CID Eclipse attack and mitigation in IPFS

Srivatsan Sridhar
Stanford University

Navin Keizer
UCL

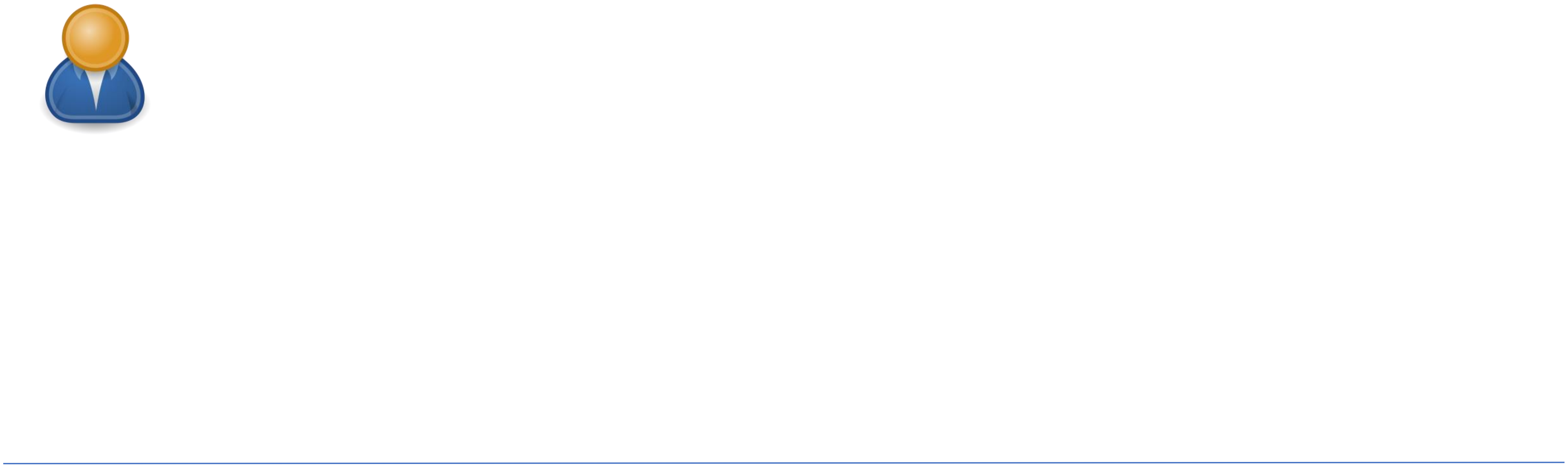
Onur Ascigil
Lancaster University

Etienne Riviere
UCLouvain

Yiannis Psaras
Protocol Labs

Michał Król
City, University
of London

Distributed Hash Table

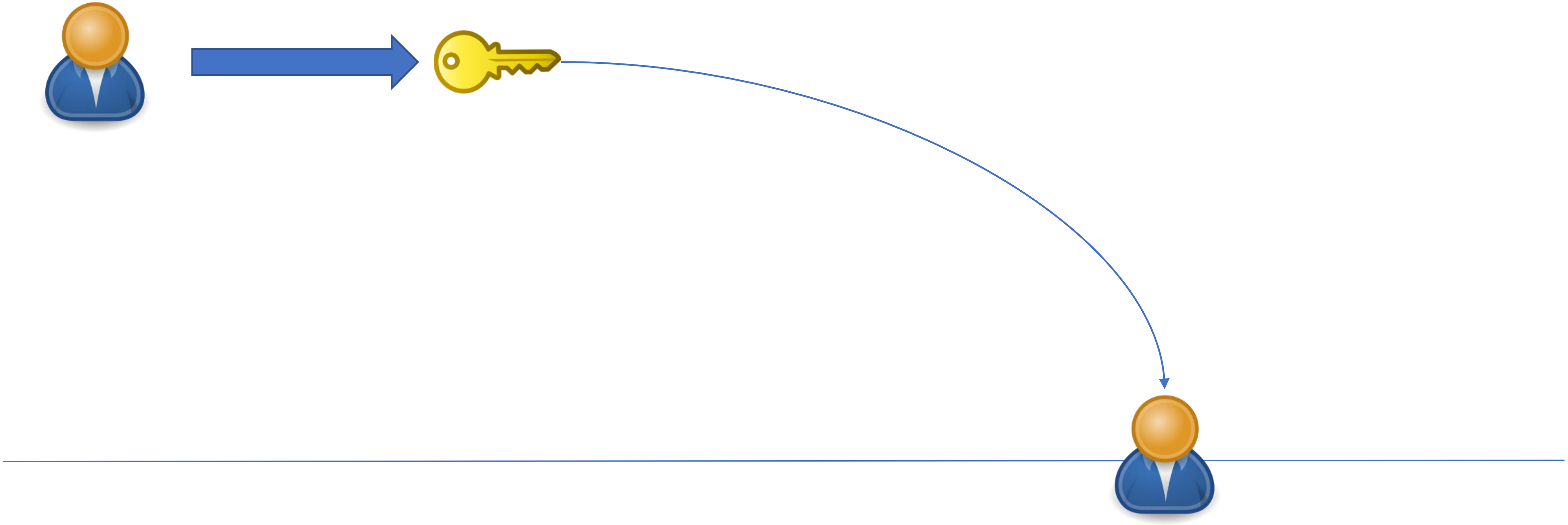


sha256 hash space

Distributed Hash Table

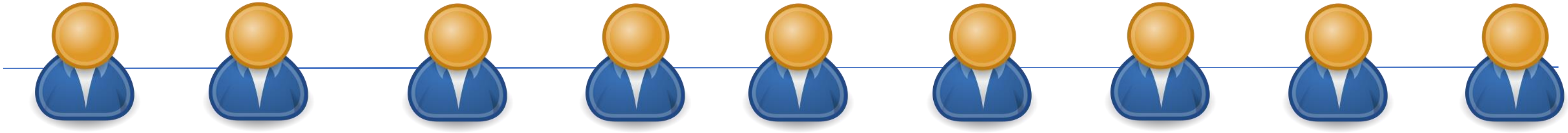
sha256 hash space

