

Monero 101

SCOTT ANECITO

Who am I?

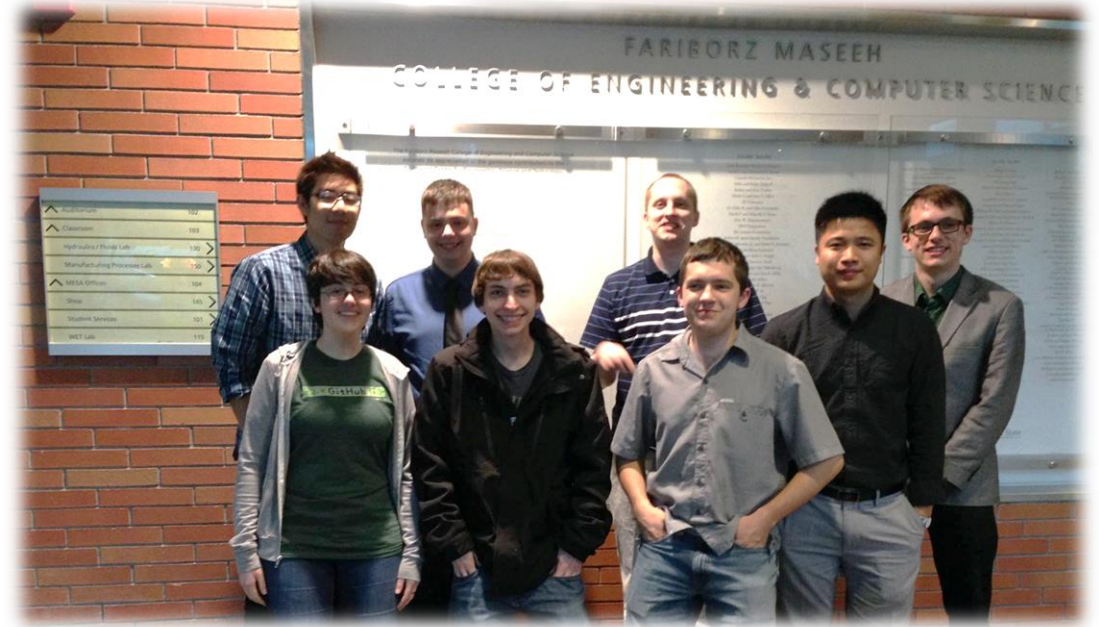
Privacy and security enthusiast

- Cookies of '00

Portland State University

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

Automation Engineer at Intel



How I came to Monero

Hides the following fingerprints:

- Sender wallet address
- Receiver wallet address
- Transaction amount
- IP Address*

Genesis and operations has no points for potential collusion

Ideally:

- Has no pre-mine
- Has no instamine
- Isn't primarily governed by a company (see: potential collusion)
- Has a relatively active and sizable community to grow project and quickly respond to exploits

Presentation Outline

Why does privacy matter?

What is Monero?

Where did Monero come from?

How does Monero compare?

Where can I buy Monero and use it?

Why would people want your data?



World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 25th Apr 2017)

interesting story

YEAR

BUBBLE COLOUR

YEAR

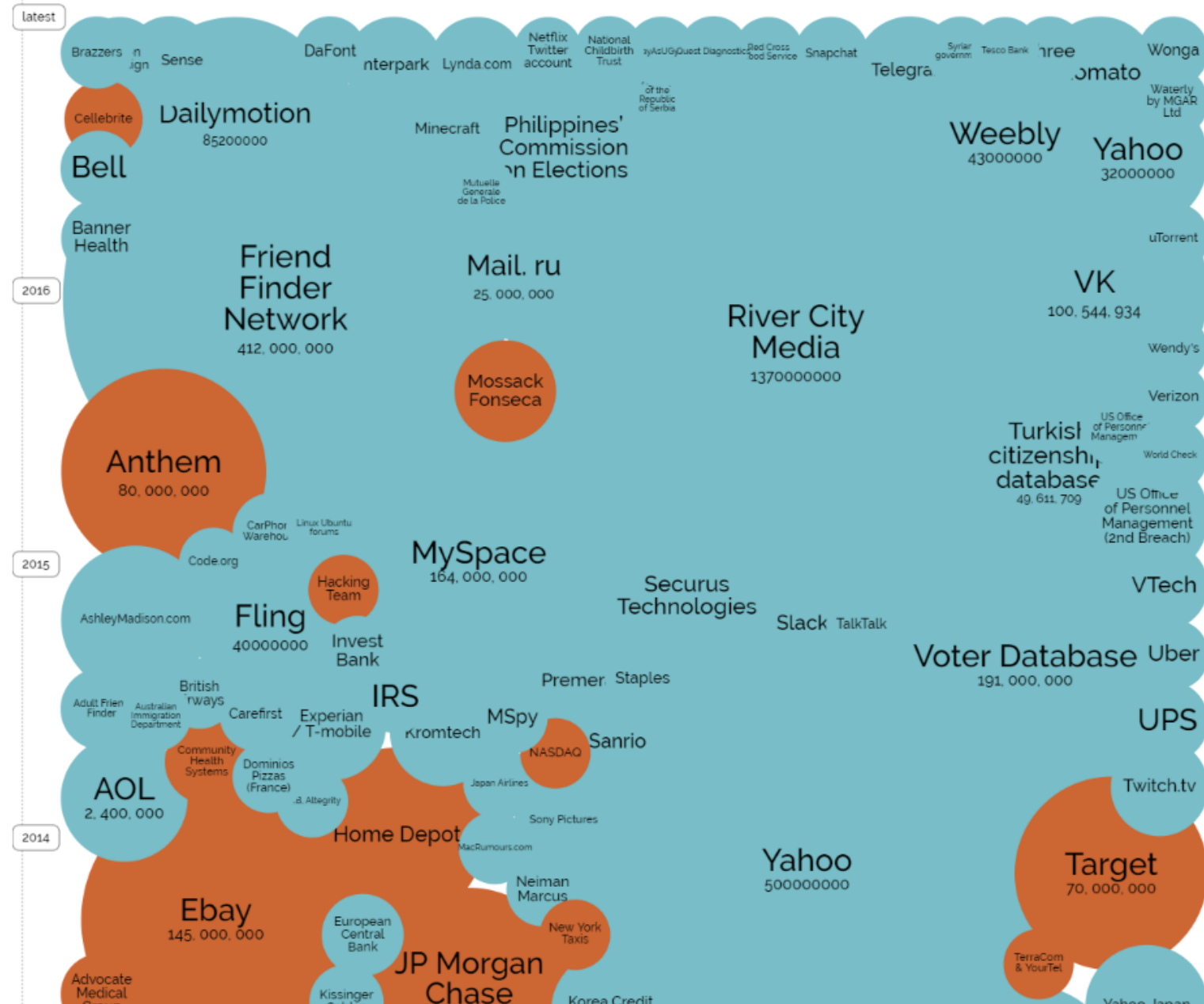
METHOD OF LEAK

BUBBLE SIZE


NO OF RECORDS STOLEN

DATA SENSITIVITY

SHOW FILTER



Office of Personnel Management



“The intruders... gained access to... employees’ Social Security numbers, job assignments, performance ratings and training information”

