



GossipSub: Secure Message Propagation in the Filecoin Blockchain

Team:

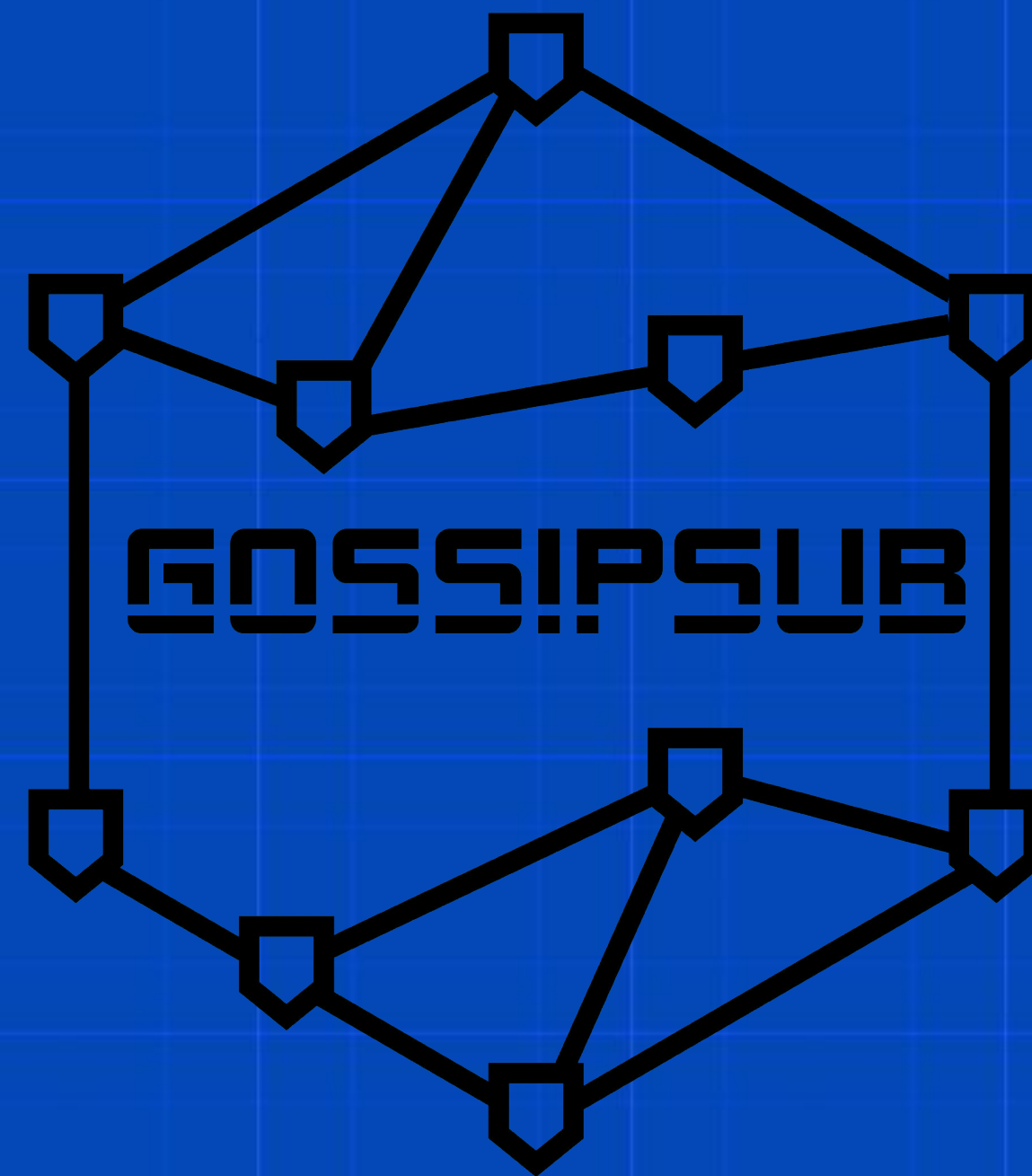
Dimitris Vyzovitis

Yusef Napora

Dirk McCormick

David Dias

Yiannis Psaras



libp2p



ResNetLab



Protocol Labs
Research



Outline

- The Filecoin Network
 - Message Propagation Protocols in Permissionless Blockchain Networks
 - The Gossipsub Protocol
 - Evaluation In Adversarial Environments
- 



**Filecoin is the decentralised storage
network for the Web3 and beyond**

Earn Filecoin for hosting files

The time to earn has arrived. Now anyone can become a cloud storage provider and make money from open hard drive space.

Start earning [↗](#)





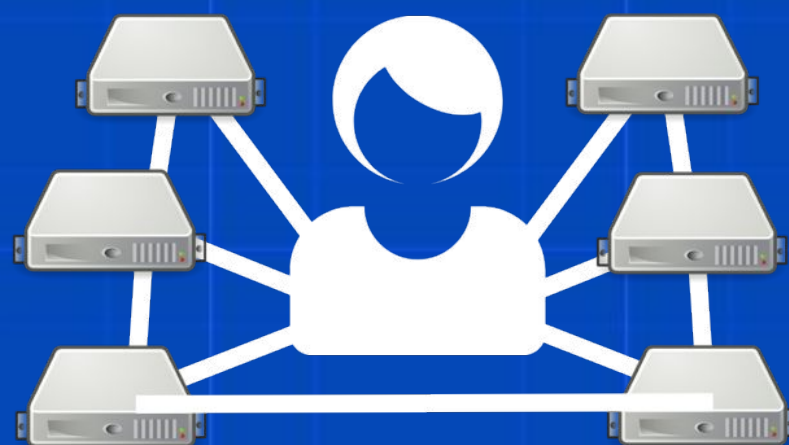
Filecoin Network Roles



Clients: hire the network to store data and pay for the storage with Filecoin



Miners: store data for the network, and its clients, collect Filecoin as a reward

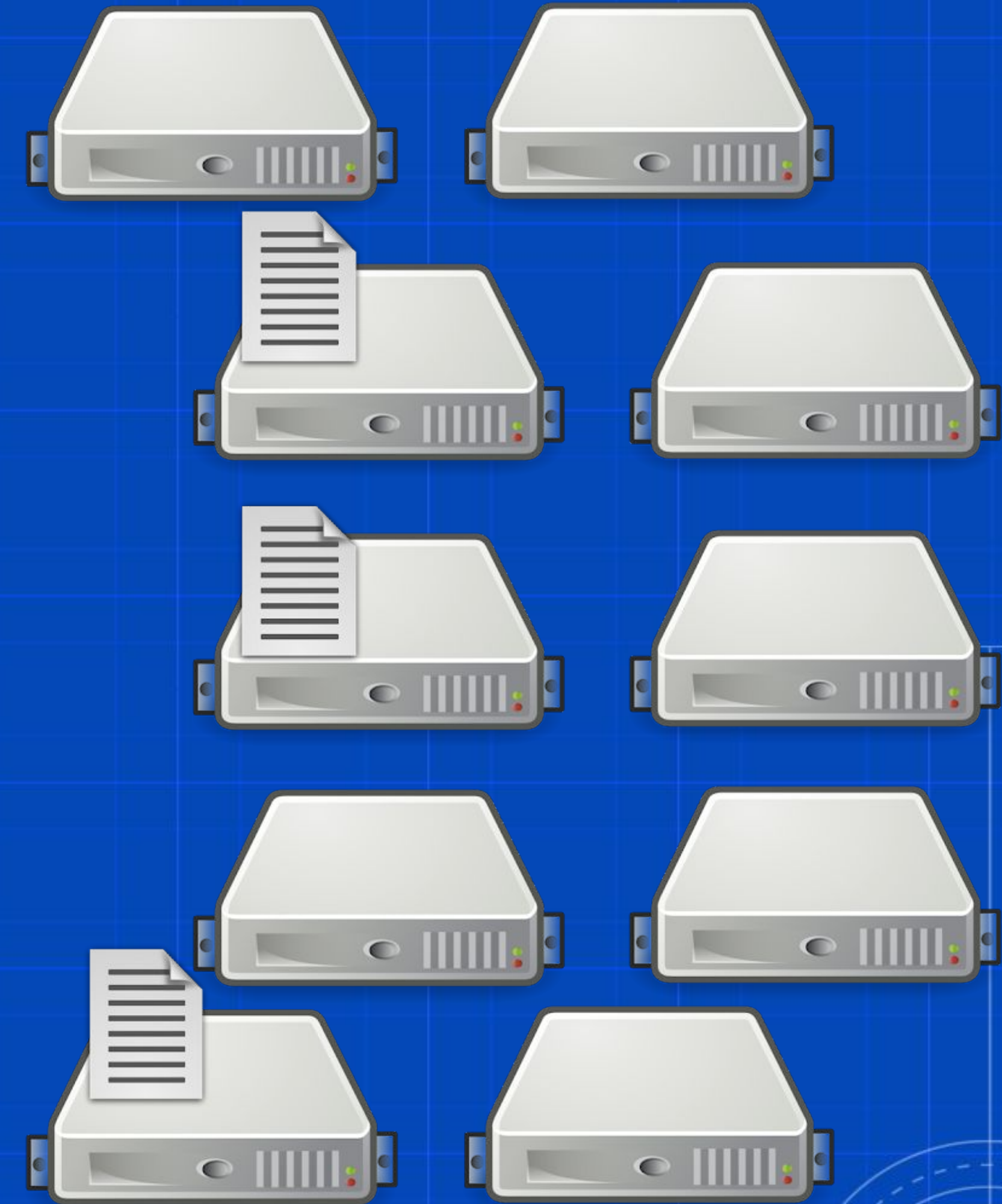


Network: organizes all work, verifies and repairs storage, rewards miners with Filecoin

