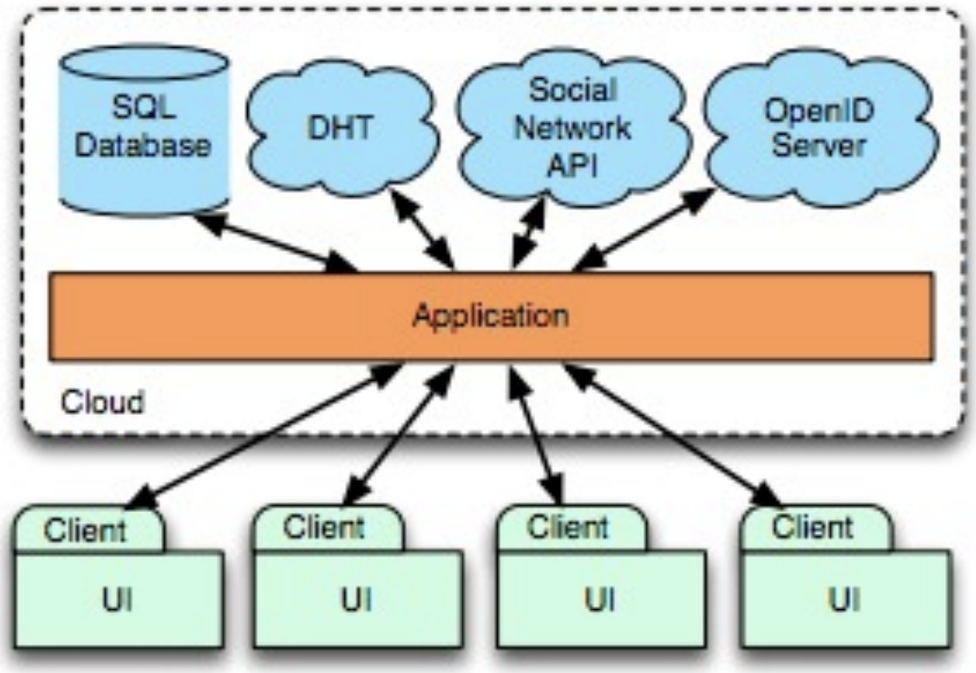
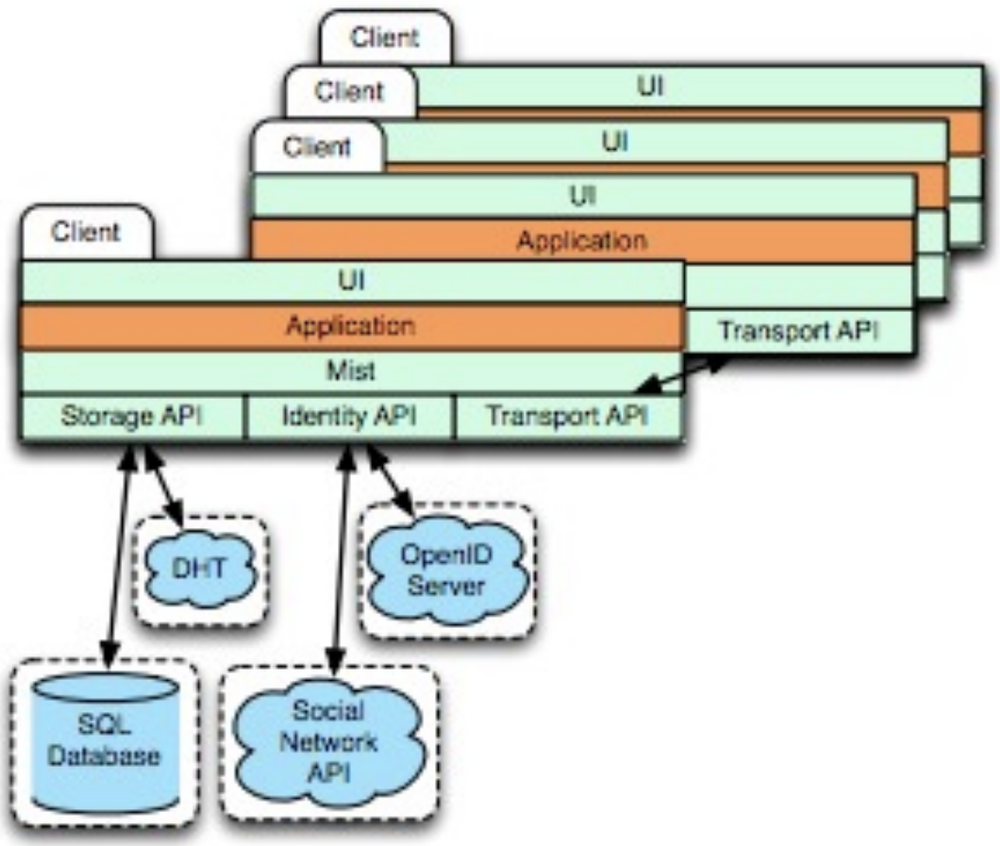
FreeDOM

452 May 30

FreeDOM


SQL Database
DHT
Social Network API
OpenID Server
Application
Cloud
Client
UI
Client
UI
Client
UI
Client
UI


Client
Client
UI
Client
UI
UI
Application
Client
UI
Application
Transport API
Mist
Storage API
Identity API
Transport API
DHT
OpenID Server
SQL Database
Social Network API