Distributed Hash Table



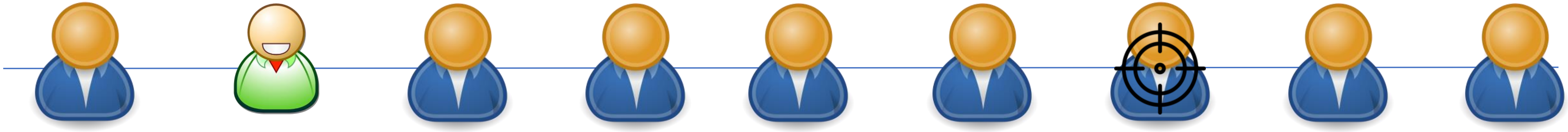
sha256 hash space

Distributed Hash Table



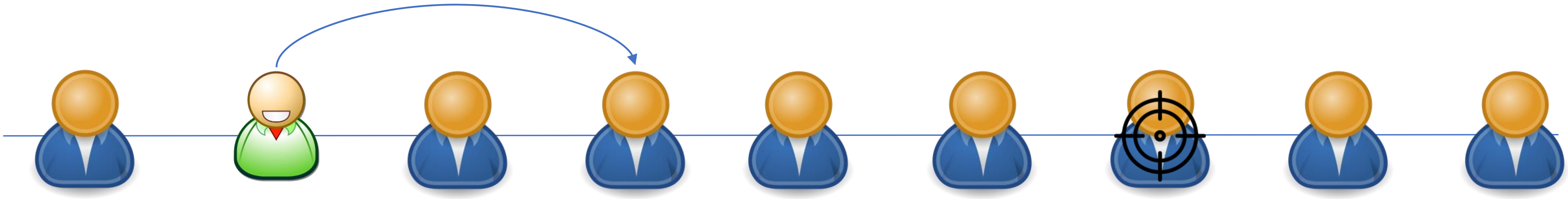
sha256 hash space

Distributed Hash Table



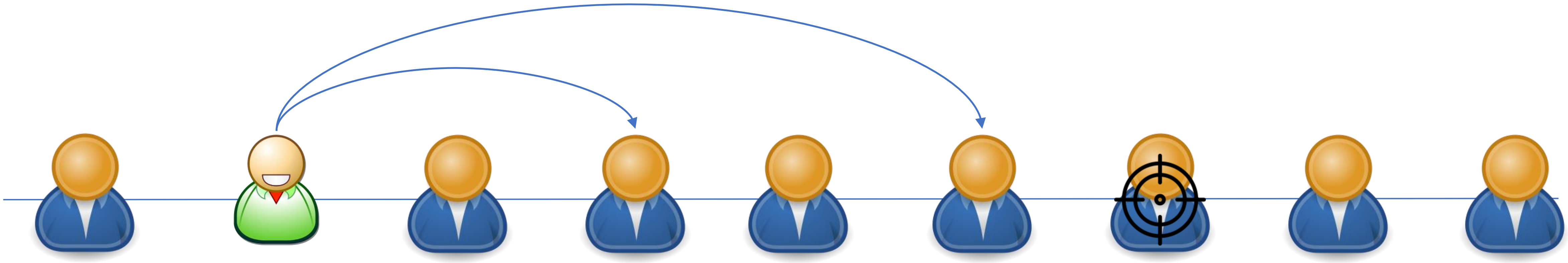
sha256 hash space

Distributed Hash Table



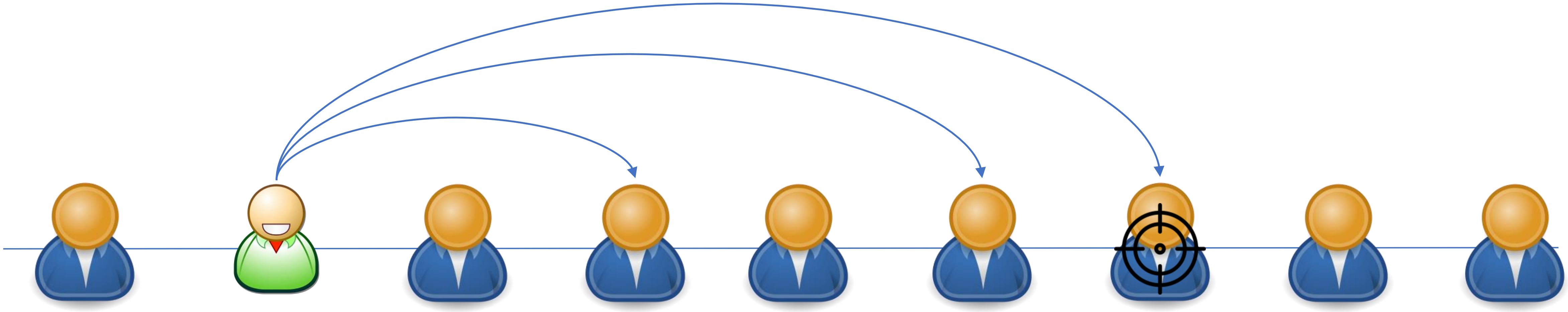
sha256 hash space

Distributed Hash Table



sha256 hash space

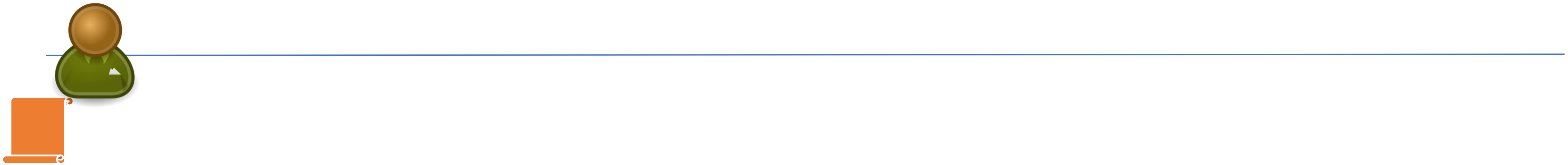
Distributed Hash Table



