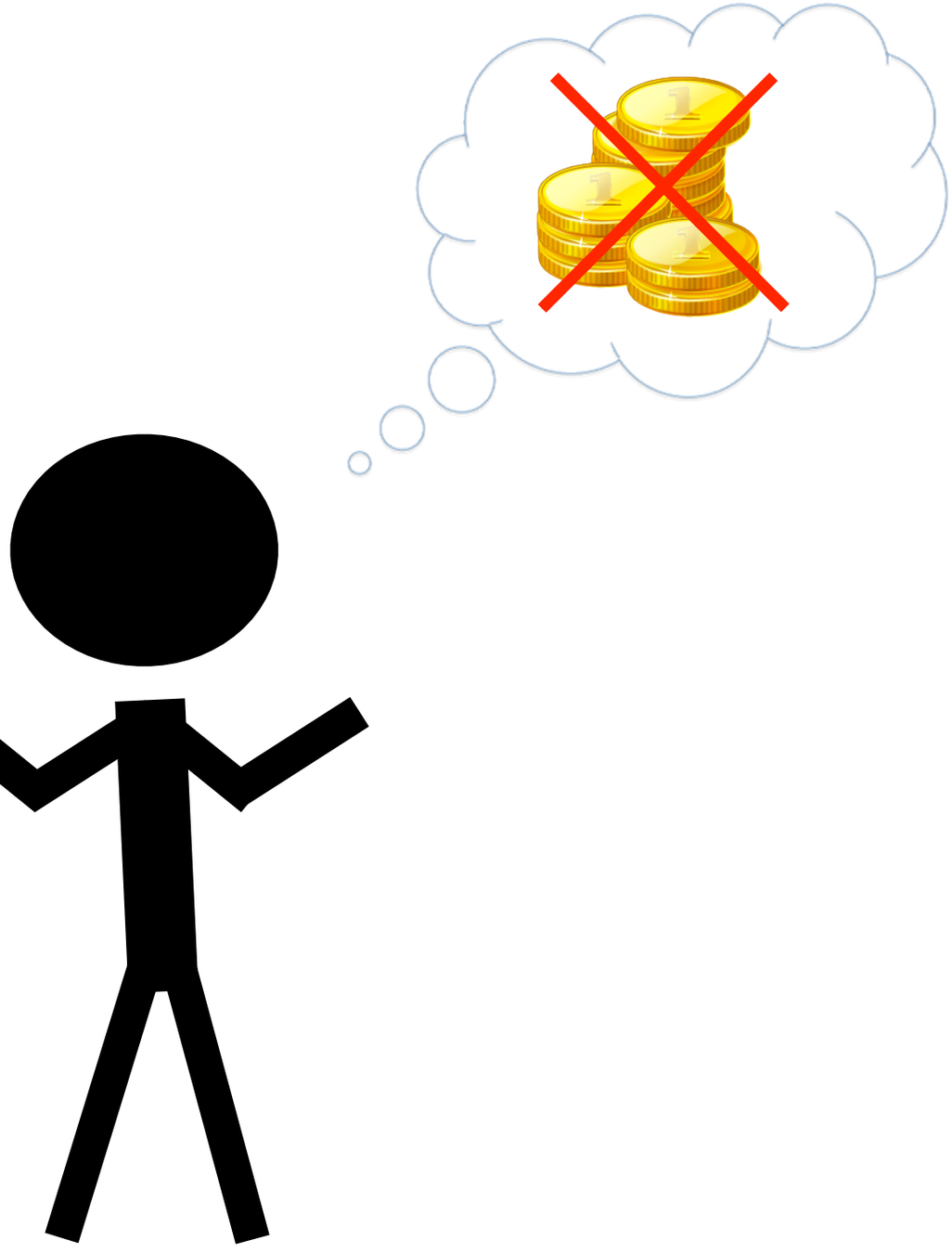
Have a Snack, Pay with Bitcoin

Tobias Bamert

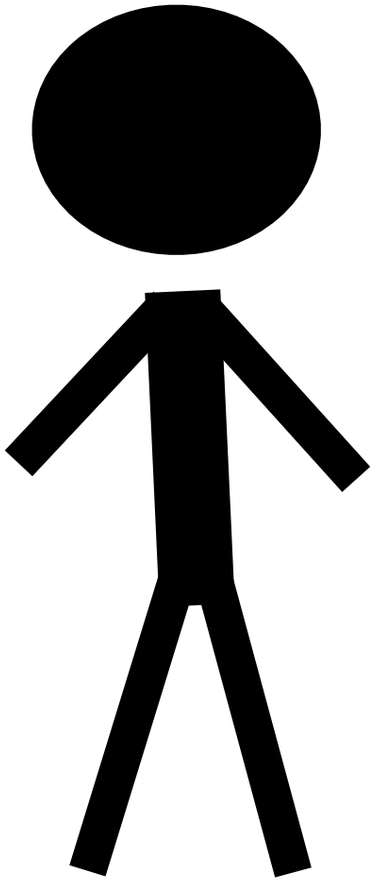
Distributed Computing, TIK, ETH Zürich

Vending Machine

Vending Machine



Vending Machine



Vending Machine

Advantages

- Funds directly transferred to merchant
- Centralized
- Small transaction fees

Confirmation Time

- Transactions instantly visible
- Confirmed at irregular intervals
- Approximately 10 minutes

Fast Payment

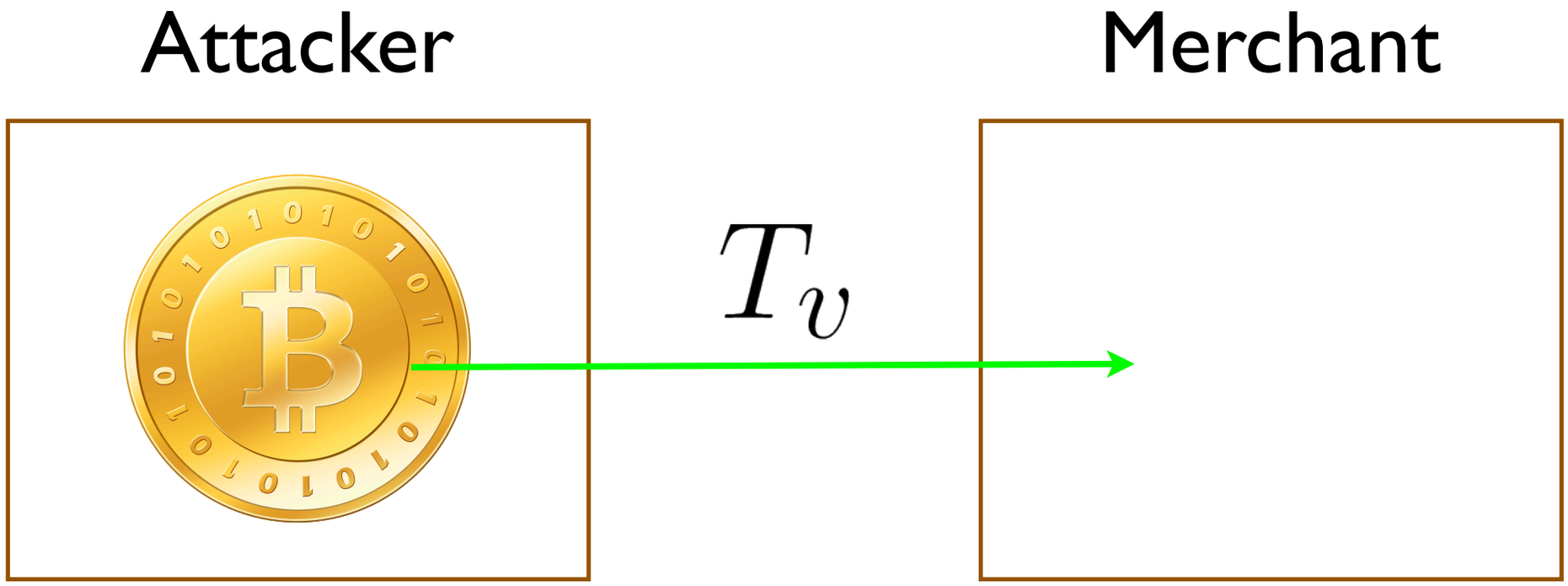
- Trust unconfirmed transaction
- Hedge against loss

