KADEMLIA

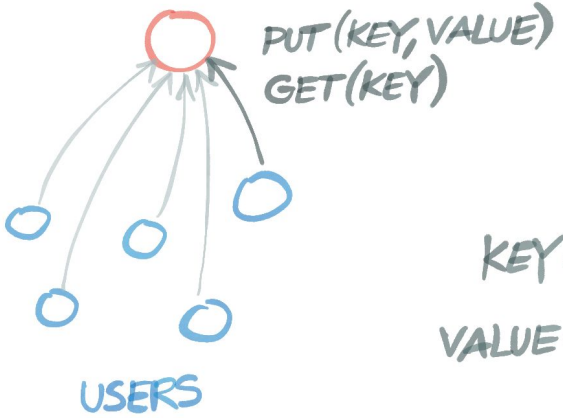
A PEER-TO-PEER DISTRIBUTED HASH TABLE

MAZIERES, MAYMOUNKOV

2001

2000: A MUSIC ODYSSEY

NAPSTER = HASHTABLE

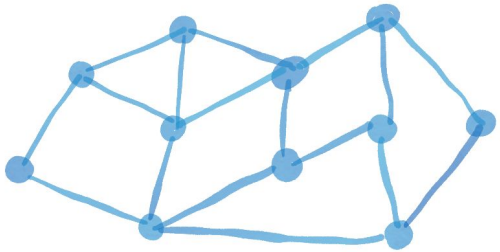


KEY = "MADONNA, LIKE A PRAYER"

VALUE = 212.1.23.78

PROBLEM

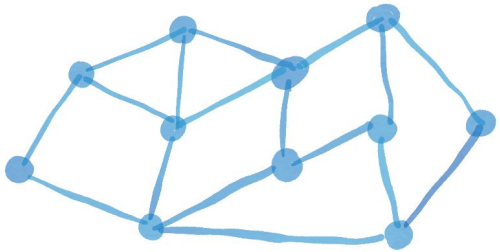
MILLIONS OF ONLINE USERS



RANDOM USER
50% PROBABILITY
OF
STAYING ONLINE
FOR
NEXT HOUR

PROBLEM

MILLIONS OF ONLINE USERS



RANDOM USER
50% PROBABILITY
OF
STAYING ONLINE
FOR
NEXT HOUR

BUILD
DECENTRALIZED
KEY/VALUE STORE?

KADEMLIA

MAZIERES, MAYMOUNKOV '2001

* WIKIPEDIA KADEMLIA

KADEMLIA

MAZIERES, MAYMOUNKOV '2001

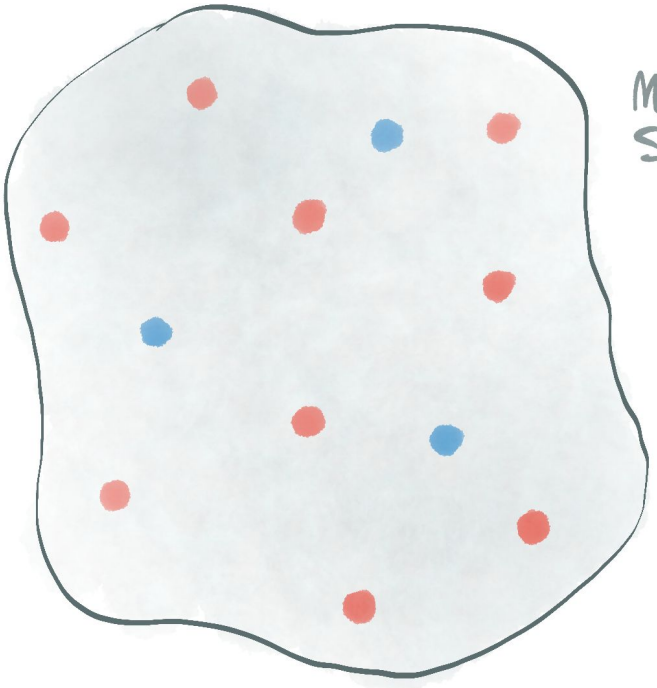
* WIKIPEDIA KADEMLIA
* 3K+ ACADEMIC CITATIONS
* 2 BILLION DOWNLOADS
* TAUGHT IN UNIVERSITIES WORLDWIDE

