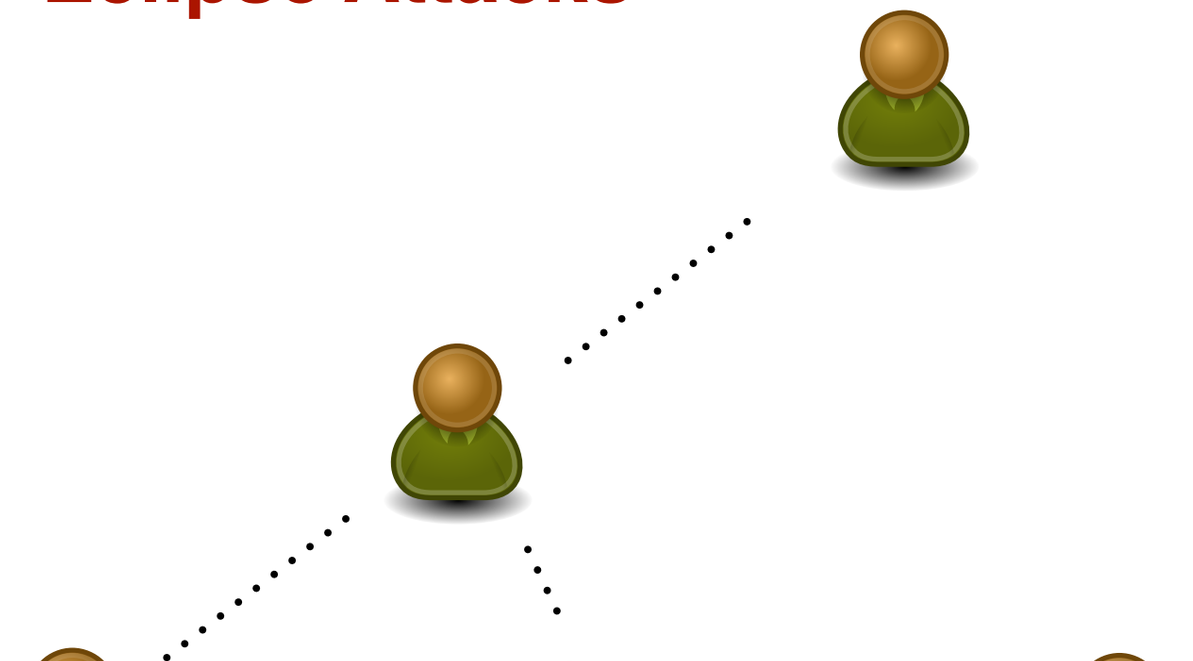
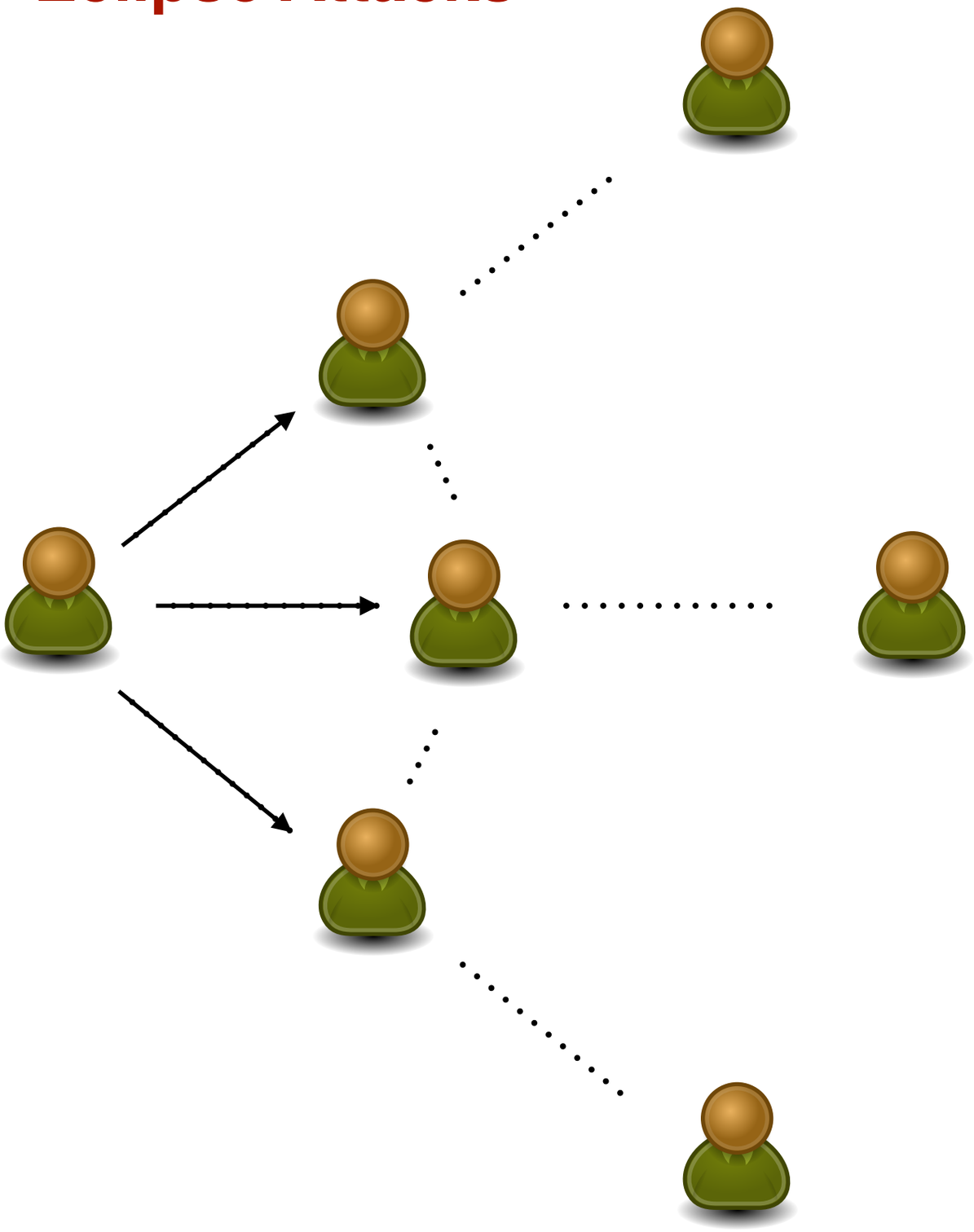
Network Security - Eclipse Attacks

