Anonymity in the Bitcoin Peer-to-Peer Network

Shaileshh Bojja Venkatakrishnan, Giulia Fanti, Pramod Viswanath



“Untraceable Bitcoin”

Teenagers using untraceable currency Bitcoin to buy dangerous drugs online

Fears have been raised as children as young as 14 are getting parcels of legal highs delivered to their home

Mirror



This is false.

Bitcoin Primer

Transaction

k_A sends k_{coin} to k_B

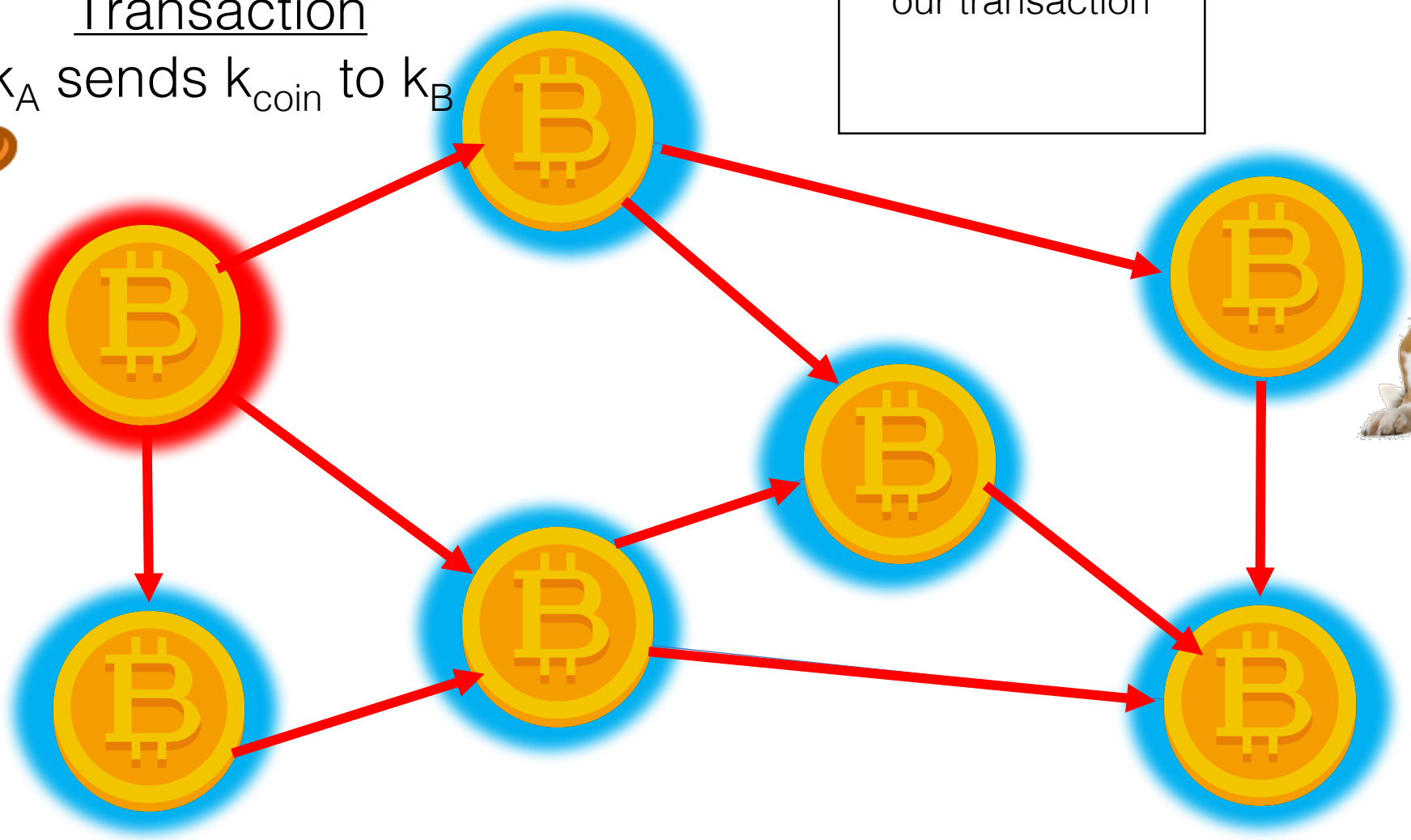
Blockchain
sd93fjj2
pckrn29
…
our transaction



Alice
k_A

k_{coin}

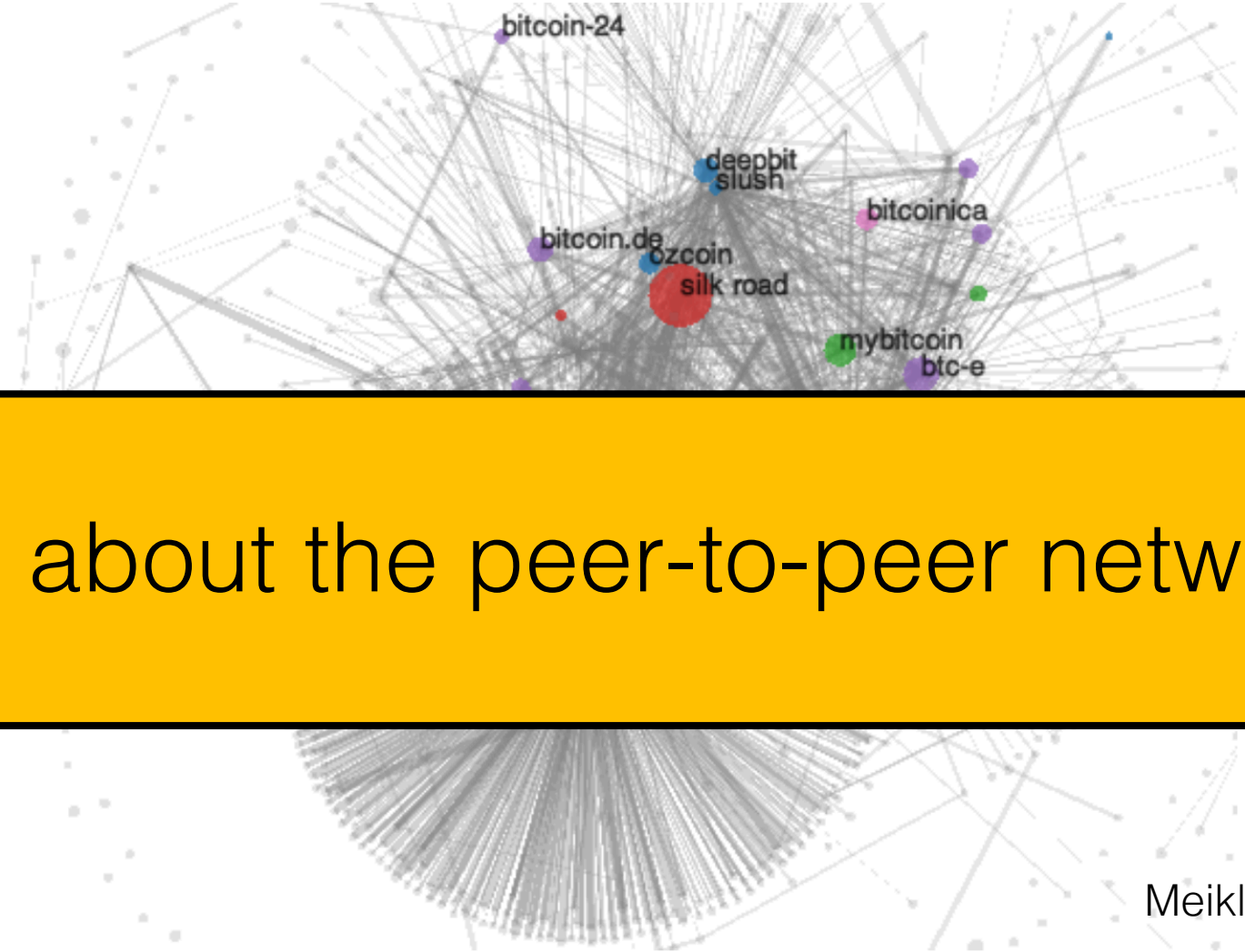






Bob
k_B

How can users be deanonymized?