“attackers have targeted the forms submitted by intelligence and military personnel for security clearances. The document includes personal information – everything from eye colour to financial history, to past substance abuse, as well as contact details for the individual’s friends and relatives”

“How to lose \$8k worth of bitcoin in 15 minutes with Verizon and Coinbase.com”

AKA Smashing SMS-2FA for Fun and Profit

Step 1: Find a target via SNS



Cody Brown ✓
@CodyBrown

 **Follow**

This incident with [@adachis](#) is pretty troubling for [@coinbase](#). I trade all my coins there, worried by their lack of transparency & response

4:55 PM - 21 May 2017 · Brooklyn, NY



67

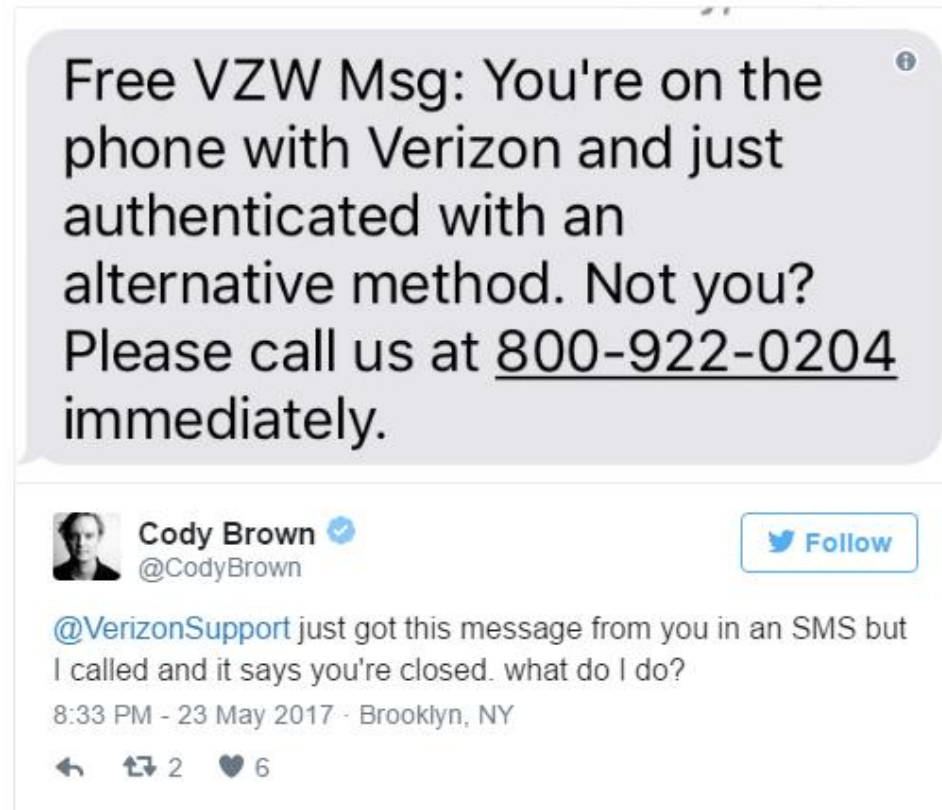


81















Step 2: Have info stolen/obtained

“After talking at length with [Verizon] customer service reps, I learned that the hacker did not need to give them my pin number or my social security number and was able to get approval to takeover my cell phone number with *simple billing information*.”

Step 3: Use info to take control of phone



Step 4: Profit

<input type="checkbox"/>			Google	Suspicious activity in your account - Suspicious activity in your account Hi Cody, We've detecte
<input checked="" type="checkbox"/>			Coinbase	You just sent 16.03894582 ETH to 0x752eaba83bb6a4fce5a7043db9ef5890b88ed6fa - Coinbe
<input checked="" type="checkbox"/>			Coinbase	You just sent 70.96992853 LTC to LUWwu4o7EXPYaJRya7EzE5MByHpaBZekf7 - Coinbase Y
<input checked="" type="checkbox"/>			Coinbase	You just sent 1.18519844 BTC to 19d9VhEgRhsHfV2XJvY7skKePbZGmpFLY1 - Coinbase You
<input checked="" type="checkbox"/>			Coinbase	New Device Confirmation - Coinbase New device access A device or location we haven't seen
<input checked="" type="checkbox"/>			Coinbase	Resetting Your Password - Coinbase We have received your request for password reset from a
<input type="checkbox"/>			Google	Security alert for your linked Google account - Your password changed You received this mess

The hacker deleted these emails but google recovered them

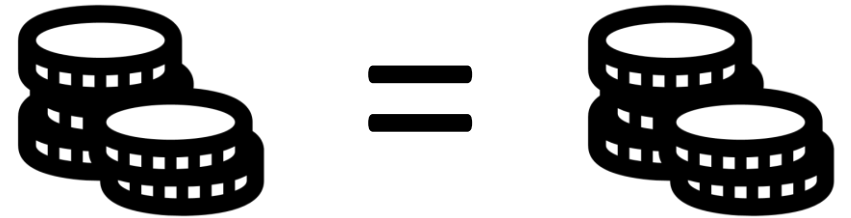
Why does *financial privacy* matter?

People know your income, wealth accumulation

Targeting and/or advertisements based on transactions

Interaction with unknown person of interest

People know your vendors and partners



What makes up a Bitcoin transaction?

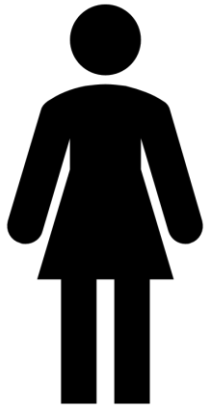
<div></div> a7ef3a8562b588a0c1b4e501af744c6cfde4c08fc739ea9ff6c009364a6cd8e7	mined Jun 12, 2017 11:28:04 PM
<div> <div>1KTb59mvMed2FBJWHEFxUPCg4mAQH69End</div> <div>0.00840765 BTC</div> </div>	<div>➔</div> <div> <div>1FFpMEykiKuVbdunSiRx4cvqWiegQAjHNr</div> <div>0.00449889 BTC (U)</div> </div>
FEE: 0.00390876 BTC	<div>1 CONFIRMATIONS</div> <div>0.00449889 BTC</div>

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.

