Bitcoin's Technical Challenges

Christian Decker

ETH Zurich – Distributed Computing Group – www.disco.ethz.ch

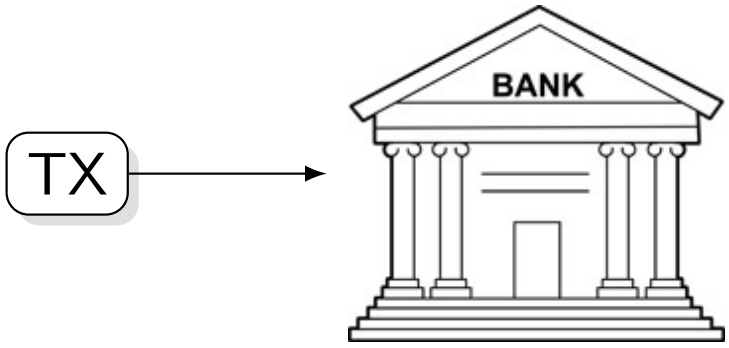
Bitcoin Basics

Bitcoin Basics

Bitcoin Basics

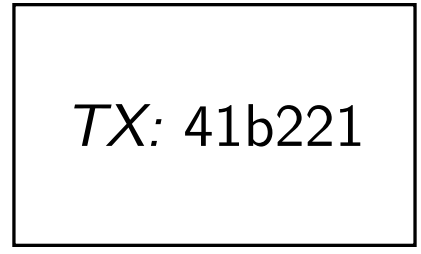
User	Balance
A	2
B	5
C	8

Bitcoin Basics

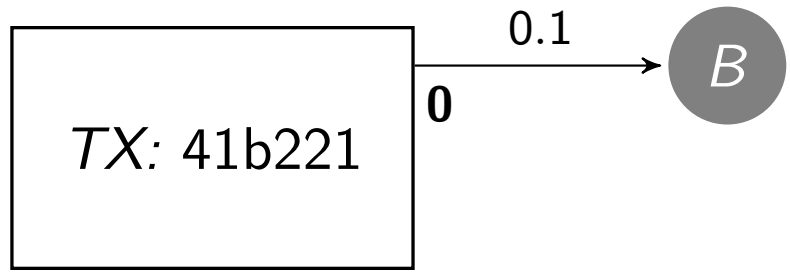


User	Balance
A	~~2~~ 4
B	~~5~~ 3
C	8

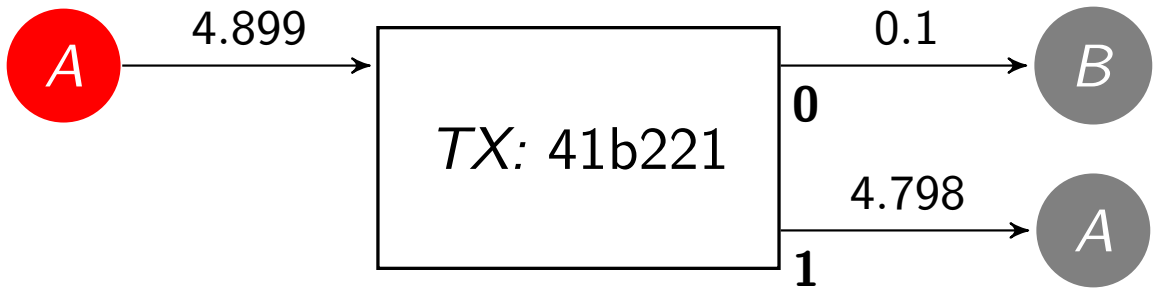
Transferring Bitcoins



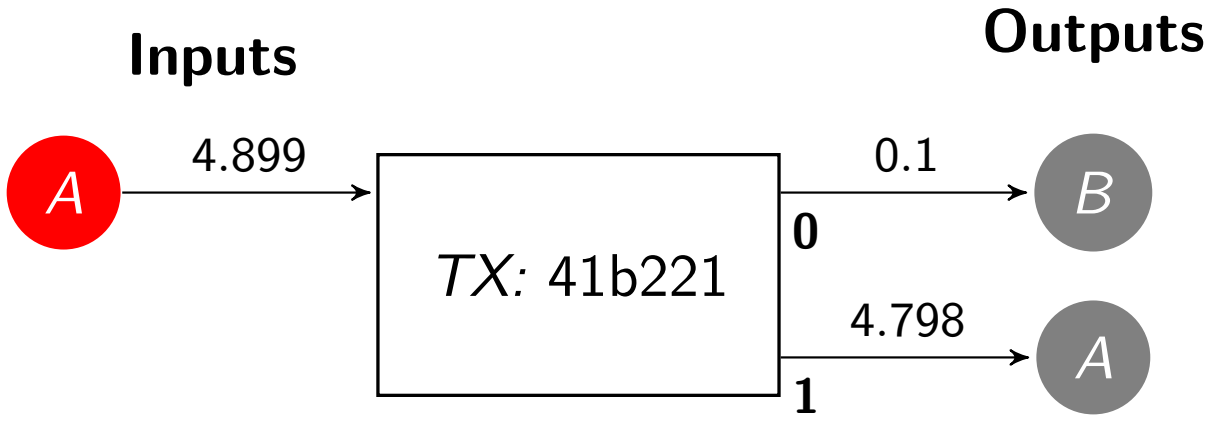
Transferring Bitcoins



