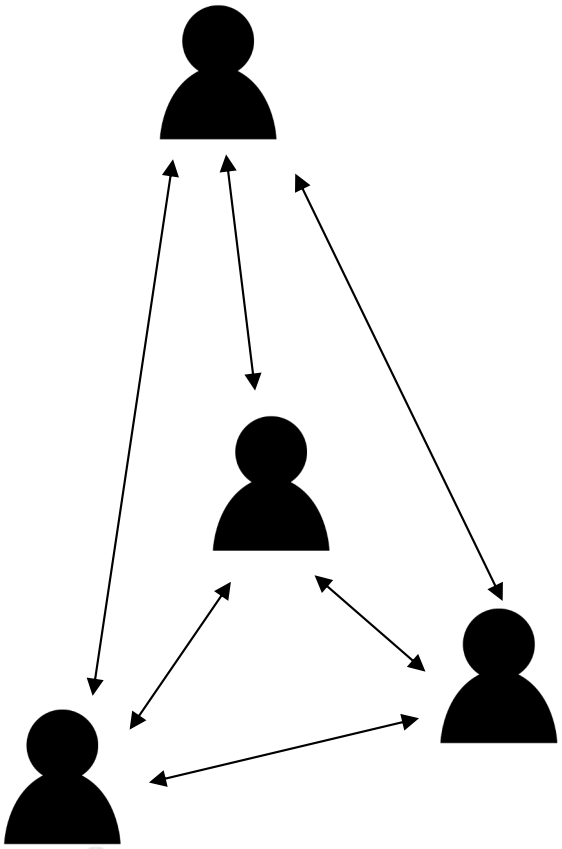
Decentralized and Secure Multimedia Sharing Application over Named Data Networking

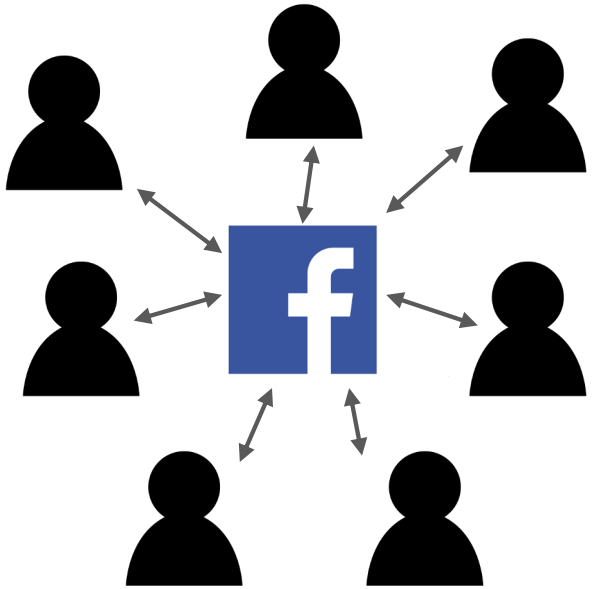
Ashlesh Gawande, Jeremy Clark, Damian Coomes, Lan Wang
University of Memphis
September 25, 2019
ACM ICN 2019
Macau, China



Motivation

- Decentralized social media platform
- Blueprint for other developers
- Popular NDN apps

What's Wrong with Centralization



- Rely on single entity
- What if it disappears?
- Single points of failure
- Censorship
- No idea how data is used

Design

Design Requirements

No central entity

No single user directory

No special infrastructure

No single trust anchor

User control of data

Naming

~~Application controlled namespace:~~ **~~simple to design, but needs central authority~~**
Solution: User owned namespaces

