

Multiple Sides of 36 coins: Measuring P2P Infrastructure Across Cryptocurrencies

Lucianna Kiffer

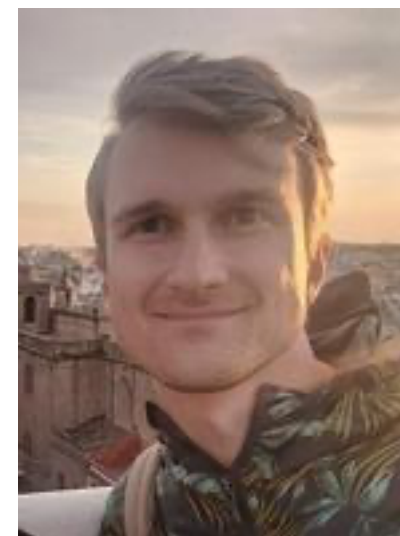
Research Assistant Professor • IMDEA Networks, Madrid



Lioba Heimbach
Category Labs



Dennis Trautwein
University of Göttingen/ ProbeLab



Yann Vonlathen
Ethereum Foundation

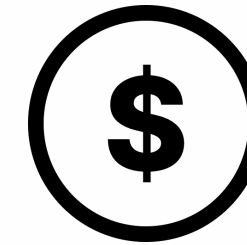


Oliver Gasser
IPInfo

The P2P Network: A Hidden Layer



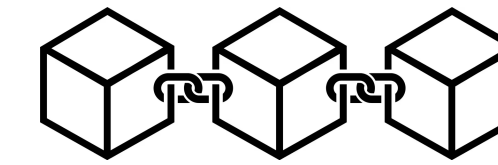
What users see



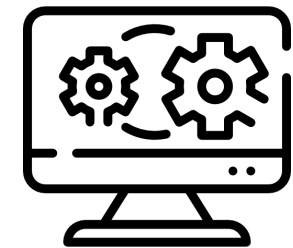
Token Price



Market Cap



Blockchain/
Transactions



Applications
& Defi

What holds it together

Peer-to-Peer Network : where all network messages propagate

Transactions

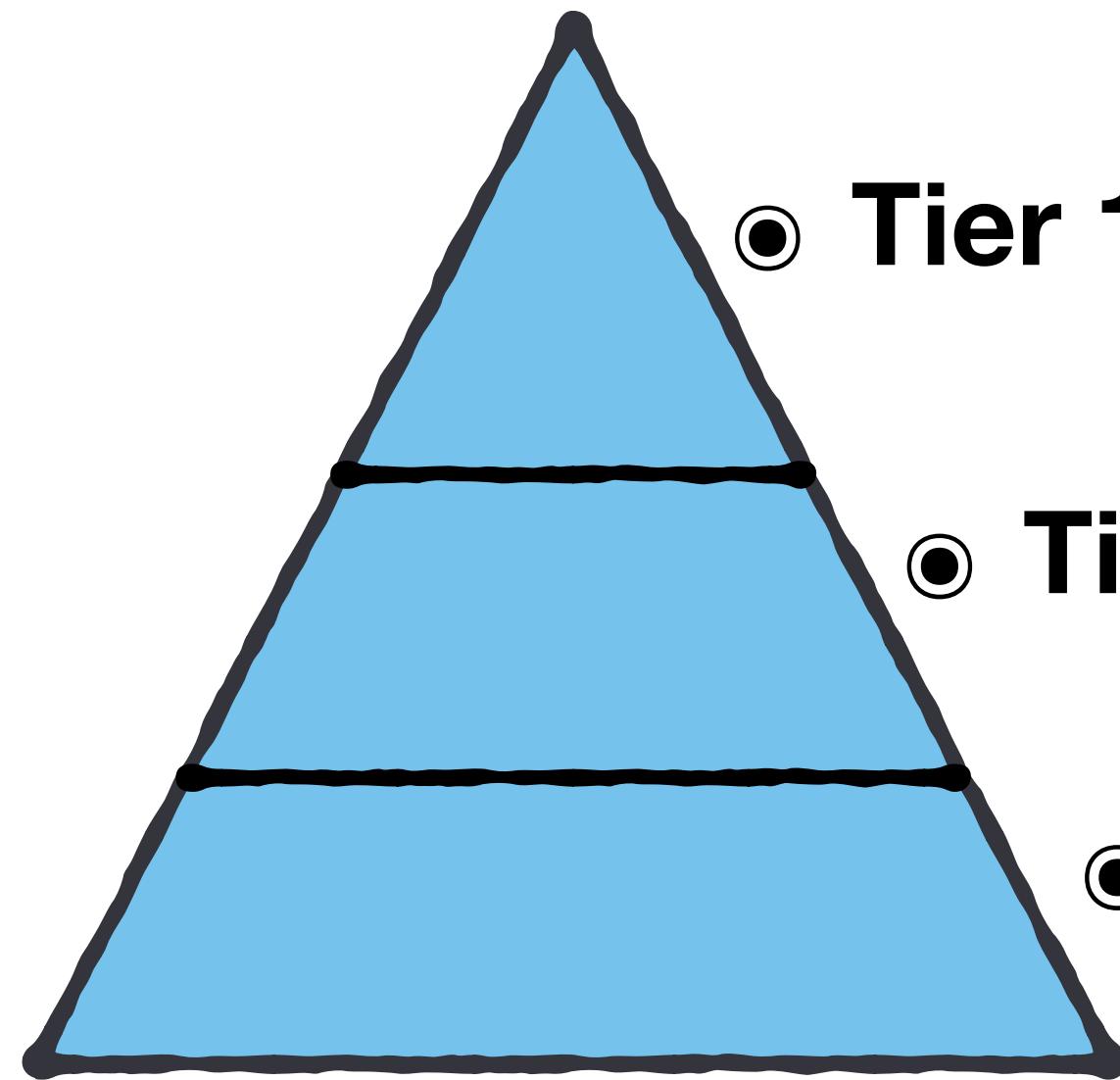
Blocks

Consensus Messages

...

Security ❖ Decentralization ❖ Censorship Resistance ❖ etc.

How observable are blockchain P2P networks?



- **Tier 1** (Bitcoin, Ethereum): reasonably rich and well-studied
- **Tier 2**: bare IP dumps, unverified, no history, limited metadata
- **Tier 3**: **no data**, or tools that **went offline mid-study**, or tools whose numbers we **directly found to be wrong**

For most blockchains, users have little reliable information about the infrastructure underpinning the system.

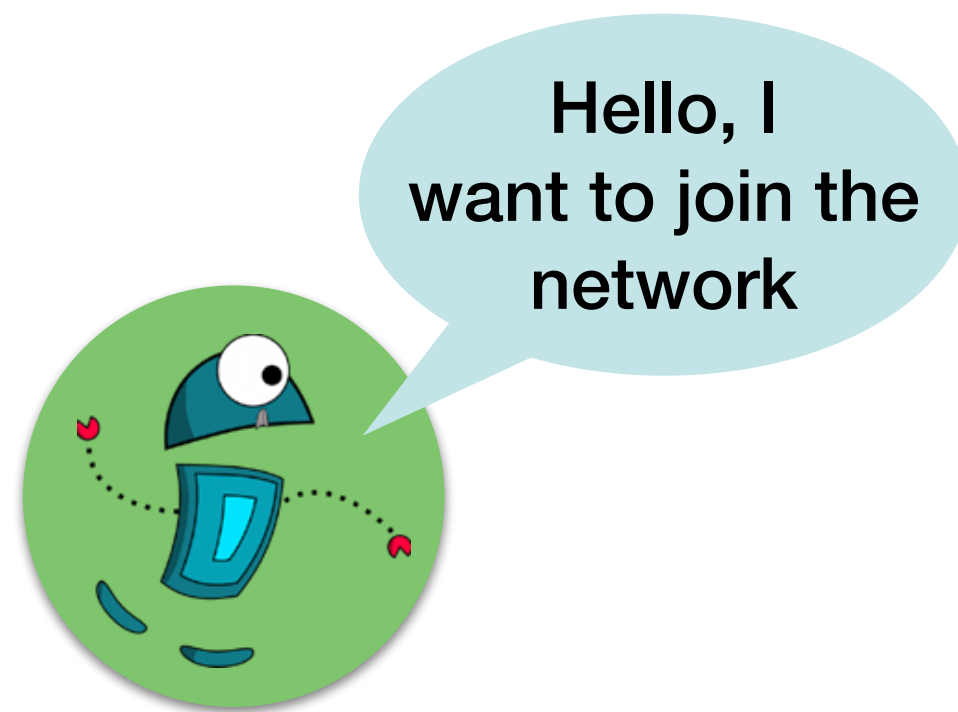
In this work:

- ★ measure network layer of **36 blockchain networks**
- ★ **9 months** + (still running since late Dec. 2024)
- ★ daily/hourly measurements over **IPv4** and **IPv6**
- ★ **public code** and **observatory** website