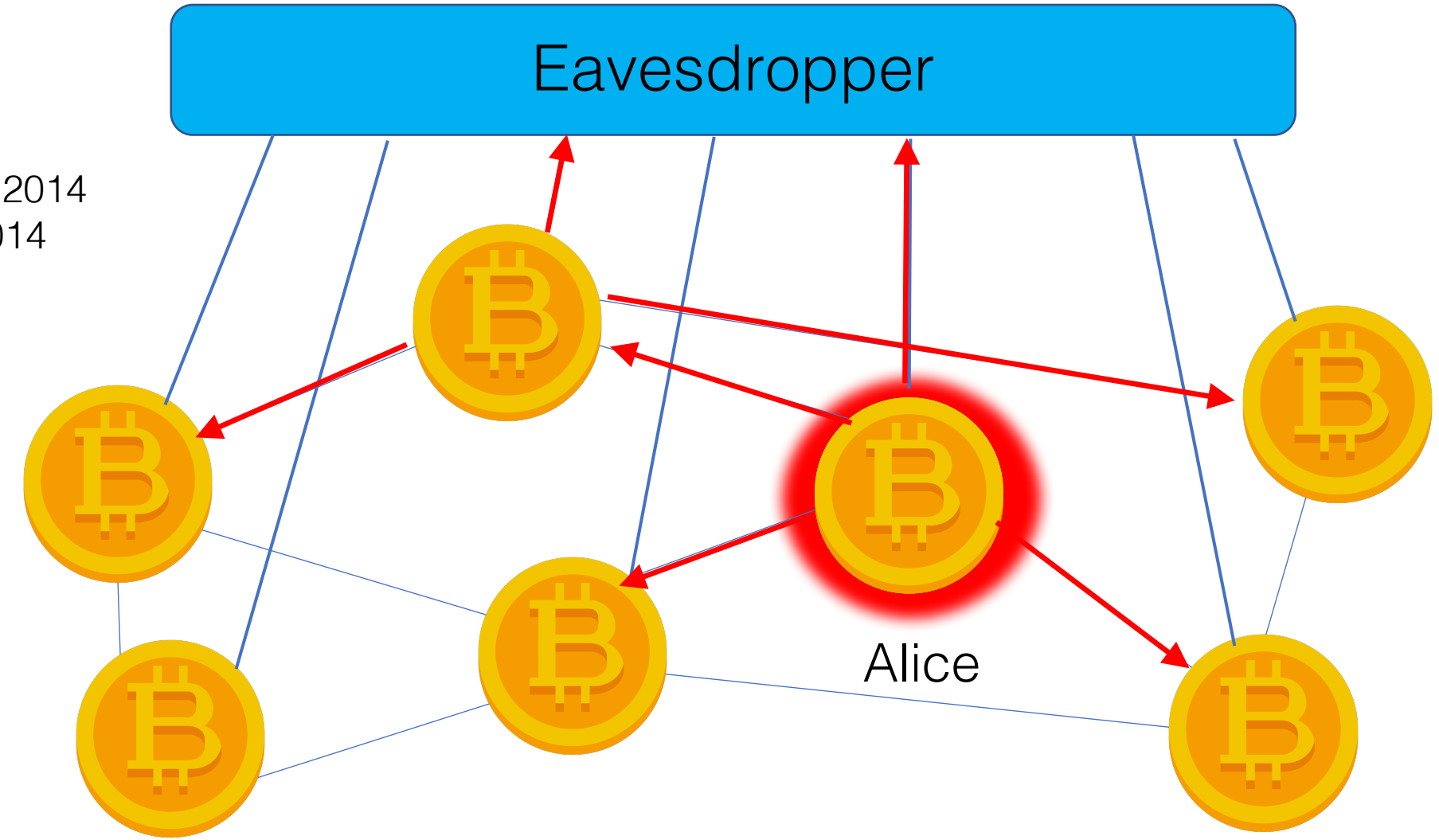


What about the peer-to-peer network?

Meiklejohn et al., 2013

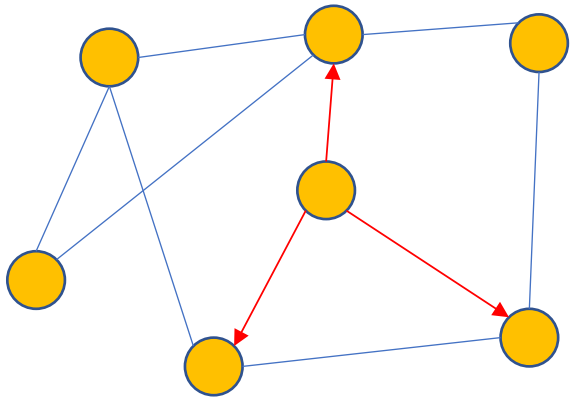
Attacks on the Network Layer

Biryukov et al., 2014
Koshy et al., 2014



Our Work

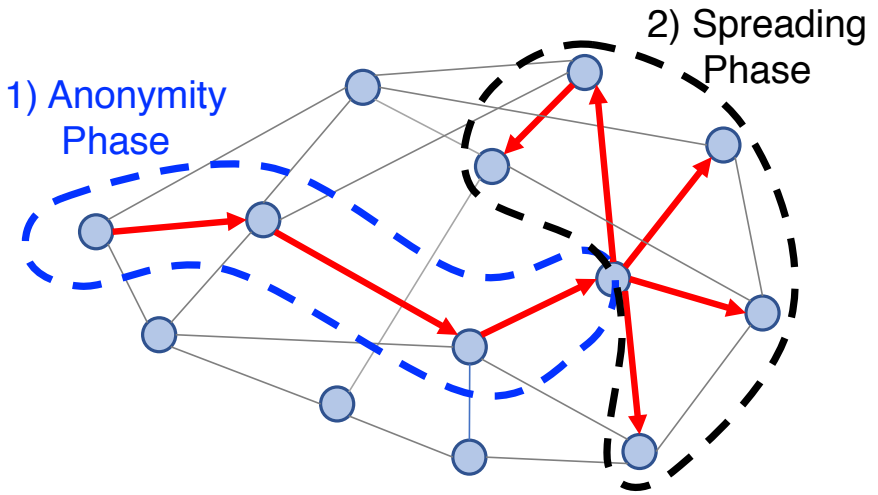
Analysis



Pr(detection)