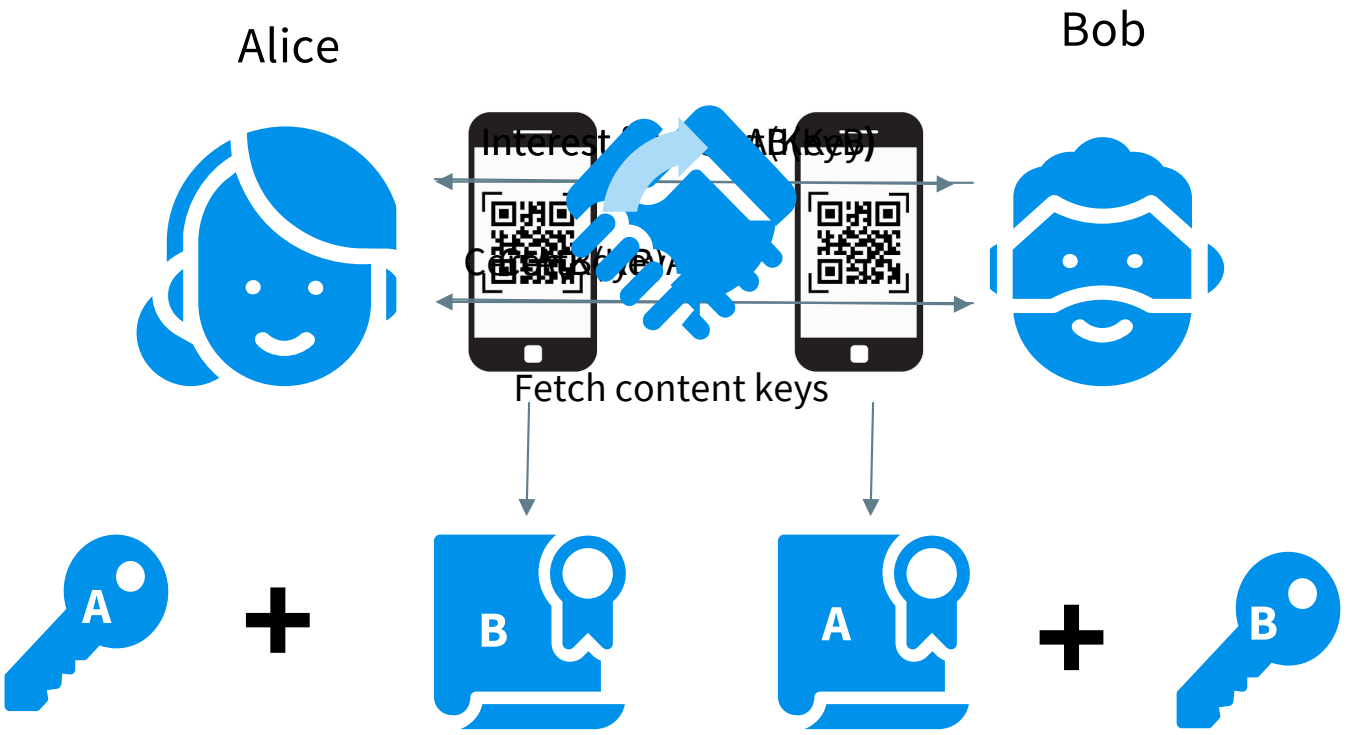
Alice

/net/att/AliceDoe/npChat/
alicedoe123

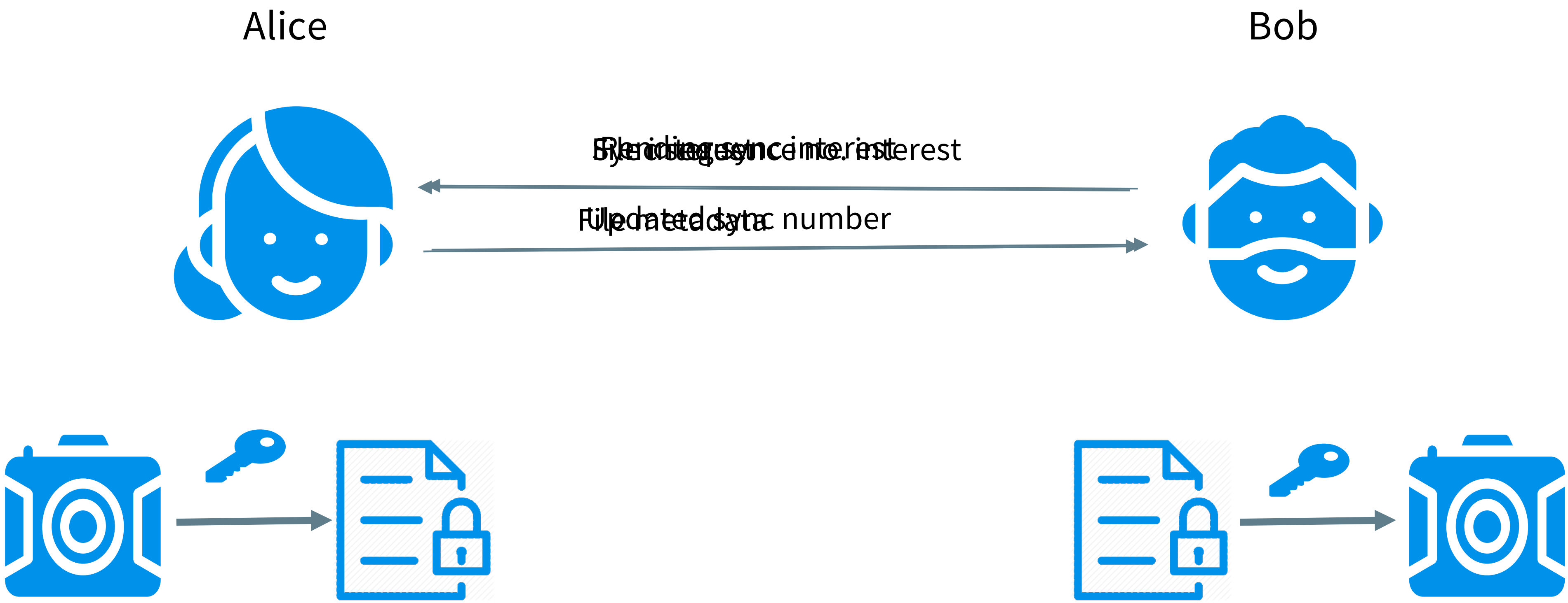
Bob

/edu/memphis/BobSmith/npChat/
bobsmith321

Becoming Friends

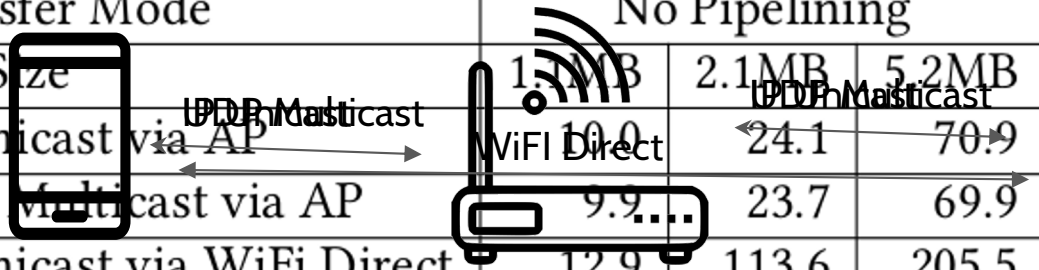


Sharing Content



File Transfer Time in Different Network Environments