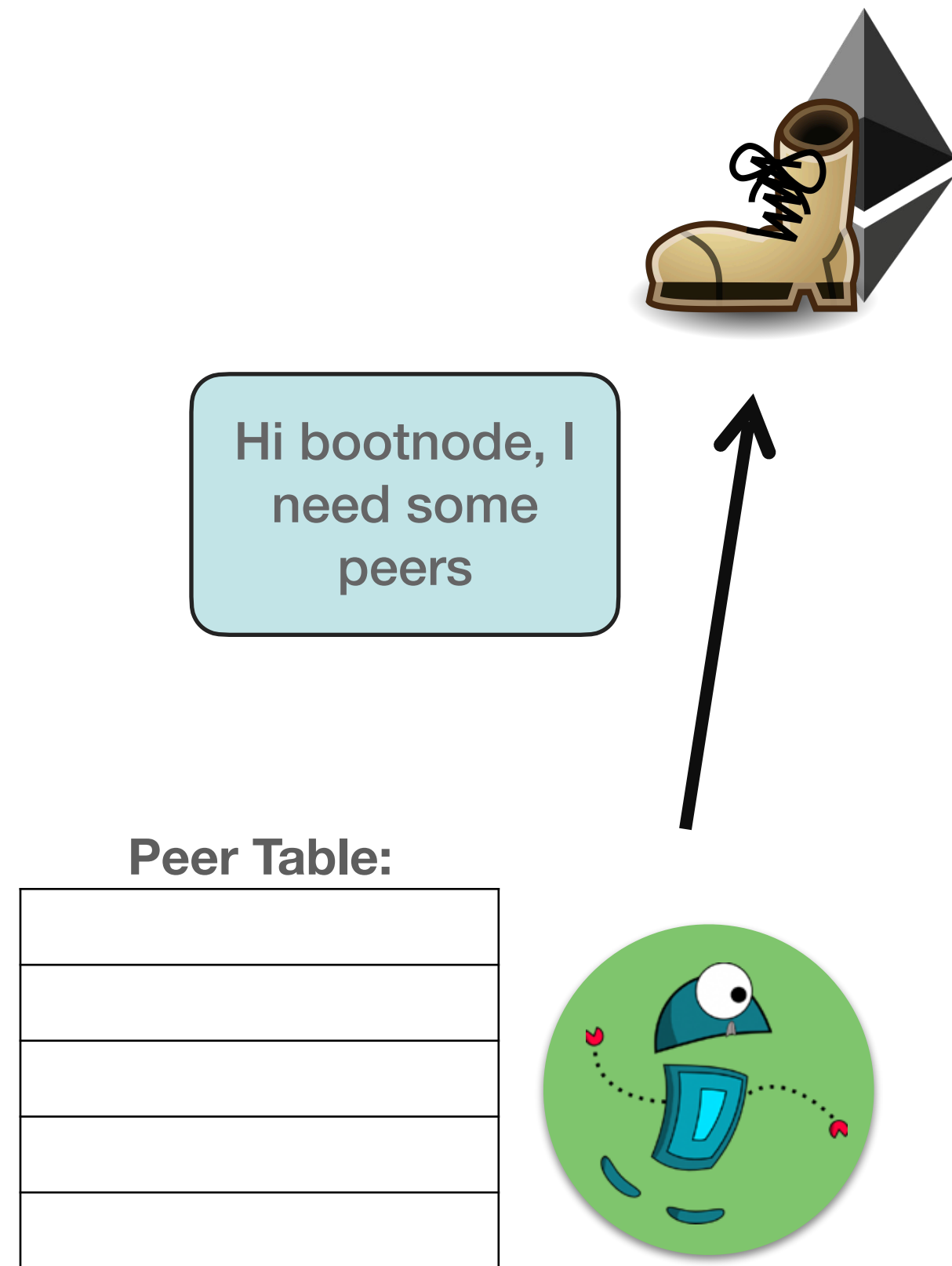
Peer Discovery Protocols



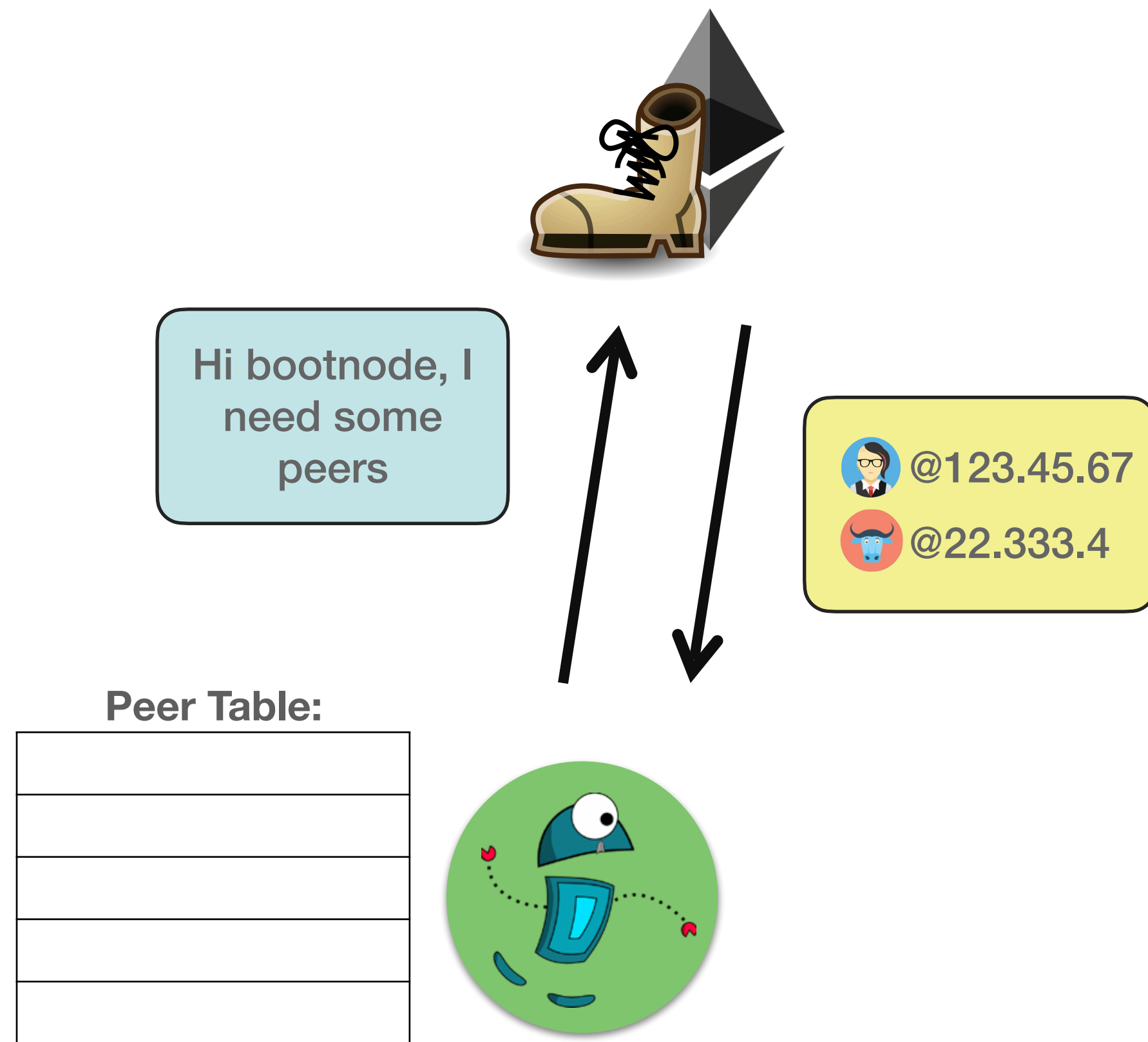
Peer Table:



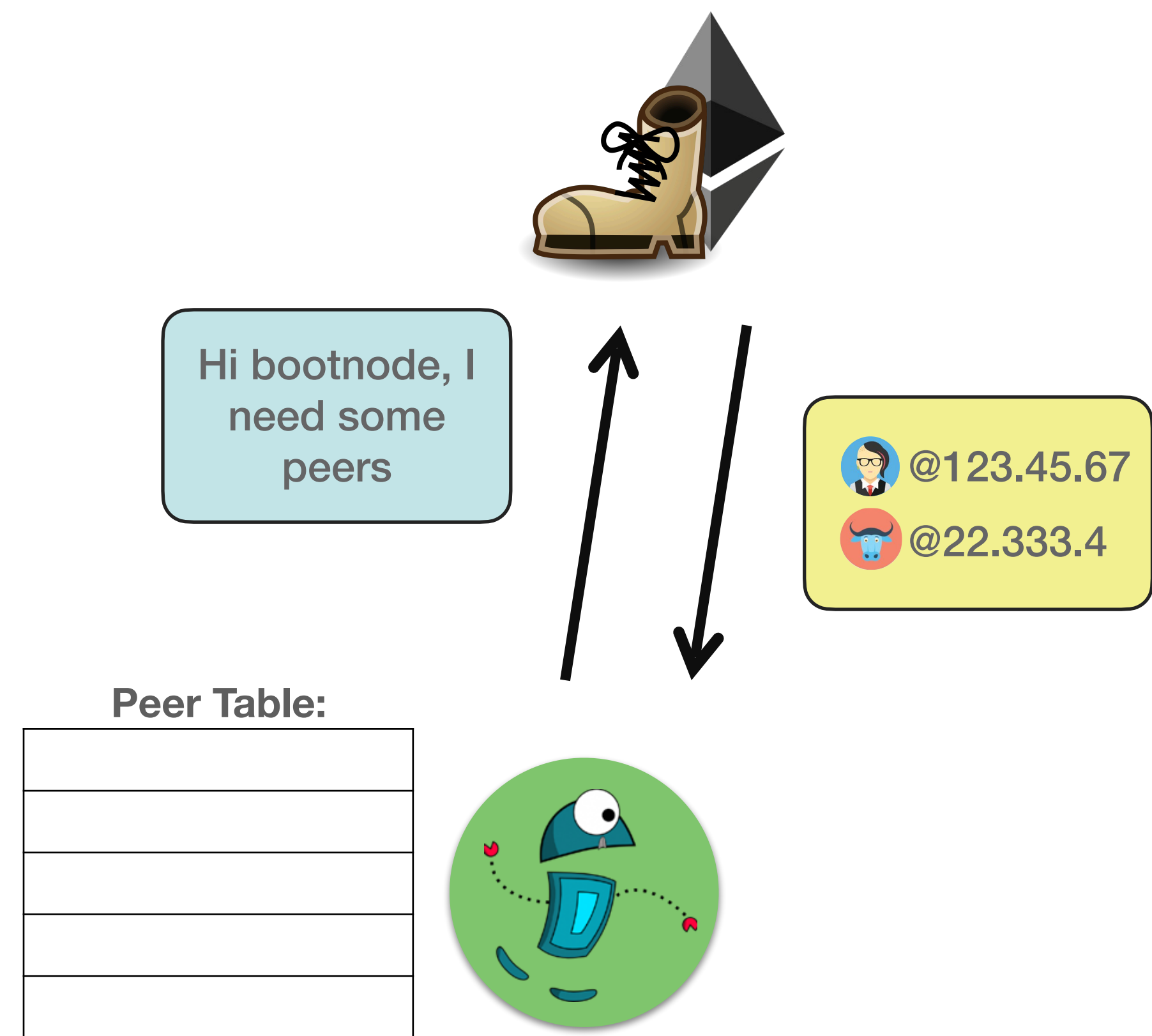
Peer Discovery Protocols



Peer Discovery Protocols



Peer Discovery Protocols



Session 9E: Web Censorship and Auditing

CCS '19, November 11–15, 2019, London, United Kingdom

You Shall Not Join: A Measurement Study of Cryptocurrency Peer-to-Peer Bootstrapping Techniques

Angelique Faye Loe
Royal Holloway, University of London
Information Security Group
angelique.loe.2016@live.rhul.ac.uk

Elizabeth Anne Quaglia
Royal Holloway, University of London
Information Security Group
elizabeth.quaglia@rhul.ac.uk

ABSTRACT

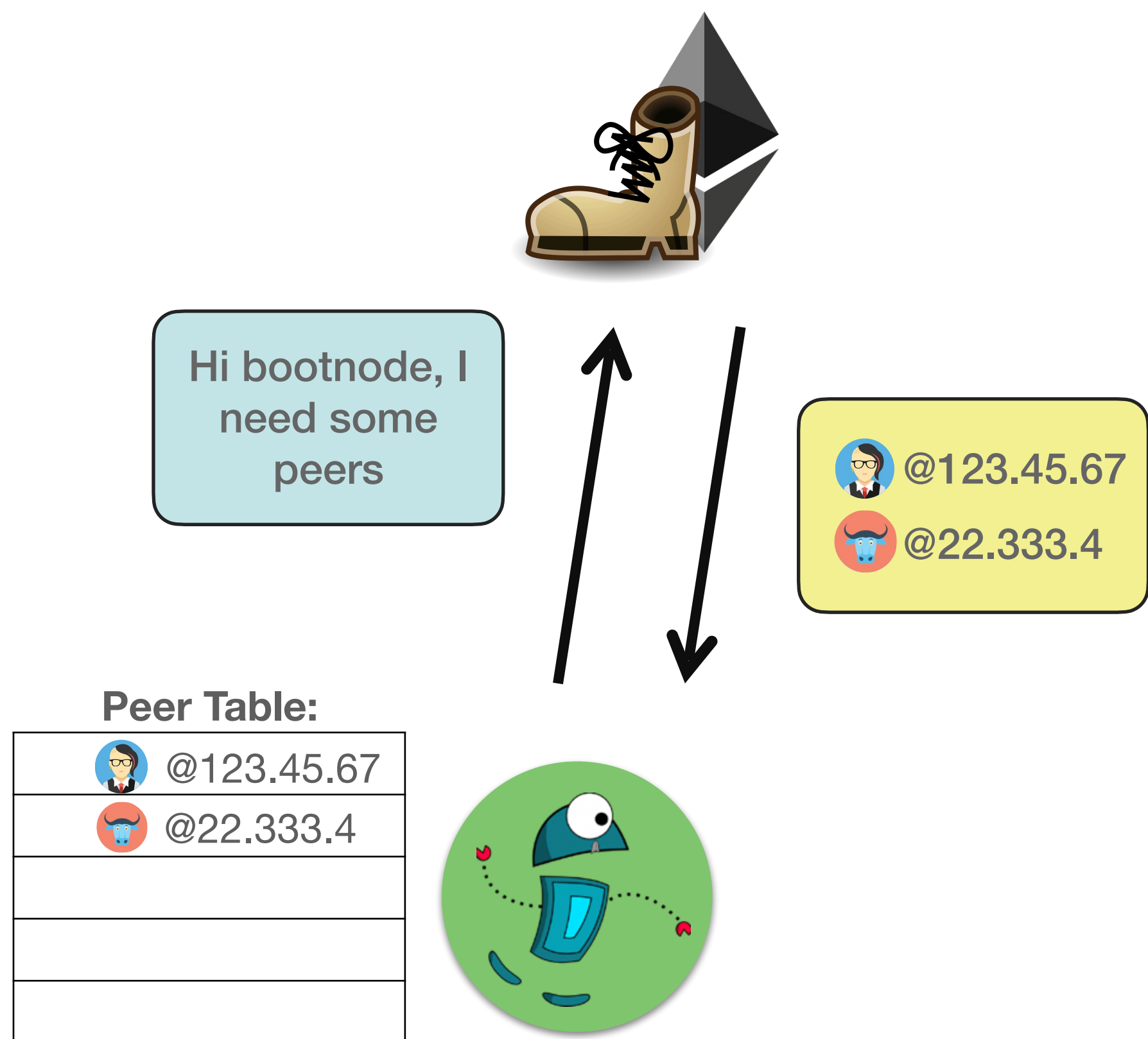
Cryptocurrencies are digital assets which depend upon the use of distributed peer-to-peer networks. The method a new peer uses to initially join a peer-to-peer network is known as bootstrapping. The ability to bootstrap without the use of a centralized resource is an unresolved challenge. In this paper we survey the bootstrapping techniques used by 74 cryptocurrencies and find that censorship-prone methods such as DNS seeding and IP hard-coding are the most prevalent. In response to this finding, we test two other bootstrapping techniques less susceptible to censorship, Tor and ZMap, to determine if they are operationally feasible alternatives more resilient to censorship. We perform a global measurement study of DNS query responses for each of the 92 DNS seeds discovered across 42 countries using the distributed RIPE Atlas network. This provides details of each cryptocurrency's peer-to-peer network topology and also highlights instances of DNS outages and query manipulation impacting the bootstrapping process. Our study also reveals that the source code of the cryptocurrencies researched comes from only five main repositories; hence accounting for the inheritance of legacy bootstrapping methods. Finally, we discuss the implications of our findings and provide recommendations to mitigate the risks exposed.

1 INTRODUCTION

Cryptocurrencies are decentralized digital assets that do not rely on trusted third parties for the execution of transactions between parties. Decentralization is achieved through the use of distributed ledger technology to provide an append-only chronicle of all transactions between parties sending and receiving funds. The immutability of transactions is achieved through a fiscally incentivized consensus protocol publicly executed by peers participating in a peer-to-peer network [51]. The decentralized nature of cryptocurrencies provides a promise of technological amelioration to traditional payment systems [23, 27, 51, 59]. Due to the unprecedented pace of mainstream adoption and investment into these digital assets, they have attracted considerable scrutiny and research [19, 24, 26, 33, 34, 40, 47–50].

