Distributed Instant Messaging System

Matthew Shea
Lauren Arpin

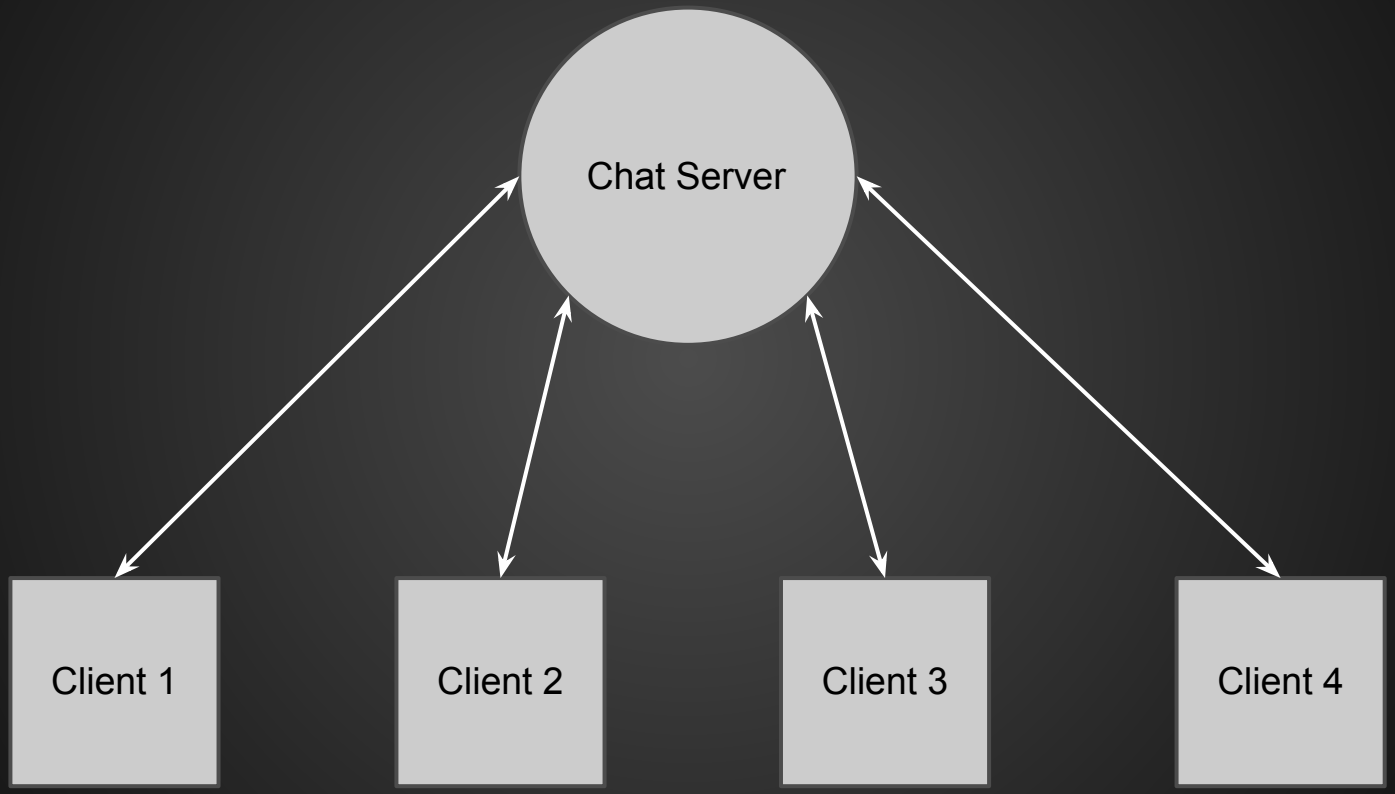
Problem

- Almost all current chat protocols are either centralised or partially decentralised
- Few chat protocols mandate the use of encryption

