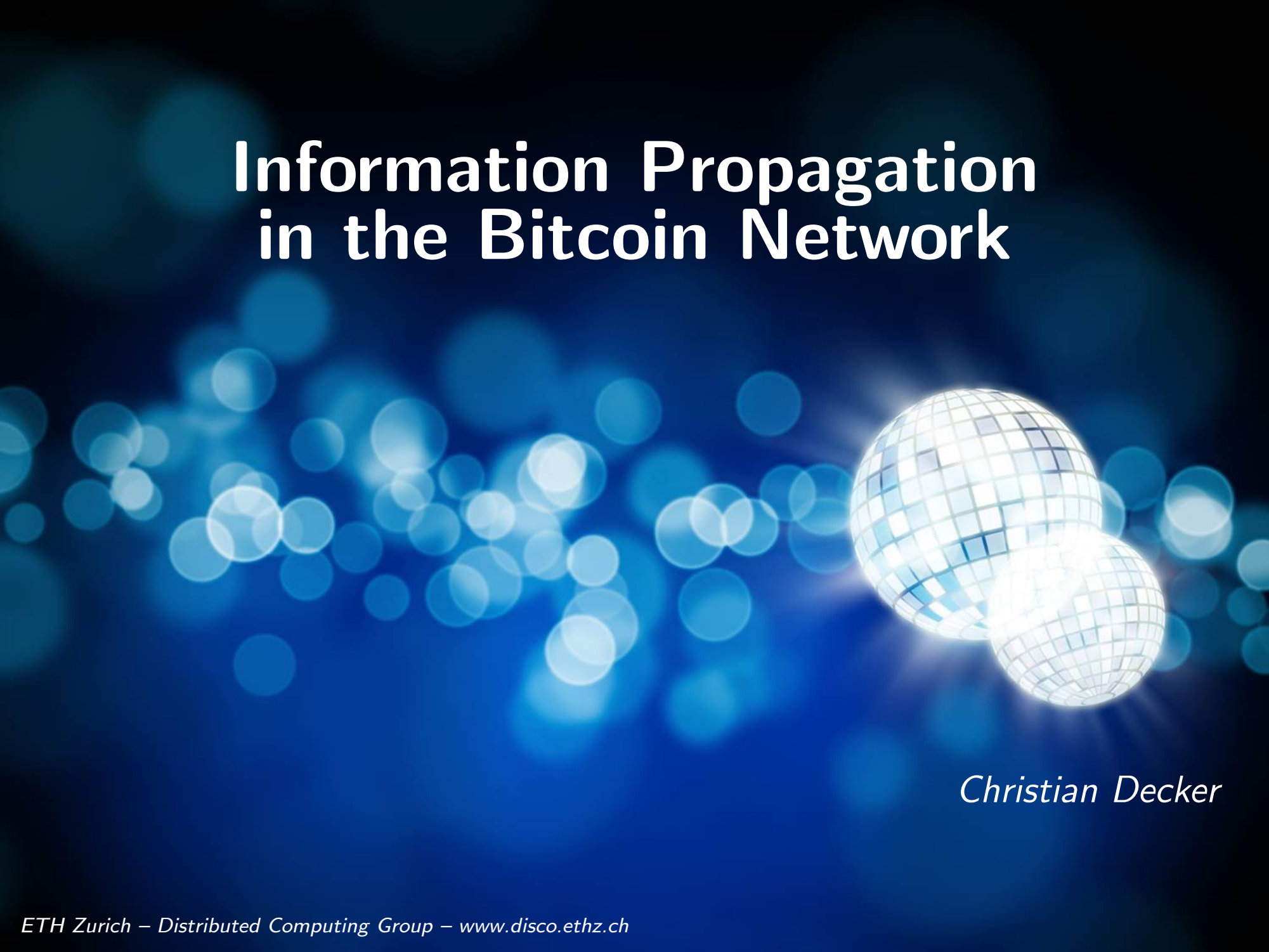
Information Propagation in the Bitcoin Network



Christian Decker

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

What is Bitcoin?

What is Bitcoin?

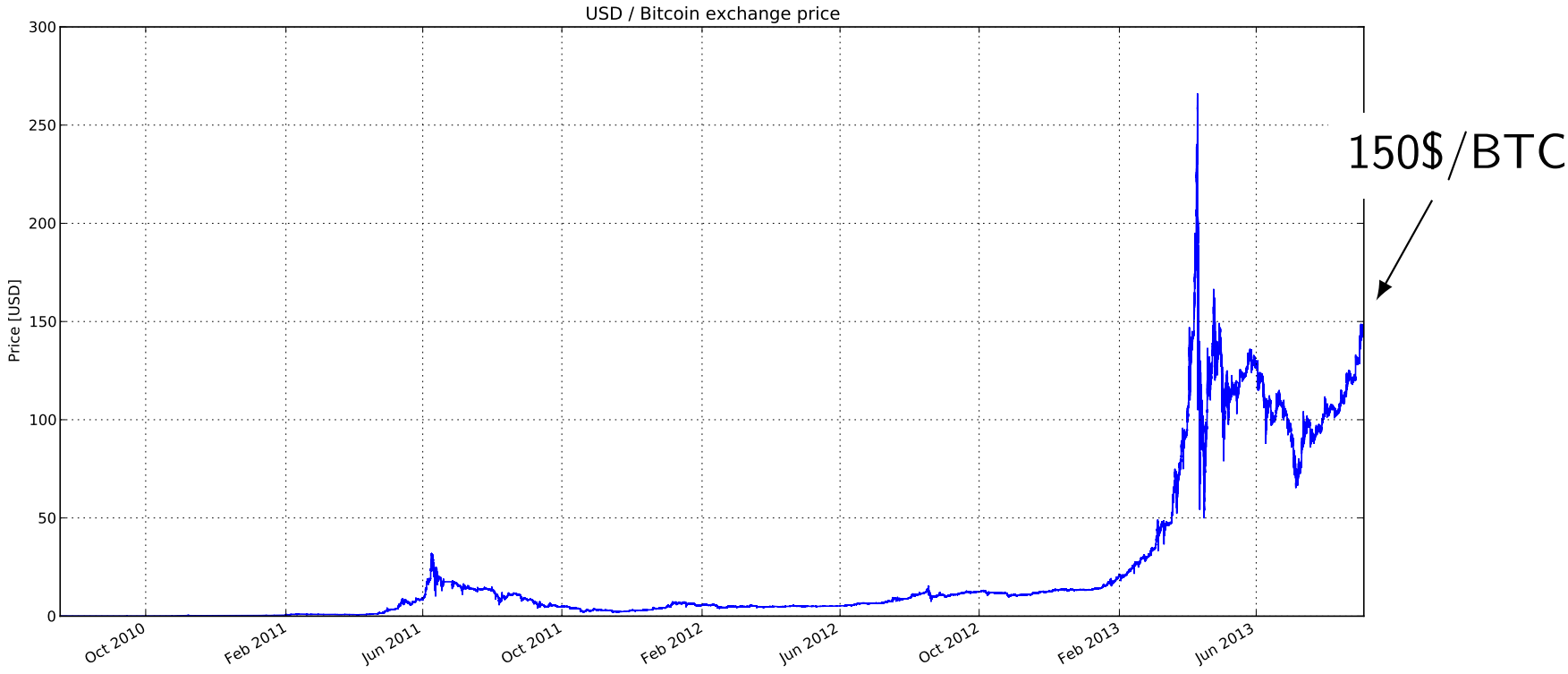
+

What is Bitcoin?