We present a measurement study of the techniques used to initially connect 74 different cryptocurrency peers to their relevant distributed peer-to-peer networks. When a new peer first joins a peer-to-peer network the action describing this initial connection is known as *bootstrapping*. By surveying the bootstrapping techniques of these cryptocurrencies we are able to uncover the following elements about their operation: the inability to resist known censorship techniques to prevent peer connectivity, the feasibility of employing censorship-resistant connection techniques, details

Peer Discovery Protocols



Session 9E: Web Censorship and Auditing

CCS '19, November 11–15, 2019, London, United Kingdom

You Shall Not Join: A Measurement Study of Cryptocurrency Peer-to-Peer Bootstrapping Techniques

Angelique Faye Loe
Royal Holloway, University of London
Information Security Group
angelique.loe.2016@live.rhul.ac.uk

Elizabeth Anne Quaglia
Royal Holloway, University of London
Information Security Group
elizabeth.quaglia@rhul.ac.uk

ABSTRACT

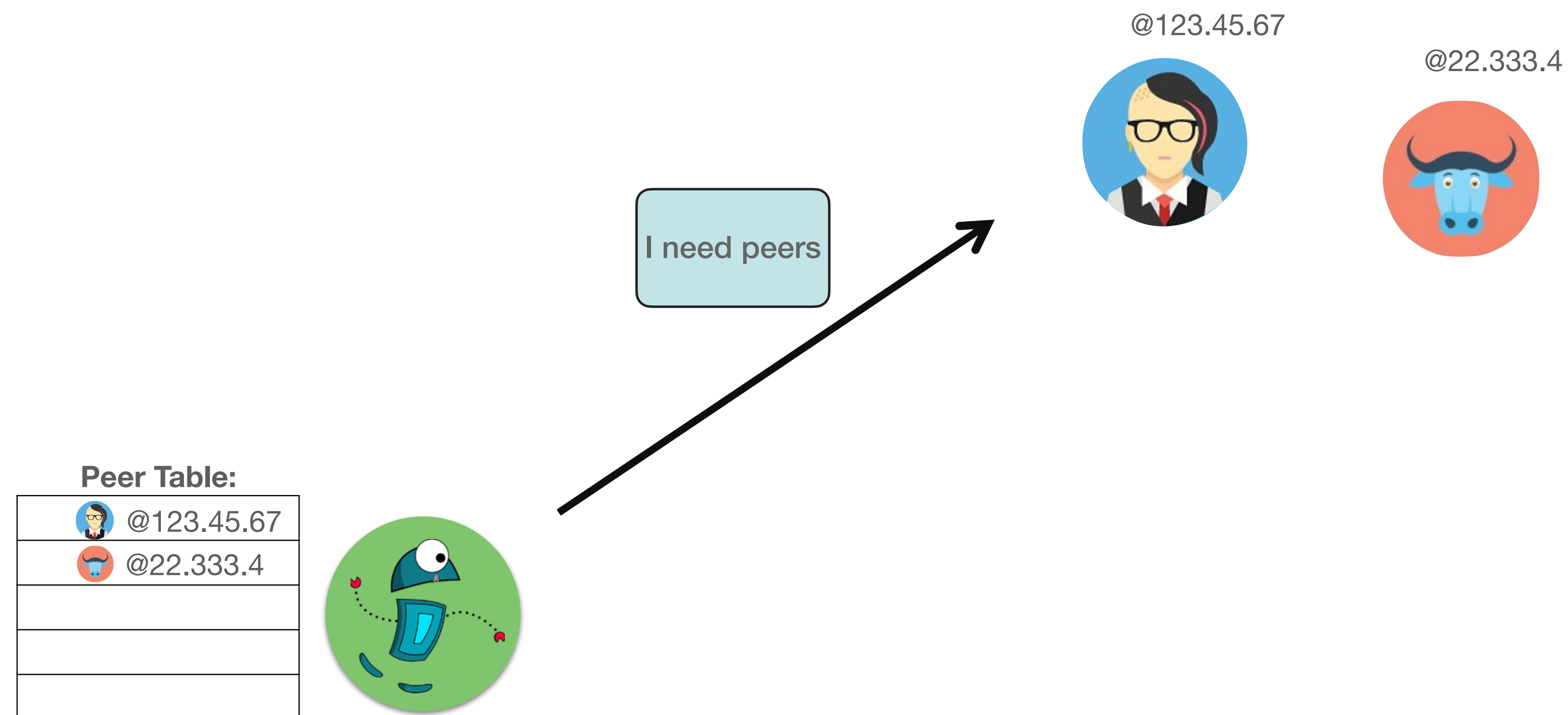
Cryptocurrencies are digital assets which depend upon the use of distributed peer-to-peer networks. The method a new peer uses to initially join a peer-to-peer network is known as bootstrapping. The ability to bootstrap without the use of a centralized resource is an unresolved challenge. In this paper we survey the bootstrapping techniques used by 74 cryptocurrencies and find that censorship-prone methods such as DNS seeding and IP hard-coding are the most prevalent. In response to this finding, we test two other bootstrapping techniques less susceptible to censorship, Tor and ZMap, to determine if they are operationally feasible alternatives more resilient to censorship. We perform a global measurement study of DNS query responses for each of the 92 DNS seeds discovered across 42 countries using the distributed RIPE Atlas network. This provides details of each cryptocurrency's peer-to-peer network topology and also highlights instances of DNS outages and query manipulation impacting the bootstrapping process. Our study also reveals that the source code of the cryptocurrencies researched comes from only five main repositories; hence accounting for the inheritance of legacy bootstrapping methods. Finally, we discuss the implications of our findings and provide recommendations to mitigate the risks exposed.

1 INTRODUCTION

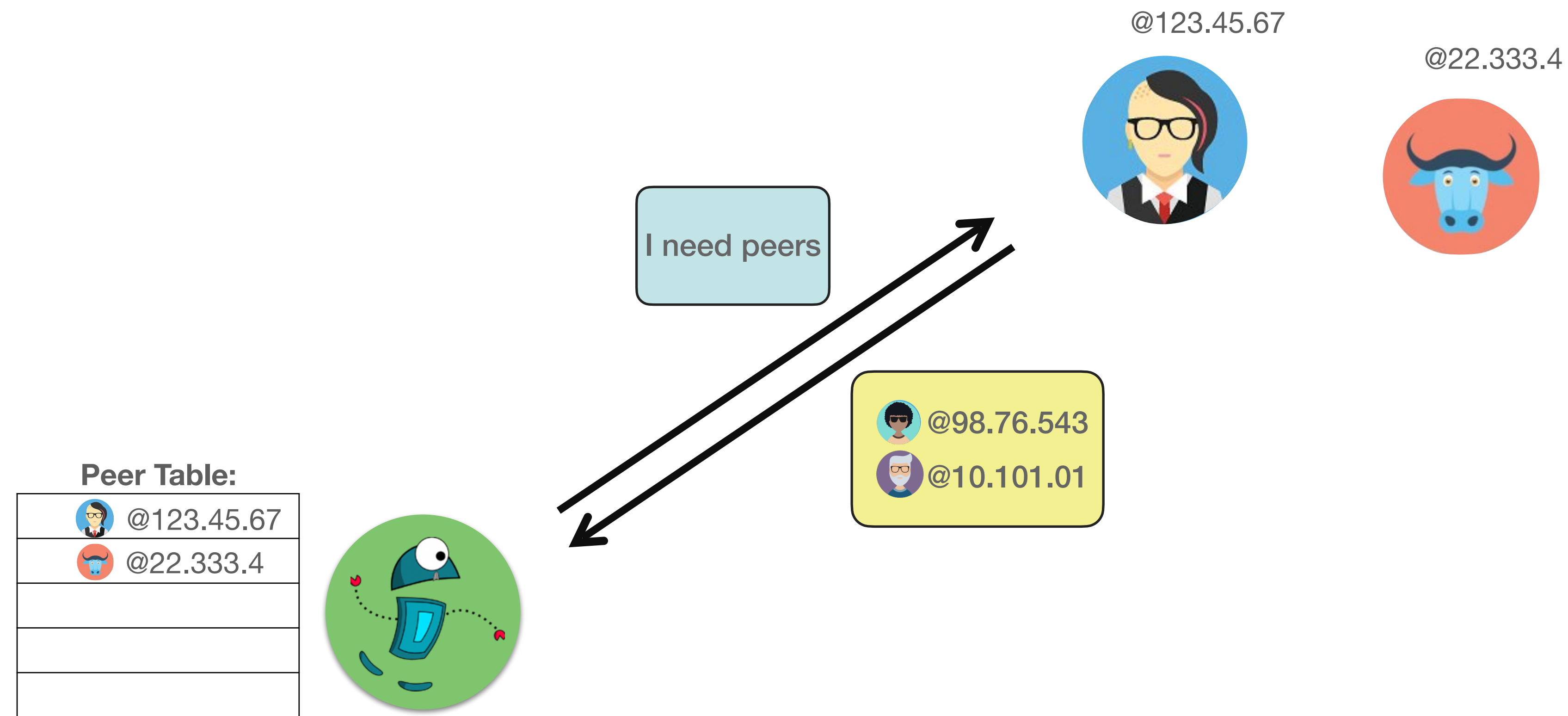
Cryptocurrencies are decentralized digital assets that do not rely on trusted third parties for the execution of transactions between parties. Decentralization is achieved through the use of distributed ledger technology to provide an append-only chronicle of all transactions between parties sending and receiving funds. The immutability of transactions is achieved through a fiscally incentivized consensus protocol publicly executed by peers participating in a peer-to-peer network [51]. The decentralized nature of cryptocurrencies provides a promise of technological amelioration to traditional payment systems [23, 27, 51, 59]. Due to the unprecedented pace of mainstream adoption and investment into these digital assets, they have attracted considerable scrutiny and research [19, 24, 26, 33, 34, 40, 47–50].

We present a measurement study of the techniques used to initially connect 74 different cryptocurrency peers to their relevant distributed peer-to-peer networks. When a new peer first joins a peer-to-peer network the action describing this initial connection is known as *bootstrapping*. By surveying the bootstrapping techniques of these cryptocurrencies we are able to uncover the following elements about their operation: the inability to resist known censorship techniques to prevent peer connectivity, the feasibility of employing censorship-resistant connection techniques, details