KADEMLIA

MAZIERES, MAYMOUNKOV '2001

* WIKIPEDIA KADEMLIA
* 3K+ ACADEMIC CITATIONS
* 2 BILLION DOWNLOADS
* TAUGHT IN UNIVERSITIES WORLDWIDE
* FILE-SHARING, BLOCKCHAIN, BOTNETS, WORMS
* NATIONAL SECURITY

SHARDING



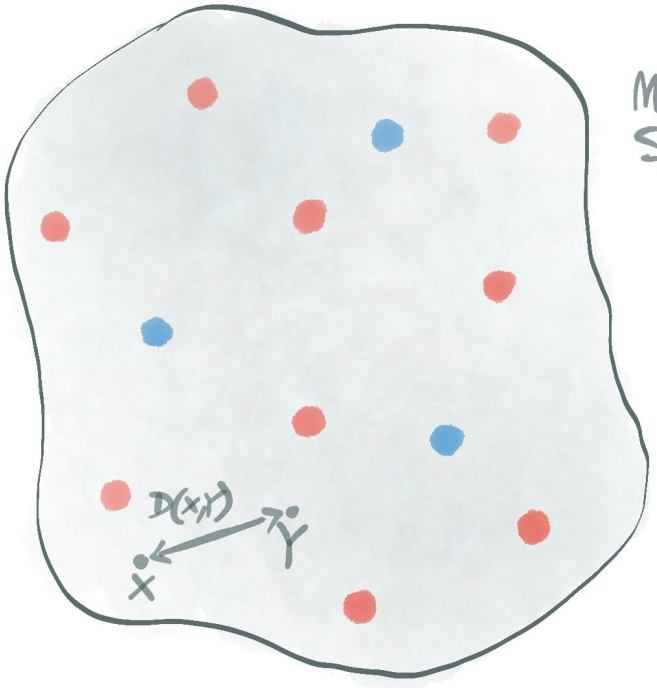
METRIC SPACE

POINT = 160-BIT NUMBER