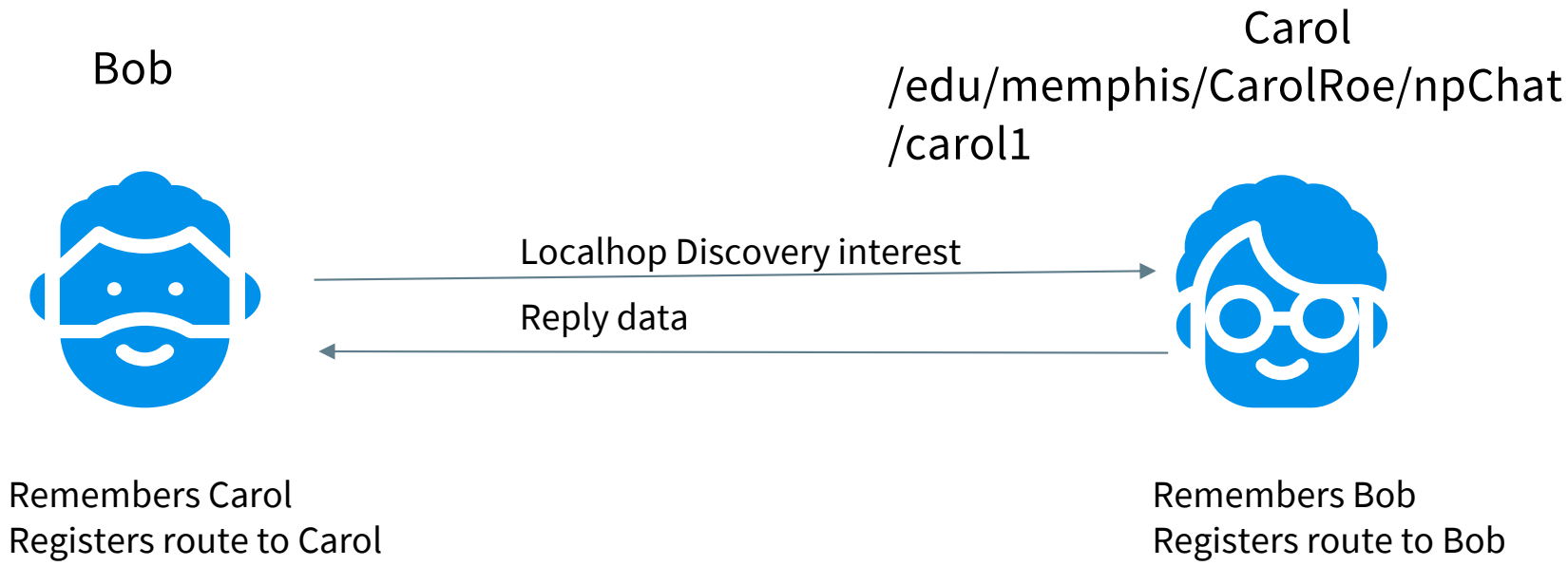
Data Transfer	Transfer Mode	No Pipelining			Pipelining		
	File Size	1.1MB	2.1MB	5.2MB	1.1MB	2.1MB	5.2MB
NDN Face Type	IP Unicast via AP	10.0	24.1	70.9	2.5	4.8	10.8
	UDP Multicast via AP	9.9	23.7	69.9	3.2	4.3	10.1
	IP Unicast via WiFi Direct	12.9	113.6	205.5	3.9	5.3	14.9