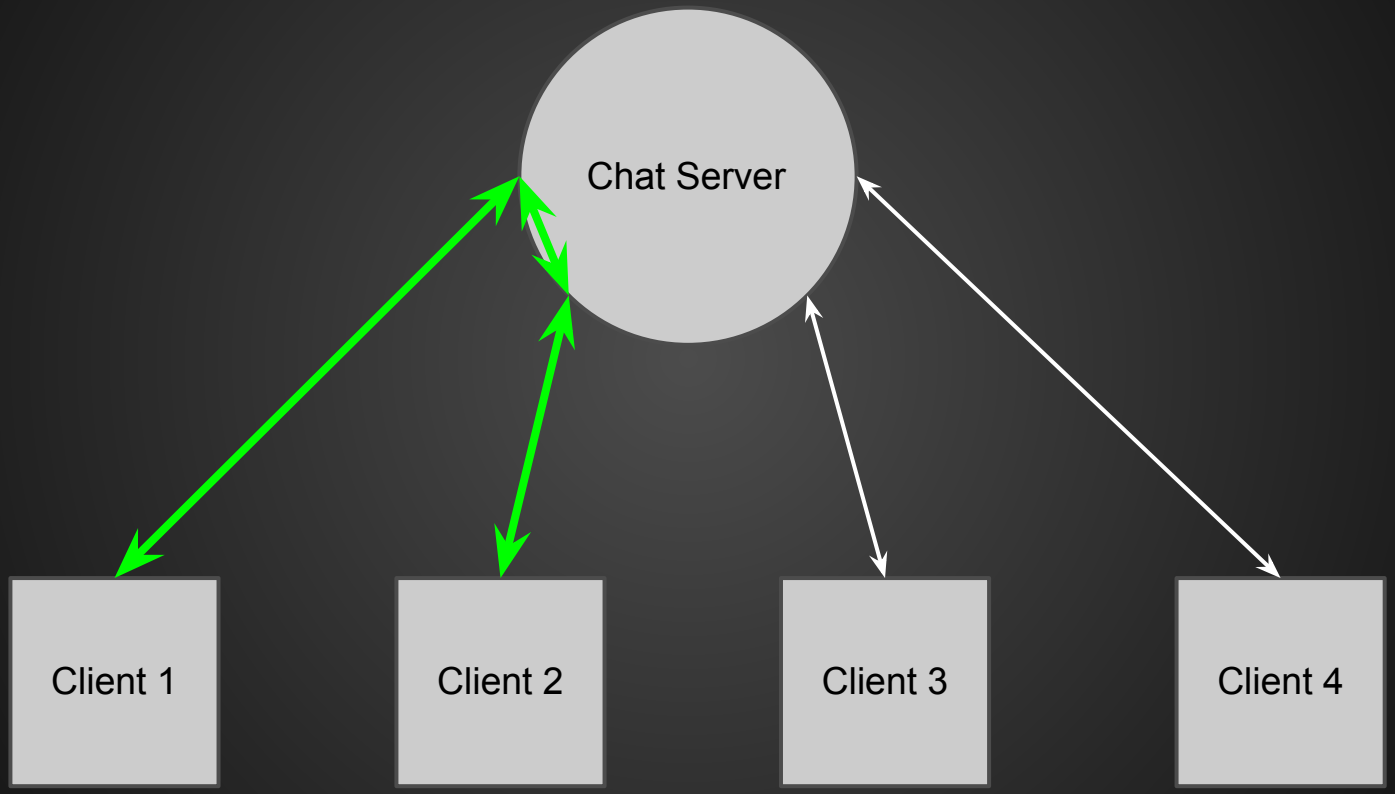
Chat Protocol Examples

- AOL Instant Messaging
  - Centralized
  - No Encryption
- XMPP / Facebook Chat / Google Chat
  - Partially Decentralised
  - No Encryption
- SILC
  - Centralised
  - Encryption Mandated

