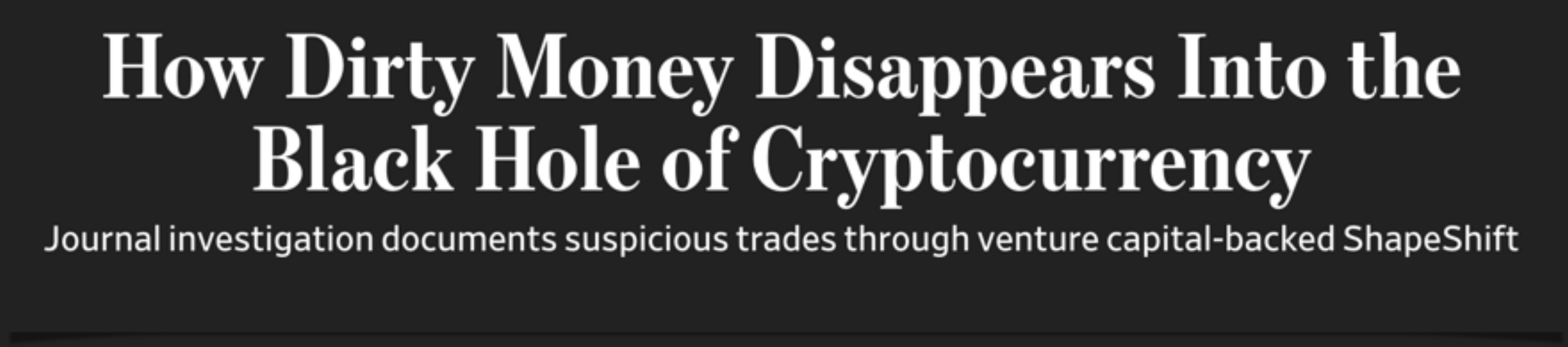
Towards Better Privacy with Monero

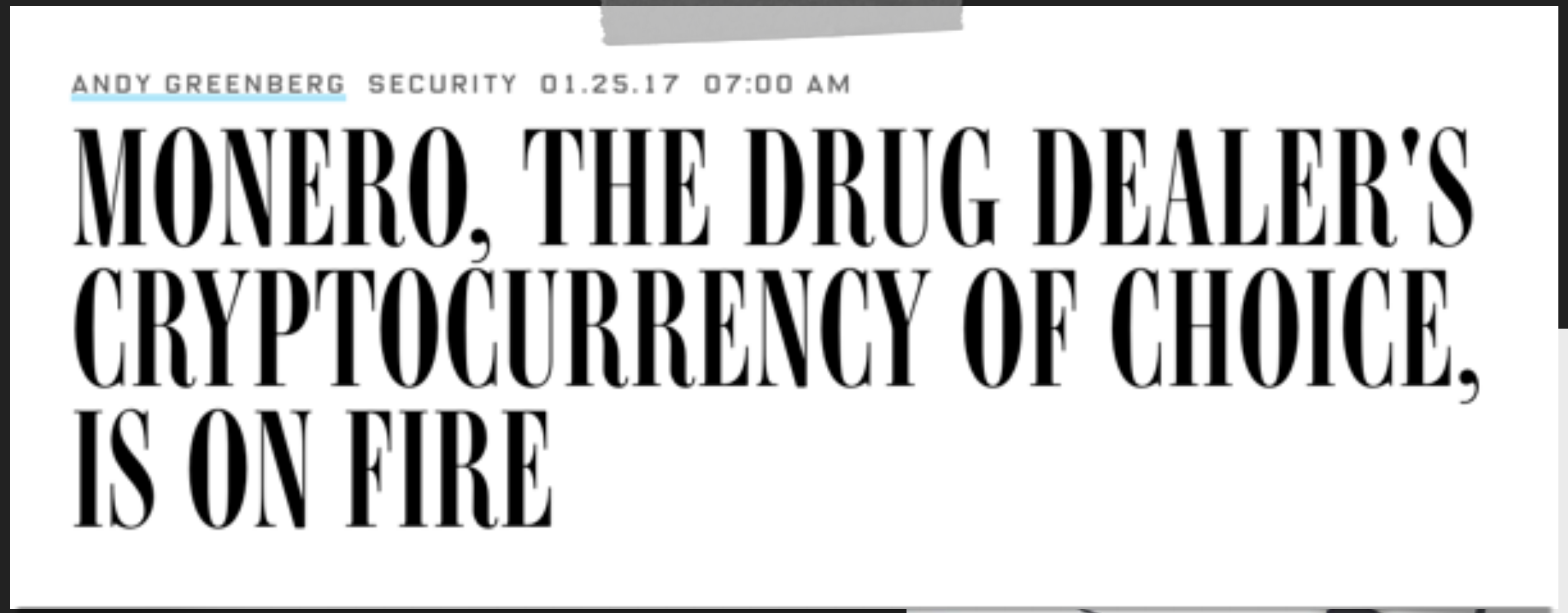
Malte Möser

Based on joint work with Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava,
Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin



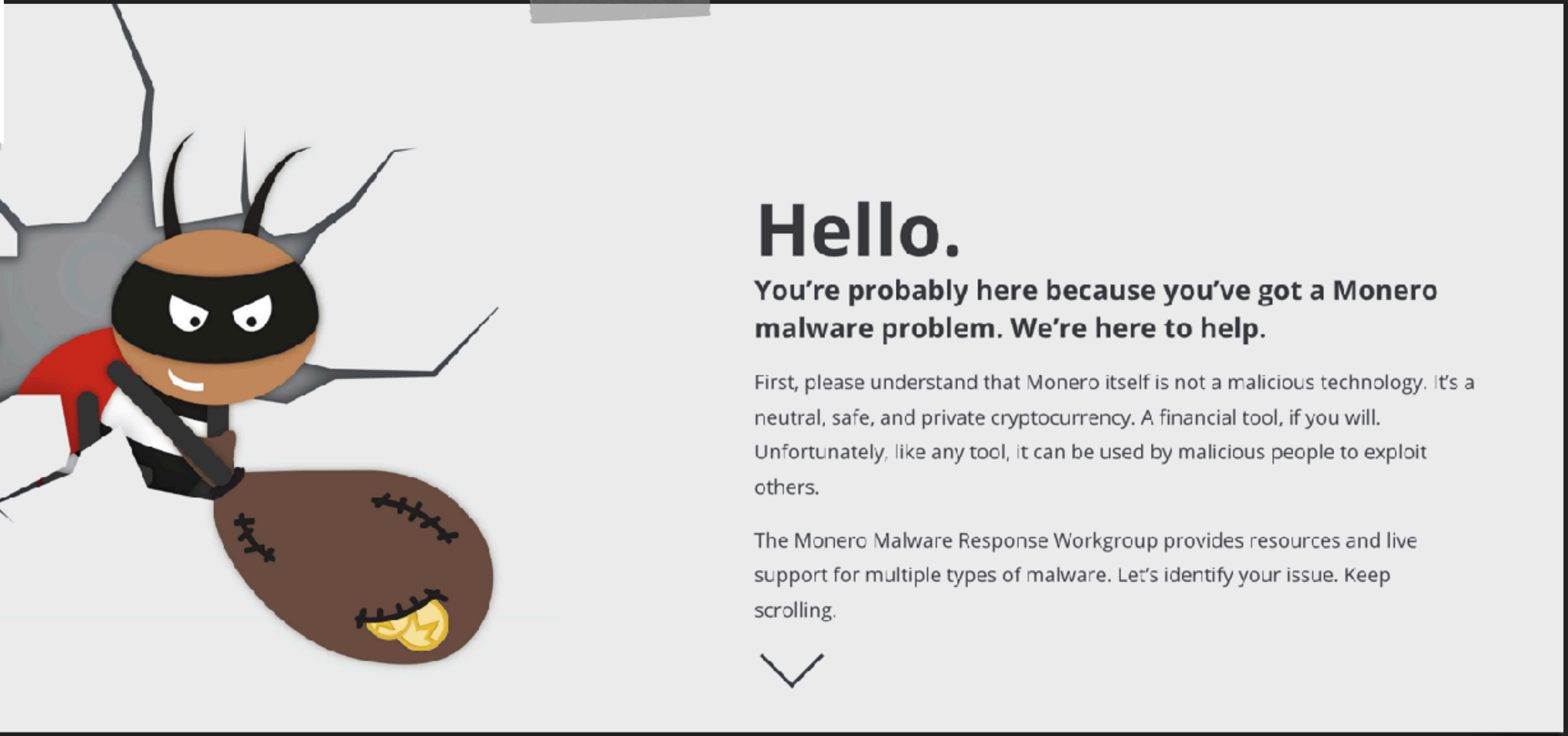
How Dirty Money Disappears Into the Black Hole of Cryptocurrency

Journal investigation documents suspicious trades through venture capital-backed ShapeShift



ANDY GREENBERG SECURITY 01.25.17 07:00 AM

MONERO, THE DRUG DEALER'S CRYPTOCURRENCY OF CHOICE, IS ON FIRE



Hello.

You're probably here because you've got a Monero malware problem. We're here to help.

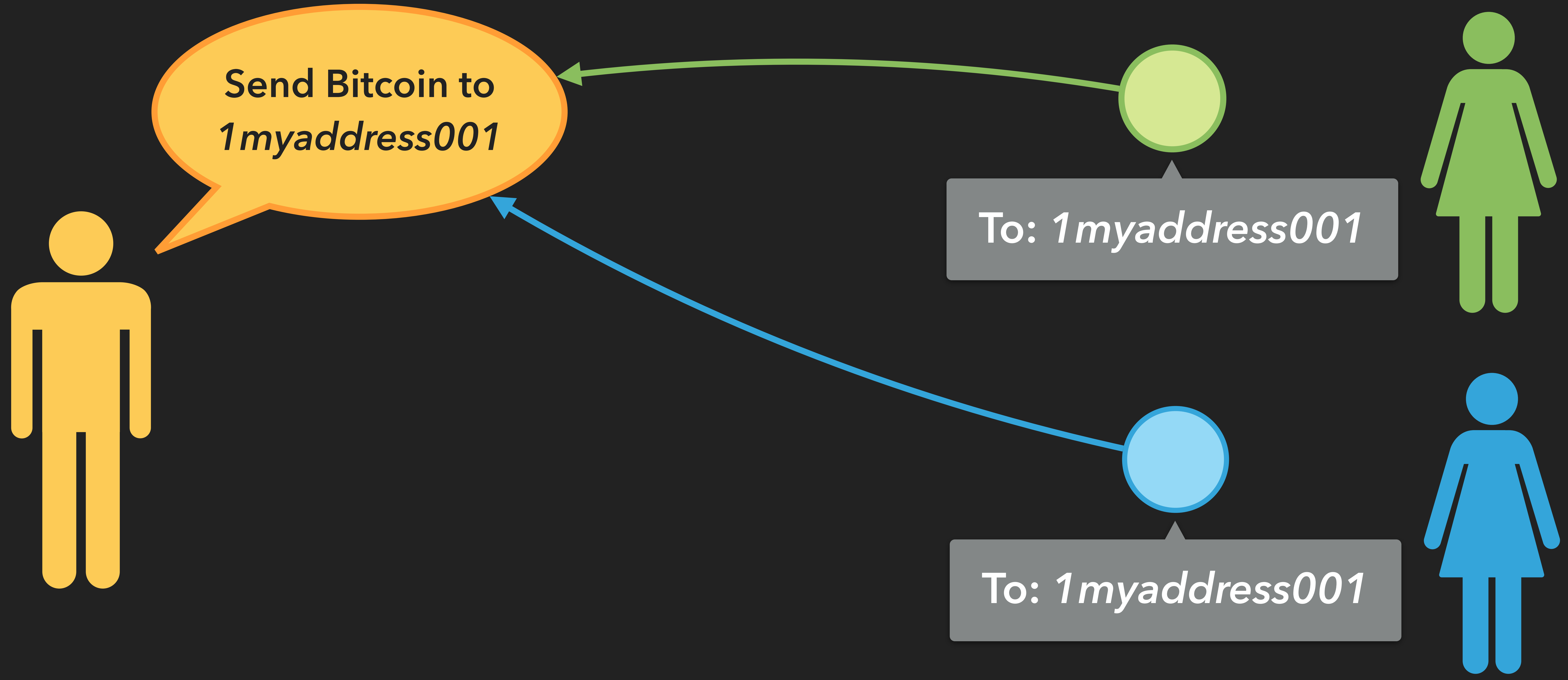
First, please understand that Monero itself is not a malicious technology. It's a neutral, safe, and private cryptocurrency. A financial tool, if you will. Unfortunately, like any tool, it can be used by malicious people to exploit others.