KEY HASH

USER ID

SHARDING



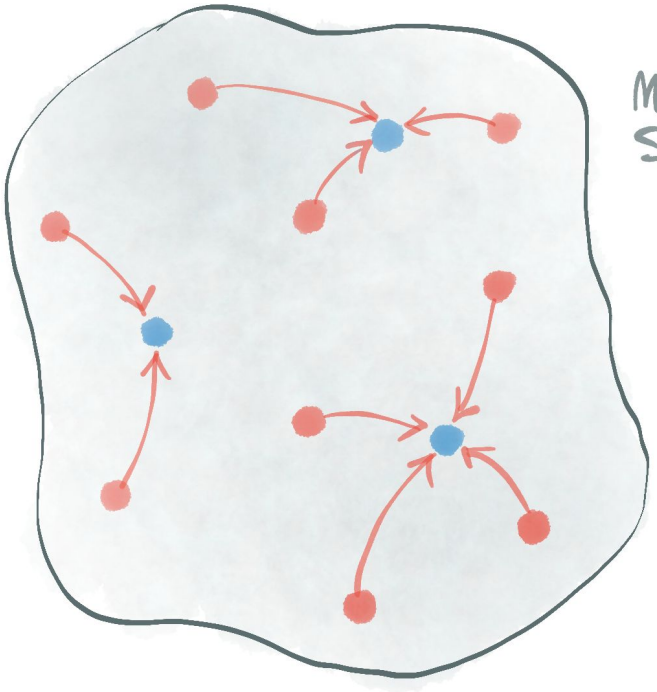
METRIC SPACE

POINT = 160-BIT NUMBER

KEY HASH

USER ID

SHARDING



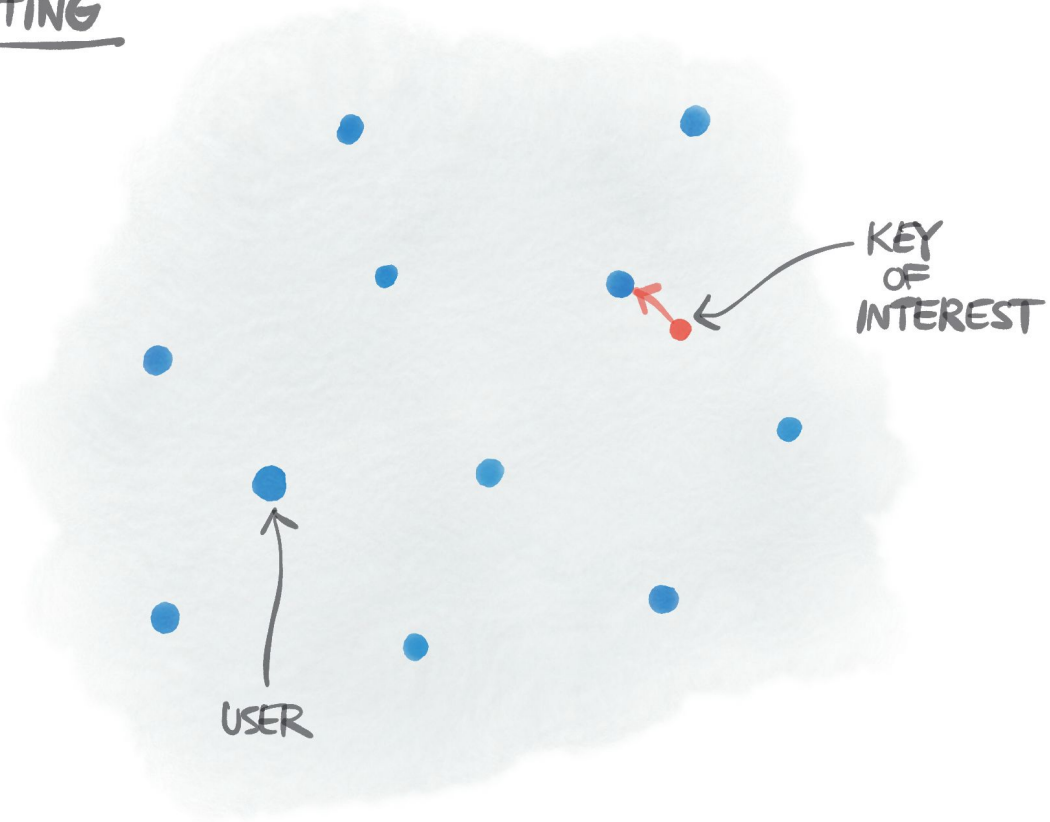
METRIC SPACE

POINT = 160-BIT NUMBER

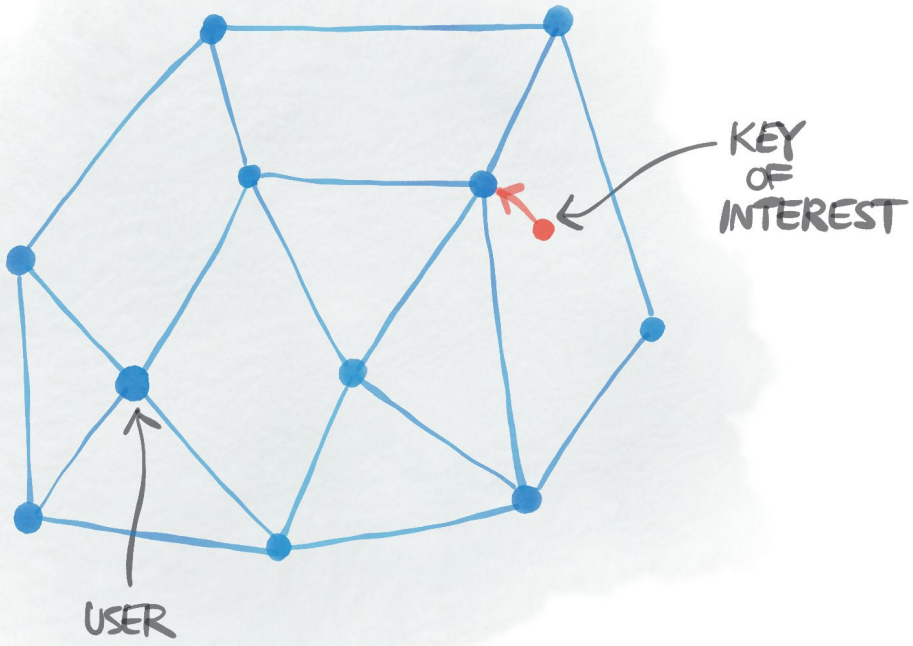
KEY HASH

USER ID

GREEDY ROUTING