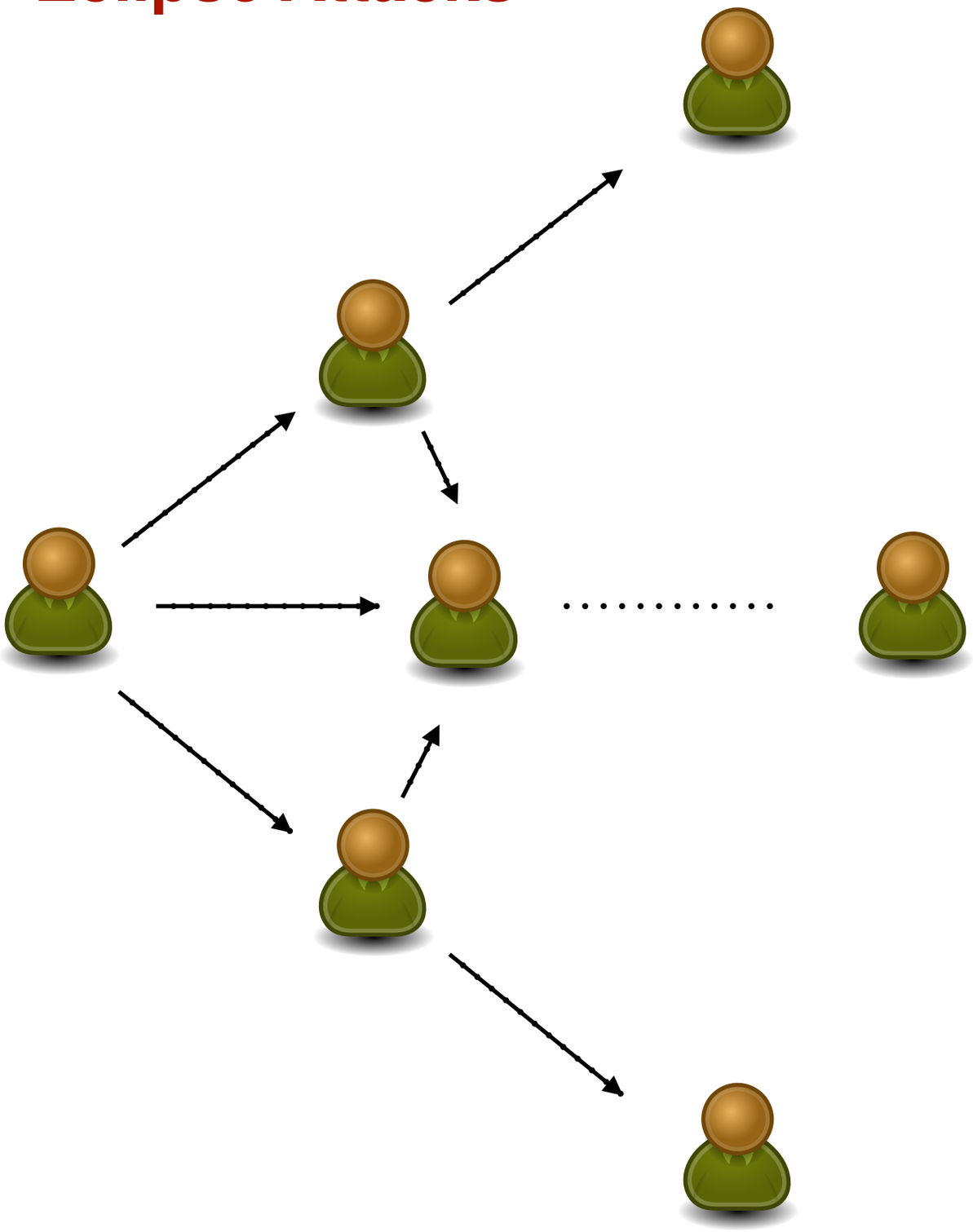
Eclipse Attacks



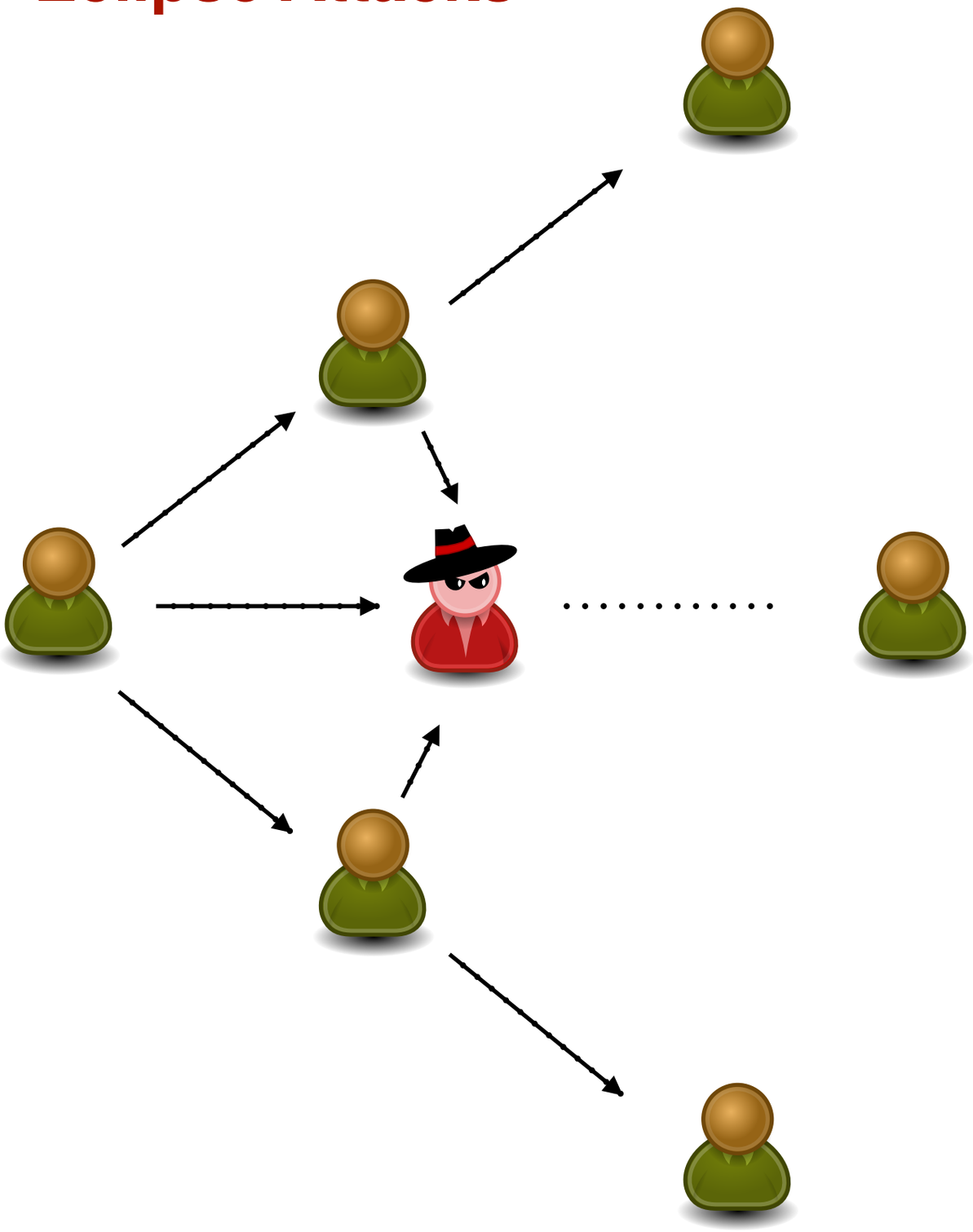
Eclipse Attacks



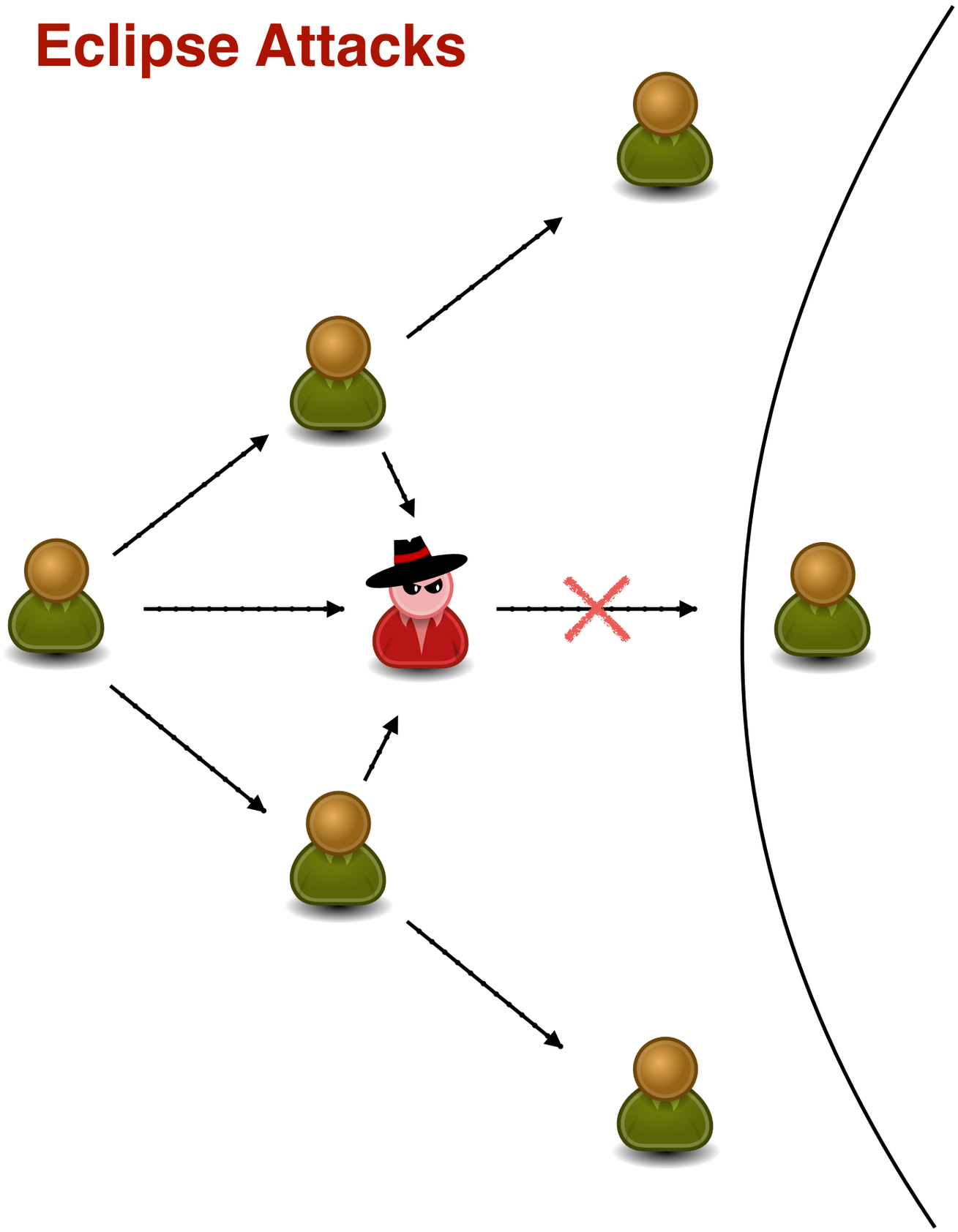
Eclipse Attacks



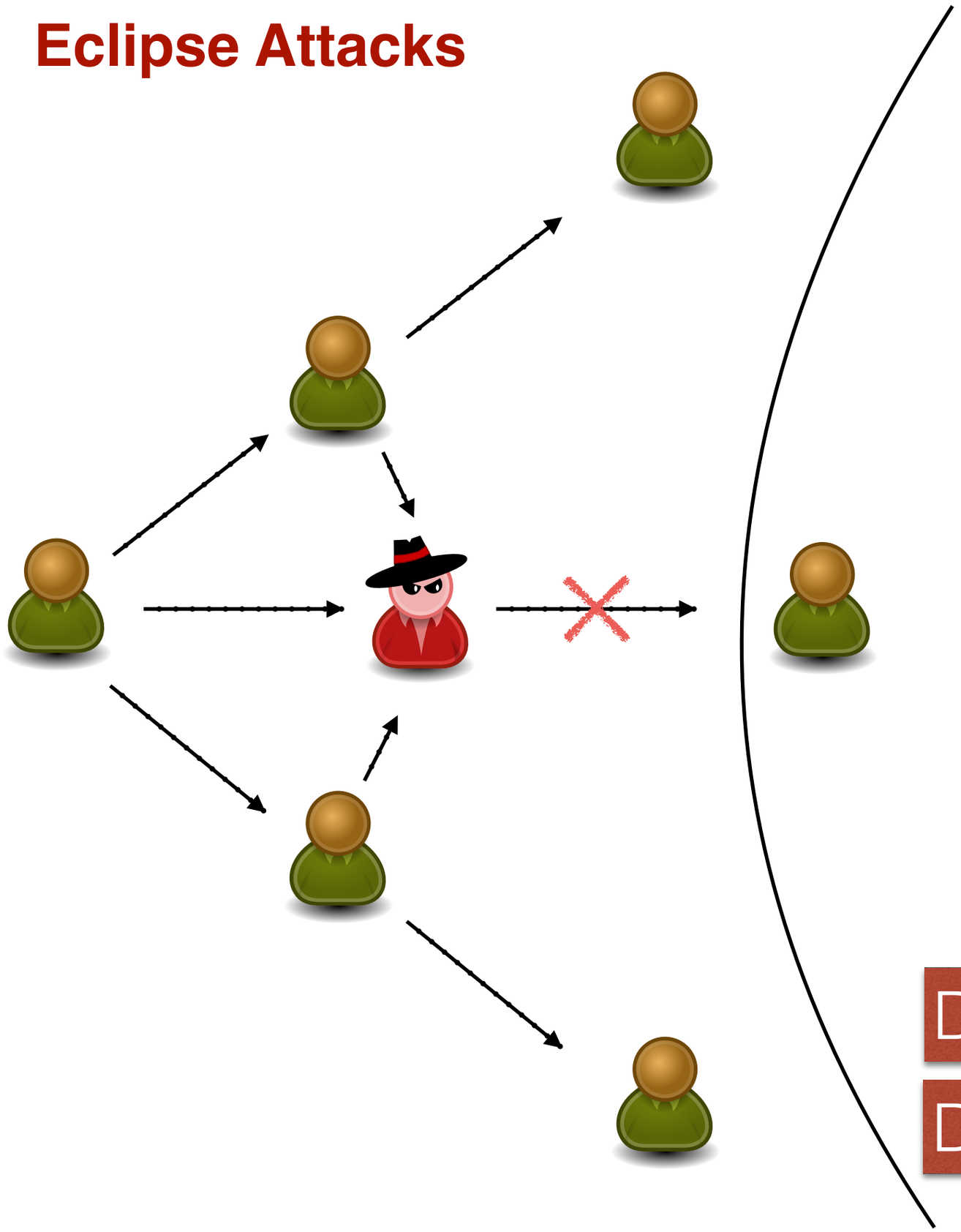
Eclipse Attacks



Eclipse Attacks



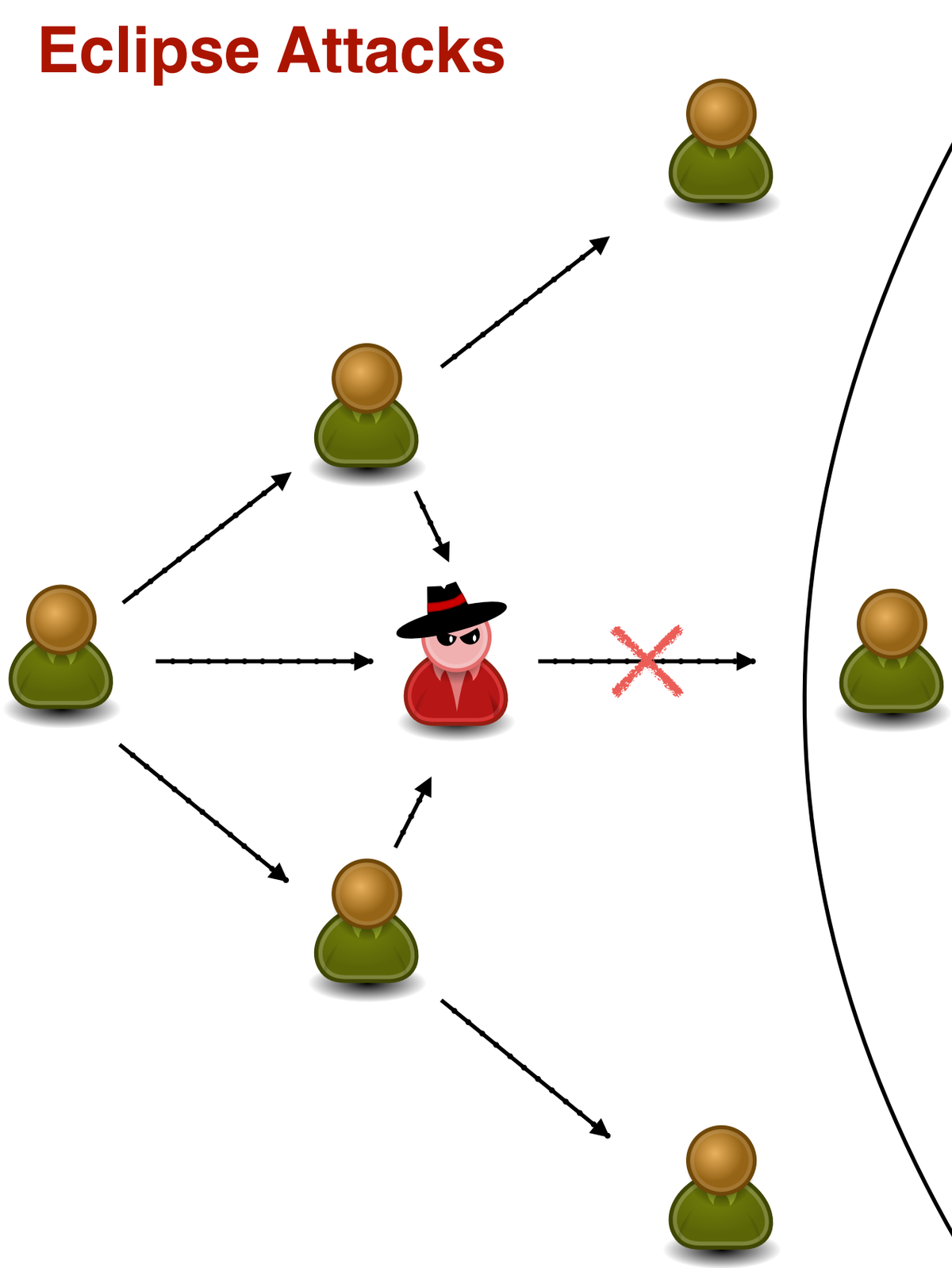
Eclipse Attacks



Denial of Service

