

SECURE. PRIVATE. UNTRACEABLE.



MONERO

Oslo, Norway

Welcome

Justin Ehrenhofer

Finance
Management Information Systems

/u/SamsungGalaxyPlayer or sgp_

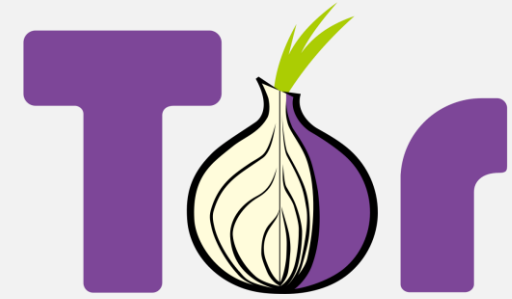


UNIVERSITY OF MINNESOTA
Driven to DiscoverSM

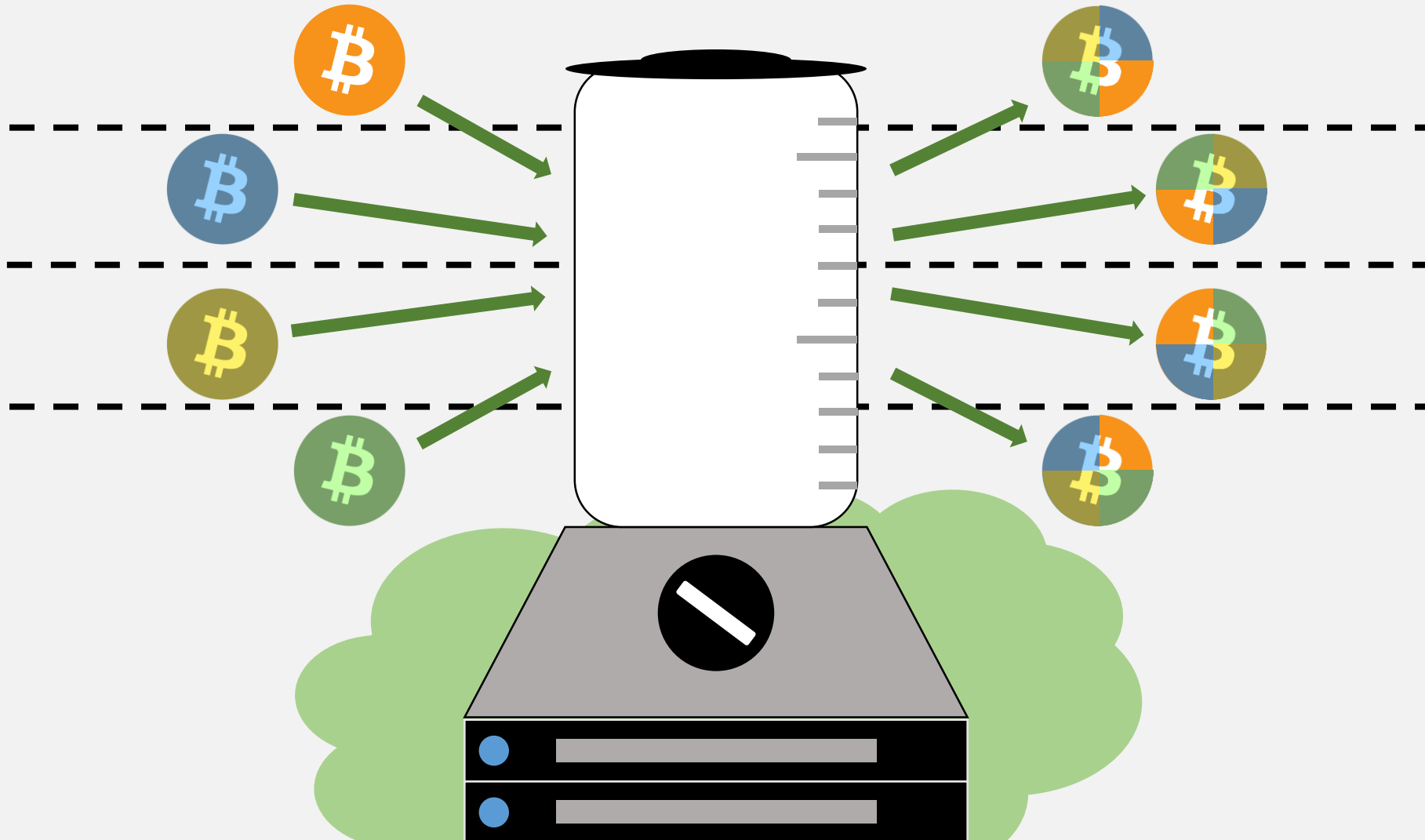


CryptoUMN.com