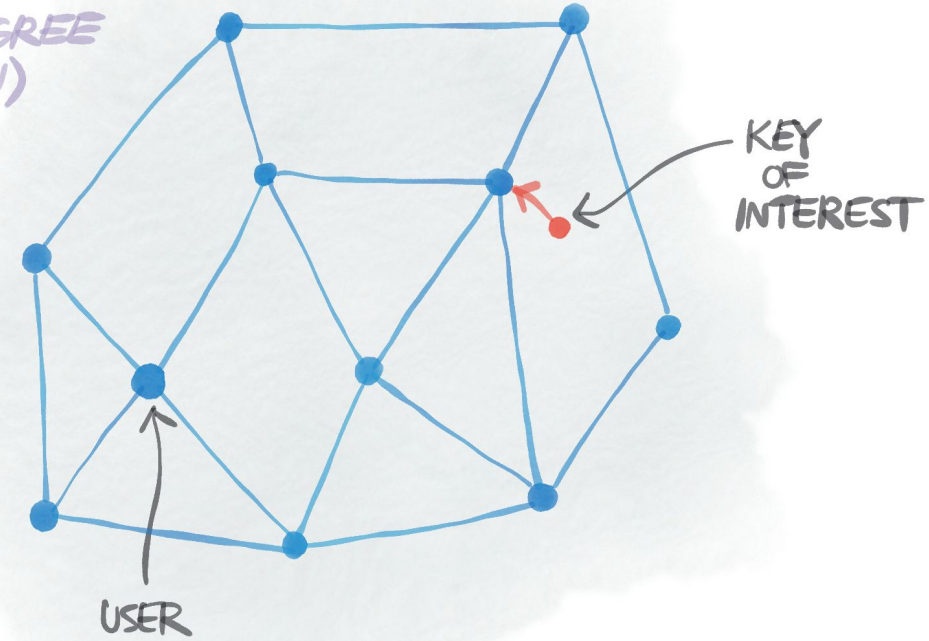


GREEDY ROUTING

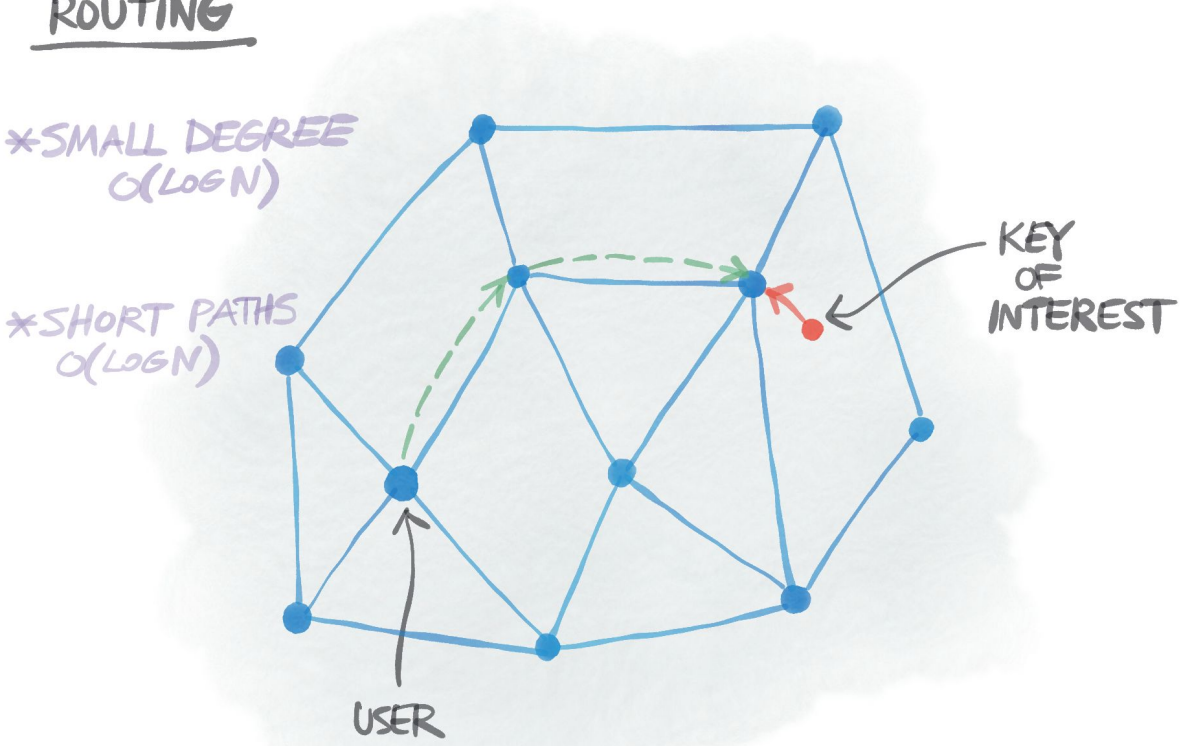


GREEDY ROUTING

*SMALL DEGREE
O(LOG N)



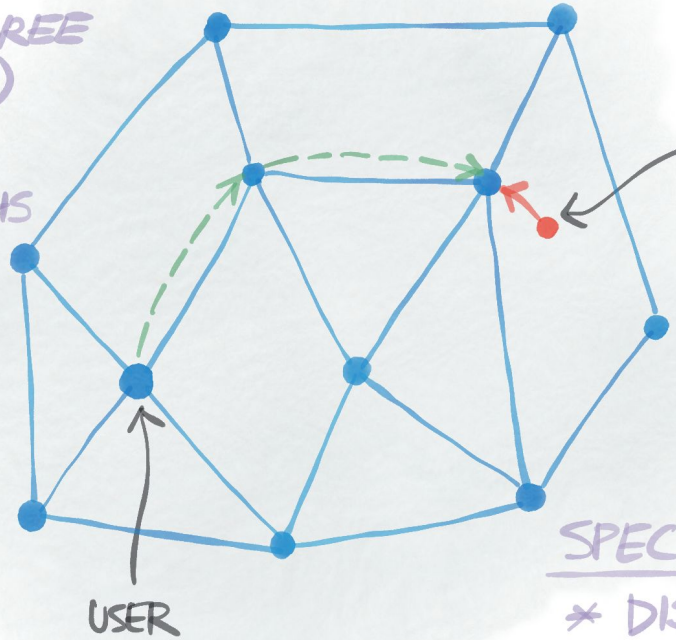
GREEDY ROUTING



GREEDY ROUTING

* SMALL DEGREE $O(\log N)$

* SHORT PATHS $O(\log N)$



SPECIFY:

* DISTANCE METRIC
* USER NEIGHBORS

DISTANCE

$$D(X,Y) = X \oplus Y$$

DISTANCE

$$D(X,Y) = X \oplus Y$$

$$\begin{array}{cccccc} \oplus & X_0 & X_1 & X_2 & X_3 & X_4 \\ & Y_0 & Y_1 & Y_2 & Y_3 & Y_4 \\ \hline & X_0 \oplus Y_0 & X_1 \oplus Y_1 & X_2 \oplus Y_2 & X_3 \oplus Y_3 & X_4 \oplus Y_4 \end{array}$$