Double Spending

Eclipse Attacks

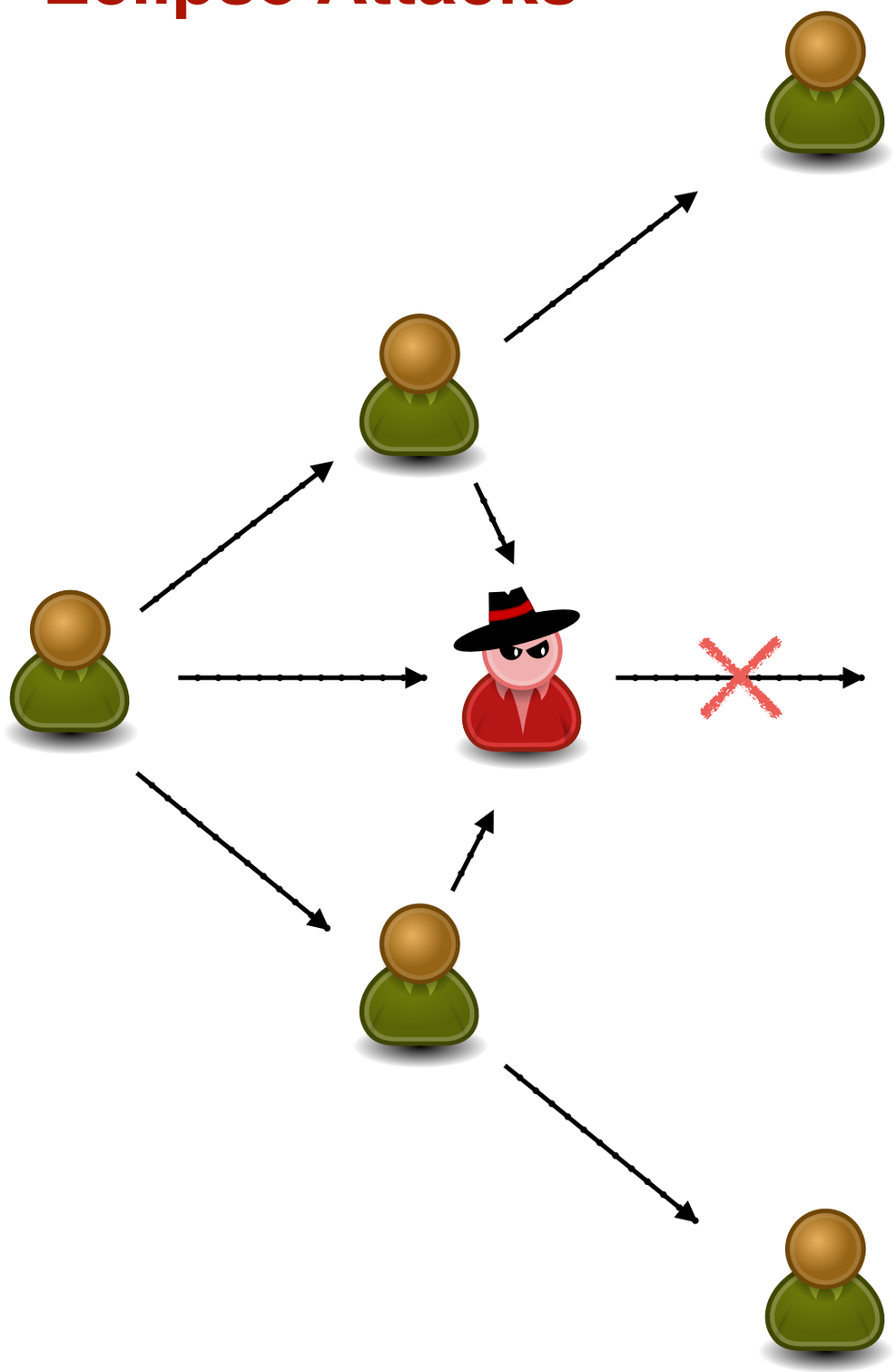


Eclipse attacks
Heilman et al., Usenix ’15

Denial of Service

Double Spending

Eclipse Attacks



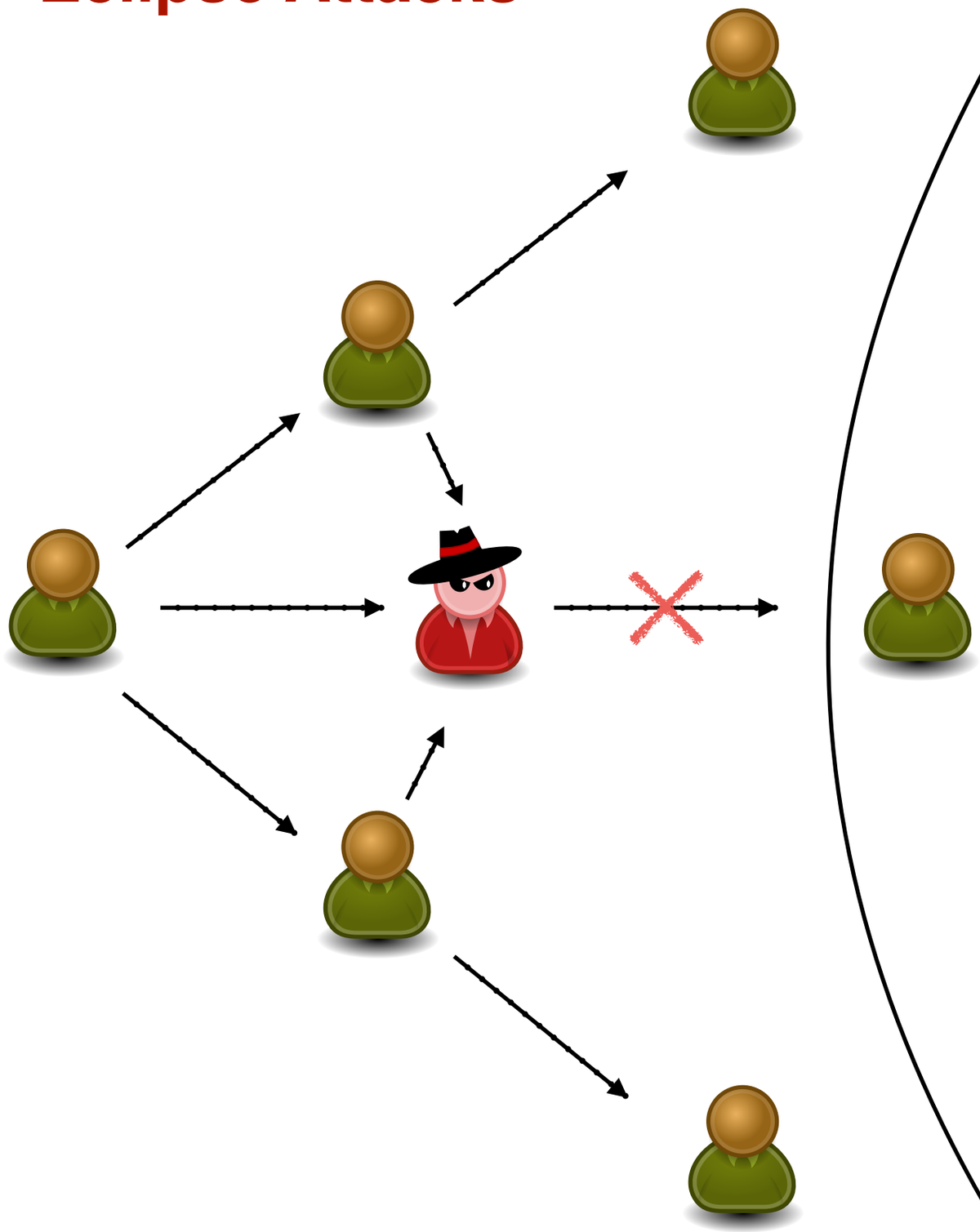
Eclipse attacks
Heilman et al., Usenix ’15

Monopolize connections
Spamming addresses
Forcing node restart
Requires many bots

