SECURE. PRIVATE. UNTRACEABLE.
MONERO
Athens, Greece

Welcome

Justin Ehrenhofer

Finance
Management Information Systems

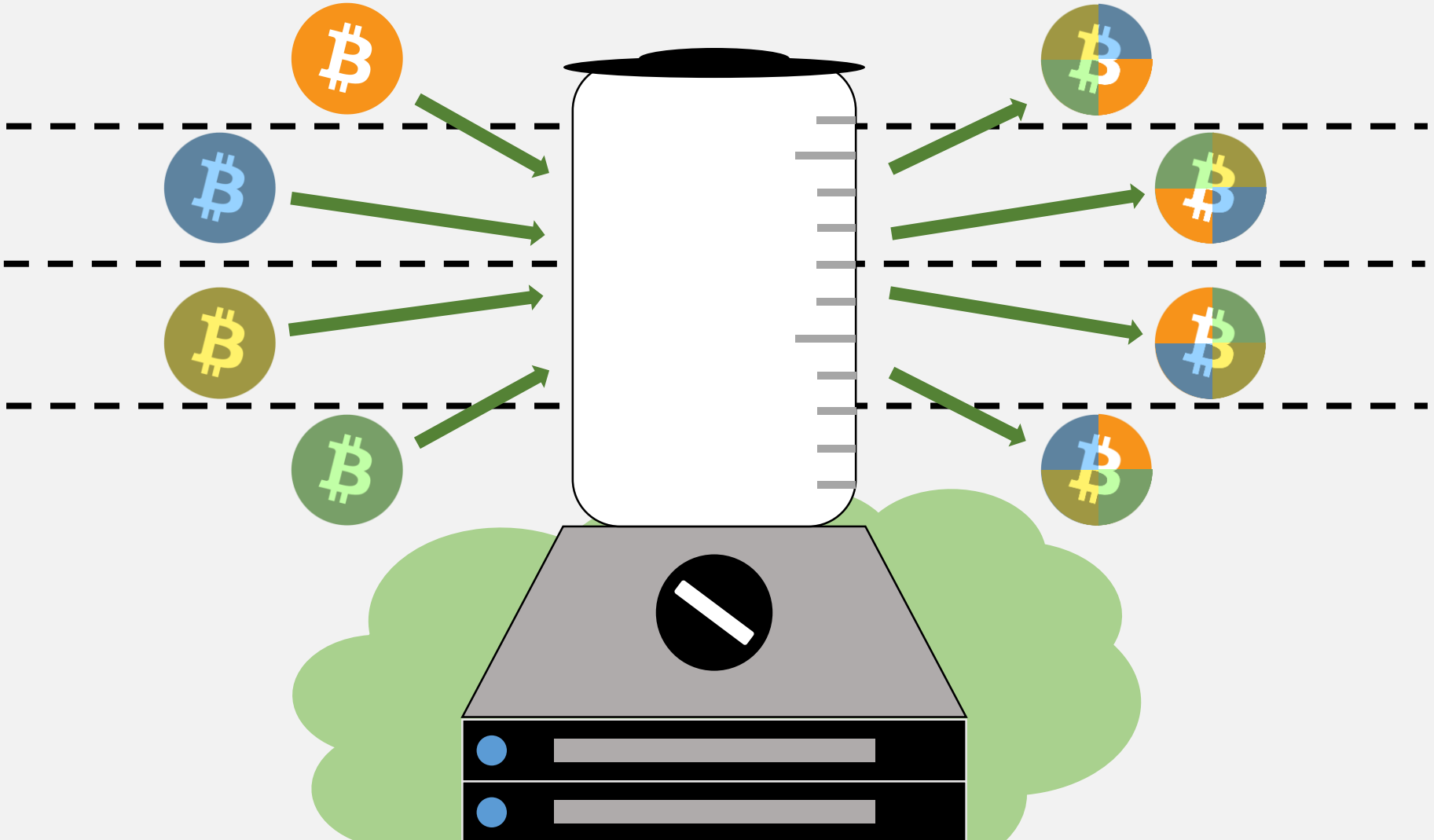
/u/SamsungGalaxyPlayer or sgp_

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

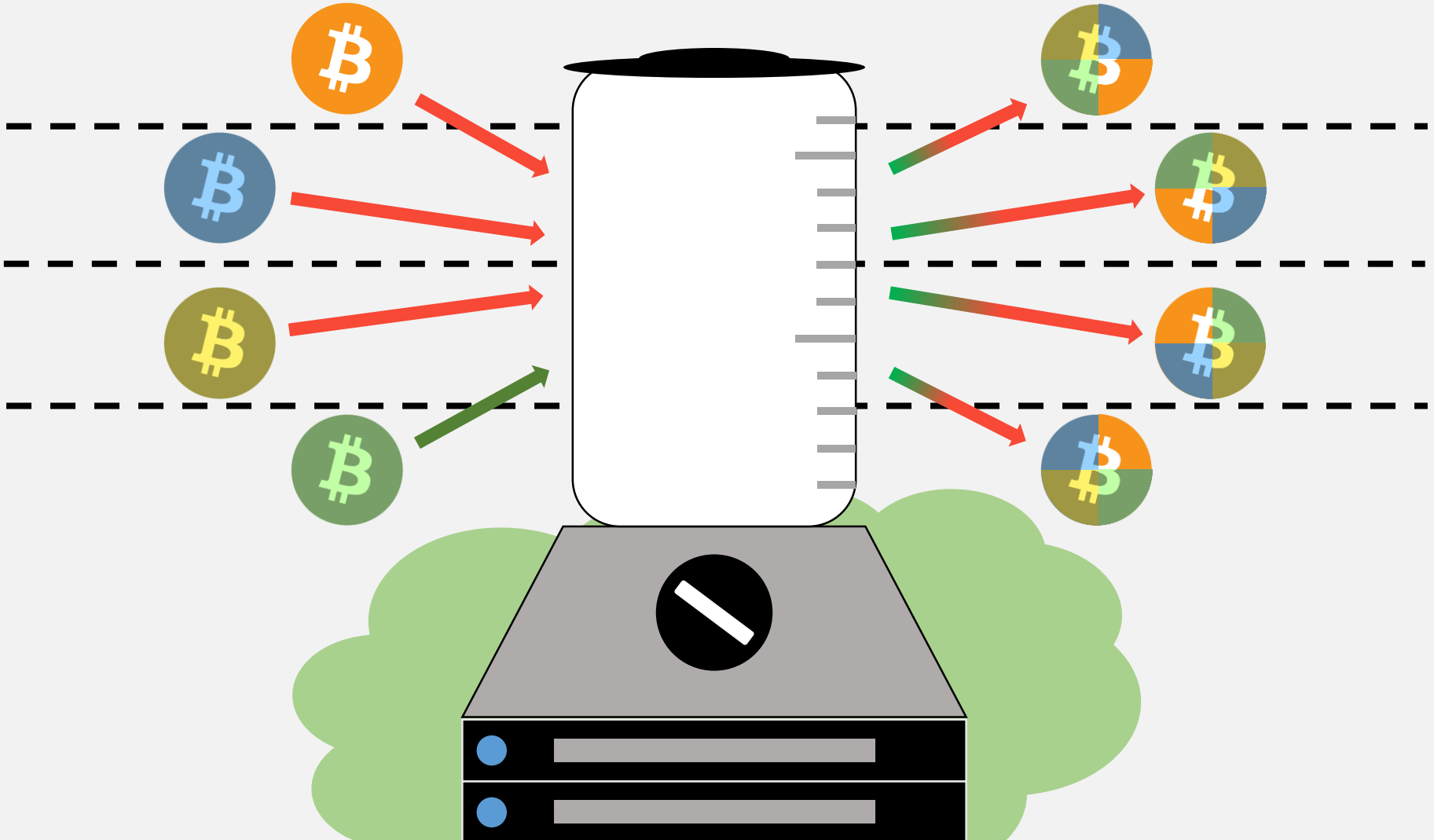
UNIVERSITY OF MINNESOTA
Driven to Discover℠

