

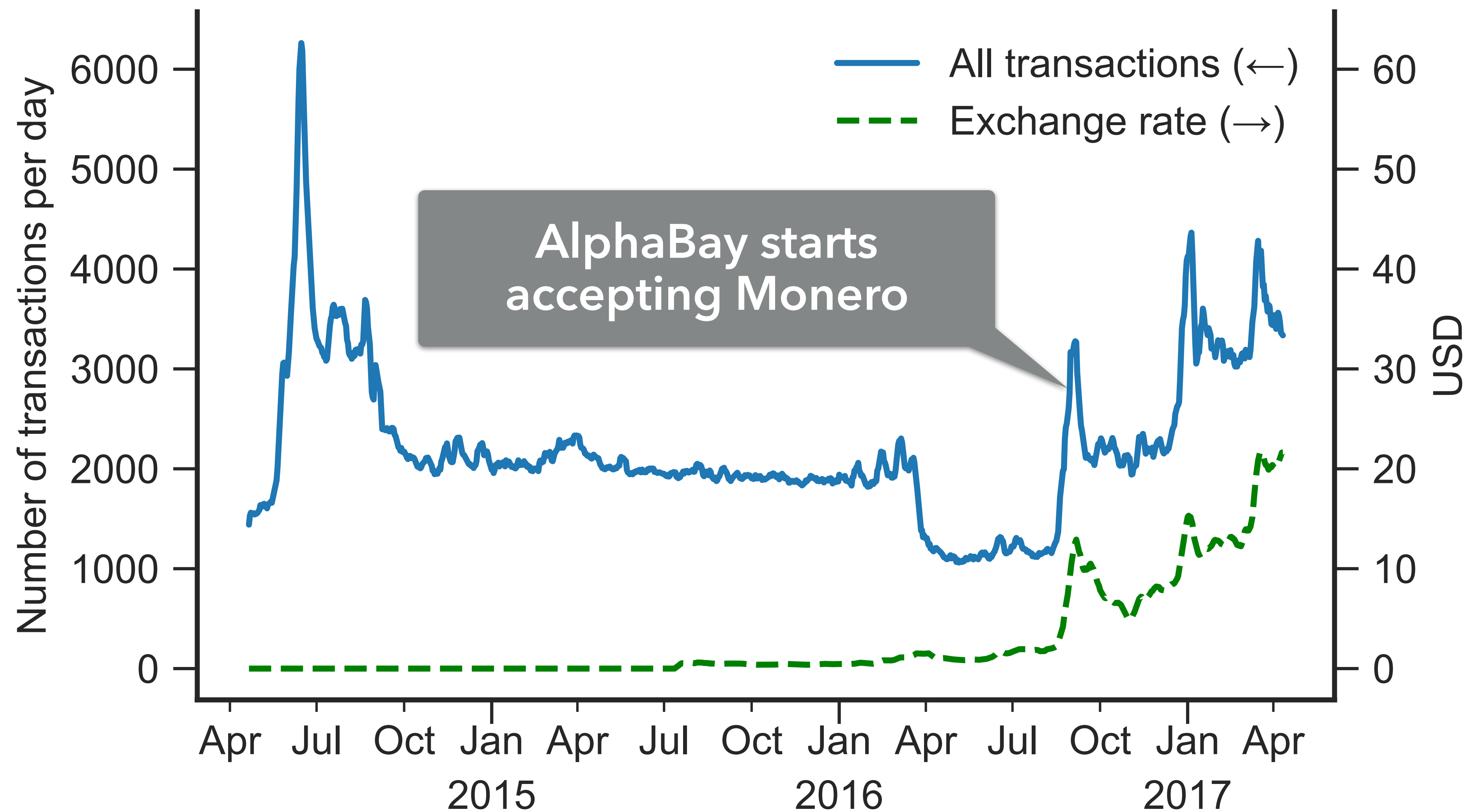
An Empirical Analysis of Traceability in the Monero Blockchain

Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava,
Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, Nicolas Christin

PETS 2018: The 18th Privacy Enhancing Technologies Symposium

Monero

- ▶ Privacy-centric cryptocurrency (currently top #12)



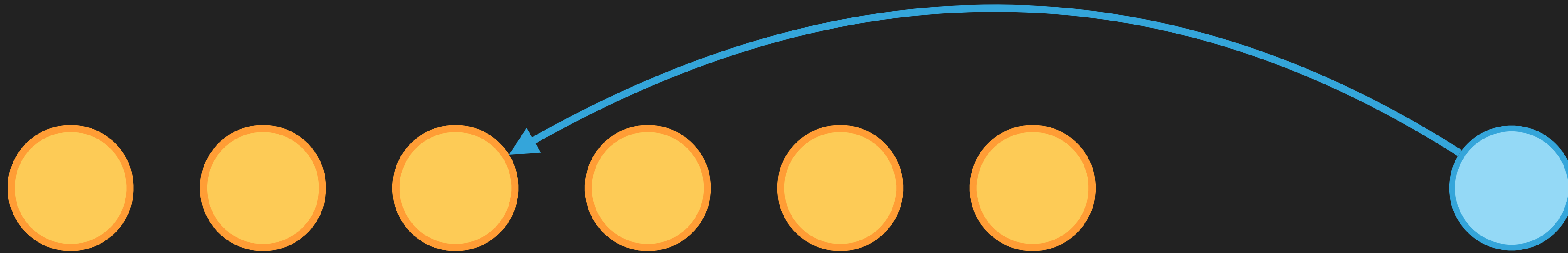
Monero

- ▶ Privacy-centric cryptocurrency (currently top #14)

This Talk

- ▶ Weaknesses in mixin sampling strategy
- ▶ Studying the ecosystem: does it matter?
- ▶ Lessons and conclusion