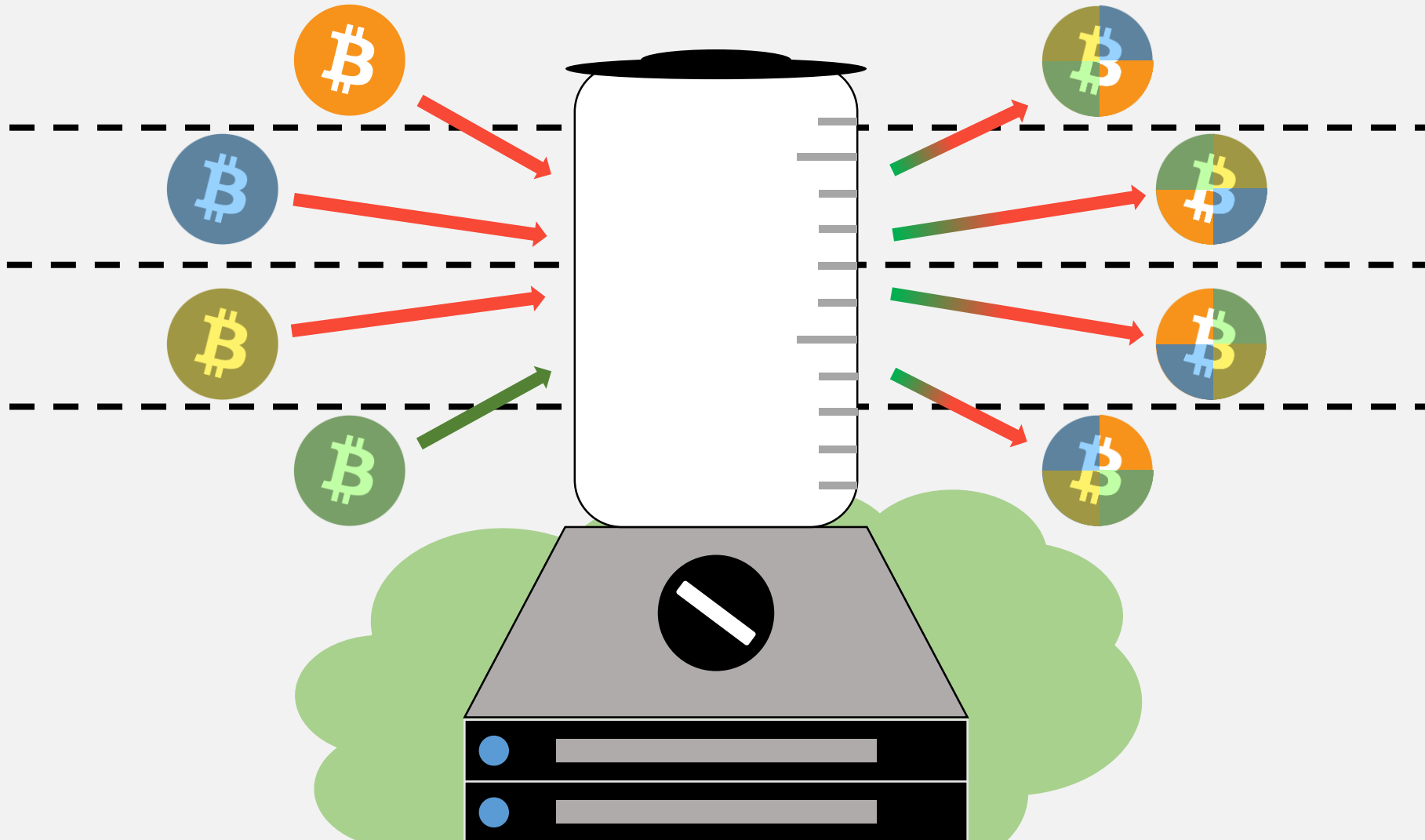
A History of Decentralized Systems



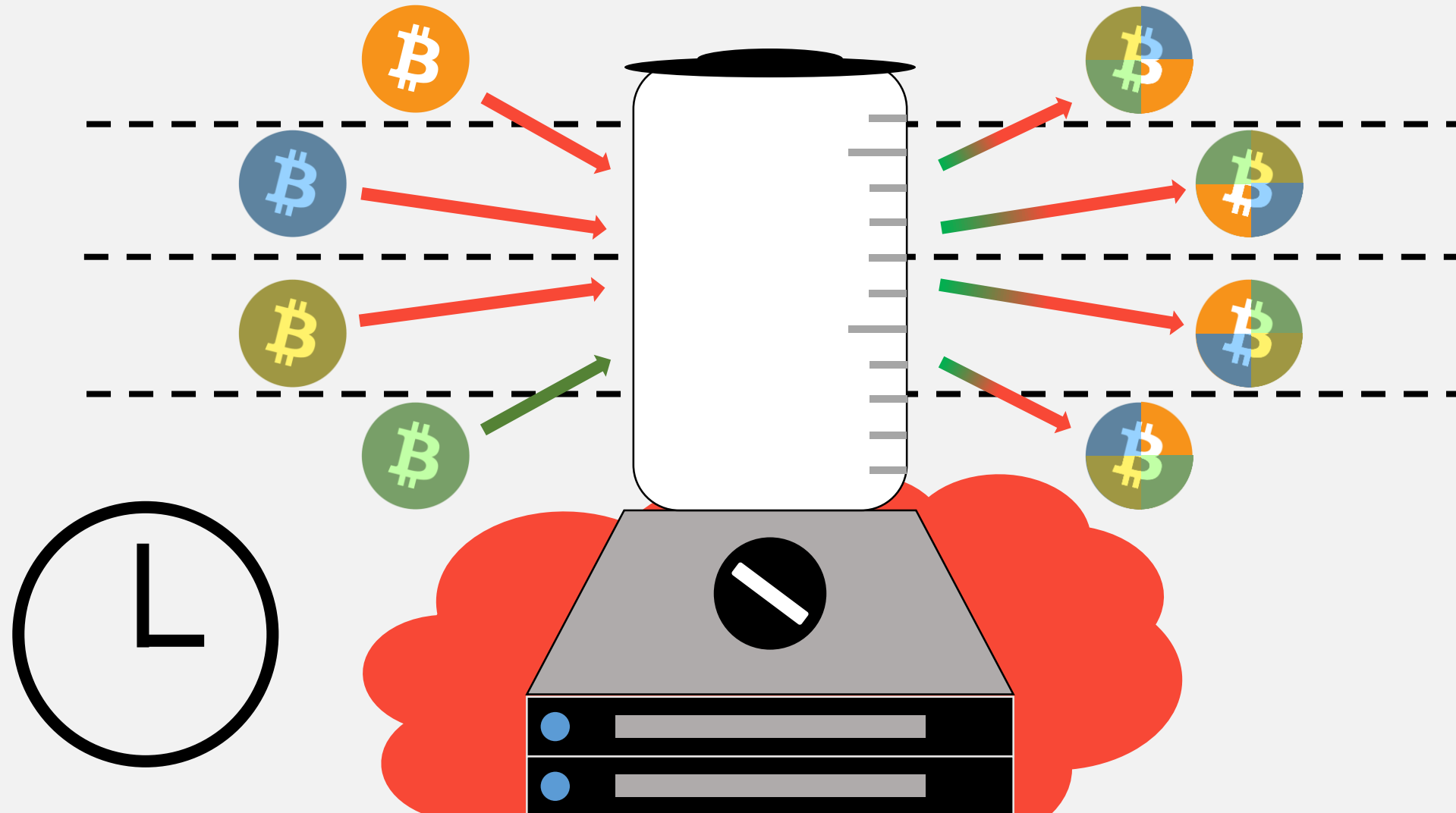
People Started Adding Tools to Bitcoin



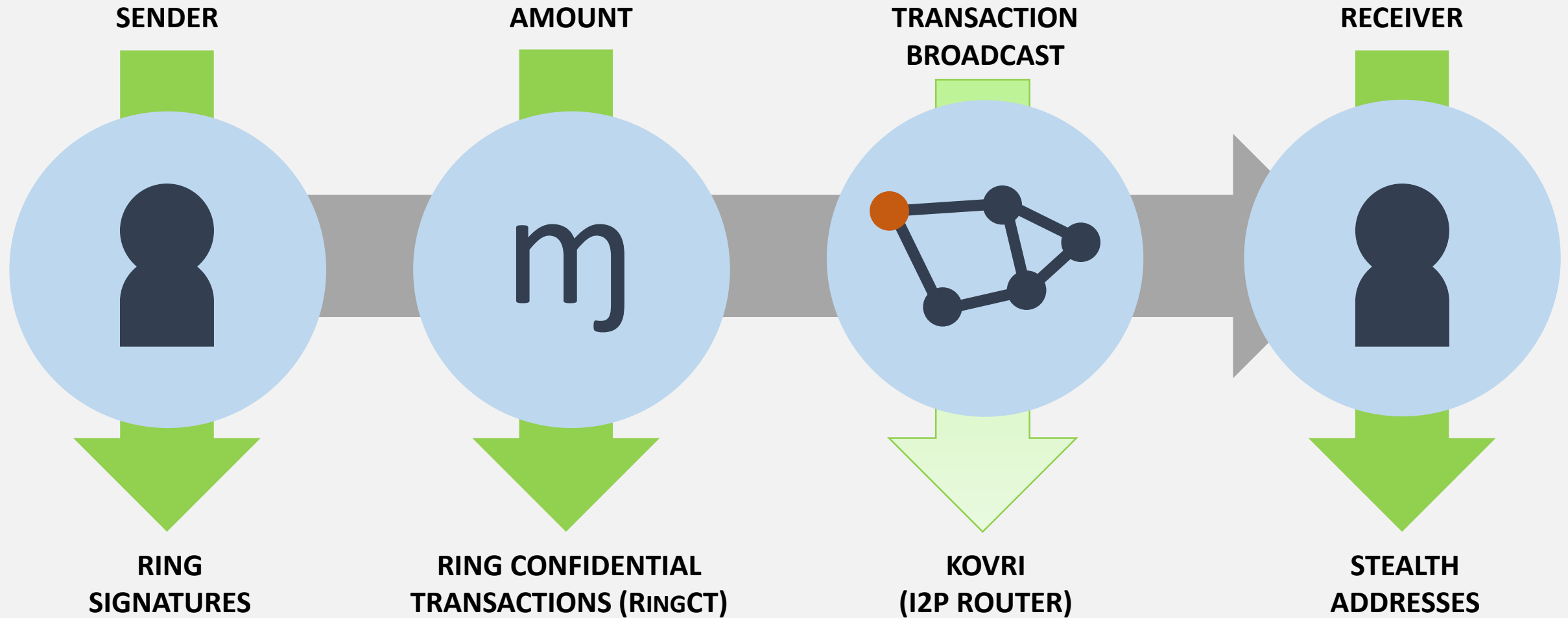
People Started Adding Tools to Bitcoin



People Started Adding Tools to Bitcoin



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)