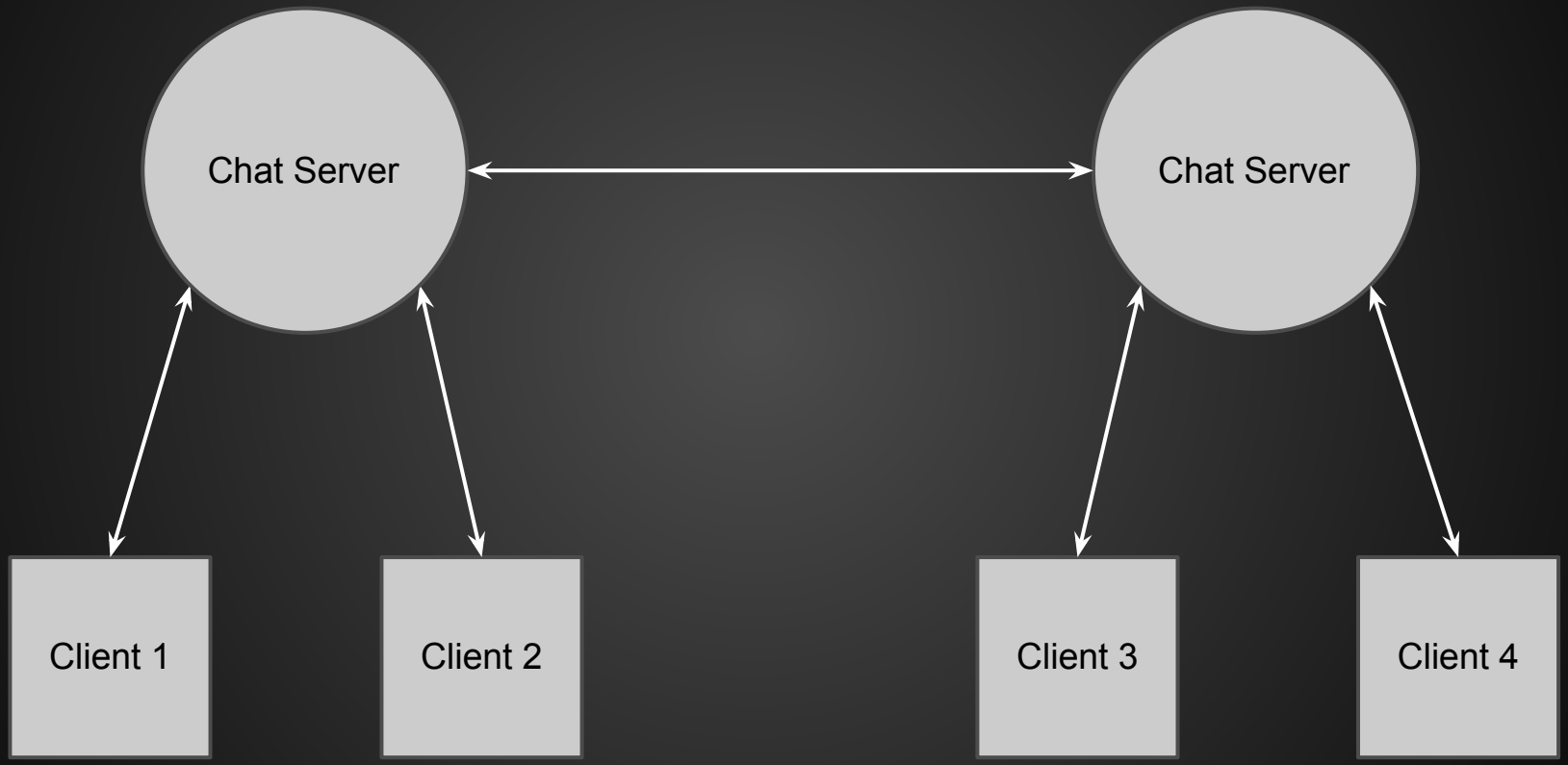
Centralised: AIM, SILC



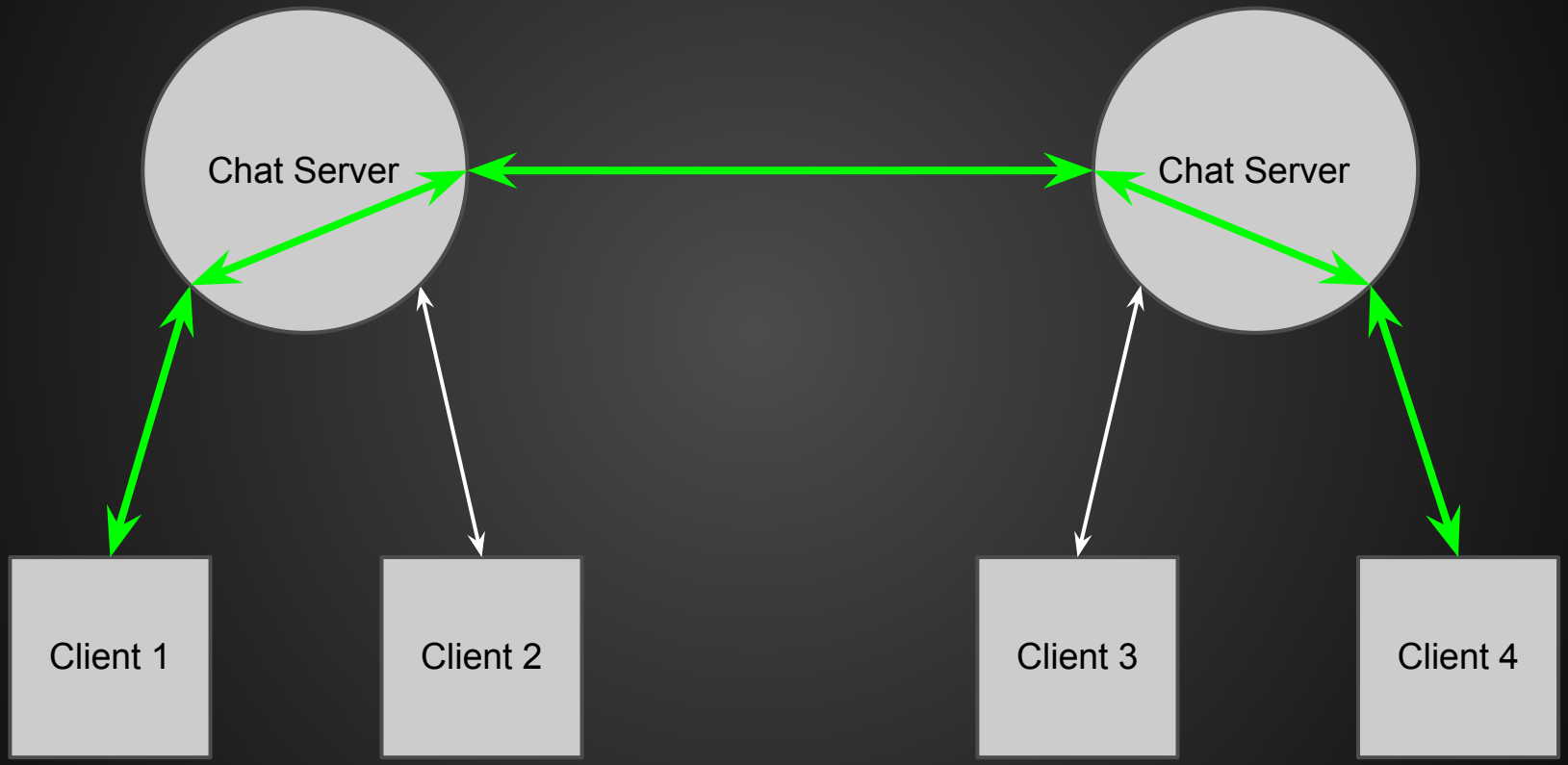
Centralised: AIM, SILC



