# Monero 101 Abridged

SCOTT ANECITO

# Who am I?

Privacy and security enthusiast

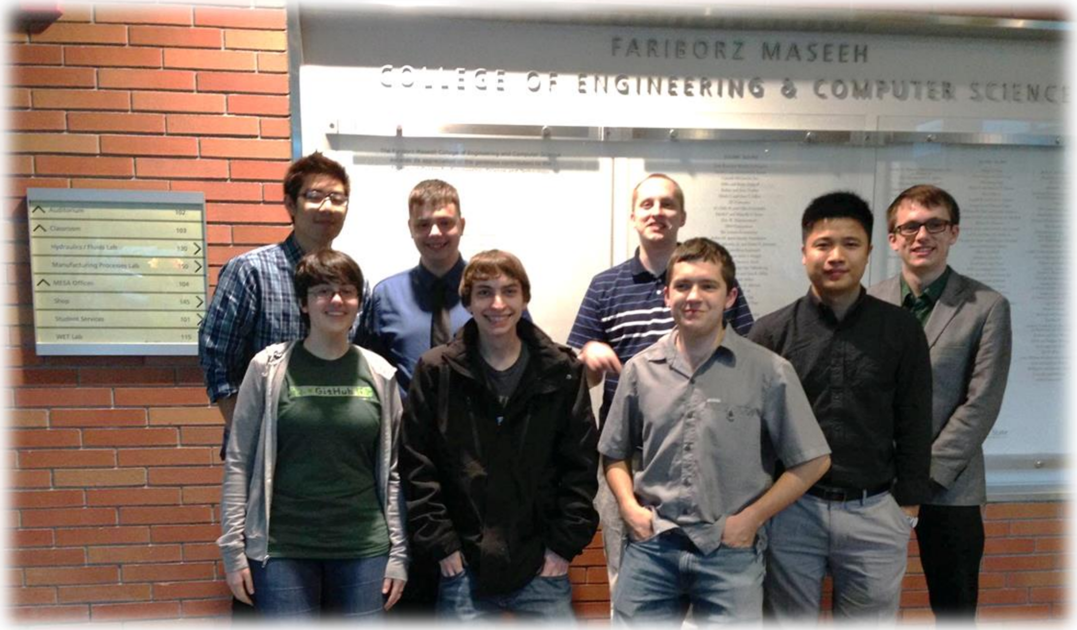
- Cookies of ‘00

Portland State University

- B.S Computer Science
- Associates in International Studies, Japanese
- Member of ACM, CTF/War Games club, DC480

Monero Contributor

Automation Engineer at Intel



/u/xmrscott

irc: xmrscott@freenode

https://github.com/sanecito/presentations

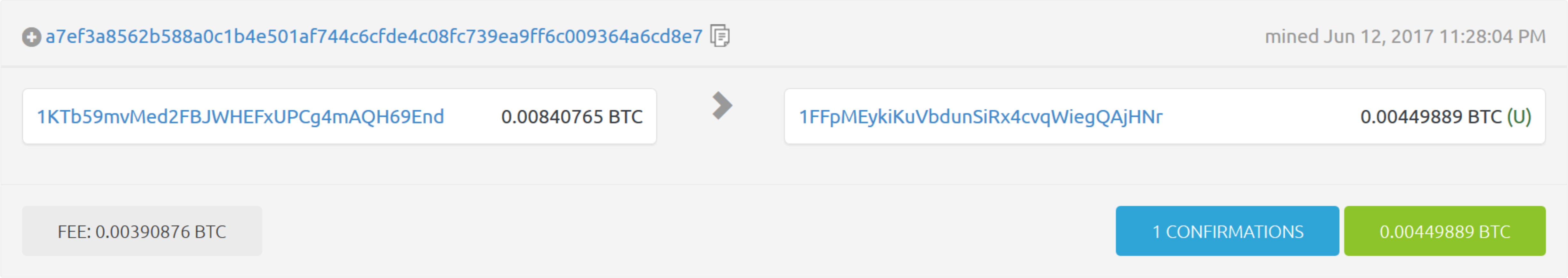
# Presentation Outline

Why does blockchain privacy matter (recap)?

What is Monero?

Where can I buy Monero and use it?

# What makes up a Bitcoin transaction?



a7ef3a8562b588a0c1b4e501af744c6cfde4c08fc739ea9ff6c009364a6cd8e7

mined Jun 12, 2017 11:28:04 PM

1KTb59mvMed2FBJWHEFxUPCg4mAQH69End 0.00840765 BTC

1FFpMEykiKuVbdunSiRx4cvqWiegQAjHNr 0.00449889 BTC (U)

FEE: 0.00390876 BTC

1 CONFIRMATIONS

0.00449889 BTC

SOURCE: BLOCKEXPLORER.COM

# Bitcoin De-anonymization

Coinbase sent Troia back an email explaining that those actions were against the exchange's rules and shut down his account. Troia then tried setting up an account with [his family’s info]. Shut down.

SOURCES: HTTP://WWW.COINDESK.COM/COINBASE-WHITE-HAT-HACKER-DONT-WANT-BITCOIN/

# Bitcoin De-anonymization

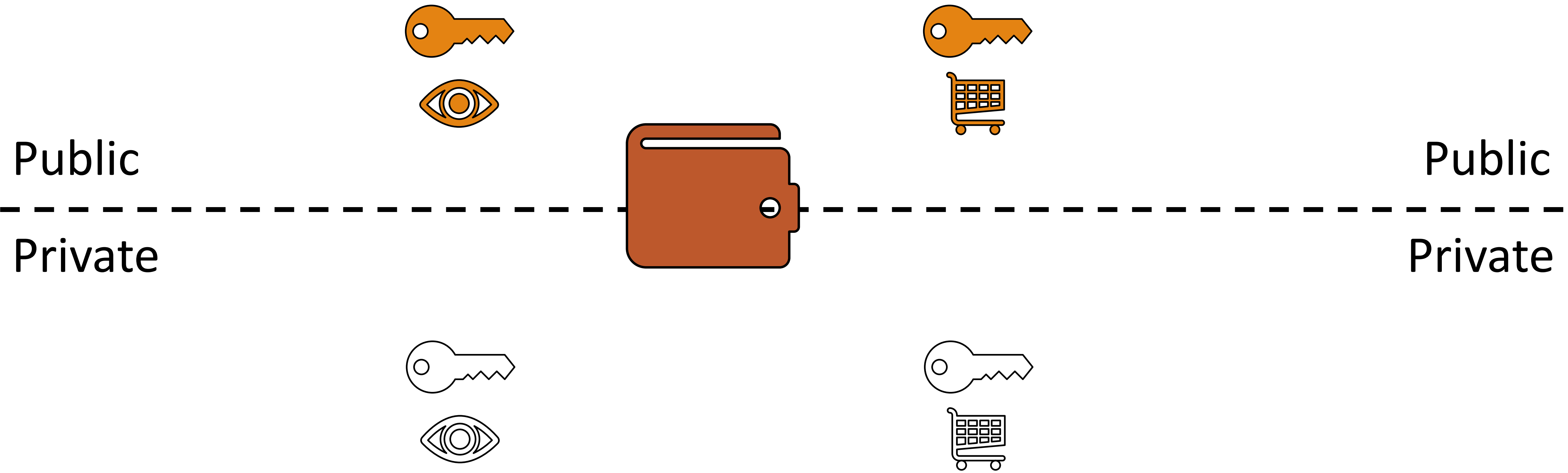
“To strengthen our efforts to combat the illicit use of digital currency transactions under our existing authorities, [Office of Foreign Assets Control] may include as identifiers on the [Specially Designated Nationals] List specific digital currency addresses associated with blocked persons” –OFAC, #561, 2018/03/19