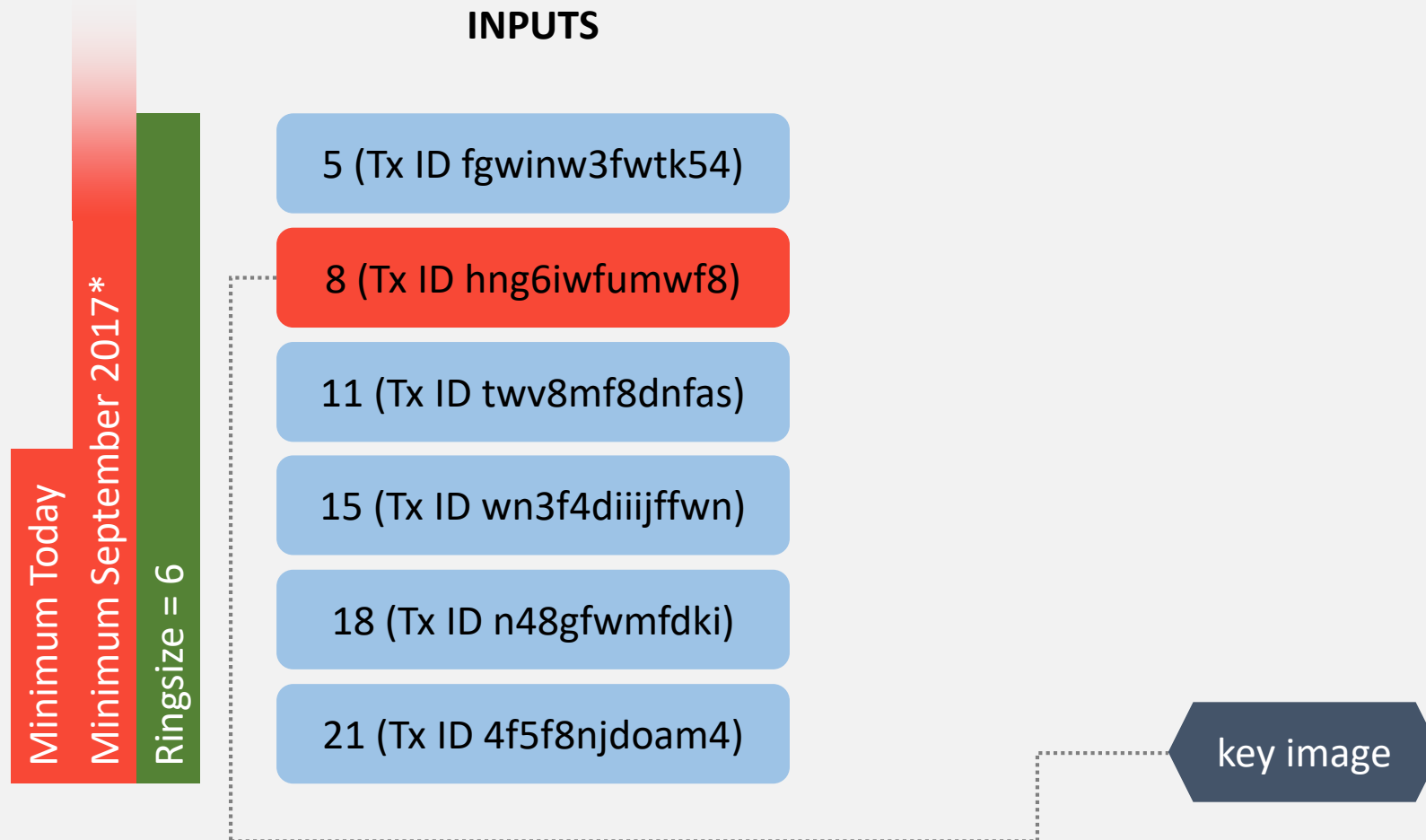
20 (Tx ID t4vn8lf8djer4)

7 (Tx ID e4bgn8flwwrj8)

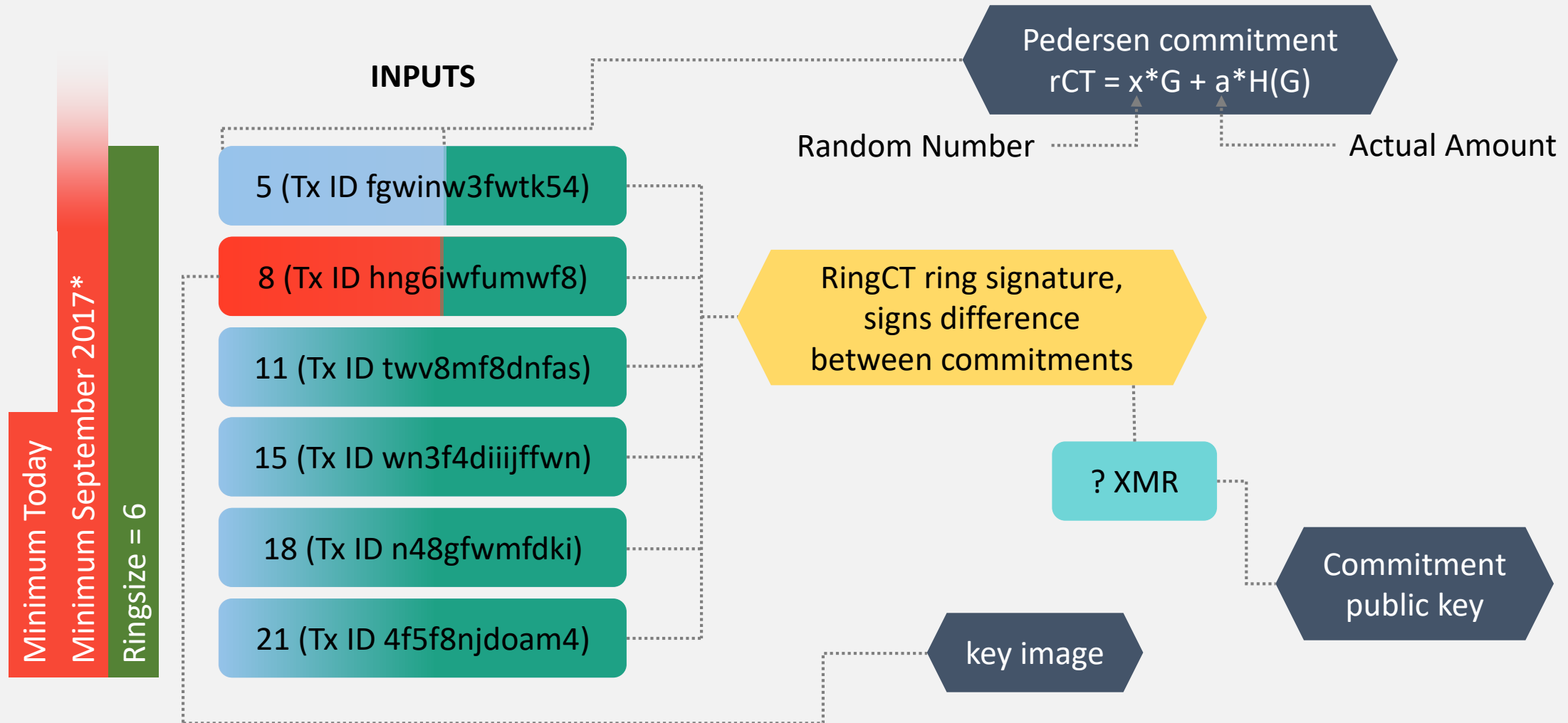
14 (Tx ID f8n8madkrjmd)

21 (Tx ID 4f5f8njdoam4)