Under submission, 2017

Redesign



Dandelion

Under submission, 2017

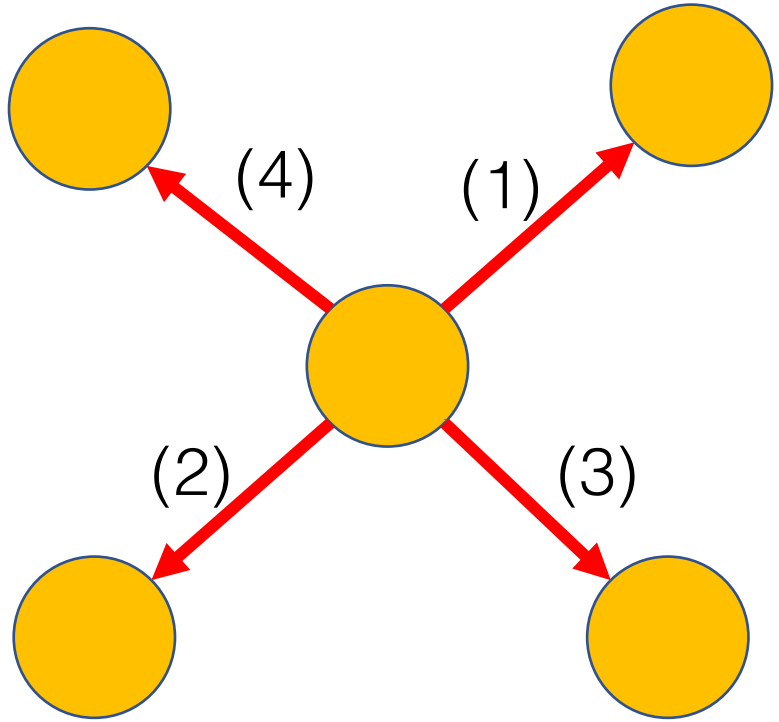
Analysis

How bad is the problem?

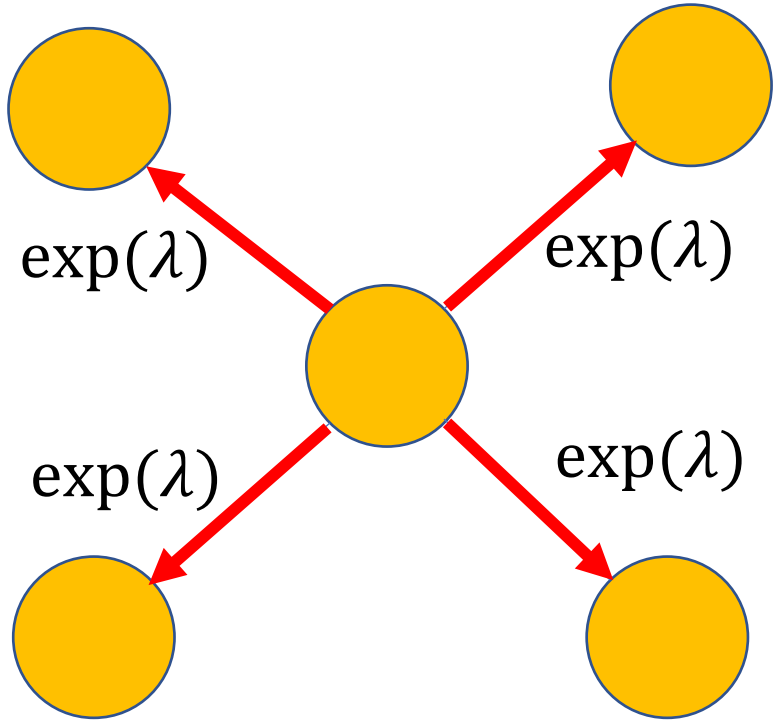


Flooding Protocols

Trickle (pre-2015)



Diffusion (post-2015)

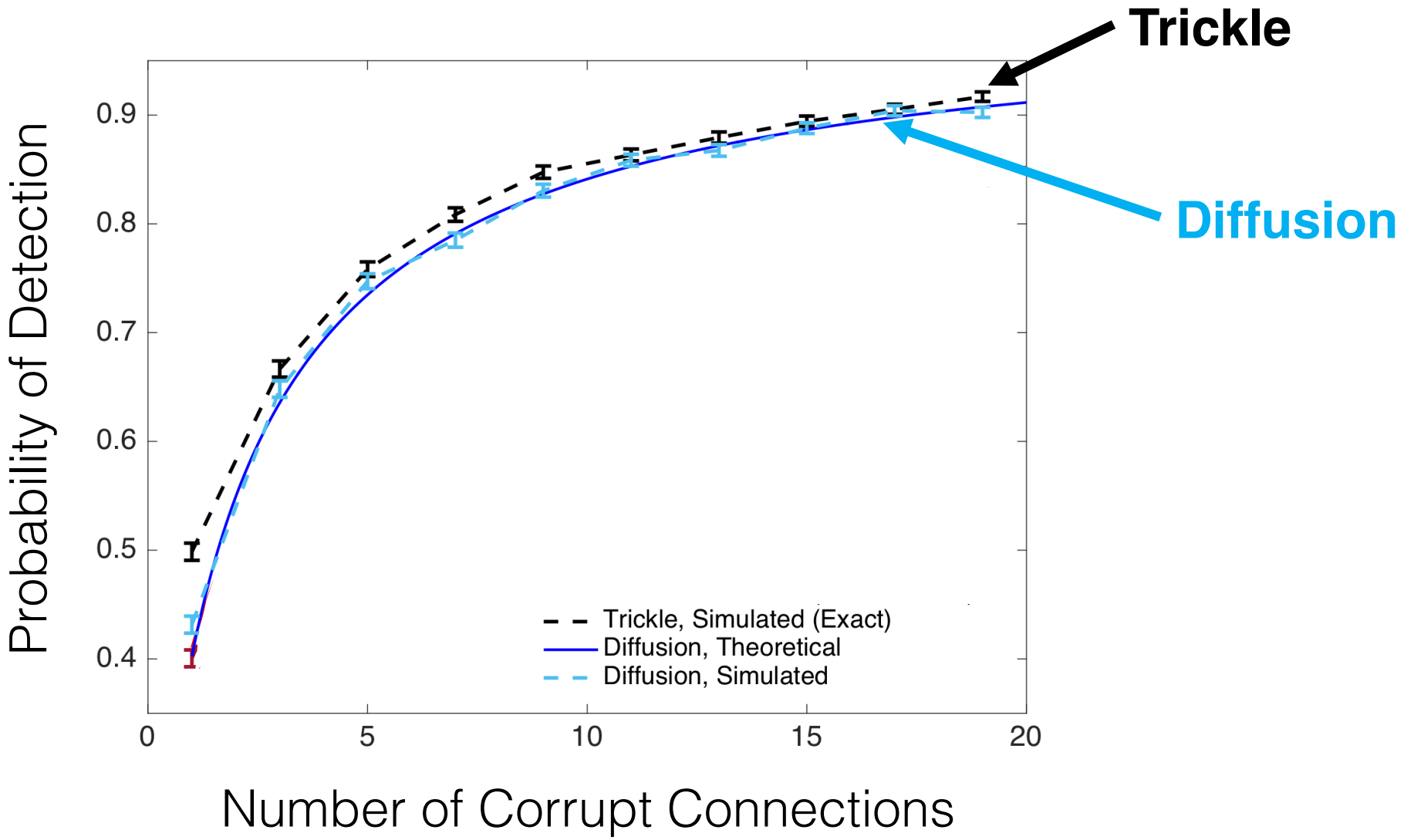


Does diffusion solve the problem?