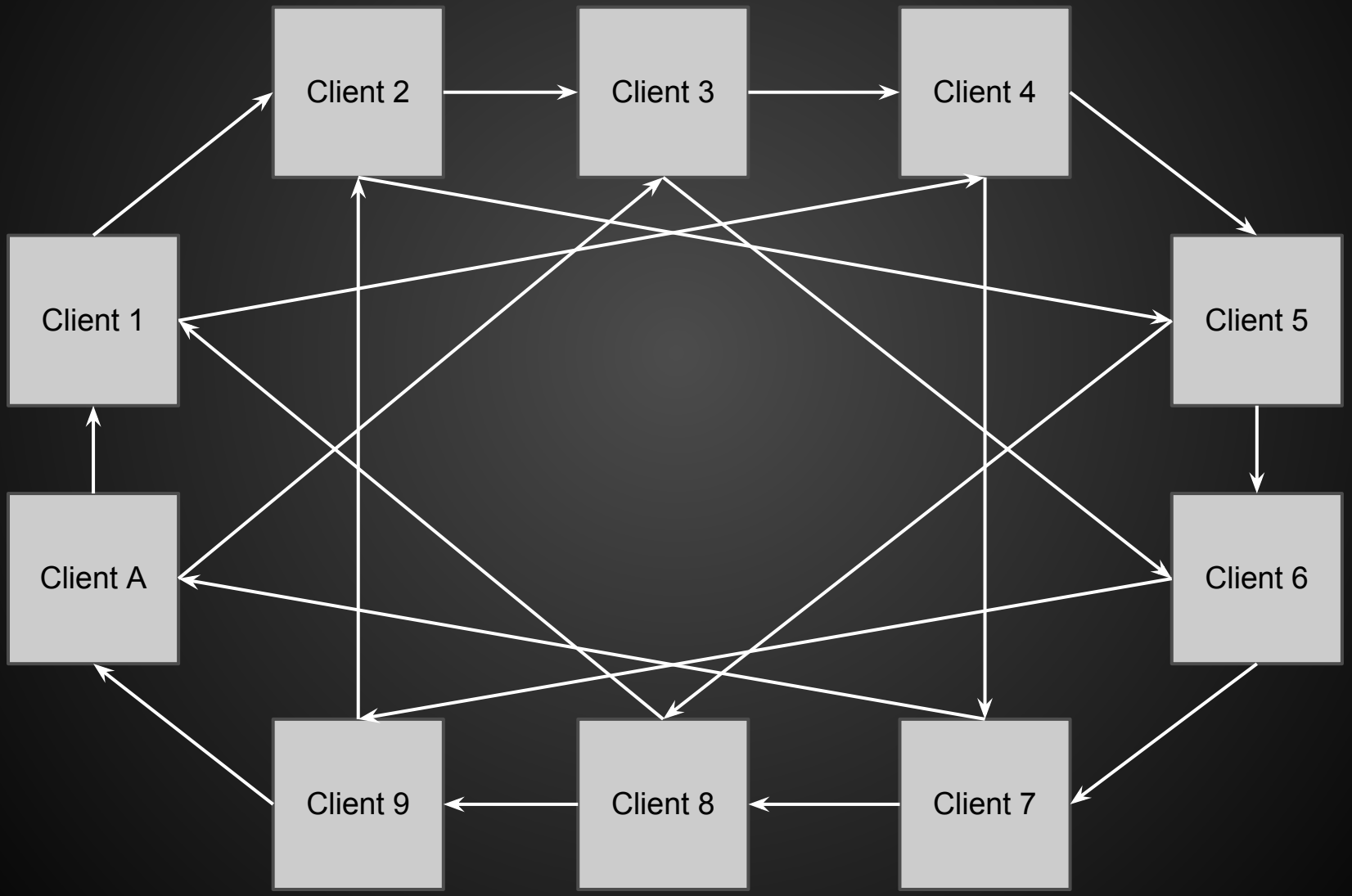
Partially Decentralised: XMPP, IRC



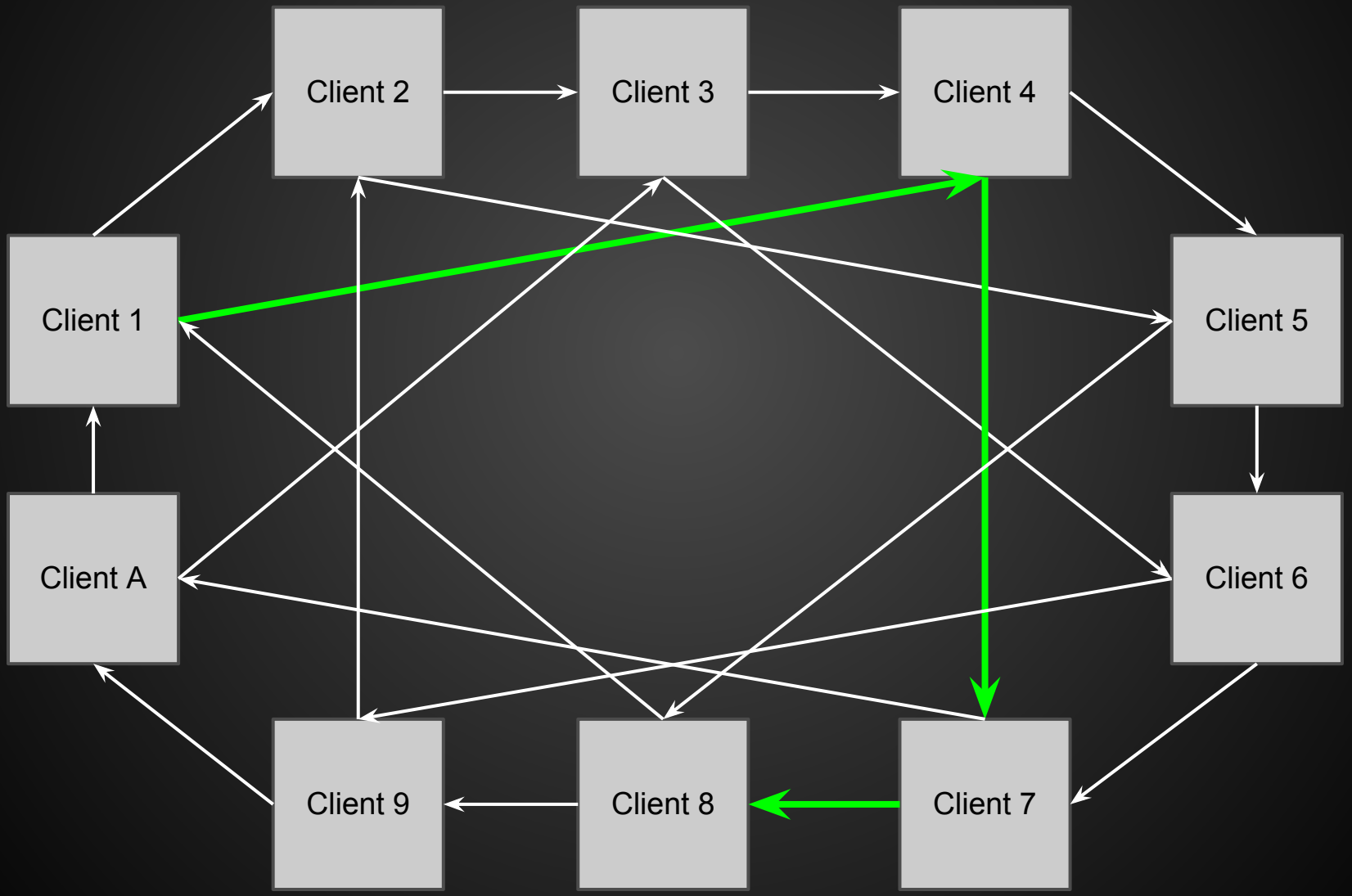
Partially Decentralised: XMPP, IRC