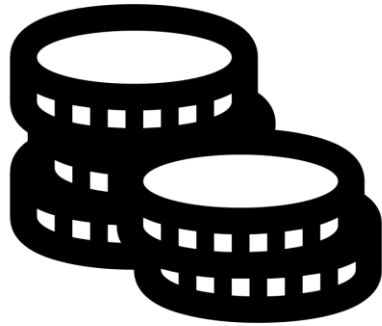
The FBI is requesting \$21m and 80 new employees in a bid to investigate emerging tech that could help the agency combat cybercrime. [...] This notably includes cases that involve "drug traffickers using virtual currencies to obscure their transactions".

Monero Protocol Protection



Sender (Alice)

Ring Signatures



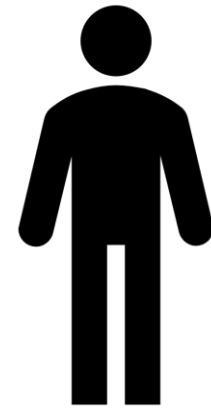
Amount

RingCT



Network

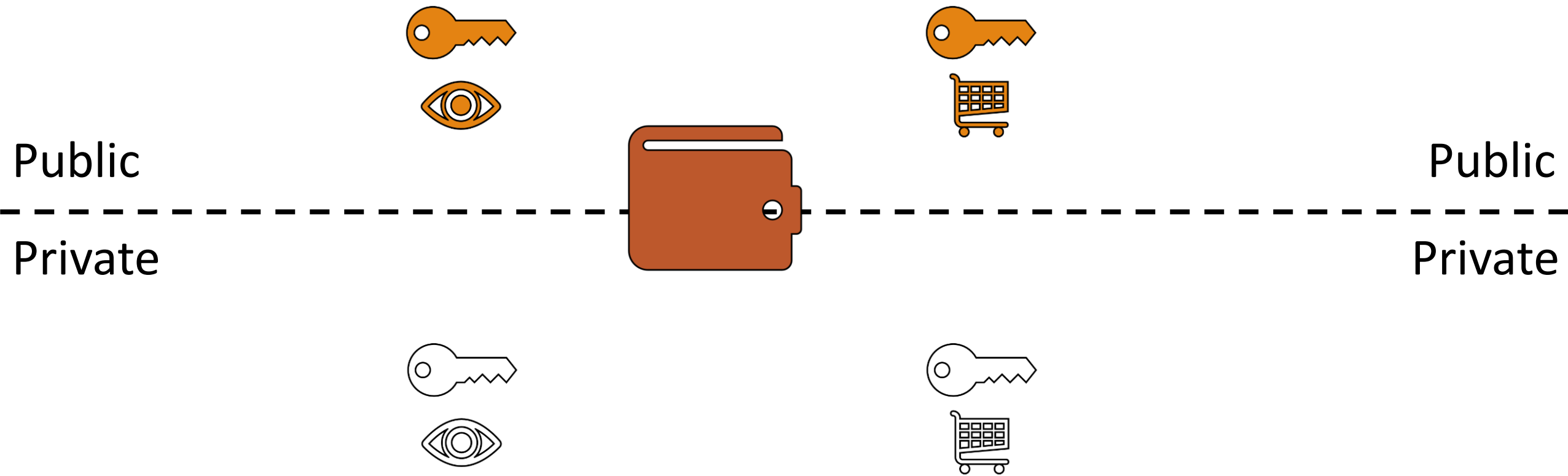
Kovri



Receiver (Bob)

Stealth Addresses

Monero Wallet



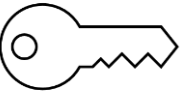
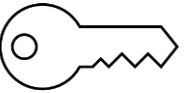
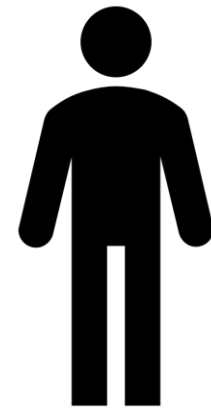
Stealth Addresses



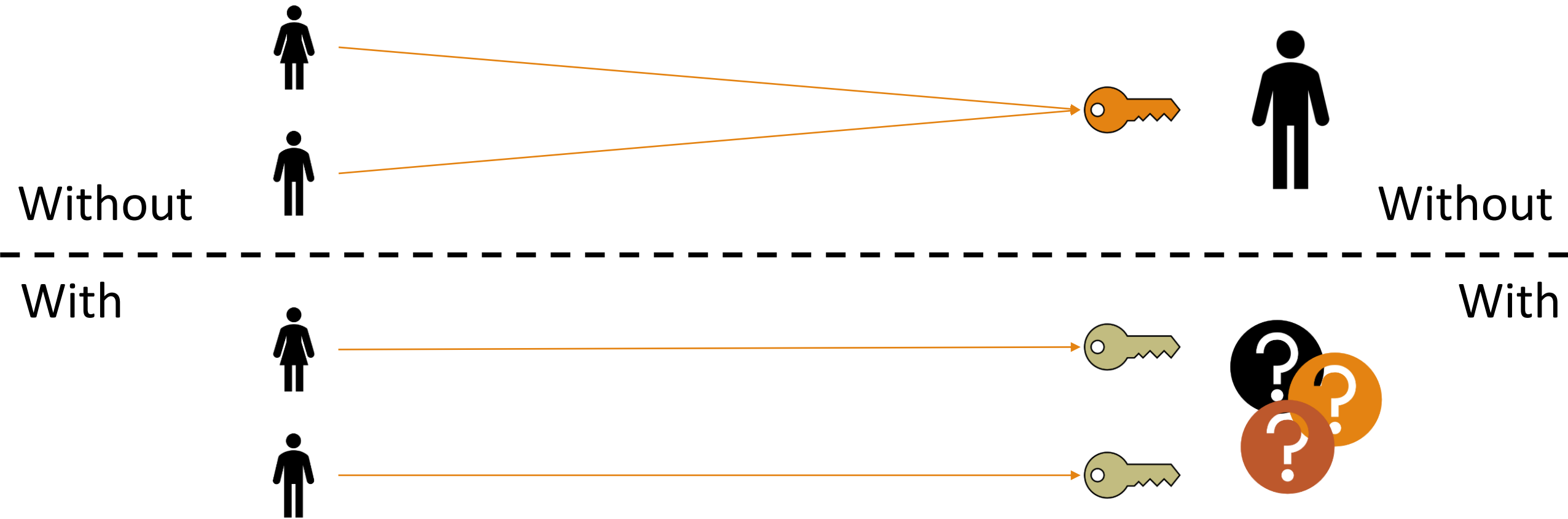
Stealth Address
AKA One Time Public Key



One Time Private Key



Stealth Addresses (cont'd)