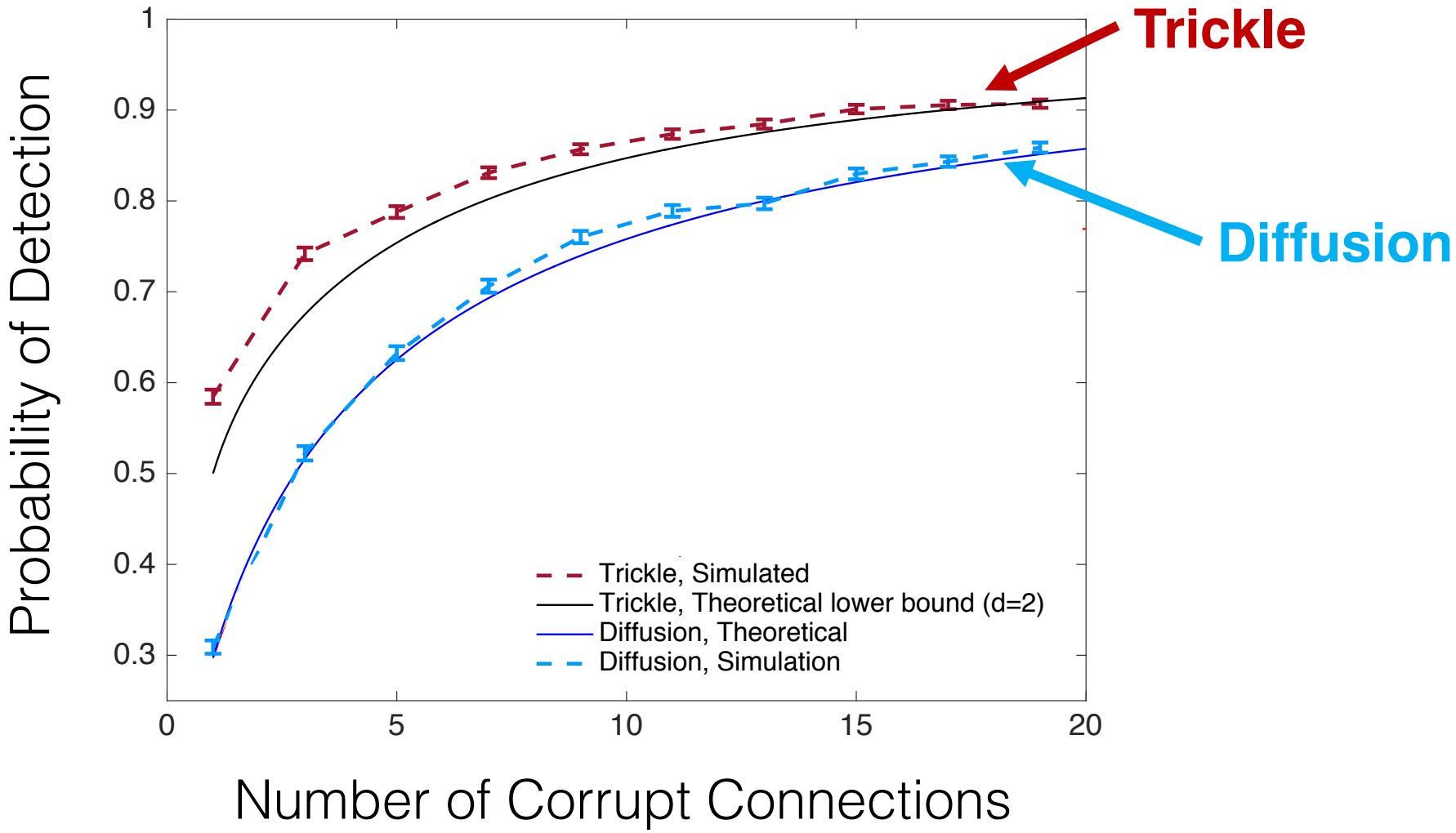
Results: d-Regular Trees

Theorem: The maximum-likelihood probabilities of detection for diffusion and trickle are asymptotically identical in d.

Results: Trees



Results: Bitcoin Graph



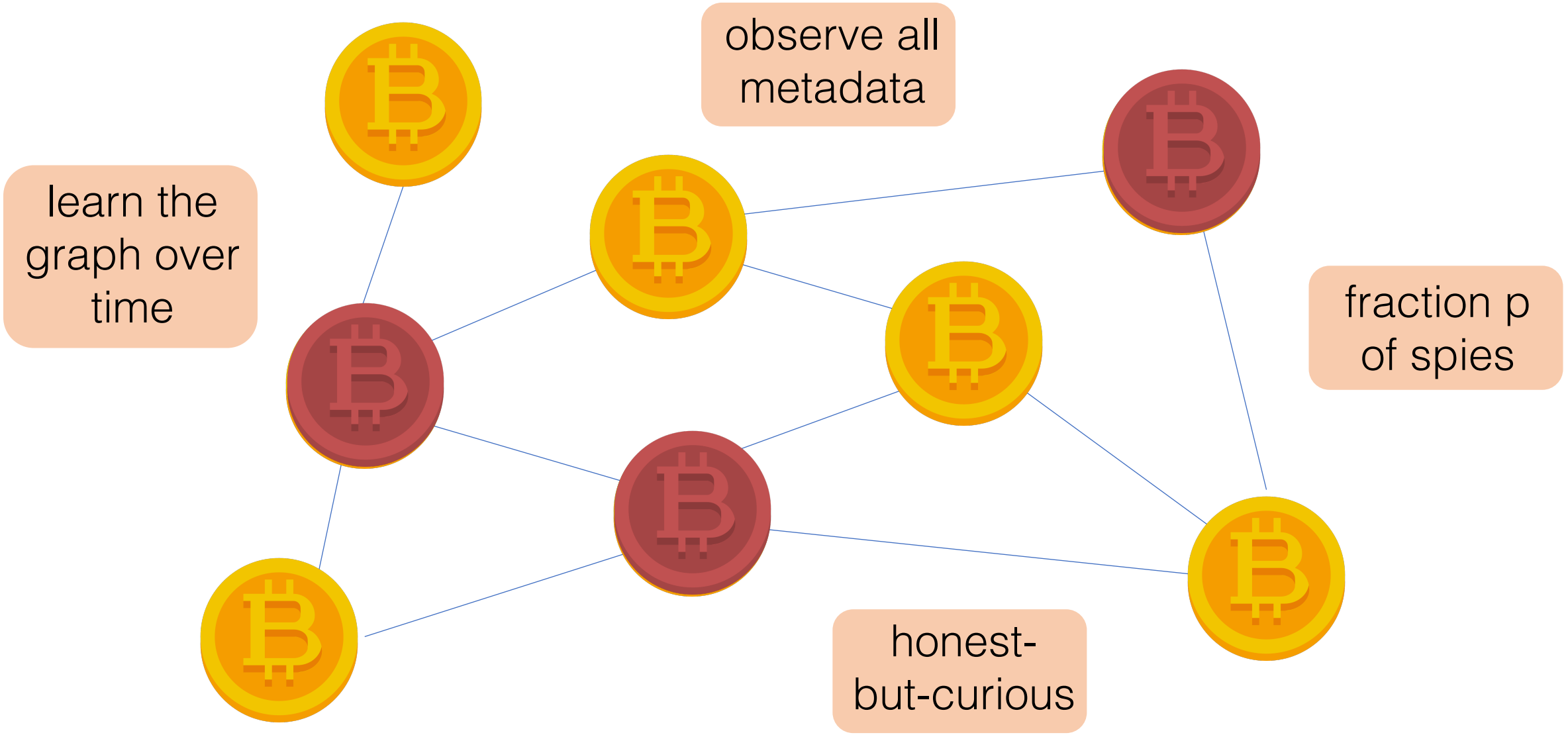
Diffusion does not have (significantly) better anonymity properties than trickle.