Ring Signatures & RingCT

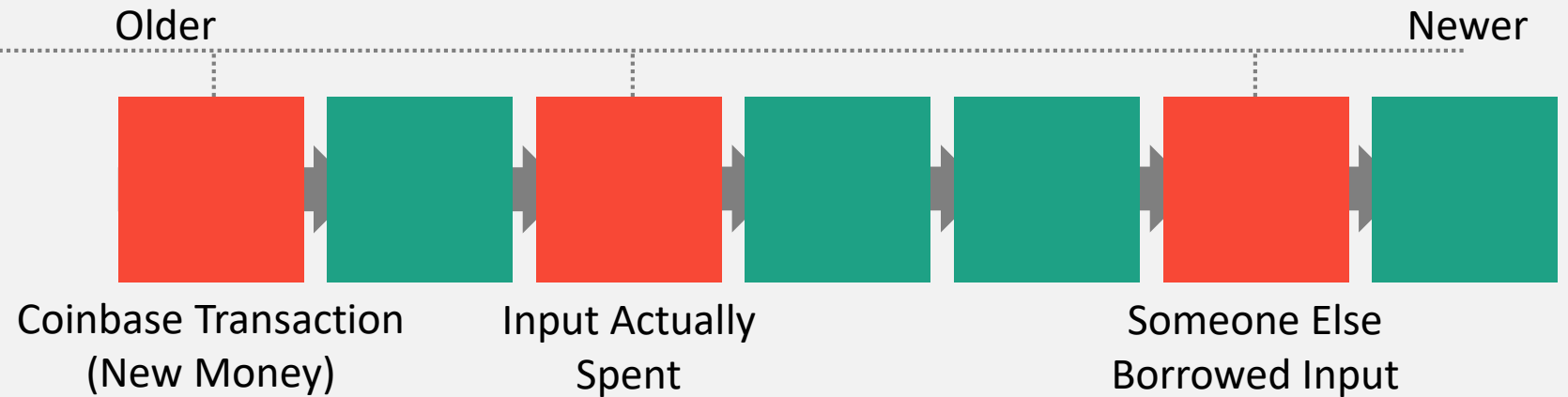
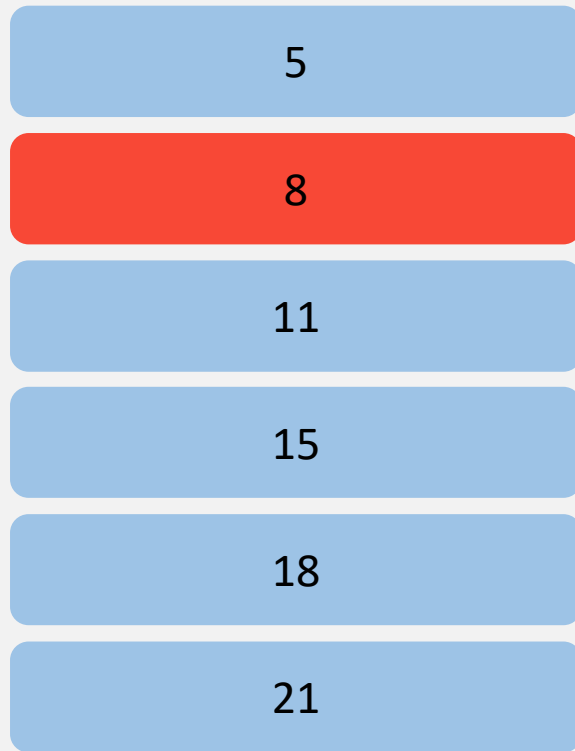


