SECURE. PRIVATE. UNTRACEABLE.

MONERO

Riga, Latvia

Welcome

Justin Ehrenhofer

Finance
Management Information Systems

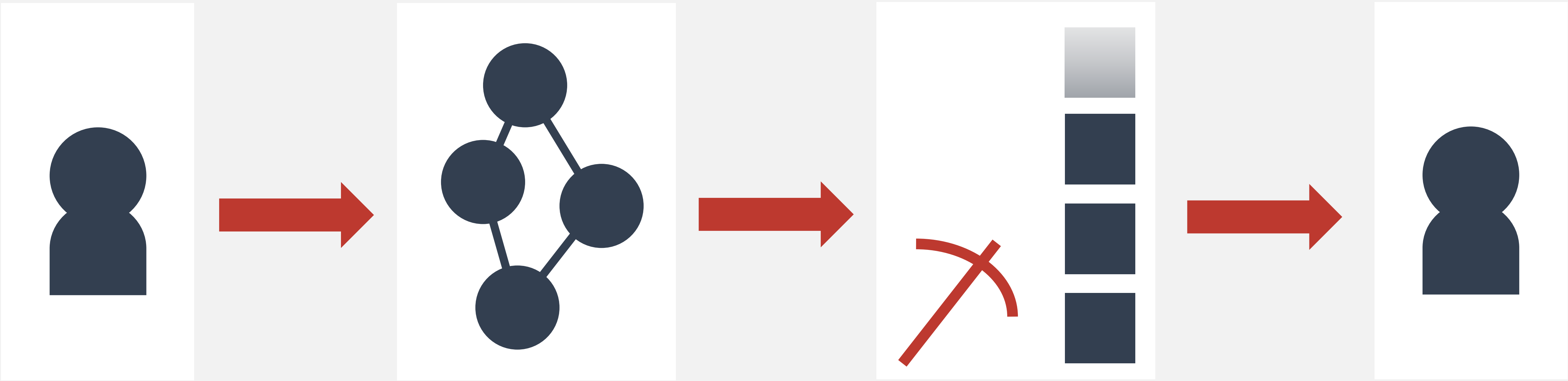
/u/SamsungGalaxyPlayer or sgp_

WU
WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

UNIVERSITY OF MINNESOTA
Driven to Discover^{SM}

CryptoUMN.com

Bitcoin Crash Course



SENDER

TRANSACTION BROADCAST

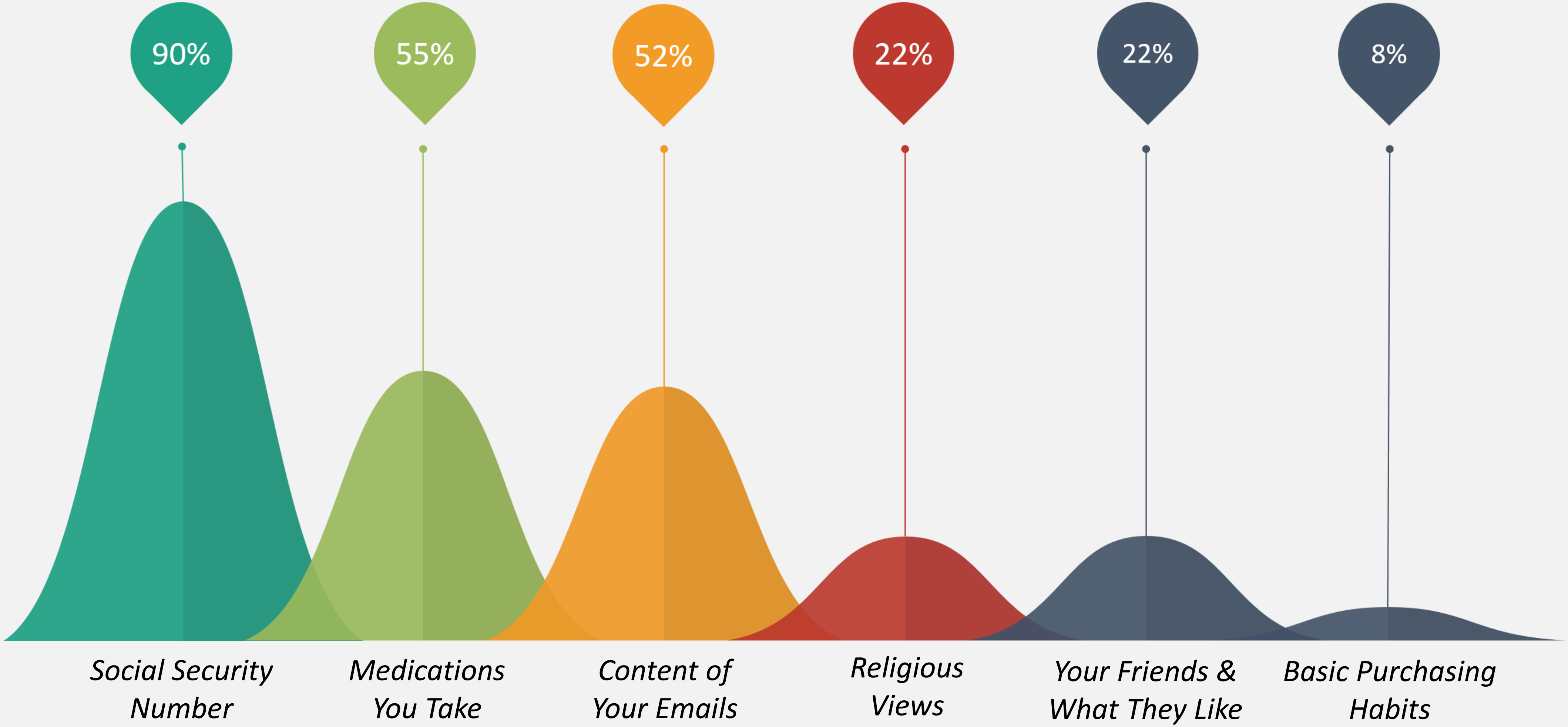
ADDED TO BLOCKCHAIN BY MINING

RECEIVER

Adapted from Fluffypony's Slides

People Don't Care About Financial Privacy

Percentage of adults, in a November, 2014, USA survey, who view the following information as "very sensitive"

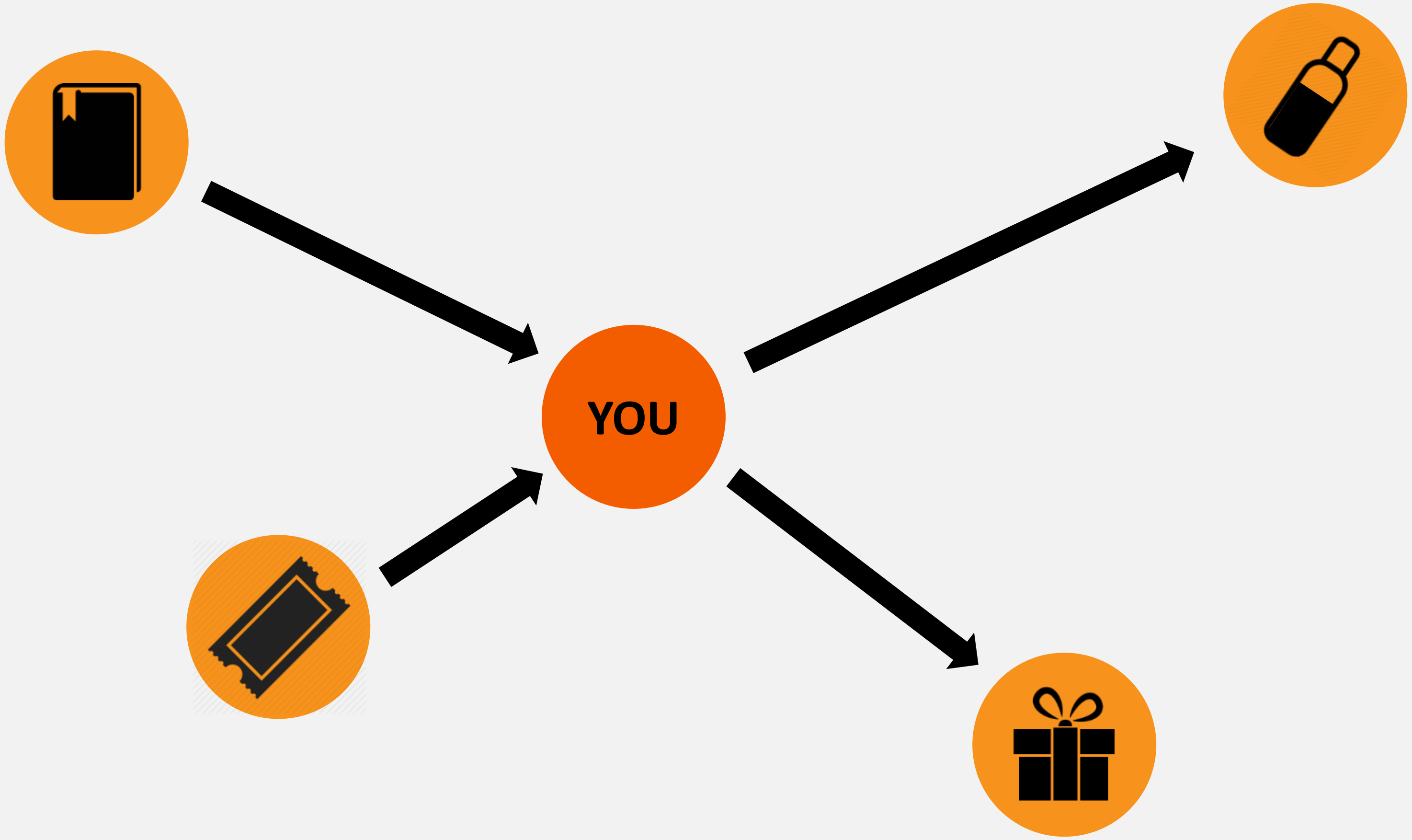


Source: **"Public Perceptions of Privacy and Security in the Post-Snowden Era", by PewResearchCenter**

