
SECURE. PRIVATE. UNTRACEABLE.
MONERO
Barcelona, Spain
Excepte serveis
Laborables
de dilluns a divendre

Welcome

Justin Ehrenhofer

Finance
Management Information Systems

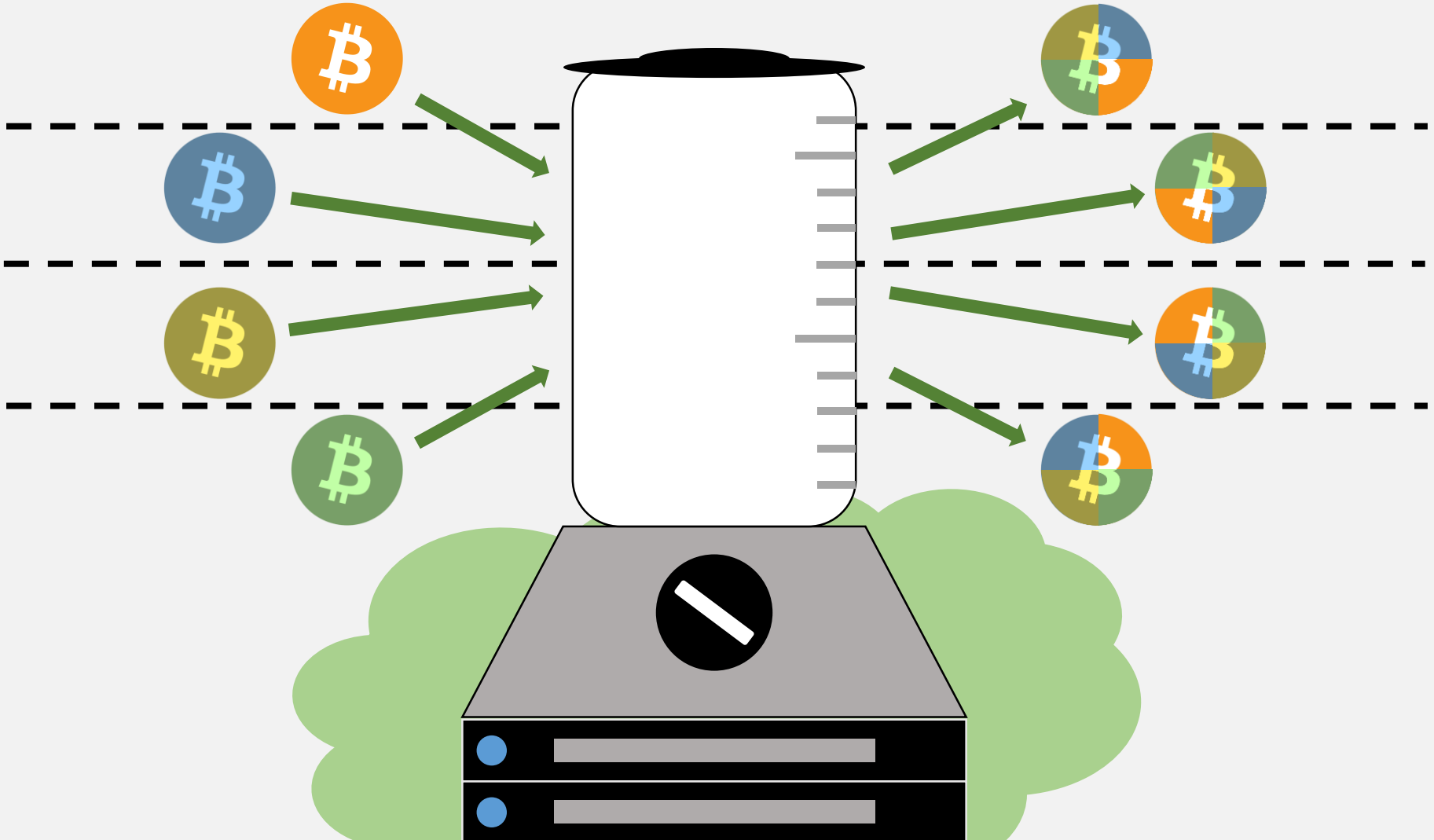
/u/SamsungGalaxyPlayer or sgp_

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

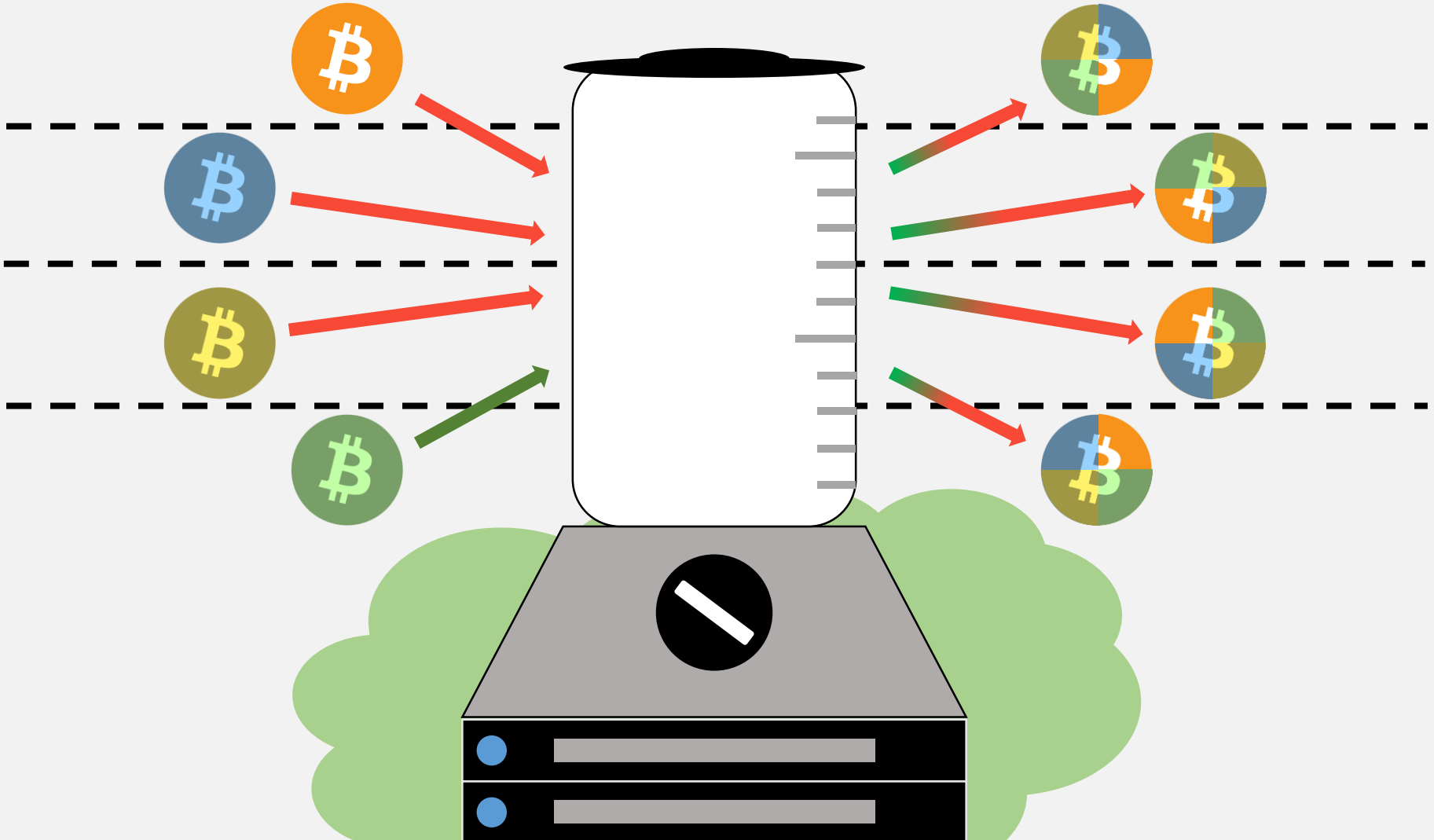
UNIVERSITY OF MINNESOTA
Driven to Discover℠