The Monero Malware Response Workgroup provides resources and live support for multiple types of malware. Let's identify your issue. Keep scrolling.

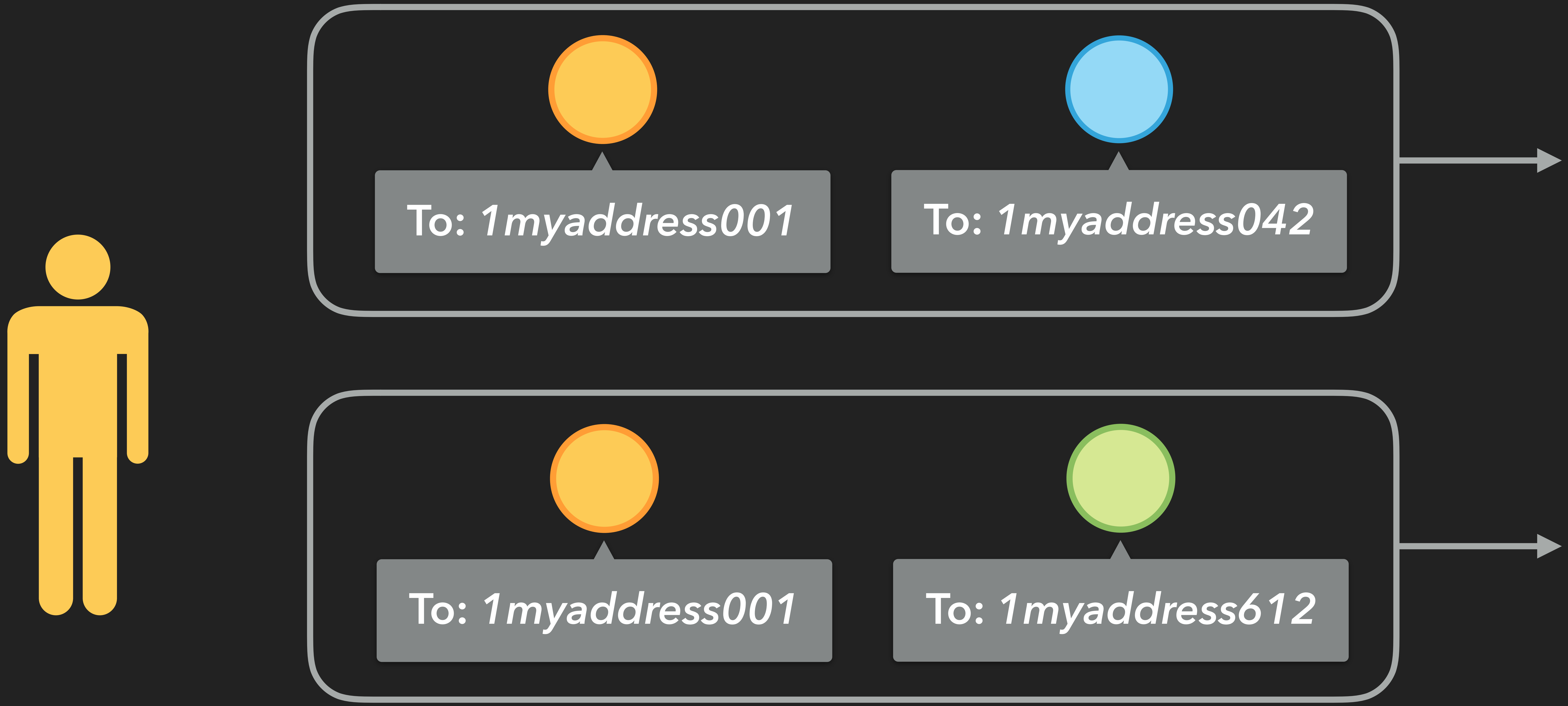
Takeaways

- Monero improves upon Bitcoin’s privacy
    - One-time addresses
    - Hidden values
    - Obfuscation of payment flows
- Incorrect use can severely hurt your anonymity
- Used for both illegitimate and legitimate purposes