Fungibility

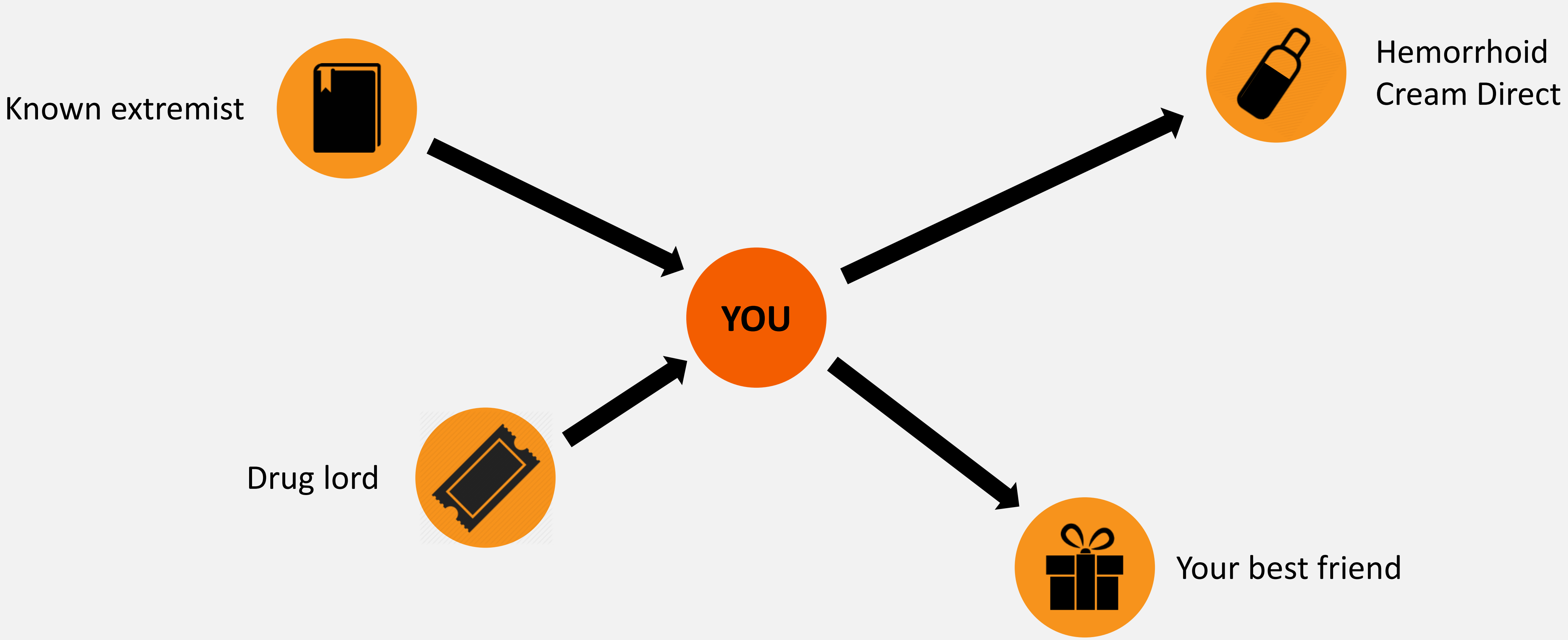
=

Why Fungibility Matters



Adapted from Keybase.io

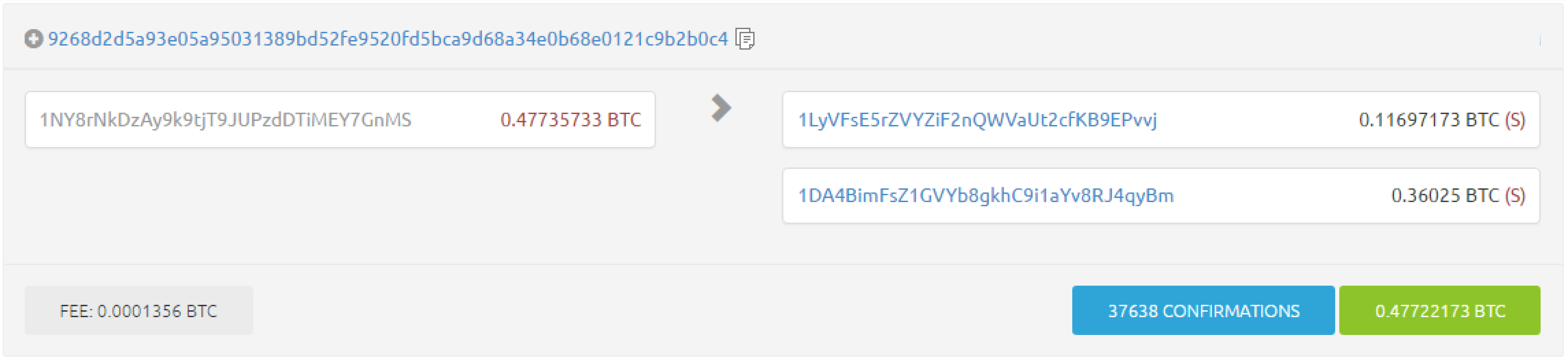
Why Fungibility Matters



Adapted from Keybase.io

History of Privacy

In the beginning, people thought Bitcoin was private because addresses did not directly reveal any information about the controller



9268d2d5a93e05a95031389bd52fe9520fd5bca9d68a34e0b68e0121c9b2b0c4

1NY8rNkDzAy9k9tjT9JUPzdDTiMEY7GnMS	0.47735733 BTC	1LyVFsE5rZVYZiF2nQWVaUt2cfKB9EPvvj	0.11697173 BTC (S)
		1DA4BimFsZ1GVYb8gkhC9i1aYv8RJ4qyBm	0.36025 BTC (S)

FEE: 0.0001356 BTC

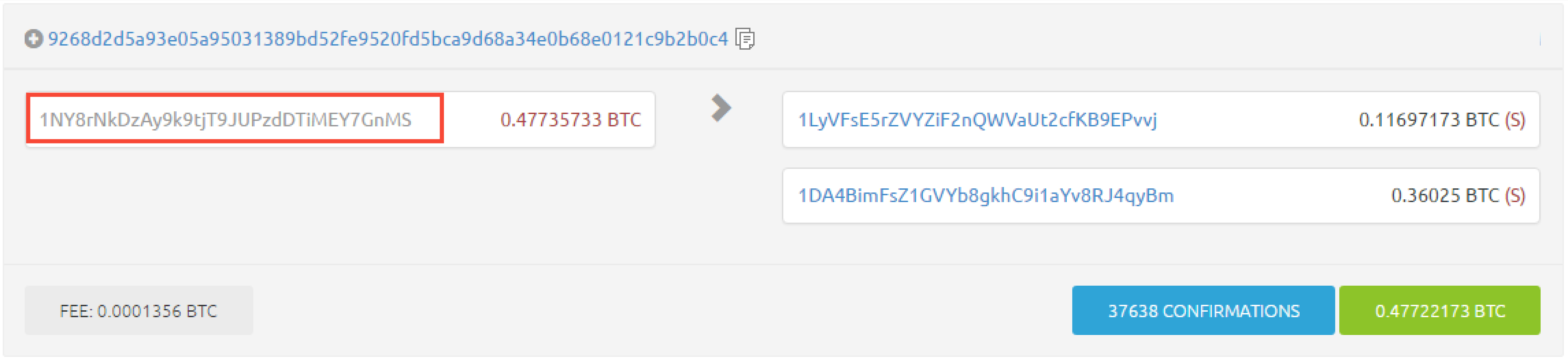
37638 CONFIRMATIONS

0.47722173 BTC

History of Privacy

Bitcoin address can be connected to personal info by:

- Exchanges
- Whoever you send Bitcoin to
- Whoever sends Bitcoin to you



9268d2d5a93e05a95031389bd52fe9520fd5bca9d68a34e0b68e0121c9b2b0c4

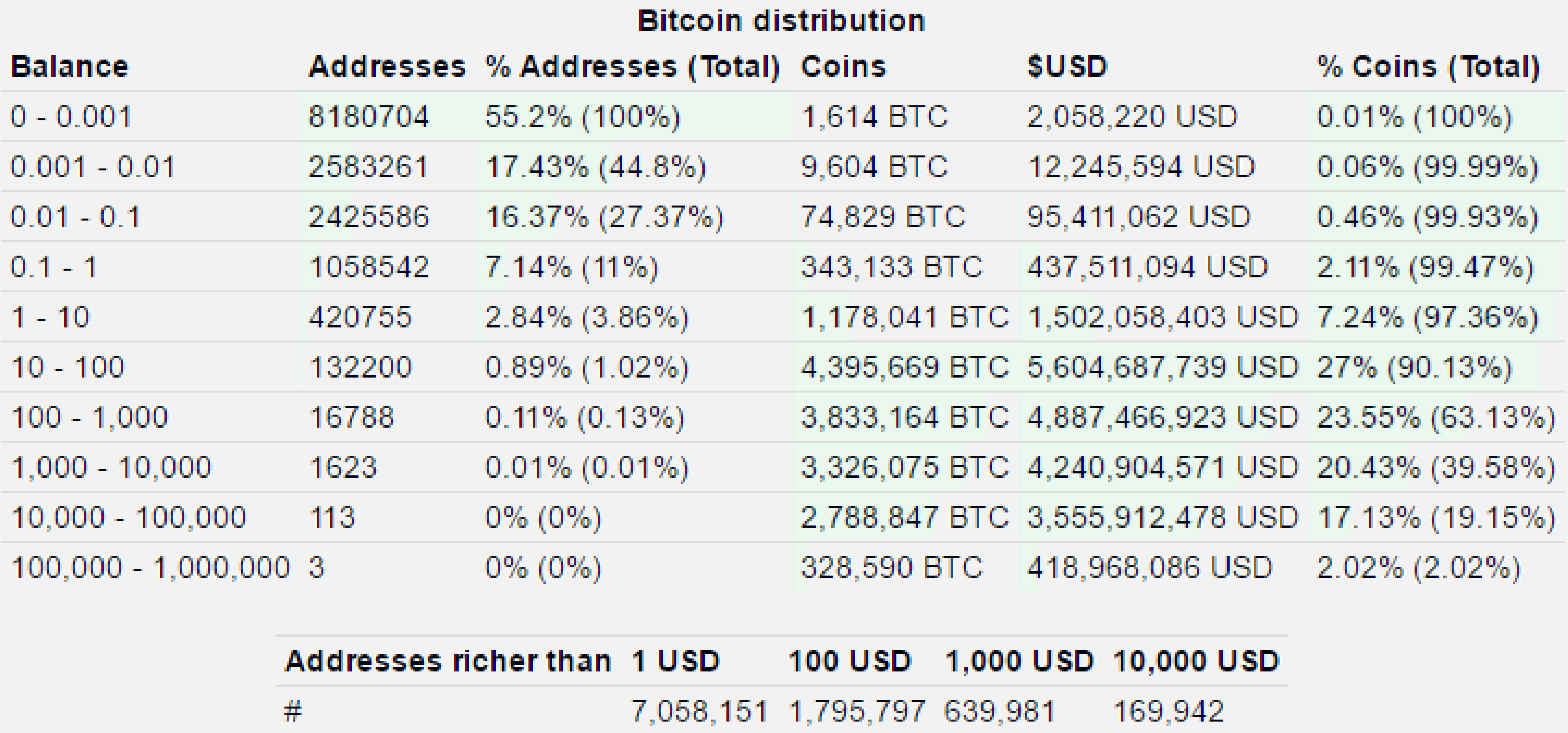
1NY8rNkDzAy9k9tjT9JUPzdDTiMEY7GnMS	0.47735733 BTC	1LyVFsE5rZVYZiF2nQWVaUt2cfKB9EPvvj	0.11697173 BTC (S)
		1DA4BimFsZ1GVYb8gkhC9i1aYv8RJ4qyBm	0.36025 BTC (S)

