The Waku Network as Infrastructure for dApps

Presenter:
Alvaro / Research Engineer at the Institute of Free Technology (Status.im)

Authors:
Hanno Cornelius
Sergei Tikhomirov
Alvaro Revuelta
Simon Pierre Vivier
Aaryamann Challani

Agenda

1. Problem statement
2. The Waku Protocol
3. The Waku Network
   - Routing
   - Rate limiting
   - Sharding
   - Peer discovery
   - Services
   - Sustainability
4. Questions

Problem Statement: A sends a message to BCD


Alice Message

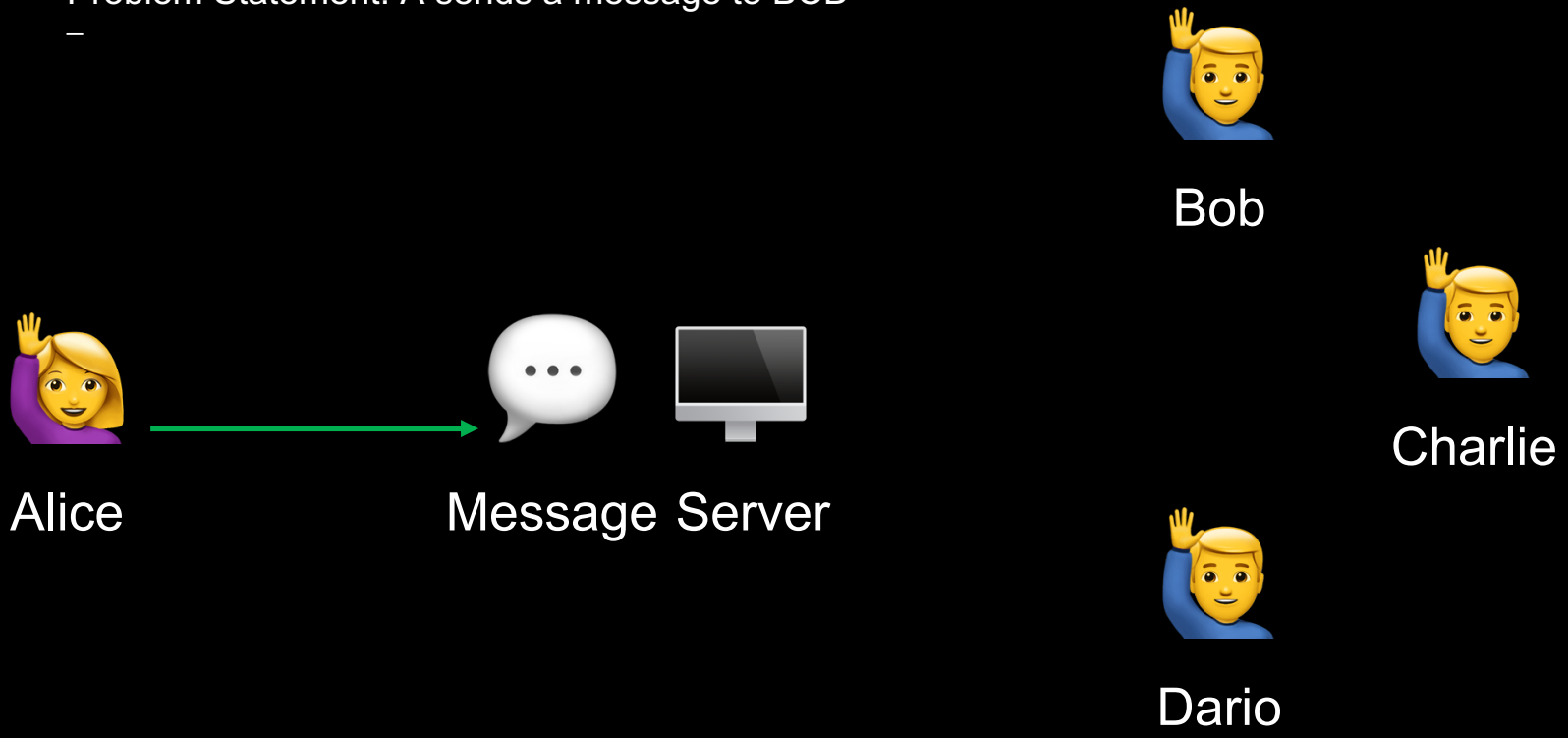
Server

Bob

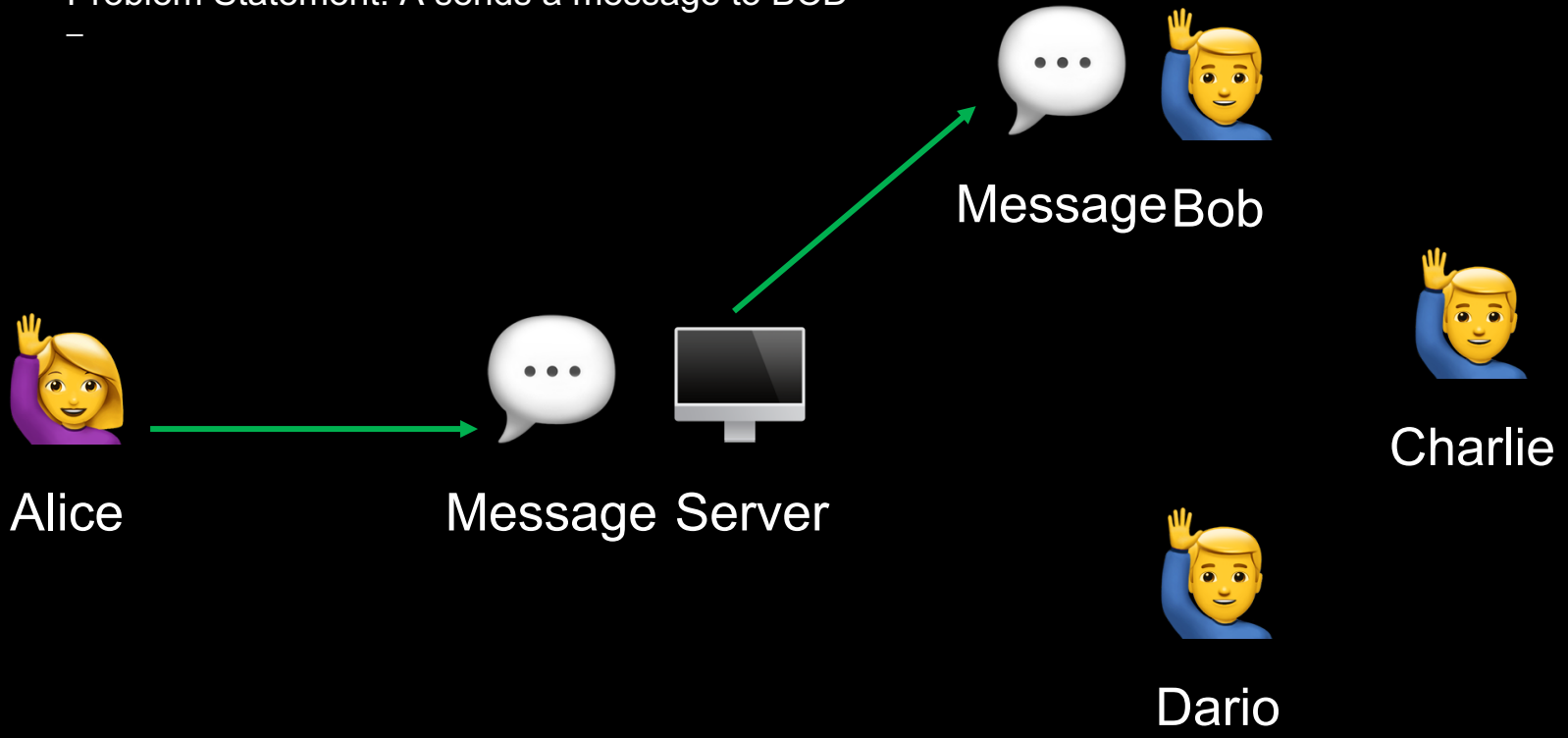
Charlie

Dario

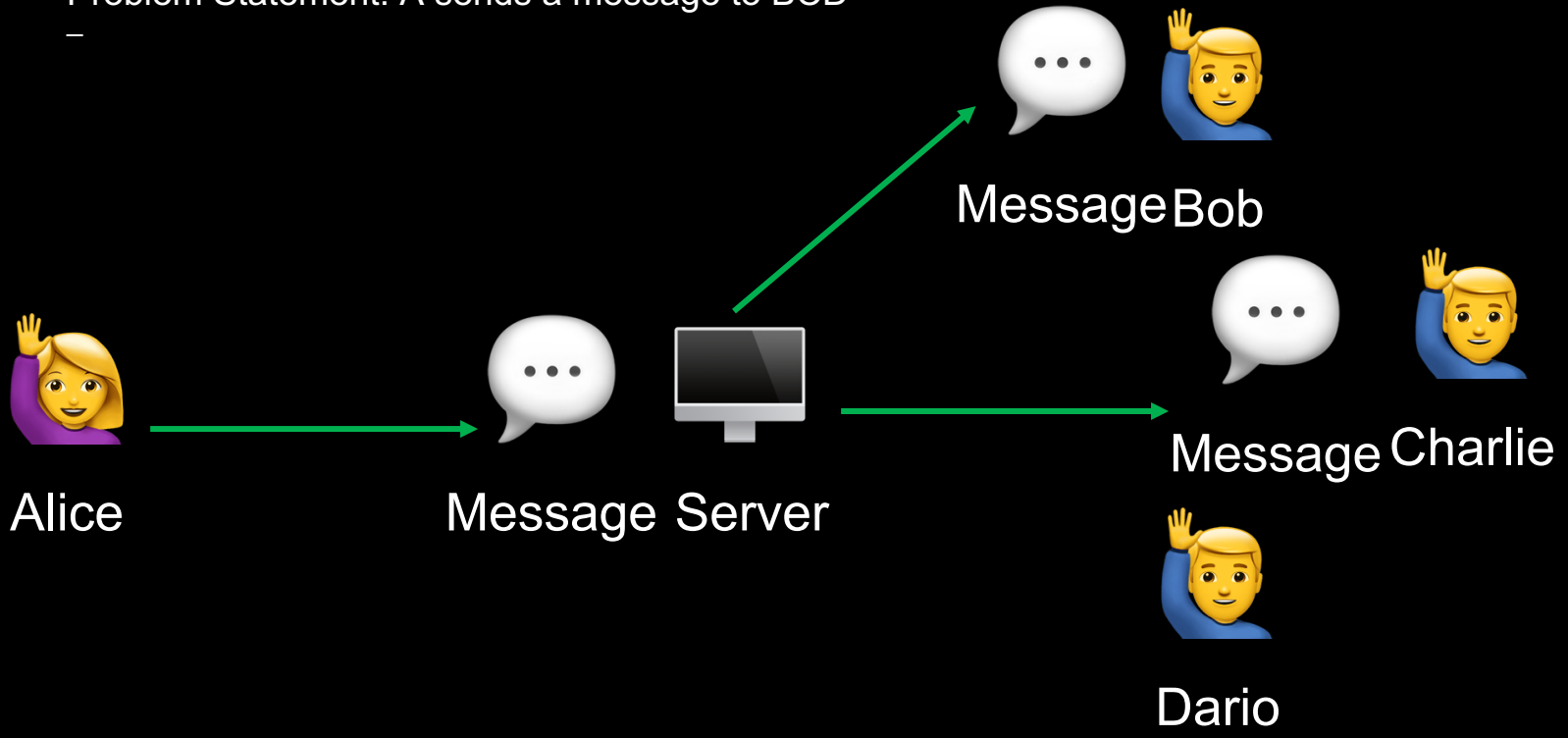
Problem Statement: A sends a message to BCD



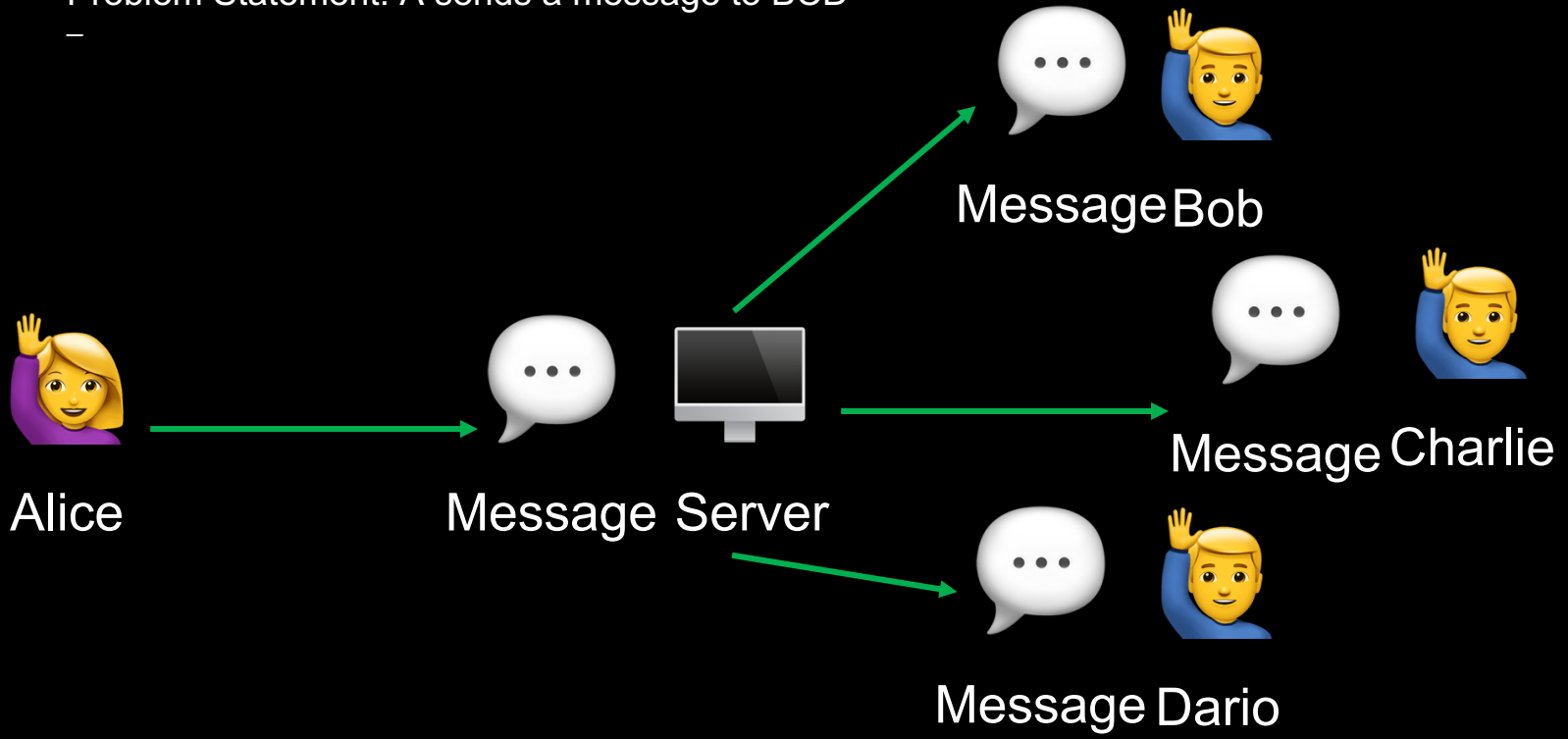
Problem Statement: A sends a message to BCD