Double Spend

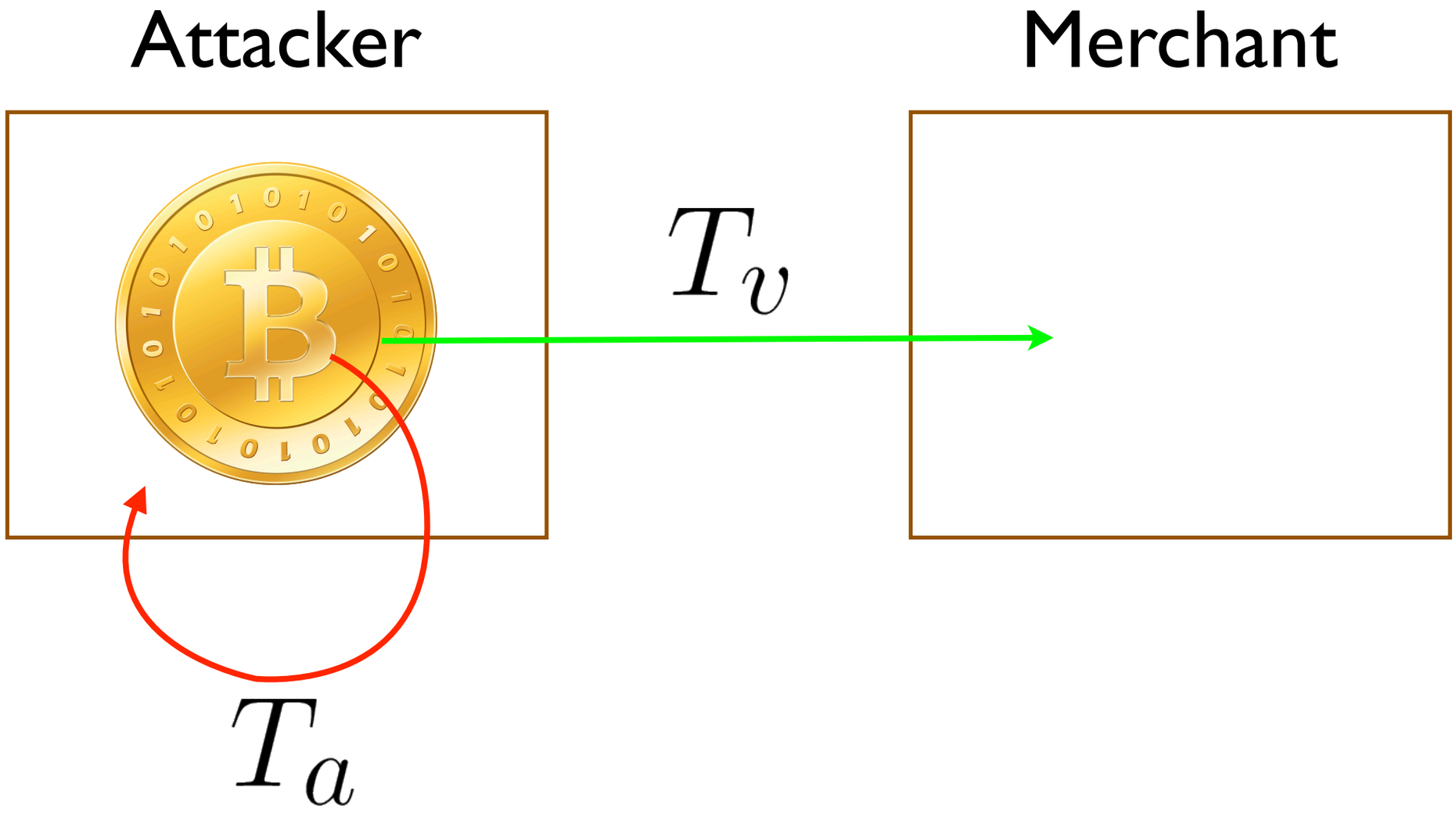
Attacker

Merchant

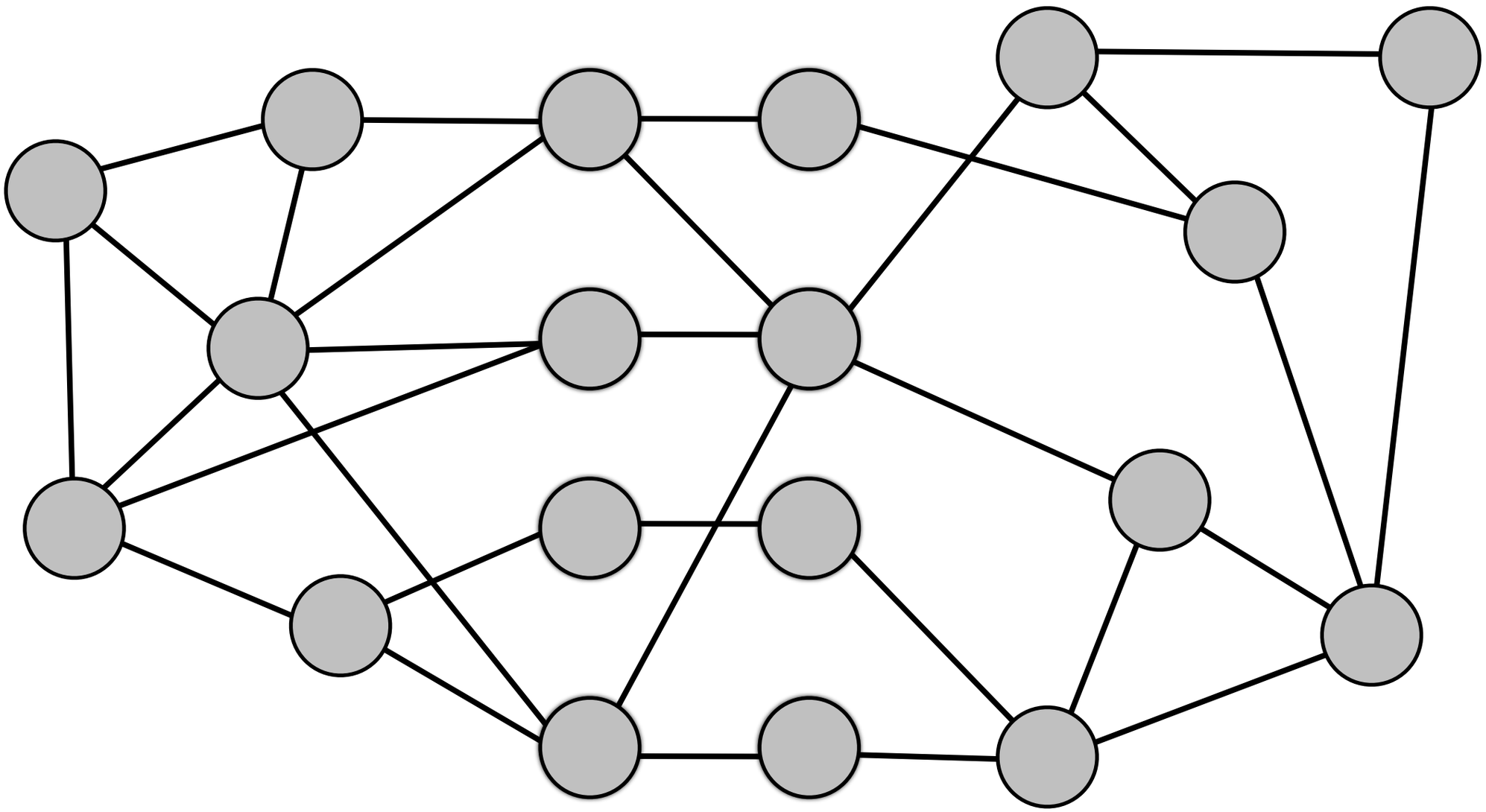
Double Spend



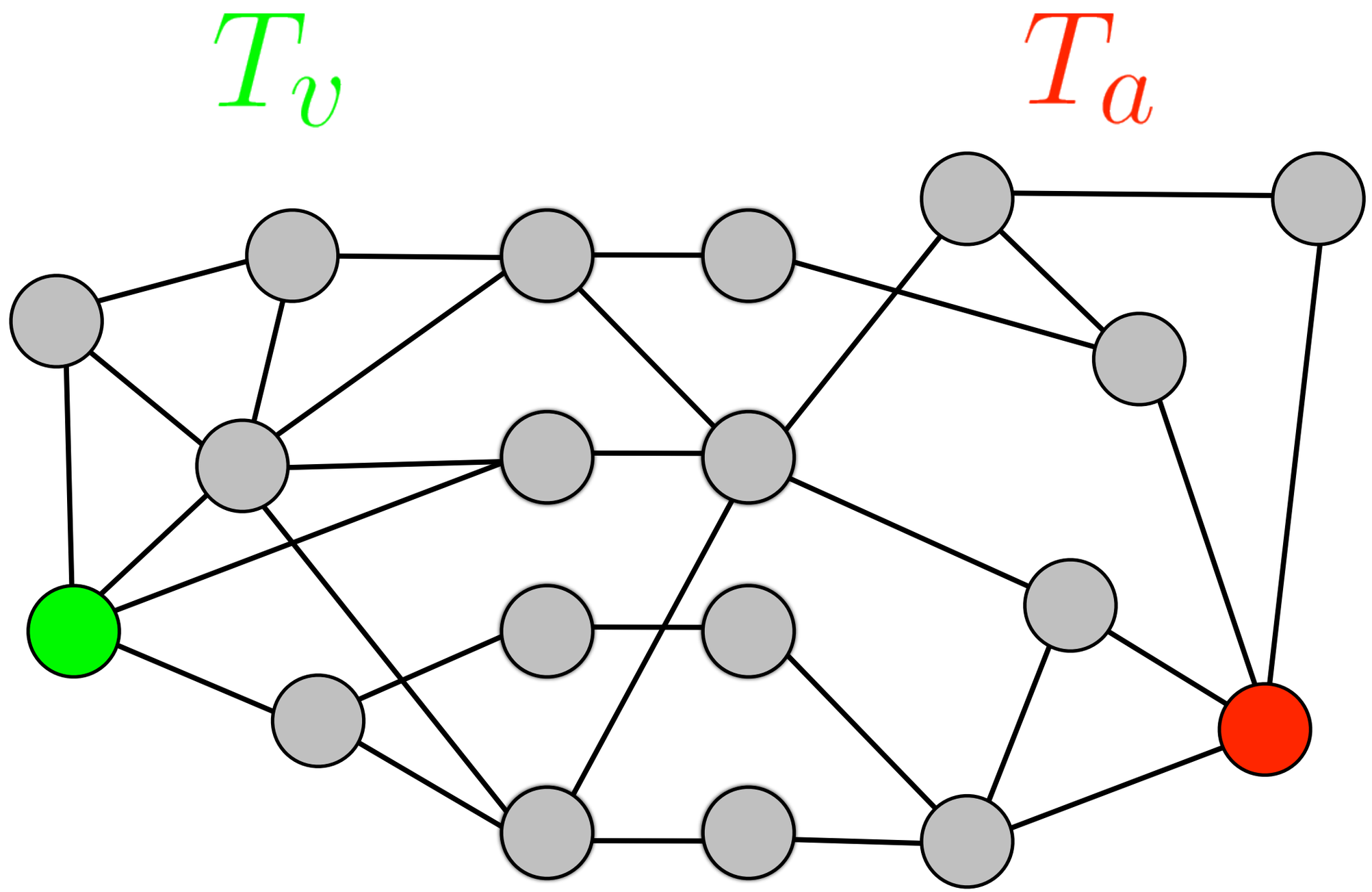