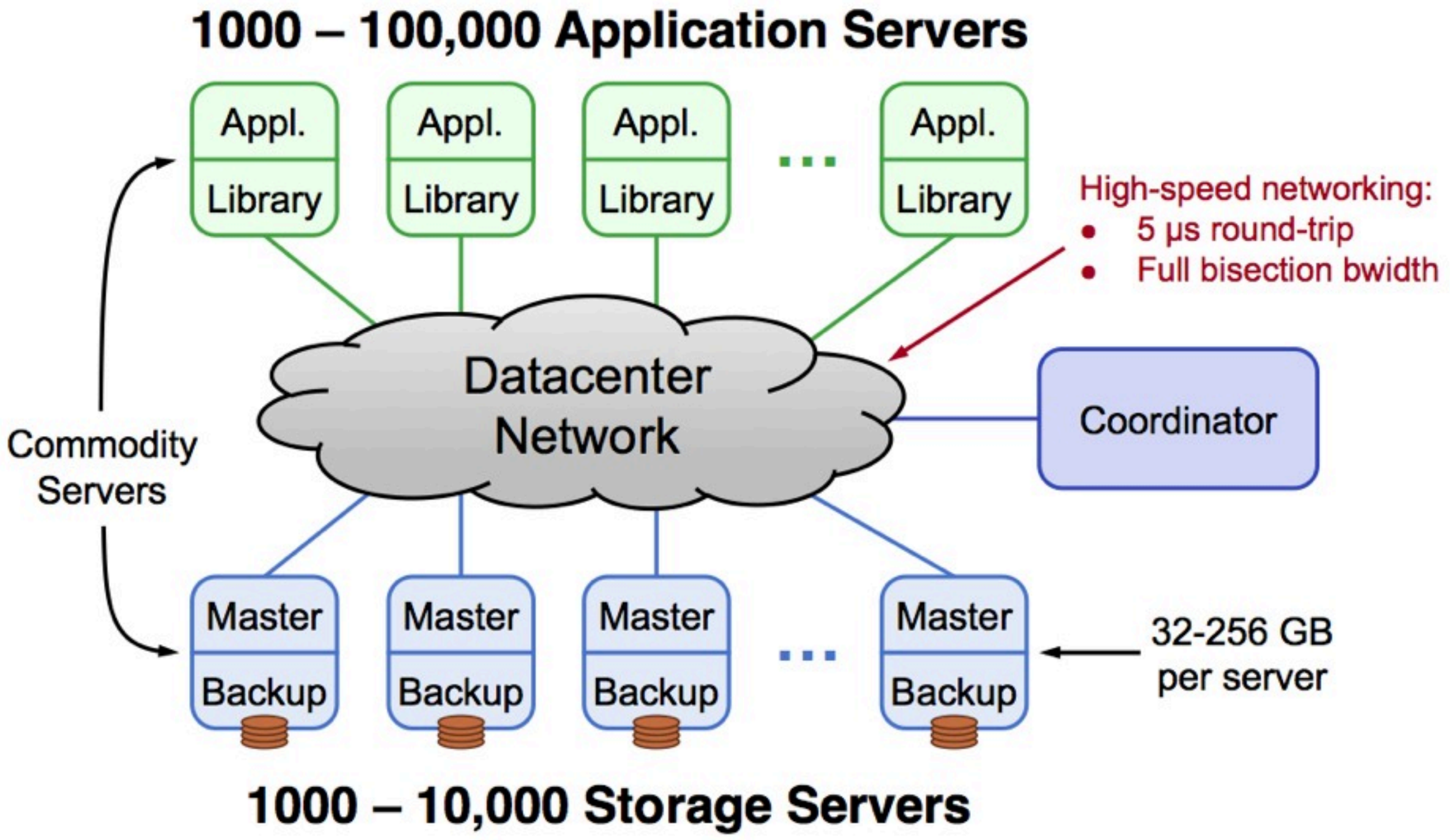
FreeDOM

- Cooperative Storage
- Resilient Communication
- Work Scheduling

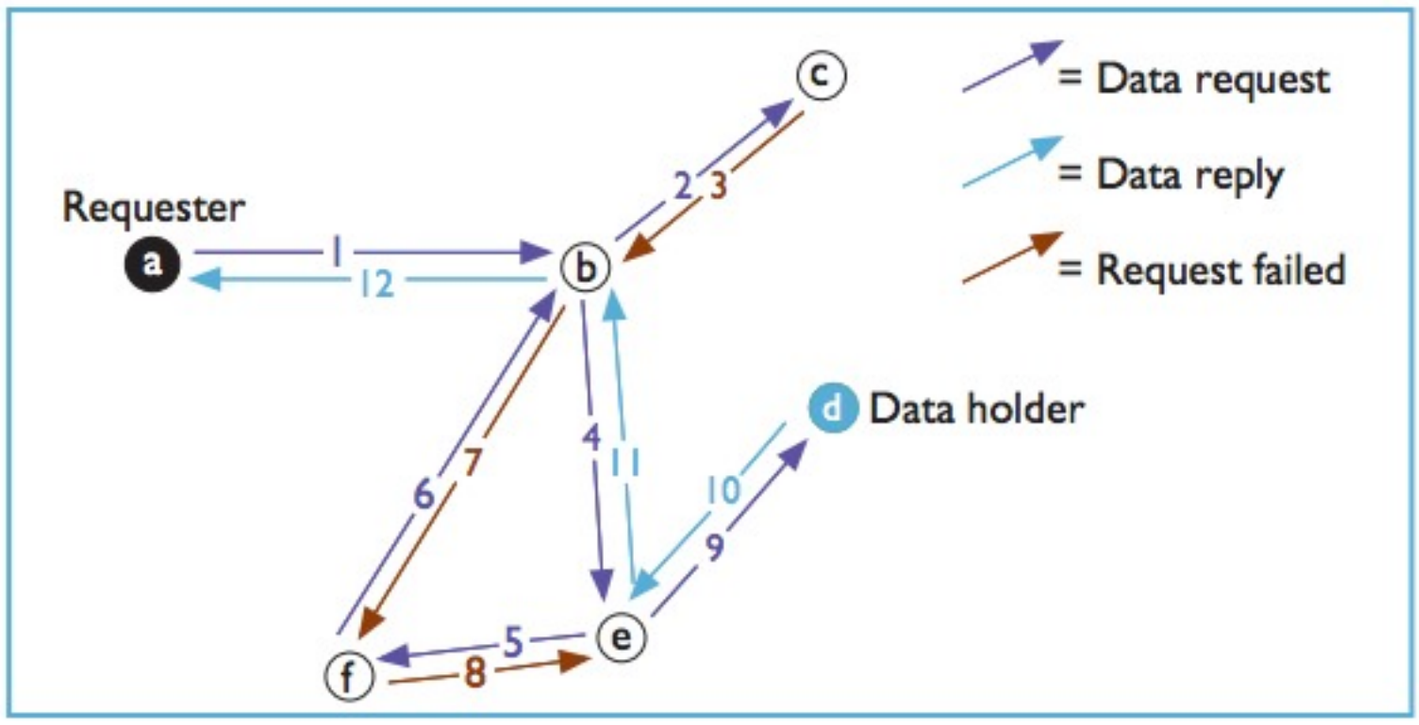
Cooperative Storage

- DHTs
- ramcloud
- Freenet

Ramcloud


1000 – 100,000 Application Servers
Appl.
Library
Appl.
Library
Appl.
Library
...
Appl.
Library
High-speed networking:
• 5 µs round-trip
• Full bisection bwidth
Datacenter
Network
Coordinator
Commodity
Servers
Master
Backup
Master
Backup
Master
Backup
...
Master
Backup
32-256 GB
per server
1000 – 10,000 Storage Servers

Freenet


= Data request
= Data reply
= Request failed
Requester
a
b
c
d Data holder
e
f
1
12
2
3
4
11
5
6
7
8
9
10