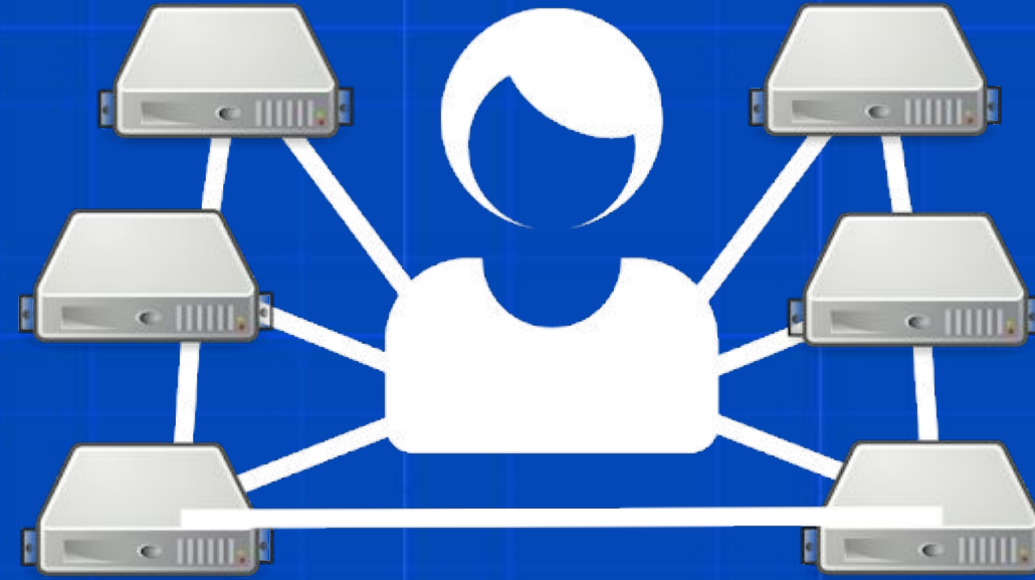
Clients want storage



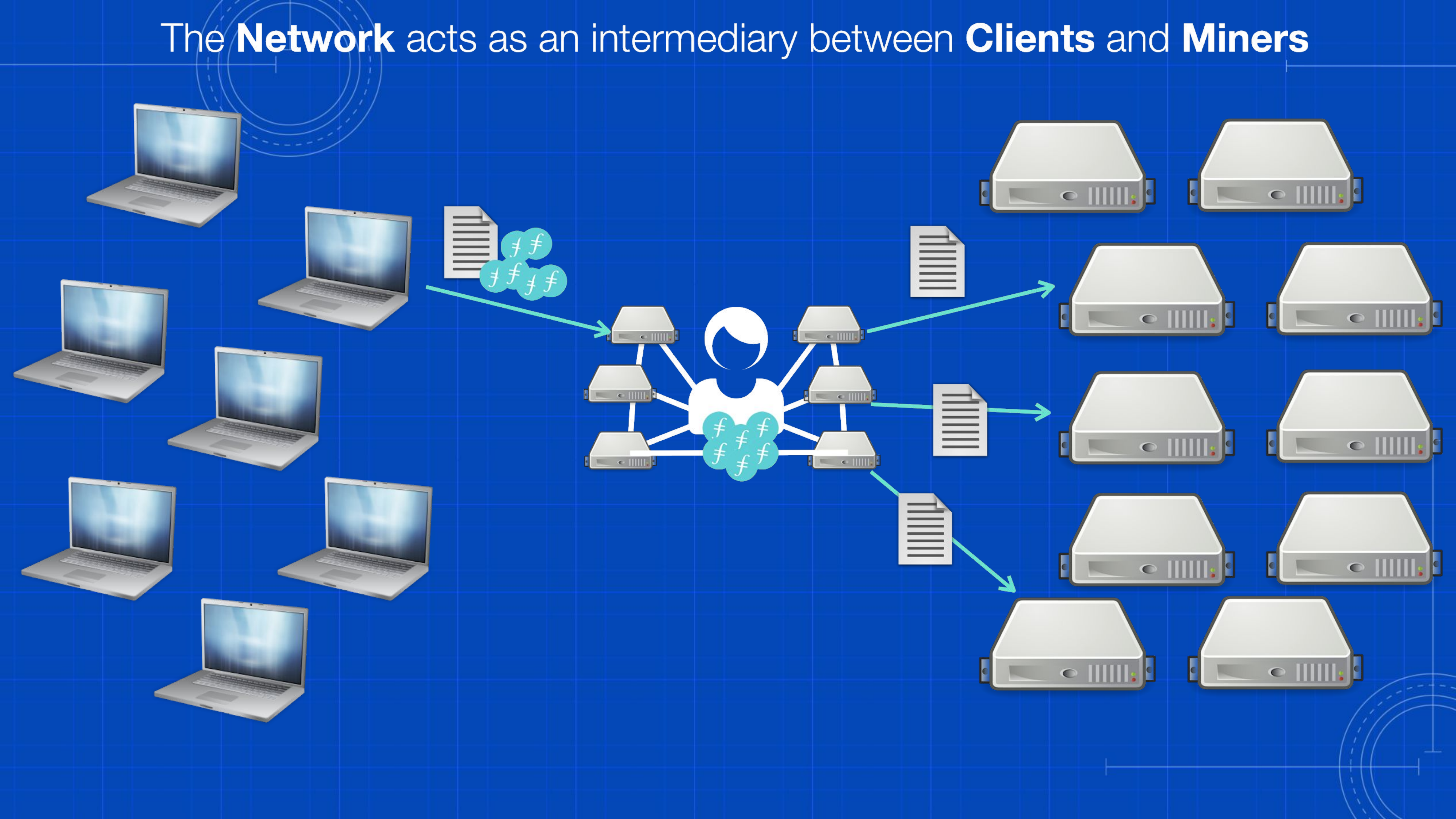
Miners provide storage



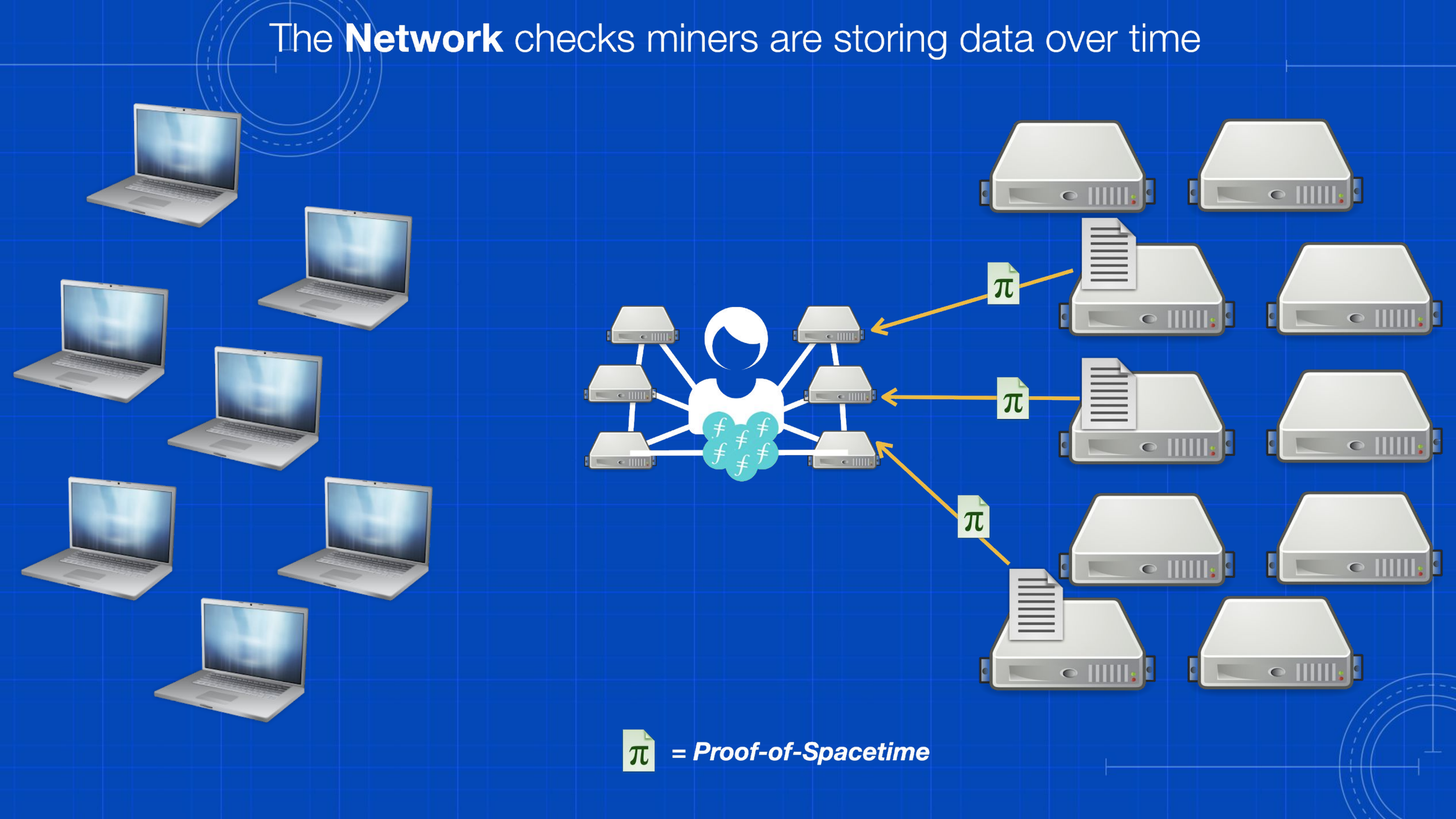
Network manages



The **Network** acts as an intermediary between **Clients** and **Miners**

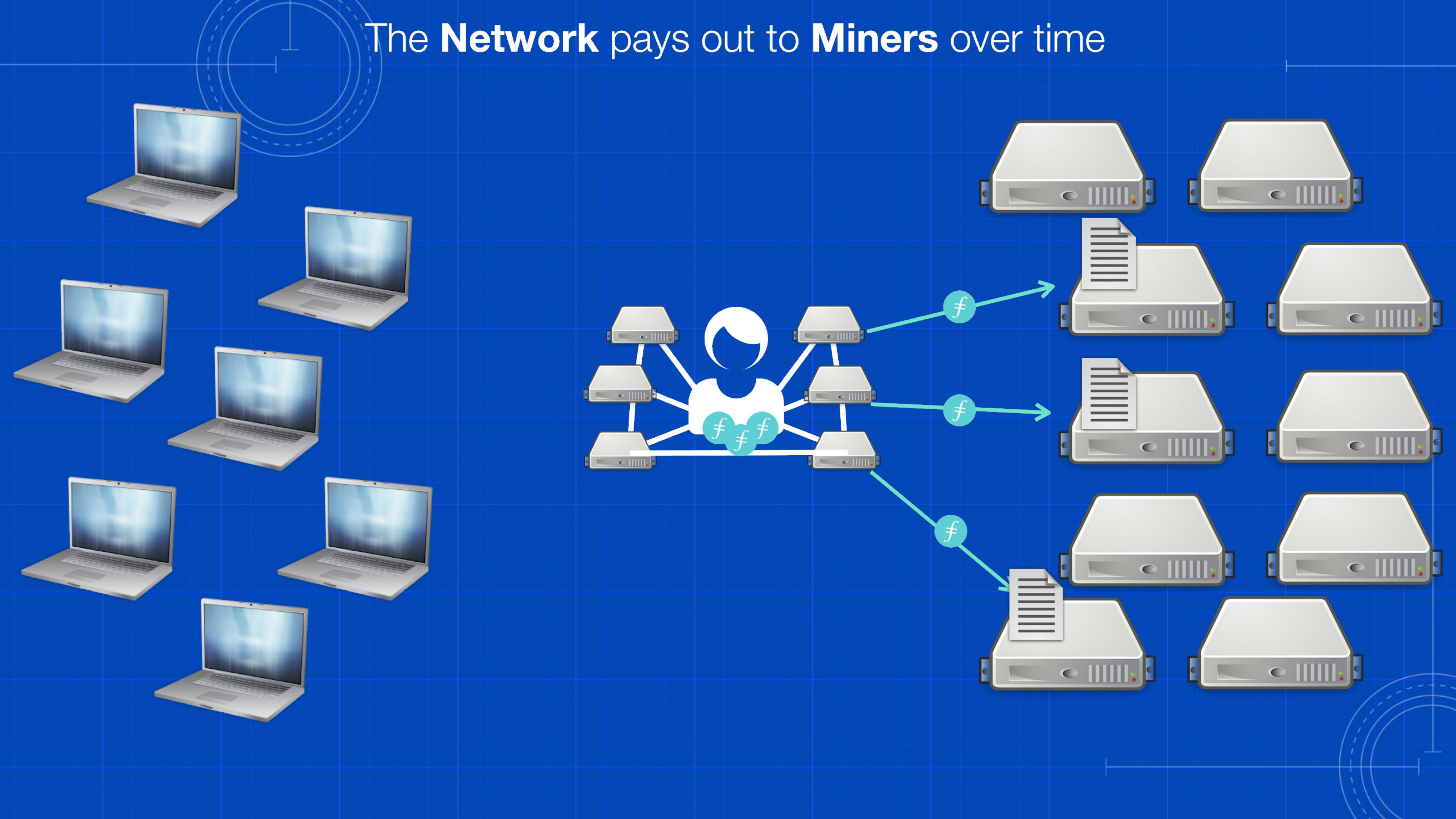


The **Network** checks miners are storing data over time

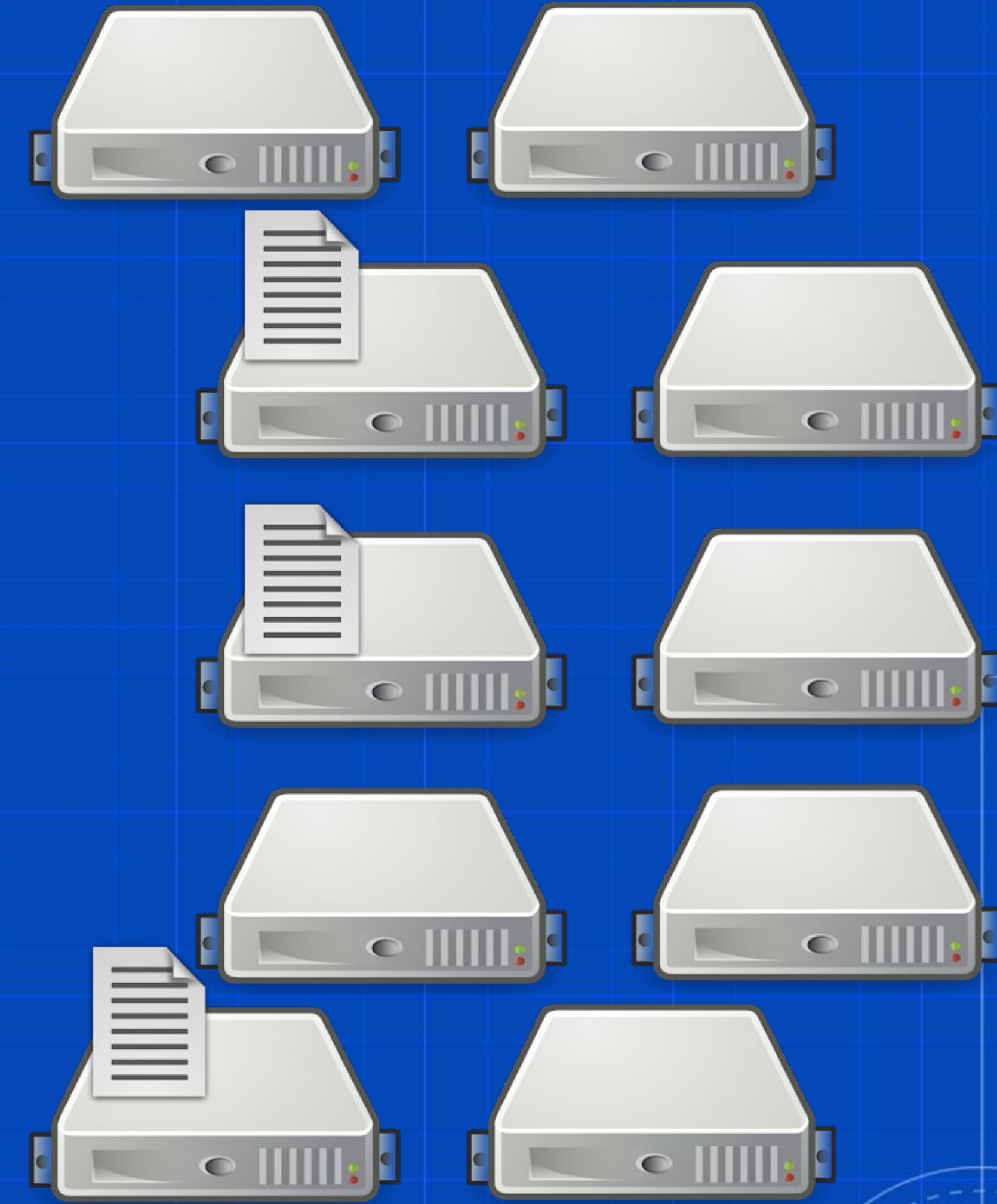
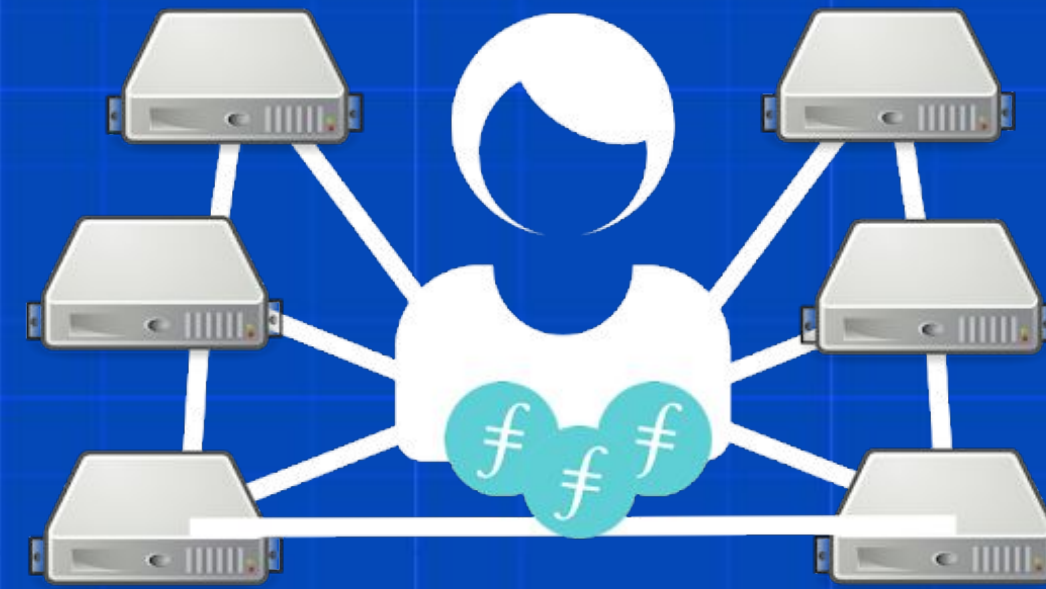


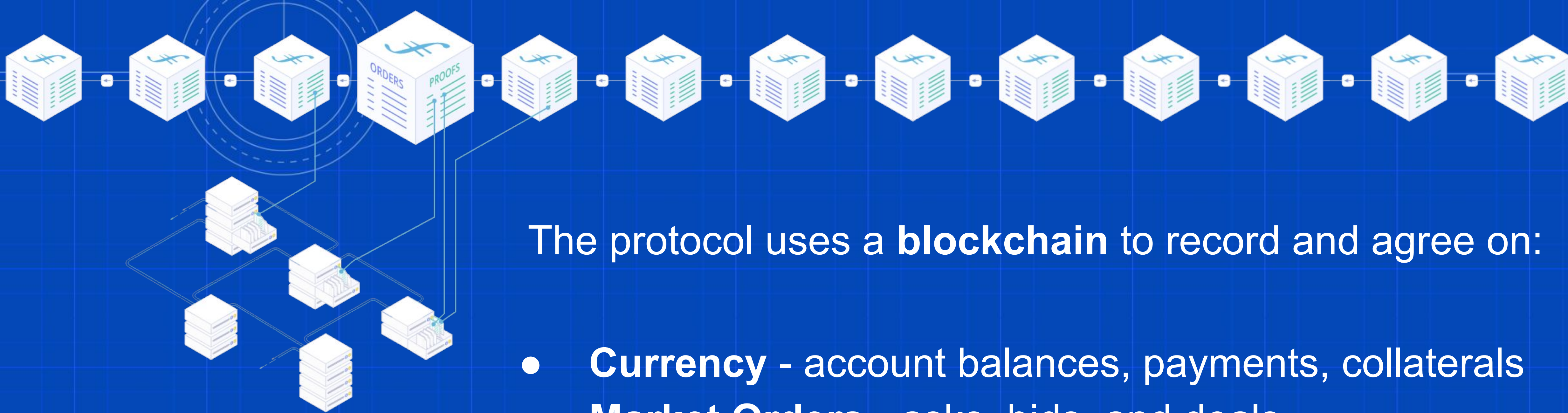
π = *Proof-of-Spacetime*

The **Network** pays out to **Miners** over time



Clients & Miners must be able to trust the **Network** to preserve data





The protocol uses a **blockchain** to record and agree on:

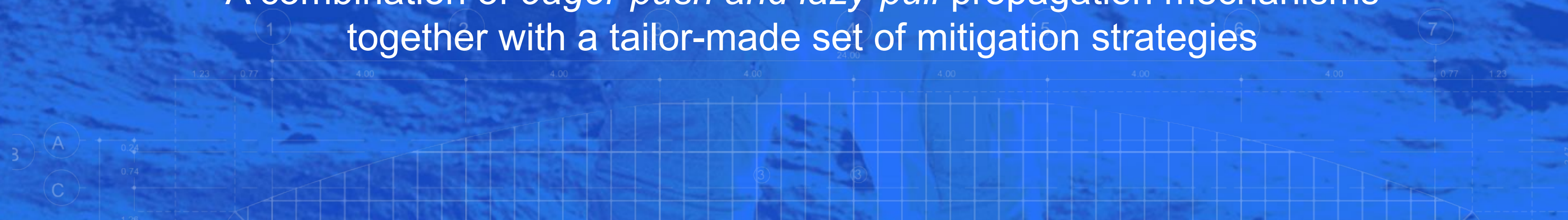
- **Currency** - account balances, payments, collaterals
- **Market Orders** - asks, bids, and deals
- **Allocations** - which miners store which pieces
- **Proofs** - a verifiable record of correct behaviors
- **Contracts** - state and execution of smart contracts



GossipSub

A PubSub protocol designed for efficiency and resilience against malicious nodes

A combination of *eager-push* and *lazy-pull* propagation mechanisms together with a tailor-made set of mitigation strategies



Problem & Requirements

Property: *Permissionless blockchains are open for anyone to join. There is no pre-authentication, or access control.*

Problem: *It is very easy for malicious nodes to join and attempt to disrupt the permissionless system*



Avoid Network Fragmentation and Forks

Fragmentation of the blockchain network gives attackers the chance to double-spend or steal monetary value



Verification & Consensus

Cryptographic proofs enable miners to verify the validity of transactions



Keep nodes in sync

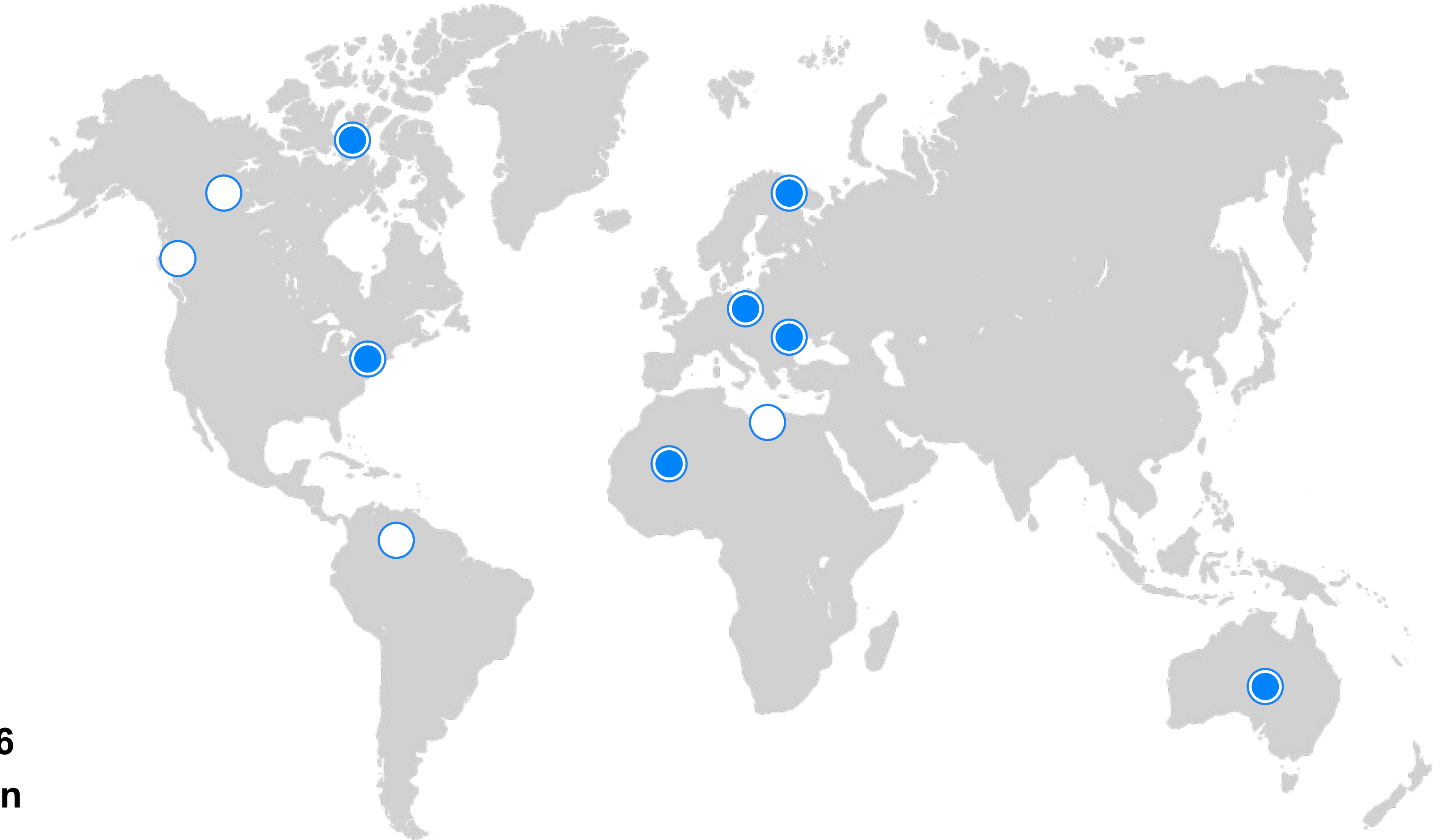
In order to enable correct verification, all nodes need to have received all published messages



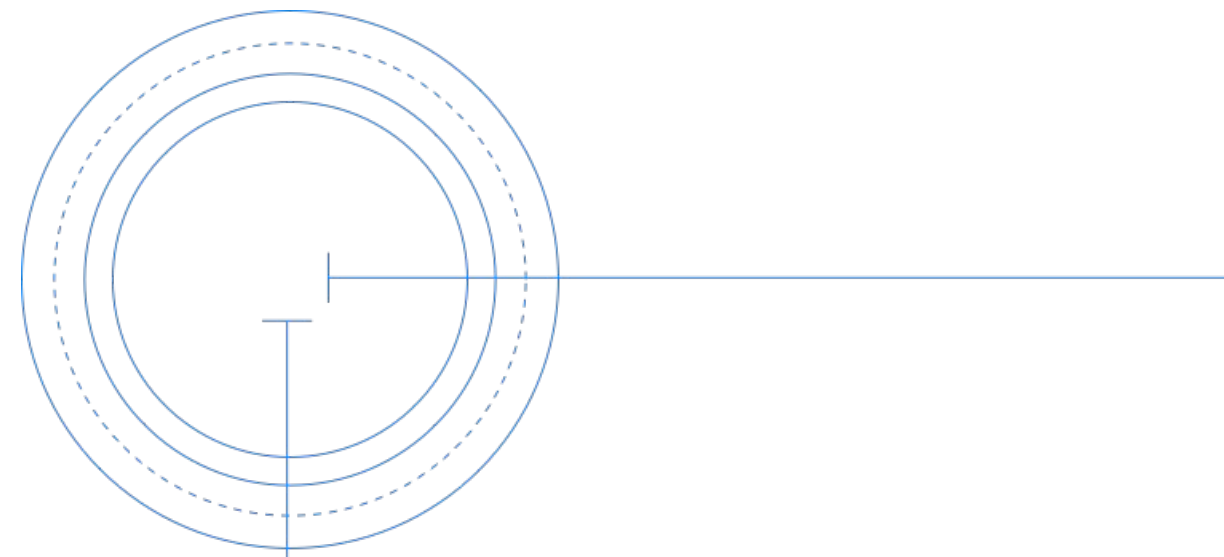
Filecoin Deadline



All nodes participating in the Filecoin Blockchain need to have received all newly published messages **within 6 seconds of their publication time**



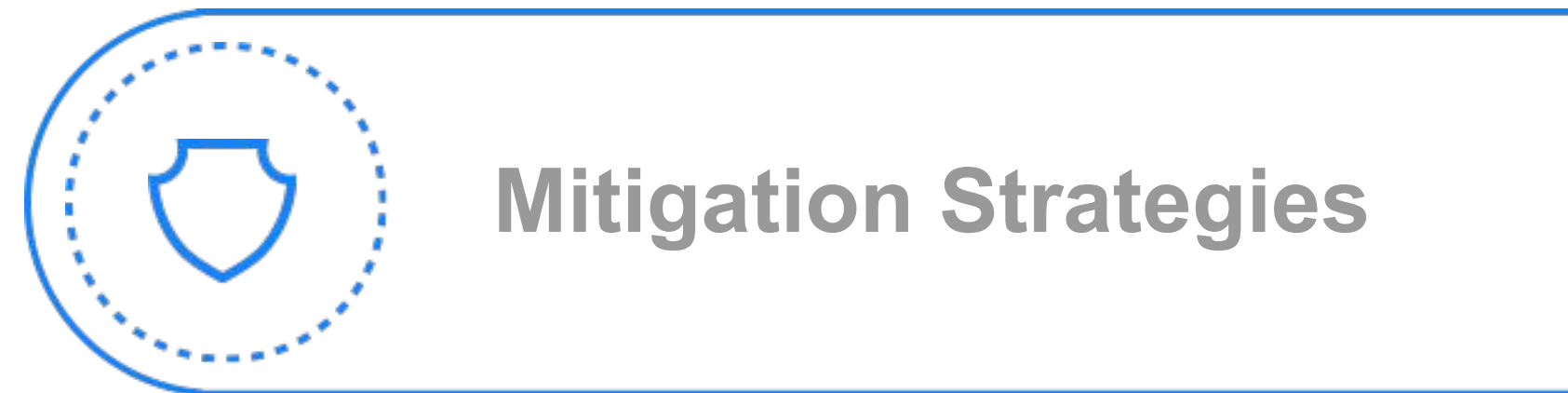
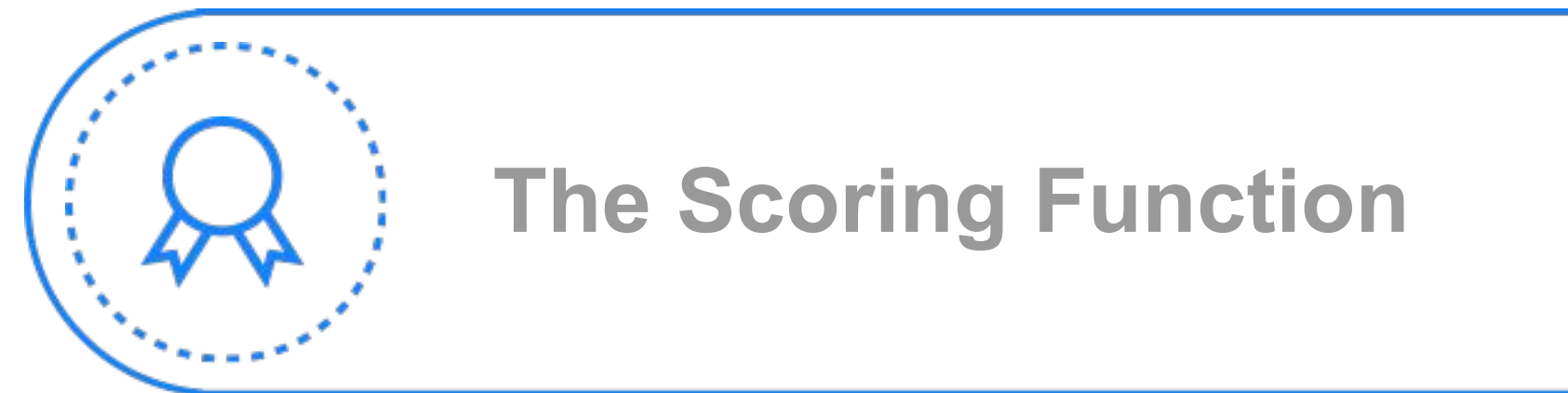
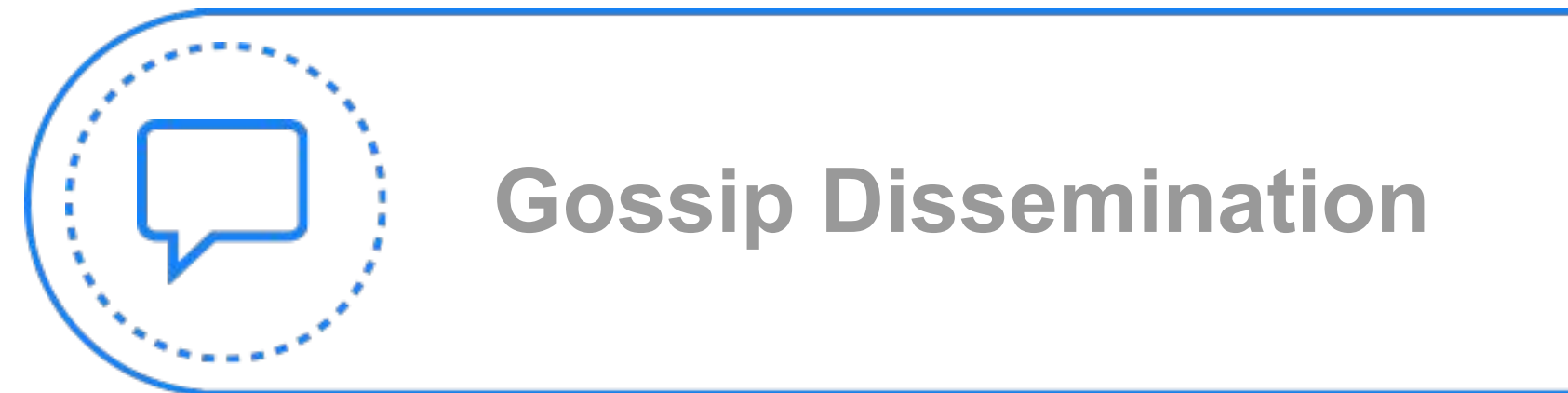
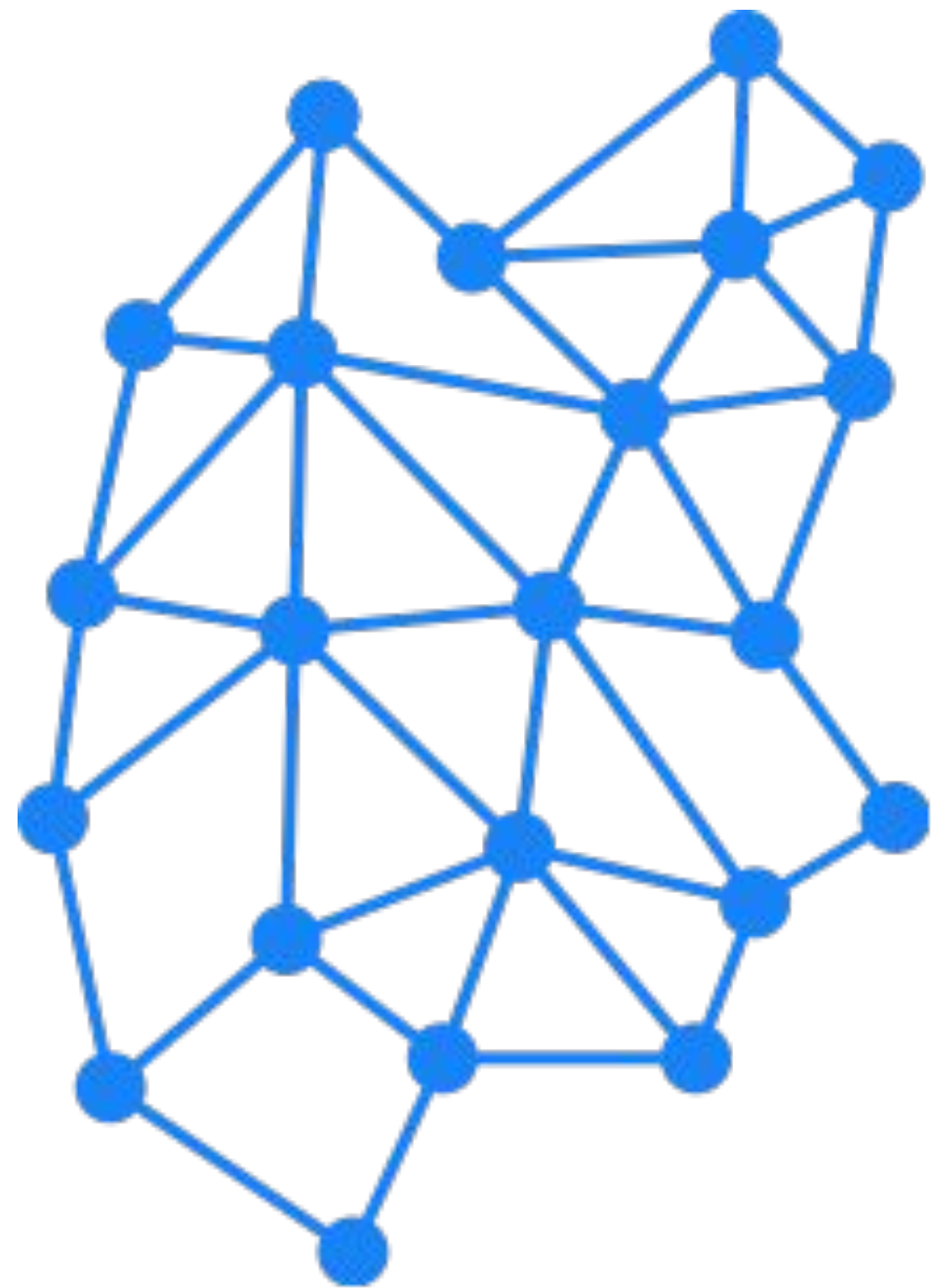
Attacks