Denial of Service

Double Spending

Eclipse Attacks



1 connection sufficient
No victim restart necessary

Eclipse attacks
Heilman et al., Usenix ’15

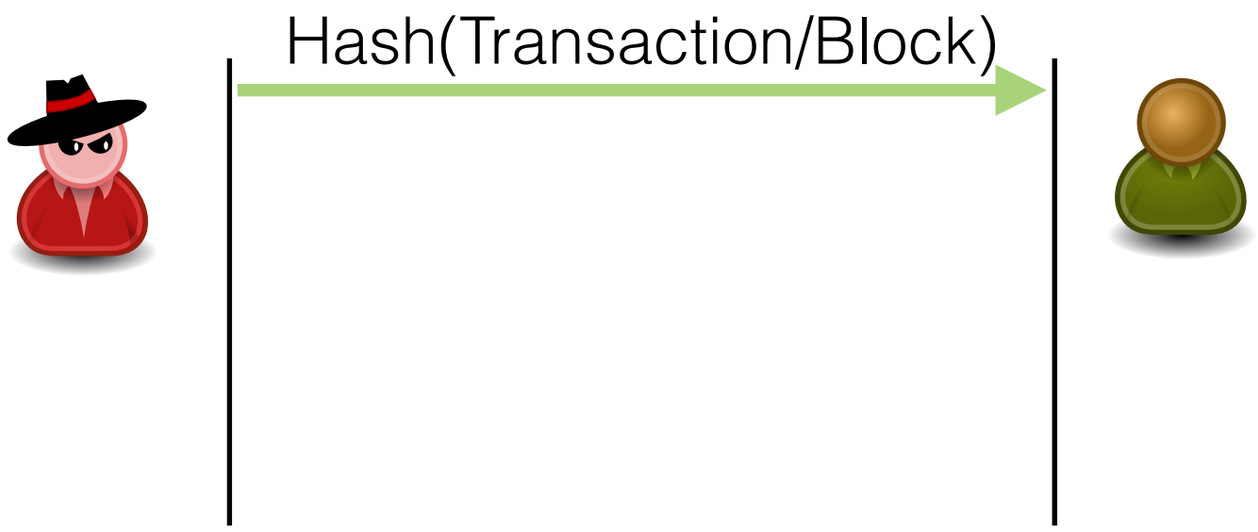
Monopolize connections
Spamming addresses
Forcing node restart
Requires many bots