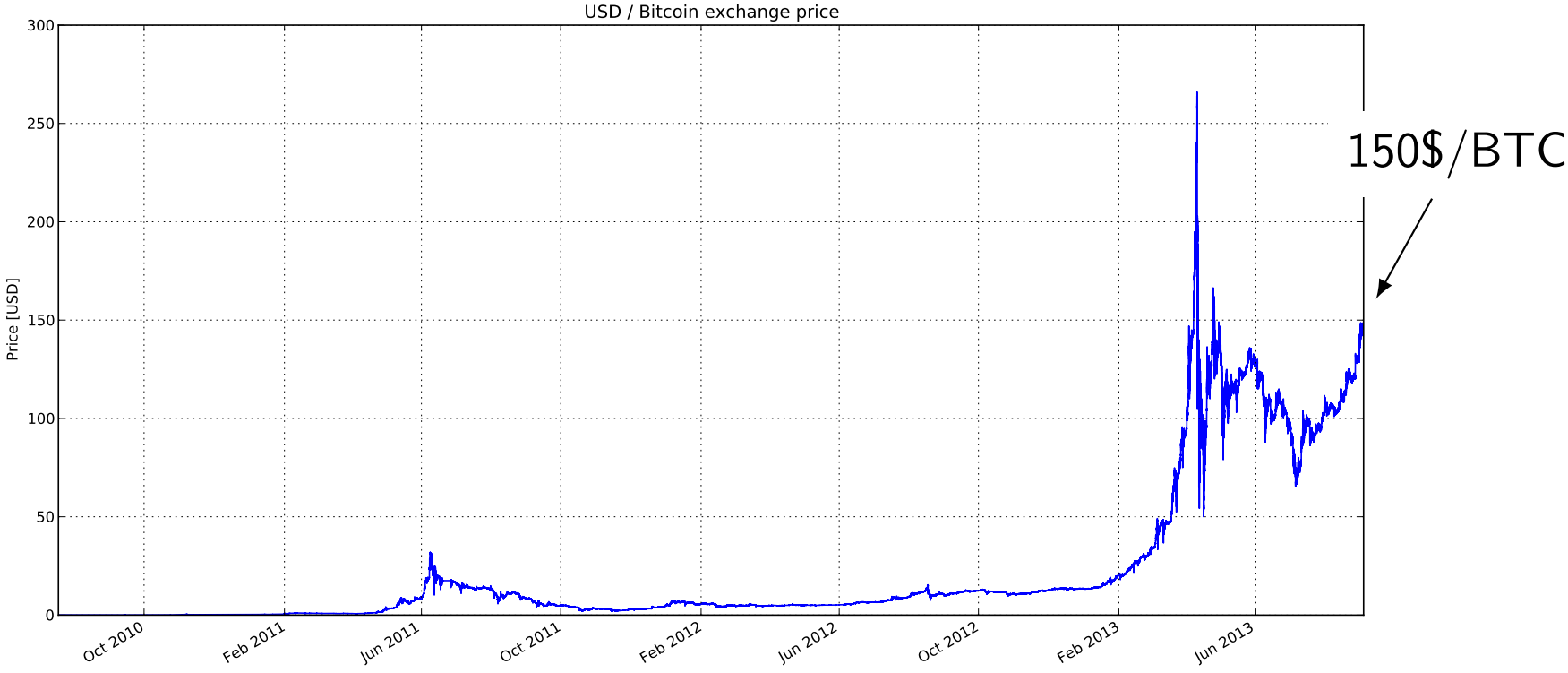
+

=

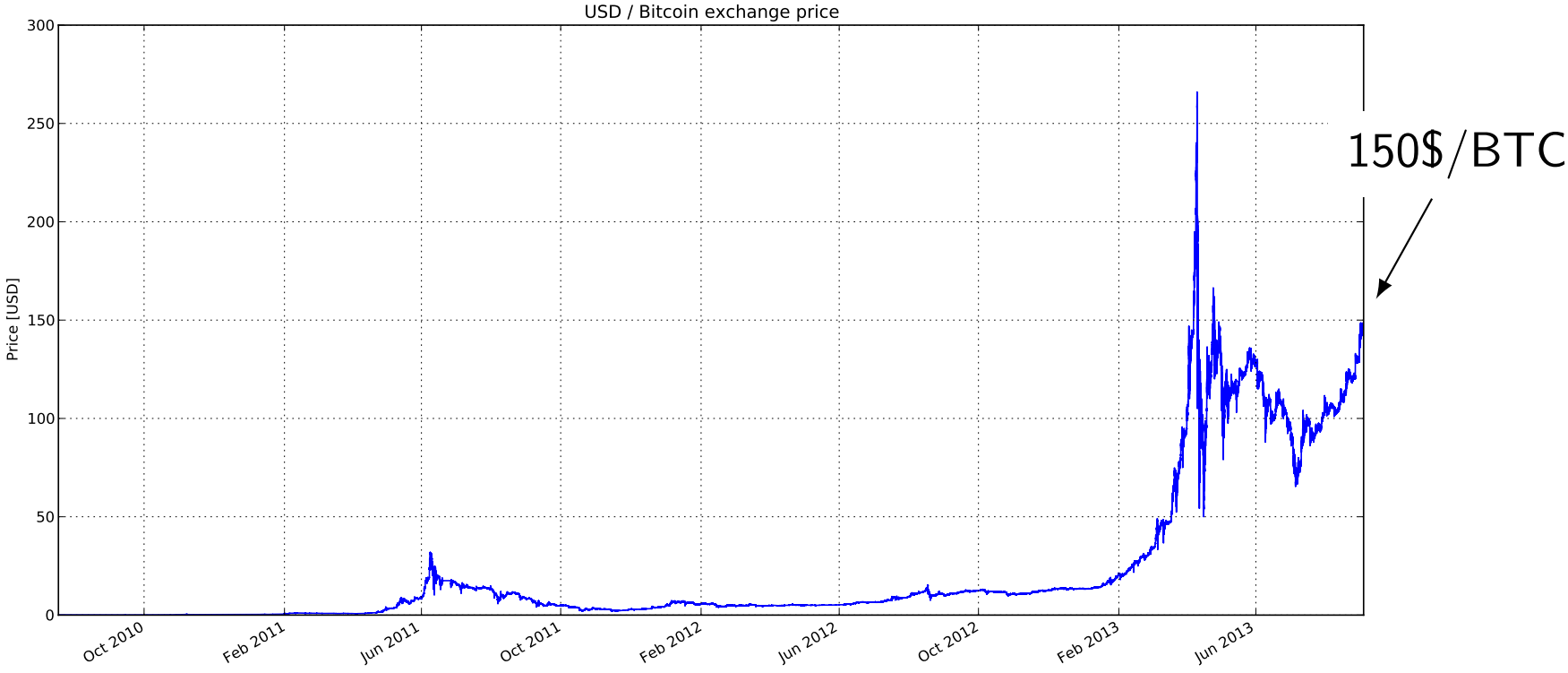
What's it worth?



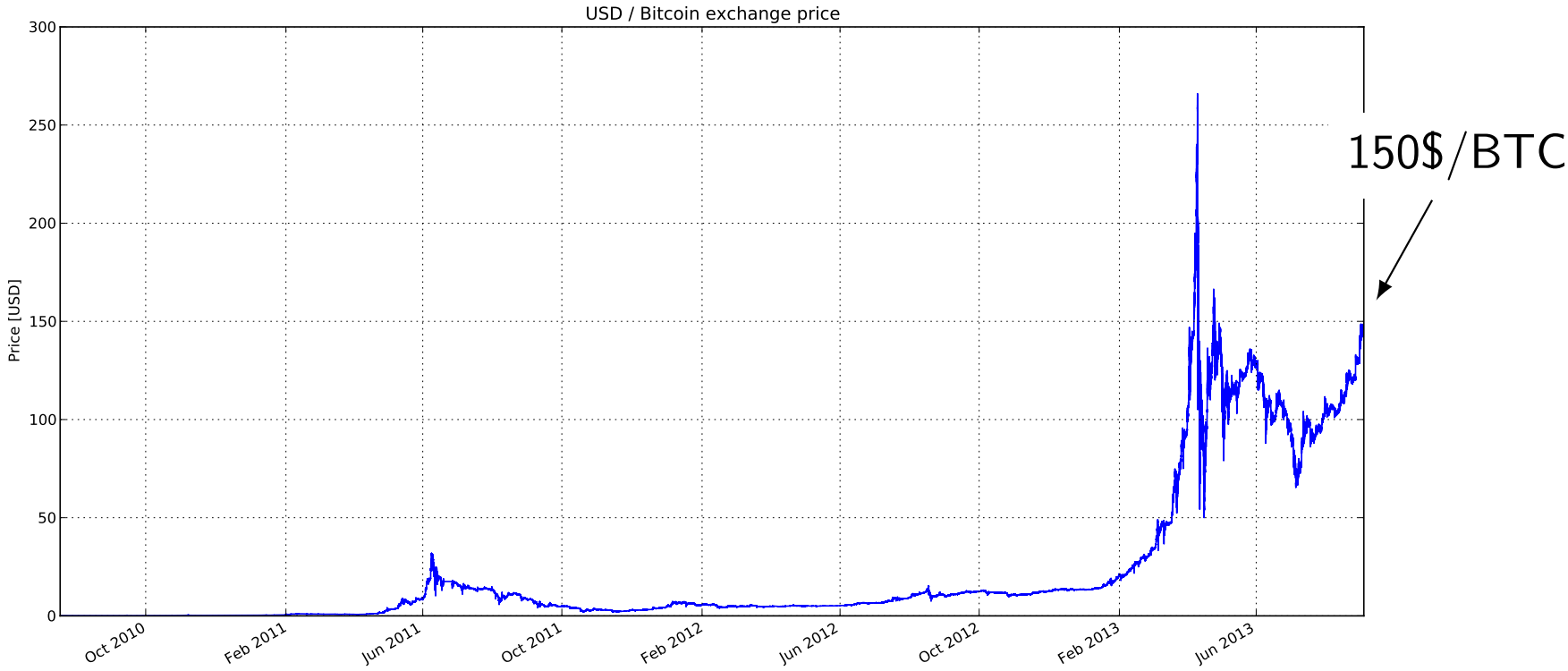
What's it worth?



What's it worth?



What's it worth?

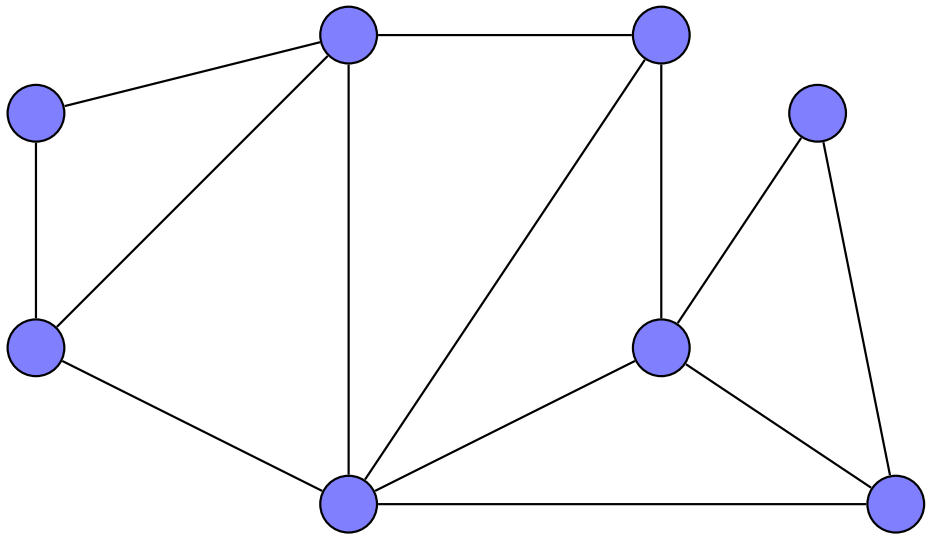


Why so popular?

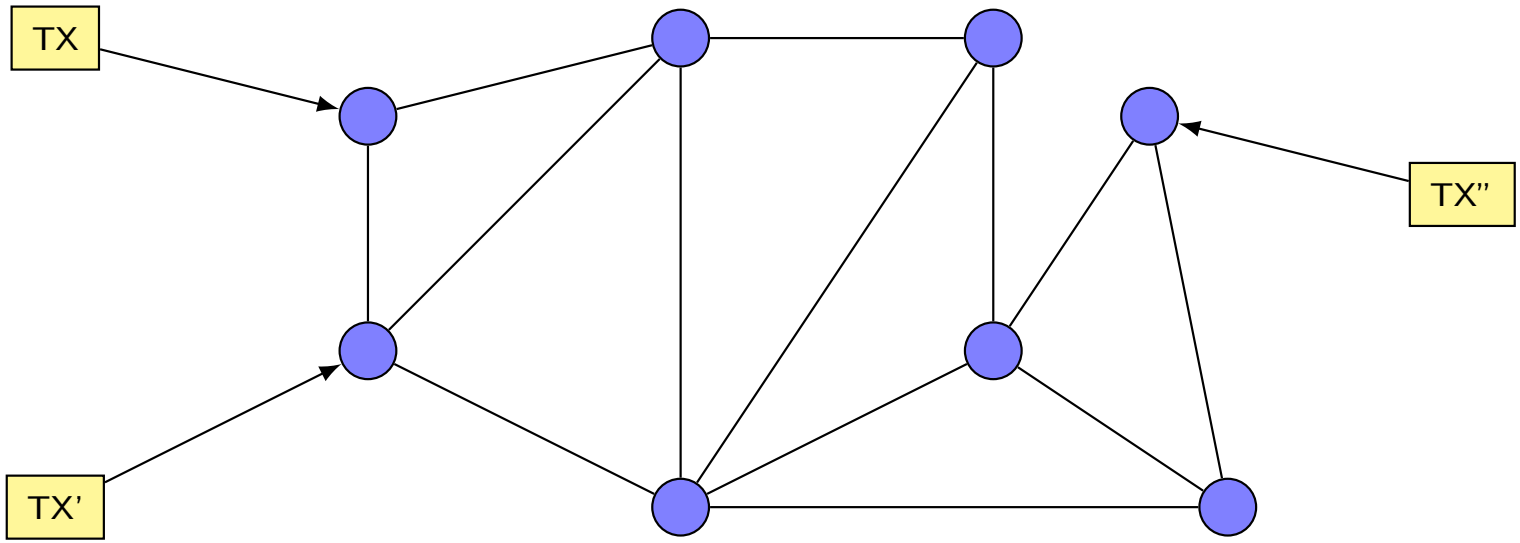
- Global
- Fast
- Irreversible
- No intermediary
- Anonymous

