

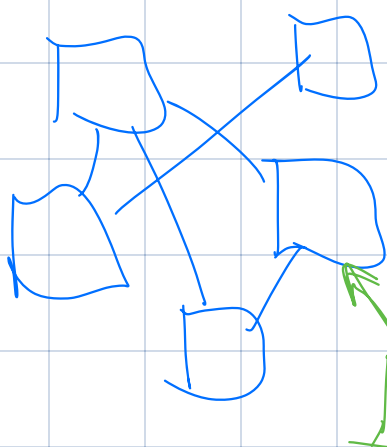
CompSci 461/661 Oct 6

- • HW & midterm (this week last topic)
- Bitcoin Networking
 - eclipse attacks
- Single (Just coinbase) txn paper
- Clock sync
 - Lamport's Logical Clock
 - Totally ordered Message Delivery
 - Breaking LLC

Bitcoin Networking

- P2P network → Every node is in the same role ~~NOT client/server!~~
- Gossip network → everyone tells everyone else everything

Server "listen" part ← Client connects
Standard TCP



- Random graph:

Benefits: difficult to partition.

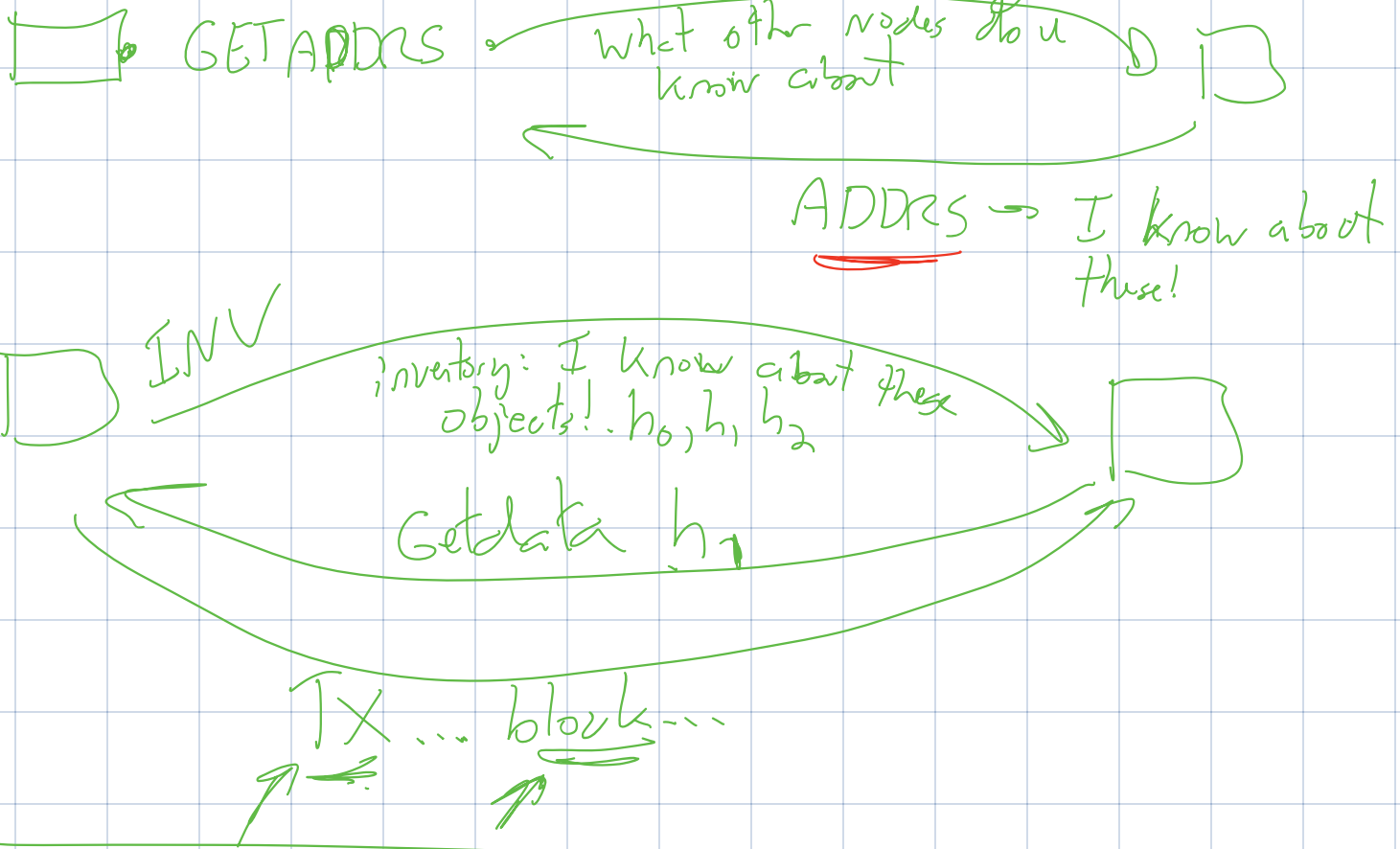
- Scale free

First

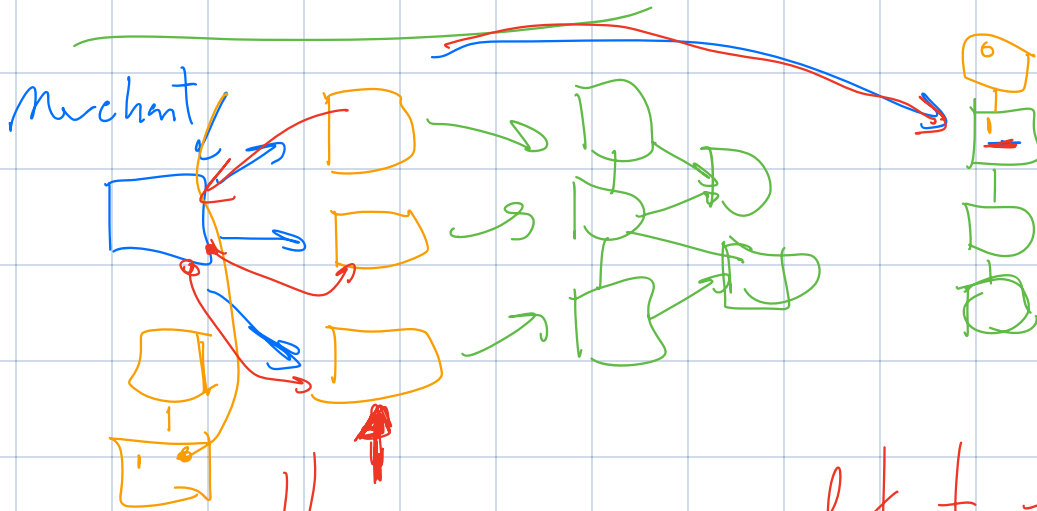
→ IRC - 1st social media

→ Now: DNS system

seeder.ruxa.org

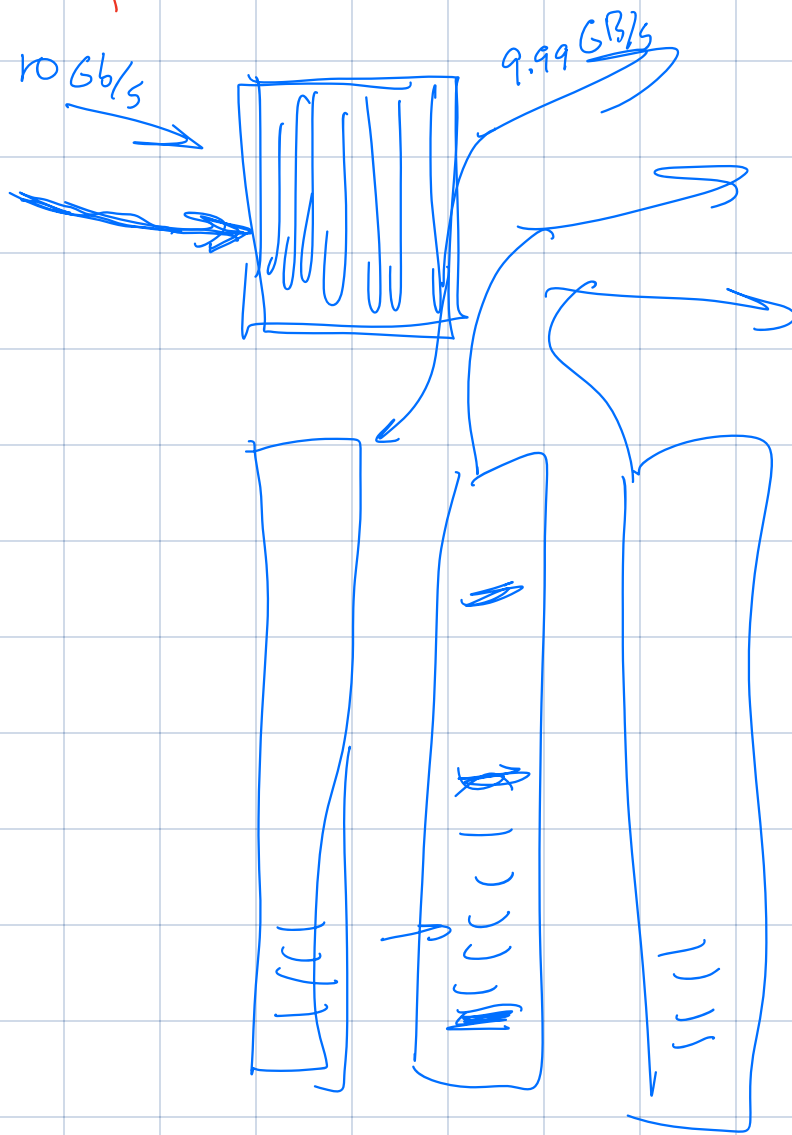


Eclipse Attacks

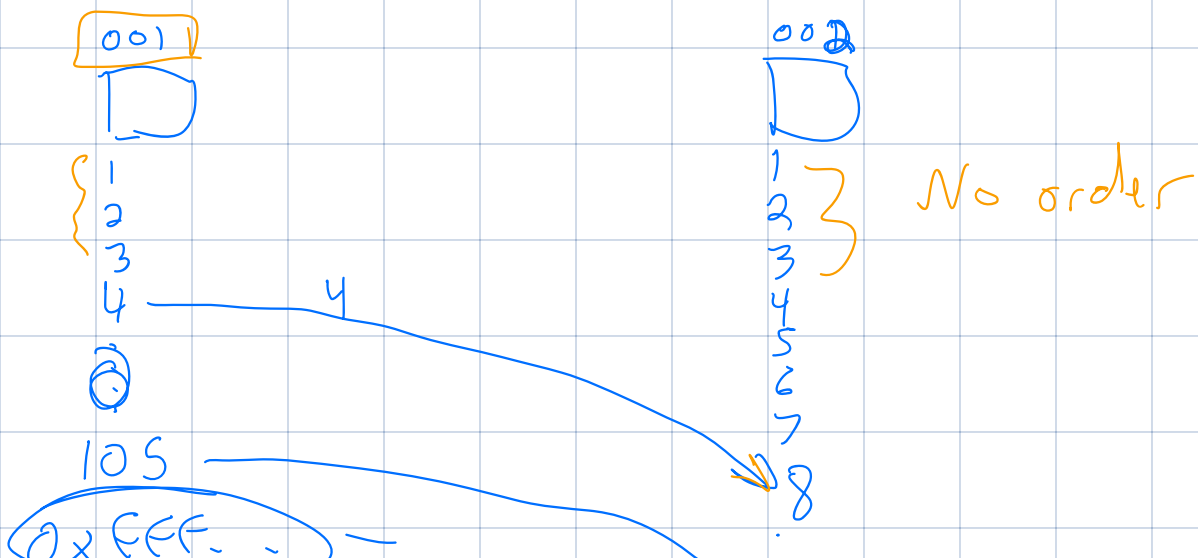


How can you detect that you've isolated the merchant?

Lamport's Logical Clock



Campport's Logical Clocks



Partial ordering → 106

→ Lamport's Totally ordered Message System

Model: multicast, reliable, ordered, not able to force msgs

receive msg:

- ACK every msg that comes in
 - • wait for every ack
 - enqueue the msg sorted by LLC
 - only send the top msg to app
- Alice hears M reverse its LLC
Send T then ack M