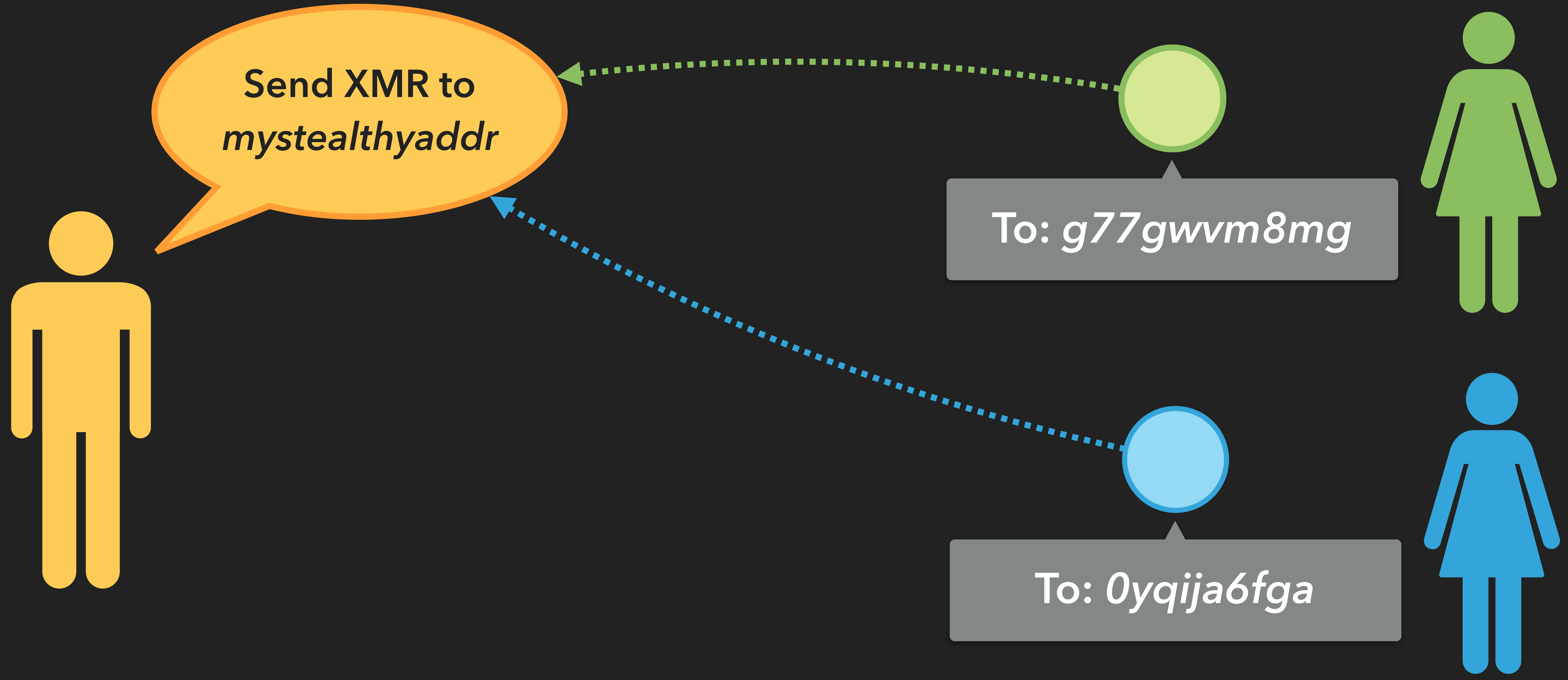
Issue 1: Public Reuse of Addresses



Issue 1: Public Reuse of Addresses



Monero Uses Stealth Addresses

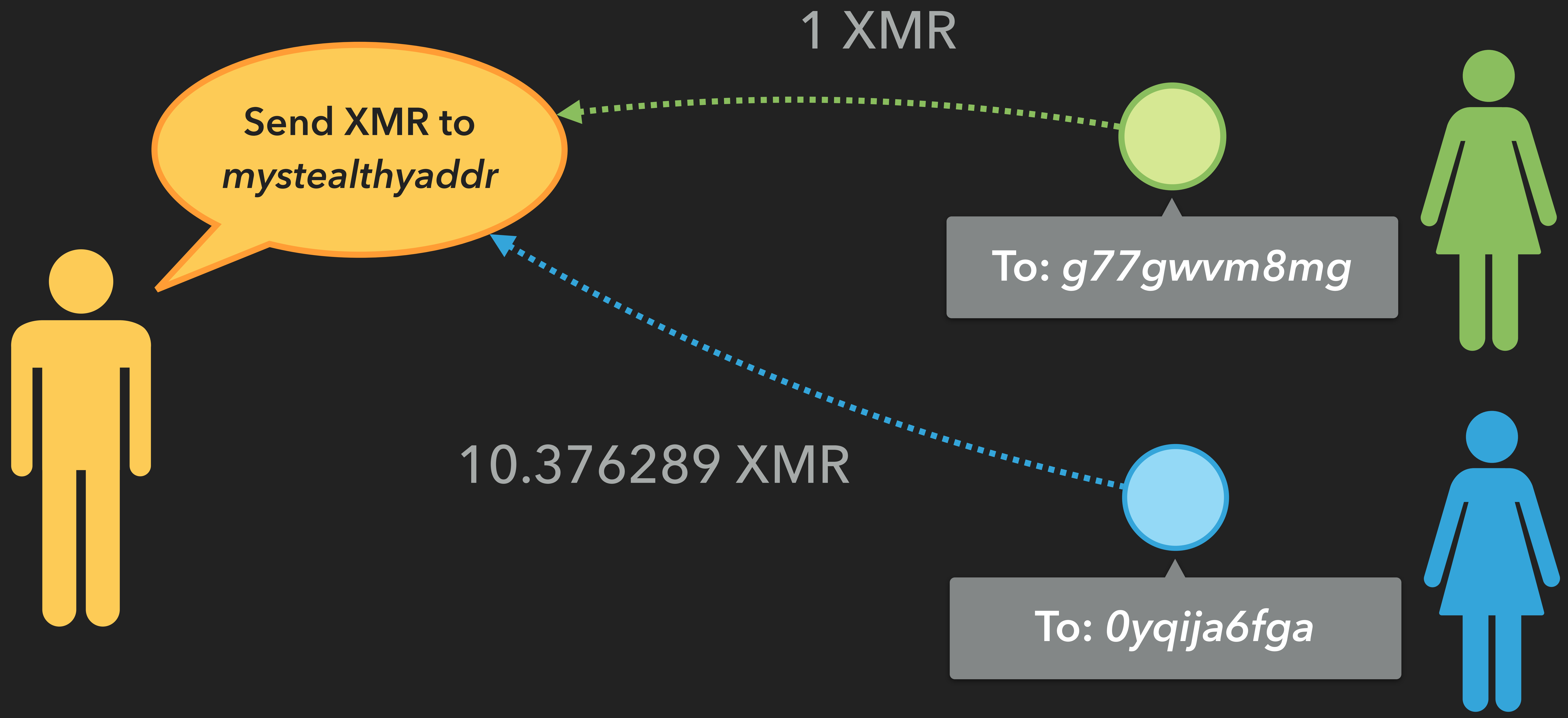


Send XMR to *mystealthyaddr*

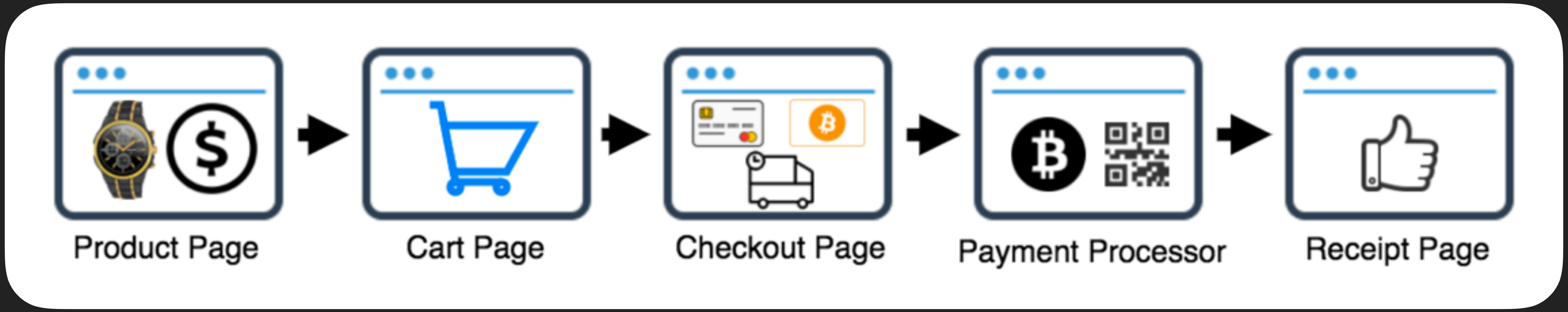
To: *g77gwvm8mg*

To: *0yqija6fga*

Issue 2: Values Are Visible



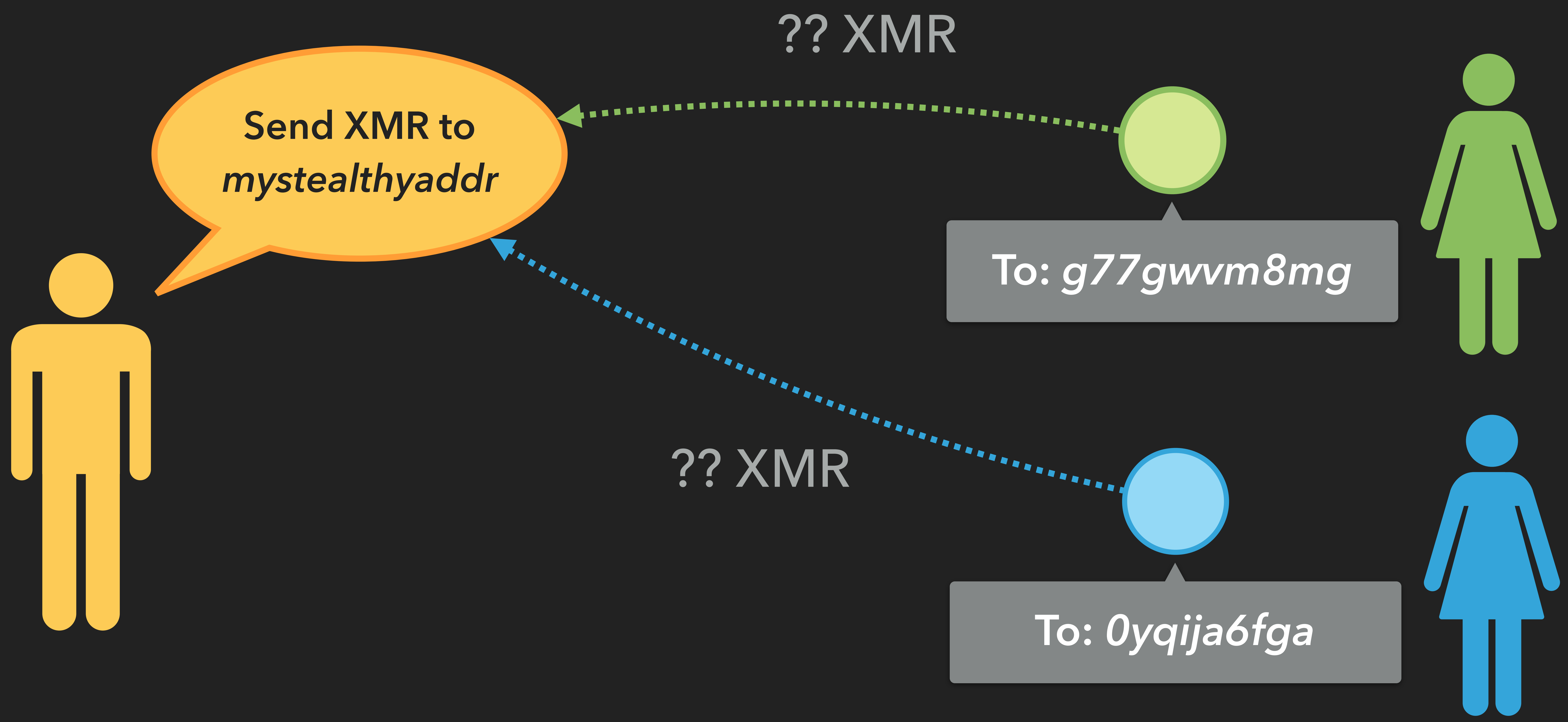
When the Cookie Meets the Blockchain



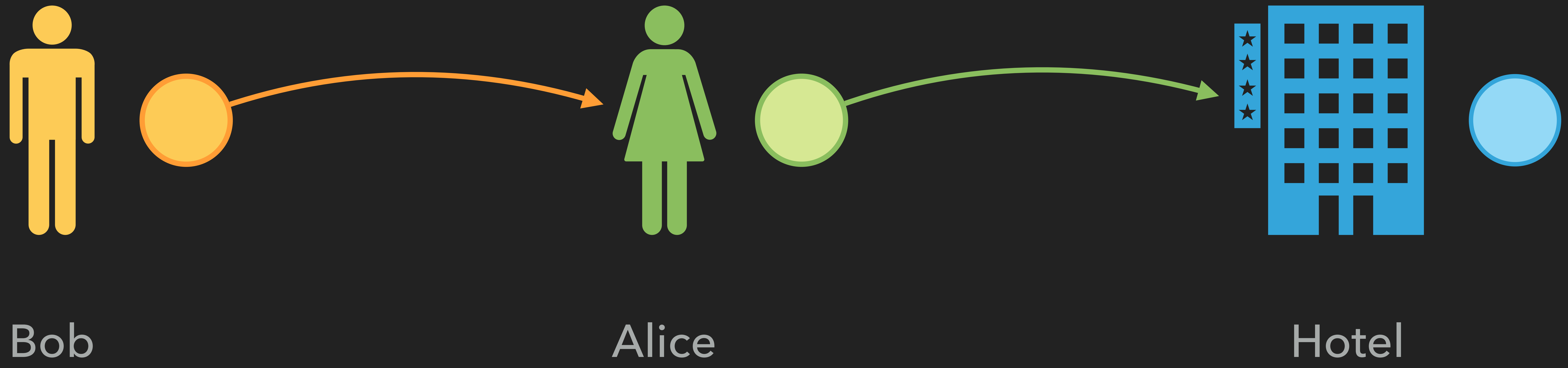
- Each step can leak information to third-party trackers
- Timing and values allow to identify corresponding transactions

Goldfeder et al. (2018). *When the cookie meets the blockchain: Privacy Risks of web payments via cryptocurrencies*

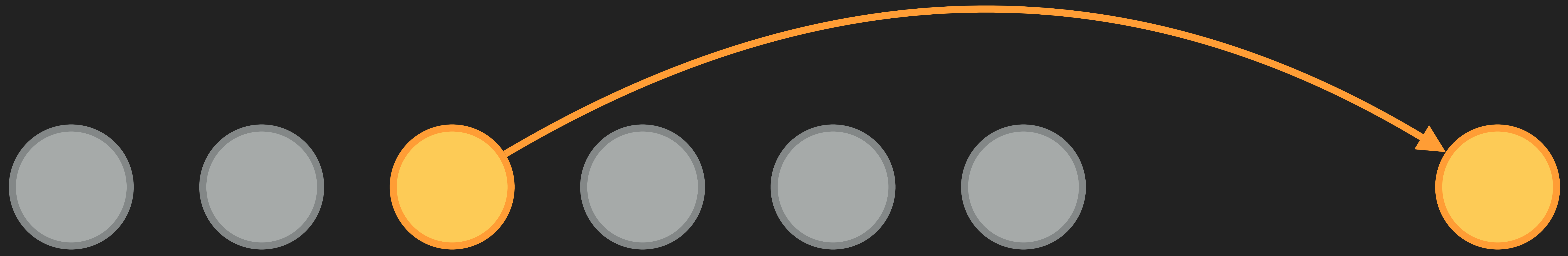
Amounts Are Encrypted (Since 2017)