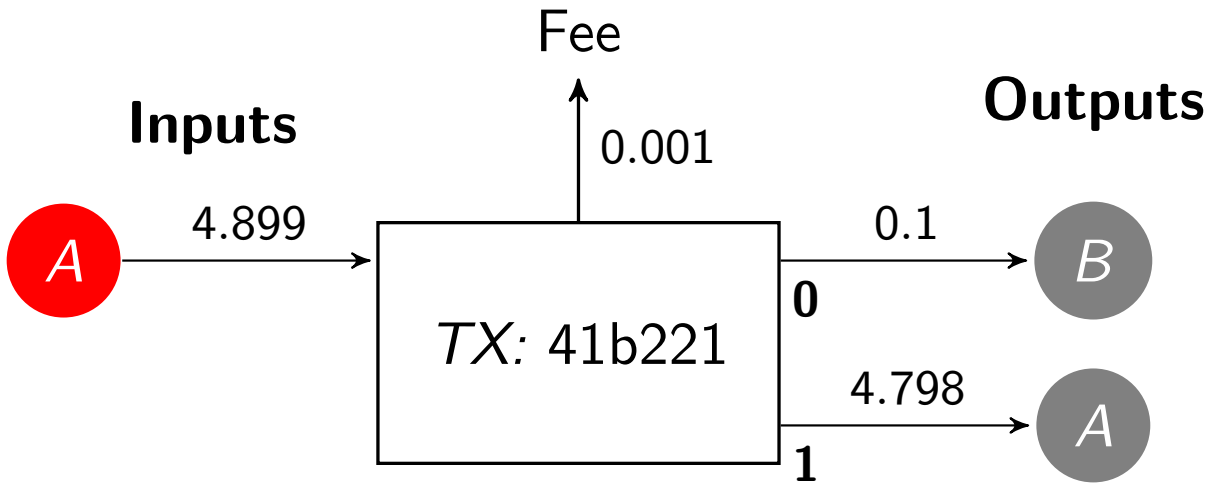
Transferring Bitcoins



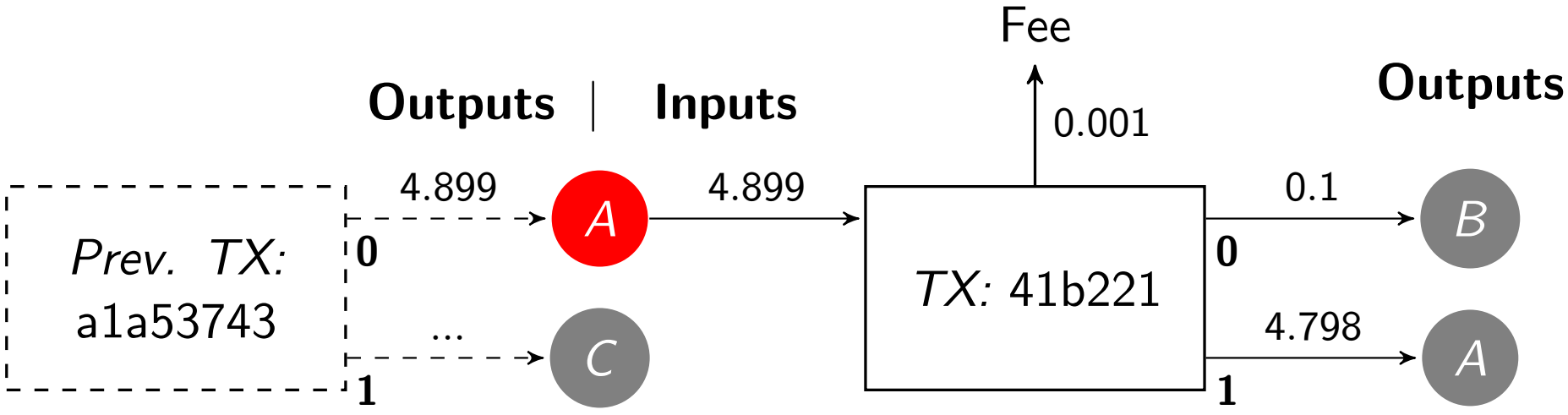
Transferring Bitcoins



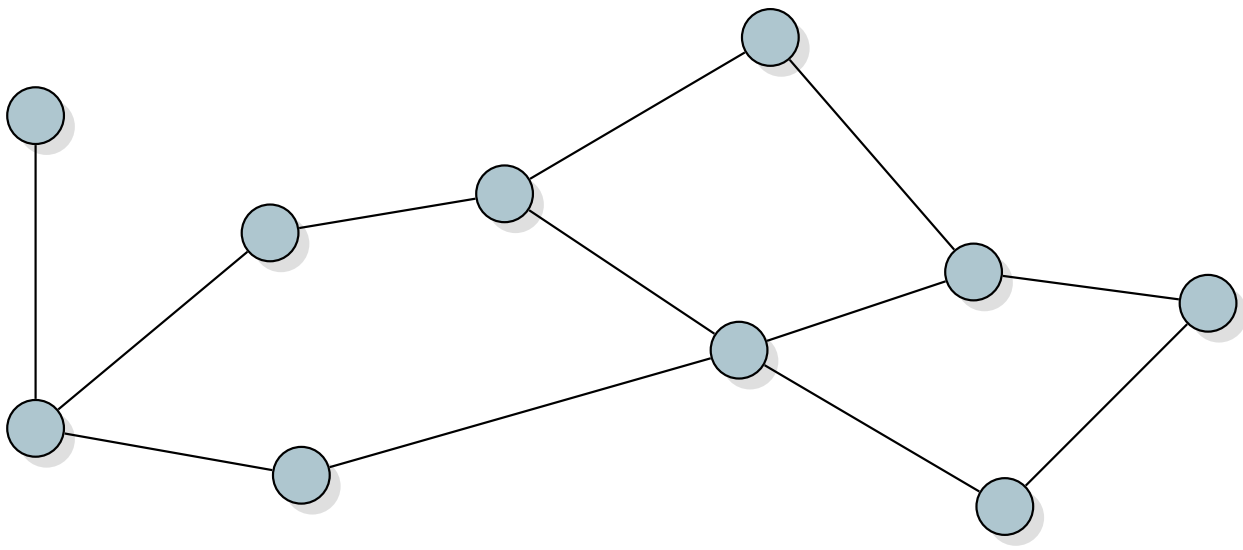
Transferring Bitcoins



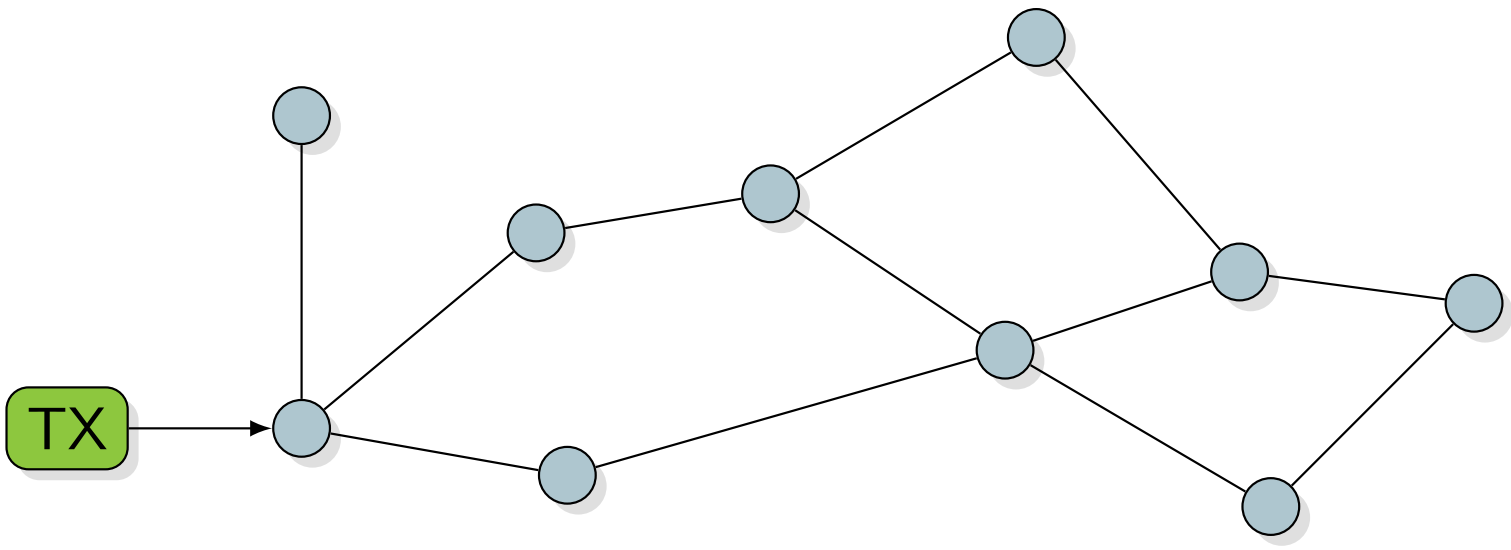
Transferring Bitcoins



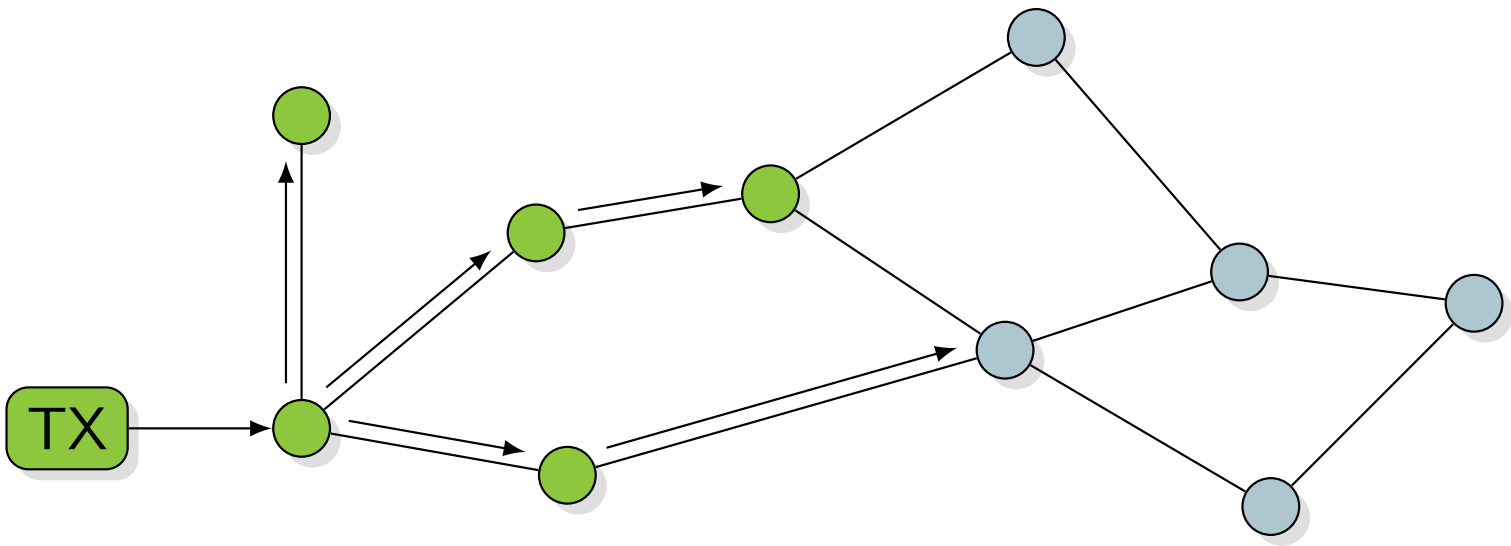
Distributing the Bank



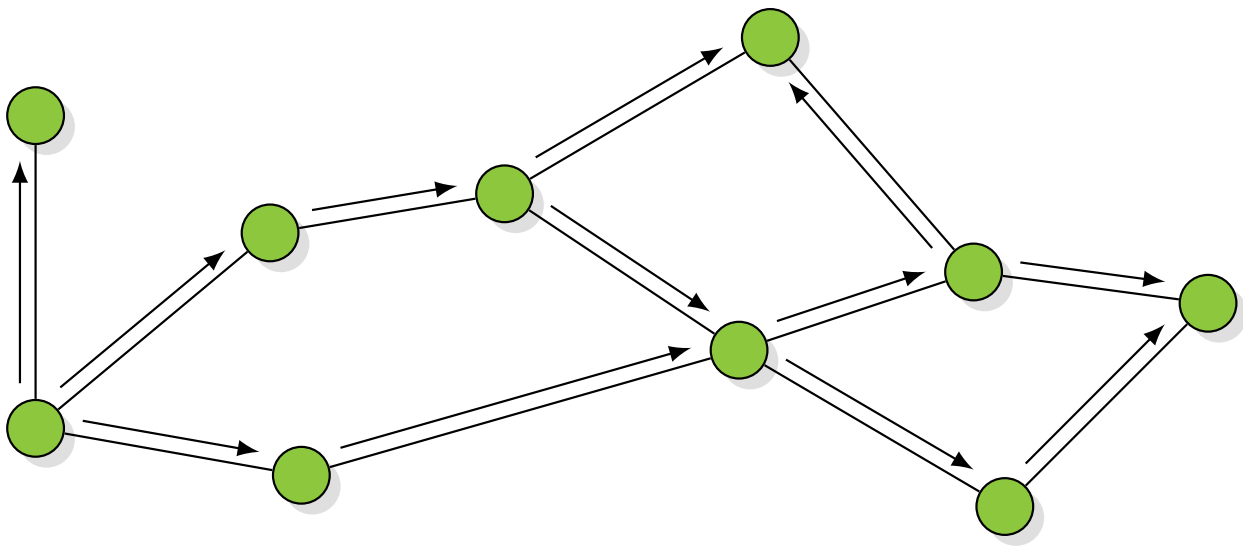
Distributing the Bank



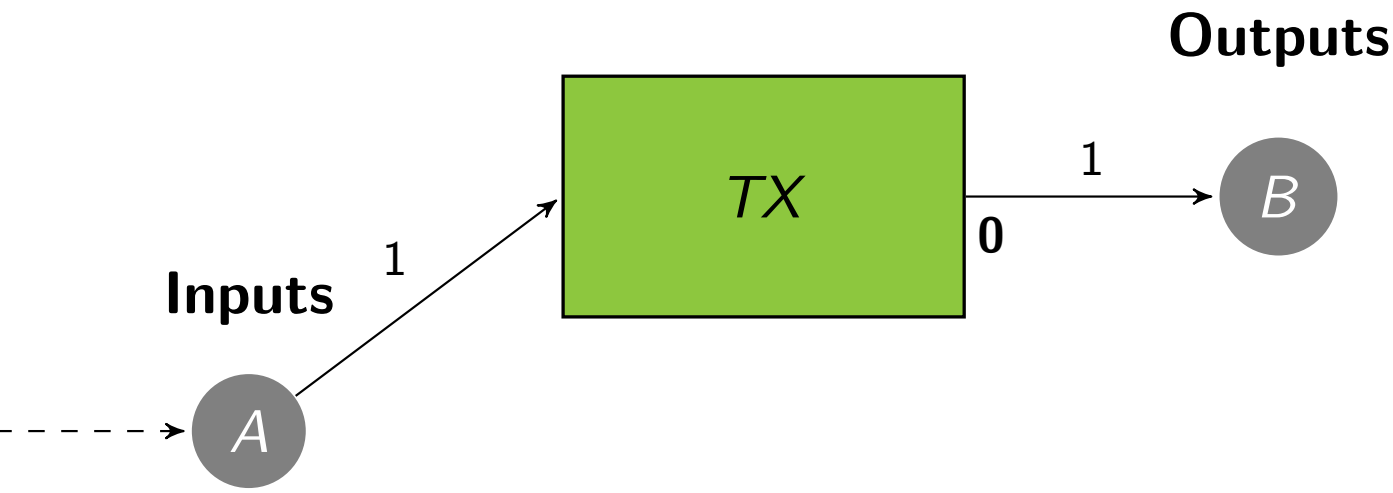
Distributing the Bank



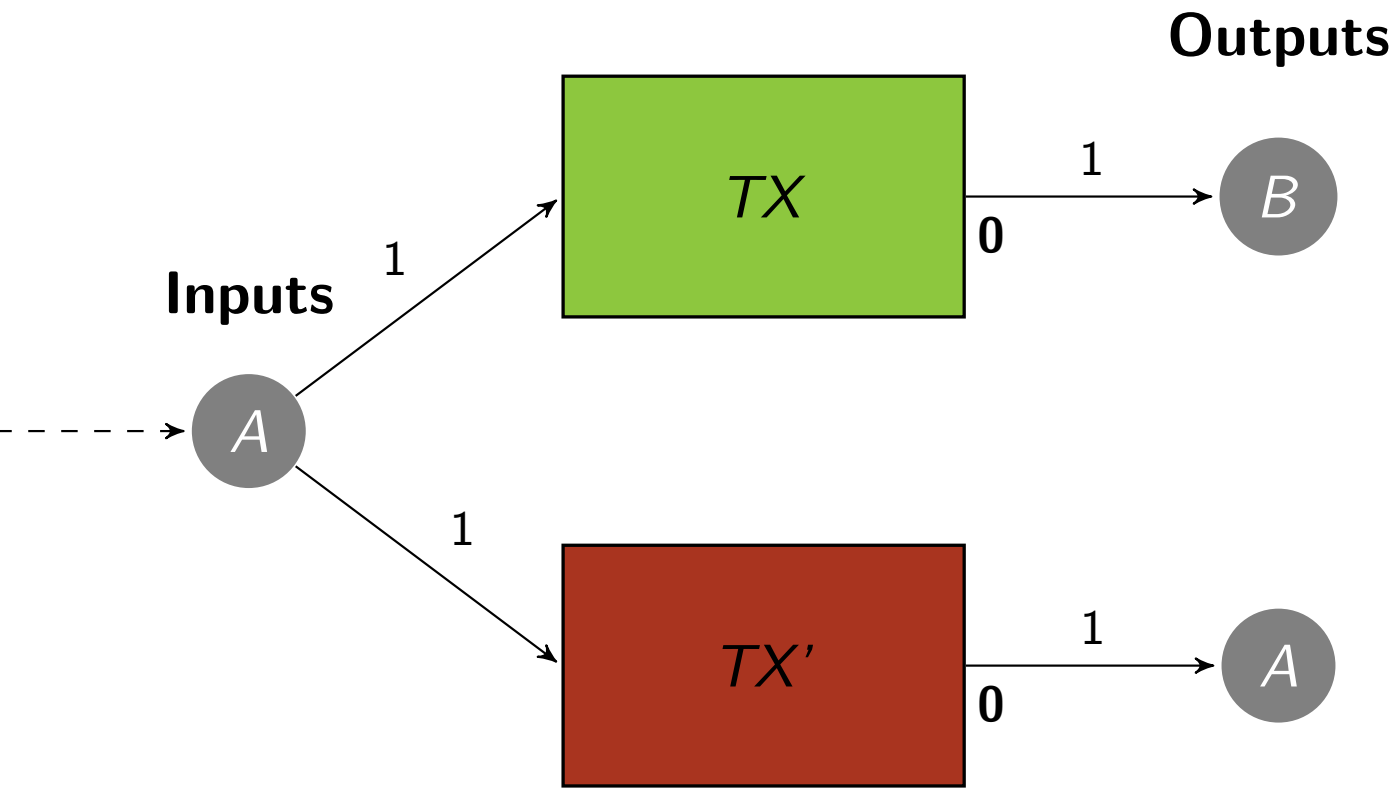
