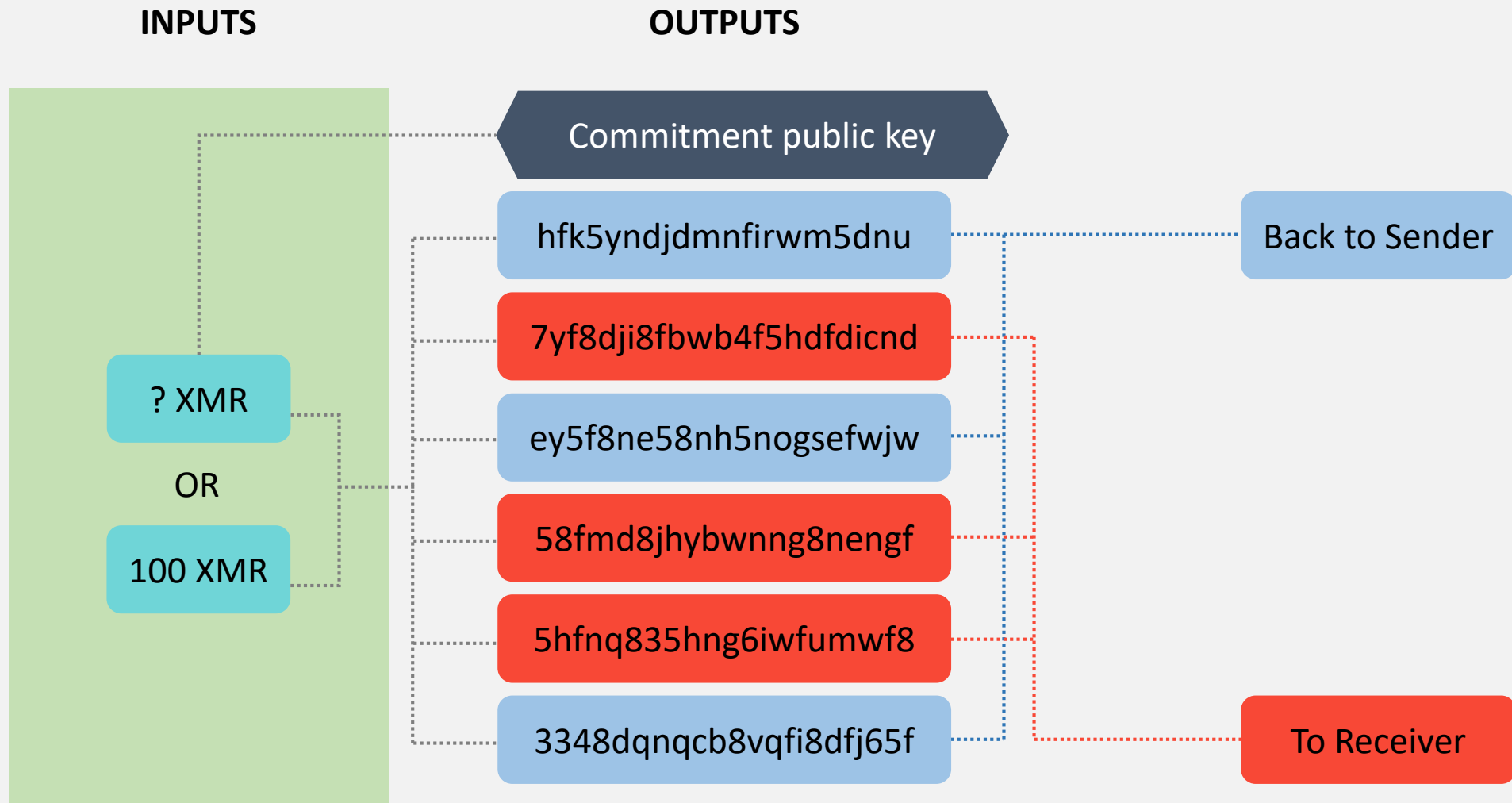
Near 100% use of
optional RingCT

Source: moneroblocks.info/stats

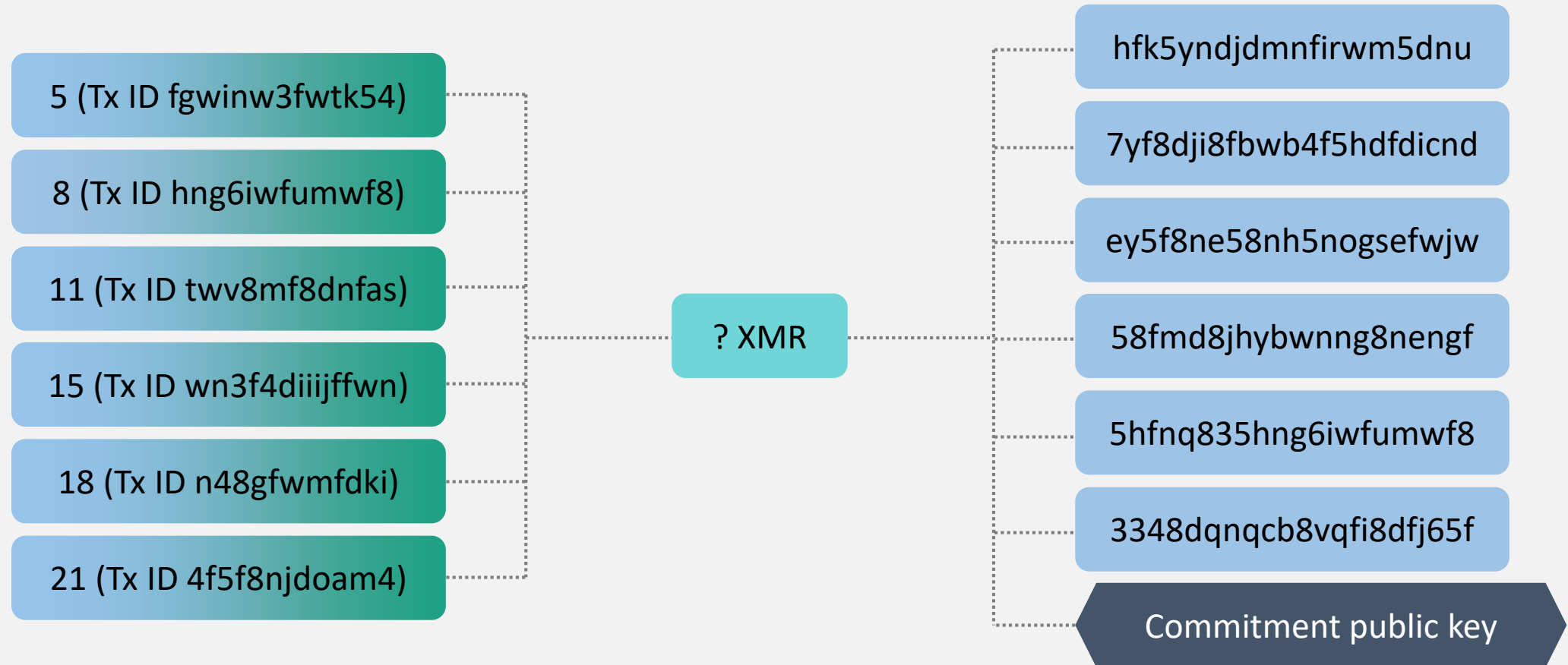




Stealth Addresses



Summary

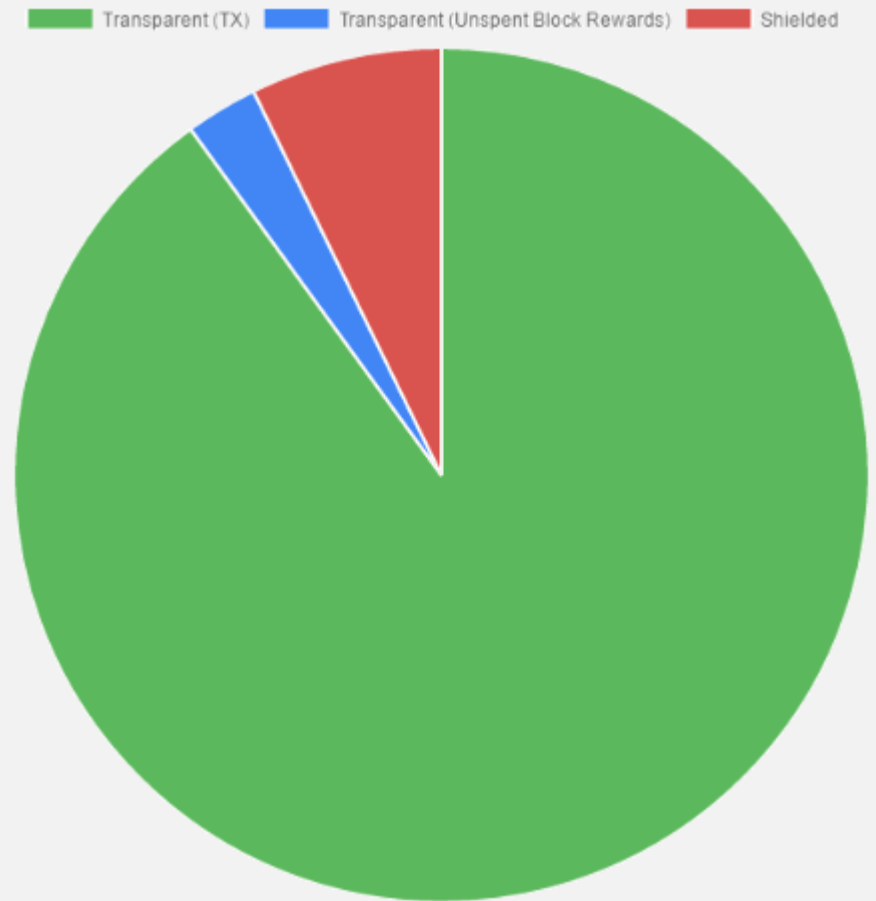


Mandatory Privacy

mixins used in transactions (%)

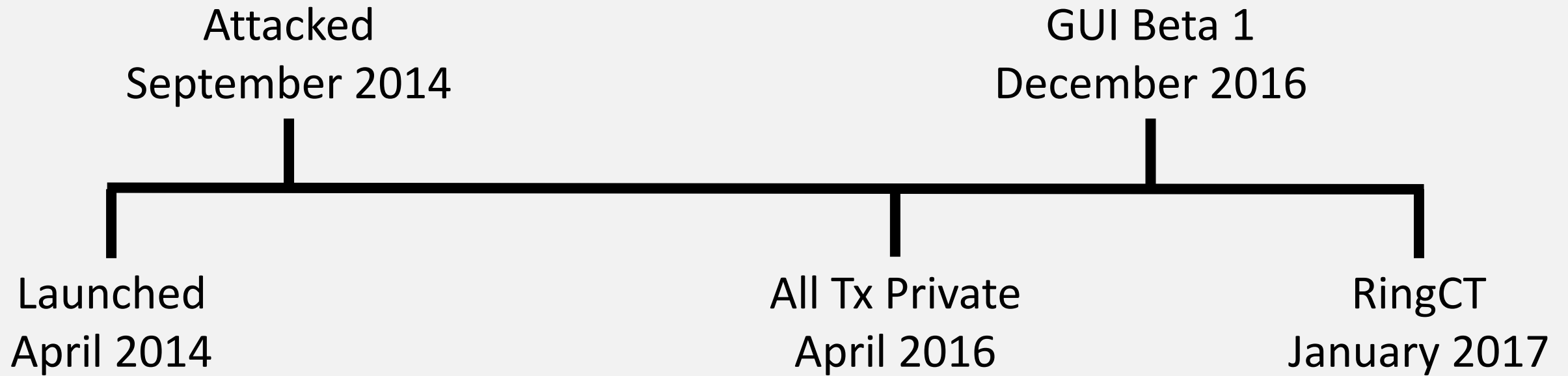
mixin:	none :(1 - 2	3 - 9
last day	66.74	10.95	20.25
last week	66.11	6.96	24.76
last month	64.47	5.42	28.13
last year	73.04	7.36	18.16

Source: MoneroBlocks.info 24 Feb 2016



Source: zcha.in 15 March 2017

A Brief History



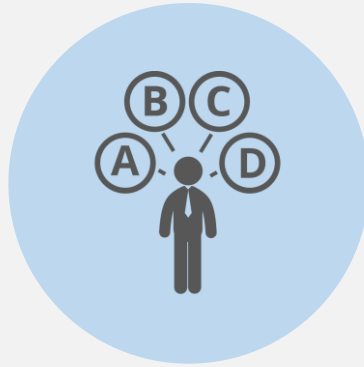
Regulatory Compliance and Transparency

(with the View Key)



Transparency

A view key is used to reveal all transactions for a Monero account, or just the key for a single transaction



Selected Parties

View keys can be given to selected parties, or can be made public



Auditing

Auditors can be given access to accounts without being able to spend those account funds



