SECURE. PRIVATE. UNTRACEABLE.

MONERO

Warsaw, Poland

Welcome

Justin Ehrenhofer

Finance
Management Information Systems

/u/SamsungGalaxyPlayer or sgp_

WU
WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

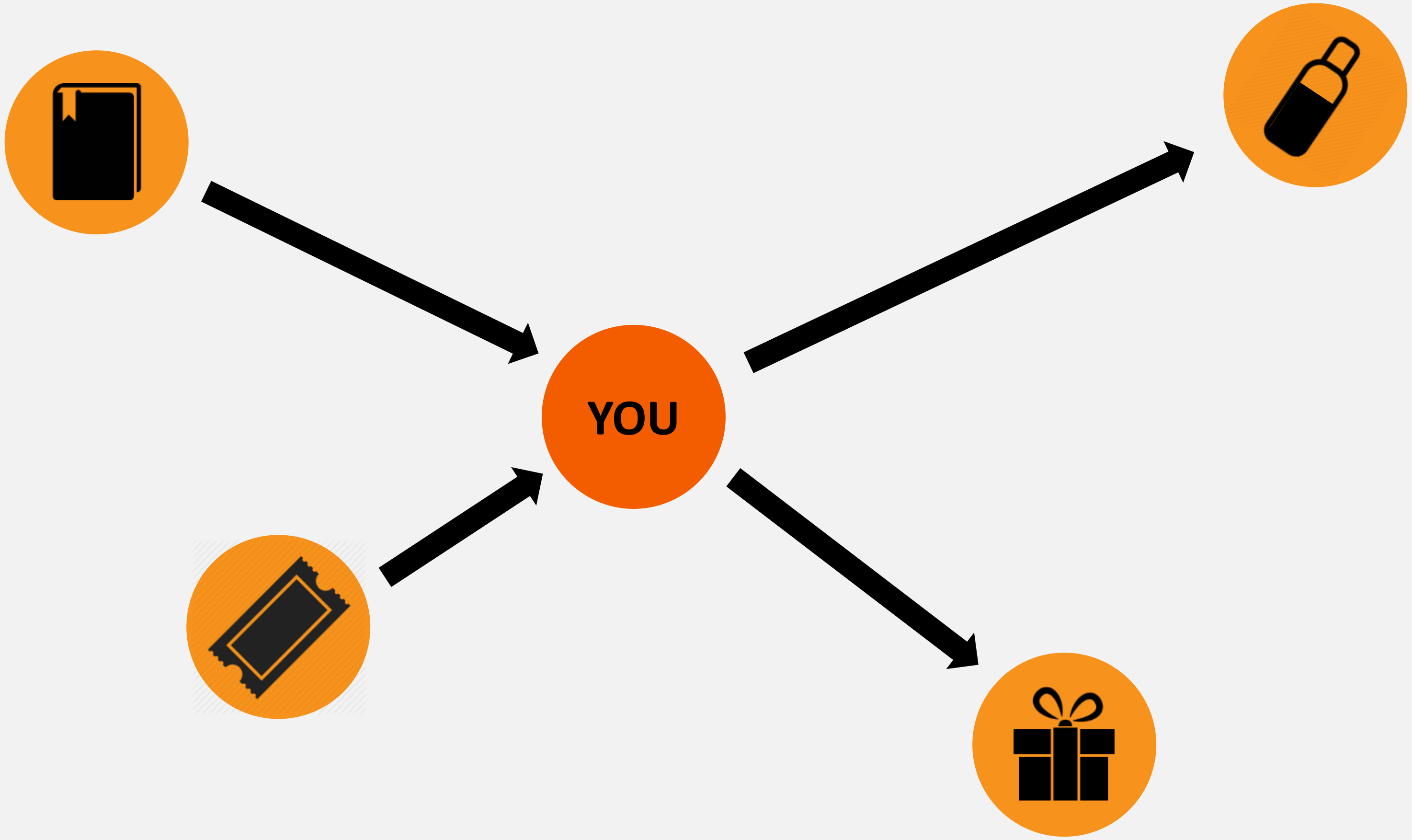
UNIVERSITY OF MINNESOTA
Driven to Discover℠