Distributing the Bank



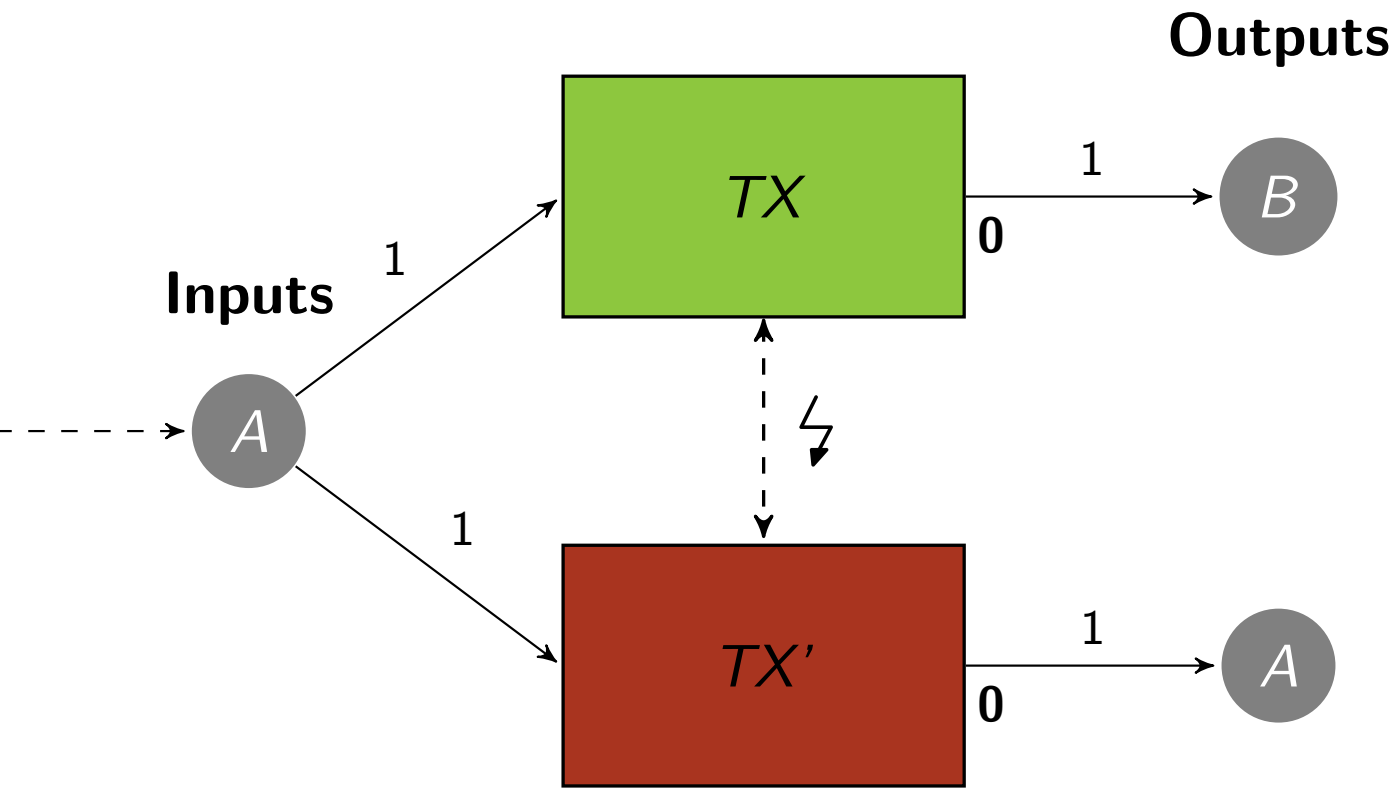
Doublespending



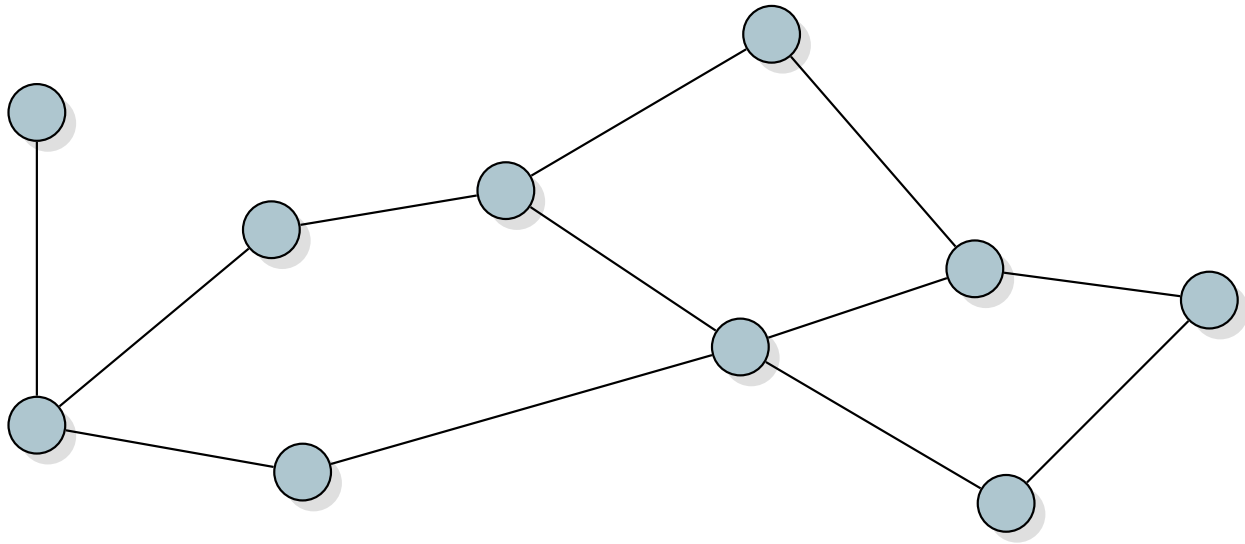
Doublespending



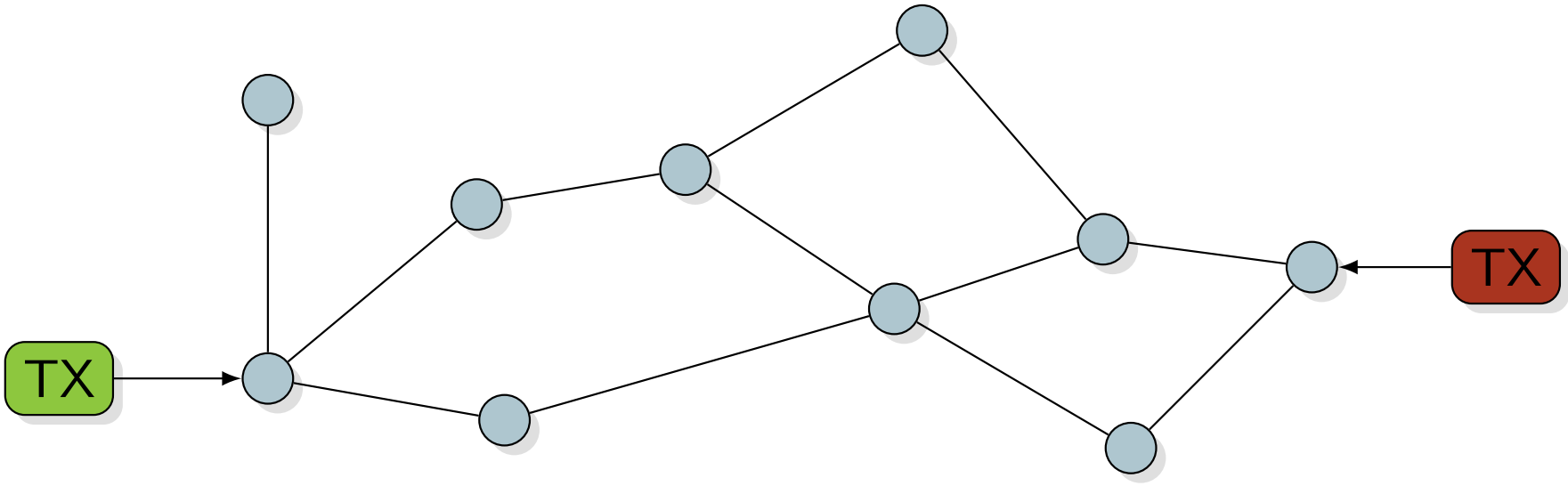
Doublespending



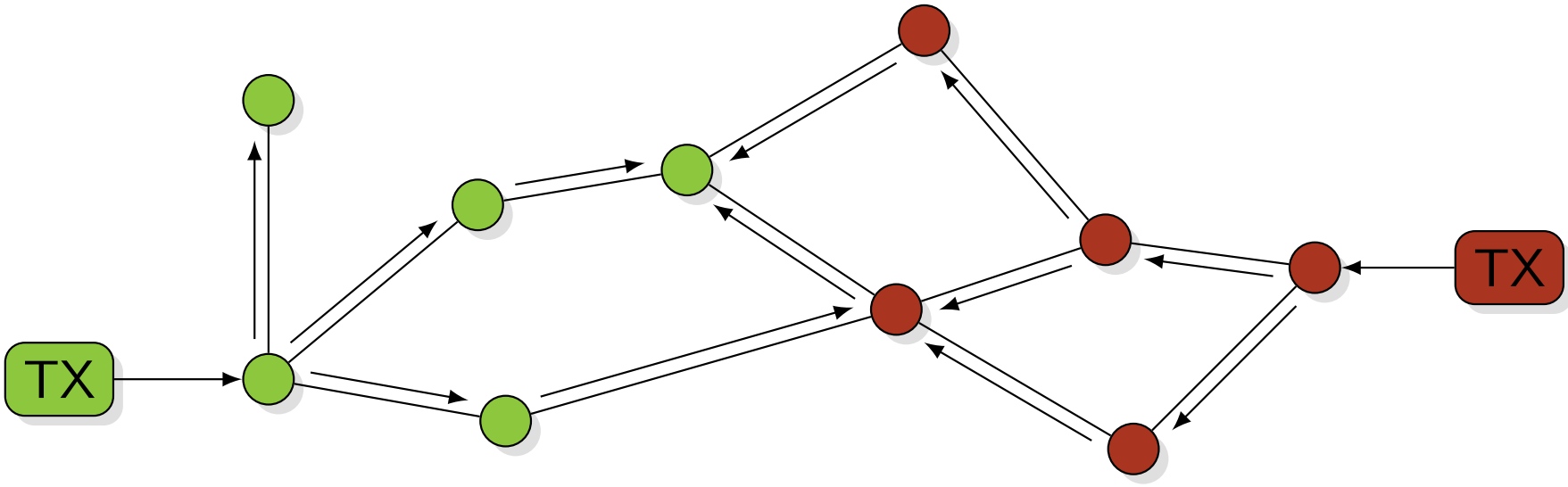
Transaction Conflicts



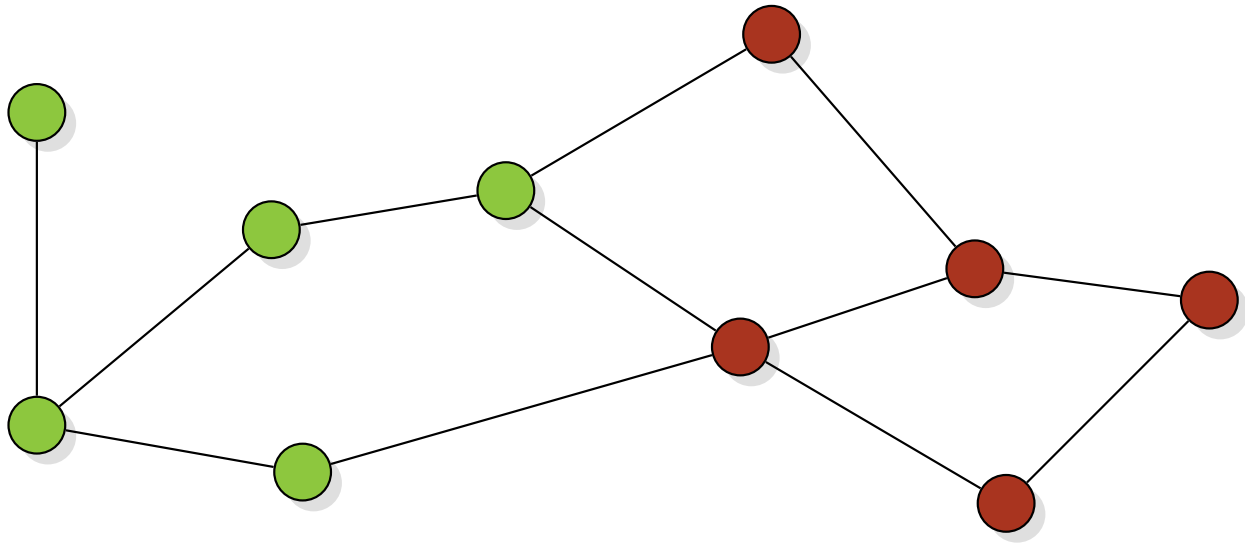
Transaction Conflicts



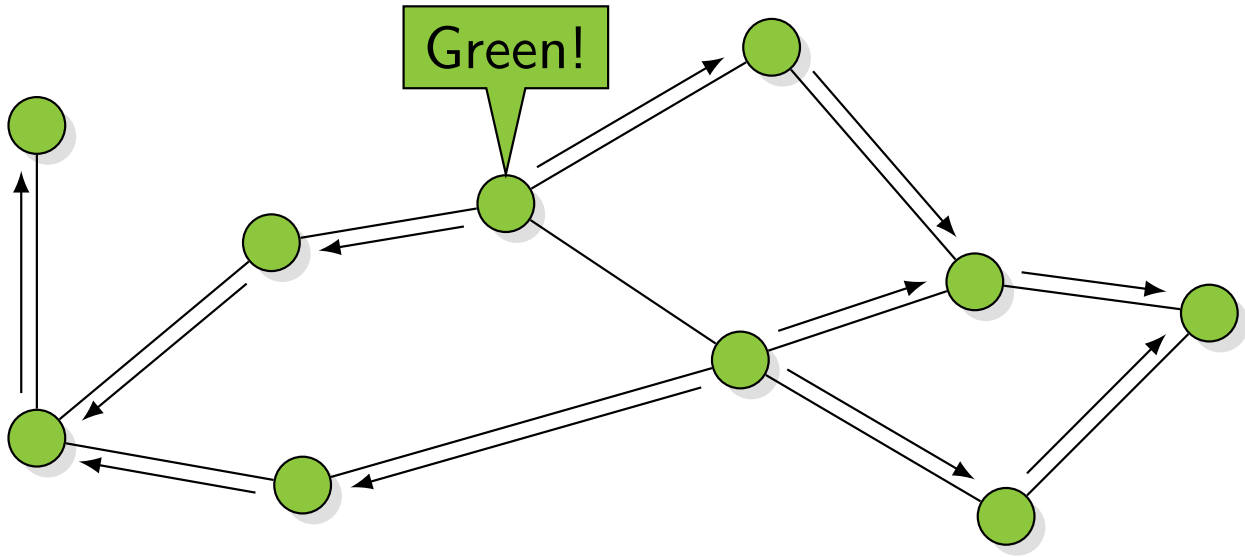
Transaction Conflicts



Resolving Conflicts



Resolving Conflicts

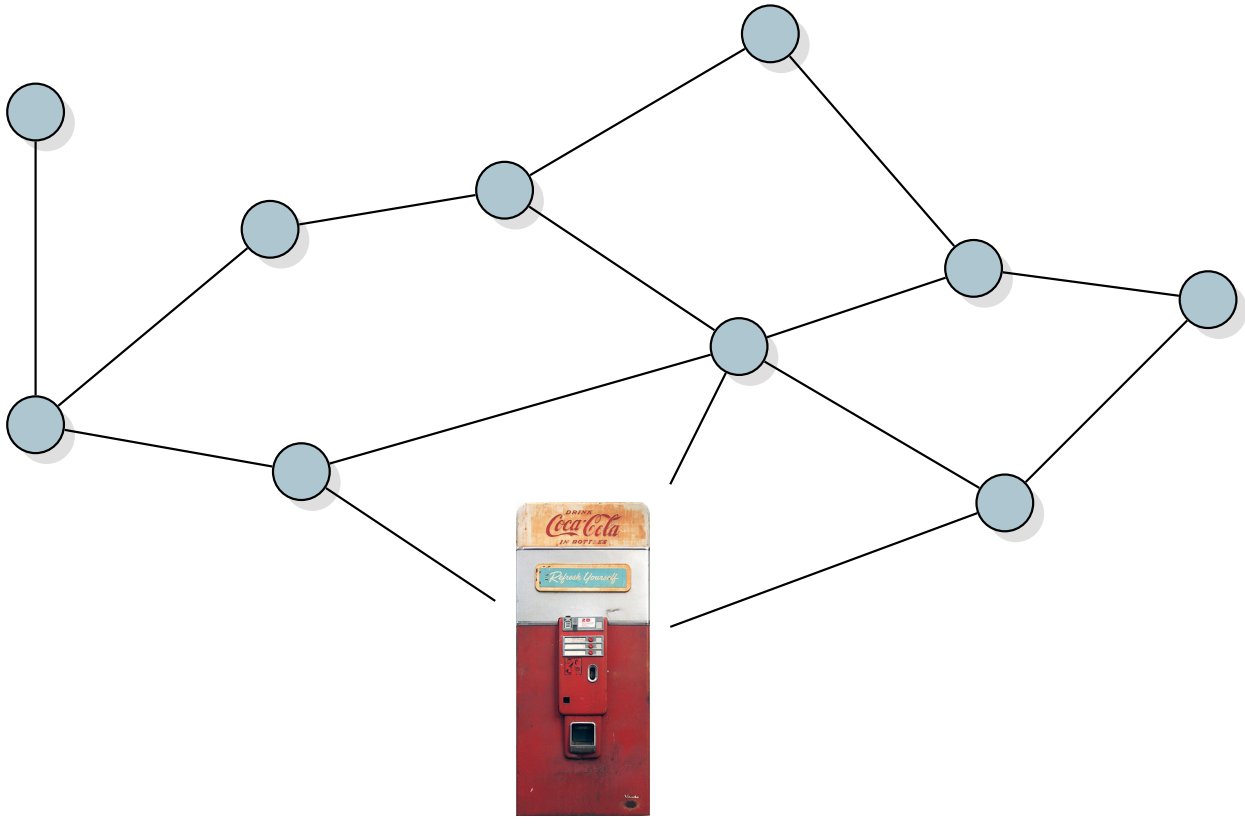


How to Choose a Leader?