CryptoUMN.com

People Started Adding Tools to Bitcoin

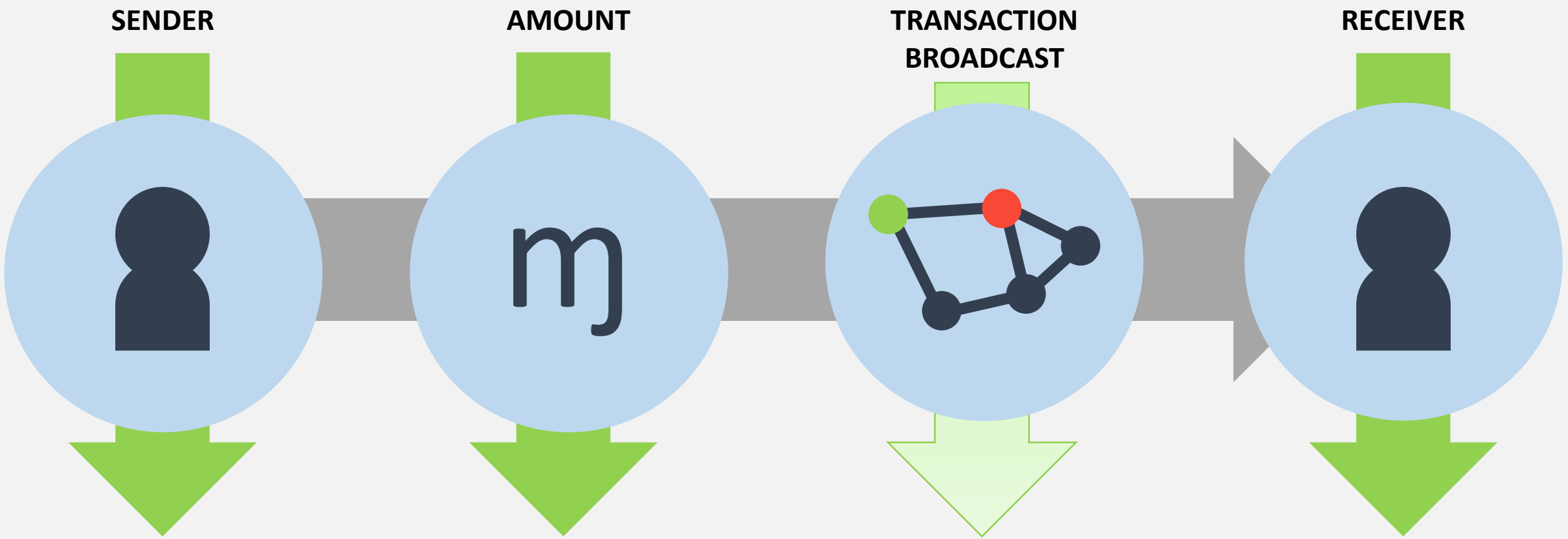


People Started Adding Tools to Bitcoin



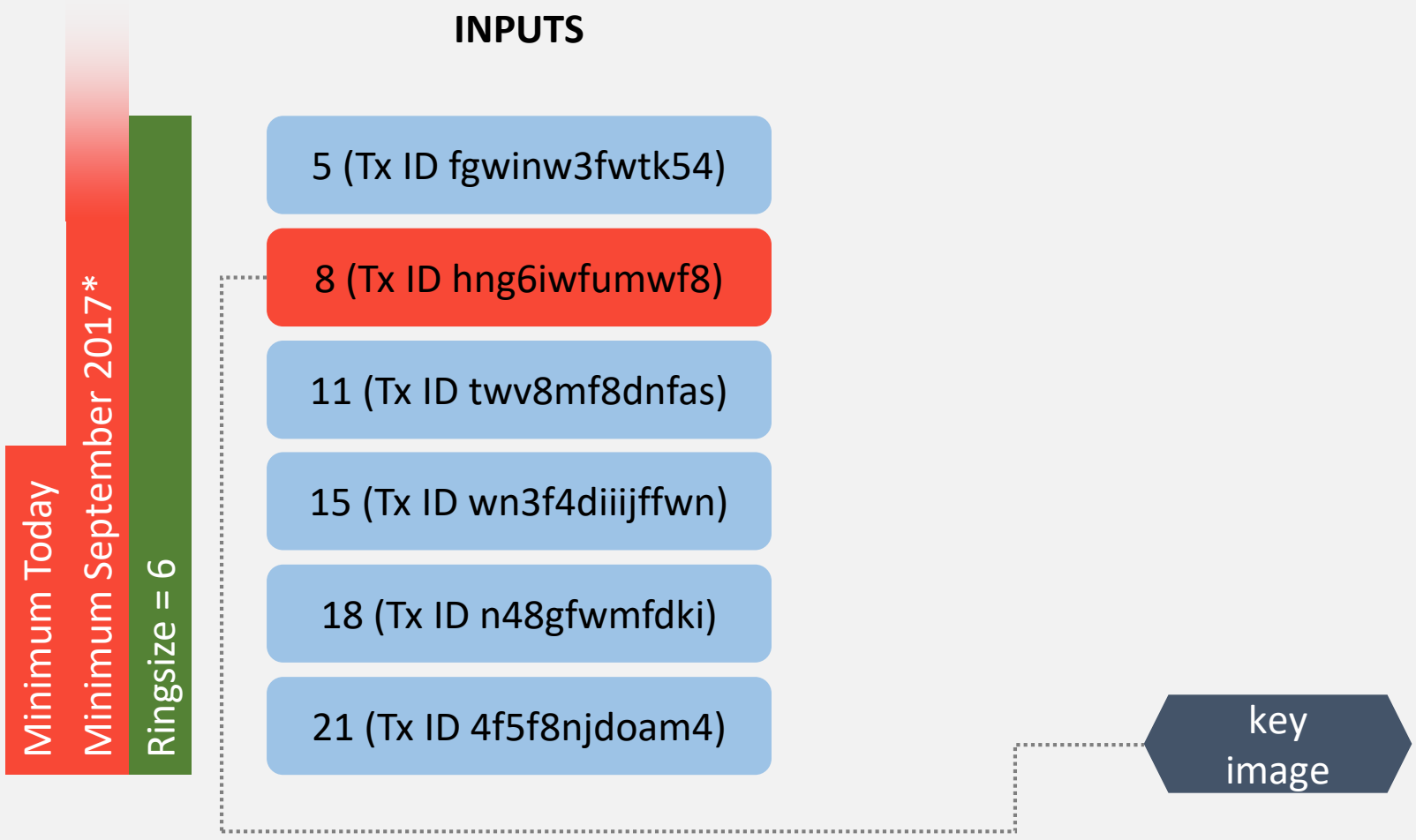
People Started Adding Tools to Bitcoin