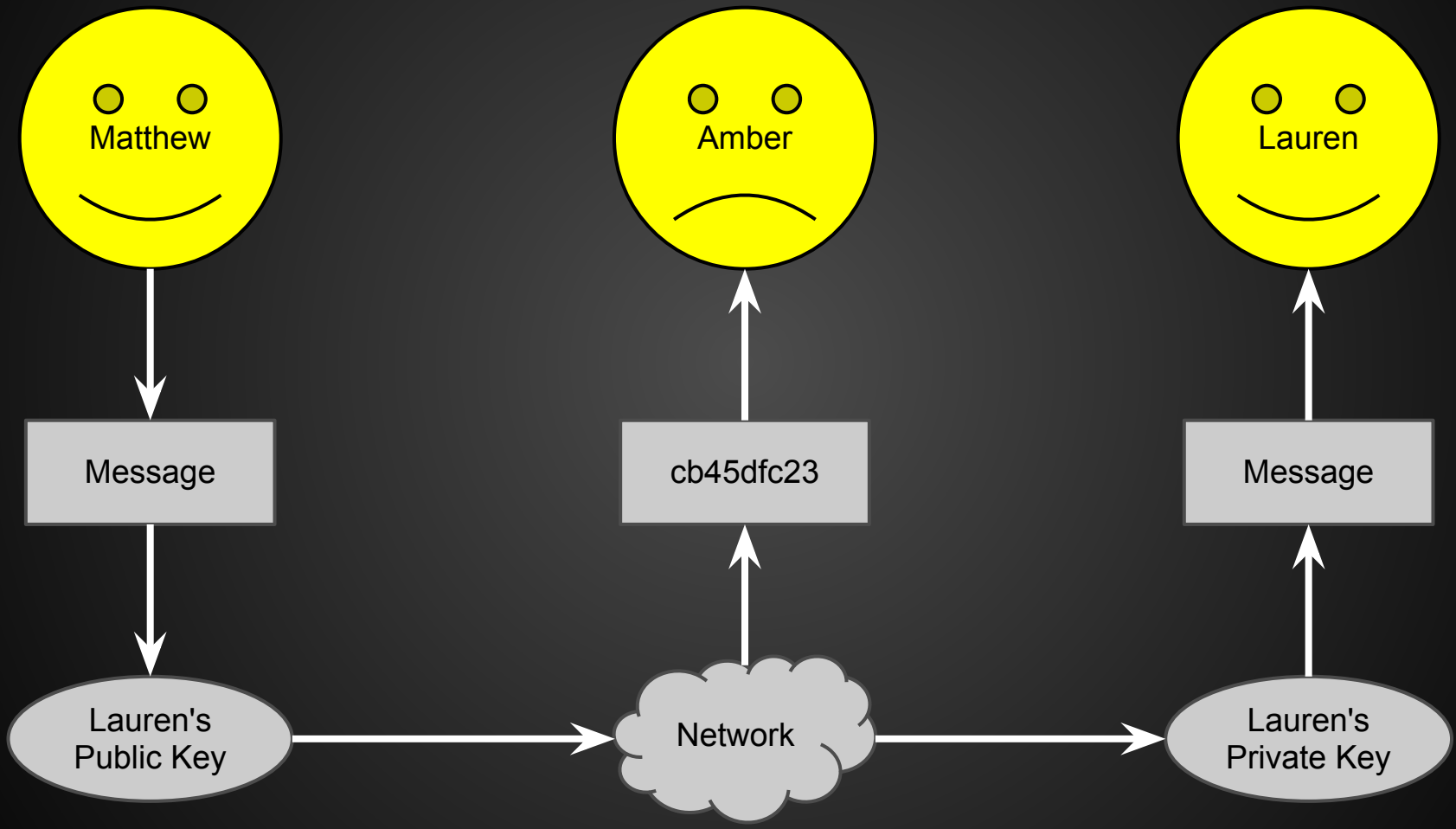
Decentralised Design: DIM



Decentralised Design: DIM



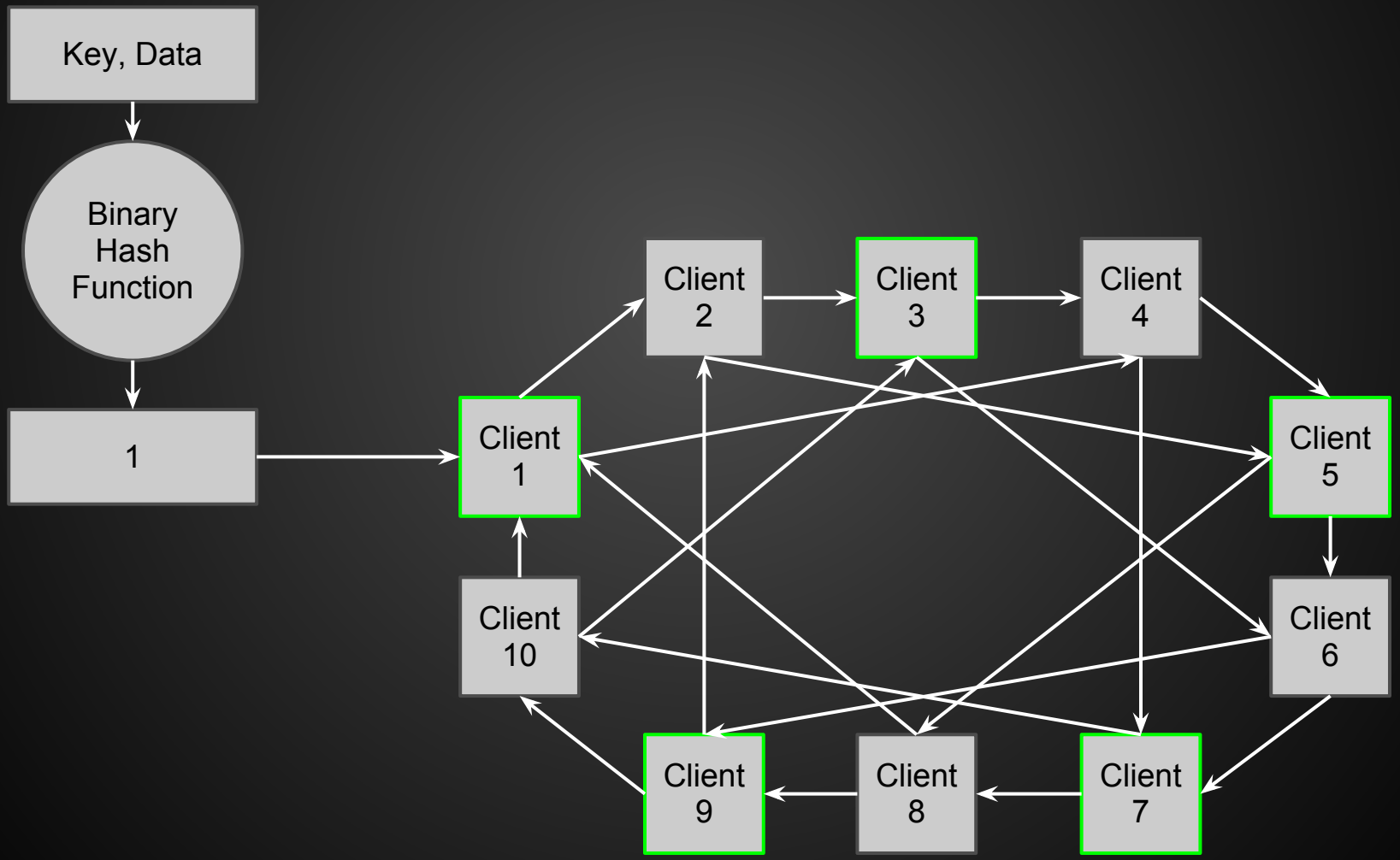
Public Key Encryption



Distributed Hash Table

- Stores (key, value) pairs in a network
- Entries are redundant
- Resistant to an individual node going offline