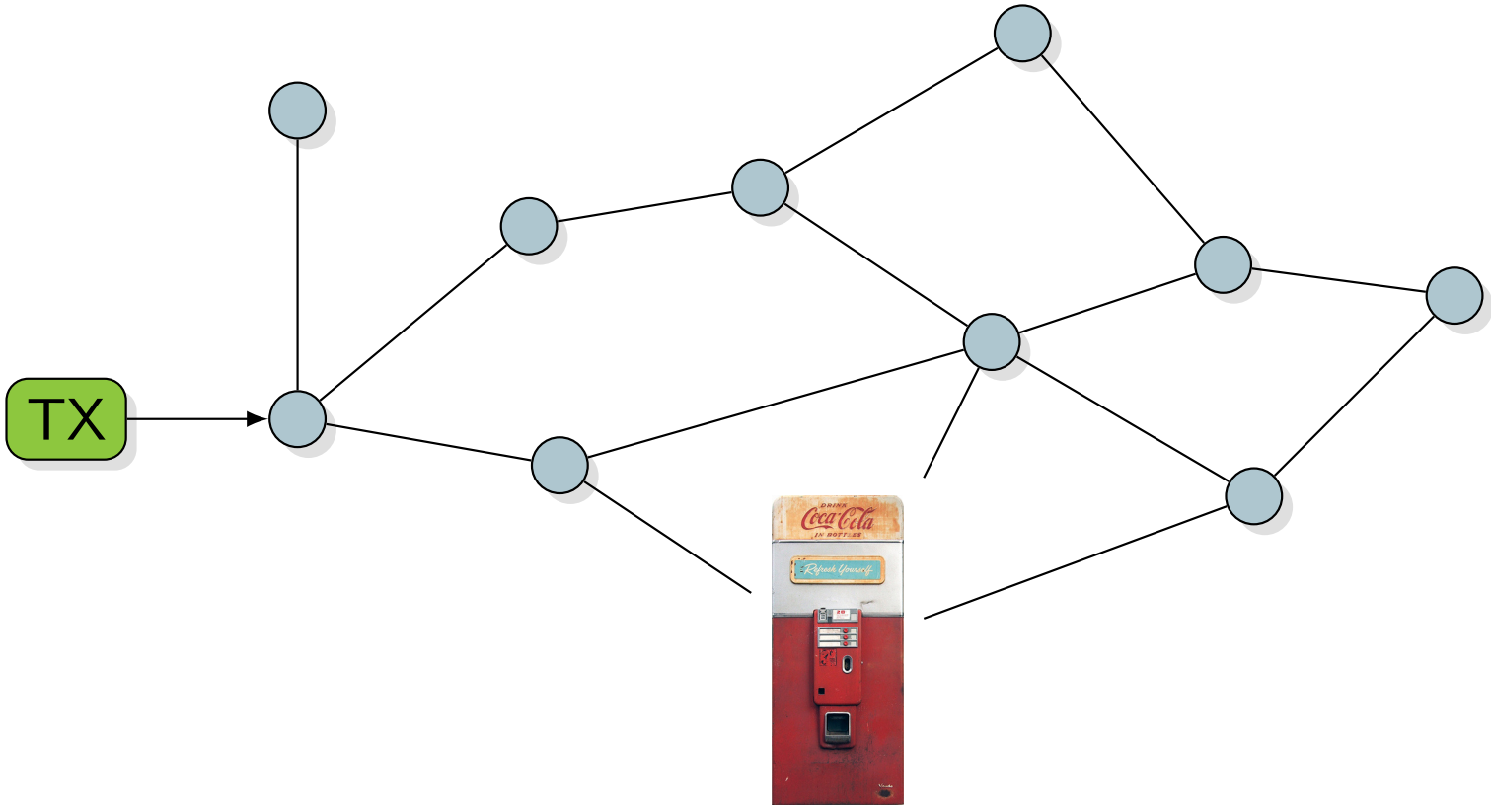
Securing Fast Payments

Let's Buy a Snack

Transaction Confidence

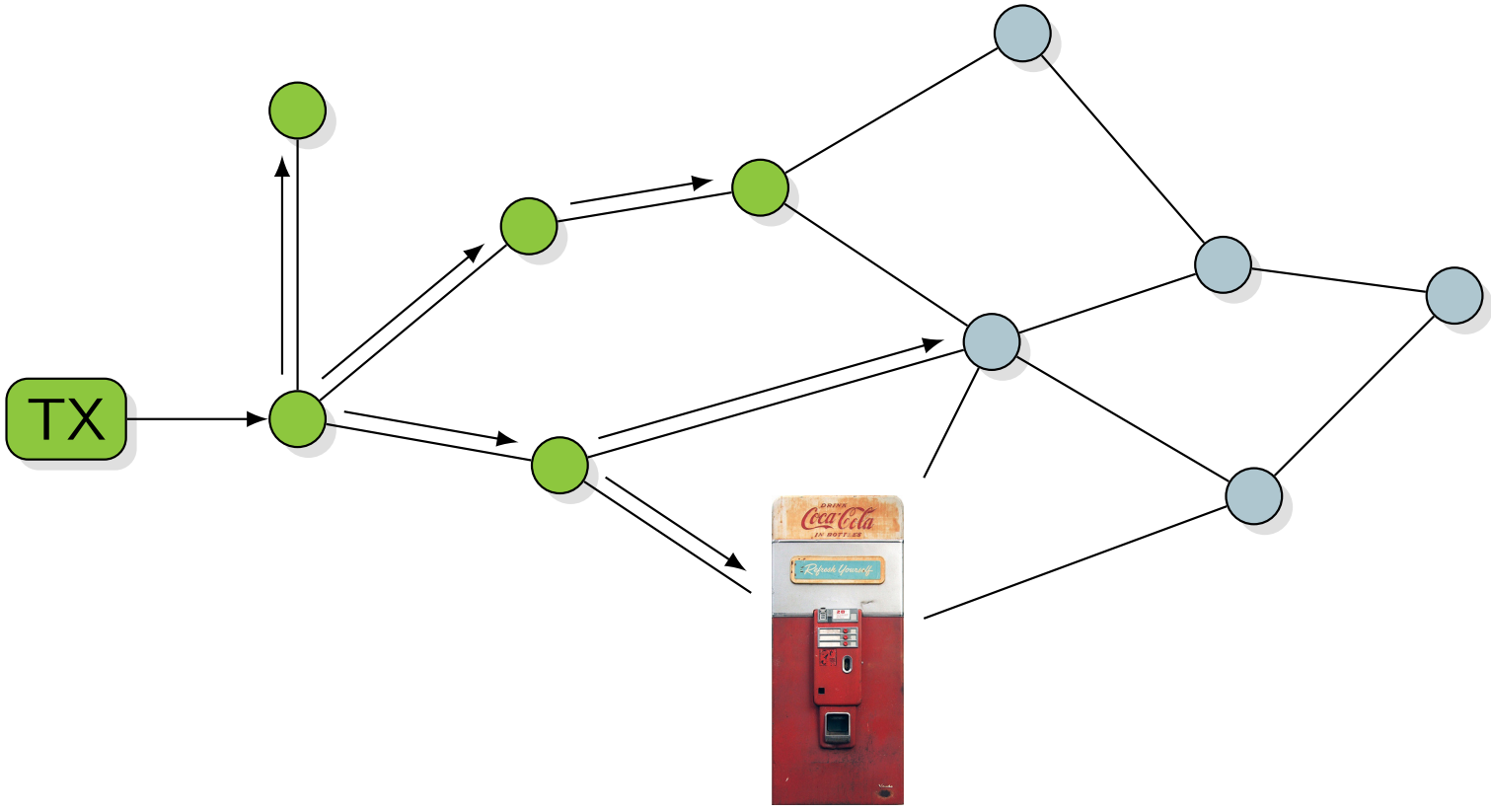


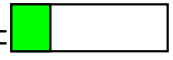
Transaction Confidence



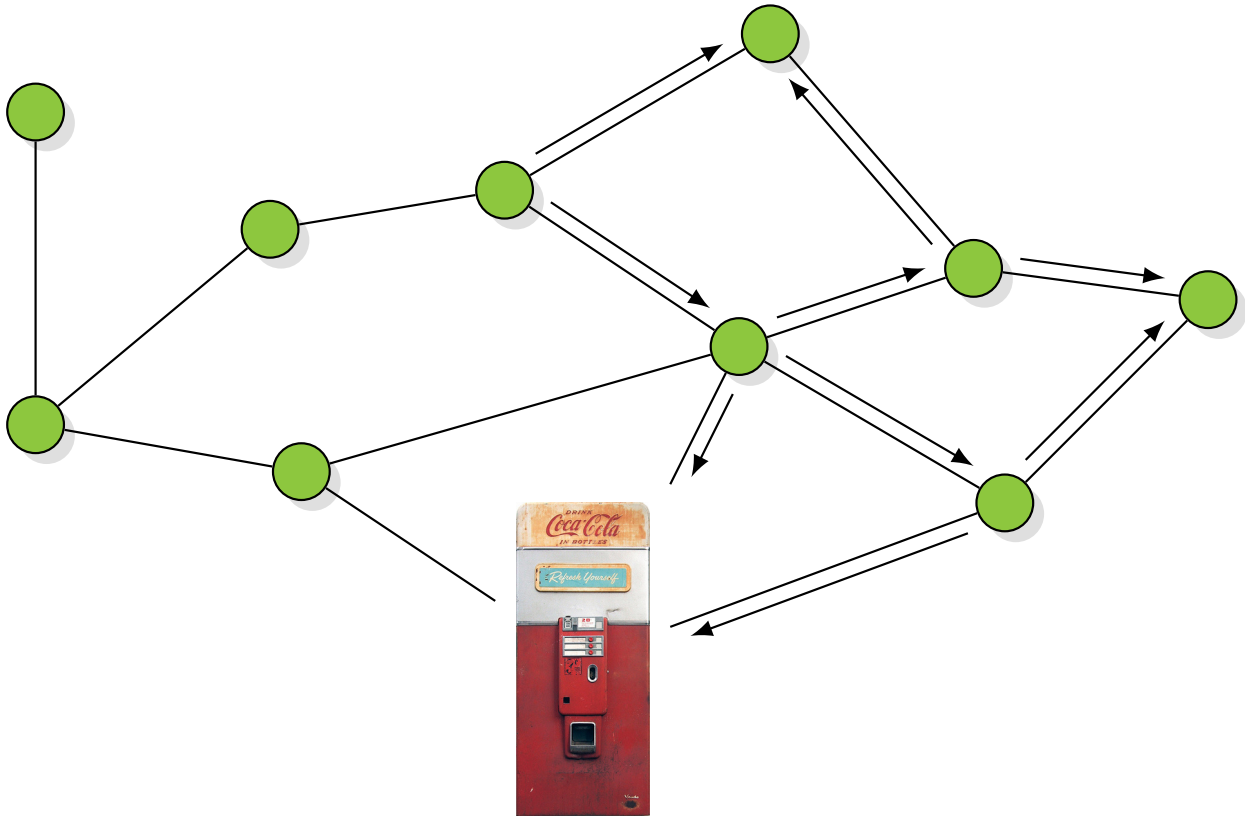
$$confidence(TX) = \square$$

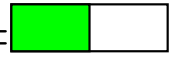
Transaction Confidence



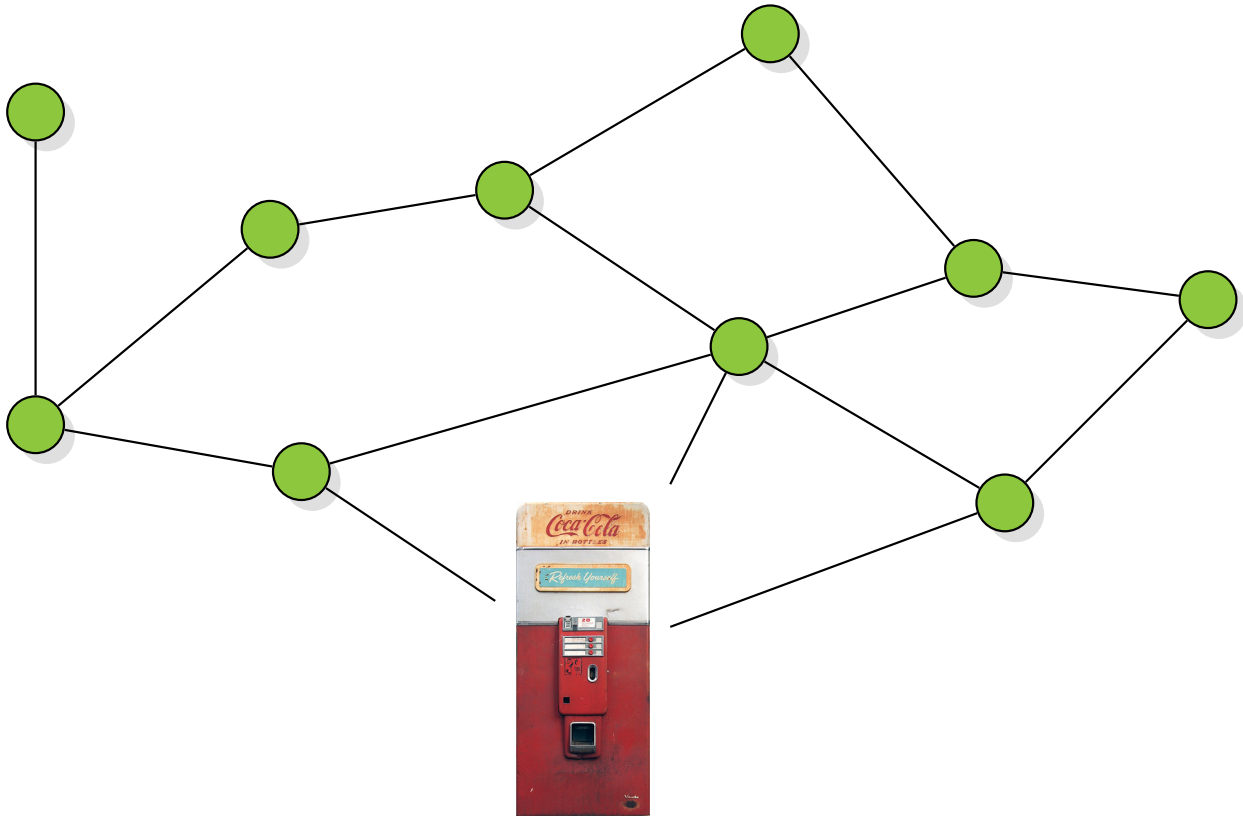
$confidence(TX) =$ 

Transaction Confidence



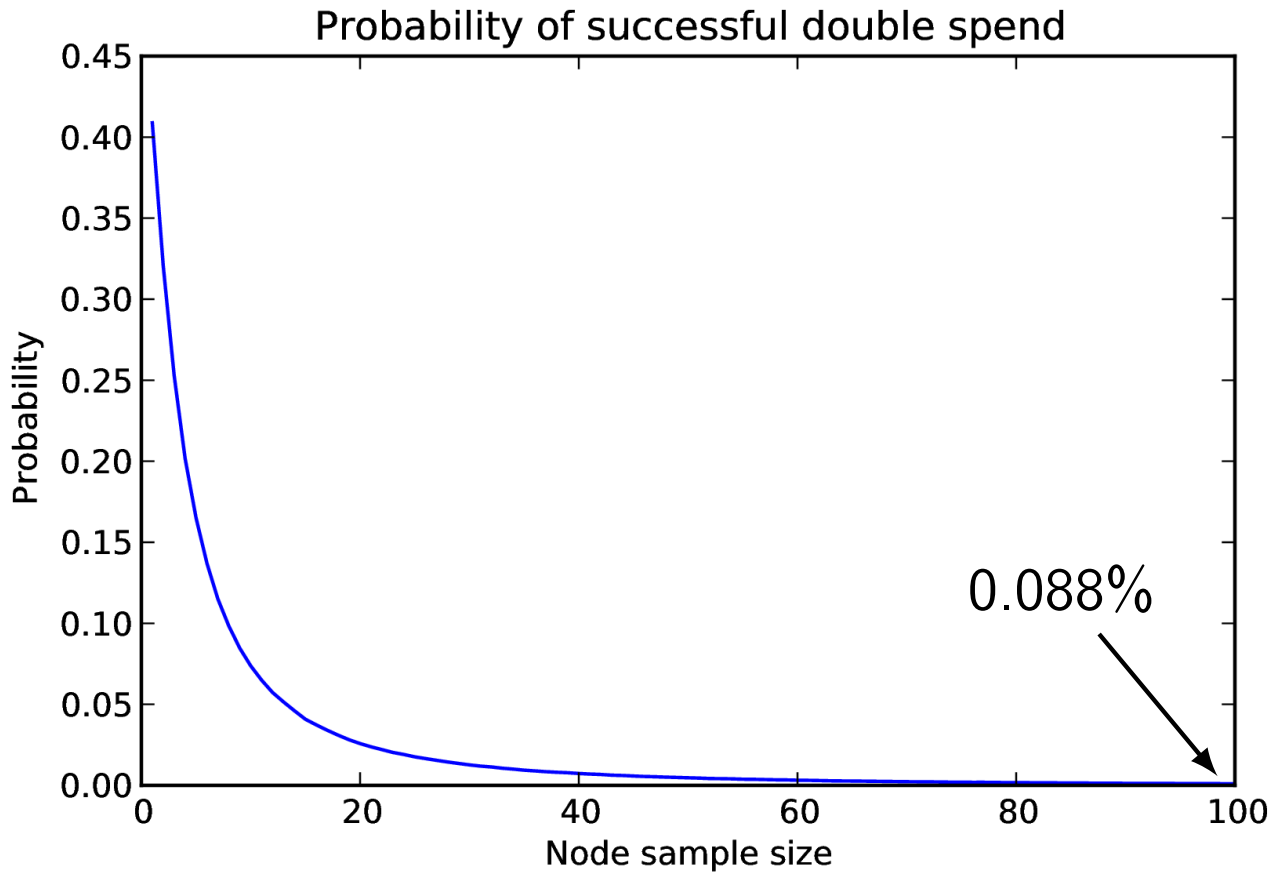
$confidence(TX) =$ 

Transaction Confidence



$confidence(TX) =$ 

Successful Doublespend

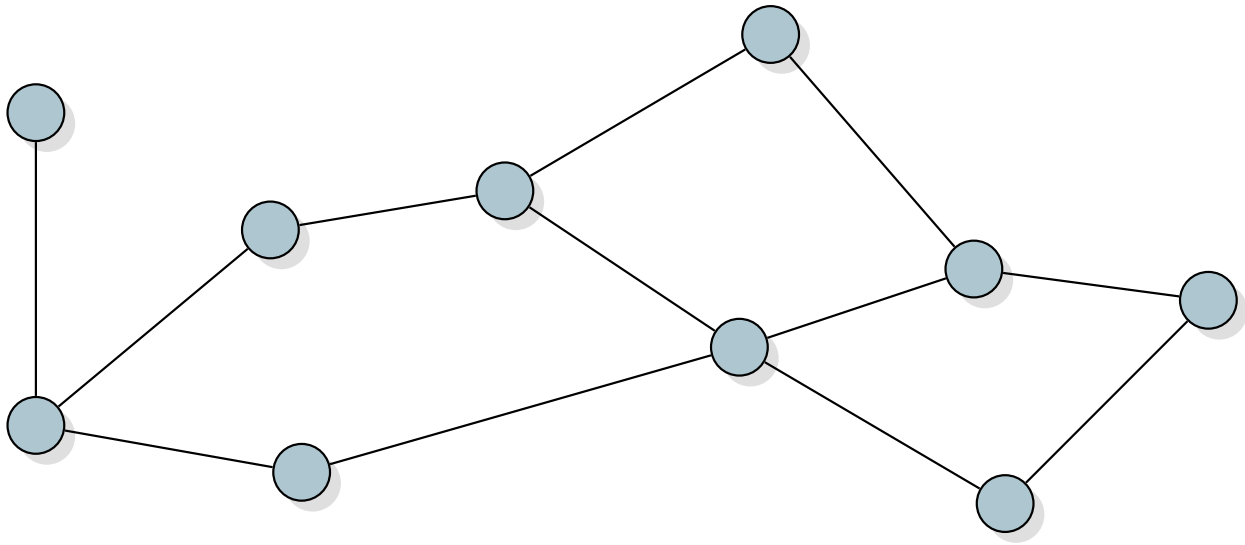


Privacy

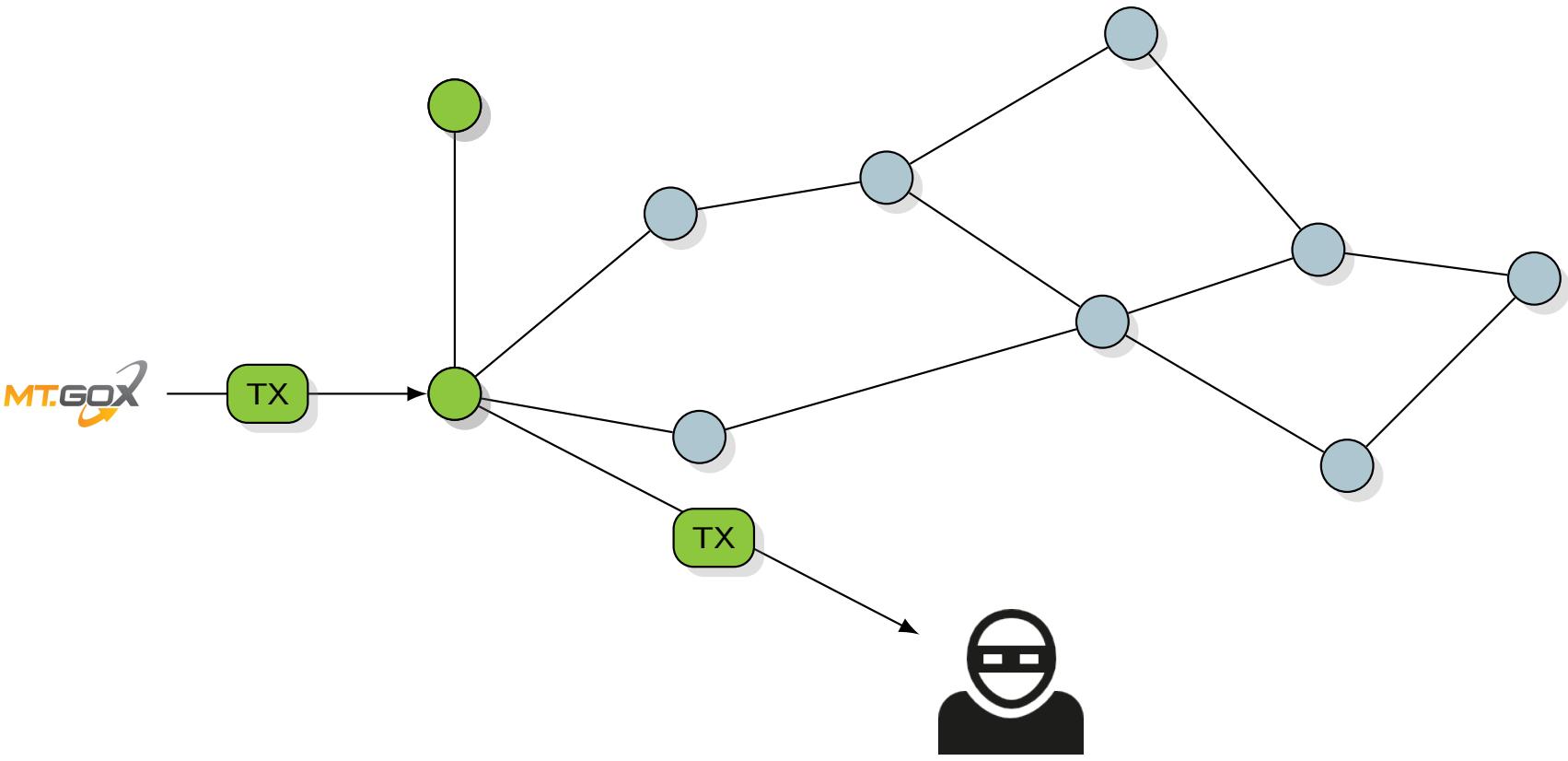
How (not) to Lose 500 Million USD

Addressing Transaction Malleability: MtGox has detected unusual activity on its Bitcoin wallets and performed investigations during the past weeks.