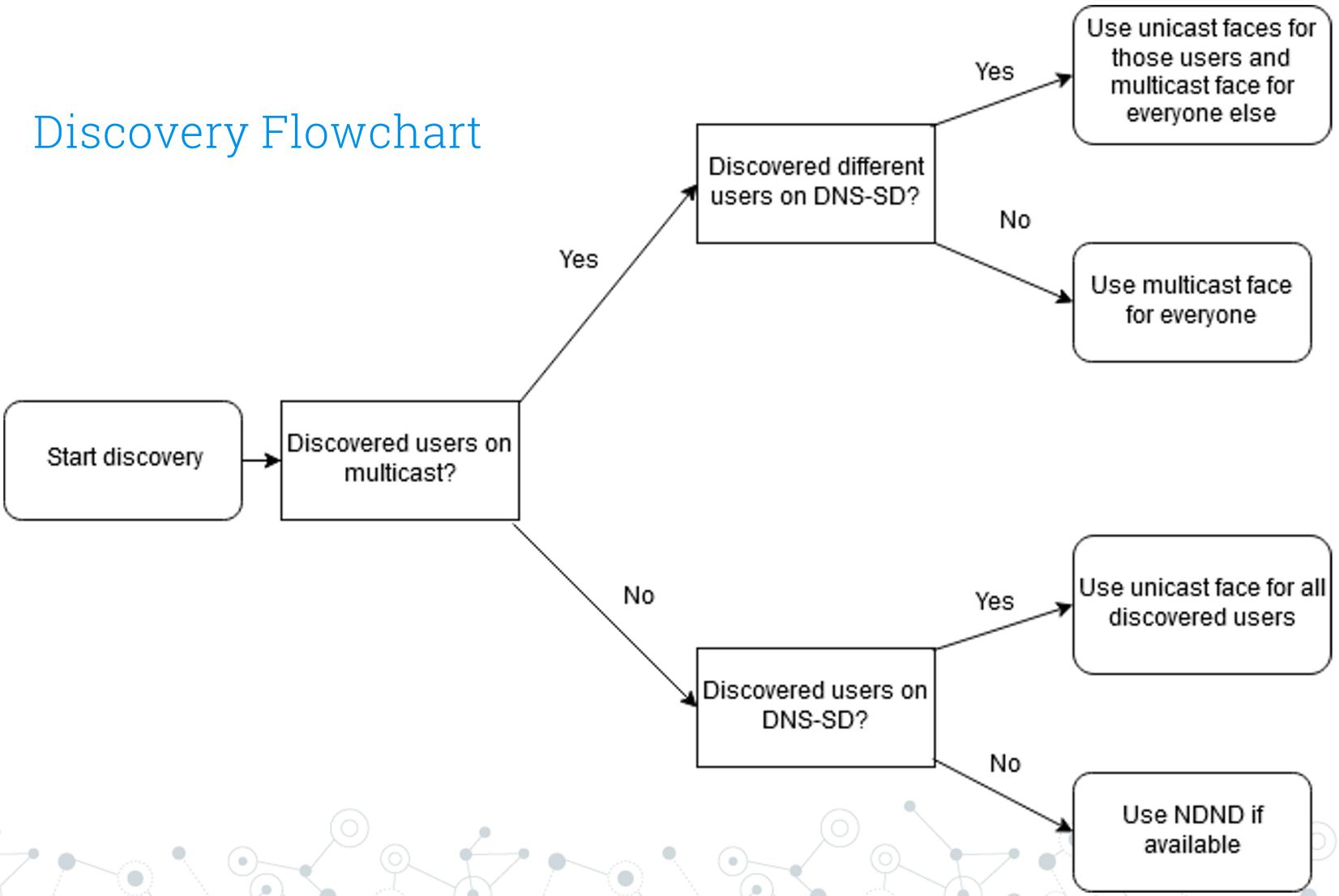
Transfer time (seconds)