DISTANCE

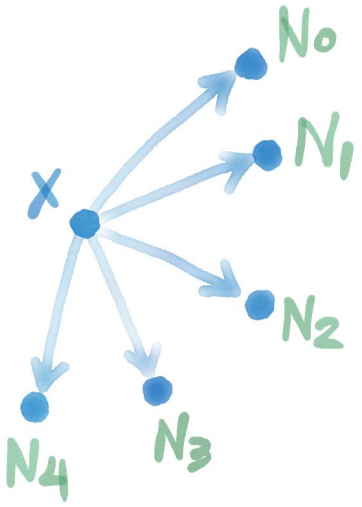
$$D(X,Y) = X \oplus Y$$

$$\begin{array}{ccccc} X_0 & X_1 & X_2 & X_3 & X_4 \\ \oplus\ Y_0 & Y_1 & Y_2 & Y_3 & Y_4 \\ \hline X_0 \oplus Y_0 & X_1 \oplus Y_1 & X_2 \oplus Y_2 & X_3 \oplus Y_3 & X_4 \oplus Y_4 \end{array}$$

$$\begin{array}{ccccc} 0 & 1 & 1 & 0 & 1 \\ \oplus\ 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 \end{array}$$

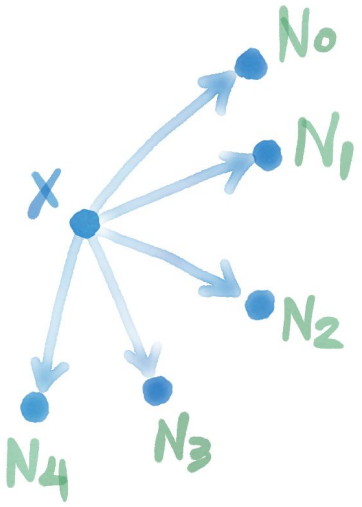
$$+2^4 + 2^3 \qquad +2^0 = 25$$

NEIGHBORS



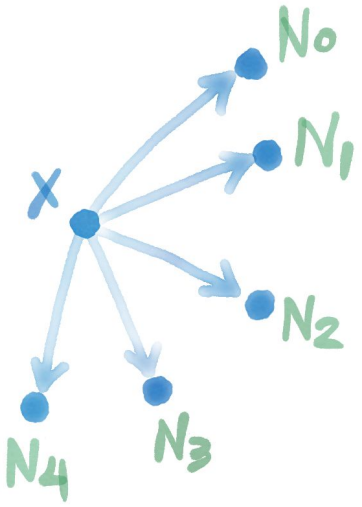
	X_0	X_1	X_2	X_3	X_4
N_0					
N_1					
N_2					
N_3					
N_4					

NEIGHBORS



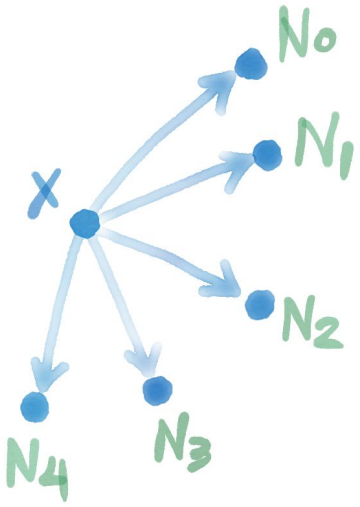
	X_0	X_1	X_2	X_3	X_4
N_0	$\overline{X_0}$	*	*	*	*
N_1					
N_2					
N_3					
N_4					

NEIGHBORS



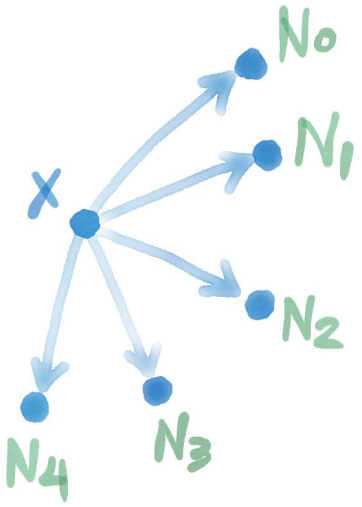
	X_0	X_1	X_2	X_3	X_4
N_0	$\overline{X_0}$	*	*	*	*
N_1	X_0	$\overline{X_1}$	*	*	*
N_2					
N_3					
N_4					