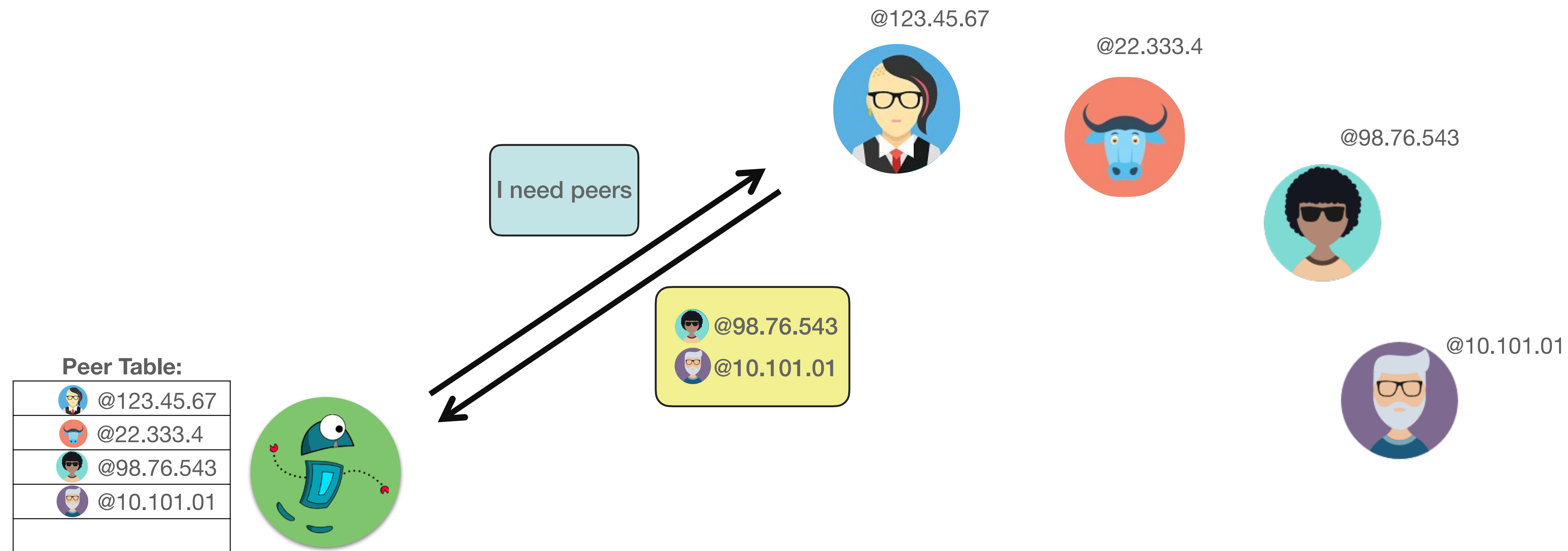
Peer Discovery Protocols



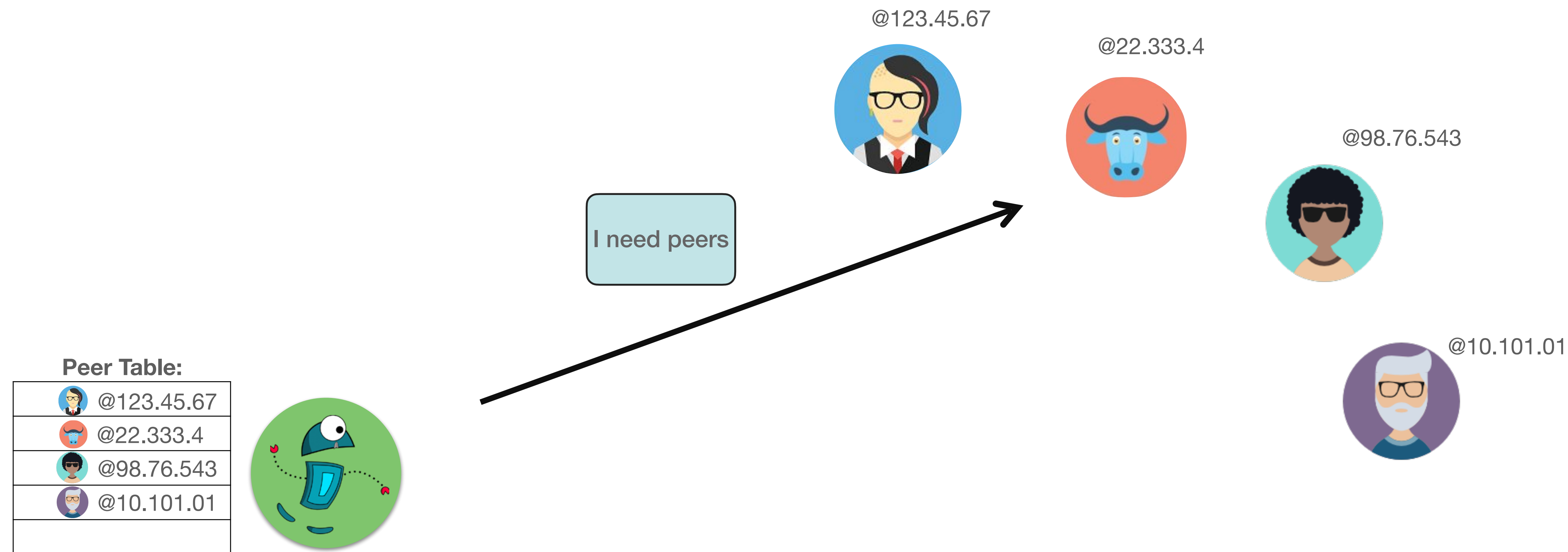
Peer Discovery Protocols



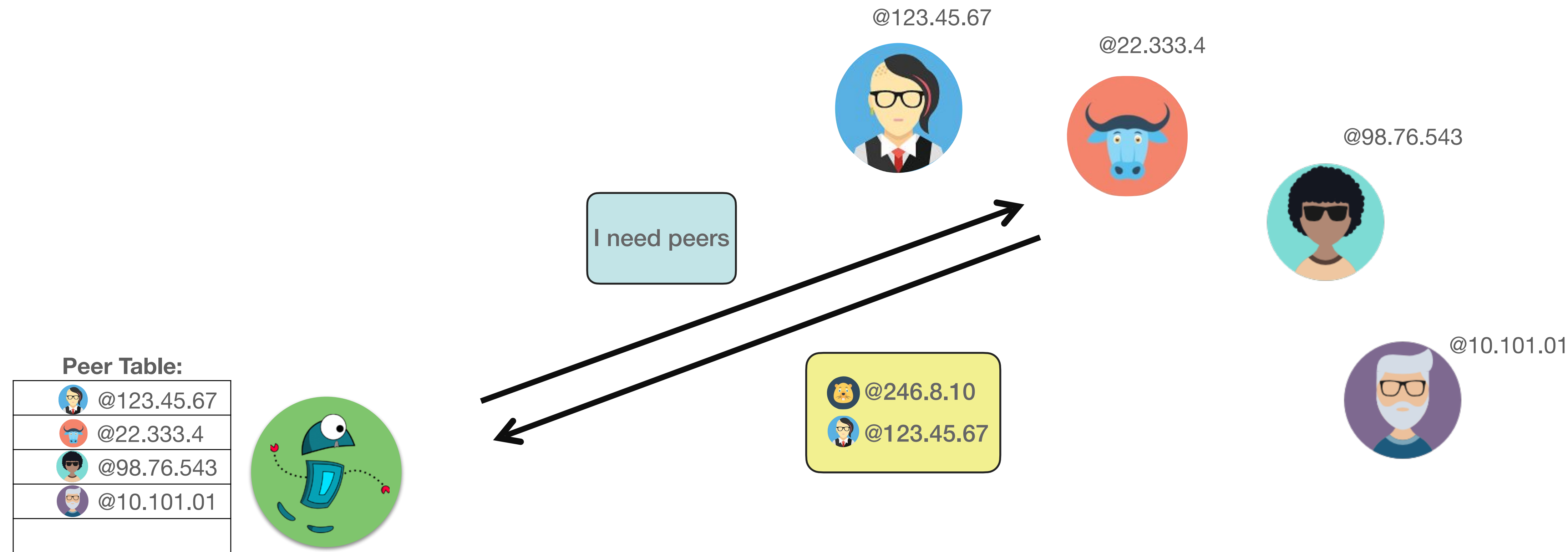
Peer Discovery Protocols



Peer Discovery Protocols



Peer Discovery Protocols



Peer Discovery Protocols

- learn about new nodes
- attack protection
(e.g., eclipsing, network partitions, etc.)
- fairness, decentralization (?)

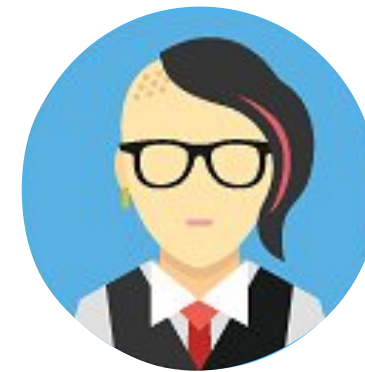
Peer Table:

	@123.45.67
	@22.333.4
	@98.76.543
	@10.101.01
	@246.8.10

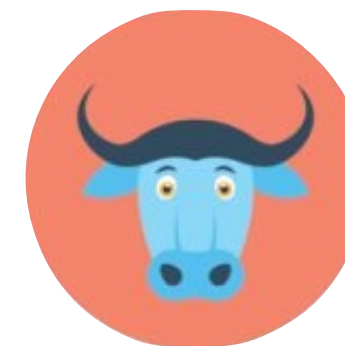


I need peers

@123.45.67



@22.333.4



@98.76.543



@10.101.01



@246.8.10

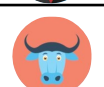
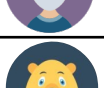


 @246.8.10
 @123.45.67

Peer Discovery Protocols

- learn about new nodes
- attack protection
(e.g., eclipsing, network partitions, etc.)
- fairness, decentralization (?)

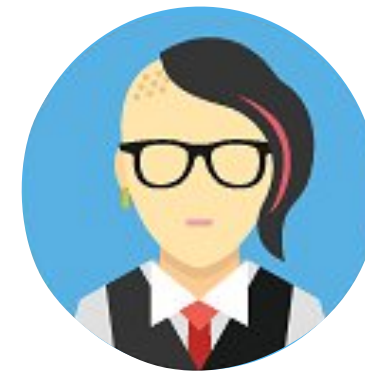
Peer Table:

	@123.45.67
	@22.333.4
	@98.76.543
	@10.101.01
	@246.8.10

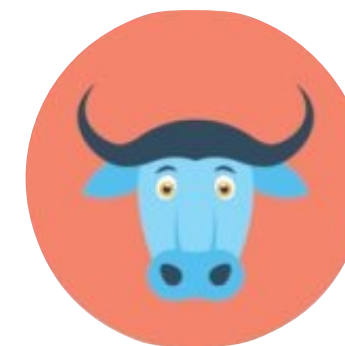


I need peers

@123.45.67



@22.333.4



@98.76.543



@10.101.01



@246.8.10



 @246.8.10
 @123.45.67

Eclipse Attacks on Bitcoin's Peer-to-Peer Network

*Ethan Heilman** *Alison Kendler** *Aviv Zohar[†]* *Sharon Goldberg**
**Boston University* *[†]Hebrew University/MSR Israel*

Abstract

used to broadcast information between bitcoin nodes (see Section 8). The bitcoin peer-to-peer network

On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin

Muoi Tran Akshaye Shenoi Min Suk Kang*
National University of Singapore National University of Singapore KAIST

Abstract

Safeguarding blockchain peer-to-peer (P2P) networks is more critical than ever in light of recent network attacks. Bitcoin has been successfully handling traditional Sybil and eclipse attacks; however, a recent Erebus attack [57] shows that effectively eclipsing a Bitcoin node is possible when the attack is combined with a network-Sybil capability; i.e., a malicious transit network can create millions or more Sybil identities. Given the immediate availability and stealthiness of the Erebus attack, Bitcoin Core has quickly implemented a few simple protocol/parameter changes to mitigate it. Our large-scale evaluations of these quick patches and three similar carefully-designed protocol tweaks confirm that, unfortu-

have been the keys to the success of cryptocurrencies and smart contracts; however, this comes with a price—they are potentially vulnerable to Sybil [15] and eclipse [51] attacks. Bitcoin [40], one of the most popular blockchain systems, has been effectively addressing Sybil and eclipse attacks. First, a Sybil attacker in Bitcoin can create many peer identities with different IP/port combinations using a single peer machine. In this way, the attacker can act like multiple peers in the system. However, the spawned Sybil identities do not cause much harm because the Bitcoin P2P protocol groups all the Sybil identities from a single IP address and contains them. Second, eclipse attacks target a specific node and manipulate the target’s peering algorithm to isolate it from the rest of the

Eclipsing Ethereum Peers with False Friends

Sebastian Henningsen Daniel Teunis Martin Florian Björn Scheuermann

Weizenbaum-Institute for the Networked Society
Humboldt-Universität zu Berlin
Berlin, Germany

Abstract—Ethereum is a decentralized Blockchain system that supports the execution of Turing-complete smart contracts. Although the security of the Ethereum ecosystem has been studied in the past, the network layer has been mostly neglected. We

v1.8.0, we only need two IP addresses from distinct /24 subnets for a successful attack. Additionally, and in contrast to [6], we do not necessarily require a restart of the victim node since peer churn is high and existing connections will

Low-Resource Eclipse Attacks on Ethereum’s Peer-to-Peer Network

Yuval Marcus^{*†}
Ethan Heilman^{*}
^{*}Boston University
[†]University of Pittsburgh

Abstract—We present eclipse attacks on Ethereum nodes that exploit the peer-to-peer network used for neighbor discovery. Our attacks can be launched using only two hosts, each with a single IP address. Our eclipse attacker monopolizes all of the victim’s incoming and outgoing connections, thus isolating the victim from the rest of its peers in the network. The attacker can then filter the victim’s view of the blockchain, or co-opt the victim’s computing power as part of more sophisticated attacks. We argue that these eclipse-attack vulnerabilities result from Ethereum’s adoption of the Kademlia peer-to-peer protocol, and present countermeasures that both harden the network against eclipse attacks and cause it to behave differently from the traditional Kademlia protocol. Several of our countermeasures have been incorporated in the Ethereum geth 1.8 client released on February 14, 2018.

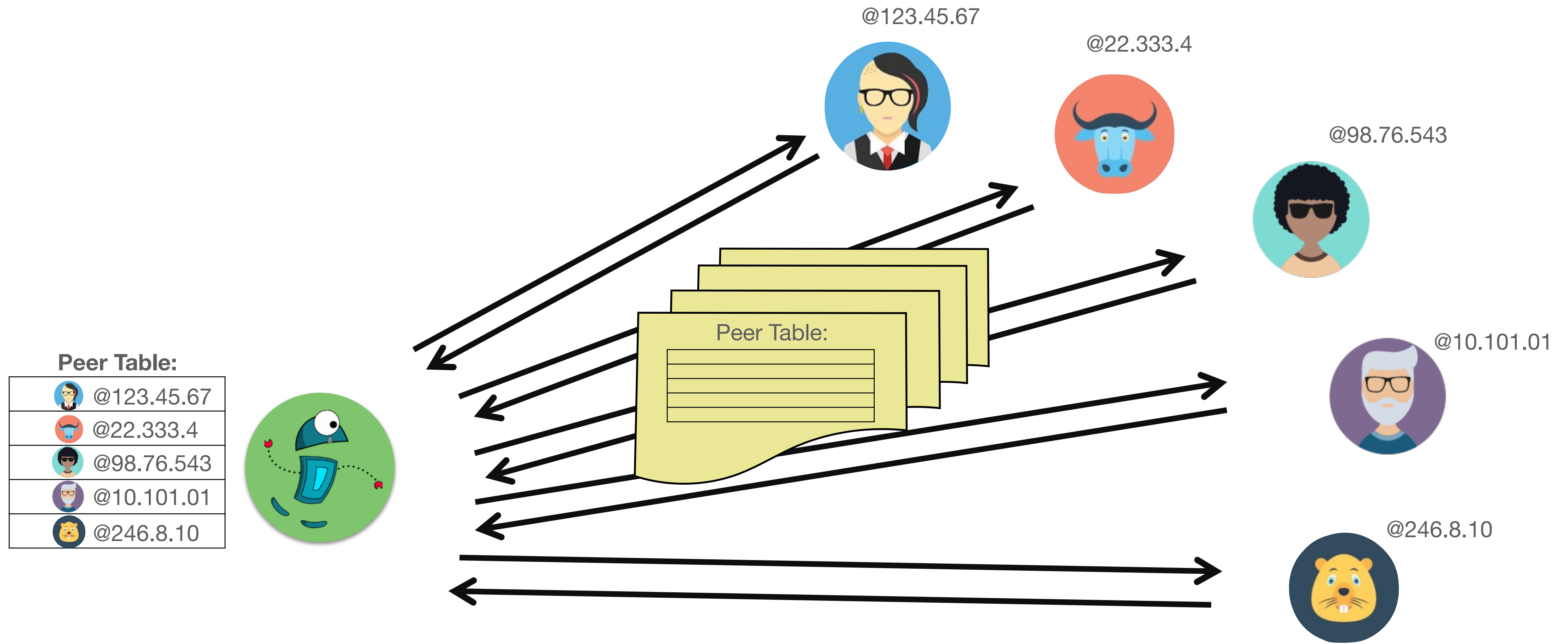
I. INTRODUCTION

The Ethereum cryptocurrency is currently second only to Bitcoin in terms of market capitalization. Ethereum has also emerged as a leading platform for raising capital

Despite the growing body of research on the security of Ethereum’s consensus algorithm [21], [25], [26], [42] and scripting language [18], [30], the properties of Ethereum’s peer-to-peer network have been largely unexplored. Nevertheless, a recent line of work [21], [37], [23], [22] has made it clear that the security properties of a proof-of-work blockchain rests on the security of its underlying peer-to-peer network. Simply put, if the peer-to-peer network partitions, causing different nodes see different views of the blockchain, then how can these nodes actually come to a consensus about what the blockchain actually is?