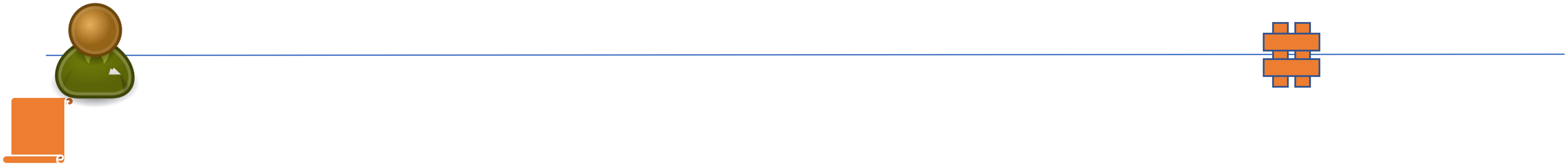
sha256 hash space

DHT-based resolution

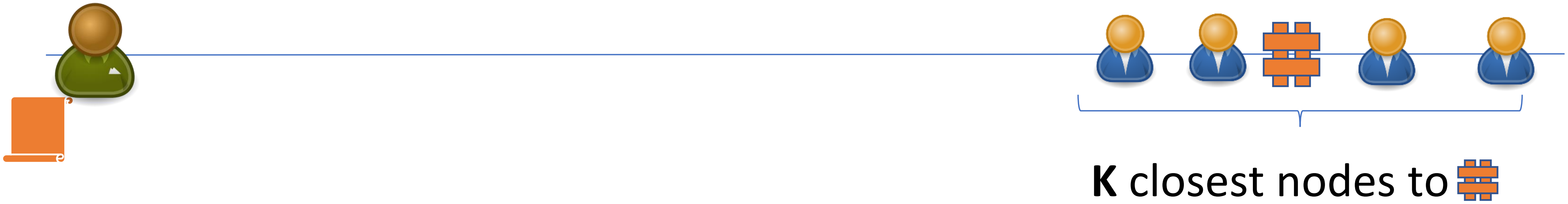
Add provider



Add provider

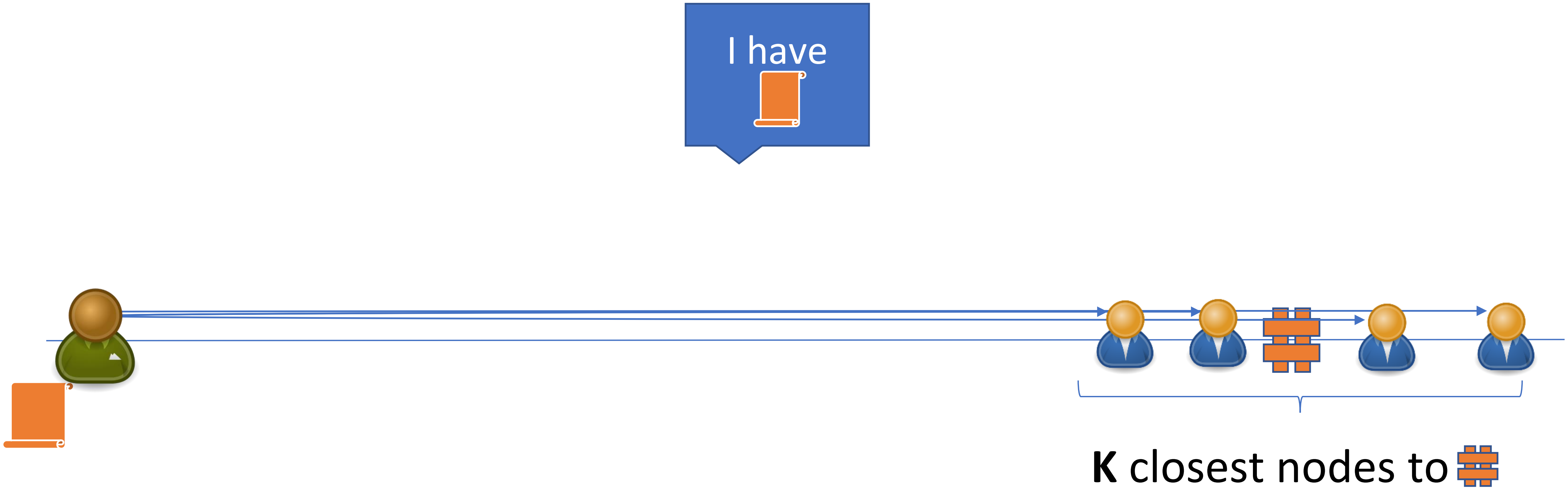


Add provider

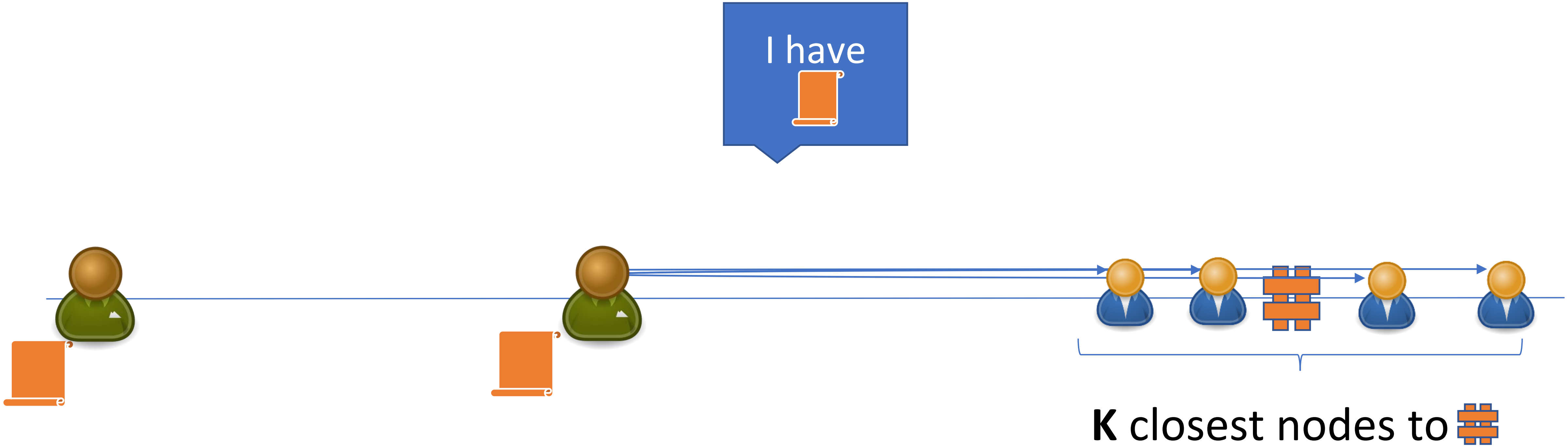


K closest nodes to #

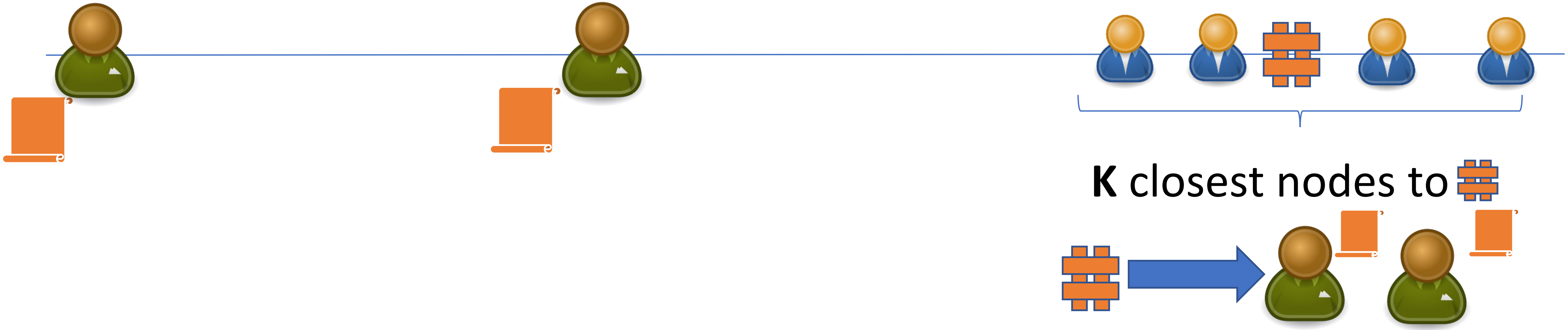
Add provider



DHT Resolution

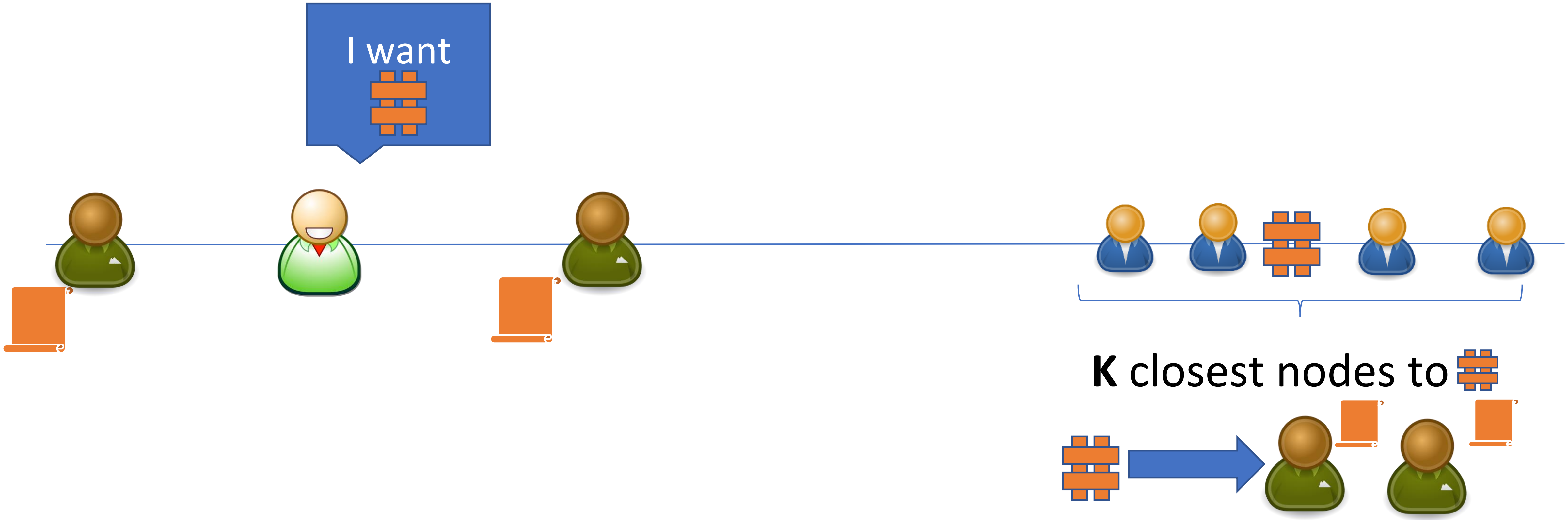


DHT Resolution



K closest nodes to #