SOURCES: HTTPS://WWW.TREASURY.GOV/RESOURCE-CENTER/FAQS/SANCTIONS/PAGES/FAQ_COMPLIANCE.ASPX#VC_FAQS

# Monero Protocol Protection

| Sender (Alice) | Amount | Network | Receiver (Bob) |
|---|---|---|---|
| Ring Signatures | RingCT | Kovri | Stealth Addresses |

# Monero Wallet



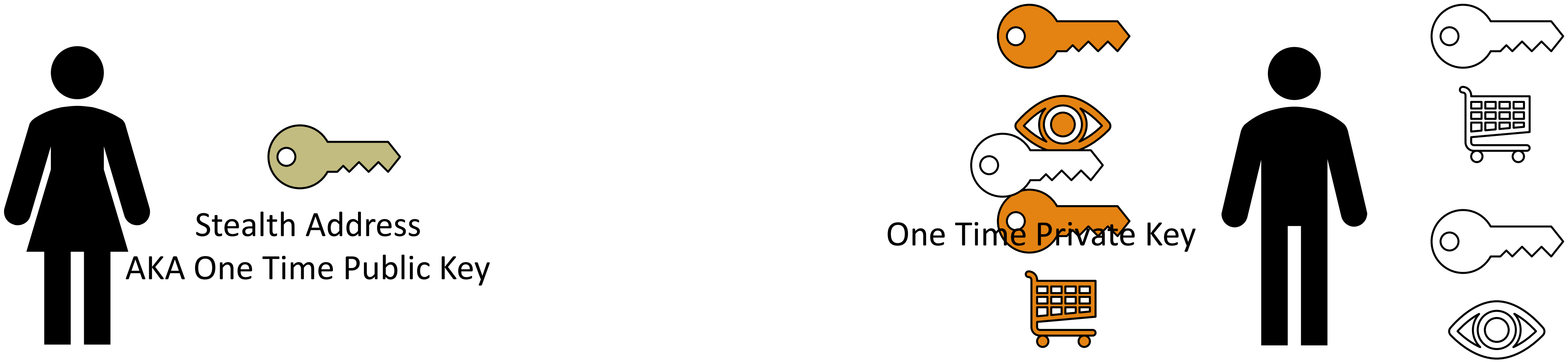
Public

Private

Public

Private

# Stealth Addresses

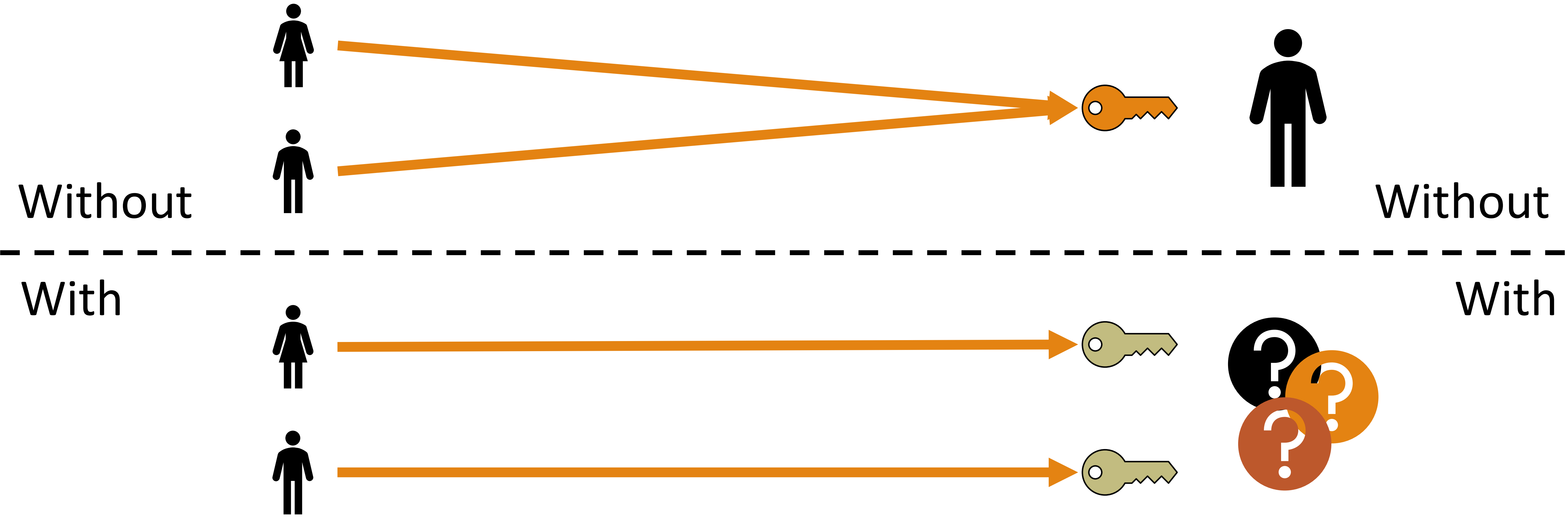


Stealth Address
AKA One Time Public Key

One Time Private Key

FOR IN-DEPTH + DEMO: HTTPS://STEEMIT.COM/MONERO/@LUIGI1111/UNDERSTANDING-MONERO-CRYPTOGRAPHY-PRIVACY-PART-2-STEALTH-ADDRESSES