CryptoUMN.com

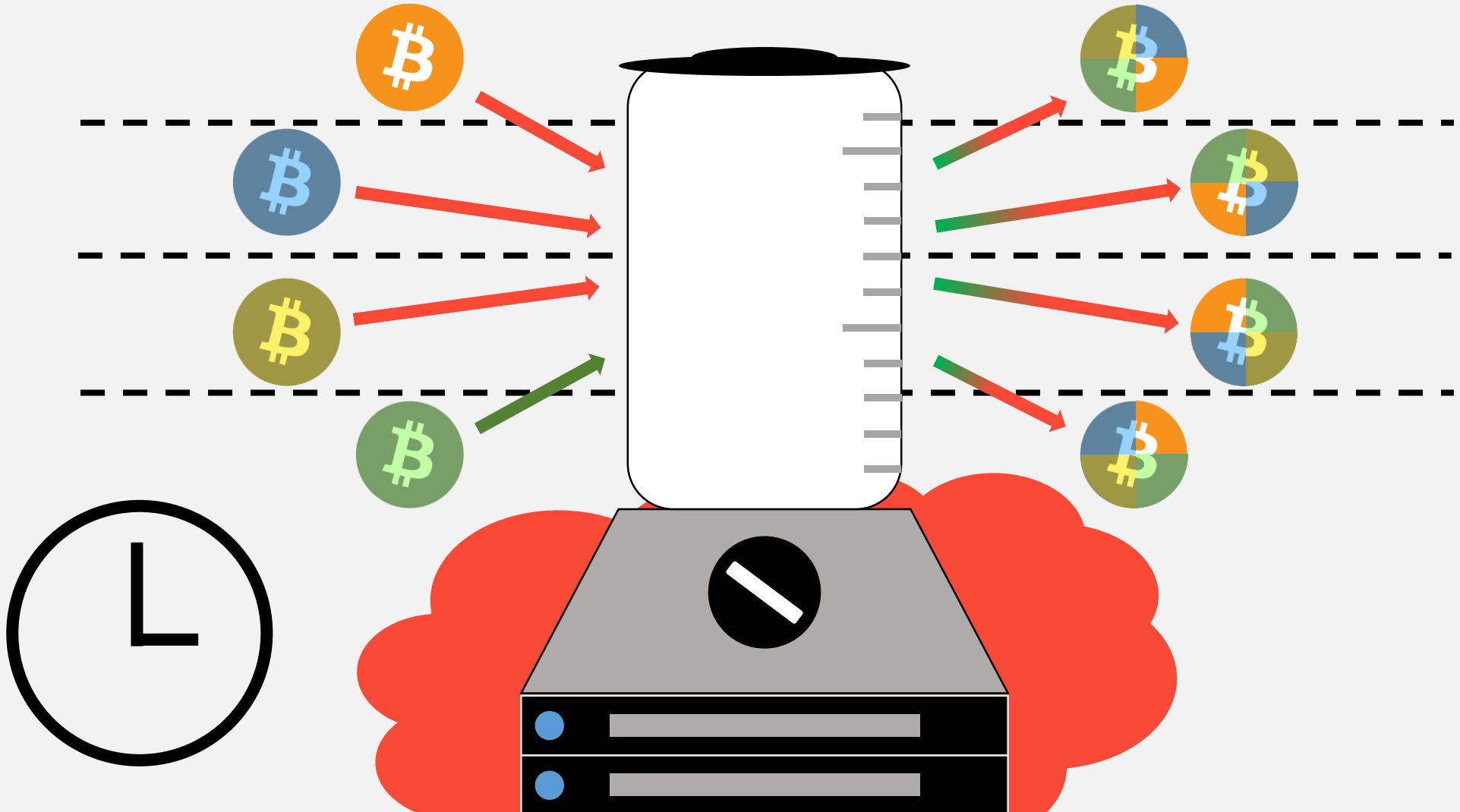
People Started Adding Tools to Bitcoin



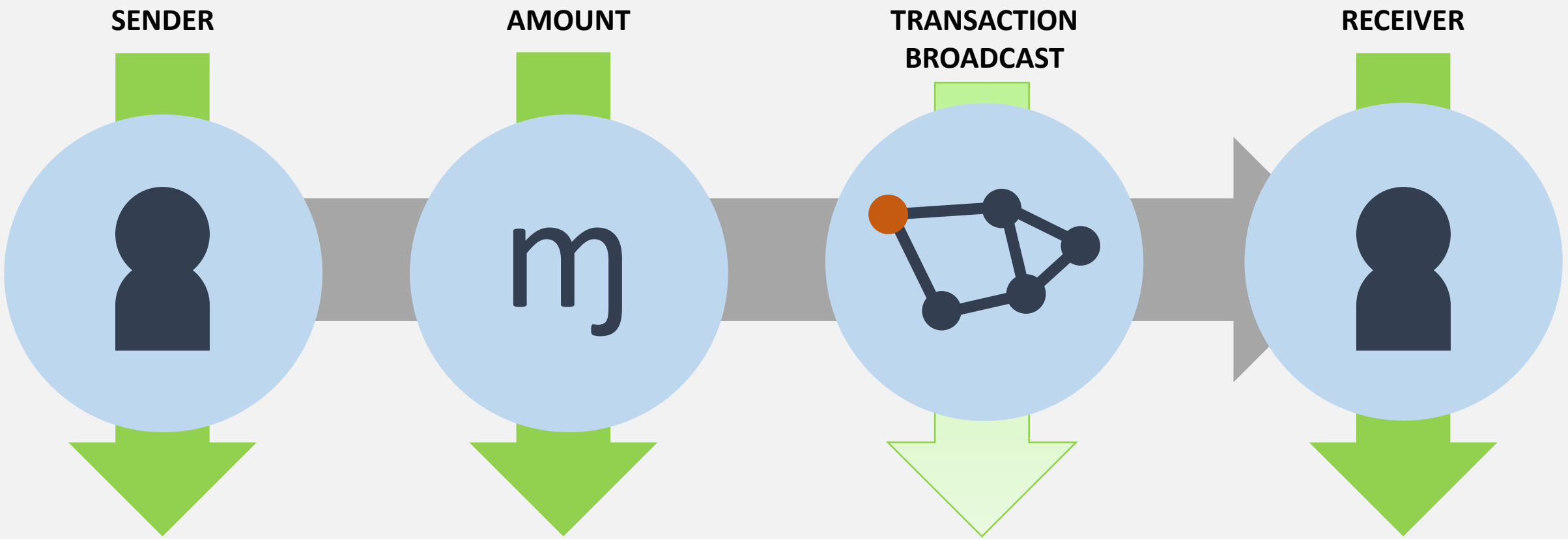
People Started Adding Tools to Bitcoin



People Started Adding Tools to Bitcoin