Ring Signatures

Tx a93dffa

Tx 9oho8r6

Tx 54thdgw

Tx xzgt491

Tx dtecp4

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 dtecp4

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

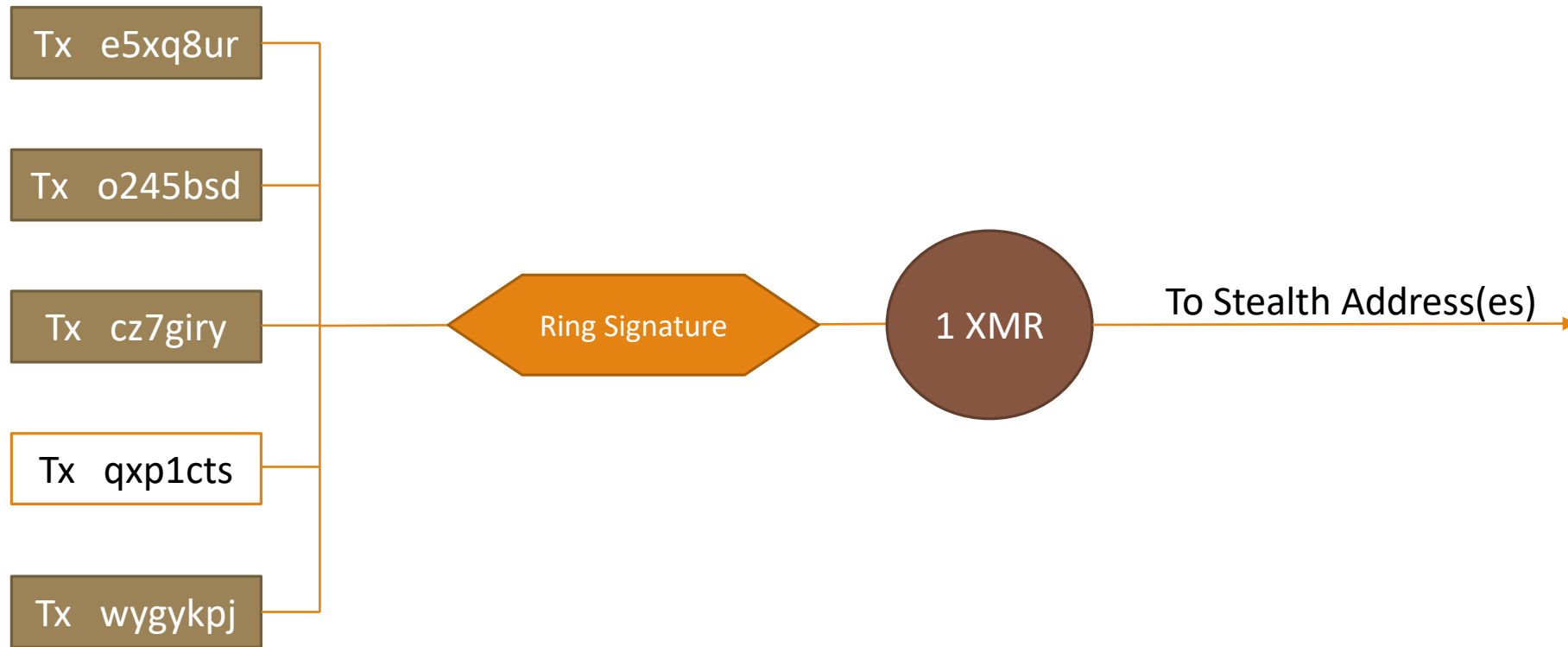
Tx 24ytr7n

Tx t9x6wz4

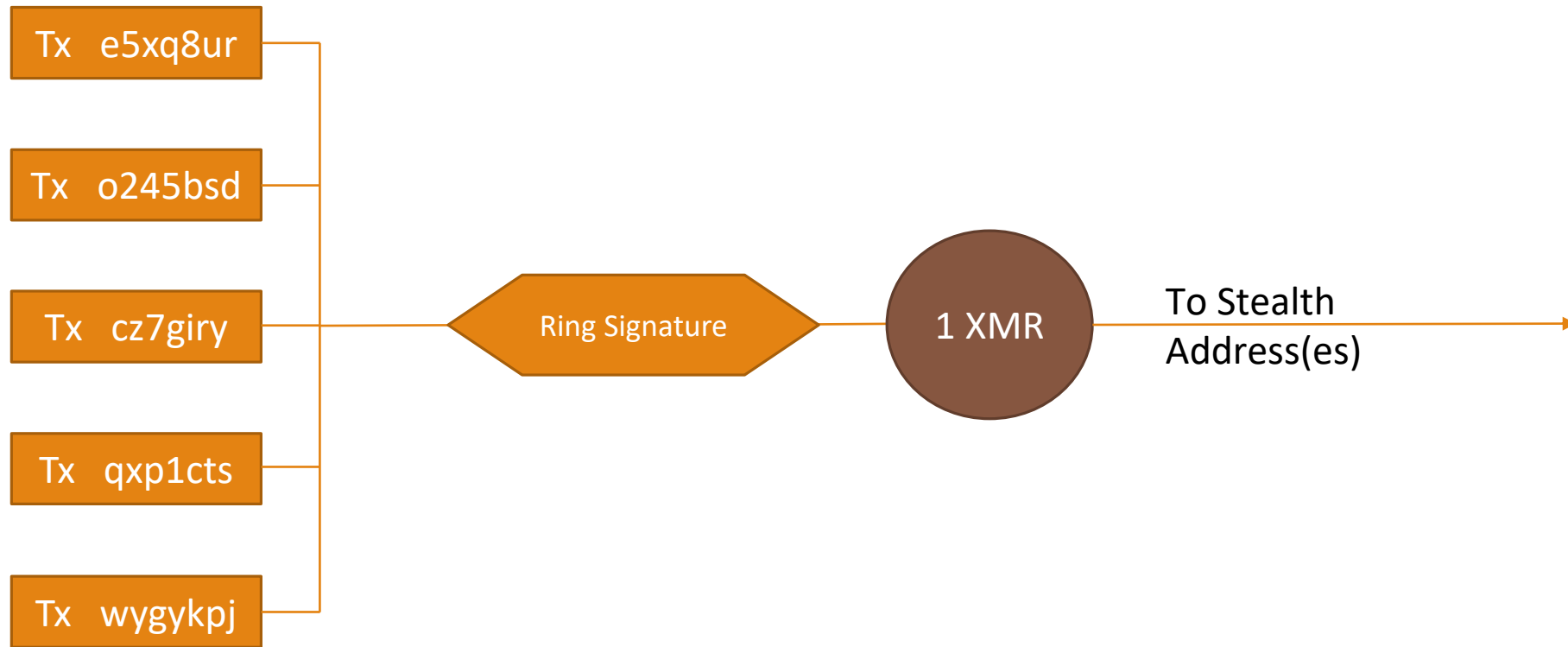
Tx 2j903x1

Tx cz7giry

Ring Signatures

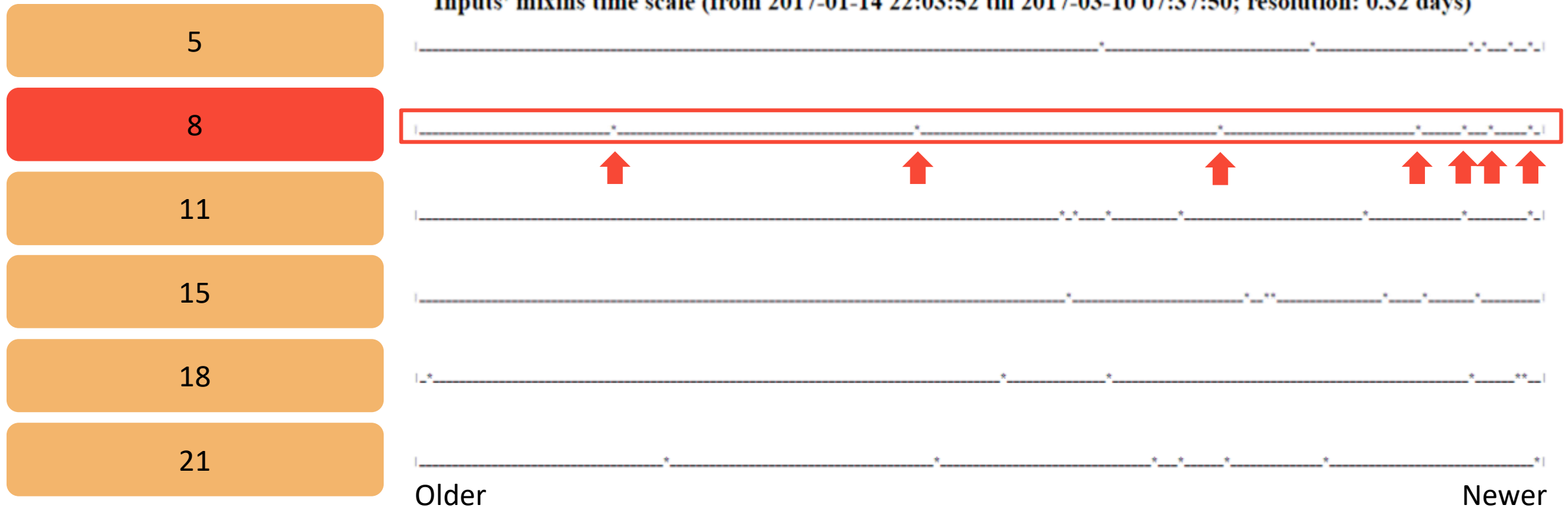