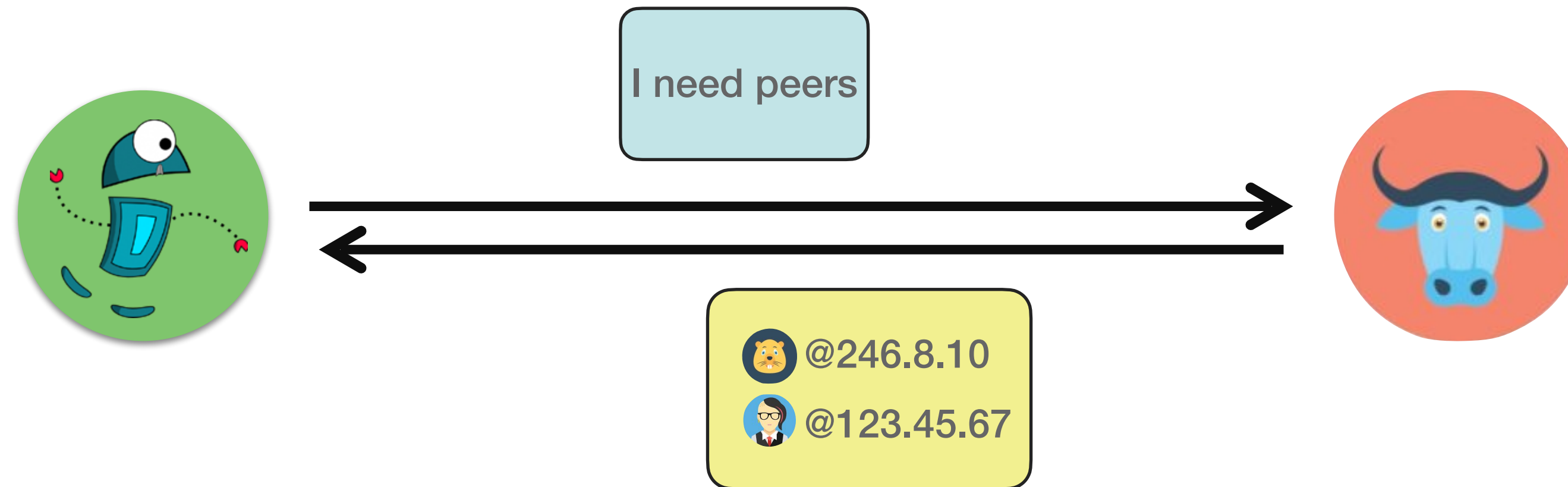
In [23], Heilman *et al.* highlighted these risks by demonstrating the first *eclipse attacks* on Bitcoin’s peer-to-peer network. In an eclipse attack, the attacker completely controls its victim’s access to information, and thus filter the victim’s view of the blockchain, or co-opt the victim’s computing power as part of more sophisti-

Peer Discovery Protocols



Crawler: learn about all nodes in the network

Peer Discovery Messages



(i) All current active peer connections



(ii) Random sampling of peer table



(iii) DHT query response

Peer Discovery Messages



- (i) All current active peer connections
- (ii) Random sampling of peer table
- (iii) DHT query response

Kademlia: A Peer-to-Peer Information System Based on the XOR Metric^{*}

Petar Maymounkov and David Mazières

New York University
{petar,dm}@cs.nyu.edu
<http://kademlia.scs.cs.nyu.edu>

Abstract. We describe a peer-to-peer distributed hash table with provable consistency and performance in a fault-prone environment. Our system routes queries and locates nodes using a novel XOR-based metric topology that simplifies the algorithm and facilitates our proof. The topology has the property that every message exchanged conveys or reinforces useful contact information. The system exploits this information to send parallel, asynchronous query messages that tolerate node failures without imposing timeout delays on users.

1 Introduction

This paper describes Kademlia, a peer-to-peer distributed hash table (DHT). Kademlia has a number of desirable features not simultaneously offered by any previous DHT. It minimizes the number of configuration messages nodes must send to learn about each other. Configuration information spreads automatically

Peer Discovery Messages

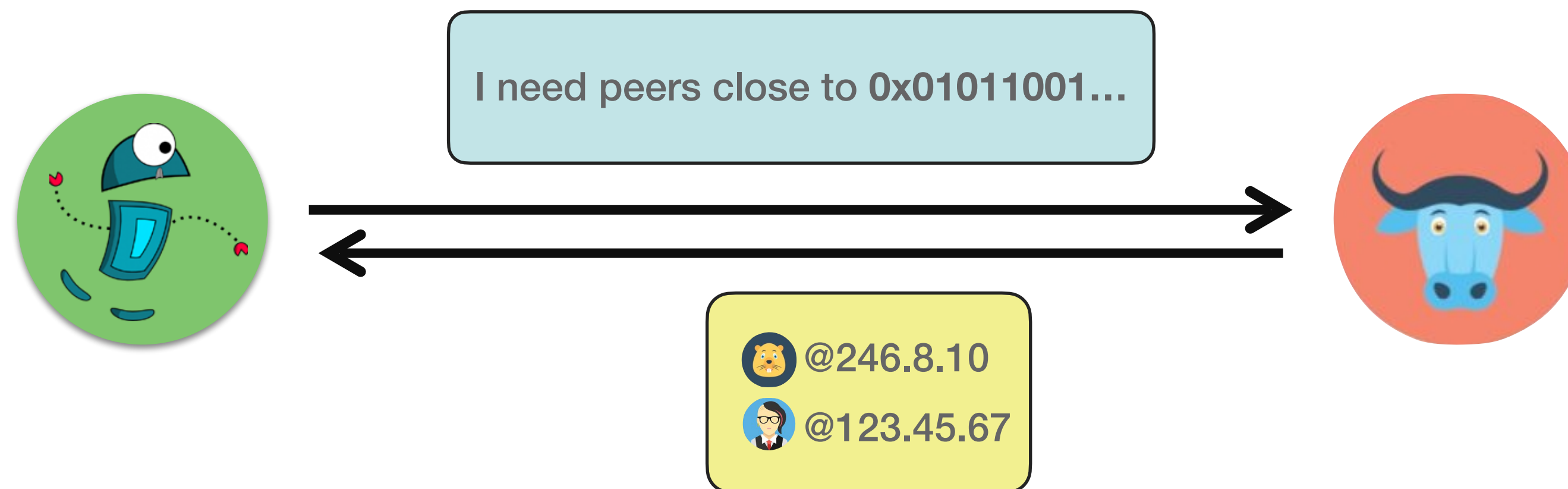
(i) All current active peer connections



(ii) Random sampling of peer table



(iii) DHT query response



Crawler methodology

(i) All current active peer connections



(ii) Random sampling of peer table



(iii) DHT query response



Full network crawl every 24hrs:

for each new node we learn about, ask for peers

Crawler methodology



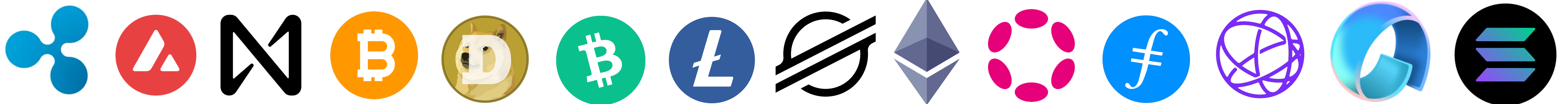
Full network crawl every 24hrs:

for each new node we learn about, ask for peers



Hourly connectivity checks:

send an in-protocol PING and TCP PING to all nodes



Crawler Results

Market Cap (12/24)		active IPs	discovered IPs	A/D ratio
\$1937.1B	Bitcoin	11309	257019	0.04
\$462.8B	Ethereum (discv4)	33318	57806	0.57
	Ethereum (discv5)	21685	80797	0.27
\$131.3B	Ripple	404	891	0.45
\$111.2B	Solana	3693	4589	0.81
\$62.8B	Dogecoin	695	14945	0.05
\$20.7B	Avalanche	1581	5290	0.28
\$15.6B	Polkadot	9151	9386	0.97
\$14.0B	Stellar	182	1118	0.16
\$11.9B	Bitcoin Cash (*)	725	27328	0.03
\$10.0B	Litecoin	952	28063	0.03
\$9.4B	Near	435	777	0.54
\$3.2B	Filecoin	411	417	0.99
\$2.5B	Celestia	138	144	0.96
\$0.19B	Avail	2224	2244	0.99

- **Bitcoin-based networks store a lot of noise in their peer tables (both old information and unreachable nodes)**

Crawler Results

Market Cap (12/24)		active IPs	discovered IPs	A/D ratio
\$1937.1B	Bitcoin	11309	257019	0.04
\$462.8B	Ethereum (discv4)	33318	57806	0.57
	Ethereum (discv5)	21685	80797	0.27
\$131.3B	Ripple	404	891	0.45
\$111.2B	Solana	3693	4589	0.81
\$62.8B	Dogecoin	695	14945	0.05
\$20.7B	Avalanche	1581	5290	0.28
\$15.6B	Polkadot	9151	9386	0.97
\$14.0B	Stellar	182	1118	0.16
\$11.9B	Bitcoin Cash (*)	725	27328	0.03
\$10.0B	Litecoin	952	28063	0.03
\$9.4B	Near	435	777	0.54
\$3.2B	Filecoin	411	417	0.99
\$2.5B	Celestia	138	144	0.96
\$0.19B	Avail	2224	2244	0.99

- **Bitcoin-based networks store a lot of noise in their peer tables (both old information and unreachable nodes)**
- **DHT-based networks seem to be doing better**

Crawler Results

Market Cap (12/24)		active IPs	discovered IPs	A/D ratio	prop. IPv4	prop. IPv6
\$1937.1B	Bitcoin	11309	257019	0.04	0.85	0.15
\$462.8B	Ethereum (discv4)	33318	57806	0.57	1.00	0.00
	Ethereum (discv5)	21685	80797	0.27	0.94	0.06
\$131.3B	Ripple	404	891	0.45	1.00	0.00
\$111.2B	Solana	3693	4589	0.81	1.00	0.00
\$62.8B	Dogecoin	695	14945	0.05	0.82	0.18
\$20.7B	Avalanche	1581	5290	0.28	1.00	0.00
\$15.6B	Polkadot	9151	9386	0.97	0.80	0.20
\$14.0B	Stellar	182	1118	0.16	1.00	0.00
\$11.9B	Bitcoin Cash (*)	725	27328	0.03	0.81	0.19
\$10.0B	Litecoin	952	28063	0.03	0.80	0.20
\$9.4B	Near	435	777	0.54	1.00	0.00
\$3.2B	Filecoin	411	417	0.99	0.92	0.08
\$2.5B	Celestia	138	144	0.96	0.84	0.16
\$0.19B	Avail	2224	2244	0.99	0.89	0.11

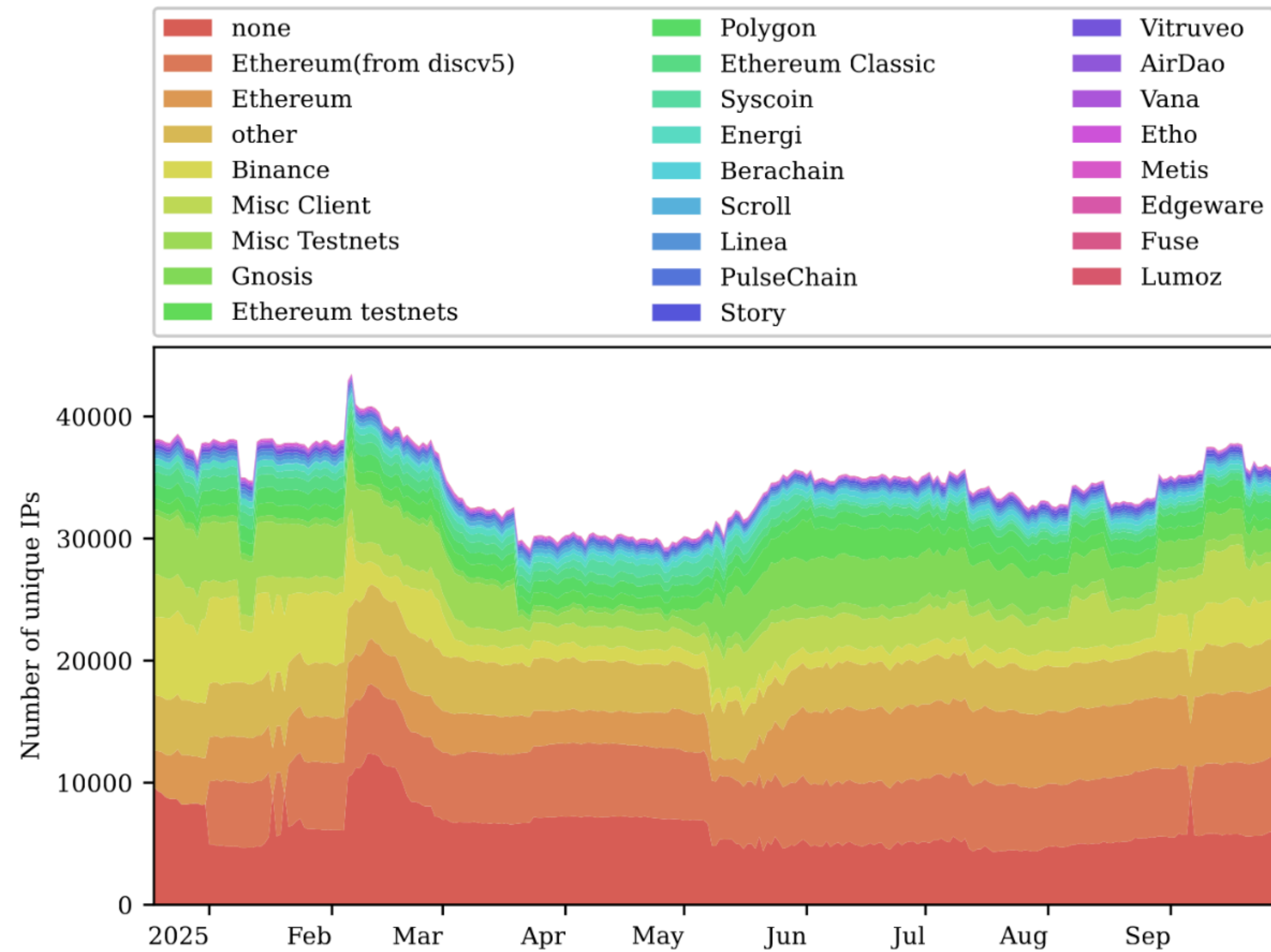
- Cryptocurrency networks are largely, if not entirely, run over IPv4