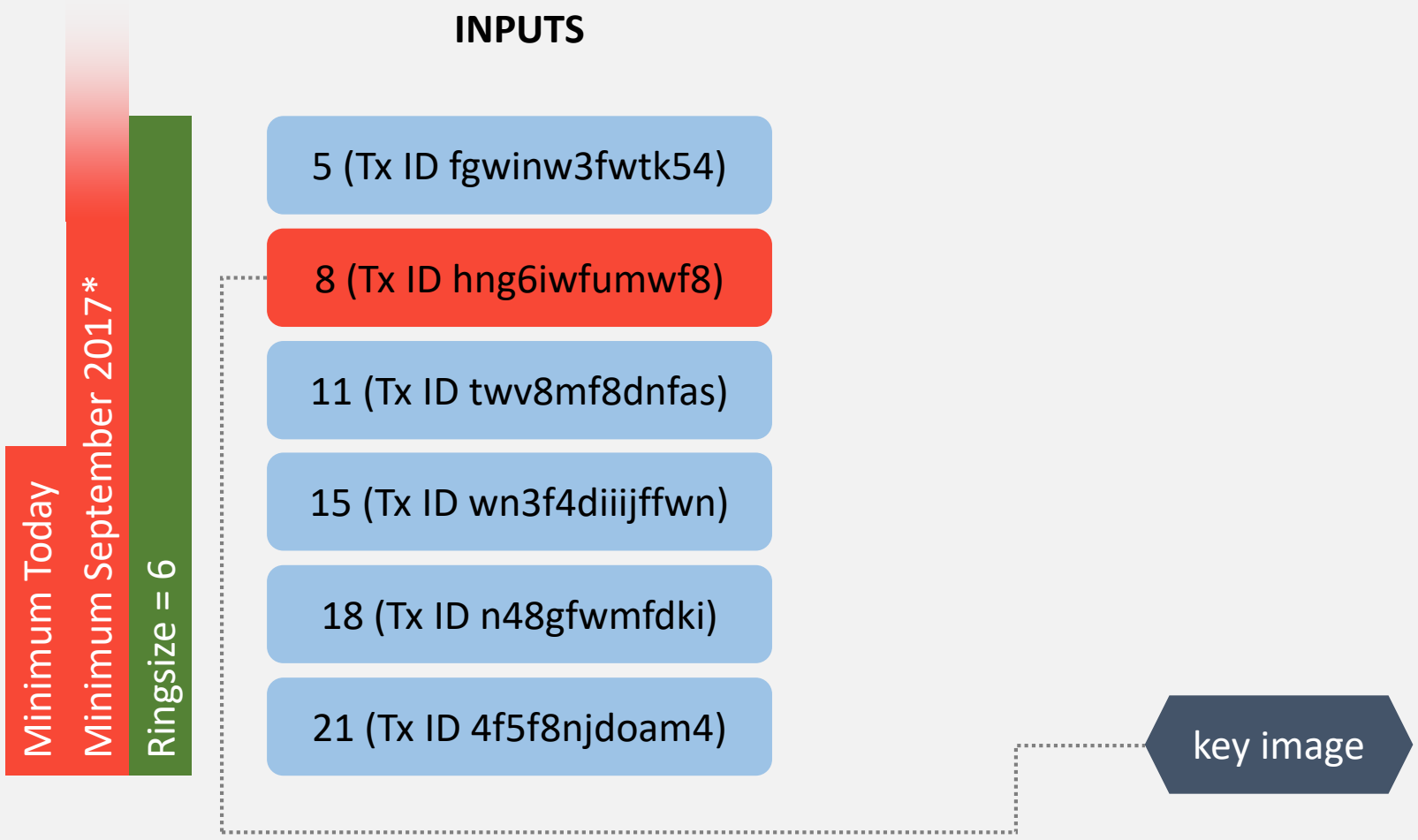


The Monero Difference

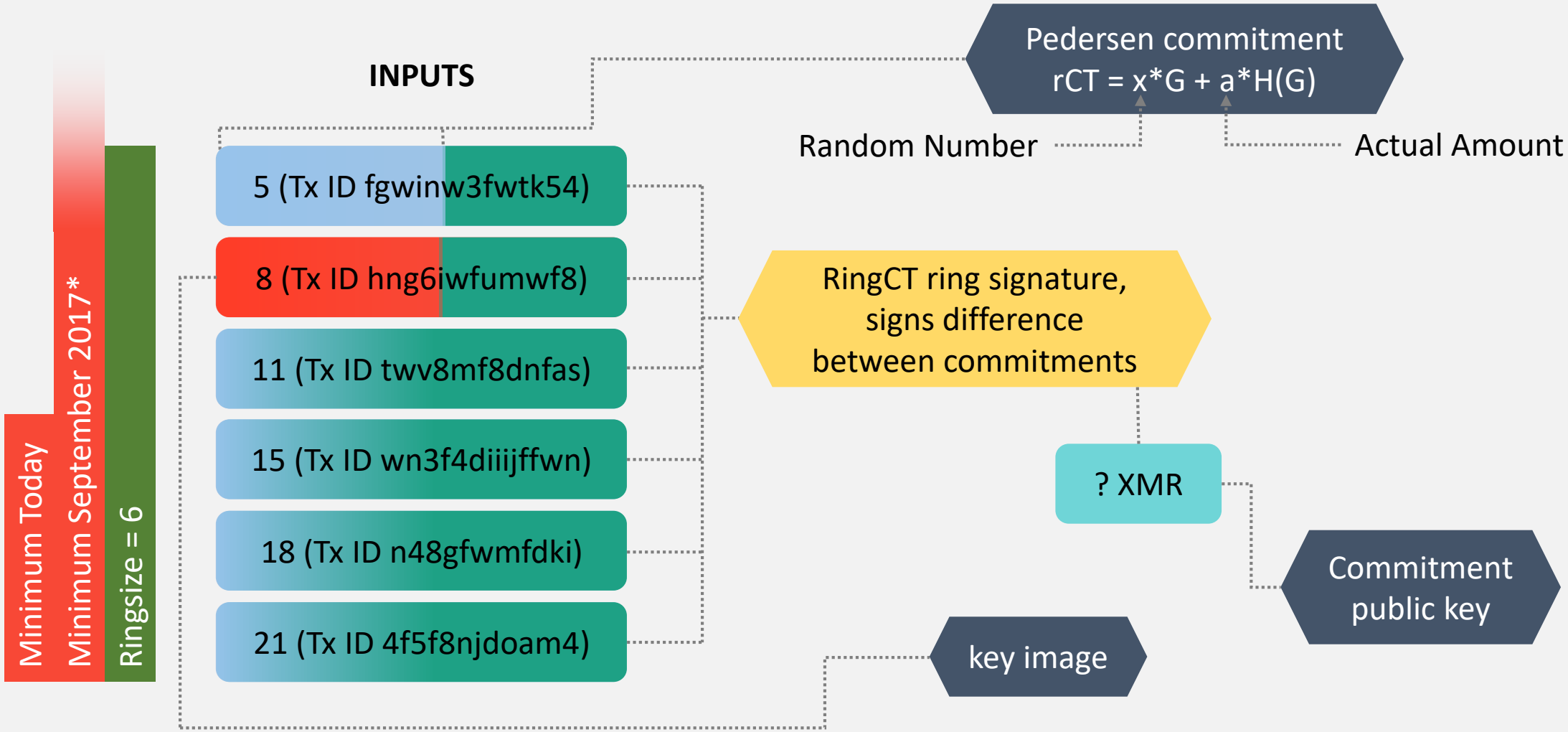


Ring Signatures & RingCT

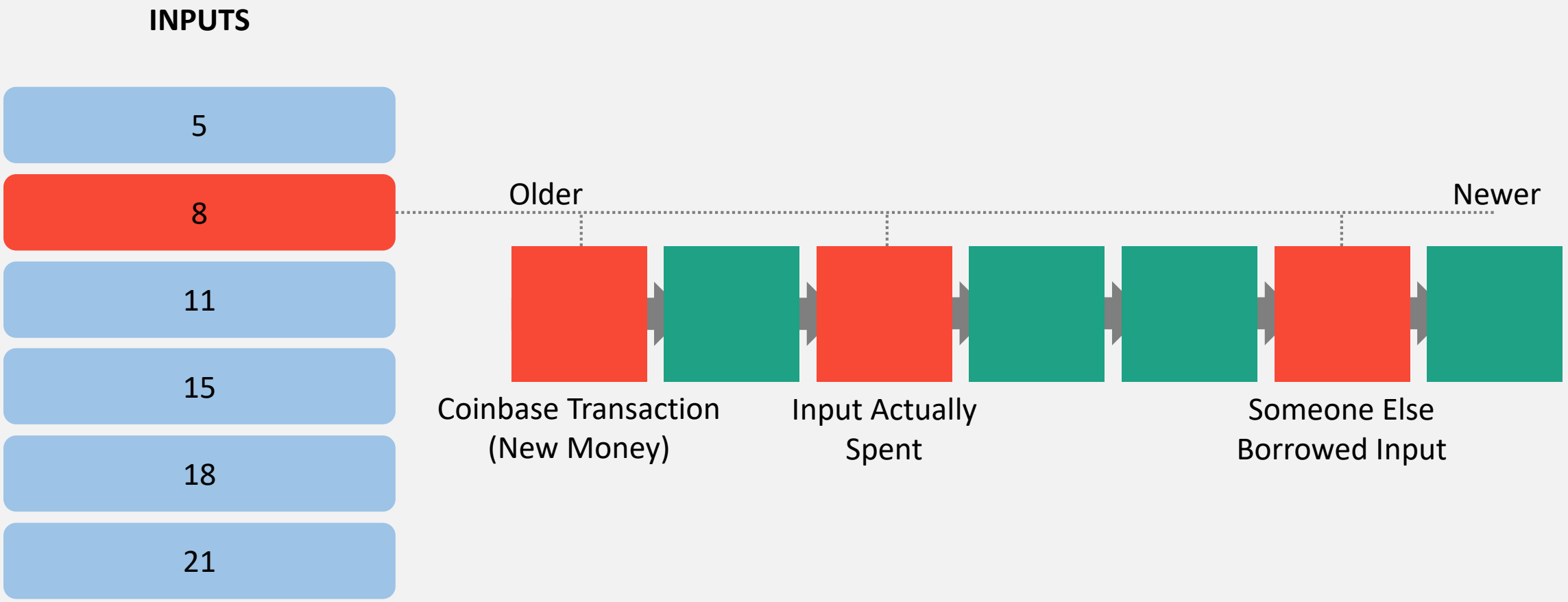
Ring Signatures & RingCT