Denial of Service

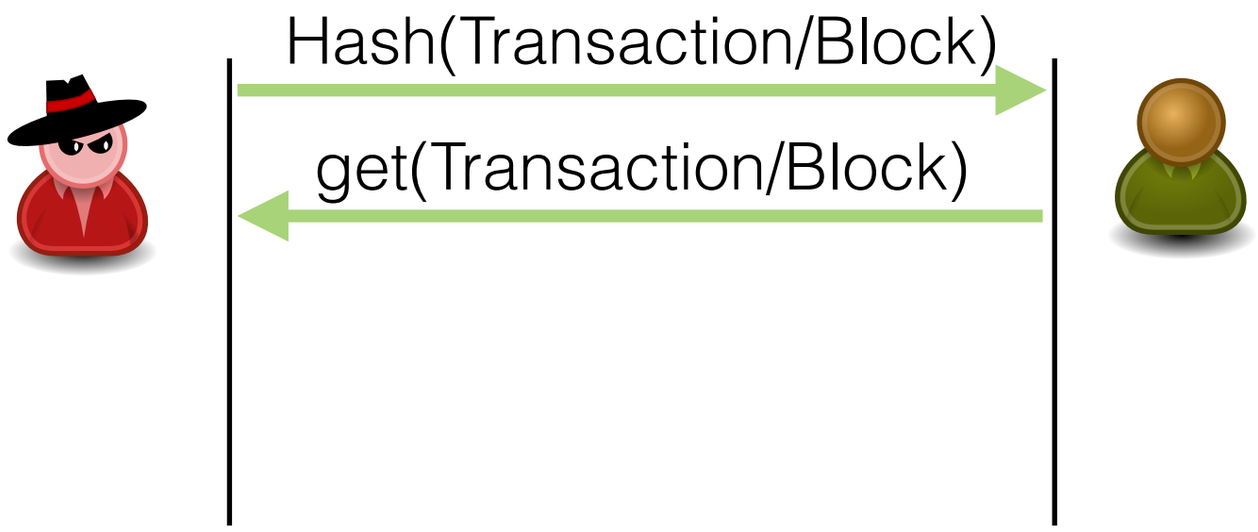
Double Spending

Request timeouts

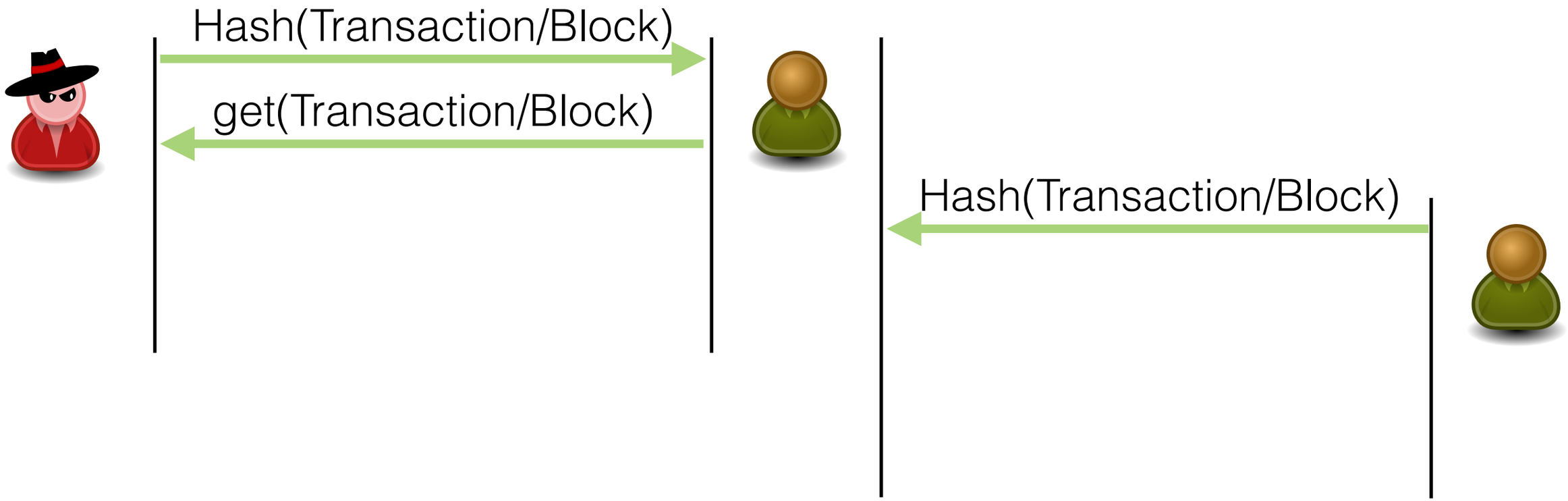
Request timeouts



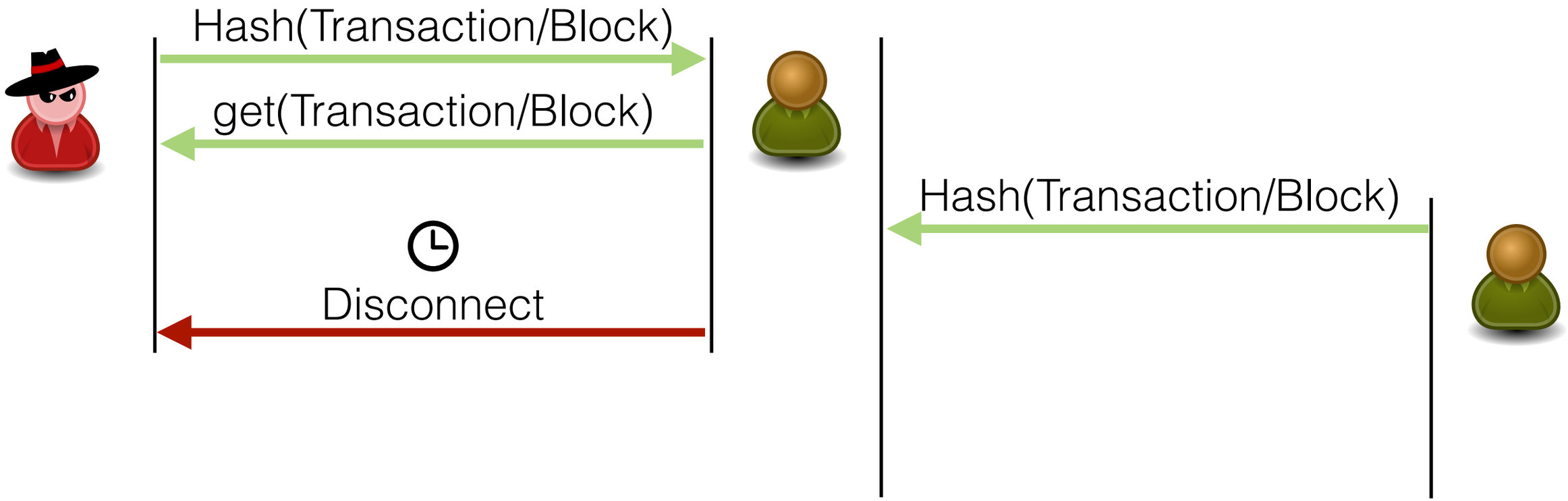
Request timeouts



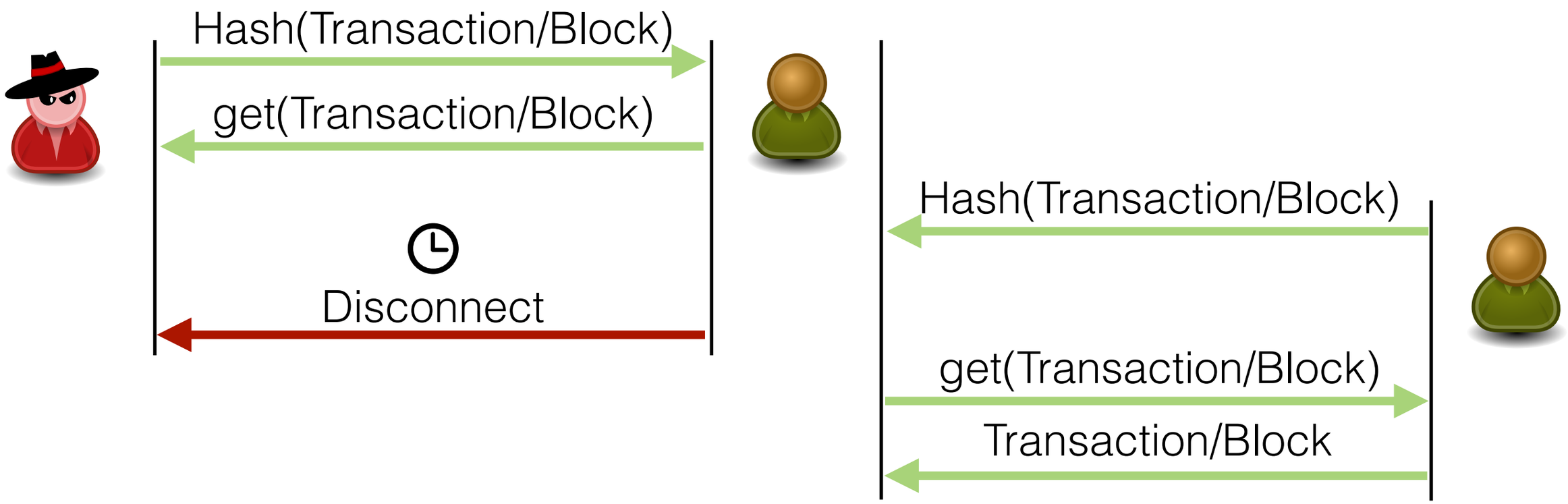
Request timeouts



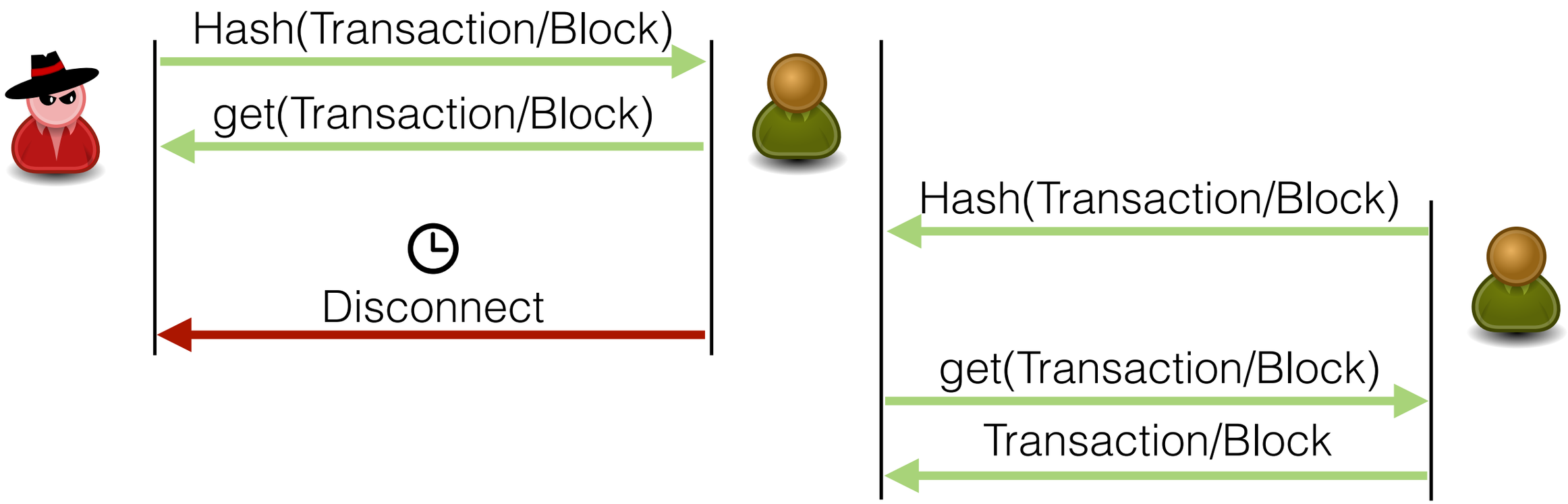
Request timeouts



Request timeouts



Request timeouts



Block timeout: 20 minutes
Transaction timeout: 2 minutes

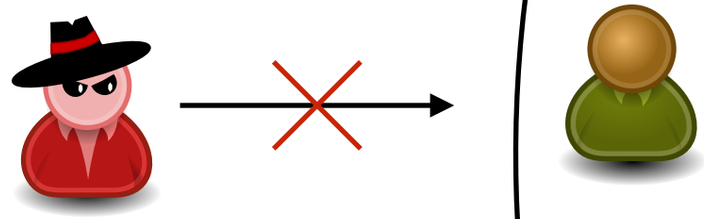
Implications

Adversary

- Blinds victim from blocks and transaction > 20 min
- Experimental validation

Impact

- **Double spend transactions**
- Aggravated selfish mining
- **Network wide Denial of Service**