CryptoUMN.com

Fungibility

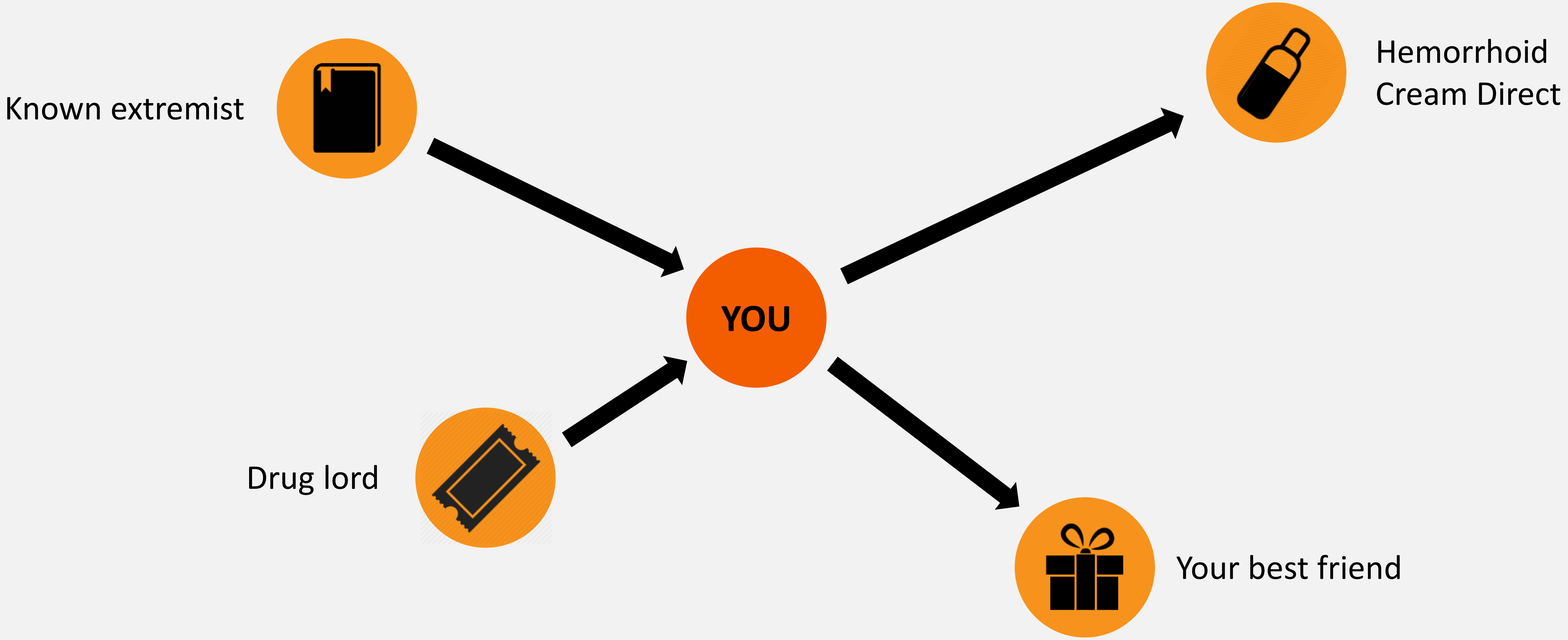
=

Why Fungibility Matters



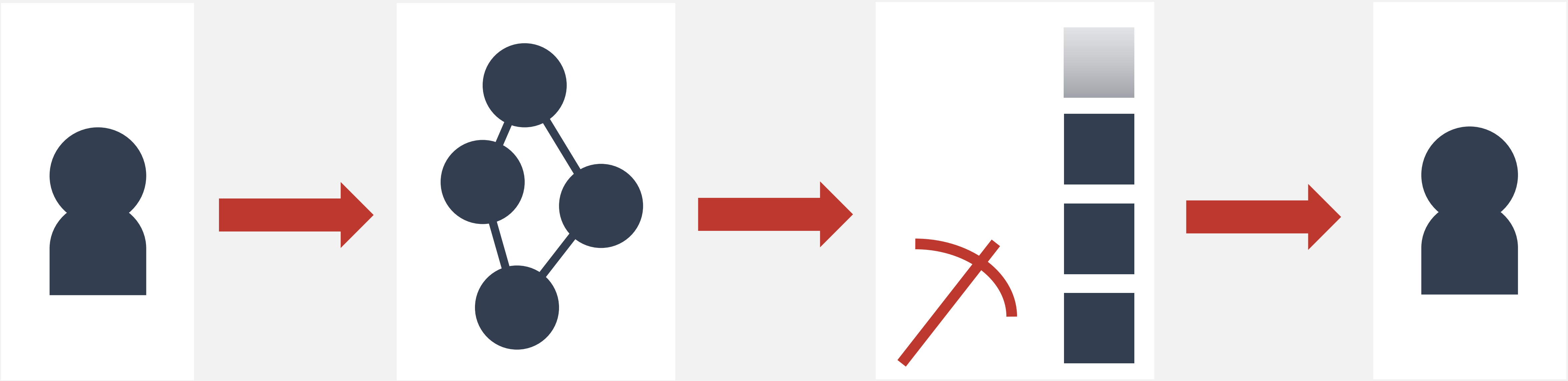
Adapted from Keybase.io

Why Fungibility Matters



Adapted from Keybase.io

Bitcoin Crash Course



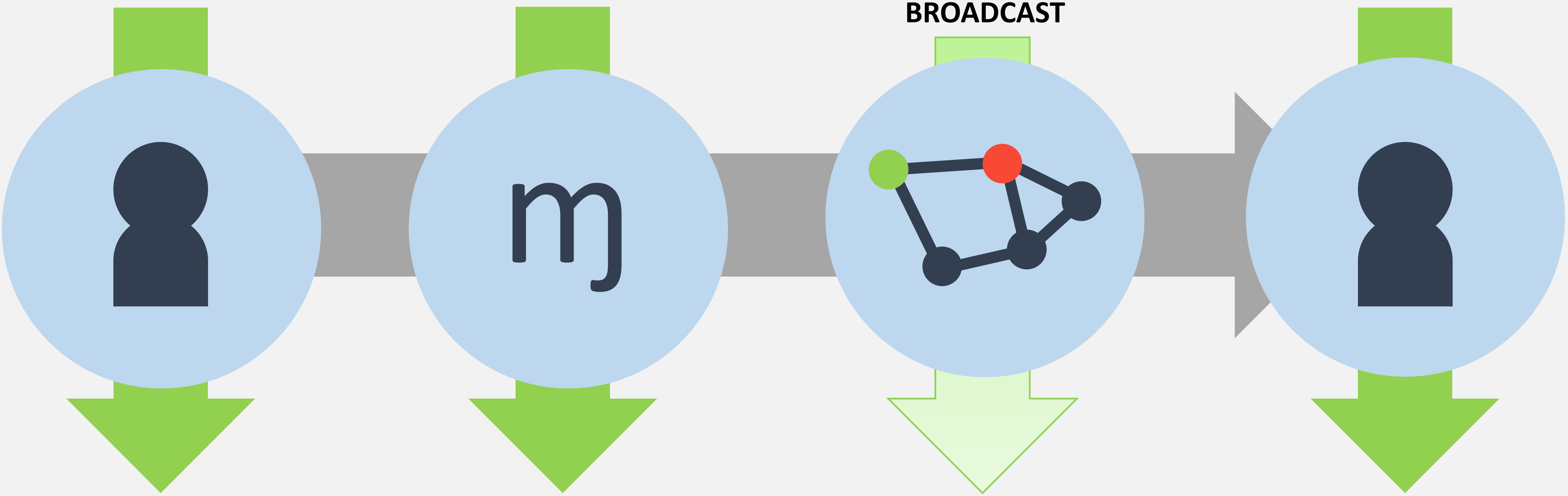
SENDER

TRANSACTION
BROADCAST

ADDED TO
BLOCKCHAIN
BY MINING

RECEIVER

The Monero Difference



SENDER

RING SIGNATURES

AMOUNT

RING CONFIDENTIAL TRANSACTIONS (RingCT)