Bitcoin Basics

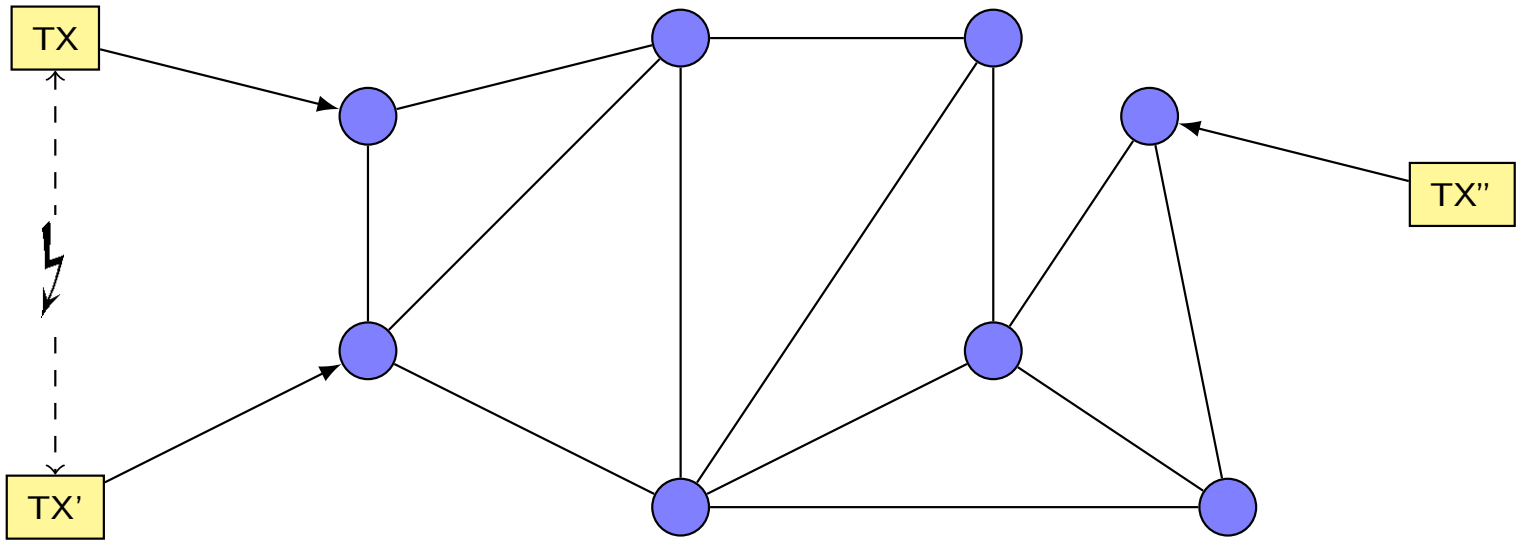
Bitcoin basics



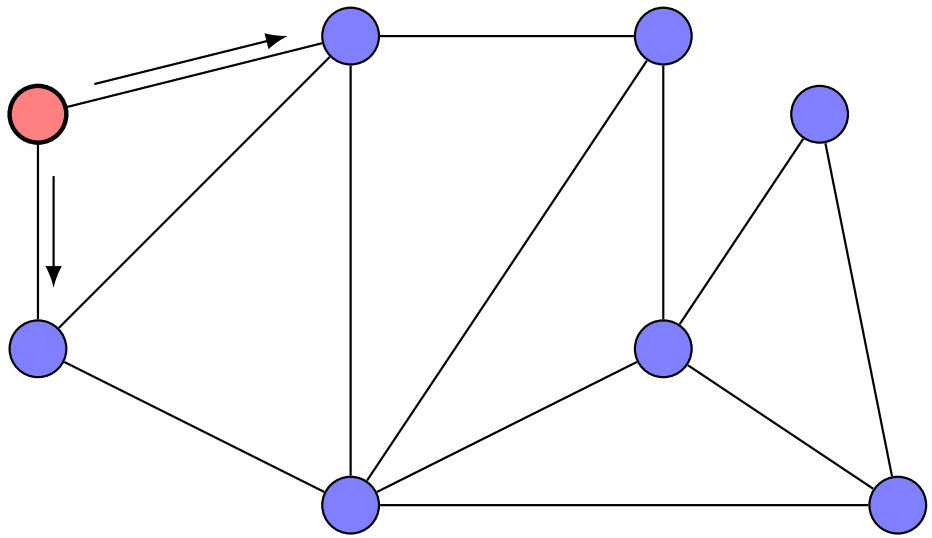
Bitcoin basics



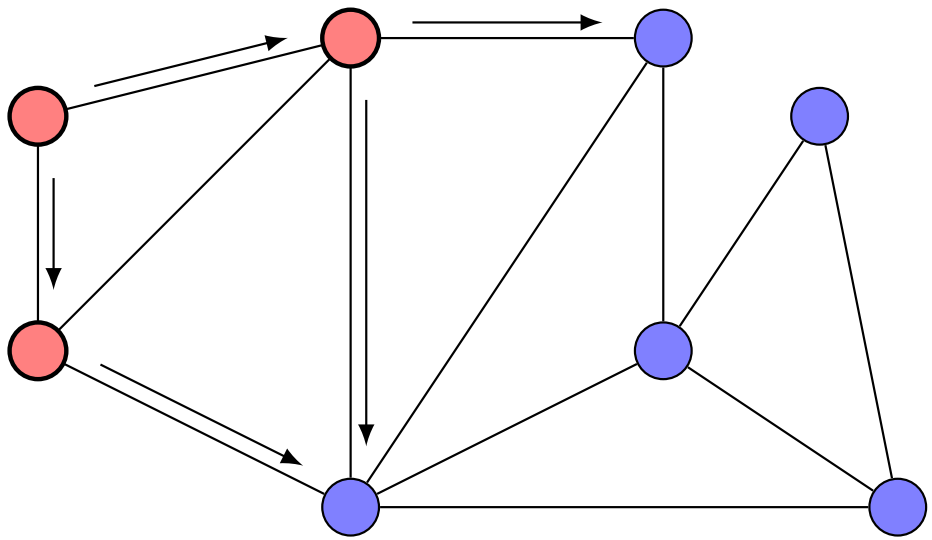
Bitcoin basics



Bitcoin basics

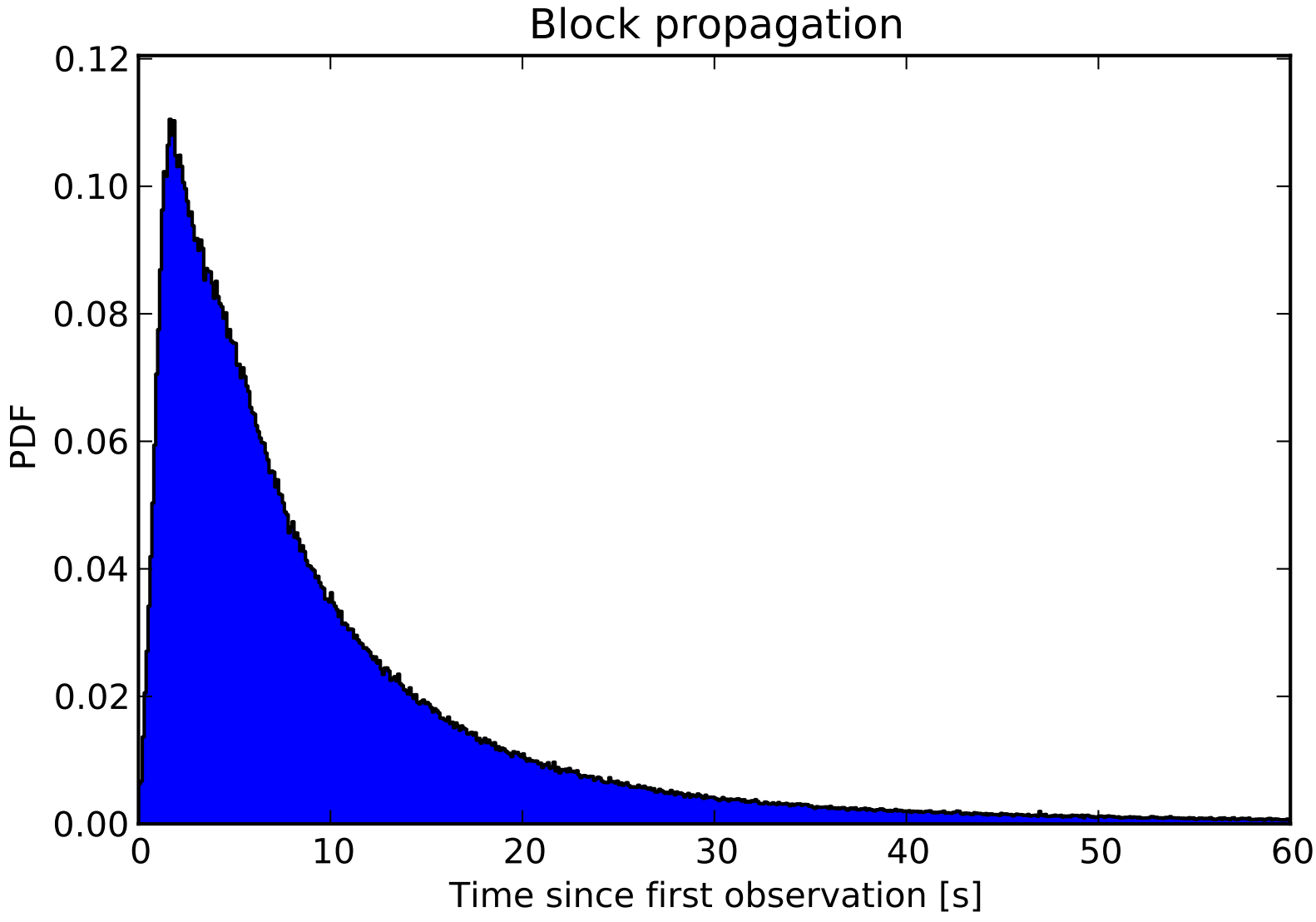


Bitcoin basics

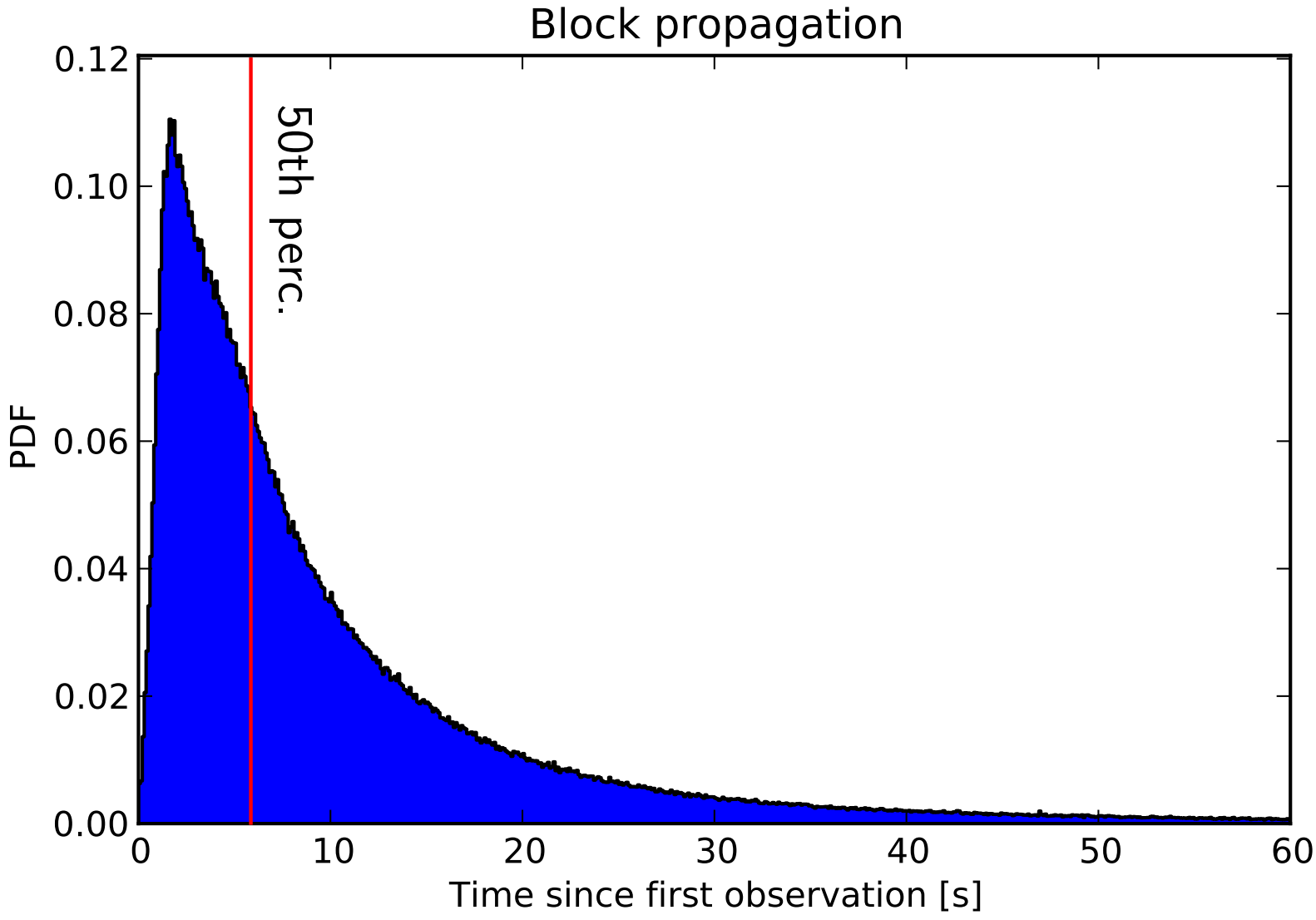


Our Results

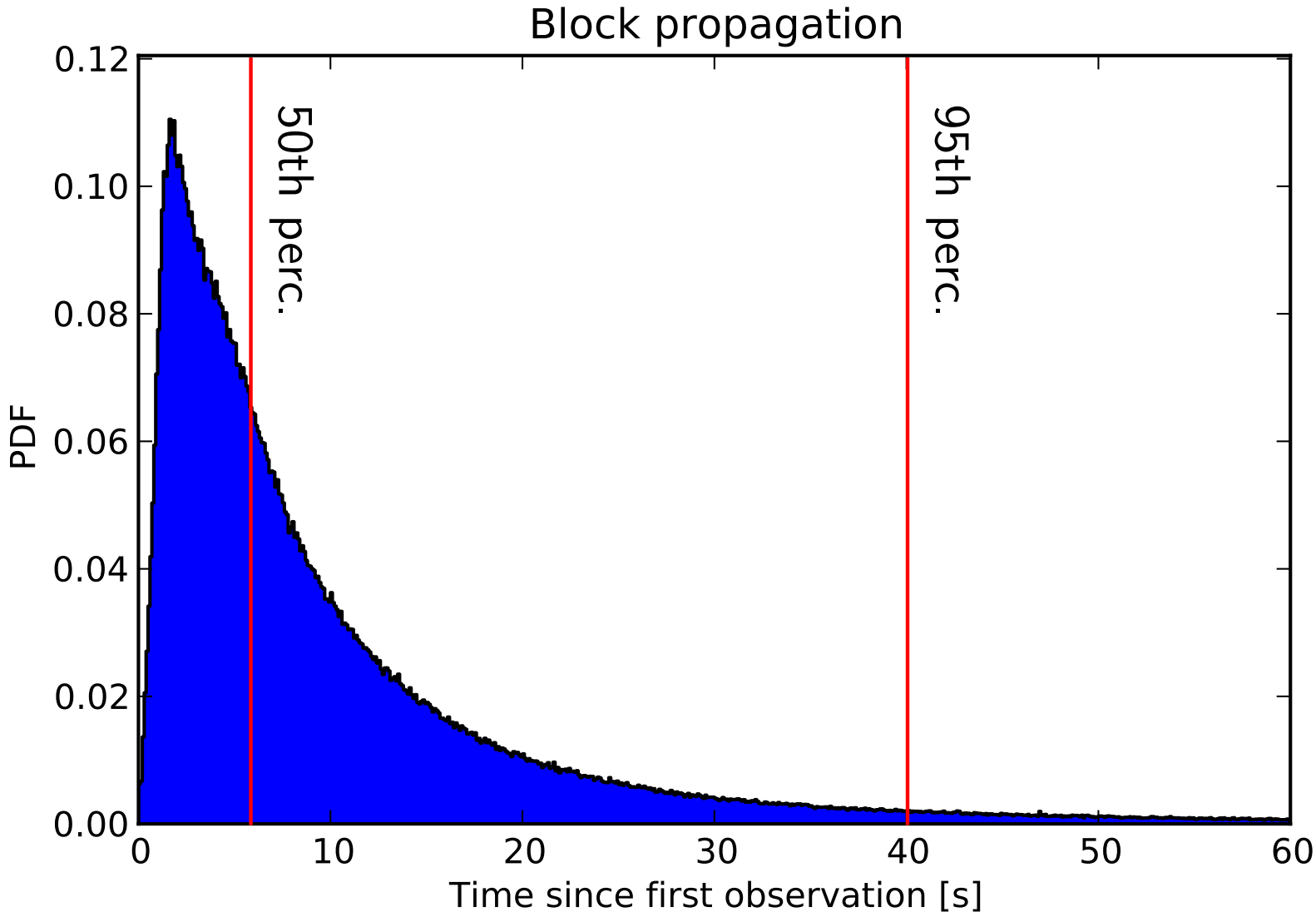
Propagation speed