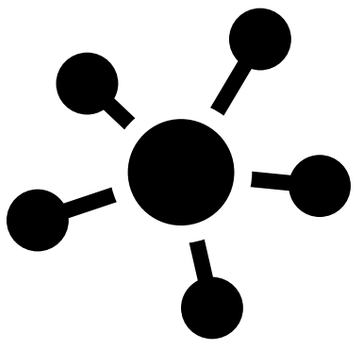


Mitigations

- **Hardening measures**
- Estimate waiting time for secure transactions

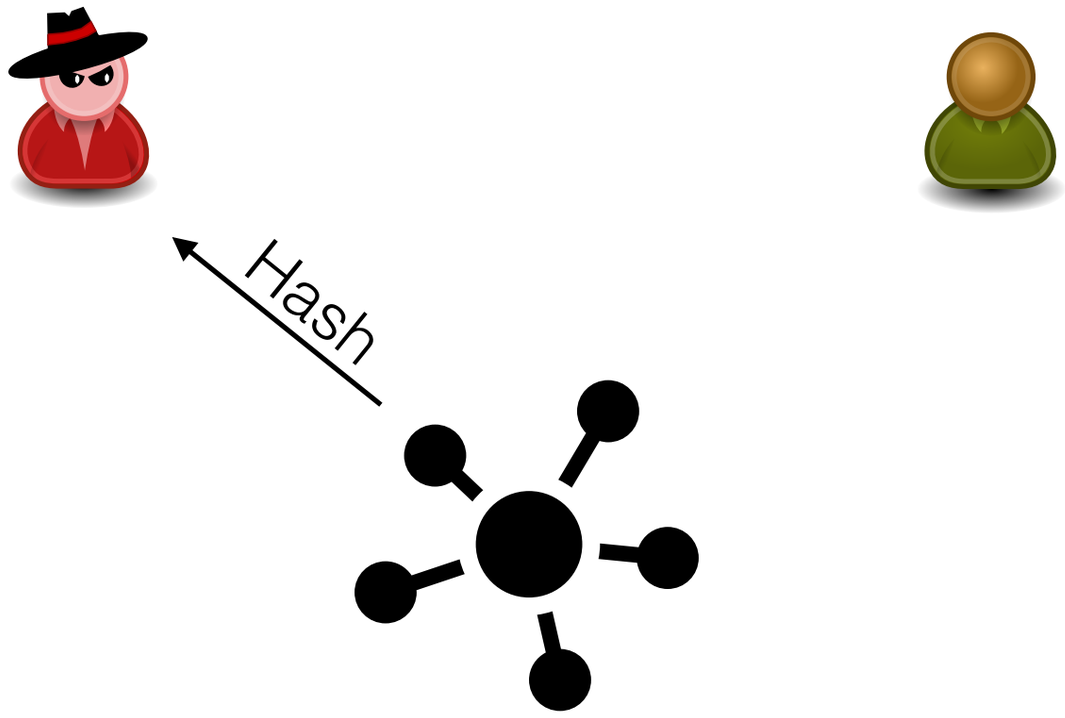
Necessary requirements

1. Must be **first** peer to advertise Transaction/Block



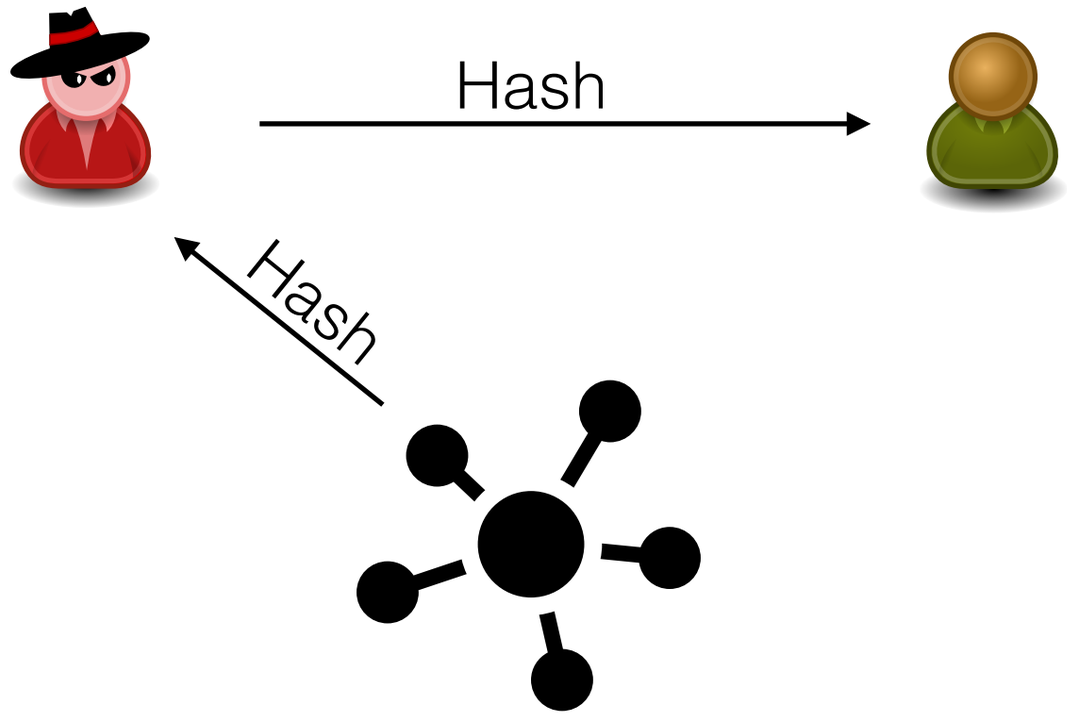
Necessary requirements

1. Must be **first** peer to advertise Transaction/Block



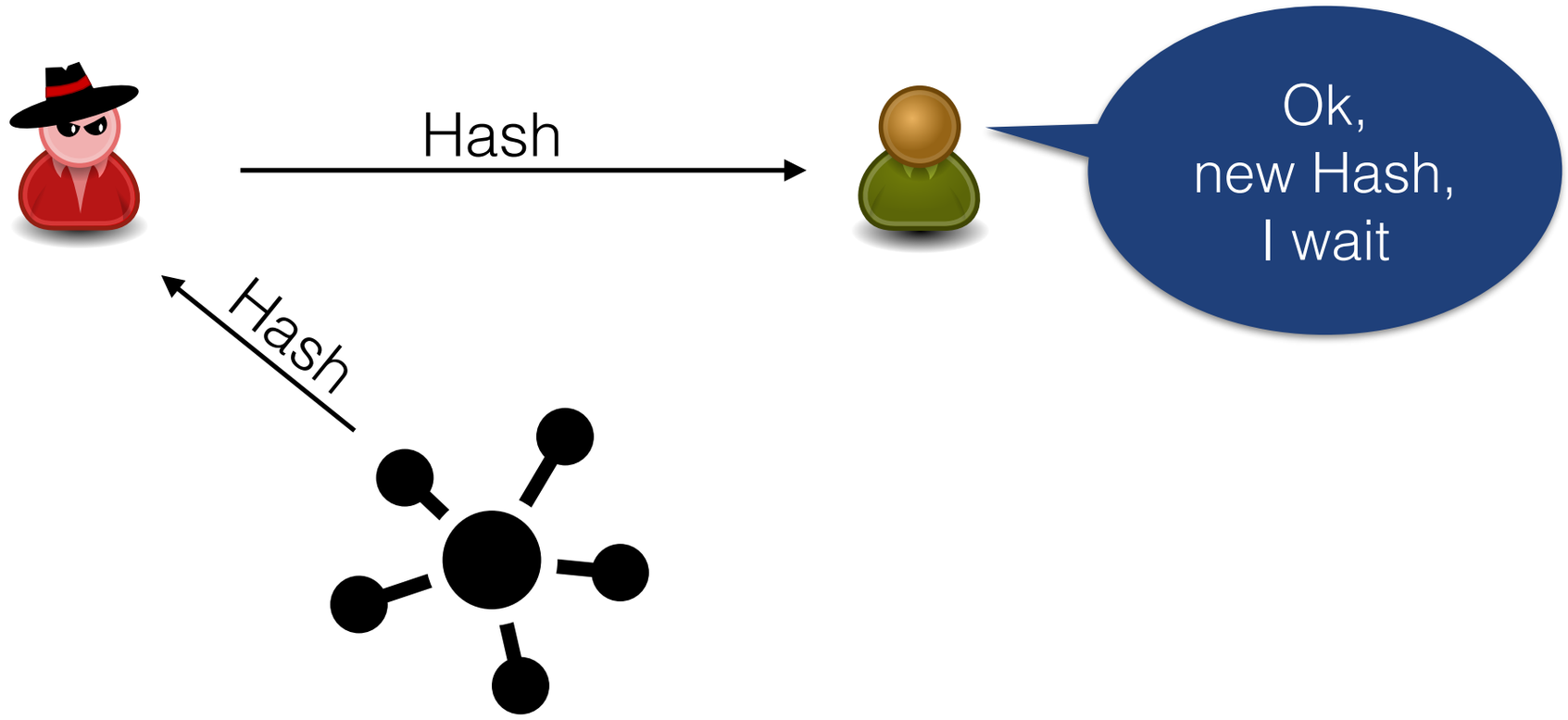
Necessary requirements

1. Must be **first** peer to advertise Transaction/Block



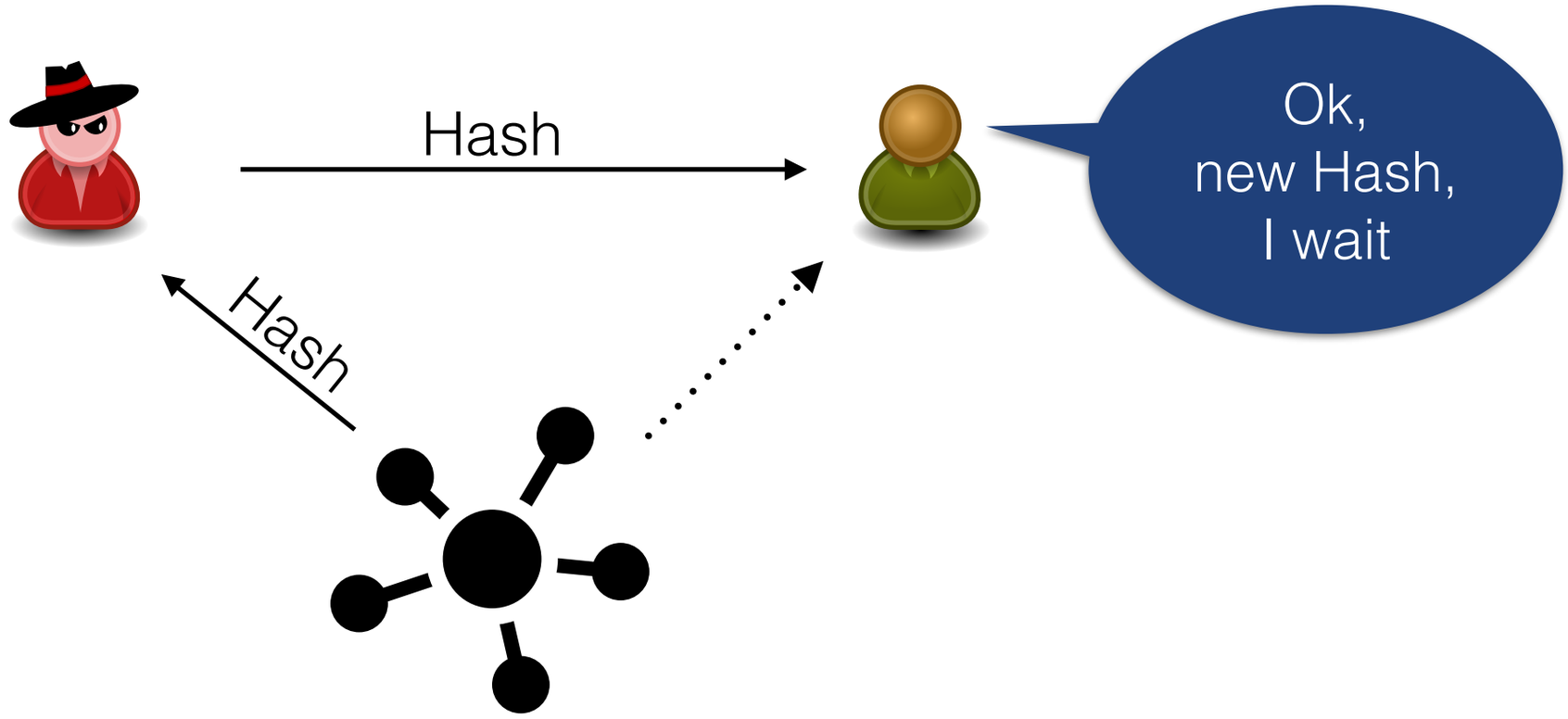
Necessary requirements

1. Must be **first** peer to advertise Transaction/Block



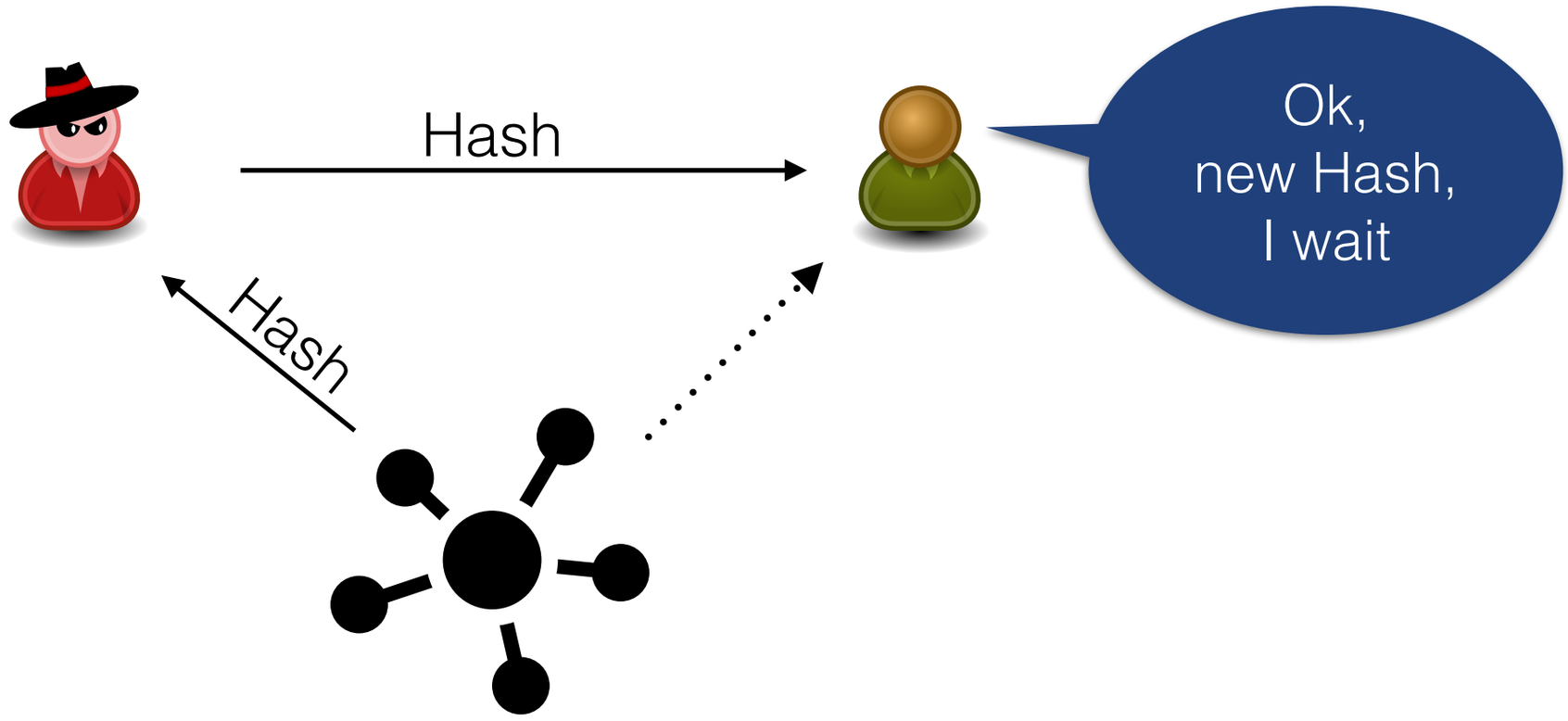
Necessary requirements

1. Must be **first** peer to advertise Transaction/Block



Necessary requirements

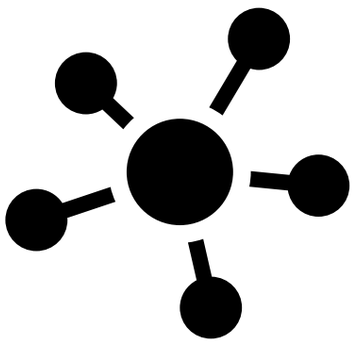
1. Must be **first** peer to advertise Transaction/Block