Not all discovery layers are unique

Ethereum (discv4)

+19 networks

Protocol	Market Cap (12/24)	Network Size
Ethereum	\$462.8B	9,203
Binance	\$103.3B	1,299
Gnosis	\$696M	1,774
Polygon	\$1.4B	1,129
ETH Classic	\$5.3B	716
Syscoin	\$91.4M	578
Energi	\$4.83M	475
Scroll	\$227M	249
Linea	\$391M	233
Berachain	\$257M	347
Pulsechain	\$843M	209
Story	\$1.29B	156
AirDao	\$26.0M	111
Vitruveo	\$4.60M	191
Etho	\$0.93M	61
Vana	\$514M	73
Metis	\$283M	72
Edgeware	0	36
Fuse	\$6.65M	21
Lumoz	\$17.4M	6
other	X	3,935
misc client	X	2,540
none	X	5,719

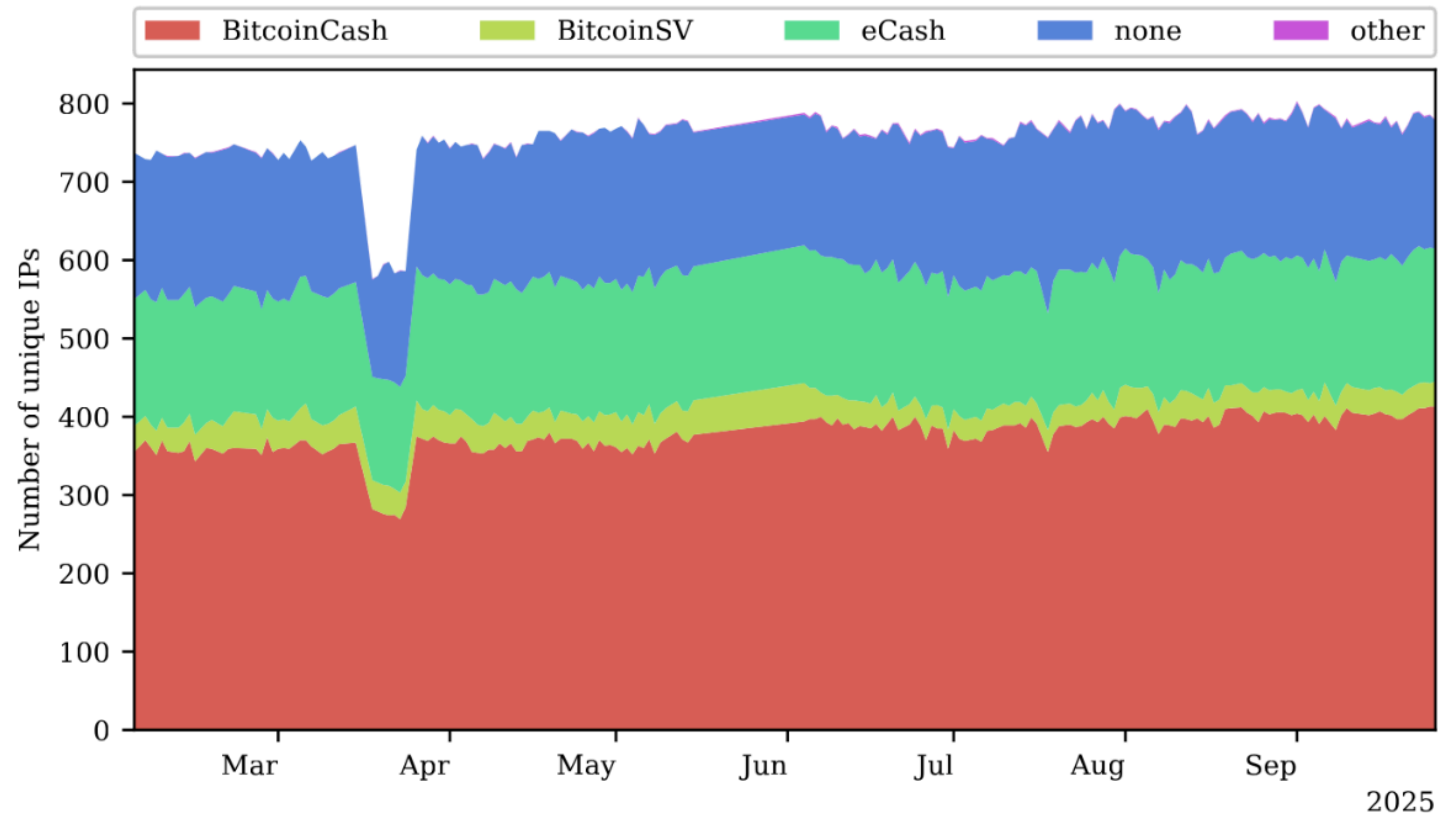


- The Majority of nodes in the discv4 peer tables are not running in the main Ethereum network

Bitcoin Cash-SV

+2 networks

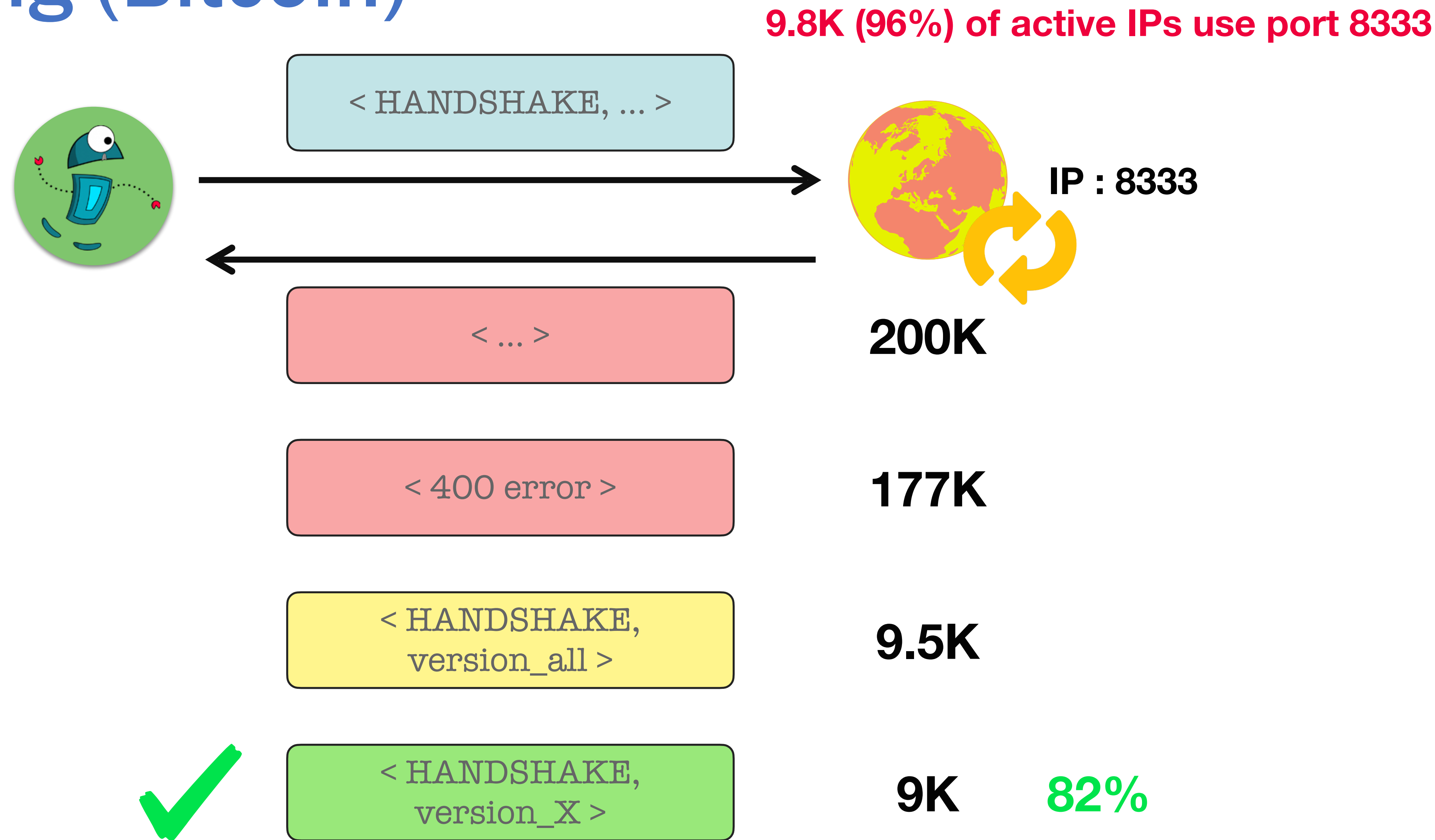
Protocol	Market Cap (12/24)	Network Size (IPv4/IPv6)
BitcoinCash	\$11.9B	289/89
BitcoinSV	\$1.6B	28/4
eCash	\$0.73B	133/36
none	X	155/24
other	X	1/0



- Bitcoin-based clients use a network MAGIC number to differentiate messages
- BitcoinSV and eCash when they forked from BitcoinCash did not change their MAGIC number. We use handshake VERSION messages to differentiate them.

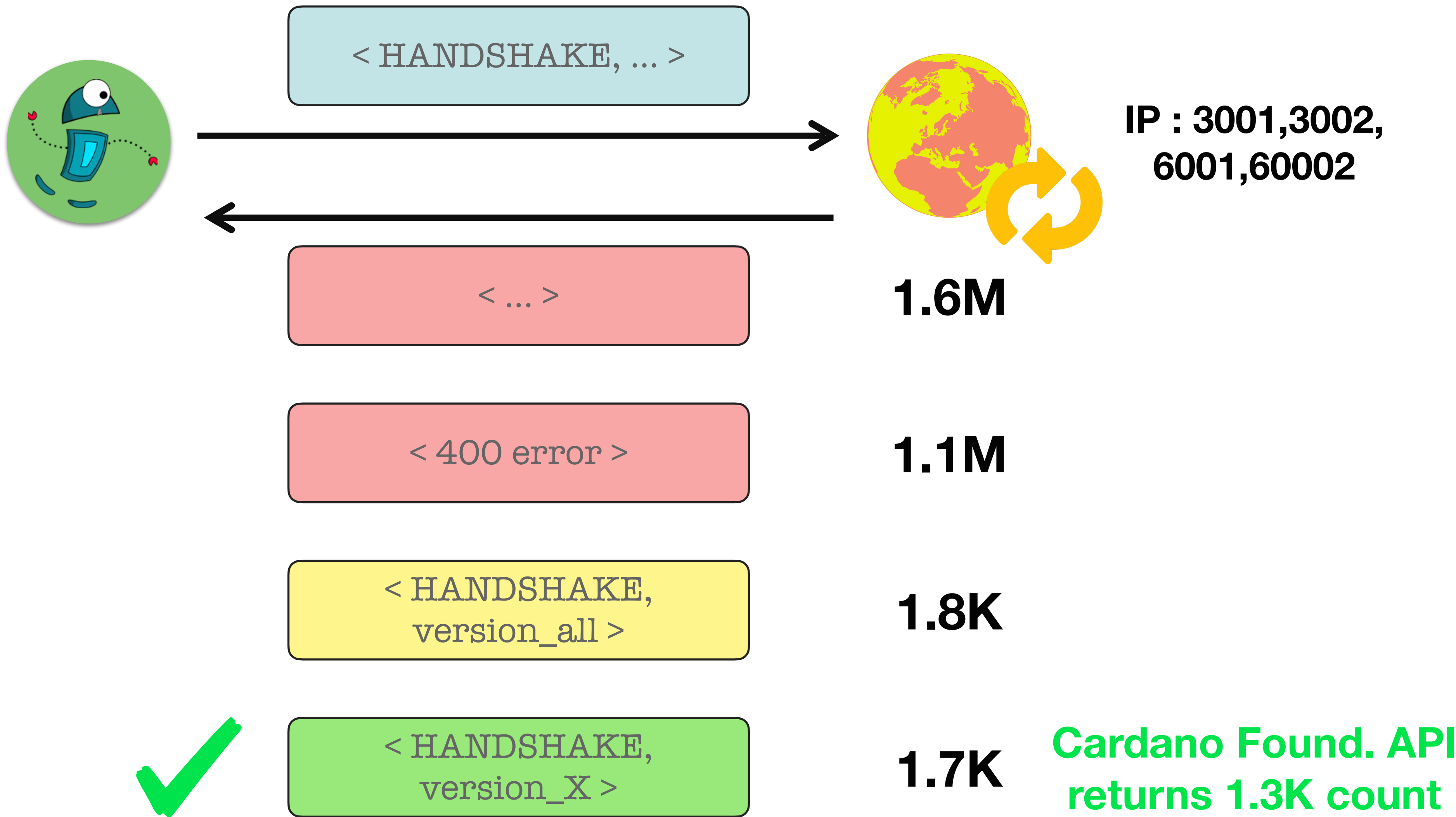
Can we use IPv4 scans to detect nodes?