FEE: 0.0001356 BTC

37638 CONFIRMATIONS

0.47722173 BTC

History of Privacy



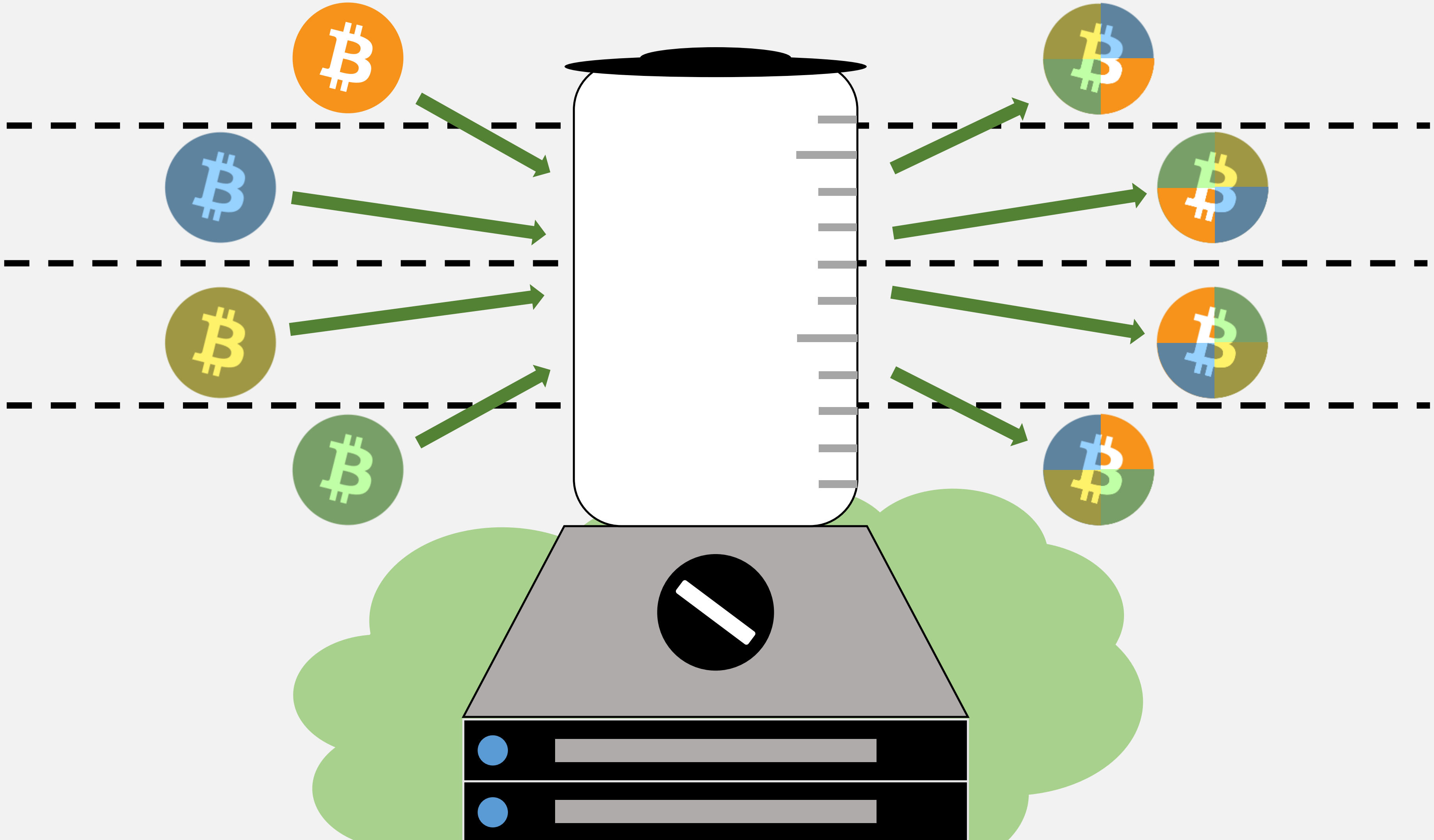
Bitcoin distribution

Balance	Addresses	% Addresses (Total)	Coins	$USD	% Coins (Total)
0 - 0.001	8180704	55.2% (100%)	1,614 BTC	2,058,220 USD	0.01% (100%)
0.001 - 0.01	2583261	17.43% (44.8%)	9,604 BTC	12,245,594 USD	0.06% (99.99%)
0.01 - 0.1	2425586	16.37% (27.37%)	74,829 BTC	95,411,062 USD	0.46% (99.93%)
0.1 - 1	1058542	7.14% (11%)	343,133 BTC	437,511,094 USD	2.11% (99.47%)
1 - 10	420755	2.84% (3.86%)	1,178,041 BTC	1,502,058,403 USD	7.24% (97.36%)
10 - 100	132200	0.89% (1.02%)	4,395,669 BTC	5,604,687,739 USD	27% (90.13%)
100 - 1,000	16788	0.11% (0.13%)	3,833,164 BTC	4,887,466,923 USD	23.55% (63.13%)
1,000 - 10,000	1623	0.01% (0.01%)	3,326,075 BTC	4,240,904,571 USD	20.43% (39.58%)
10,000 - 100,000	113	0% (0%)	2,788,847 BTC	3,555,912,478 USD	17.13% (19.15%)
100,000 - 1,000,000	3	0% (0%)	328,590 BTC	418,968,086 USD	2.02% (2.02%)

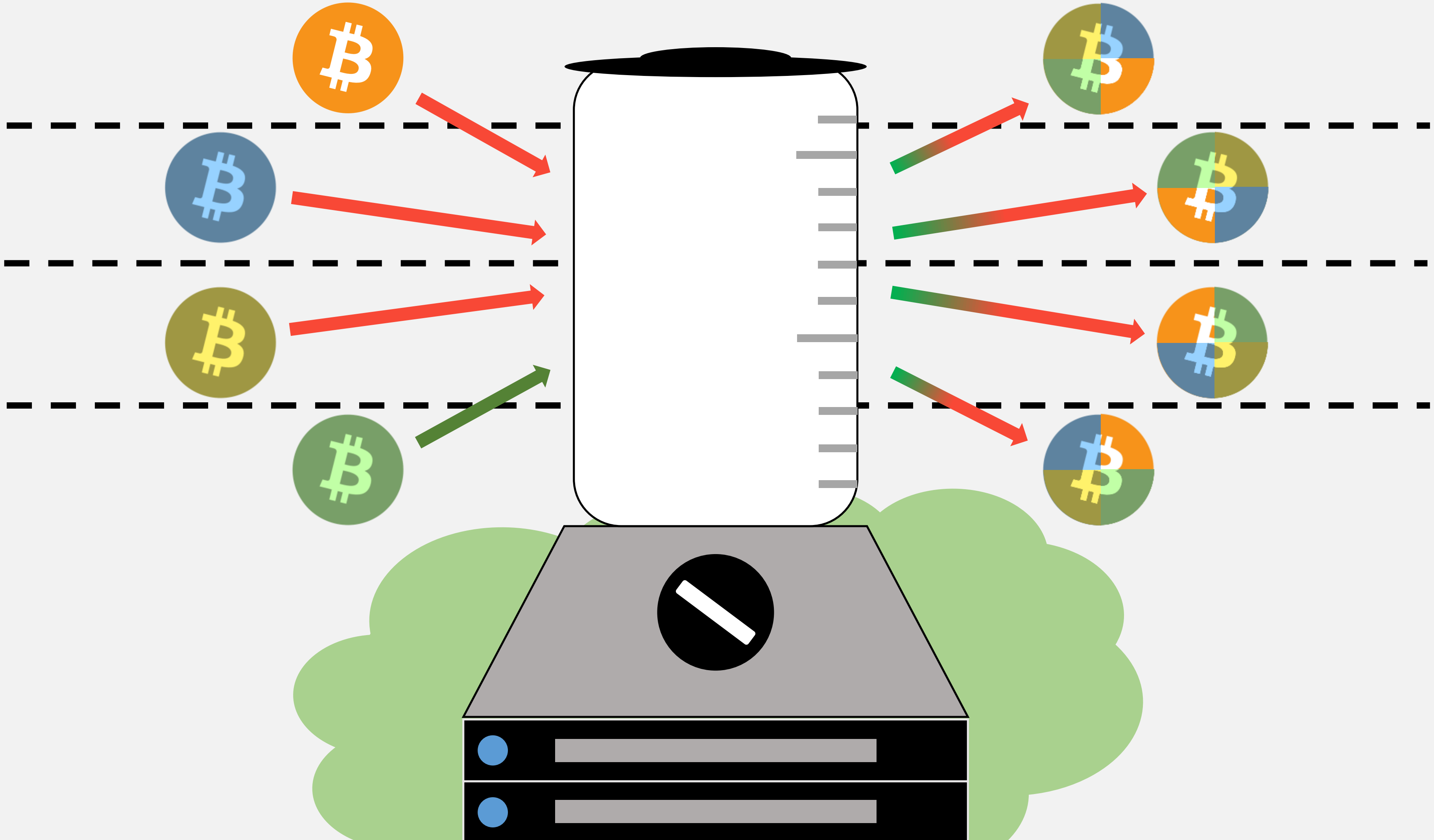
Addresses richer than	1 USD	100 USD	1,000 USD	10,000 USD
#	7,058,151	1,795,797	639,981	169,942

Source: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

People Started Adding Tools to Bitcoin

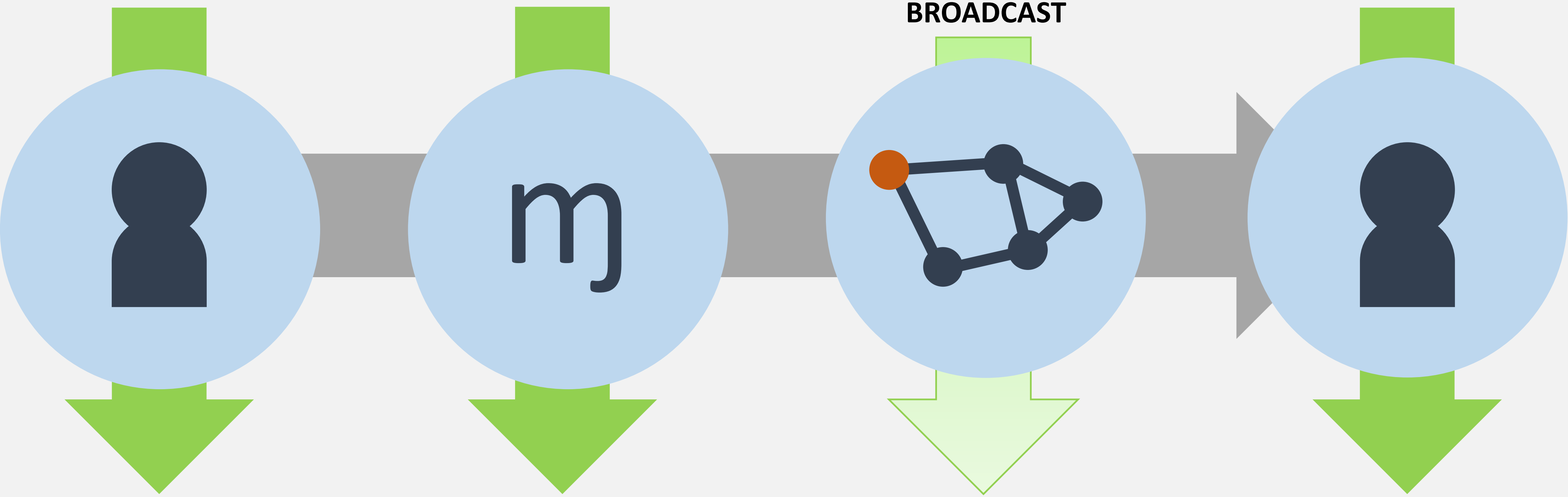


People Started Adding Tools to Bitcoin



People Started Adding Tools to Bitcoin

The Monero Difference



SENDER

RING SIGNATURES

AMOUNT

RING CONFIDENTIAL TRANSACTIONS (RingCT)