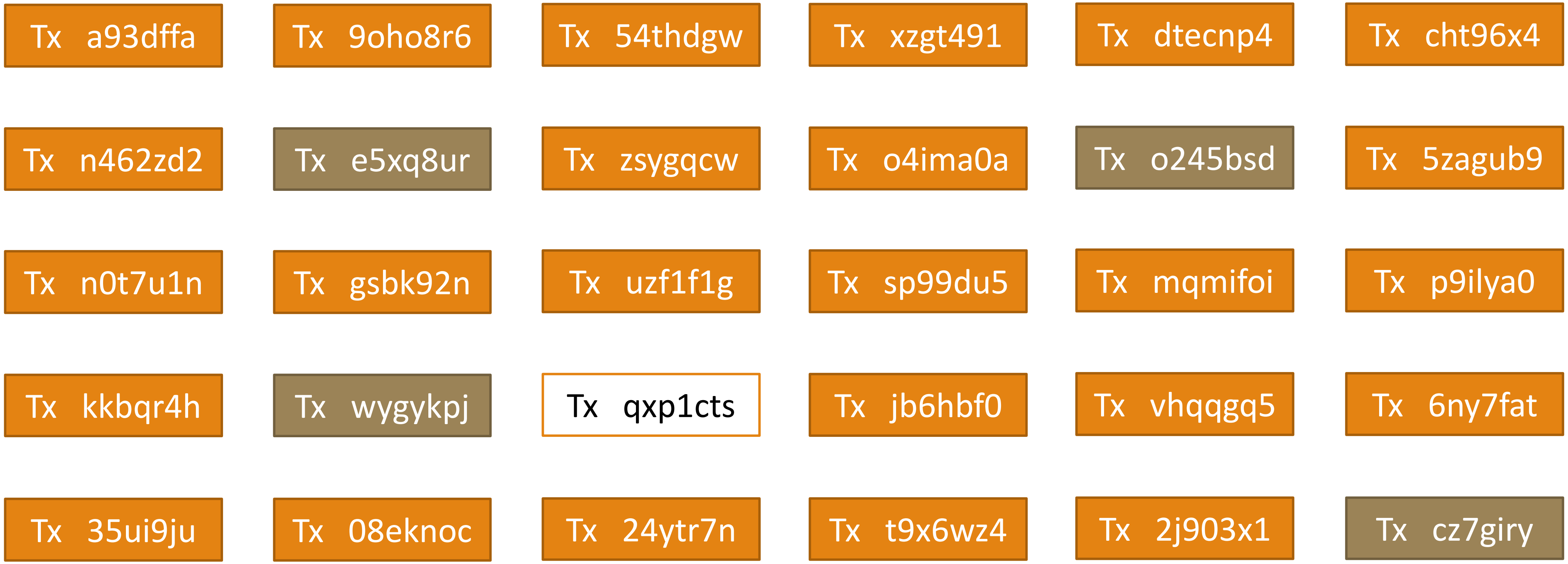
# Stealth Addresses (cont'd)



# Ring Signatures

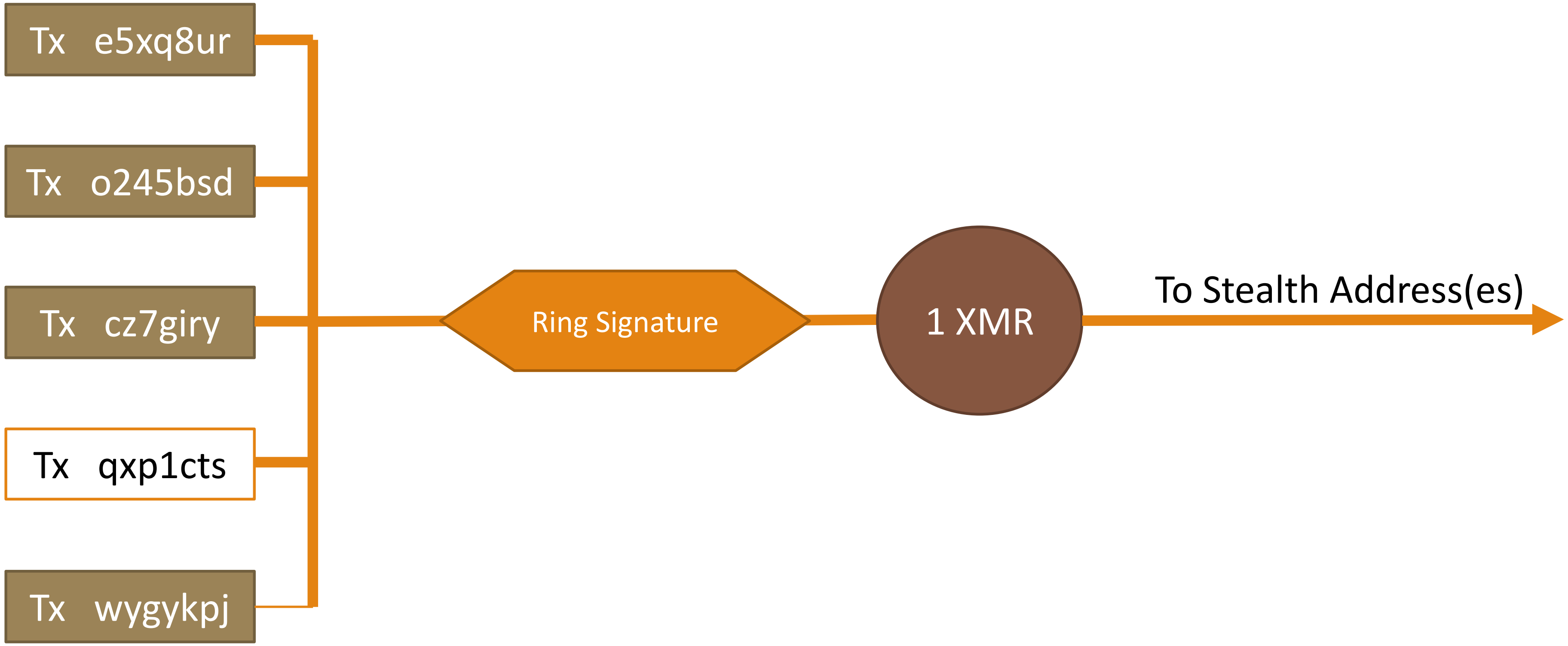
| | | | | | |
|---|---|---|---|---|---|
| Tx a93dffa | Tx 9oho8r6 | Tx 54thdgw | Tx xzgt491 | Tx dtecnp4 | Tx cht96x4 |
| Tx n462zd2 | Tx e5xq8ur | Tx zsygqcw | Tx o4ima0a | Tx o245bsd | Tx 5zagub9 |
| Tx n0t7u1n | Tx gsbk92n | Tx uzf1f1g | Tx sp99du5 | Tx mqmifoi | Tx p9ilya0 |
| Tx kkbqr4h | Tx wygykpj | Tx qxp1cts | Tx jb6hbf0 | Tx vhqqgq5 | Tx 6ny7fat |
| Tx 35ui9ju | Tx 08eknoc | Tx 24ytr7n | Tx t9x6wz4 | Tx 2j903x1 | Tx cz7giry |