Ring Signatures & RingCT

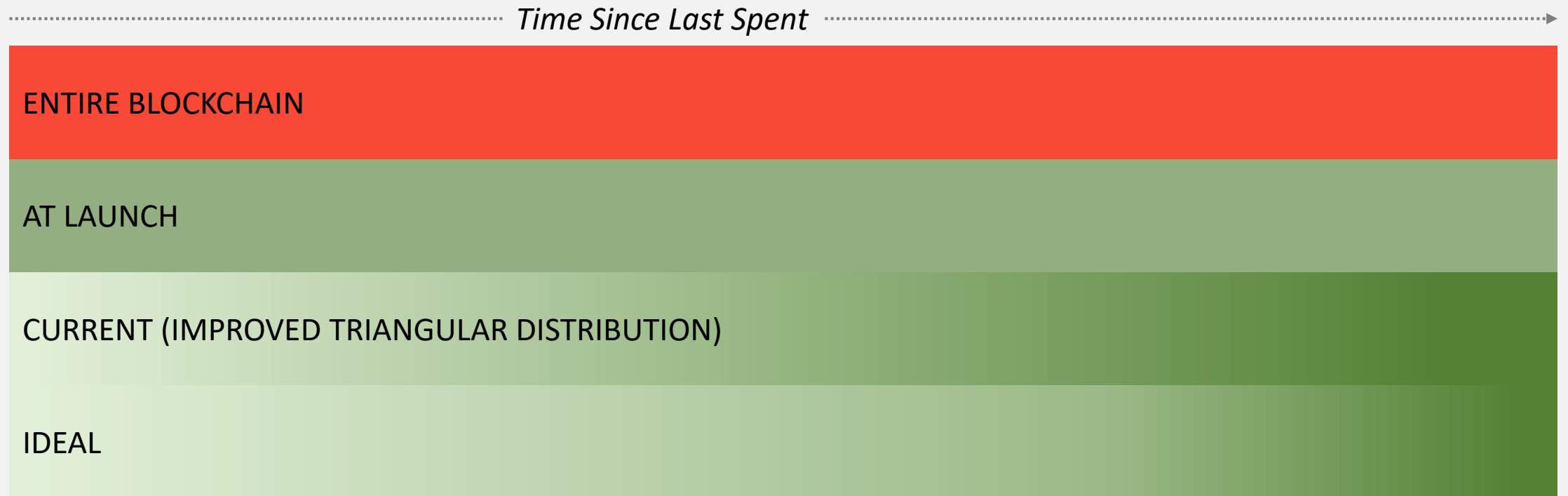


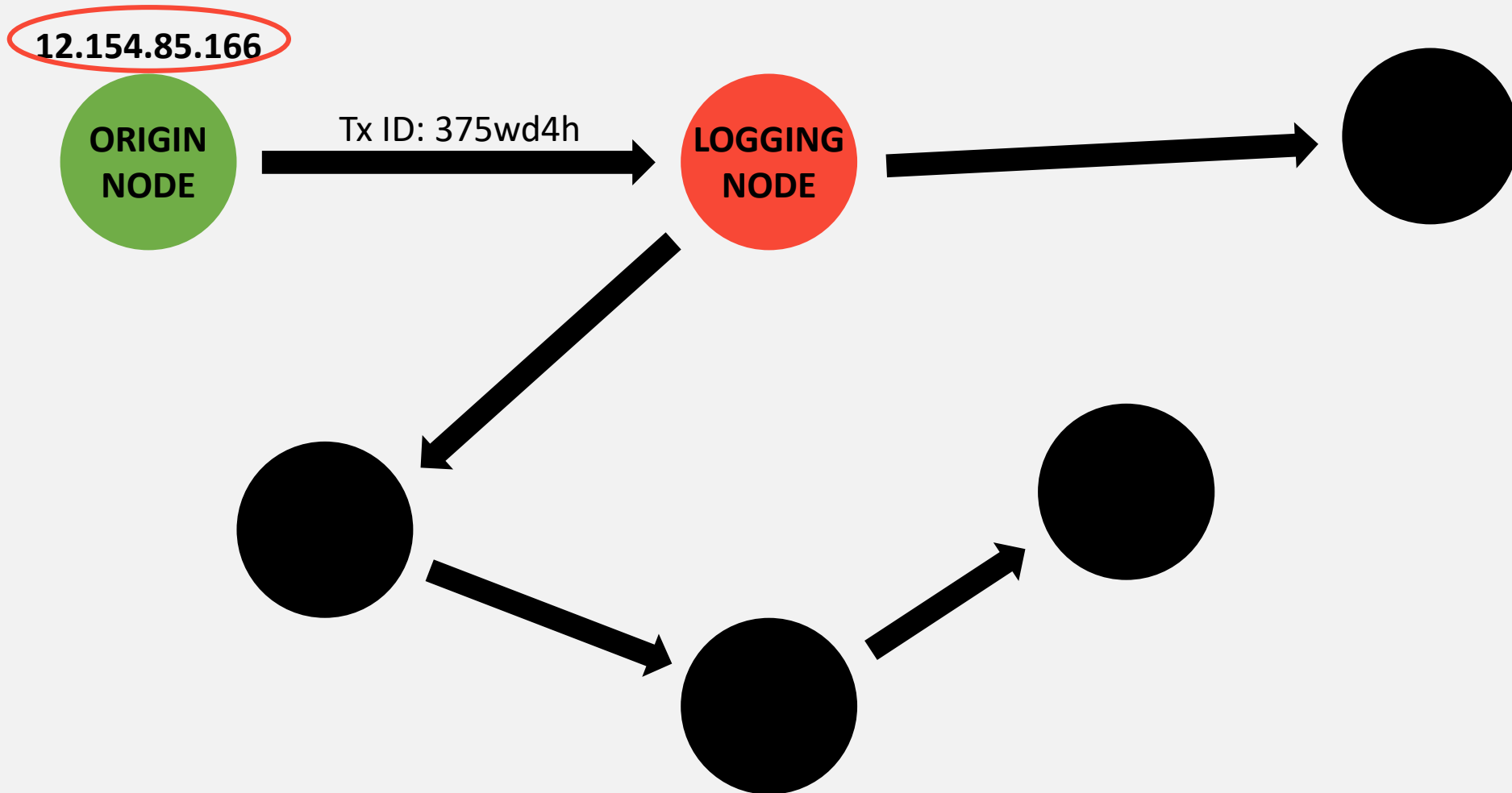
Ring Signatures & RingCT

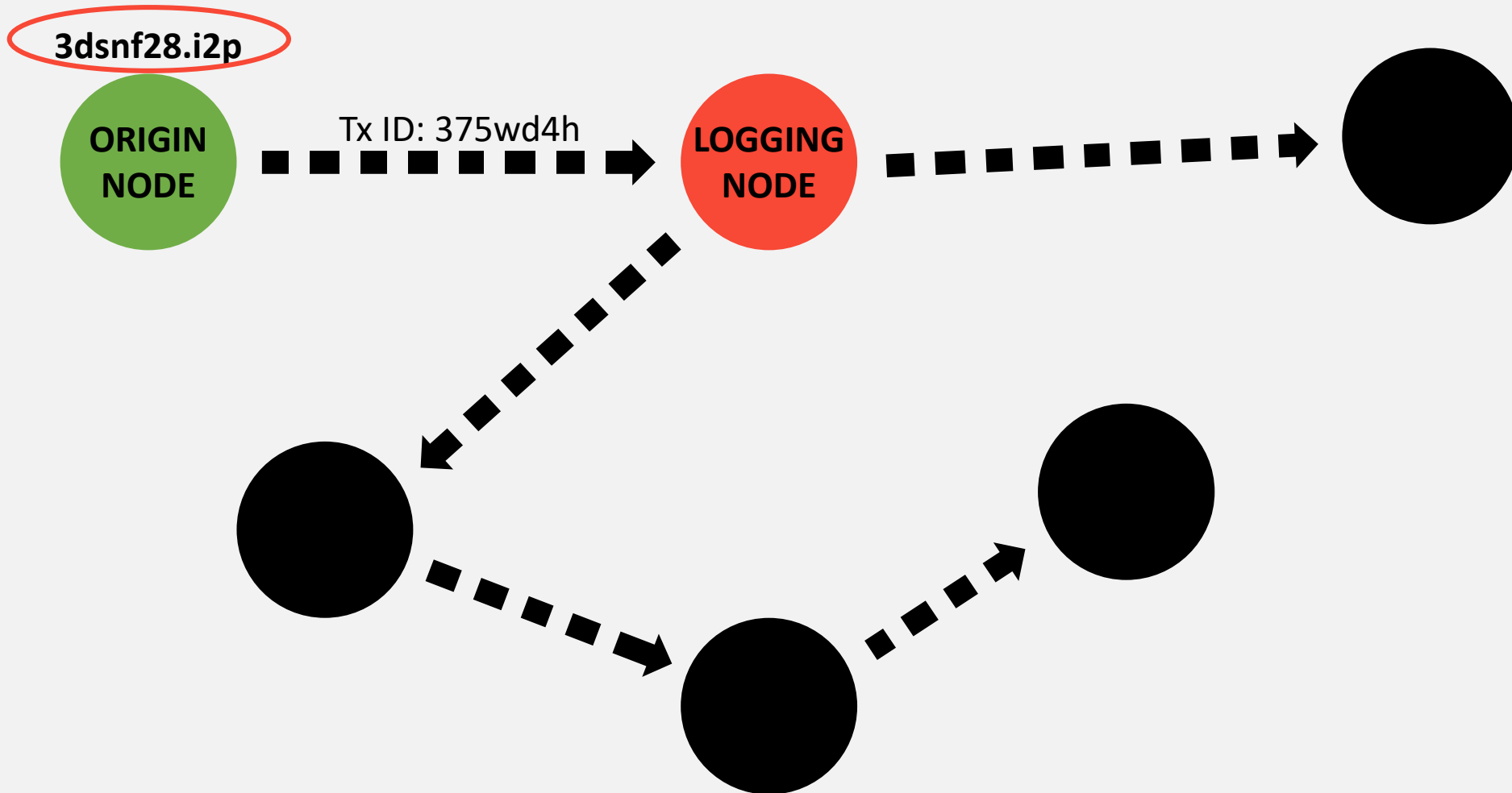
INPUTS



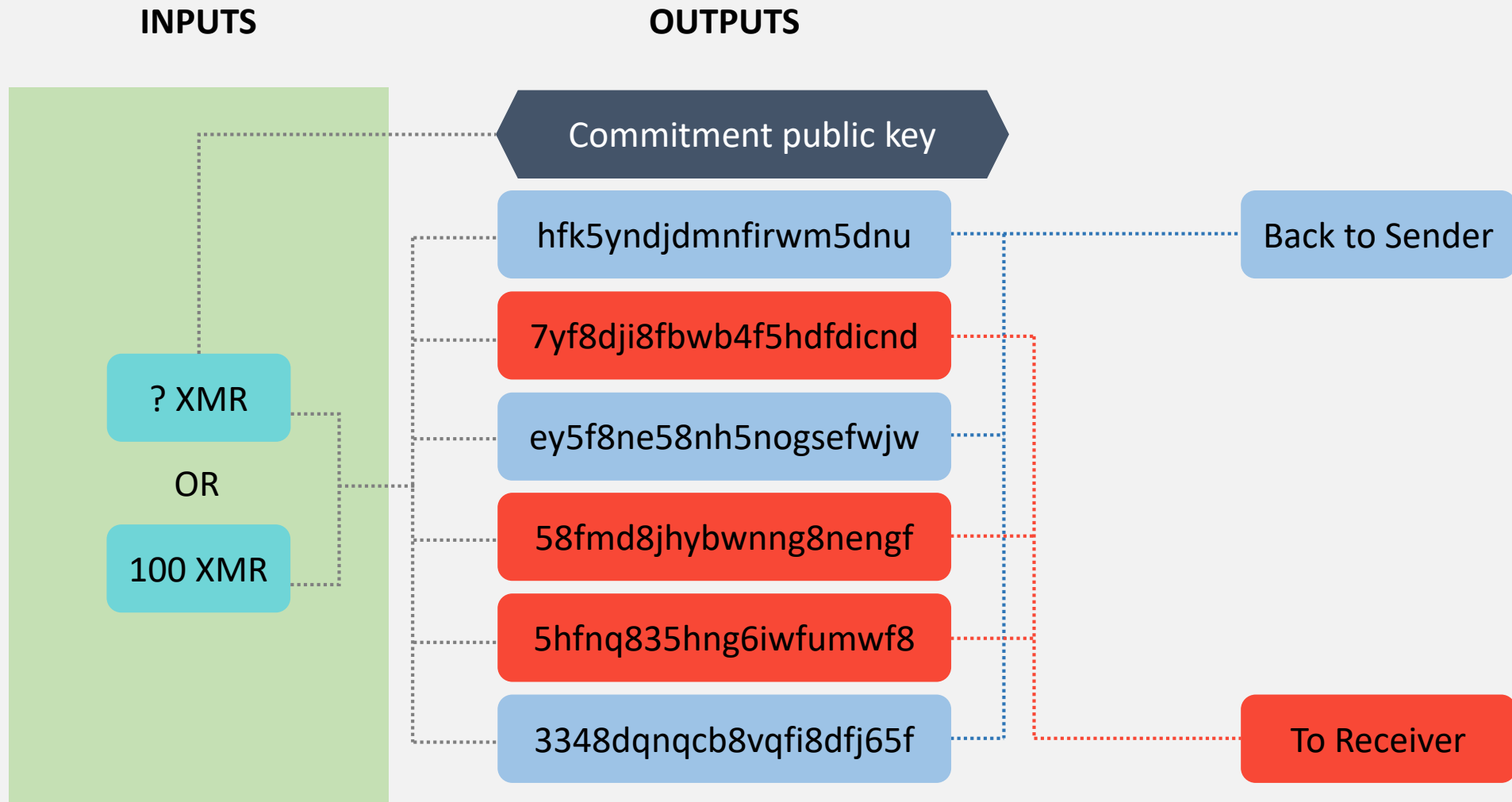