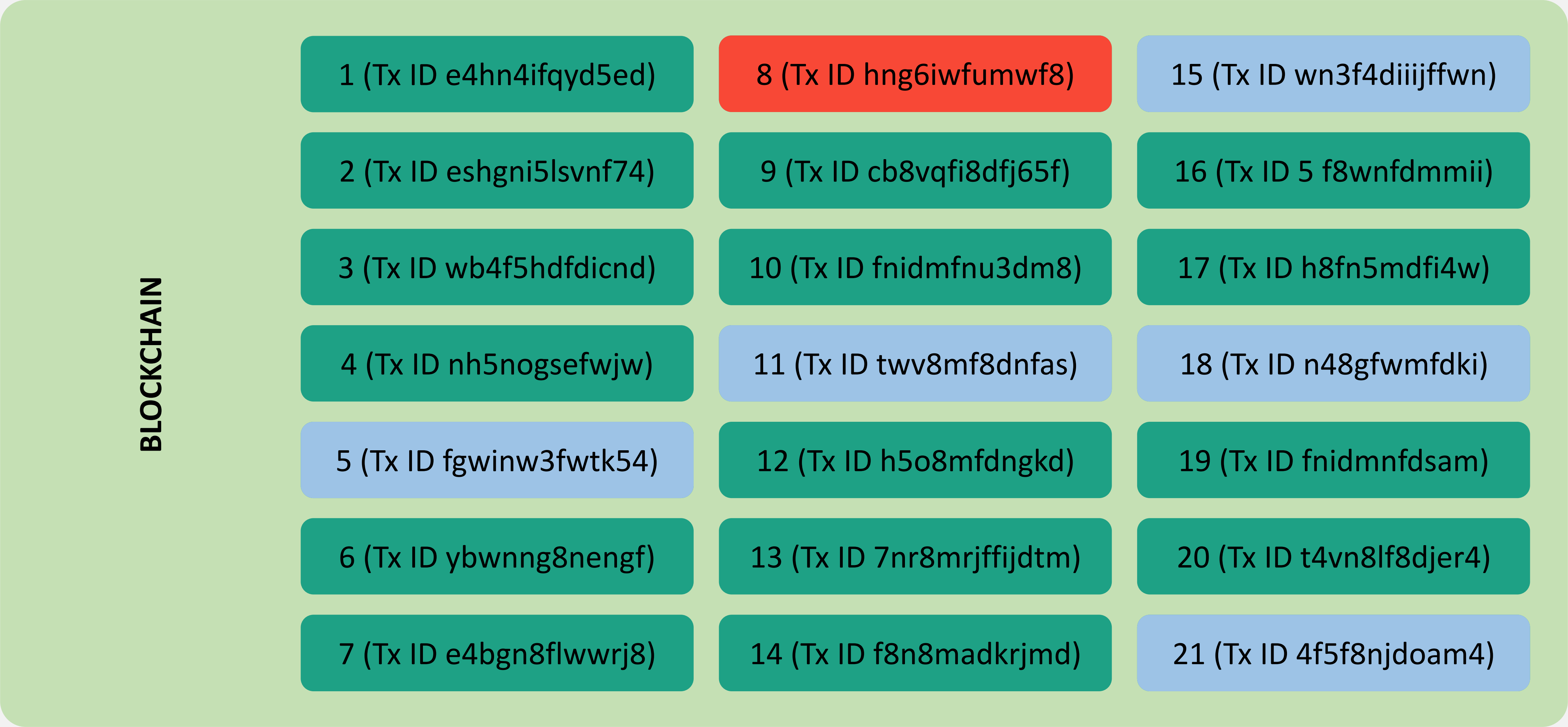
TRANSACTION BROADCAST

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)

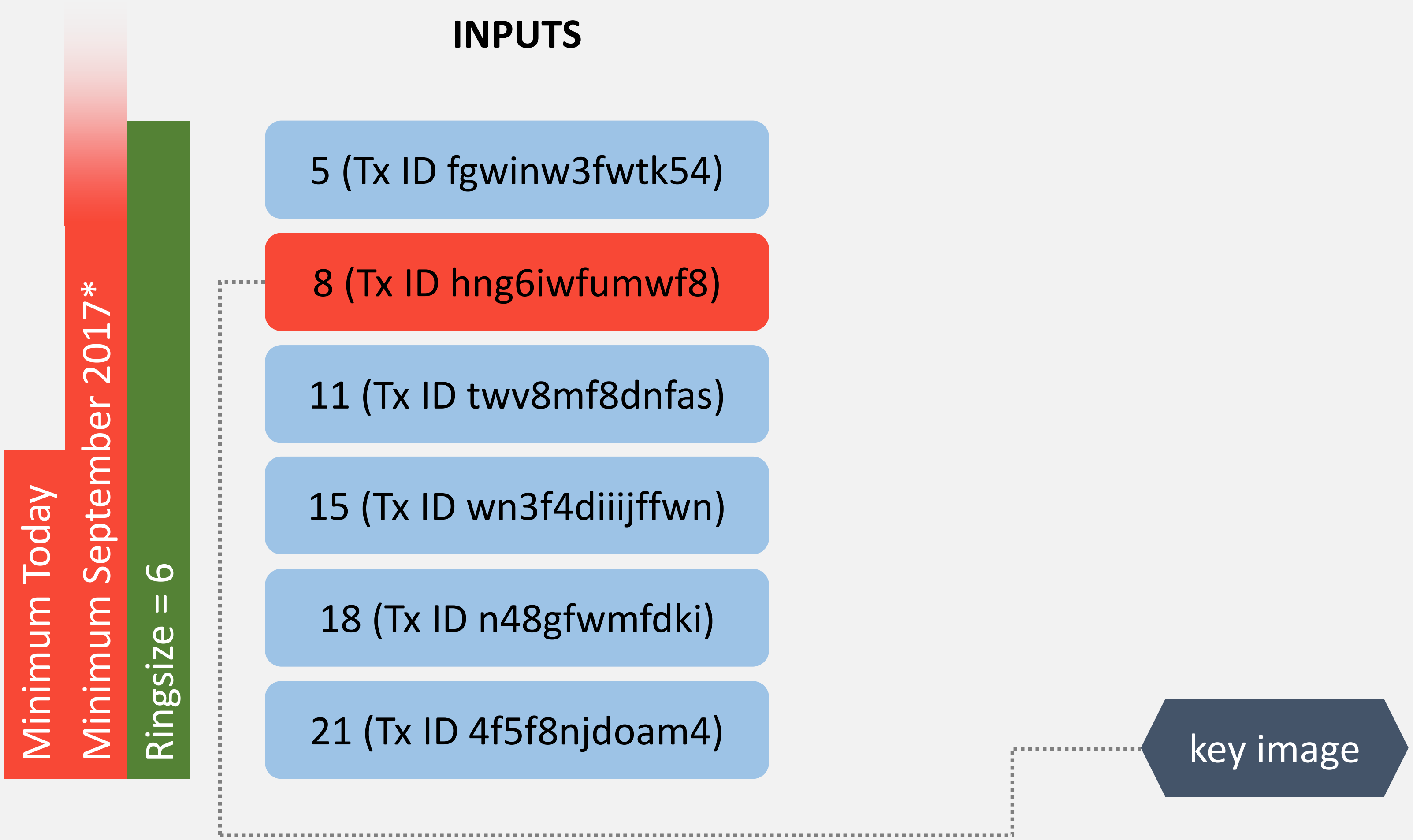
18 (Tx ID n48gfwmfdki)

19 (Tx ID fnidmnfdsam)

20 (Tx ID t4vn8lf8djer4)

21 (Tx ID 4f5f8njdoam4)

Ring Signatures & RingCT



INPUTS

Minimum Today

Minimum September 2017*

Ringsize = 6

5 (Tx ID fgwinw3fwtk54)

8 (Tx ID hng6iwfumwf8)

11 (Tx ID twv8mf8dnfas)

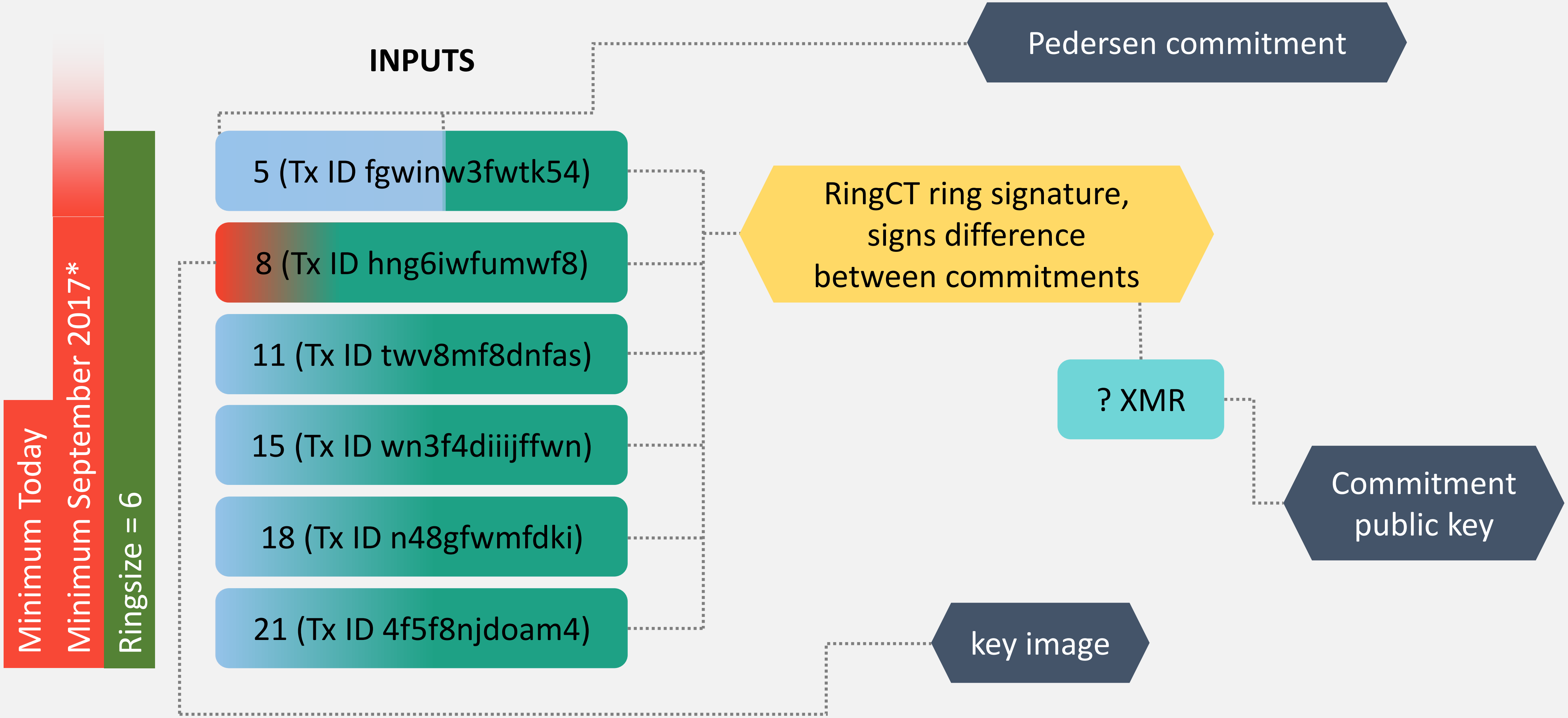
15 (Tx ID wn3f4diiijffwn)