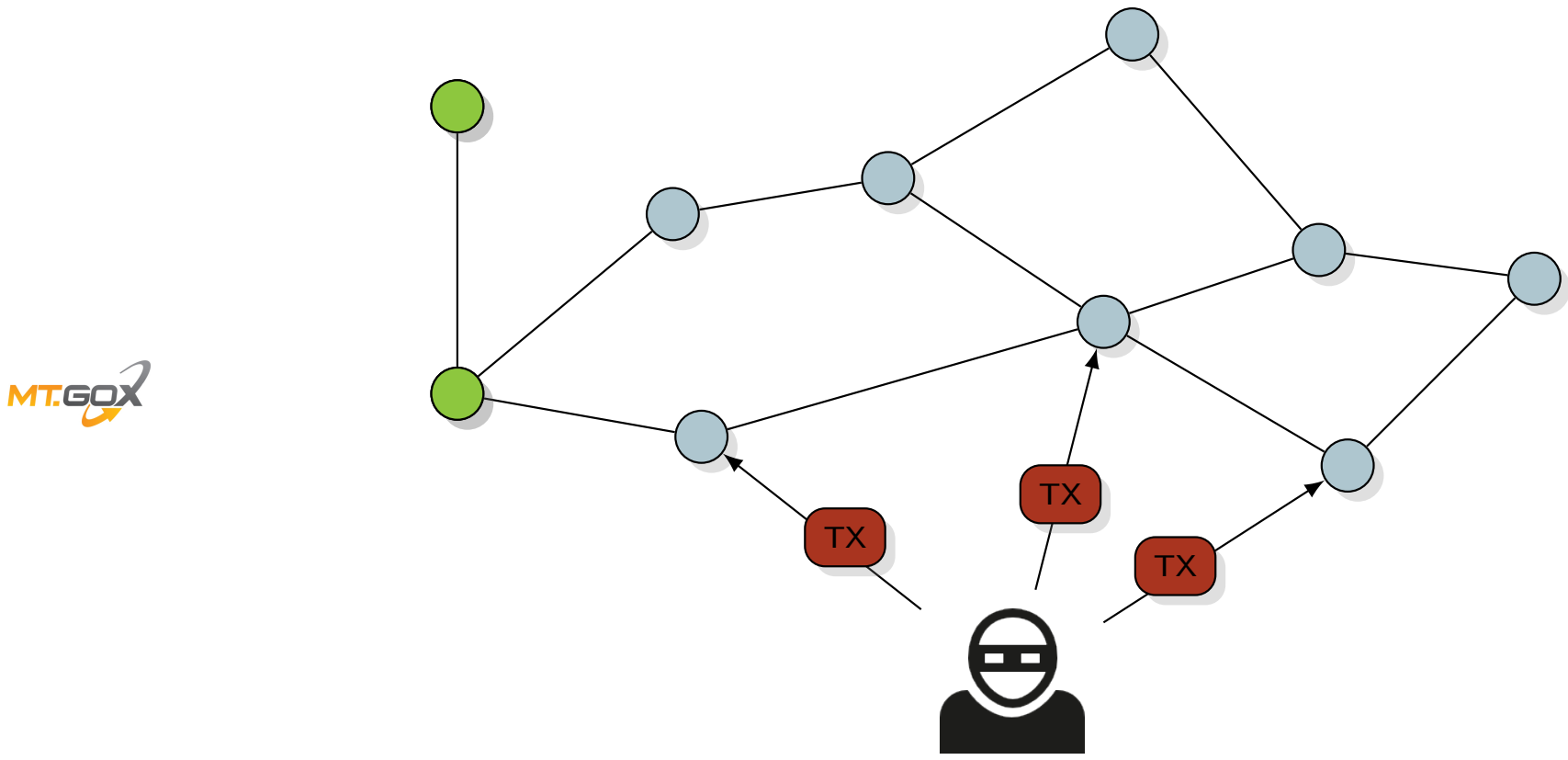
Transaction Malleability Attack



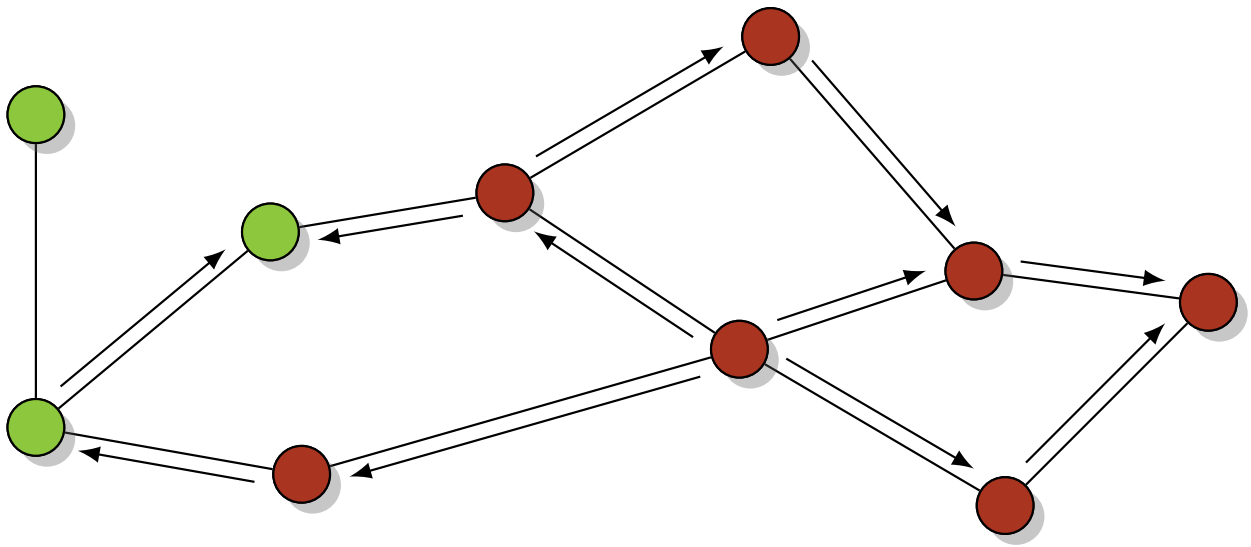
Transaction Malleability Attack



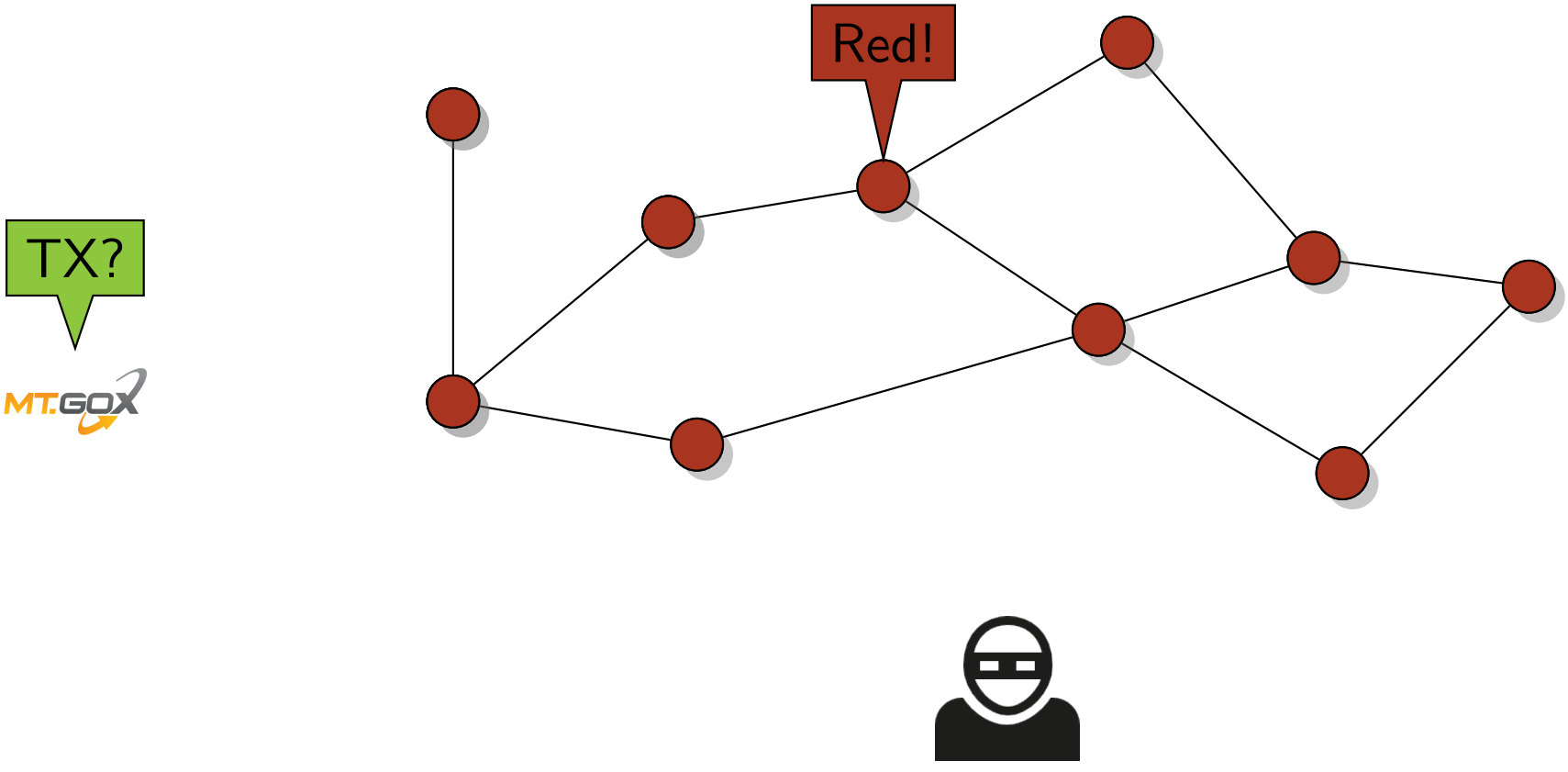
Transaction Malleability Attack



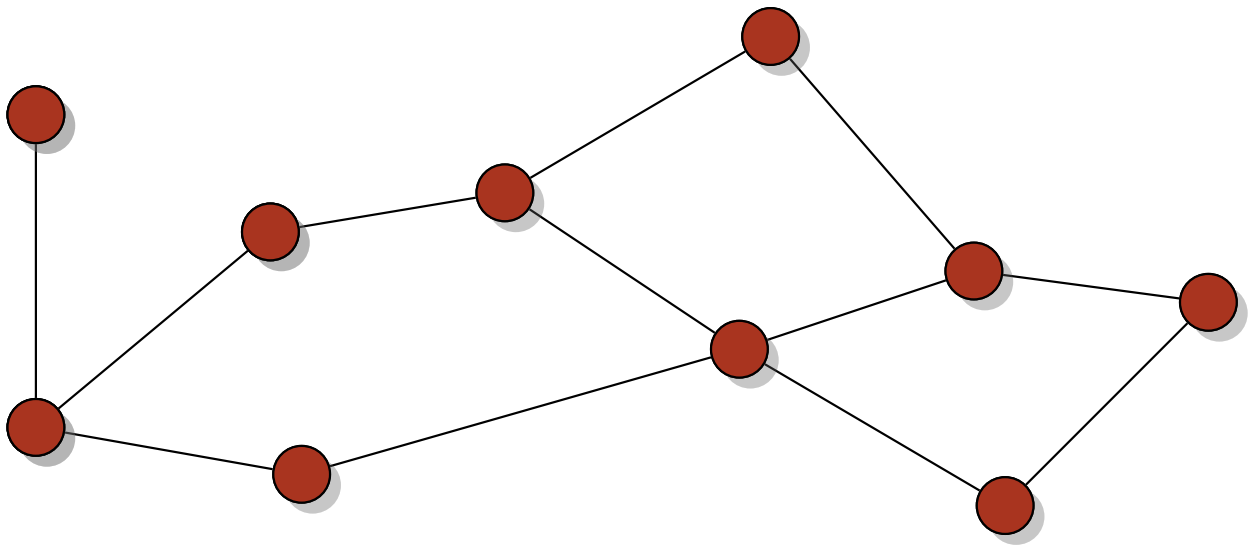
Transaction Malleability Attack