Range of primitive attacks tested:

1. Sybil Attack
2. Eclipse Attack
3. Censorship Attack
4. Degrade Attack
5. Cold Boot Attack
6. Covert Flash Attack

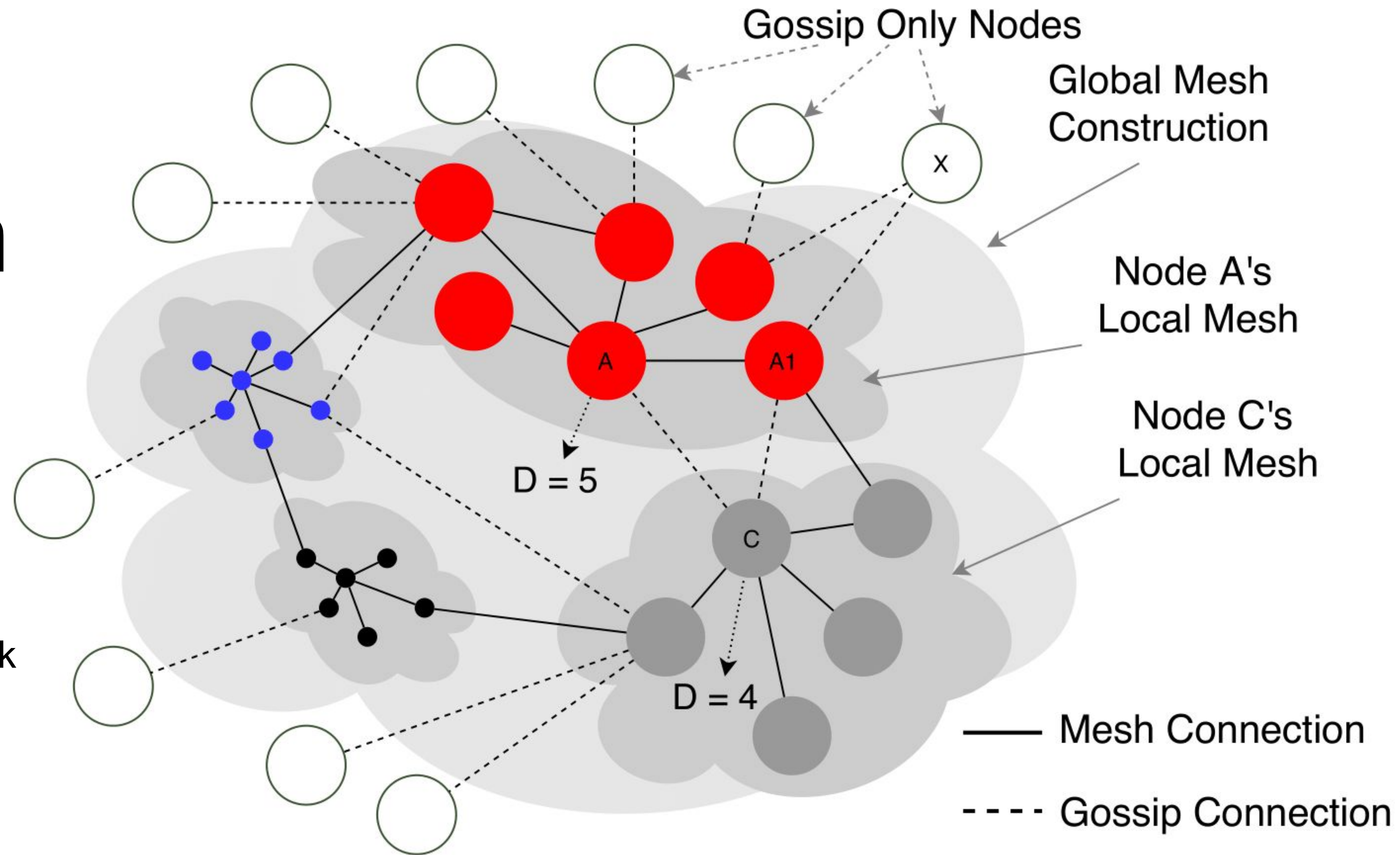
GossipSub in a Nutshell



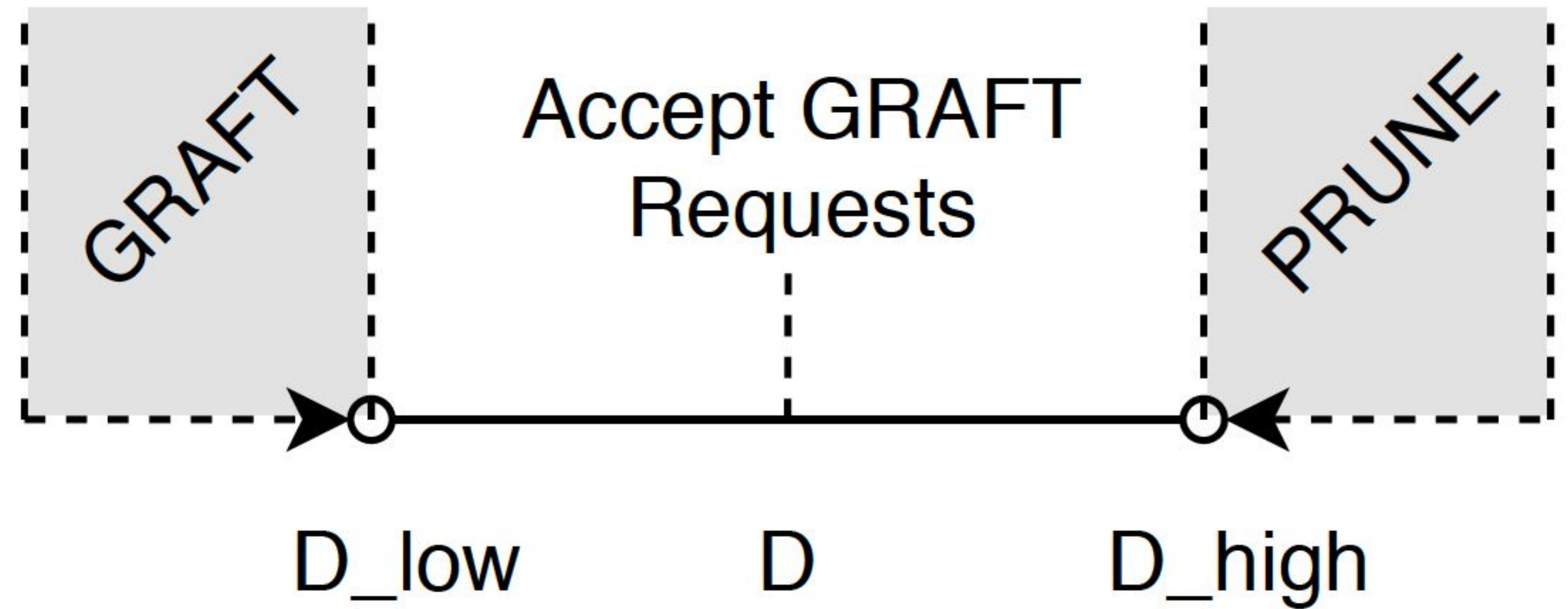
The Mesh Construction

Concepts:

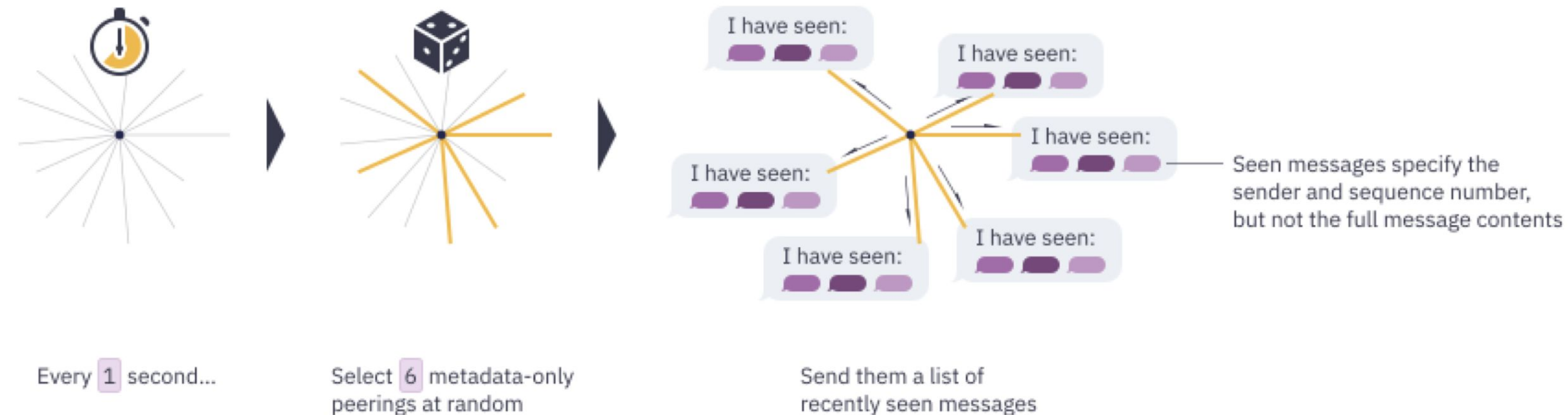
- Global Mesh vs Local Mesh
- No peer has full view of the network
- Three types of messages:
 - GRAFT,
 - PRUNE,
 - PRUNE Peer Exchange