Output Selection in Bitcoin



each input refers to a single output

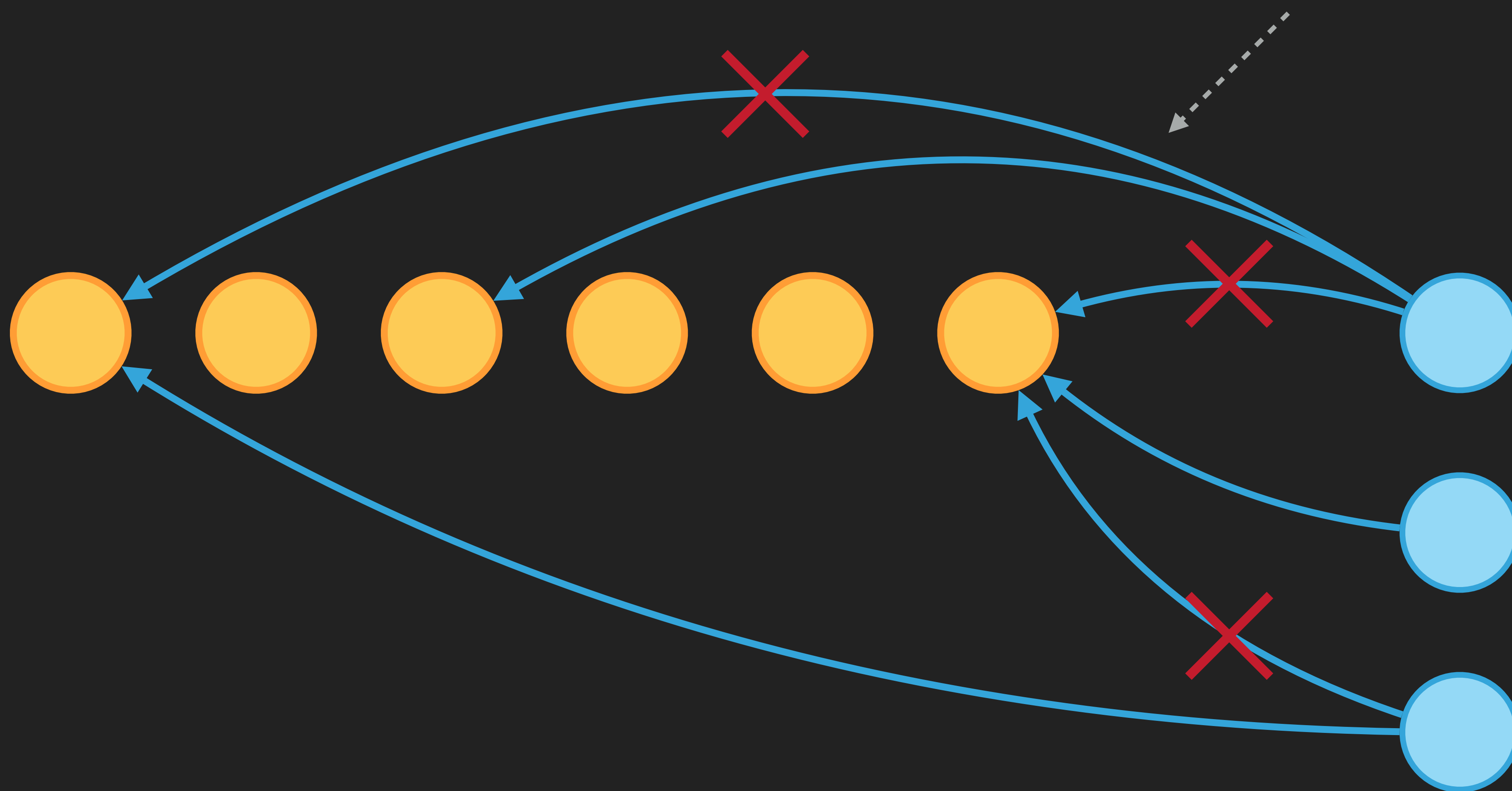
Output Selection in Monero



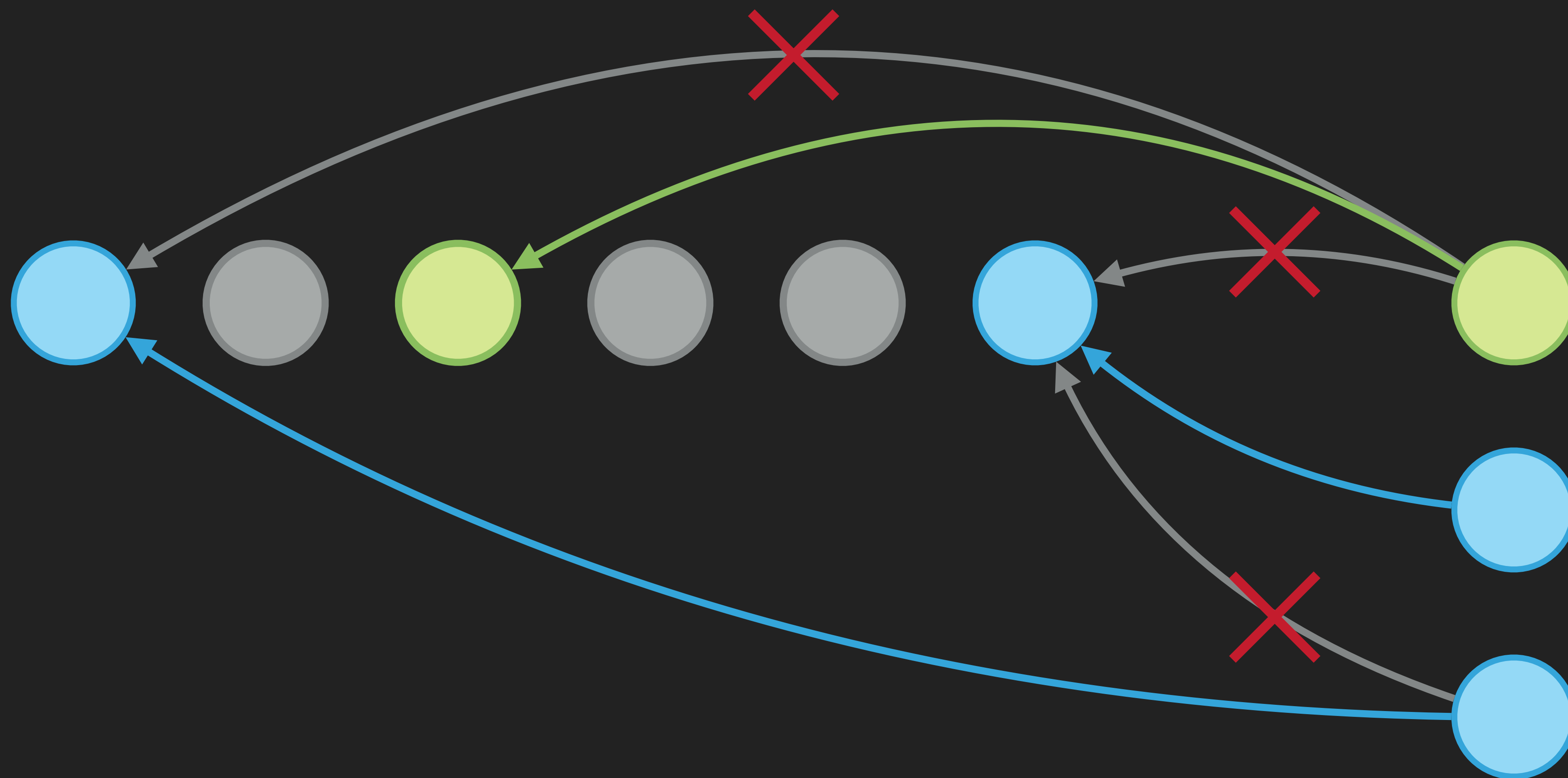
each input refers to multiple outputs
(with the same denomination)