Issue 3: Tracing Payments

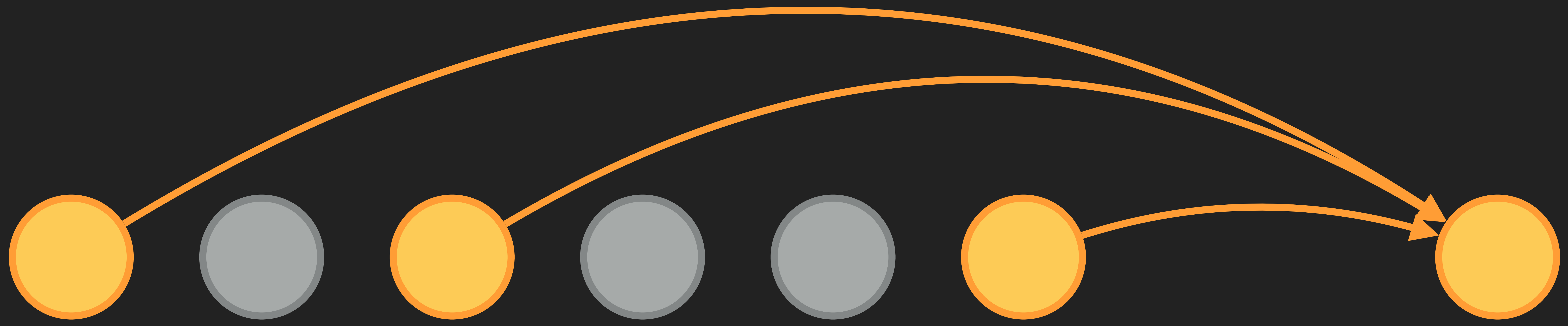


Output Selection in Bitcoin



each input spends a single output

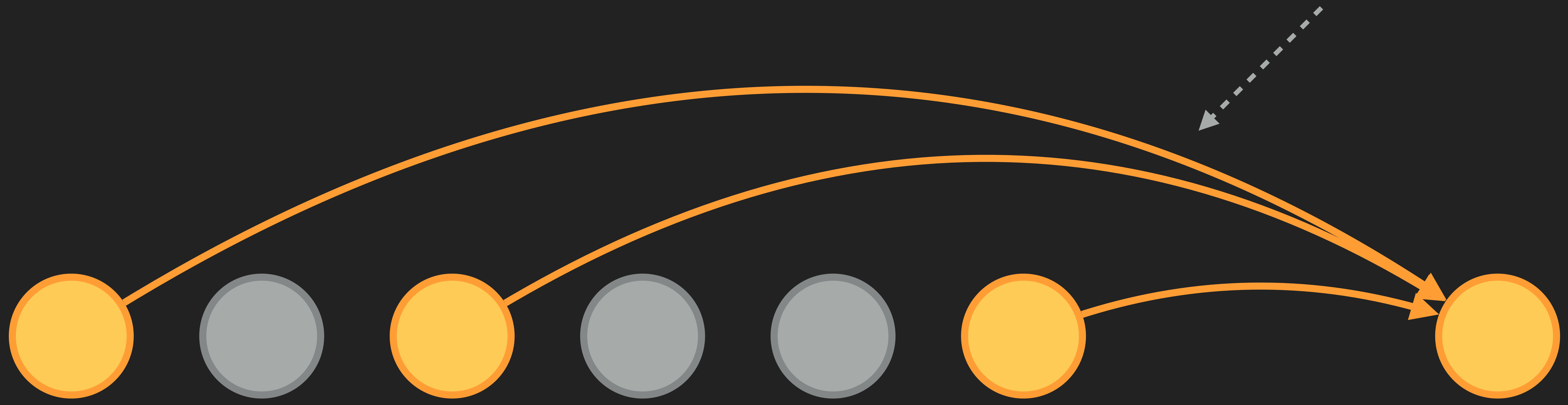
Output Selection in Monero



each input spends one of multiple outputs

ring signature + key image

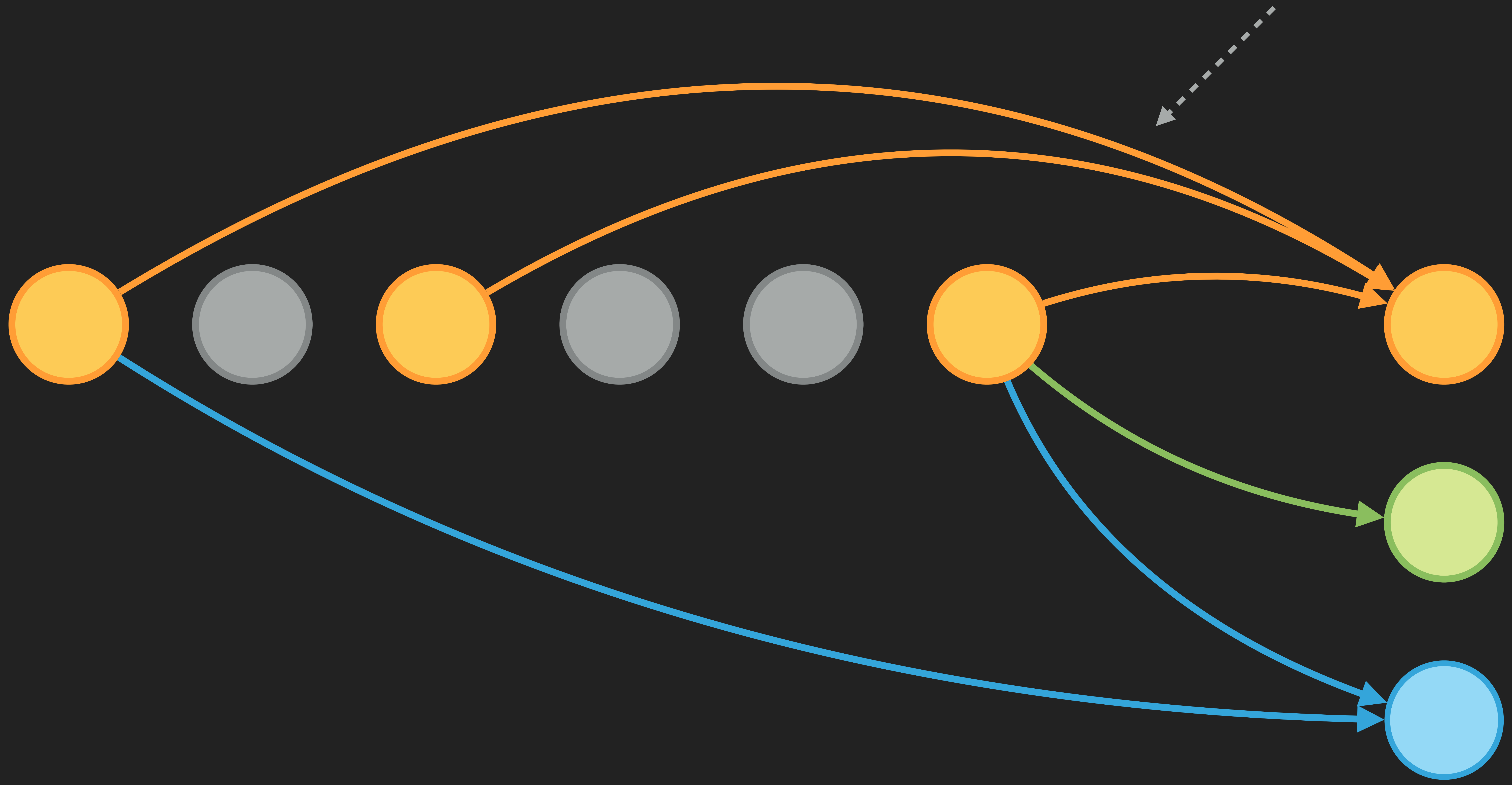