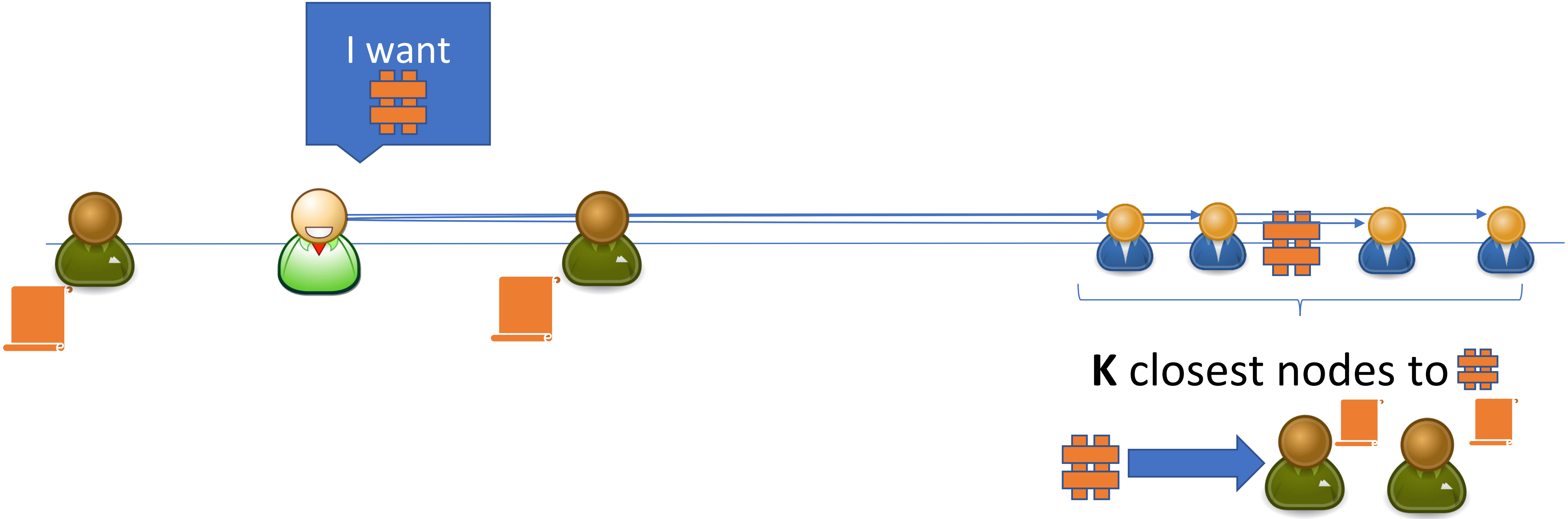
DHT Resolution



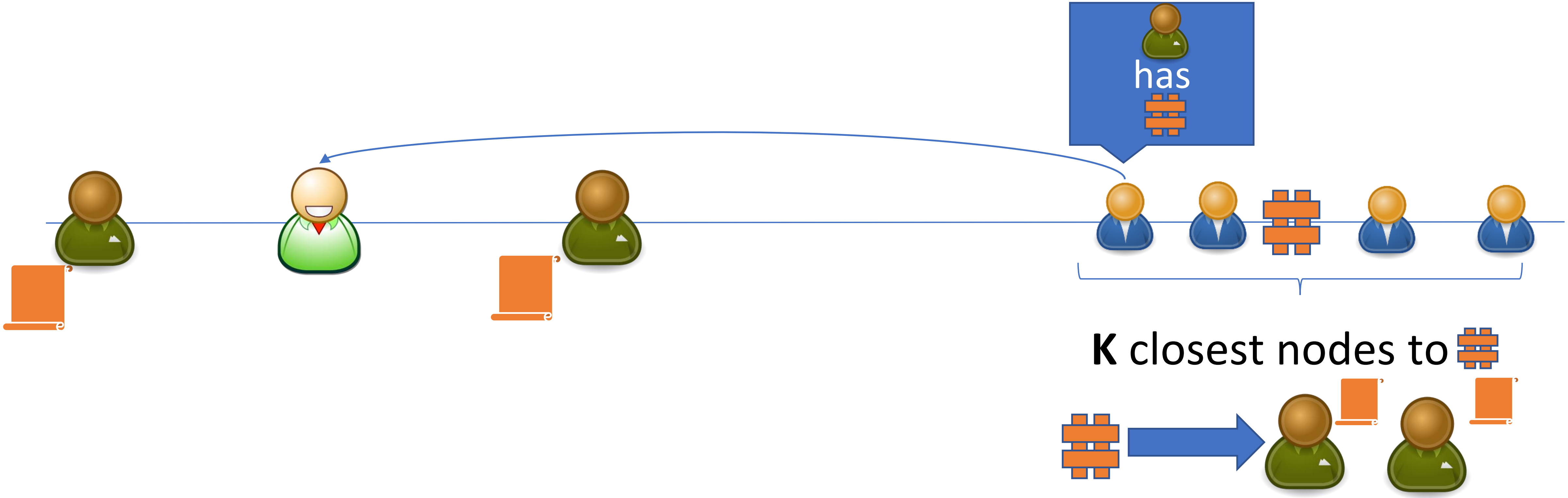
I want #

K closest nodes to #

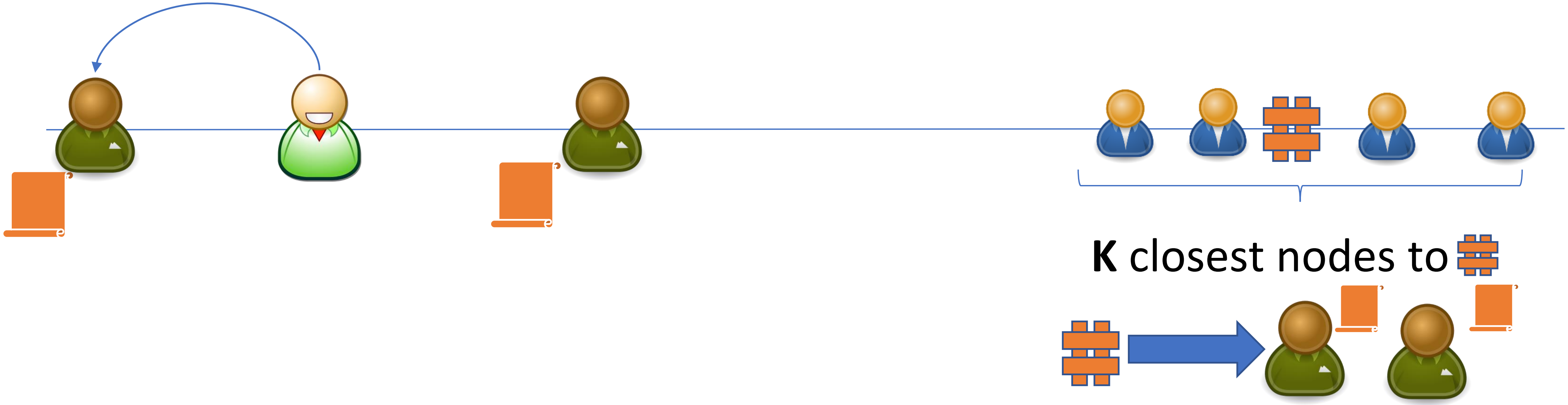
DHT Resolution



DHT Resolution

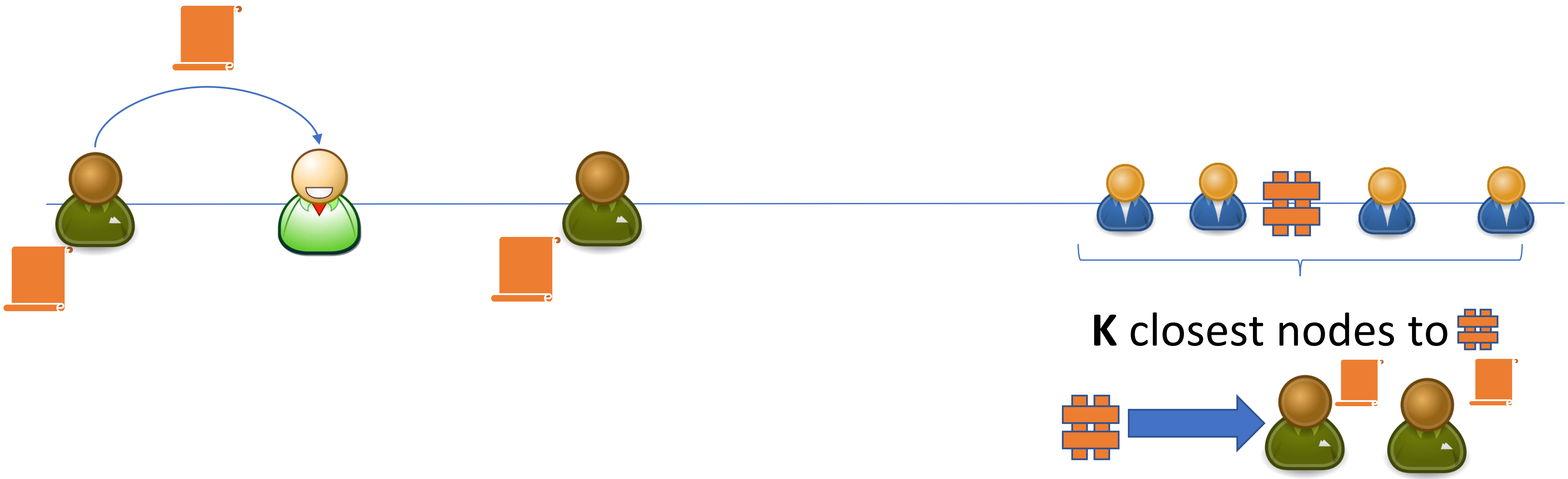


DHT Resolution



K closest nodes to #

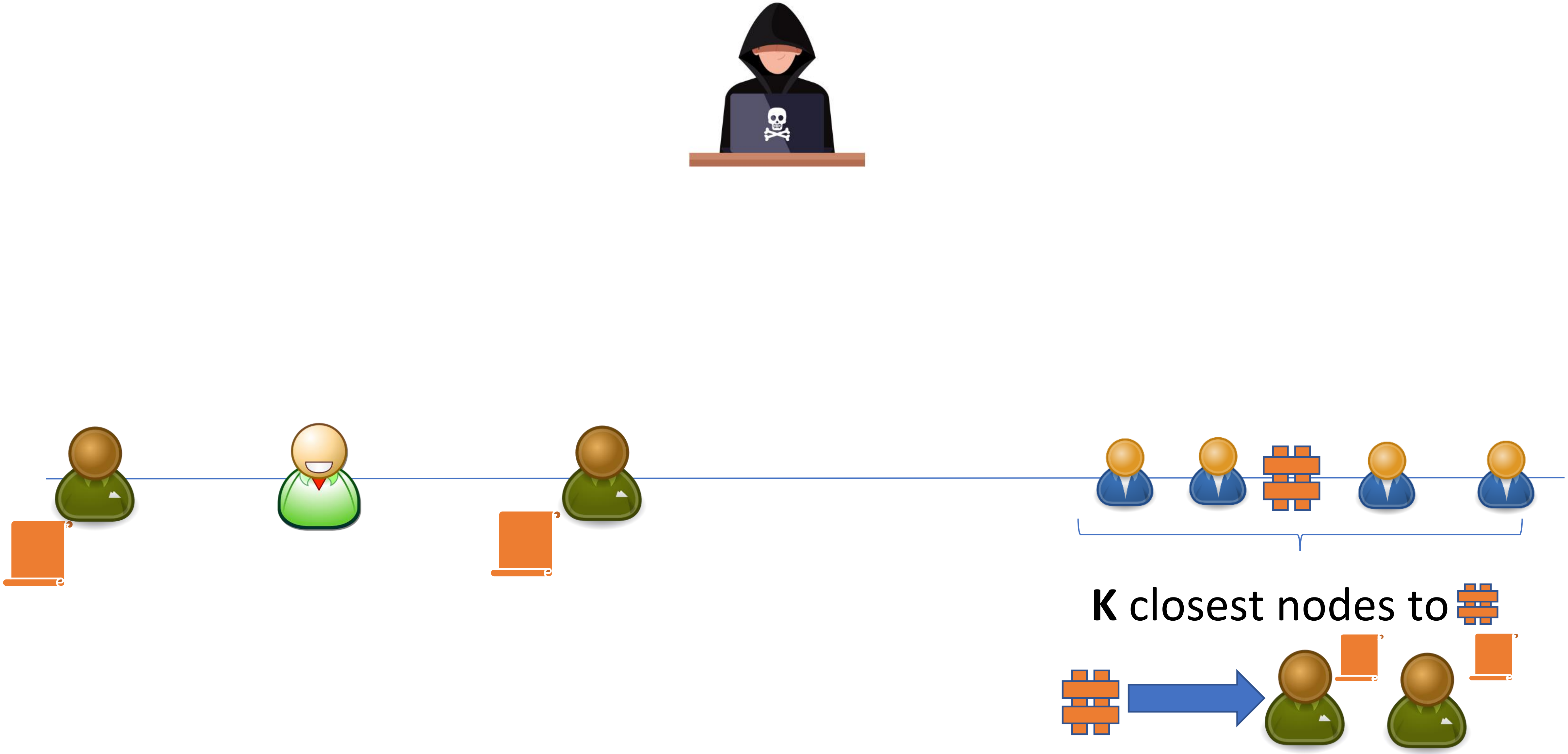
DHT Resolution



K closest nodes to #

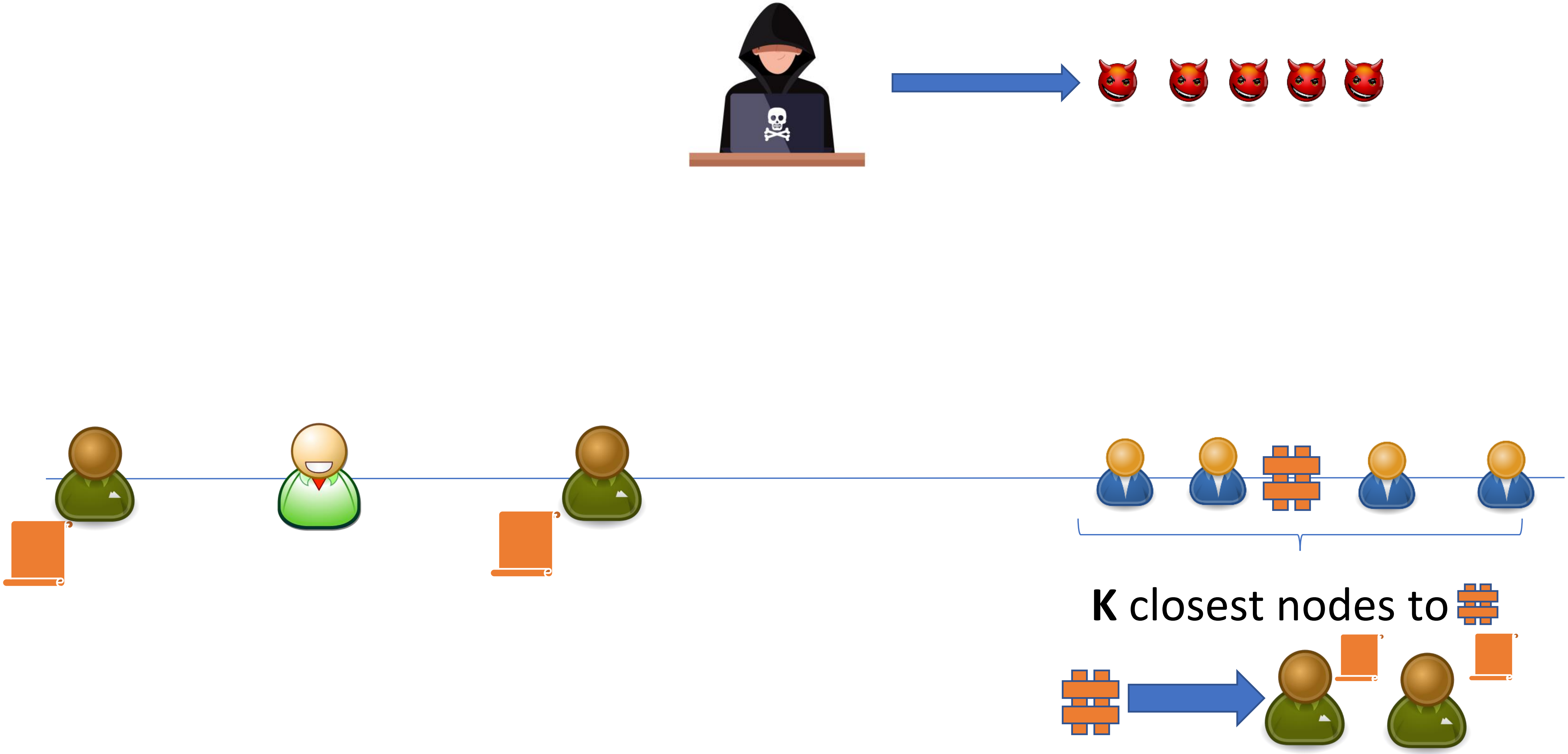
CID eclipse attack

CID Eclipse Attack