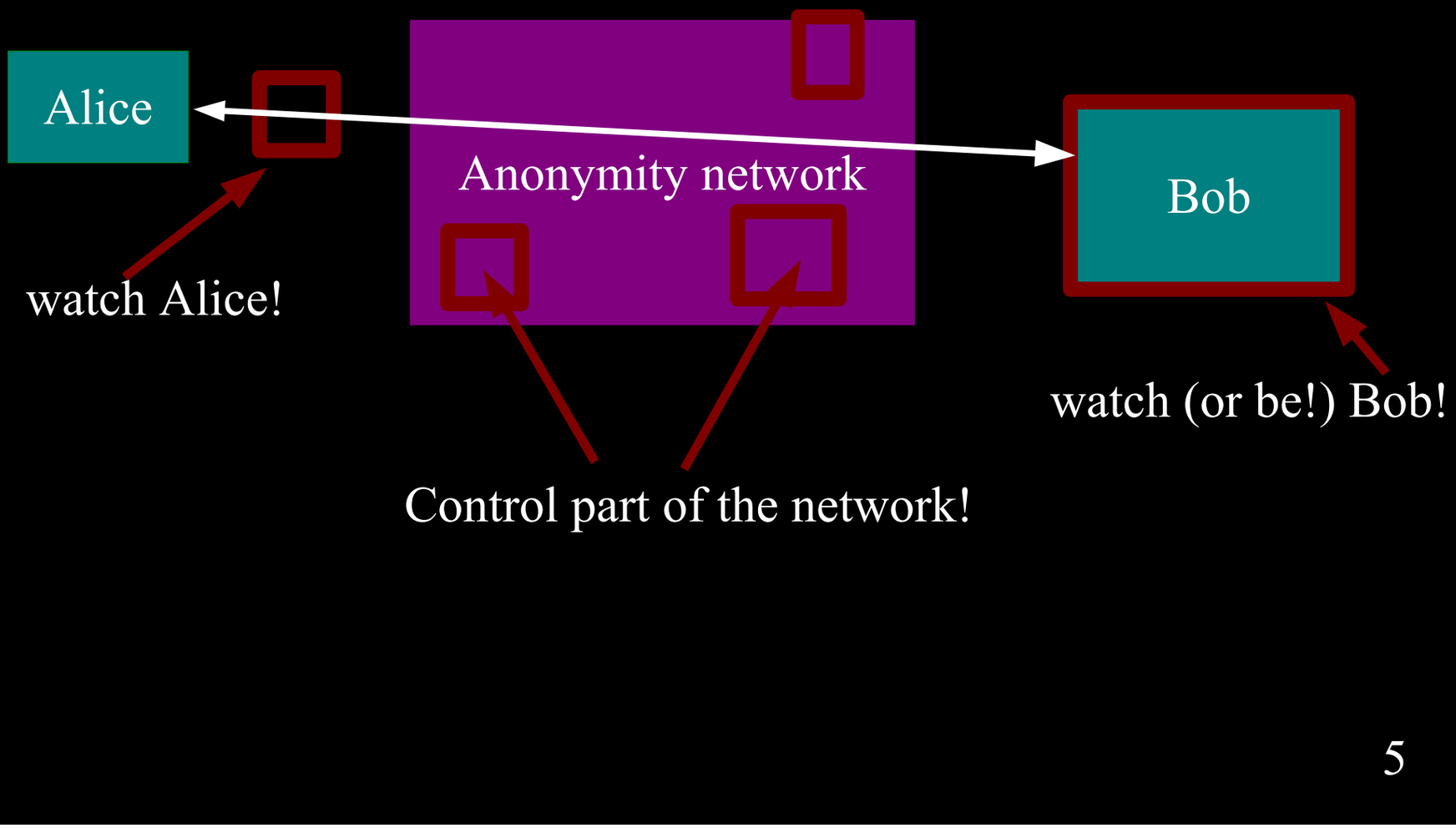
Communication Resilience

- RON
- Tor
- Diaspora

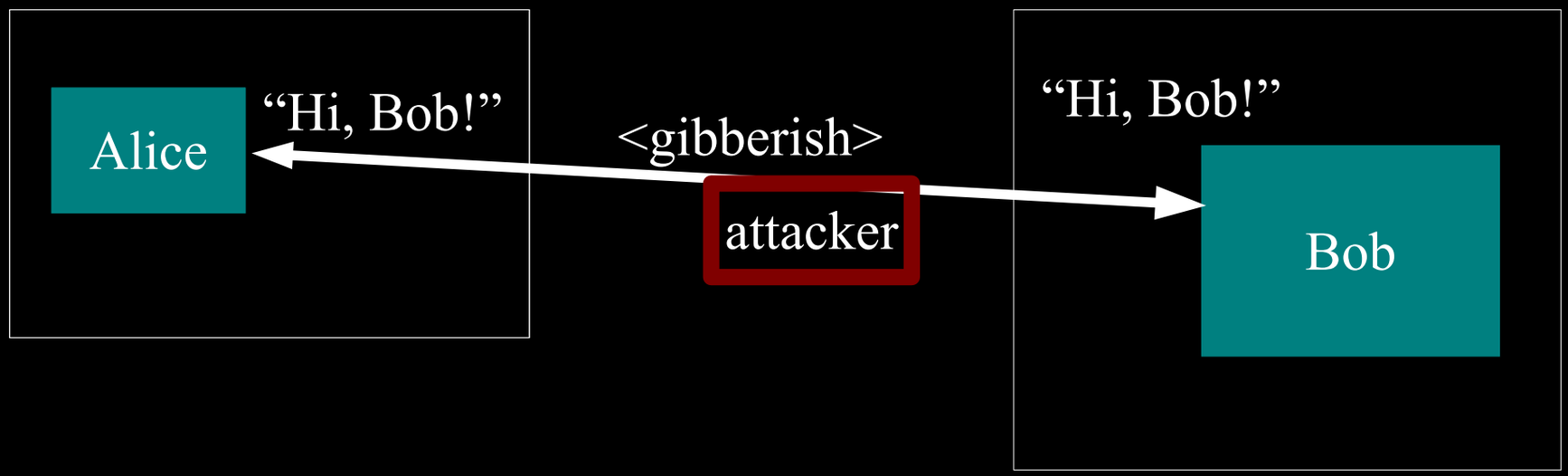
Resilient Overlay Networks

RON was able to successfully detect and recover from 100% (in RON_1) and 60% (in RON_2) of all complete outages and all periods of sustained high loss rates of 30% or more.	6.2
RON takes 18 seconds, on average, to route around a failure and can do so in the face of a flooding attack.	6.2
RON successfully routed around bad throughput failures, doubling TCP throughput in 5% of all samples.	6.3
In 5% of the samples, RON reduced the loss probability by 0.05 or more.	6.3
Single-hop route indirection captured the majority of benefits in our RON deployment, for both outage recovery and latency optimization.	6.4

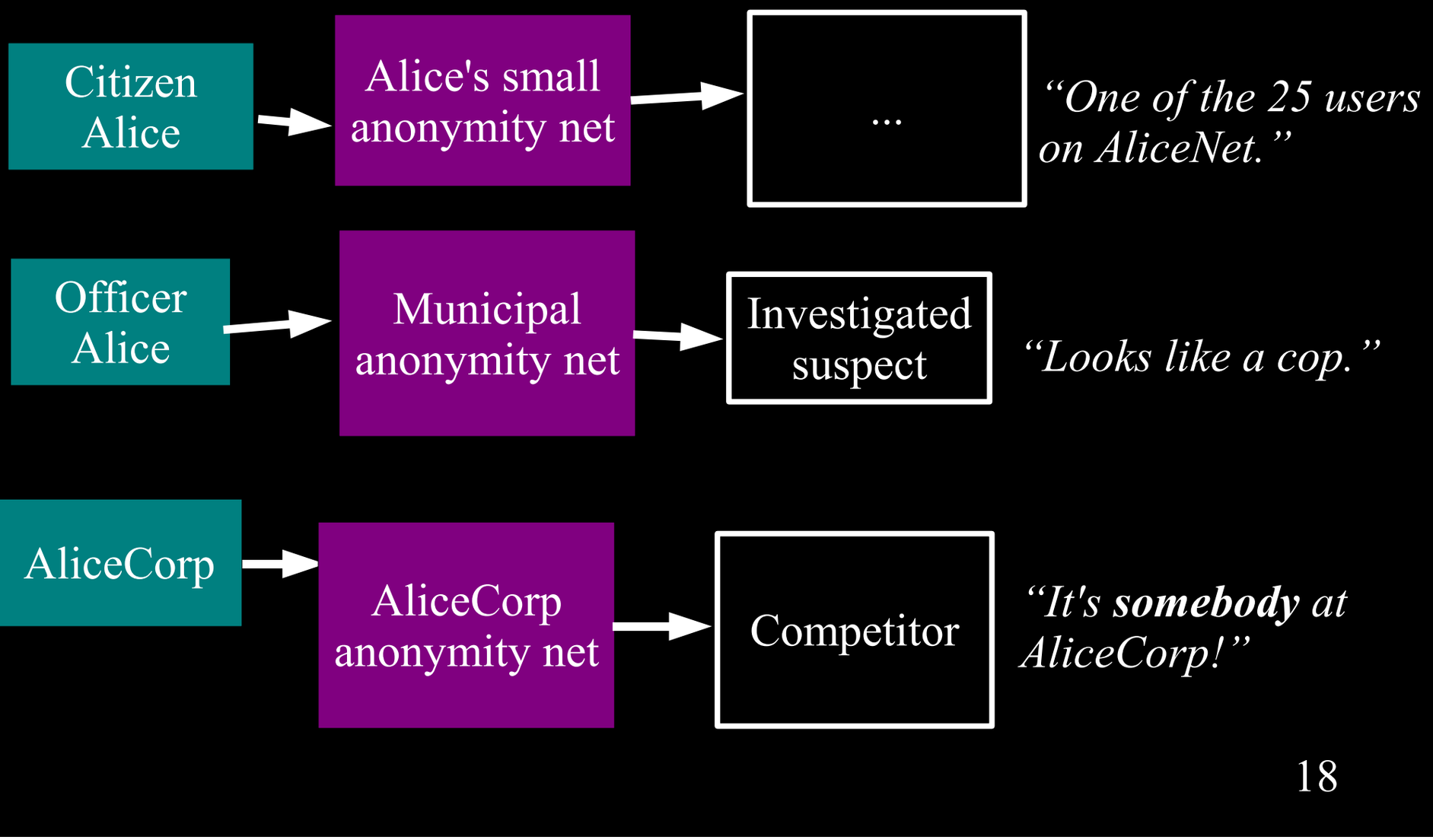
Threat model: what can the attacker do?



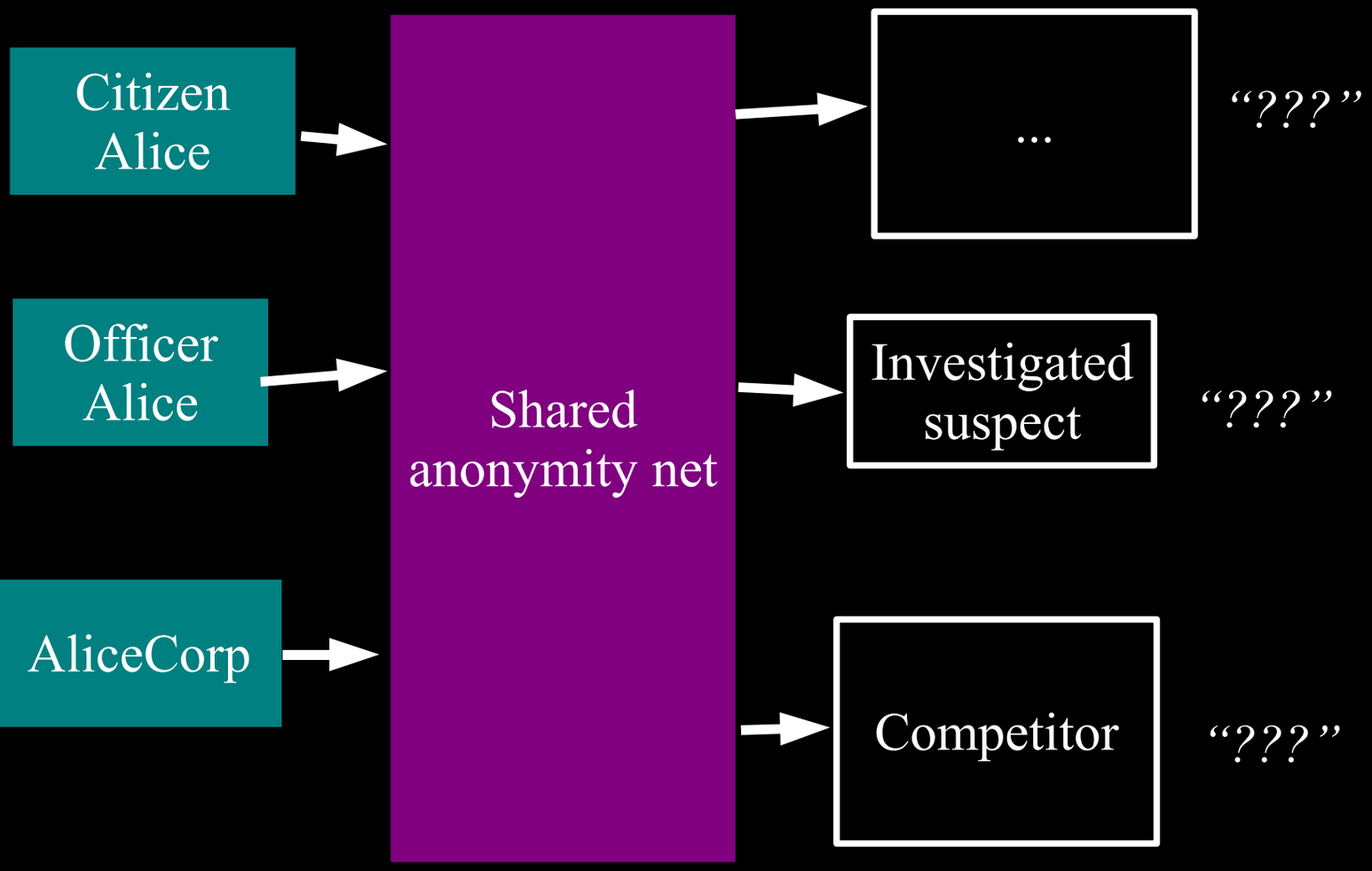
Anonymity isn't cryptography: Cryptography just protects contents.



