Quantifying Security with an MDP

Quantifying Blockchain Security

Optimal Adversarial Strategies

Honest Behaviour

Quantifying Blockchain Security

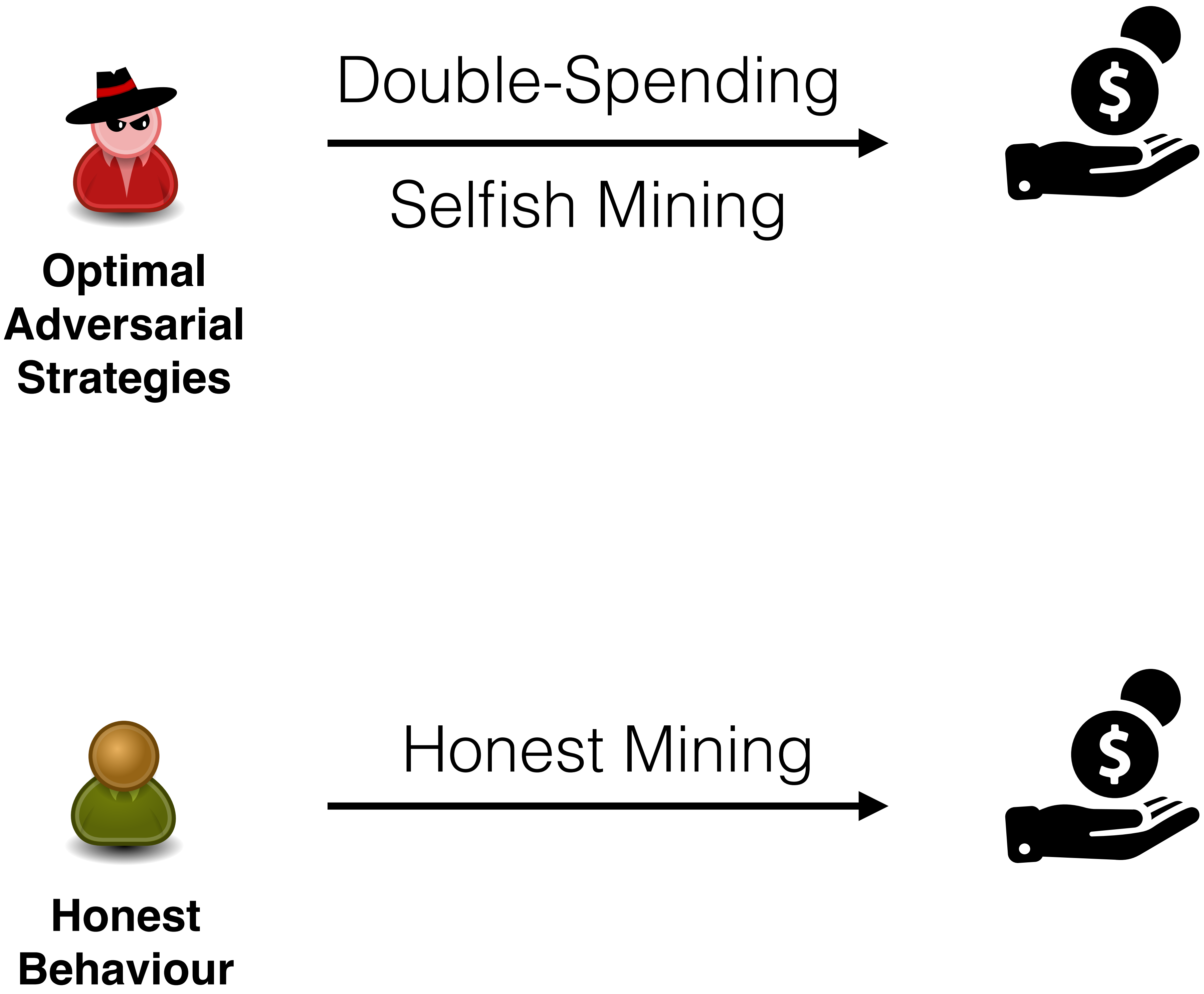
Double-Spending

Selfish Mining

Optimal Adversarial Strategies