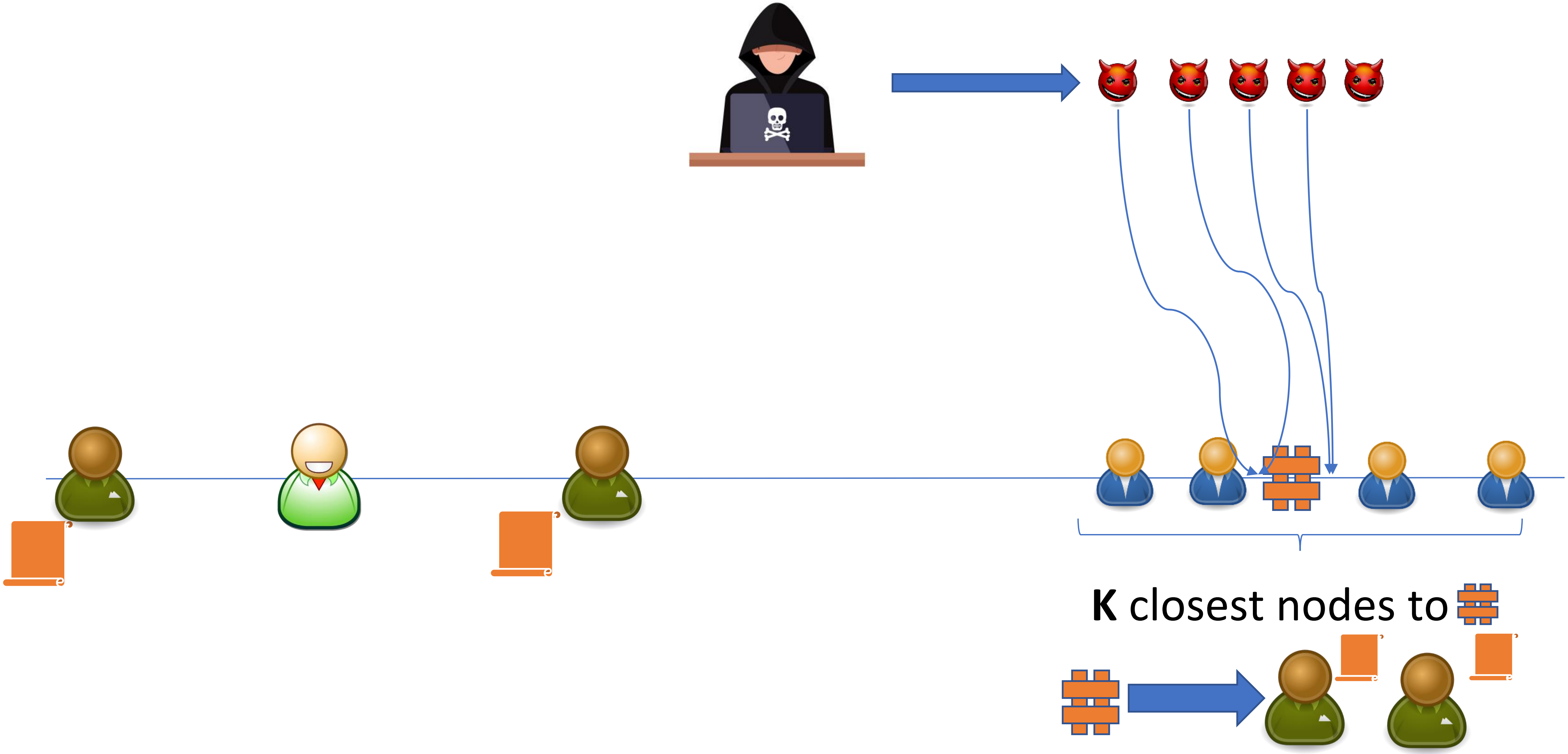


K closest nodes to #

CID Eclipse Attack

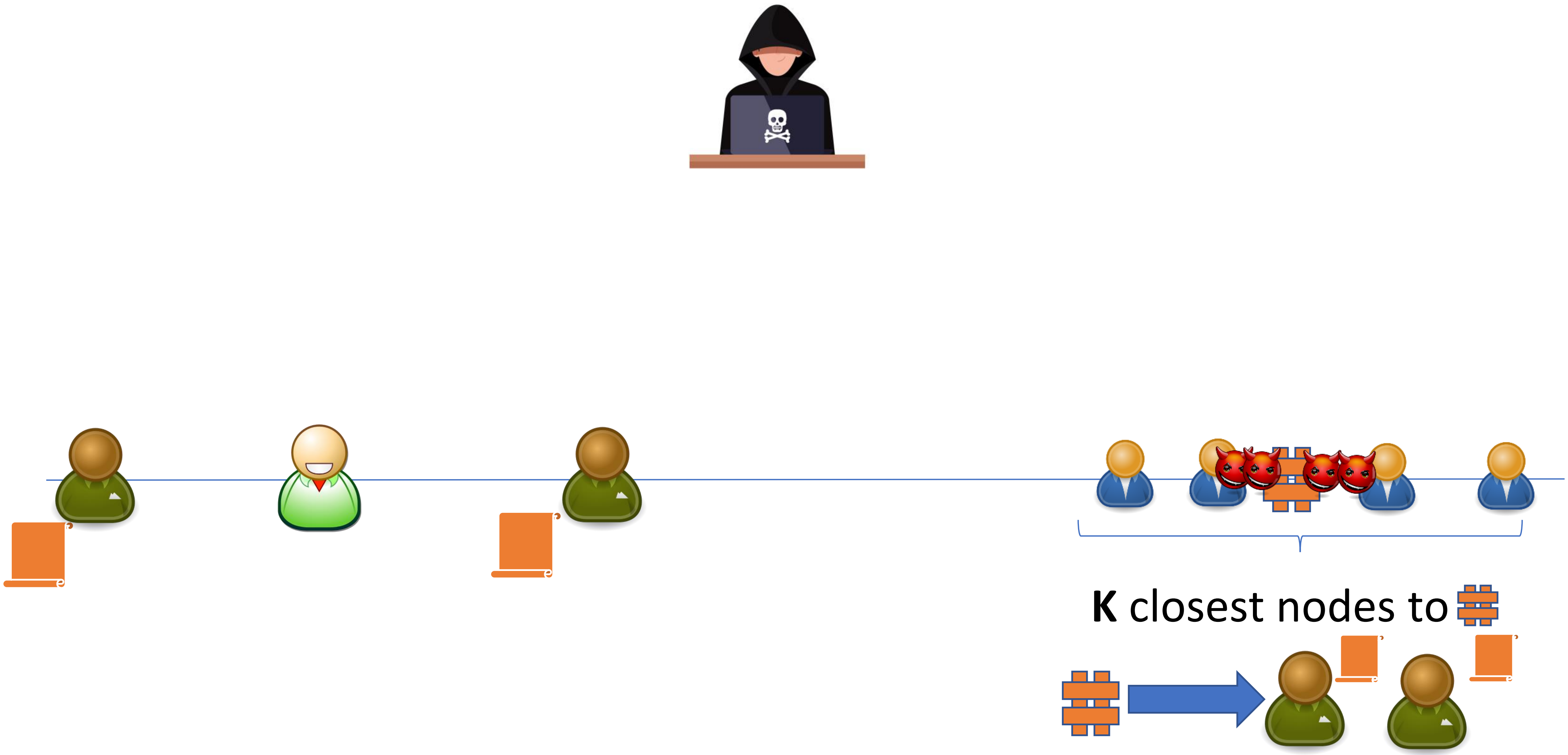


CID Eclipse Attack



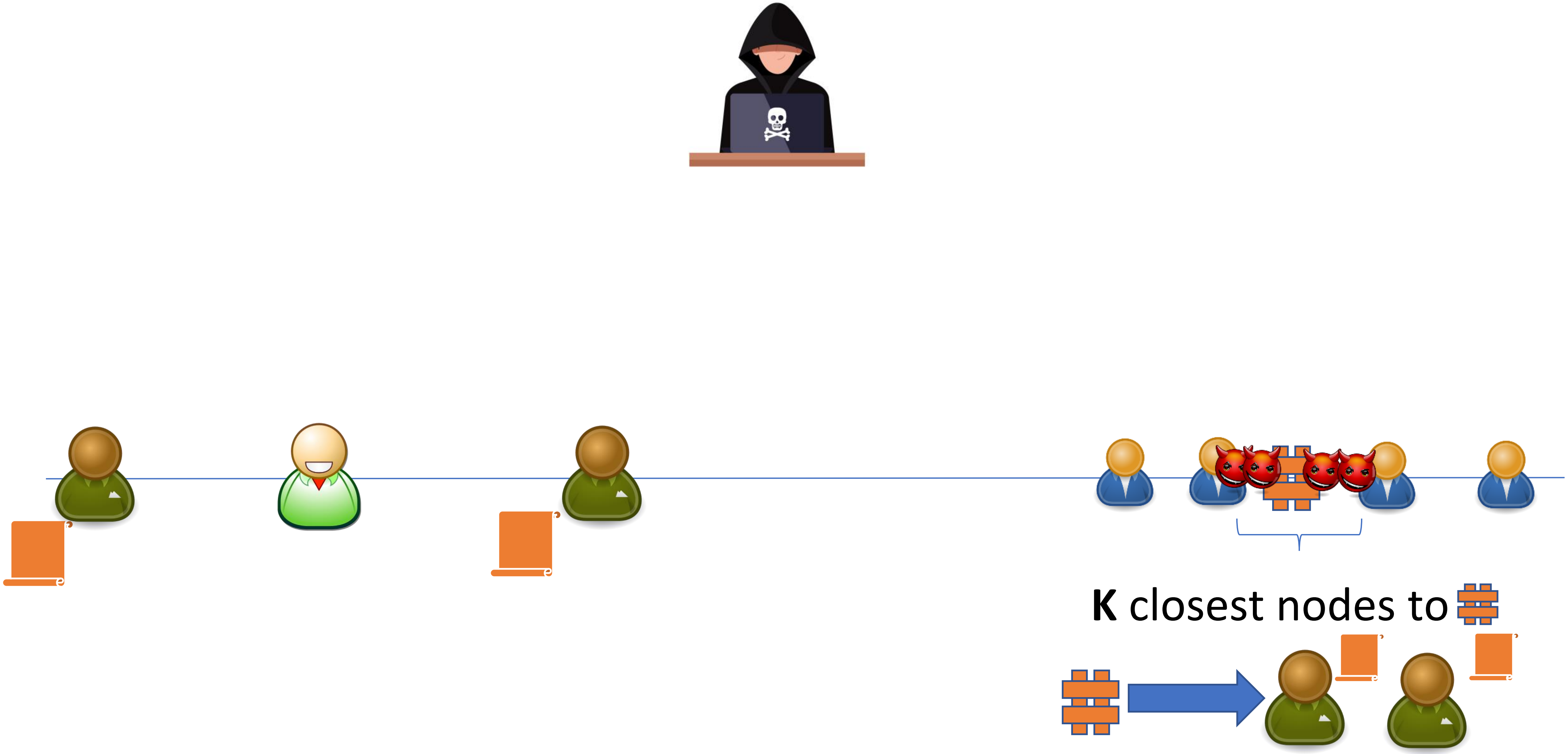
K closest nodes to #

CID Eclipse Attack



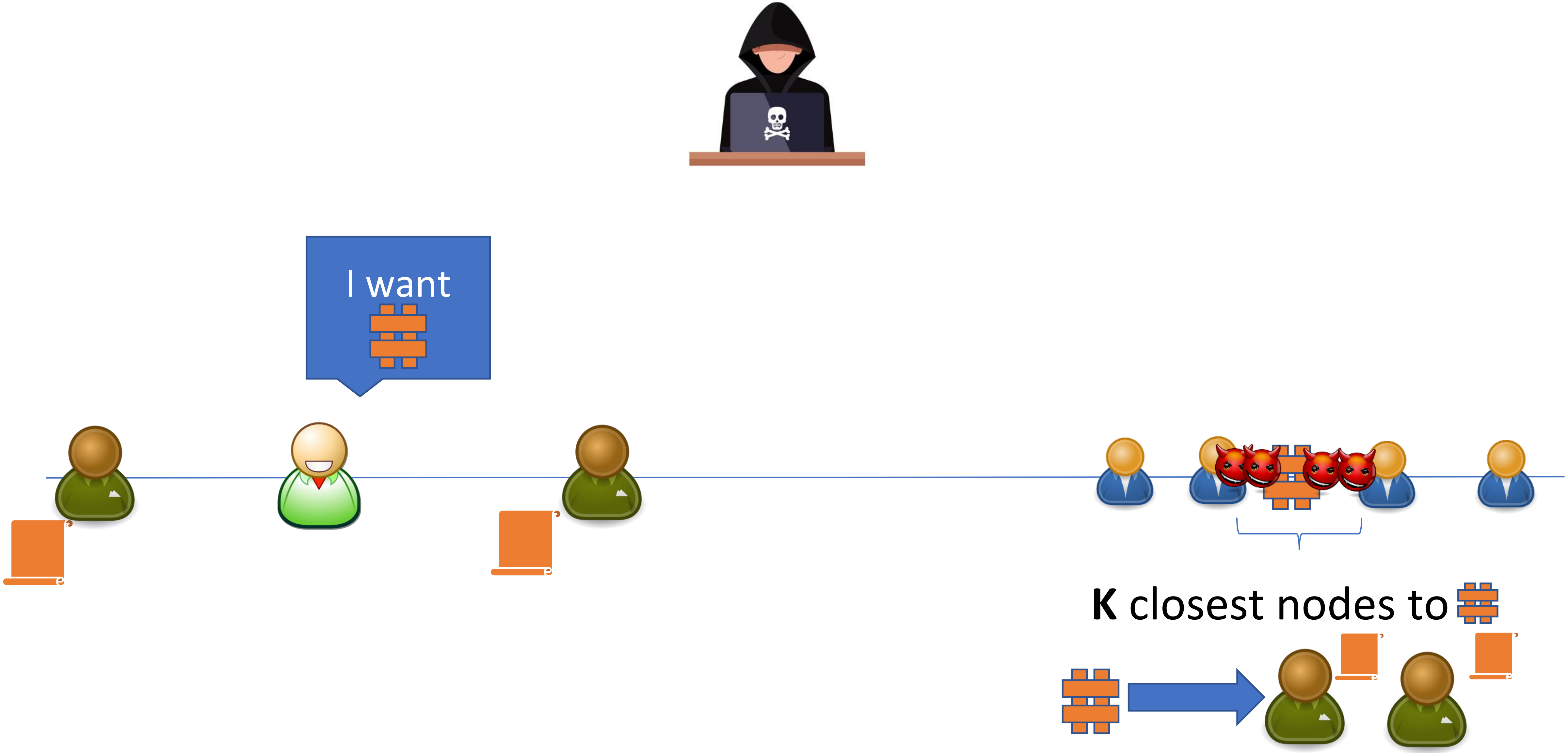
K closest nodes to #

CID Eclipse Attack

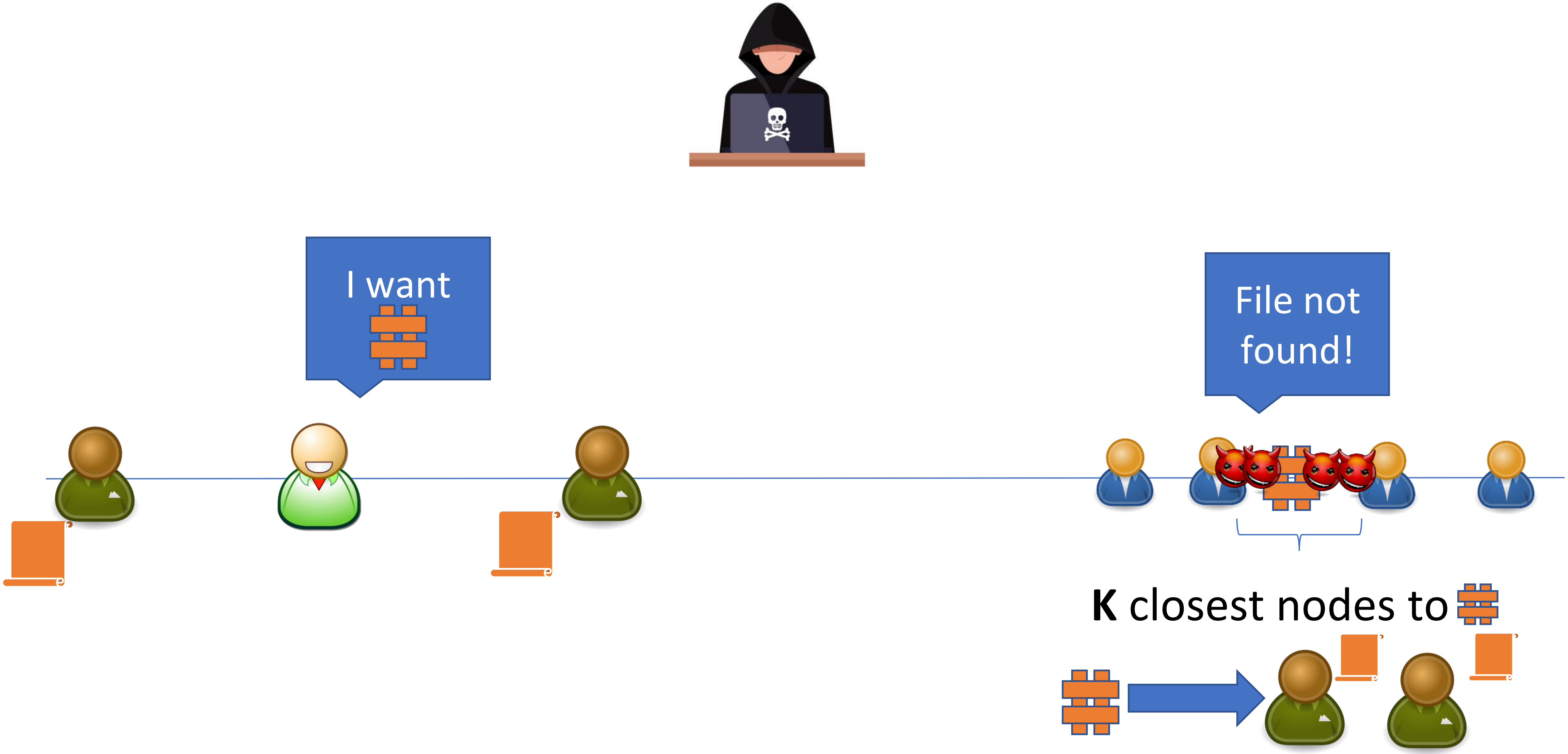


K closest nodes to #

CID Eclipse Attack



CID Eclipse Attack



I want #

File not found!