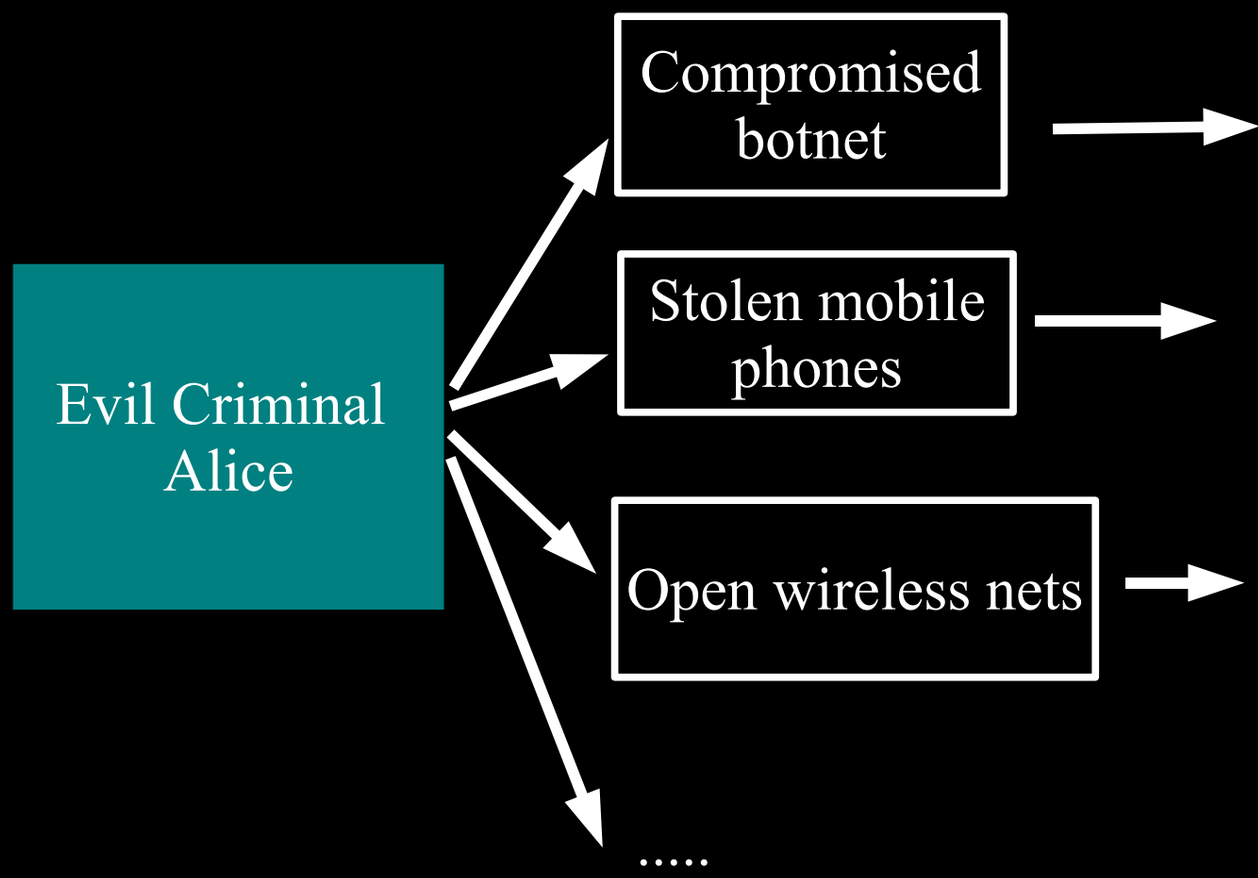
You can't get anonymity on your own: private solutions are ineffective...



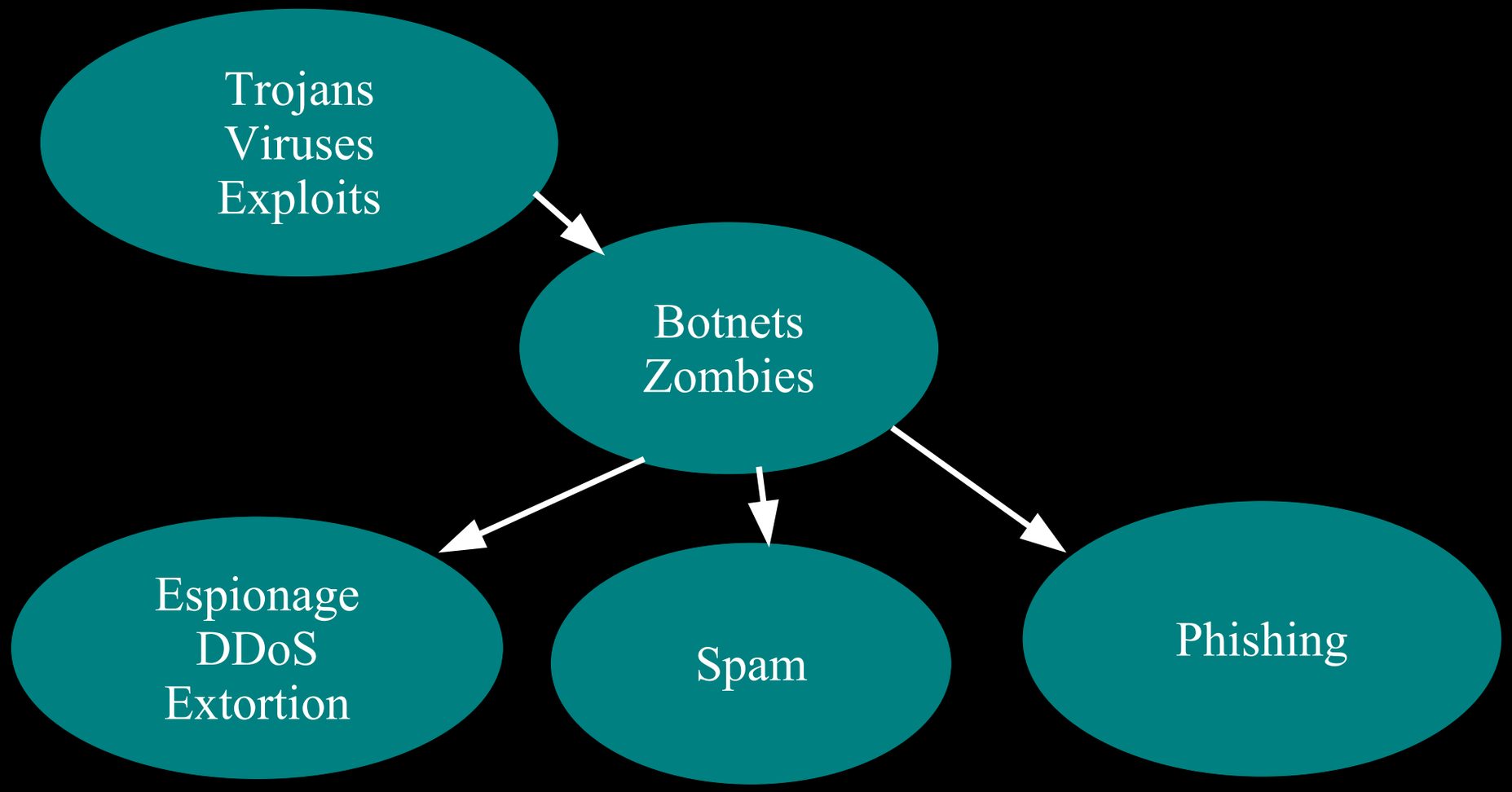
... so, anonymity loves company!