IP Scanning (Bitcoin)

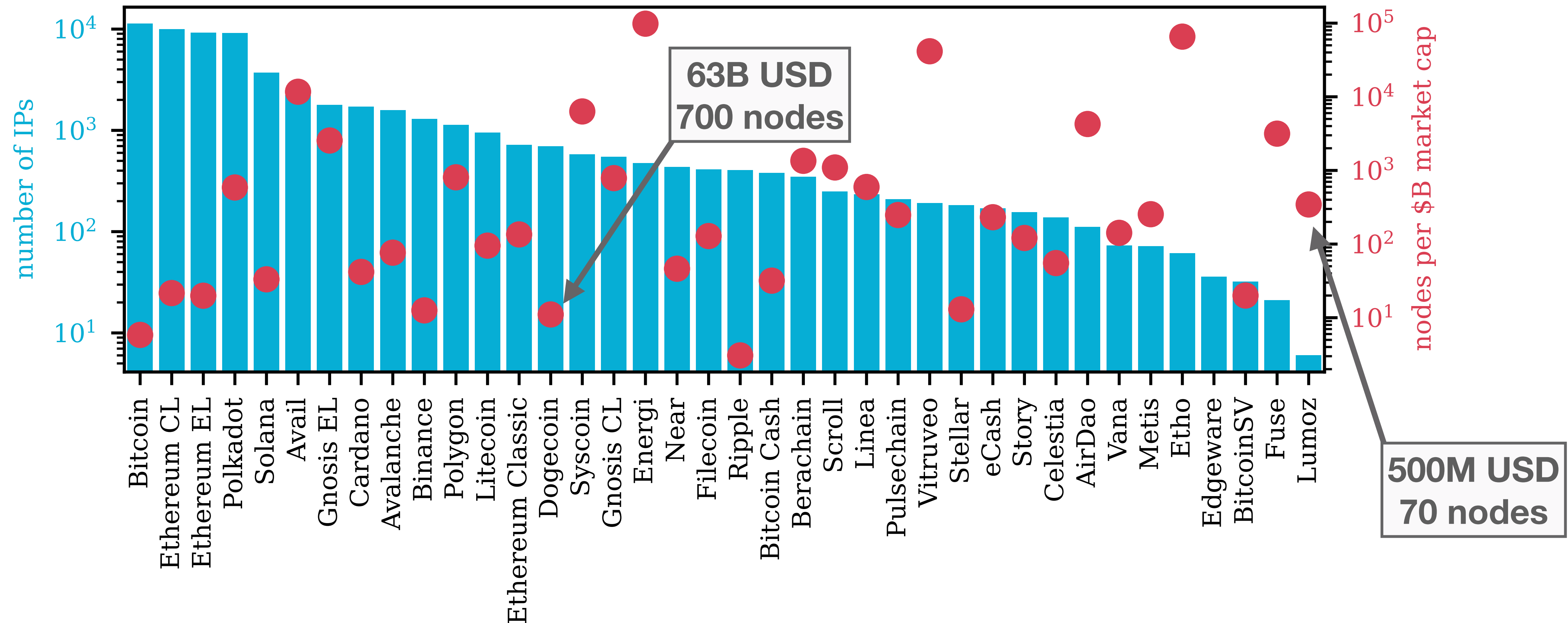


IP Scanning (Cardano)

+1 network

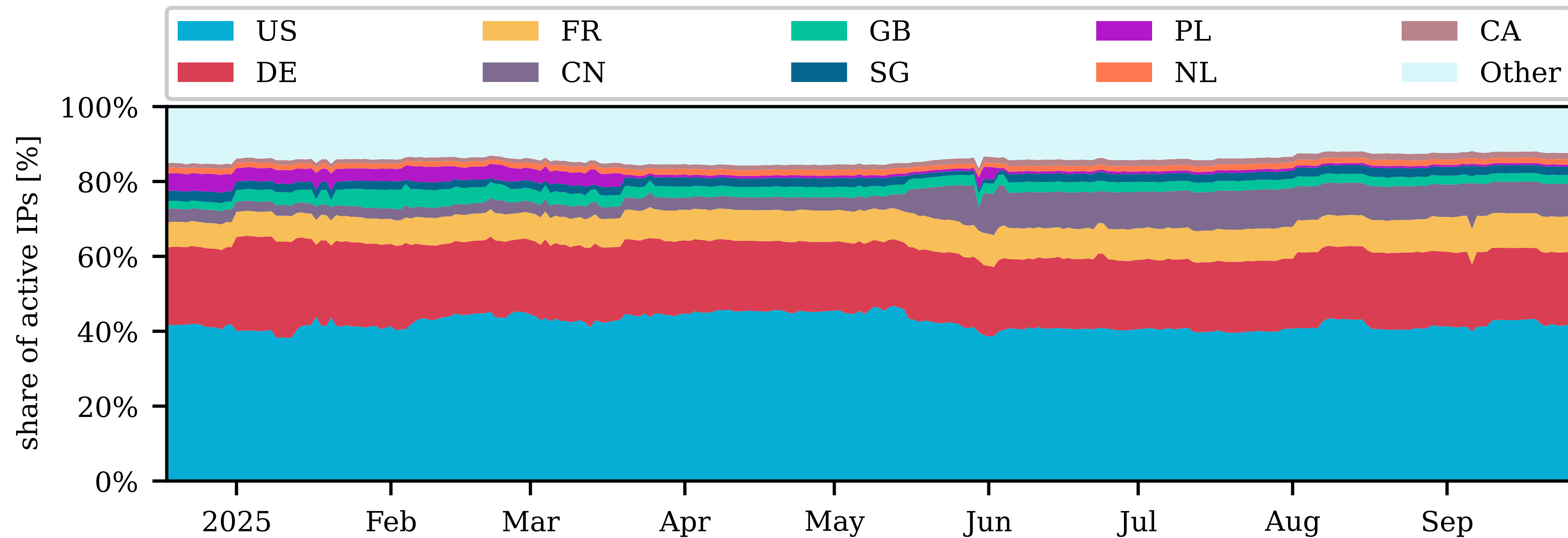


Size of 36 blockchain networks



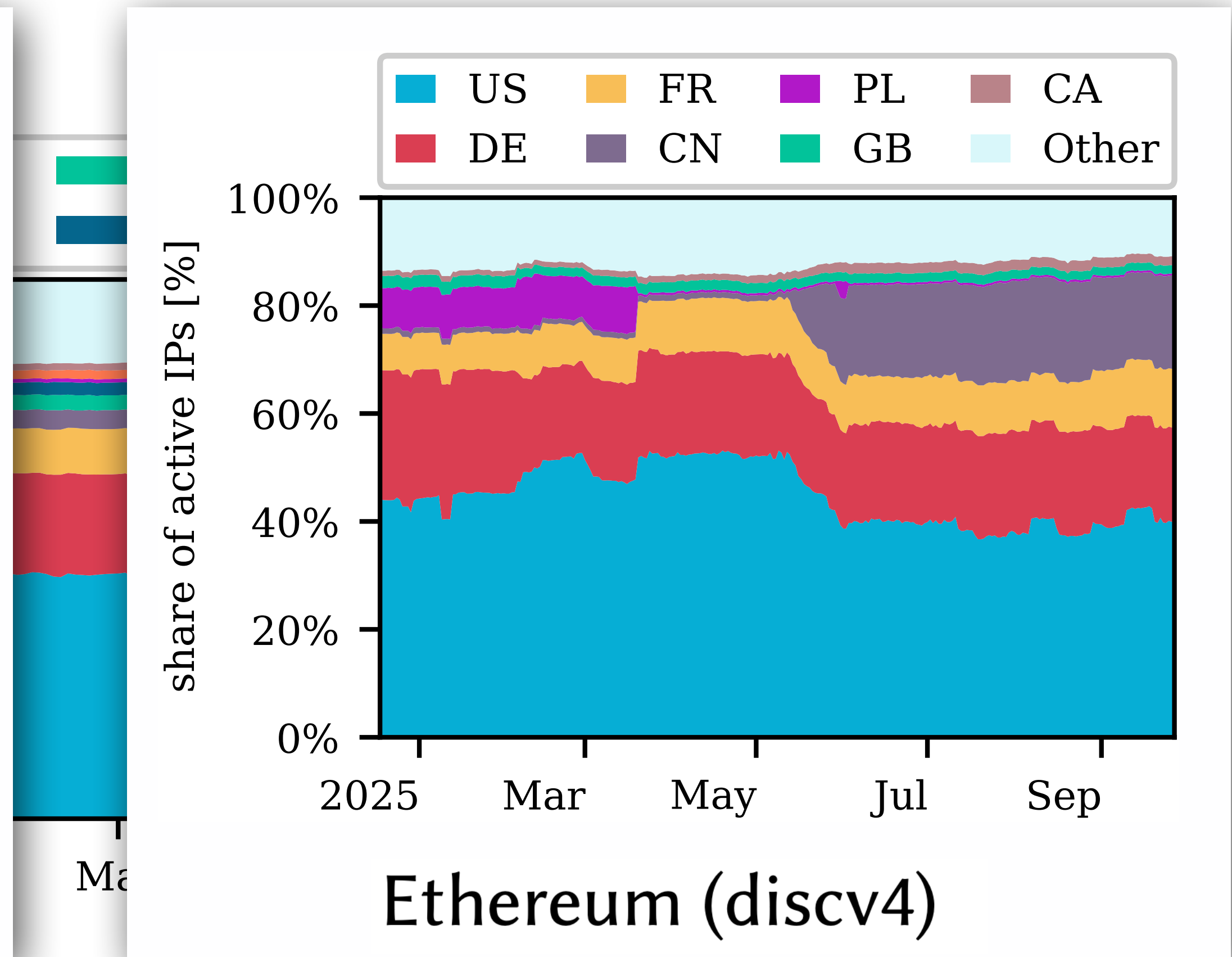
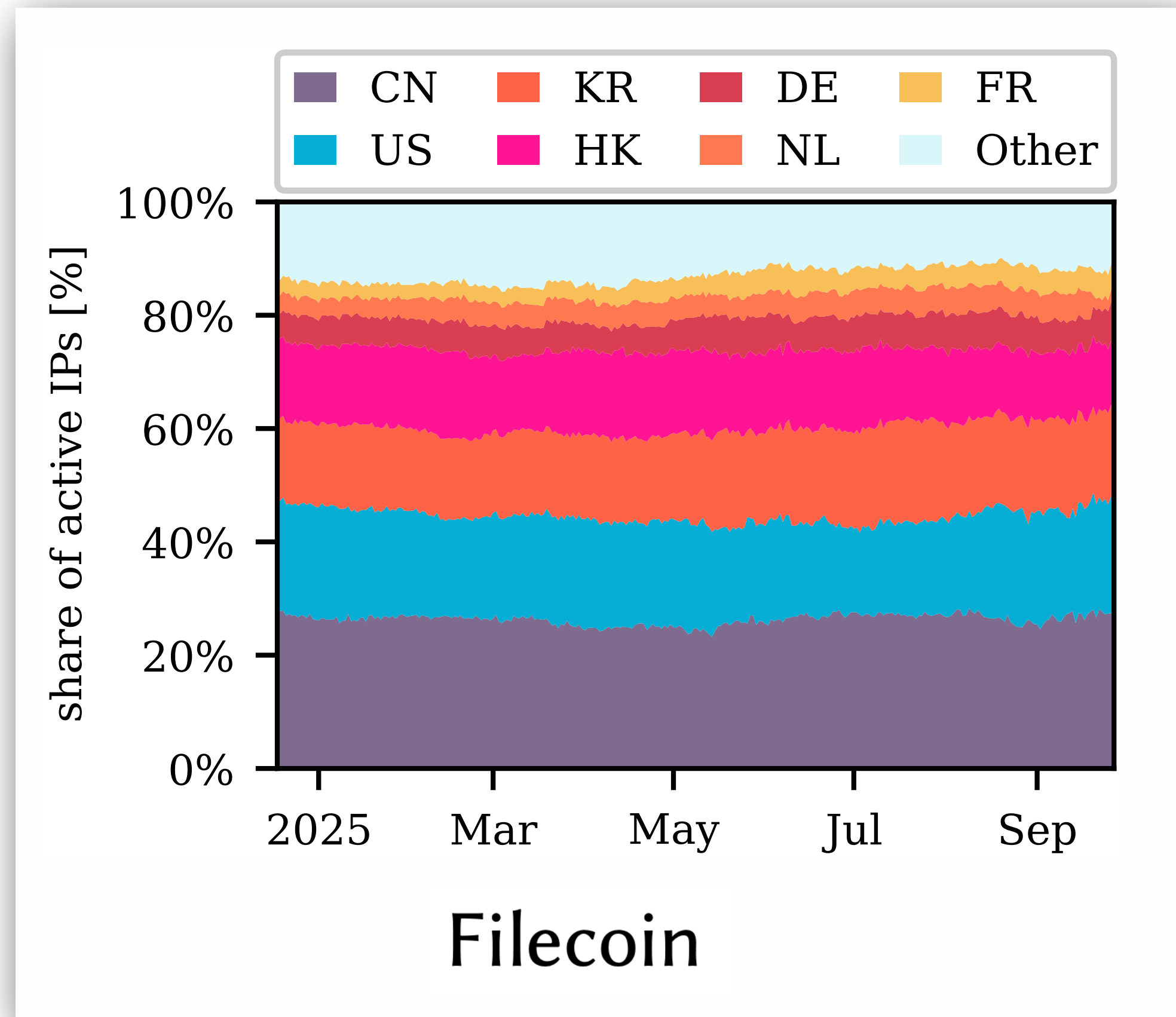
- Huge variance in network sizes, with some small networks securing ecosystems with large market caps