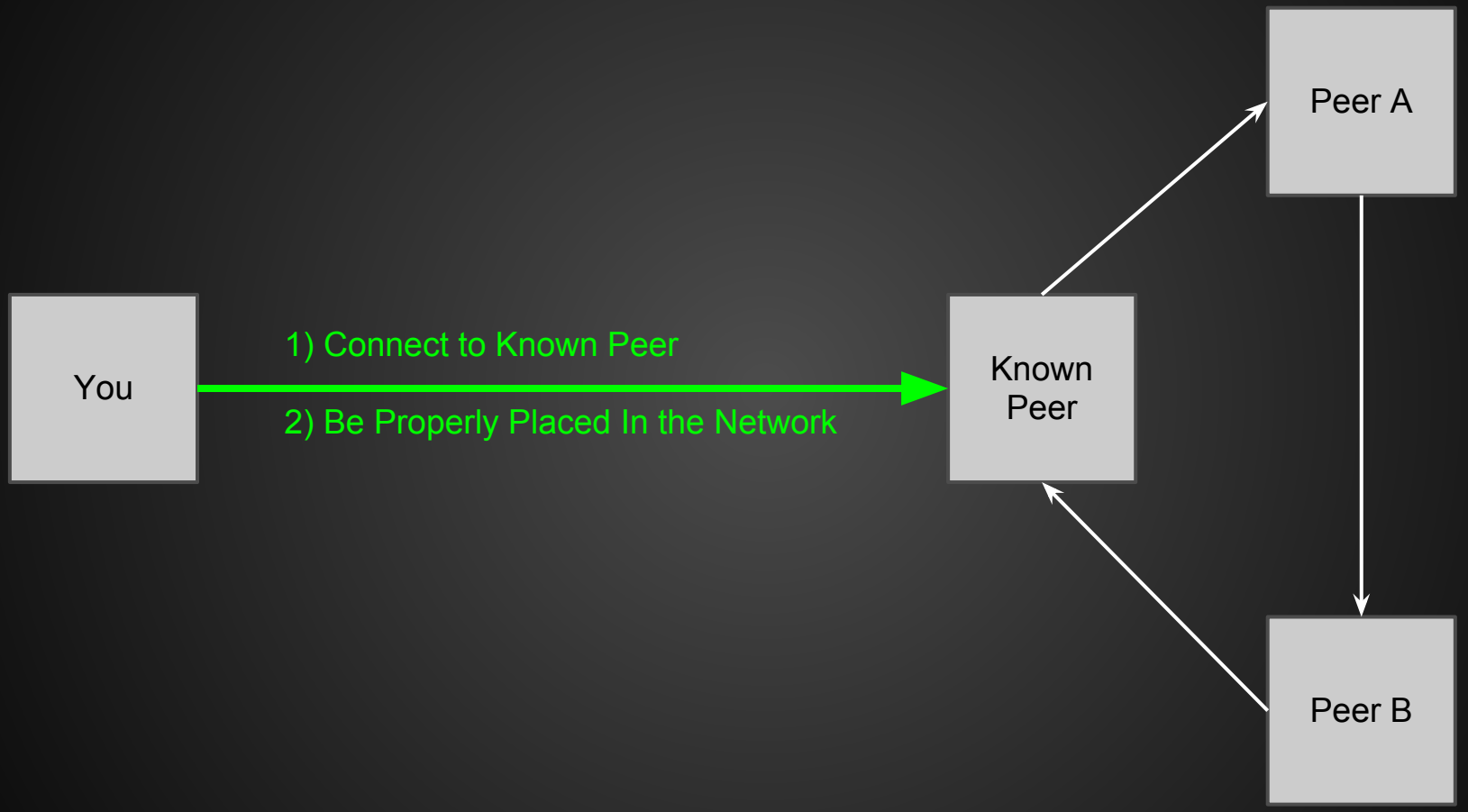
Simple Example



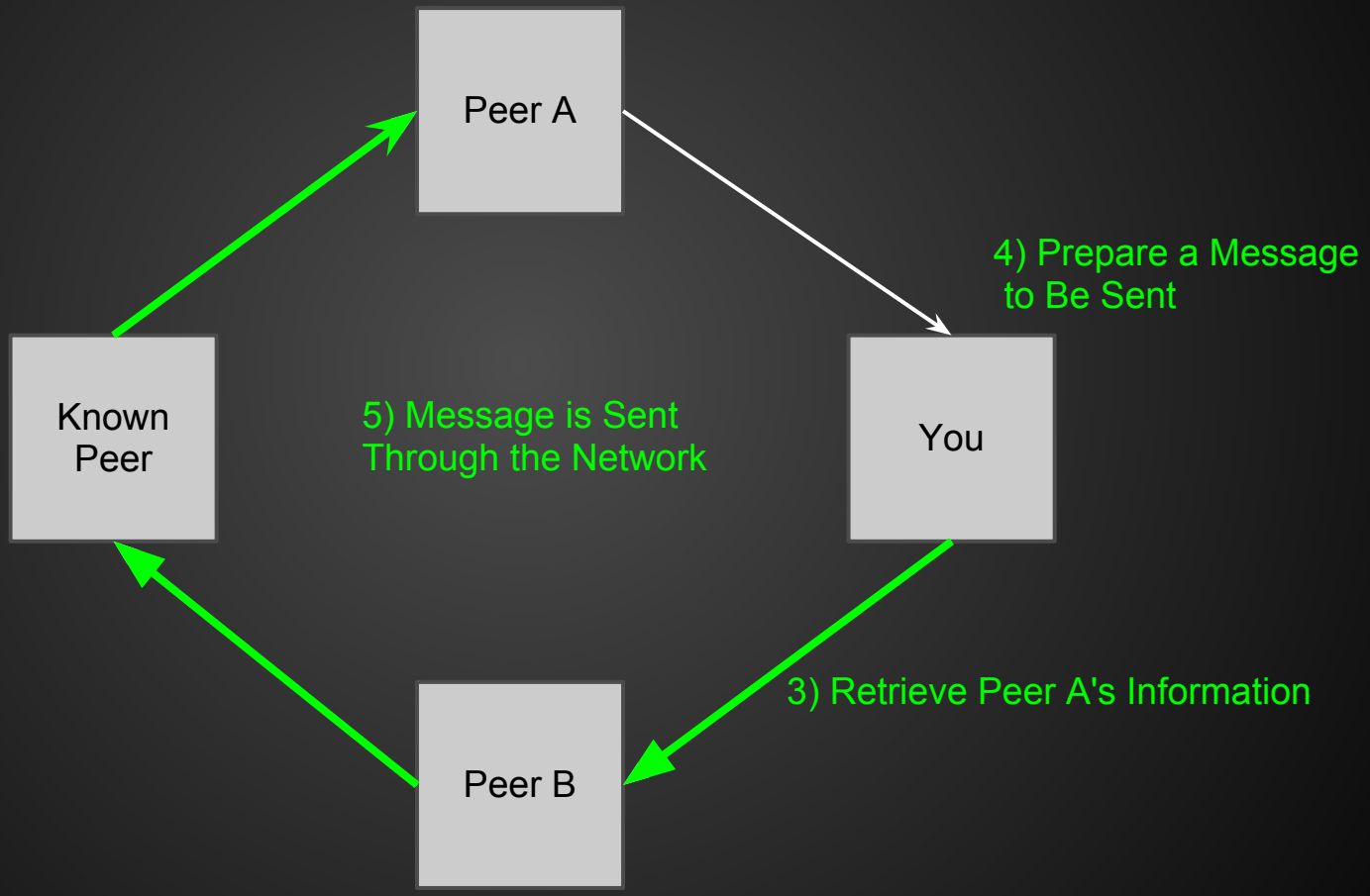
Distributed Instant Messaging

- Extended distributed hash table
  - Maintains the distributed network
  - Allows users to store data in the network
  - Allows the passing of directed messages
  - TomP2P DHT Library Used
- Public Key Encryption
  - Messages Encrypted with AES
  - AES Key encrypted with recipient's public key and sent with message
  - Ensures that messages are only read by the recipient
  - Allows users to sign data placed into the network