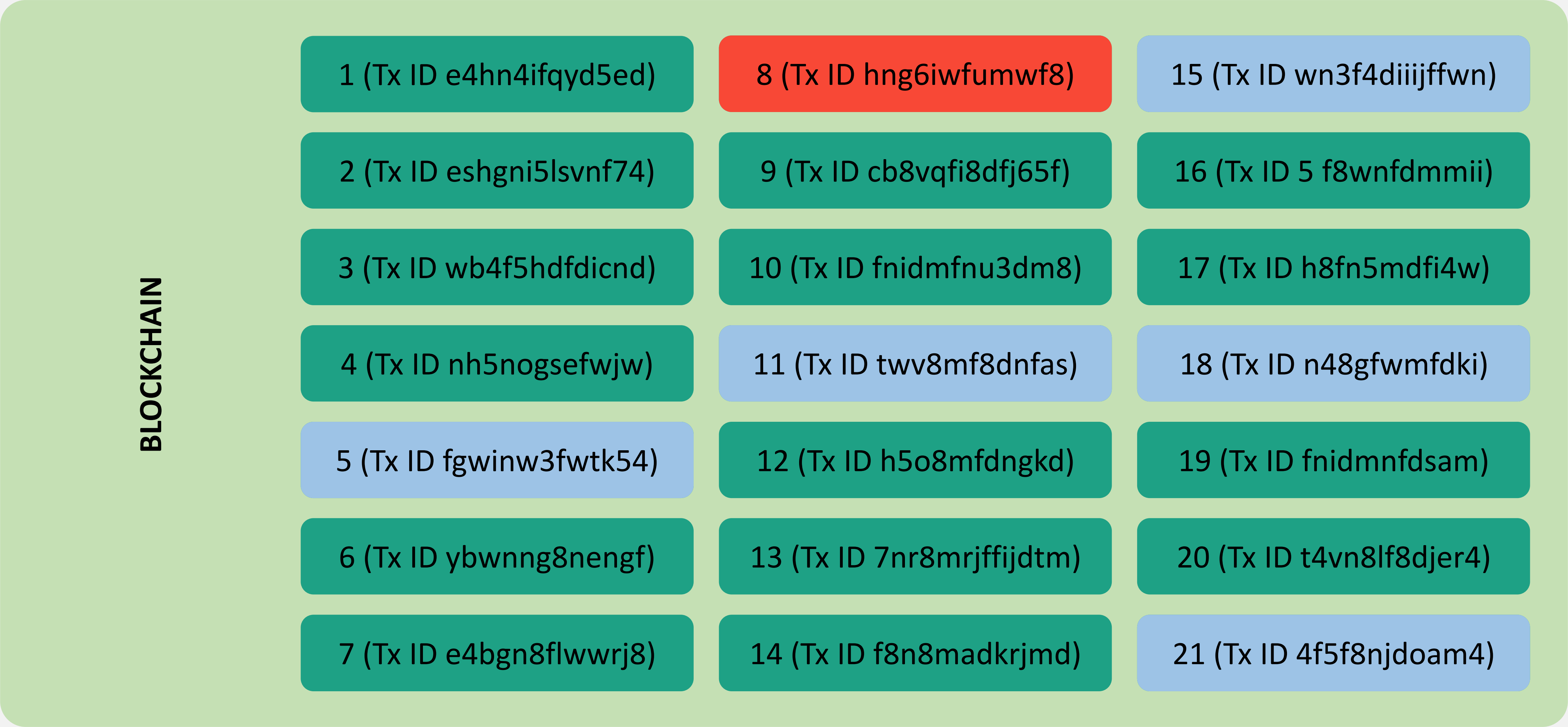
TRANSACTION BROADCAST

KOVRI (I2P ROUTER)

RECEIVER

STEALTH ADDRESSES

Ring Signatures & RingCT



BLOCKCHAIN

1 (Tx ID e4hn4ifqyd5ed)

2 (Tx ID eshgni5lsvnf74)

3 (Tx ID wb4f5hdfdicnd)

4 (Tx ID nh5nogsefwjw)

5 (Tx ID fgwinw3fwtk54)

6 (Tx ID ybwnng8nengf)

7 (Tx ID e4bgn8flwwrj8)

8 (Tx ID hng6iwfumwf8)

9 (Tx ID cb8vqfi8dfj65f)

10 (Tx ID fnidmfnu3dm8)

11 (Tx ID twv8mf8dnfas)

12 (Tx ID h5o8mfdngkd)

13 (Tx ID 7nr8mrjffijdtm)

14 (Tx ID f8n8madkrjmd)

15 (Tx ID wn3f4diiijffwn)

16 (Tx ID 5 f8wnfdmmii)

17 (Tx ID h8fn5mdfi4w)

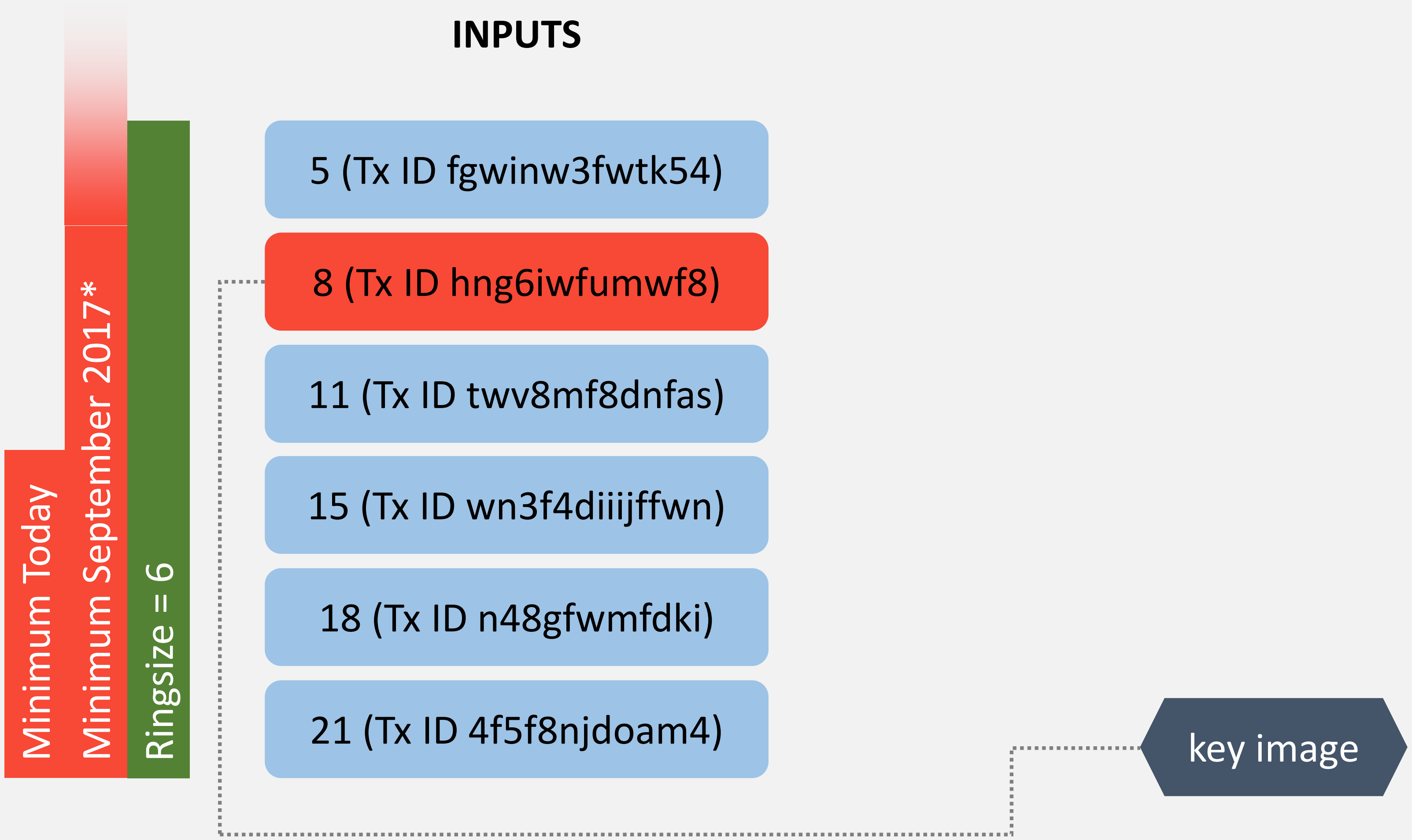
18 (Tx ID n48gfwmfdki)

19 (Tx ID fnidmnfdsam)

20 (Tx ID t4vn8lf8djer4)

21 (Tx ID 4f5f8njdoam4)

Ring Signatures & RingCT



INPUTS

5 (Tx ID fgwinw3fwtk54)

8 (Tx ID hng6iwfumwf8)