K closest nodes to #

Attack Success Rate

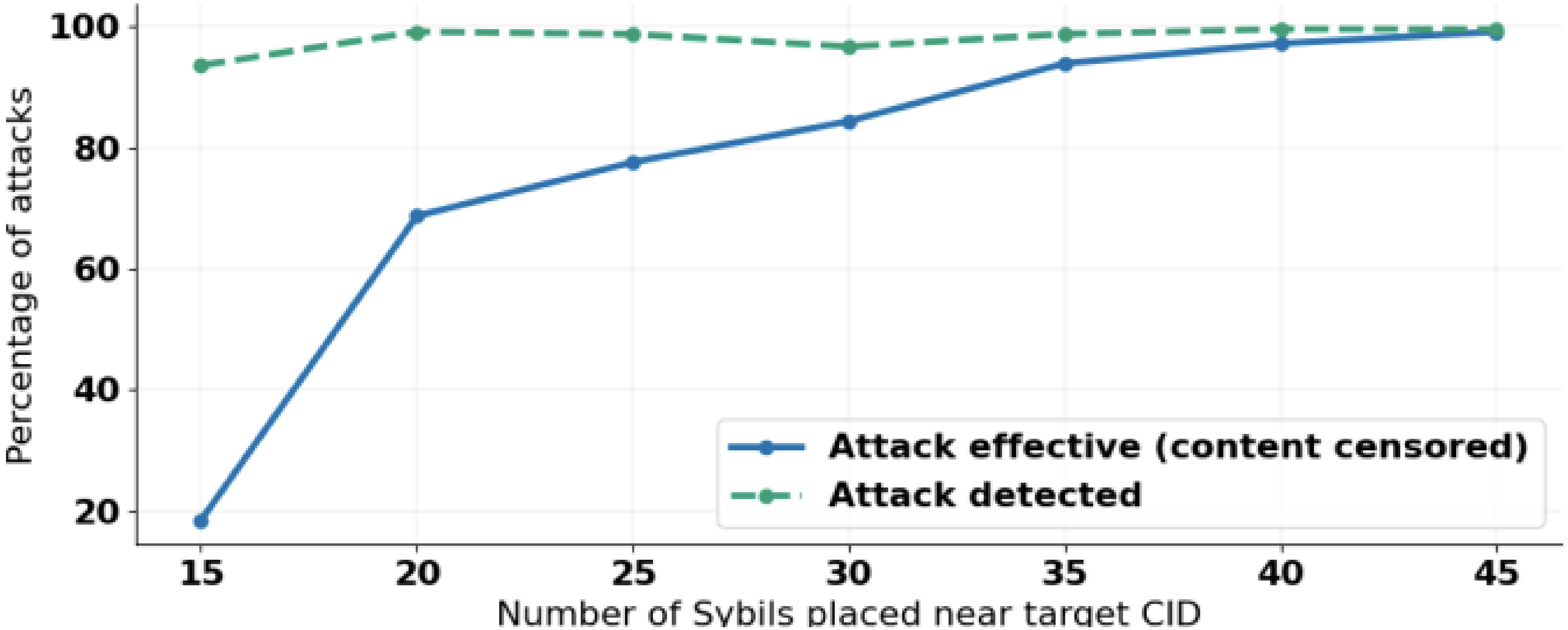


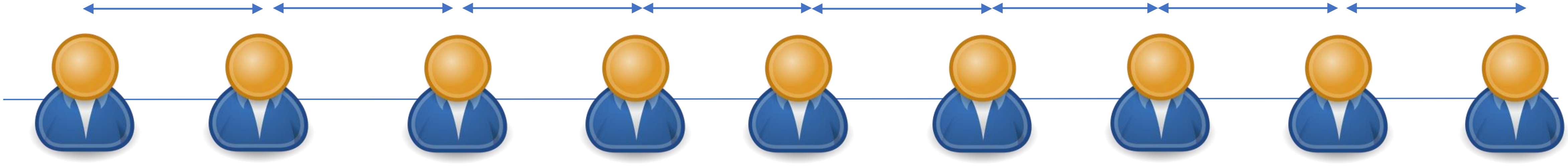
Fig. 7: Percentage of attacks in which *i)* the atack was effective and *ii)* the detection algorithm detected the attack.

Impact

- Any CID can be eclipsed from the network.
- Hundreds of applications build on IPFS and use the DHT - they’re all vulnerable.
- The attack applies to any Kademlia-based DHT (e.g., Ethereum, I2P, DAT).

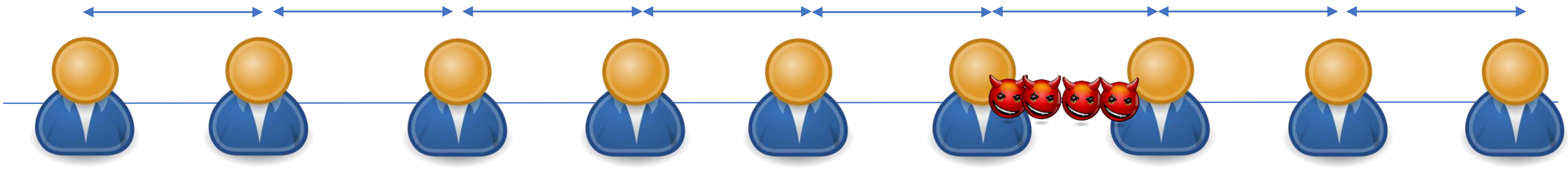
Attack Detection

CID Eclipse Detection



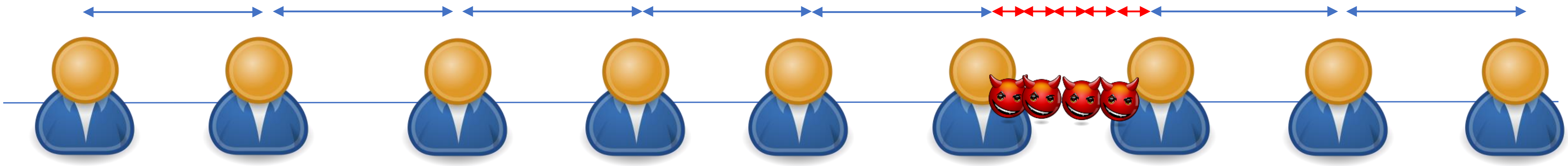
sha256 hash space

CID Eclipse Detection



sha256 hash space

CID Eclipse Detection



sha256 hash space

PeerID Distribution

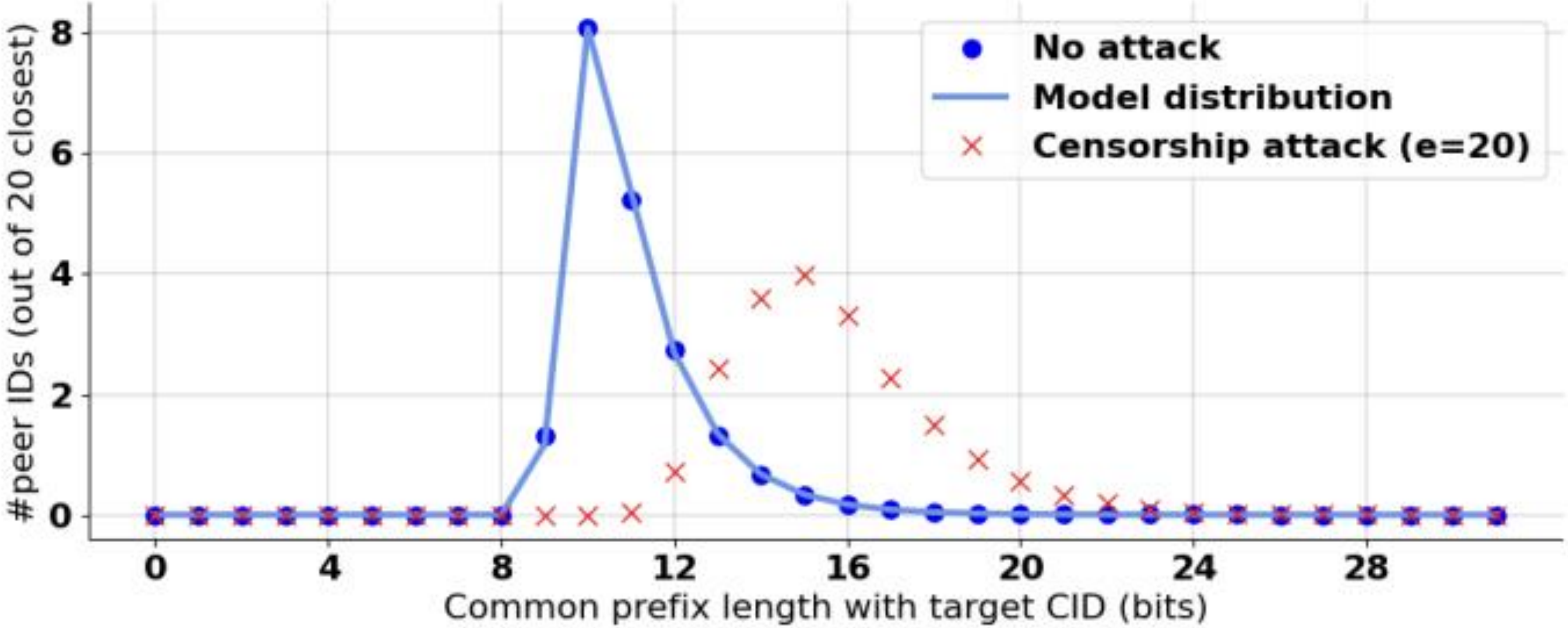


Fig. 3: Probability distribution of common prefix lengths of the target CID with its $k = 20$ closest peer IDs.

KL Divergence

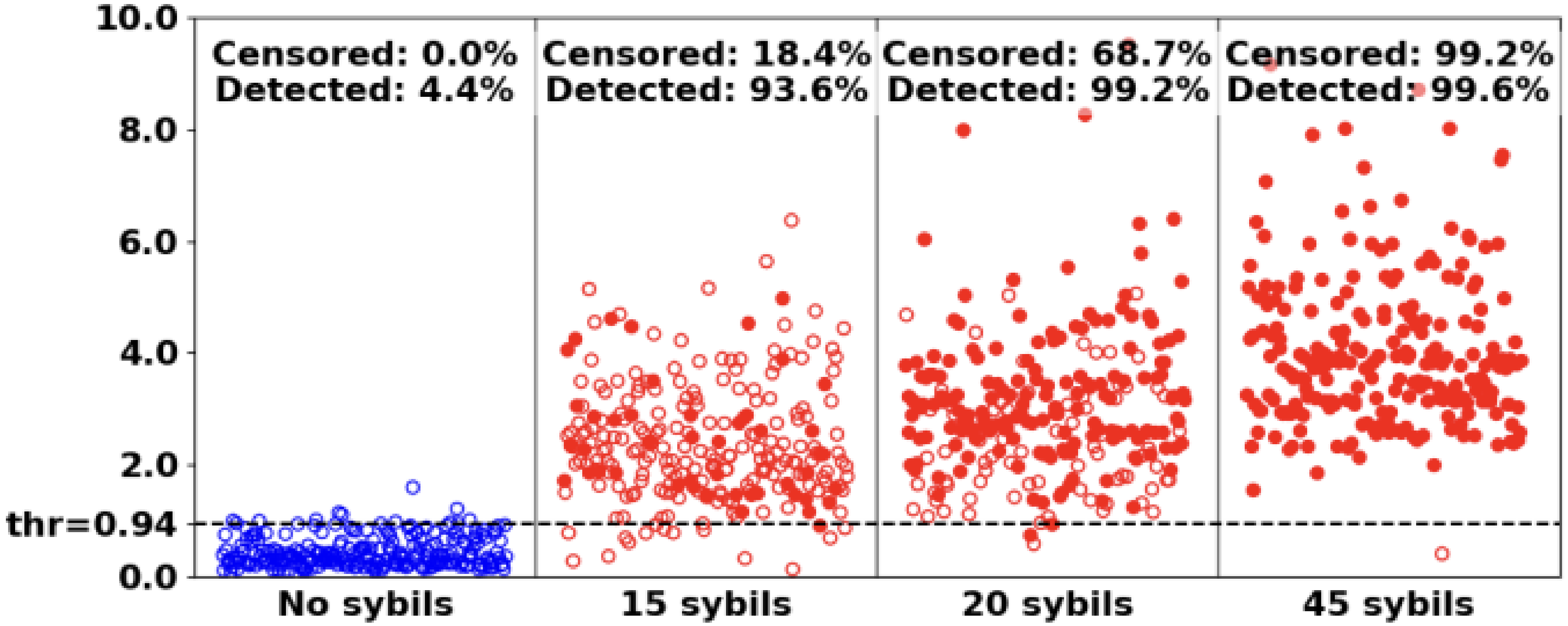
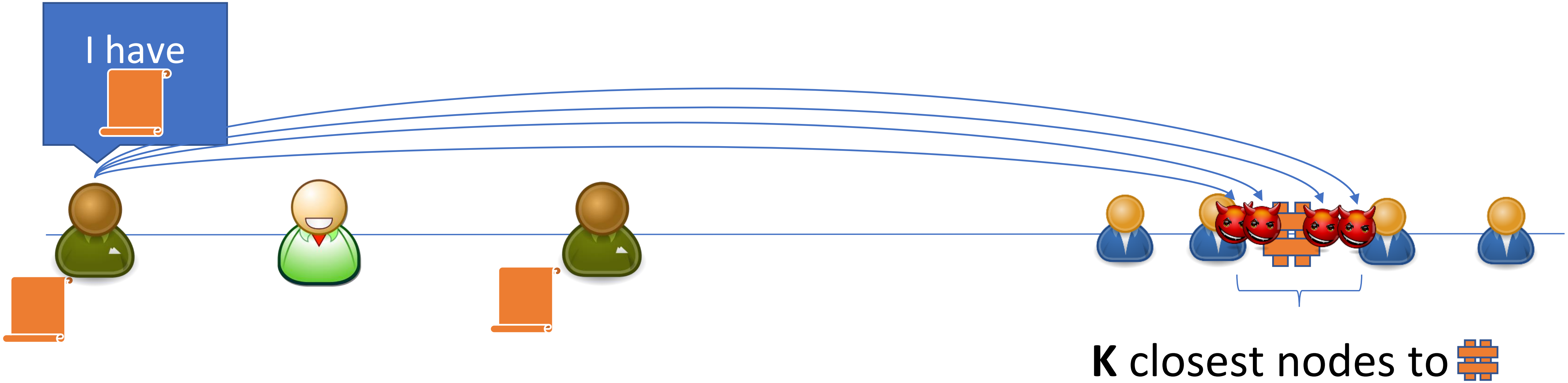