Double Spend



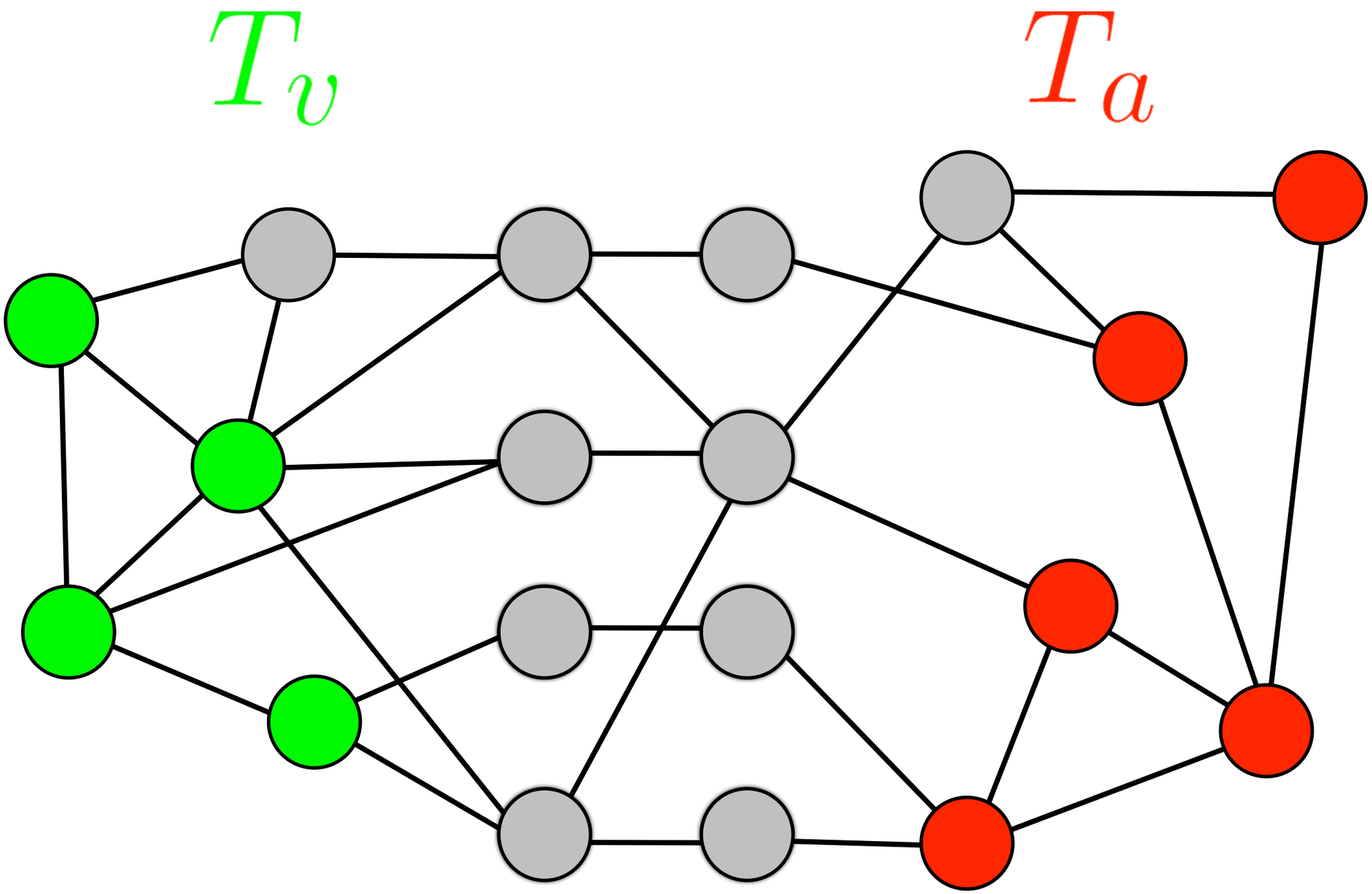
Double Spend



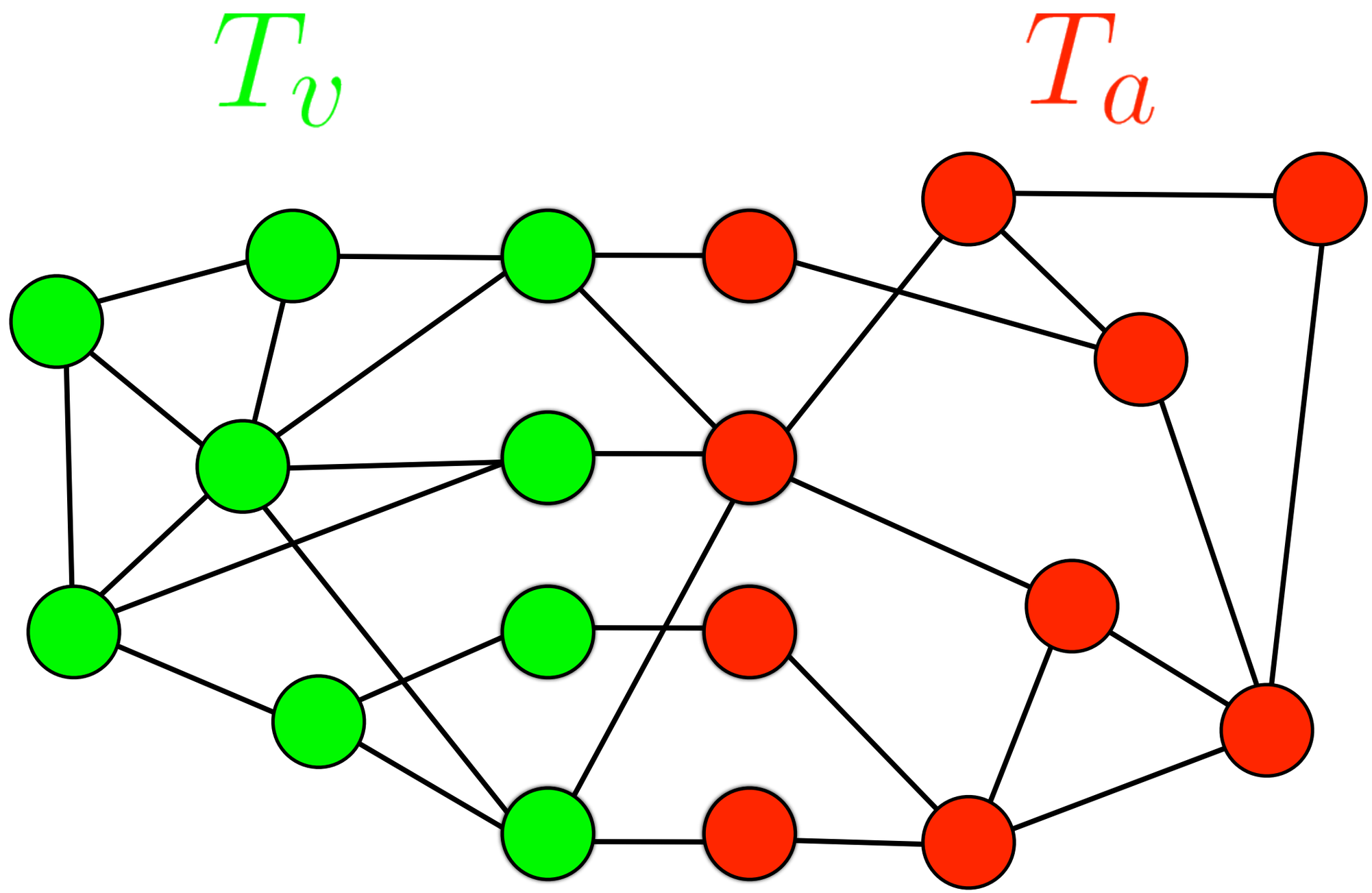
Double Spend