18 (Tx ID n48gfwmfdki)

21 (Tx ID 4f5f8njdoam4)

key image

Ring Signatures & RingCT



Ring Signatures & RingCT

INPUTS

5

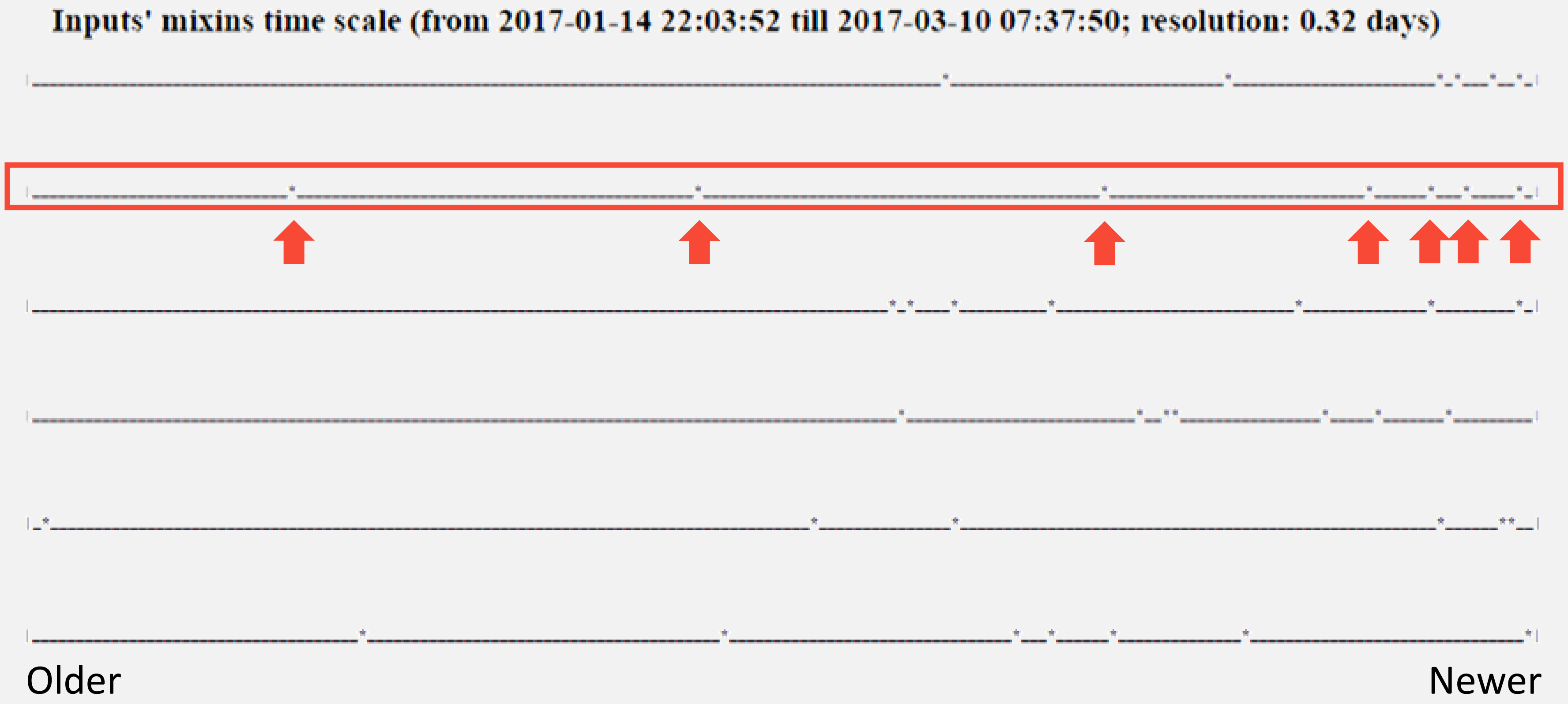
8

11

15

18

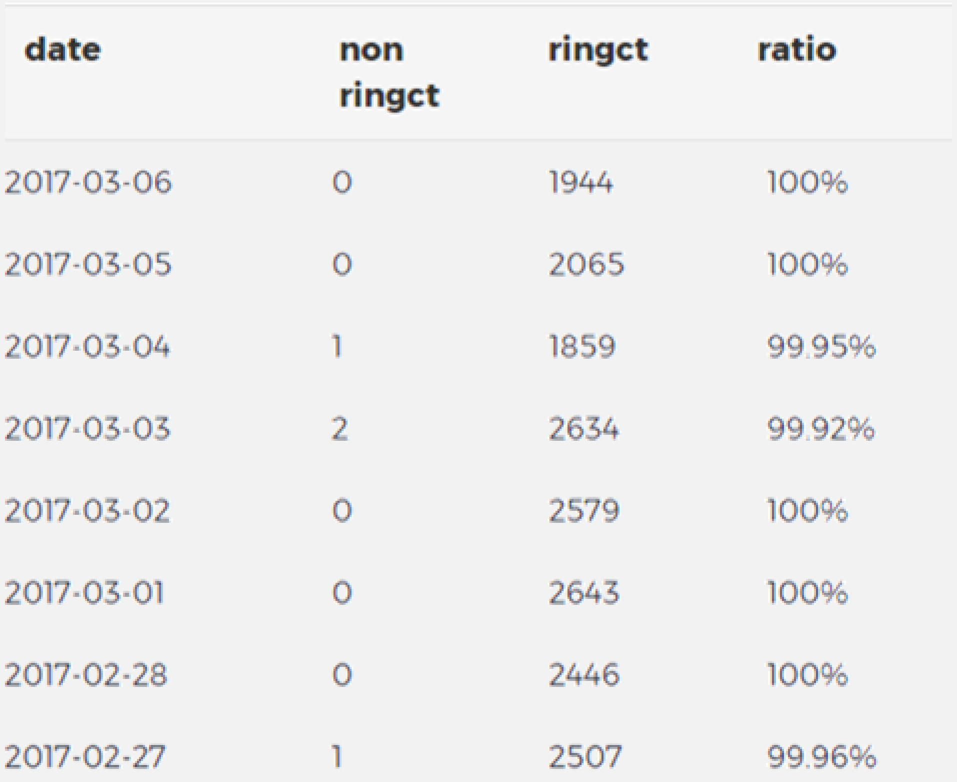
21



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

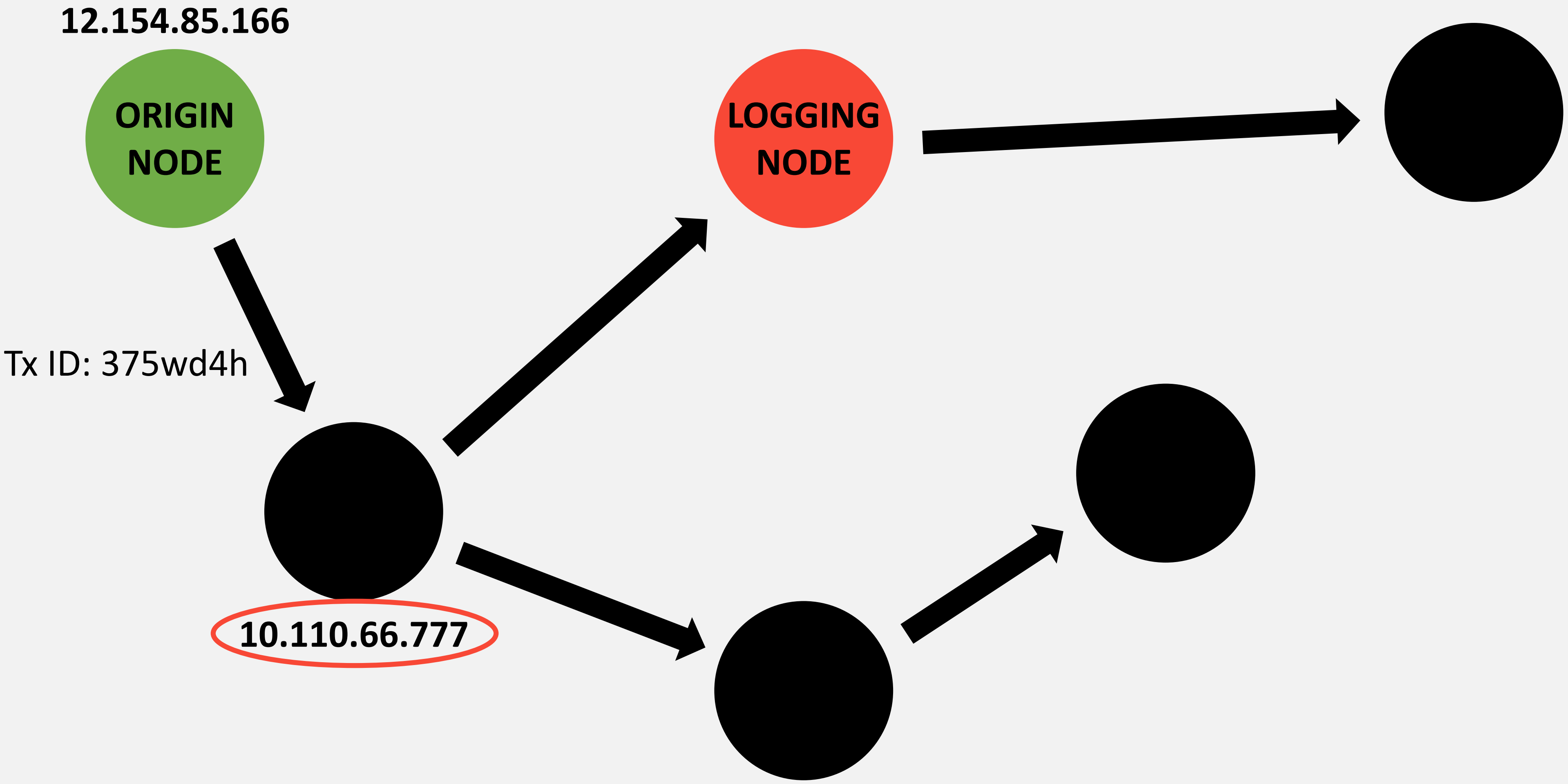


date	non ringct	ringct	ratio
2017-03-06	0	1944	100%
2017-03-05	0	2065	100%
2017-03-04	1	1859	99.95%
2017-03-03	2	2634	99.92%
2017-03-02	0	2579	100%
2017-03-01	0	2643	100%
2017-02-28	0	2446	100%
2017-02-27	1	2507	99.96%