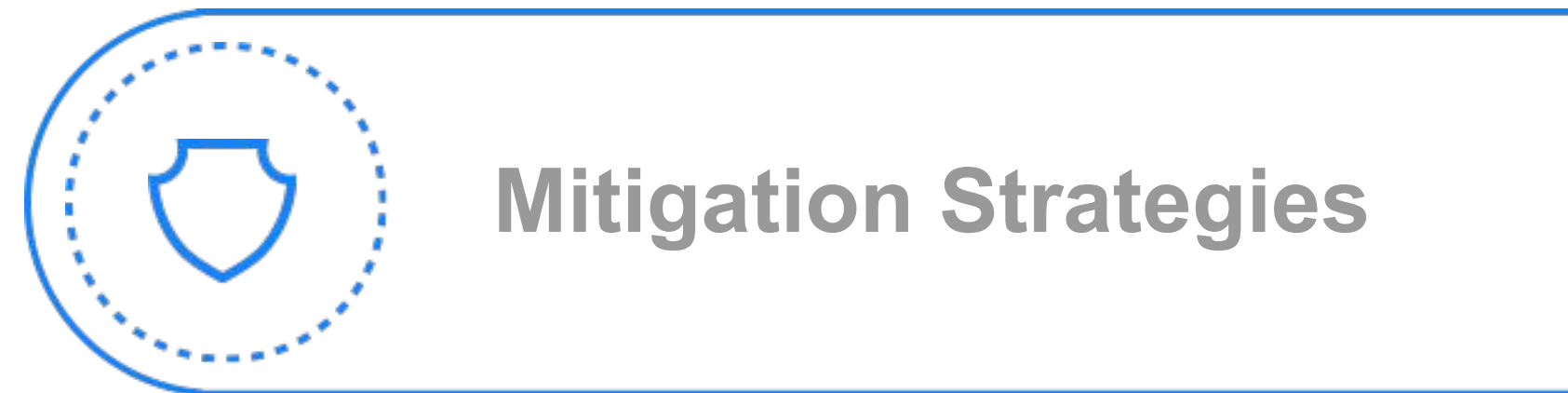
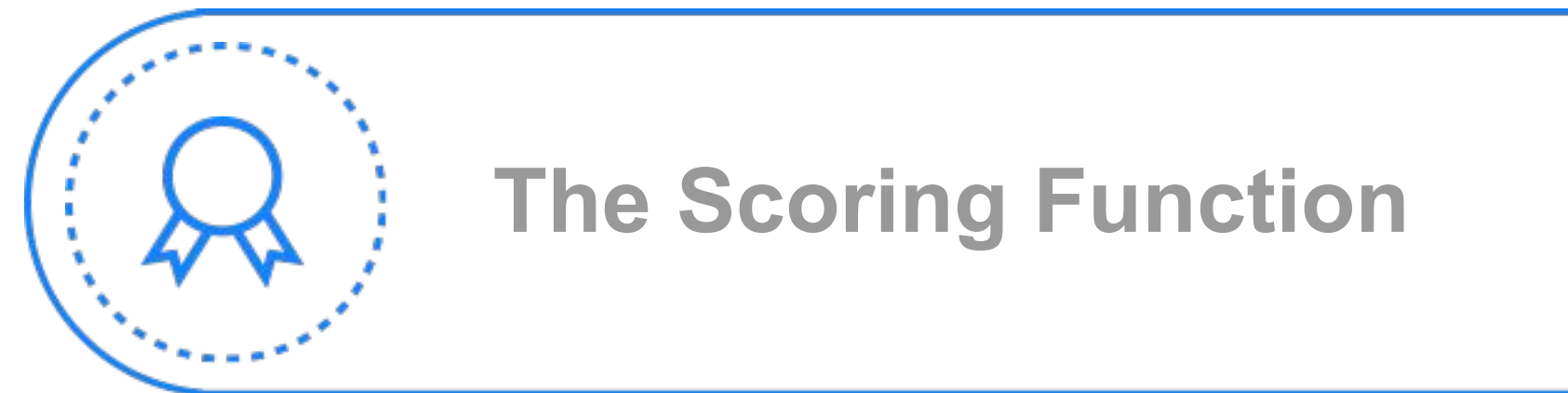
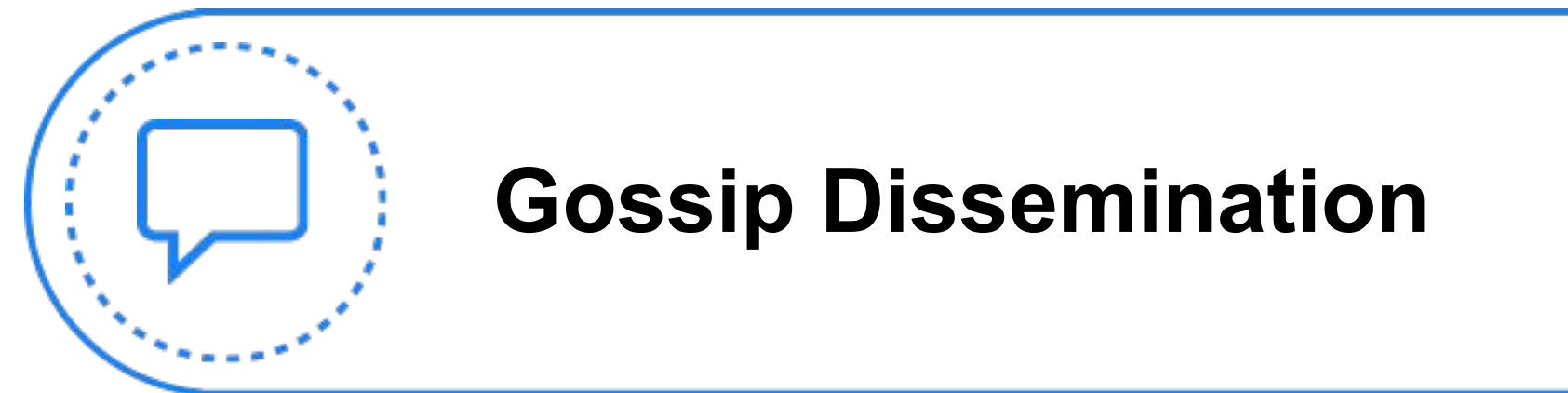
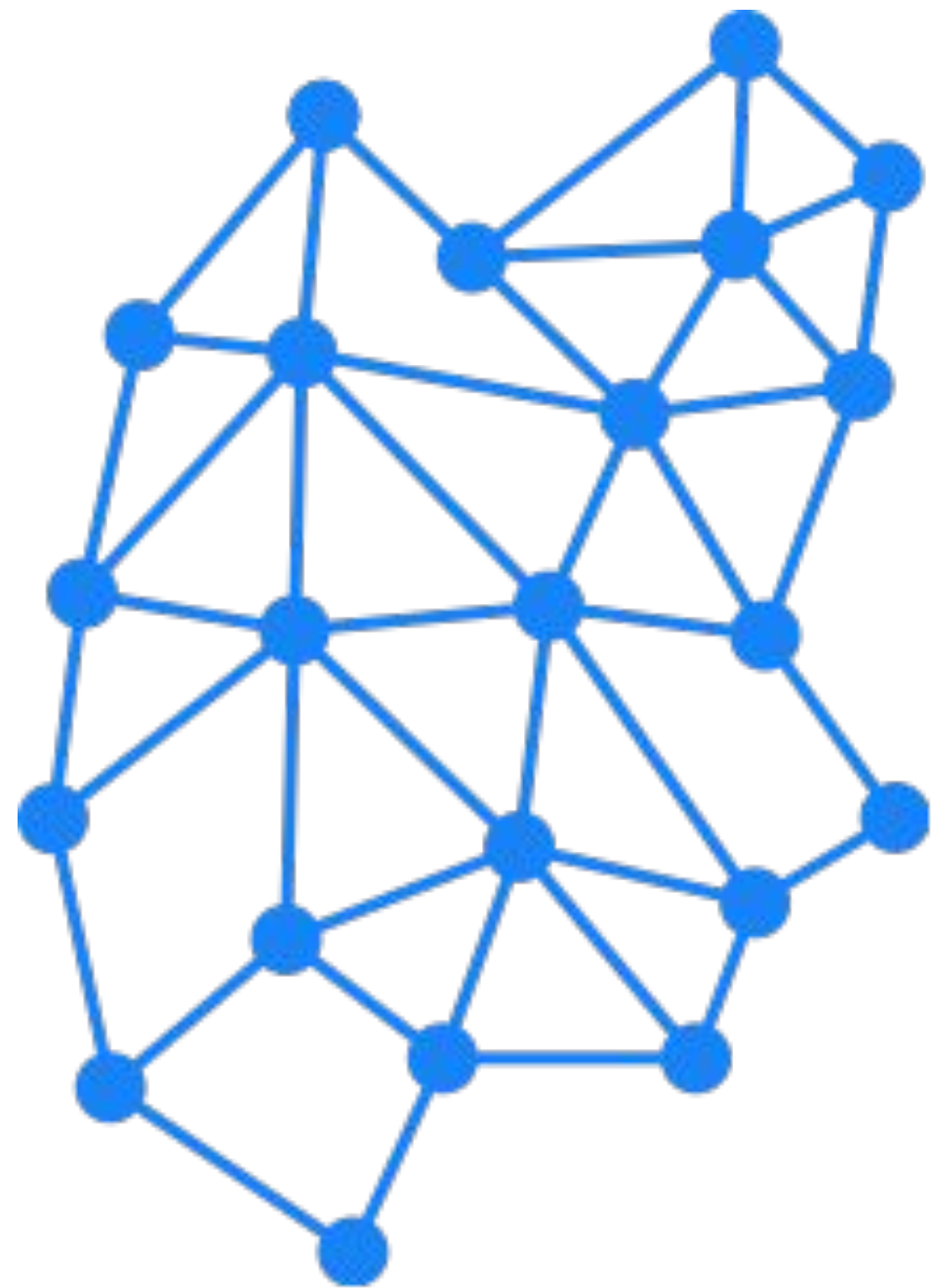
Node Degree & Heartbeat



$D_{low} = 6, D = 8, D_{high} = 12$



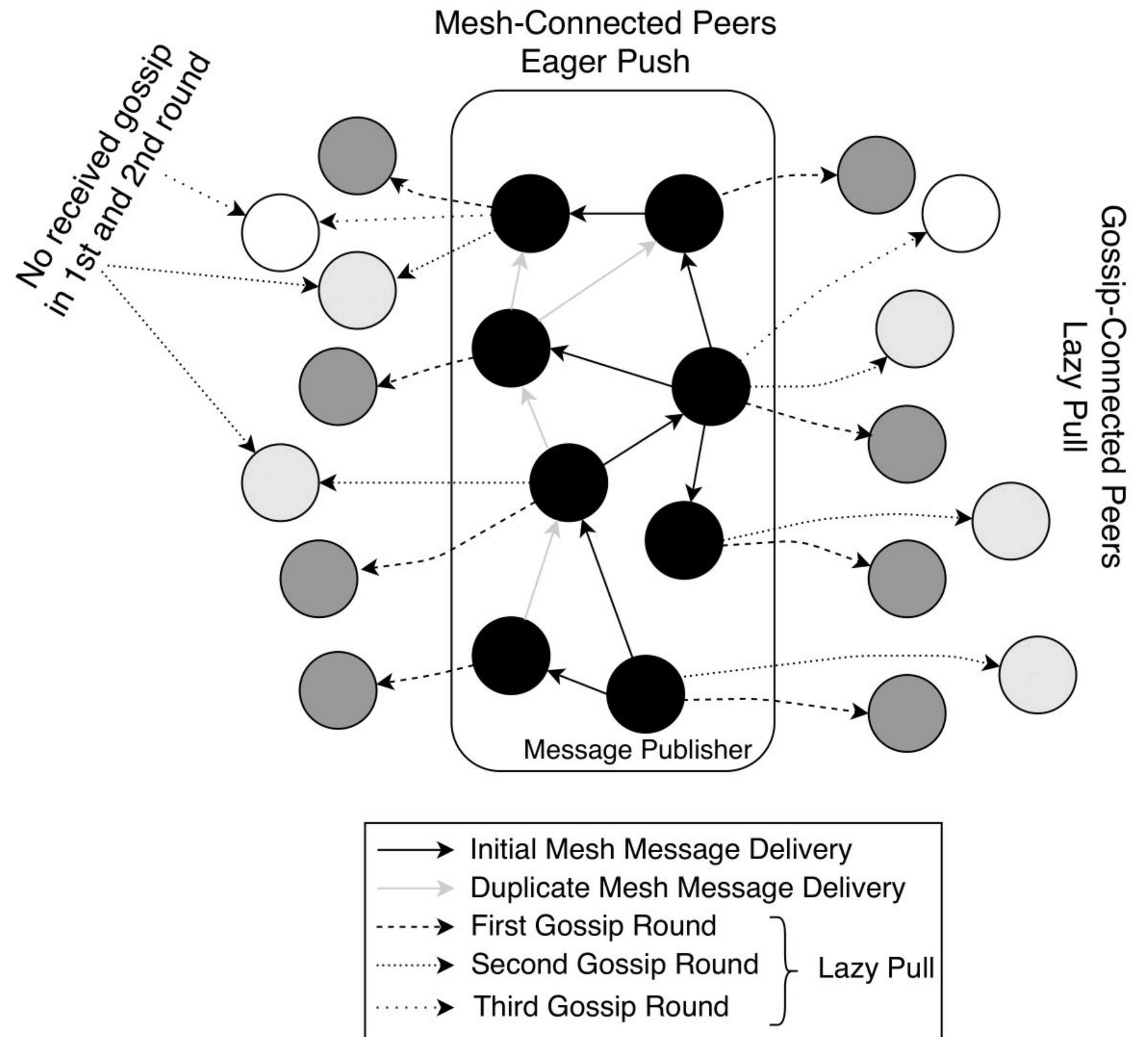
GossipSub in a Nutshell



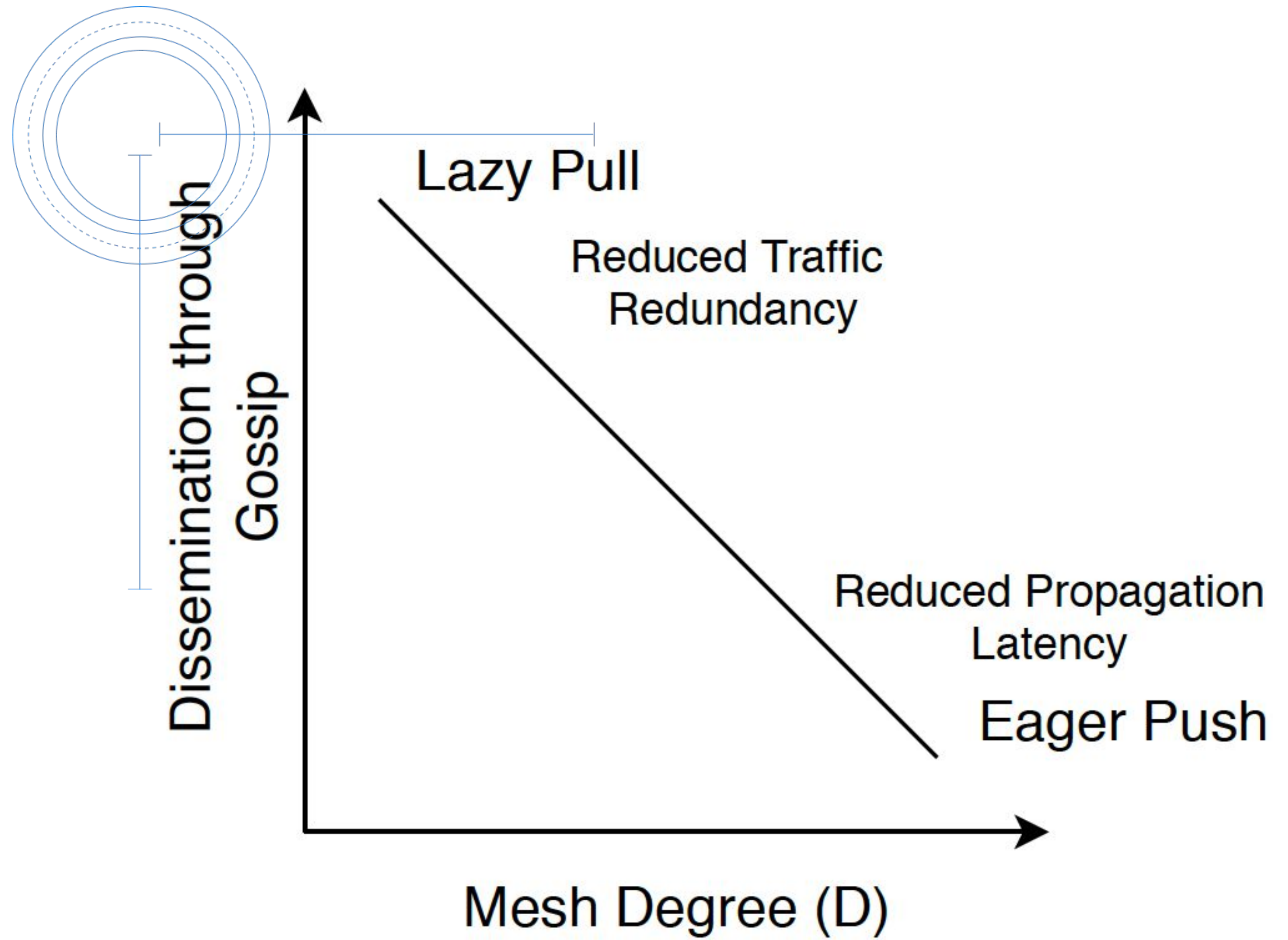
Gossip - Metadata only

Concepts:

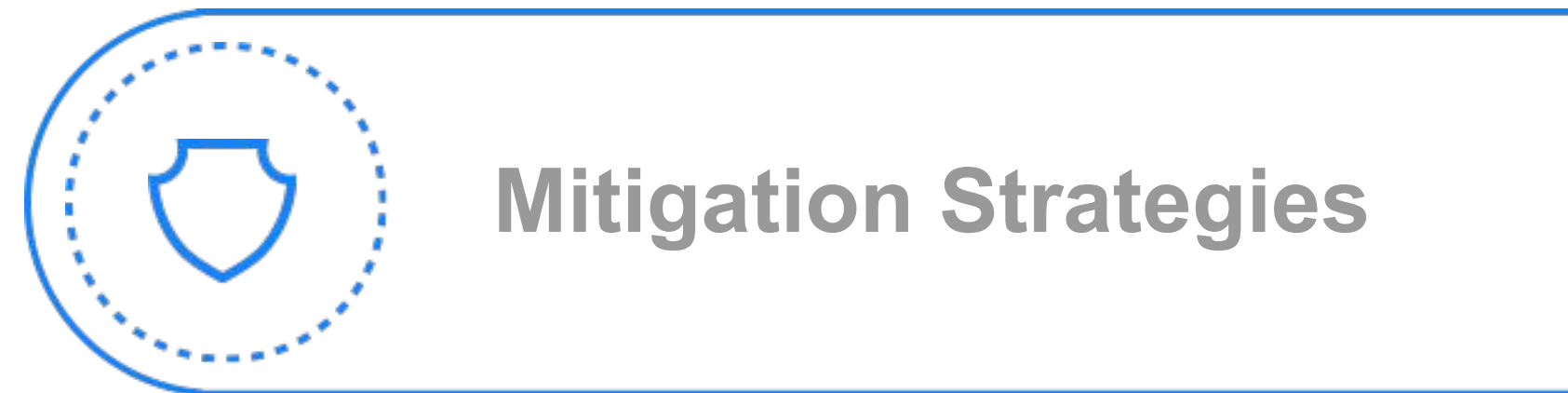
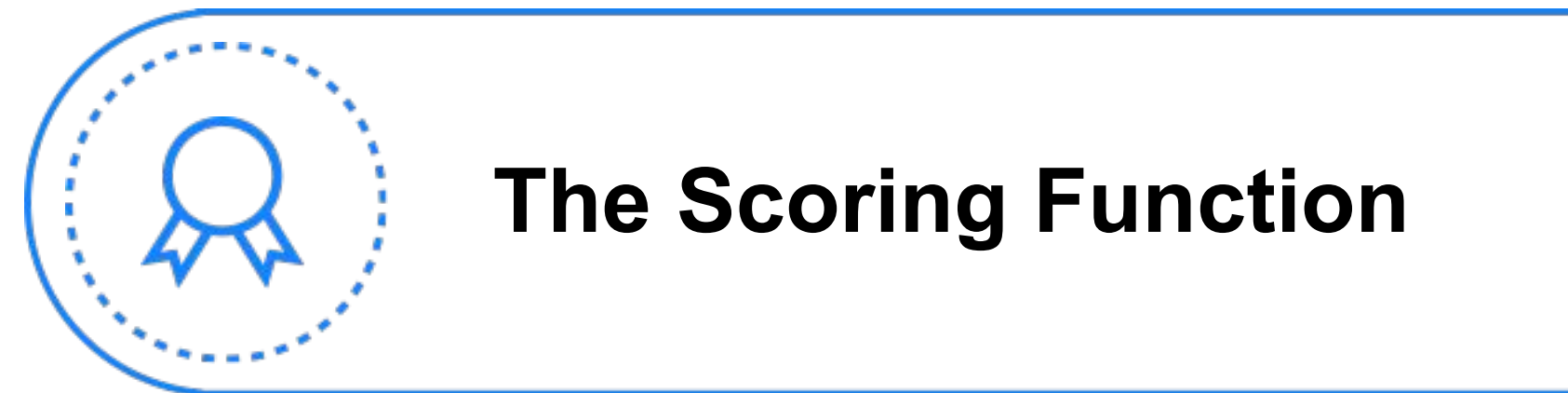
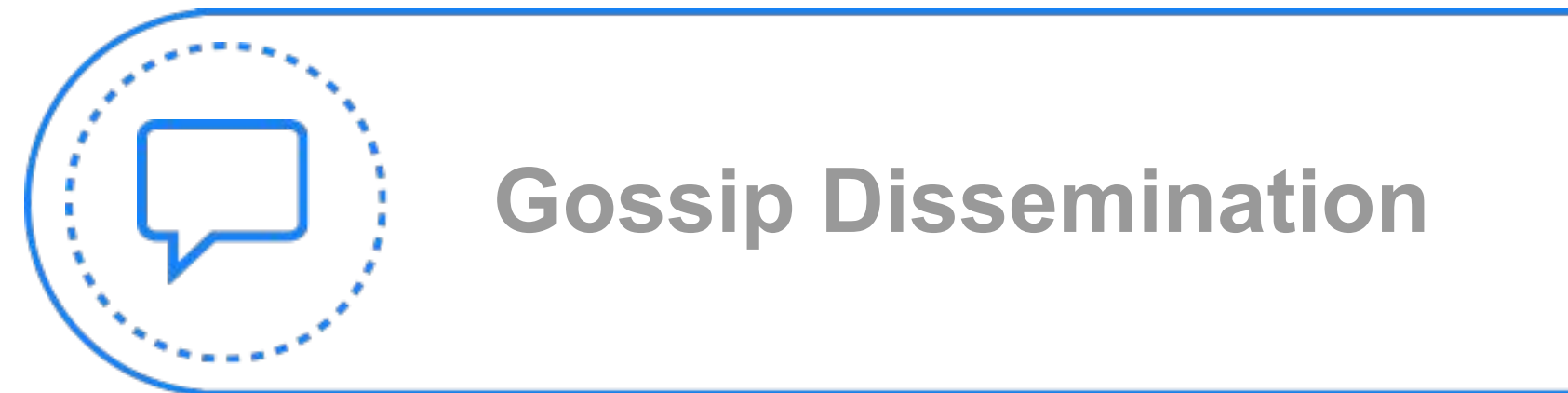
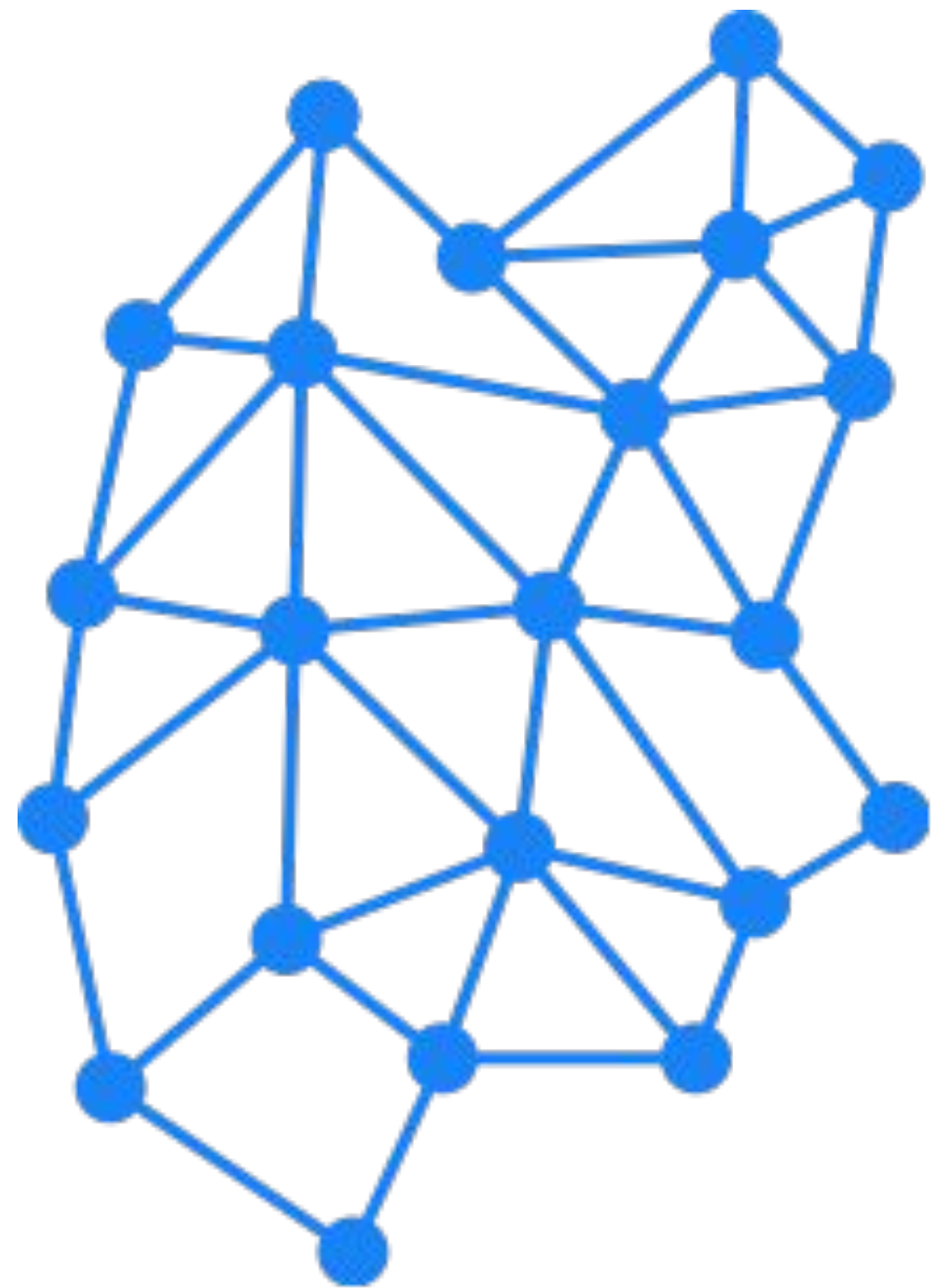
- Three rounds of gossip, on every *heartbeat* = 1sec
- Two types of messages:
 - IHAVE
 - IWANT