Deduction Technique



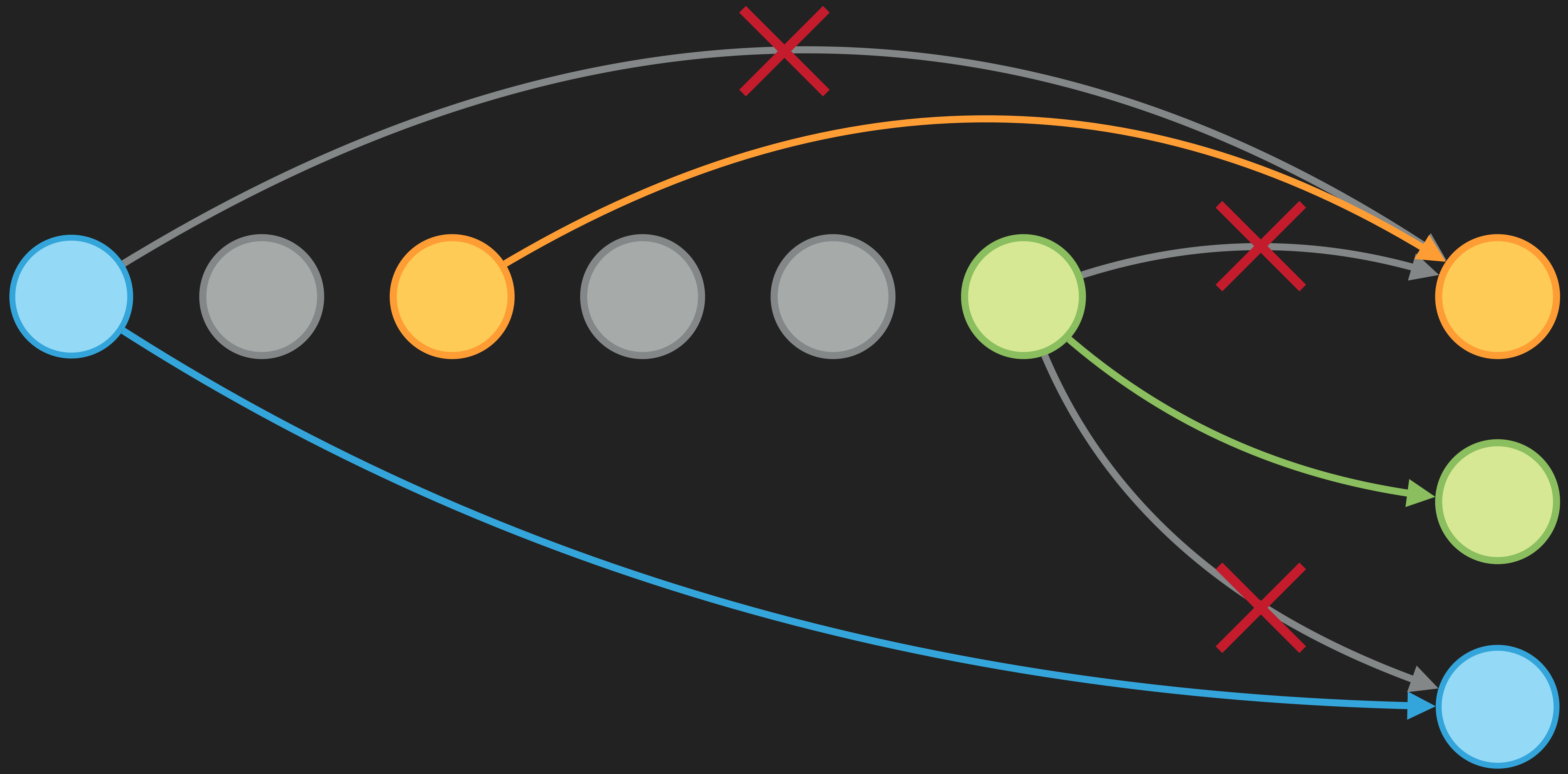
initially no mandatory number of mixins

Deduction Technique

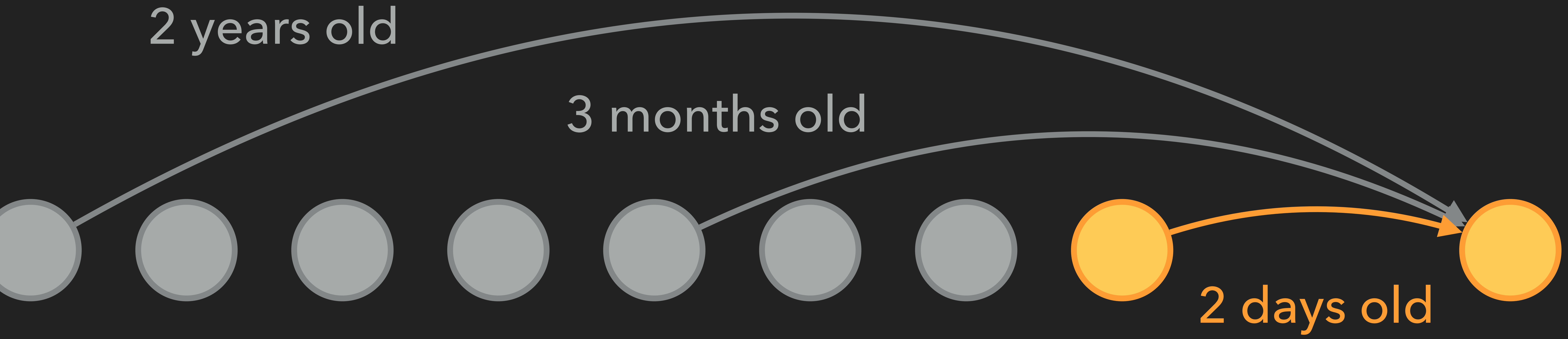
initially no mandatory
number of mixins



Deduction Technique

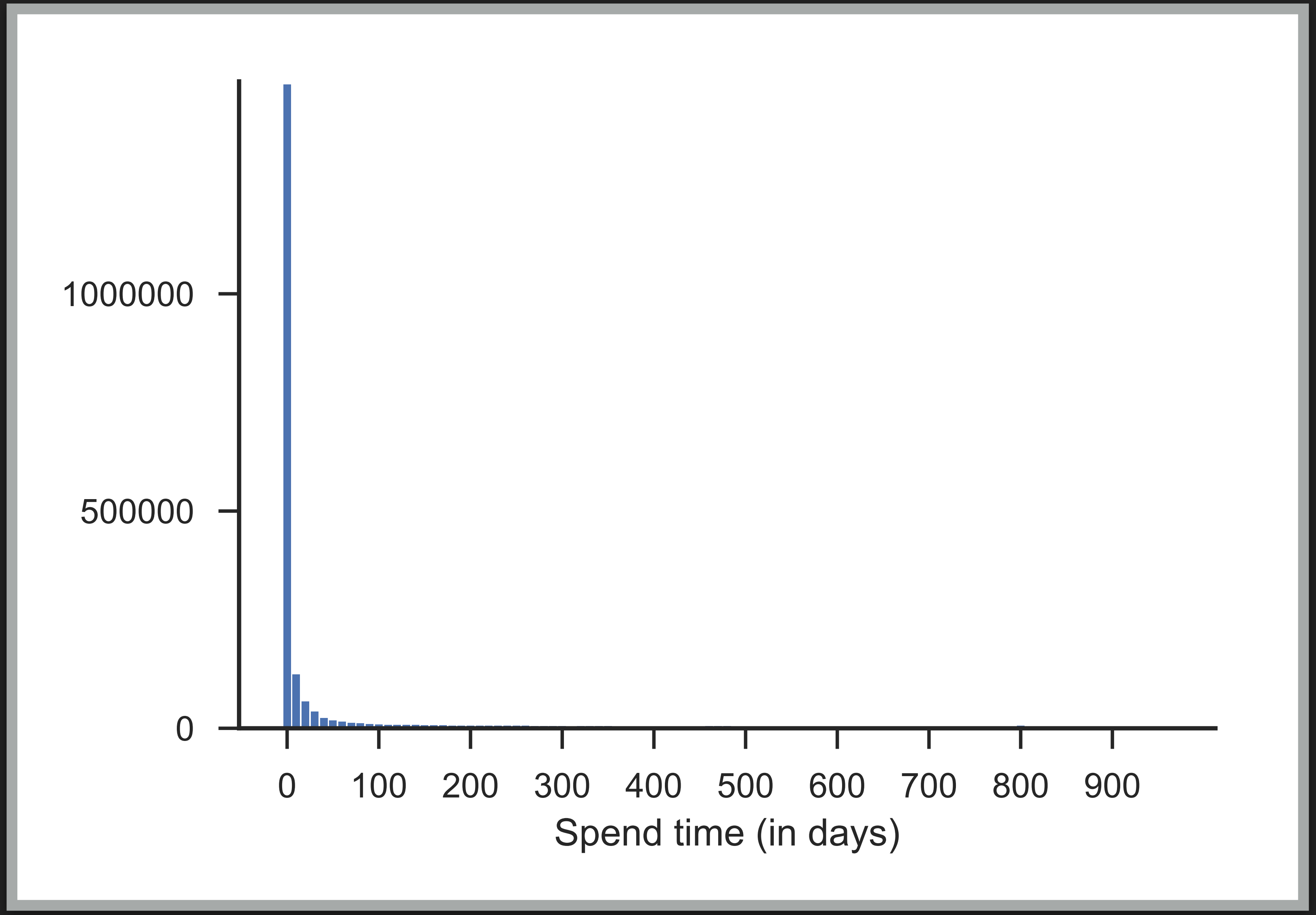


How Do You Choose Fake Coins?