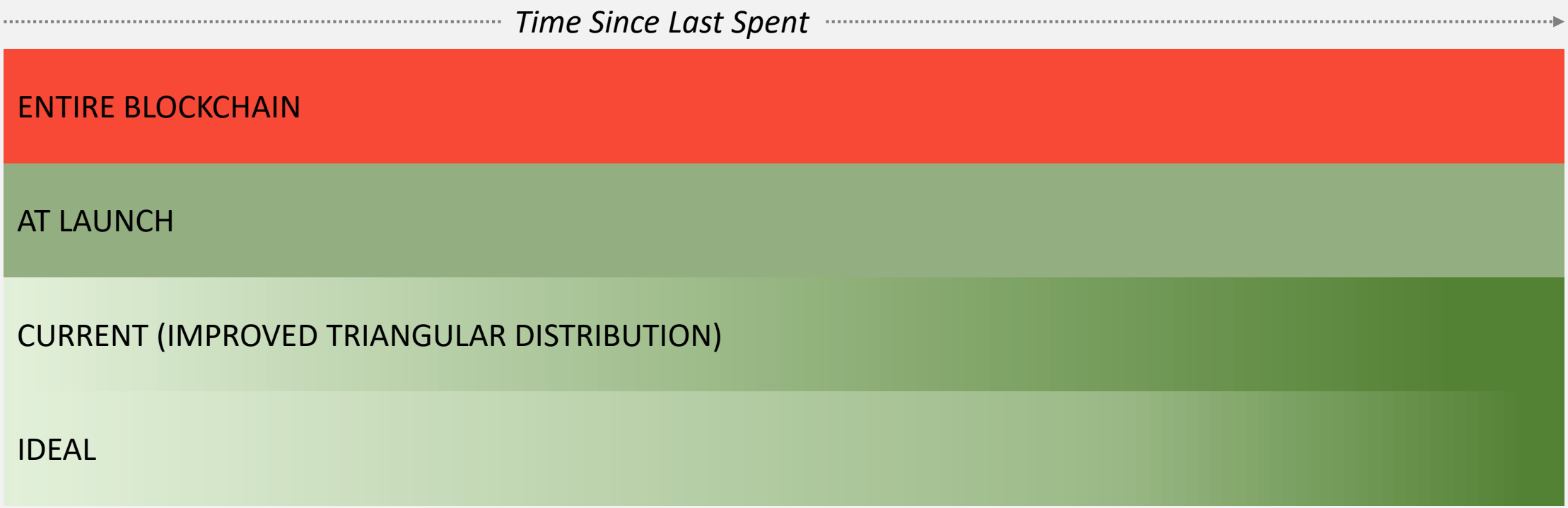
Ring Signatures & RingCT



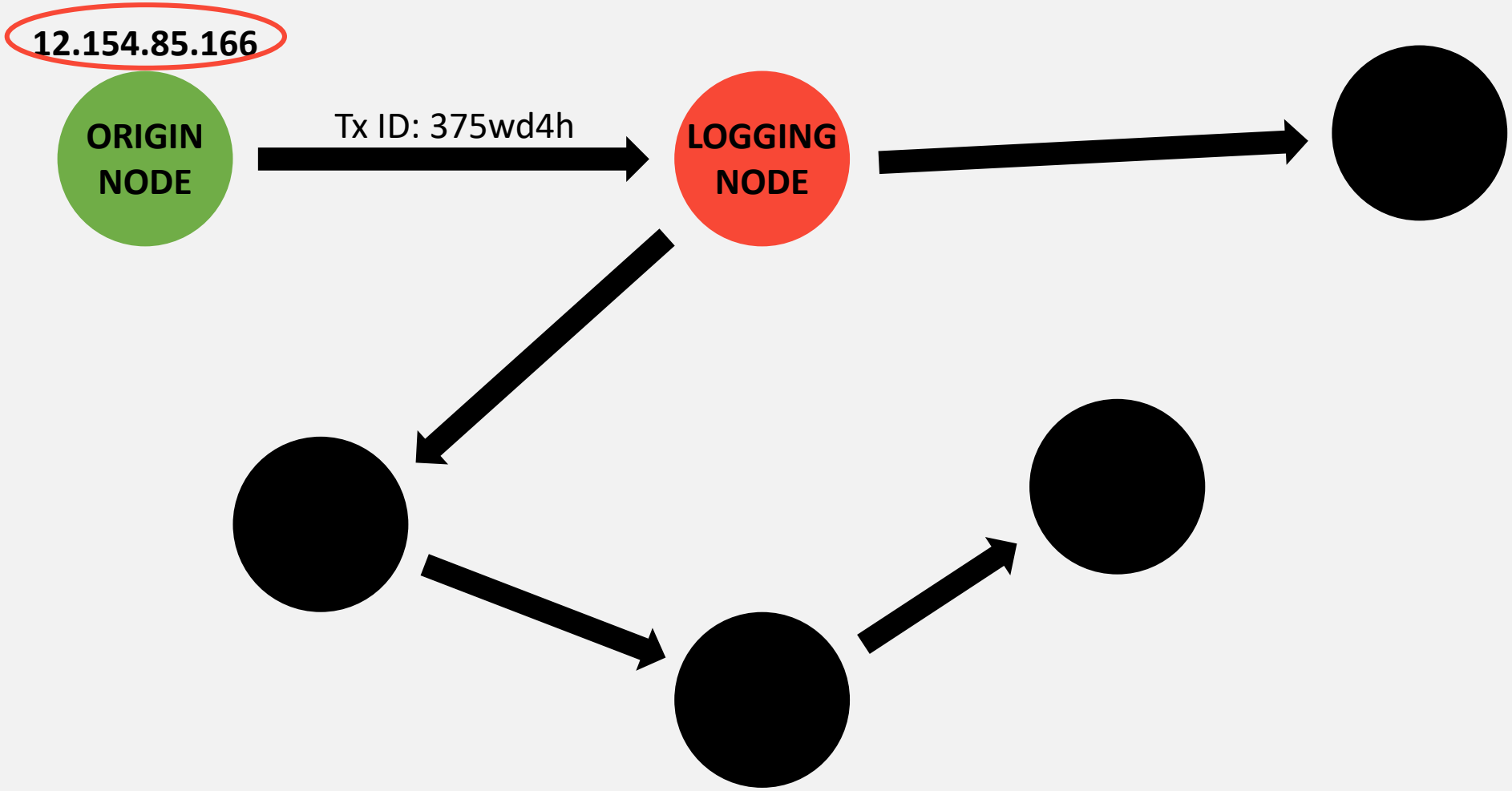
Ring Signatures & RingCT



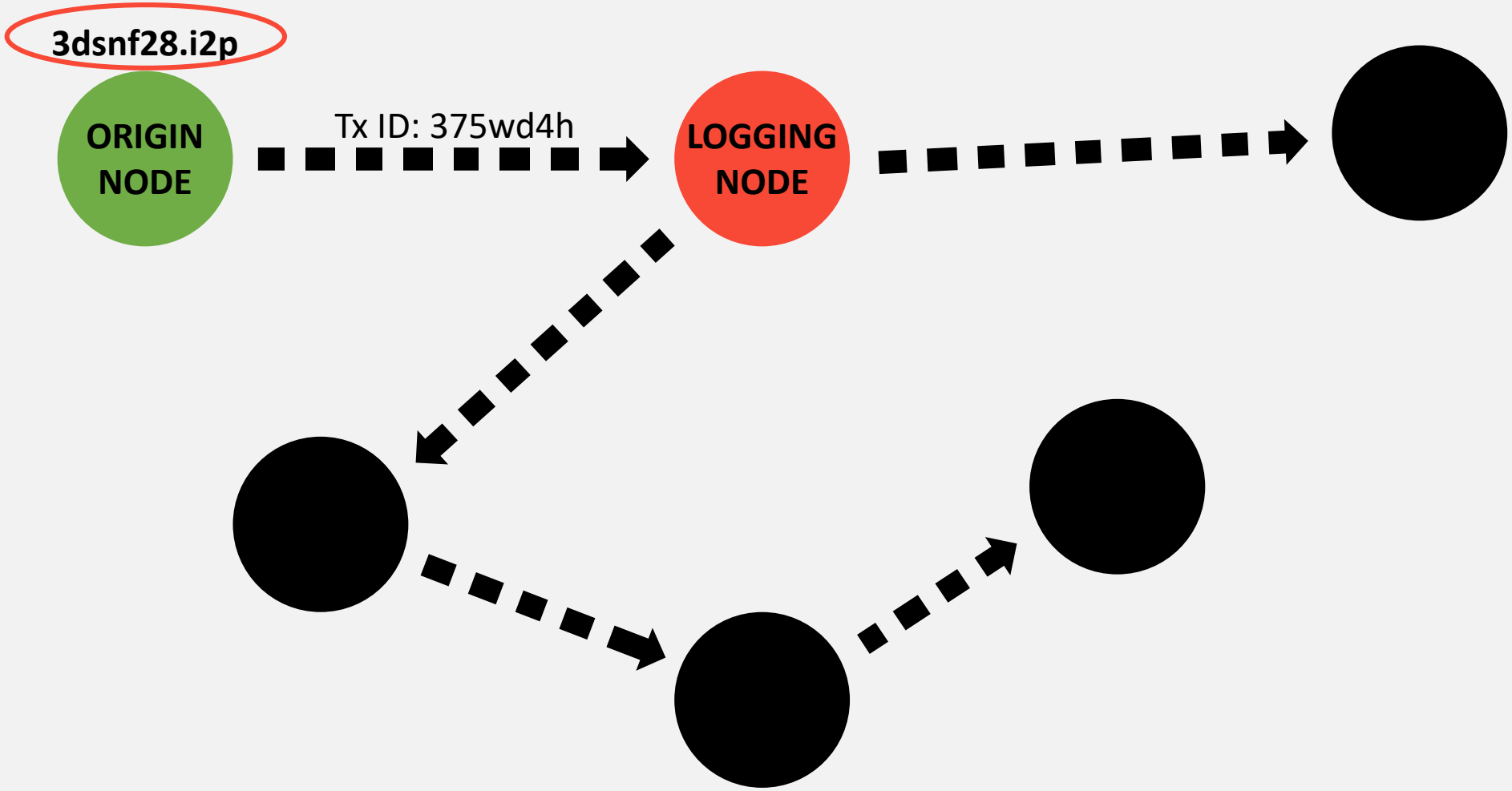
How Inputs Are Selected



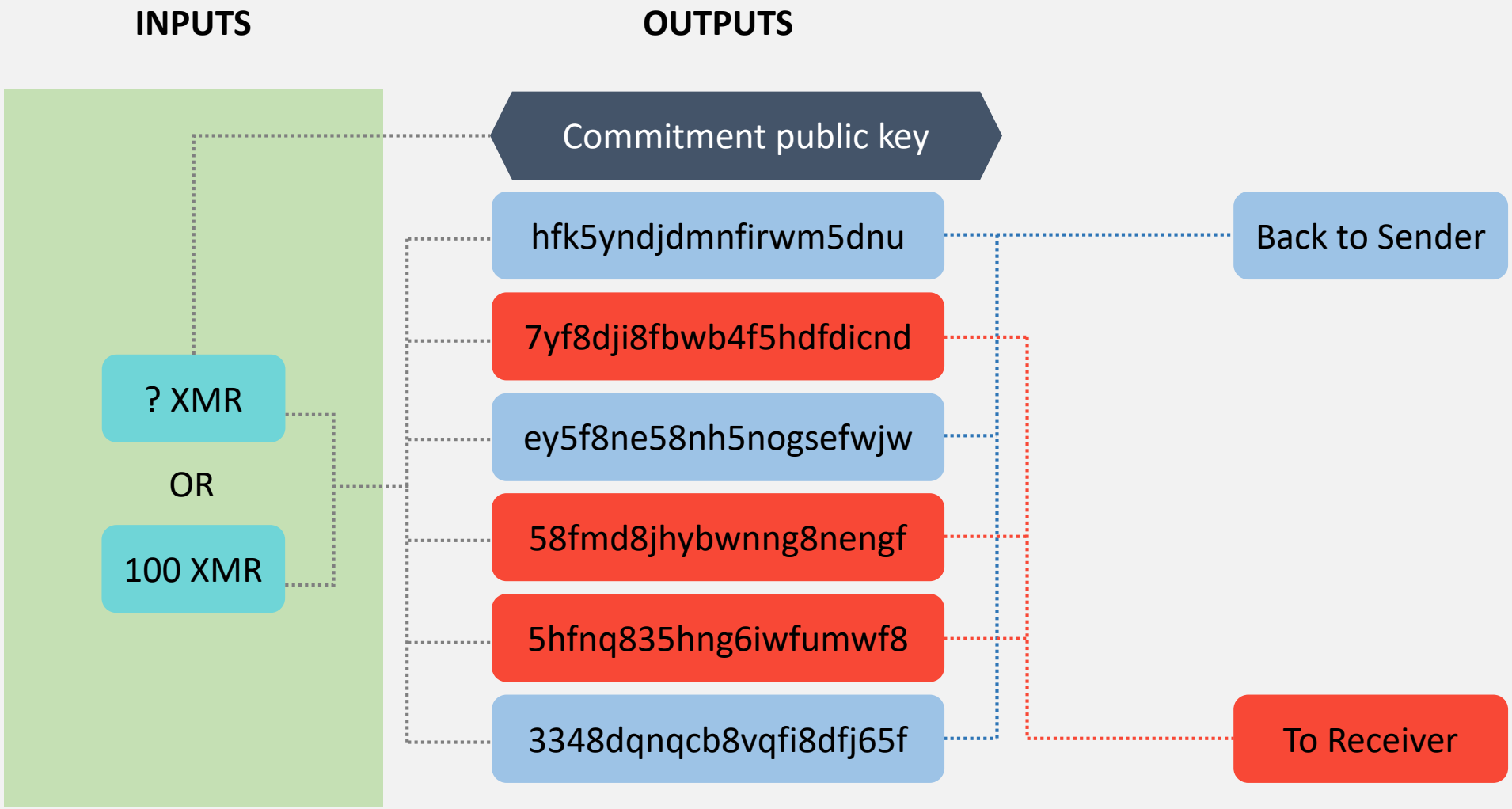