Deduction Technique

initially no mandatory
number of mixins

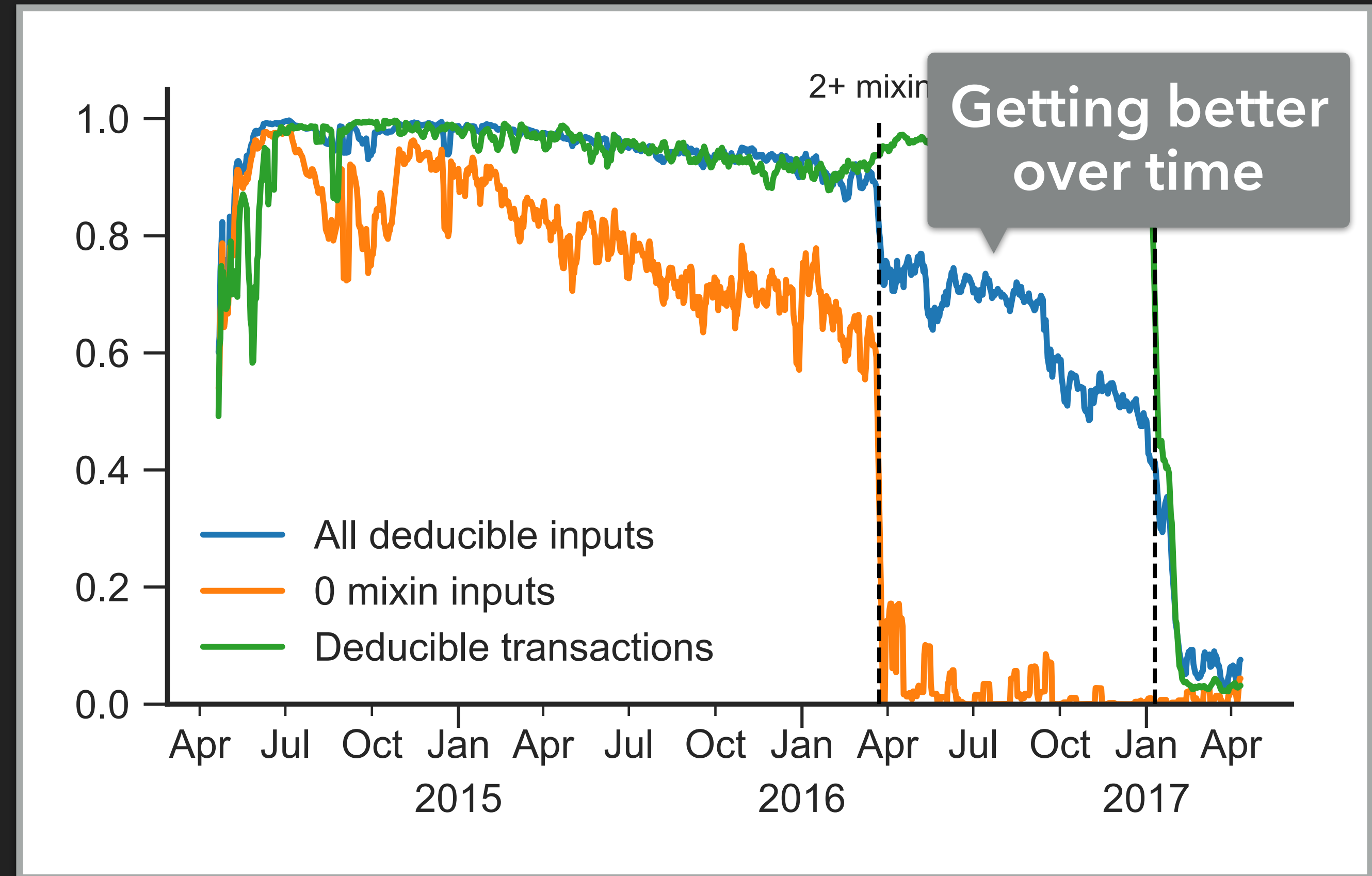


Deduction Technique

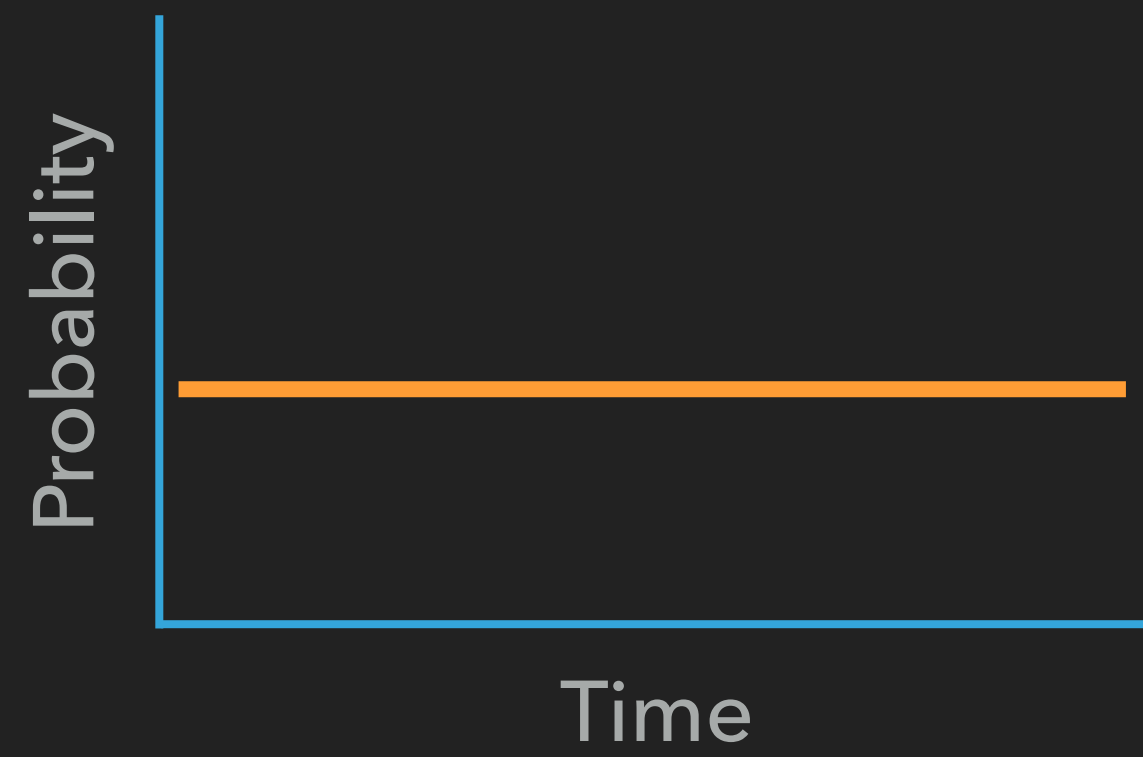


Results of Deducibility Attack

- ▶ 64% of inputs have no mixins
- ▶ 63% of inputs with mixins are deducible

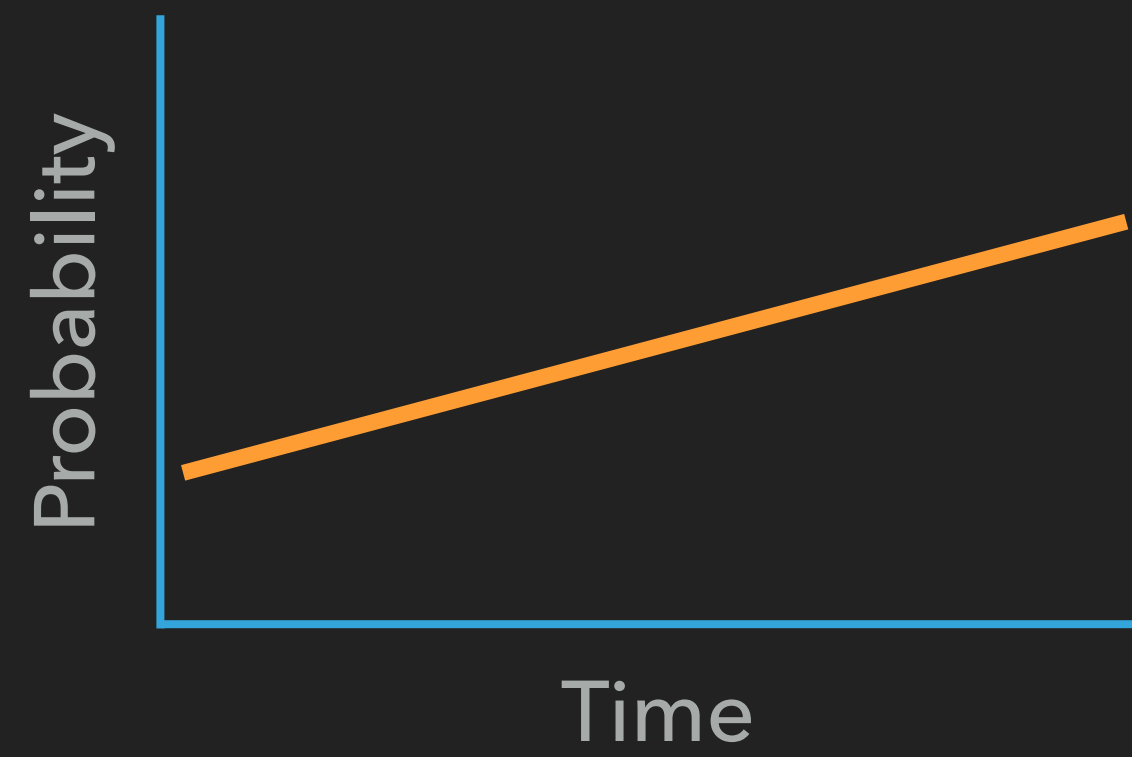


Mixin Selection Distributions



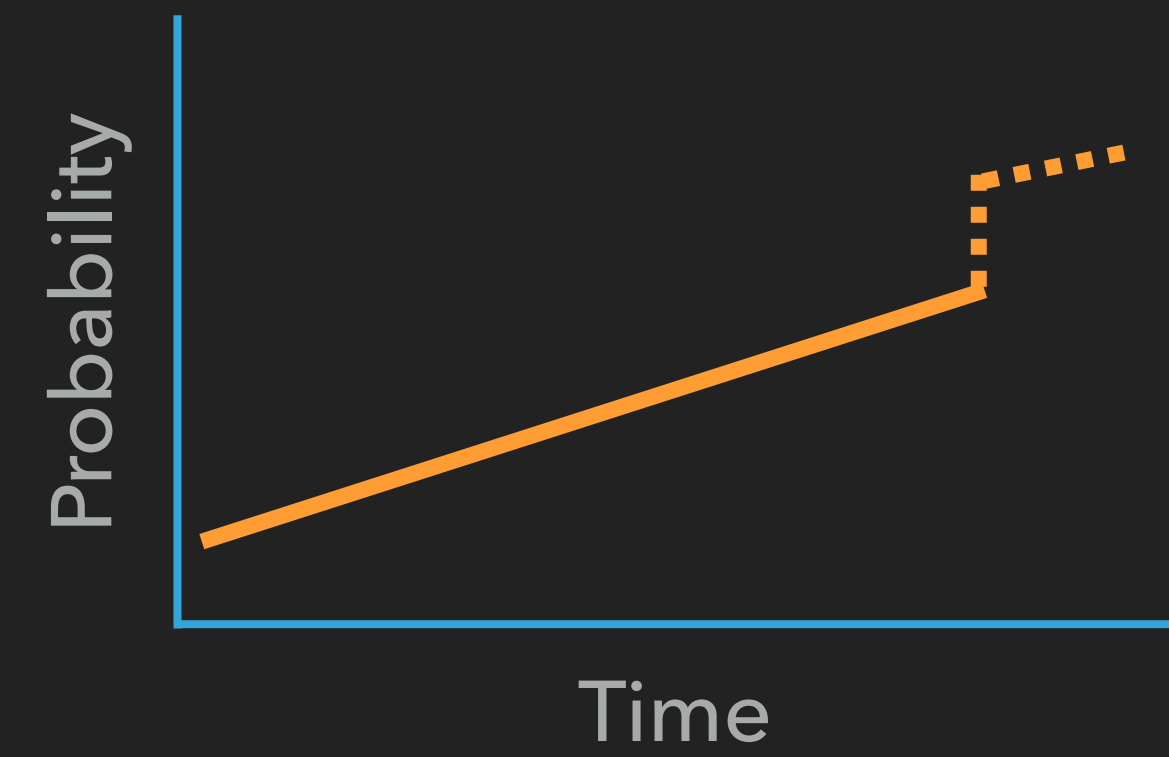