Redesign

Can we design a better network?

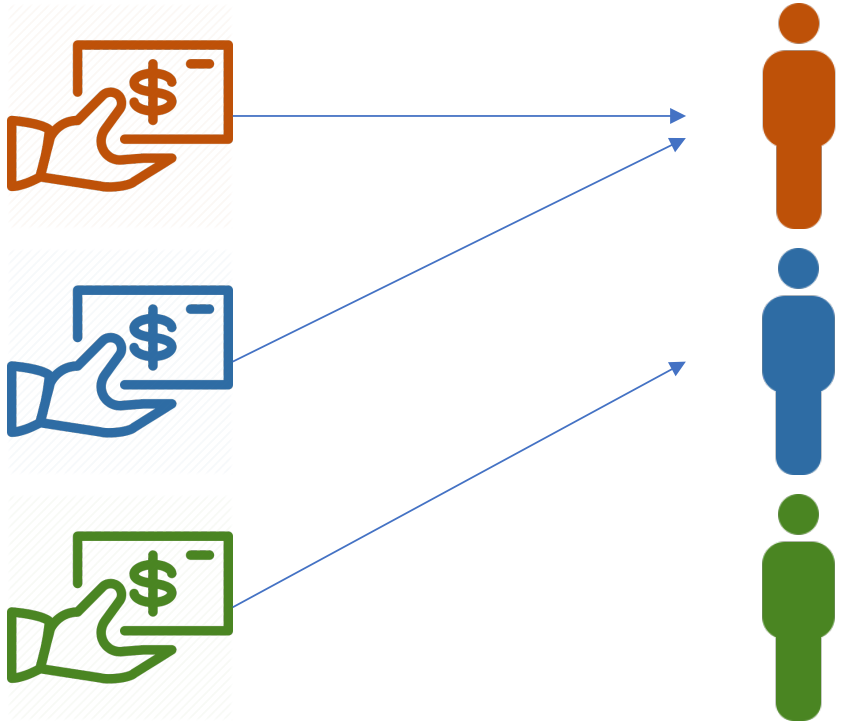


Adversarial Model



Metric for Anonymity

Recall (Probability of Detection)