KOVRI



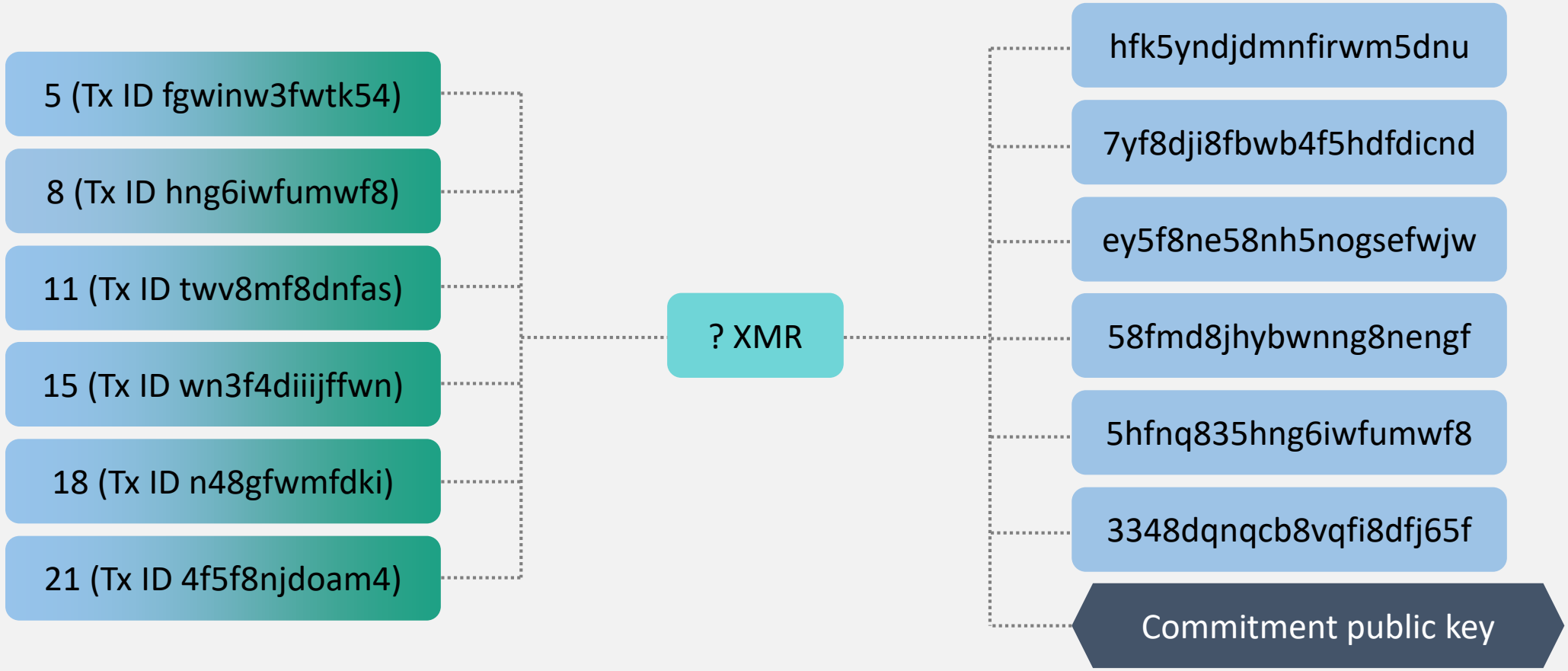
KOVRI



Stealth Addresses



Summary

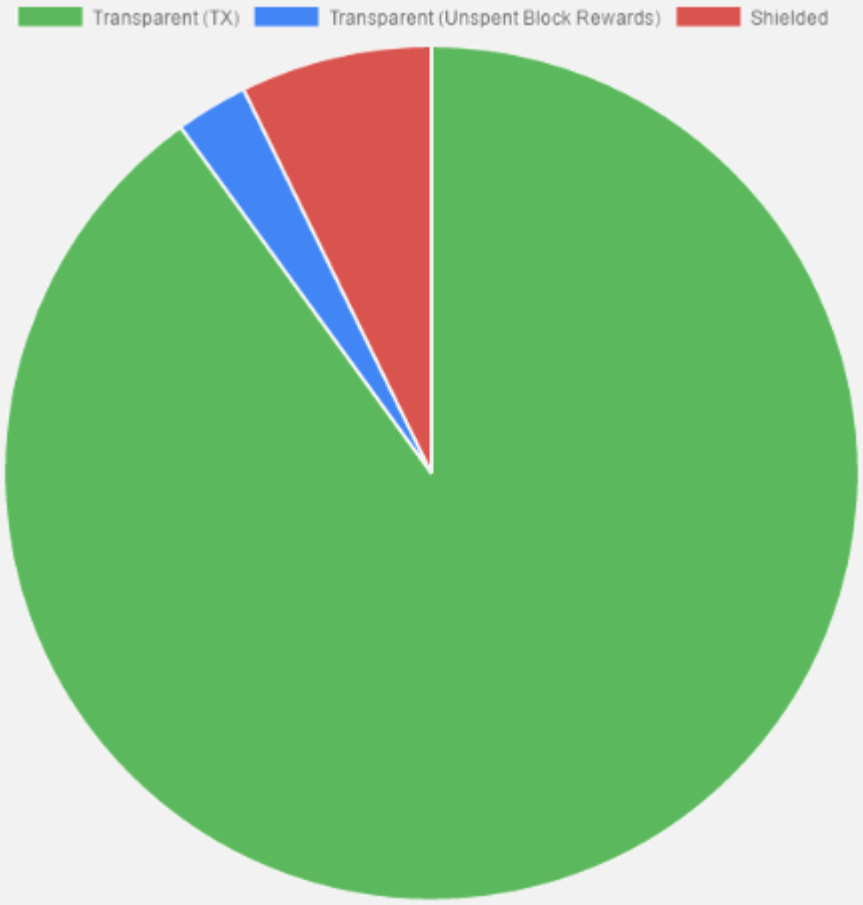

5 (Tx ID fgwinw3fwtk54)
8 (Tx ID hng6iwfumwf8)
11 (Tx ID twv8mf8dnfas)
15 (Tx ID wn3f4diiijffwn)
18 (Tx ID n48gfwmfdki)
21 (Tx ID 4f5f8njdoam4)
? XMR
hfk5yndjdmnfirwm5dnu
7yf8dji8fbwb4f5hdfdicnd
ey5f8ne58nh5nogsefwjw
58fmd8jhybwnng8nengf
5hfnq835hng6iwfumwf8
3348dqnqcb8vqfi8dfj65f
Commitment public key