Tradeoffs



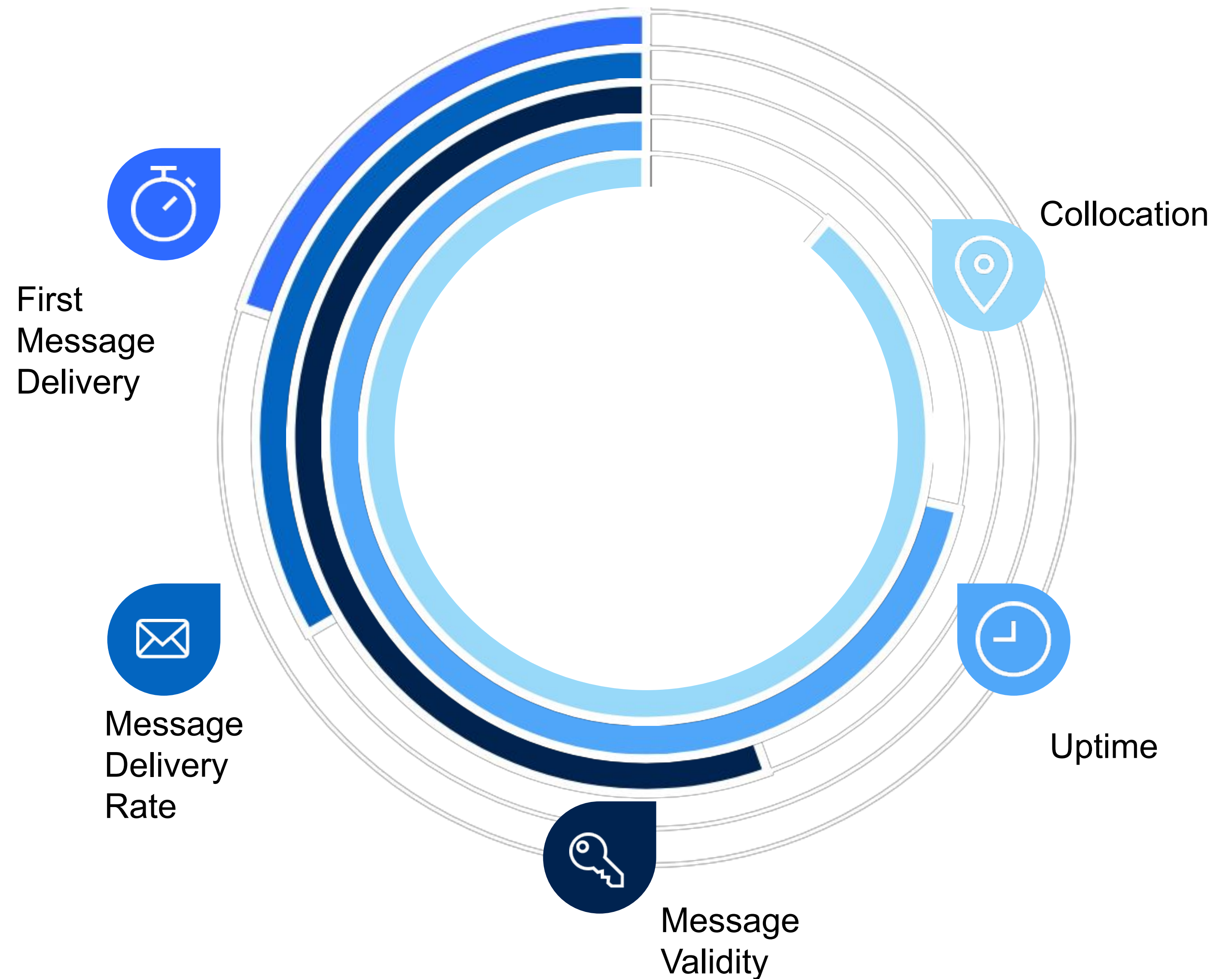
GossipSub in a Nutshell



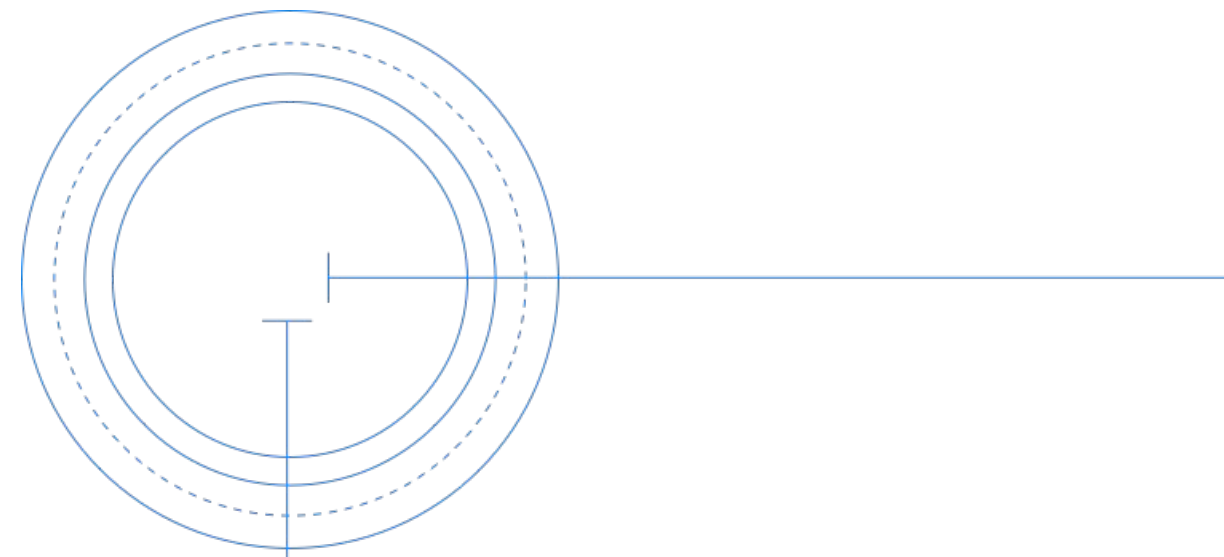
The Score Function

★ Reward good behaviour

★ Penalise malicious behaviour



The Score Function

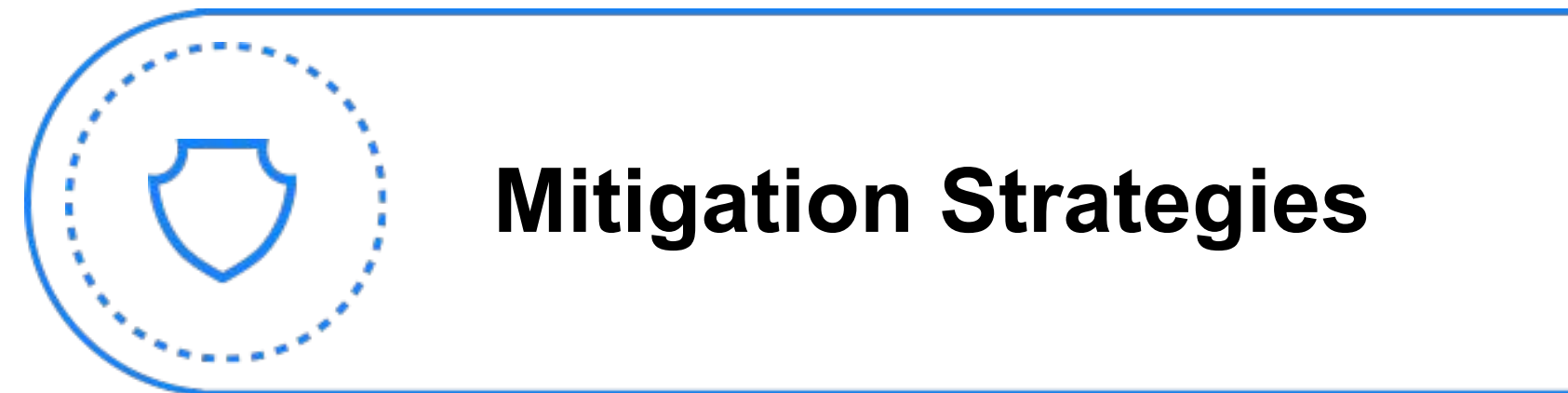
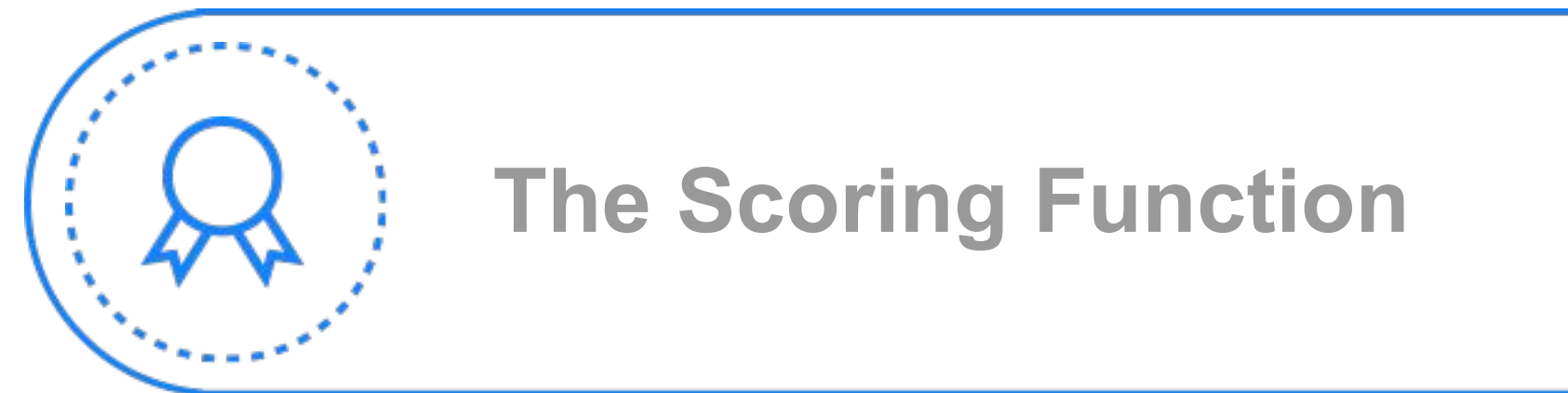
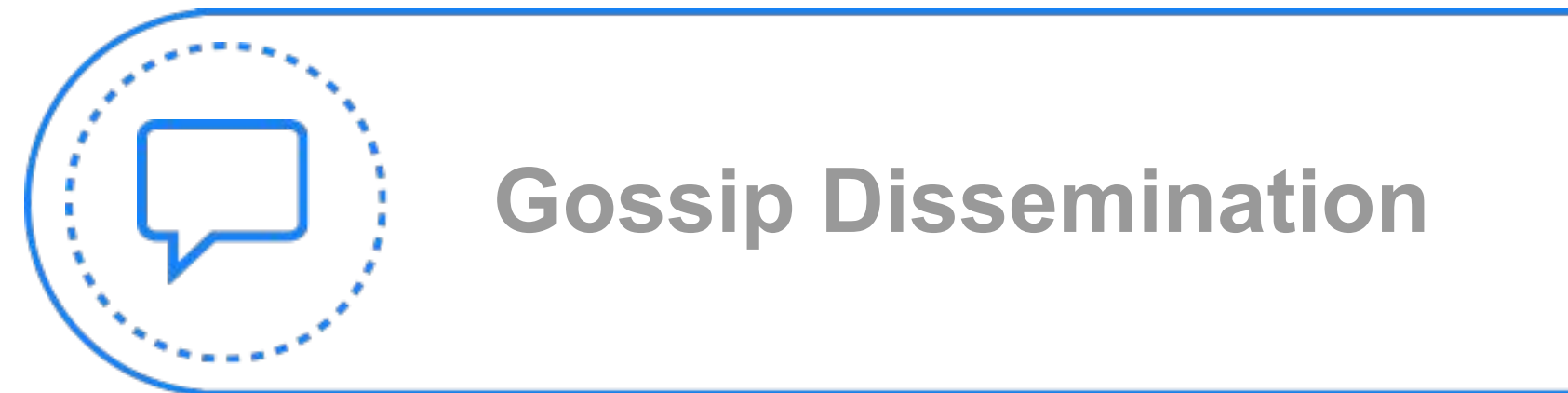
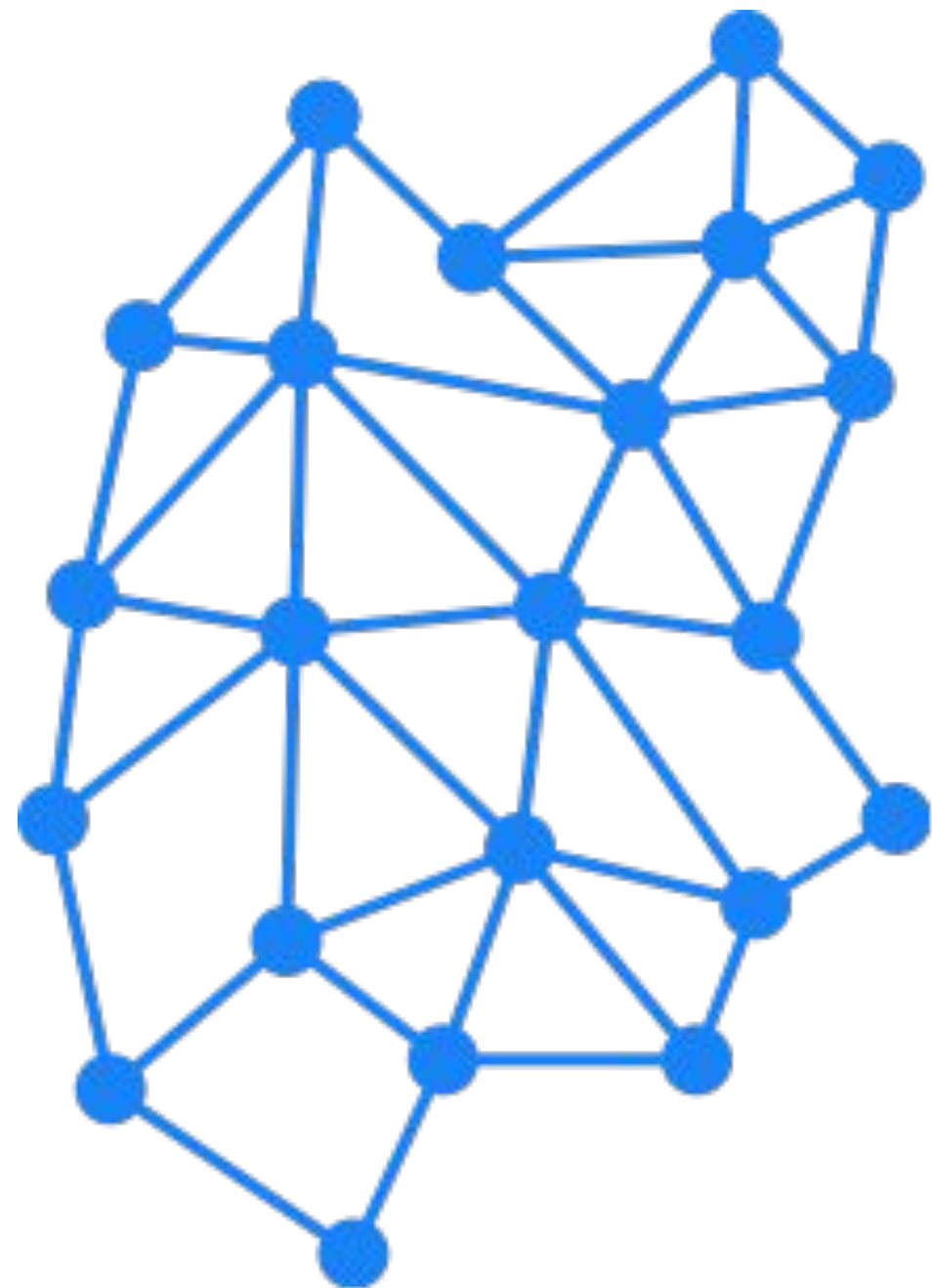


→ Function Parameters:

- P_1 : Time in Mesh
- P_2 : First Message Deliveries
- P_3 : Mesh Message delivery Rate & Failures
- P_4 : Invalid Messages
- P_5 : Application Specific Score
- P_6 : IP Address Collocation

$$Score(peer) = TC\left(\sum_{n=1}^4 w_n(t_i) * P_n(t_i)\right) + w_5 * P_5 + w_6 * P_6$$

GossipSub in a Nutshell



Mitigation Strategies



✓ Controlled Mesh Maintenance

✓ Flood Publishing

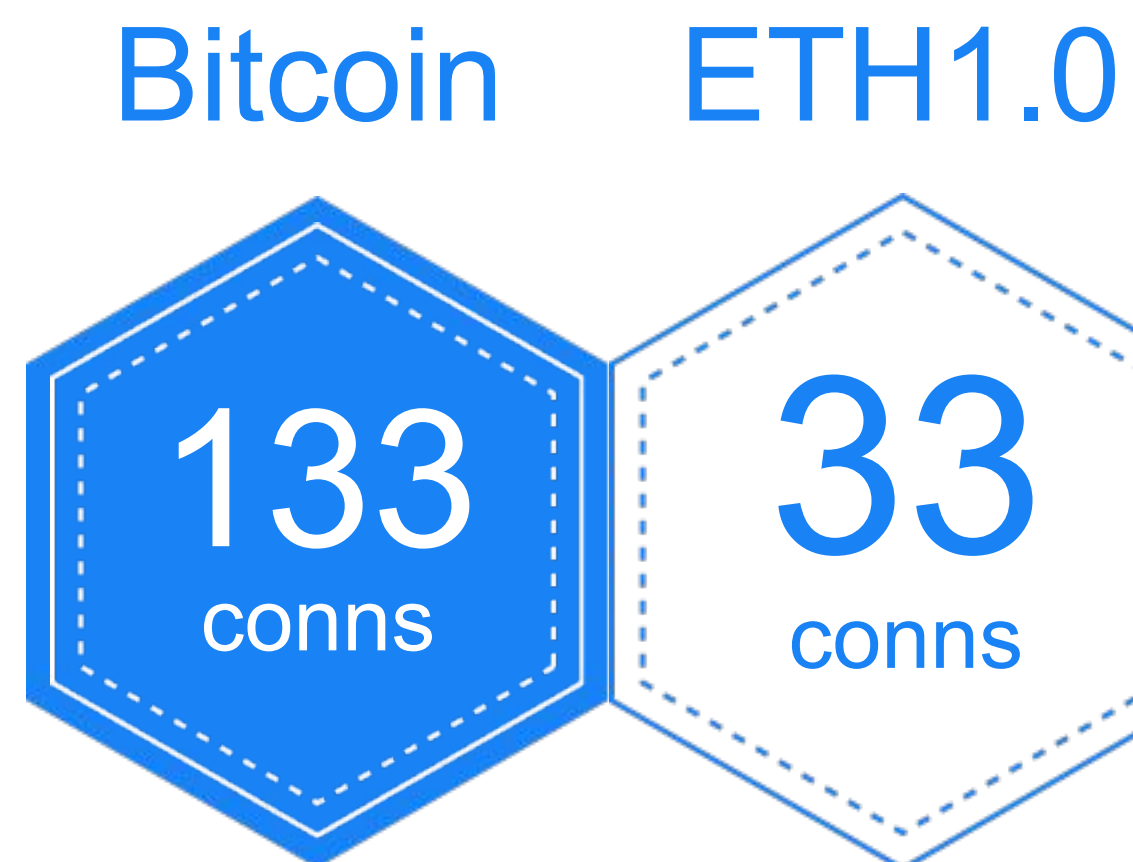
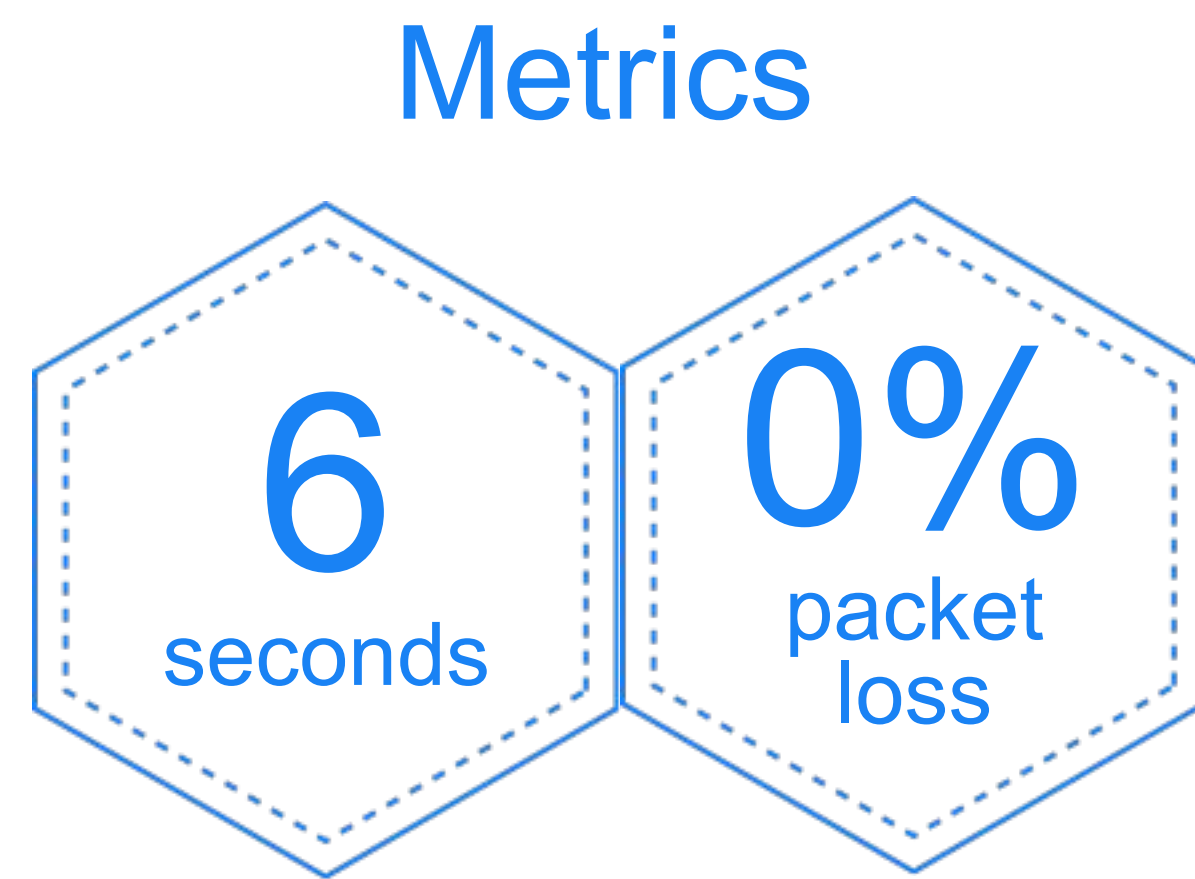
✓ Adaptive Gossip Dissemination