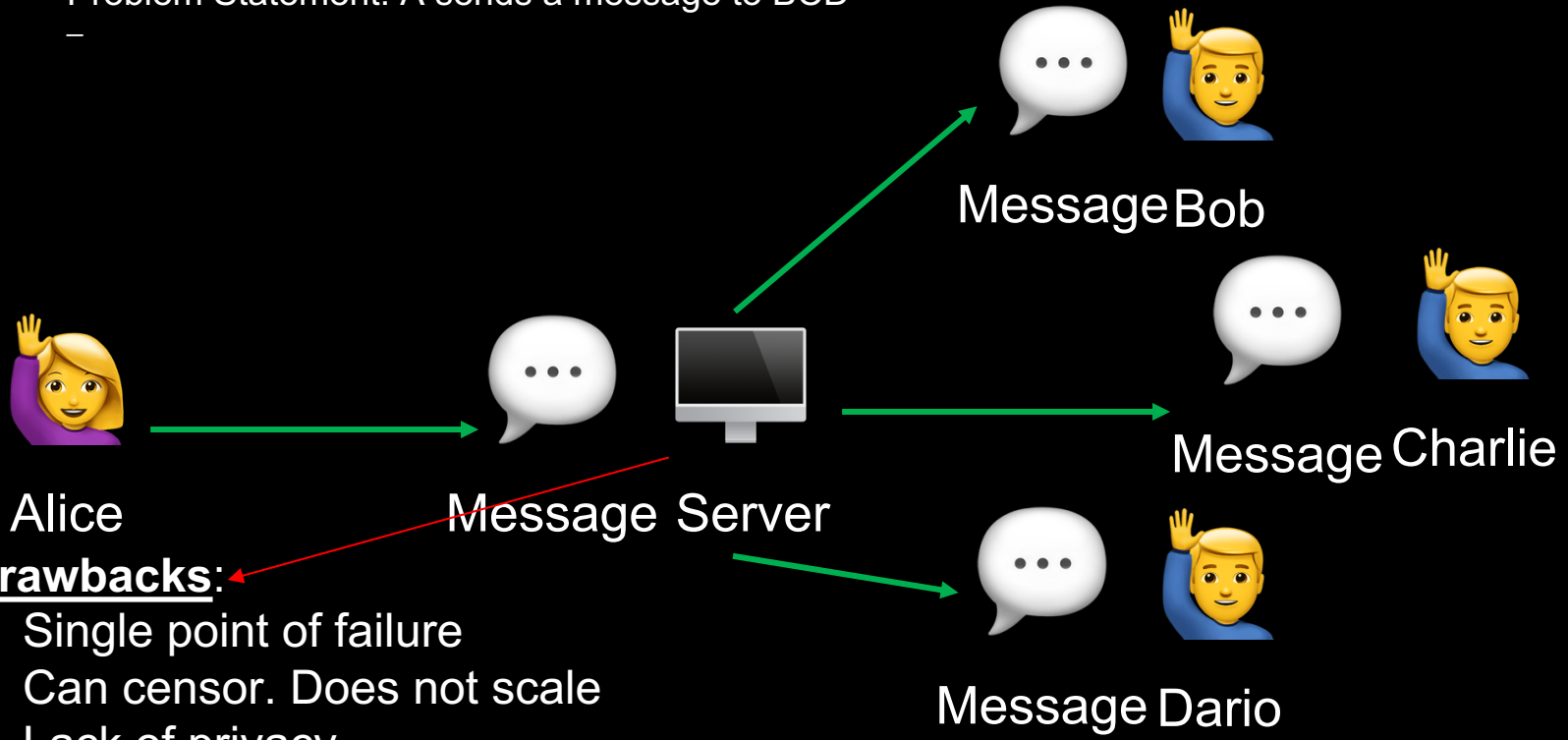
Problem Statement: A sends a message to BCD