Mandatory Privacy

mixins used in transactions (%)

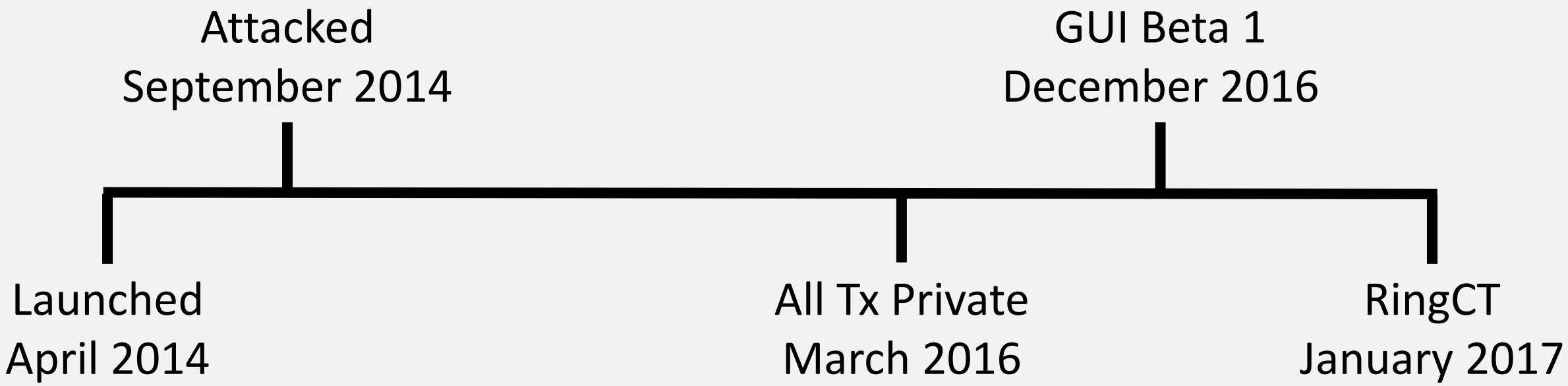
mixin:	none :(	1 - 2	3 - 9
last day	66.74	10.95	20.25
last week	66.11	6.96	24.76
last month	64.47	5.42	28.13
last year	73.04	7.36	18.16