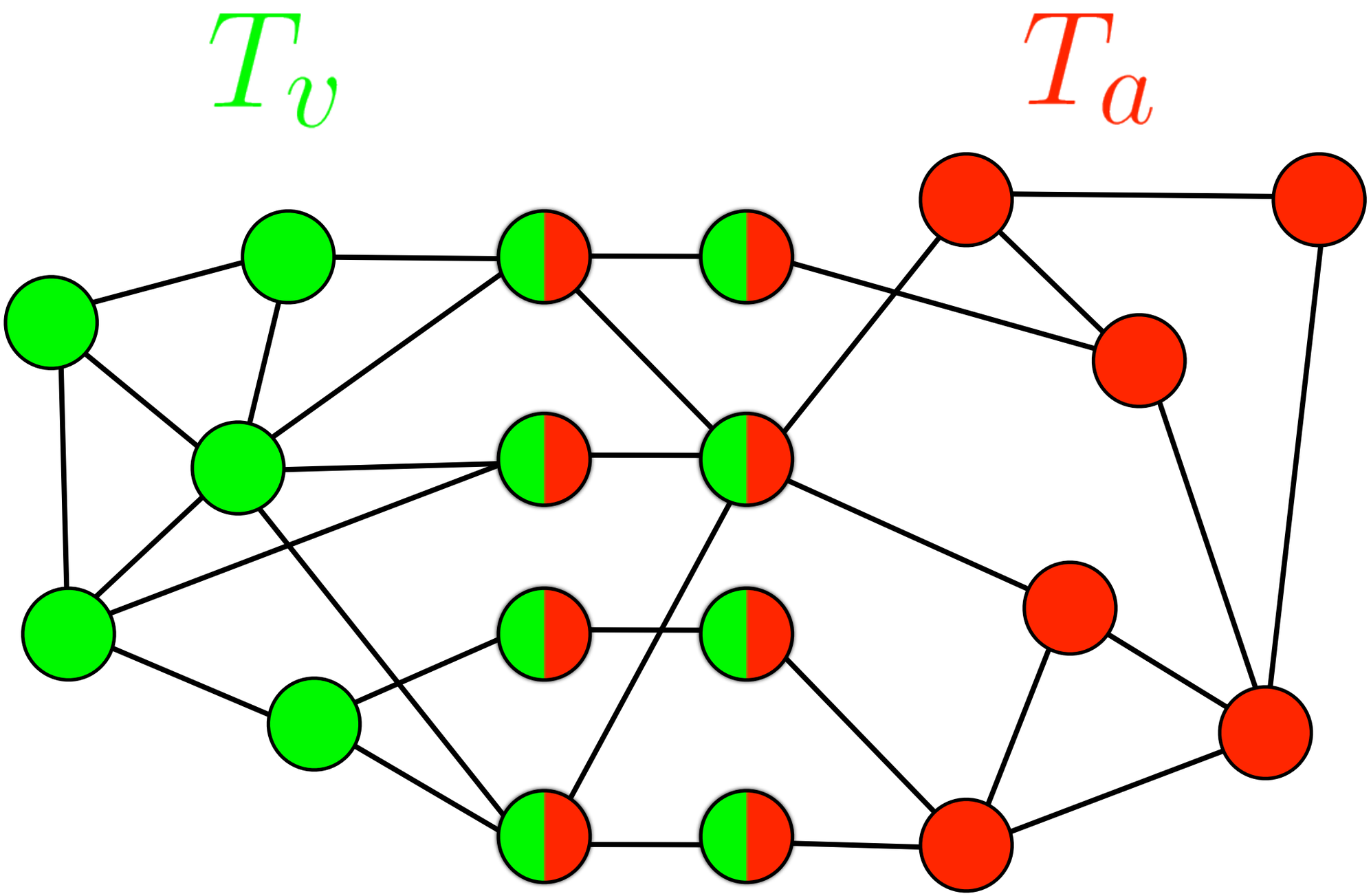
Double Spend



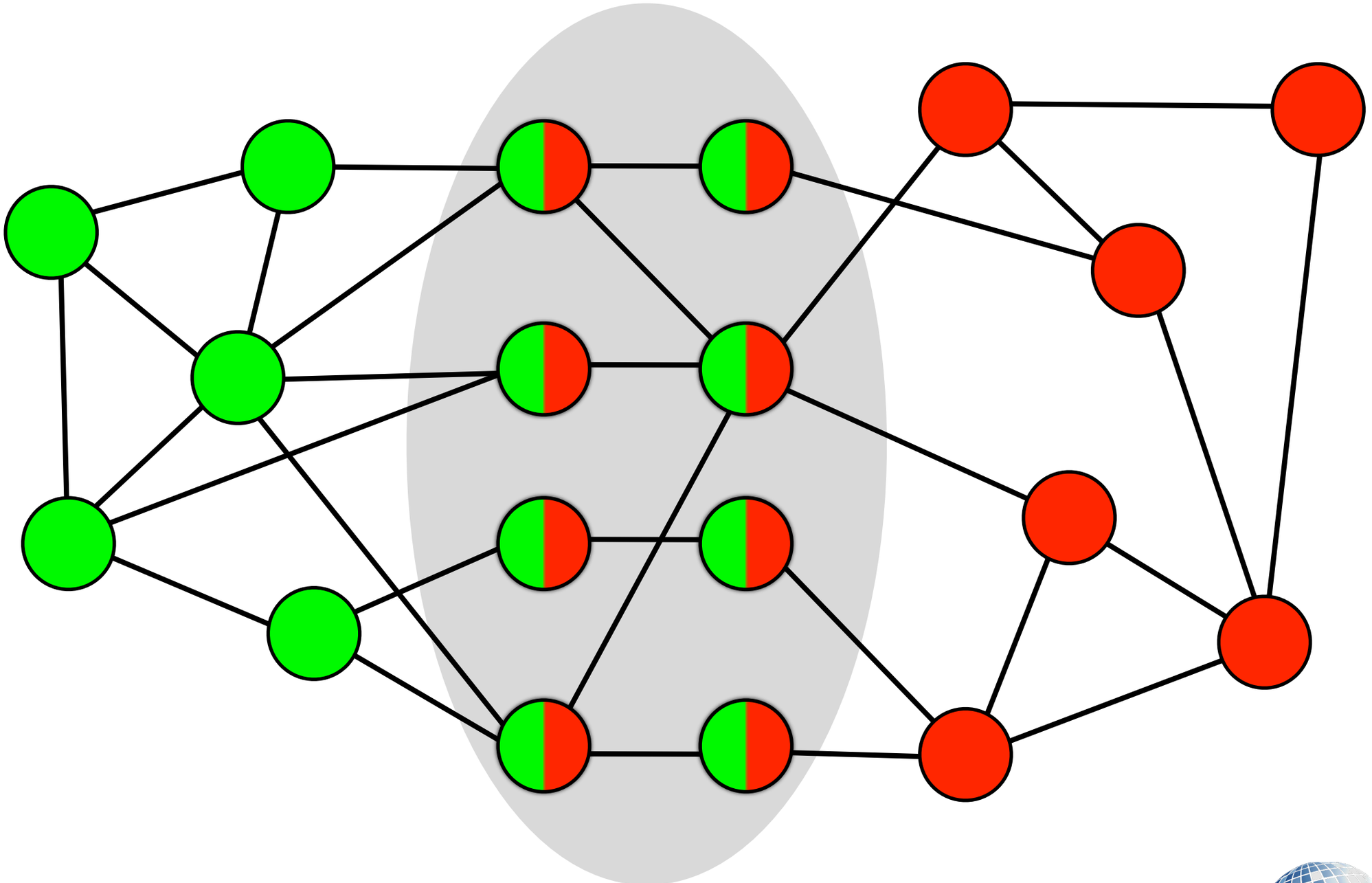
Double Spend



Double Spend

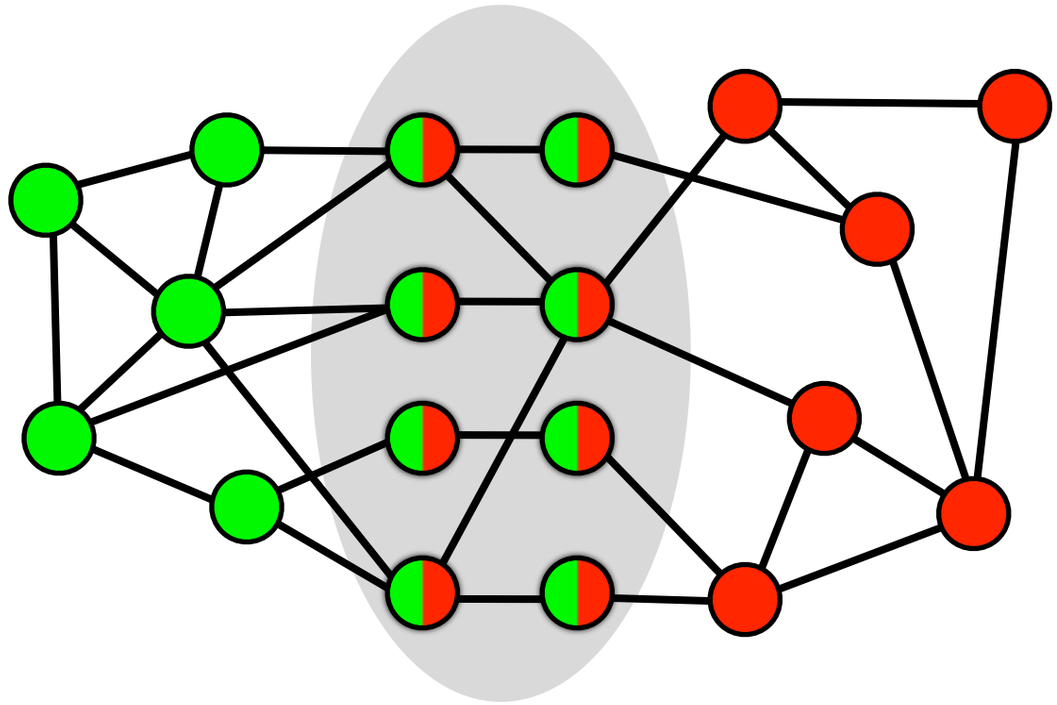