- Notably faster over an AP
- Unicast and multicast perform similarly

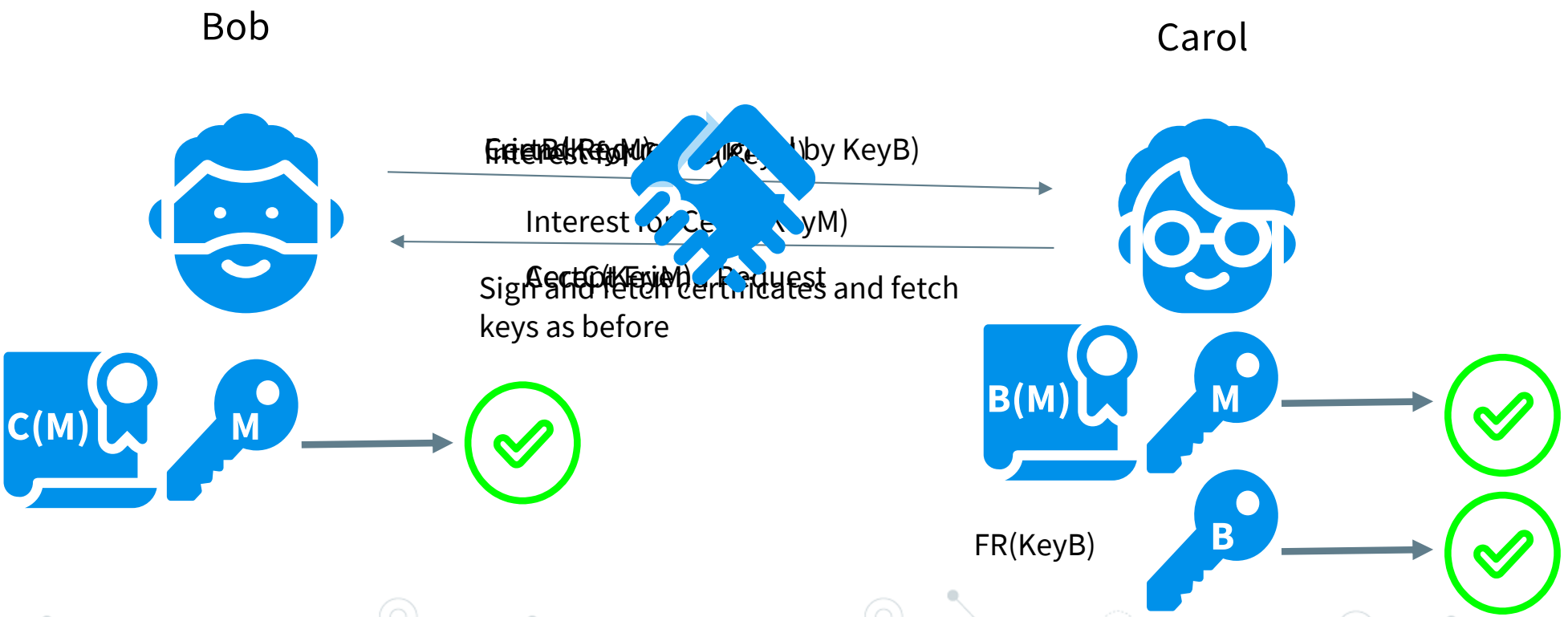
Local User Discovery



Discovery Flowchart

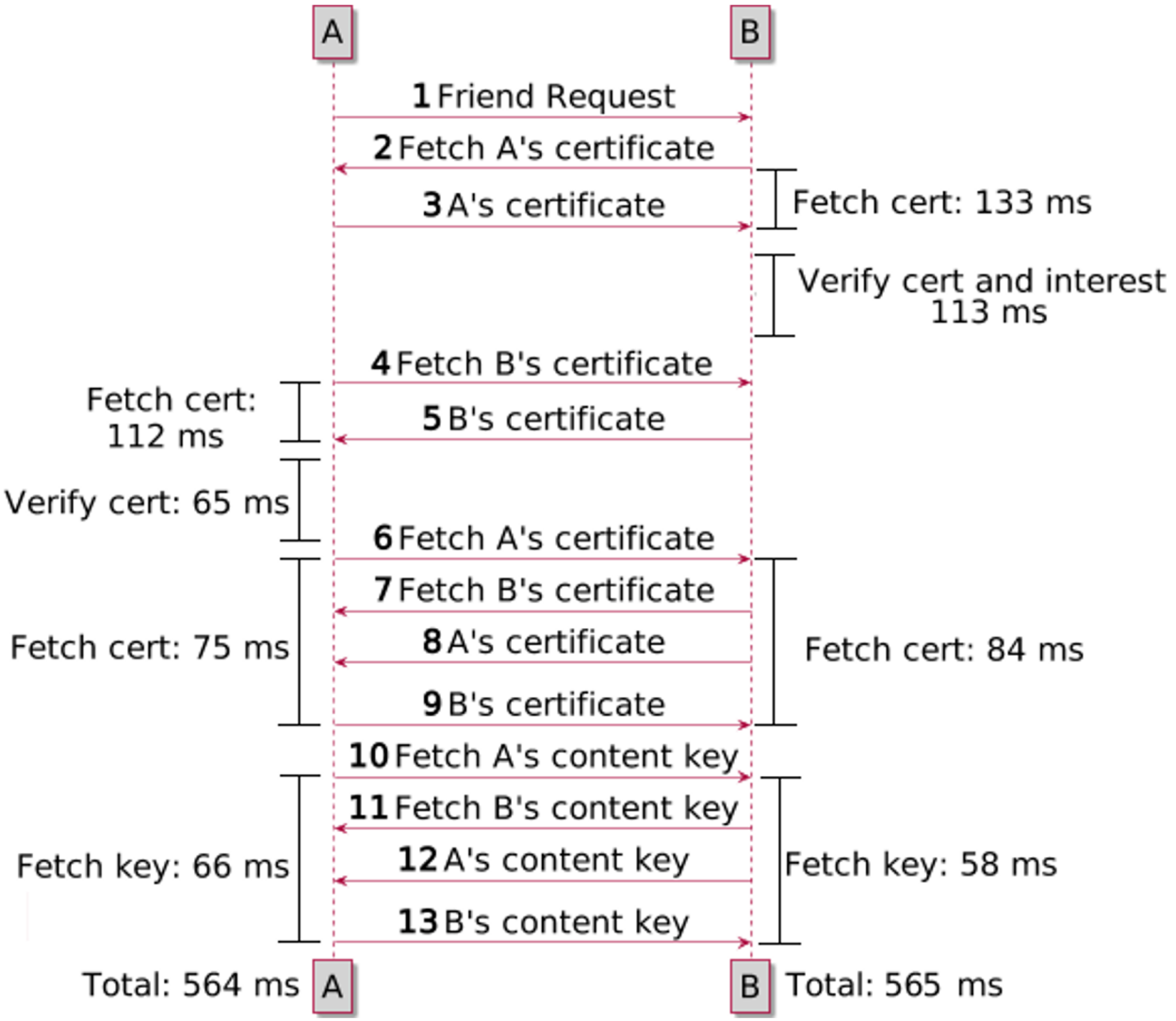