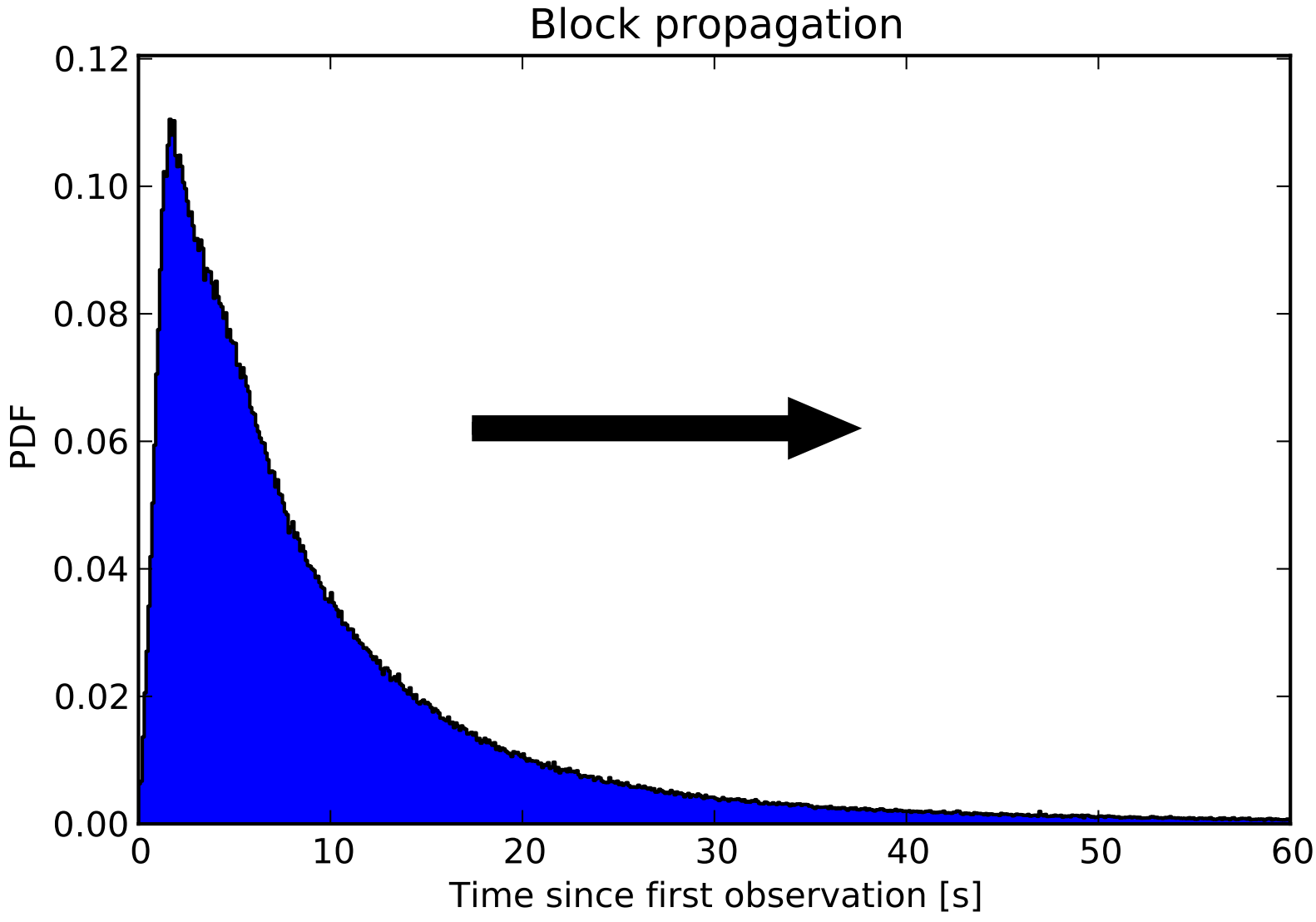
Propagation speed



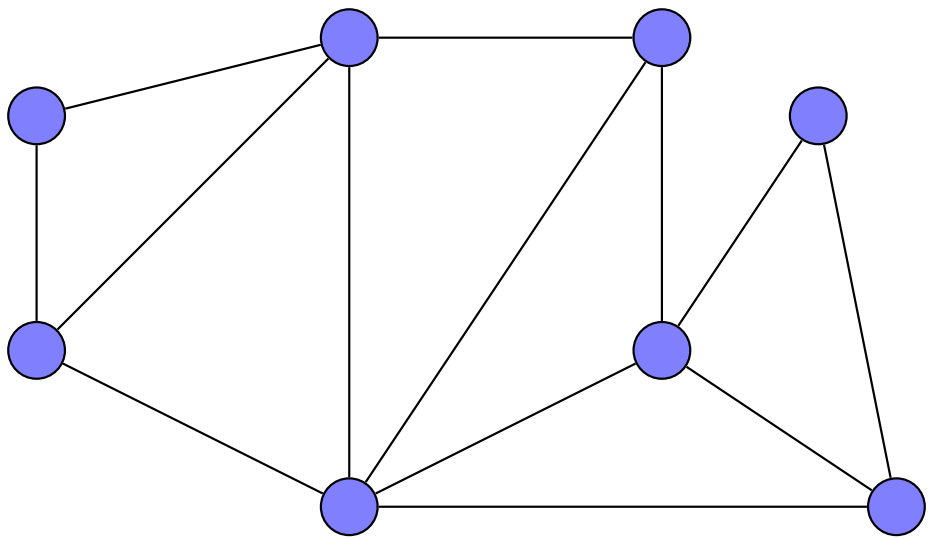
Propagation speed



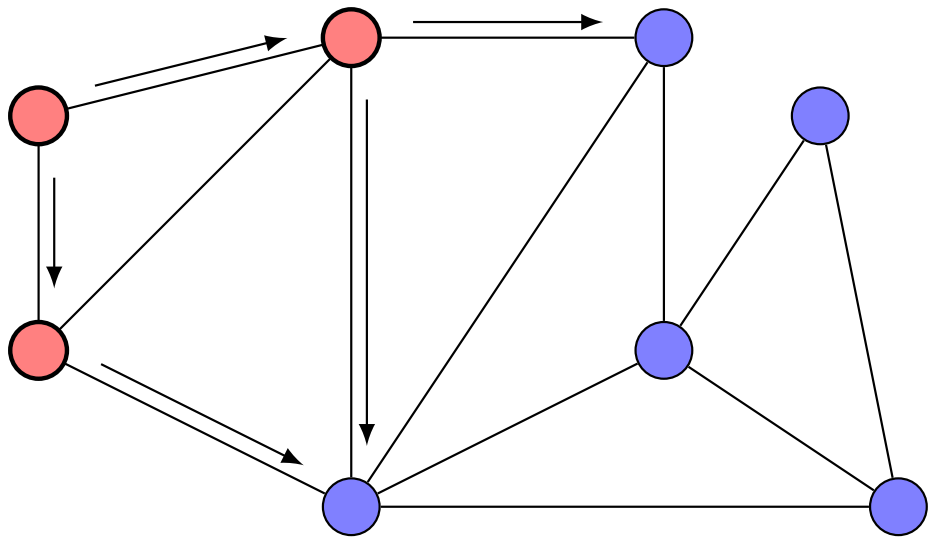
Propagation speed



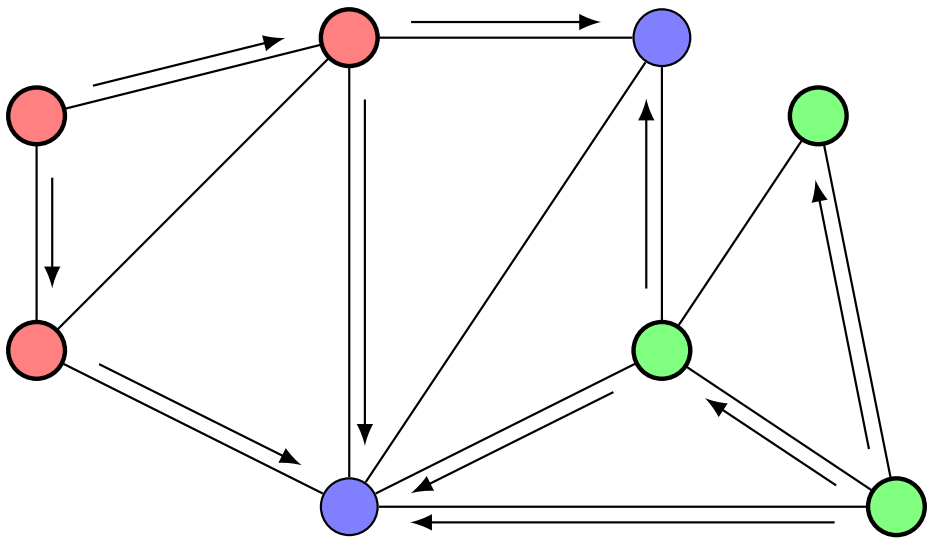
Information eclipsing



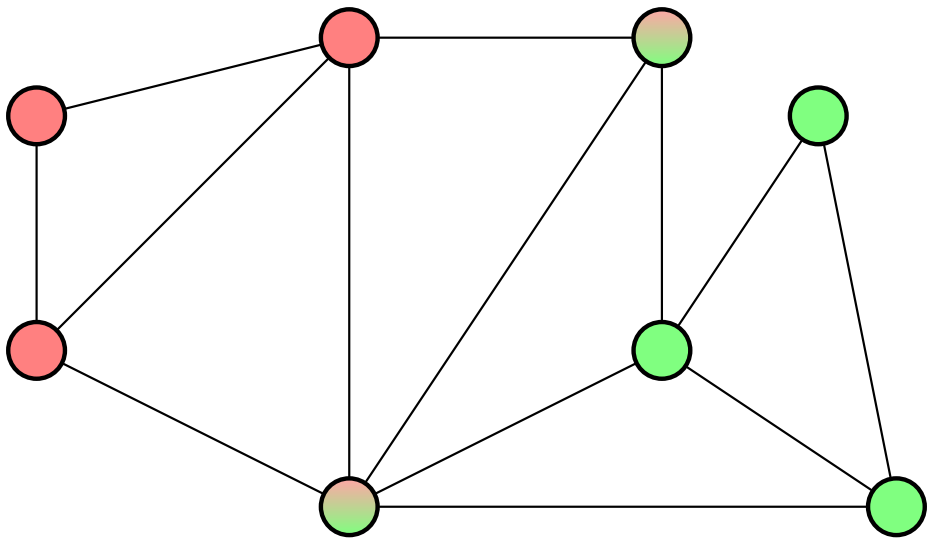
Information eclipsing



Information eclipsing

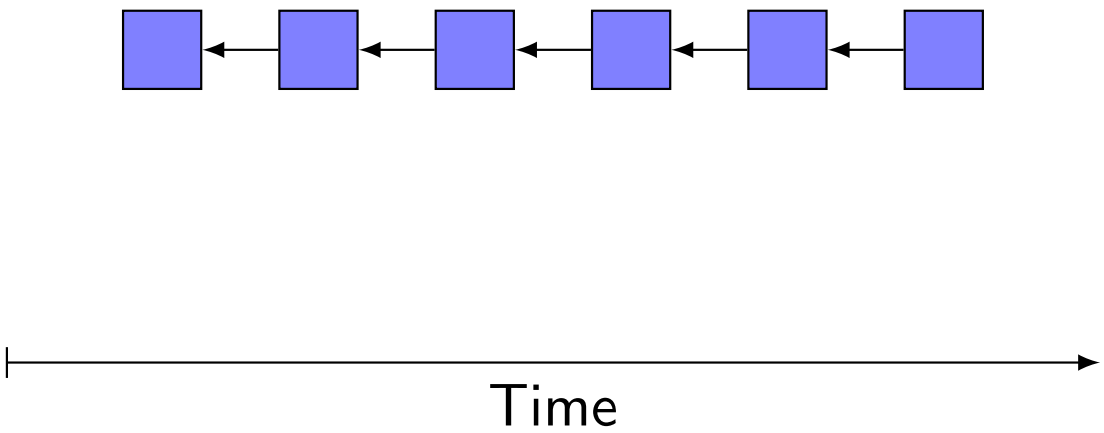


Information eclipsing