Ring Signatures

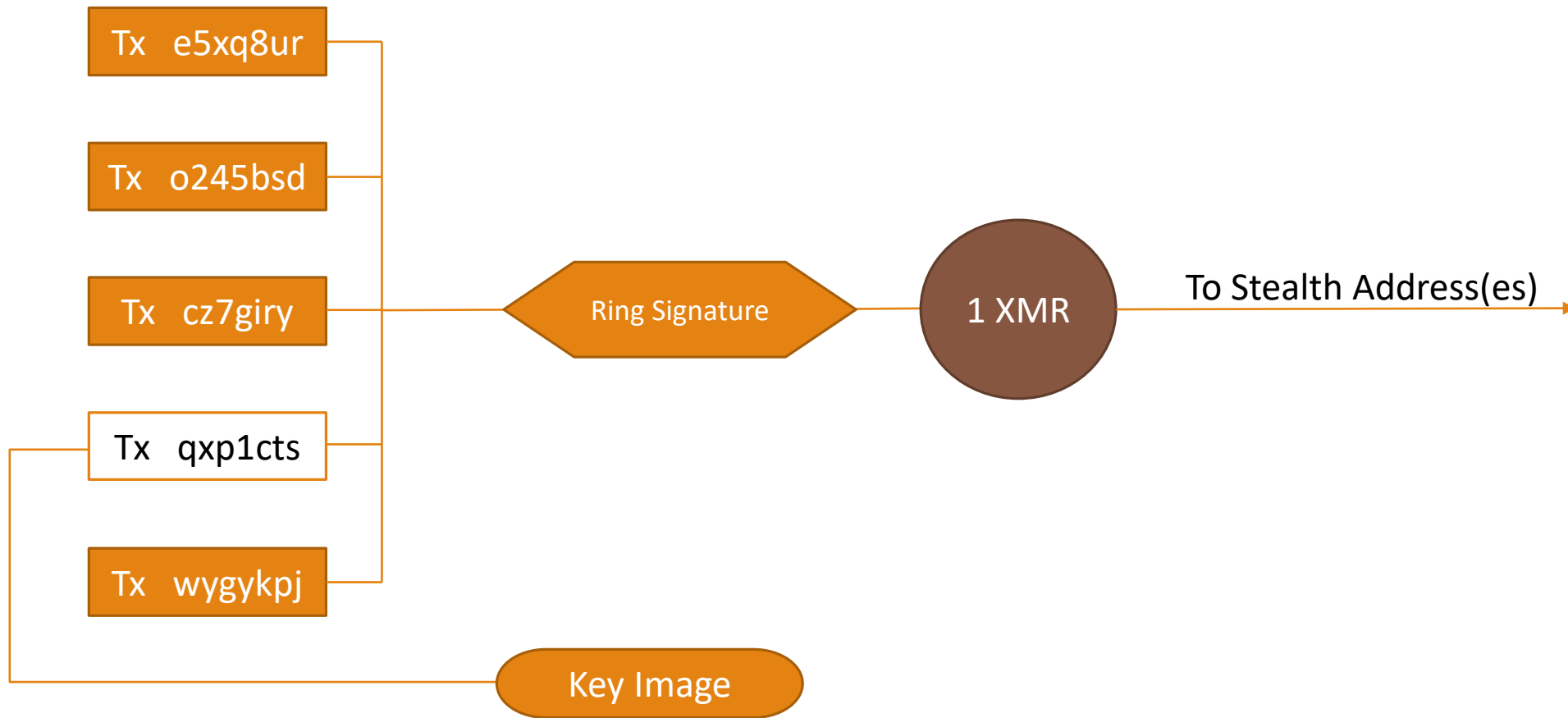


Ring Signatures & RingCT

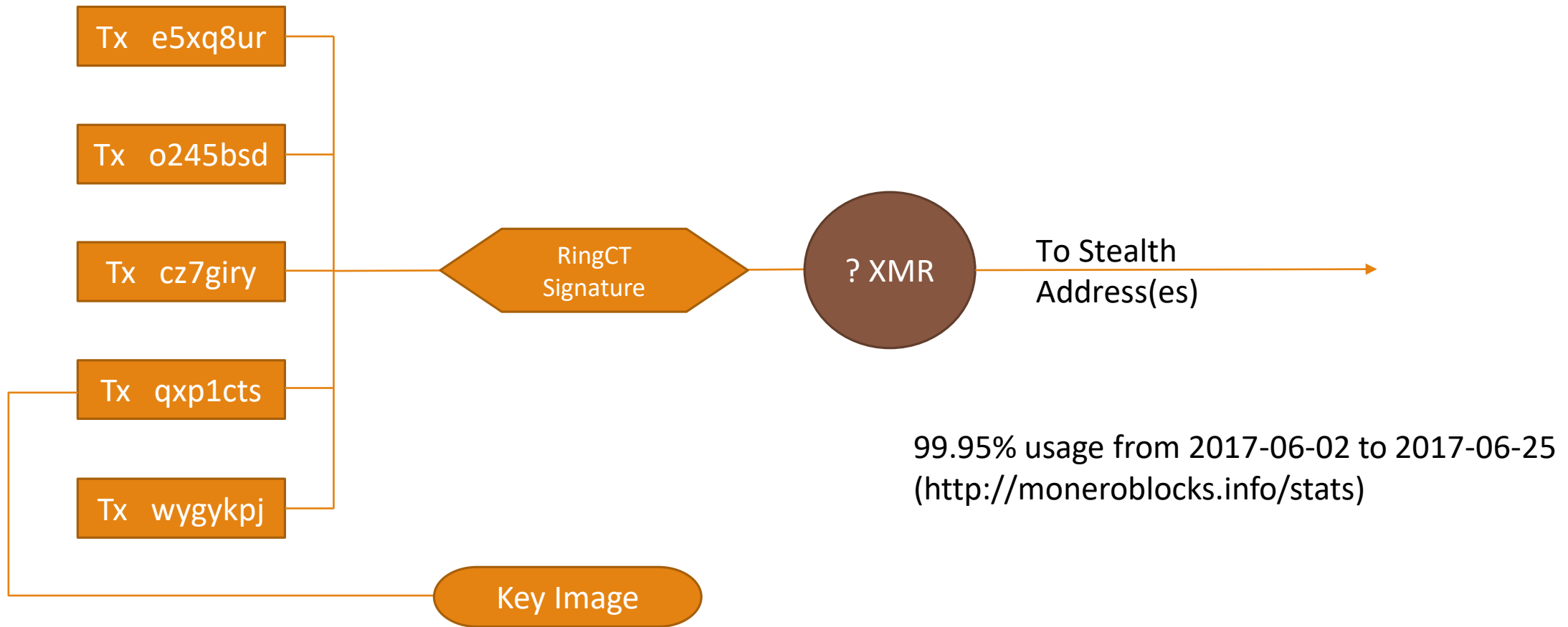
INPUTS



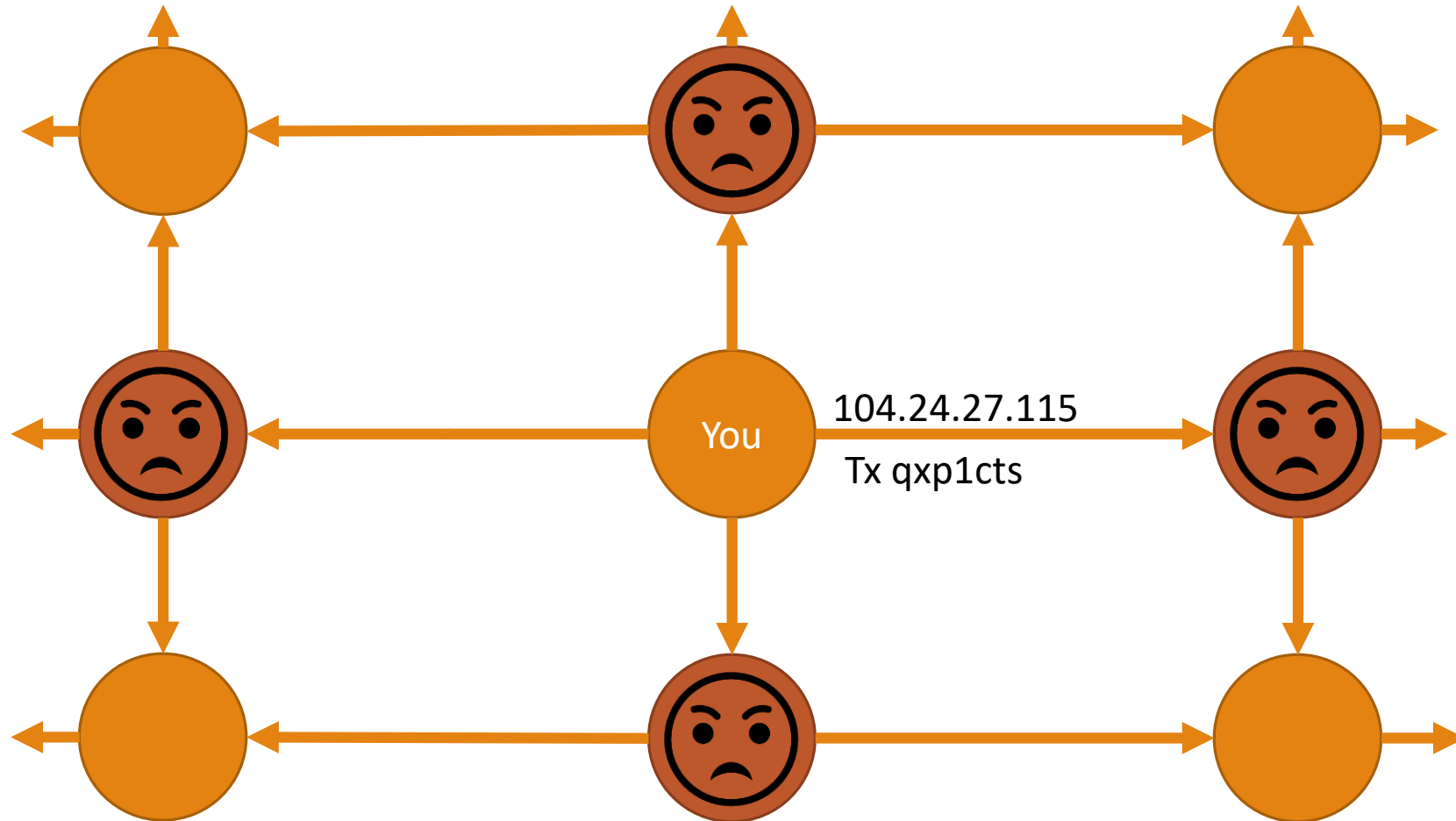