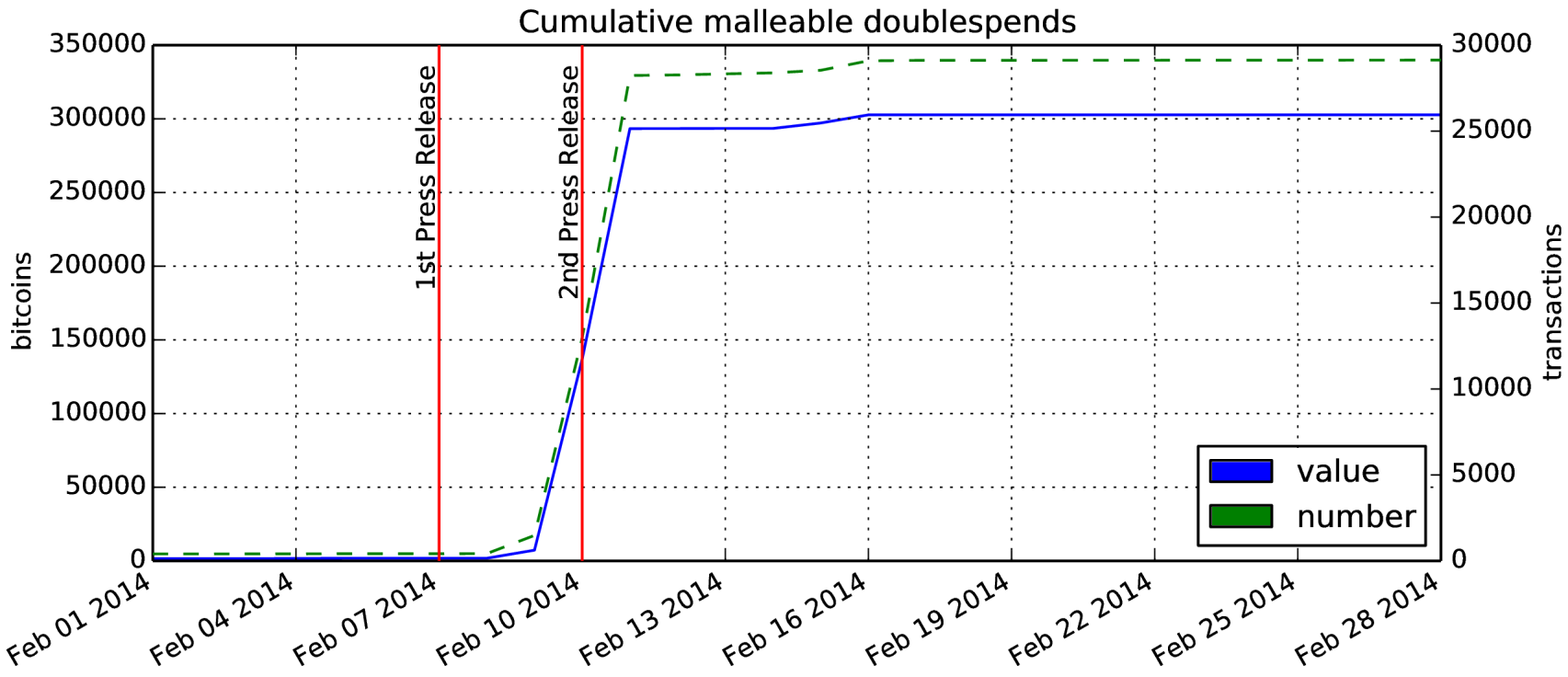
Transaction Malleability Attack



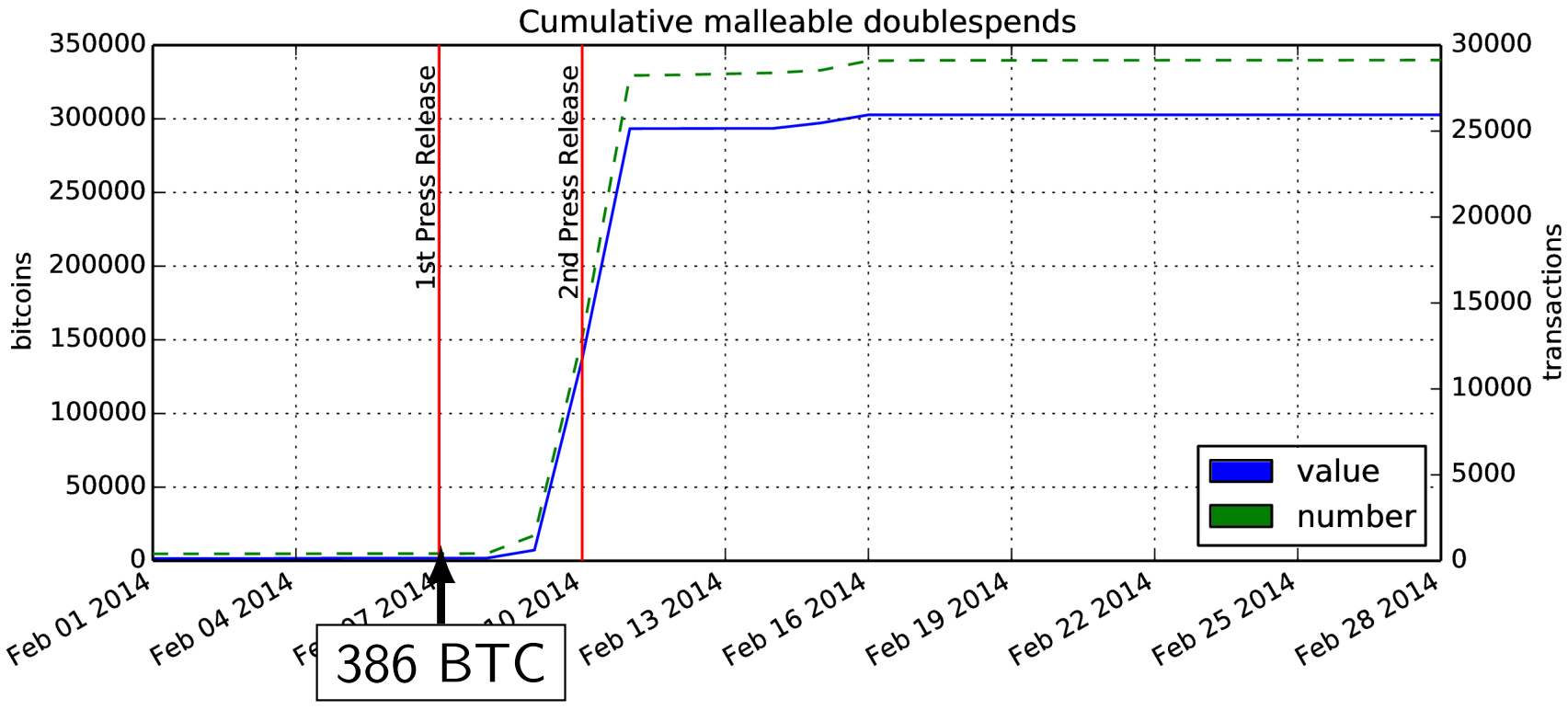
Transaction Malleability Attack



Incident Timeline

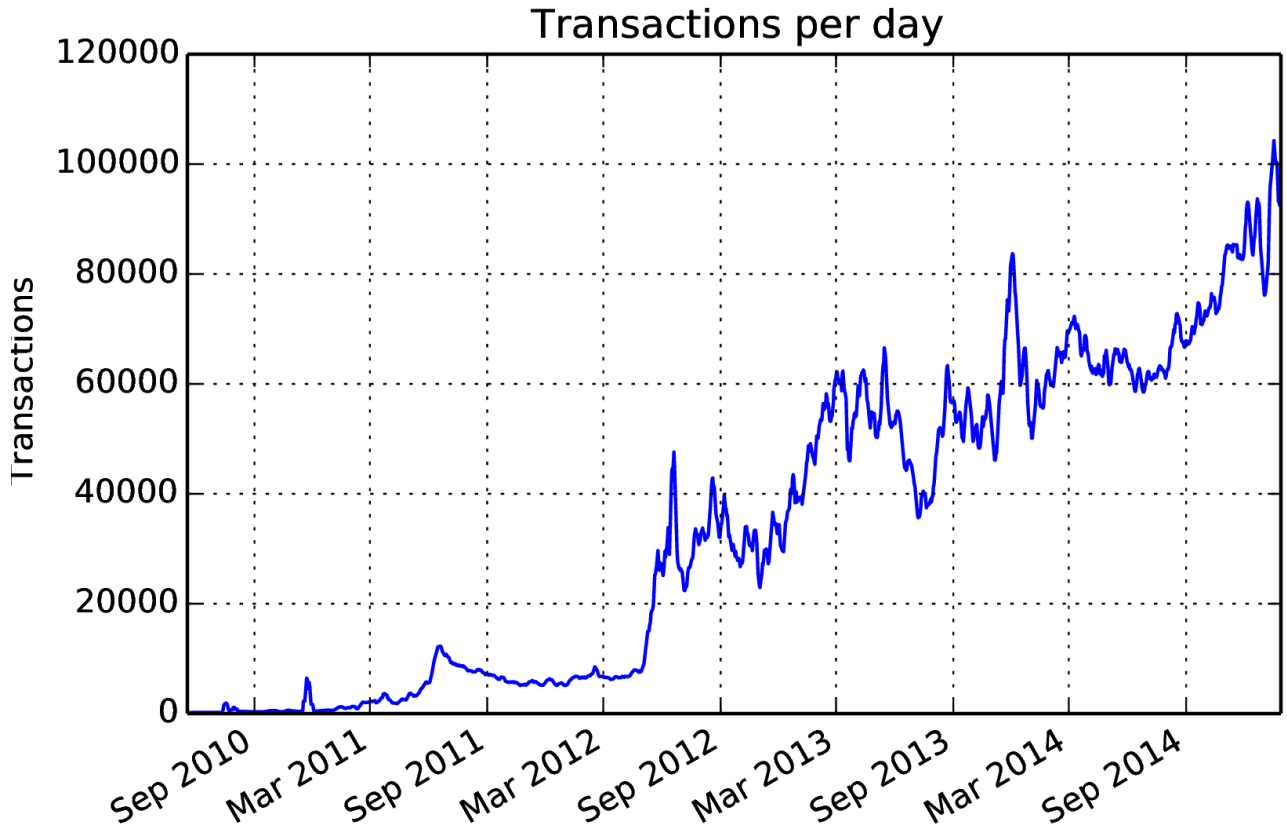


Incident Timeline

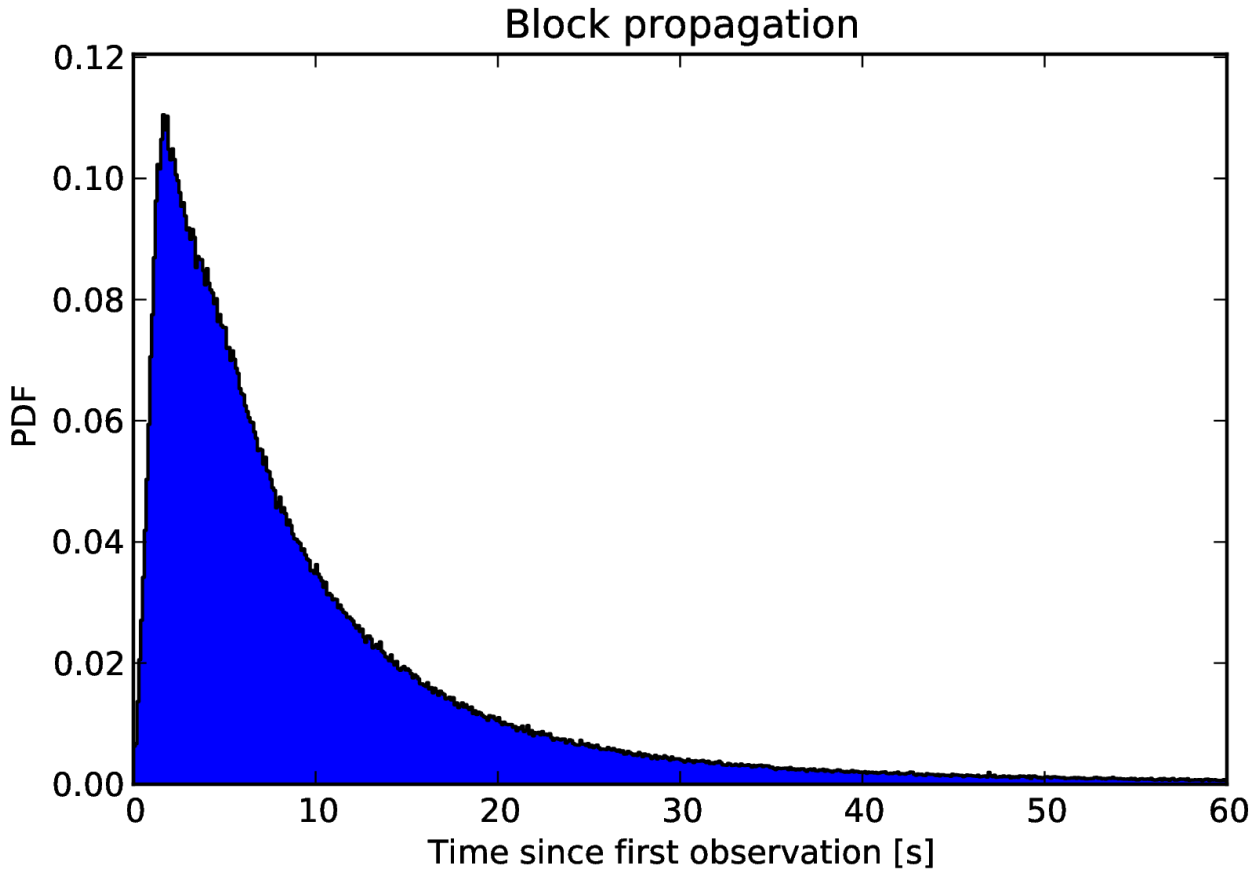


Does Bitcoin Scale?