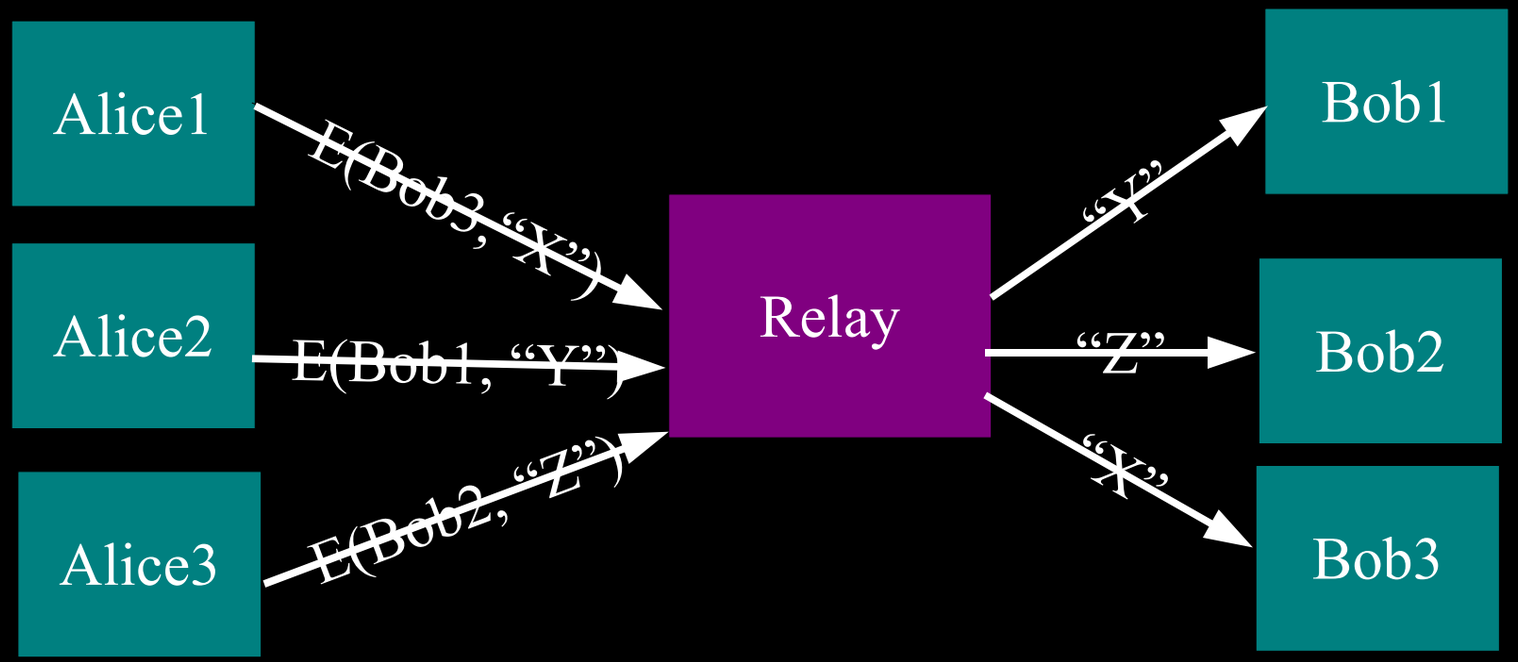
Yes, bad people need anonymity too. But they are *already* doing well.



Current situation: Bad people on the Internet are doing fine

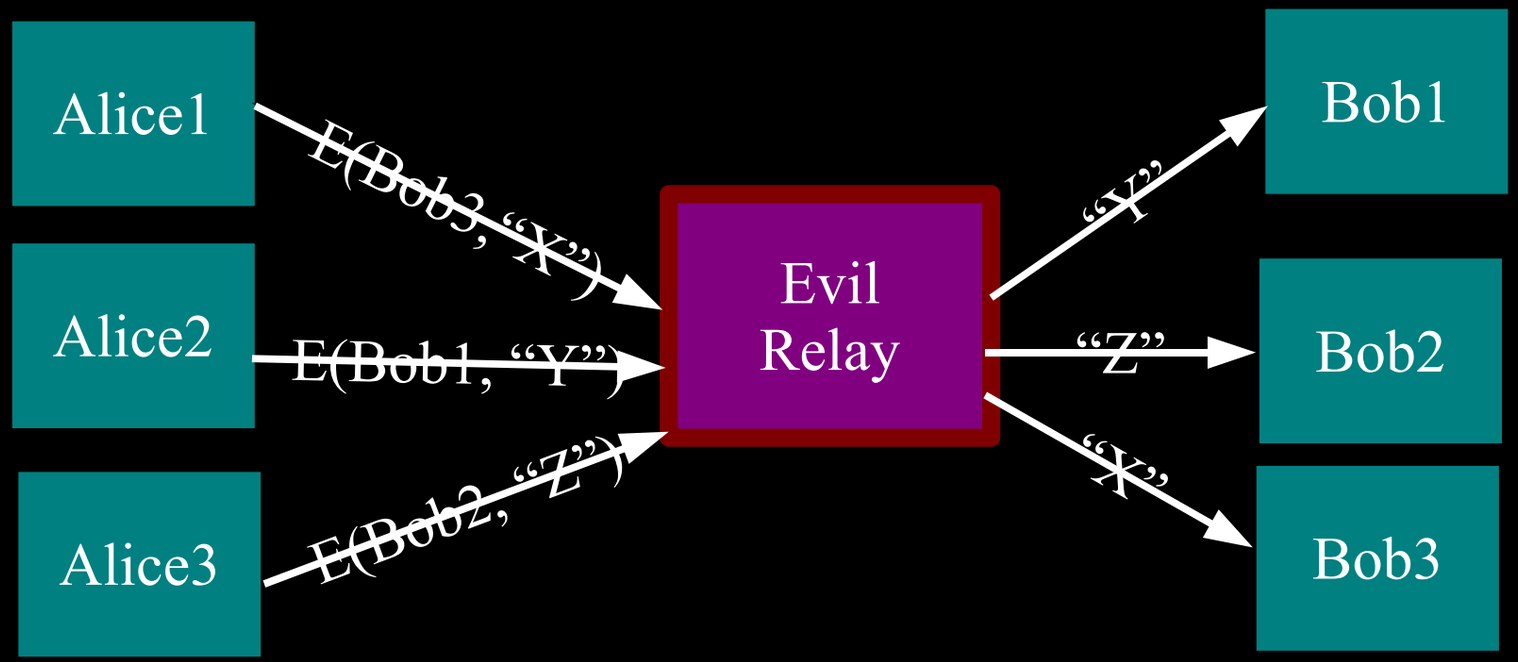


The simplest designs use a single relay to hide connections.