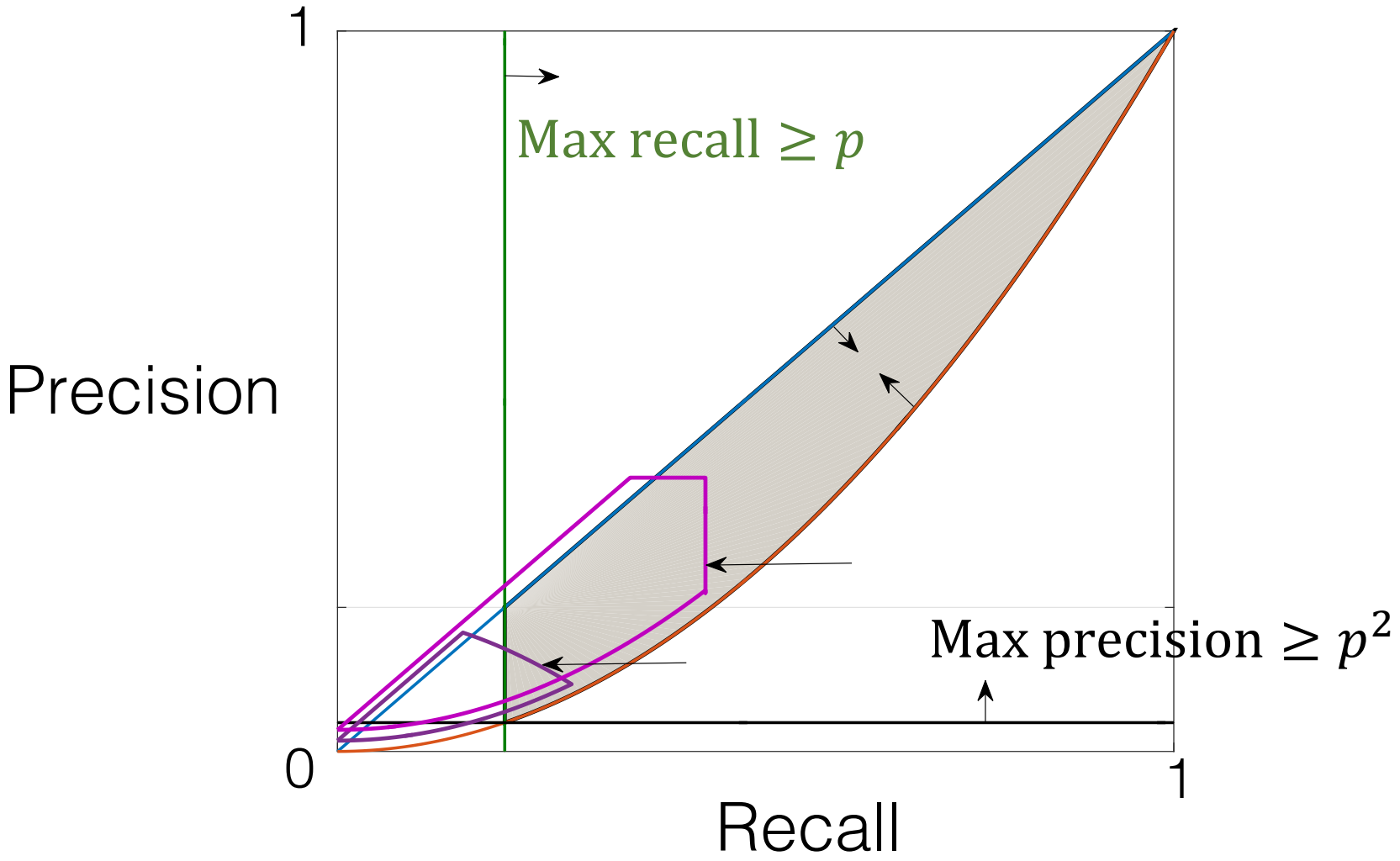


Precision

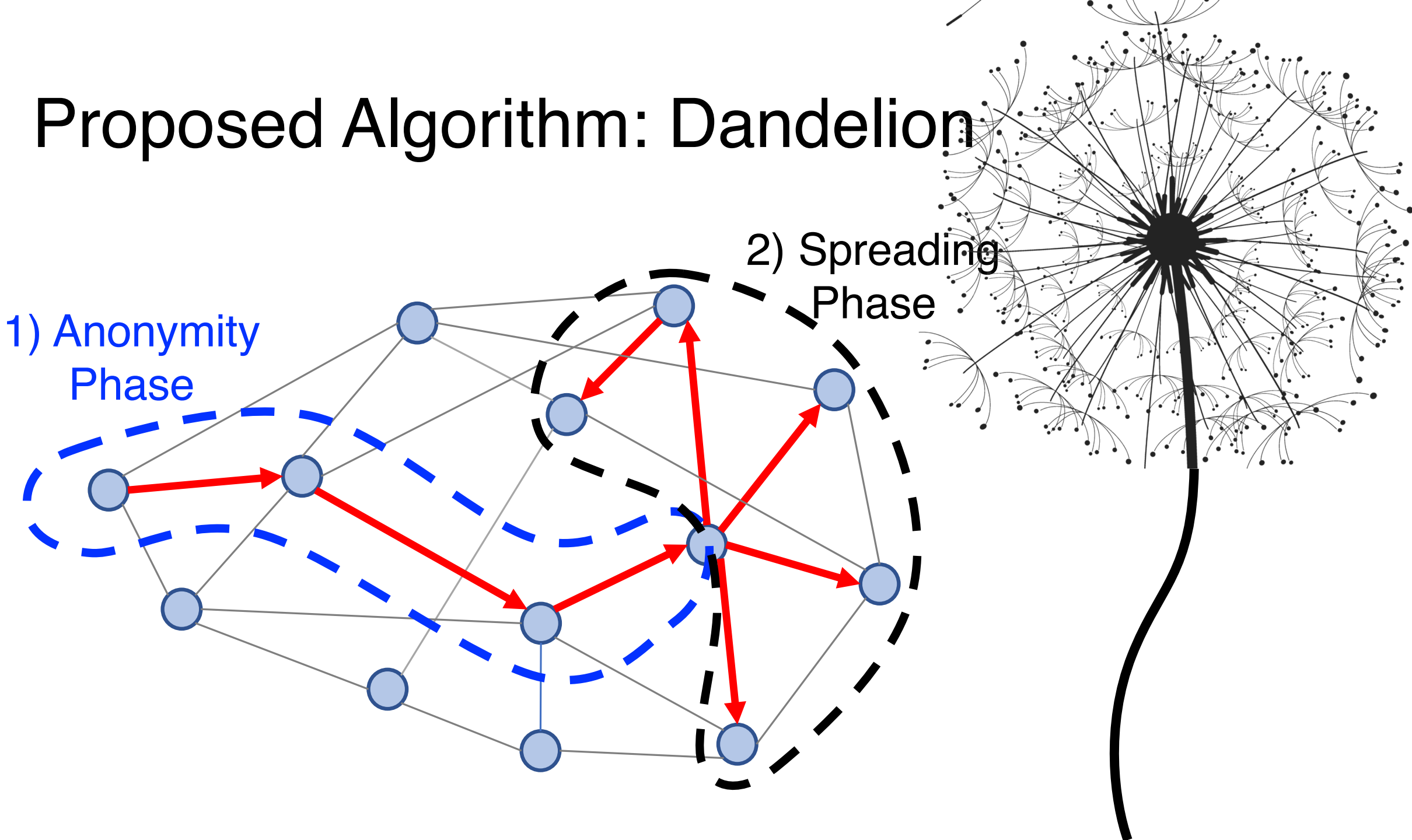
Goal:

Design a distributed flooding protocol that minimizes the maximum precision and recall achievable by a computationally-unbounded adversary.

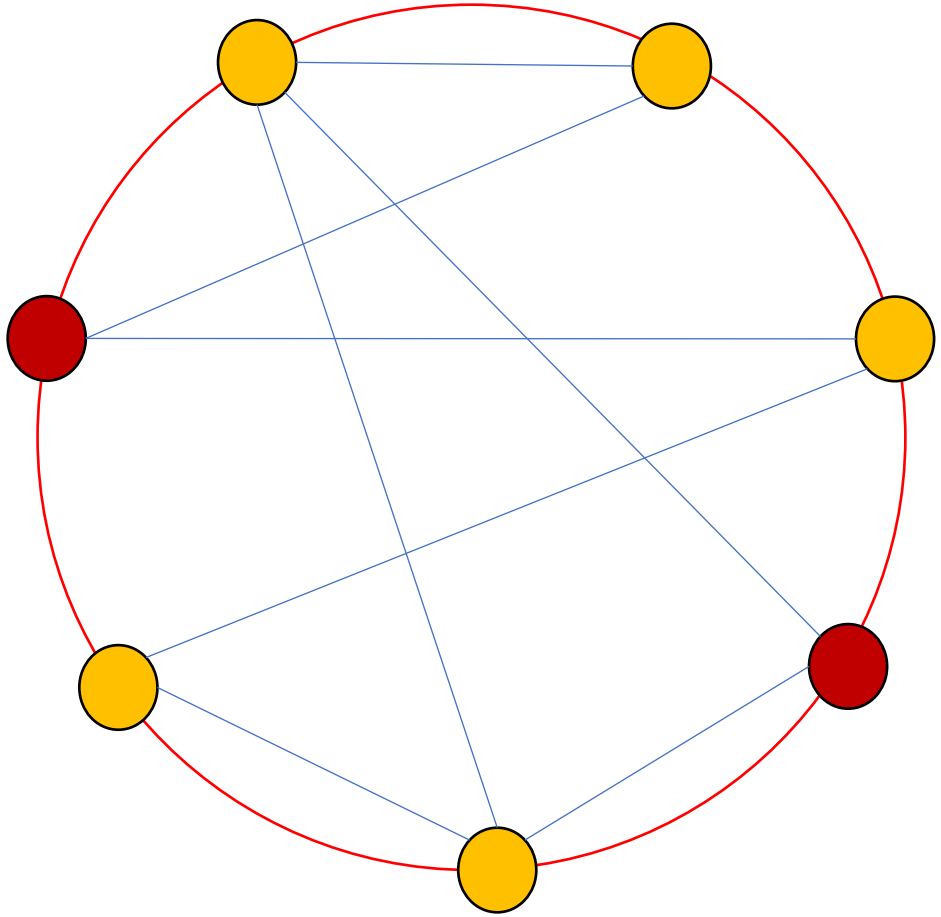
Fundamental Limits



Proposed Algorithm: Dandelion



How is Dandelion different from Tor?