The Monero Difference

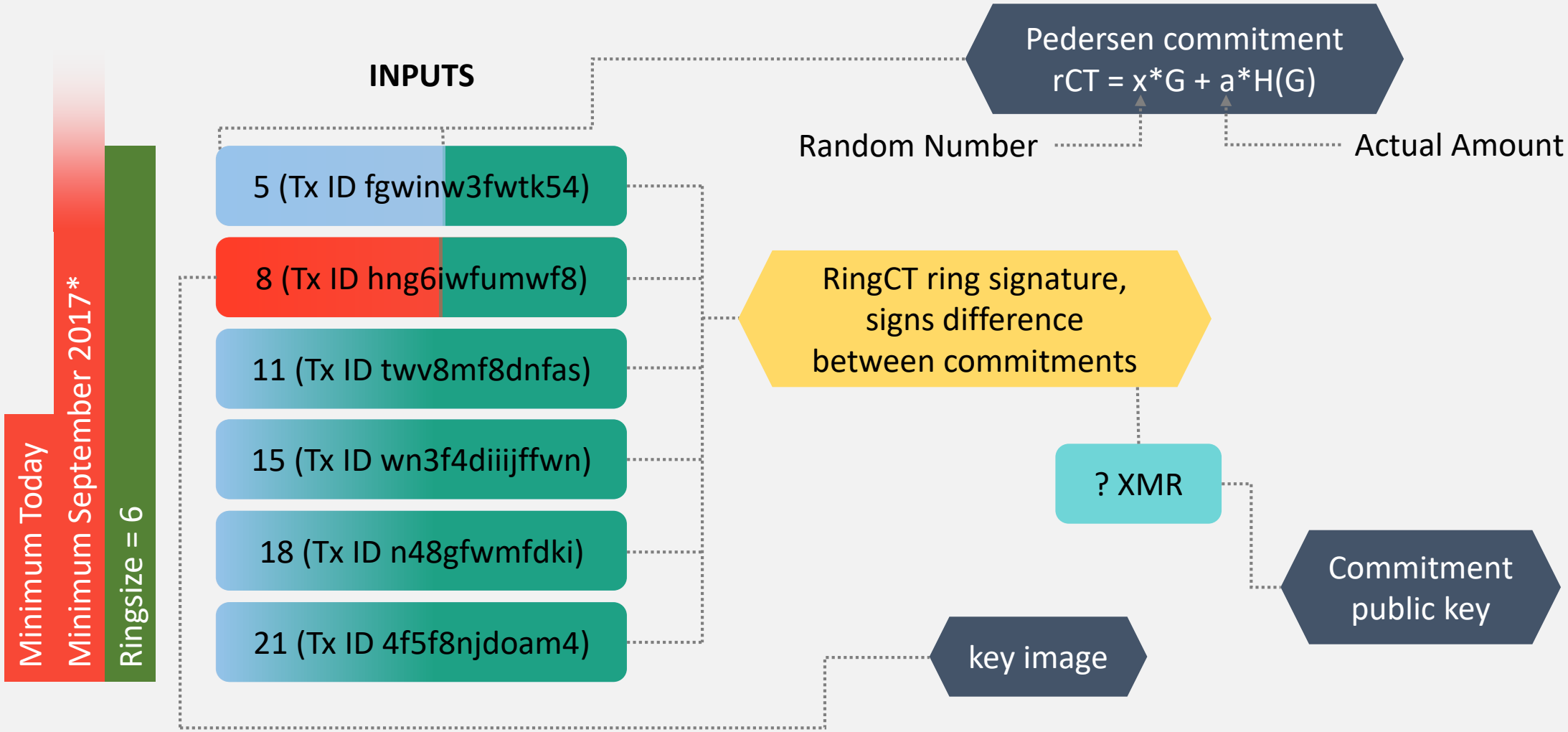


Ring Signatures & RingCT

Ring Signatures & RingCT



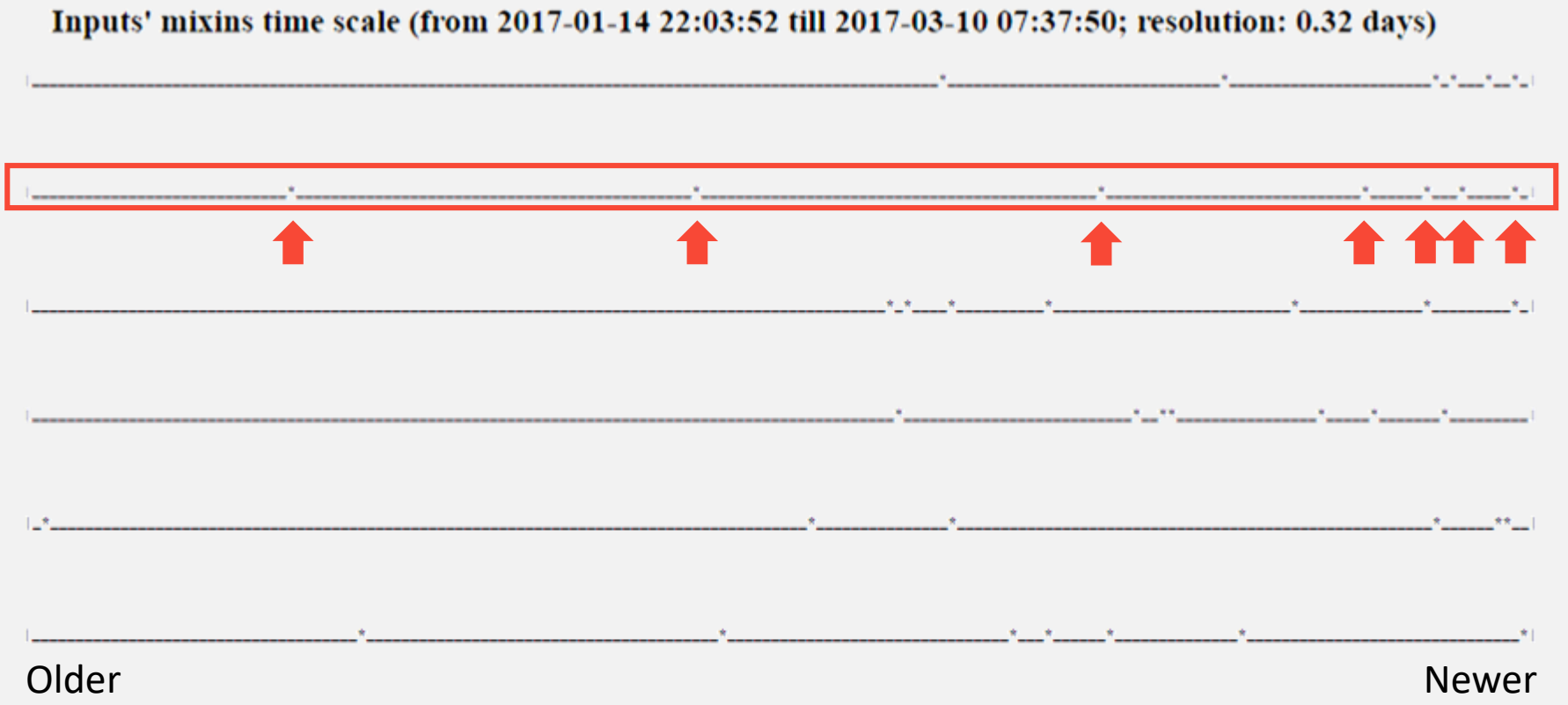
Ring Signatures & RingCT



Ring Signatures & RingCT