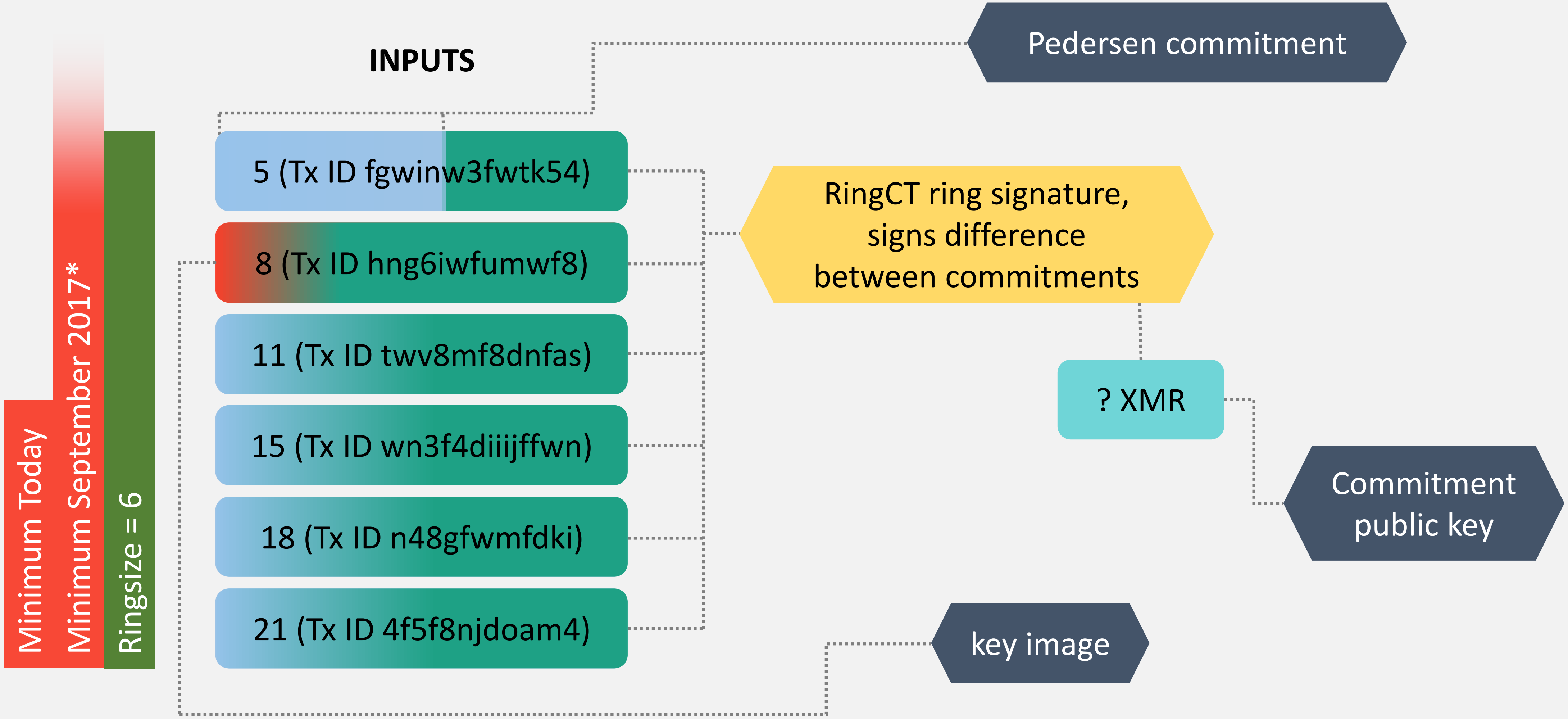
11 (Tx ID twv8mf8dnfas)

15 (Tx ID wn3f4diiijffwn)

18 (Tx ID n48gfwmfdki)

21 (Tx ID 4f5f8njdoam4)

