Footprint Scheduling

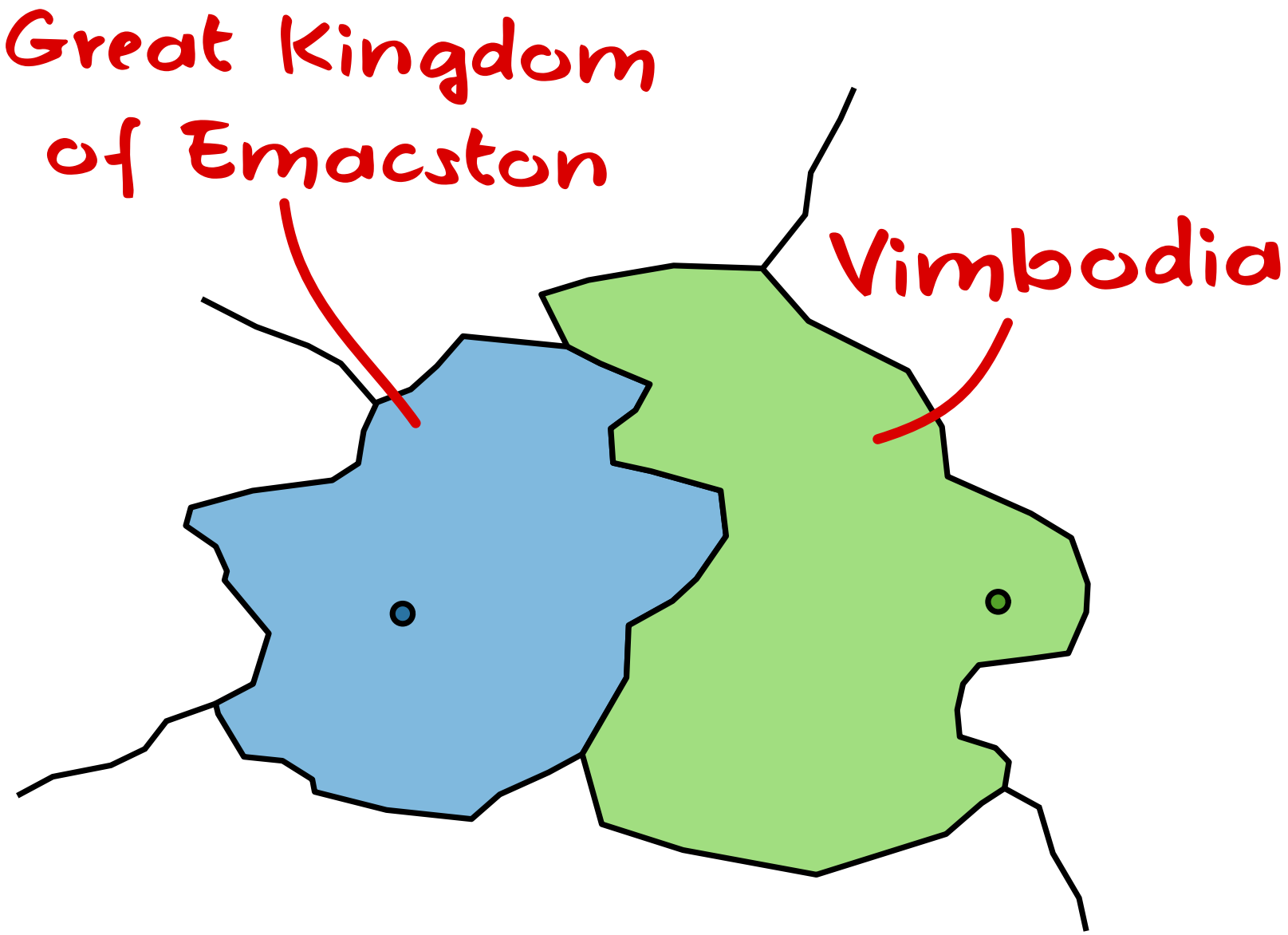
for dining-cryptographer networks

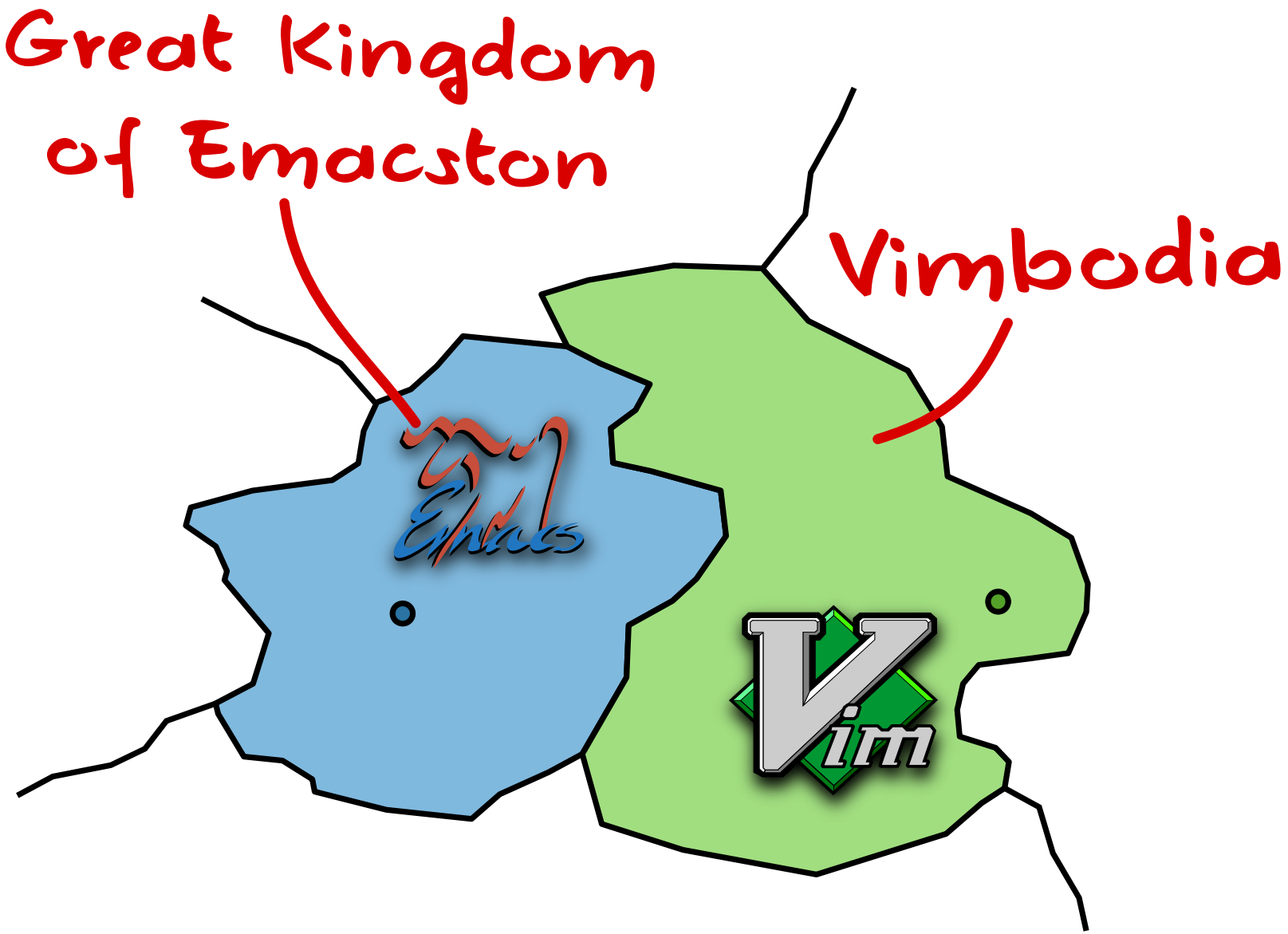
Radboud Universiteit Nijmegen

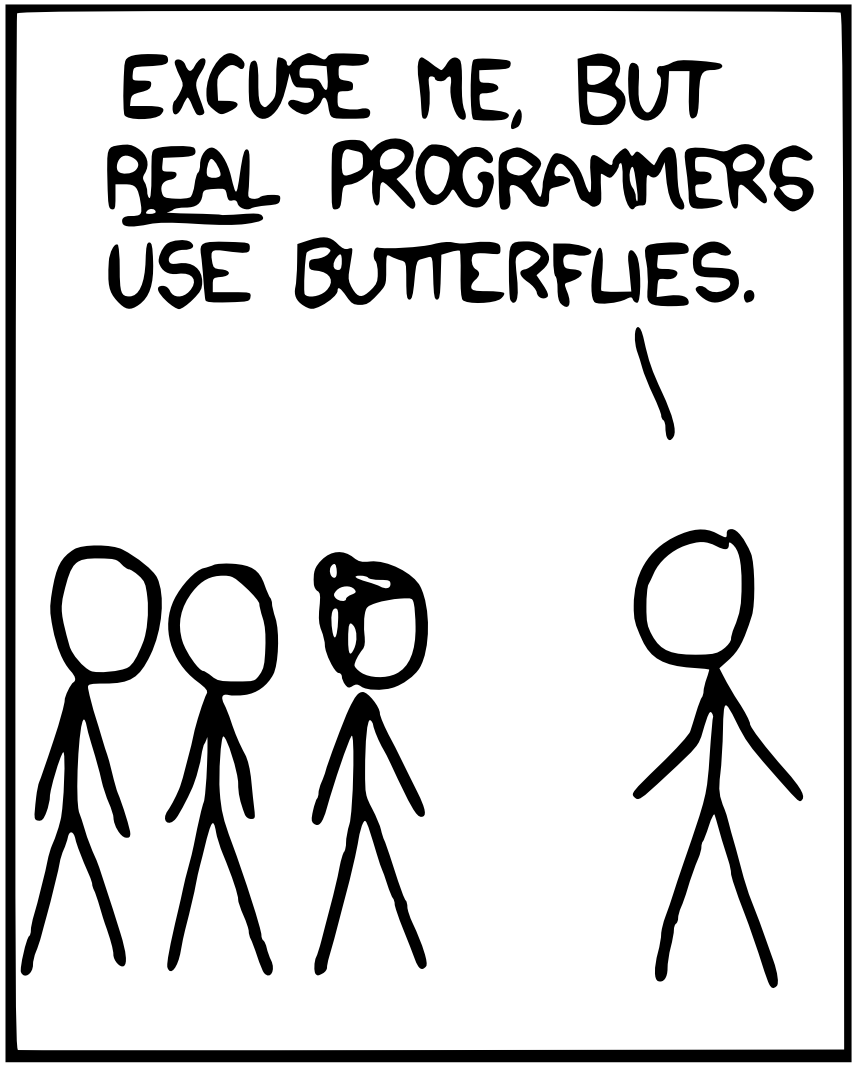
Peter Schwabe
peter@cryptojedi.org

Moritz Neikes
moritz@post-apocalyptic-crypto.org

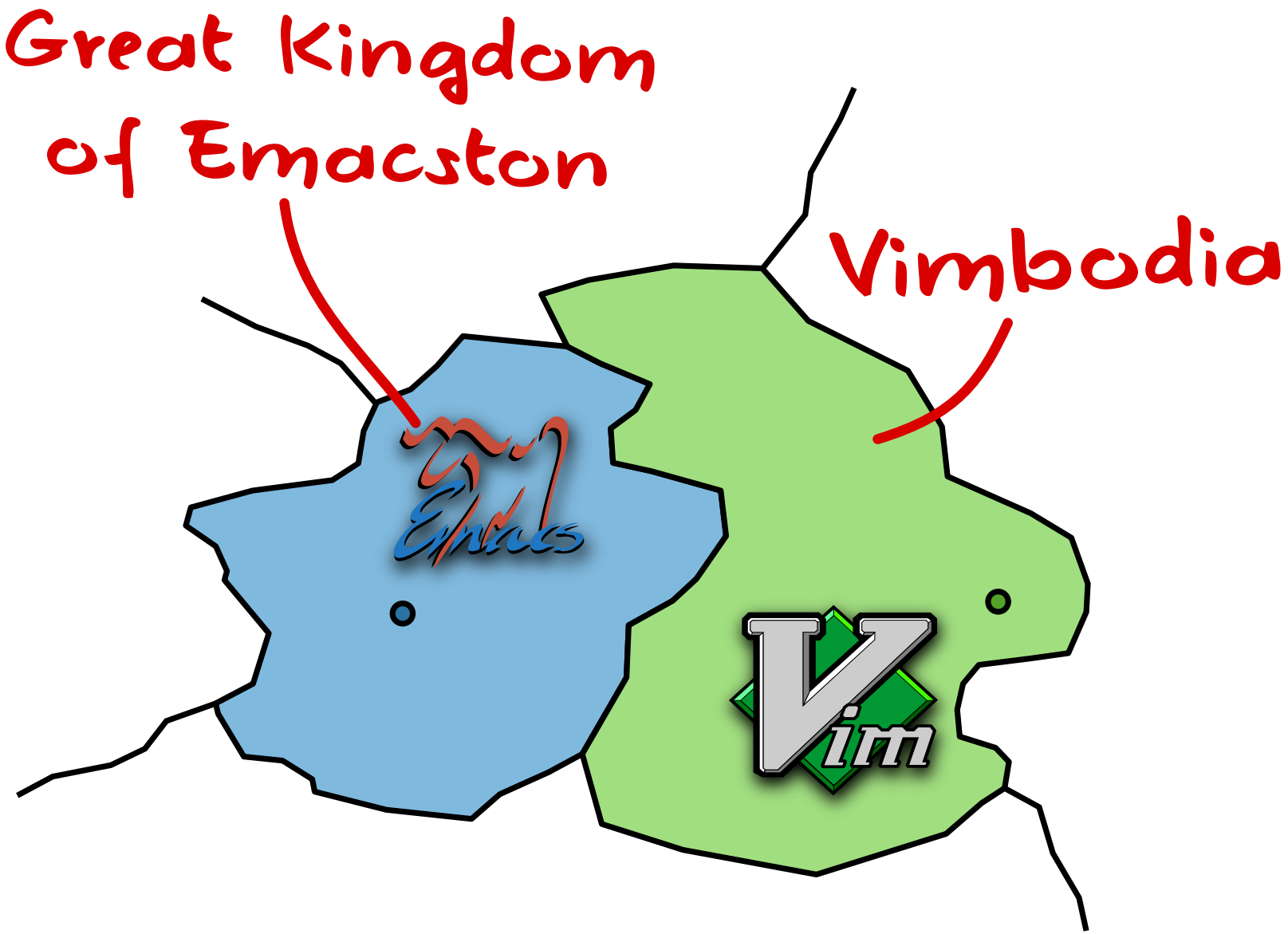
Anna Krasnova
anna@mechanical-mind.org

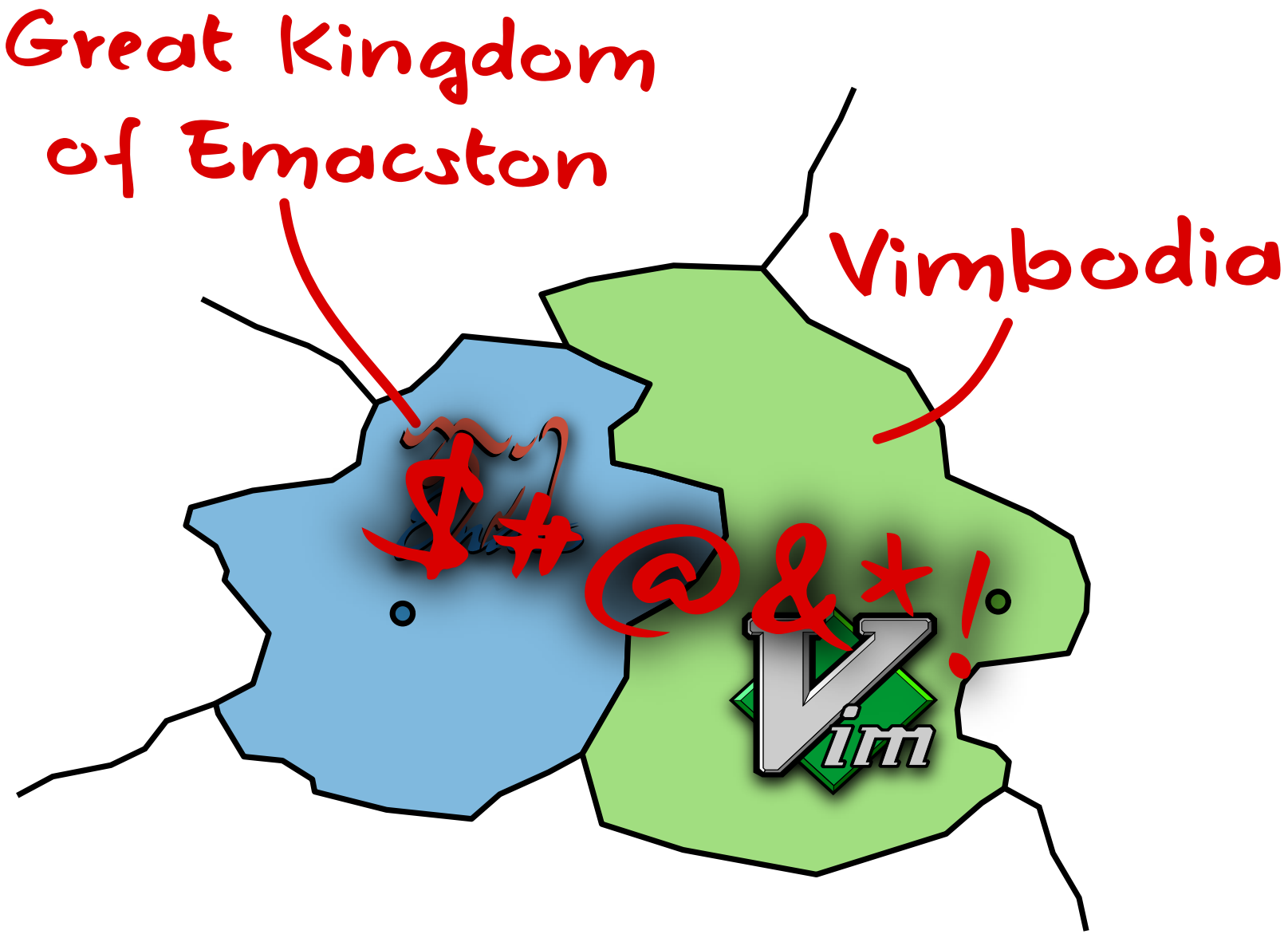

Great Kingdom
of Emacston
Vimbodia


Great Kingdom