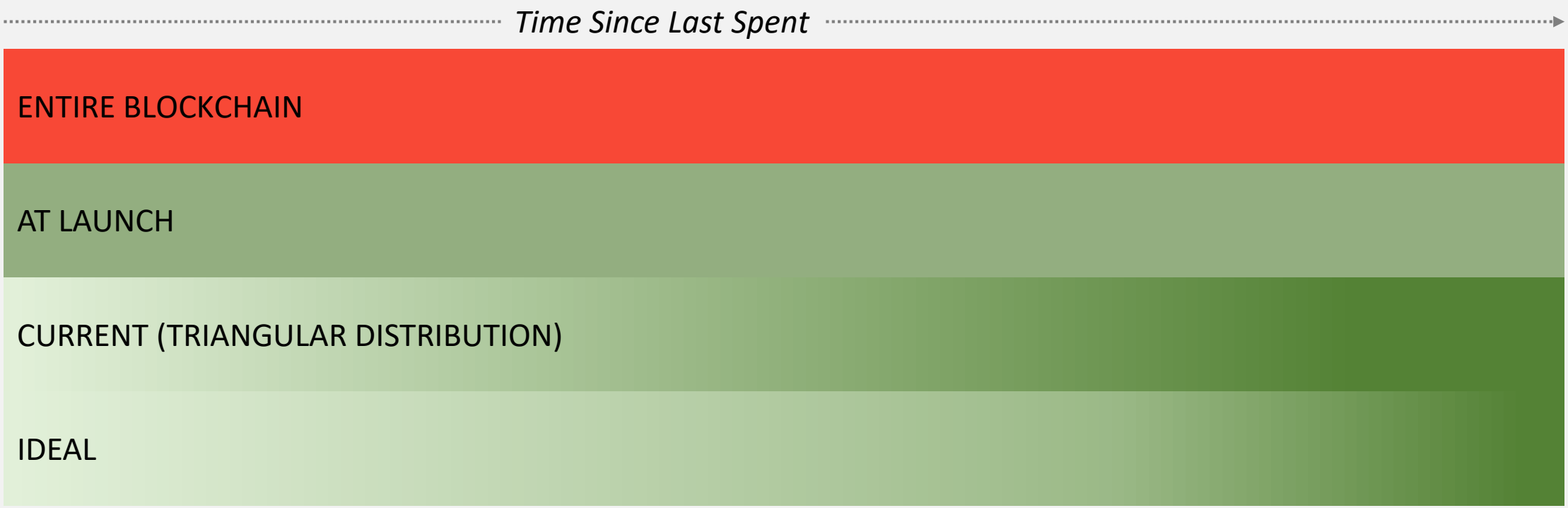
INPUTS

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

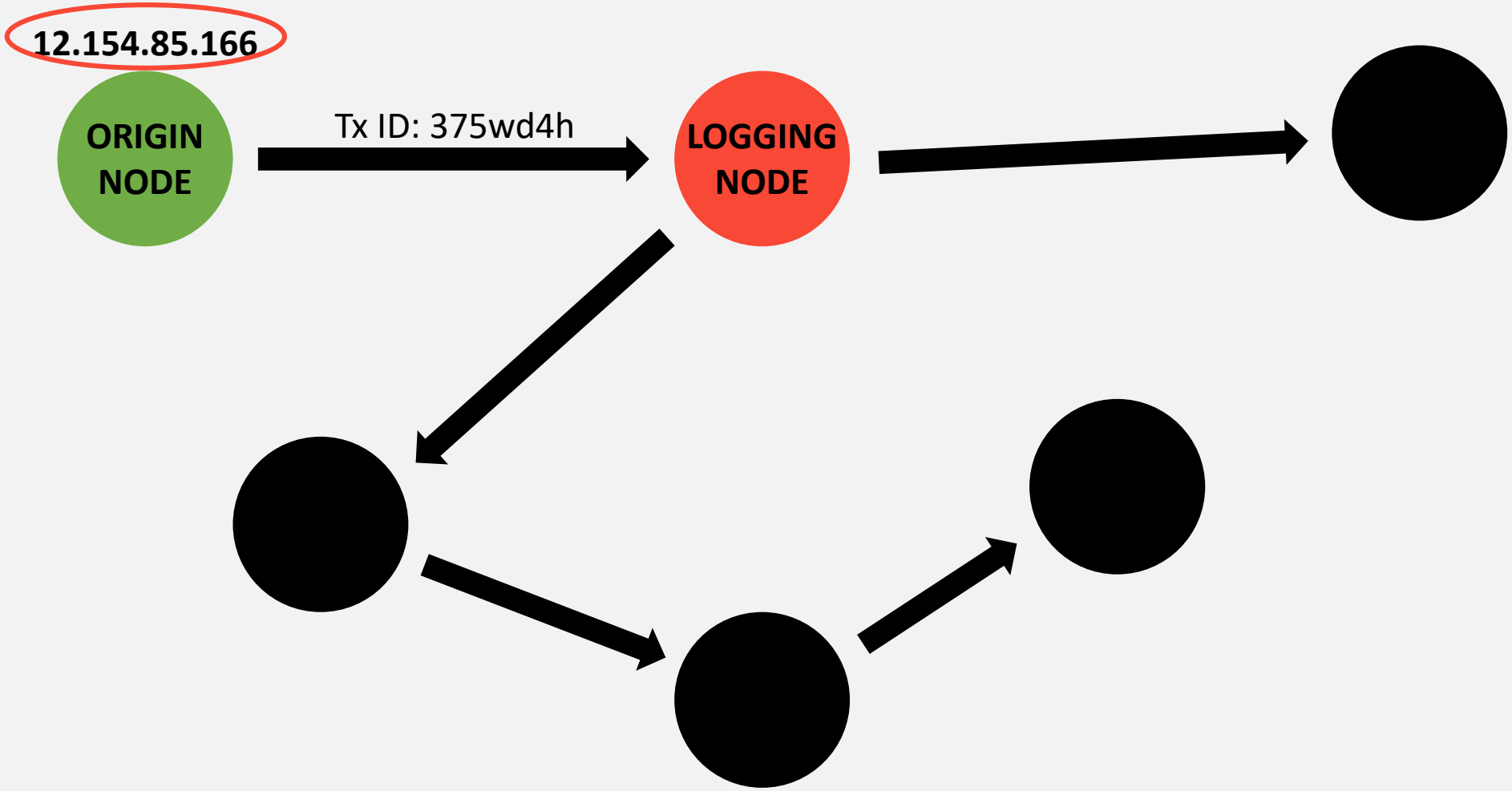


https://xmrchain.net/search?value=9bb608c70622ce67333c267103241f19b8aca21b7915f237813e451e1f03576e