# Ring Signatures

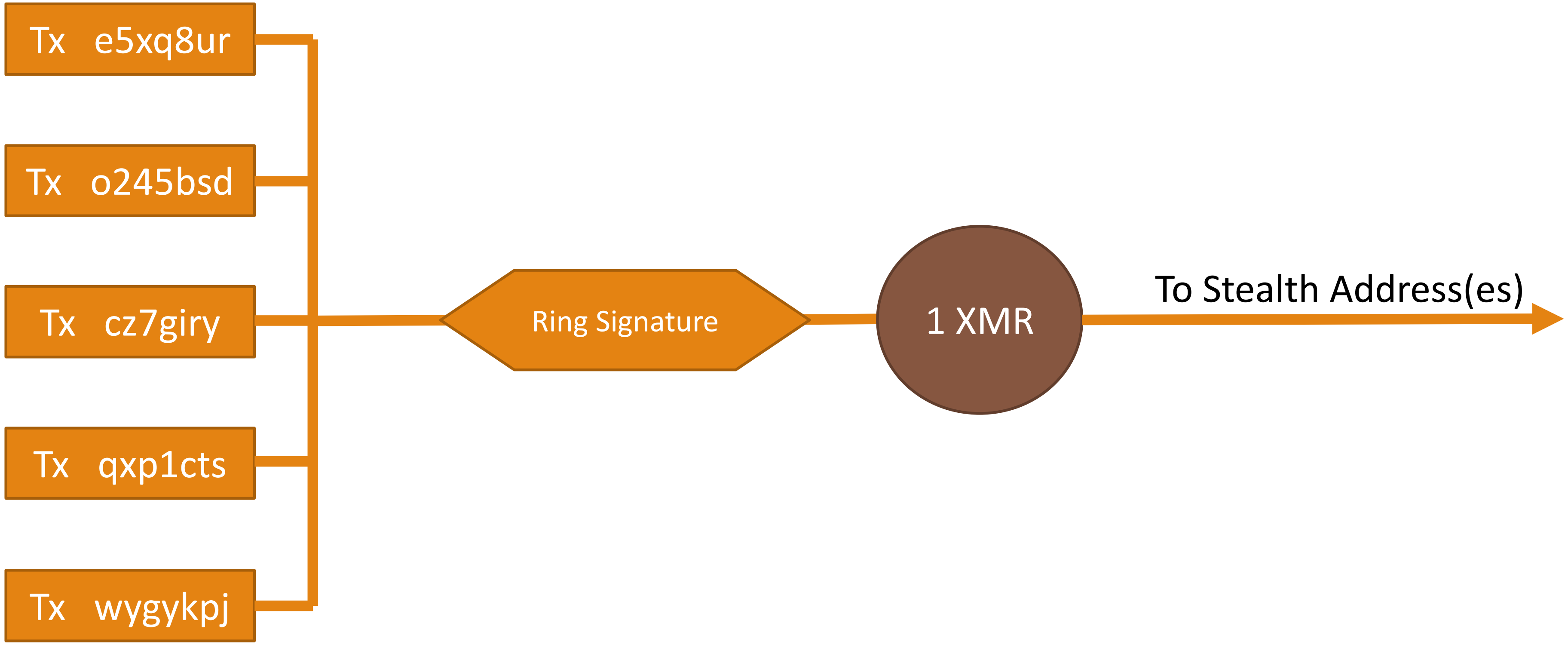


| | | | | | |
|---|---|---|---|---|---|
| Tx a93dffa | Tx 9oho8r6 | Tx 54thdgw | Tx xzgt491 | Tx dtecnp4 | Tx cht96x4 |
| Tx n462zd2 | Tx e5xq8ur | Tx zsygqcw | Tx o4ima0a | Tx o245bsd | Tx 5zagub9 |
| Tx n0t7u1n | Tx gsbk92n | Tx uzf1f1g | Tx sp99du5 | Tx mqmifoi | Tx p9ilya0 |
| Tx kkbqr4h | Tx wygykpj | Tx qxp1cts | Tx jb6hbf0 | Tx vhqqgq5 | Tx 6ny7fat |
| Tx 35ui9ju | Tx 08eknoc | Tx 24ytr7n | Tx t9x6wz4 | Tx 2j903x1 | Tx cz7giry |