Countermeasures



Countermeasures

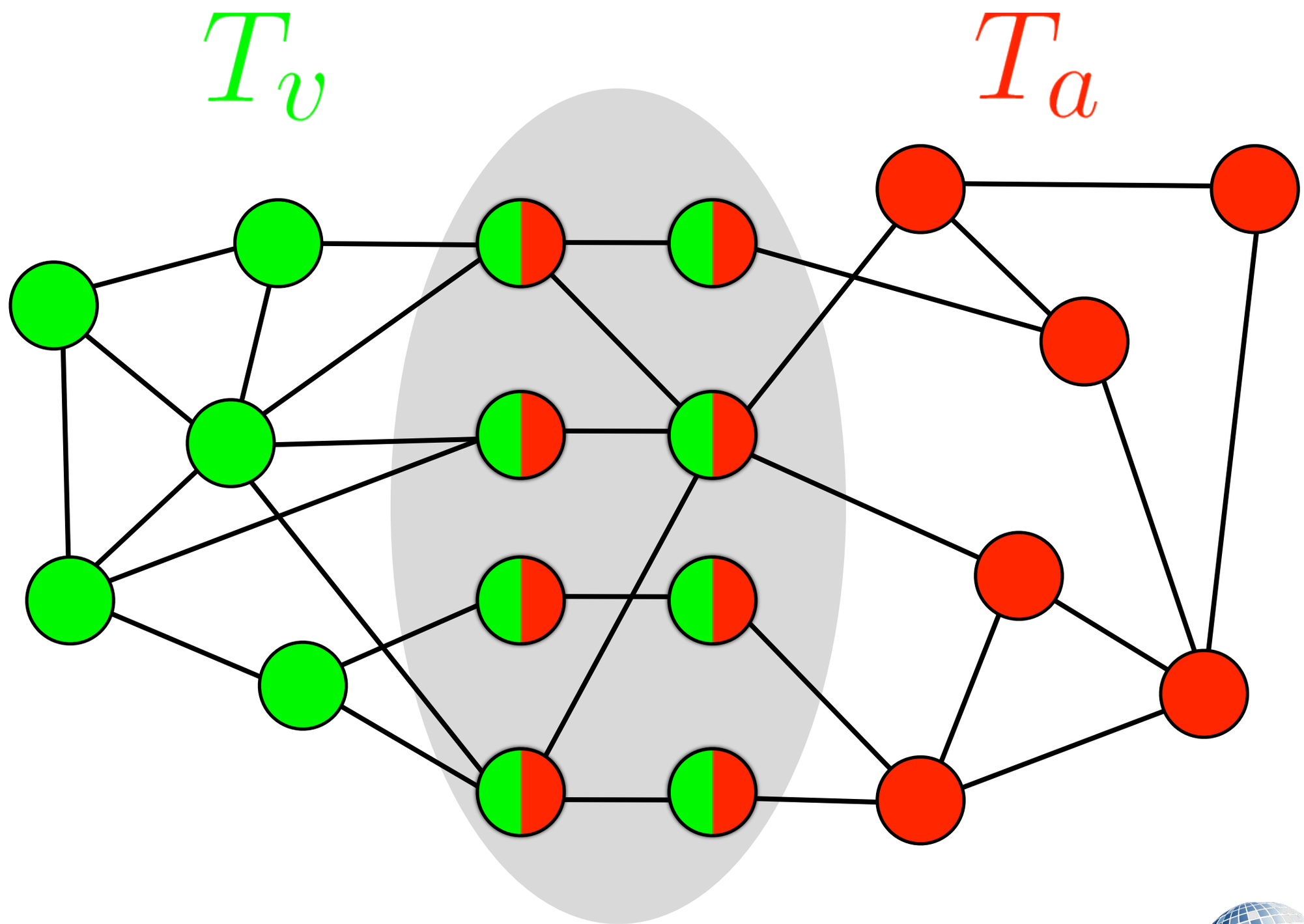
- Connect to many nodes
- No incoming connections
- No transaction relay