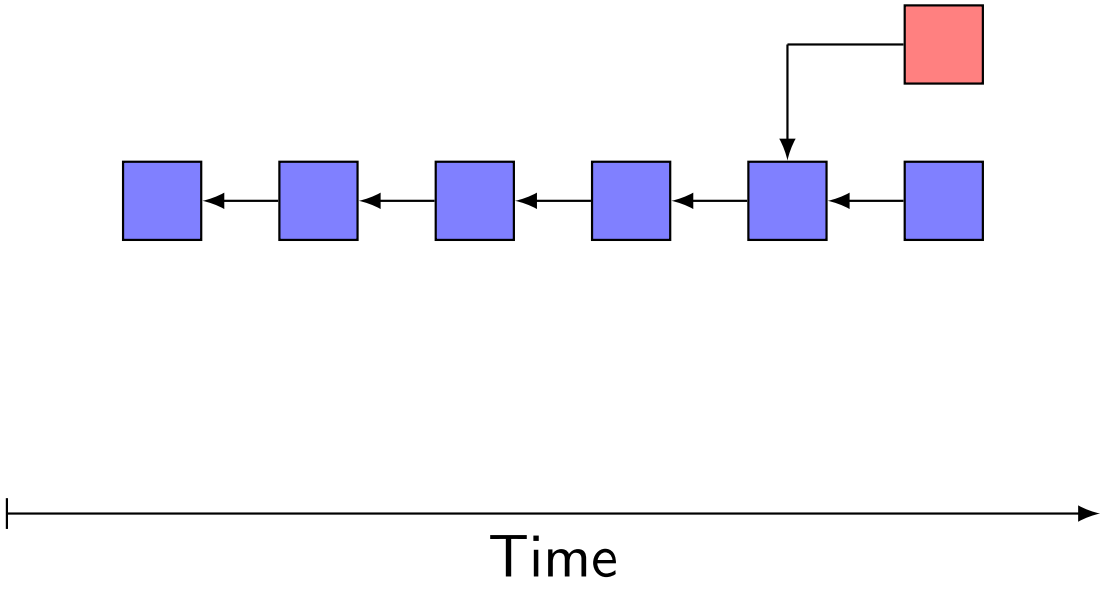


Blockchain Basics

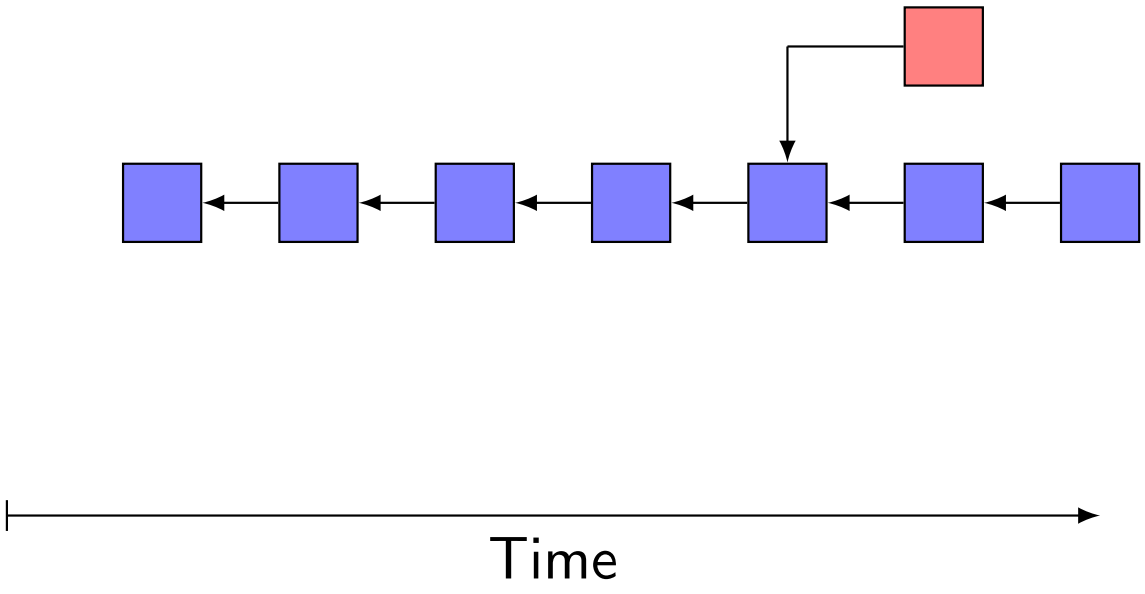
The Blockchain



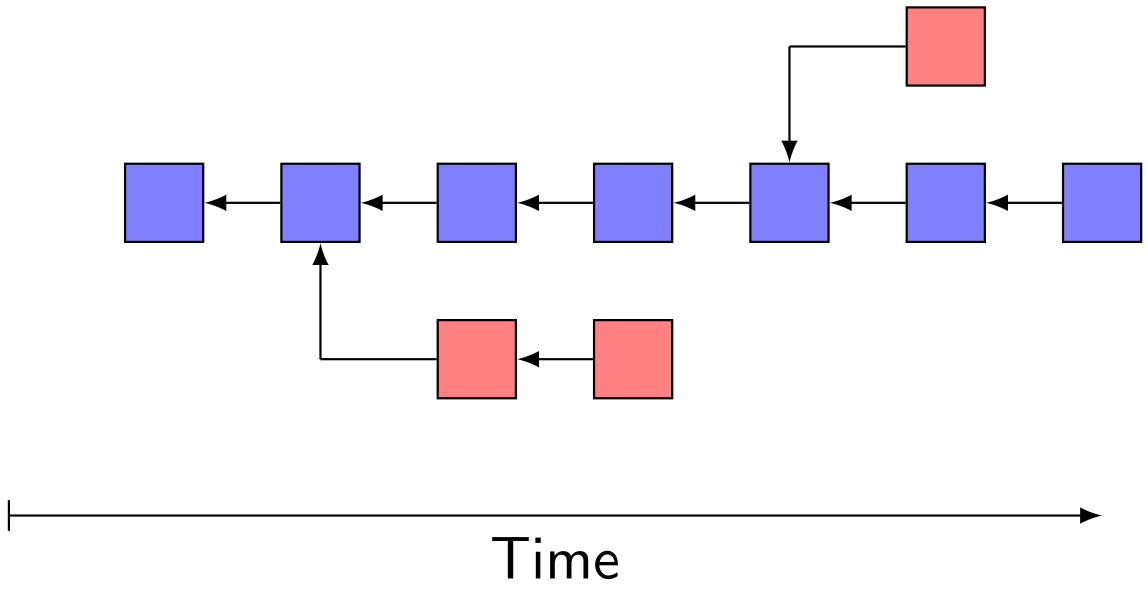
The Blockchain



The Blockchain

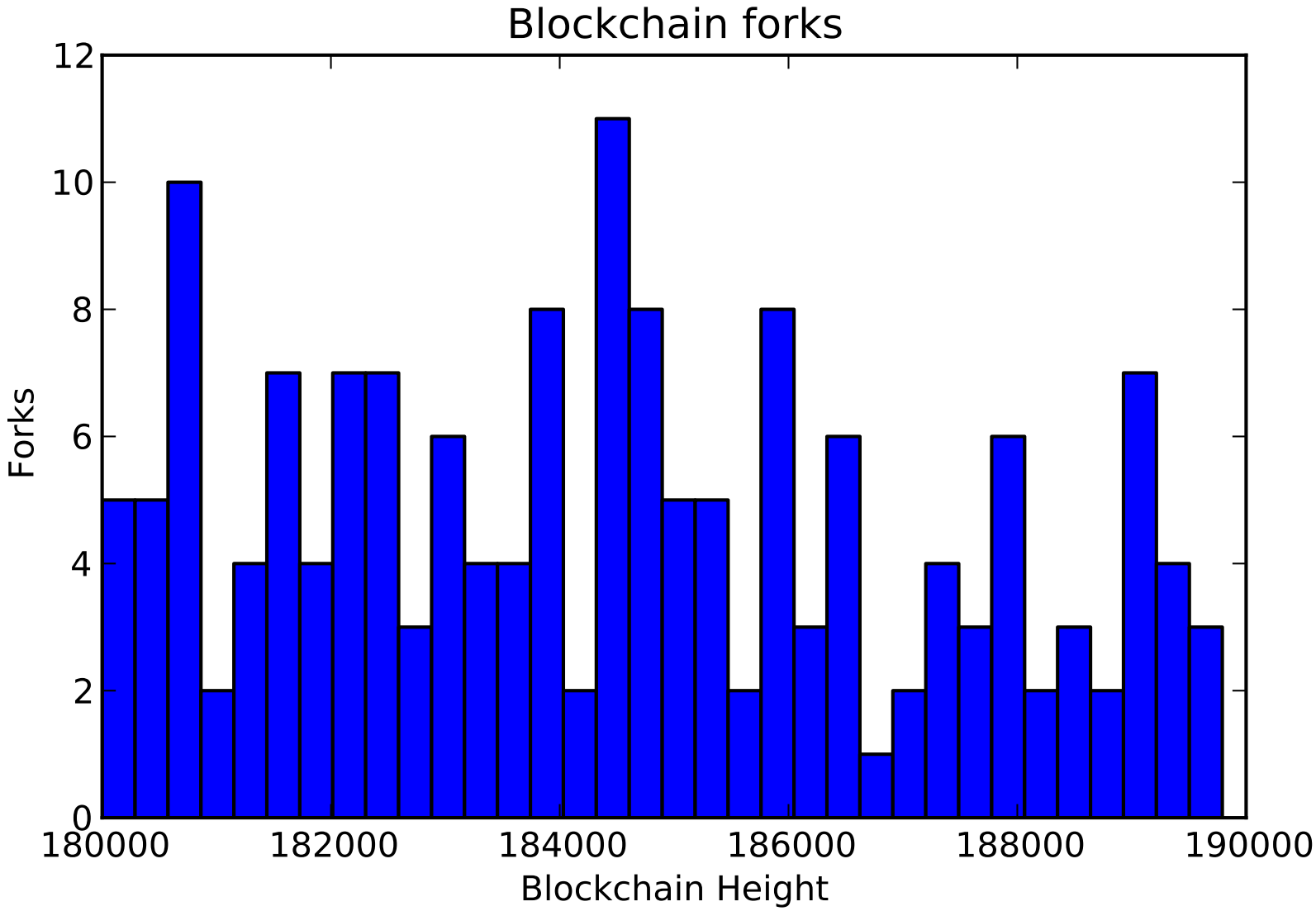


The Blockchain

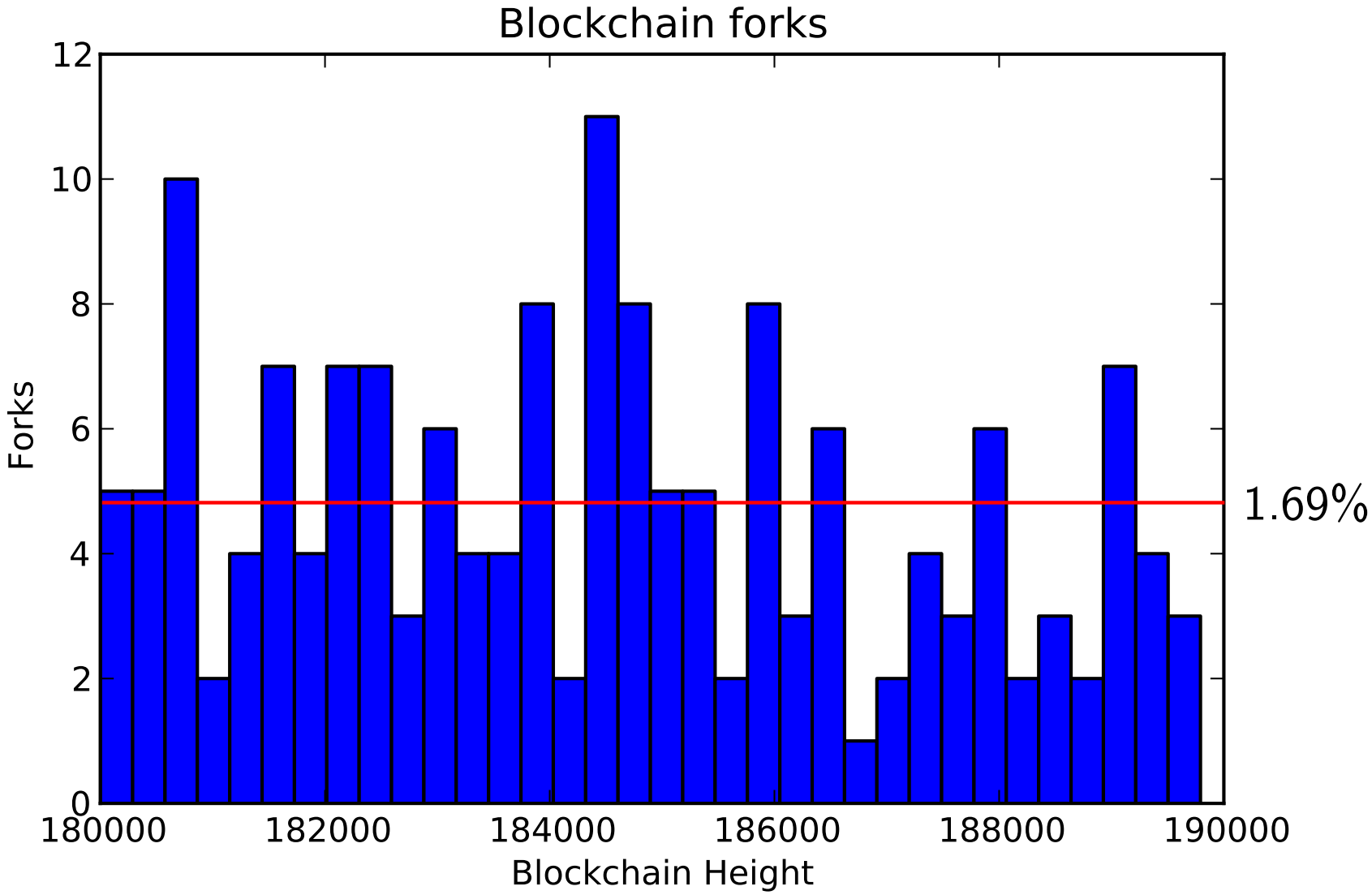


Our Results

Blockchain Forks



Blockchain Forks



Blockchain Forks: Model

Probability of finding a block:

$$P_b = Pr[X_b < t + 1 | X_b \geq t] \approx 1/600$$

Blockchain Forks: Model

Probability of finding a block:

$$P_b = Pr[X_b < t + 1 | X_b \geq t] \approx 1/600$$

Part of the network that may fork:

$$f(t) = \text{fraction of network knowing block at time } t$$

Blockchain Forks: Model

Probability of finding a block:

$$P_b = Pr[X_b < t + 1 | X_b \geq t] \approx 1/600$$

Part of the network that may fork:

$$f(t) = \text{fraction of network knowing block at time } t$$

Probability of a blockchain fork

$$P_f = 1 - (1 - P_b)^{\int_0^\infty (1 - f(t))dt}$$

Blockchain Forks: Validating our Model

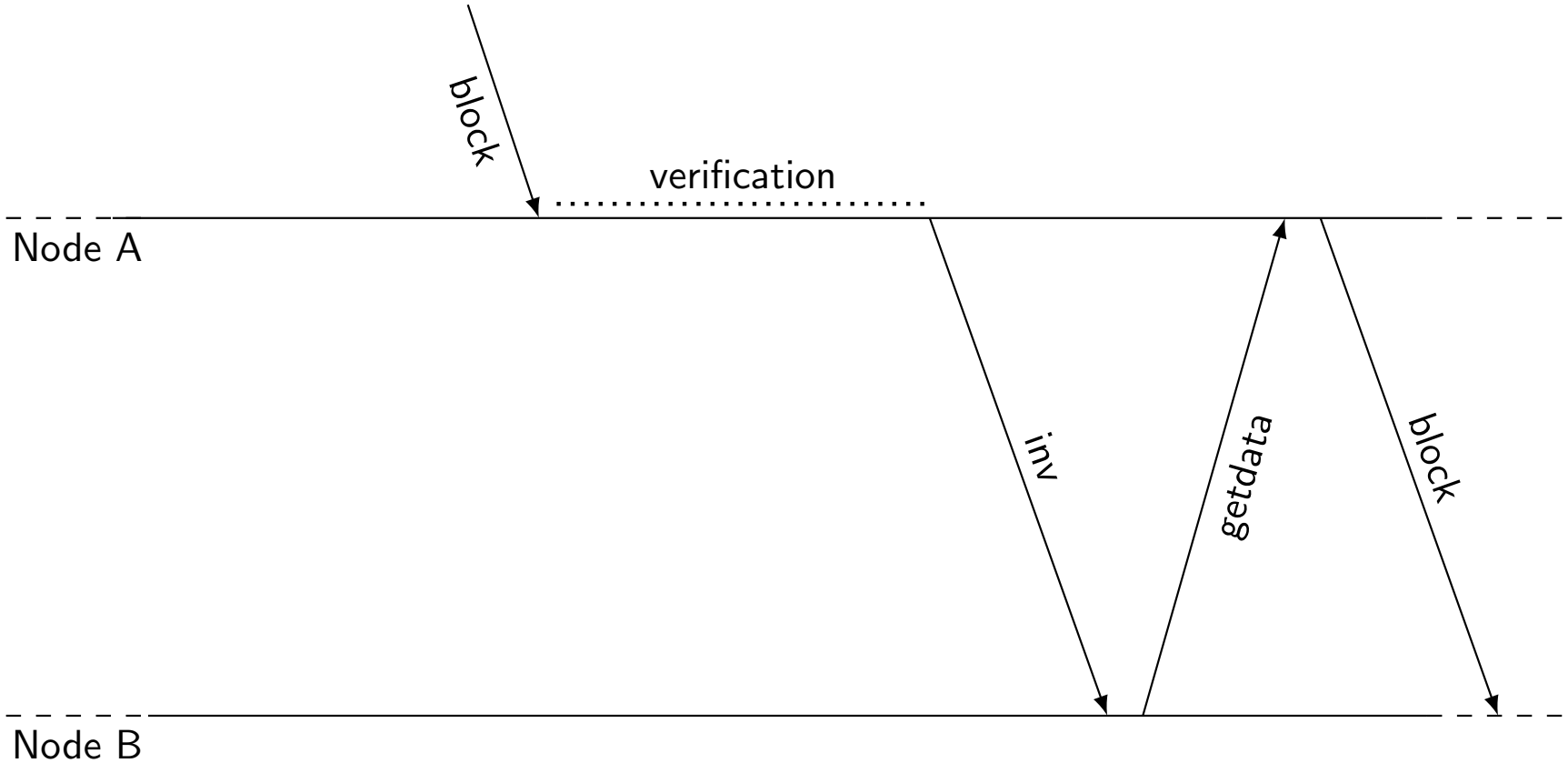
$$P_b = 1/633.68$$

$$\bar{F} = \int_0^\infty (1 - f(t))dt = 11.37$$

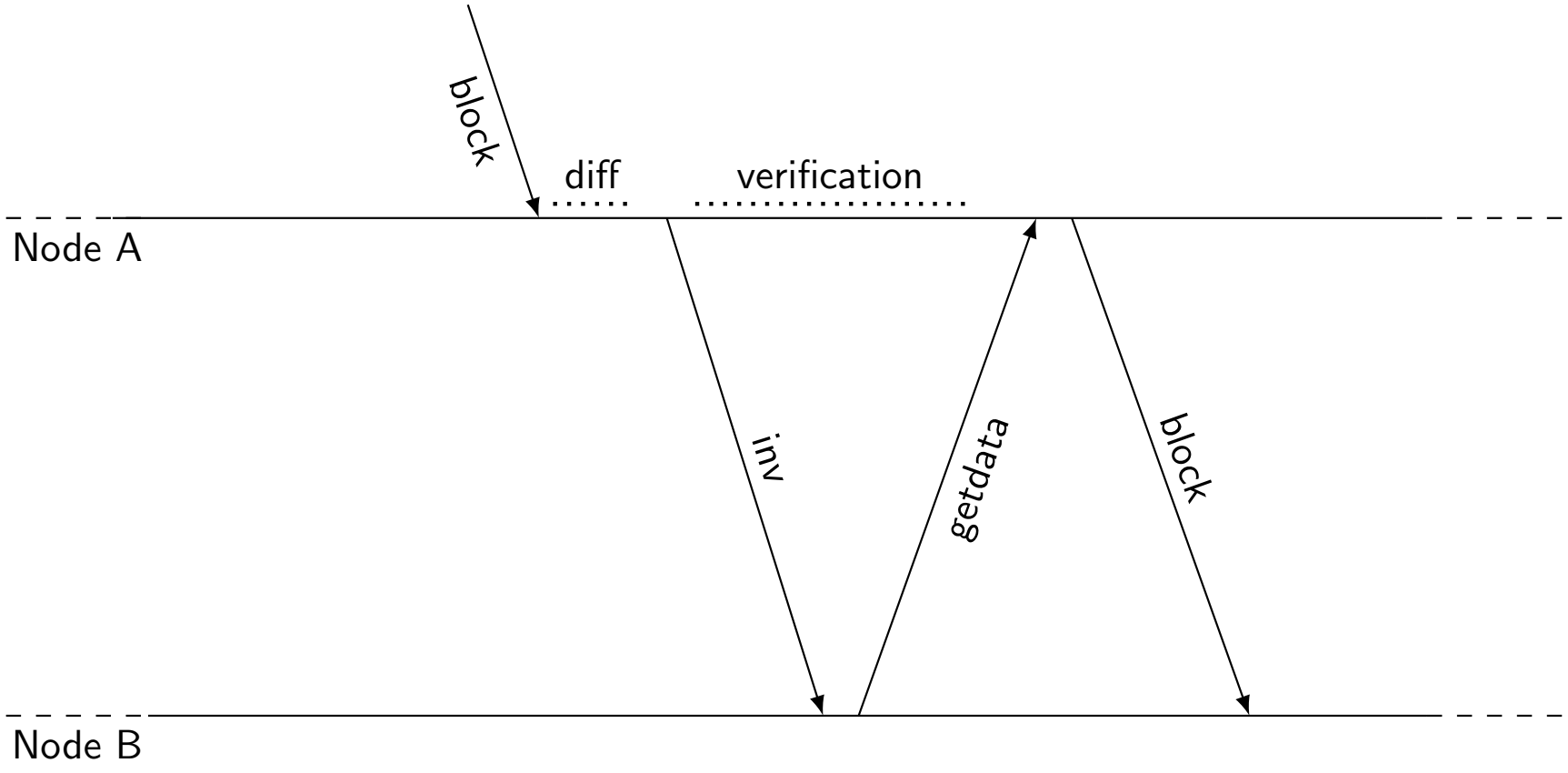
$$P_f = 1 - (1 - P_b)^{\bar{F}} = 1.78\%$$