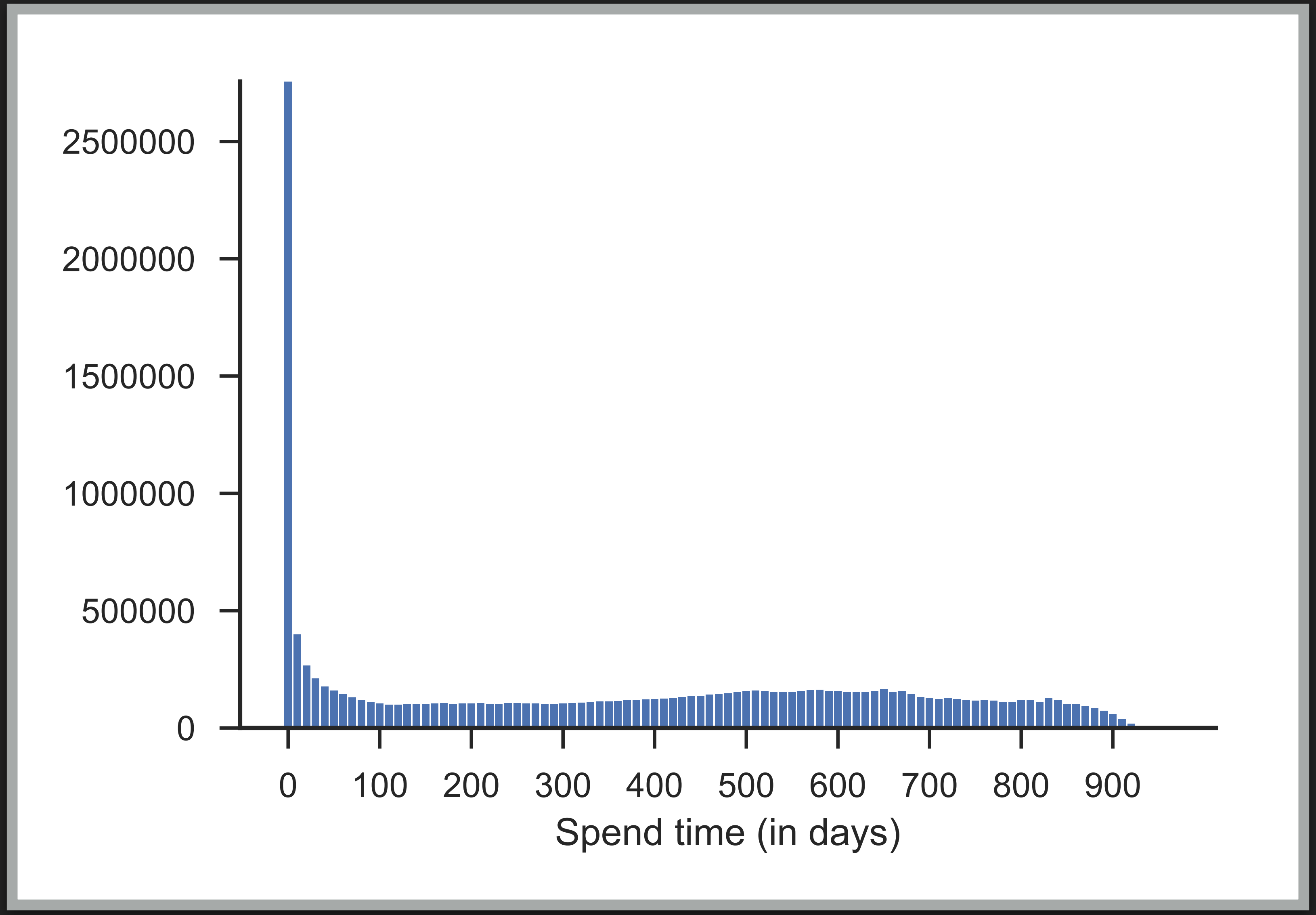


Most likely to be the real coin being spent

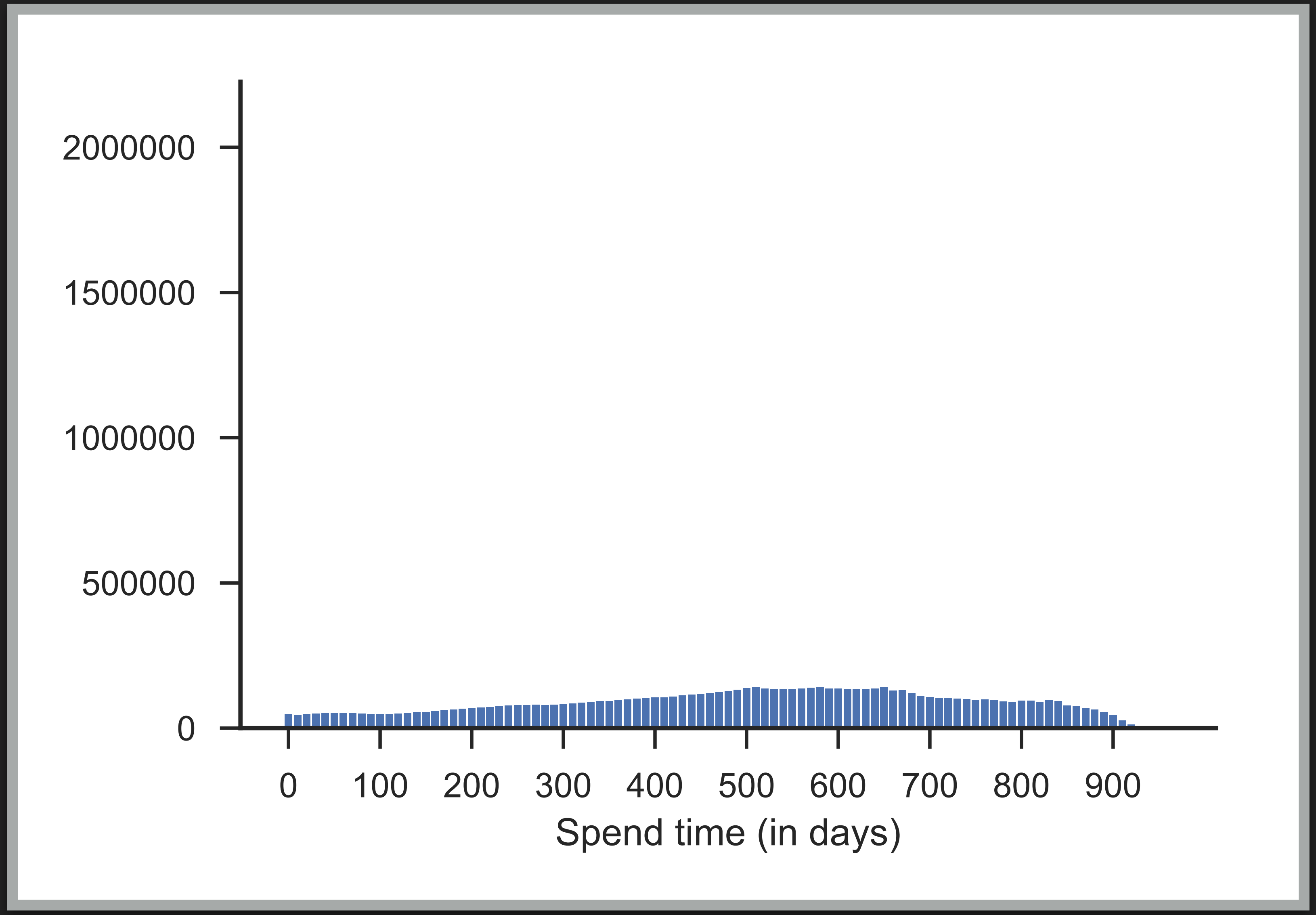
Distributions Do Not Match



Real

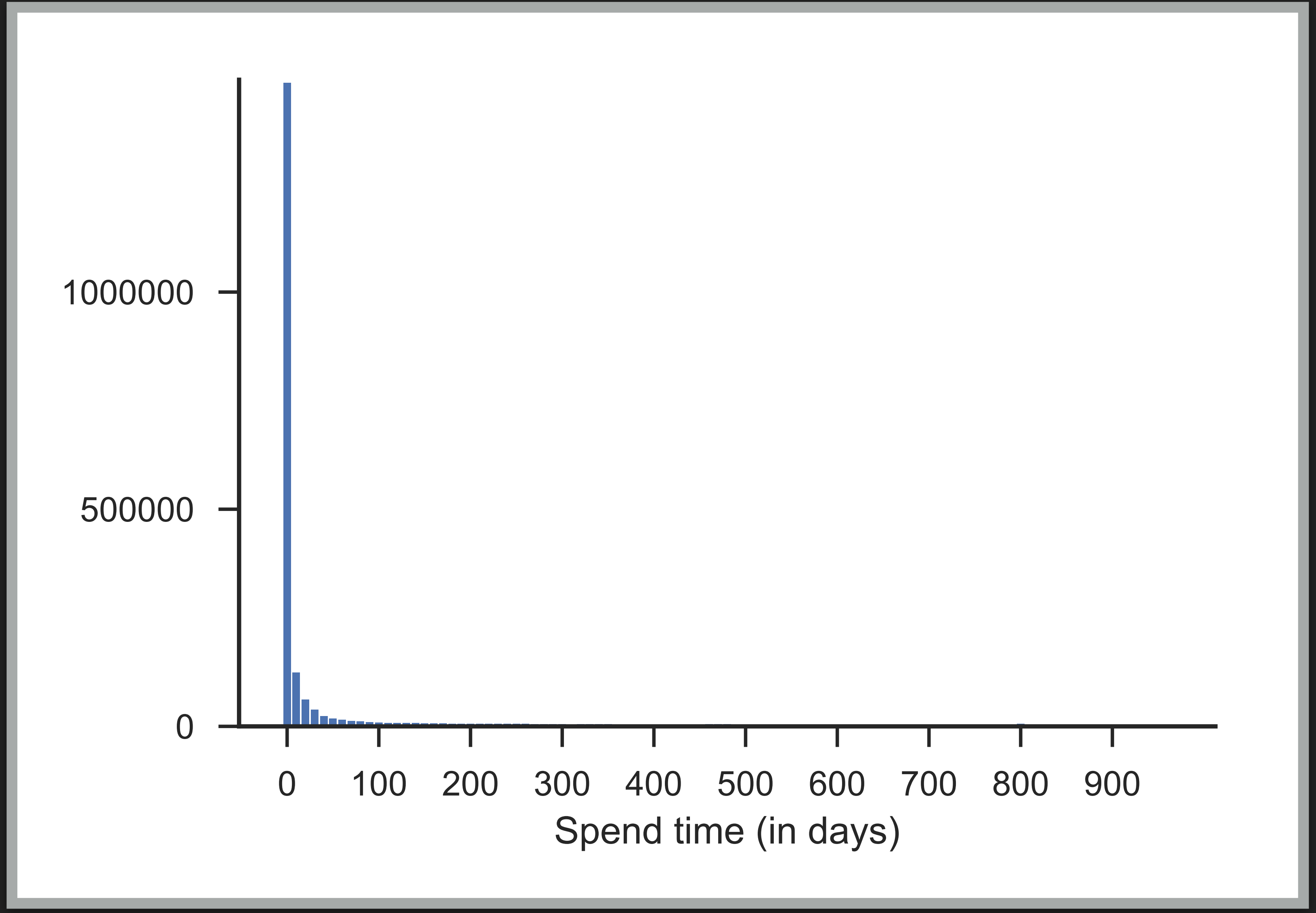


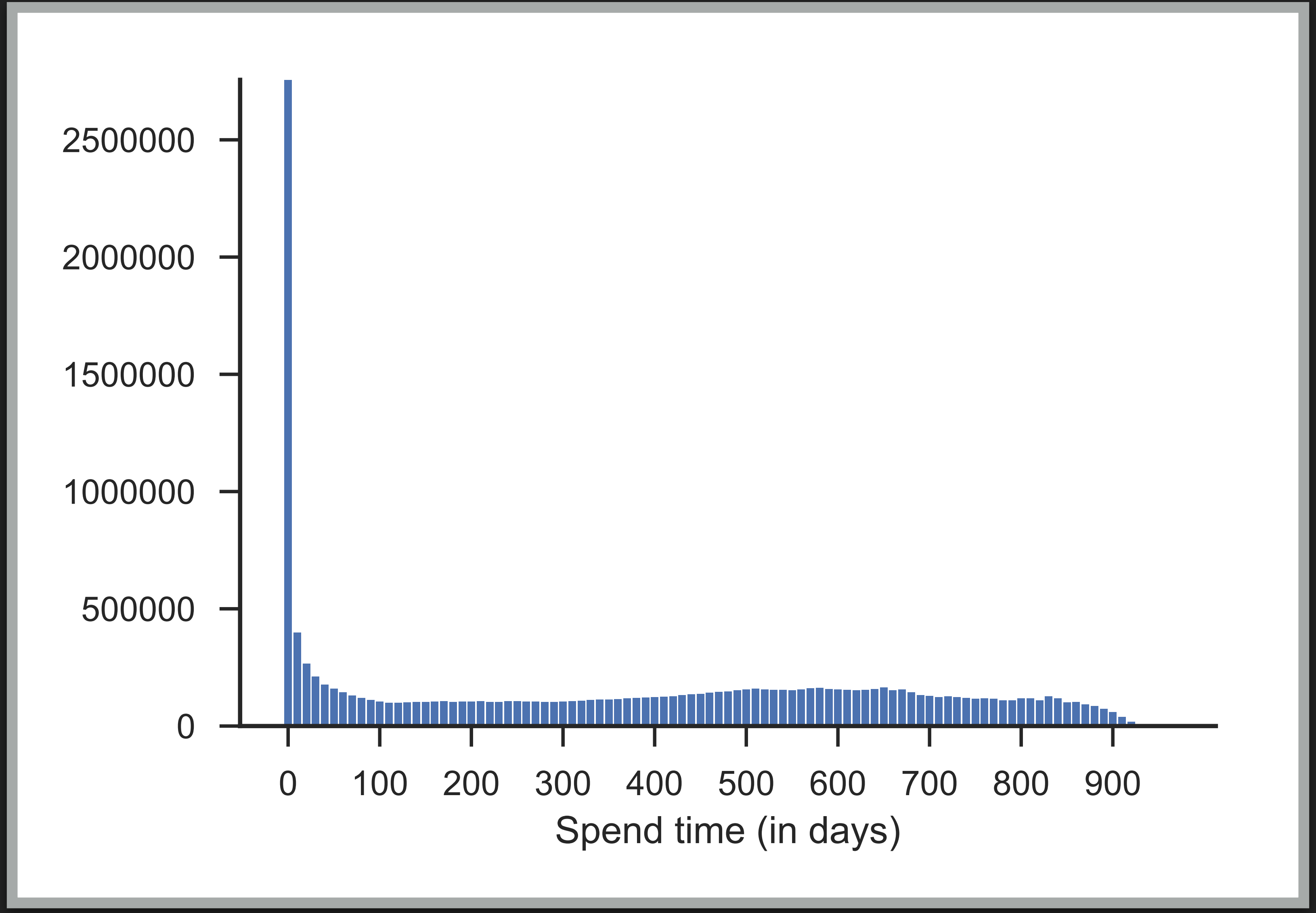
Real + Fake

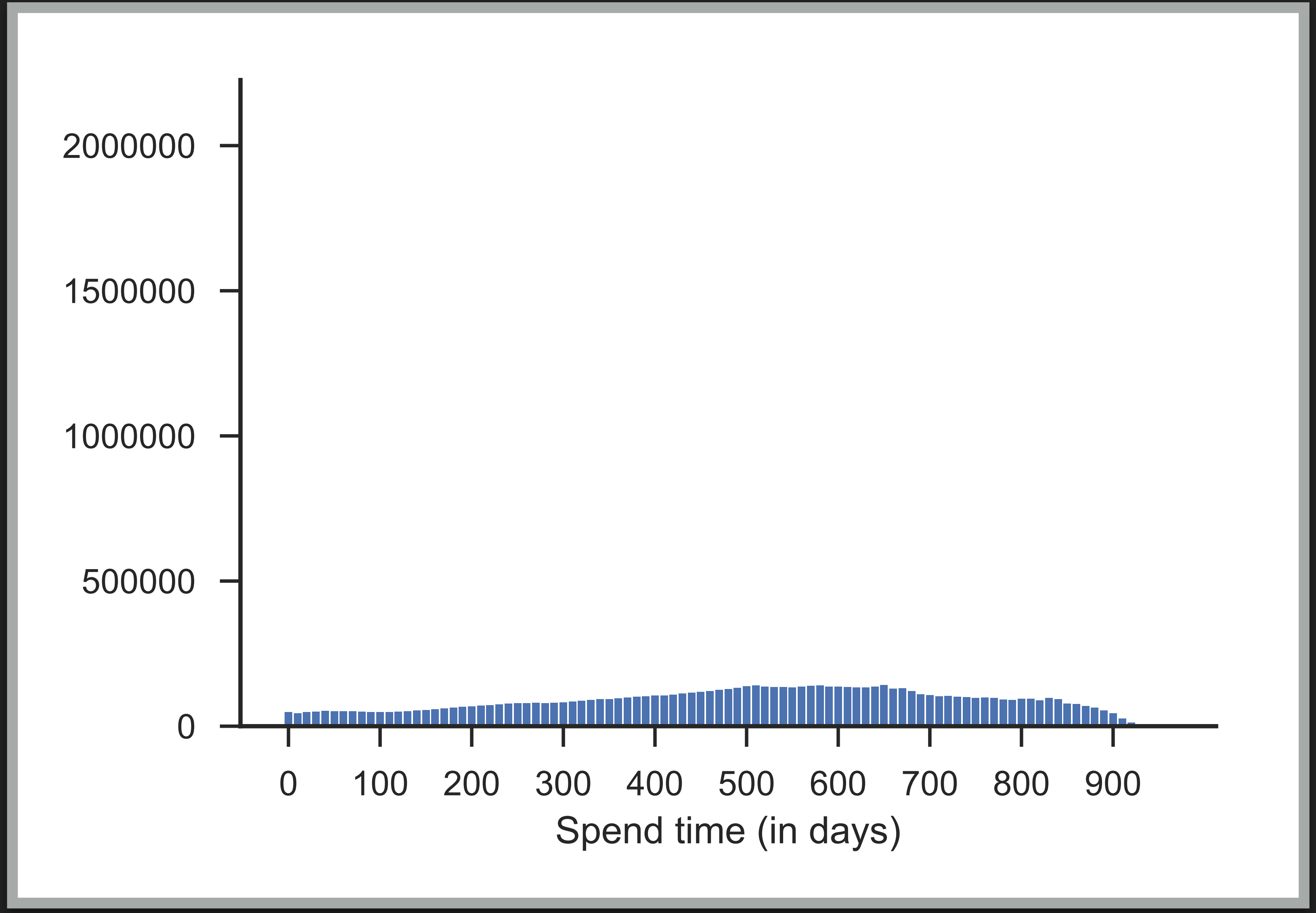


Ruled-out

The Newest Input Is Usually the Real One

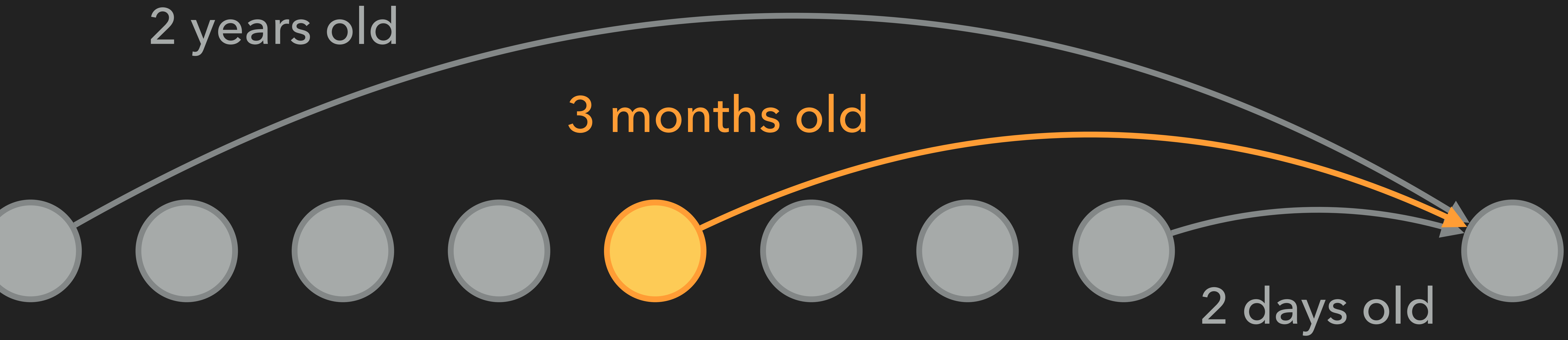






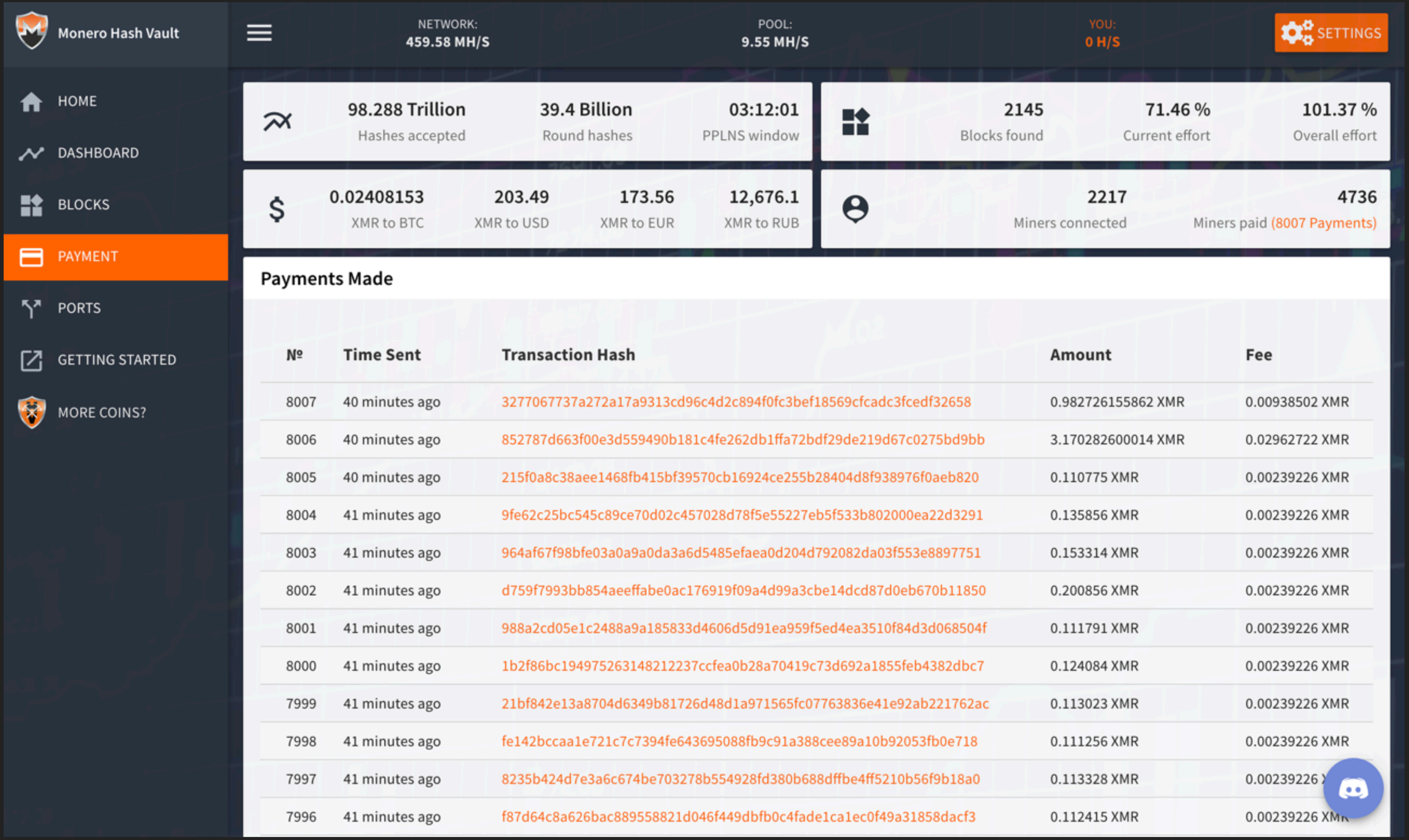
Successful for 80% of all inputs between April 2014 and April 2017

Timing Attacks



- Bob is one of five suspects to have bought drugs at AlphaBay today
- I know Bob bought some XMR exactly 3 months ago

Mining Pools Announce Payouts



NETWORK: 459.58 MH/S

POOL: 9.55 MH/S

YOU: 0 H/S

98.288 Trillion	39.4 Billion	03:12:01
Hashes accepted	Round hashes	PPLNS window

2145	71.46 %	101.37 %
Blocks found	Current effort	Overall effort

0.02408153	203.49	173.56	12,676.1
XMR to BTC	XMR to USD	XMR to EUR	XMR to RUB

2217	4736
Miners connected	Miners paid (8007 Payments)

Payments Made

№	Time Sent	Transaction Hash	Amount	Fee
8007	40 minutes ago	3277067737a272a17a9313cd96c4d2c894f0fc3bef18569cfcadc3fcedf32658	0.982726155862 XMR	0.00938502 XMR