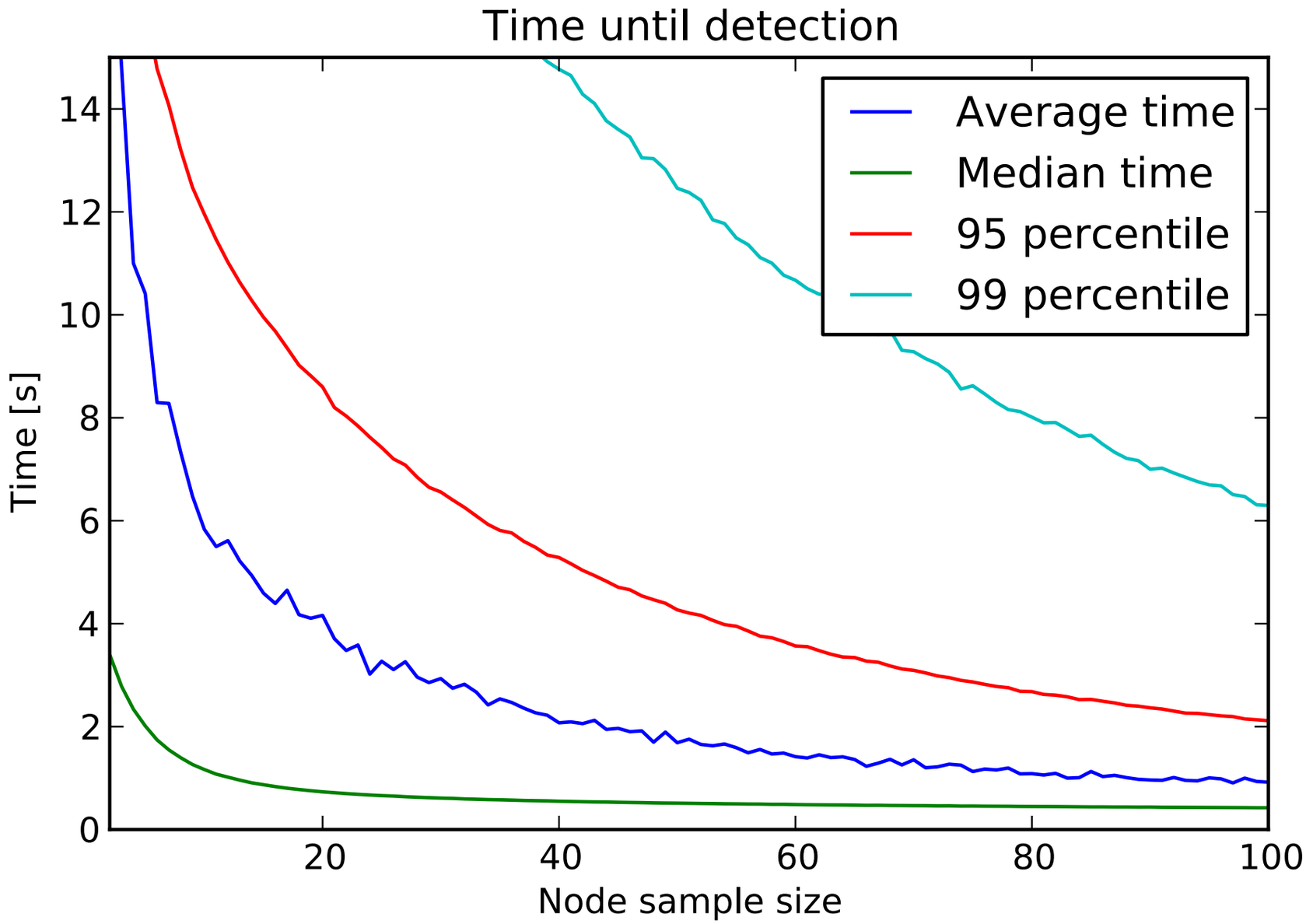
Evaluation

- Attacker and merchant
- Double spend attempts
- Random release points

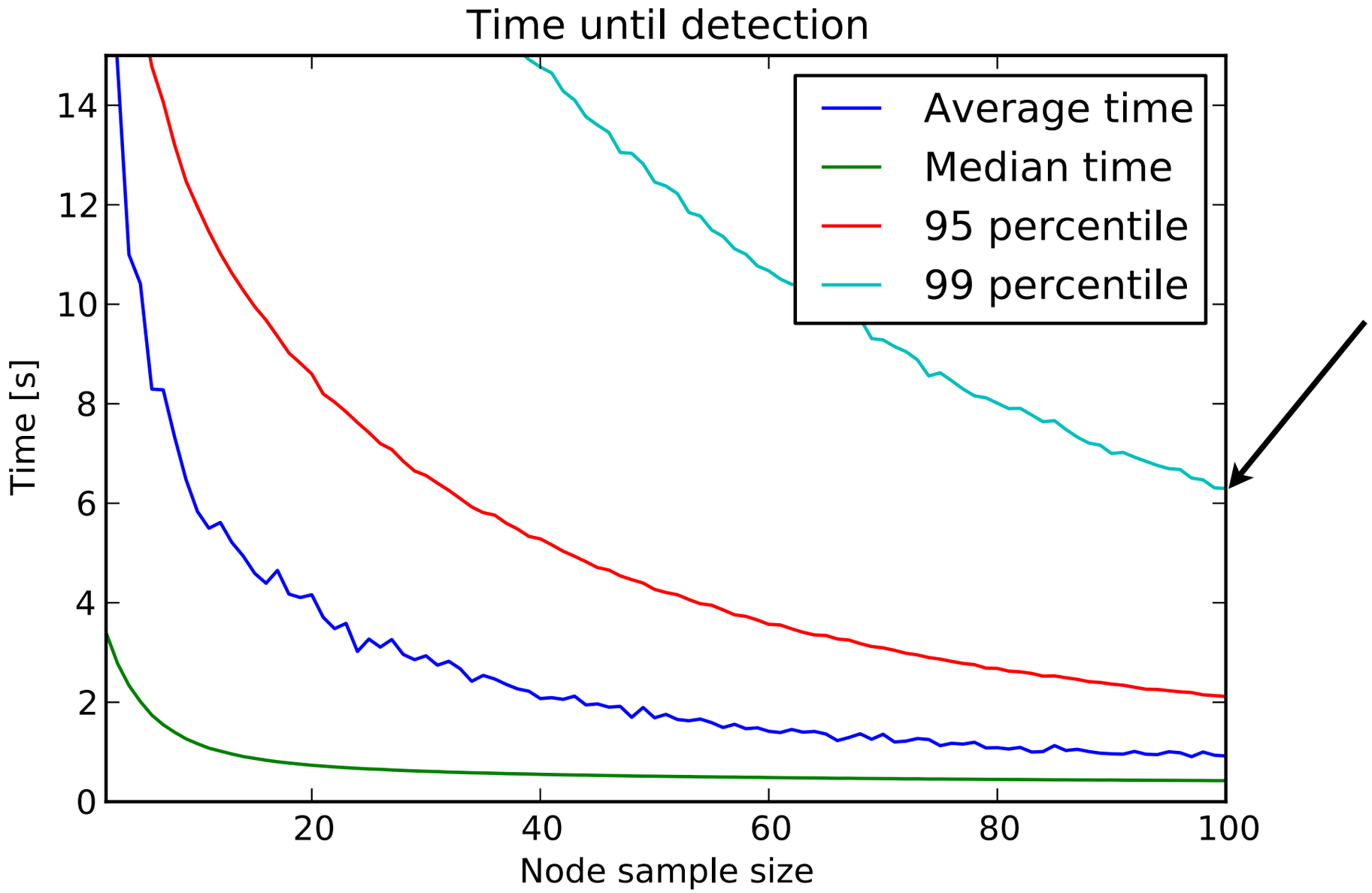
Evaluation



Evaluation


Time until detection
Average time
Median time
95 percentile
99 percentile
Time [s]
0
2
4
6
8
10
12
14
20
40
60
80
100
Node sample size

Evaluation


Time until detection
Average time
Median time
95 percentile
99 percentile
Time [s]