Honest Behaviour

Quantifying Blockchain Security



Double-Spending

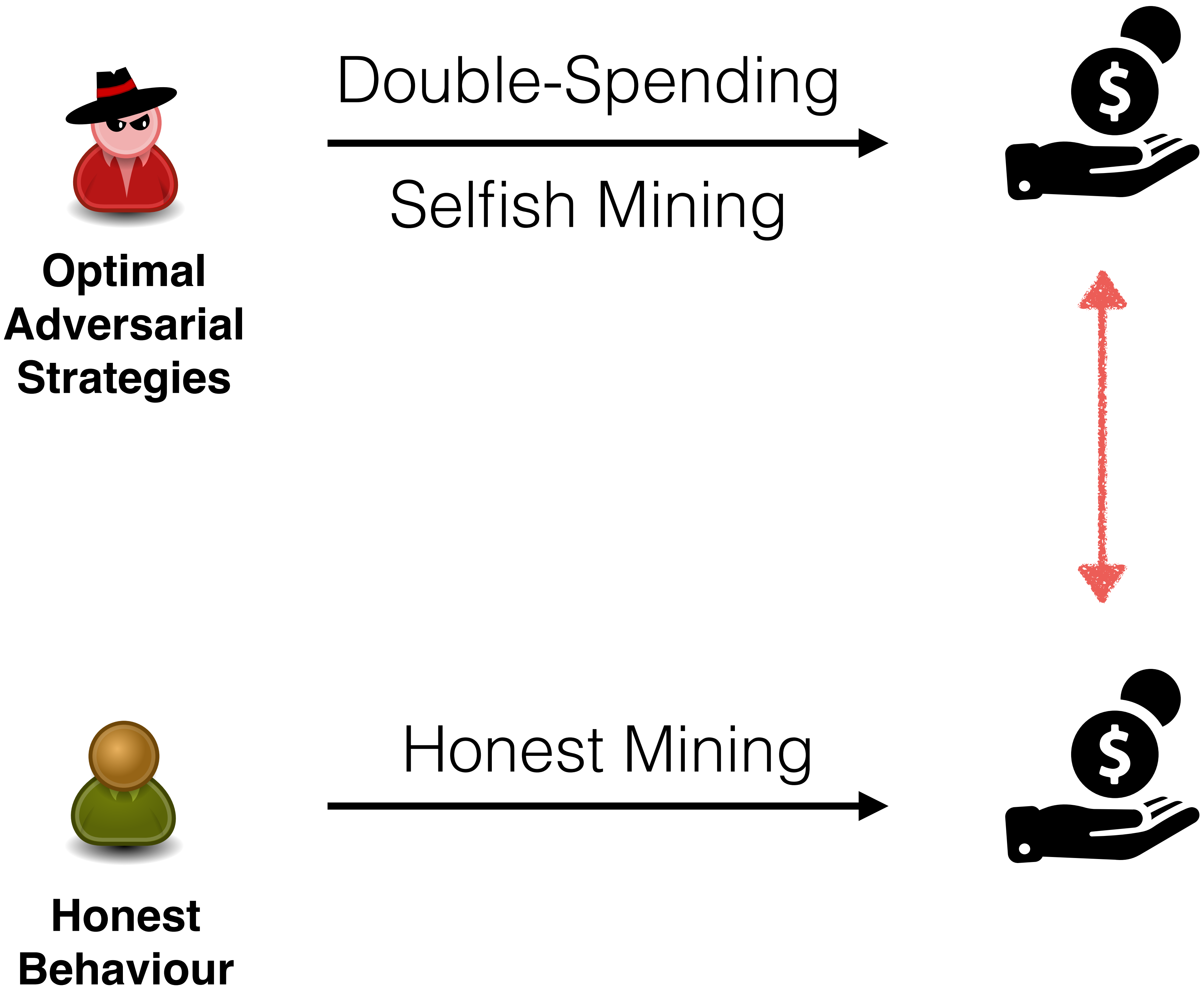
Selfish Mining

Optimal Adversarial Strategies

Honest Mining

Honest Behaviour

Quantifying Blockchain Security