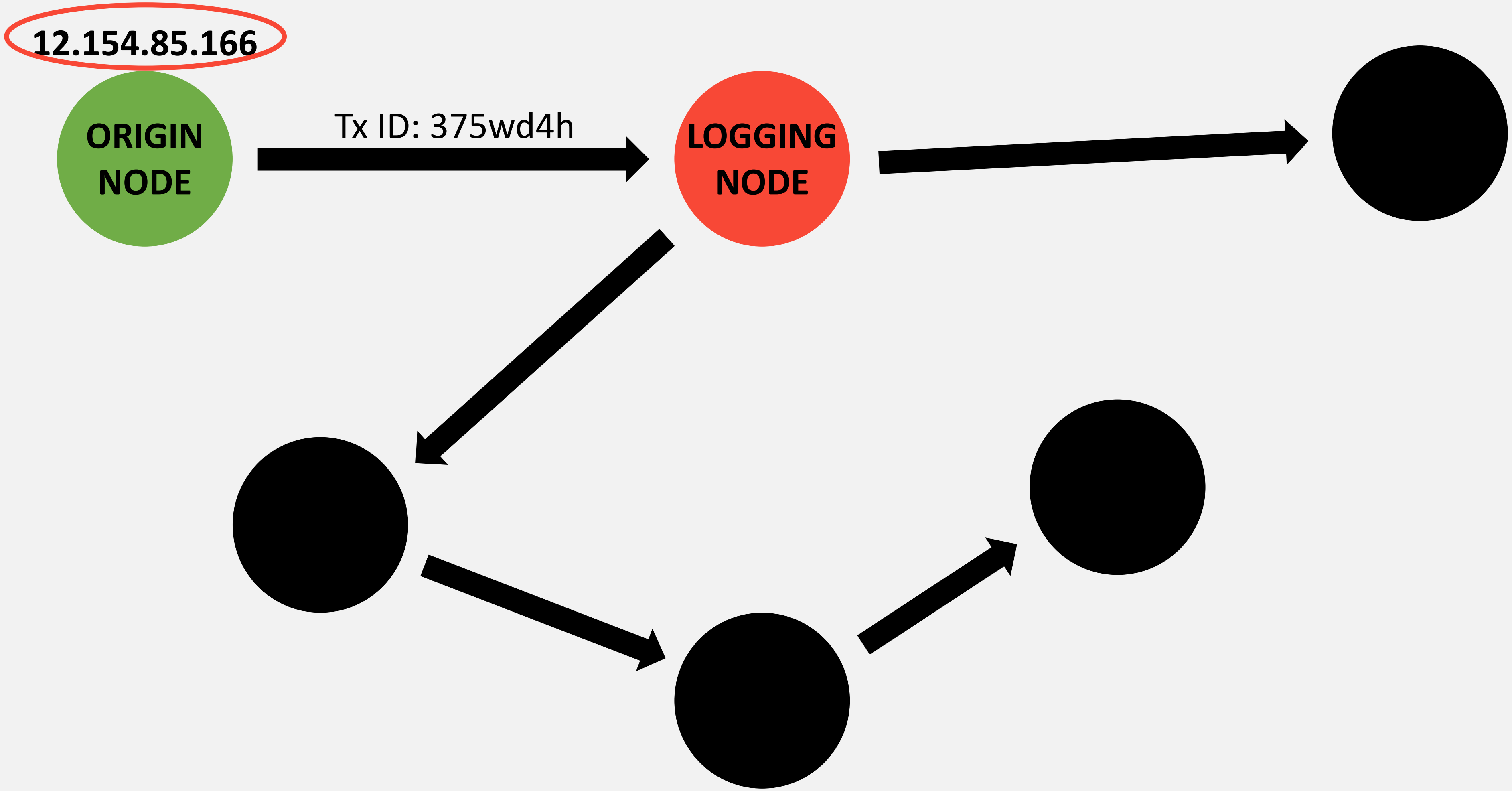
Near 100% use of optional RingCT

Source: moneroblocks.info/stats

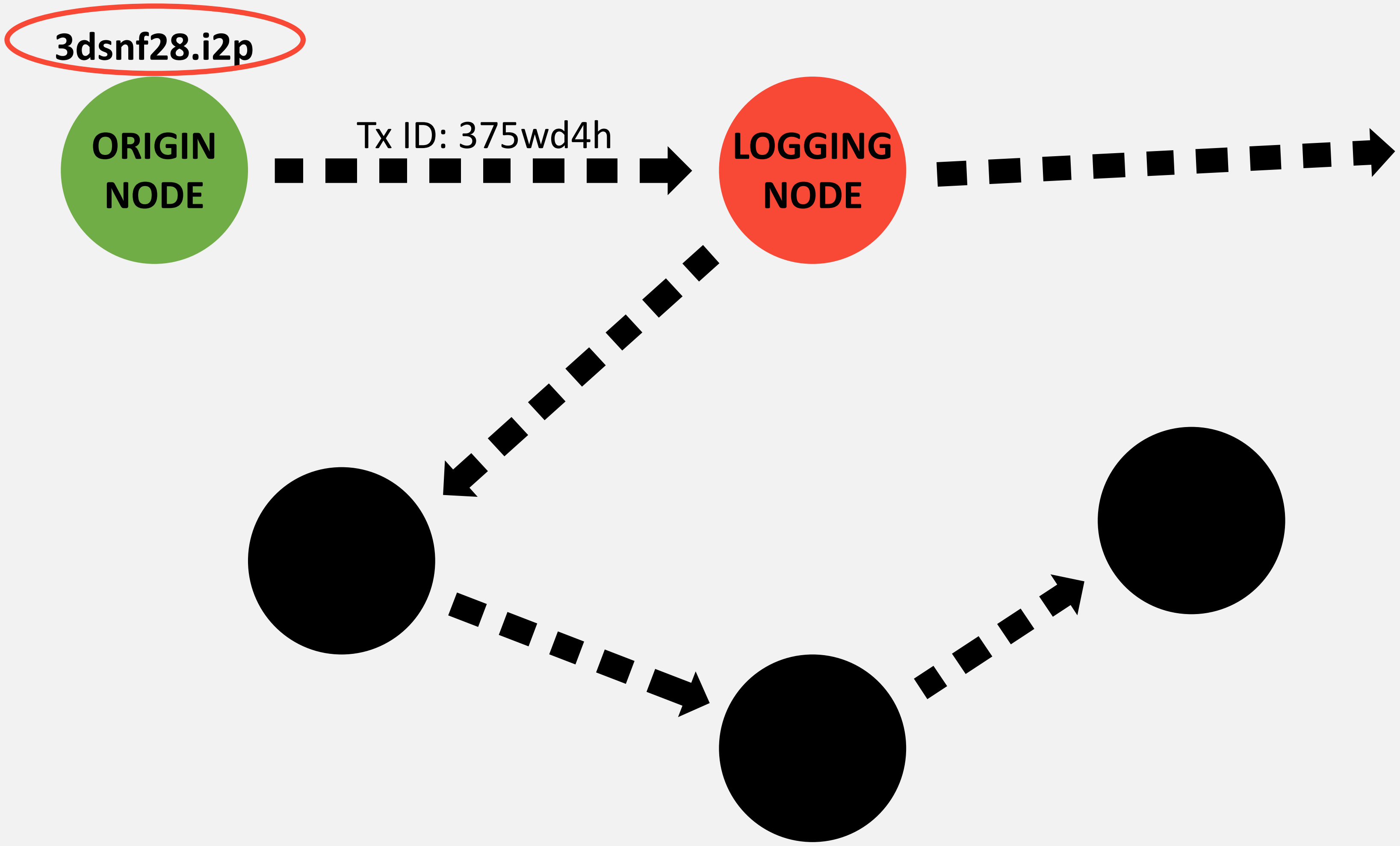
KOVRI

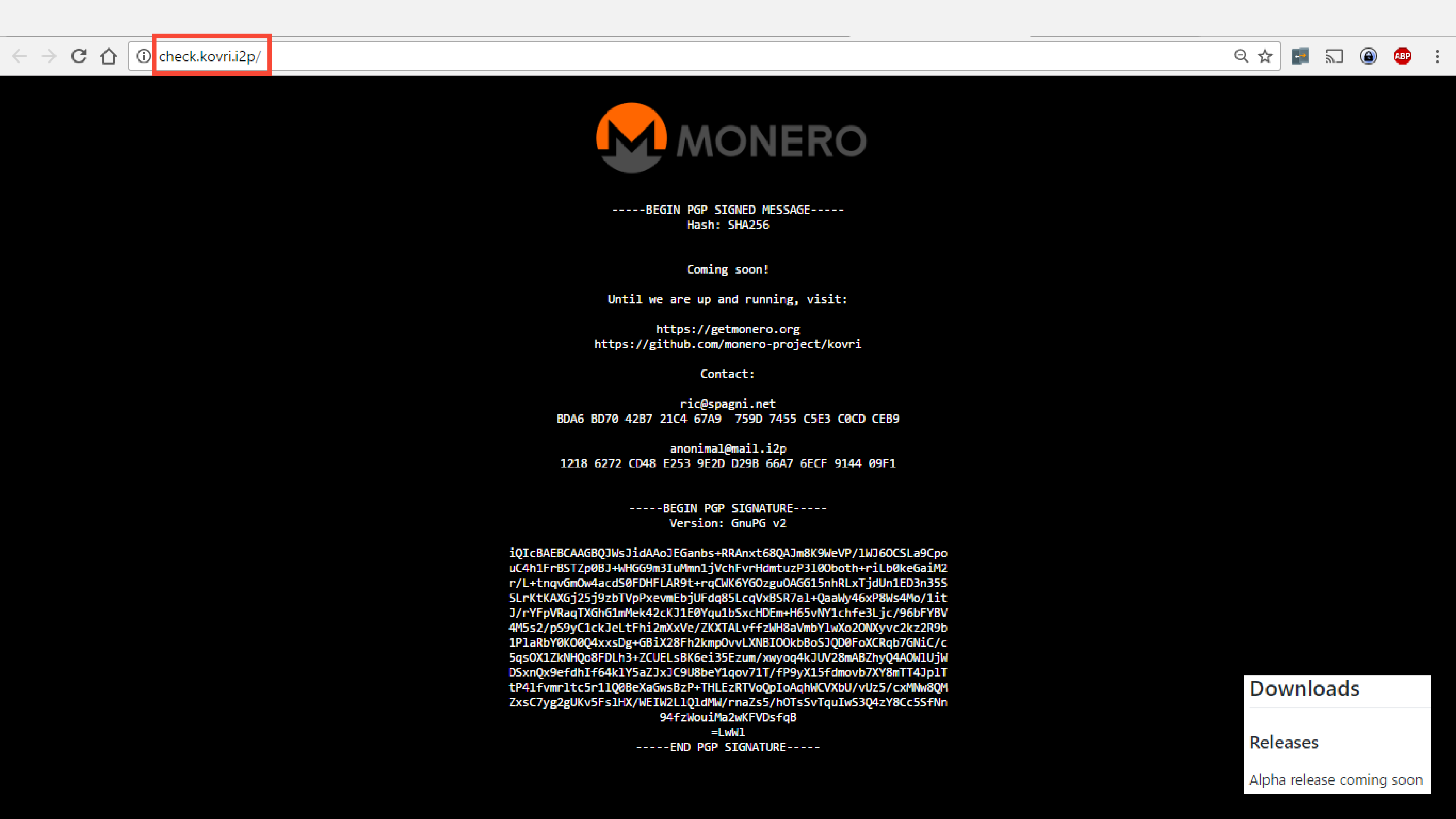

12.154.85.166
ORIGIN NODE
Tx ID: 375wd4h
LOGGING NODE
10.110.66.777

KOVRI



KOVRI





check.kovri.i2p/

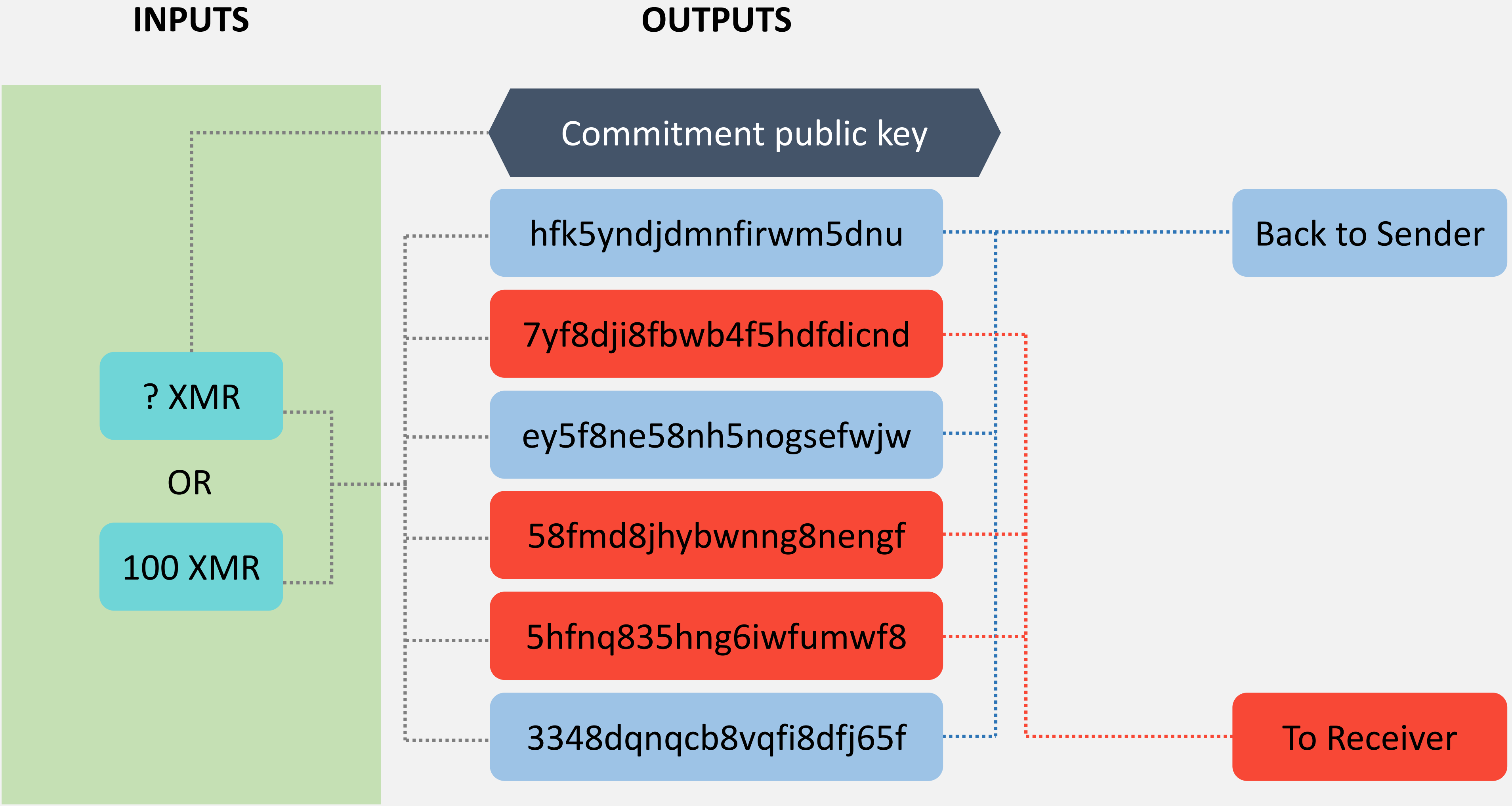
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256


Coming soon!

Until we are up and running, visit:

https://getmonero.org
https://github.com/monero-project/kovri

Contact:

ric@spagni.net
BDA6 BD70 42B7 21C4 67A9  759D 7455 C5E3 C0CD CEB9

anonimal@mail.i2p
1218 6272 CD48 E253 9E2D D29B 66A7 6ECF 9144 09F1


-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2

iQIcBAEBCAAGBQJWsJidAAoJEGanbs+RRAnxt68QAJm8K9WeVP/1WJ6OCSLa9Cpo
uC4h1FrBSTZp0BJ+WHGG9m3IuMmn1jVchFvrHdmtuzP310Oboth+riLb0keGaiM2
r/L+tnqvGmOw4acdS0FDHFLAR9t+rqCWK6YGOzguOAGG15nhRLxTjdUn1ED3n35S
SLrKtKAXGj25j9zbTVpPxevmEbjUFdq85LcqVxBSR7a1+QaaWy46xP8Ws4Mo/1it
J/rYFpVRaqTXGhG1mMek42cKJ1E0Yqu1bSxcHDEm+H65vNY1chfe3Ljc/96bFYBV
4M5s2/pS9yC1ckJeLtFhi2mXxVe/ZKXTALvffzWH8aVmbY1wXo2ONXyvc2kz2R9b
1P1aRbY0KO0Q4xxsDg+GBiX28Fh2kmpOvvLXNBIOOkbBoSJQD0FoXCRqb7GNiC/c
5qsOX1ZkNHQo8FDLh3+ZCUELsBK6ei35Ezum/xwyoq4kJUV28mABZhyQ4AOW1UjW
DSxnQx9efdhIf64k1Y5aZJxJC9U8beY1qov71T/fP9yX15fdmovb7XY8mTT4JplT
tP41fvmr1tc5r11Q0BeXaGwsBzP+THLEzRTVoQpIoAqhWCVXbU/vUz5/cxMNw8QM
ZxsC7yg2gUKv5Fs1HX/WEIW2L1Q1dMW/rnaZs5/hOTsSvTquIwS3Q4zY8Cc5SfNn
94fzWouiMa2wKFVDsfqB
=LwWl
-----END PGP SIGNATURE-----
```

Downloads

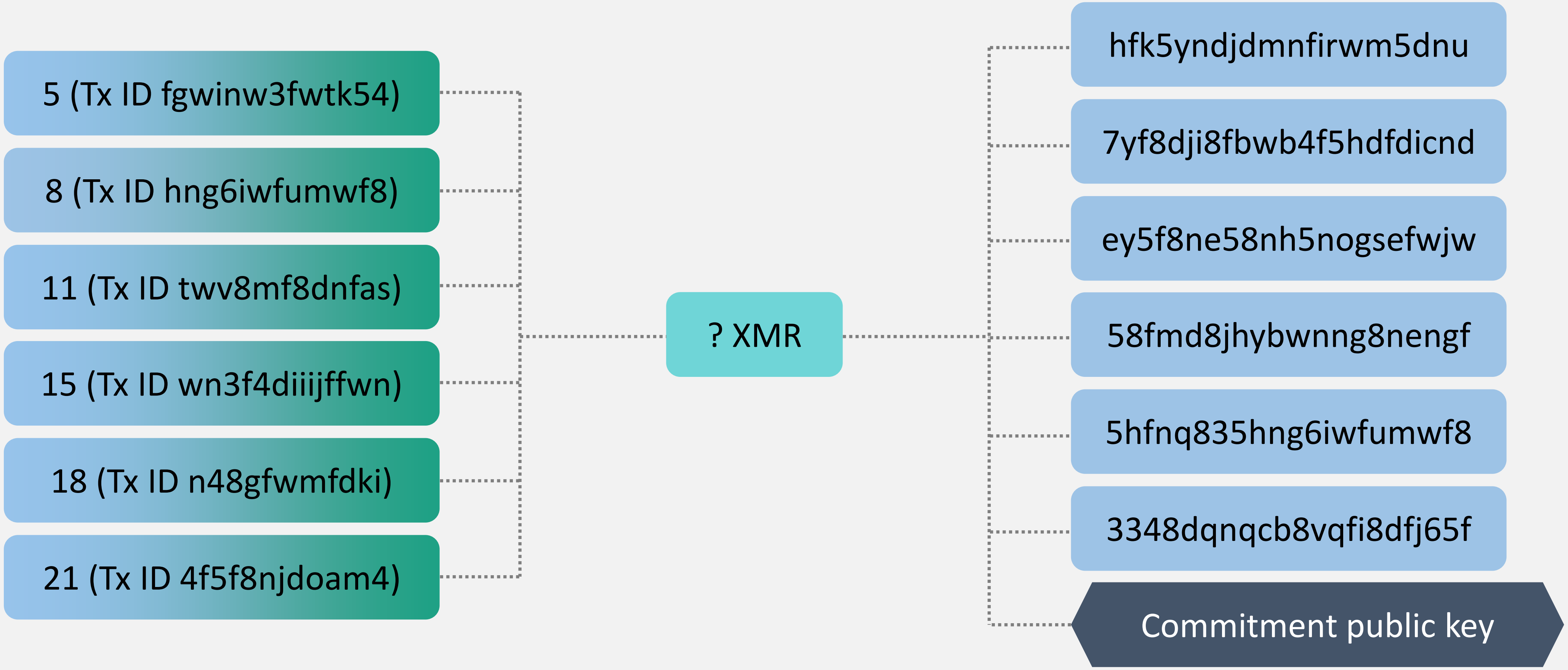
Releases

Alpha release coming soon

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

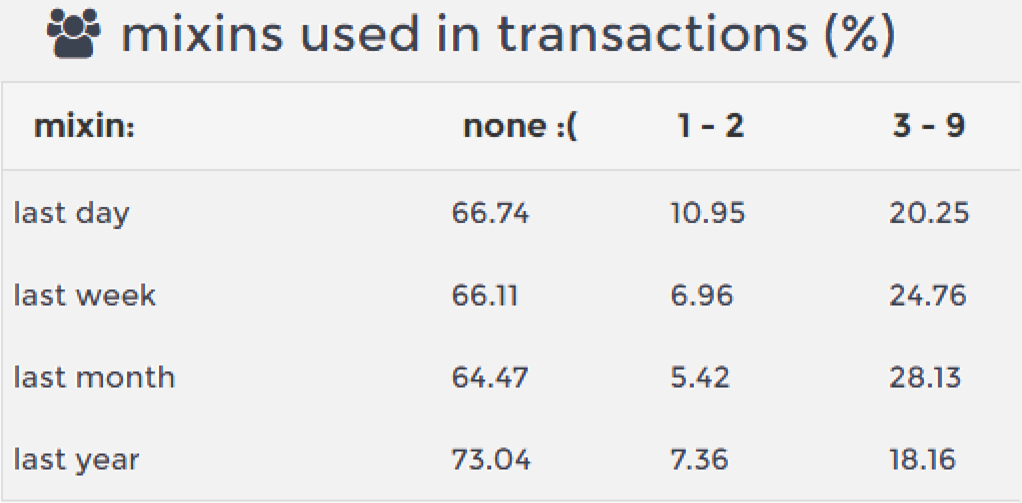
58fmd8jhybwnng8nengf

5hfnq835hng6iwfumwf8