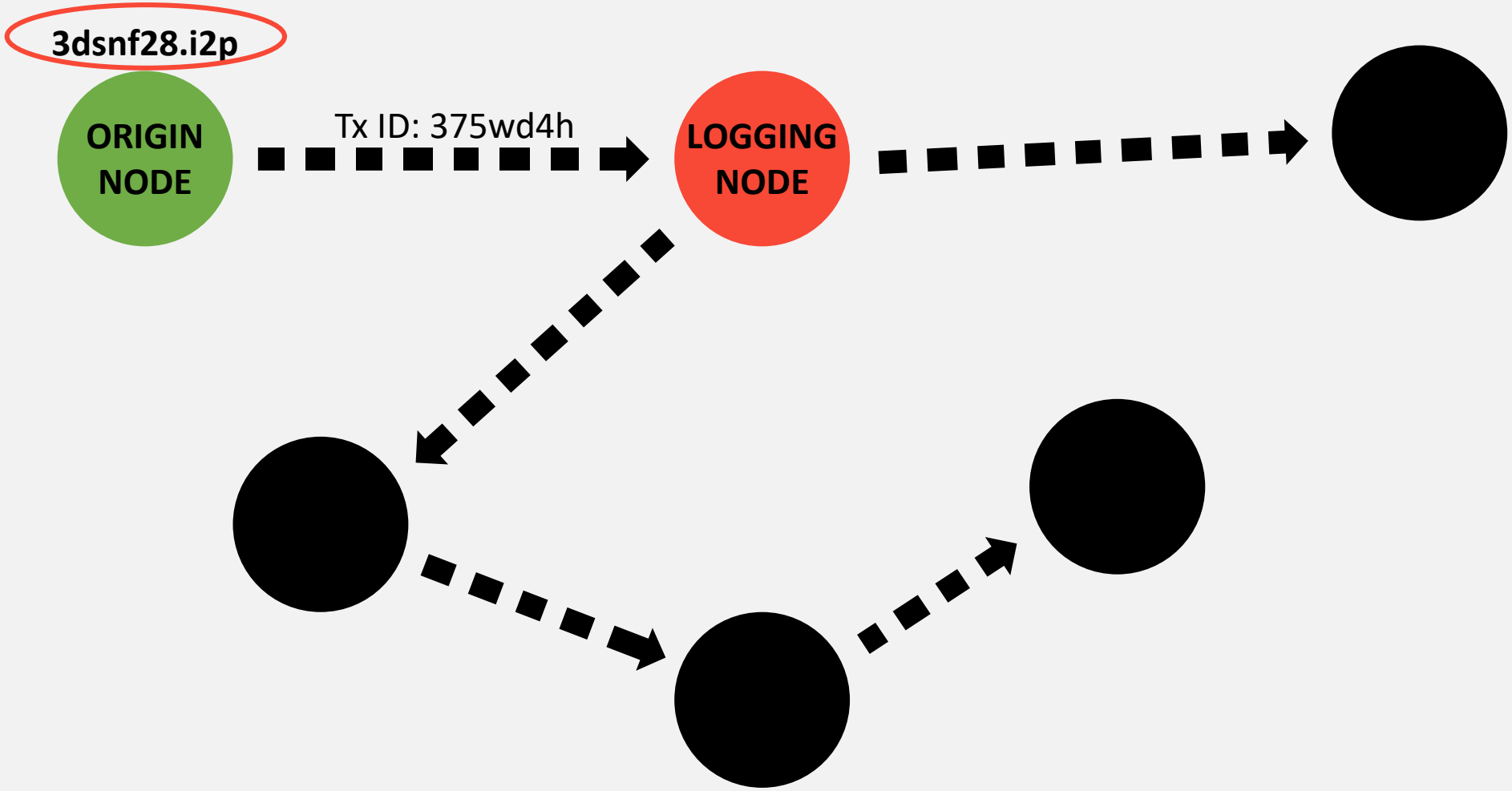
How Inputs Are Selected



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

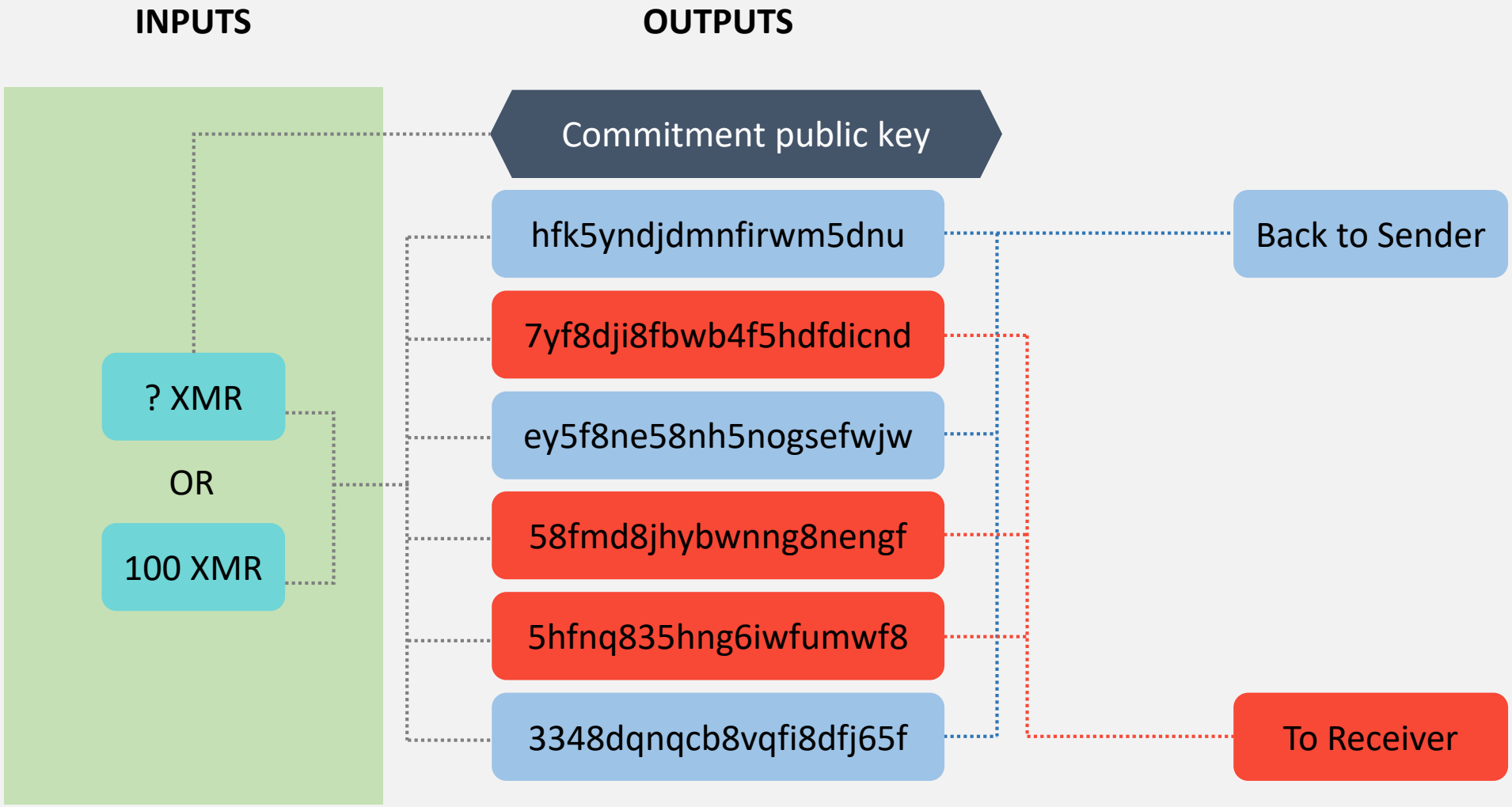
```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2

iQIcBAEBCAAGBQJWsJidAAoJEGanbs+RRAnxt68QAJm8K9WeVP/1WJ6OCSLa9Cpo
uC4h1FrBSTZp0BJ+WHGG9m3IuMmn1jVchFvrHdmtuzP3l0Both+riLb0keGaiM2
r/L+tnqvGmOw4acdS0FDHFLAR9t+rqCWK6YGOzguOAGG15nhRLxTjdUn1ED3n35S
SLrKtKAXGj25j9zbTVpPxevmEbjUFdq85LcqVxBSR7al+QaaWy46xP8Ws4Mo/1it
J/rYFpVRaqTXGhG1mMek42cKJ1E0Yqu1bSxcHDEm+H65vNY1chfe3Ljc/96bFYBV
4M5s2/pS9yC1ckJeLtFhi2mXxVe/ZKXTALvffzWH8aVmbY1wXo2ONXyvc2kz2R9b
1P1aRbY0KO0Q4xxsDg+GBiX28Fh2kmpOvvLXNBIOOkbBoSJQD0FoXCRqb7GNiC/c
5qsOX1ZkNHQo8FDLh3+ZCUELsBK6ei35Ezum/xwyoq4kJUV28mABZhyQ4AOWlUjW
DSxnQx9efdhIf64klY5aZJxJC9U8beY1qov71T/fP9yX15fdmovb7XY8mTT4Jp1T
tP4lfvmr1tc5r1lQ0BeXaGwsBzP+THLEzRTVoQpIoAqhWCVXbU/vUz5/cxMNw8QM
ZxsC7yg2gUKv5FslHX/WEIW2LlQldMW/rnaZs5/hOTsSvTquIwS3Q4zY8Cc5SfNn
94fzWouiMa2wKFVDsfqB
=LwWl
-----END PGP SIGNATURE-----
```