Ring Signatures



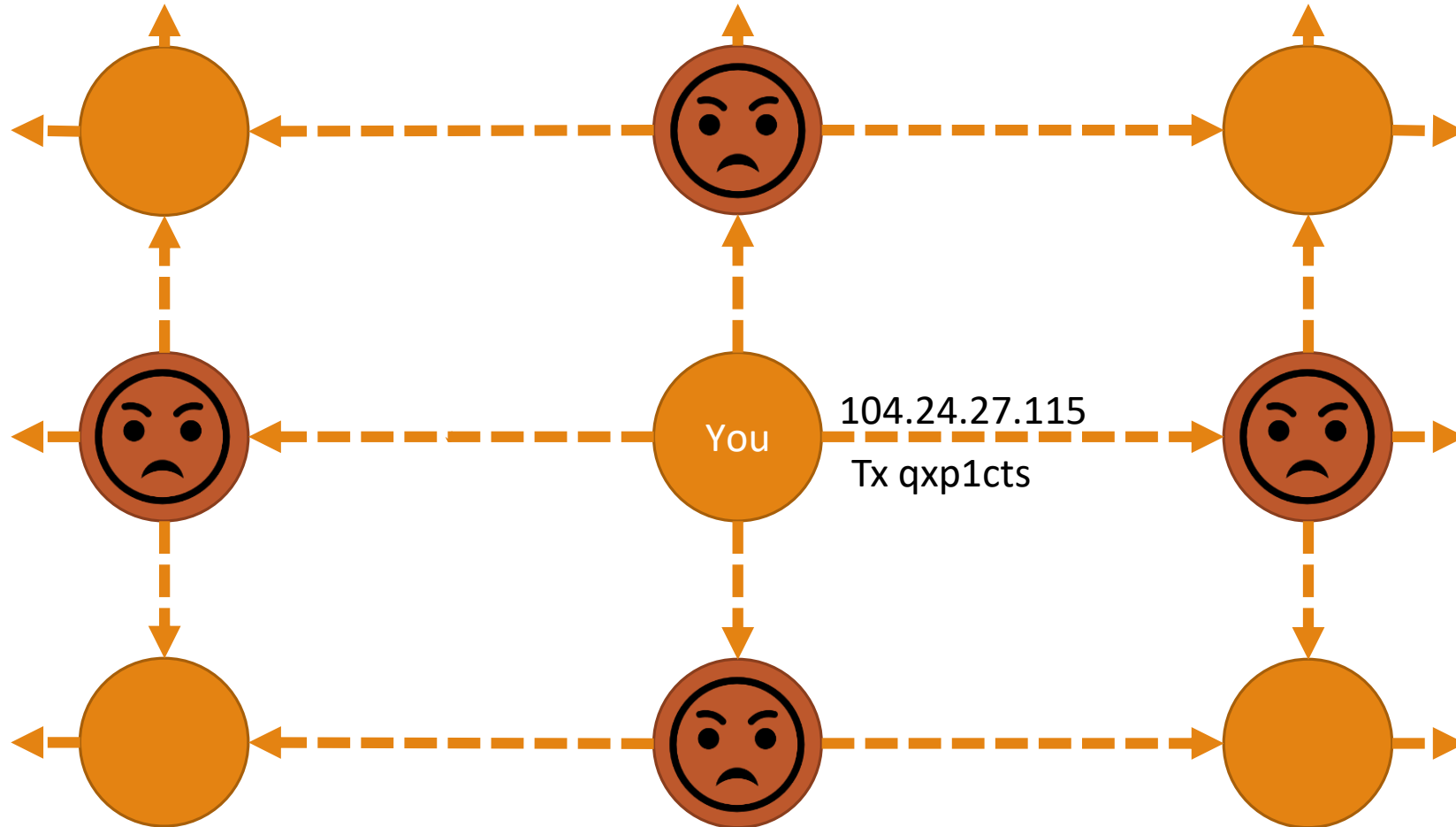
Ring Confidential Transactions (RingCT)



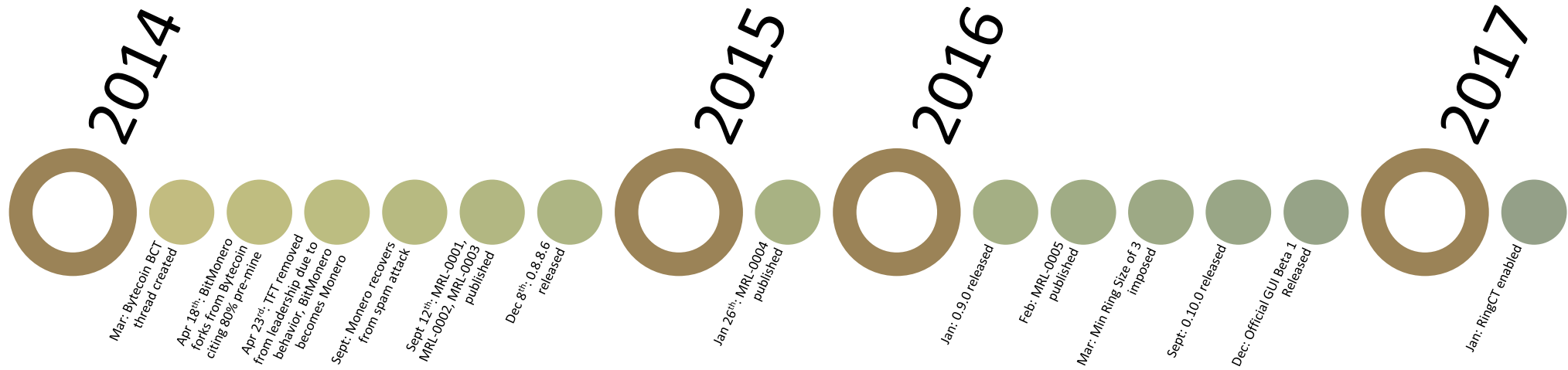
Kovri (without)