of Emacston
Vimbodia



https://xkcd.com/378/


Great Kingdom
of Emacston
Vimbodia
Emacs
Vim


Great Kingdom
of Emacston
Vimbodia
$#@&*!
Vim

Problem

Anonymous communication

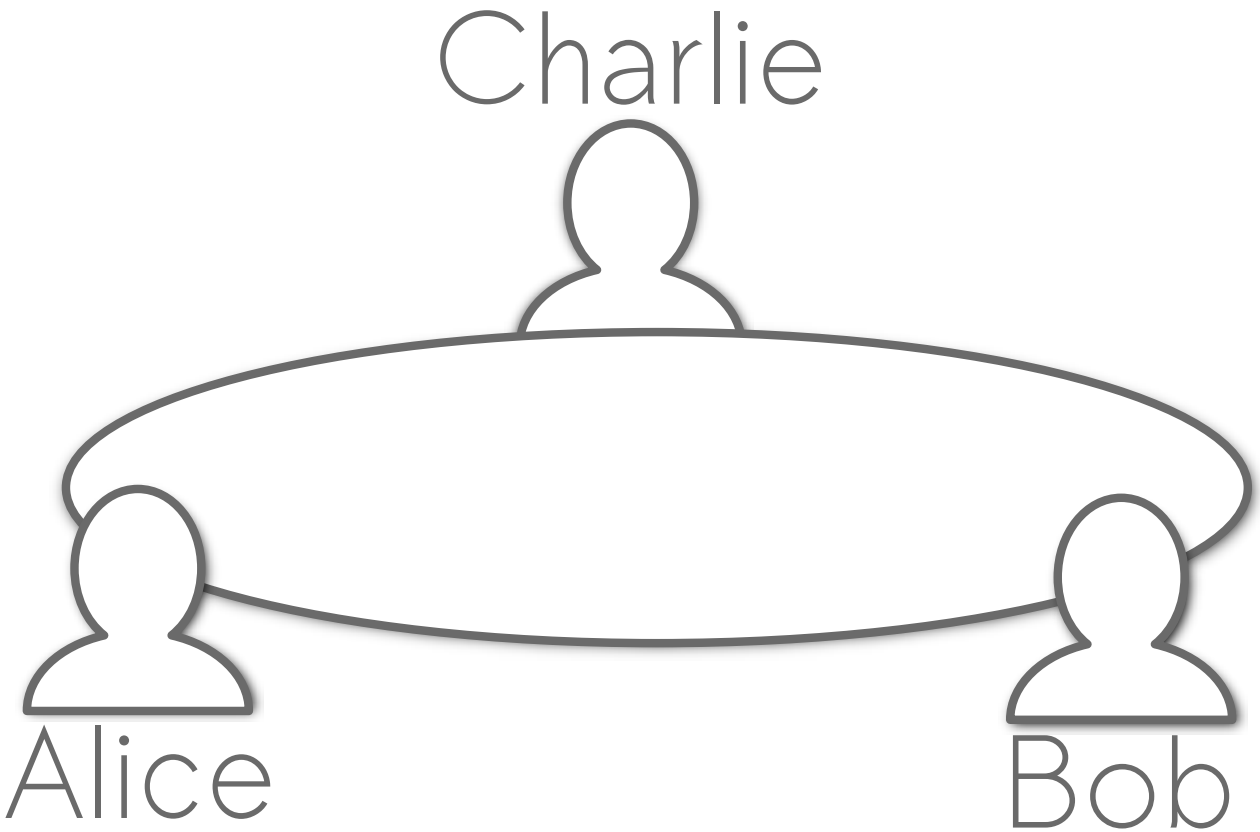
- even against very strong adversaries

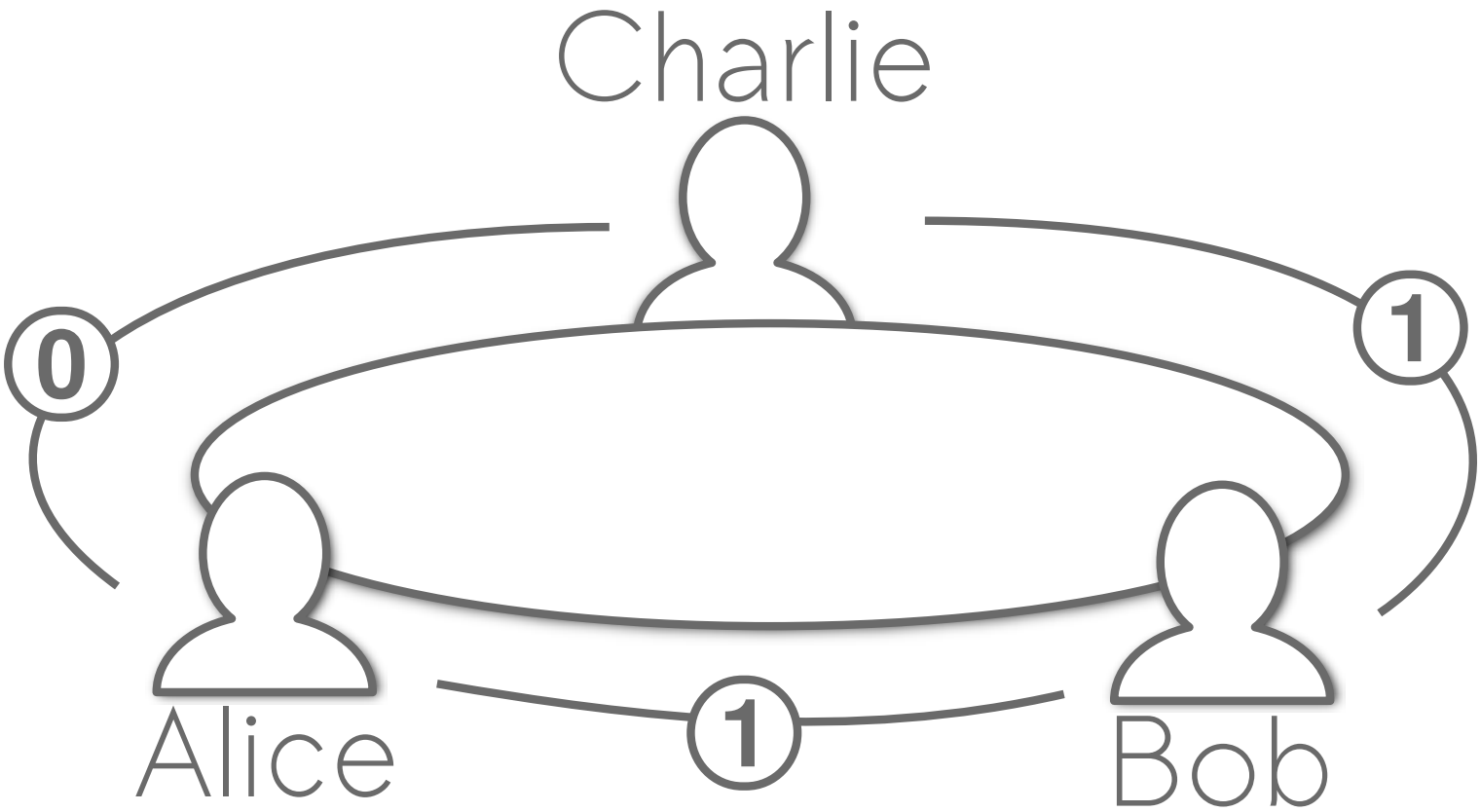
Many users

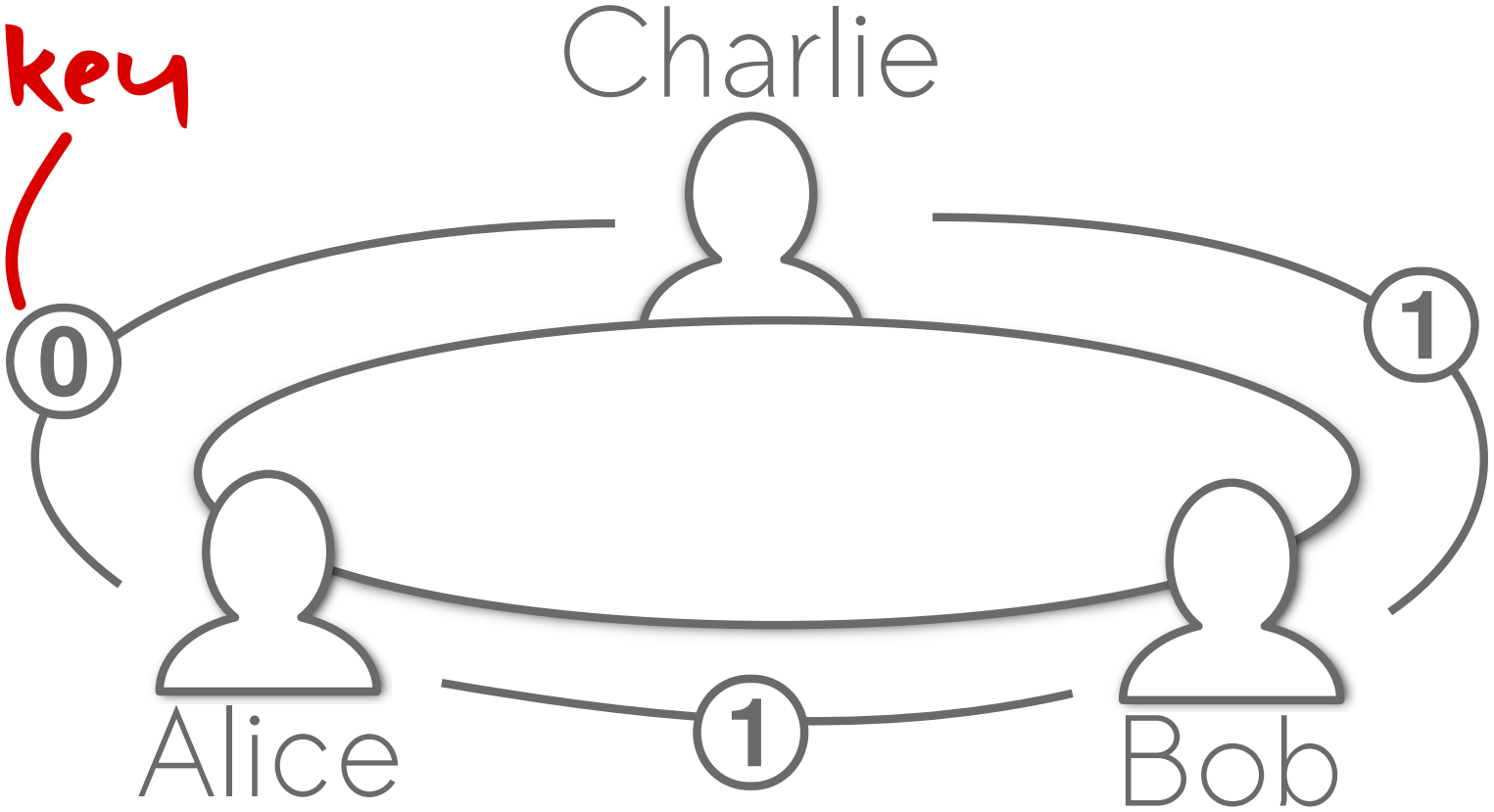
Unstable connections

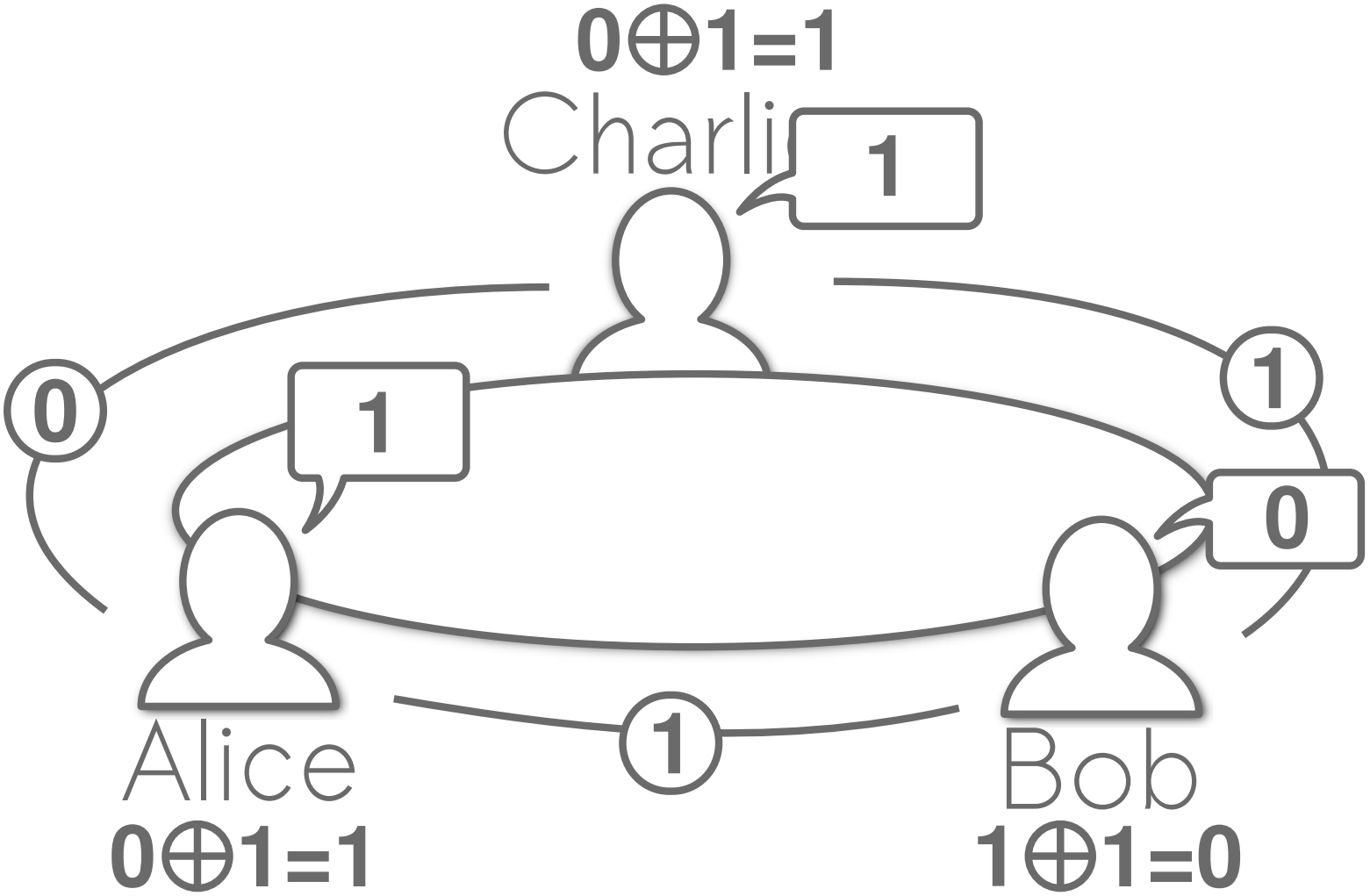
DC networks

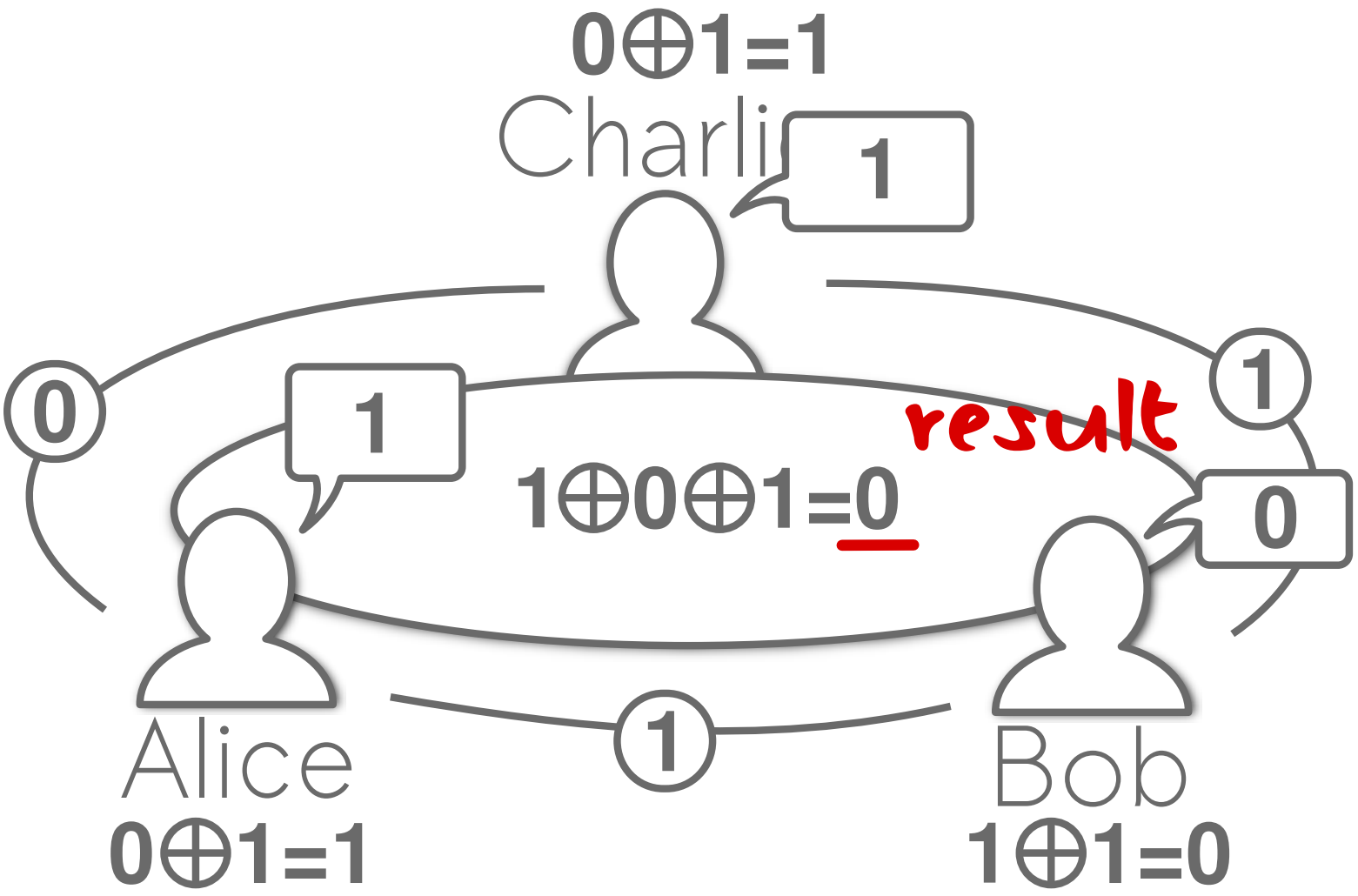
(Chaum, 1988)