Optimal Adversarial Strategies

Double-Spending

Selfish Mining

Honest Behaviour

Honest Mining

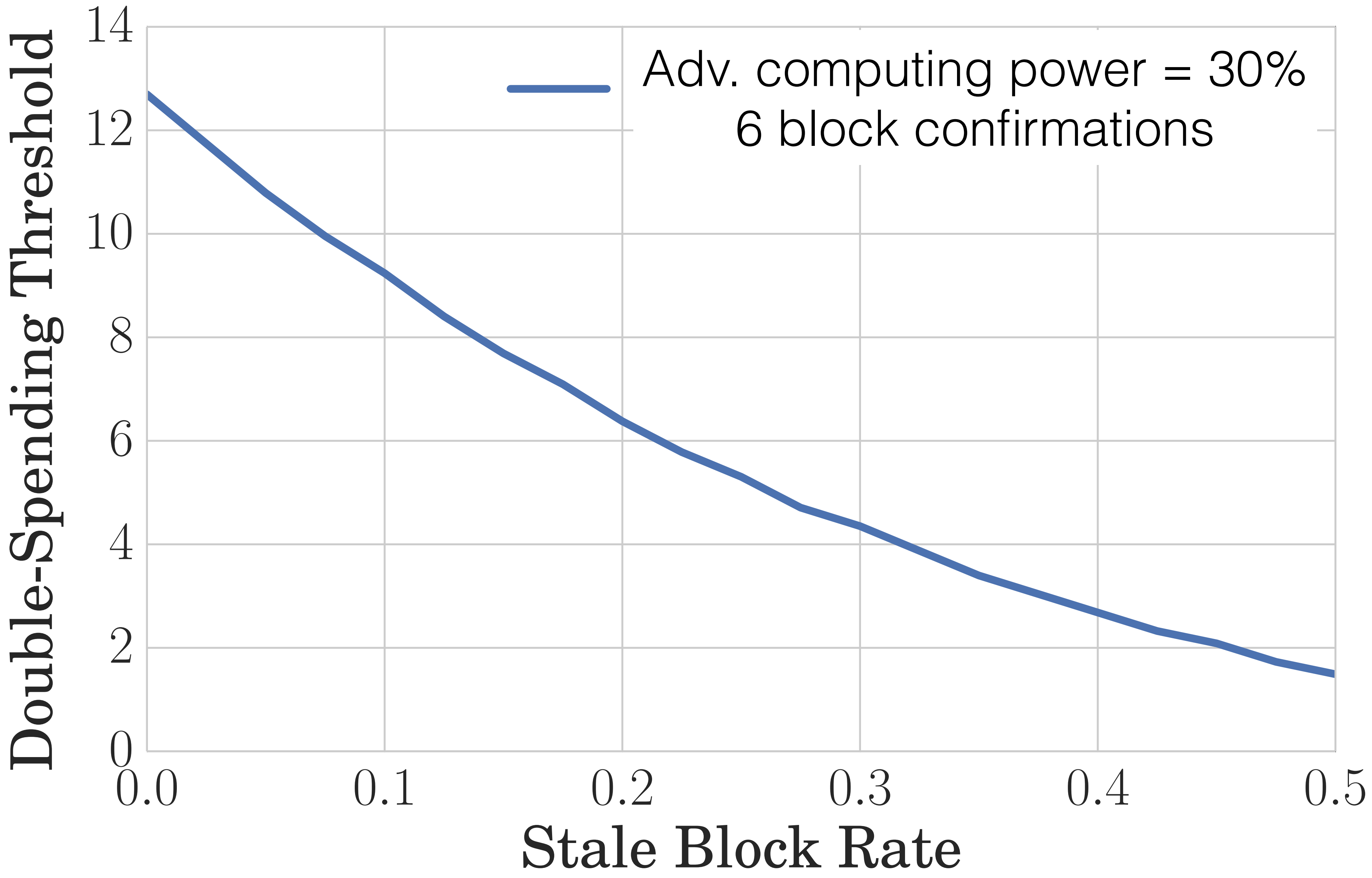
Double-Spending Threshold

Double-Spending Threshold

Profitability depends on transaction value.