Problem Statement: A sends a message to BCD



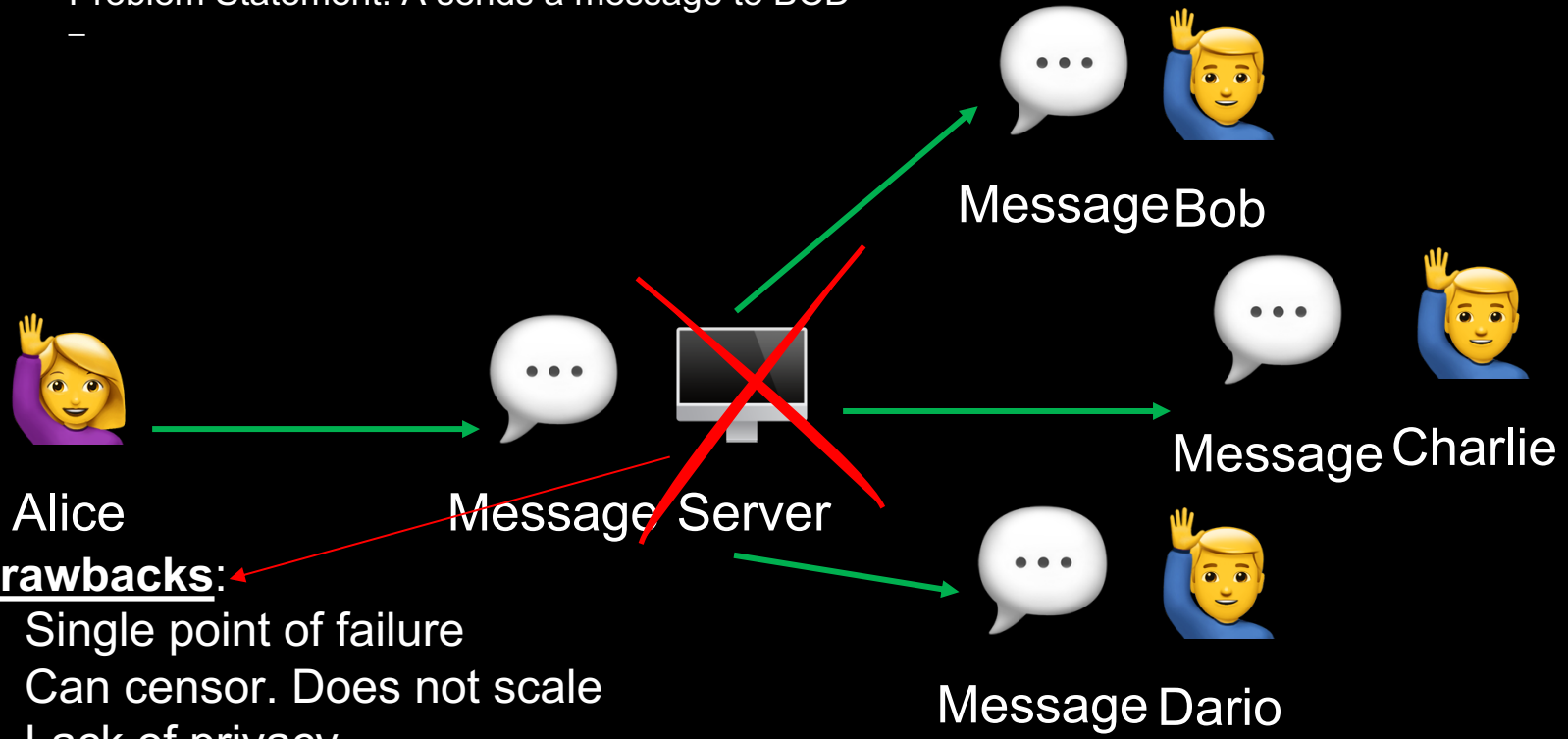
Problem Statement: A sends a message to BCD



Drawbacks:

- Single point of failure
- Can censor. Does not scale
- Lack of privacy
- Can we get rid of it? YES

Problem Statement: A sends a message to BCD



Drawbacks:

- Single point of failure
- Can censor. Does not scale
- Lack of privacy
- Can we get rid of it? YES

The Waku Protocol

- Open-source project:
  - github.com/waku-org/nwaku
- A suite of protocols, based on libp2p
- Provides privacy-preserving, scalable, spam-resistant, and censorship-resistant messaging services for decentralized applications

The Waku Network

- Public instance of The Waku Protocol
- Not linked to a single entity
- Rate-limited to ensure fair usage
- Live in a public testnet (EVM based)
- > 500 nodes
- Anyone can use it (users)
- Anyone can run a node (operator)
- Don’t like it? Deploy your own

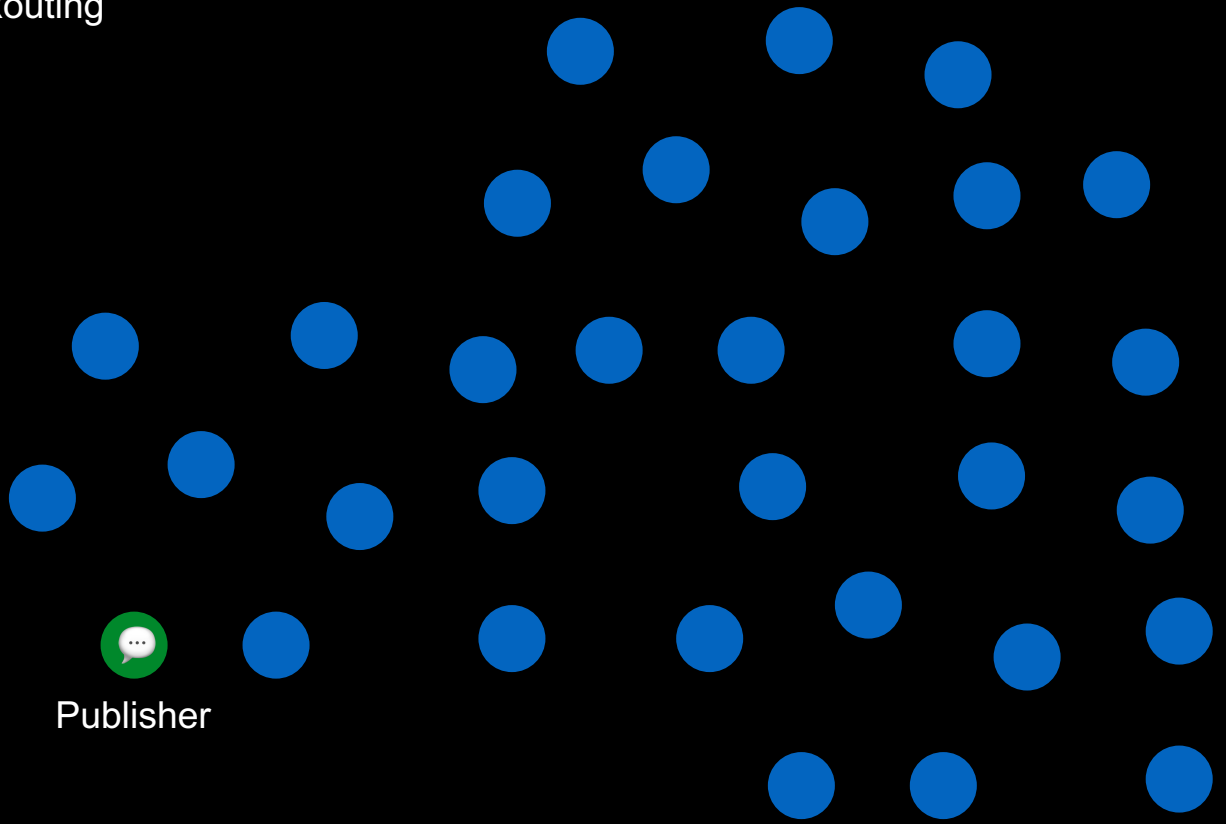
The Waku Network

Routing:

How are messages routed tx->rx?