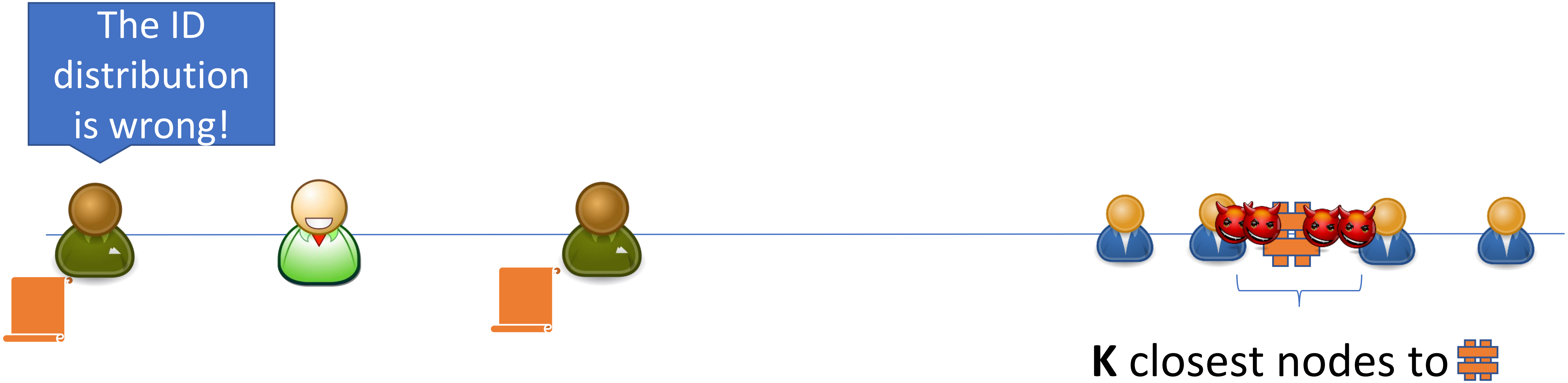
Fig. 11: KL divergence for varying numbers of Sybils *e*.