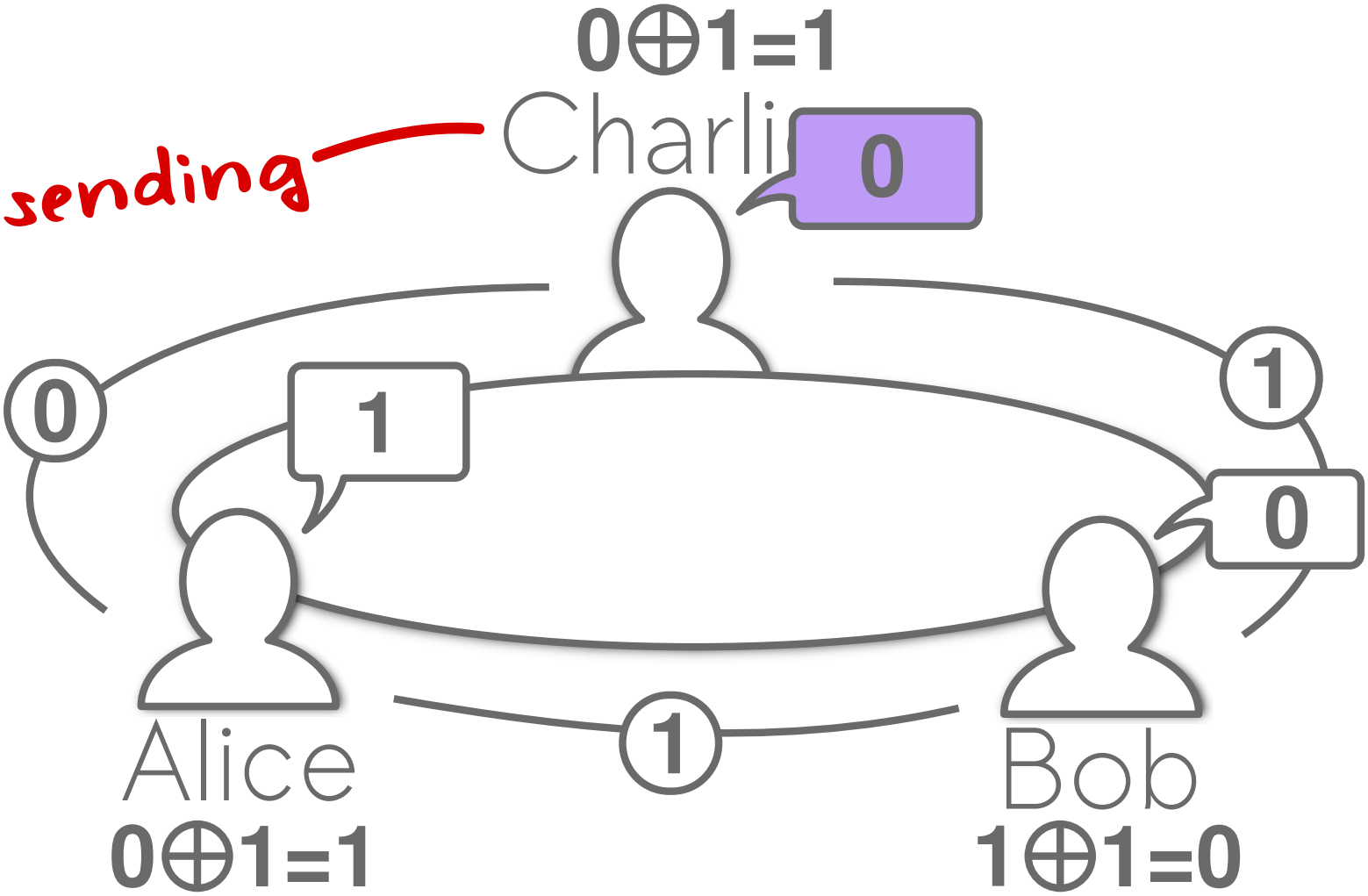

Charlie
Alice
Bob

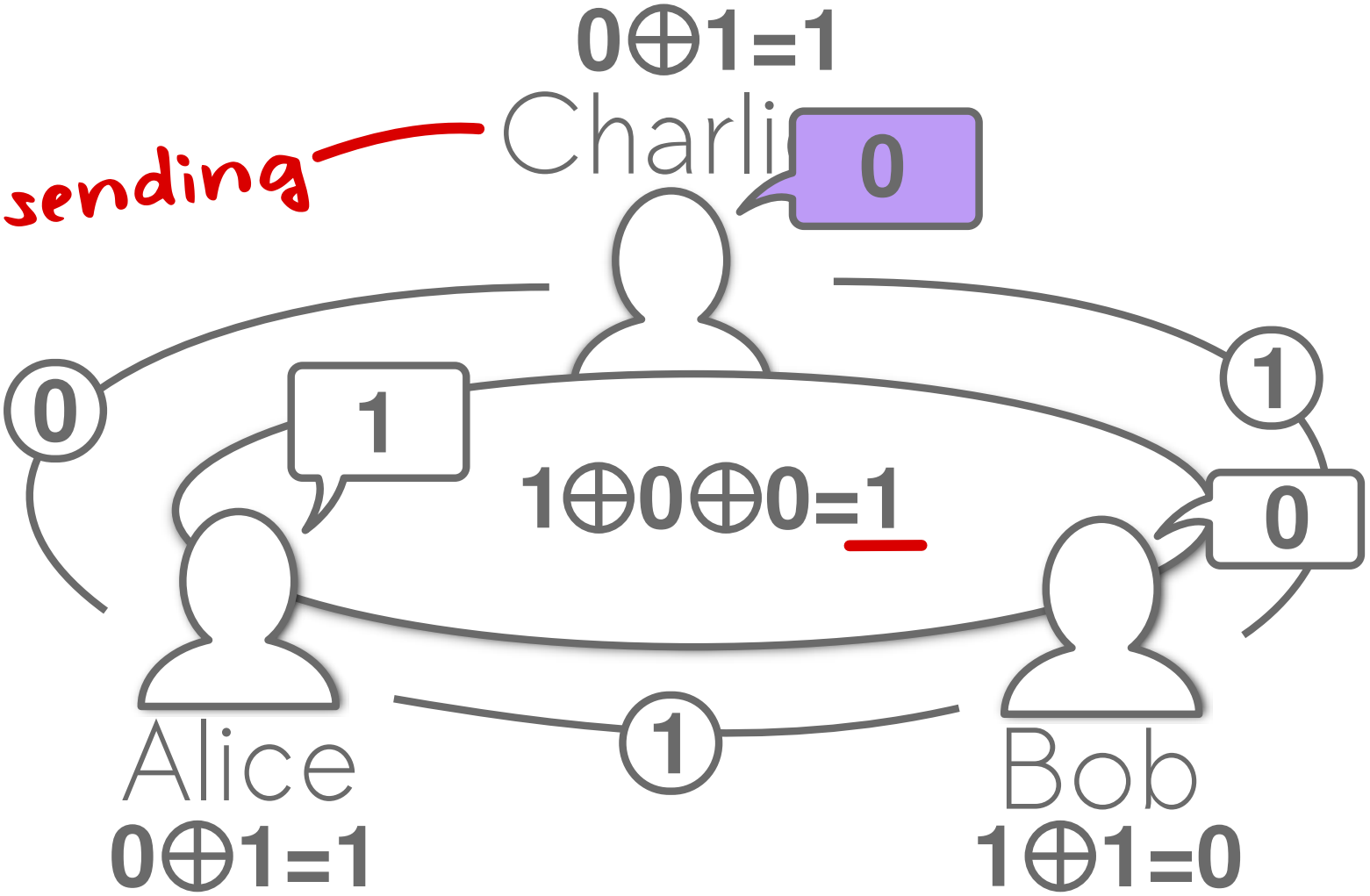

Charlie
0
1
Alice
1
Bob


key
Charlie
0
1
Alice
1
Bob

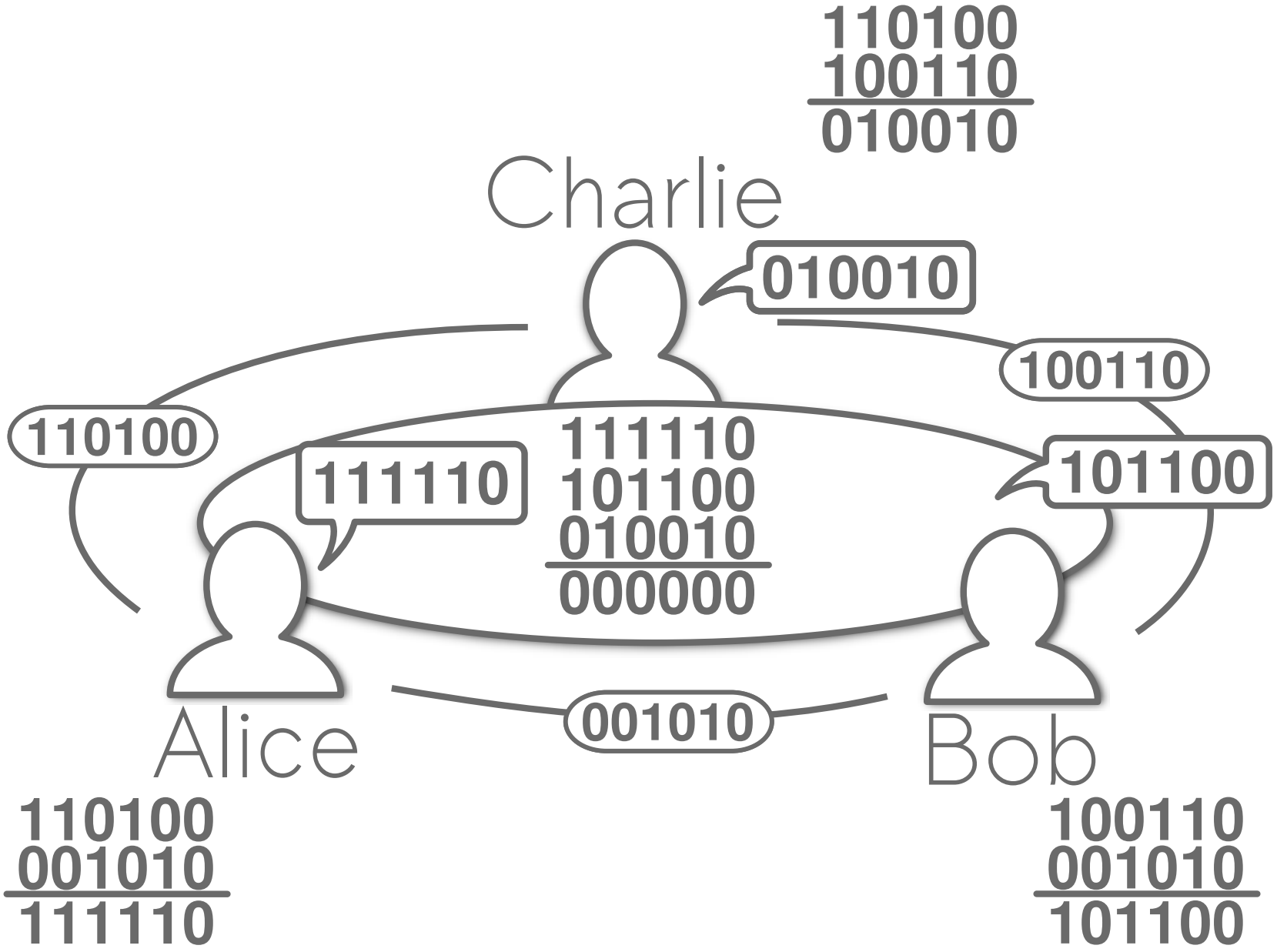

0⊕1=1
Charli
1
0
1
1
1
0
Alice
0⊕1=1
Bob
1⊕1=0

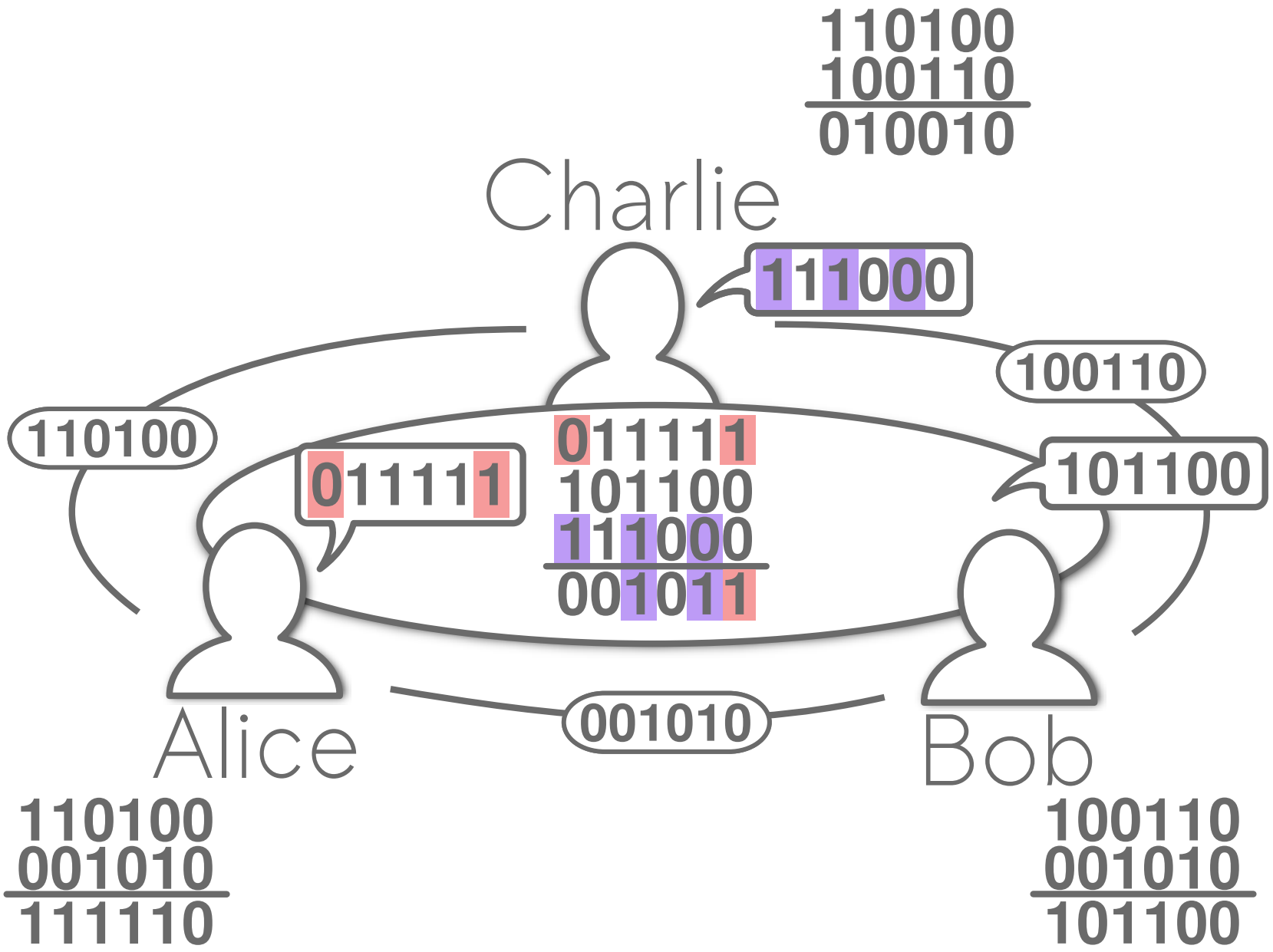

0⊕1=1
Charli
1
0
1
1
result
1⊕0⊕1=0
0
1
Alice
0⊕1=1
Bob
1⊕1=0

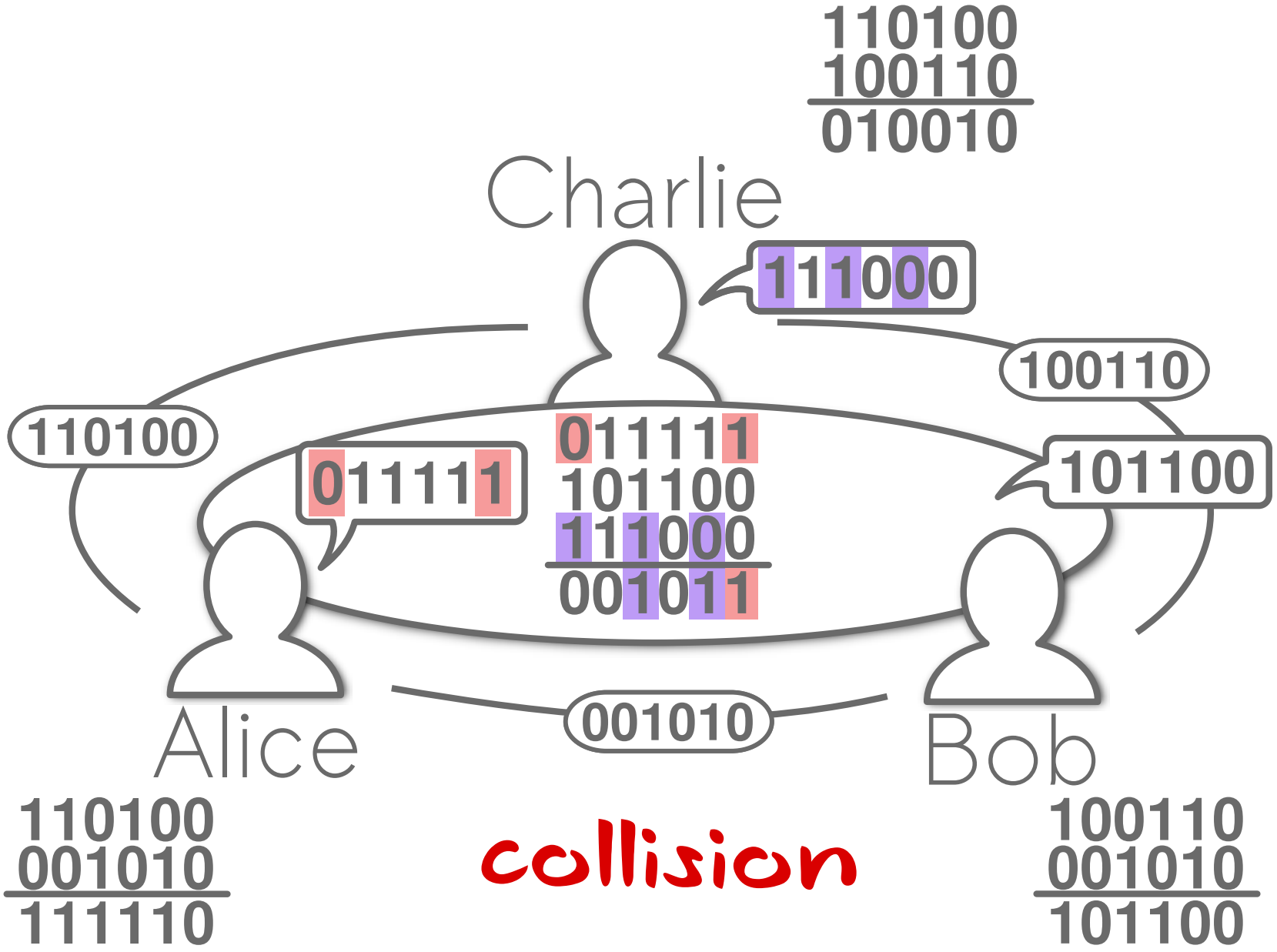

0⊕1=1
Charlie
sending
0
0
1
1
0
1
Alice
0⊕1=1
Bob
1⊕1=0


0⊕1=1
Charlie
sending
0
0
1
1
1⊕0⊕0=1
0
1
Alice
0⊕1=1
Bob
1⊕1=0

More Bits


110100
100110
010010
Charlie
010010
100110
110100
111110
101100
010010
000000
111110
101100
Alice
001010
Bob
110100
001010
111110
100110
001010
101100


110100
100110
010010
Charlie
111000
100110
110100
011111
101100
011111
101100
111000
001011
001010
Alice
Bob
110100
001010
111110
100110
001010
101100


110100
100110
010010
Charlie
111000
100110
110100
011111
101100
011111
101100
111000
001011
Alice
001010
Bob
110100
001010
111110
collision
100110
001010
101100

Collisions

Multiple senders	→	Collision
Corruption	→	Retransmission
Wasted traffic	→	Inefficient

Collisions

Multiple senders → Collision
Corruption → Retransmission
Wasted traffic → Inefficient

BAD

Collisions

More users → More collisions
→ More corruption
→ More wasted traffic

WORSE

Recap

DC networks:

Unconditional anonymity

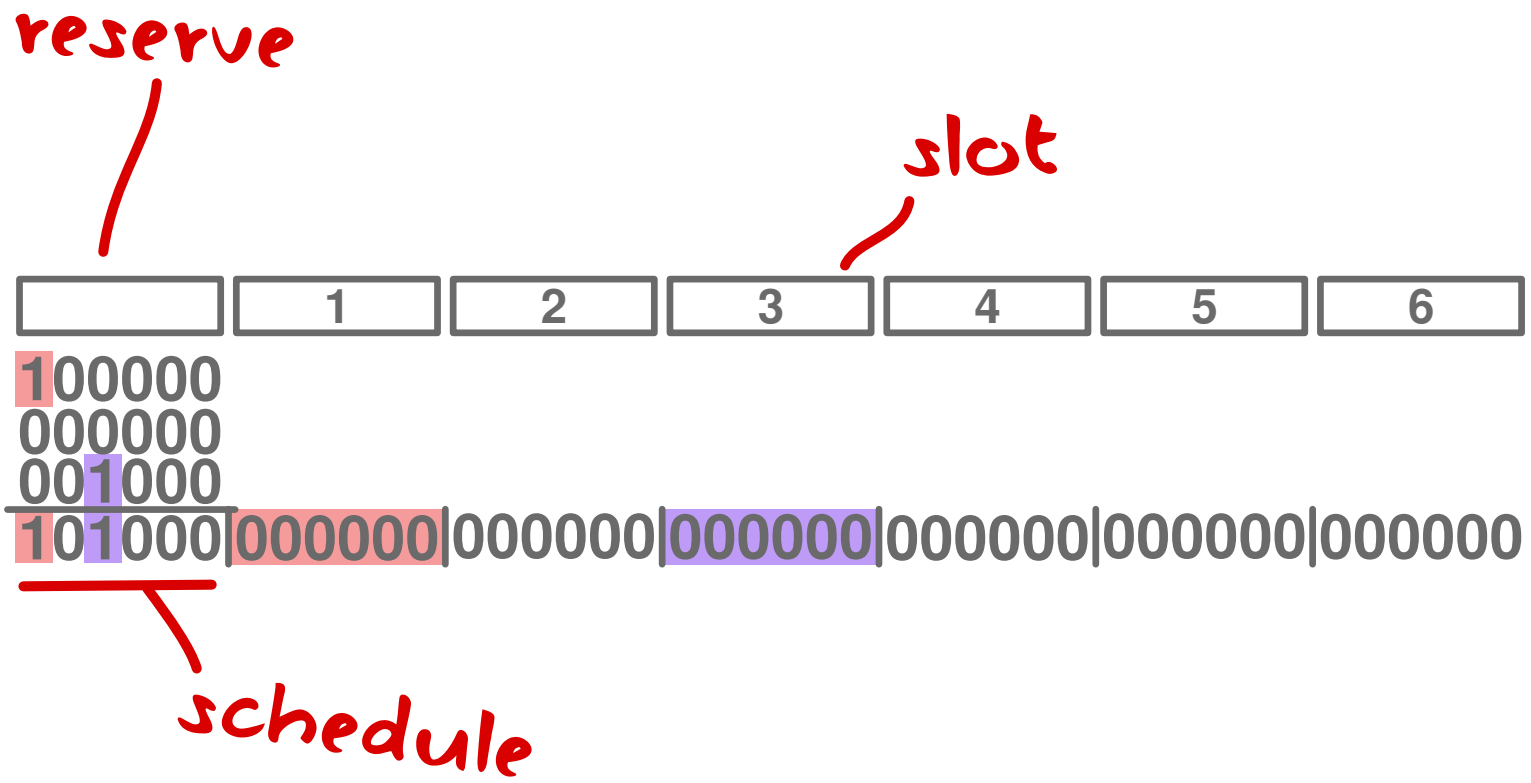
Arbitrary messages

Many participants

High traffic load

Collisions

Scheduling


reserve
slot
1
2
3
4
5
6
100000
000000
001000
101000|000000|000000|000000|000000|000000|000000
schedule

Collisions during reservation?

Detectable

```
001000
000000
001000
------
000000
```

Undetectable

```
001000
001000
001000
------