Pushing the protocol to its limits

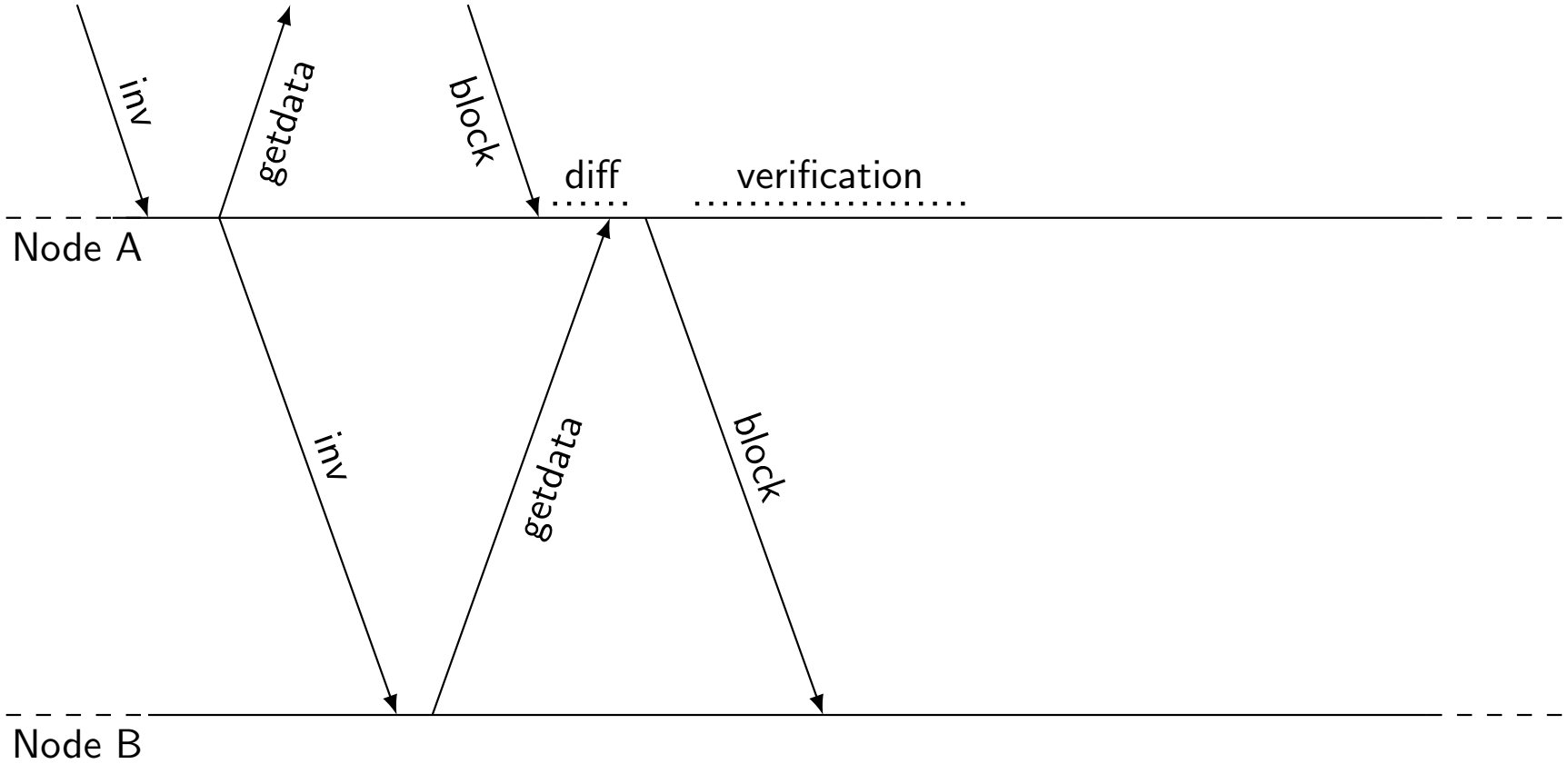
Pushing the protocol to its limits



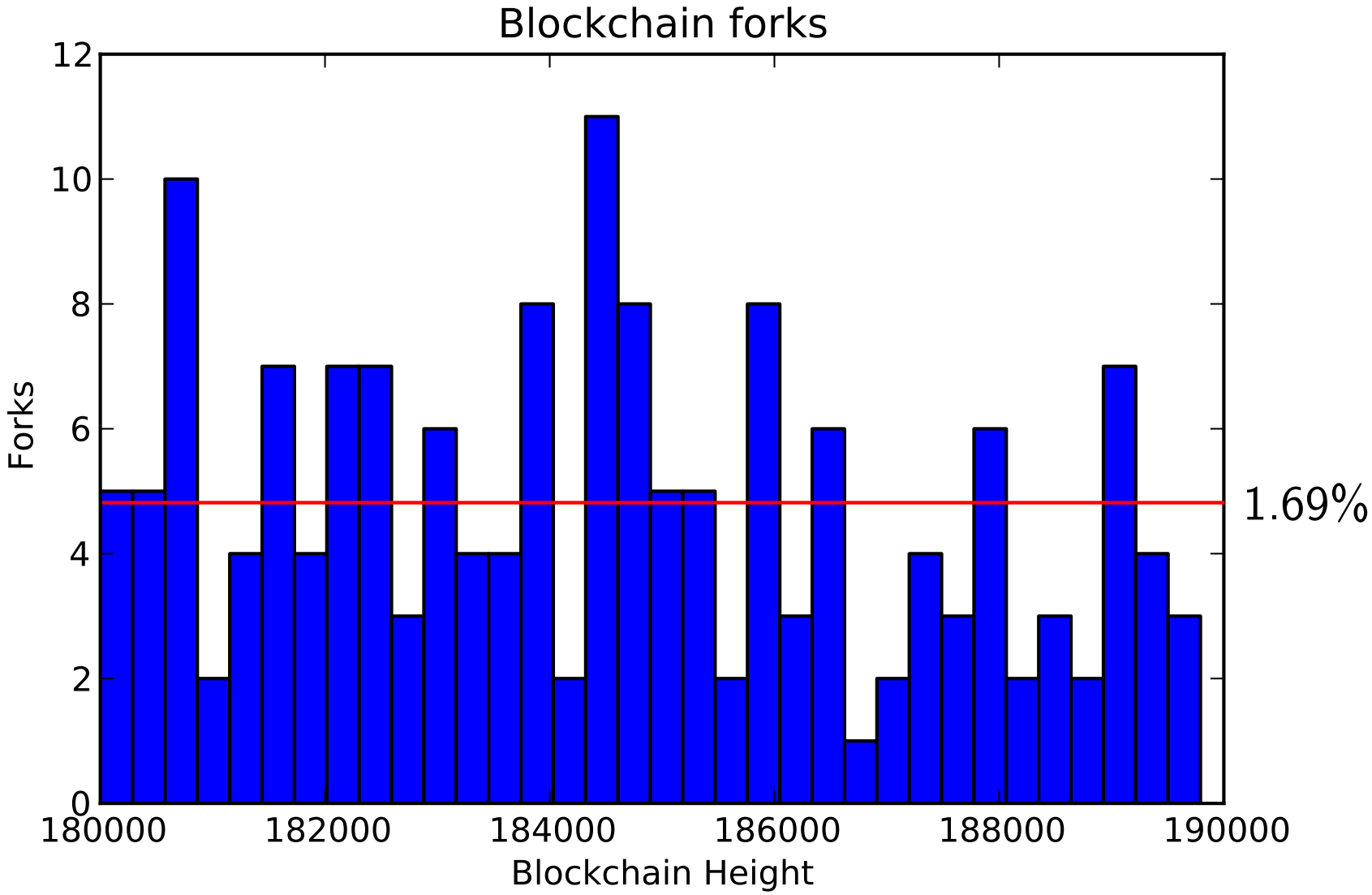
Pushing the protocol to its limits



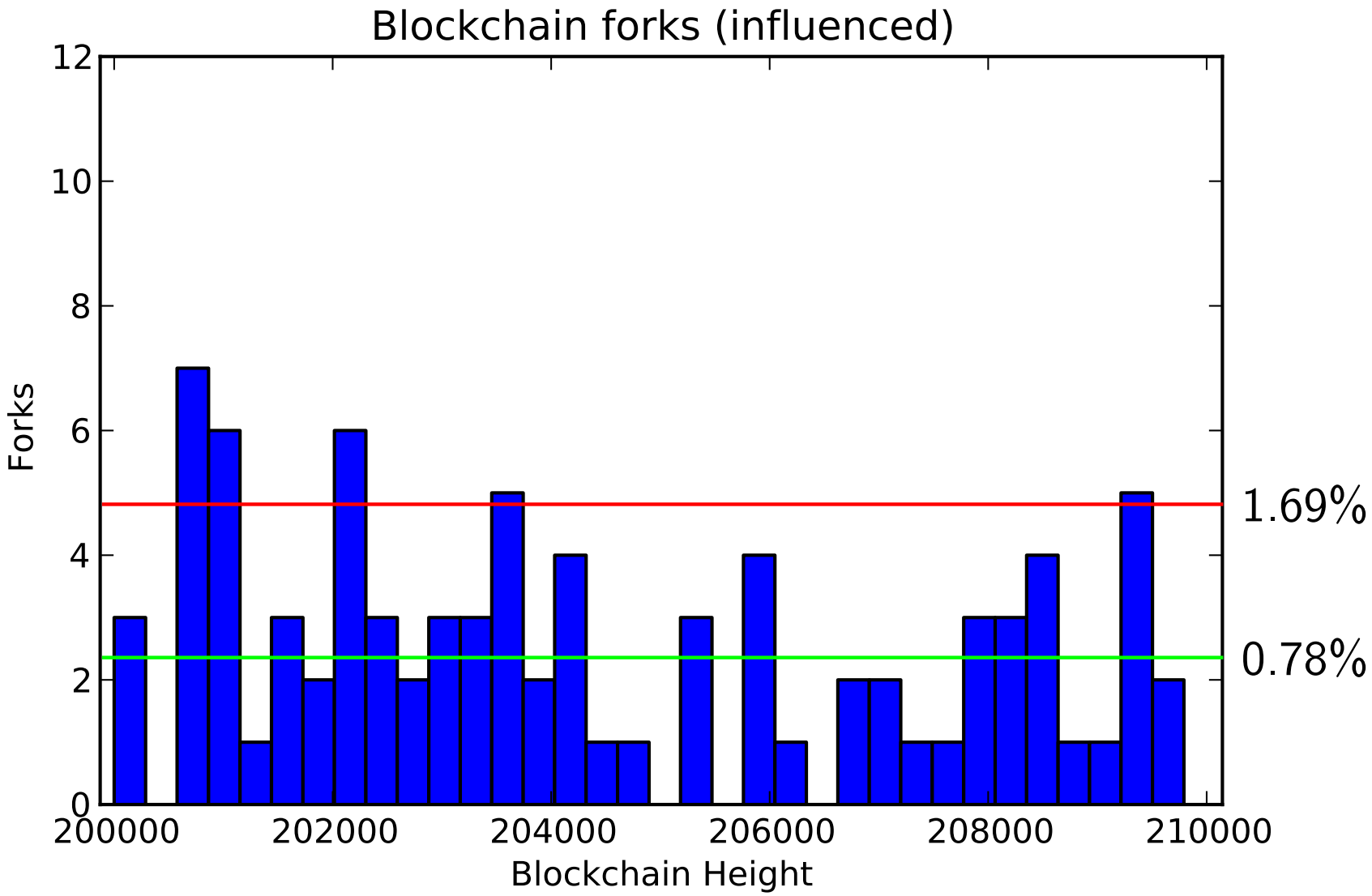
Pushing the protocol to its limits



Did it work?


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

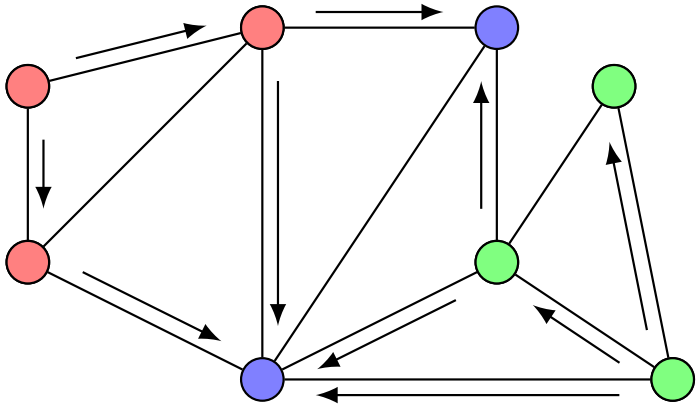
Did it work?


Blockchain forks (influenced)
Forks
Blockchain Height
0
2
4
6
8
10
12
200000
202000
204000
206000
208000
210000
1.69%
0.78%

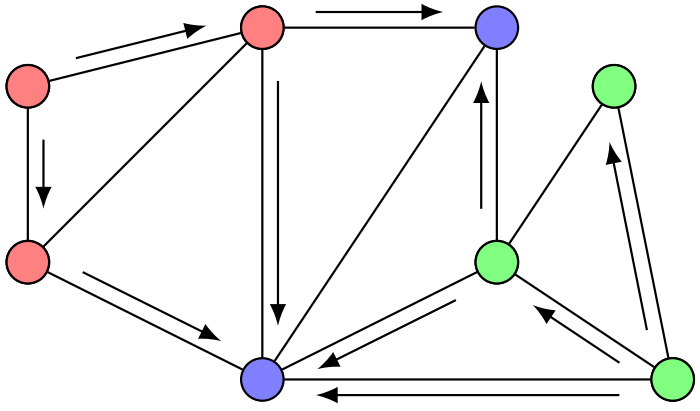
What does this mean?

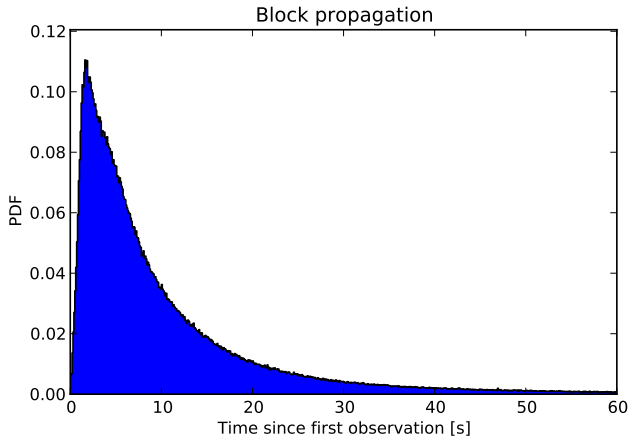
What does this mean?

Conclusion

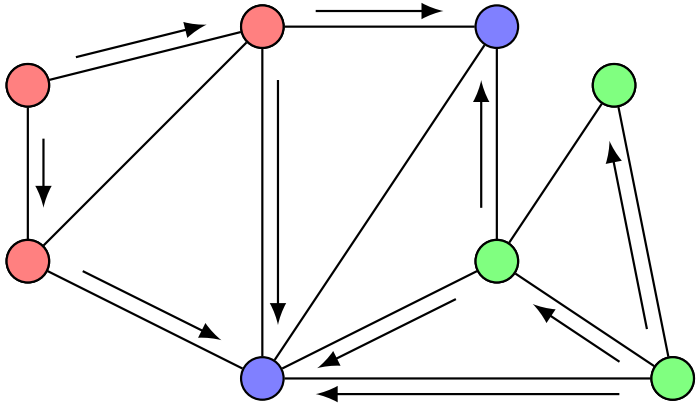


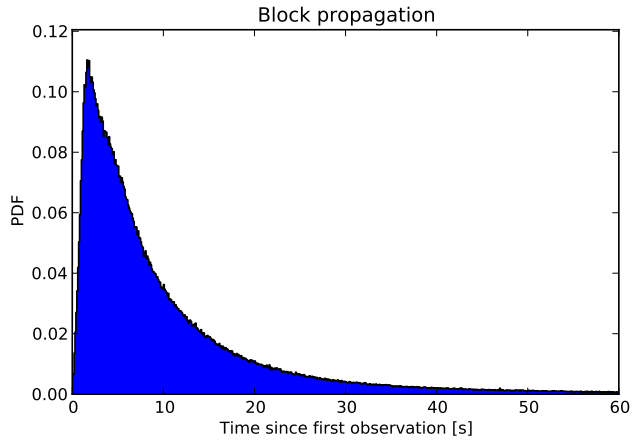
Conclusion

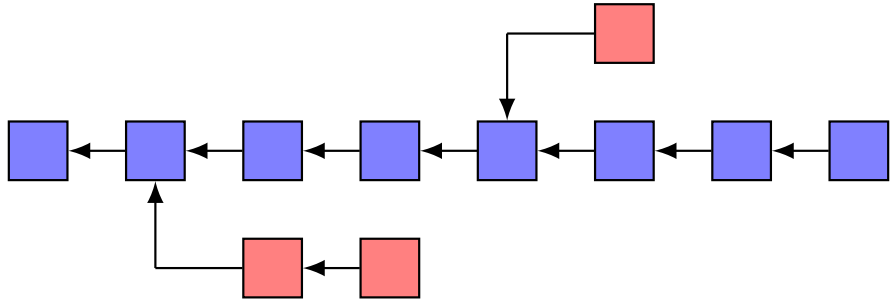



Block propagation
PDF
0.12
0.10
0.08
0.06
0.04
0.02
0.00
0
10
20
30
40
50
60
Time since first observation [s]

Conclusion




Block propagation
PDF
0.12
0.10
0.08
0.06
0.04
0.02
0.00
0
10
20
30
40
50
60
Time since first observation [s]



Thank you, questions?

Authors:
Christian Decker
Roger Wattenhofer