✓ Backoff on PRUNE

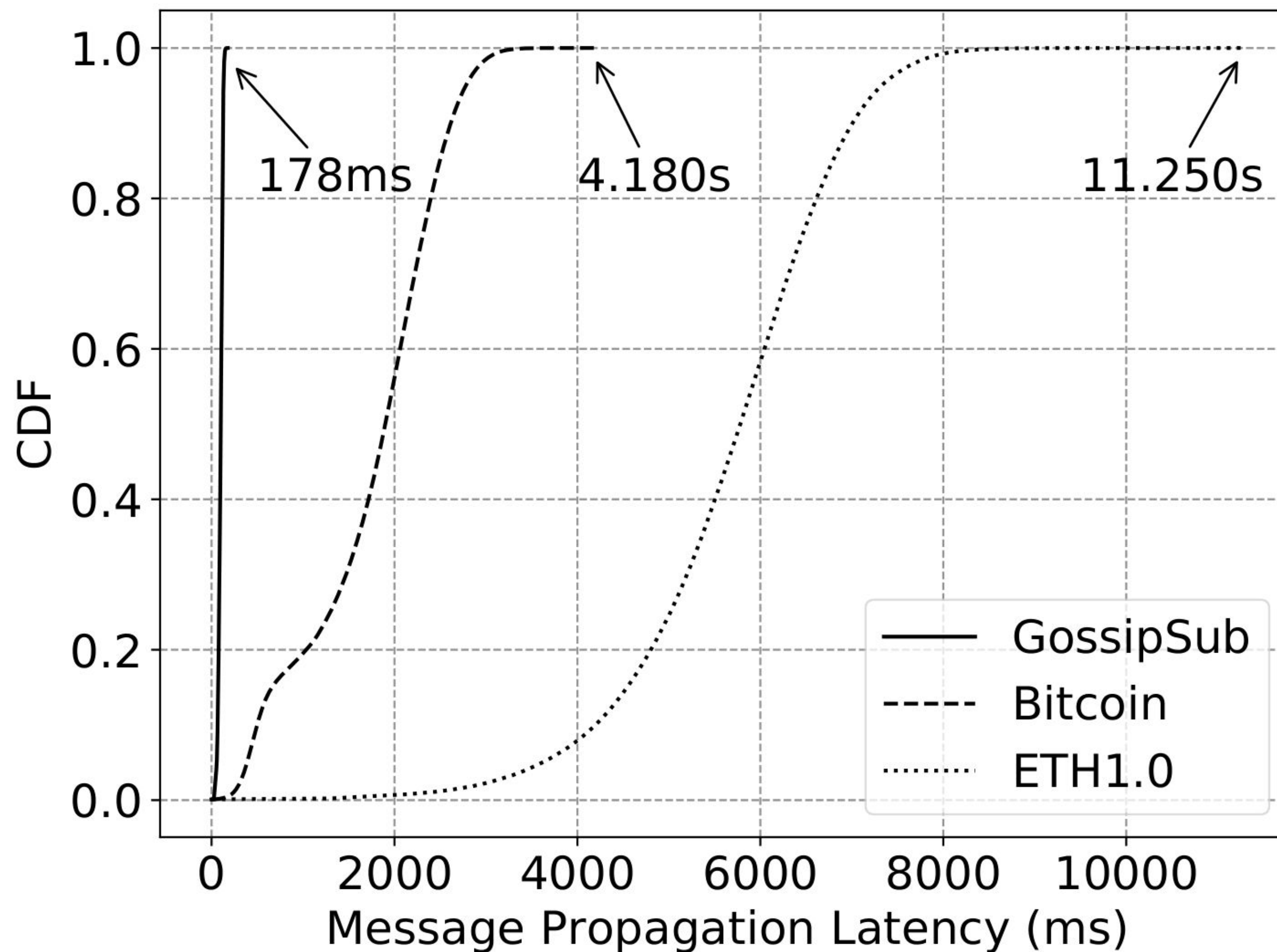
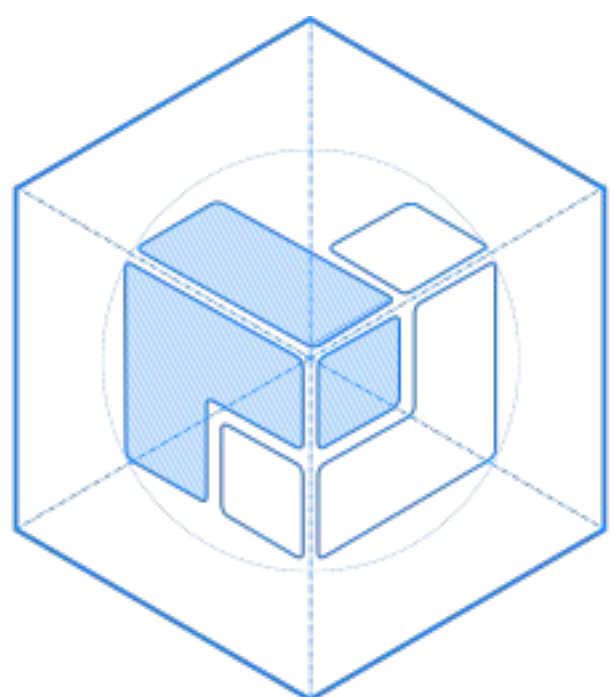
Test Setup

We have used **Testground** (see <https://testground.ai>) and tested production code in realistic a environment

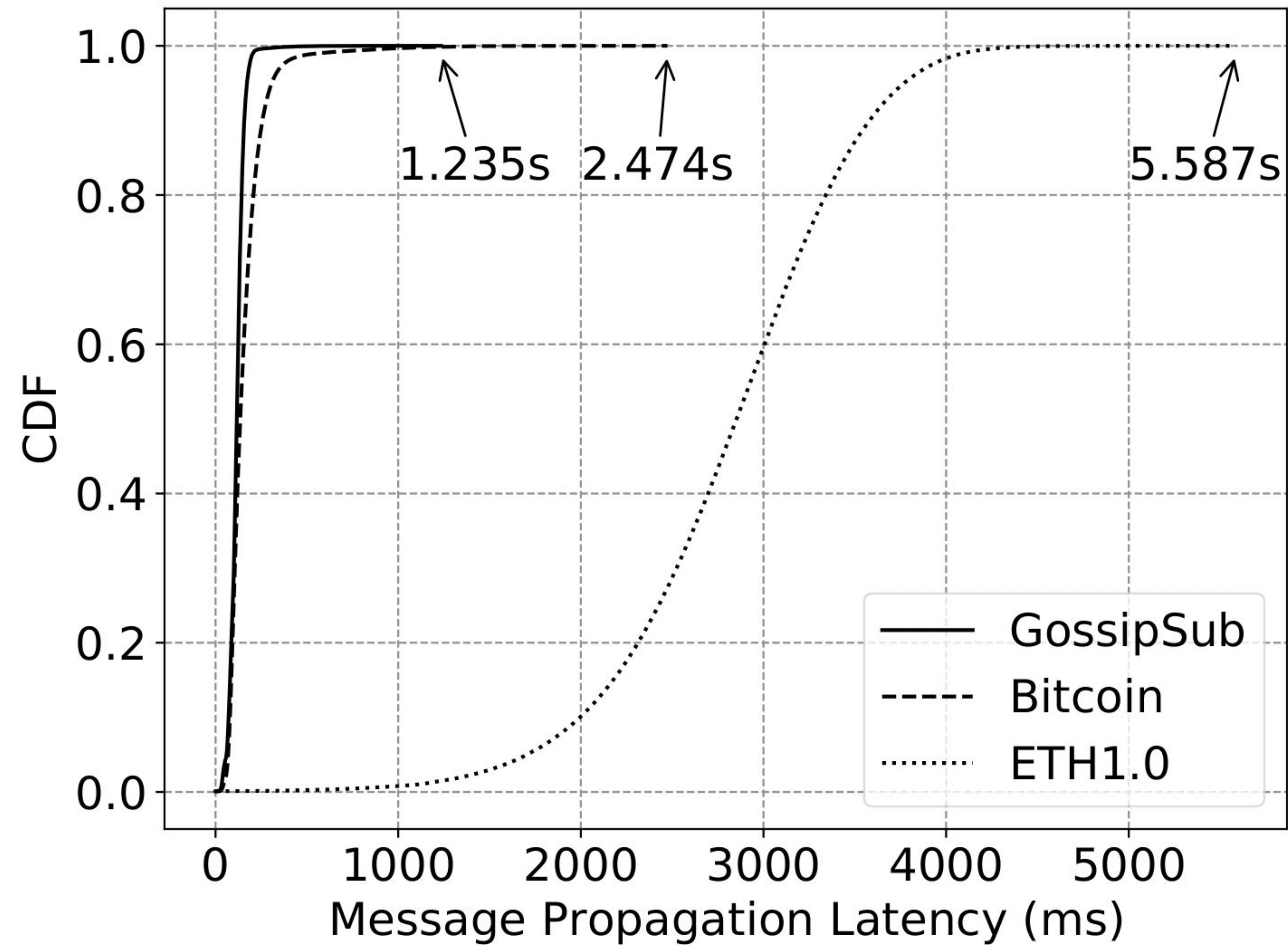
All our results and test plans are open-source to support reproducibility.



Network-wide Eclipse Attack CDF

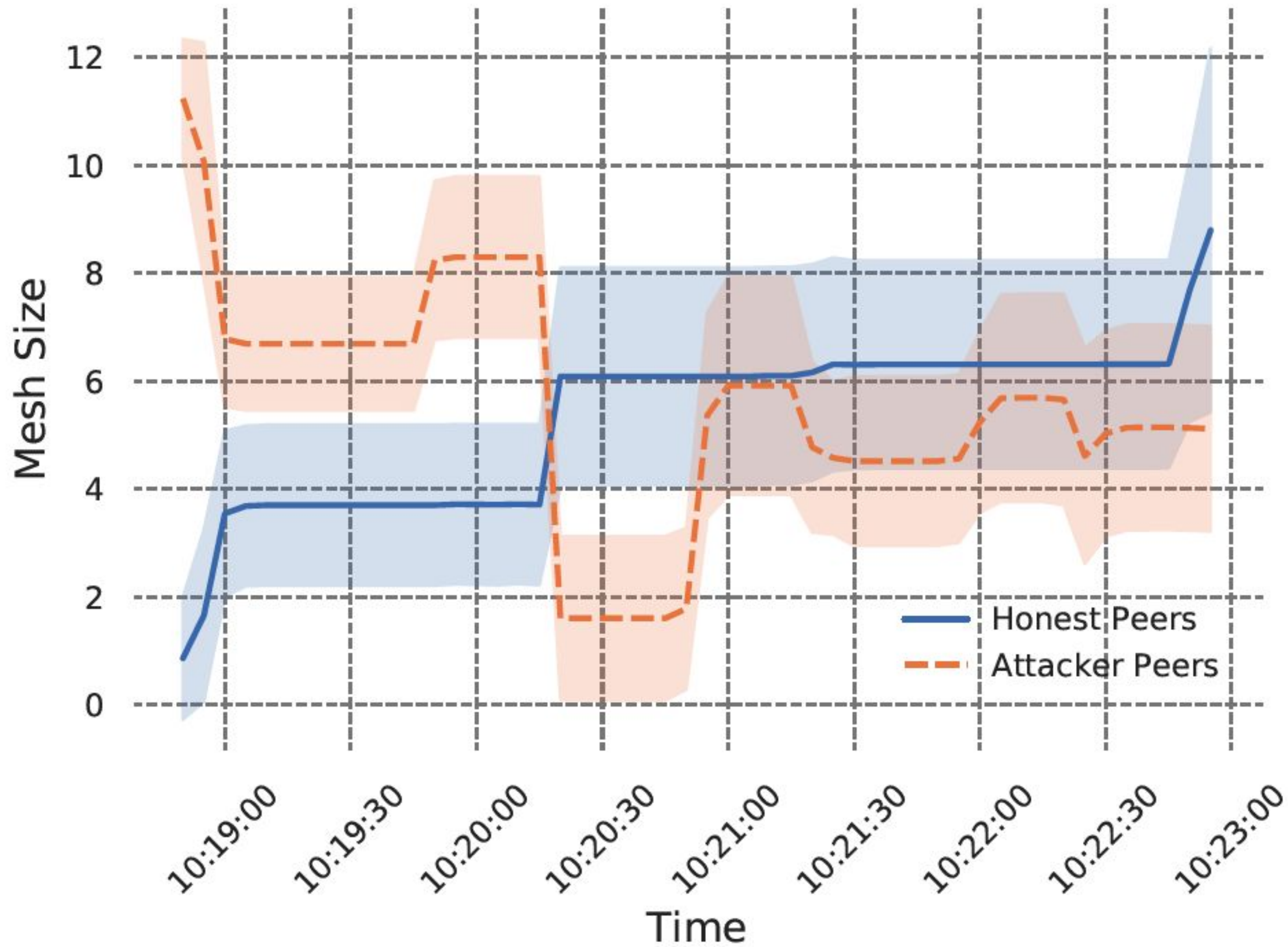


Cold Boot Attack CDF



Cold Boot Attack

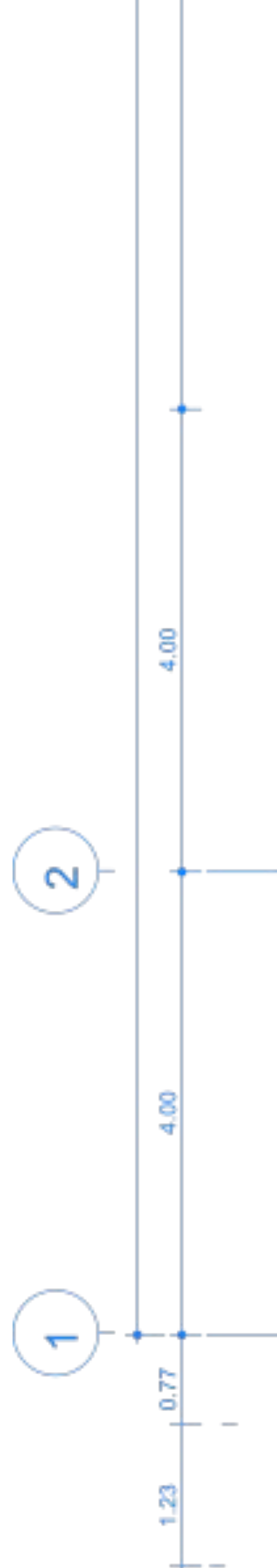
Mesh Status



Summary



- ★ This is a new era of protocol design for unstructured and permissionless P2P networks that carry monetary value.
- ★ GossipSub is a solid first step on this direction.
- ★ We have not found an attack that successfully bends the performance of GossipSub
- ★ Come along, let's collaborate!



Filecoin Website: <https://filecoin.io>
Filecoin Blog: <https://filecoin.io/blog>
Filecoin Spec:
<https://spec.filecoin.io>
Filecoin Network stats:
<https://network.filecoin.io>

Gossipsub spec:
<https://github.com/libp2p/specs/blob/master/pubsub/gossipsub/gossipsub-v1.1.md>

Gossipsub paper preprint:
<https://arxiv.org/abs/2007.02754>

Get in touch!
yiannis@protocol.ai