How Does It Work?



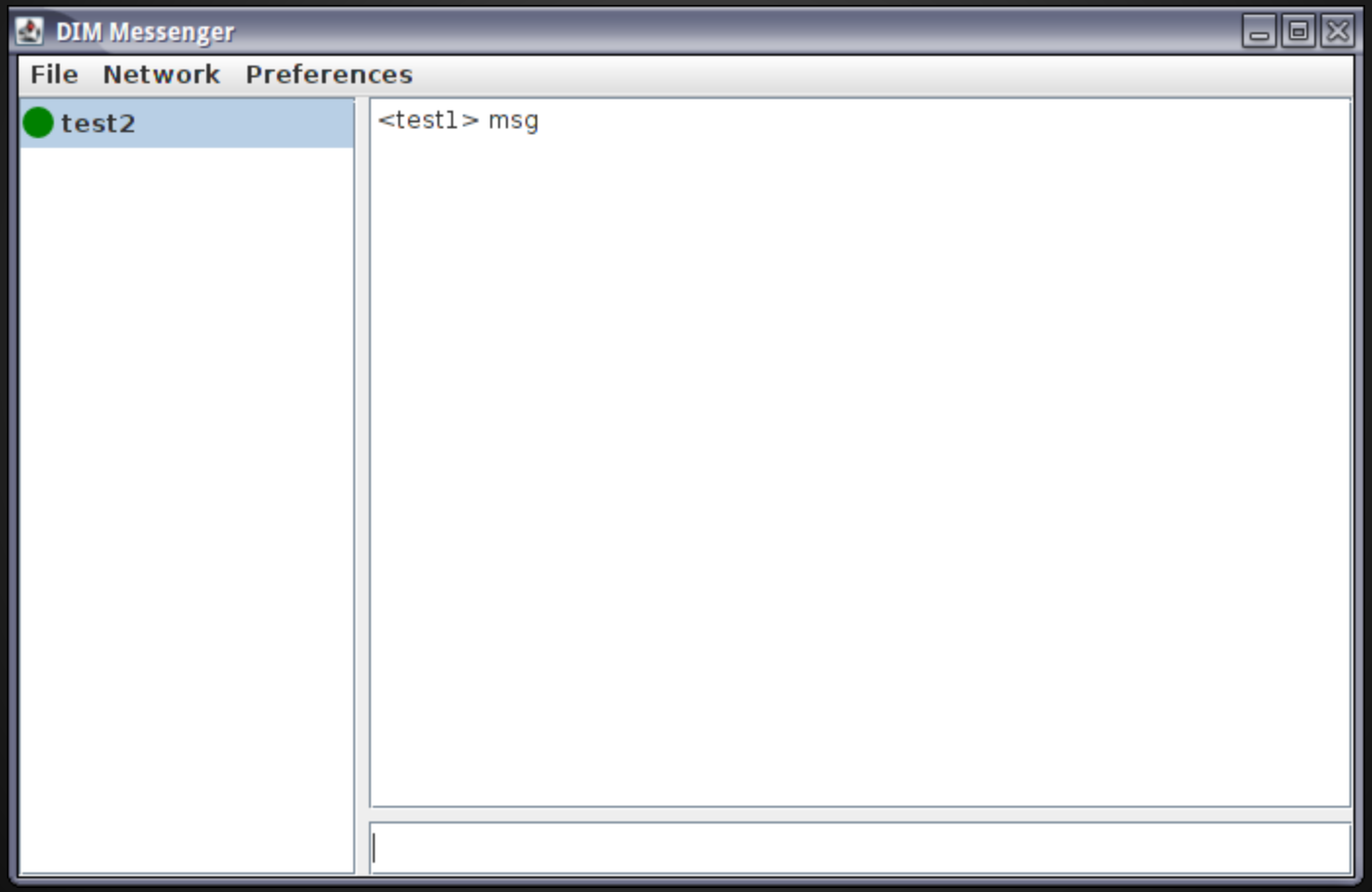
How Does It Work?



Implementation

- KeyManager
- NetworkService
  - SenderThread
  - ReceiverThread
  - tomp2p.Peer
- ContactManager
  - DIMContact

Interface



Results

- Partially secure communications
  - Does not provide perfect forward secrecy
- Resistant to shutdown
- Fairly high transmission speeds
  - Has not been extensively stress-tested due to a lack of computer systems, but TomP2P promises good scalability

Credits

- Thomas Bocek, University of Zurich
  - Author of TomP2P Extended DHT library