0
2
4
6
8
10
12
14
20
40
60
80
100
Node sample size

Successful Double Spend

$$P_{ds} = P_{fTv} \cap P_{nd} \cap P_{cTa}$$

Successful Double Spend

1. Merchant sees T_v first

$$P_{ds} = \underline{P_{fTv}} \cap P_{nd} \cap P_{cTa}$$

Successful Double Spend

1. Merchant sees T_v first
2. Only sees one transaction

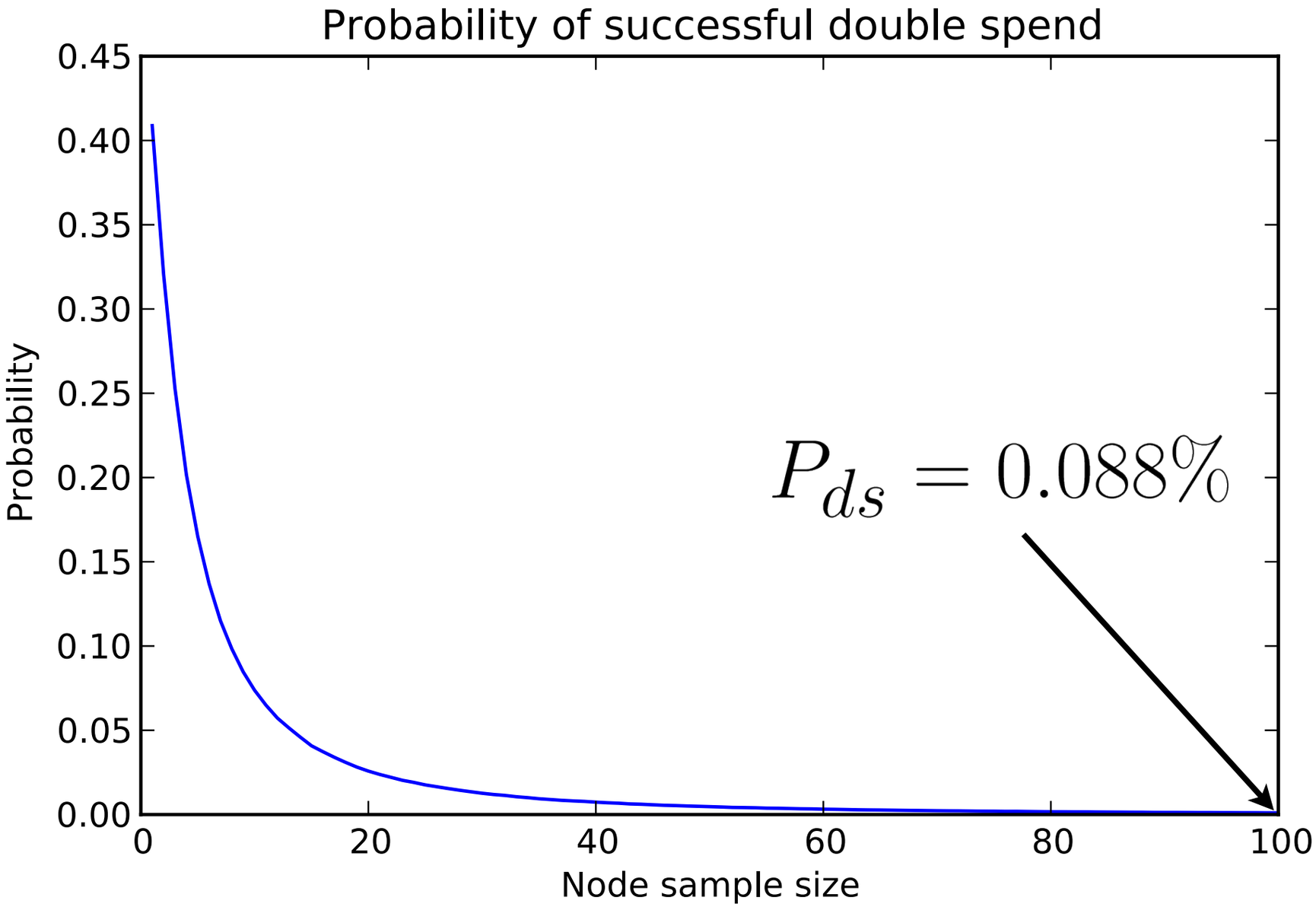
$$P_{ds} = P_{fTv} \cap \underline{P_{nd}} \cap P_{cTa}$$