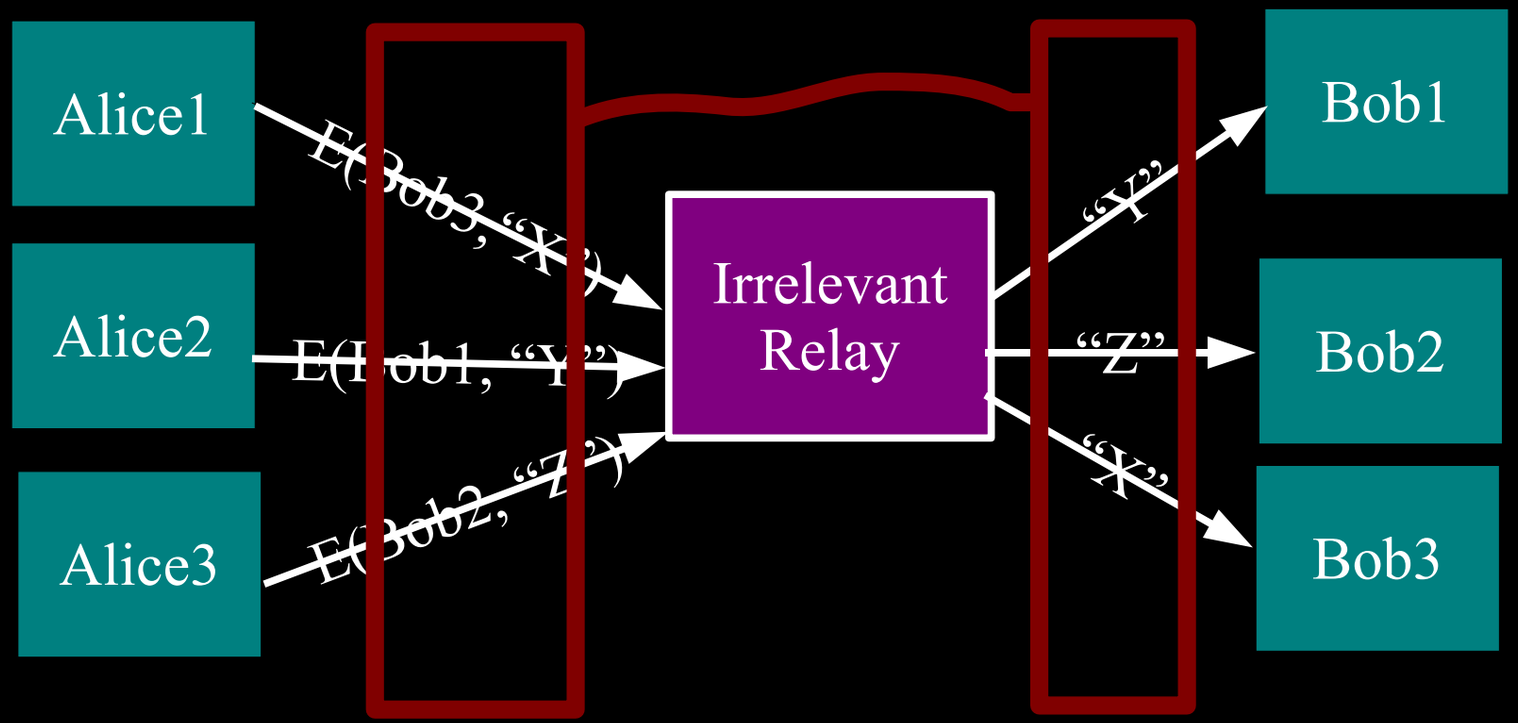


(example: some commercial proxy providers)

But a single relay (or eavesdropper!) is a single point of failure.

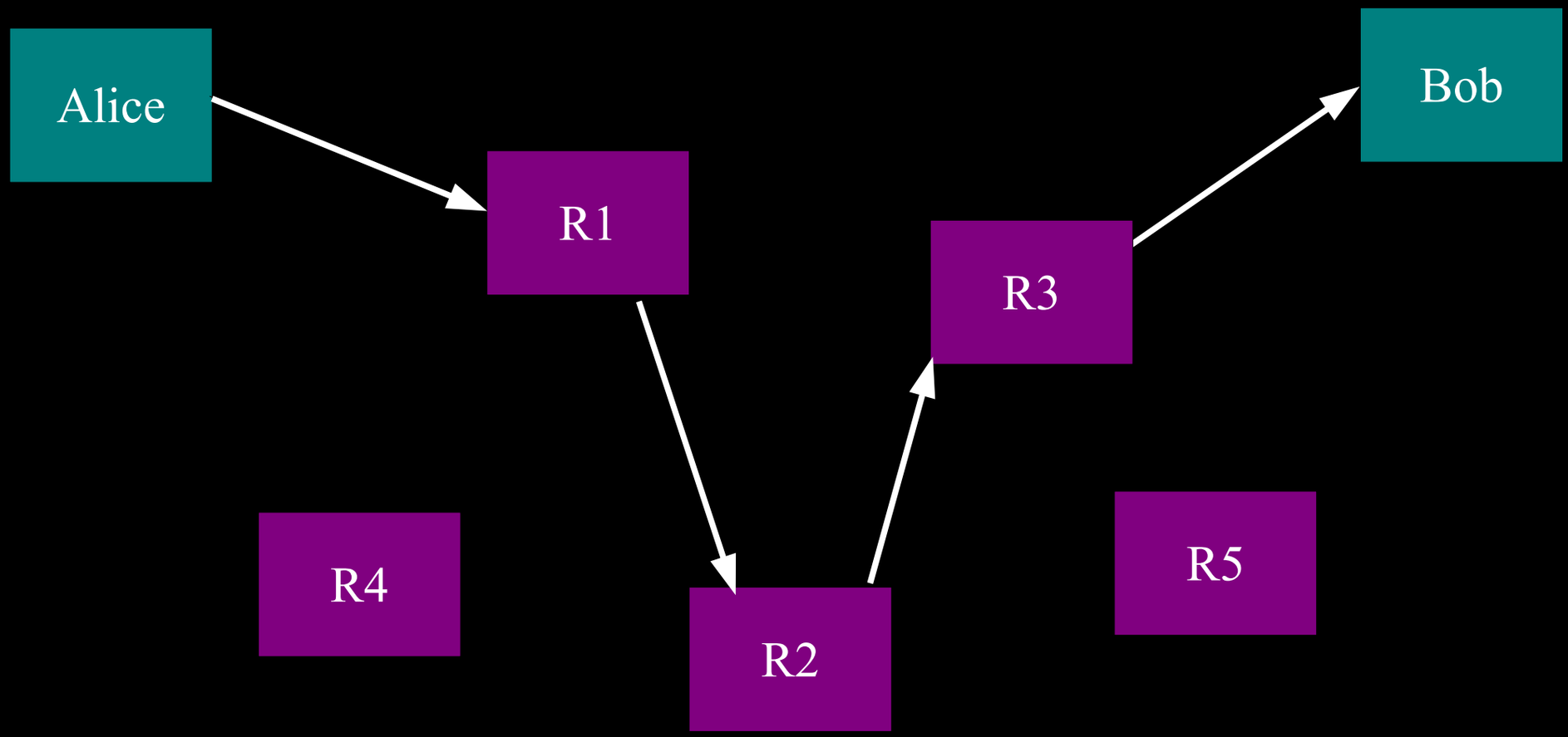


... or a single point of bypass.