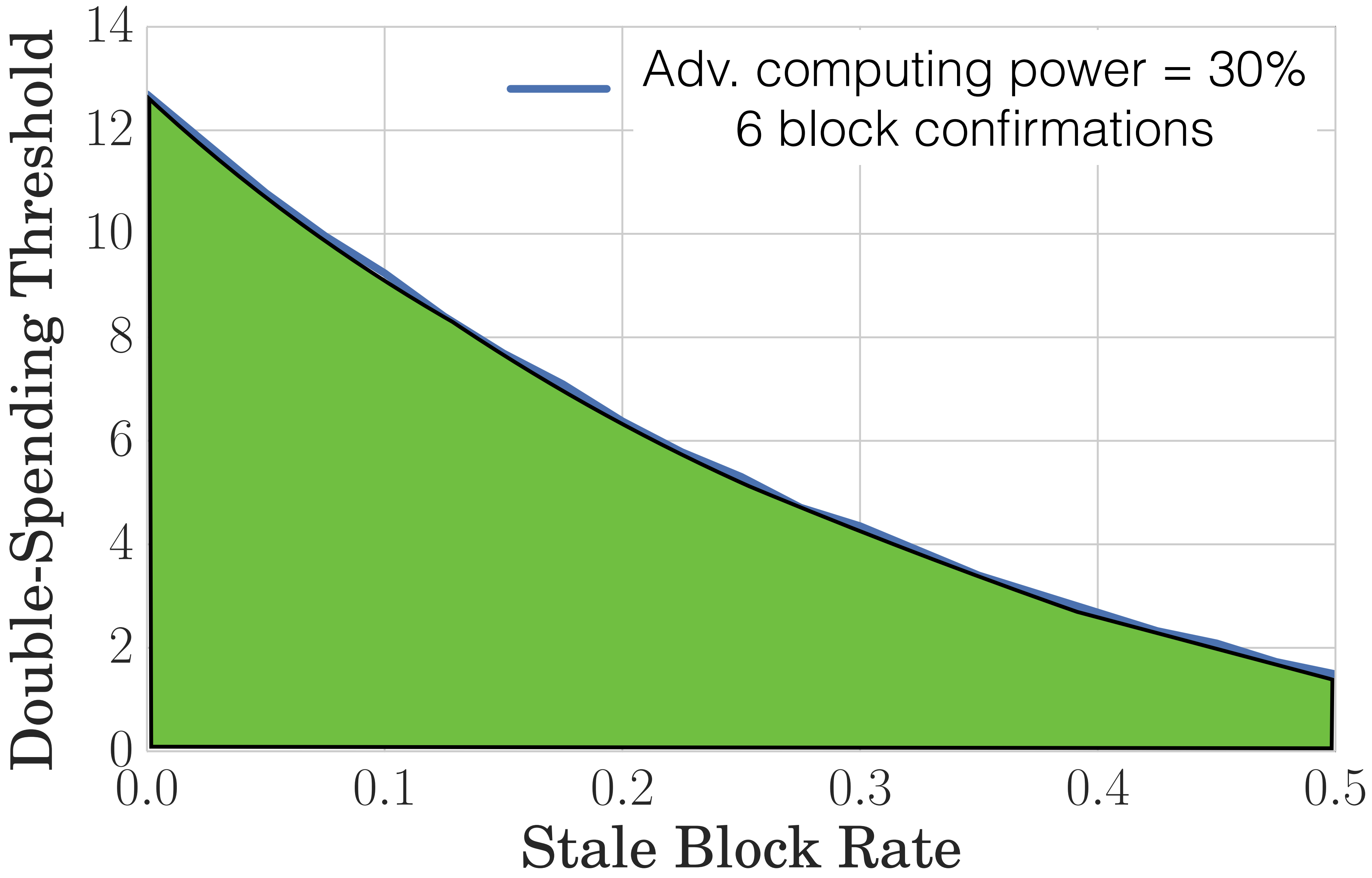
Double-Spending Threshold

Profitability depends on transaction value.