001000
```

Collisions during reservation?

Detectable

```
001000
000000
001000
------
000000
```

Undetectable

```
001000
001000
001000
------
001000
```

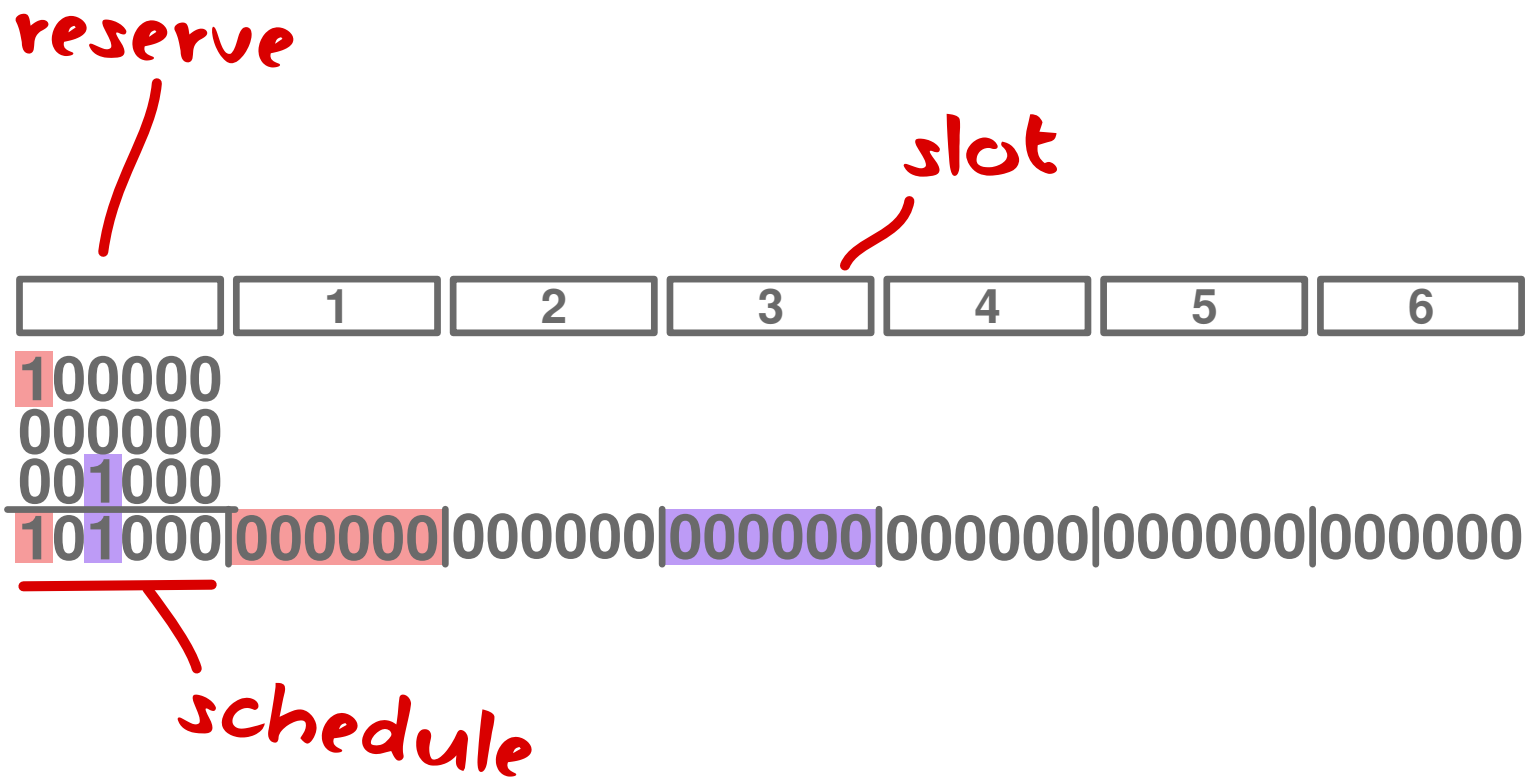
not enough :(

Tree-like collision resolution with superposed receiving

Andreas Pfitzmann, 1990

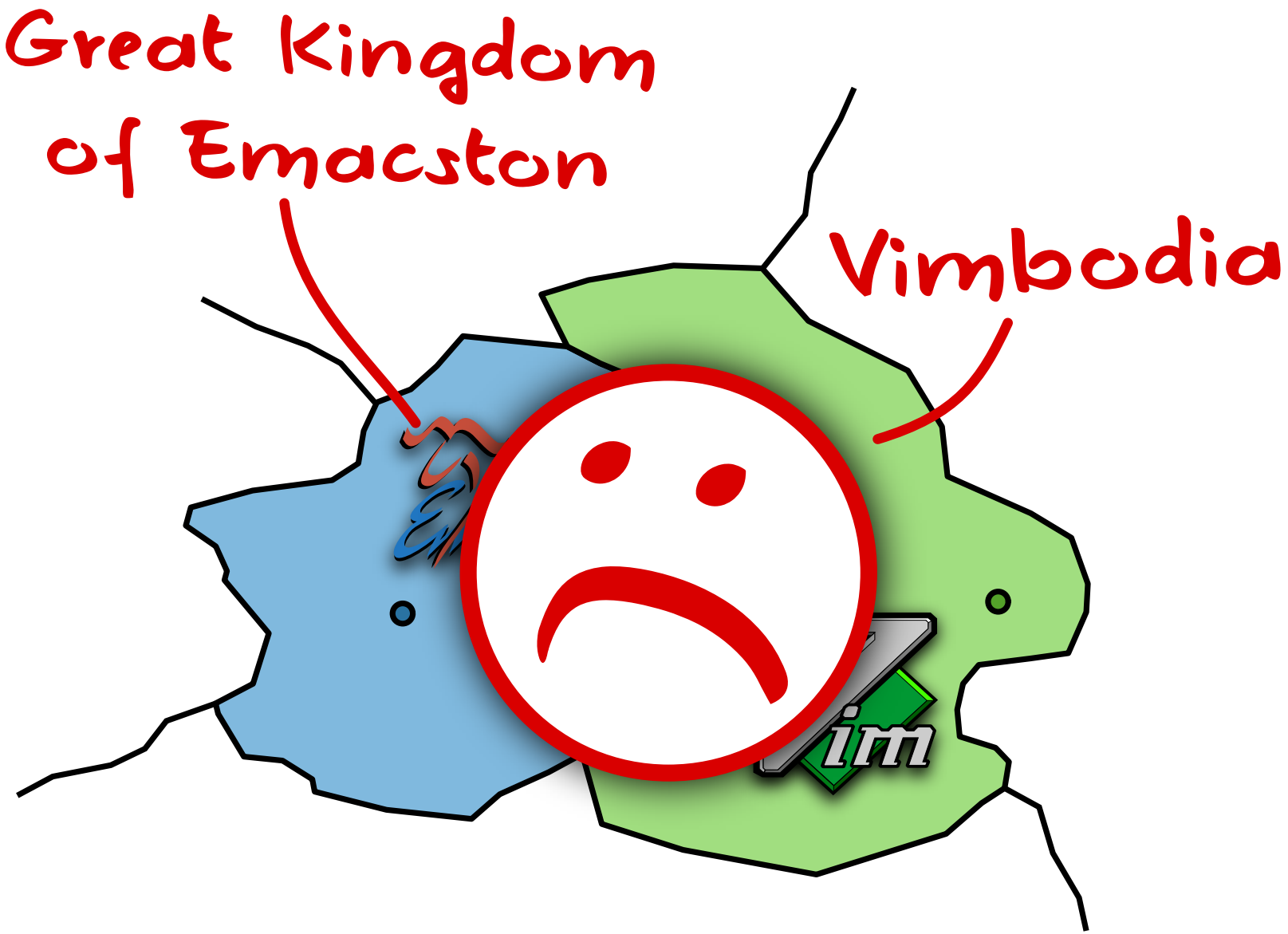
Existing algorithms

	Pfitzmann		
scales	# senders		
disconnect	breaks		
hides # senders	no		
message collisions	none		


reserve
slot
1
2
3
4
5
6
100000
000000
001000
101000|000000|000000|000000|000000|000000|000000
schedule

Existing algorithms

	Pfitzmann	Chaum	
scales	# senders	# users	
disconnect	breaks	unaffected	
hides # senders	no	no	
message collisions	none	trade-off	


Great Kingdom
of Emacston
Vimbodia
Vim

Collisions during reservation?

Detectable

```
001000
000000
001000
------
000000
```

Undetectable

```
001000
001000
001000
------
001000
```

More slots!

More bits! → Footprint scheduling

Footprint scheduling

- More bits per slot
  - 2 bits for now
- More choices
  - Flip left / right / both bit(s)
  - → detect more collisions

footprint

Alice: **10**
Bob: **11**
Charlie: **01**

footprint

Alice: **10**
Bob: **11**
Charlie: **01**

00.10.00
00.11.00
01.00.00

01.01.00

3 slots

Alice: **10**
Bob: **11**
Charlie: **01**

00.10.00
00.11.00
01.00.00

01.01.00

taken

free

Alice: **10**
Bob: **11**
Charlie: **01**

00.10.00
00.11.00
01.00.00
01.01.00

taken

free

DEDUCE
REUSE
RECYCLE

II.

Alice: **01**
Bob: **11**
Charlie: **11**

00.00.01
00.00.11
11.00.00

11.00.10

01.01.00

previously

III.

Alice: **10**
Bob: **10**
Charlie: **01**

00.00.10
00.10.00
01.00.00

01.10.10

11.00.10
01.01.00 previously

III.

converged!