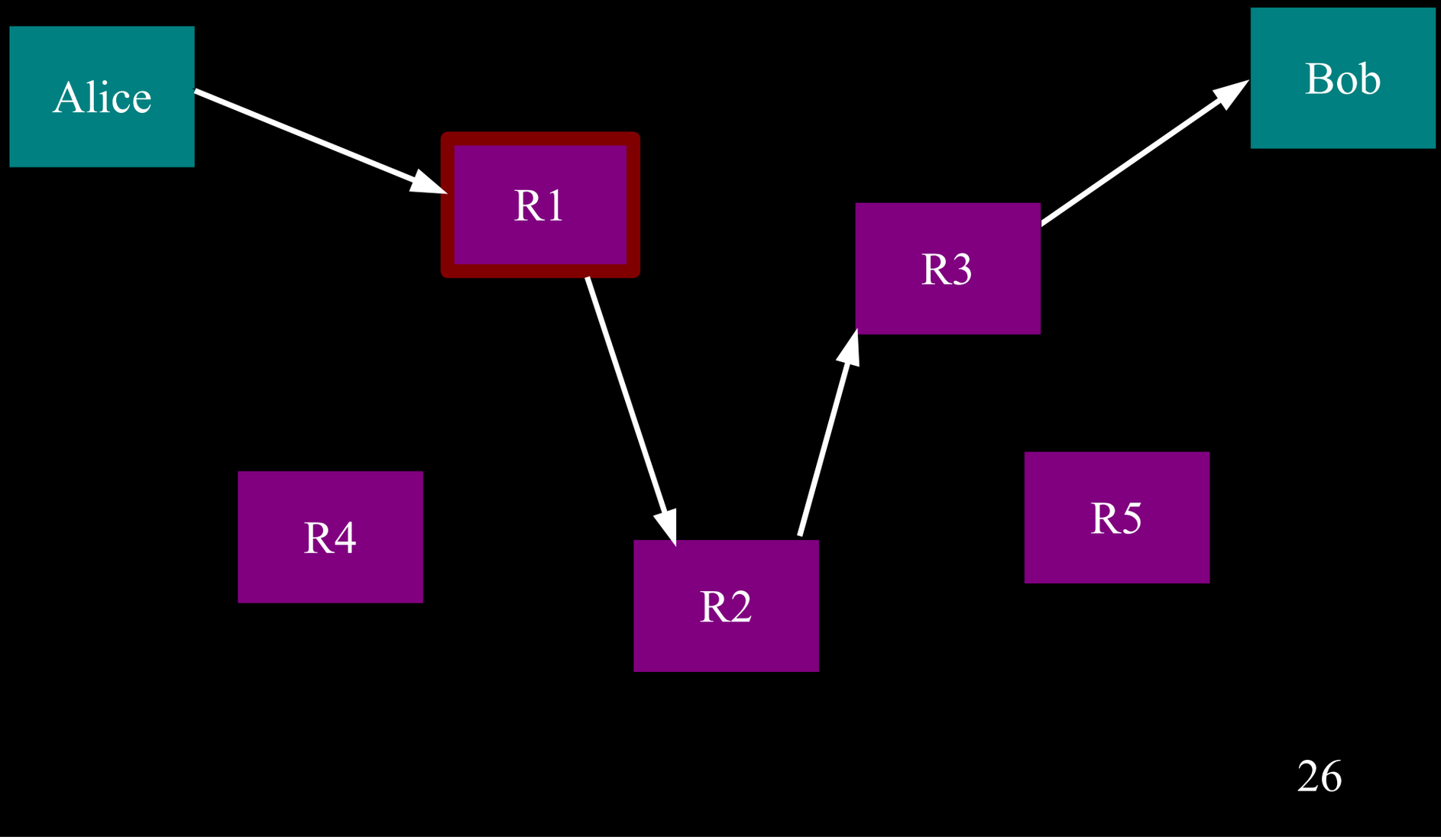


Timing analysis bridges all connections through relay ⇒ An attractive fat target

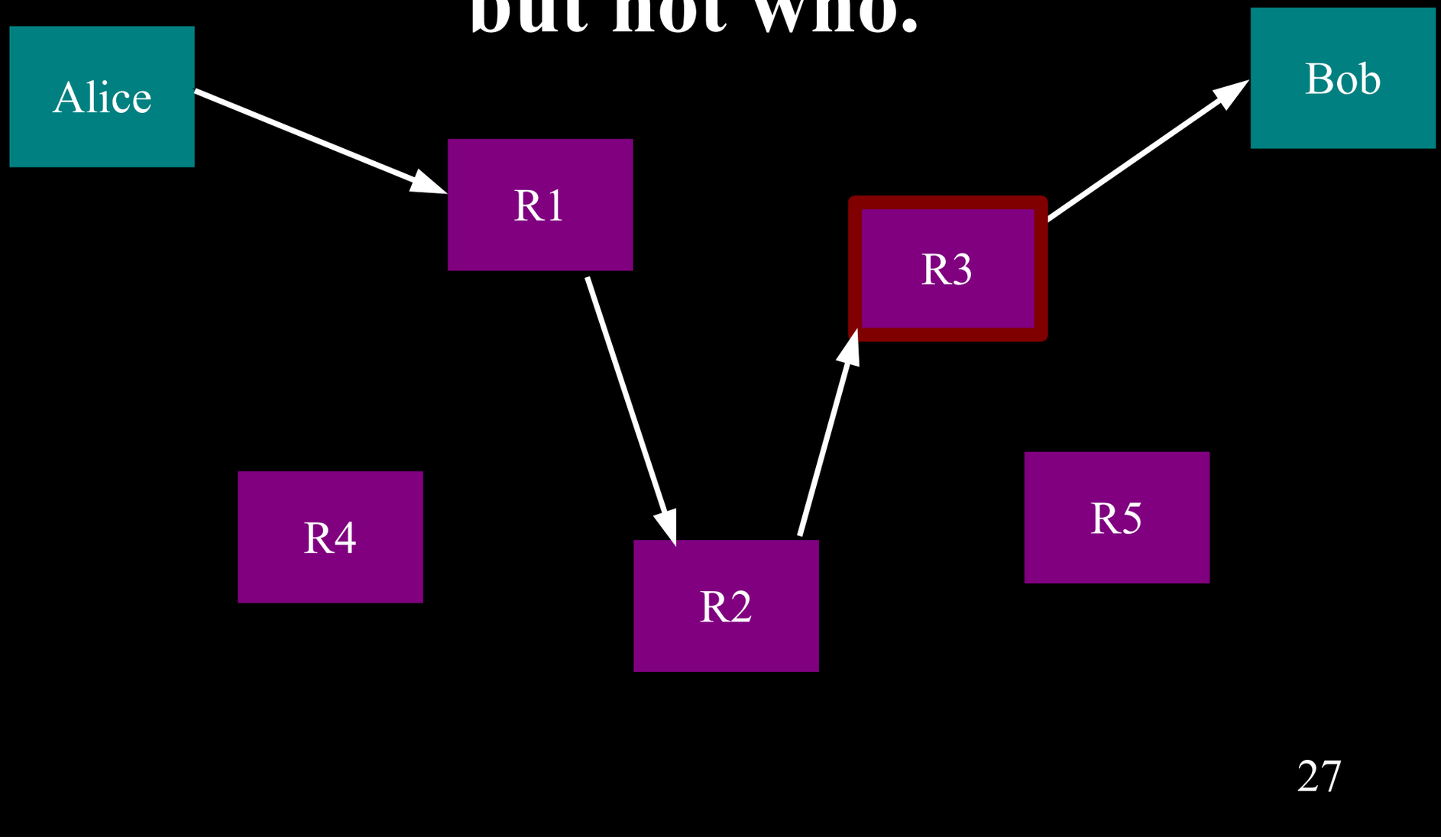
So, add multiple relays so that no single one can betray Alice.



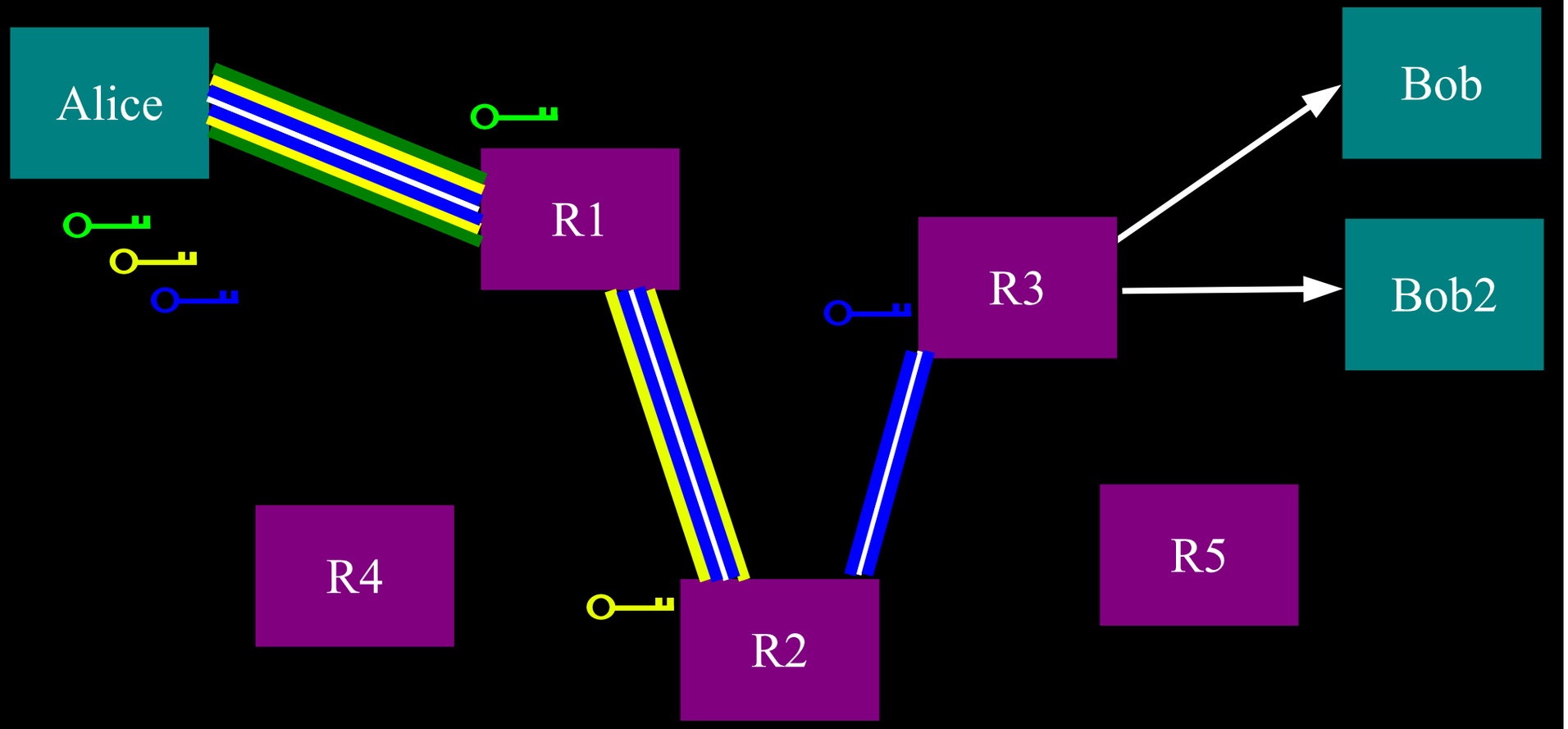
A corrupt first hop can tell that Alice is talking, but not to whom.