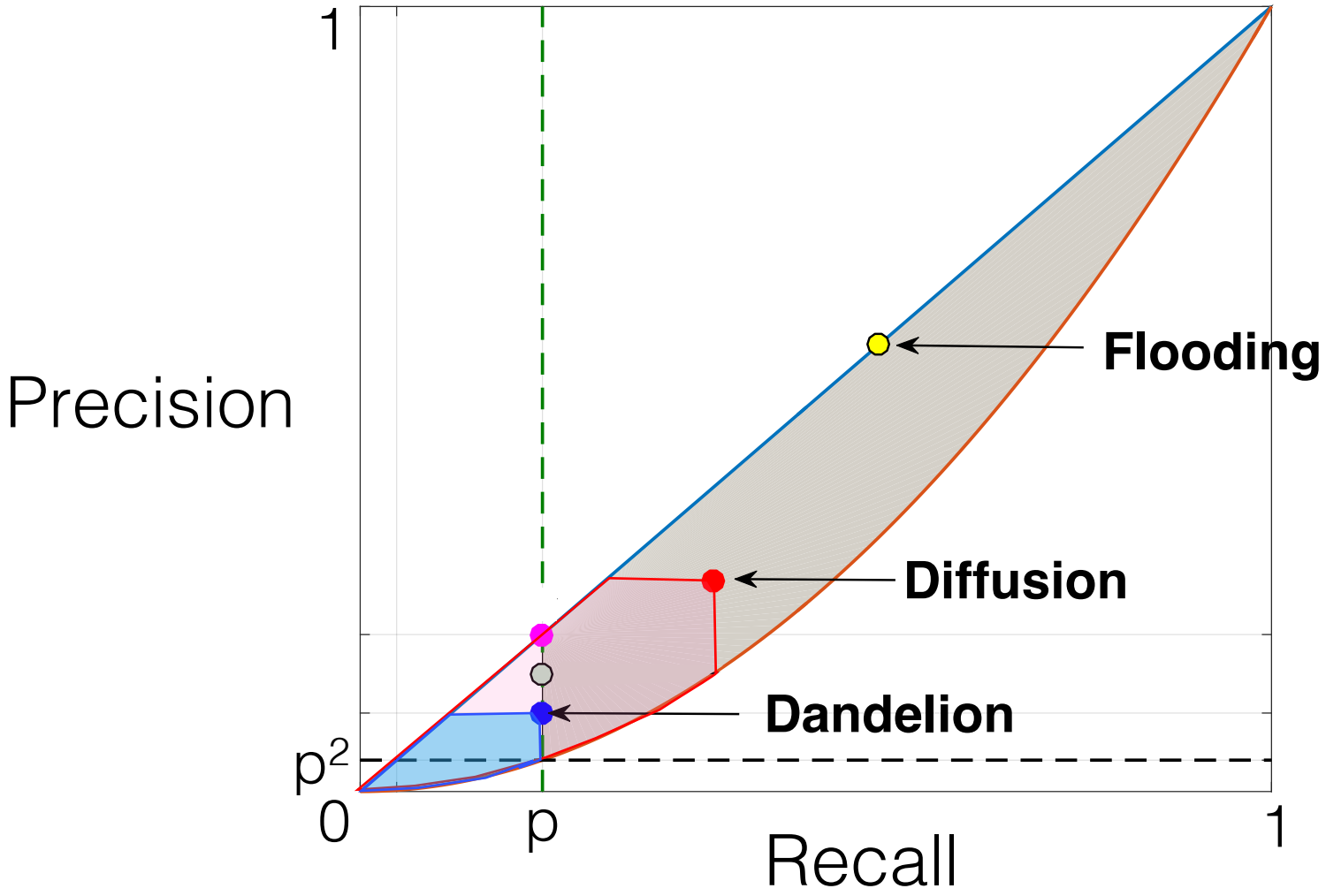


1) Messages propagate over the **same** cycle graph

2) Cycle graph changes dynamically.

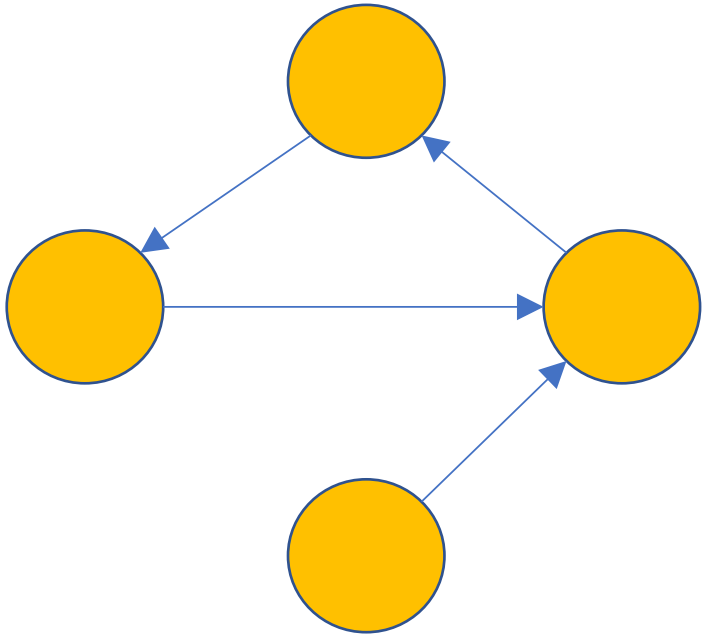
3) No encryption required.