NEIGHBORS



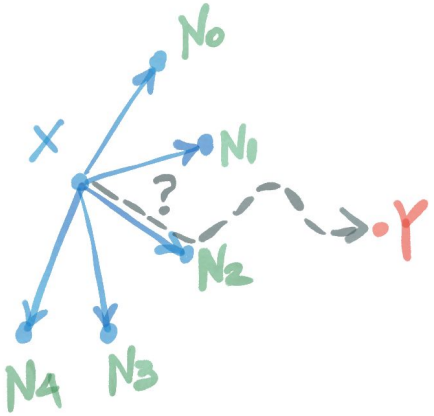
	X_0	X_1	X_2	X_3	X_4
N_0	$\overline{X_0}$	*	*	*	*
N_1	X_0	$\overline{X_1}$	*	*	*
N_2	X_0	X_1	$\overline{X_2}$	*	*
N_3					
N_4					

NEIGHBORS

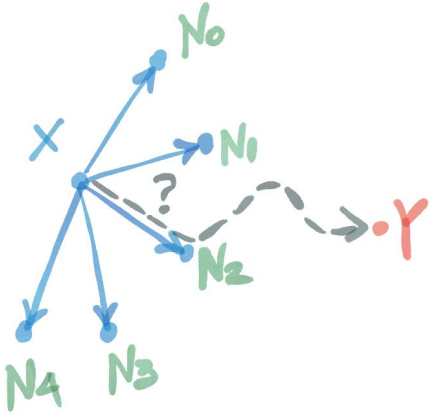


	X_0	X_1	X_2	X_3	X_4
N_0	$\overline{X_0}$	*	*	*	*
N_1	X_0	$\overline{X_1}$	*	*	*
N_2	X_0	X_1	$\overline{X_2}$	*	*
N_3	X_0	X_1	X_2	$\overline{X_3}$	*
N_4	X_0	X_1	X_2	X_3	$\overline{X_4}$