Kovri

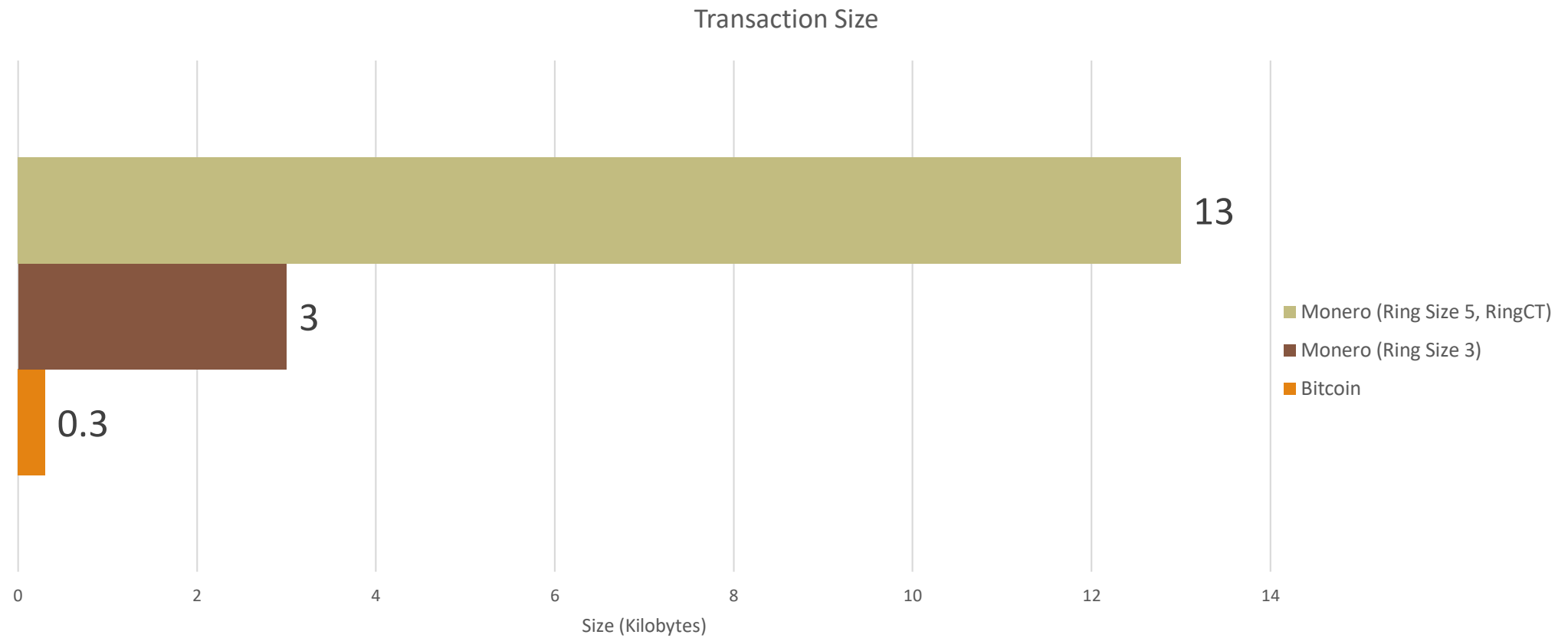


A Brief History of Monero



	Xcoin Darkcoin Dash	Monero	Zcash
Hides Sender?	PrivateSend*	Yes	Z-addr Tx*
Hides Receiver?	PrivateSend*	Yes	Z-addr Tx*
Hides Transaction \$?	PrivateSend*	Yes	Z-addr Tx*
Hides IP?*	No	No	No
% of Tx that are ‘Private’?	Unknown	100% Ring, ~100% RingCT	25%*
Trustless?	No	Yes	No
Primary Governance?	US Company / Masternodes	FLOSS	US Company
Pre-mine or Insta-mine?	Insta-mine	No	No*
Block Reward Fee	45% to Masternodes 10% to Treasury	No	20% for 4 years, “Founders’ Reward”
Block Time	2.5 minutes	2 minutes	2.5 minutes
CoinCap	84 18.9 million	18.4 mil + .3/min emission	21 million

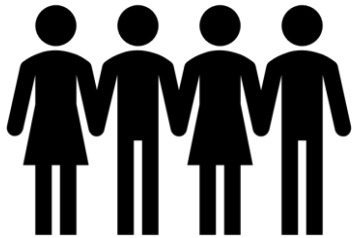
Scalability



Probability

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

Roadmap



Multisig



NanoS integration into Monero

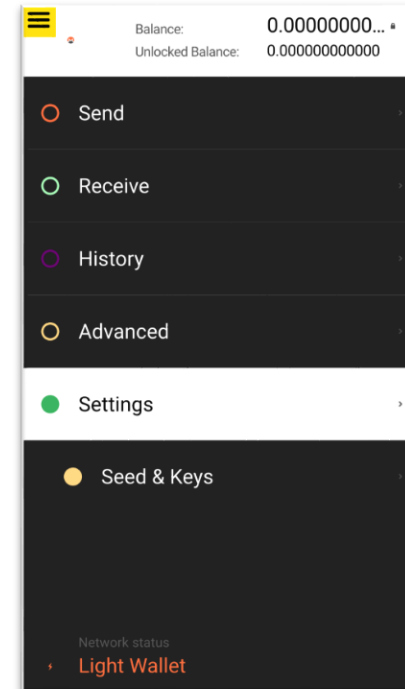
(Ledger SAS, cedric@ledger.fr, Draft Note v0.5)

Table of Contents

I.Short introduction.....	2
II. Notations and definitions.....	2
III. Reminders.....	2
IV. Goals.....	3
V. Nanos Integration.....	3
V.1. Step 1: TX key.....	3
V.2. Step 2: spend key.....	4
V.3. Step 3: destination key.....	5
V.4. Step 4: range proof and blinding.....	5
V.5. Step 5: RCT.....	6
V.5.1. Raw explanation.....	6
V.5.1.1. Interaction Overview.....	6
V.5.1.2. Amount and destination validation.....	6
V.5.2. Nanos interaction.....	7
V.5.2.1. MLSAG: Prehash.....	7
V.5.2.2. MLSAG: signature.....	8
VI. Conclusion.....	10

September 2017 Hardfork

- RingCT enforced
- Increased min Ring Size



fluffyblocks

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)

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.

BTC

[Create](#)

TRACK AN ORDER

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

[Track](#)

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

44TVFcSHebEQp4LnapFkhhb2pondb2Ed7GJJLc6TkKwtSyumUnQ6QzkCCKoj2ycH2MRfLcuJCM7QR1gdnRULRraV4UpB5n4

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



Monero.stackexchange.com

irc: #monero
(freenode)