How Inputs Are Selected



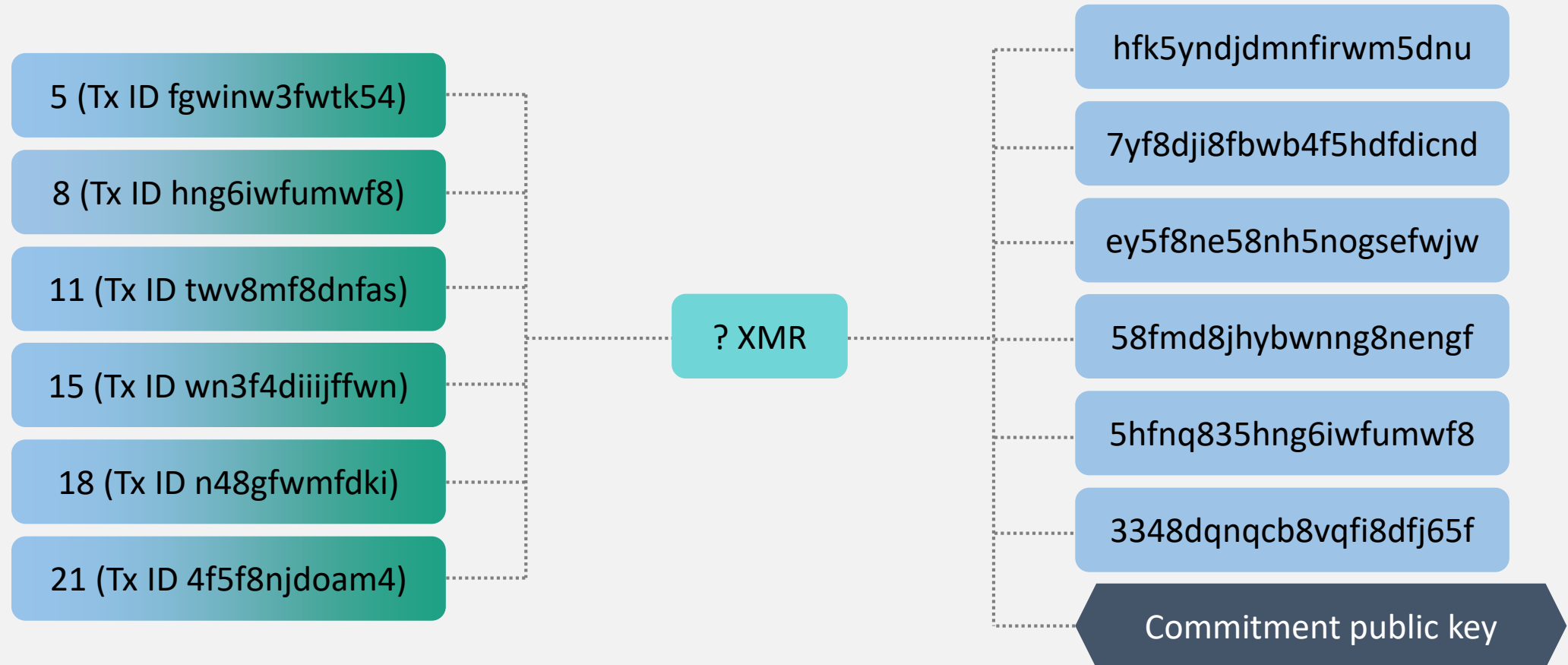




Stealth Addresses



Summary

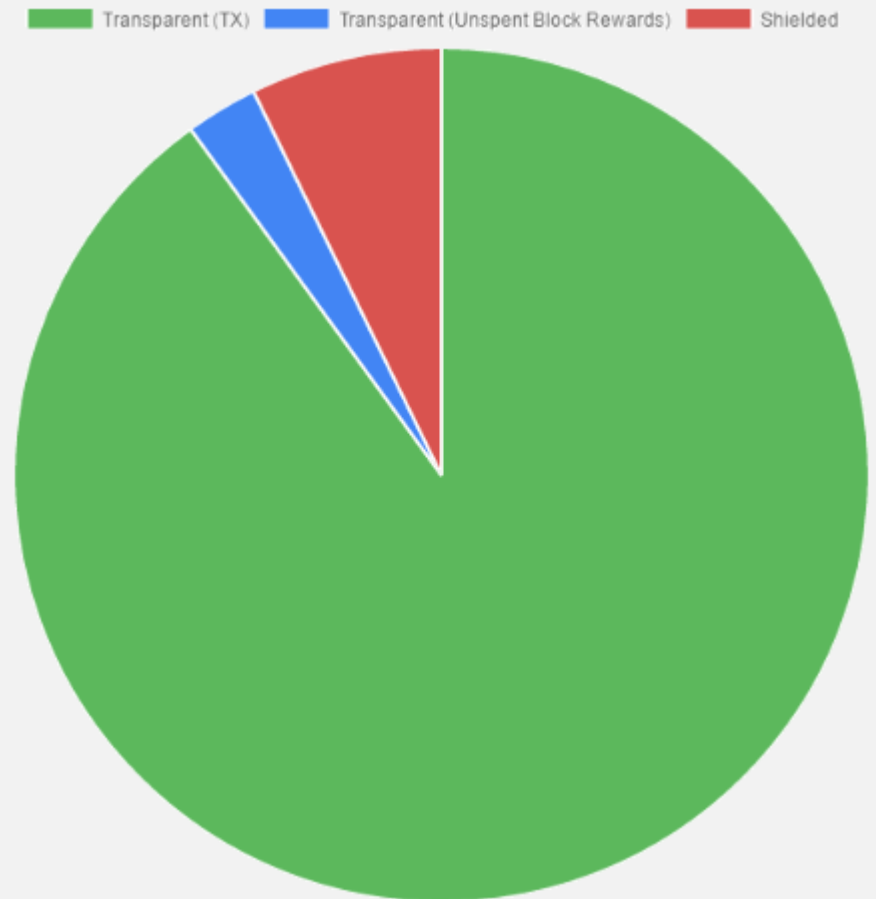


Mandatory Privacy

mixins used in transactions (%)