Performance: Achievable Region

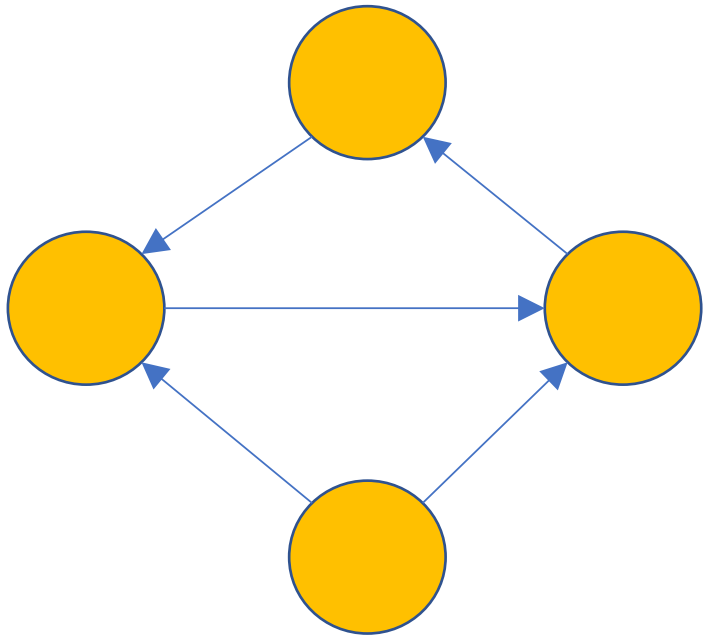


Practical Issues

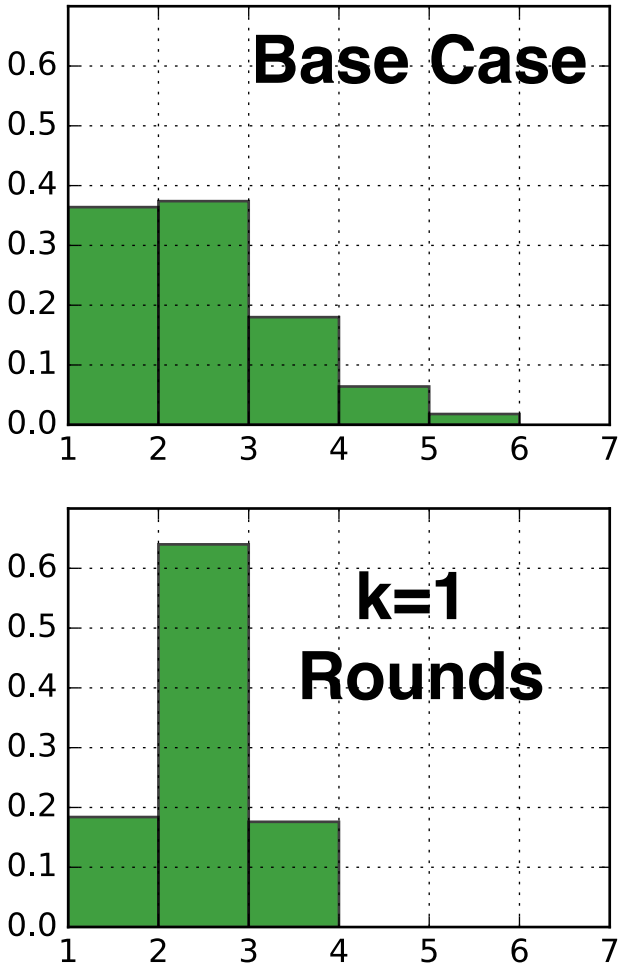
Constructing a Hamiltonian cycle



Base Case



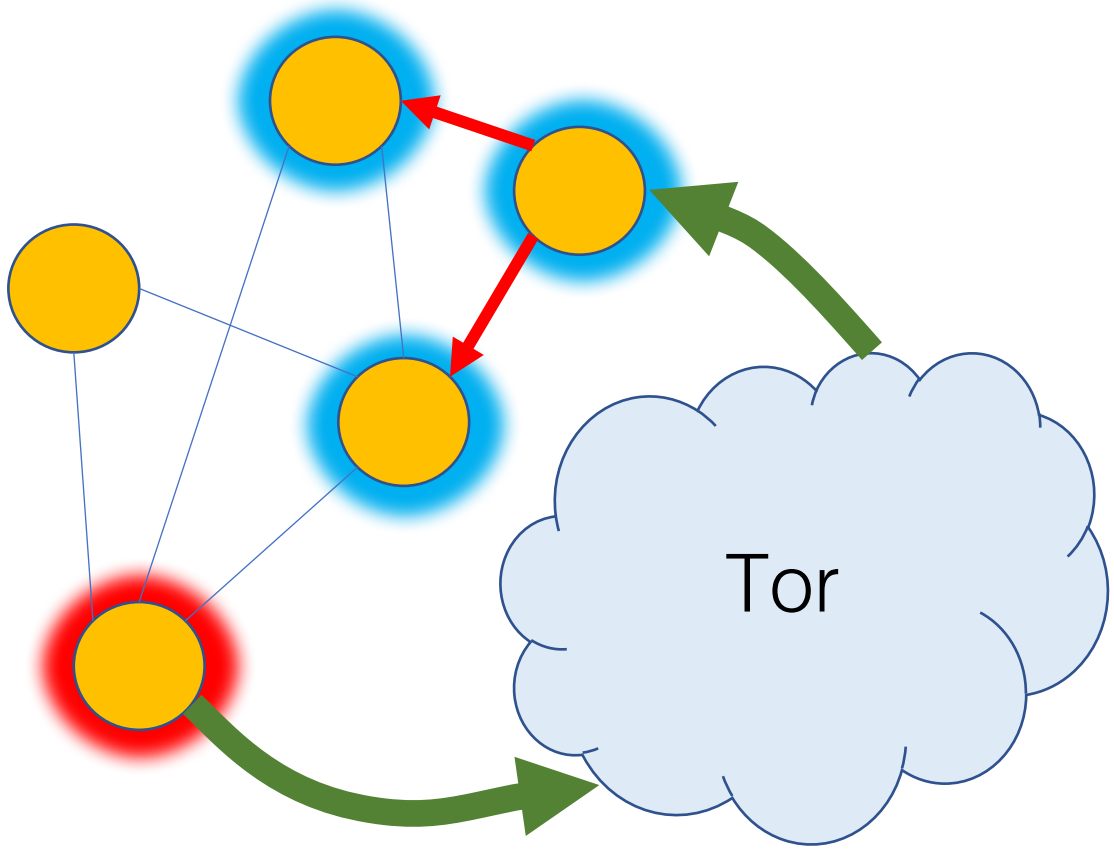
k=1 rounds of Degree-Checking



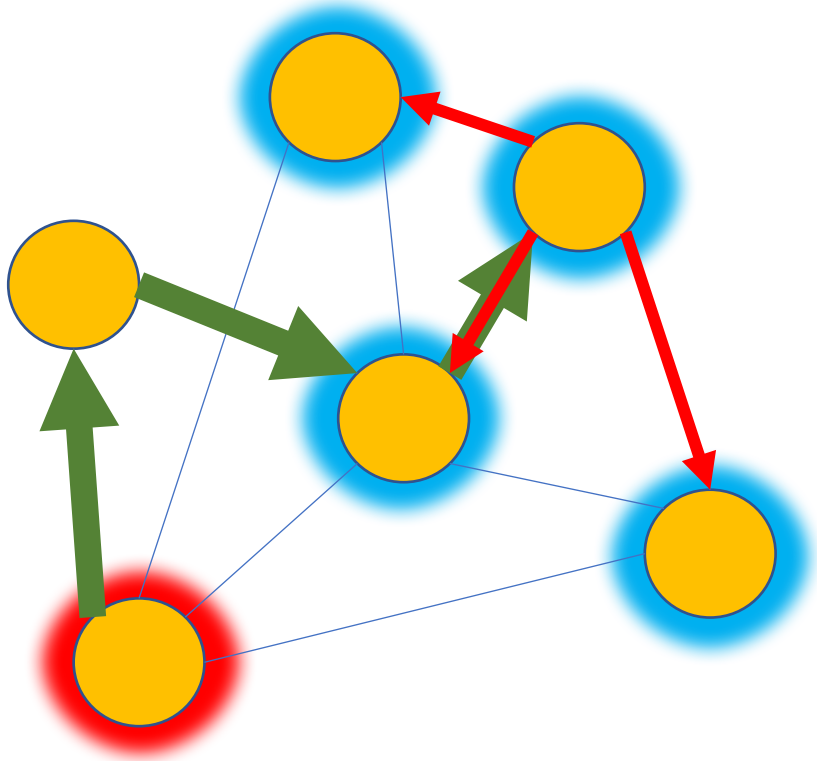
Degree

Comparison with Alternative Solutions

Connect through Tor



I2P Integration (e.g. Monero)



Next Steps

Byzantine nodes

Other adversarial models

Practical demonstration of viability

Take-Home Messages

1) Bitcoin P2P anonymity = ☹.

2) Moving from trickle to diffusion did not help.

3) Dandelion may be a lightweight solution for certain classes of adversaries.