Uniform

until January 2016



Triangular

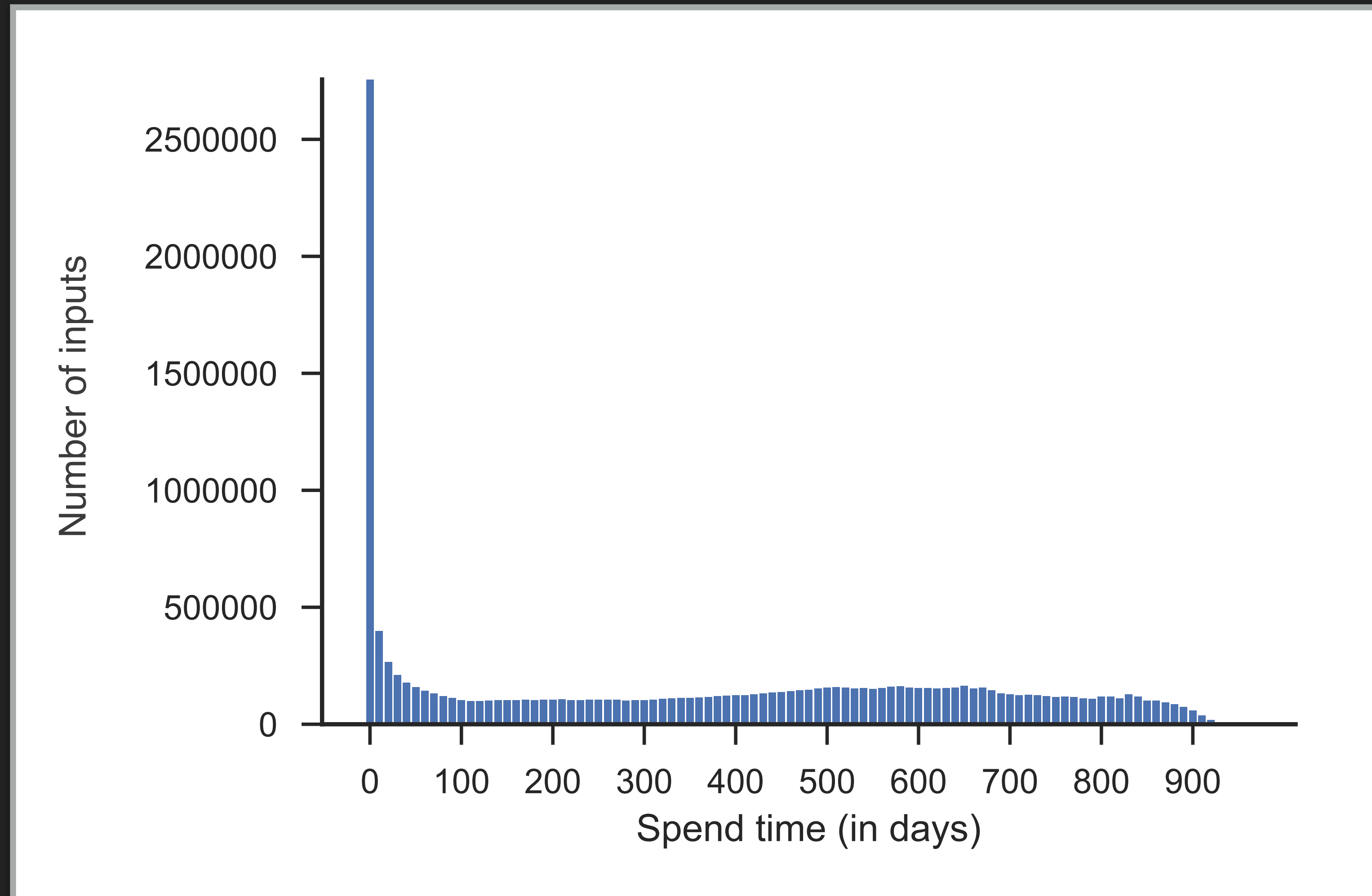
January-December 2016



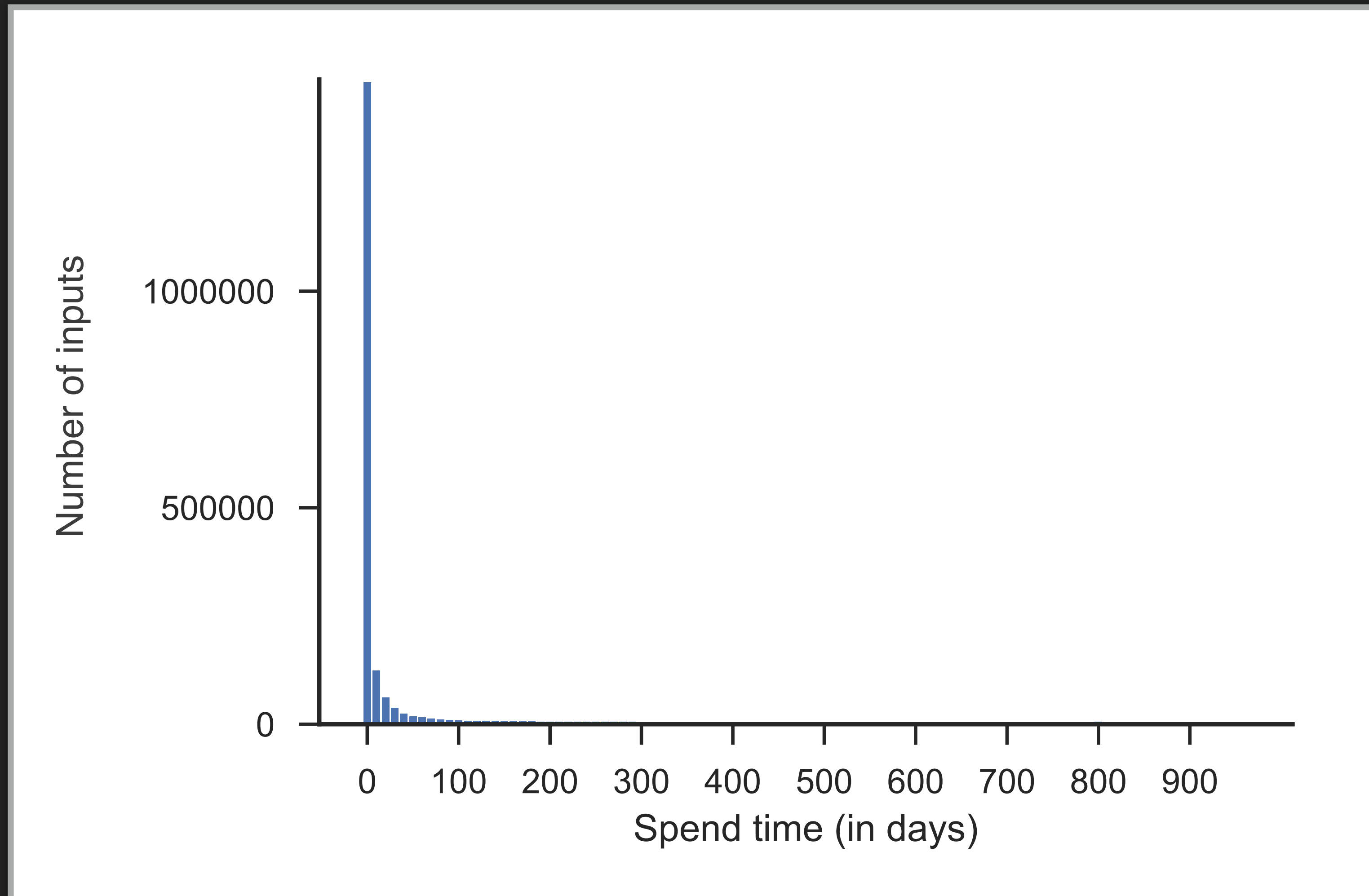
Triangular
+ recent

since December 2016

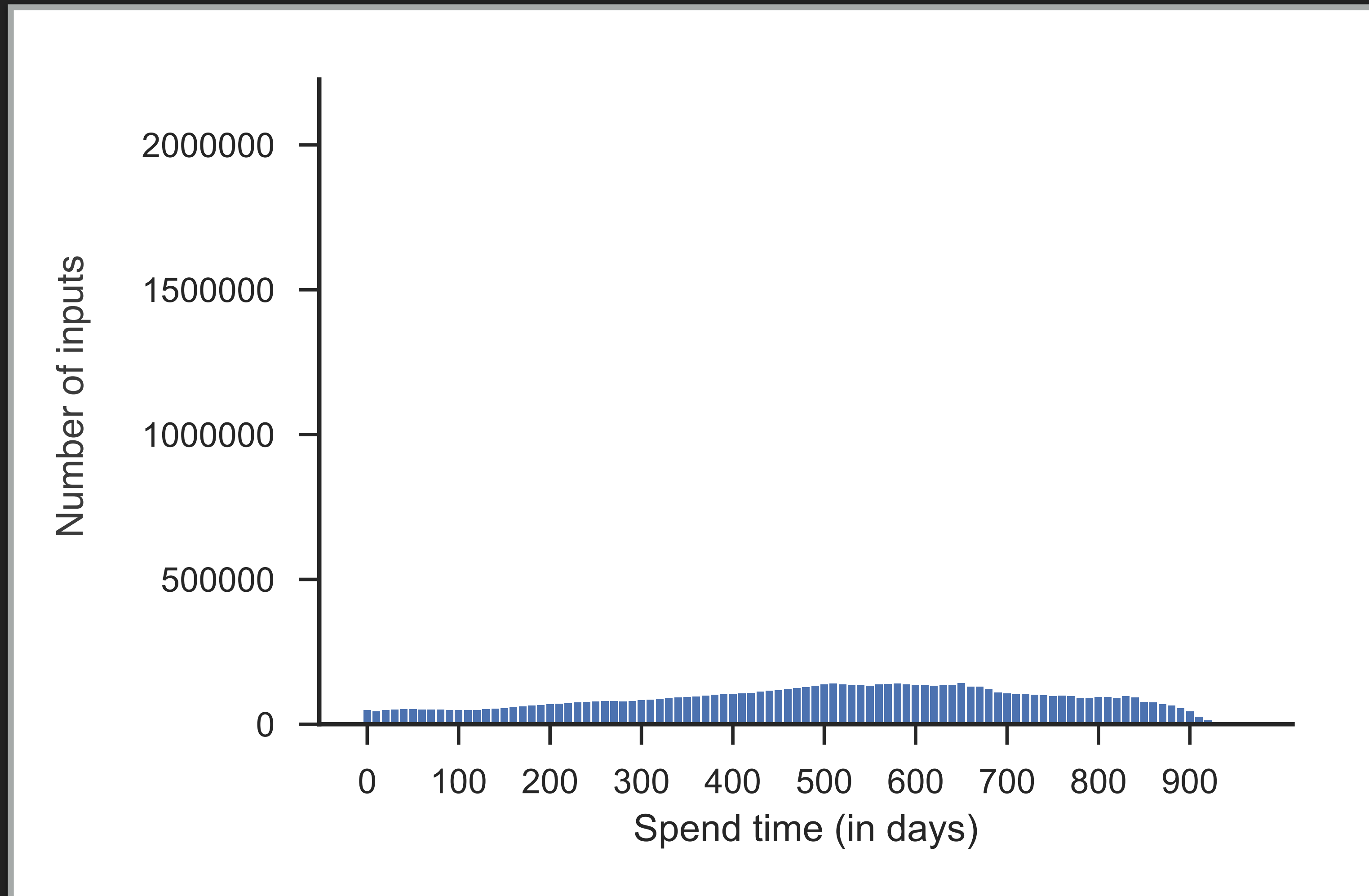
Spend Time of "Real" Inputs and Mixins



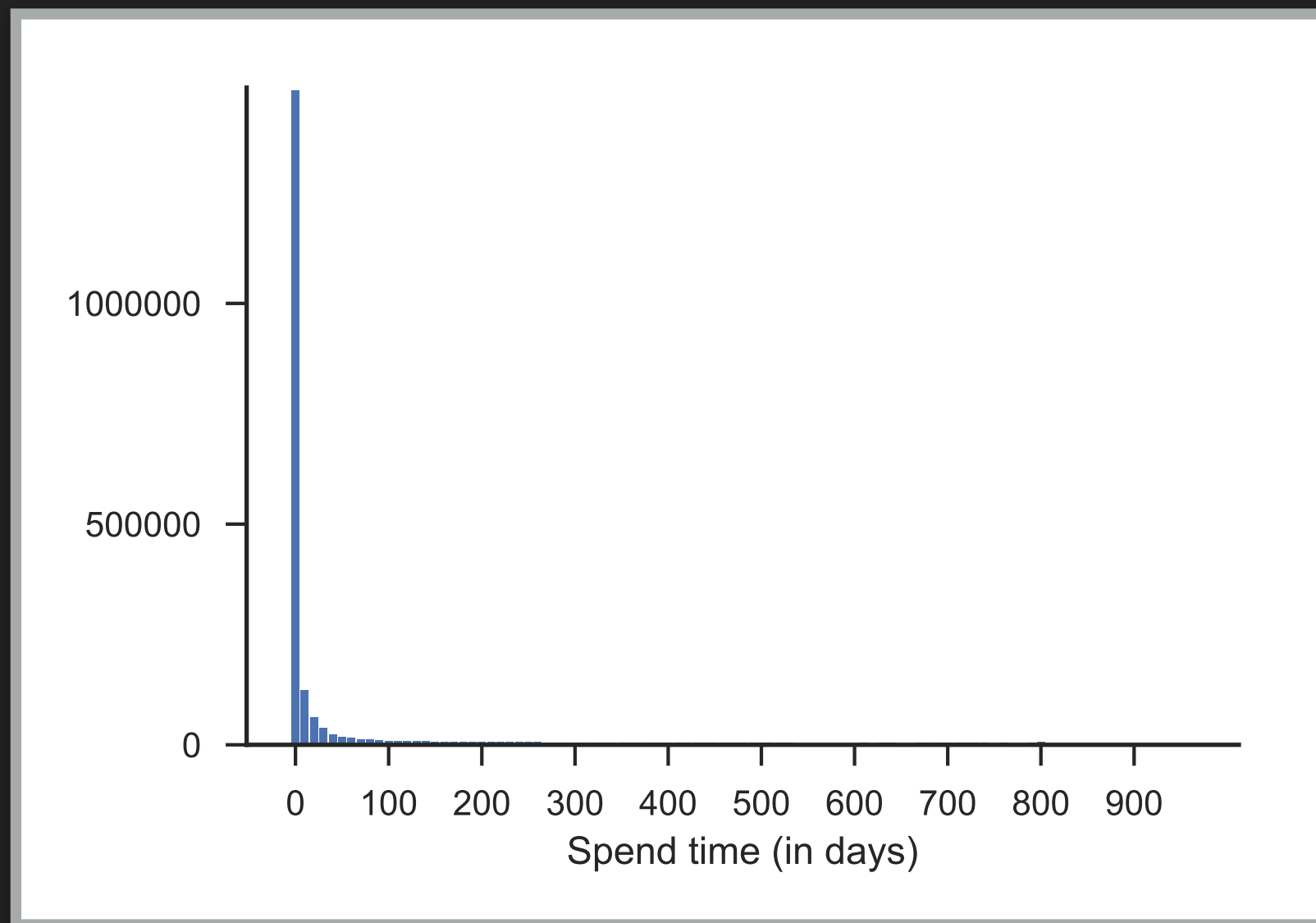
Spend Time of "Real" Inputs



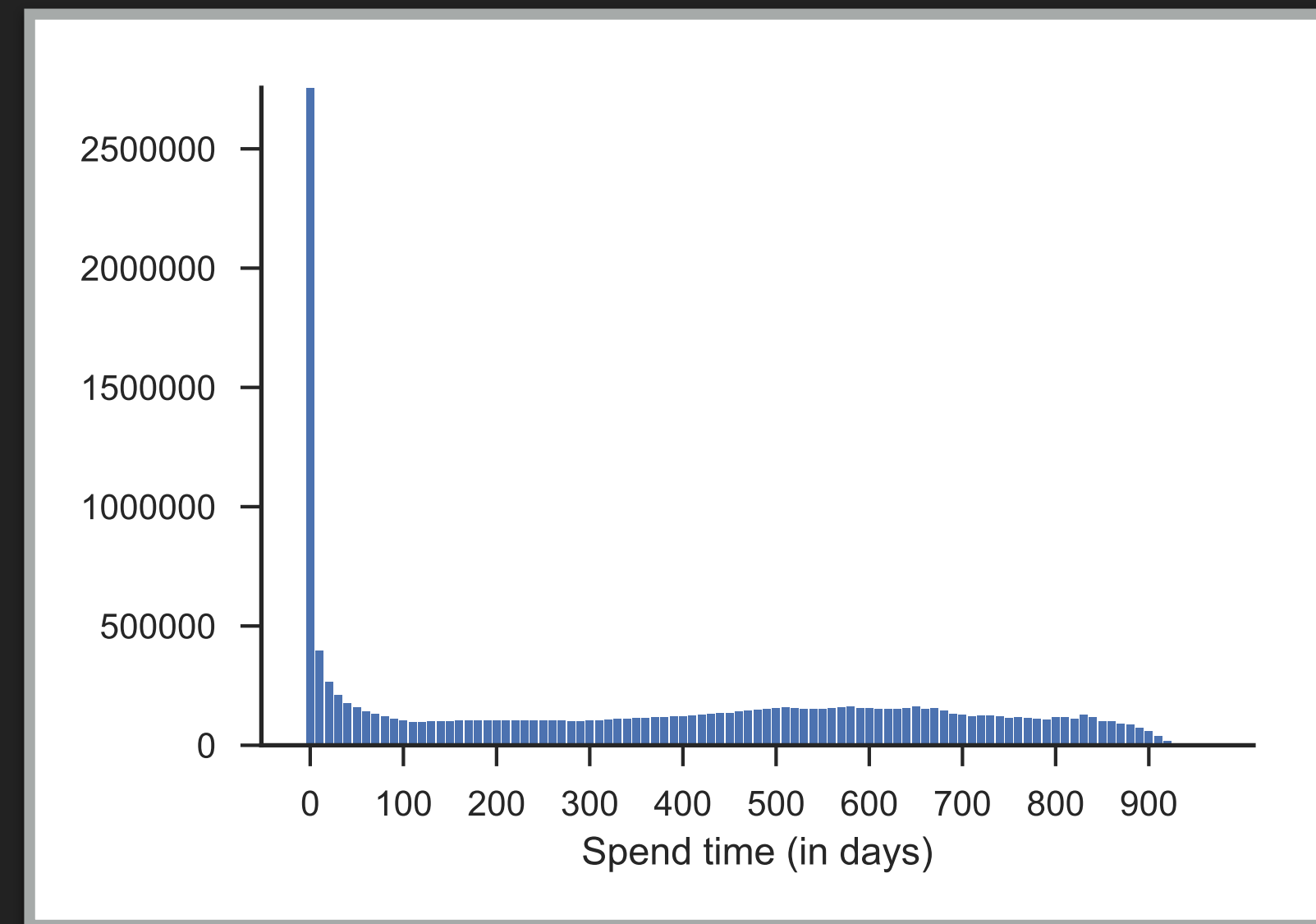