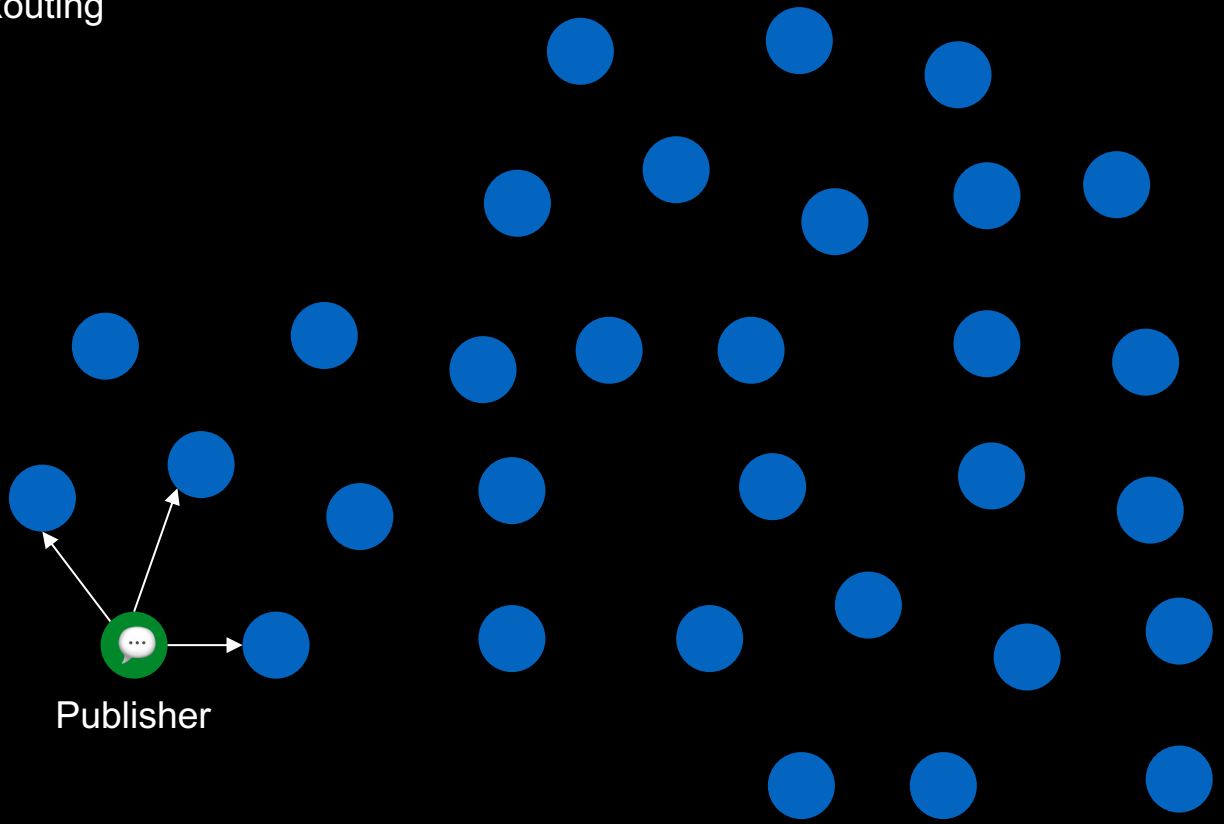
- Publisher-subscriber architecture. Uses gossipsub
- Nodes are organized around topics
- A message published to a topic reaches all nodes subscribed to it
- Origin of the message can’t be tracked
- No PII (Personal Identifiable Information) is included
- D=4/8 and max message size 150KB