The Bitcoin Ecosystem is Growing

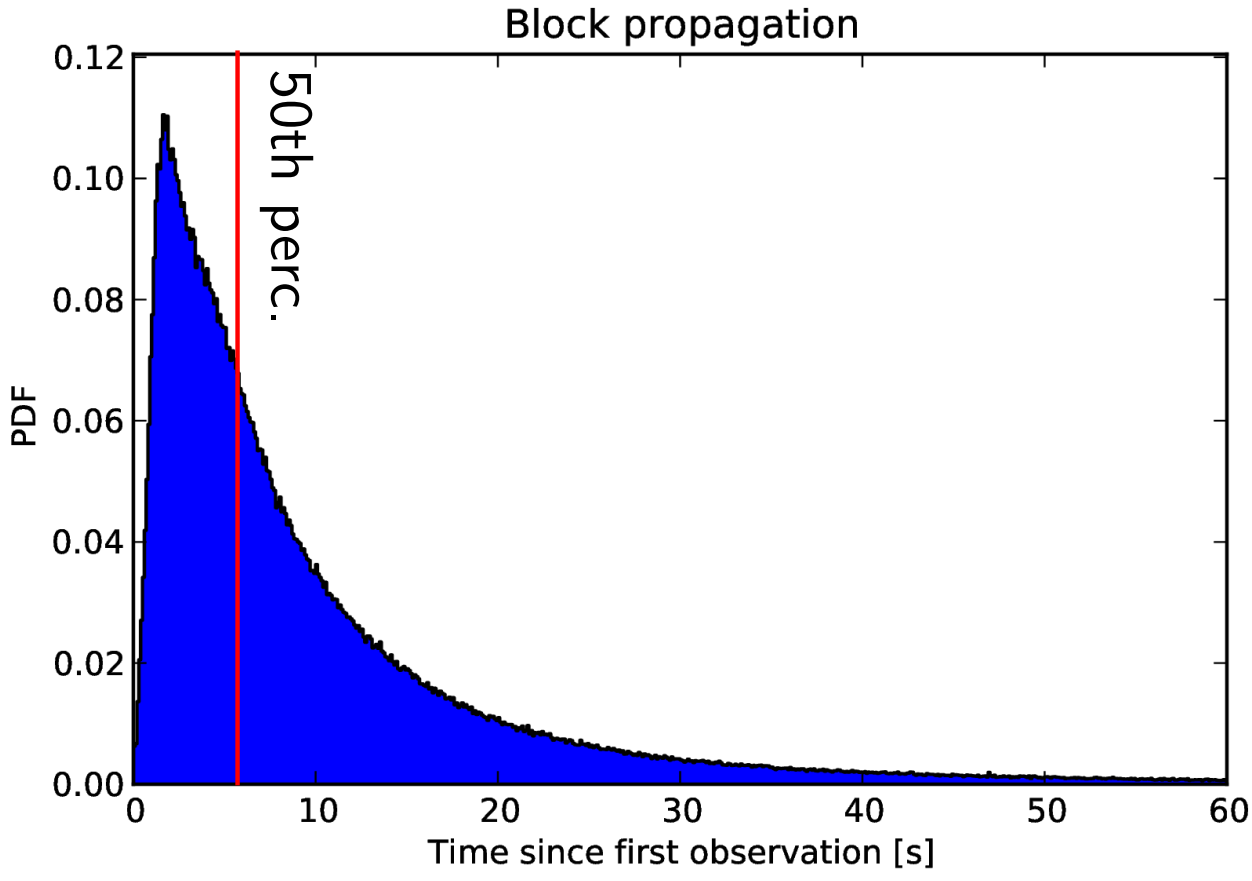


Propagation Speed



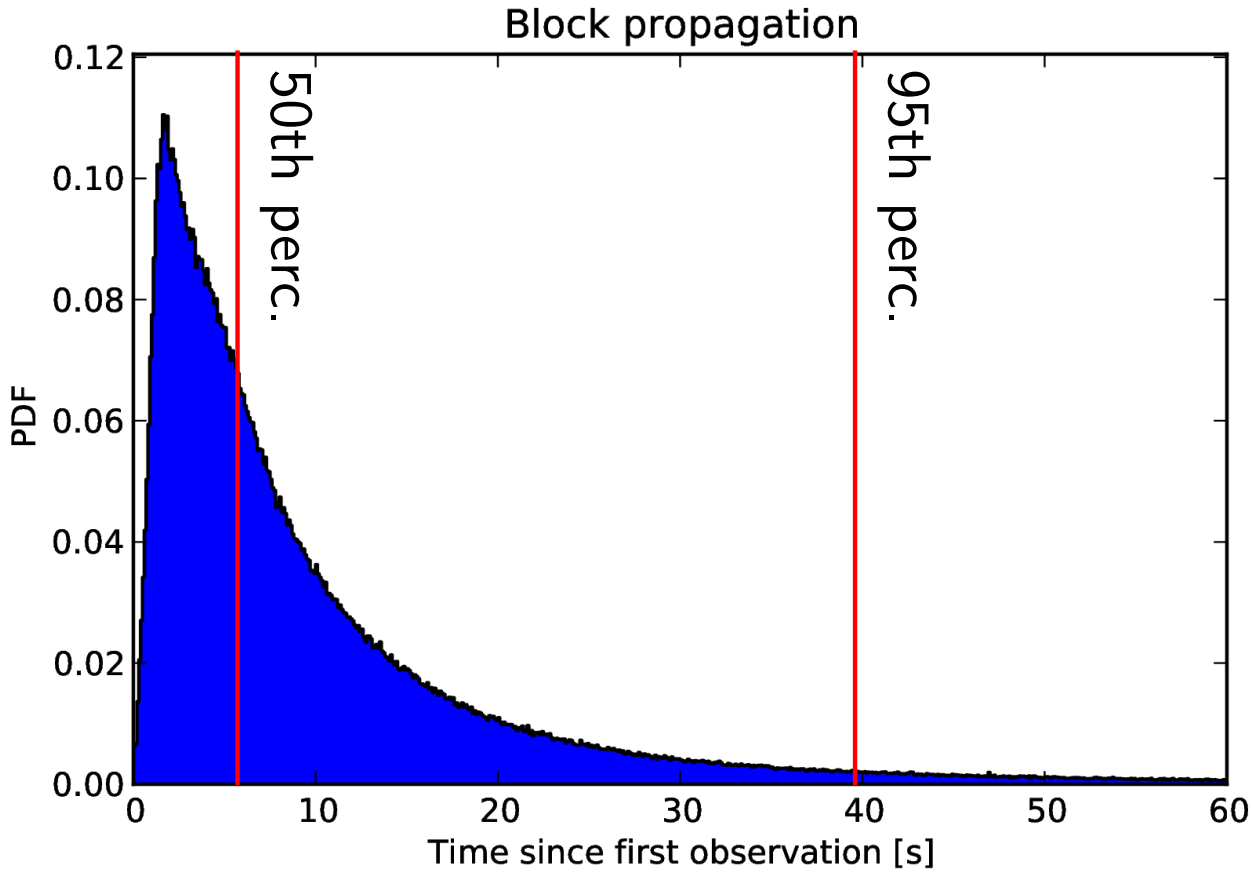
http://bitcoinstats.com

Propagation Speed



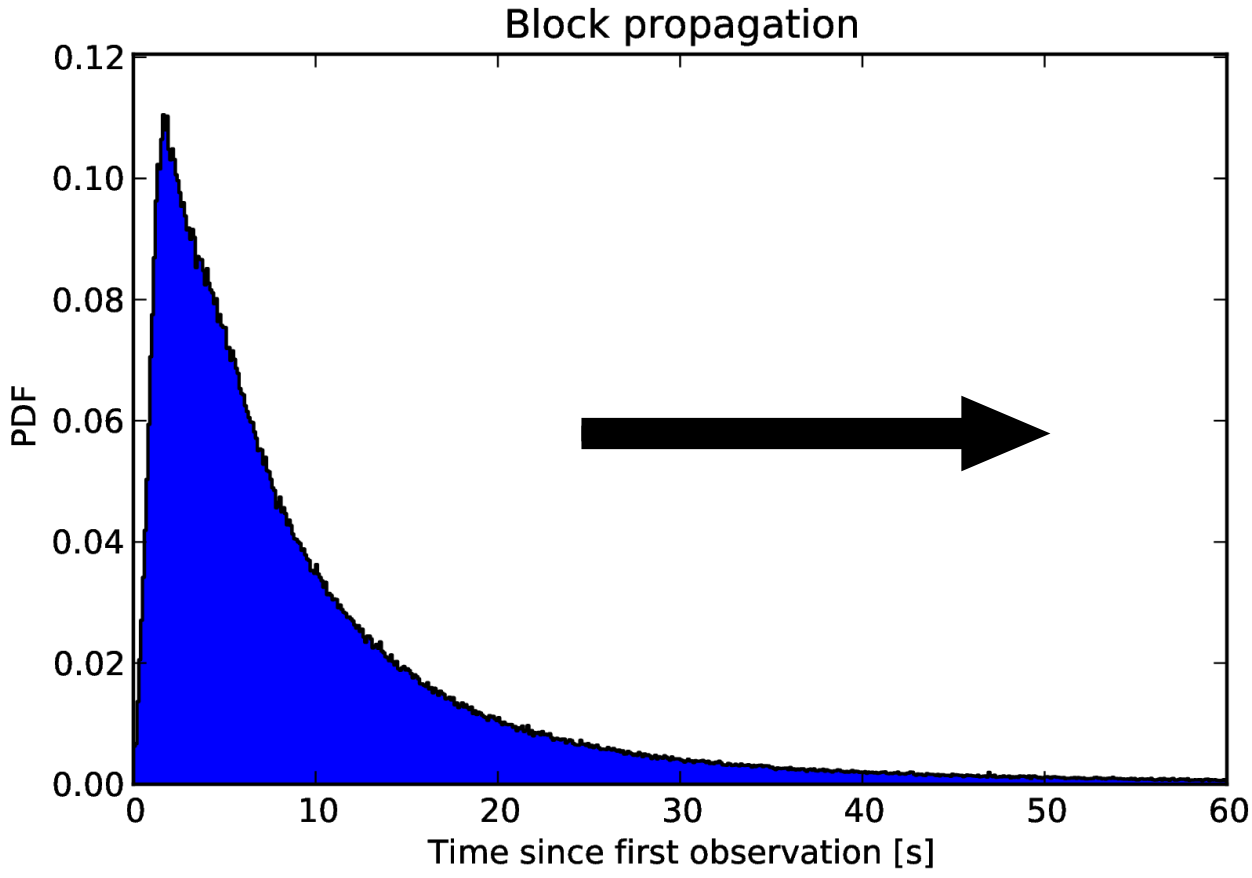
http://bitcoinstats.com

Propagation Speed



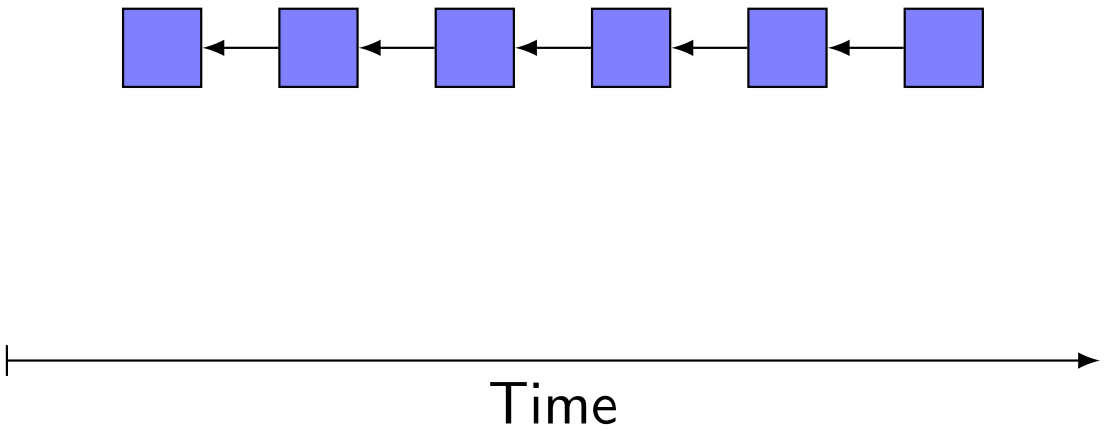
http://bitcoinstats.com

Propagation Speed

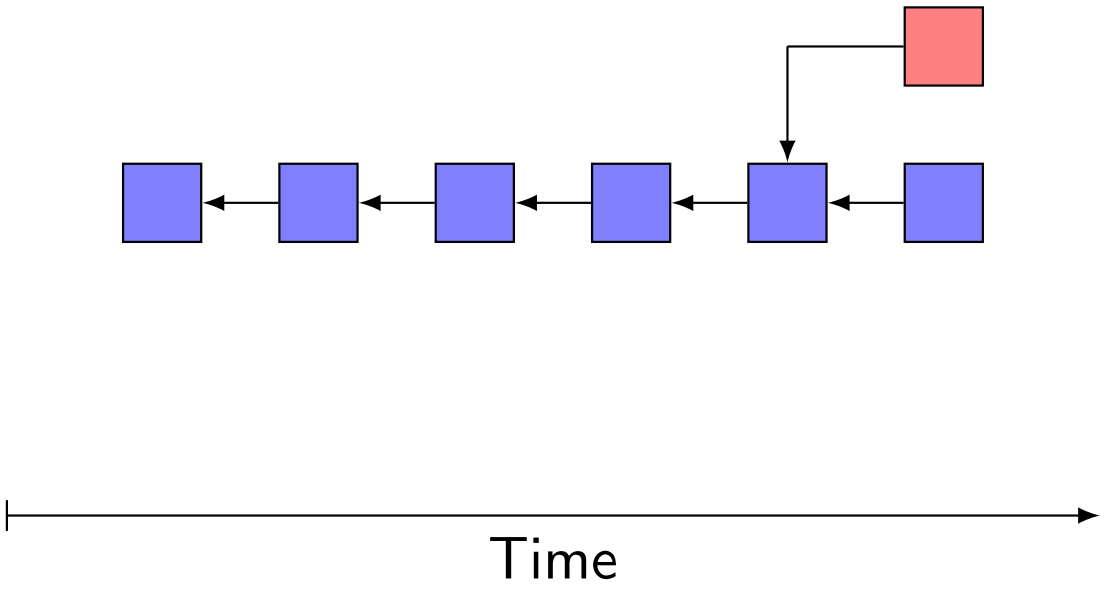


http://bitcoinstats.com

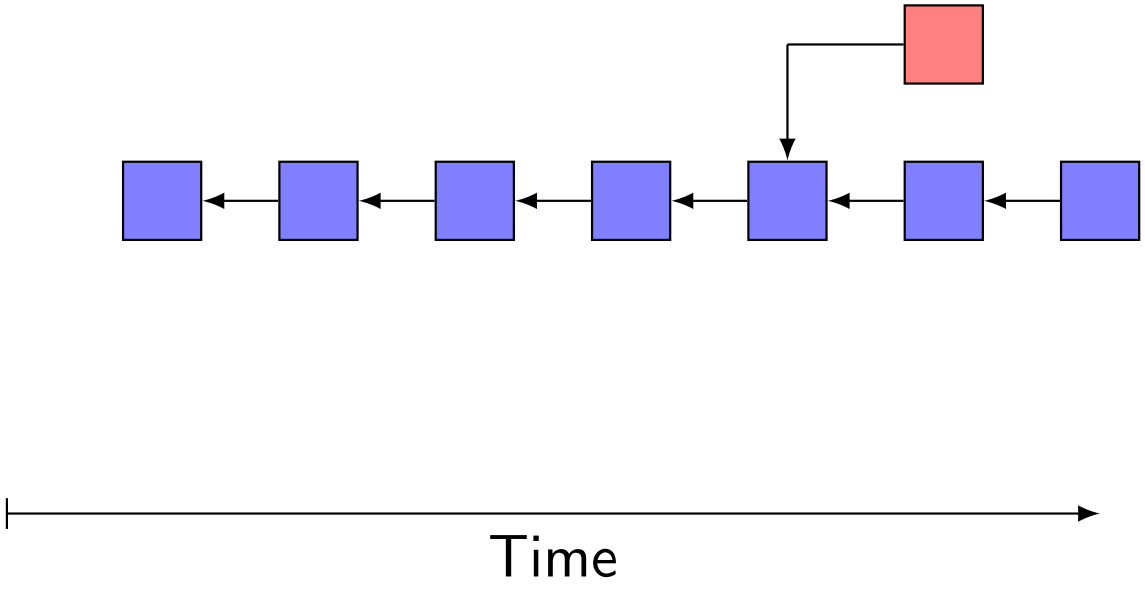
Blockchain



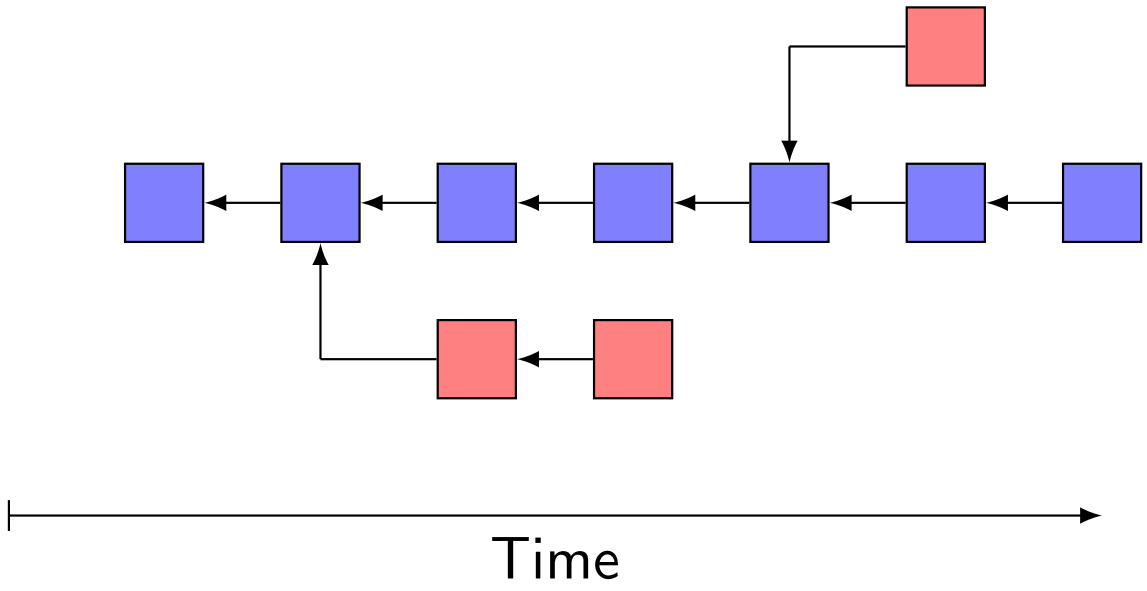
Blockchain



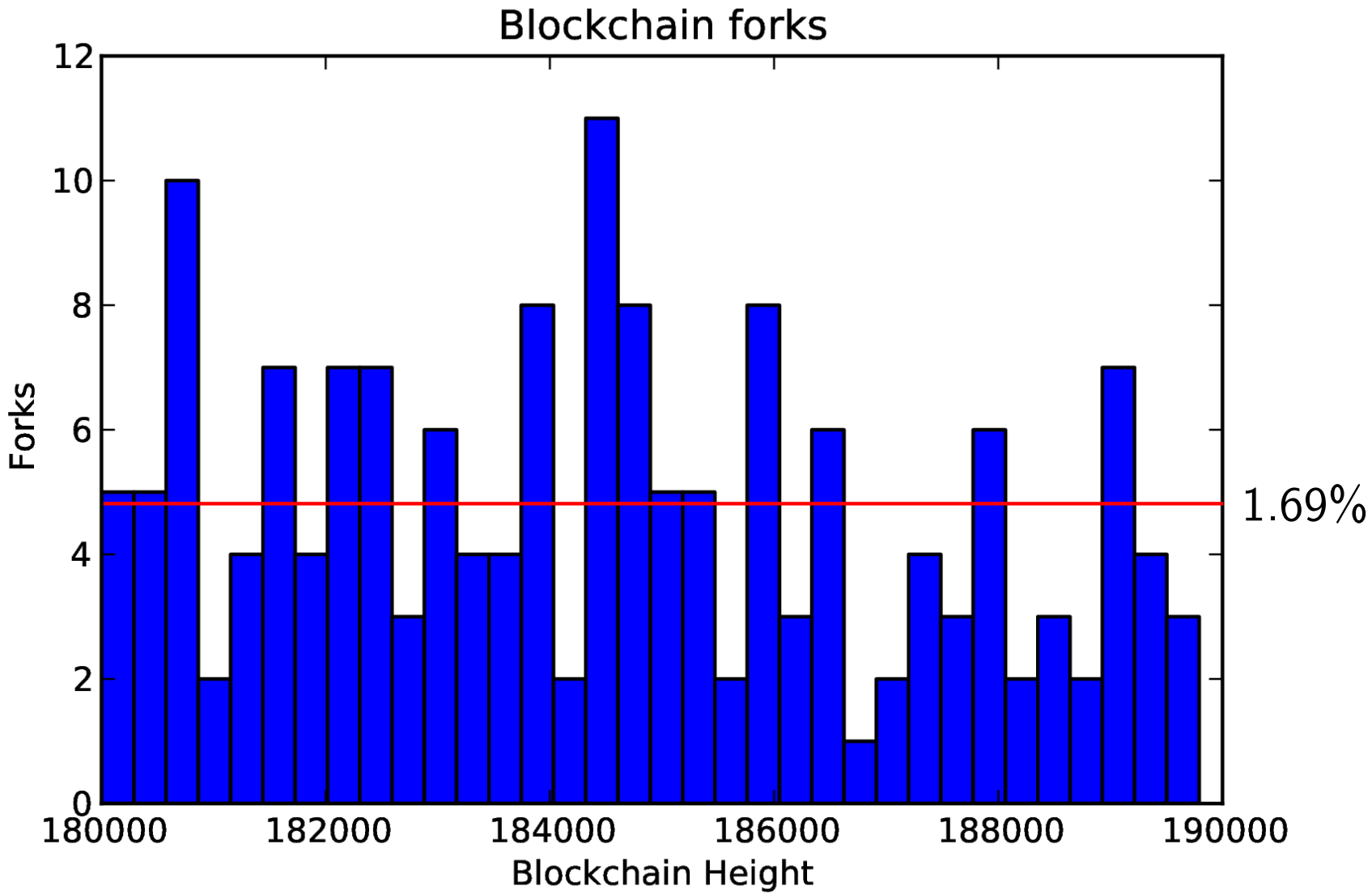
Blockchain



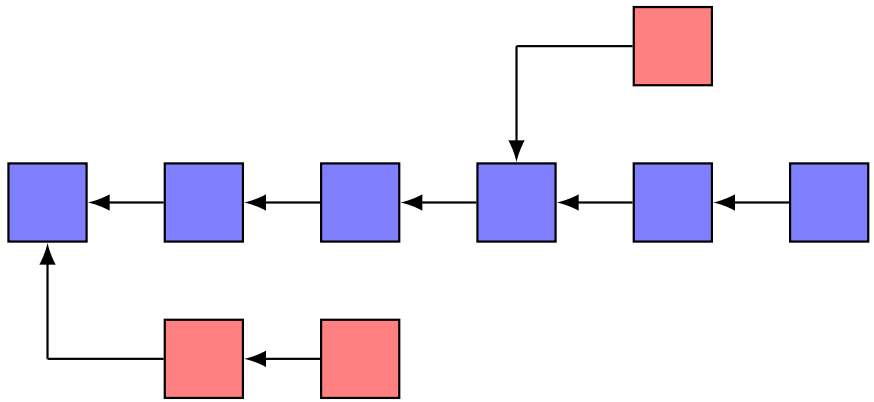
Blockchain



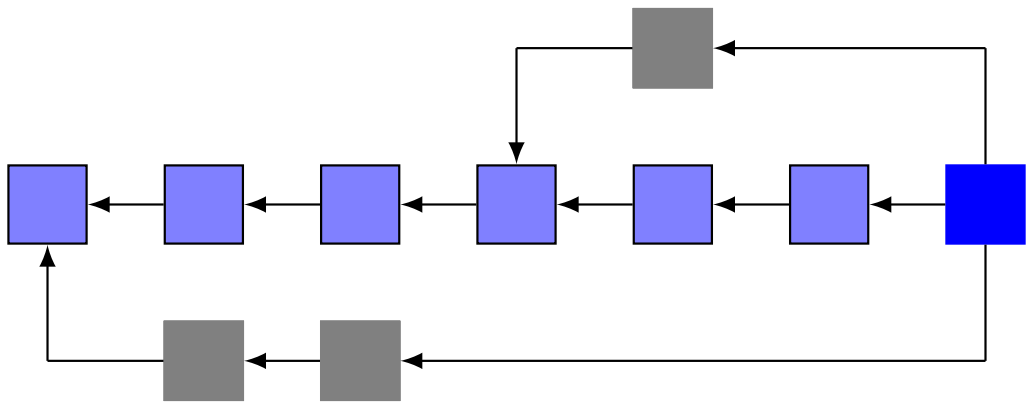
Forks


Blockchain forks
Forks
Blockchain Height
0
2
4
6
8
10
12
180000
182000
184000
186000
188000
190000
1.69%