Spend Time of Ruled-Out Mixins



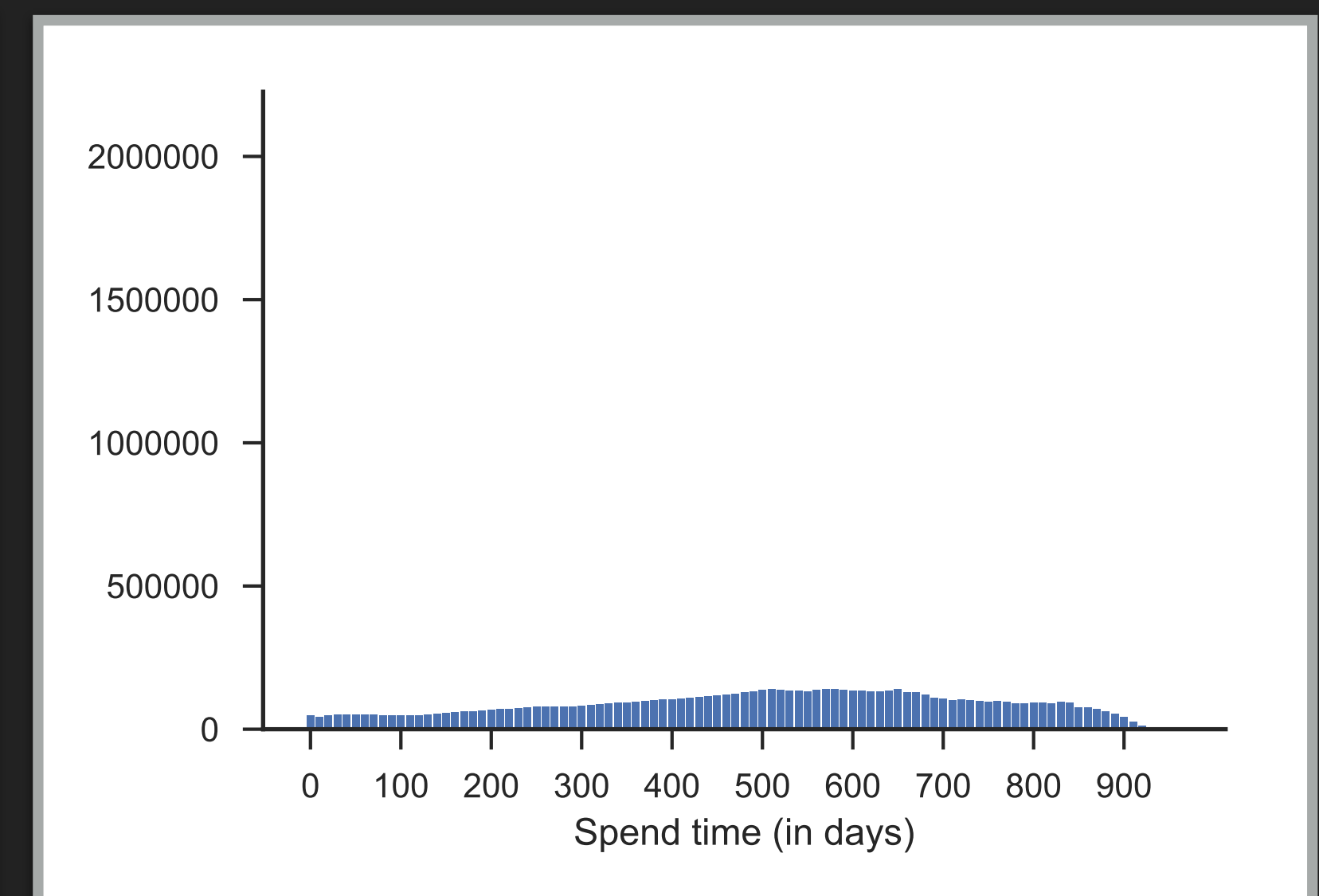
Distributions Do Not Match



Real



Real + Mixins



Ruled-out Mixins

Guess-Newest Heuristic

- ▶ The newest input is usually the real one
- ▶ Successful for
 - ▶ 92% of deduced inputs
 - ▶ 80% of all inputs (based on simulation)

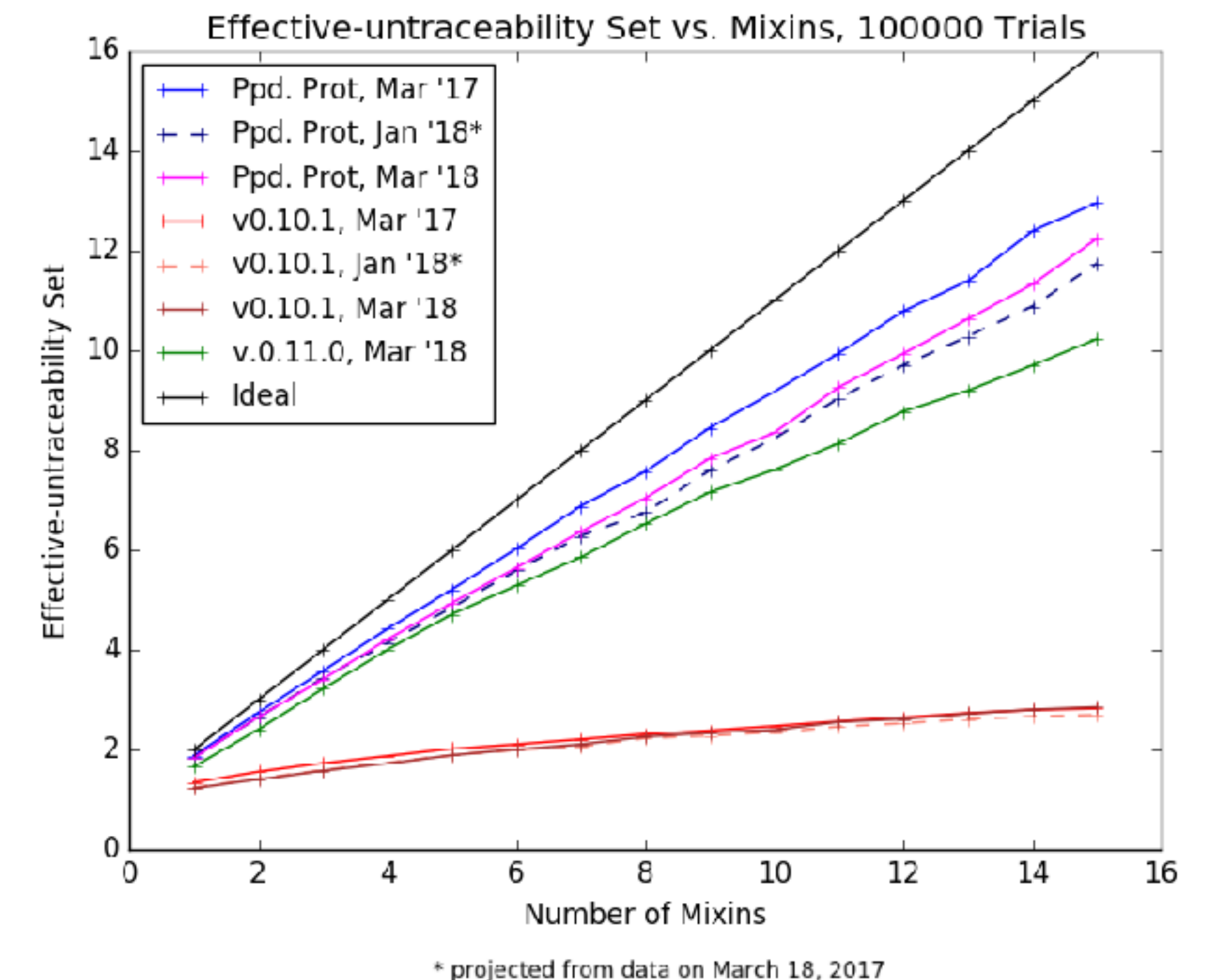
How Can We Fix This?