8006	40 minutes ago	852787d663f00e3d559490b181c4fe262db1ffa72bdf29de219d67c0275bd9bb	3.170282600014 XMR	0.02962722 XMR
8005	40 minutes ago	215f0a8c38aee1468fb415bf39570cb16924ce255b28404d8f938976f0aeb820	0.110775 XMR	0.00239226 XMR
8004	41 minutes ago	9fe62c25bc545c89ce70d02c457028d78f5e55227eb5f533b802000ea22d3291	0.135856 XMR	0.00239226 XMR
8003	41 minutes ago	964af67f98bfe03a0a9a0da3a6d5485efaea0d204d792082da03f553e8897751	0.153314 XMR	0.00239226 XMR
8002	41 minutes ago	d759f7993bb854aeeffabe0ac176919f09a4d99a3cbe14dcd87d0eb670b11850	0.200856 XMR	0.00239226 XMR
8001	41 minutes ago	988a2cd05e1c2488a9a185833d4606d5d91ea959f5ed4ea3510f84d3d068504f	0.111791 XMR	0.00239226 XMR
8000	41 minutes ago	1b2f86bc194975263148212237ccfea0b28a70419c73d692a1855feb4382dbc7	0.124084 XMR	0.00239226 XMR
7999	41 minutes ago	21bf842e13a8704d6349b81726d48d1a971565fc07763836e41e92ab221762ac	0.113023 XMR	0.00239226 XMR
7998	41 minutes ago	fe142bccaa1e721c7c7394fe643695088fb9c91a388cee89a10b92053fb0e718	0.111256 XMR	0.00239226 XMR
7997	41 minutes ago	8235b424d7e3a6c674be703278b554928fd380b688dffbe4ff5210b56f9b18a0	0.113328 XMR	0.00239226 X
7996	41 minutes ago	f87d64c8a626bac889558821d046f449dbfb0c4fade1ca1ec0f49a31858dacf3	0.112415 XMR	0.00239226 XMR