Alice: **10**
Bob: **10**
Charlie: **01**

00.00.10
00.10.00
01.00.00

01.10.10

11.00.10
01.01.00 previously

III. converged!

Alice: **10**
Bob: **10**
Charlie: **01**

00.00.10
00.10.00
01.00.00

01.10.10

11.00.10
01.01.00 previously

	1	2	3
01.10.10	000000	000000	000000

Footprint scheduling

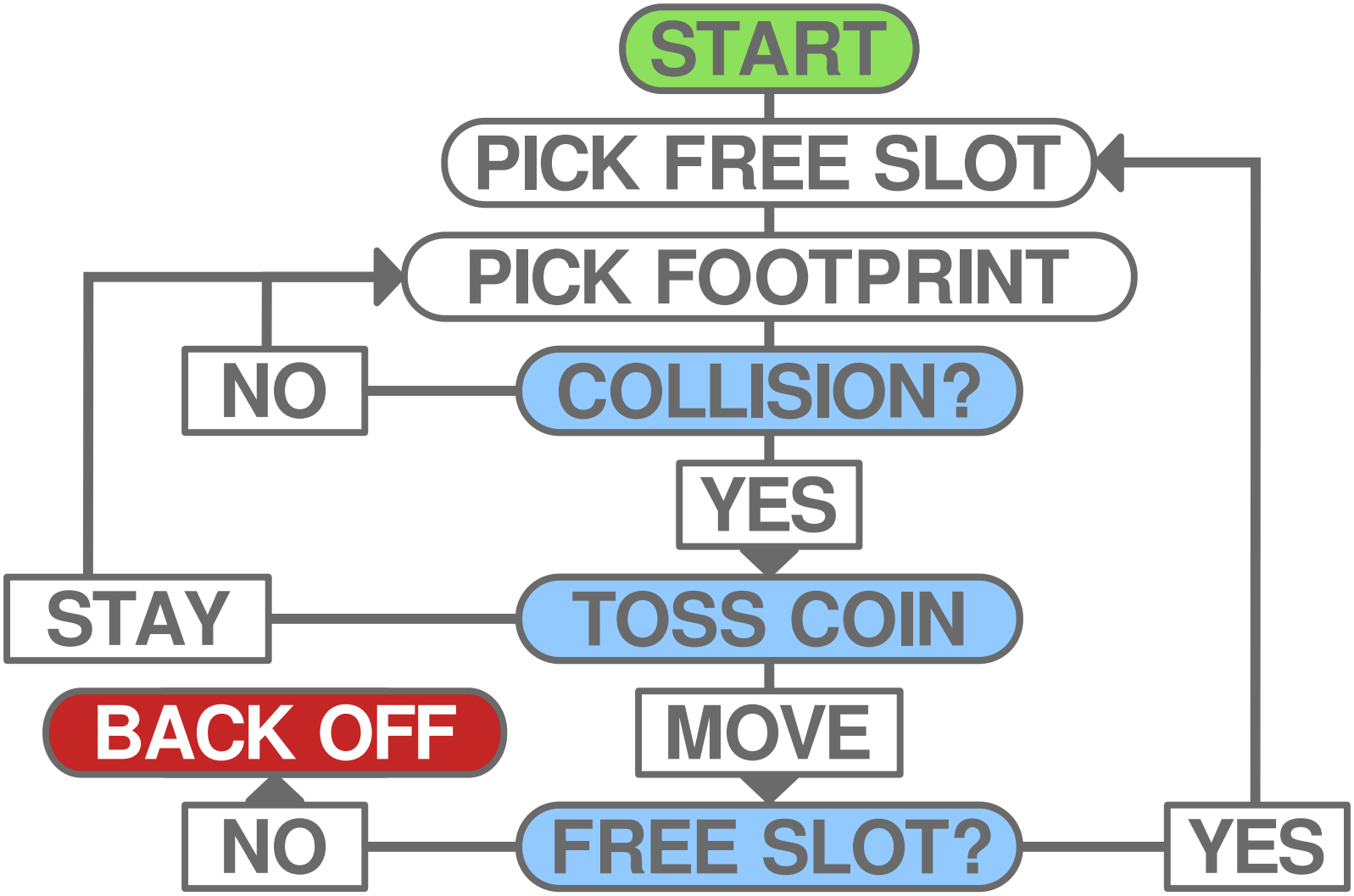
$\mathtt{s}$ slots

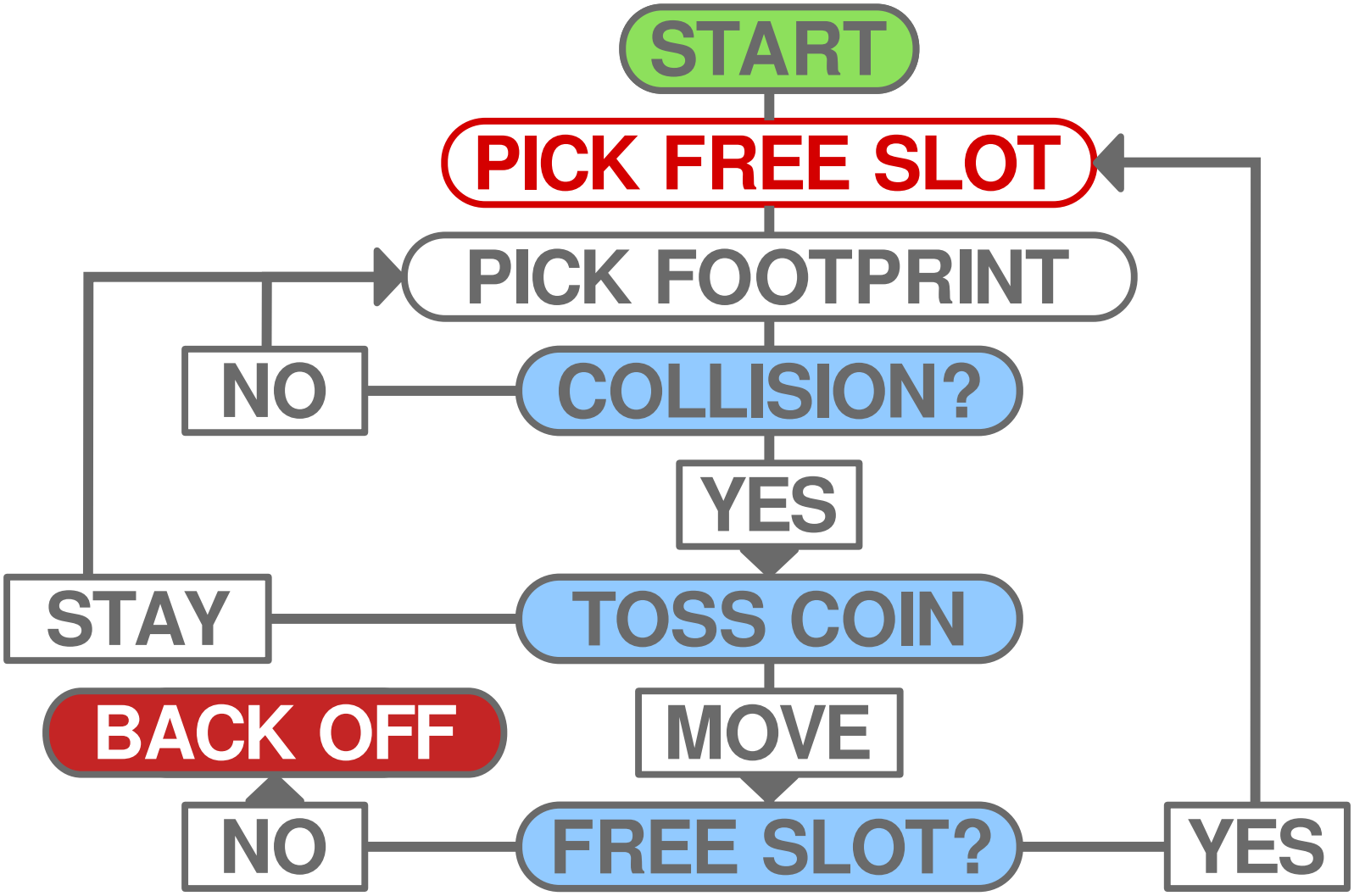
$\mathtt{s} \ll$ # users

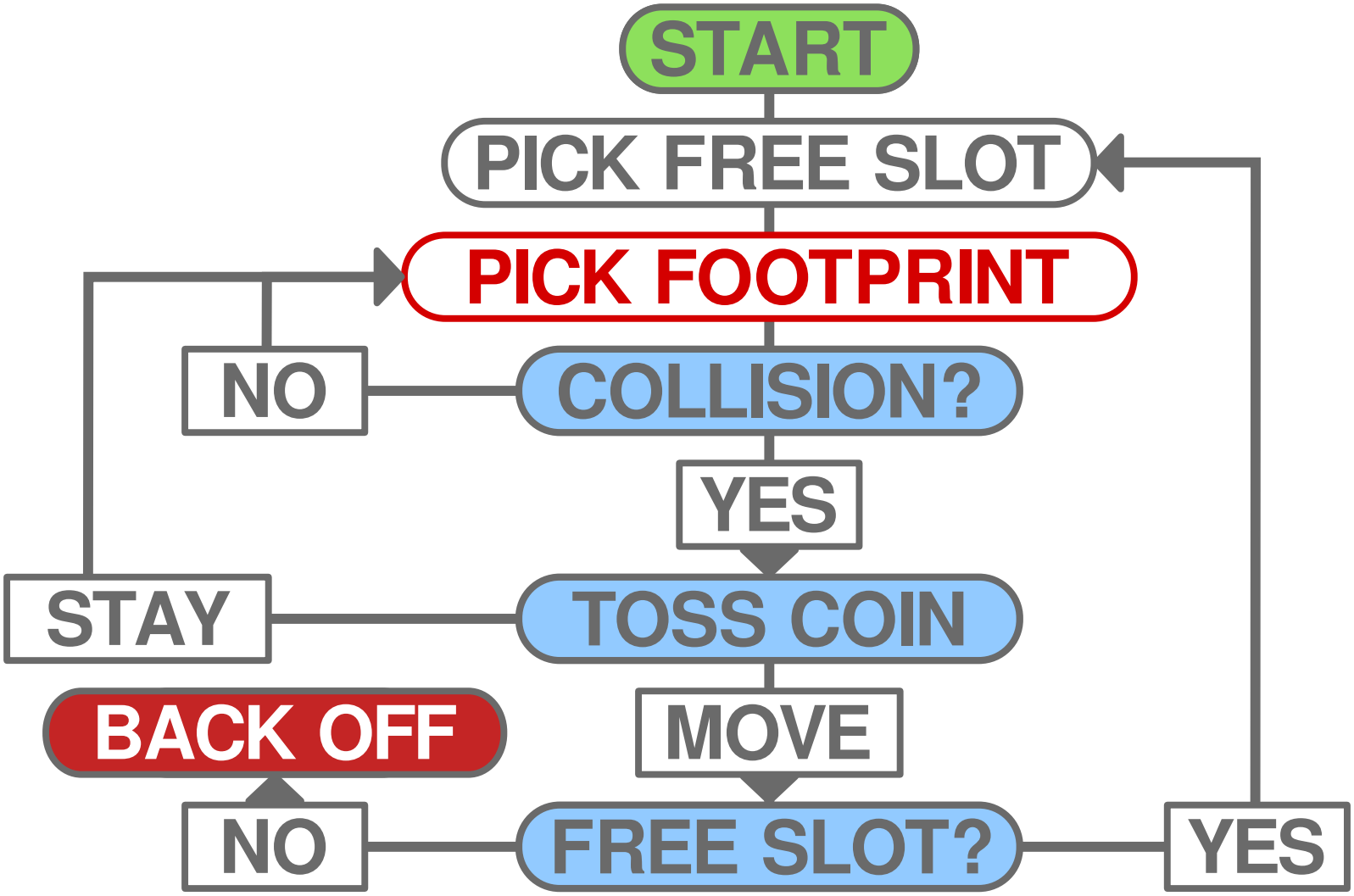
$\mathtt{2}$ bits per slot

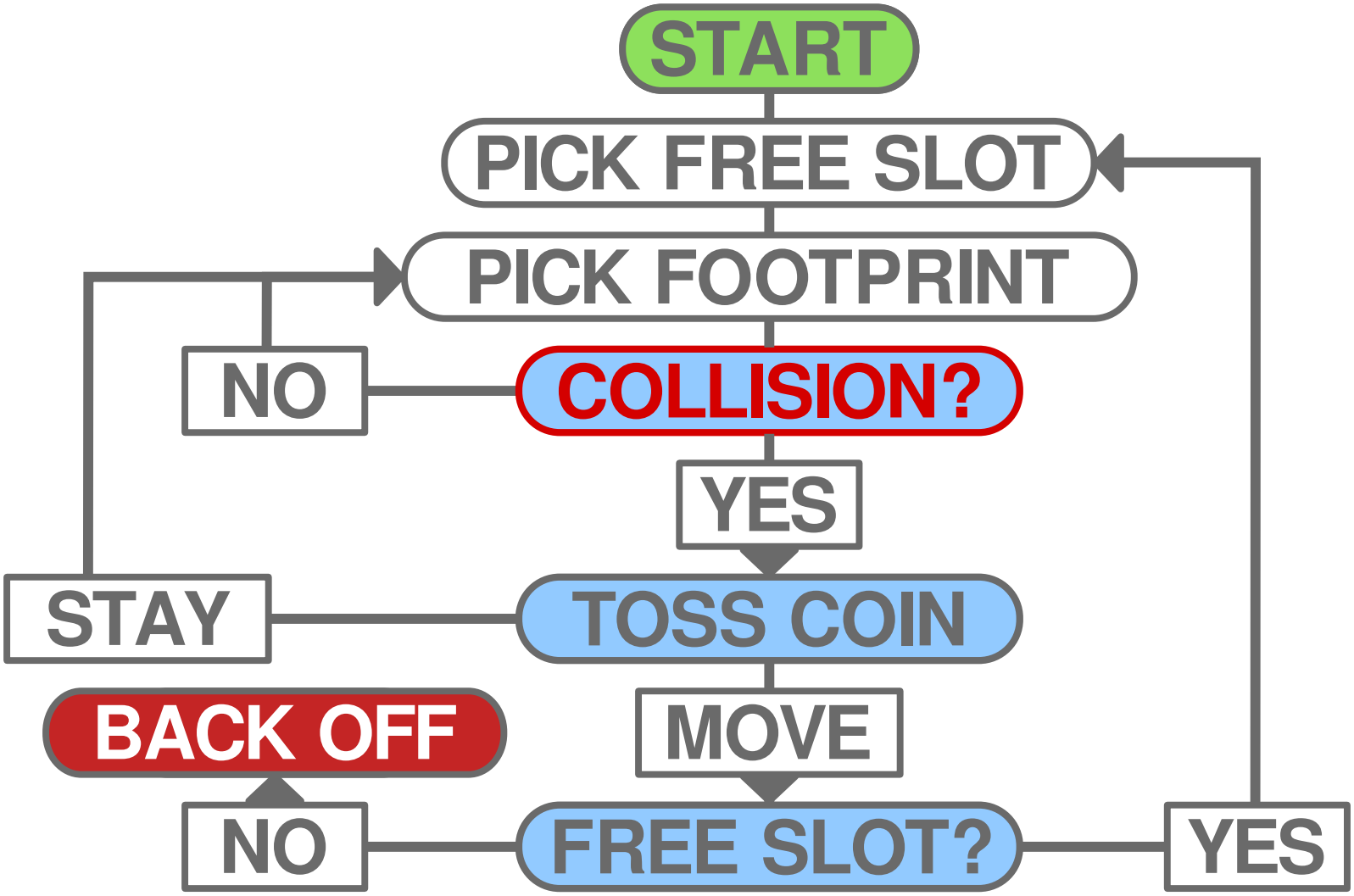
Iterate

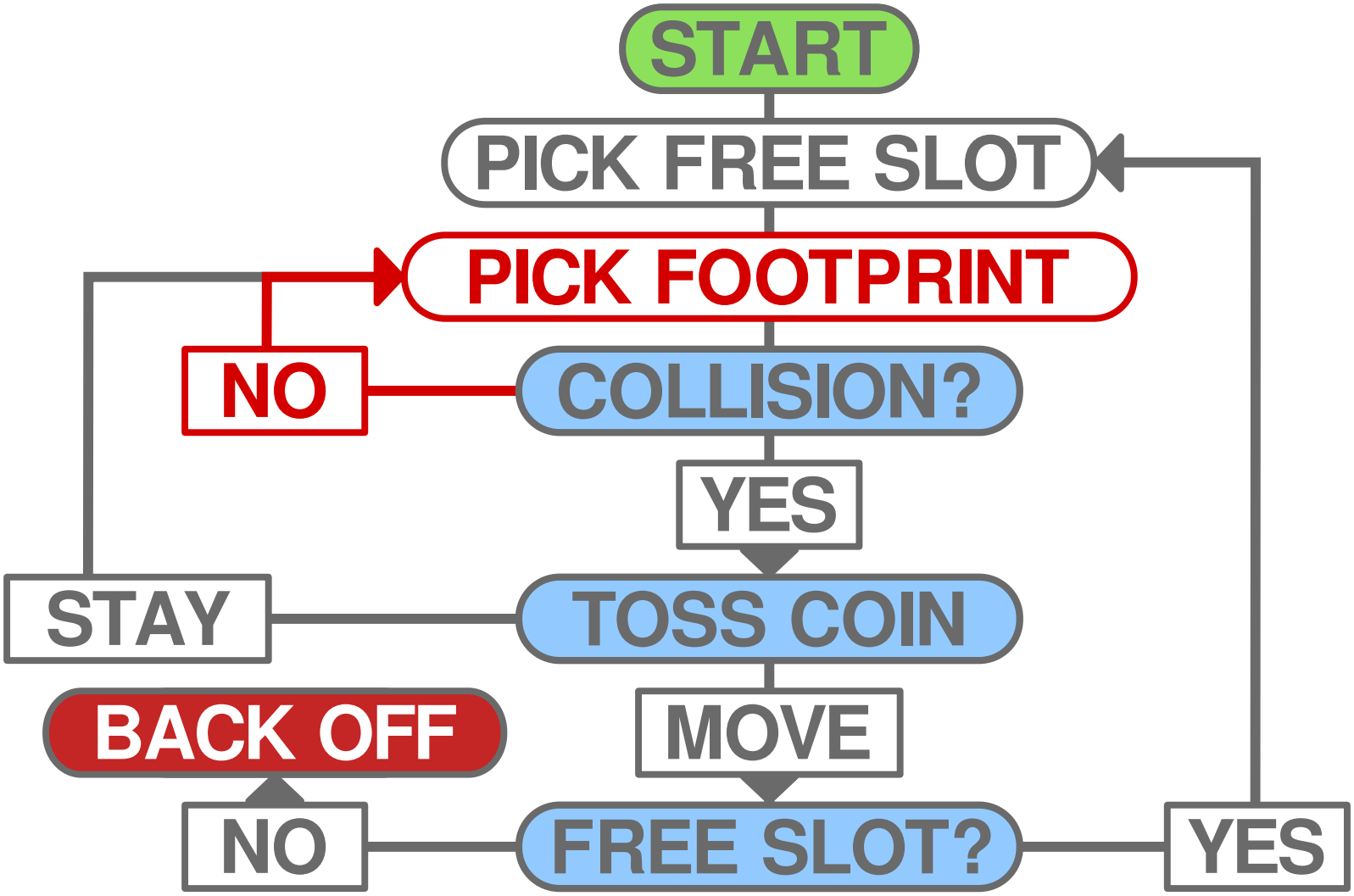
Discuss for $\mathtt{r}$ rounds

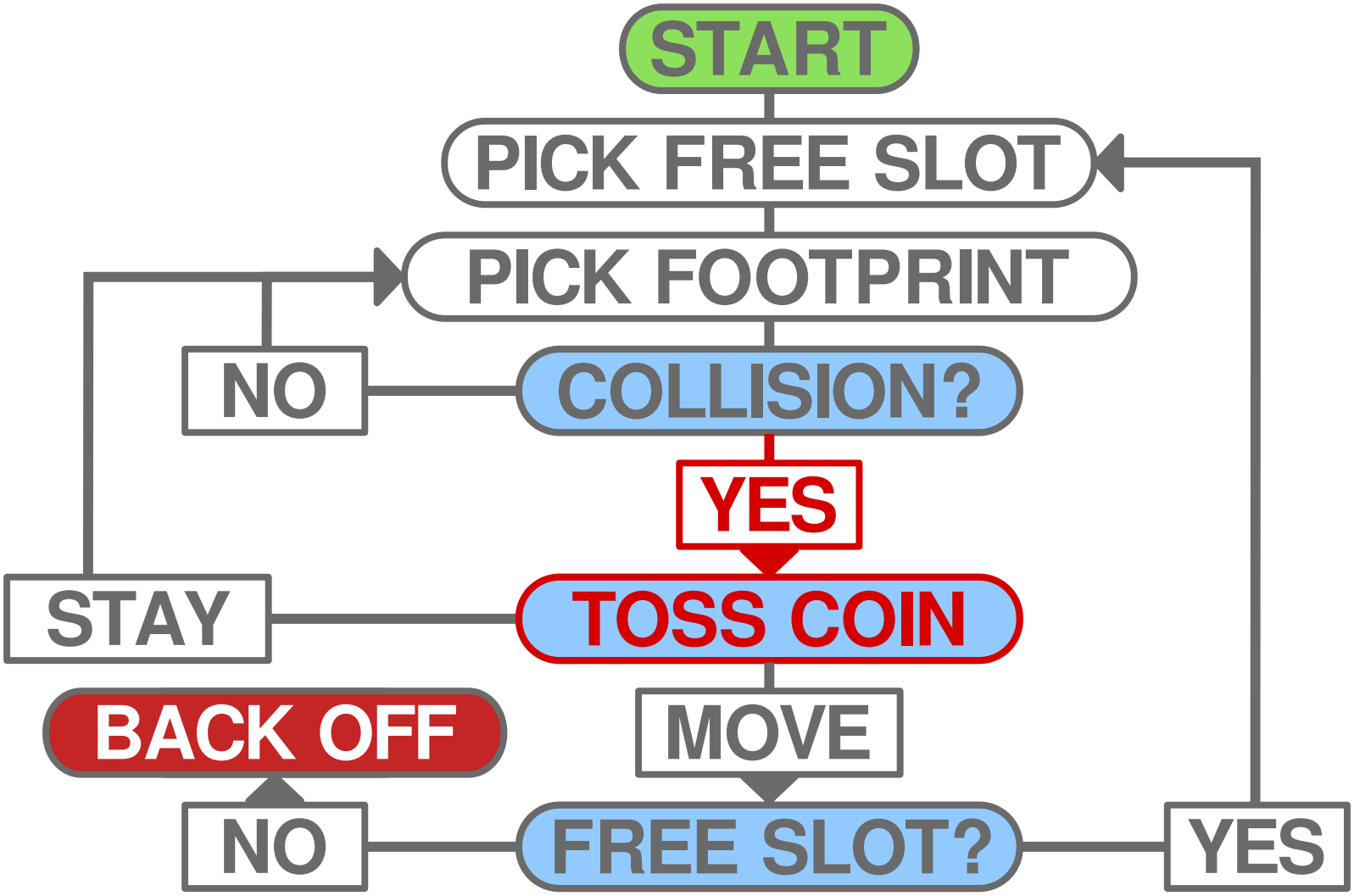

START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES

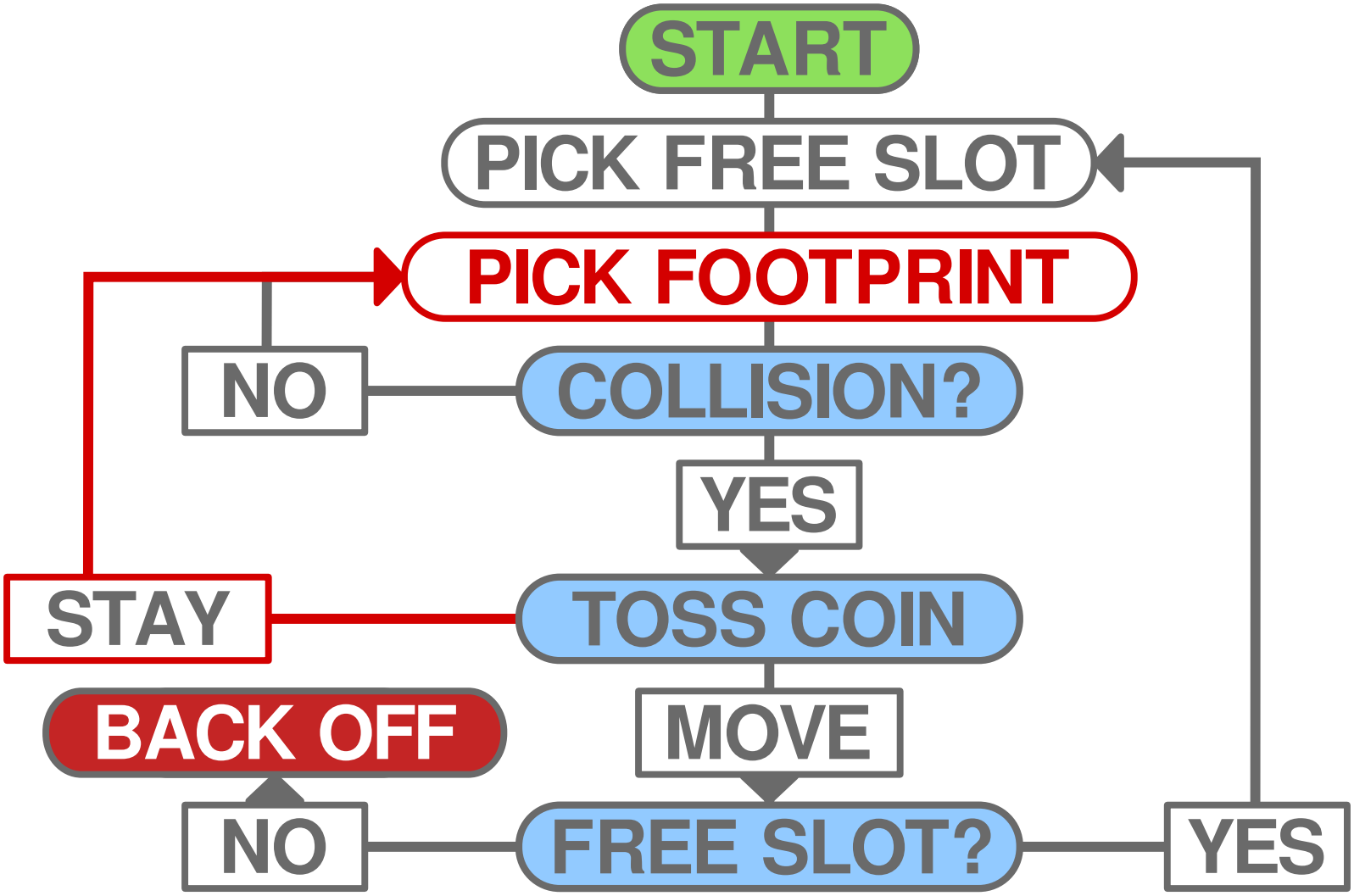

START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES

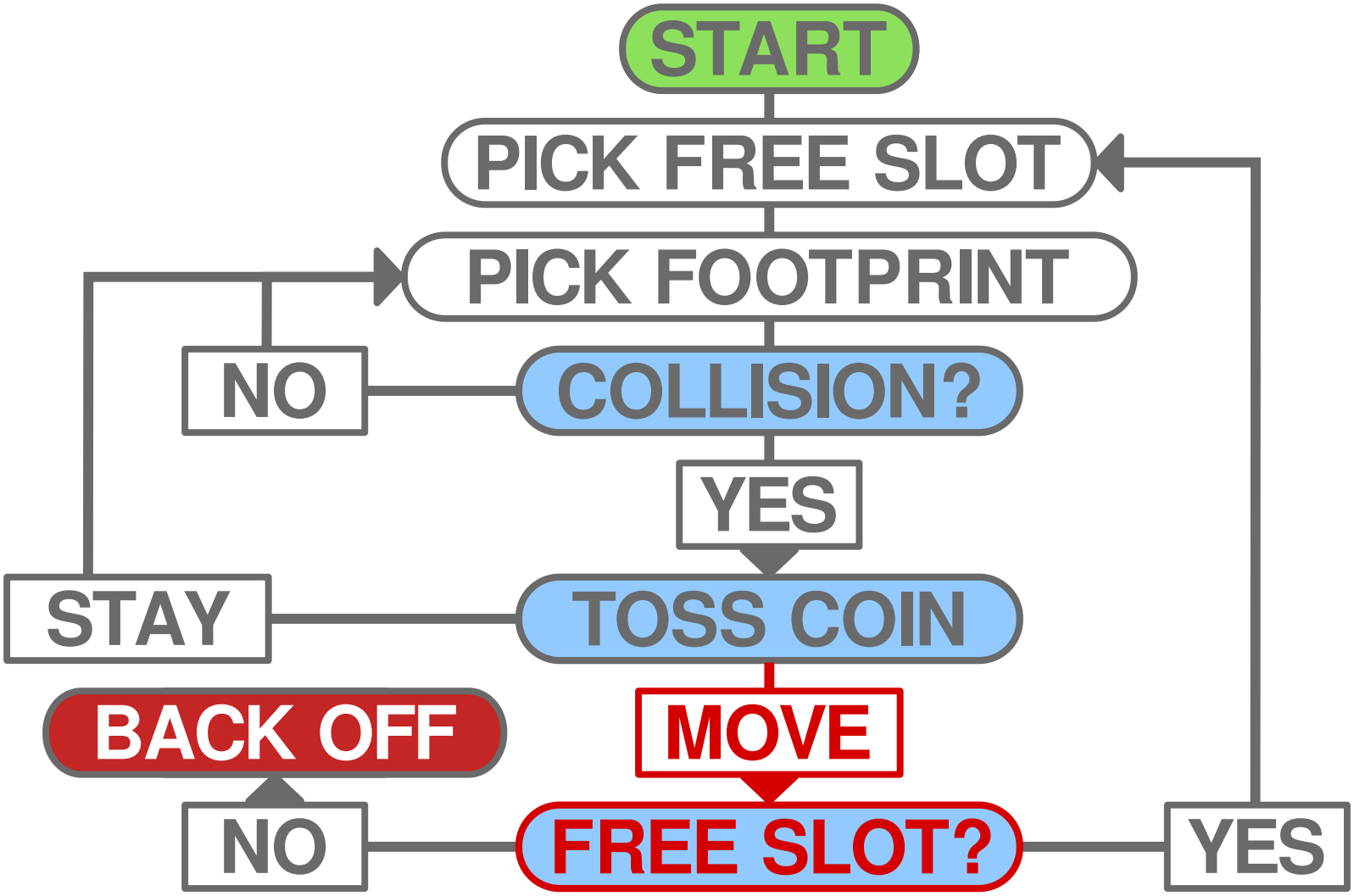

START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES

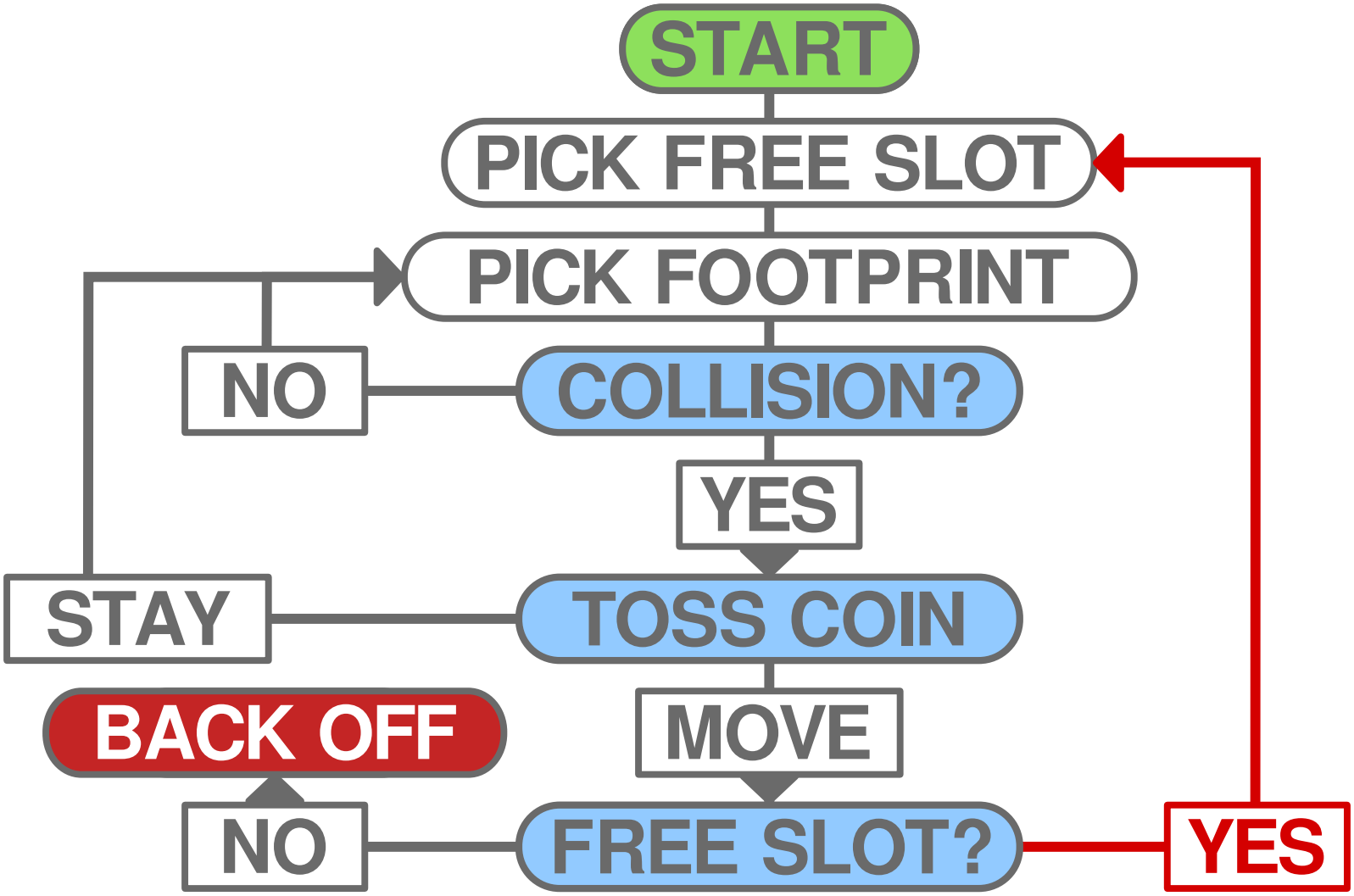

START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES

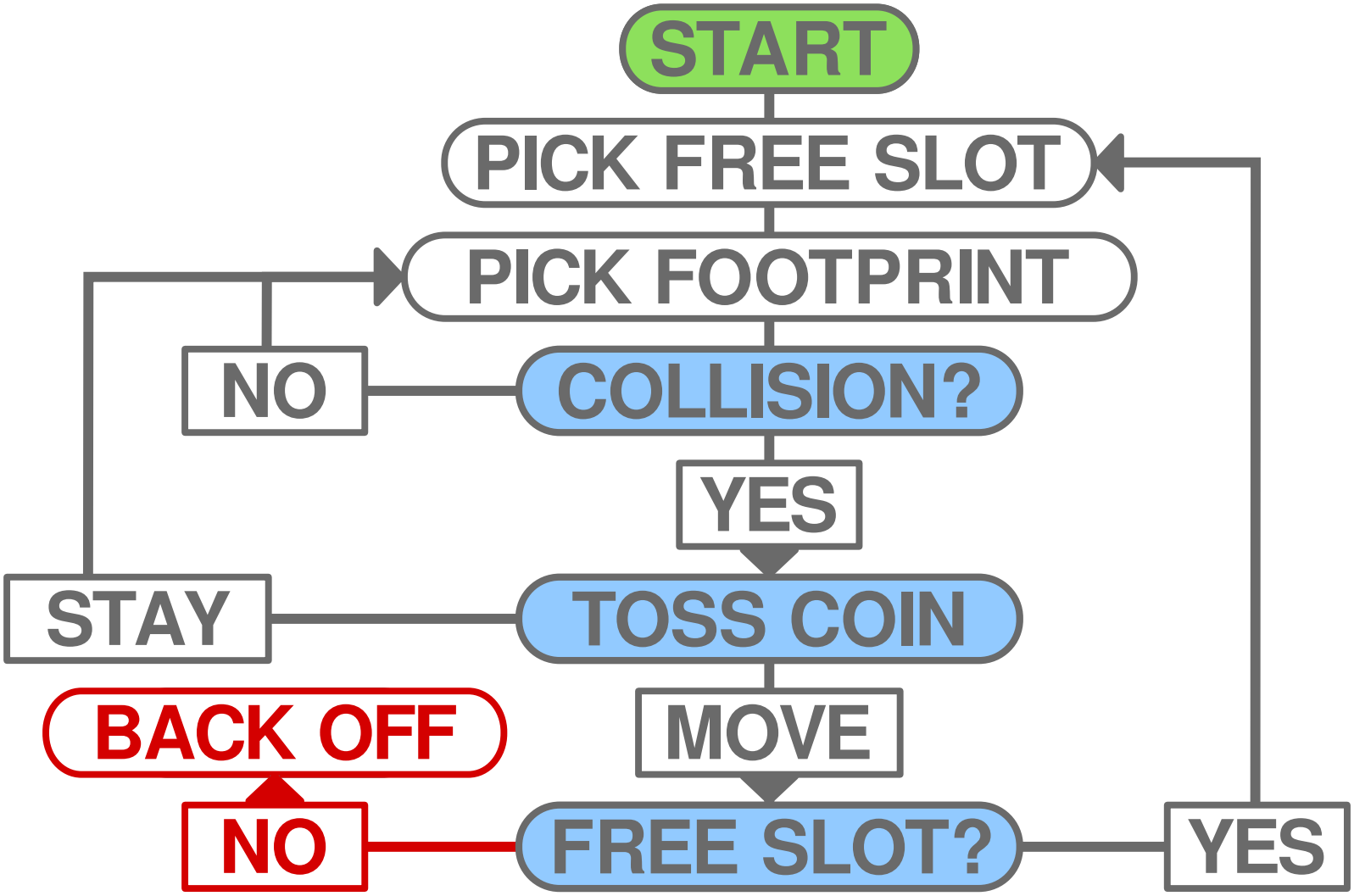

START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES


START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES


START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES


START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES


START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES


START
PICK FREE SLOT
PICK FOOTPRINT
NO
COLLISION?
YES
STAY
TOSS COIN
BACK OFF
MOVE
NO
FREE SLOT?
YES

Disconnects

Alice: **10**
Bob: **10**
~~Charlie: **01**~~

00.00.10
00.10.00
00.00.00

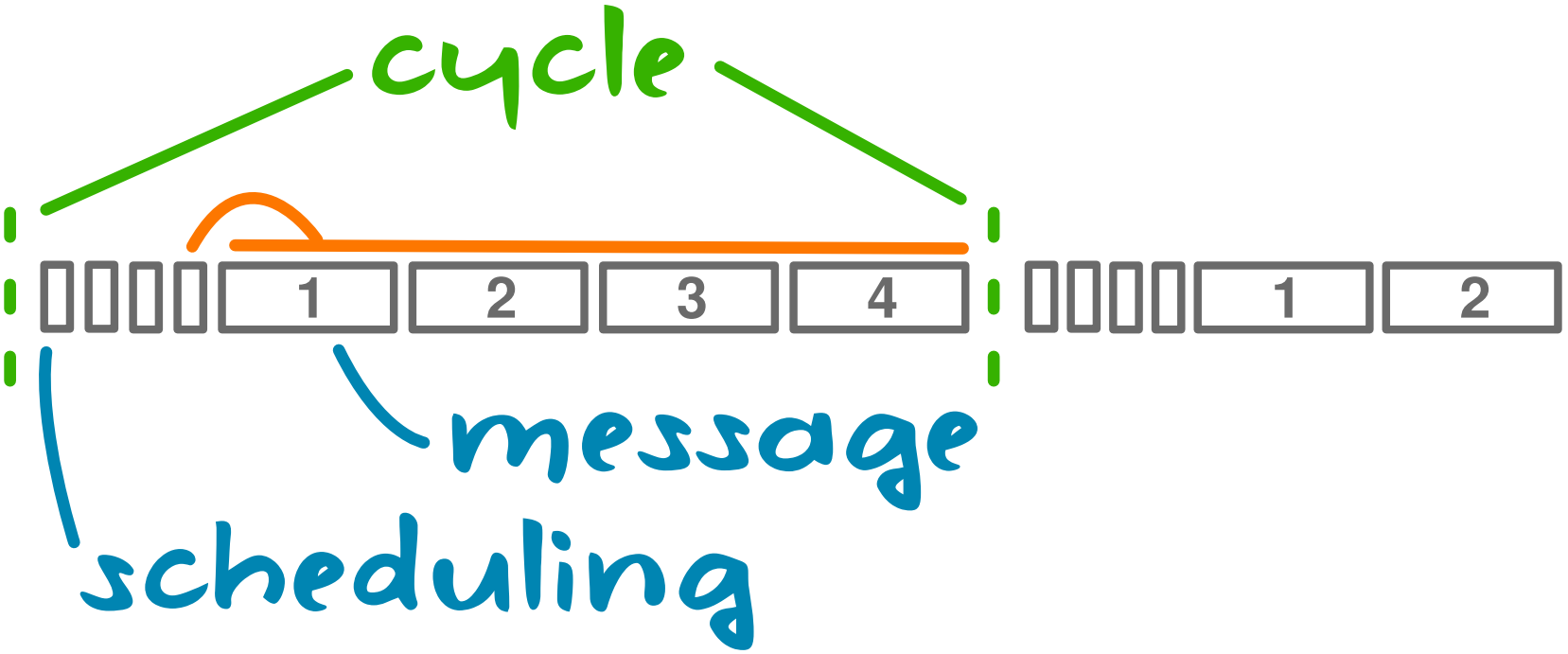
00.10.10

free

11.00.10
01.01.00 previously