Sample More "Recent" Mixins

- ▶ More mixins, reduce size of "recent" window
- ▶ Simulation results in paper

Estimate Empirical Distribution

Binned Mixin



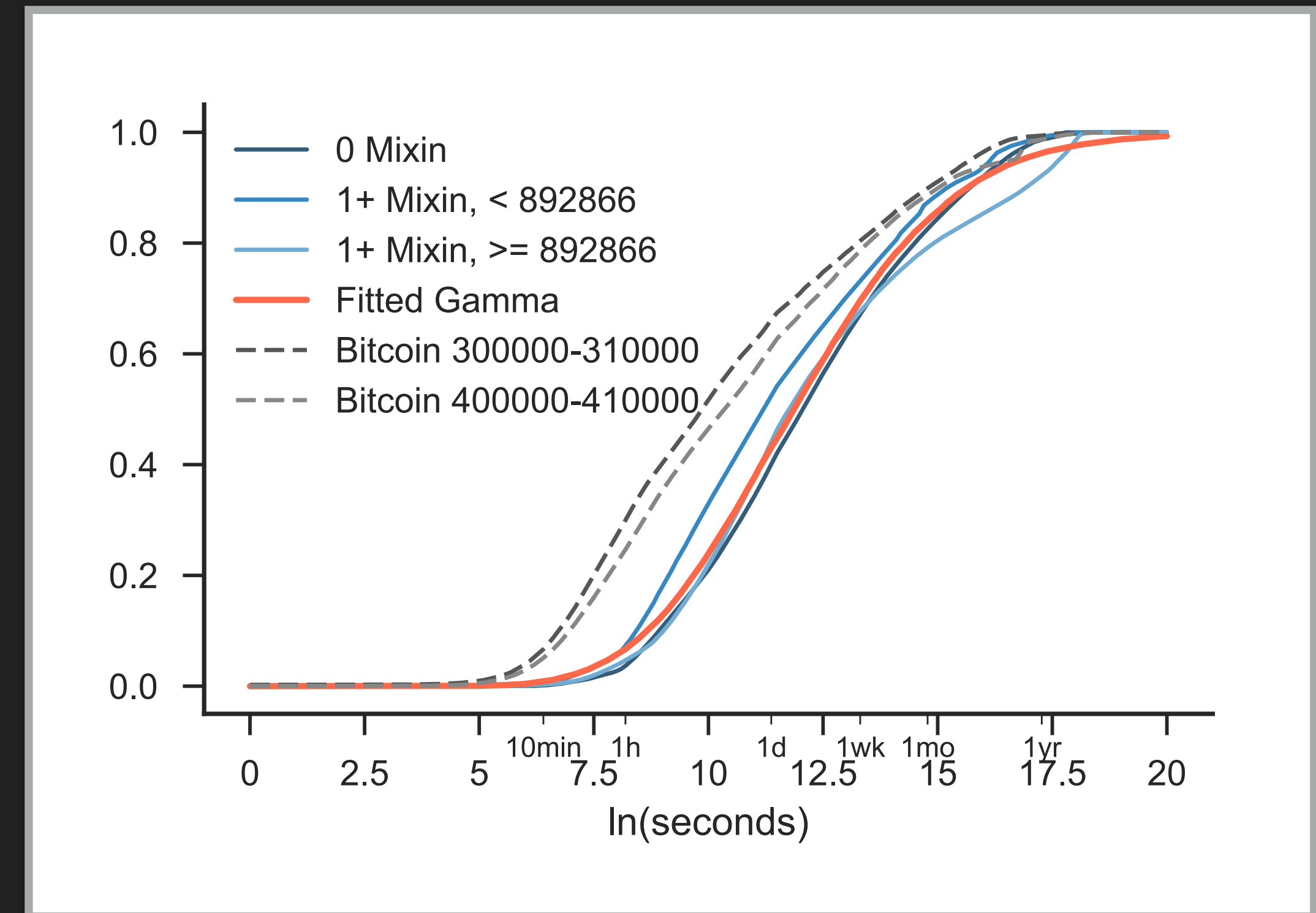
How Can We Fix This?

Sample More “Recent” Mixins

Estimate Empirical Distribution

- ▶ Fit distribution to ground truth data
- ▶ Good fit: Log-Gamma distribution

Binned Mixin



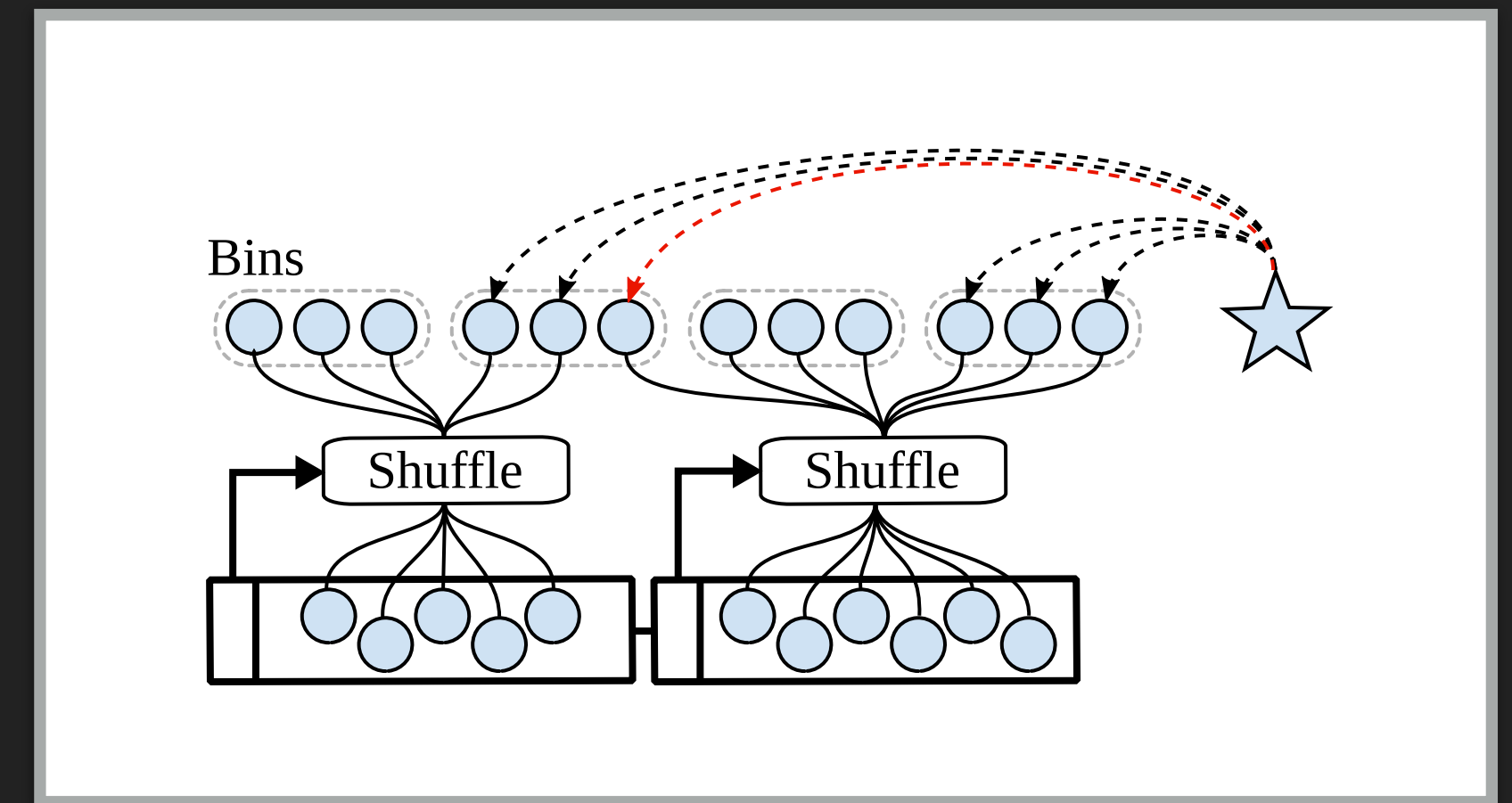
How Can We Fix This?