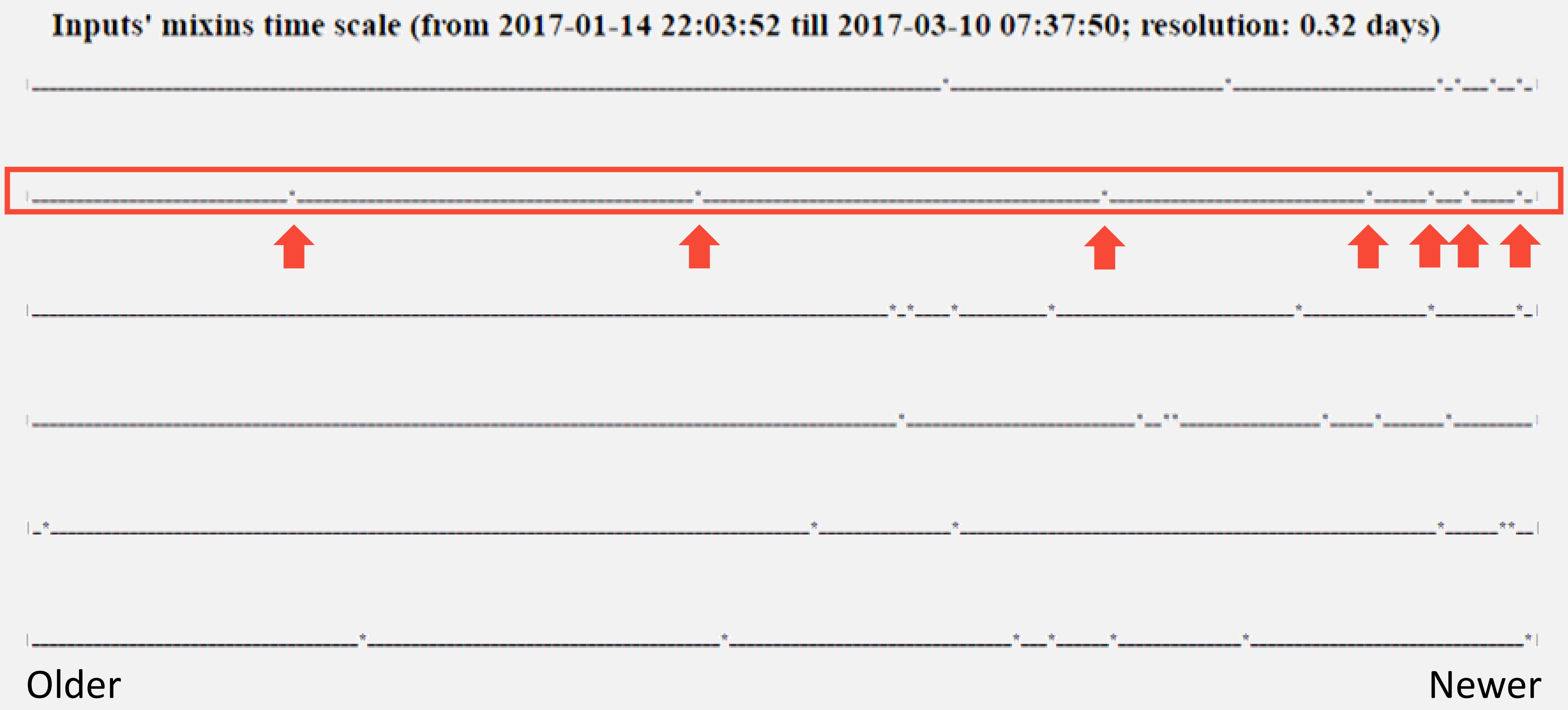
Ring Signatures & RingCT



Ring Signatures & RingCT

INPUTS

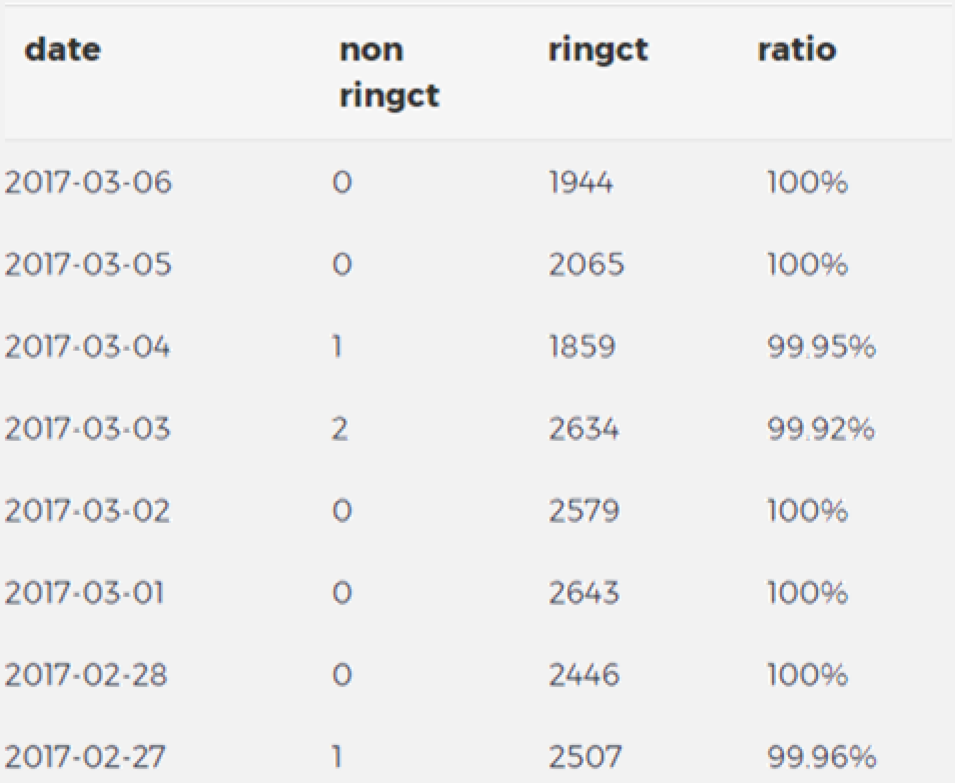
- 5
- 8
- 11
- 15
- 18
- 21



Inputs' mixins time scale (from 2017-01-14 22:03:52 till 2017-03-10 07:37:50; resolution: 0.32 days)

https://xmrchain.net/search?value=9bb608c70622ce67333c267103241f19b8aca21b7915f237813e451e1f03576e

Ring Signatures & RingCT

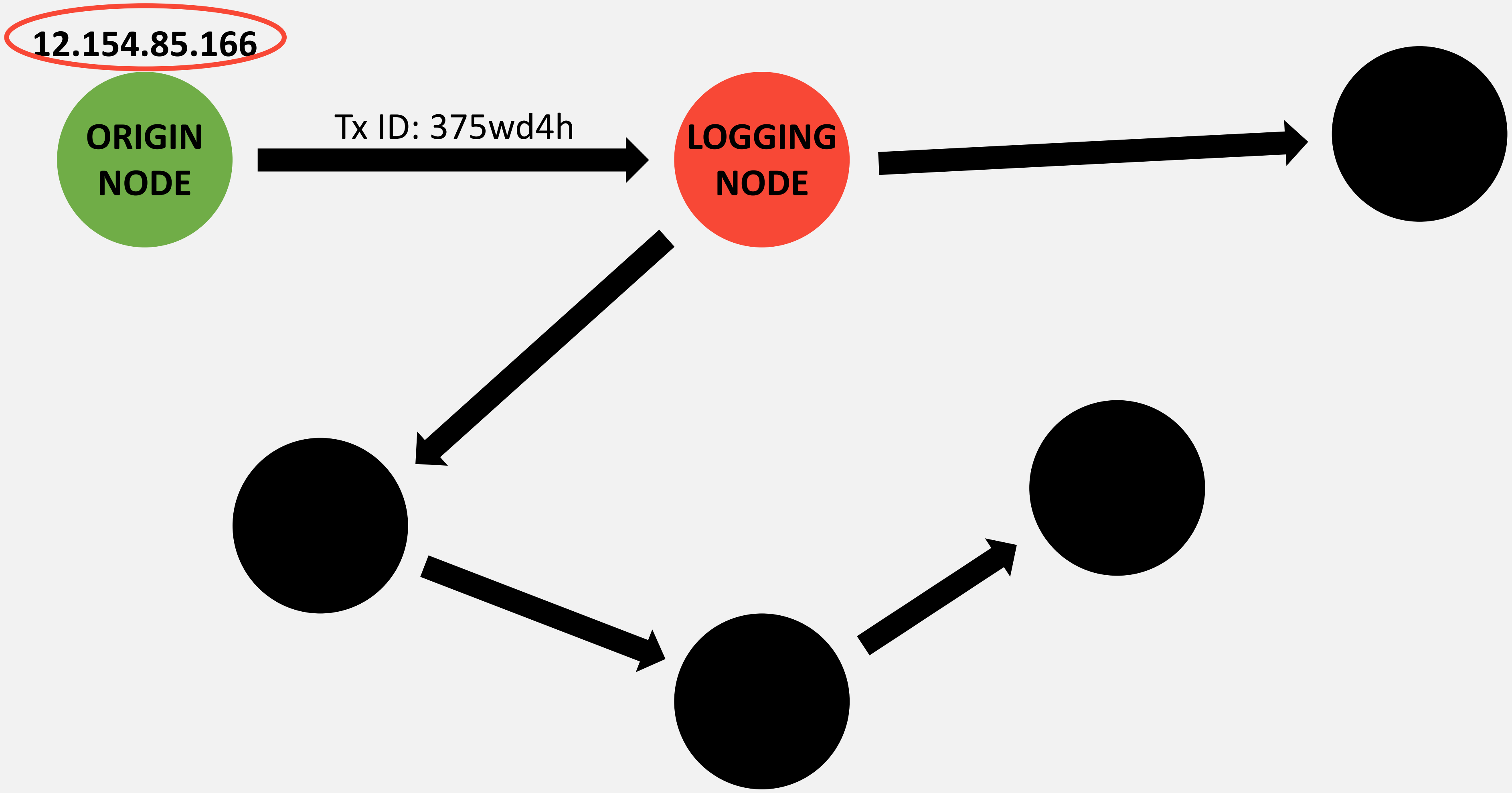


date	non ringct	ringct	ratio
2017-03-06	0	1944	100%
2017-03-05	0	2065	100%
2017-03-04	1	1859	99.95%
2017-03-03	2	2634	99.92%
2017-03-02	0	2579	100%
2017-03-01	0	2643	100%
2017-02-28	0	2446	100%
2017-02-27	1	2507	99.96%