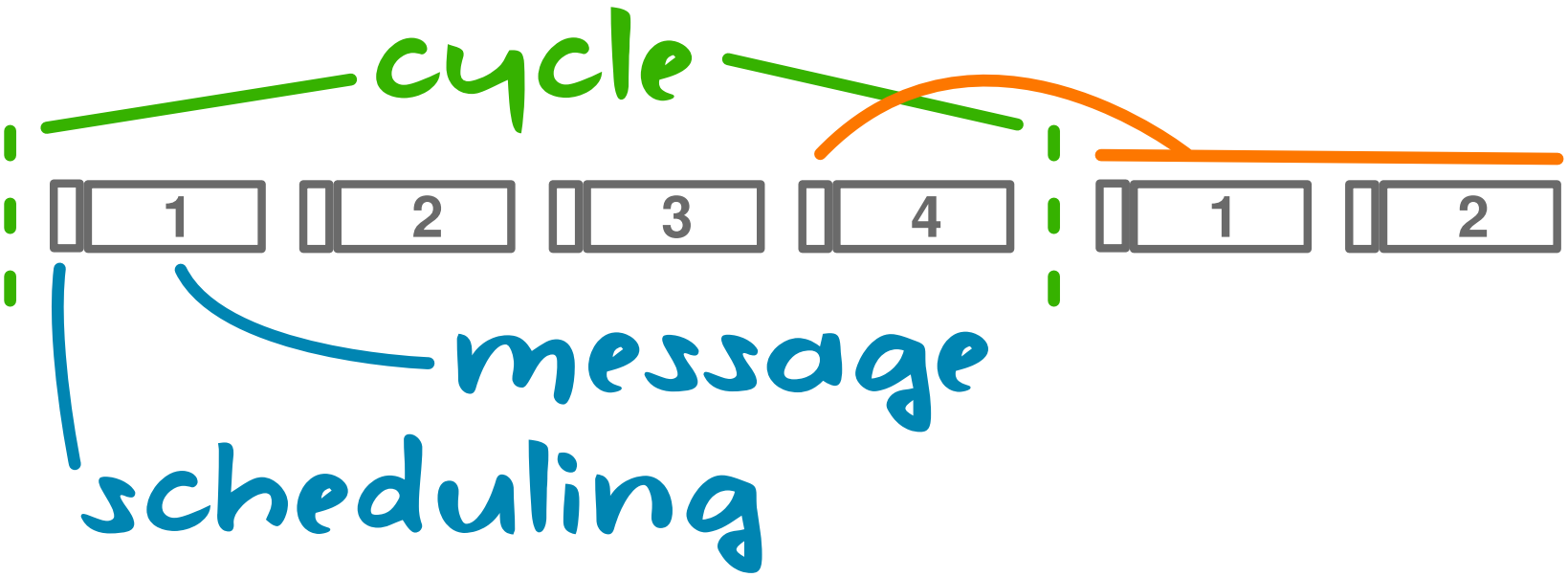
Interleaving

Header: 42B
Payload: 8B



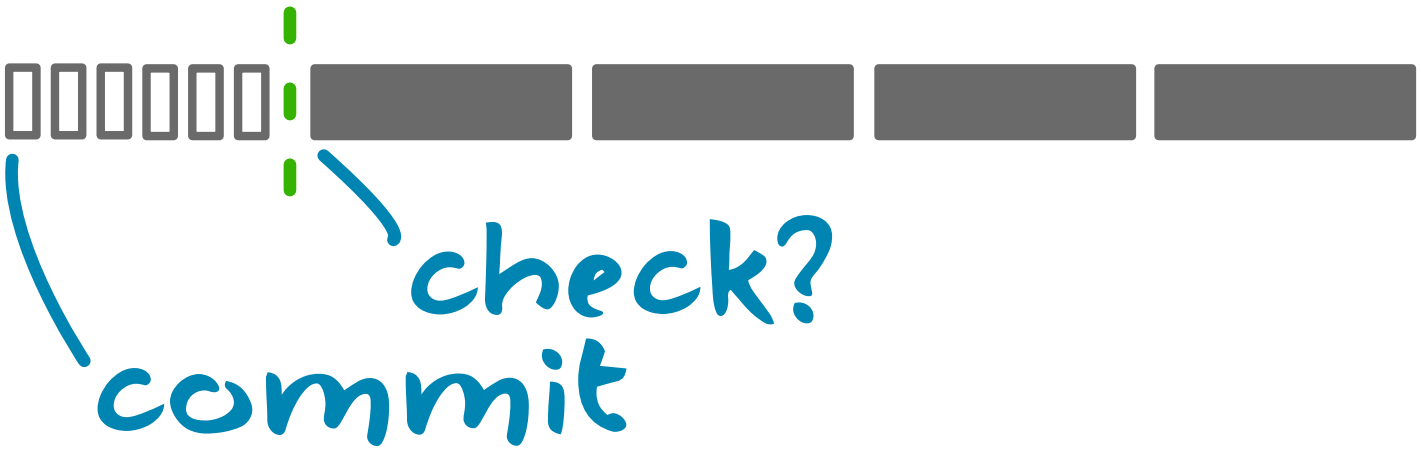
Interleaving

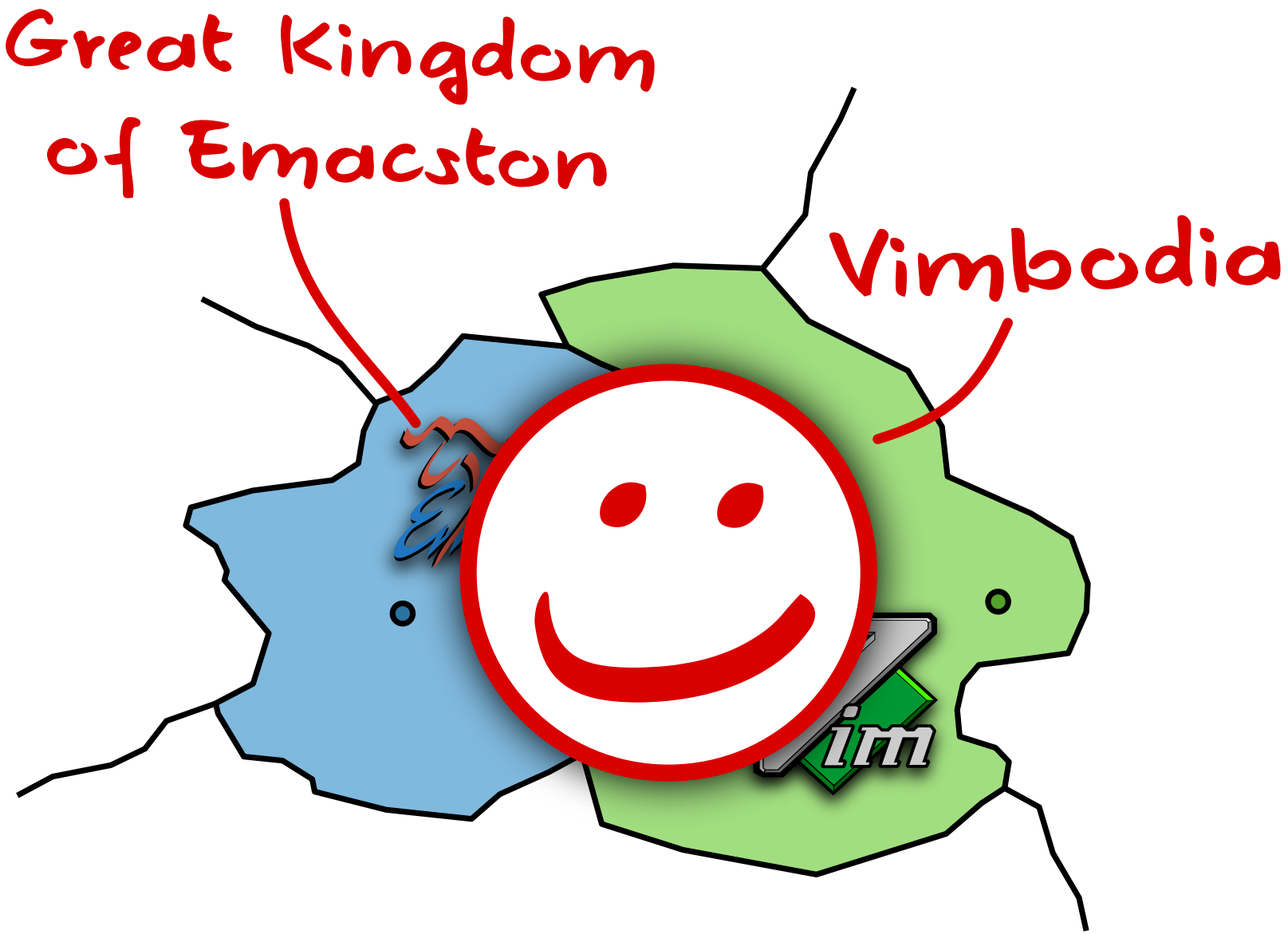
Header: 42B
Payload: 8B



Disruptors

commit to PRNG seed
random checks
discard schedule




Great Kingdom
of Emacston
Vimbodia
Vim

Existing algorithms

	Pfitzmann	Chaum	Footprint Scheduling
scales	# senders	# users	# senders
disconnect	breaks	unaffected	unaffected
hides # senders	no	no	passive
message collisions	none	trade-off	none*

Existing algorithms

	Pfitzmann	Chaum	Footprint Scheduling
scales	# senders	# users	# senders
disconnect	breaks	unaffected	unaffected
hides # senders	no	no	passive
message collisions	none	trade-off	none*

peter@cryptojedi.org
moritz@post-apocalyptic-crypto.org
anna@mechanical-mind.org

Traditional alg.