Friend Requests

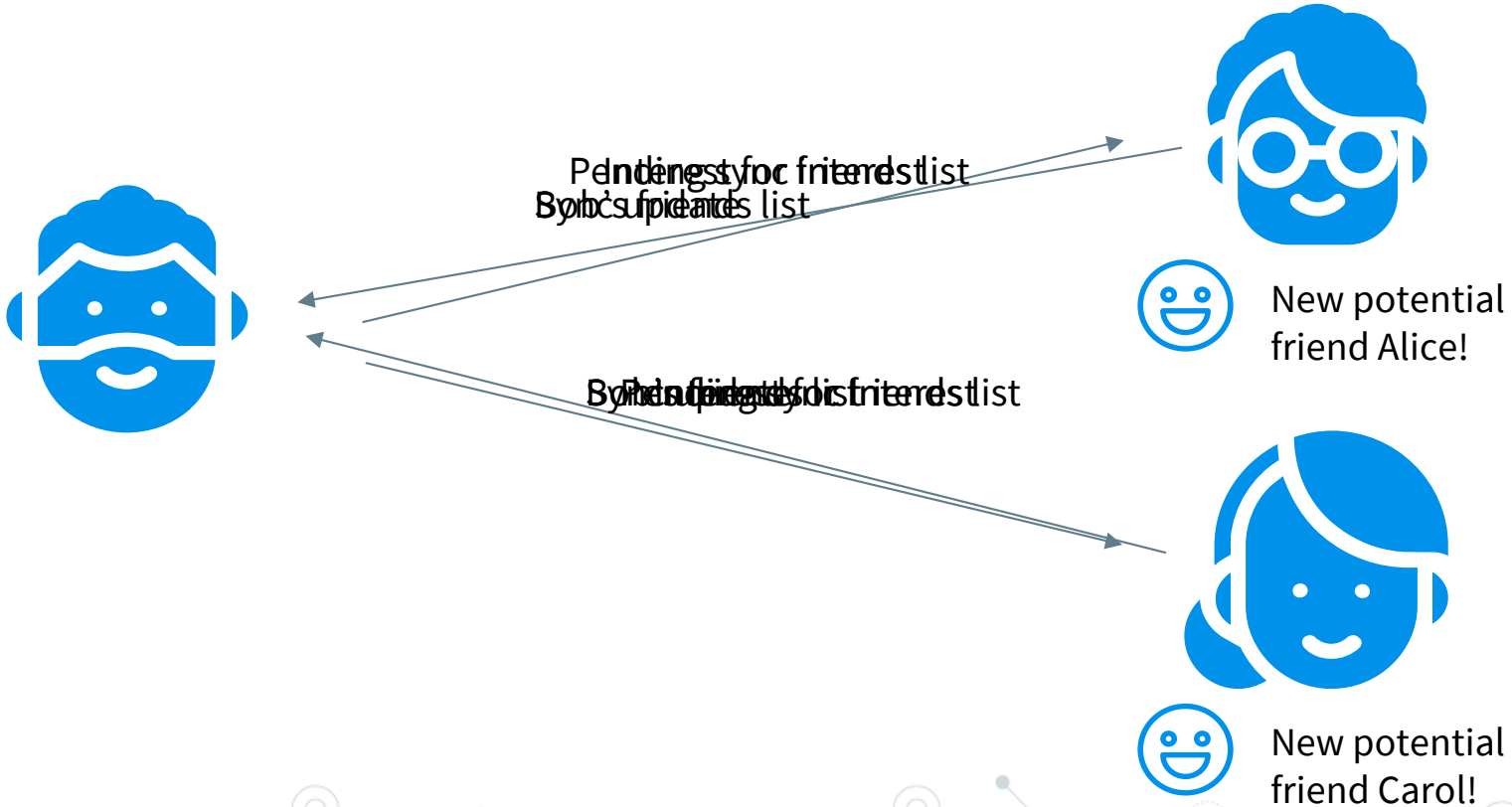


Friend Requests

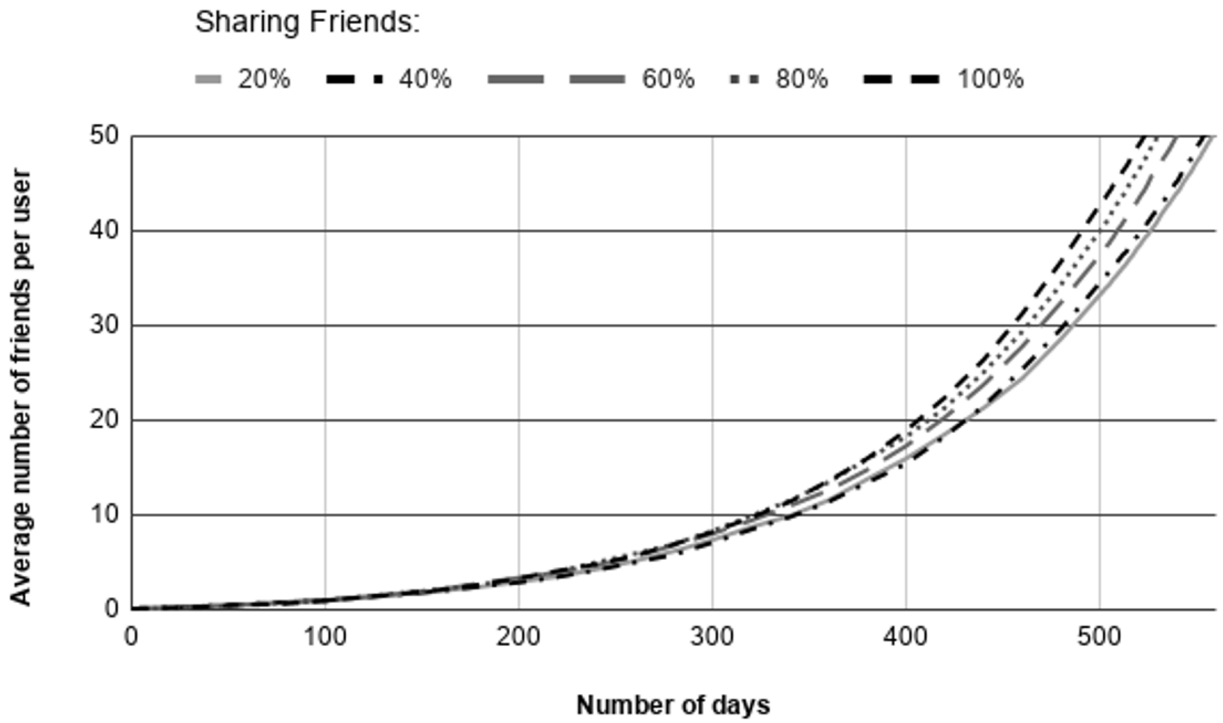
- **Process is fast and finished in a few steps**