# Ring Signatures



# Ring Signatures



Taken from Justin Ehrenhofer’s presentations

# Ring Signatures & RingCT

**INPUTS**

5

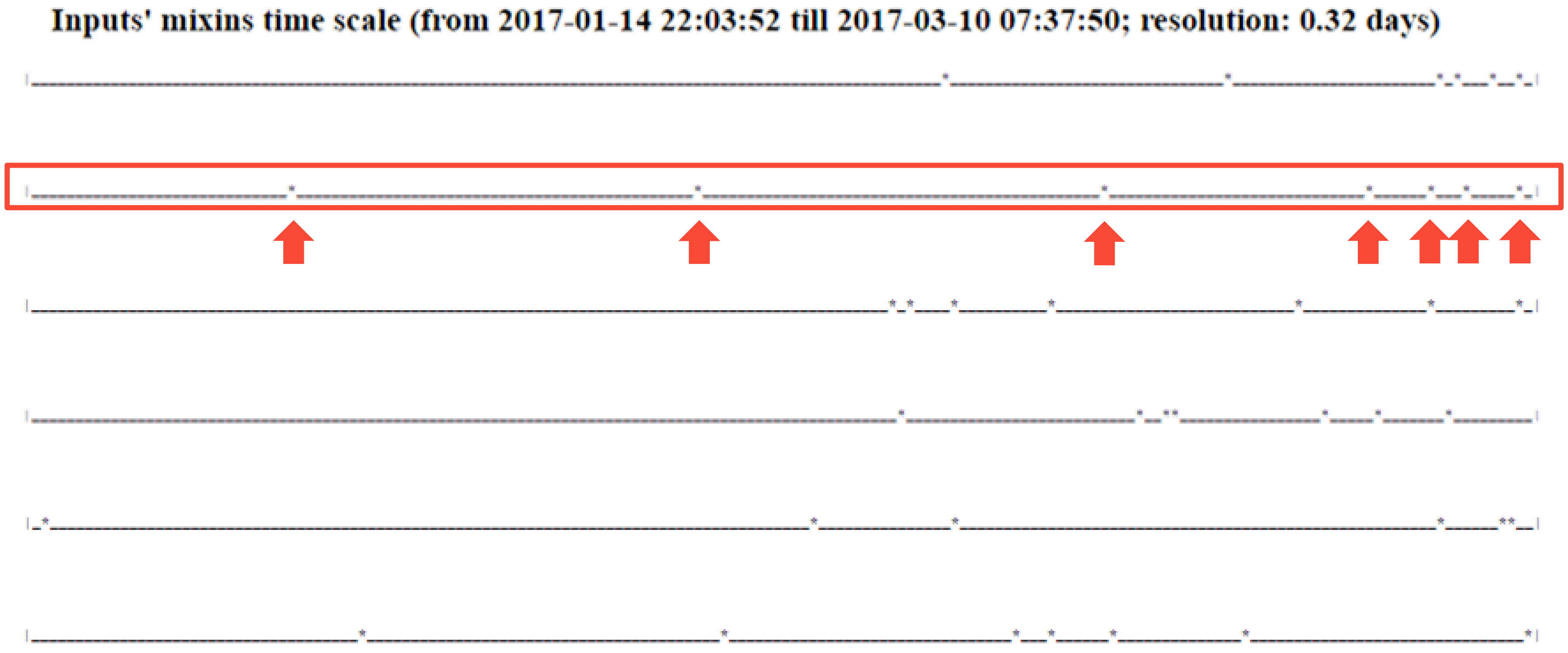
8

11

15

18

21



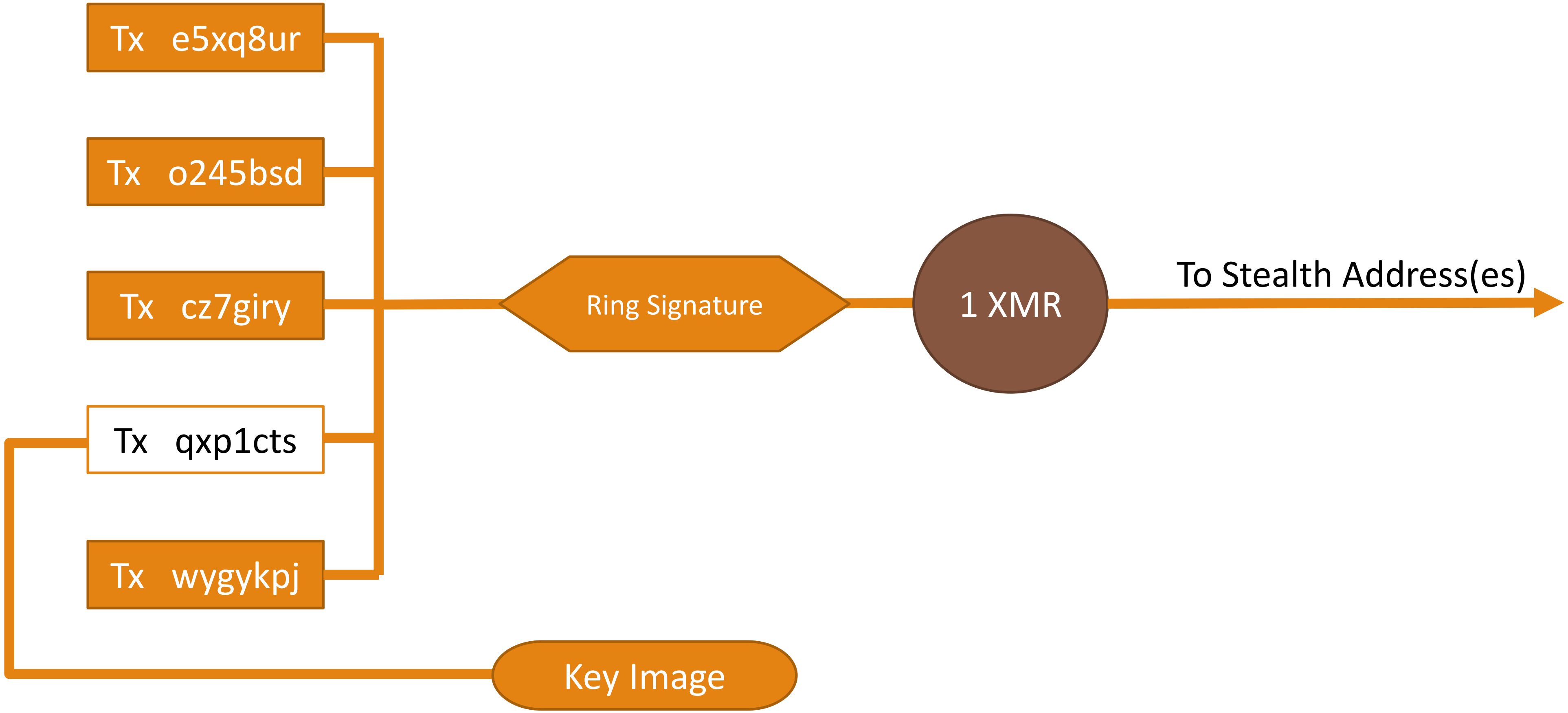
Inputs' mixins time scale (from 2017-01-14 22:03:52 till 2017-03-10 07:37:50; resolution: 0.32 days)

Older

Newer

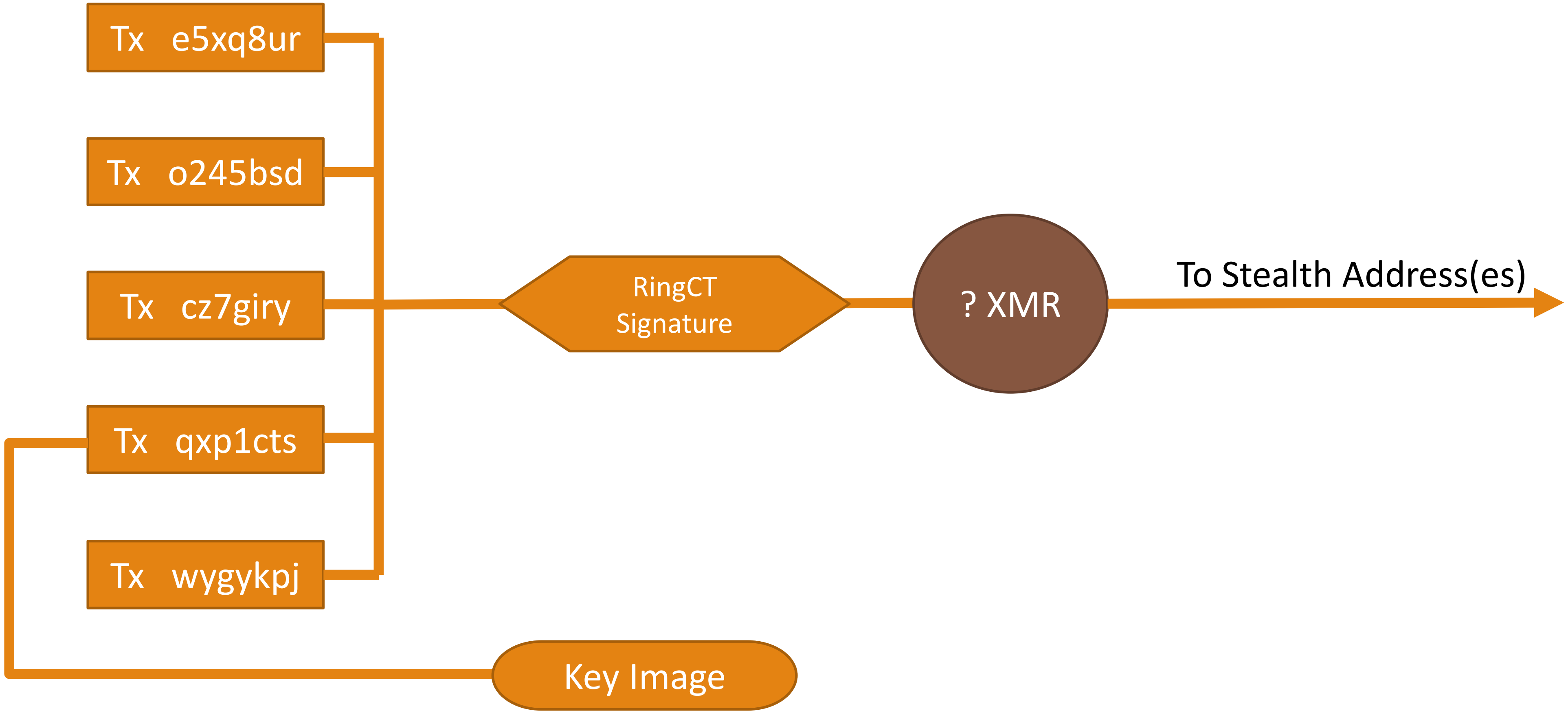
HTTPS://XMRCHAIN.NET/SEARCH?VALUE=9BB608C70622CE67333C267103241F19B8ACA21B7915F237813E451E1F03576E