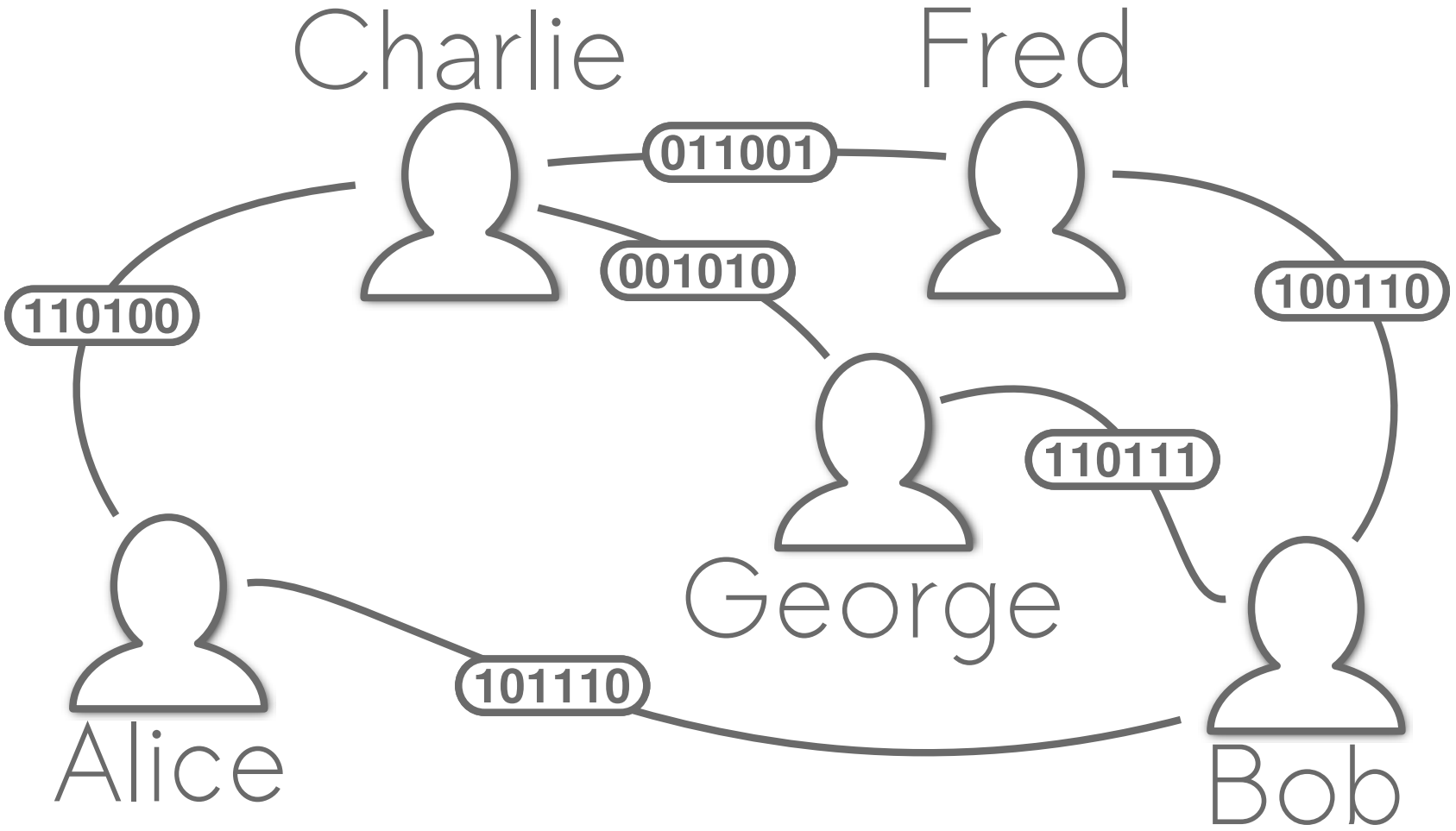
Collision resolution

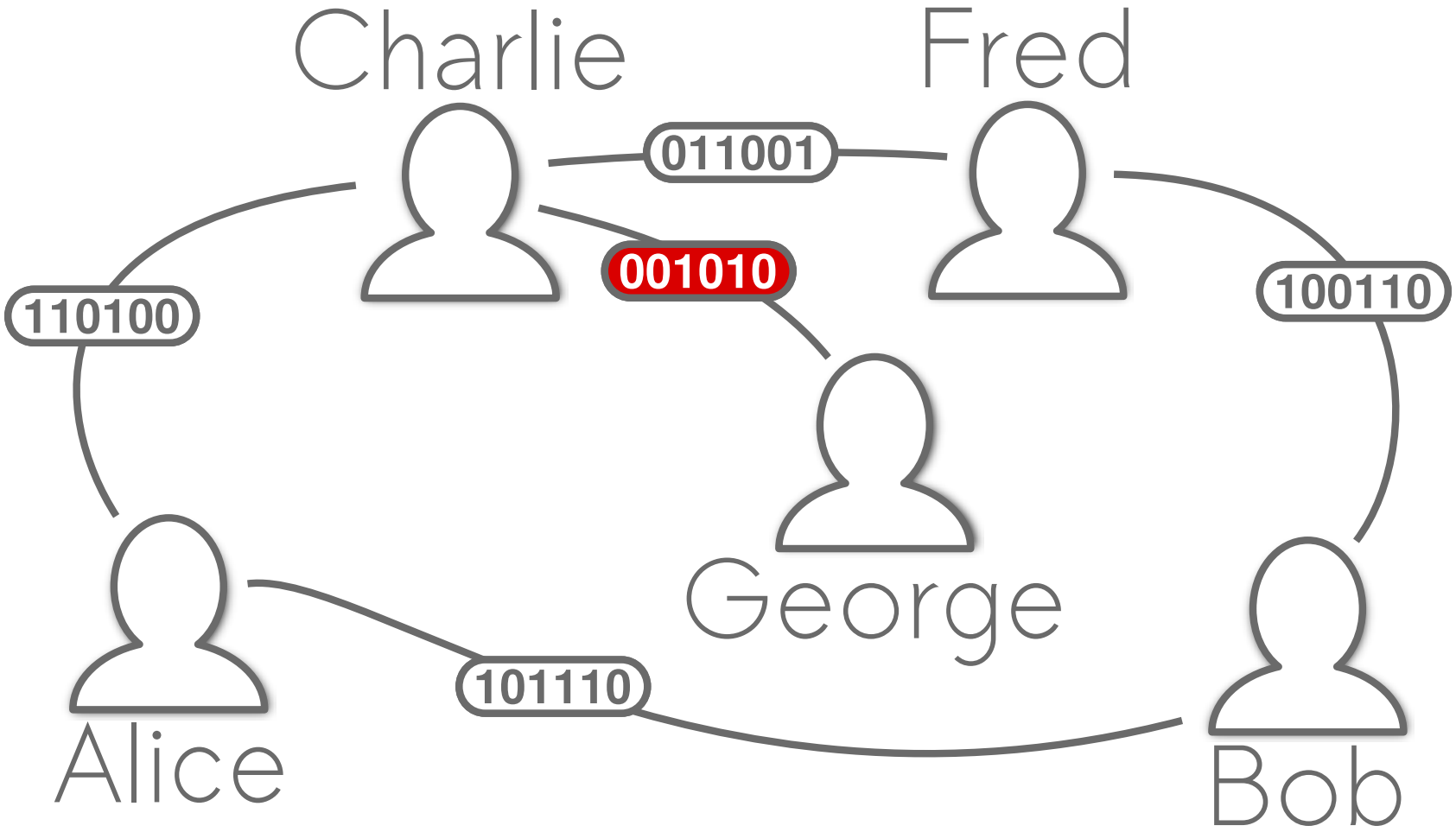
- (slotted) ALOHA — doesn't scale
- CSMA Carrier Sense Multiple Access — inefficient

Collision-free

- Bit-map protocols
- Tokens

no anonymity


Charlie
Fred
011001
001010
110100
100110
110111
George
101110
Alice
Bob


Charlie
Fred
011001
001010
110100
100110
George
101110
Alice
Bob

Pfitzmann's algorithm

Andreas Pfitzmann, 1990

Cleverly utilizes collisions

Scales with # senders

By design no undetectable collisions

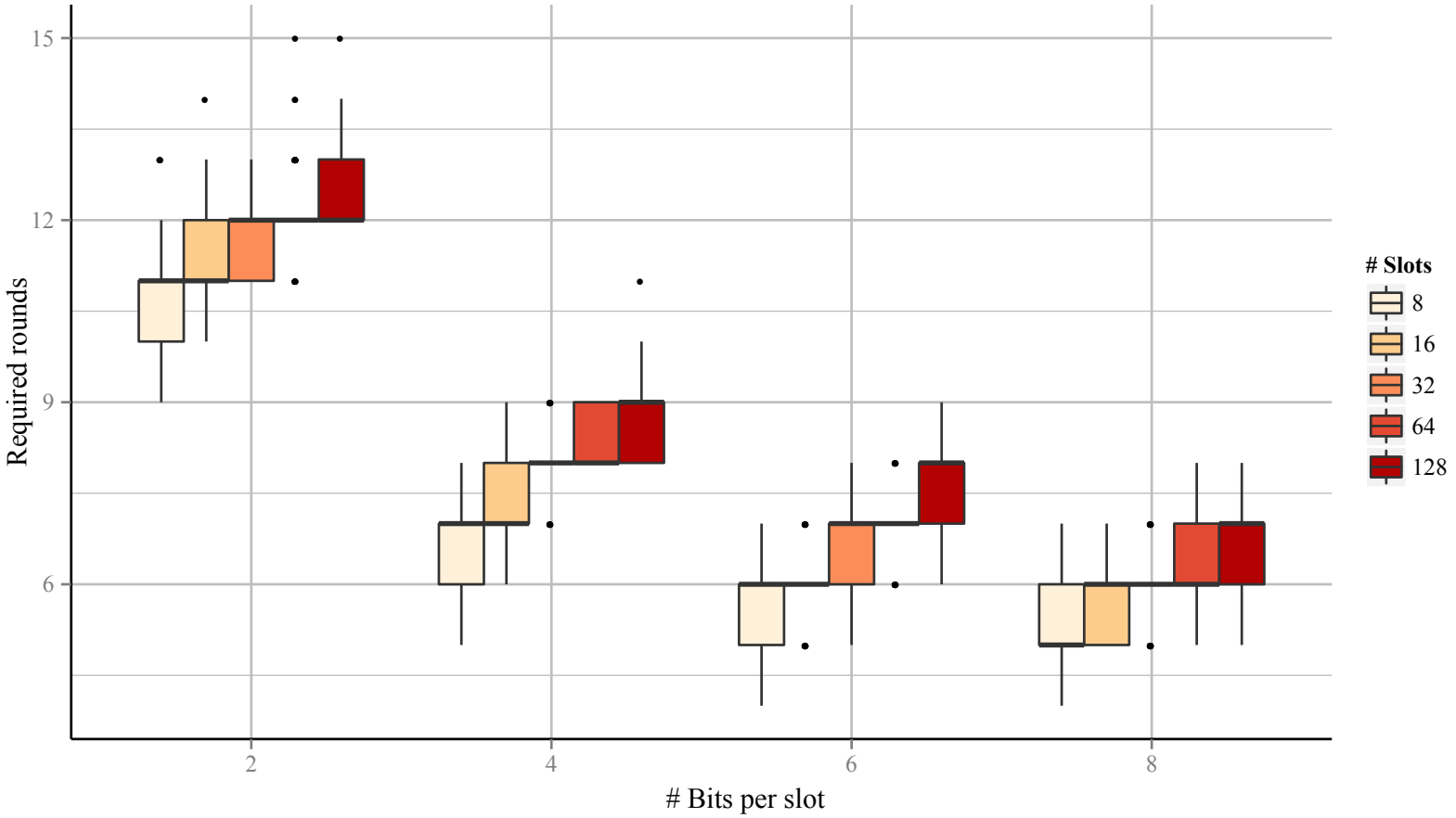
>11 min to complete

- 10,000 users
- based on latency between major US cities

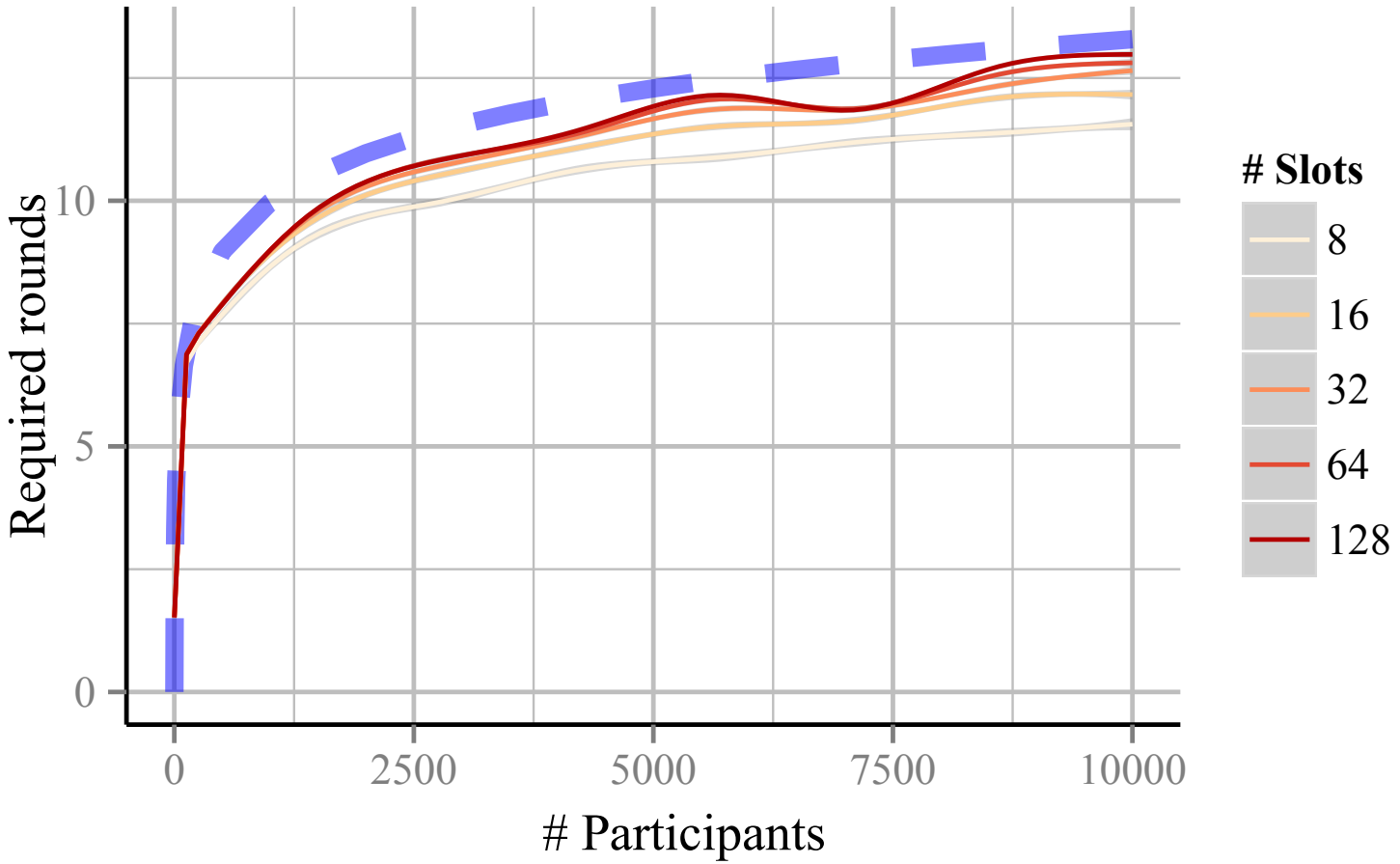
Breaks on disconnect

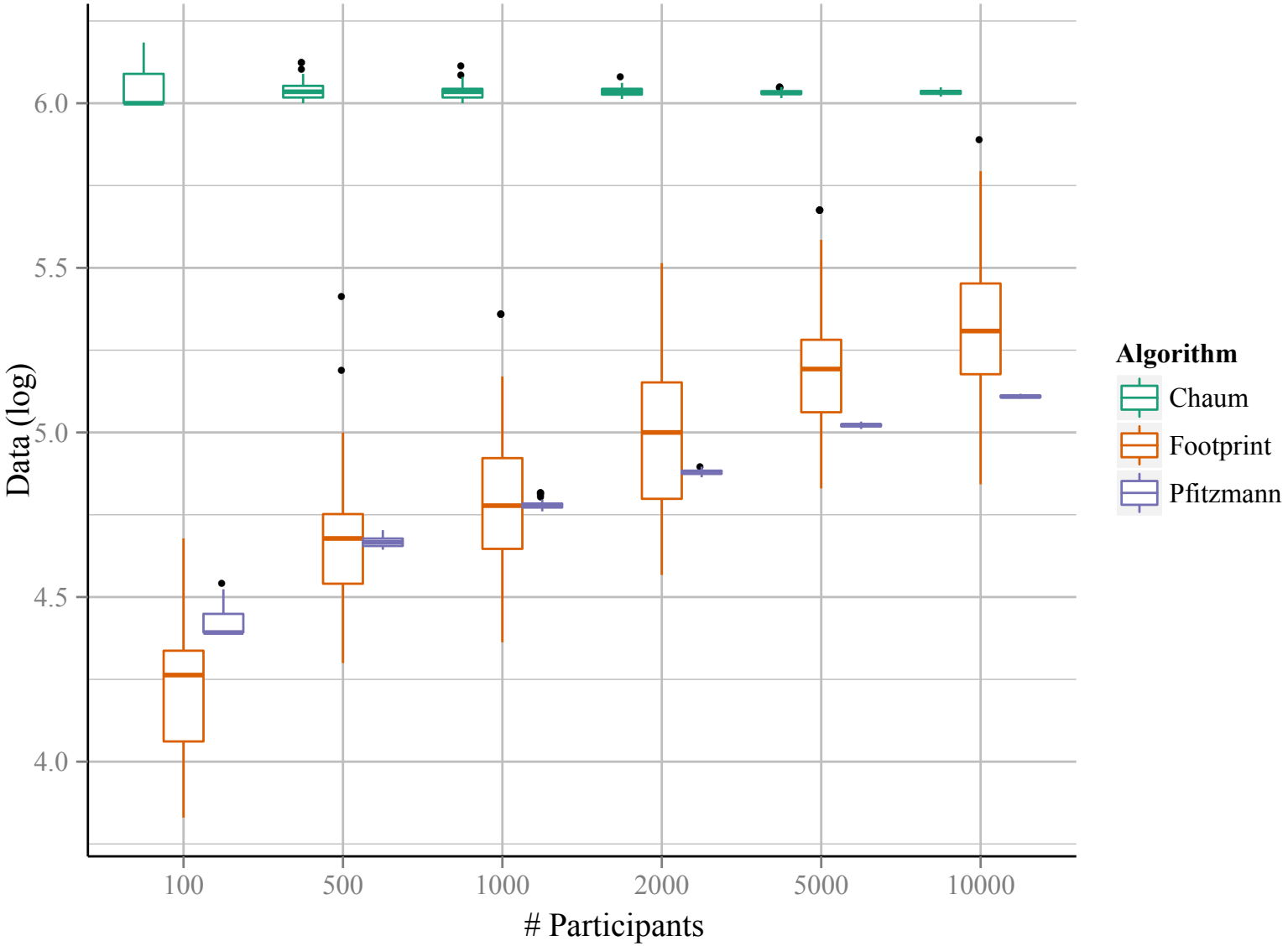
http://dud.inf.tu-dresden.de/sirene/publ/Pfit_88_0.pdf … _6.pdf

Optimization



Optimization




6.0
5.5
5.0
4.5
4.0
Data (log)
100
500
1000
2000
5000
10000
Participants
Algorithm
Chaum
Footprint
Pfitzmann