Sample More “Recent” Mixins

Estimate Empirical Distribution

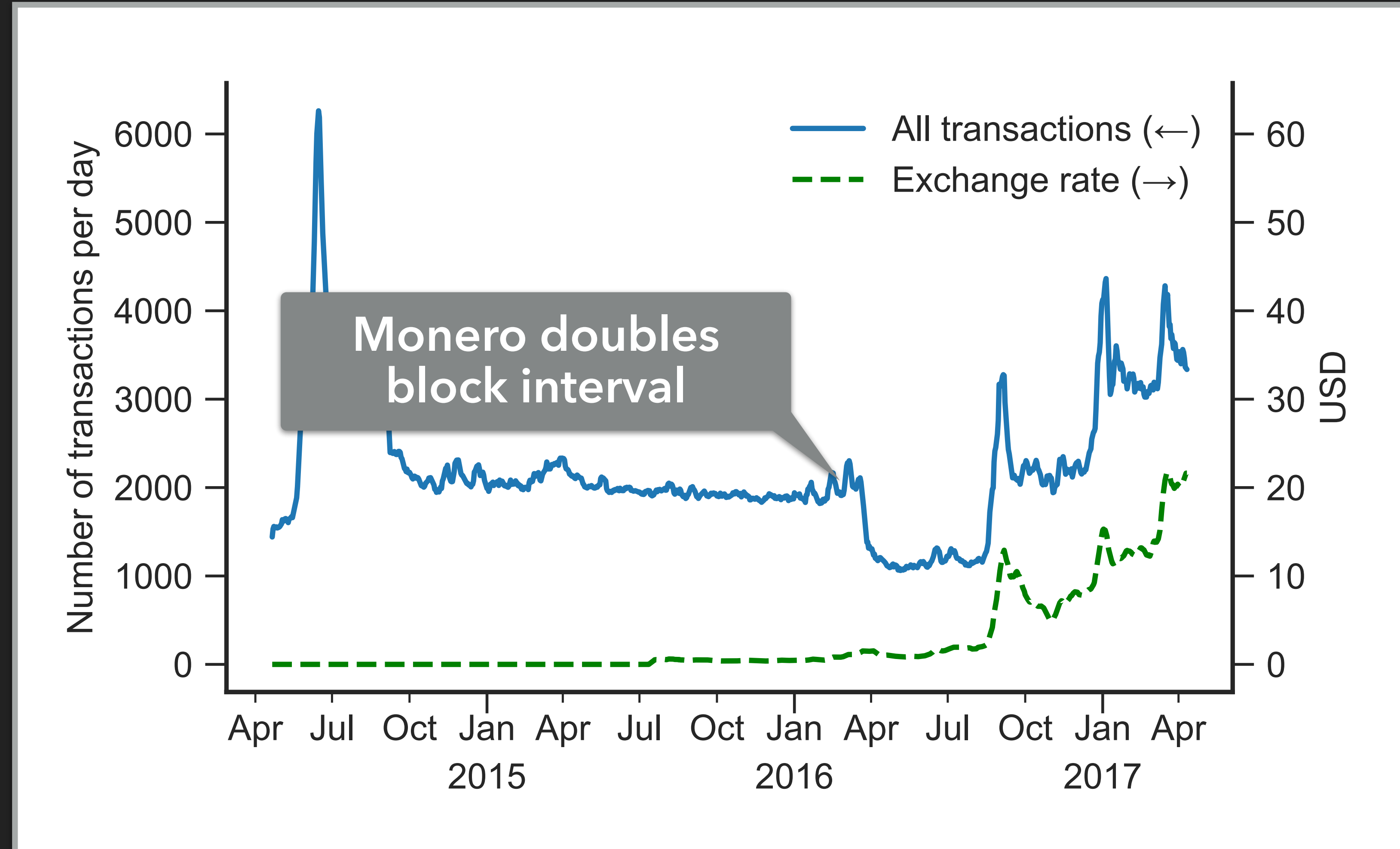
Binned Mixins

- ▶ Group outputs to defend against timing attacks
- ▶ Helps against attacker with prior information




Do These Weaknesses Matter?

- ▶ Not all transactions are equally privacy sensitive
- ▶ Goal: quantify different usage types



Mining Pools Announce Payouts

 Monero Hash Vault

HOME

DASHBOARD

BLOCKS

PAYMENT

PORTS

GETTING STARTED


MORE COINS?

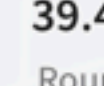
NETWORK:
459.58 MH/S


POOL:
9.55 MH/S


YOU:
0 H/S

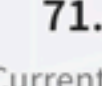
SETTINGS

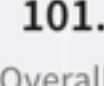
 98.288 Trillion
Hashes accepted


 39.4 Billion
Round hashes

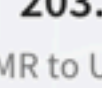
 03:12:01
PPLNS window

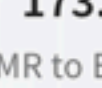
 2145
Blocks found

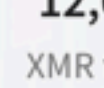
 71.46 %
Current effort


 101.37 %
Overall effort

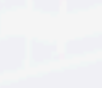
 0.02408153
XMR to BTC

 203.49
XMR to USD

 173.56
XMR to EUR

 12,676.1
XMR to RUB

 2217
Miners connected

 4736
Miners paid (8007 Payments)

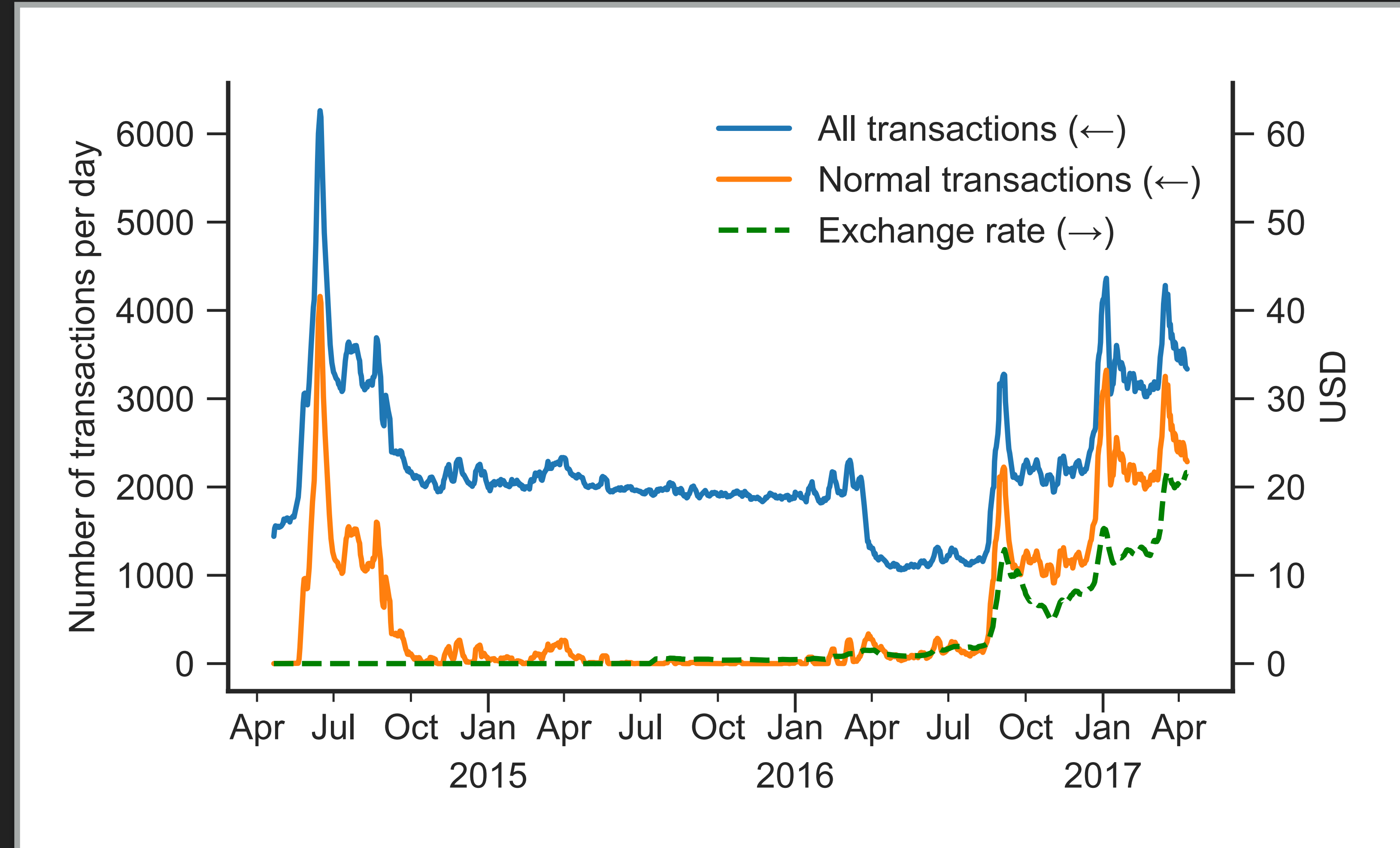
Payments Made

Nº	Time Sent	Transaction Hash	Amount	Fee
8007	40 minutes ago	32770677737a272a17a9313cd96c4d2c894f0fc3bef18569cfcadc3cedf32658	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	d759f7993bb854aeffabe0ac176919f09a4d99a3cbe14dcd87d0eb670b11850	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 XMR
7996	41 minutes ago	f87d64c8a626bac889558821d046f449dbfb0c4fade1ca1ec0f49a31858dacf3	0.112415 XMR	0.00239226 XMR