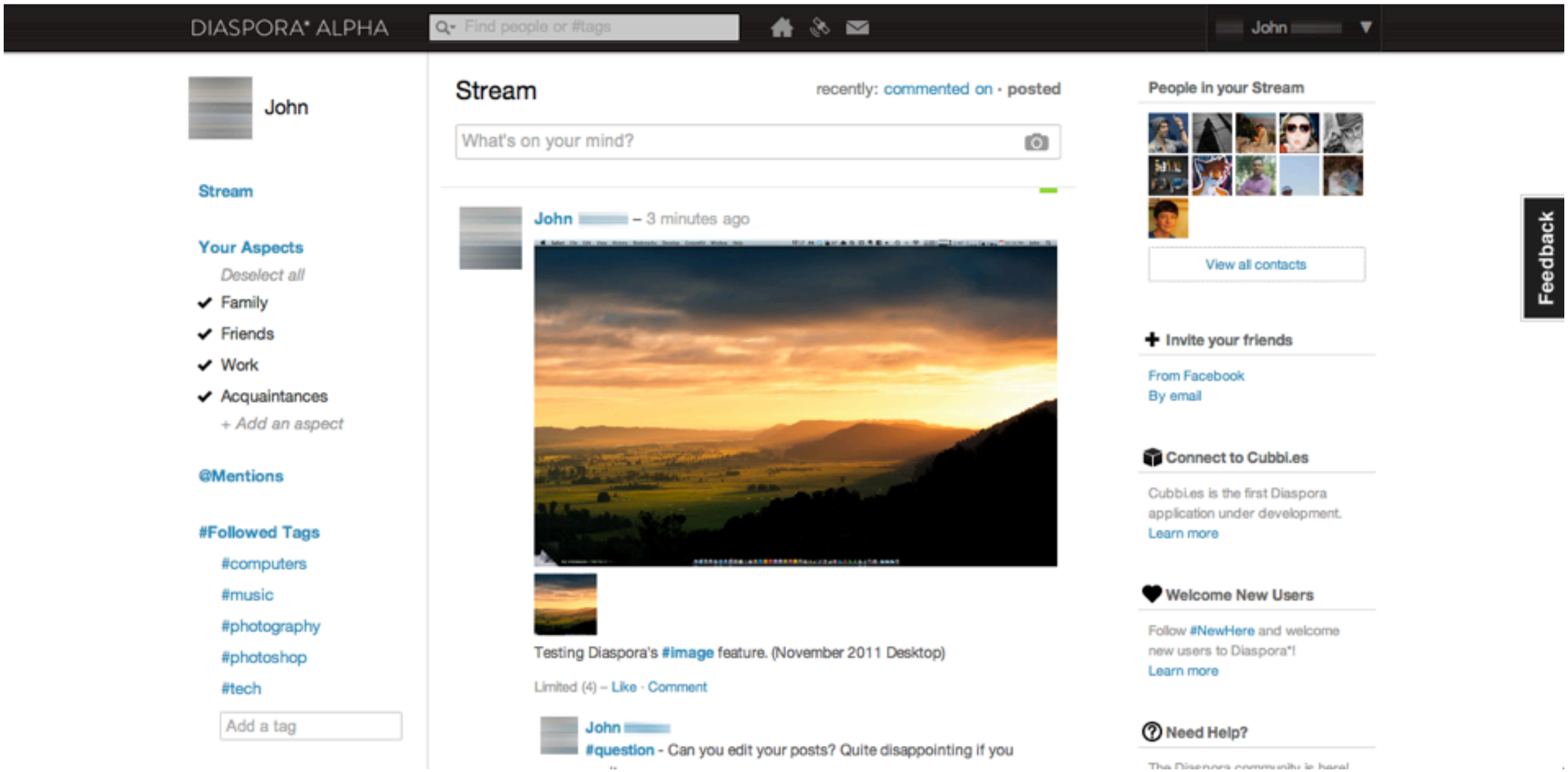
A corrupt final hop can tell that somebody is talking to Bob, but not who.



Alice makes a session key with R1 ...And then tunnels to R2...and to R3



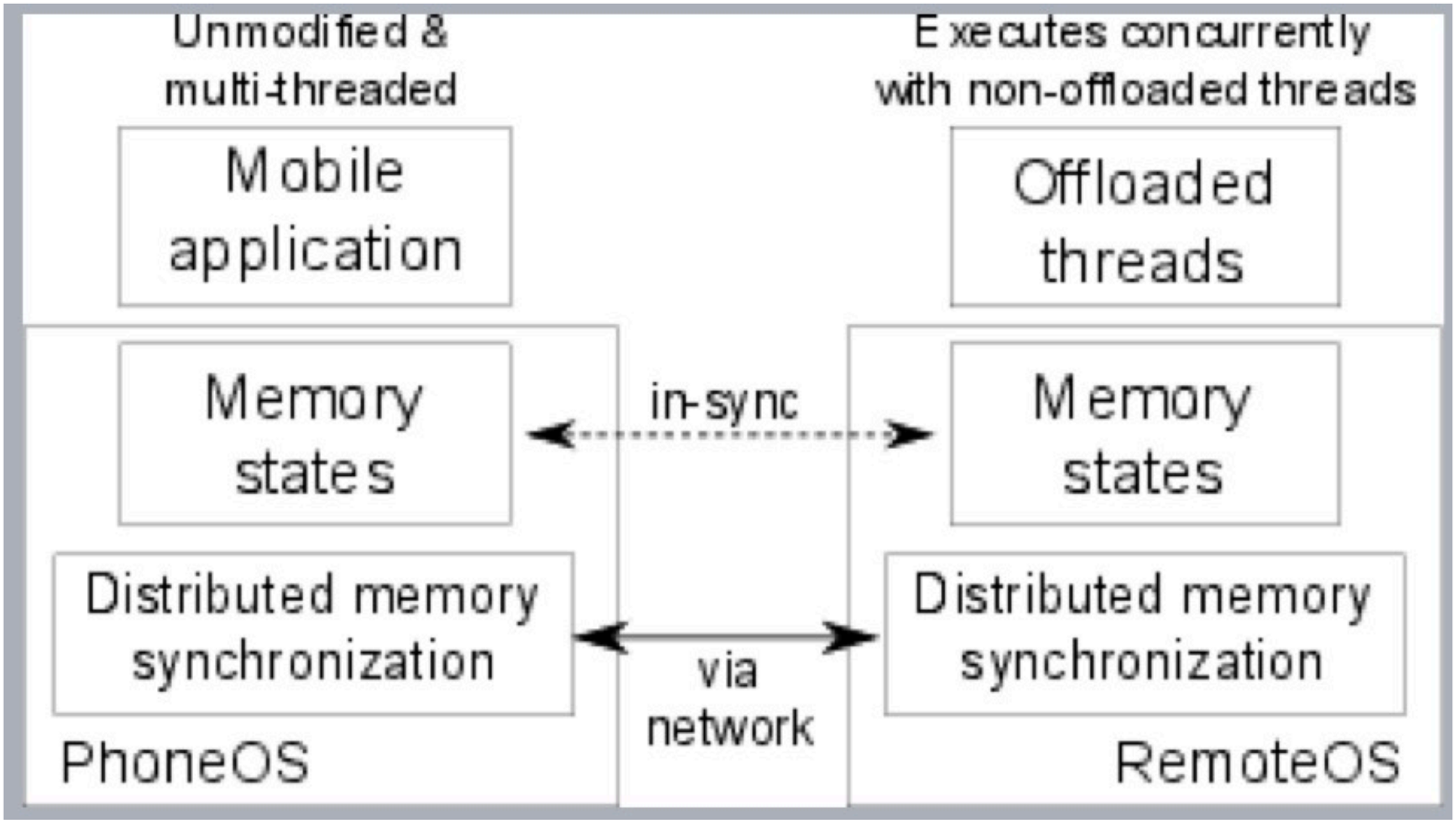
Diaspora


DIASPORA* ALPHA
Find people or #tags
John
John
Stream
Your Aspects
Deselect all
Family
Friends
Work
Acquaintances
+ Add an aspect
@Mentions
#Followed Tags
#computers
#music
#photography
#photoshop
#tech
Add a tag
Stream
recently: commented on · posted
What's on your mind?
John – 3 minutes ago
Testing Diaspora's #image feature. (November 2011 Desktop)
Limited (4) – Like · Comment
John
#question - Can you edit your posts? Quite disappointing if you
People in your Stream
View all contacts
Invite your friends
From Facebook
By email
Connect to Cubbi.es
Cubbi.es is the first Diaspora application under development.
Learn more
Welcome New Users
Follow #NewHere and welcome new users to Diaspora*!
Learn more
Need Help?
Feedback

Work Offloading

- COMET
- CloneCloud
- Maul

COMET: Code Offload by Migrating Execution Transparently



Web Security & Isolation Model

- Currently: Both parties should both agree to communication.
- Previously: Including party should agree to communication.