Downloads

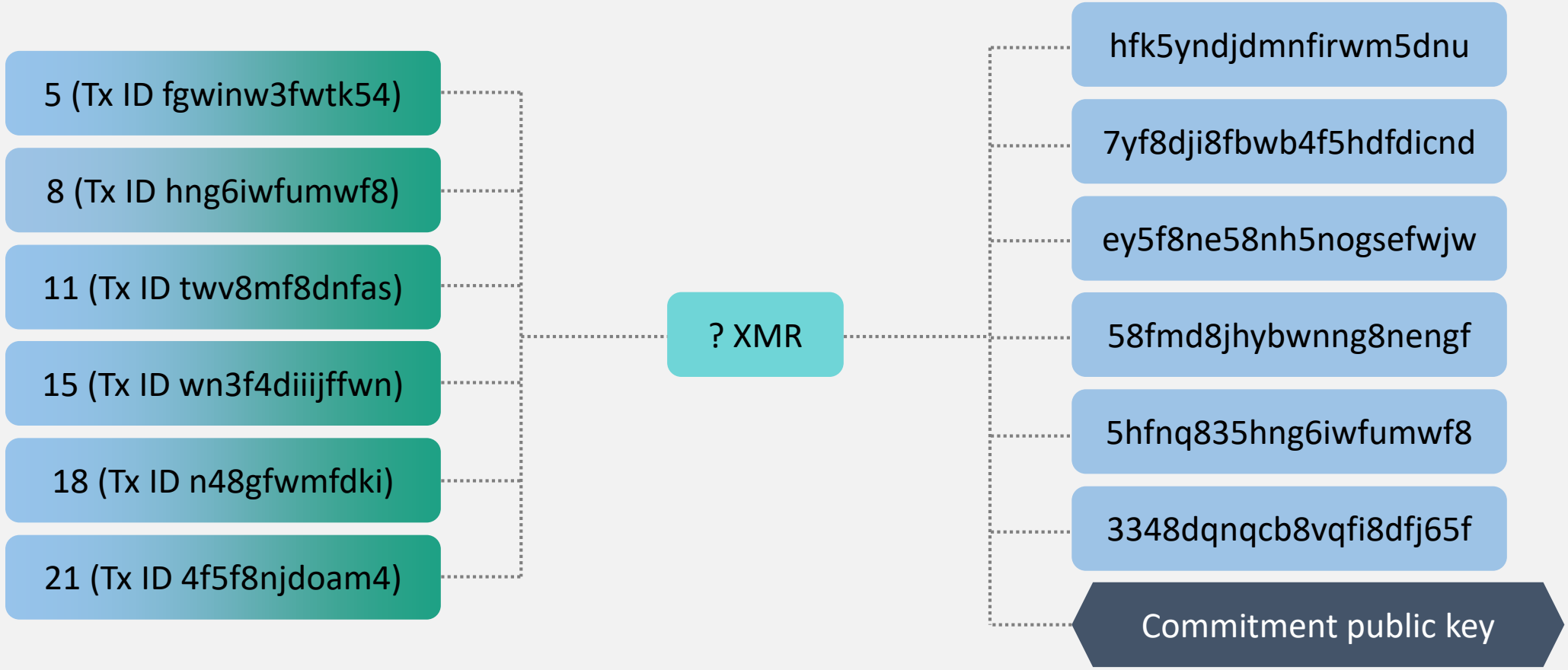
Releases

Alpha release coming soon

Stealth Addresses



Summary

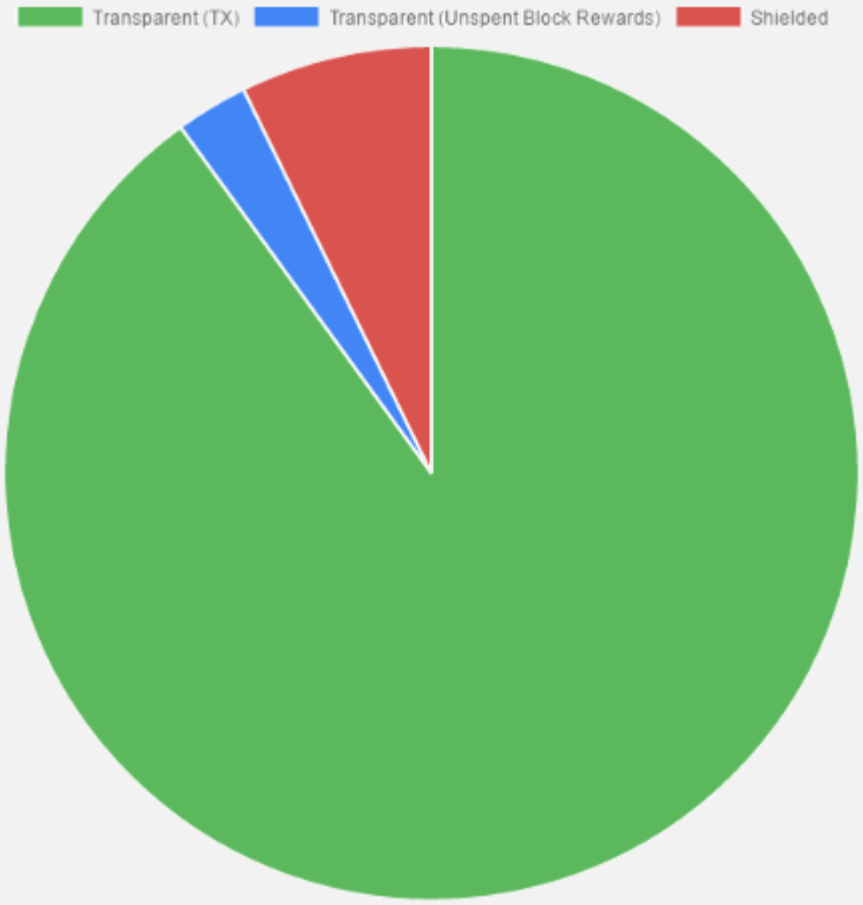

5 (Tx ID fgwinw3fwtk54)
8 (Tx ID hng6iwfumwf8)
11 (Tx ID twv8mf8dnfas)
15 (Tx ID wn3f4diiijffwn)
18 (Tx ID n48gfwmfdki)
21 (Tx ID 4f5f8njdoam4)
? XMR
hfk5yndjdmnfirwm5dnu
7yf8dji8fbwb4f5hdfdicnd
ey5f8ne58nh5nogsefwjw
58fmd8jhybwnng8nengf
5hfnq835hng6iwfumwf8
3348dqnqcb8vqfi8dfj65f
Commitment public key

Mandatory Privacy

mixins used in transactions (%)