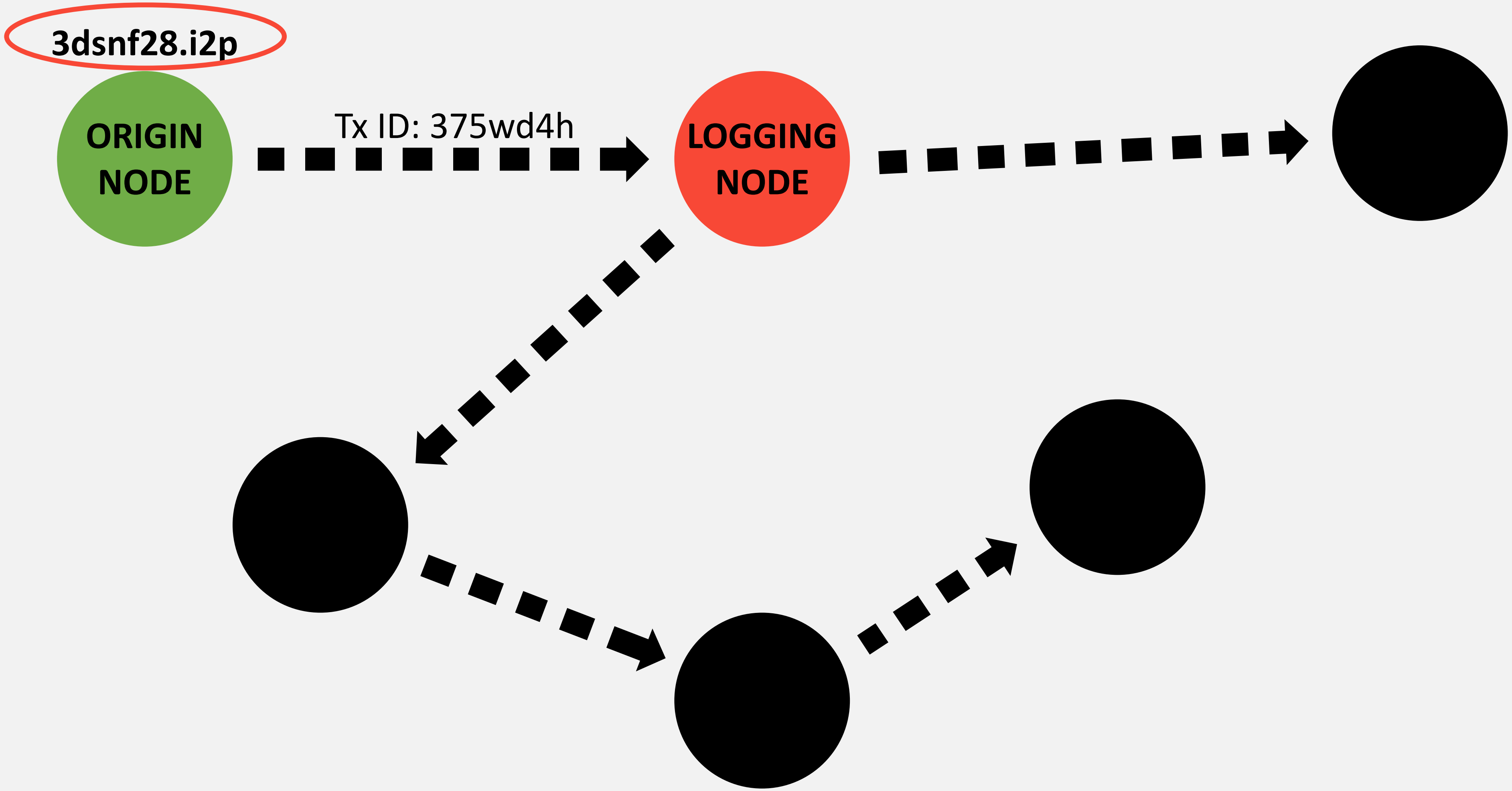
Near 100% use of optional RingCT

Source: moneroblocks.info/stats

KOVRI



KOVRI



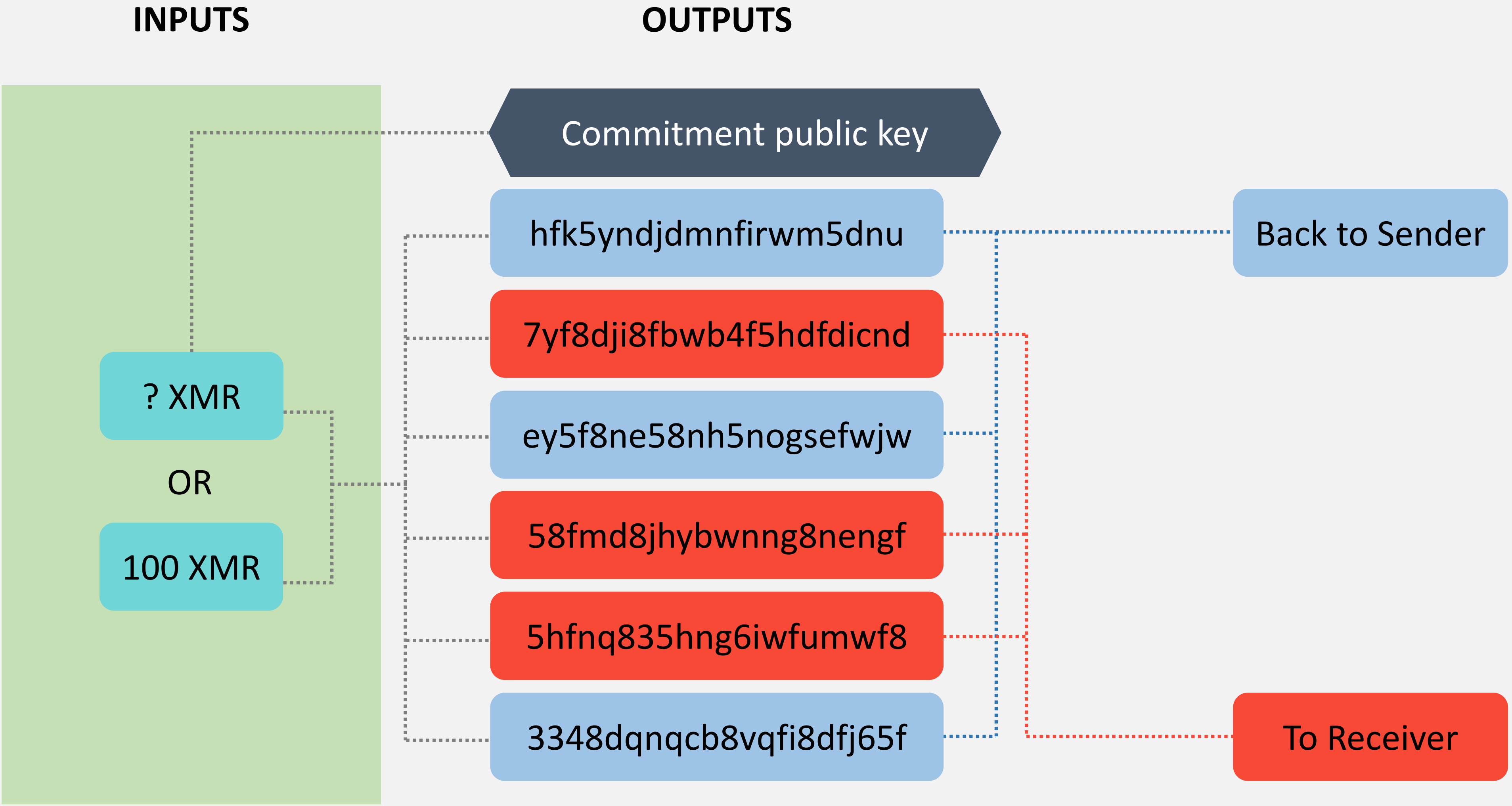
3dsnf28.i2p

ORIGIN NODE

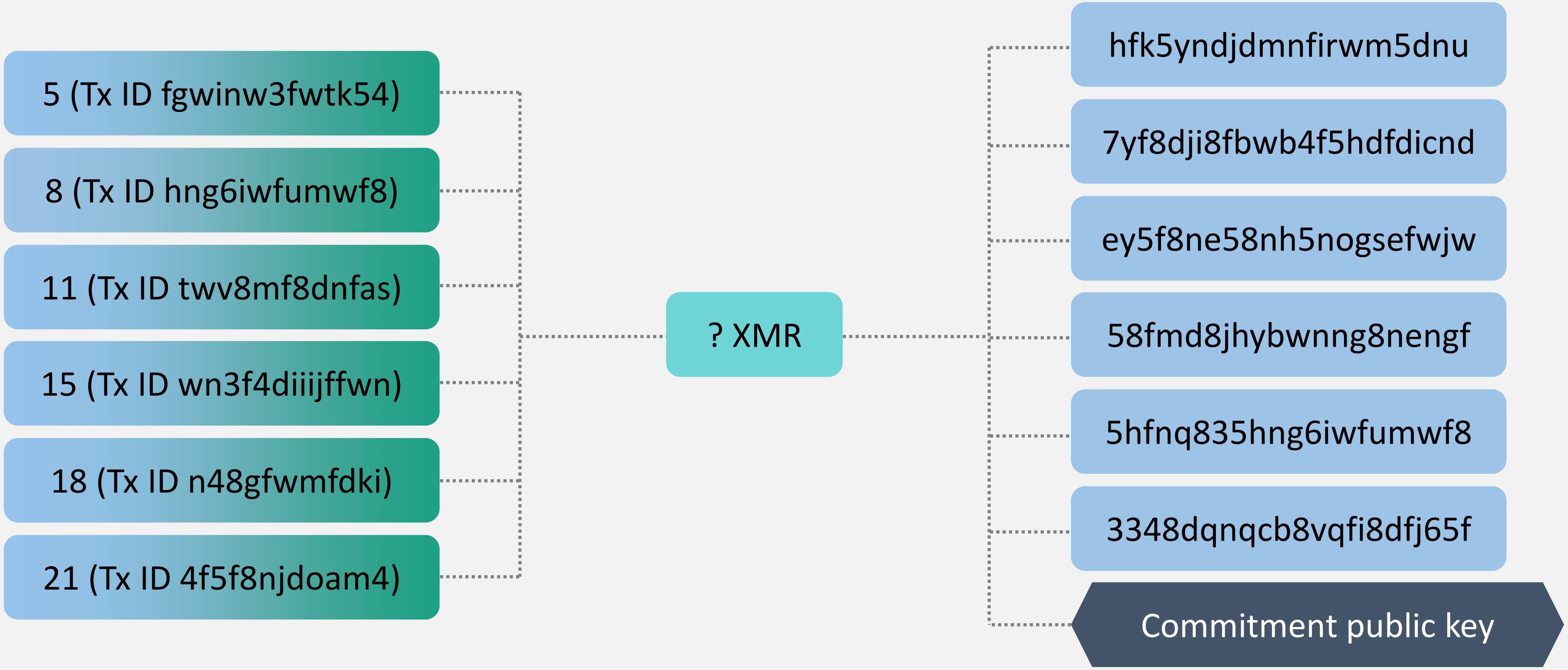
Tx ID: 375wd4h

LOGGING NODE

Stealth Addresses



Summary



5 (Tx ID fgwinw3fwtk54)

8 (Tx ID hng6iwfumwf8)

11 (Tx ID twv8mf8dnfas)