Sharing Friends List



Network Growth



- Large number of users discovered even if few people share friends

Friend Requests

Alice

Carol

Same as before, but using their certificates signed by Bob

Trust Model

Meeting in Person

Hierarchical/
Same Organization

Mutual Friends

Trust and Friendship

Trust

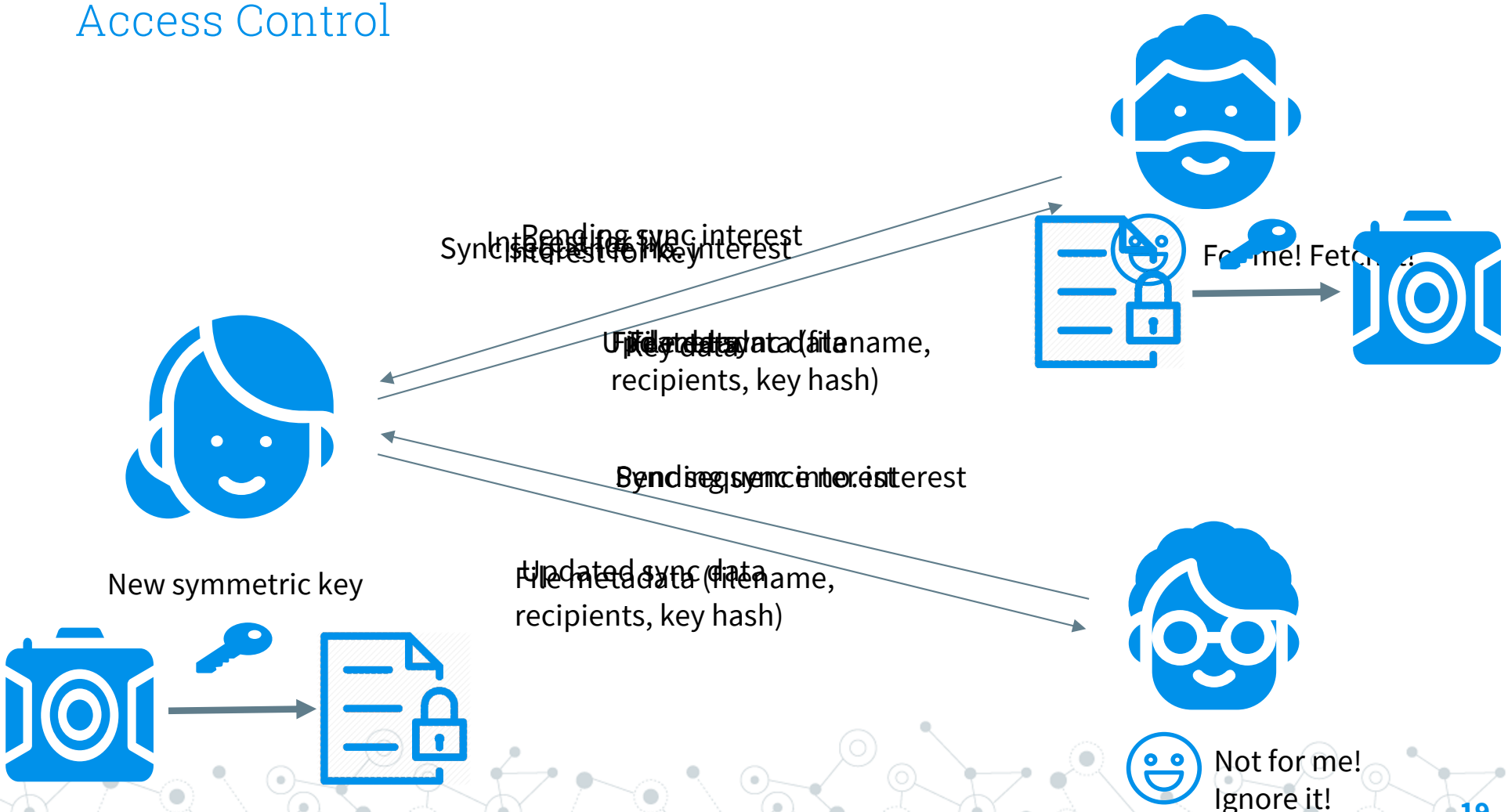
acceptance of some key/data after verification

Friendship

willingness of two users to connect

Friendship is built on trust, but trust does not require friendship.