2. Victim should wait
   - Block timeout: 20 minutes
   - Transaction timeout: 2 minutes

Being First

Zurich



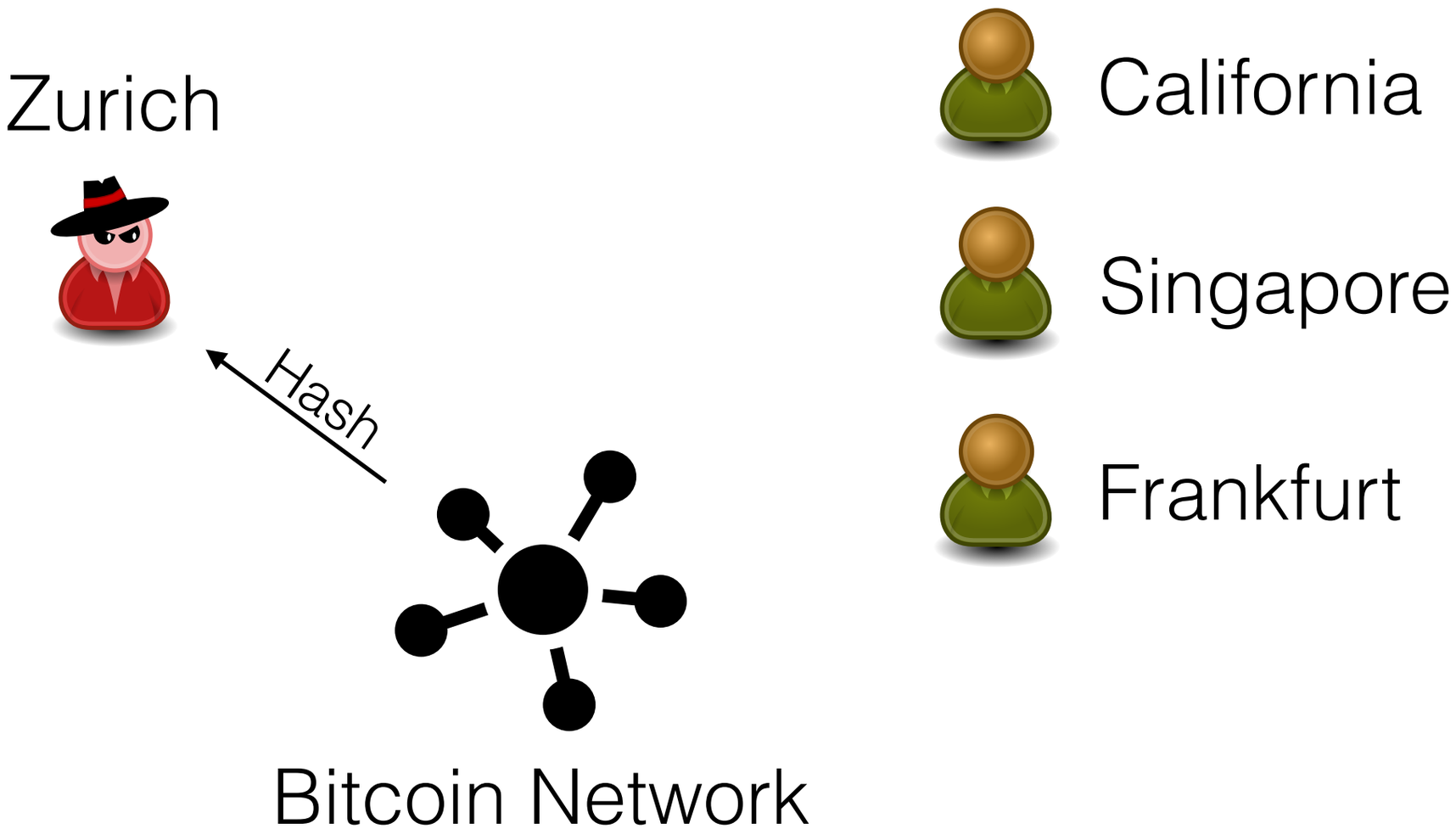
Bitcoin Network

California

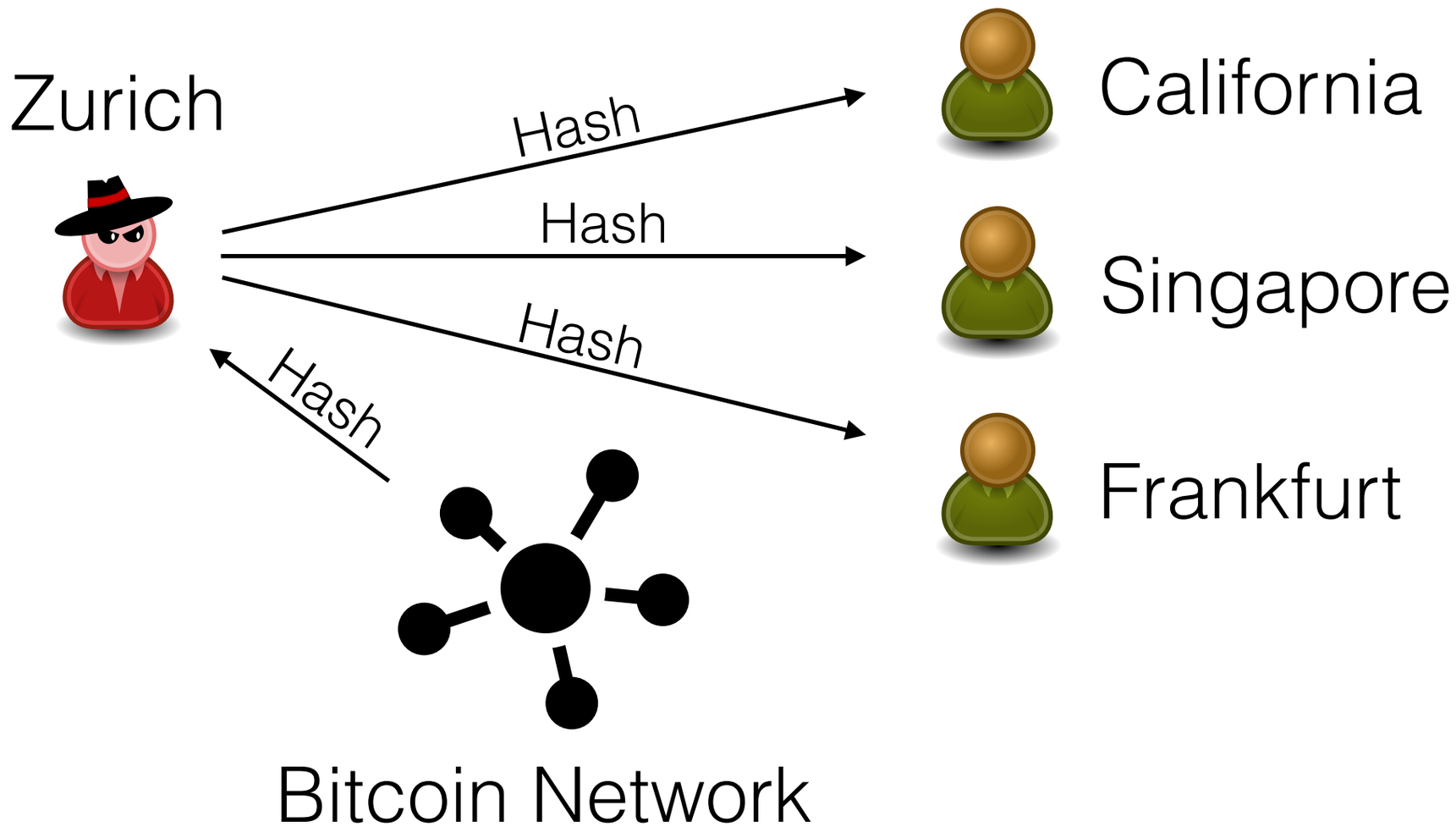
Singapore

Frankfurt

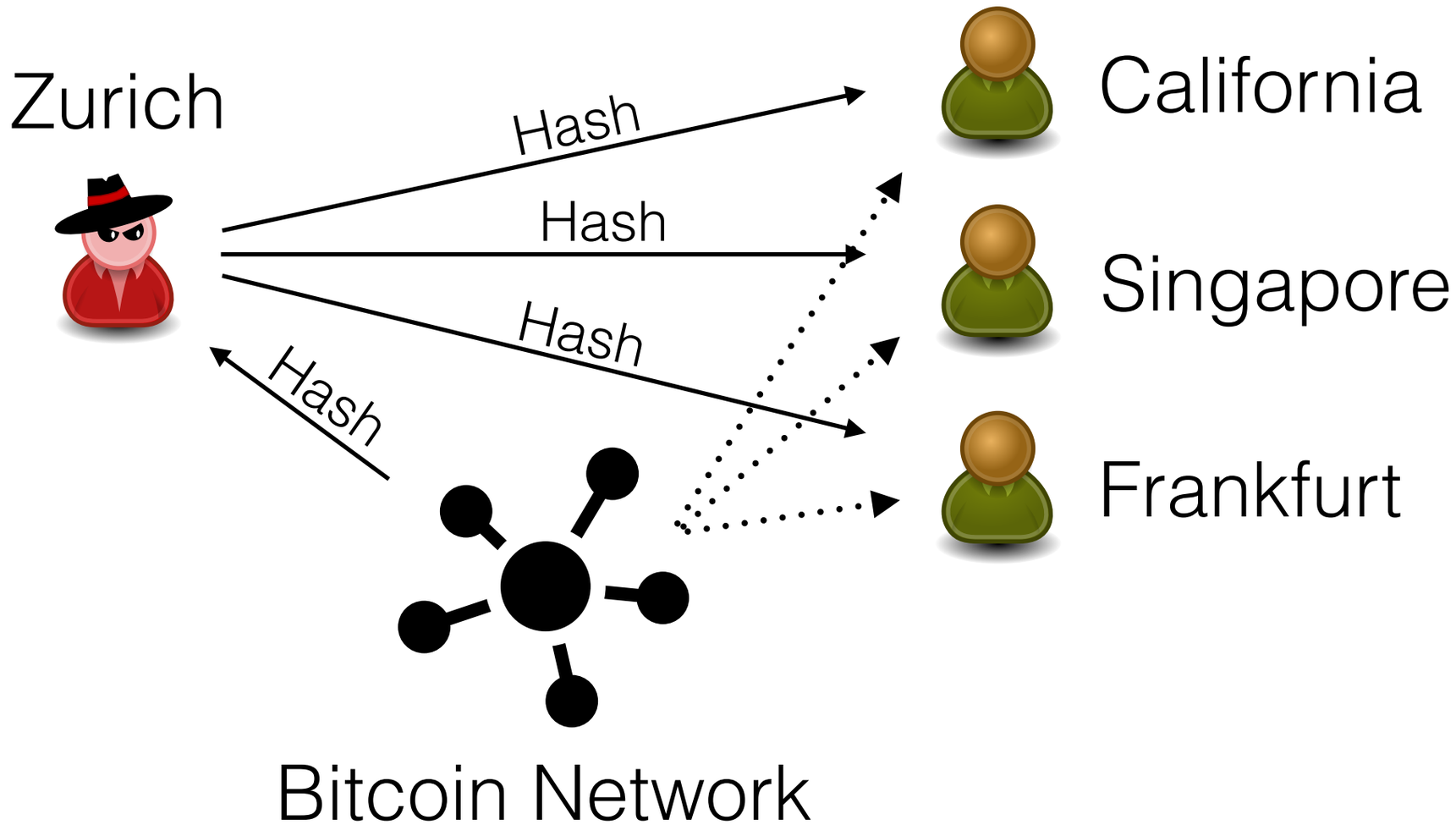
Being First


Zurich
Hash
Bitcoin Network
California
Singapore
Frankfurt

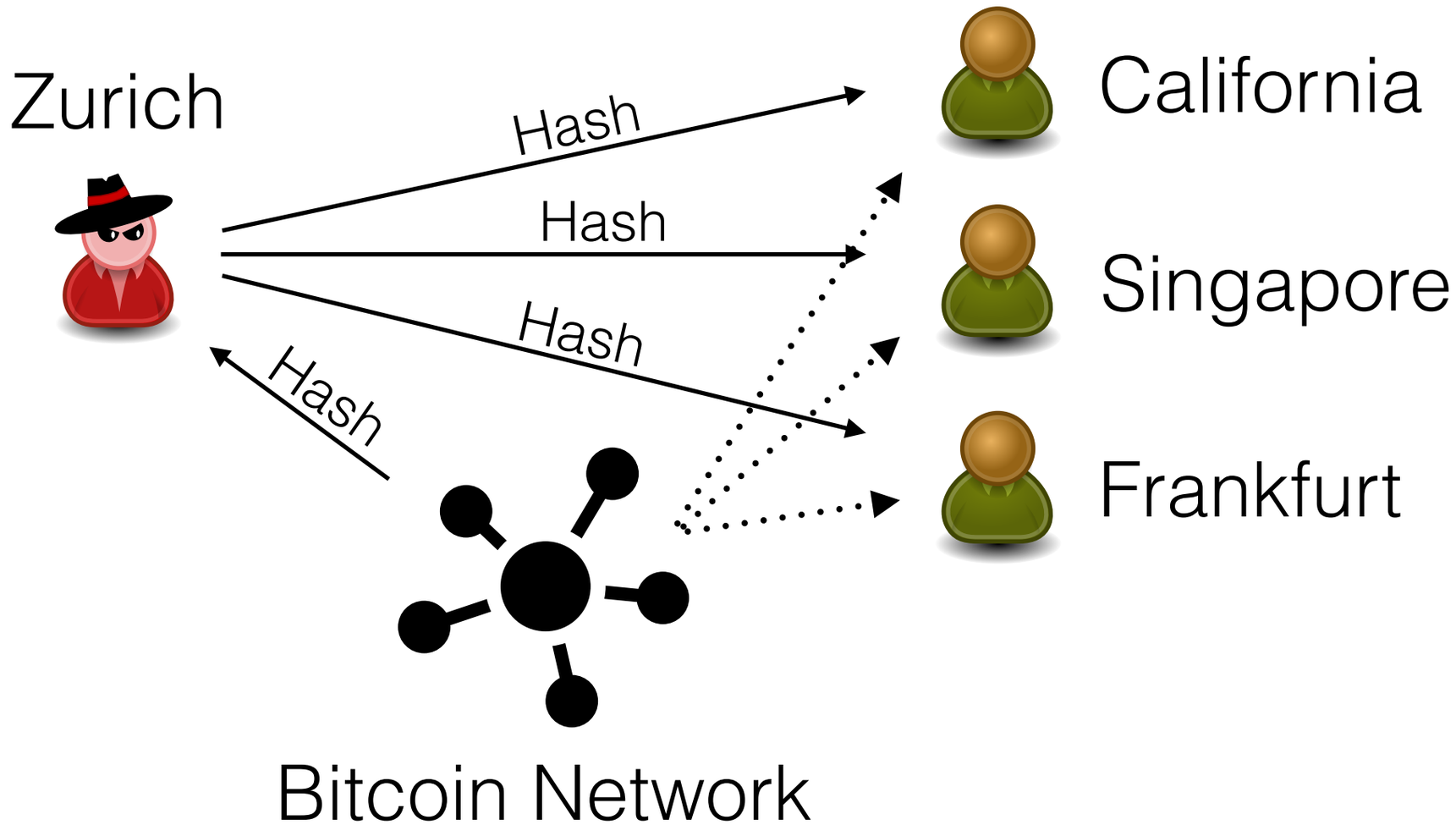
Being First


Zurich
Hash
Hash
Hash
Hash
California
Singapore
Frankfurt
Bitcoin Network

Being First


Zurich
Hash
Hash
Hash
Hash
California
Singapore
Frankfurt
Bitcoin Network

Being First



Connections of Adversary	40	80	200	800
Connections of Victim	40	40	40	40
Average success in being first	0.44± 0.14	0.57± 0.20	0.80± 0.14	**0.89± 0.07**

Waiting

Transactions

- After 2 minutes request from other peer (FIFO)

Waiting

Transactions