Routing

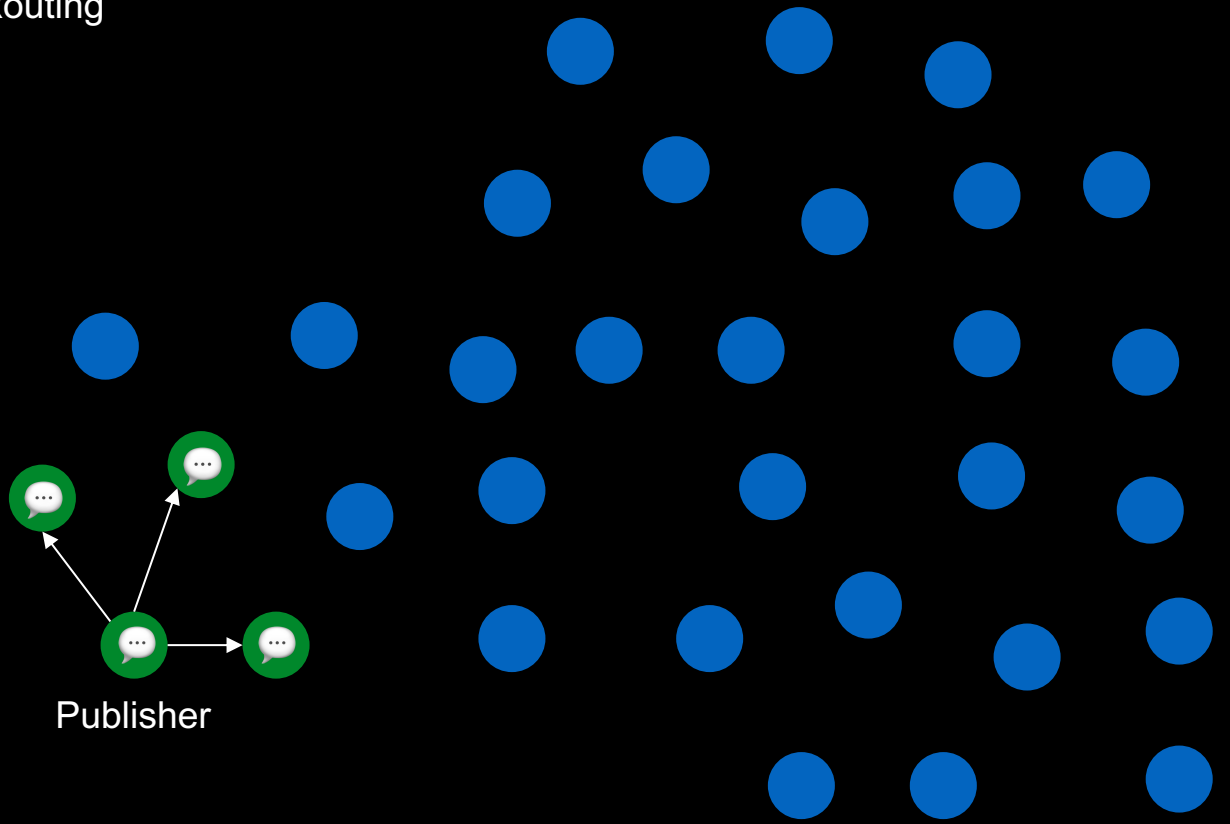


Routing

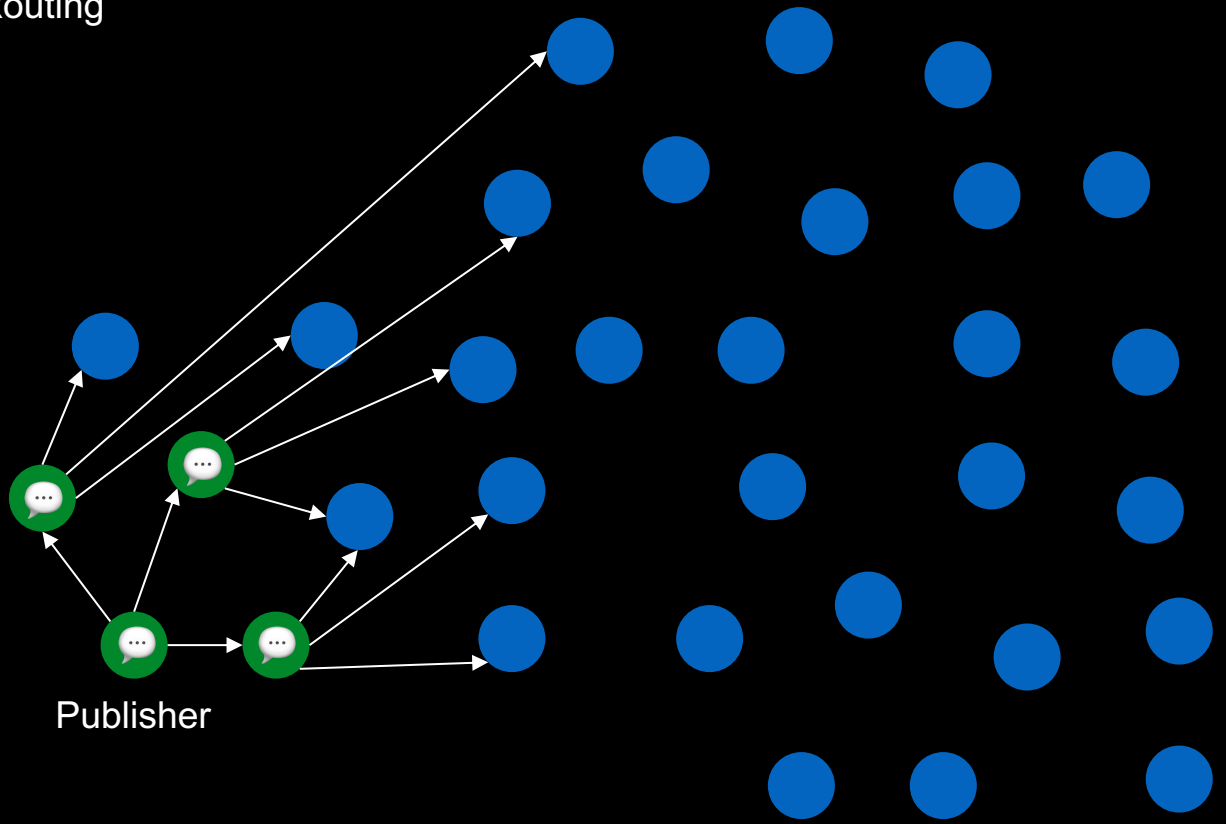
Network D=3
Nodes=32



Routing

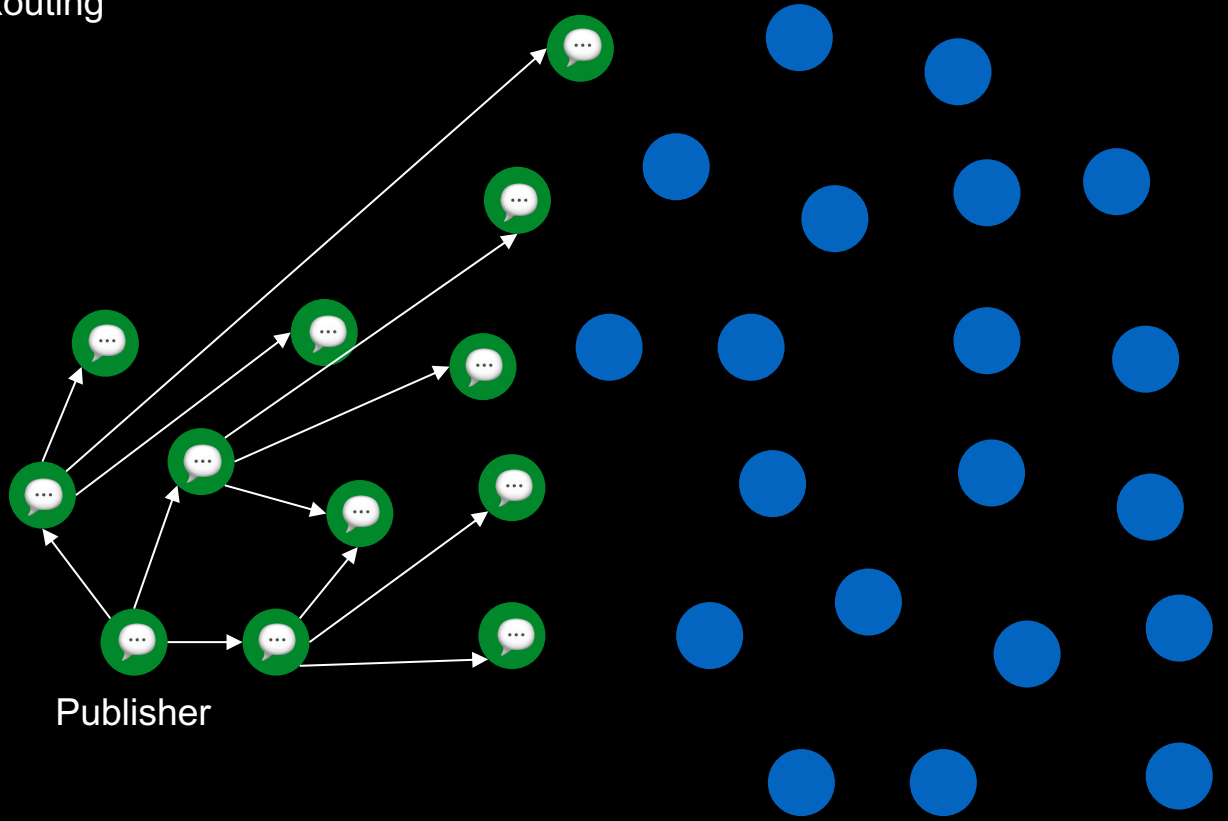


Routing



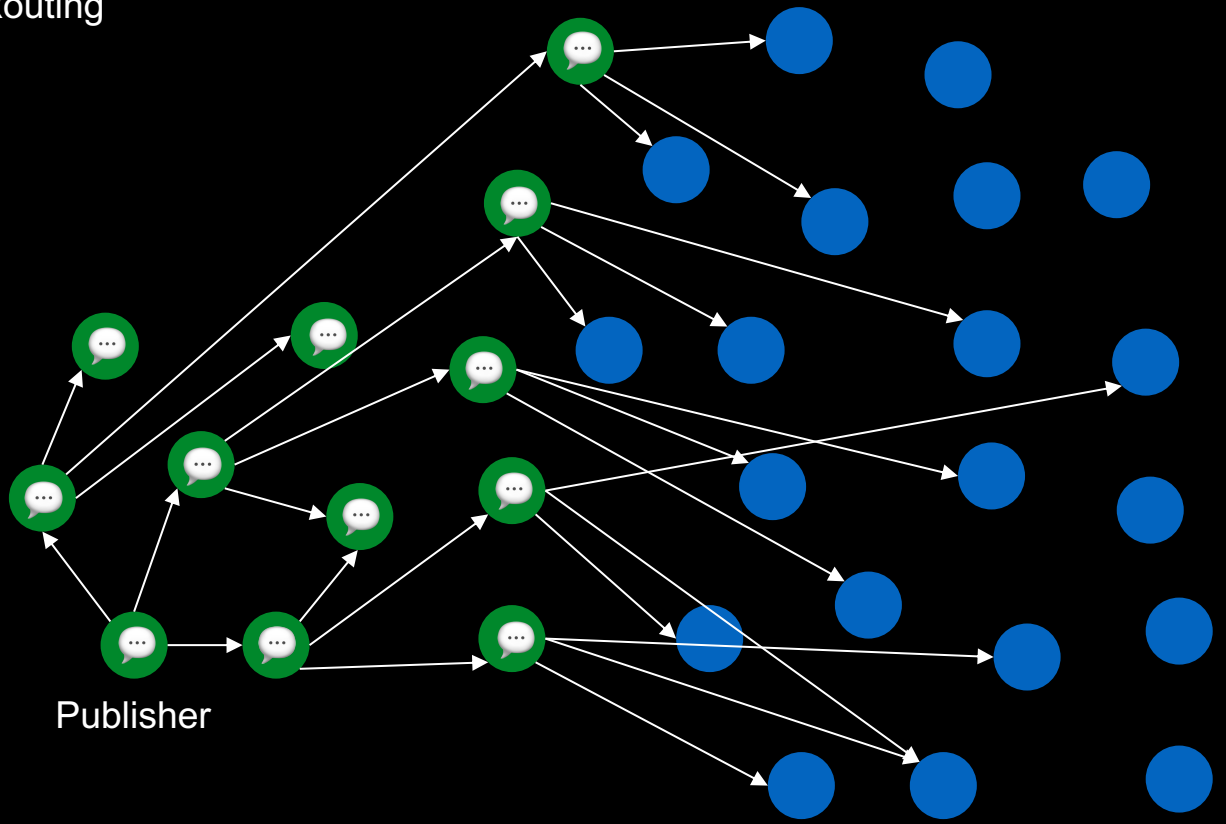
Network D=3
Nodes=32

Routing

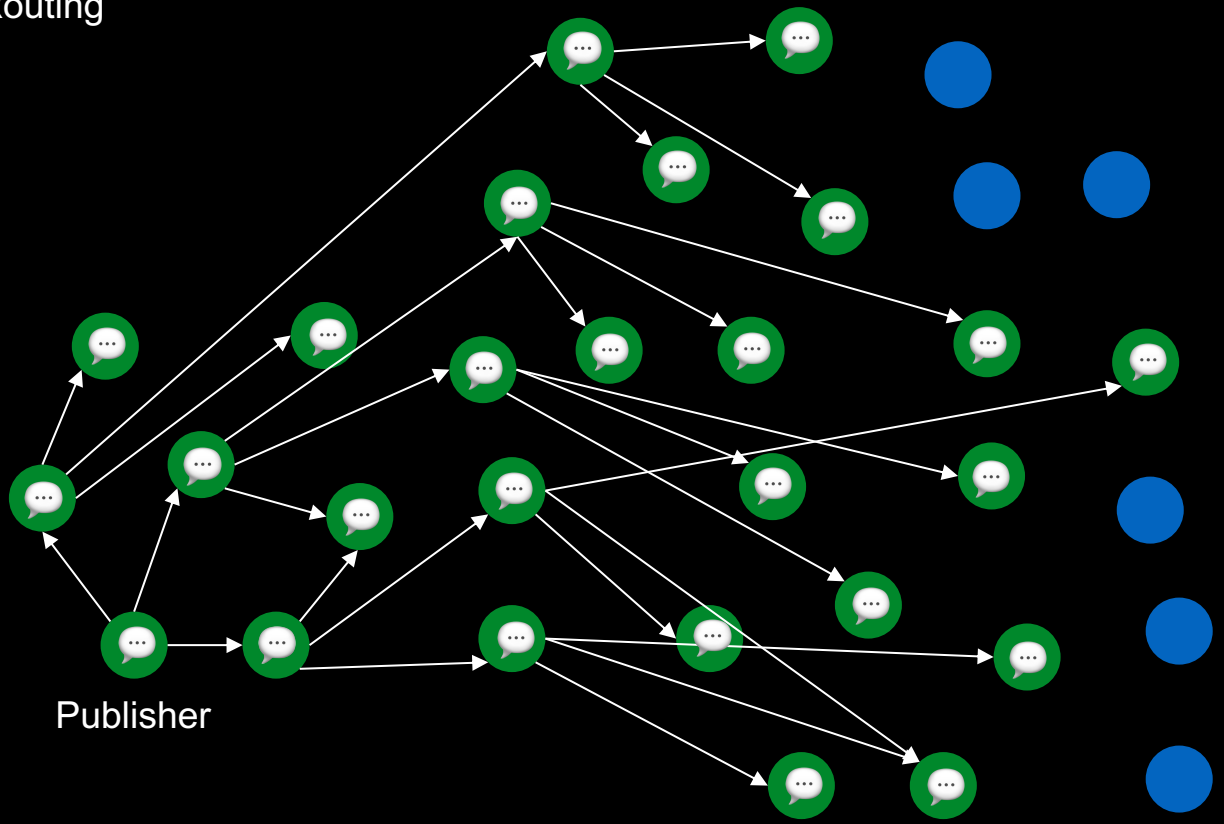


Network D=3
Nodes=32

Routing



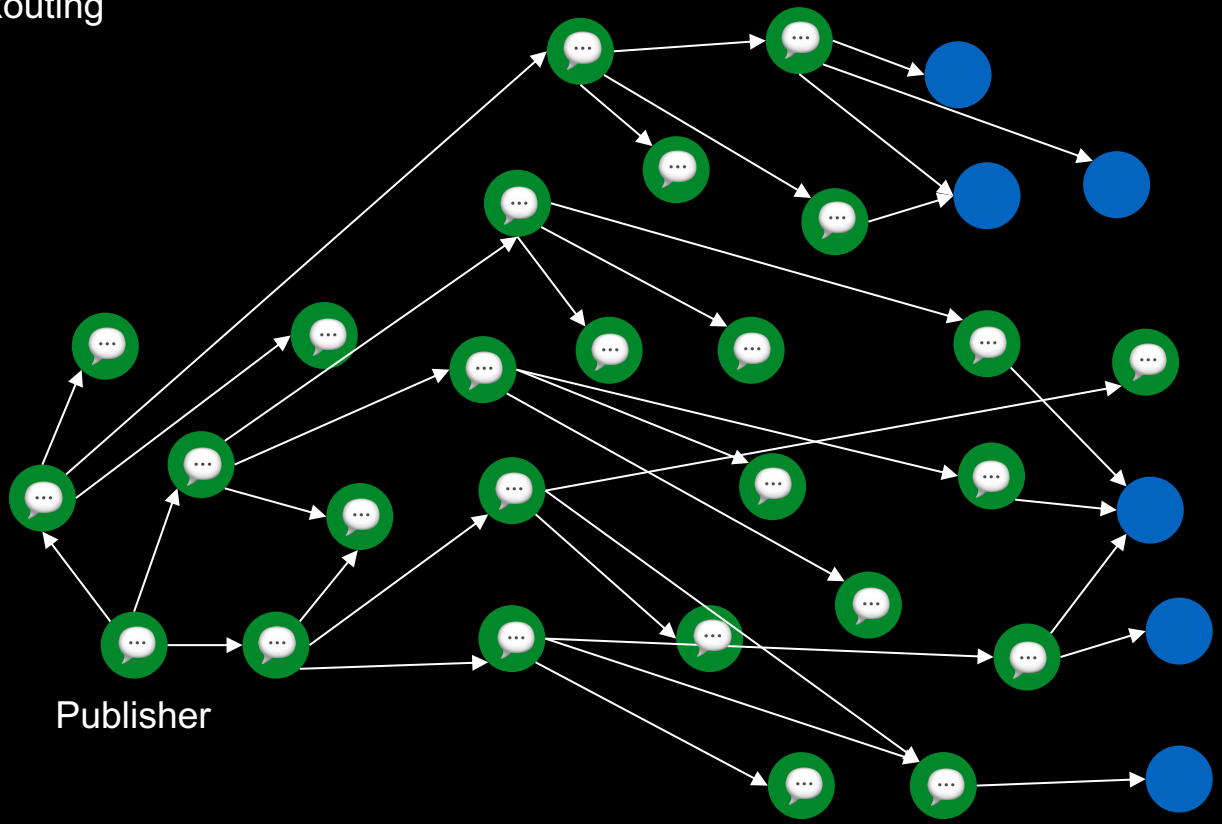
Routing



Network D=3
Nodes=32

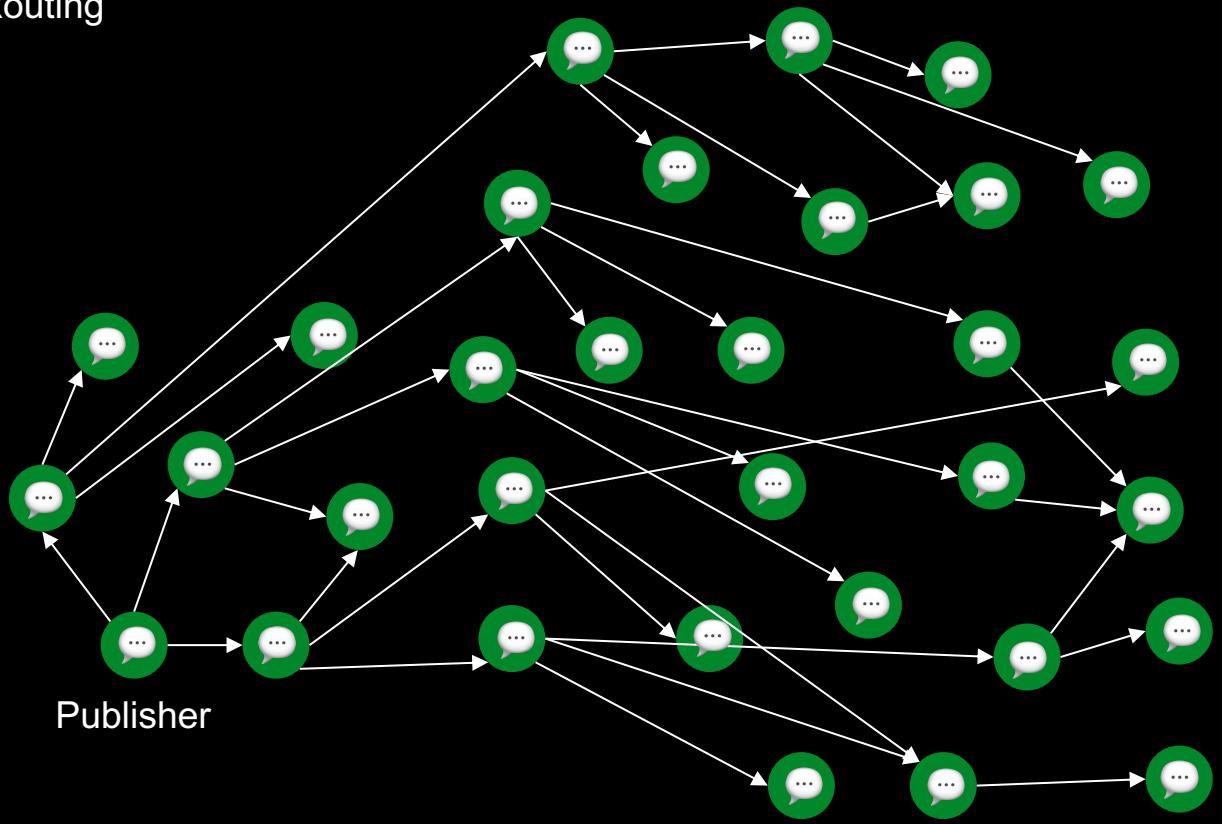
Routing

Network D=3
Nodes=32



Routing

Network D=3
Nodes=32



The Waku Network

Rate limiting:

How do we prevent Denial of Service?

- The protocol is permissionless, we need to rate limit to ensure fair usage.
- But preserving privacy.
- Uses RLN (Rate Limiting Nullifiers), based on zero-knowledge cryptography.
- Anyone can register a membership in the contract.
- Currently set to 100 messages every 10 minutes per membership.

The Waku Network

Sharding:

How does the network scale?

- Since it is publisher/subscribed-based, all nodes get all the traffic
- This does not scale
- Fixed with sharding
- The network is split on shards (subnetworks)
- Nodes opt to which shards they participate in
- Currently, 8 shards.

The Waku Network

Peer discovery:

How do peers find each other?

- Peers discover each other using DISCV5
- A DHT (Distributed Hash Table) is used to find other peers in a decentralized way
- Nodes uses ENR (Ethereum Name Record) to advertise themselves

The Waku Network

Services:

Which services are offered?

- Store: To retrieve historical messages
- Lightpush/filter: For light clients running in resource-restricted devices.

The Waku Network

Sustainability:

How is it sustainable?

- Use of incentives to ensure sustainability:
  - Reputation-based: Already in place
  - Economic-based: Under research

Questions