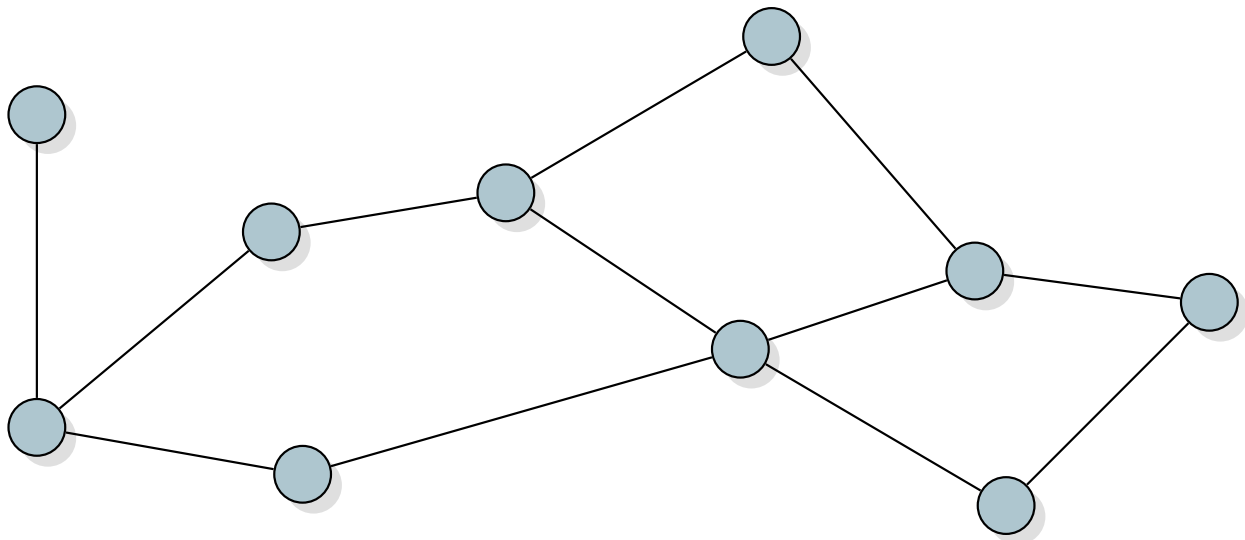
GHOST



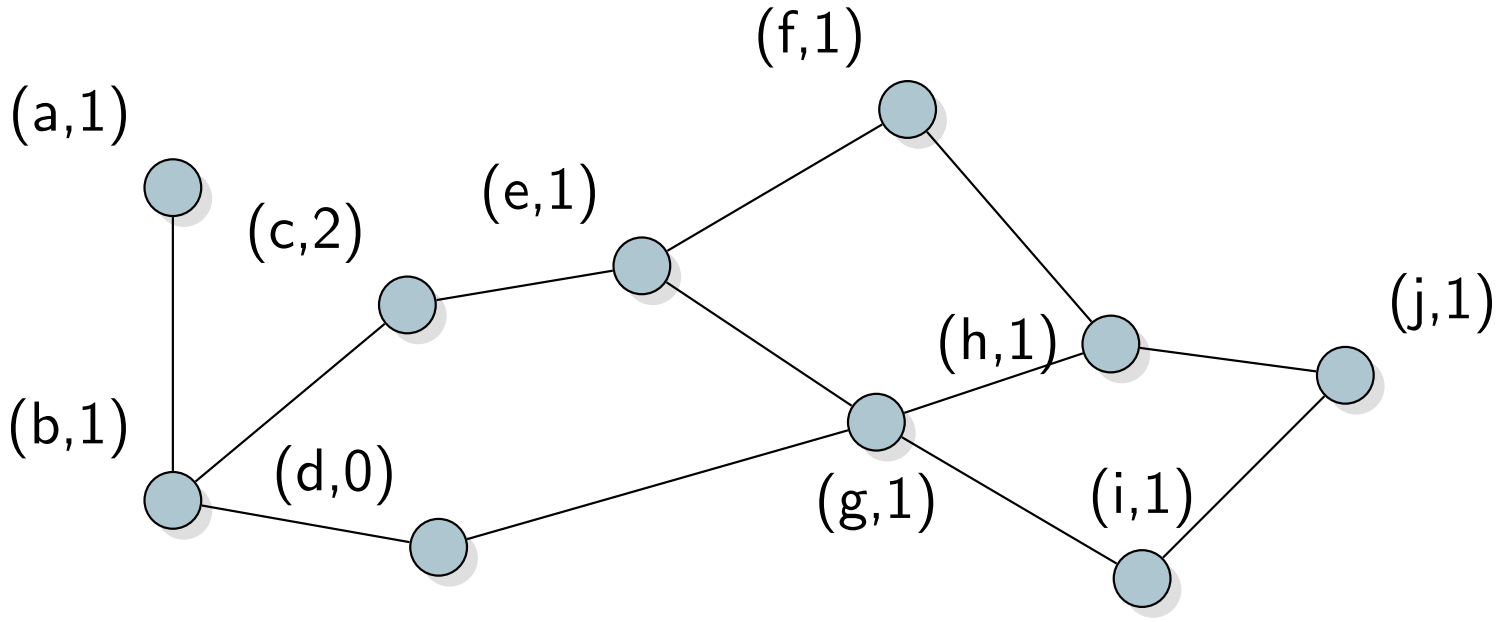
GHOST



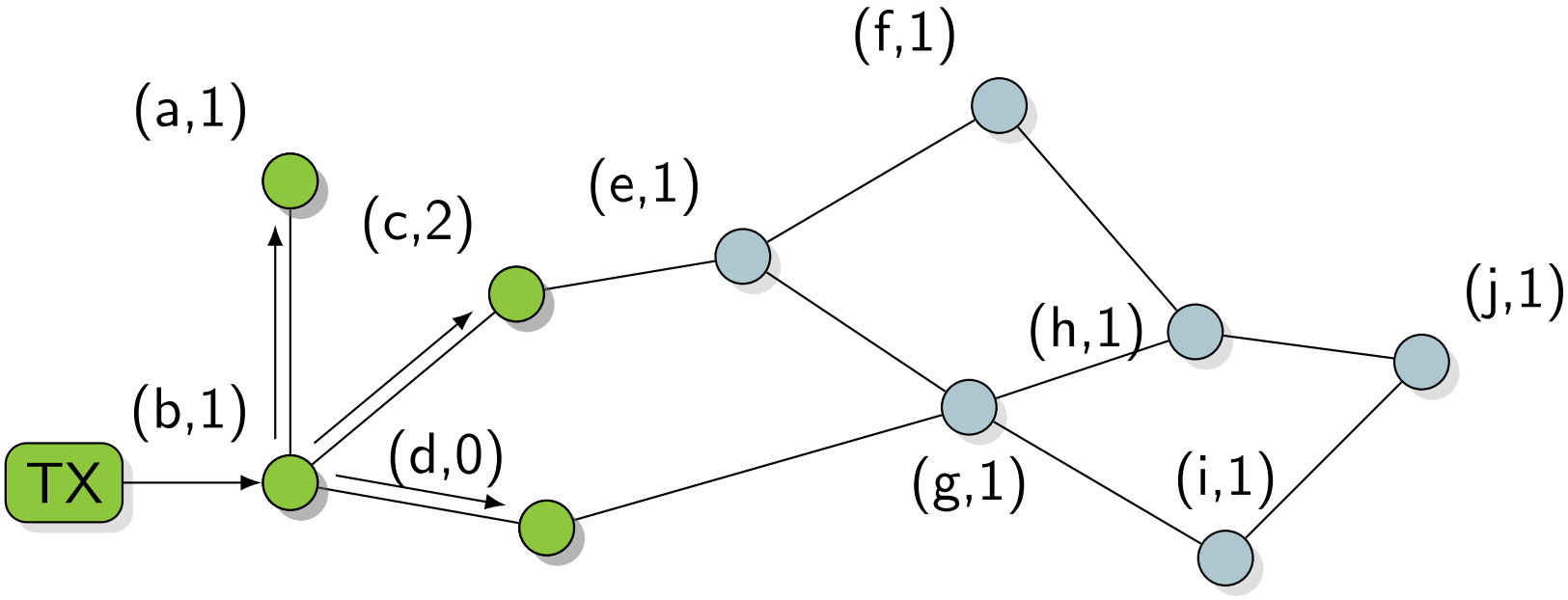
Bitcoin Meets Strong Consistency

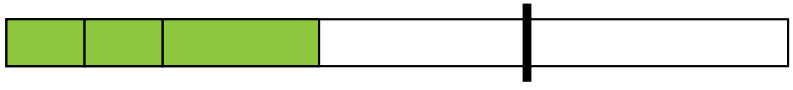


Bitcoin Meets Strong Consistency

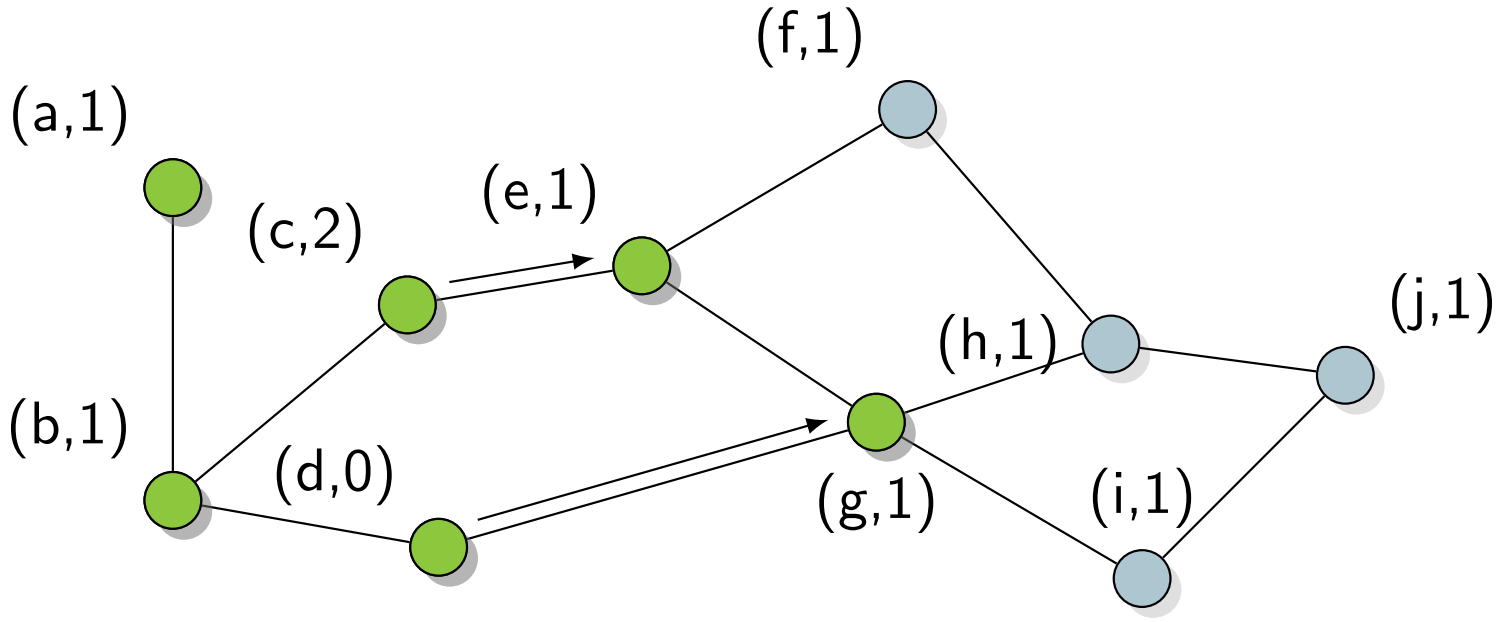


Bitcoin Meets Strong Consistency



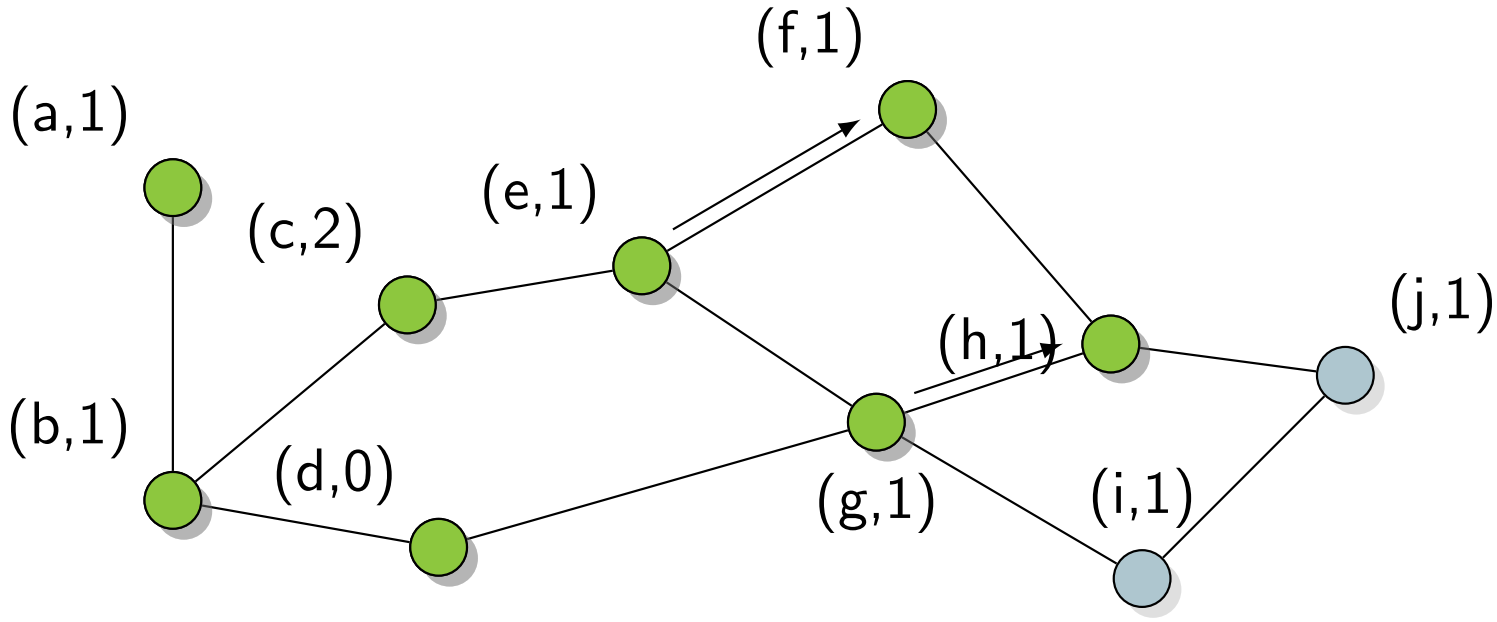
$votes(TX) =$ 

Bitcoin Meets Strong Consistency



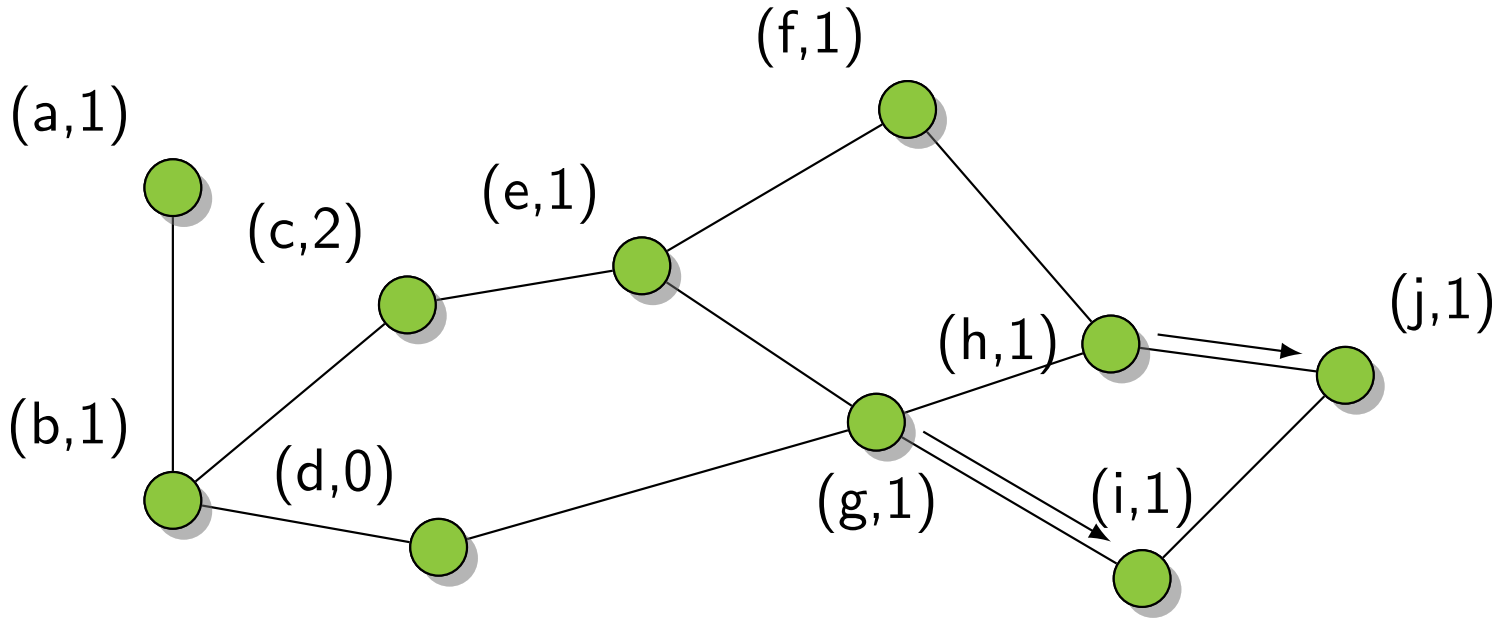
$votes(TX) =$ 

Bitcoin Meets Strong Consistency



$votes(TX) =$ 

Bitcoin Meets Strong Consistency



$votes(TX) =$ 

Summary

- Bitcoin is not perfect. . .

Summary

- Bitcoin is not perfect...
- ...but we're working on it

Summary

- Bitcoin is not perfect...
- ...but we're working on it
- Be aware of tradeoffs!

Thank you, questions?