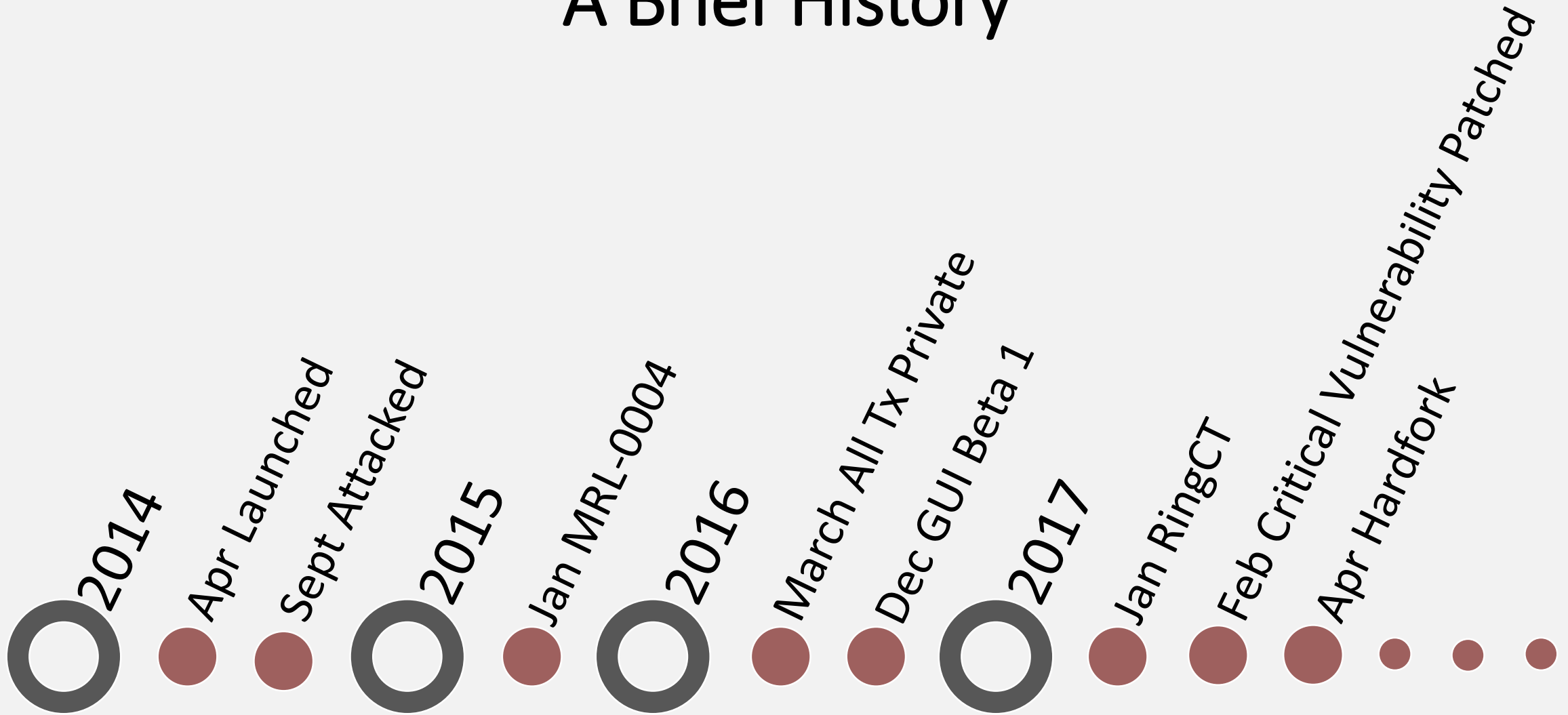
mixin:	none :(1 - 2	3 - 9
last day	66.74	10.95	20.25
last week	66.11	6.96	24.76
last month	64.47	5.42	28.13
last year	73.04	7.36	18.16