- After 2 minutes request from other peer (FIFO)

FIFO queue

Waiting

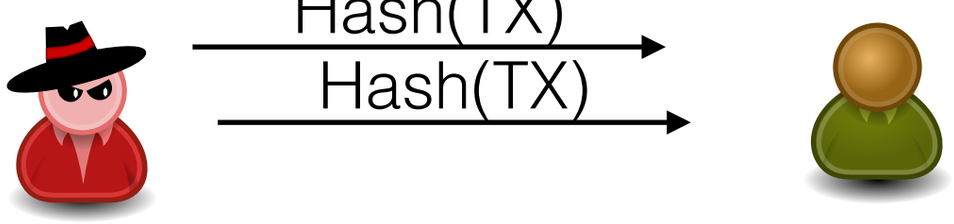
Transactions

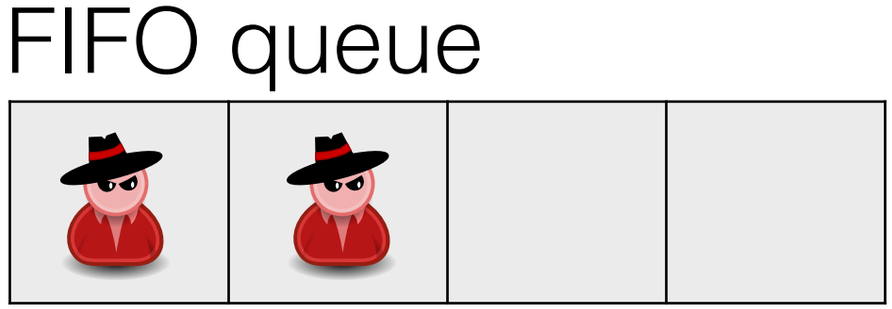
- After 2 minutes request from other peer (FIFO)

Waiting

Transactions

- After 2 minutes request from other peer (FIFO)

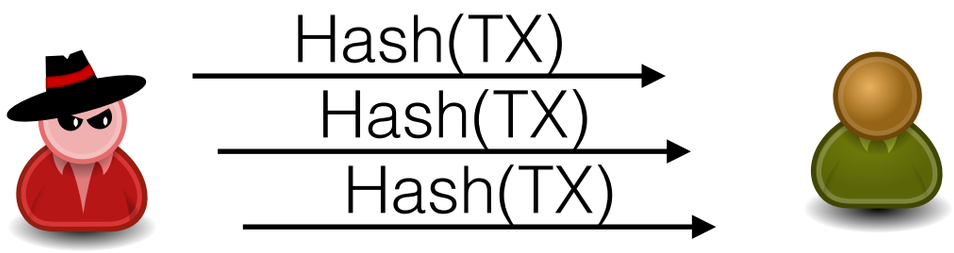


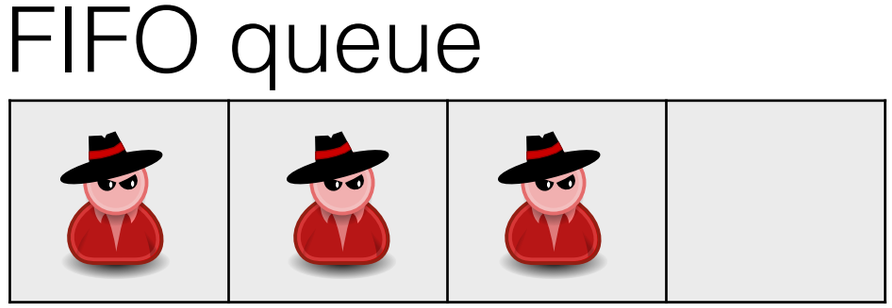


Waiting

Transactions

- After 2 minutes request from other peer (FIFO)

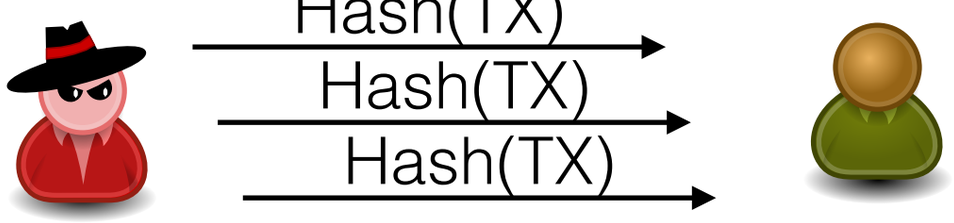


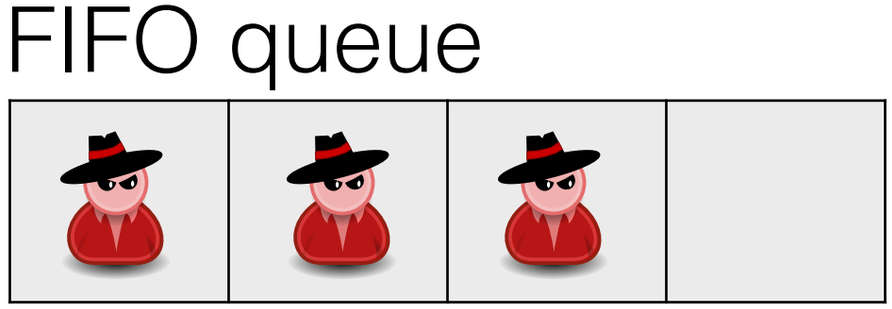


Waiting

Transactions

- After 2 minutes request from other peer (FIFO)

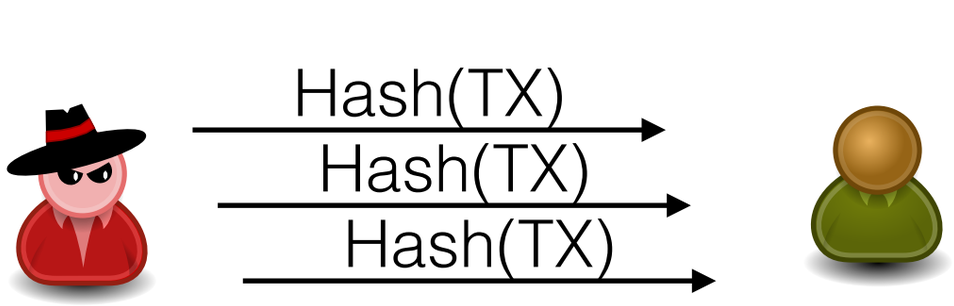


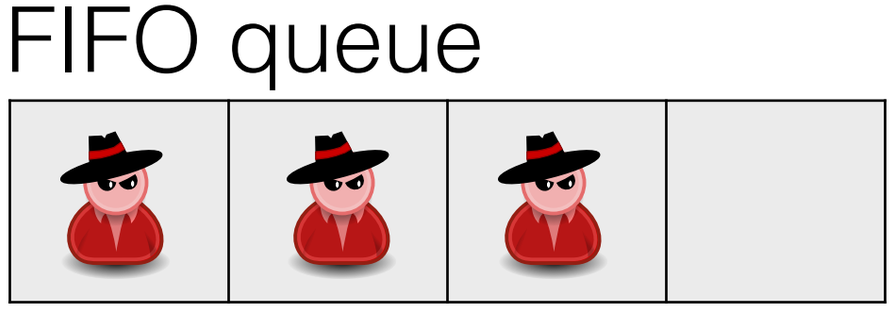


Waiting

Transactions

- After 2 minutes request from other peer (FIFO)





Blocks

- After 20 minutes disconnect and do nothing
- If received header, disconnect and request block from another peer