Source: MoneroBlocks.info 24 Feb 2016

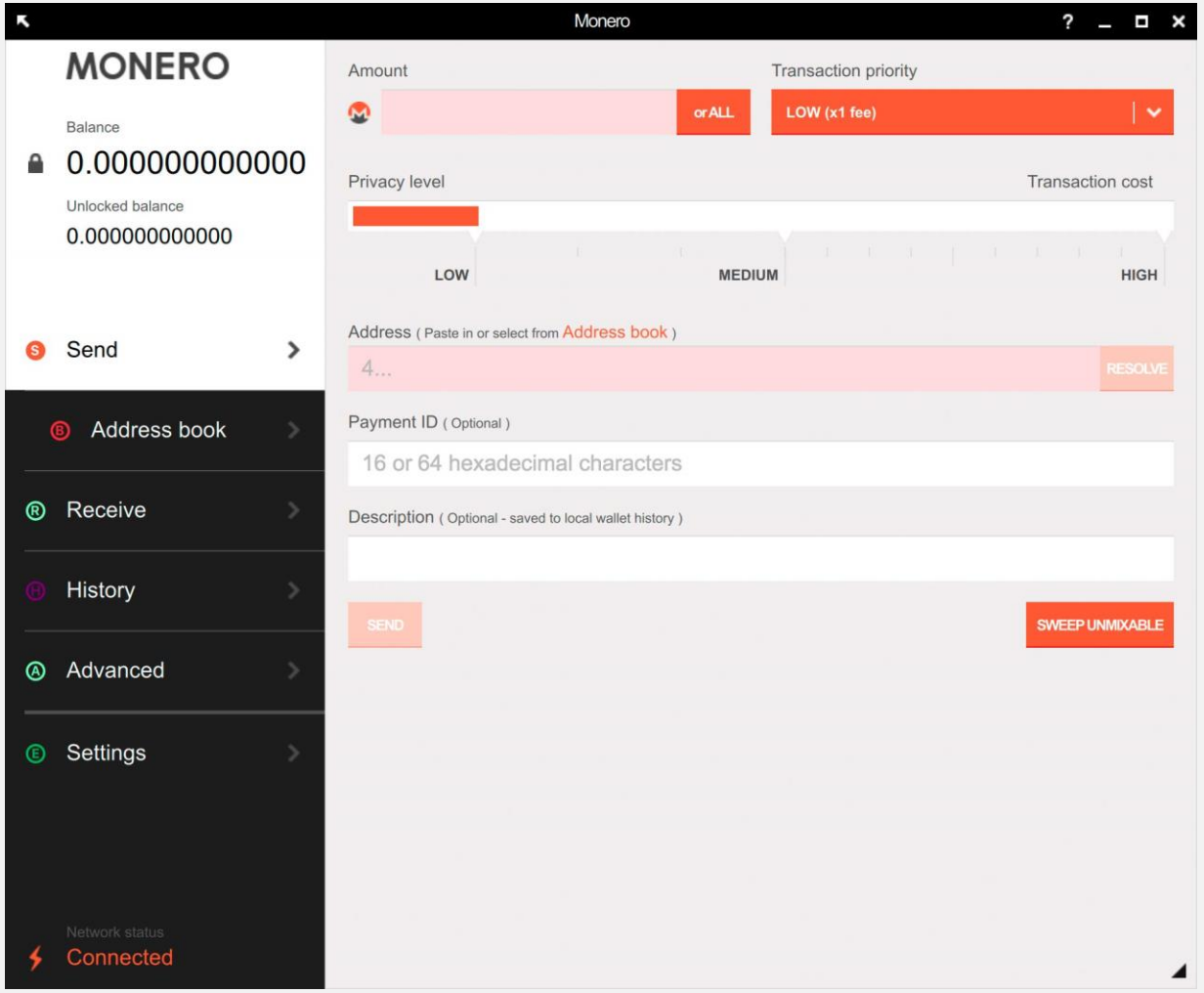


Source: zcha.in 15 March 2017

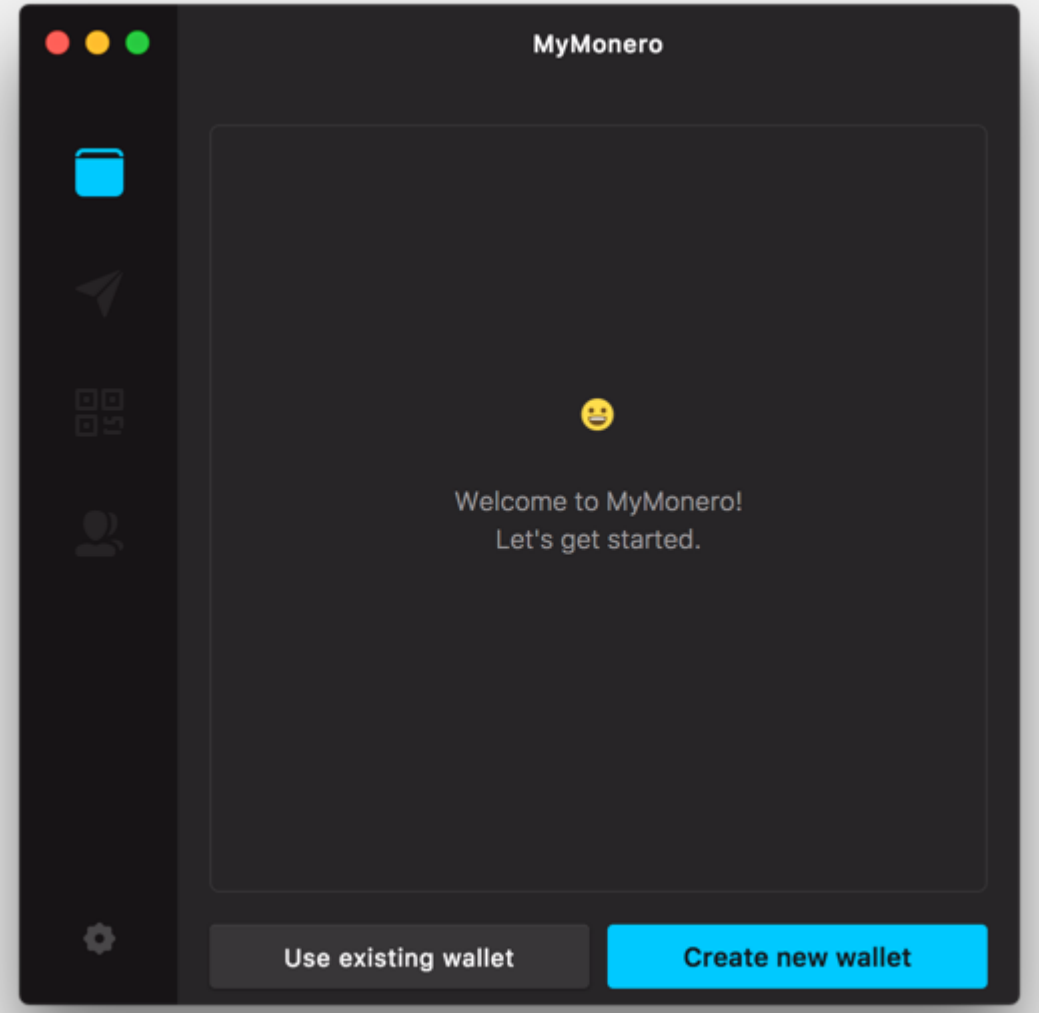
A Brief History



The Infamous GUI



MyMonero Lightweight Wallet

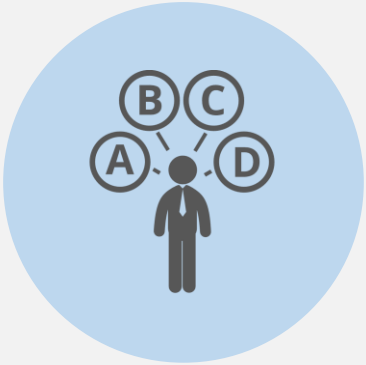


Regulatory Compliance and Transparency

(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

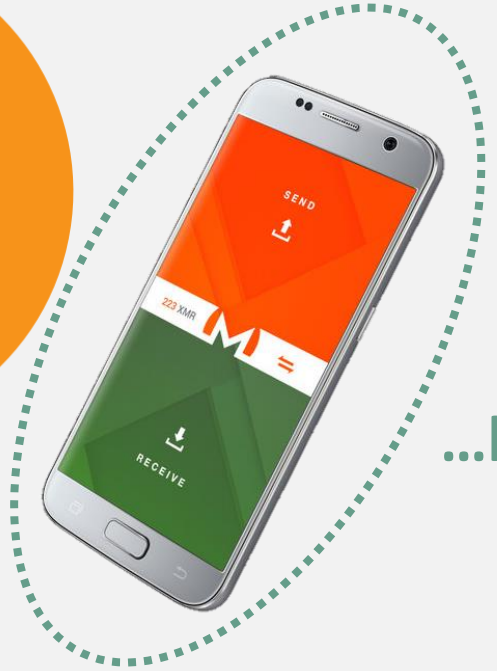
Charities

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!

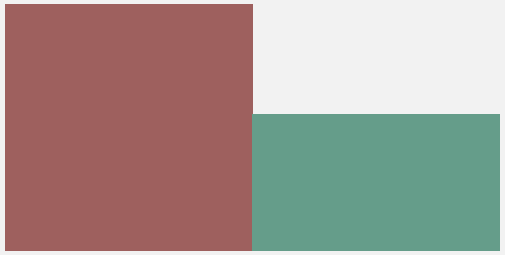
Ongoing Development

Multisig

Sub-Addresses

Translations

Lightweight Wallet

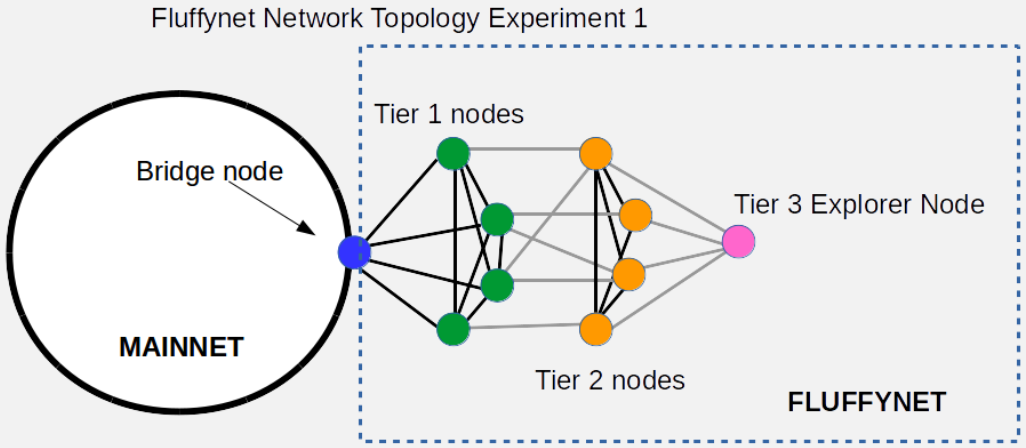


RingCT Optimizations

Hardfork Schedule

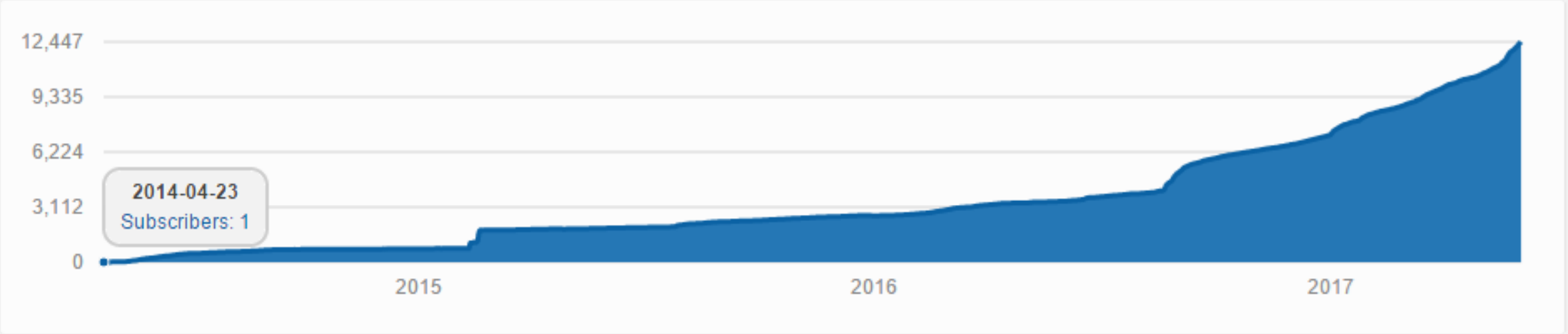
January — April — September

September 18th*



- **Mandatory RingCT**
- **Minimum ringsize ≥5** (likely 10)
- Fluffy blocks (in testing now)
- Improved input selection algorithm
- 0MQ
- Sub-Addresses

Community Growth



Community Growth

Thank You!

getmonero.org

/r/Monero

monero.stackexchange.com

justin@ehrenhofer.org