15 (Tx ID wn3f4diiijffwn)

18 (Tx ID n48gfwmfdki)

21 (Tx ID 4f5f8njdoam4)

? XMR

hfk5yndjdmnfirwm5dnu

7yf8dji8fbwb4f5hdfdicnd

ey5f8ne58nh5nogsefwjw

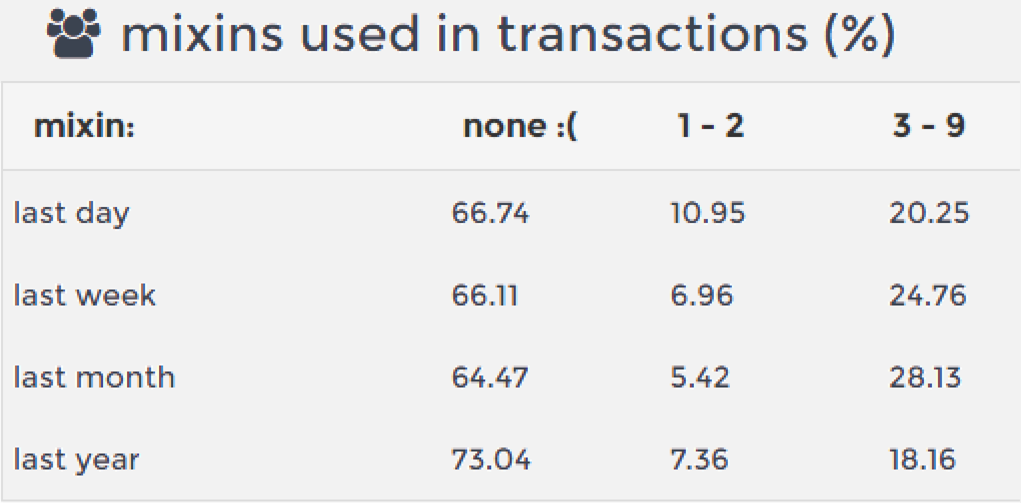
58fmd8jhybwnng8nengf

5hfnq835hng6iwfumwf8

3348dqnqcb8vqfi8dfj65f

Commitment public key

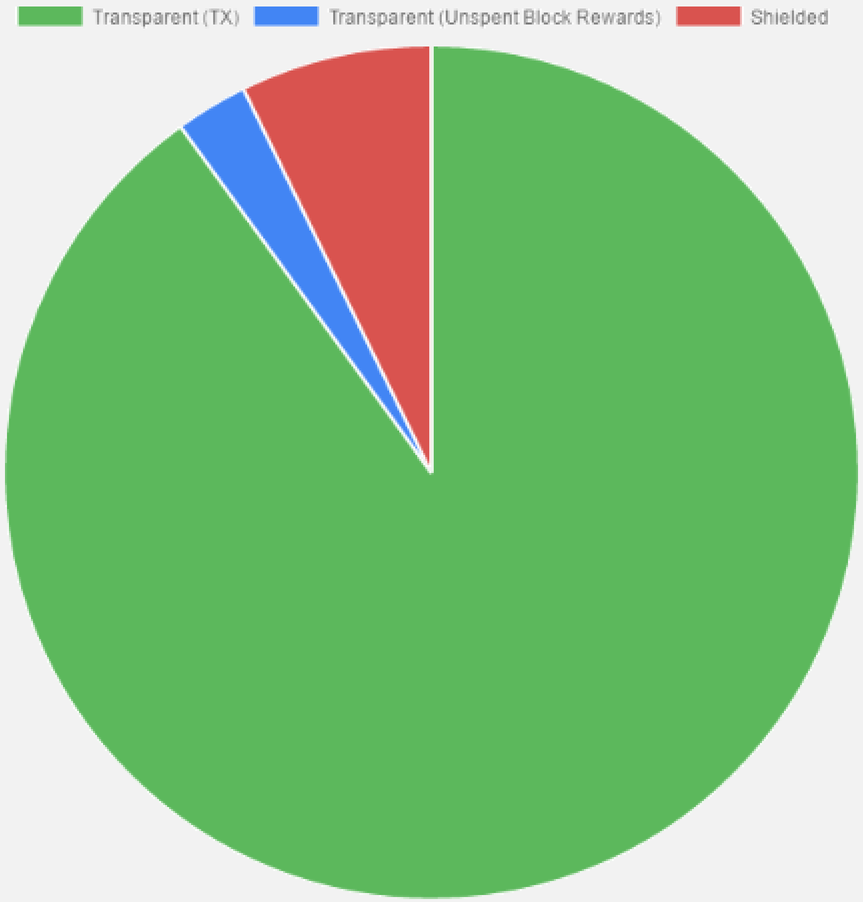
Mandatory Privacy



mixins used in transactions (%)