Charities

By publishing their view key, charities can invite easy public oversight



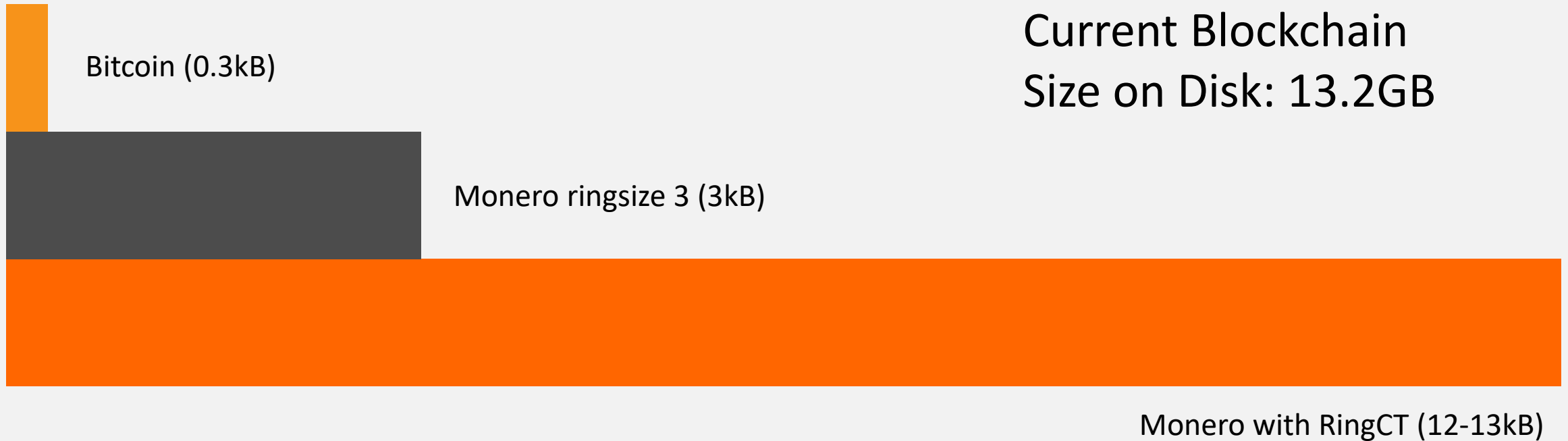
Parents

Children can be given their own accounts, and parents can monitor their spending

Monero Limitations



Monero Limitations



Addressing Transaction Size



1. RingCT is brand new; optimizations could reduce transaction sizes by 20%
2. Prune non-essential parts of blockchain for 50% size reduction. Sharding possible
3. Large hard drives are cheap, and prices continue to fall (even if it can't meet Moore's Law)
4. Any real scaling needs to be done off-chain anyway

Ongoing Development



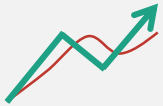
Multisig



Sub-Addresses &
Disposable Addresses



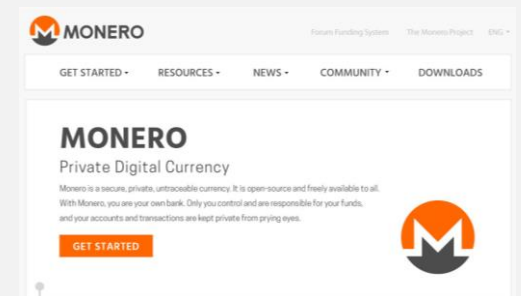
Translations



Improvements to
Dynamic Fees &
Dynamic Blocks

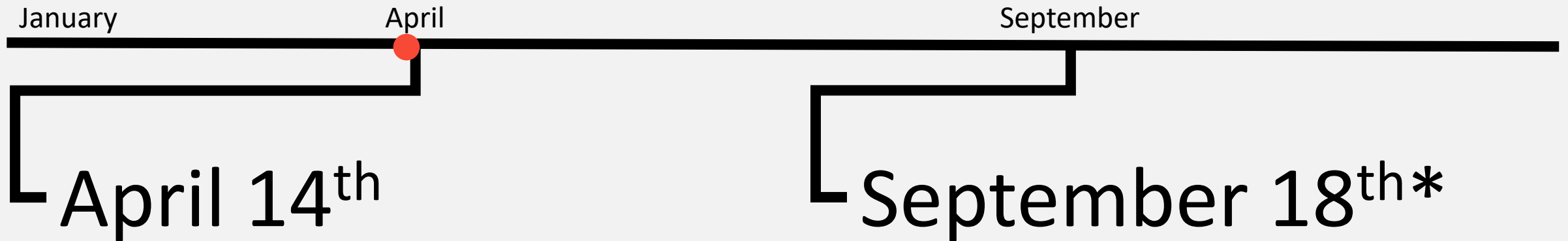


Lightweight
Wallet



Website
Redesign

Hardfork Schedule



- **Dynamic Block Improvements**
- **Dynamic Fee Improvements**

- **Mandatory RingCT**
- **Minimum ringsize ≥ 5**
- Fluffy blocks
- Wallet sync optimizations
(prefetch and resource allocation)

Thank You!



getmonero.org



/r/Monero



monero.stackexchange.com

People Started Adding Tools to Bitcoin