# Ring Signatures



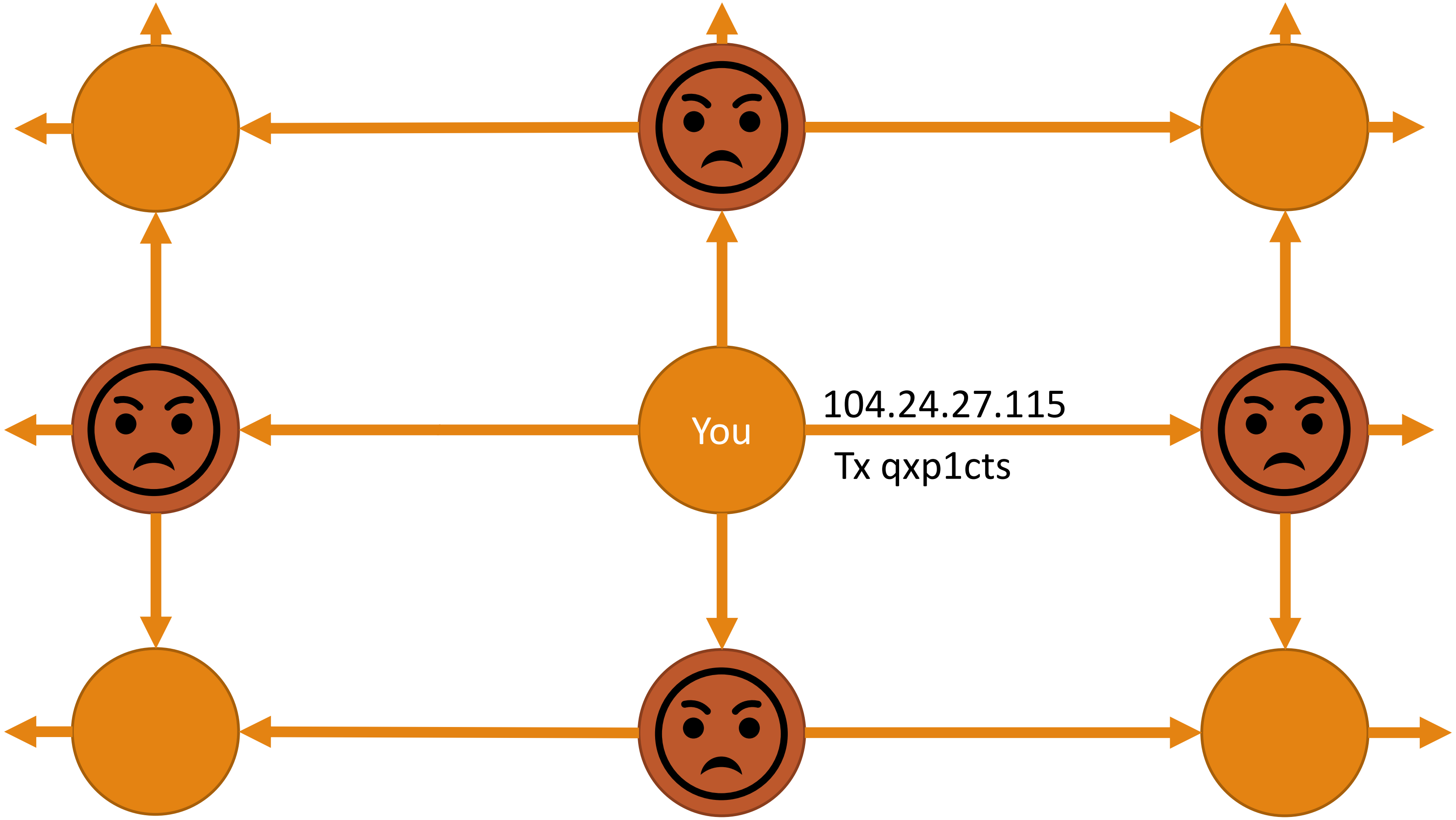
SEE: HTTPS://LAB.GETMONERO.ORG/PUBS/MRL-0005.PDF