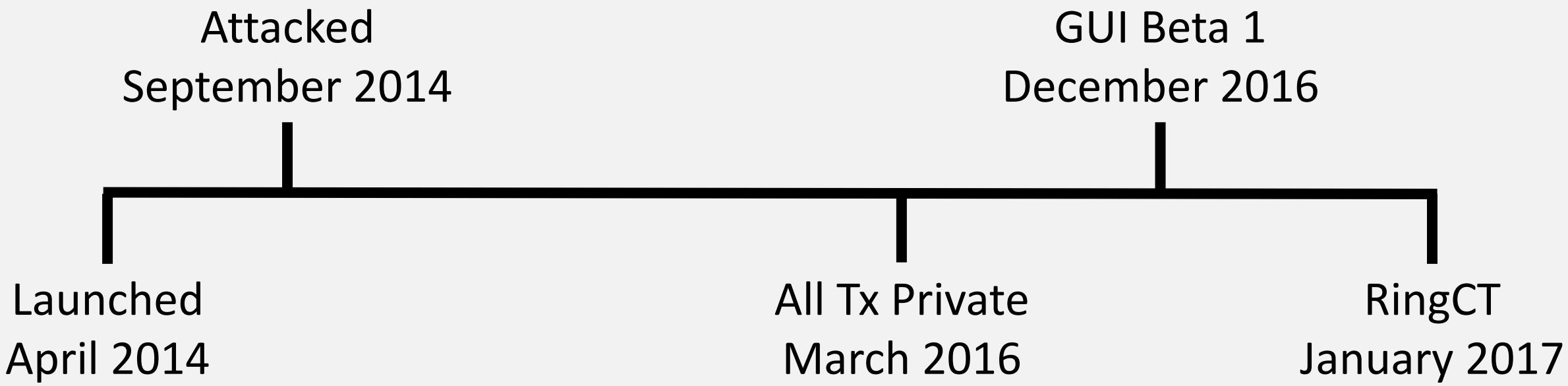
mixin:	none :(	1 - 2	3 - 9
last day	66.74	10.95	20.25
last week	66.11	6.96	24.76
last month	64.47	5.42	28.13
last year	73.04	7.36	18.16

Source: MoneroBlocks.info 24 Feb 2016



Source: zcha.in 15 March 2017

A Brief History

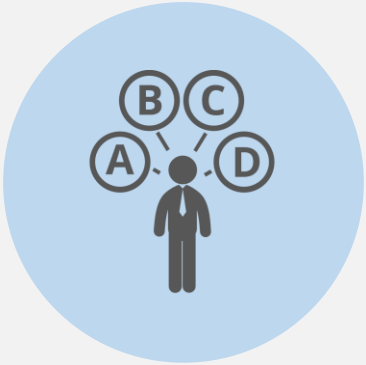


Regulatory Compliance and Transparency

(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

Charities

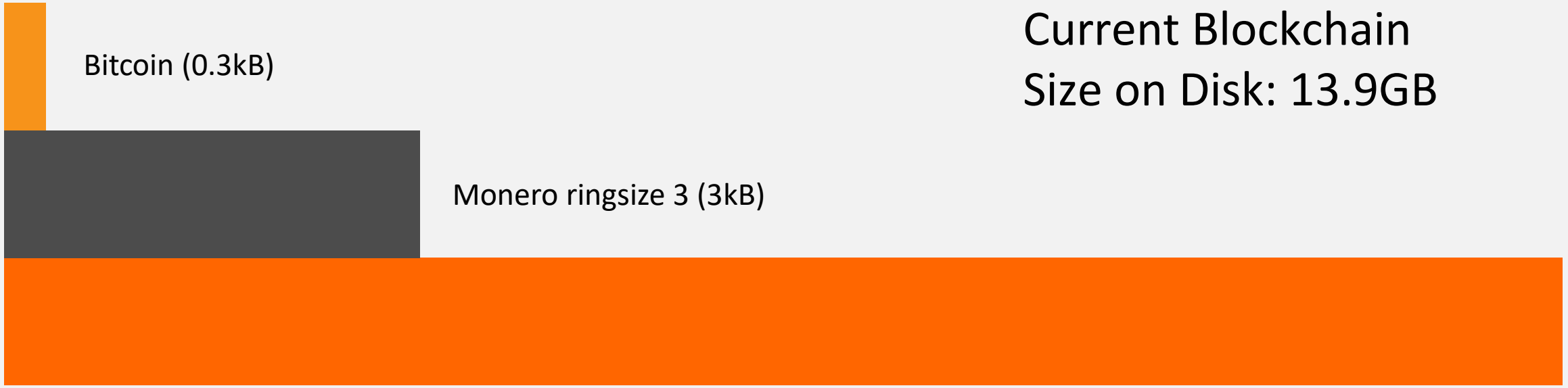
By publishing their view key, charities can invite easy public oversight

Parents

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

Monero Limitations

Monero Limitations



Current Blockchain
Size on Disk: 13.9GB

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

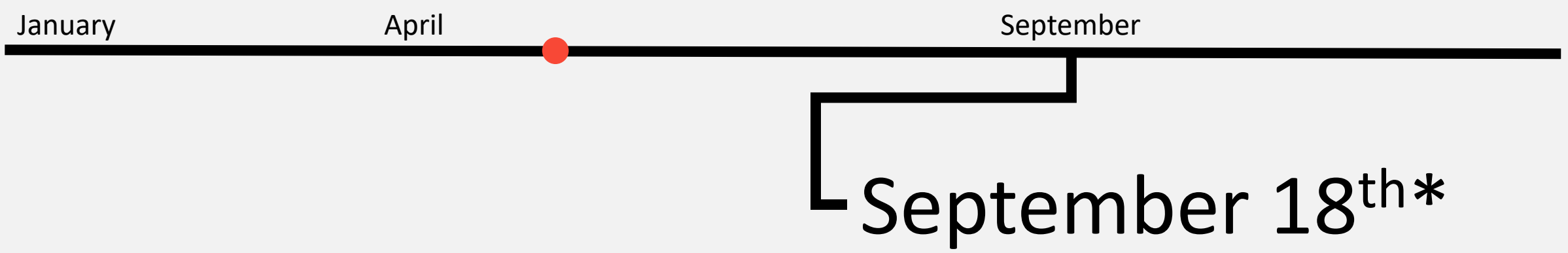
Sub-Addresses &
Disposable Addresses

Translations

Lightweight
Wallet

Website
Redesign

Hardfork Schedule



September 18th*

- **Mandatory RingCT**
- **Minimum ringsize ≥5**
- Fluffy blocks
- Improved input selection algorithm

Thank You!

getmonero.org

/r/Monero

monero.stackexchange.com