Chain Forks Are a Privacy Hazard

Monero
MoneroV

Chain Forks Are a Privacy Hazard

linked by key image

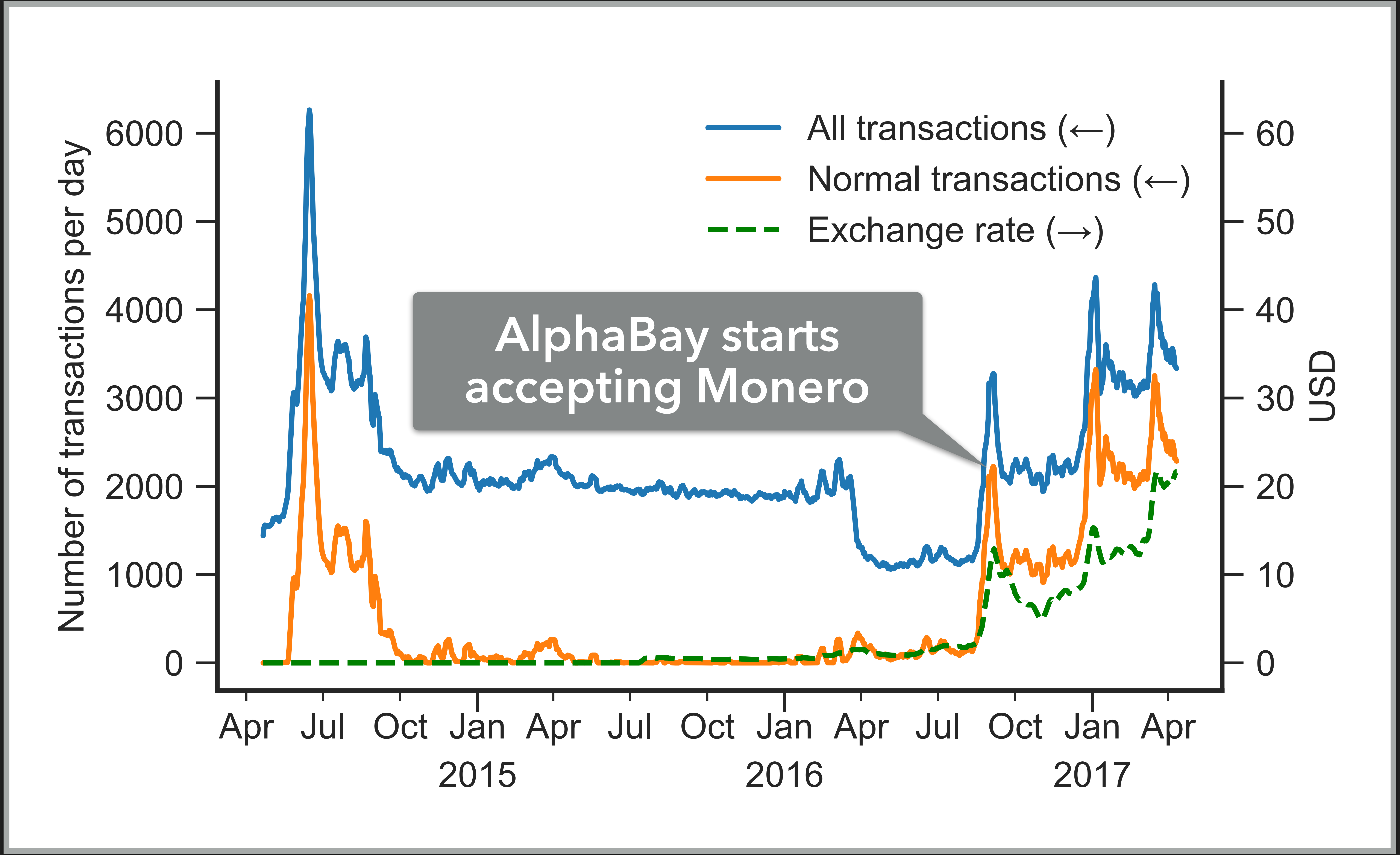
Chain Forks Are a Privacy Hazard

linked by key image

Intersection reveals true spend

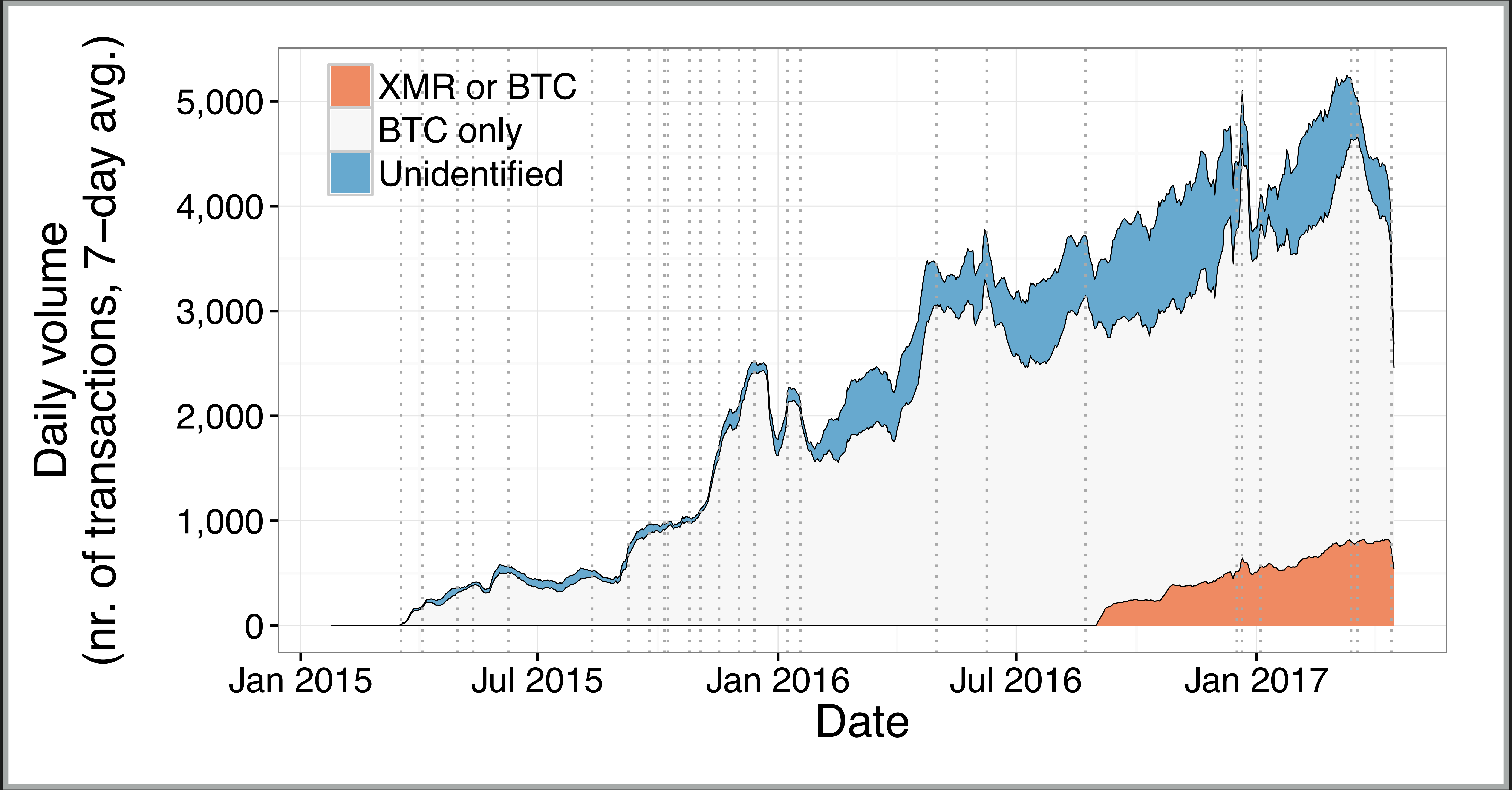
AlphaBay

- Volume spiked when AlphaBay started accepting Monero



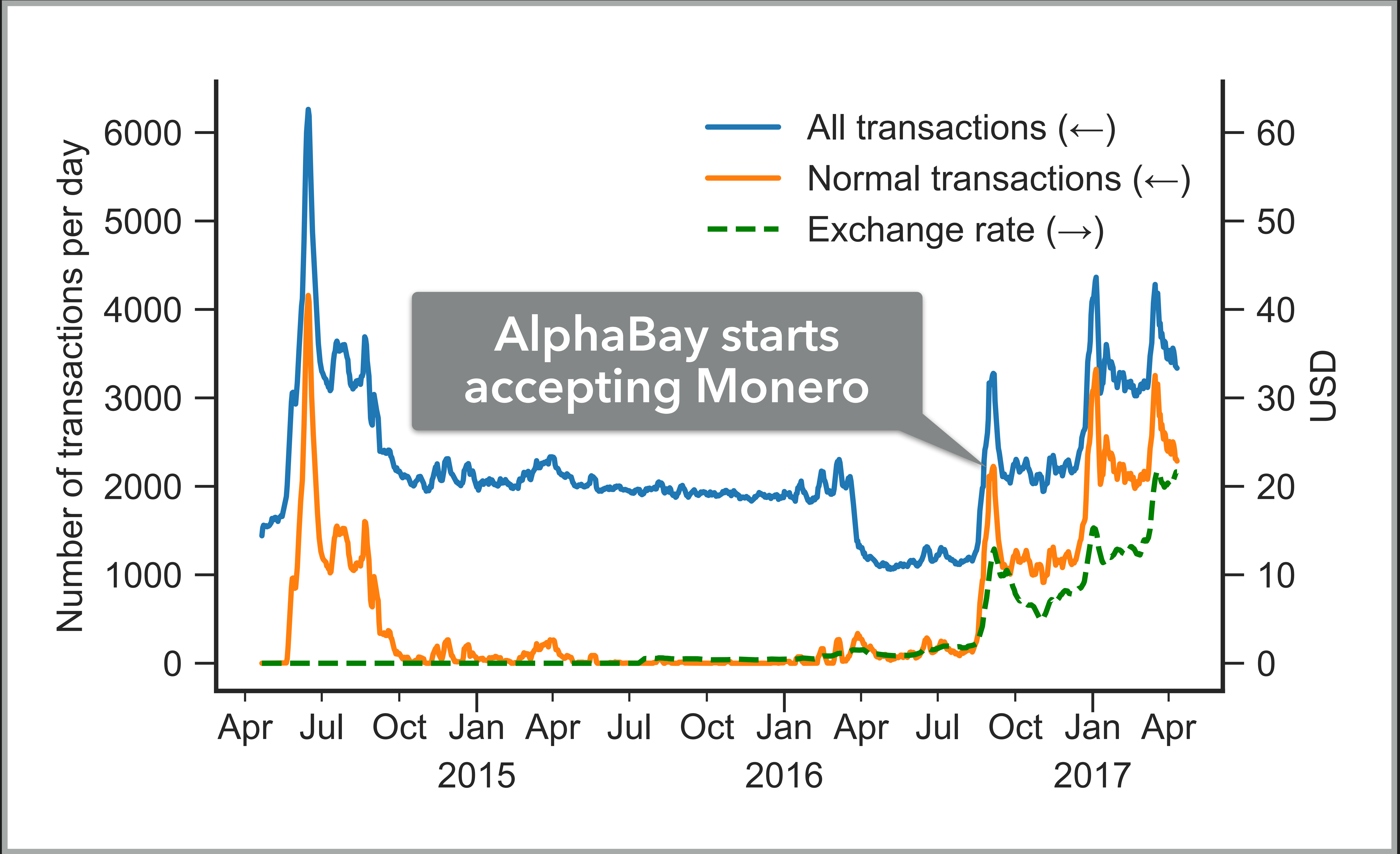
AlphaBay starts accepting Monero

AlphaBay - Daily Volume (Number of Transactions)



AlphaBay

- Volume spiked when AlphaBay started accepting Monero
- At most 25% of txs can be deposits at AlphaBay



AlphaBay starts accepting Monero

Summary

- Monero improves upon the limited privacy of Bitcoin
  - Correct use of technology is paramount
  - It’s hard to patch a broken system
- Illicit business tends to be early adopters of new technologies
  - Many legitimate uses that are less visible