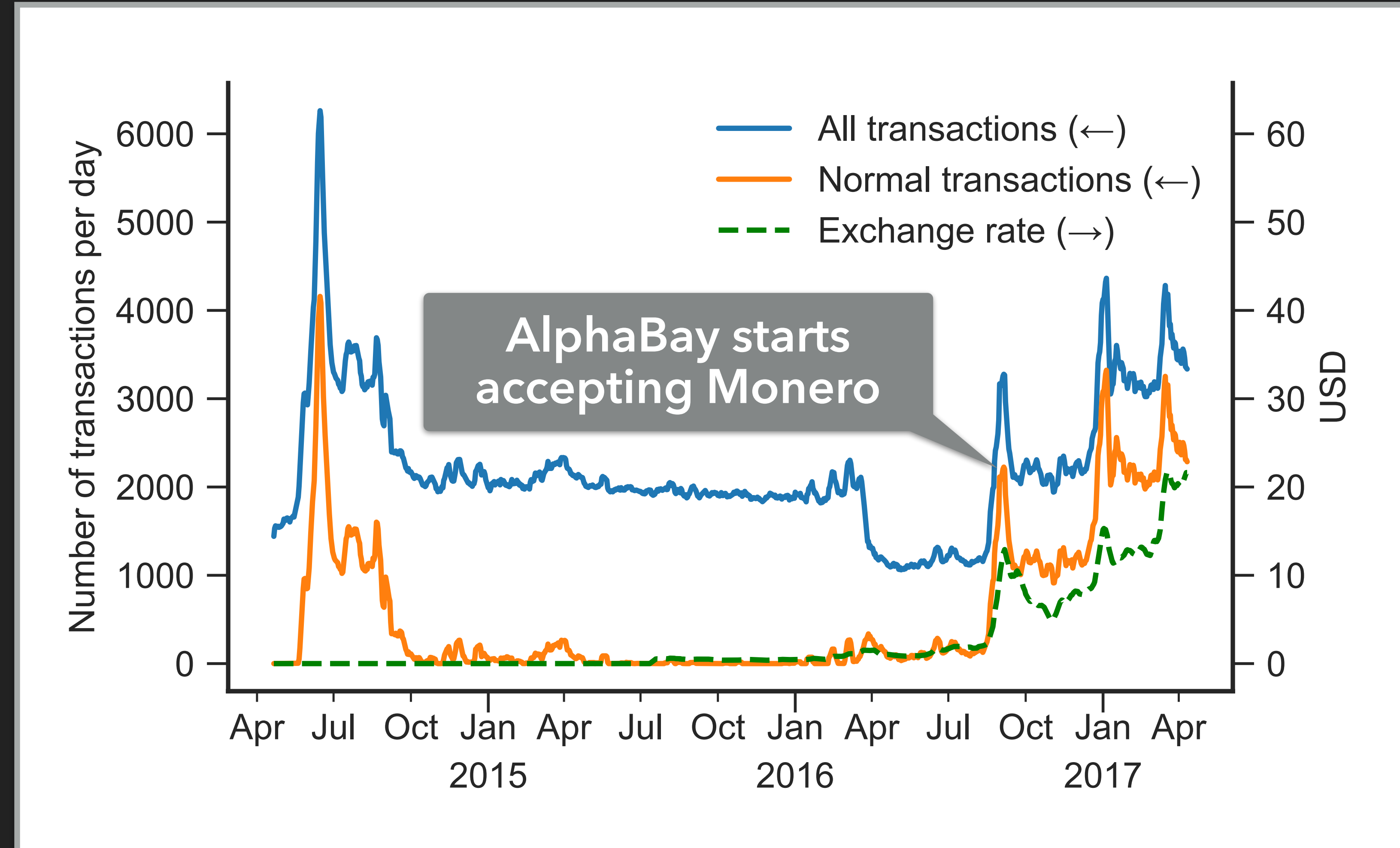
Estimating Mining Activity

- ▶ Miners announce blocks and payouts
- ▶ Website crawl
 - ▶ # blocks found
 - ▶ # payout txs
- ▶ 0.44 txs per block related to mining

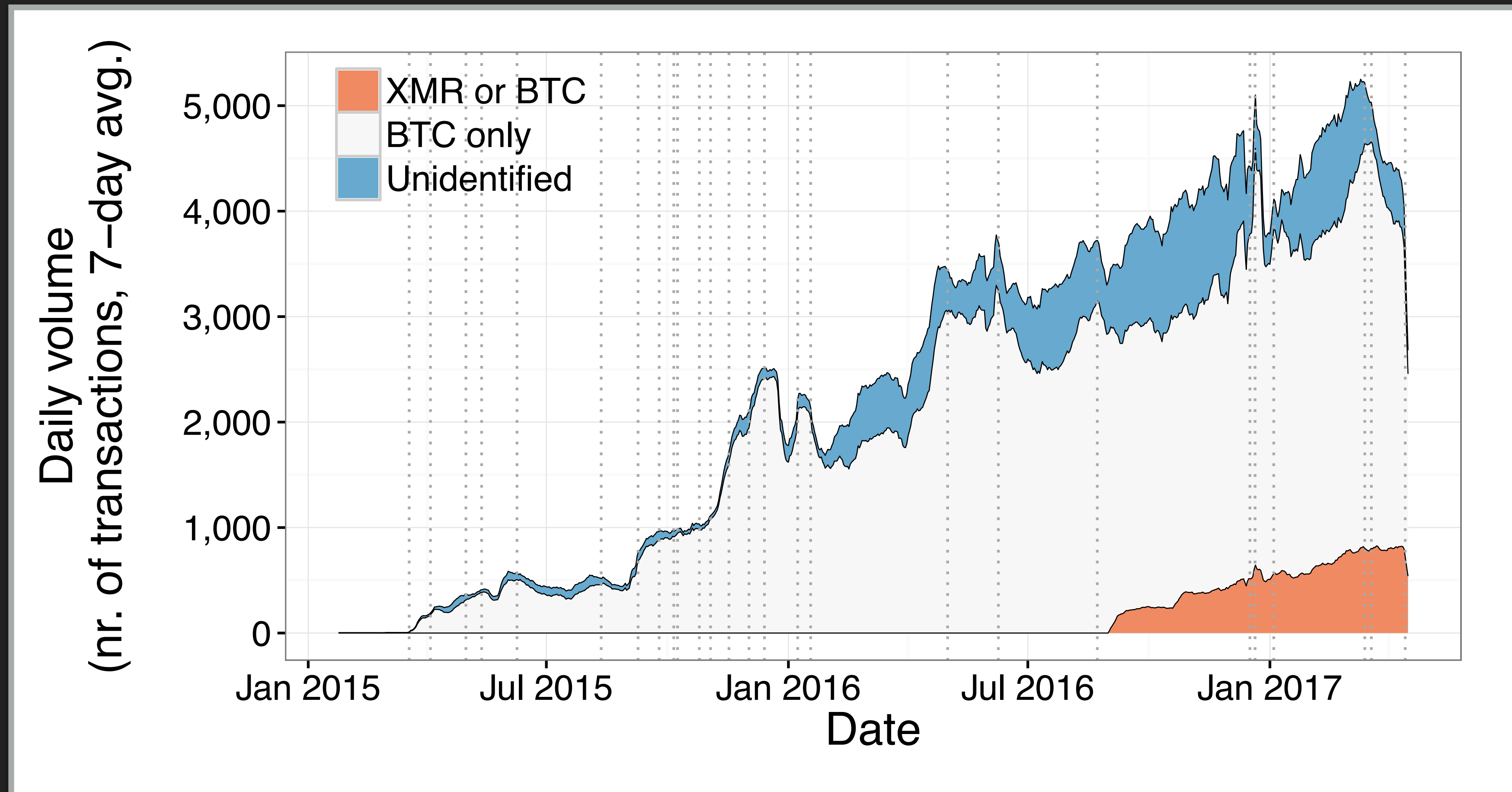


AlphaBay

- ▶ Volume spiked when AlphaBay started accepting Monero

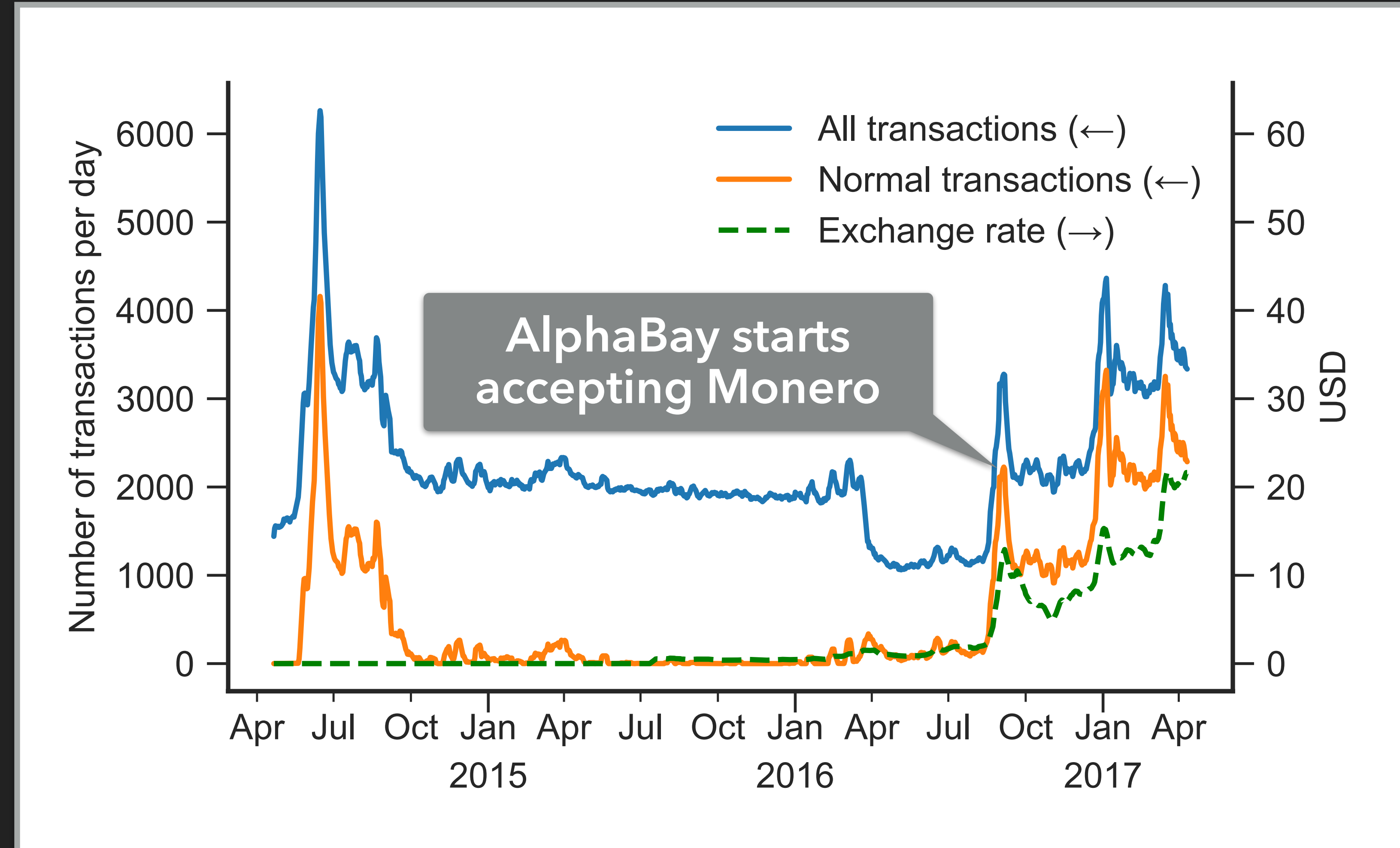


AlphaBay - Daily Volume (Number of Transactions)



AlphaBay

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



Cryptocurrency Privacy Inherits the Worst of

- ▶ Data anonymization
 - ▶ Blockchain data is public
 - ▶ Weakness can be exploited retroactively
- ▶ Communication anonymity
 - ▶ Behavior of some users influences anonymity of others
 - ▶ "Anonymity loves company"

Summary

- ▶ Identified and quantified two weaknesses in Monero's mixin selection
- ▶ Many privacy-sensitive transactions are vulnerable to deanonymization
 - ▶ More than a thousand transactions per day in late 2016
 - ▶ Criminal offenses take years to expire (if at all)
- ▶ Illicit business tends to be early adopters of new technologies
 - ▶ Many legitimate uses that are less visible