Attack Response

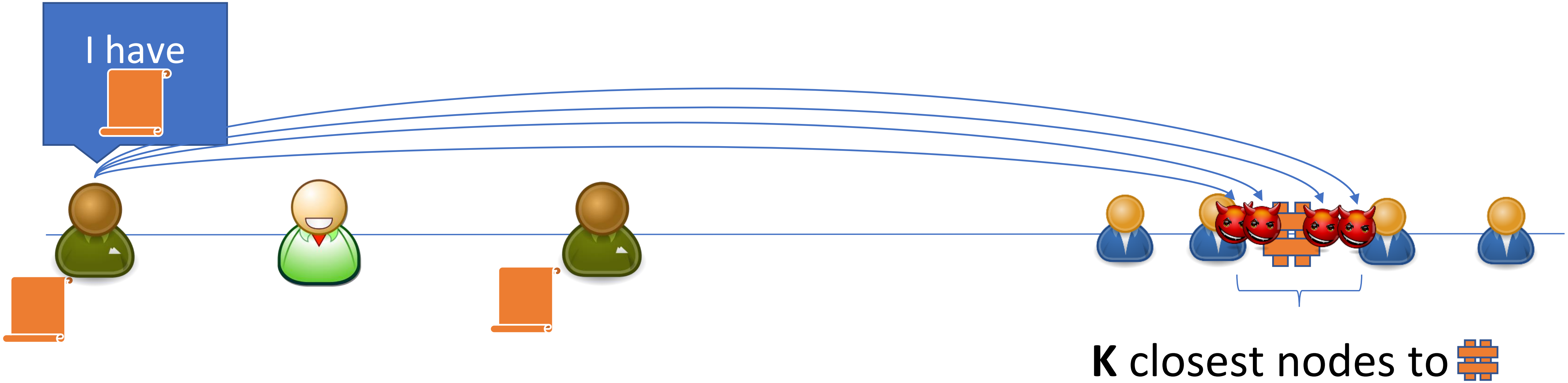
CID Eclipse Response



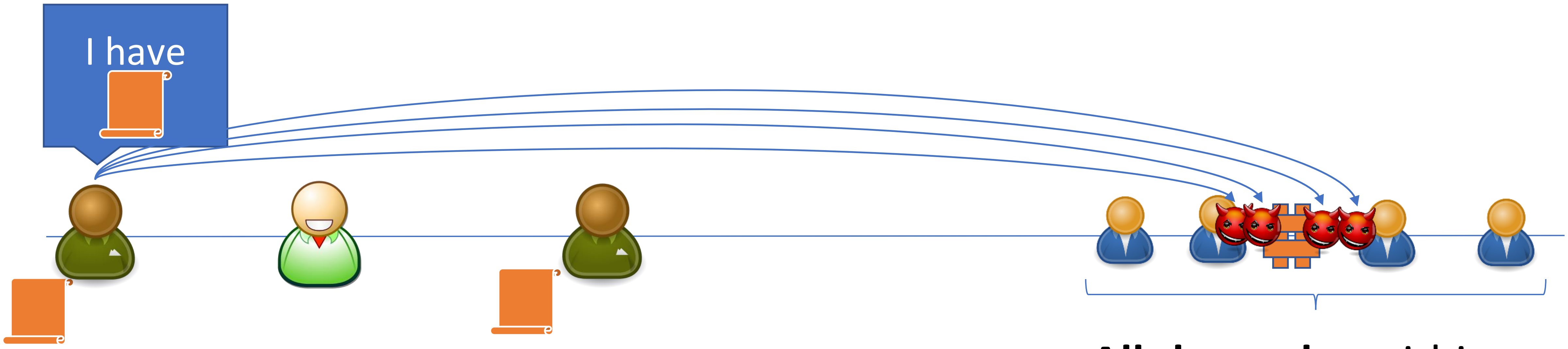
CID Eclipse Response



CID Eclipse Response

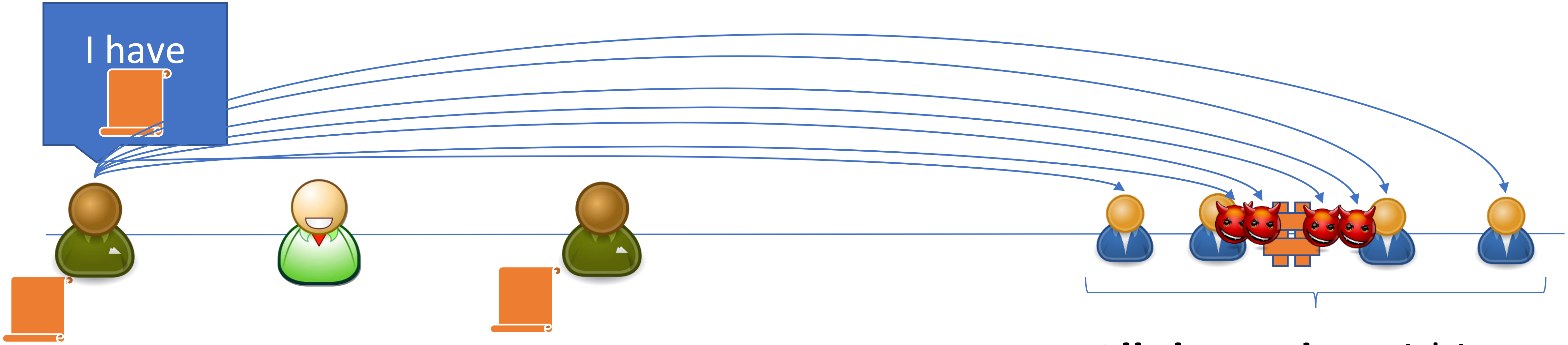


CID Eclipse Response



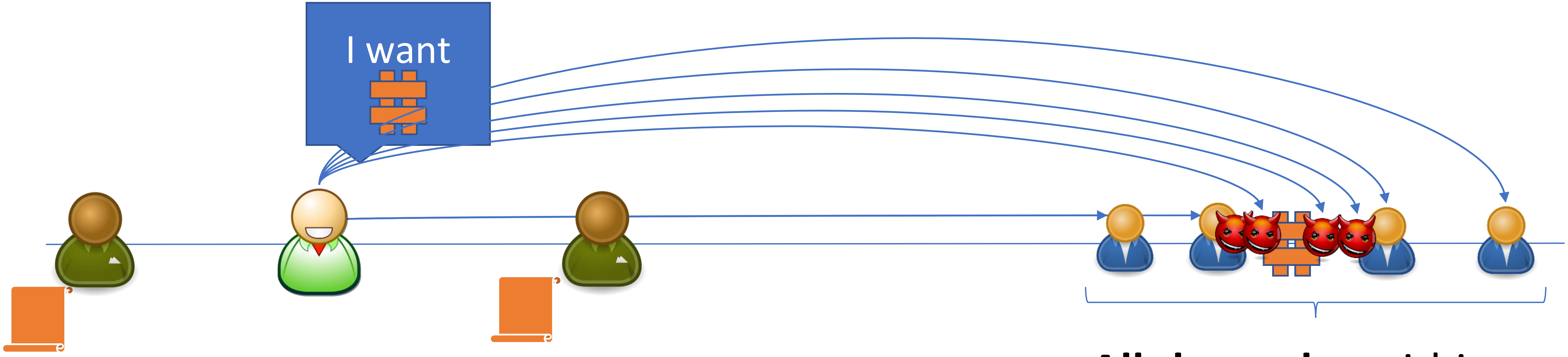
All the nodes within region close to #

CID Eclipse Response



All the nodes within region close to #

CID Eclipse Response



All the nodes within region close to

Mitigation Overhead

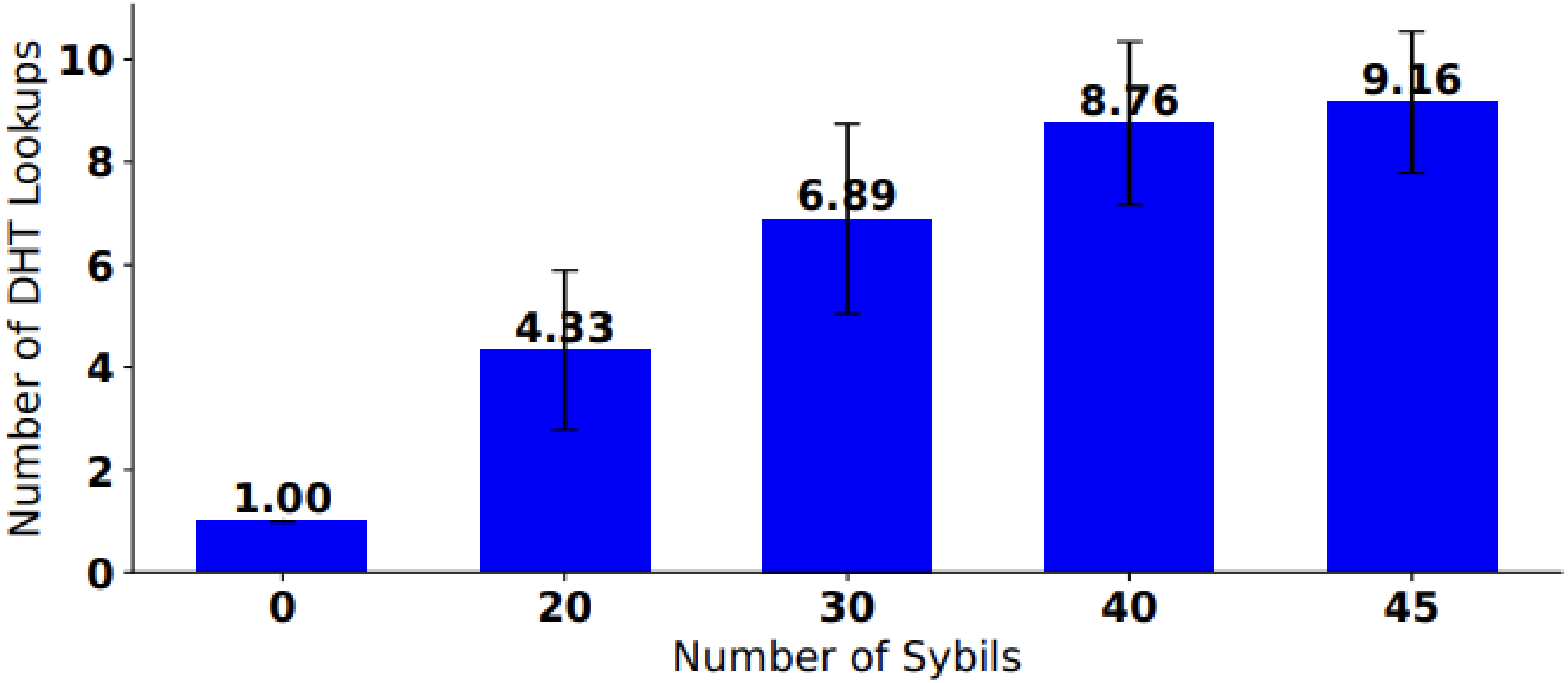


Fig. 15: The number of DHT lookups involved in a region-based query.

Mitigation Success Rate

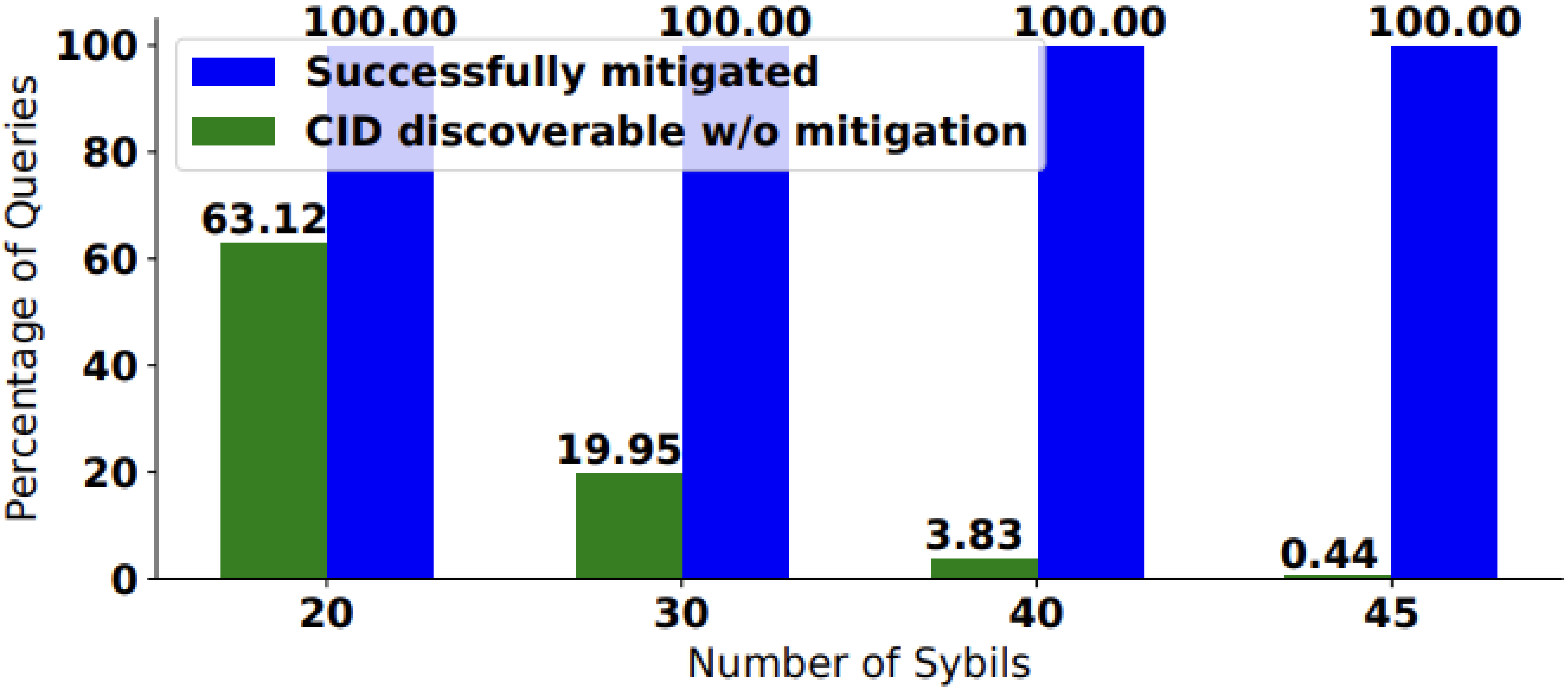


Fig. 13: Percentage of attacks that are mitigated.

What now?

- Working with engineers at Protocol Labs to fix the vulnerability in kubo (primary IPFS client).
- CVE-2023-26248 assigned
- Paper to appear at NDSS 2024
  - Preprint available at: https://ssg.lancs.ac.uk/wp-content/uploads/ndss_preprint.pdf
  - IPFS CID: bafybeieg6imrz23ut6inhaqvhpzq5n7gb5bvb6fbpom4b7ij4aqzxrjqyi

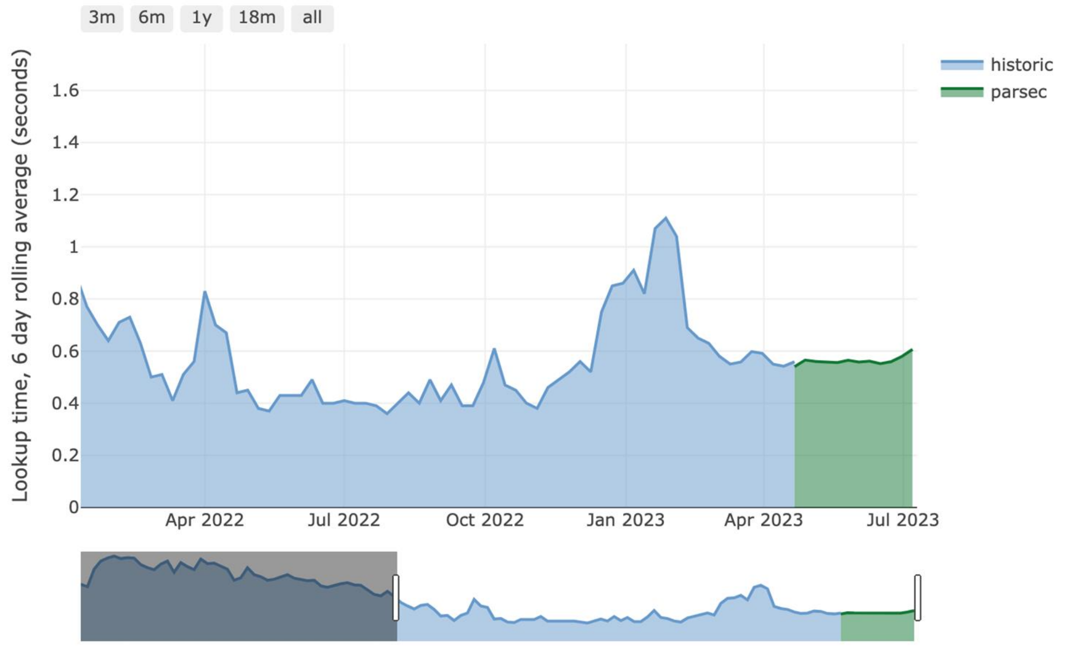
BUT...

Half the IPFS DHT network becomes unresponsive

Q1’23

IPFS ÞING
Brussels, Belgium
2023

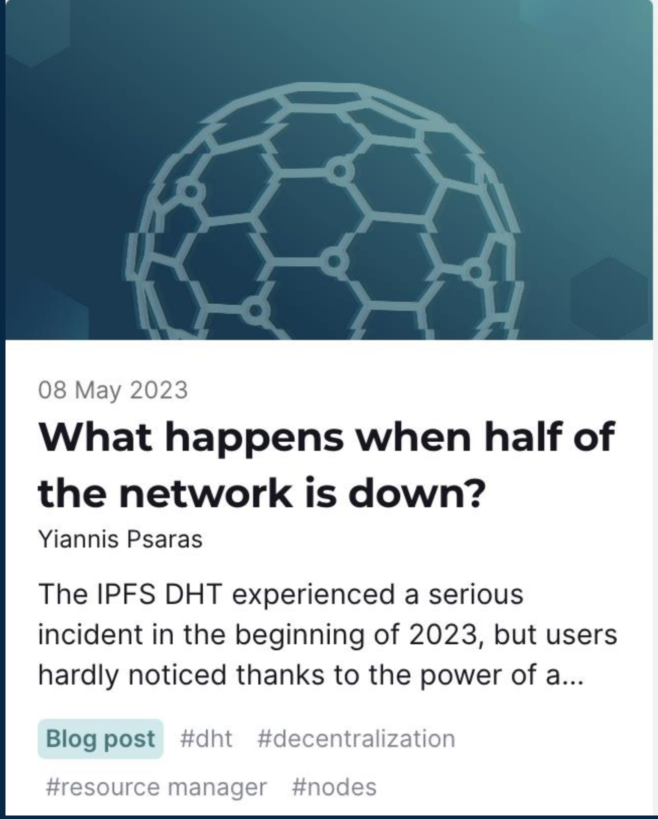
- 60% of nodes unresponsive ⍰
- BUT no content unreachable
- Network kept functioning, albeit much slower



Data: 12 Feb 2021 to 9 Jul 2023. Source: Legacy monitoring script and Parsec.

Check:

- Blogpost: https://blog.ipfs.tech/2023-ipfs-unresponsive-nodes/
- Video: https://youtu.be/8cGEjdCfm14
- https://probelab.io for lots more measurements



08 May 2023

What happens when half of the network is down?

Yiannis Psaras

The IPFS DHT experienced a serious incident in the beginning of 2023, but users hardly noticed thanks to the power of a...

Blog post #dht #decentralization #resource manager #nodes

IPFS ÞING
Brussels, Belgium
2023

THANK YOU!

yiannis@protocol.ai

IPFS ÞING
Brussels, Belgium
2023