Access Control



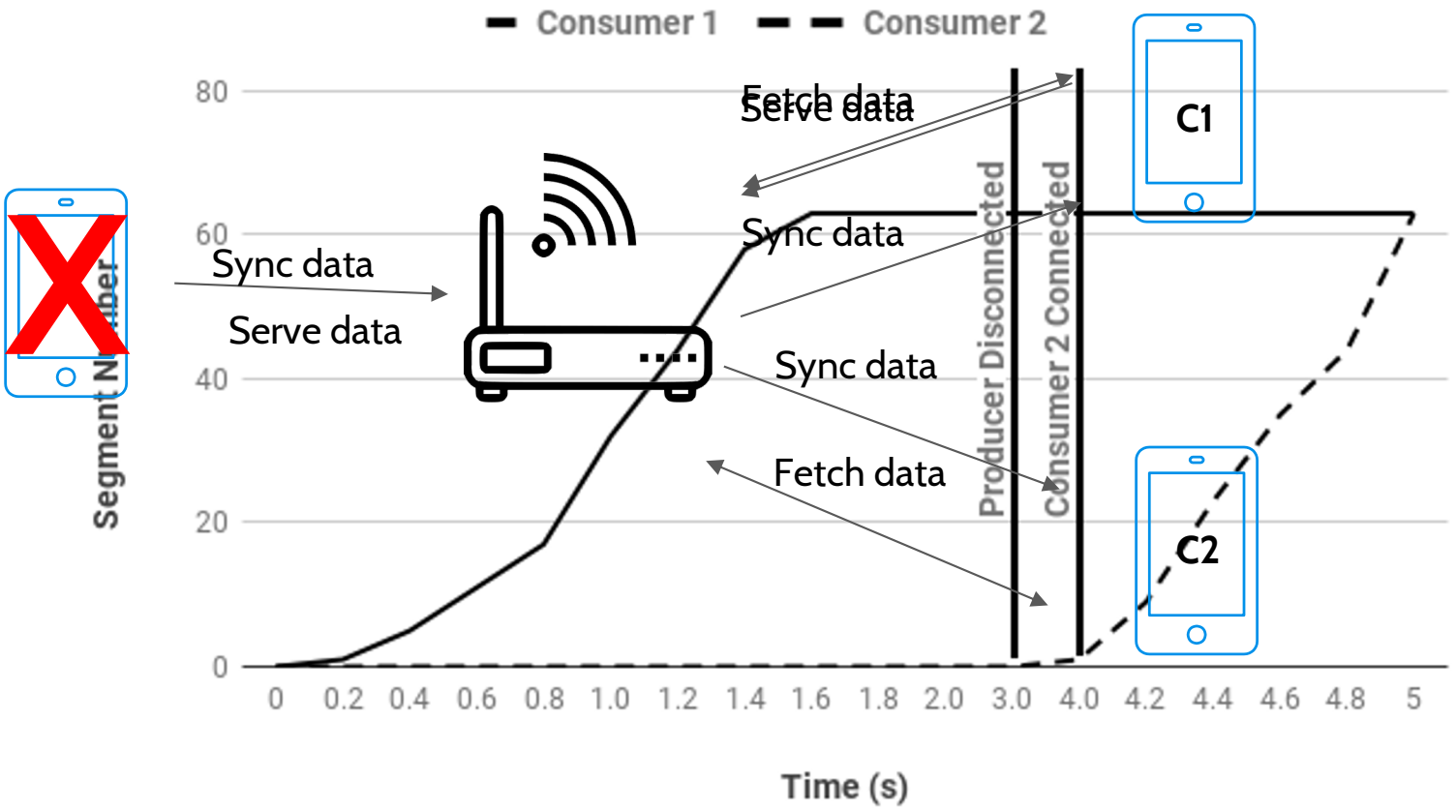
Encryption

	Encryption		Decryption	
	MotoX	Nexus 5X	MotoX	Nexus 5X
1.1MB	54	10	10	4
2.1MB	80	10	12	5
5.2MB	144	11	19	7

Access Control Cost: Data Encryption and Decryption Time (milliseconds) with Different Devices

- **Adds insignificant cost**

Content Store



Related Work: Fediverse

Federated Systems

- Relies on individual servers
- Some apps don’t encrypt server data
- Data pushed to servers; must always be online
- Step in the right direction

Related Work: NDN Apps

- Remove single point-of-failure
- Decentralization not the primary goal
  - Central application prefix
  - Single trust anchor

What We Learned

It’s feasible with right approach

Need the right design

What is Next?

- Better access control
- More complex trust models
- NDN testbed
- Better UI
- App store

Thanks!

Questions?

jrclark2@memphis.edu