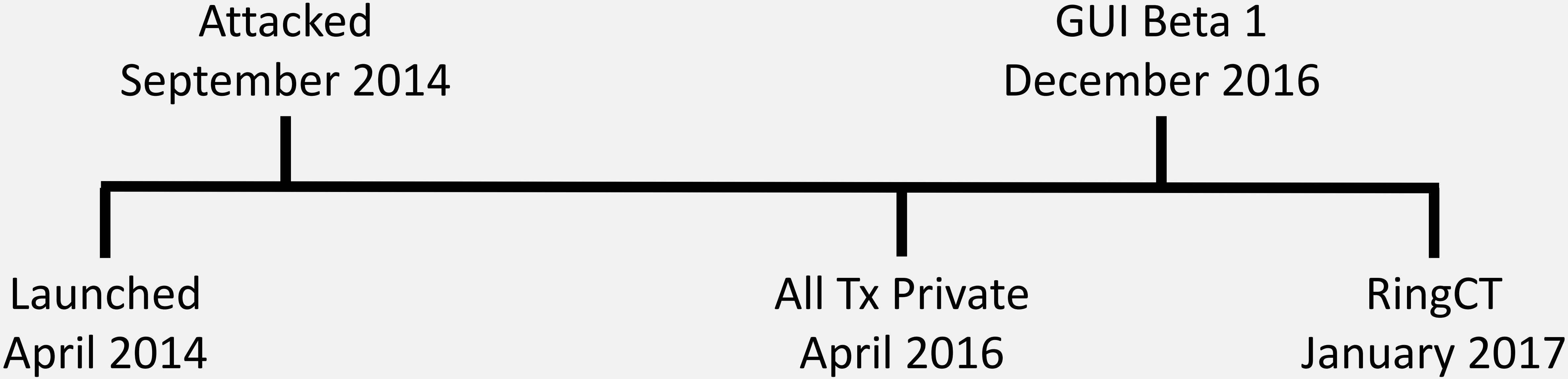
mixin:	none :(	1 - 2	3 - 9
last day	66.74	10.95	20.25
last week	66.11	6.96	24.76
last month	64.47	5.42	28.13
last year	73.04	7.36	18.16

Source: MoneroBlocks.info 24 Feb 2016



Source: zcha.in 15 March 2017

A Brief History



Launched
April 2014

Attacked
September 2014

All Tx Private
April 2016

GUI Beta 1
December 2016

RingCT
January 2017

Adapted from Fluffypony's Slides

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

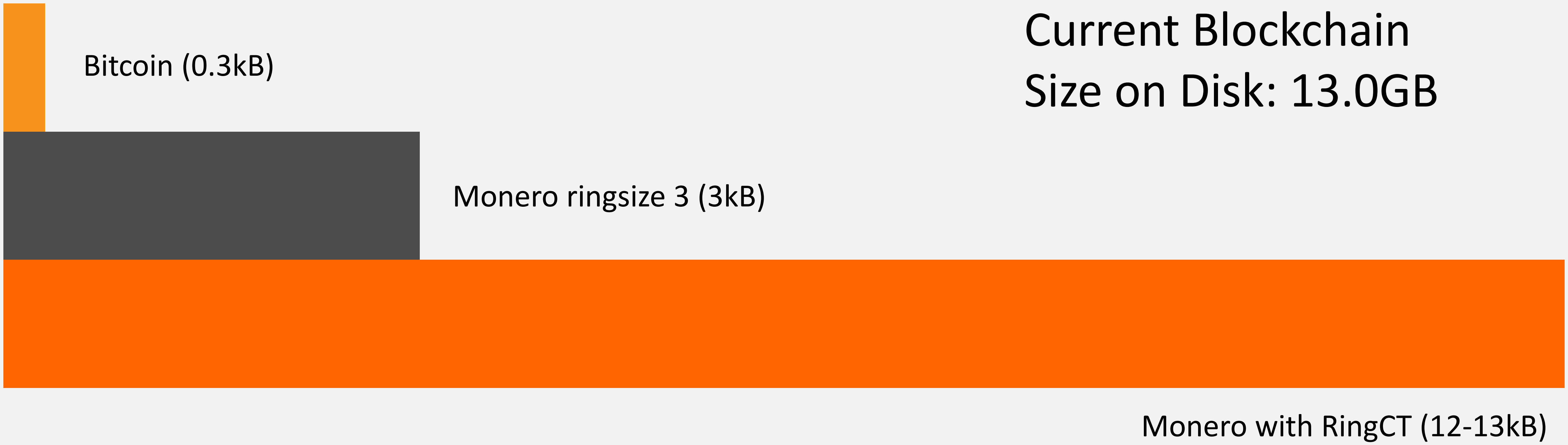
By publishing their view key, charities can invite easy public oversight

Parents

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

Monero Limitations

Monero Limitations



Current Blockchain
Size on Disk: 13.0GB

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

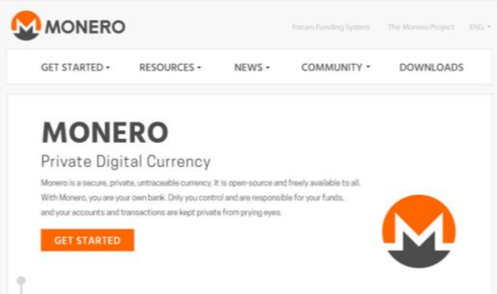
Multisig

Sub-Addresses &
Disposable Addresses

Translations

Improvements to
Dynamic Fees &
Dynamic Blocks

Lightweight
Wallet



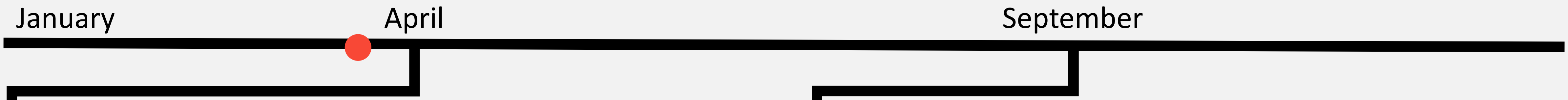
MONERO

Private Digital Currency

Monero is a secure, private, untraceable currency. It is open-source and freely available to all. With Monero, you are your own bank. Only you control and are responsible for your funds, and your accounts and transactions are kept private from prying eyes.

Website
Redesign

Hardfork Schedule



April 15th

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

September 18th*

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

Adapted from Fluffypony’s Slides

Thank You!

getmonero.org

/r/Monero

monero.stackexchange.com

People Started Adding Tools to Bitcoin