Successful Double Spend

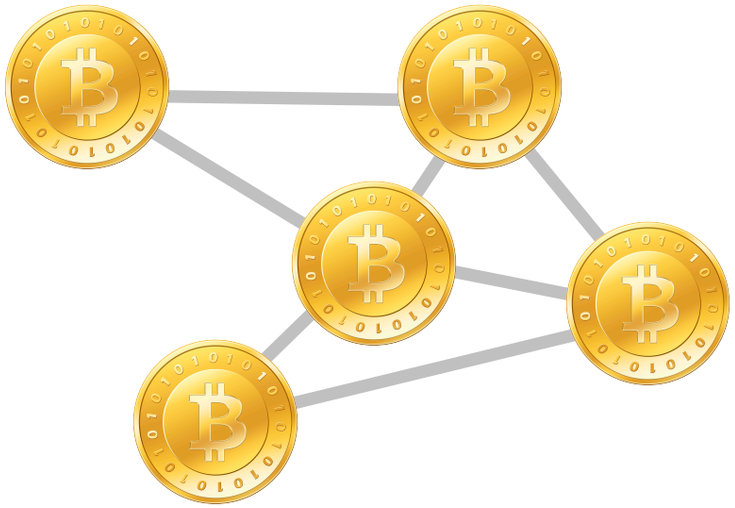
1. Merchant sees T_v first
2. Only sees one transaction
3. T_a is later confirmed

$$P_{ds} = P_{fTv} \cap P_{nd} \cap \underline{P_{cTa}}$$

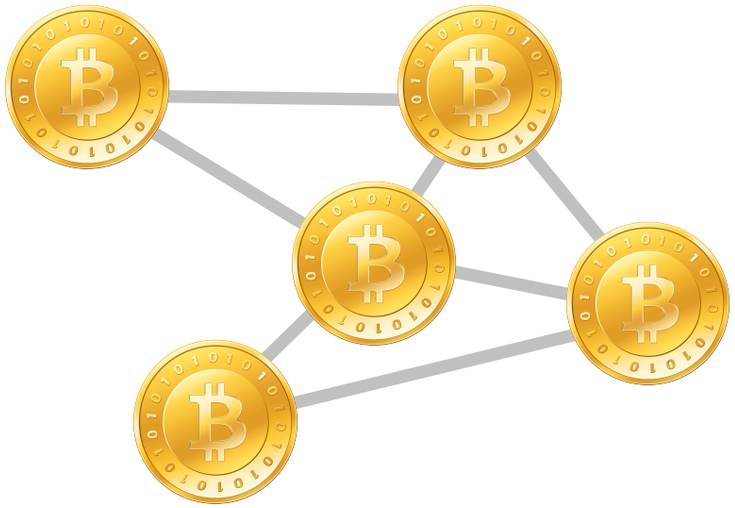
Evaluation

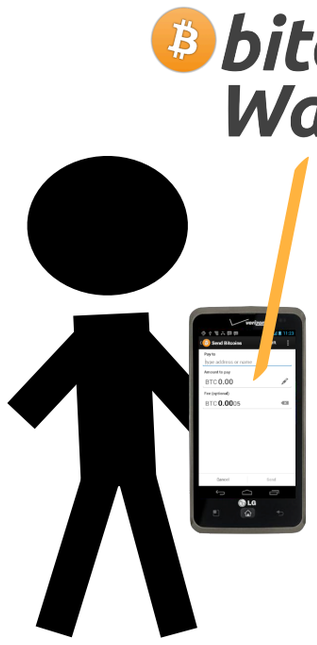

Probability of successful double spend
Probability
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
0
20
40
60
80
100
Node sample size
$P_{ds} = 0.088\%$

One loss in 1000 purchases

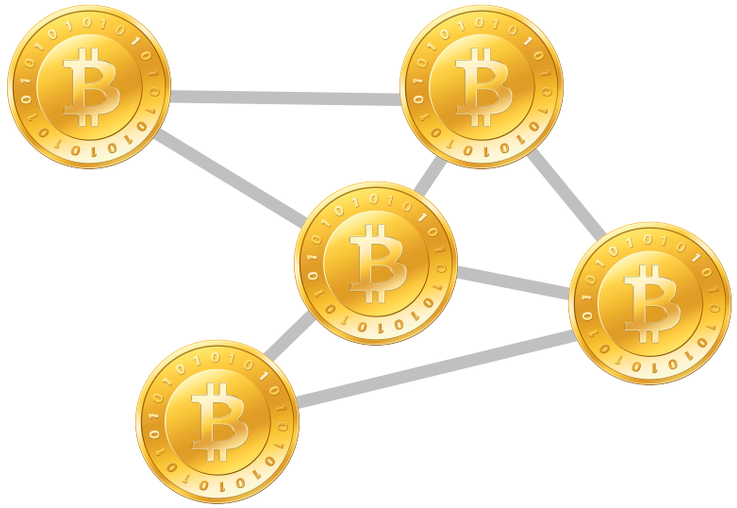


Select product



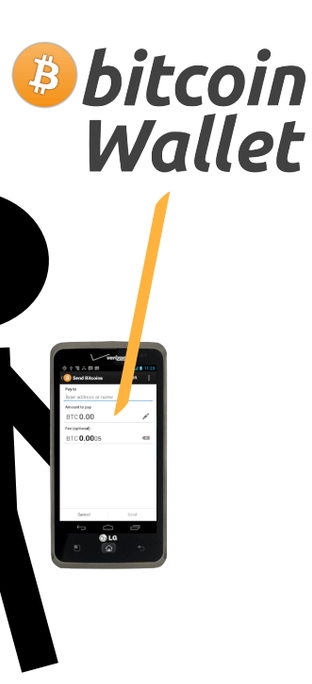


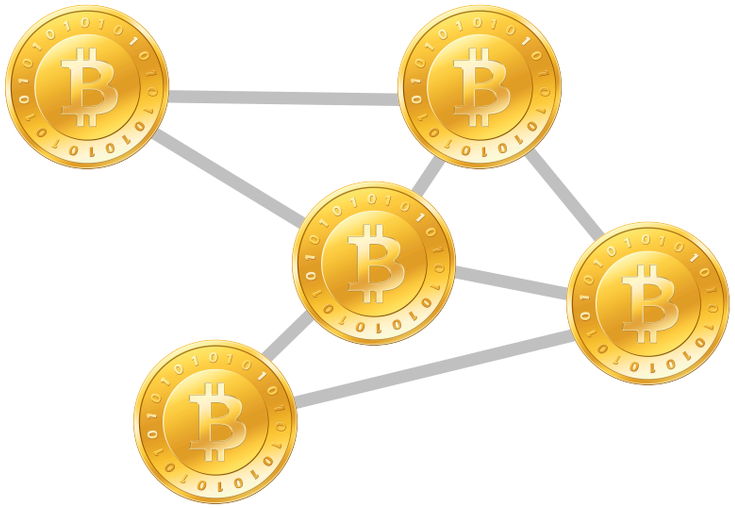
Display QR tag



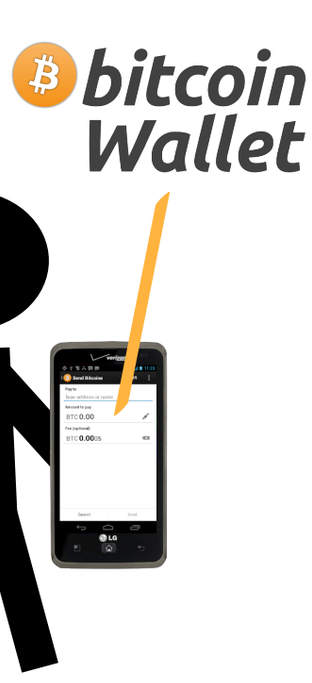
Listen for Announcements

Send Bitcoins





OK!



Thank you!

Questions?

Tobias Bamert
Christian Decker
Lennart Elsen
Roger Wattenhofer
Samuel Welten