3348dqnqcb8vqfi8dfj65f

Commitment public key

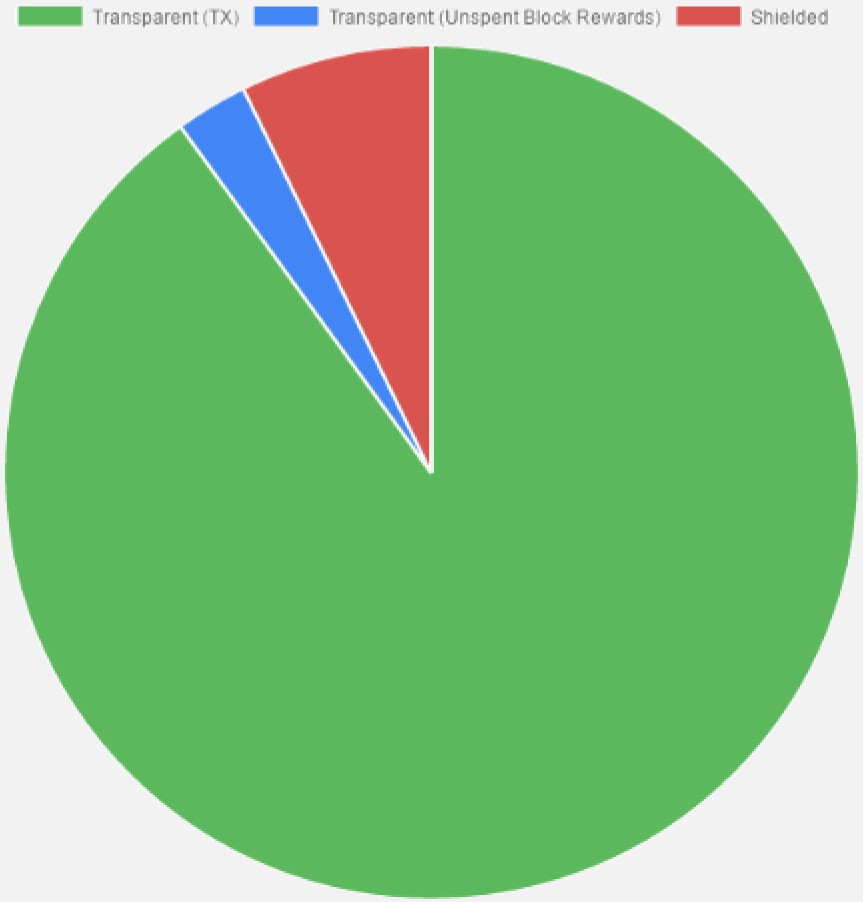
Mandatory Privacy



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

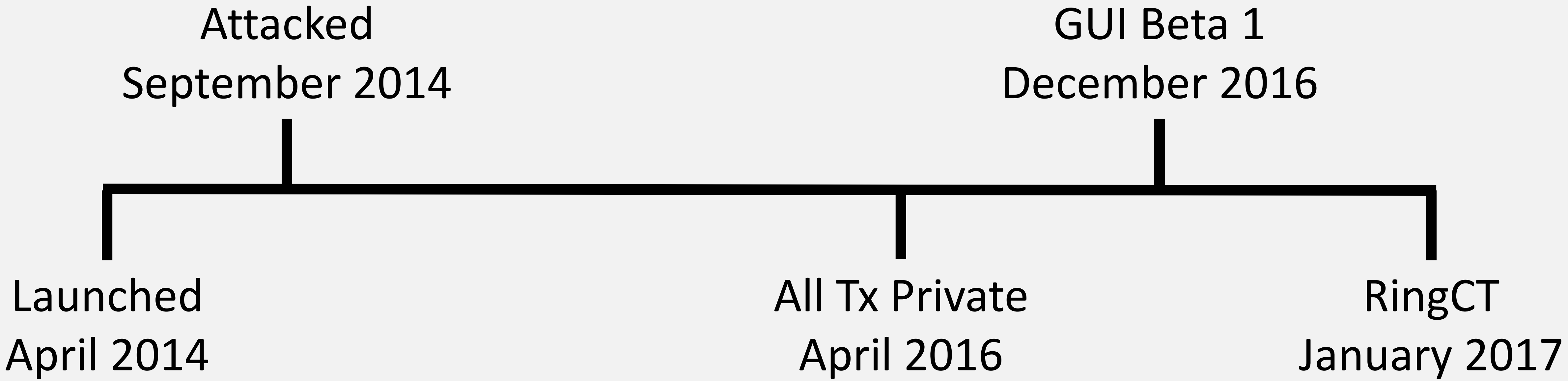
Adapted from Fluffypony's Slides

Evaluating Privacy Technology

Monero contributors know that our code:

- Is responsible for securing people's money
- May need to protect someone's life savings
- May need to keep an innocent person out of jail
- May mean the difference between life or death

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

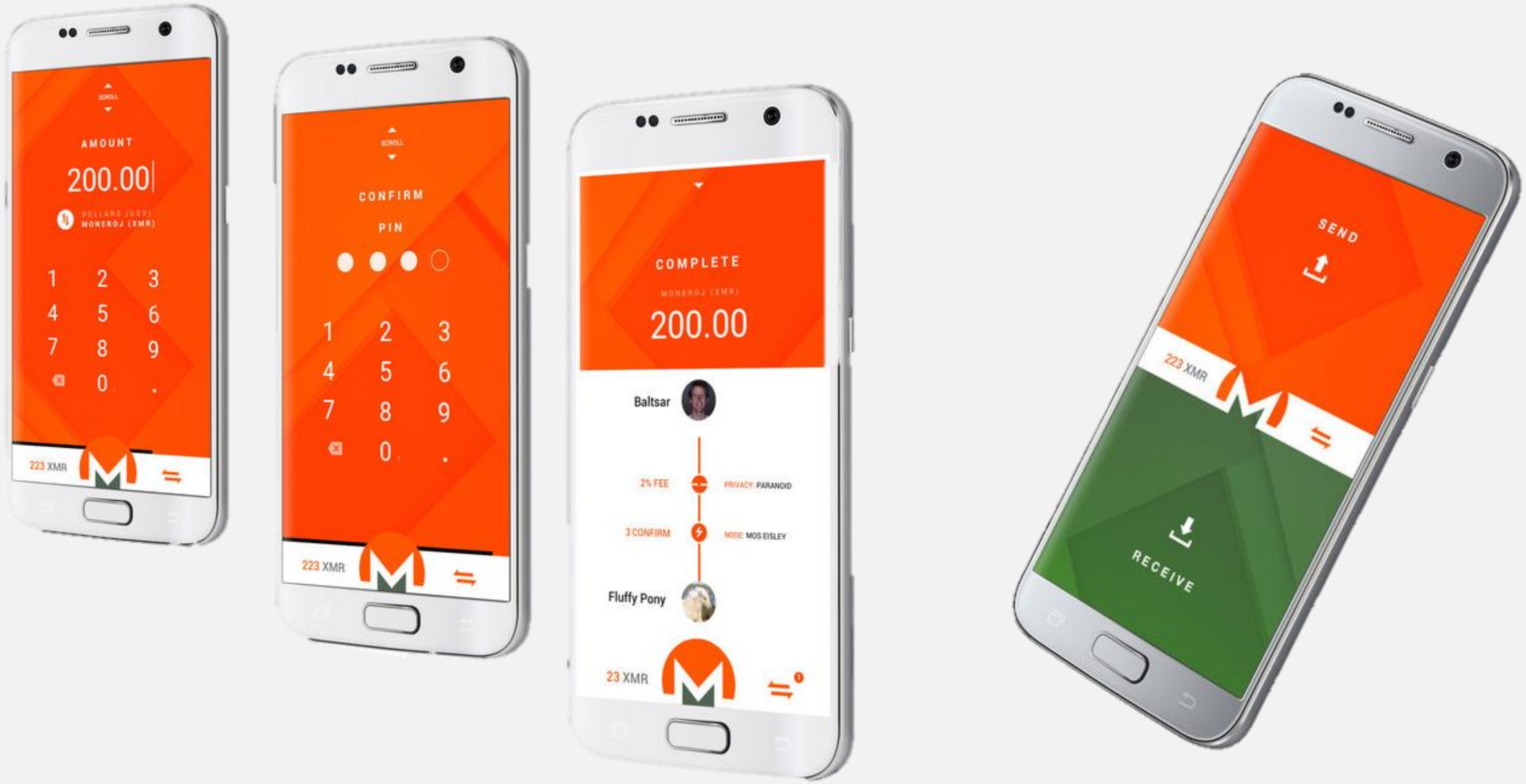
By publishing their view key, charities can invite easy public oversight

Parents

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

Monero Limitations

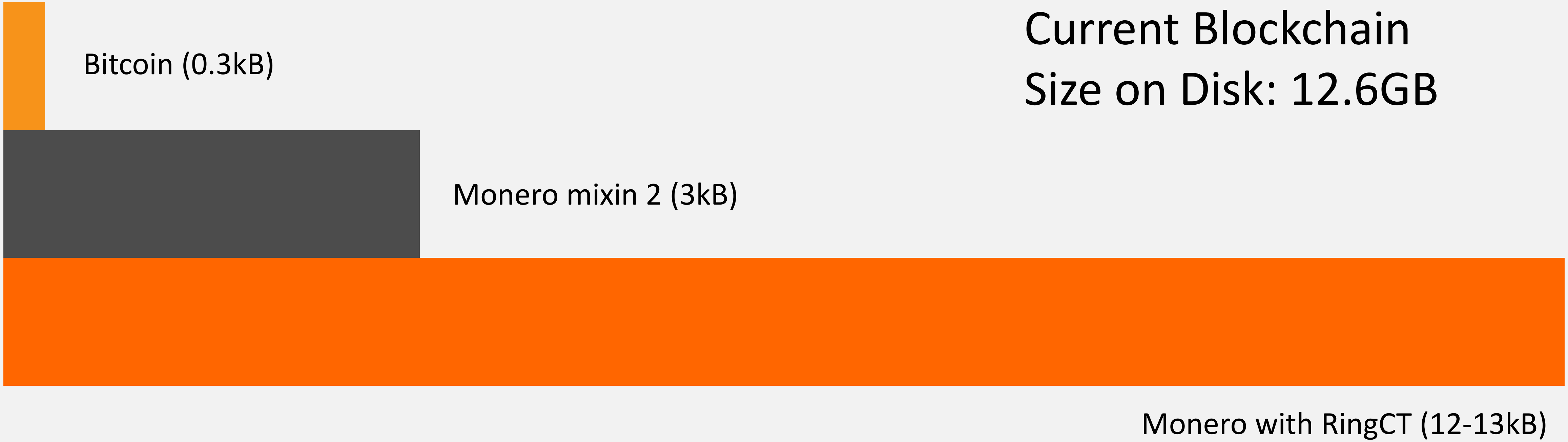
Monero Limitations



Monero Limitations

Send 0.024 BTC to
18PnKsP1f3mVnKg32aS4TMHXmCMg99R6f8

Monero Limitations



Current Blockchain
Size on Disk: 12.6GB

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

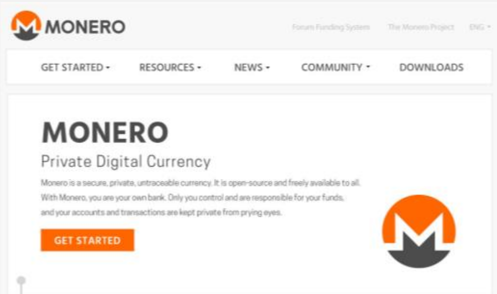
Multisig

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

January
April
September

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