Country Breakdown



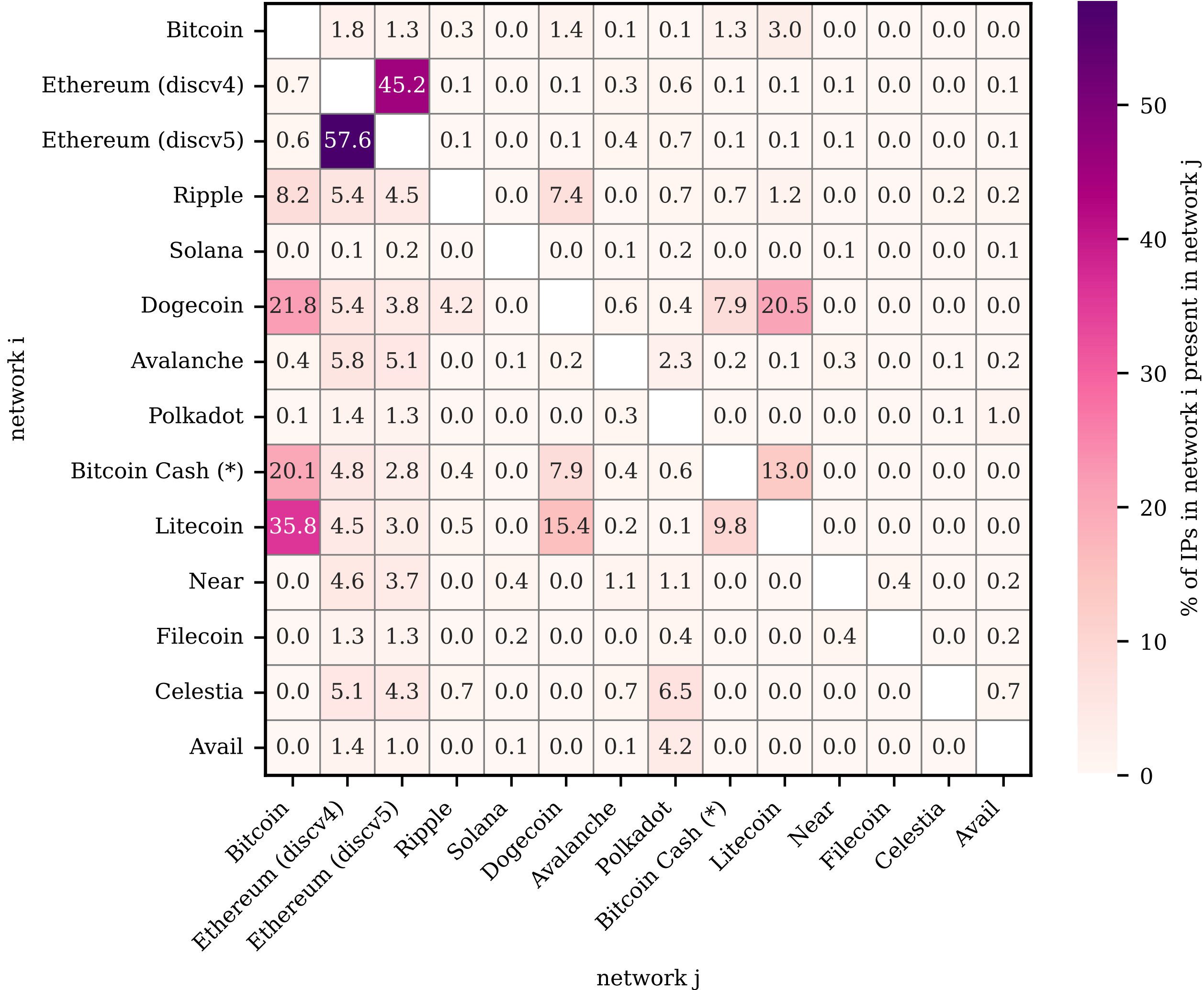
- **Cryptocurrency networks are largely run from N. America (47%) and Europe (41%) with 11% in Asia, and less than 2% in all others.**

Country Breakdown



- **Cryptocurrency networks are largely run from N. America (47%) and Europe (41%) with 11% in Asia, and less than 2% in all others.**

IP Overlap



Summary

- Developed custom crawlers, protocol-specific discovery breakdowns, and Internet-wide scanning techniques to measure **36 blockchain networks**.
- Built a **longitudinal dataset** with continuous measurements since December 2024.
- Found major differences in **network size, reachability, churn, discovery coverage, and decentralization** across ecosystems.
- Released an **open-source** measurement framework and **live observatory** for continuous monitoring.



Overview

Filter networks...

- Bitcoin
- Ethereum (discv4)
- Ethereum (discv5)
- Dogecoin
- Avalanche
- Polkadot
- Stellar
- Bitcoin Cash (*)
- Litecoin
- Near
- Filecoin
- Celestia
- Avail

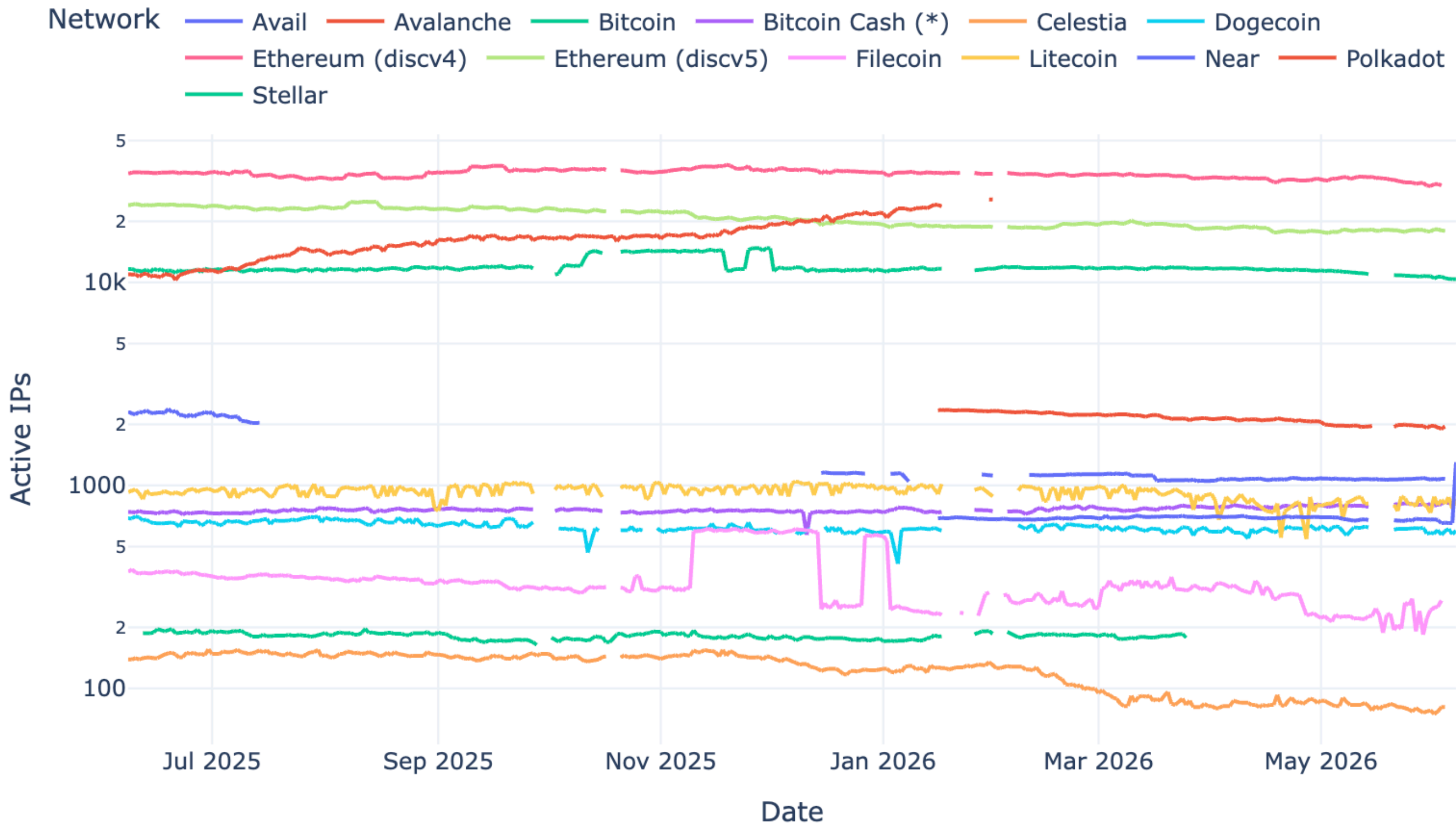
Aggregate Network Metrics

Longitudinal analysis of 13 public blockchains (Dec 2024 - Present).

Daily Active Nodes

Daily count of active nodes per blockchain network. Data gaps reflect days with missing observations.

1m 6m 1y Max Custom



On this page

- Daily Active Nodes
- Market Concentration (ASN)
- Network Overlap
- Day-to-Day IP Retention
- Geographic Distribution



Overview



Bitcoin



Ethereum (discv4)



Ethereum (discv5)



Dogecoin



Avalanche



Polkadot



Stellar



Bitcoin Cash (*)



Litecoin



Near



Filecoin



Celestia



Avail

Amazon.com, Inc.

0

10

20

30

0

50

100

Median Nodes

ASN Rank

Global Node Distribution

Geographic distribution of active nodes.

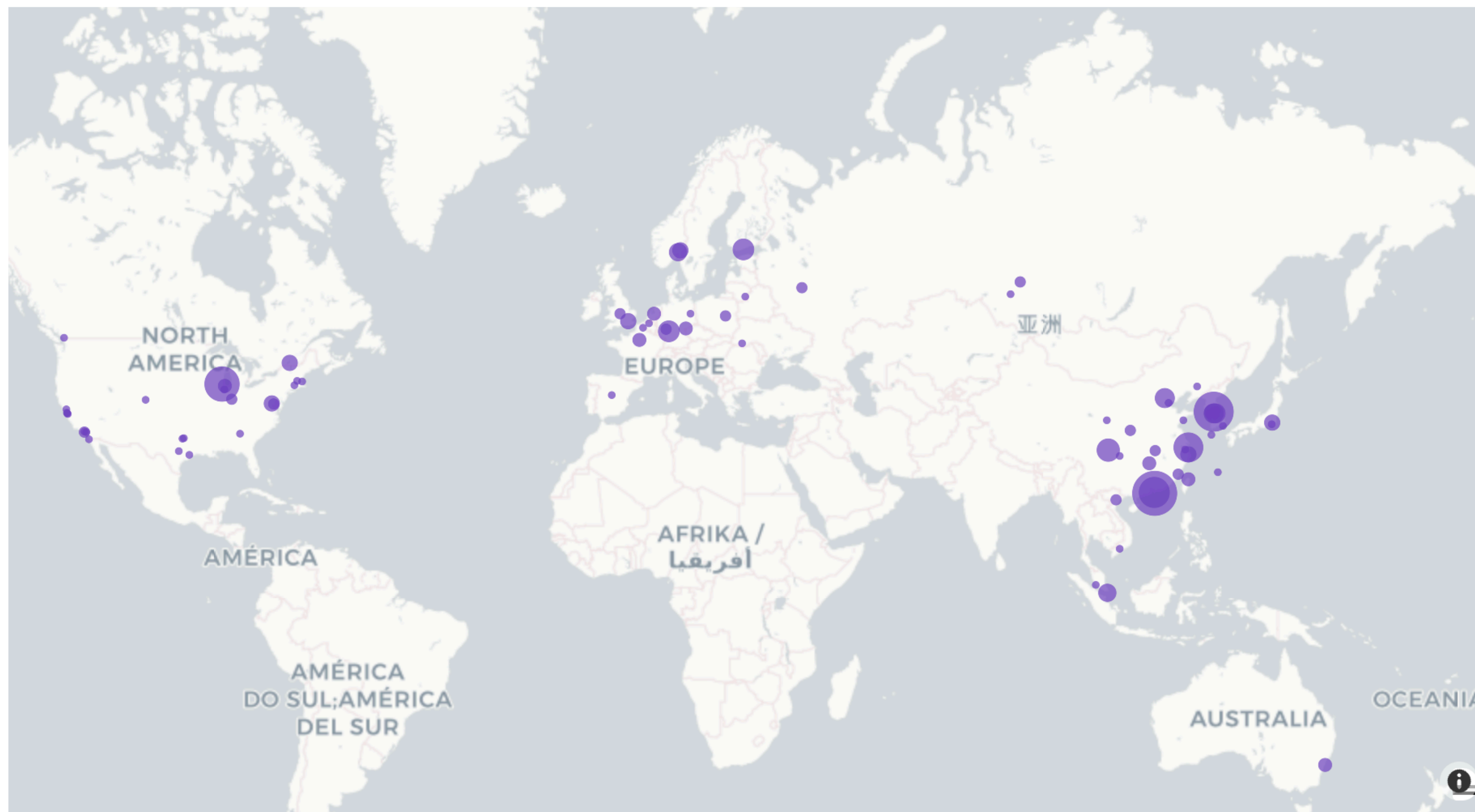
1m

6m

1y

Max

Custom



On this page

[Network Activity](#)

[Network Churn](#)

[Hosting Distribution](#)

[IPv6 Adoption](#)

[ASN Centralization](#)

[Global Node Distribution](#)

For more analysis checkout:



p2pobservatory.networks.imdea.org
probelab.io