# Ring Confidential Transactions (RingCT)

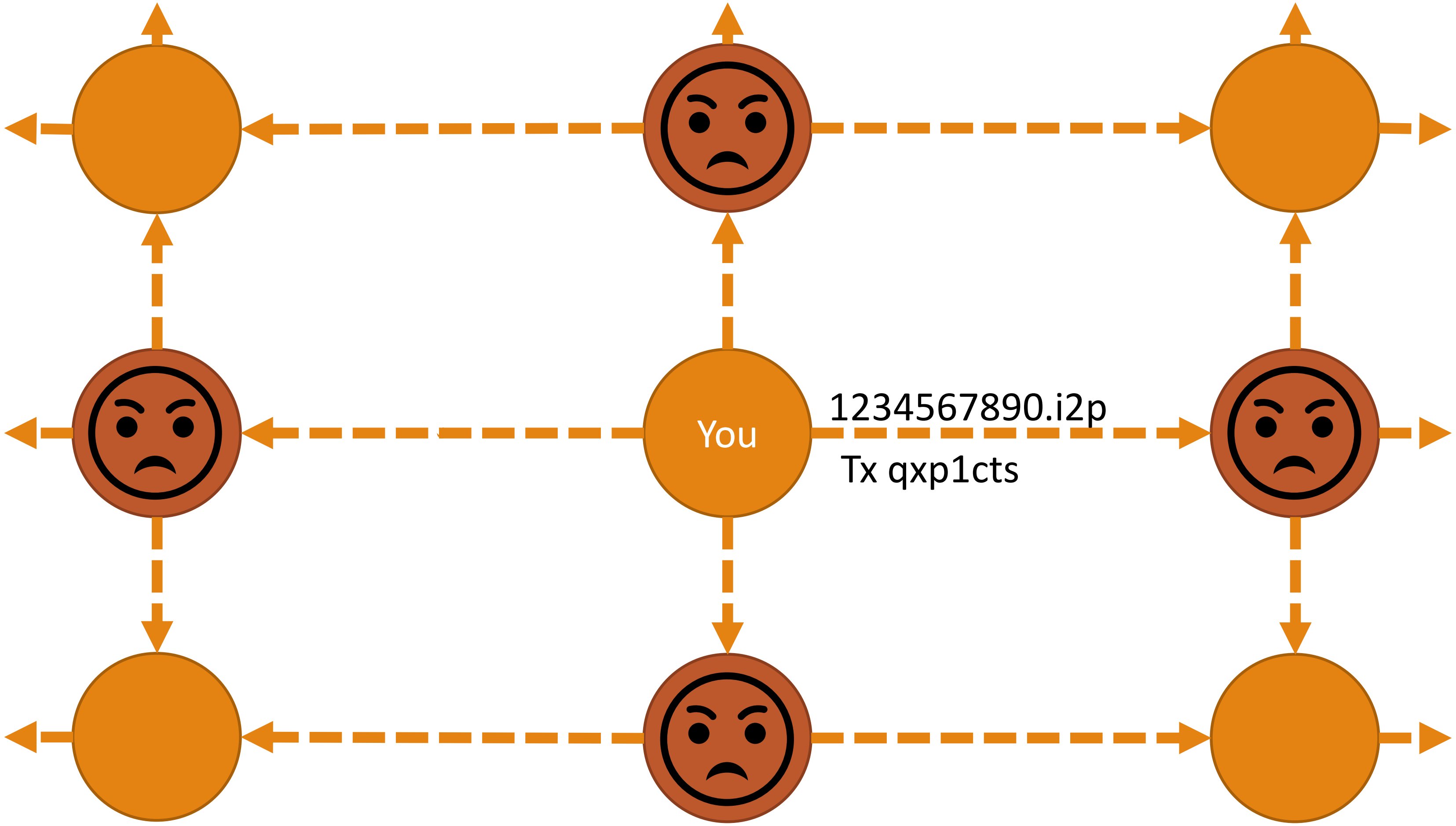


SEE: HTTPS://LAB.GETMONERO.ORG/PUBS/MRL-0005.PDF

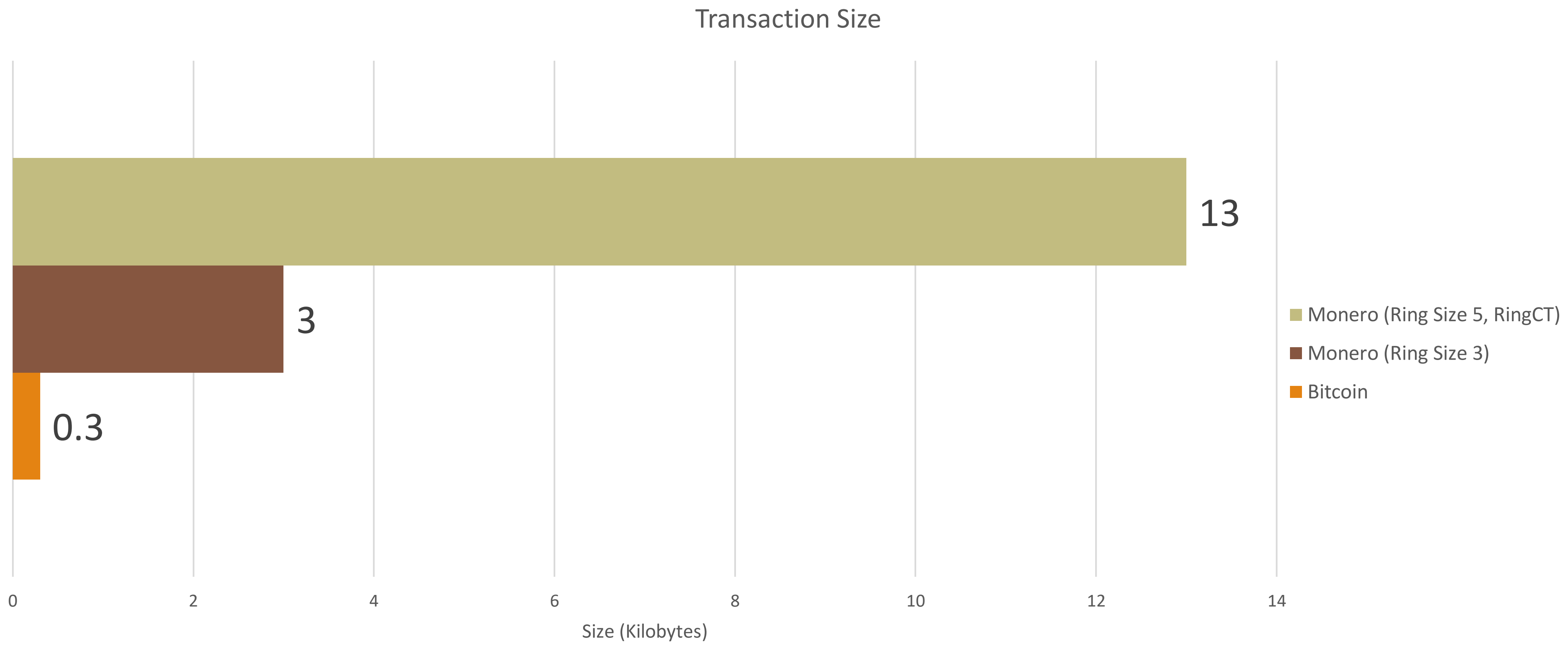
# Kovri (without)



# Kovri



# Scalability



# Probability

Ring Size 5 != 20 / 20 / 20 / 20 / 20 Probability

# Rates Compared (*Circa Sept 2016 for $100)

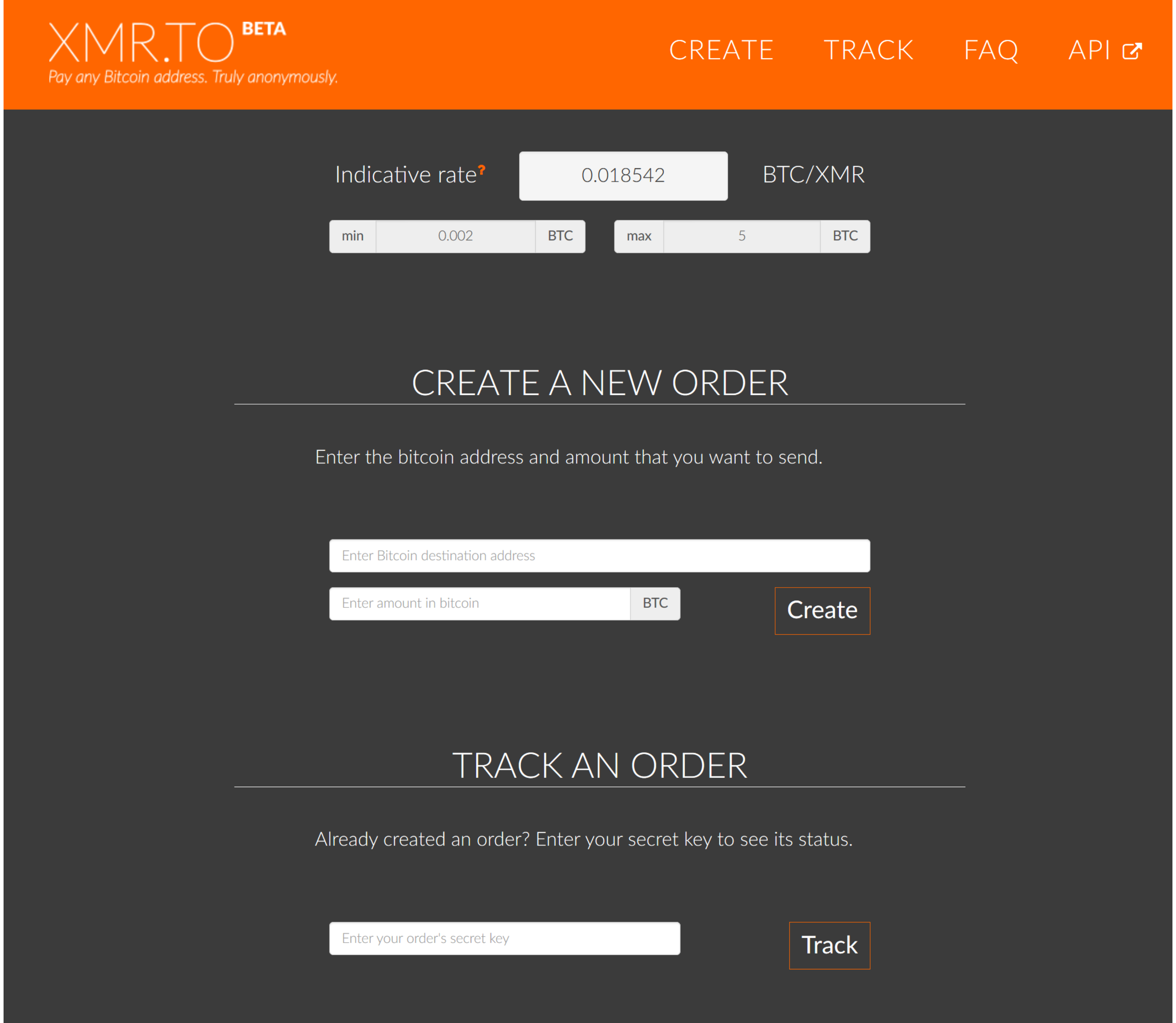
Poloniex: 0.25% (GDAX) + 0.25% (Poloniex) + .2 XMR = **~2.5% fees***