GREEDY FORWARDING



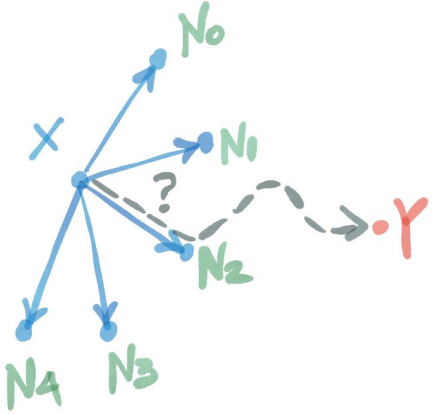
GREEDY FORWARDING



CURRENT X_0 X_1 X_2 X_3 X_4

TARGET Y_0 Y_1 Y_2 Y_3 Y_4

GREEDY FORWARDING

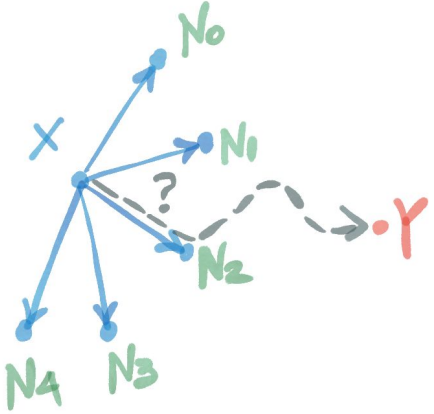


CURRENT X_0 X_1 X_2 X_3 X_4

$=$ $=$ $\neq$

TARGET Y_0 Y_1 Y_2 Y_3 Y_4

GREEDY FORWARDING



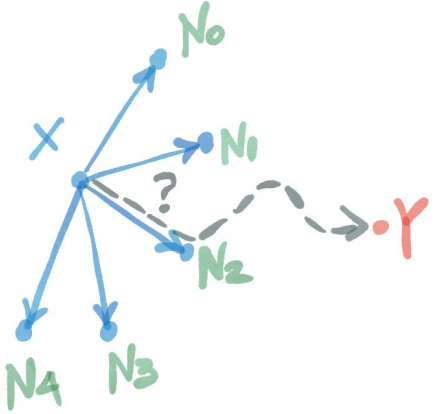
CURRENT X_0 X_1 X_2 X_3 X_4

$=$ $=$ $\neq$

TARGET Y_0 Y_1 Y_2 Y_3 Y_4

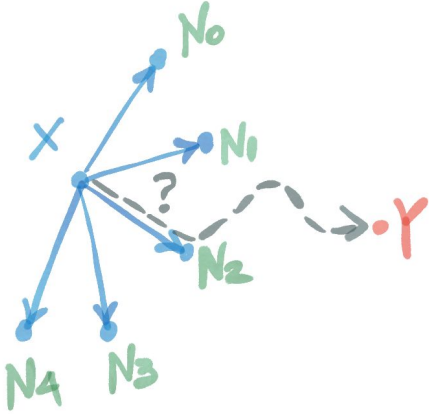
TARGET X_0 X_1 $\overline{X_2}$ Y_3 Y_4

GREEDY FORWARDING



CURRENT	X_0	X_1	X_2	X_3	X_4
	=	=	≠		
TARGET	Y_0	Y_1	Y_2	Y_3	Y_4
TARGET	X_0	X_1	$\overline{X_2}$	Y_3	Y_4
NEIGHBOR	X_0	X_1	$\overline{X_2}$	*	*

GREEDY FORWARDING



CURRENT X_0 X_1 X_2 X_3 X_4

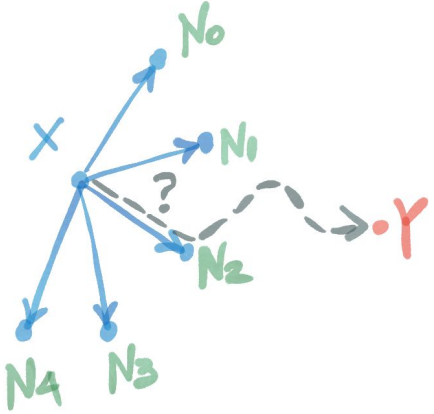
TARGET Y_0 Y_1 Y_2 Y_3 Y_4

TARGET X_0 X_1 $\overline{X_2}$ Y_3 Y_4

NEIGHBOR X_0 X_1 $\overline{X_2}$ * *

Y_0 Y_1 Y_2

GREEDY FORWARDING



CURRENT X_0 X_1 X_2 X_3 X_4

TARGET Y_0 Y_1 Y_2 Y_3 Y_4

TARGET X_0 X_1 $\overline{X_2}$ Y_3 Y_4

NEIGHBOR X_0 X_1 $\overline{X_2}$ * *

Y_0 Y_1 Y_2

REMAINING DETAILS

FAULT TOLERANCE

REMAINING DETAILS

FAULT TOLERANCE

- OF KEY/VALUE STORAGE
  - STORE KEY/VALUE AT CLOSEST R USERS TO KEY

REMAINING DETAILS

FAULT TOLERANCE

- OF KEY/VALUE STORAGE
  - STORE KEY/VALUE AT CLOSEST R USERS TO KEY
- OF ROUTING CONNECTIVITY
  - MAINTAIN Q NEIGHBORS IN EACH ROUTING BUCKET $X_1 X_2 \overline{X_3} **$

REMAINING DETAILS

FAULT TOLERANCE

- OF KEY/VALUE STORAGE
  - STORE KEY/VALUE AT CLOSEST R USERS TO KEY
- OF ROUTING CONNECTIVITY
  - MAINTAIN Q NEIGHBORS IN EACH ROUTING BUCKET $X_1X_2\overline{X}_3**$

BOOTSTRAP ROUTING

- LOOKUP RANDOM $X_1X_2\overline{X}_3**$ TO POPULATE ROUTING BUCKETS