Source: MoneroBlocks.info 24 Feb 2016

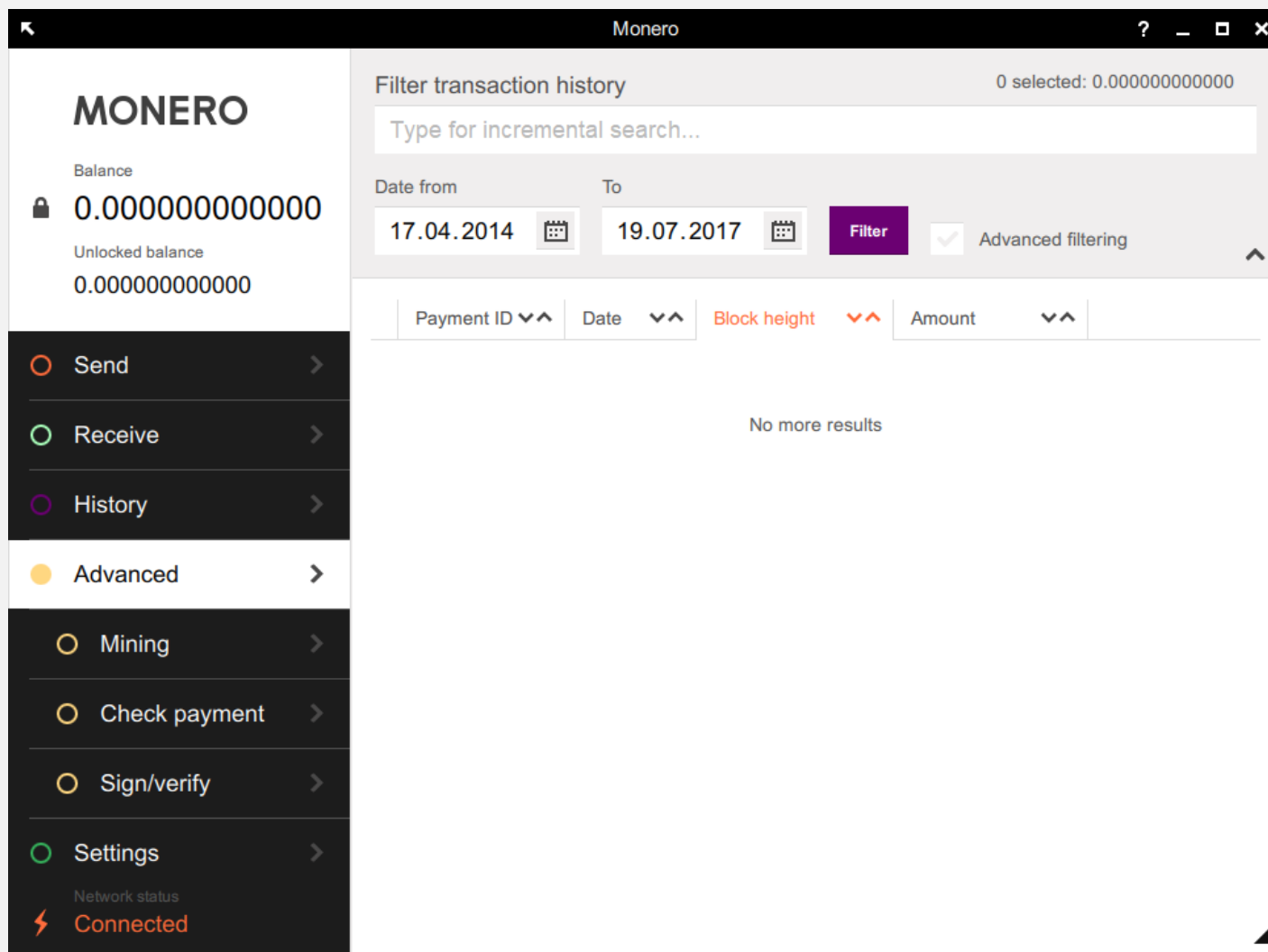


Source: zcha.in 15 March 2017

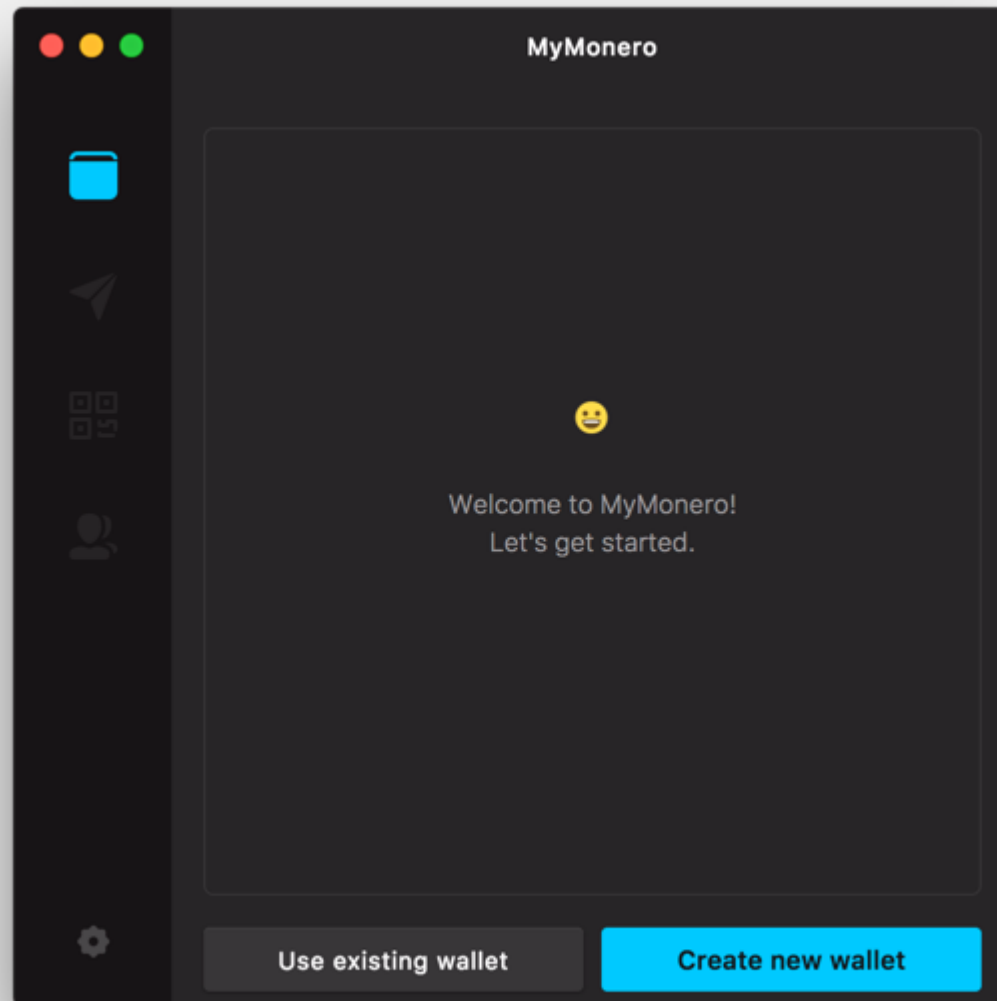
A Brief History



The Infamous GUI



MyMonero Lightweight Wallet



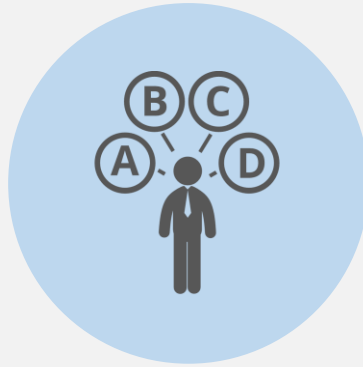
Regulatory Compliance and Transparency

(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



...but so close!

- Coinomi
- GUI port
- MyMonero
- Jaxx

Ongoing Development



Multisig



Sub-Addresses



Translations



Lightweight
Wallet



RingCT
Optimizations



Community

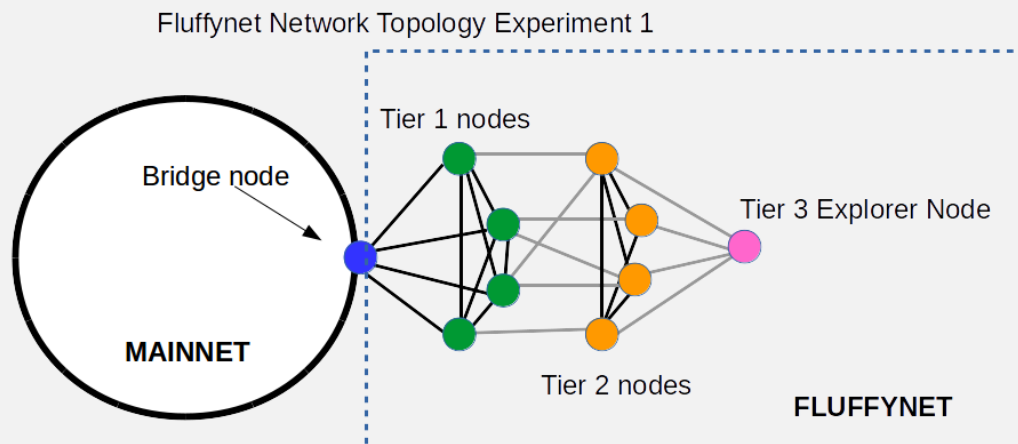
Hardfork Schedule

January

April

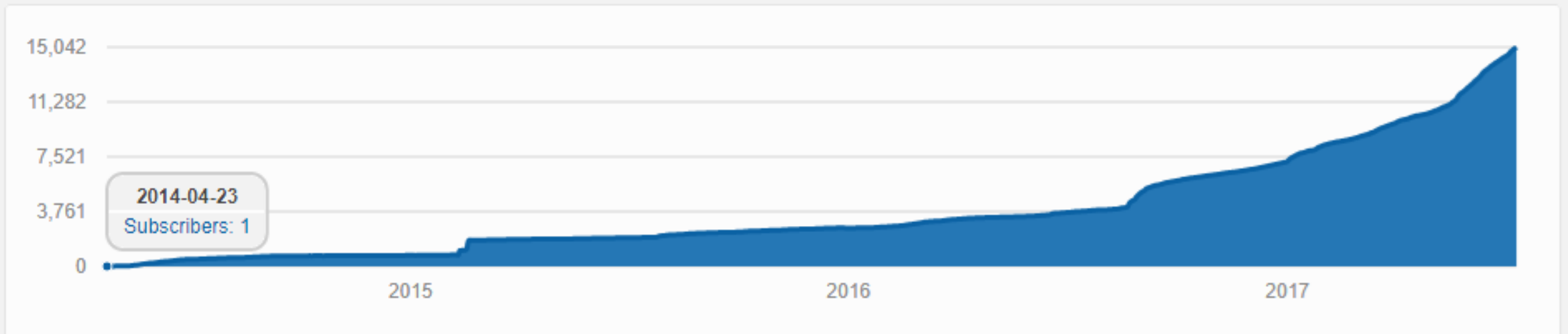
September

September 18th*



- **Mandatory RingCT**
- **Minimum ringsize ≥ 5** (likely 10)
- Fluffy blocks (in testing now)
- Improved input selection algorithm
- OMQ
- Sub-Addresses

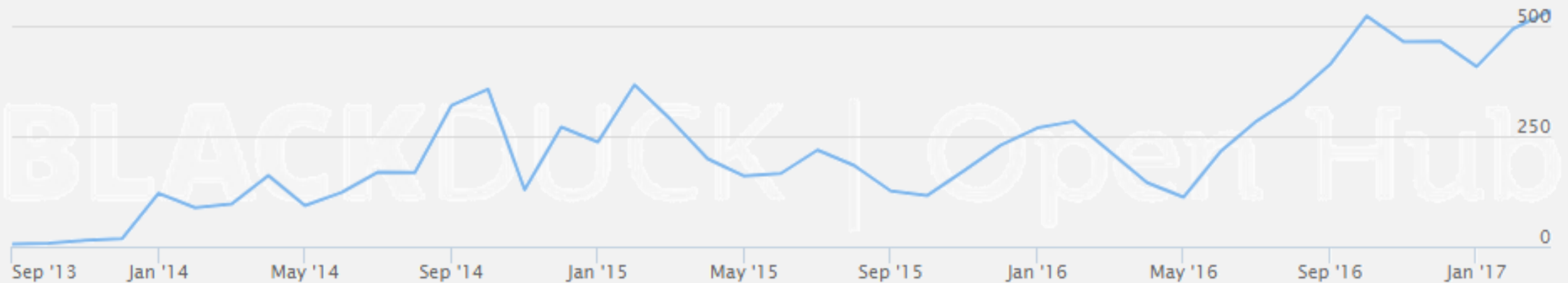
Community Growth



Community Growth

Commits per Month

Zoom 1yr 3yr All



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 1GwV7fPX97hmavc6iNrUZUogmjplPrPFoE.
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

Thank You!



getmonero.org



/r/Monero



monero.stackexchange.com



justin@ehrenhofer.org