Shapeshift: GDAX + Shapeshift Exchange Rate = **~7% fees***

Kraken: $10 (Wire Transfer) + $? (Bank’s Wire Transfer Fee) + 0.26%

Bisq (Formerly Bitsquare): Depends on seller (Fiat/BTC) + chosen exchange rate (BTC/XMR)

TAKEN FROM: HTTPS://MONEROERIC.COM/BUY-MONERO-BITCOIN-SHAPESHIFT-POLONIEX/



Indicative rate? 0.018542 BTC/XMR

min 0.002 BTC

max 5 BTC

## CREATE A NEW ORDER

Enter the bitcoin address and amount that you want to send.

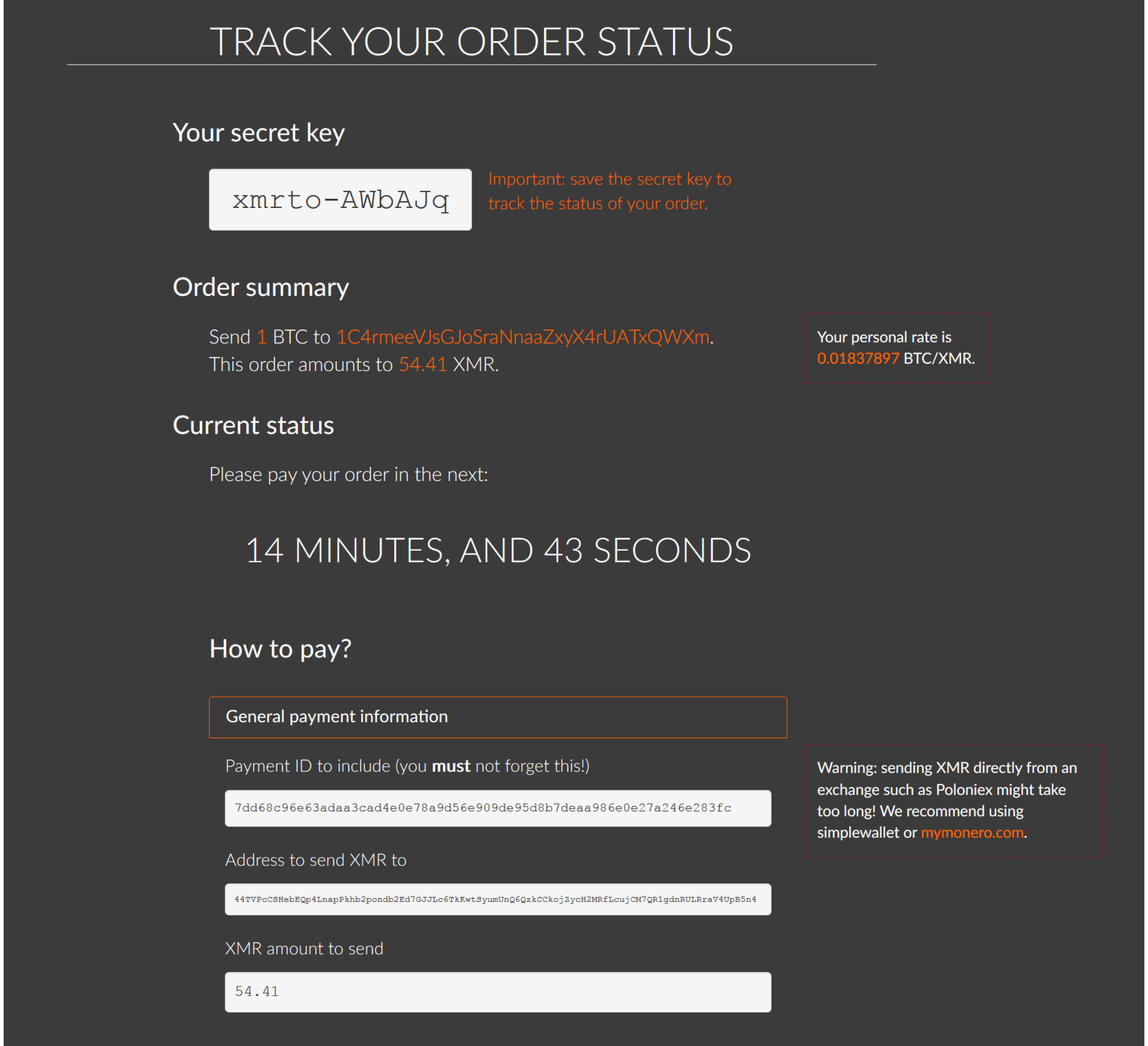
Enter Bitcoin destination address

Enter amount in bitcoin BTC

## TRACK AN ORDER

Already created an order? Enter your secret key to see its status.

Enter your order's secret key



# TRACK YOUR ORDER STATUS

## Your secret key

`xmrto-AWbAJq`

Important: save the secret key to track the status of your order.

## Order summary

Send 1 BTC to 1C4rmeeVJsGJoSraNnaaZxyX4rUATxQWXm.
This order amounts to 54.41 XMR.

Your personal rate is 0.01837897 BTC/XMR.

## Current status

Please pay your order in the next:

14 MINUTES, AND 43 SECONDS

## How to pay?

General payment information

Payment ID to include (you **must** not forget this!)

```
7dd68c96e63adaa3cad4e0e78a9d56e909de95d8b7deaa986e0e27a246e283fc
```

Address to send XMR to

```
44TVPcCSHebEQp4LnapPkhb2pondb2Ed7GJJLc6TkKwtSyumUnQ6QzkCCkojZycH2MRfLcujCM7QR1gdnRULRraV4UpB5n4
```

XMR amount to send

```
54.41
```

Warning: sending XMR directly from an exchange such as Poloniex might take too long! We recommend using simplewallet or mymonero.com.

GetMonero.org

/r/Monero
/r/MoneroMining
/r/XMRTrader
/r/MoneroCommunity

/u/xmrscott

Monero.stackexchange.com

irc: #monero
(freenode)

xmrscott@freenode