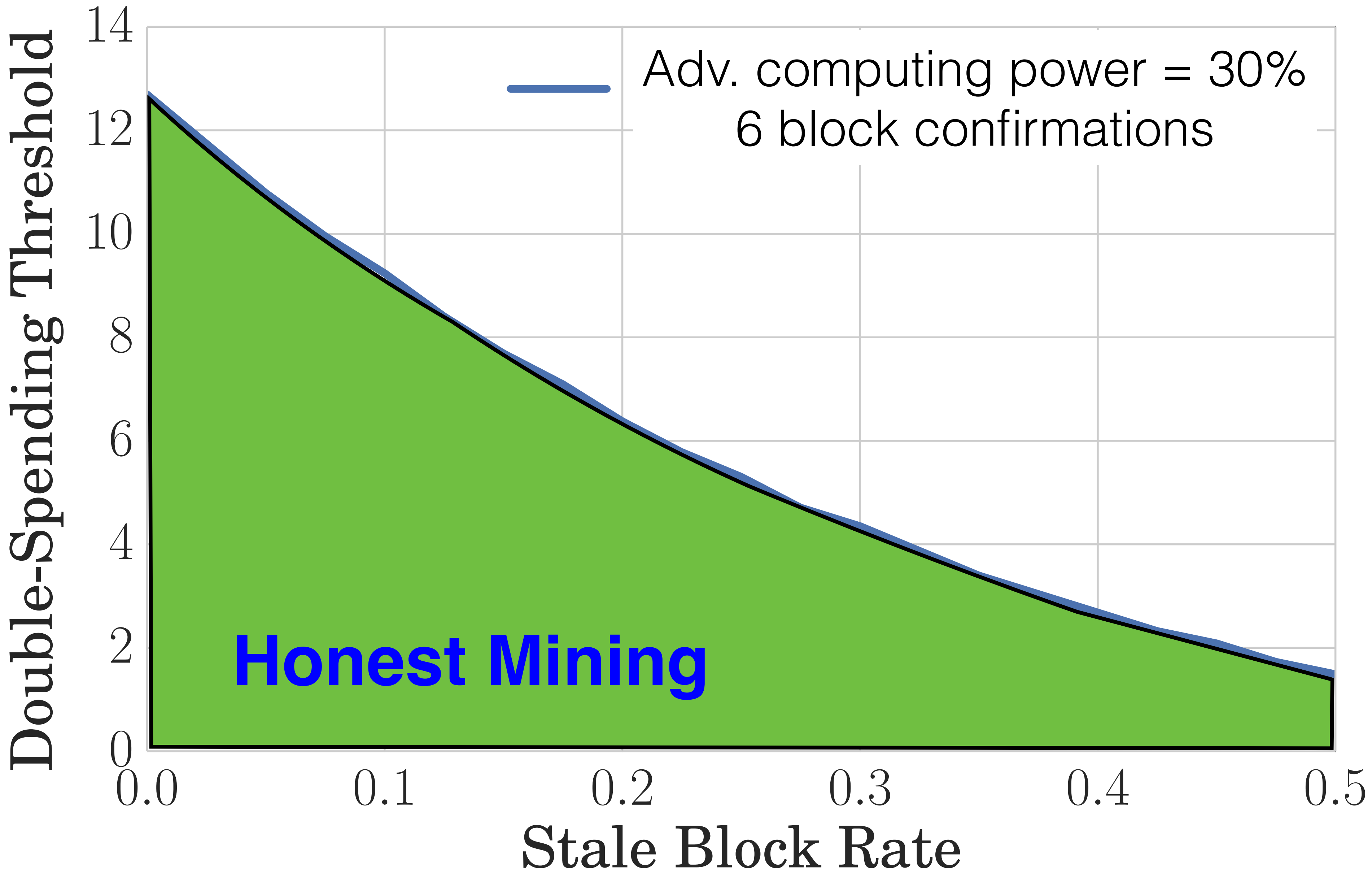
Double-Spending Threshold

Profitability depends on transaction value.



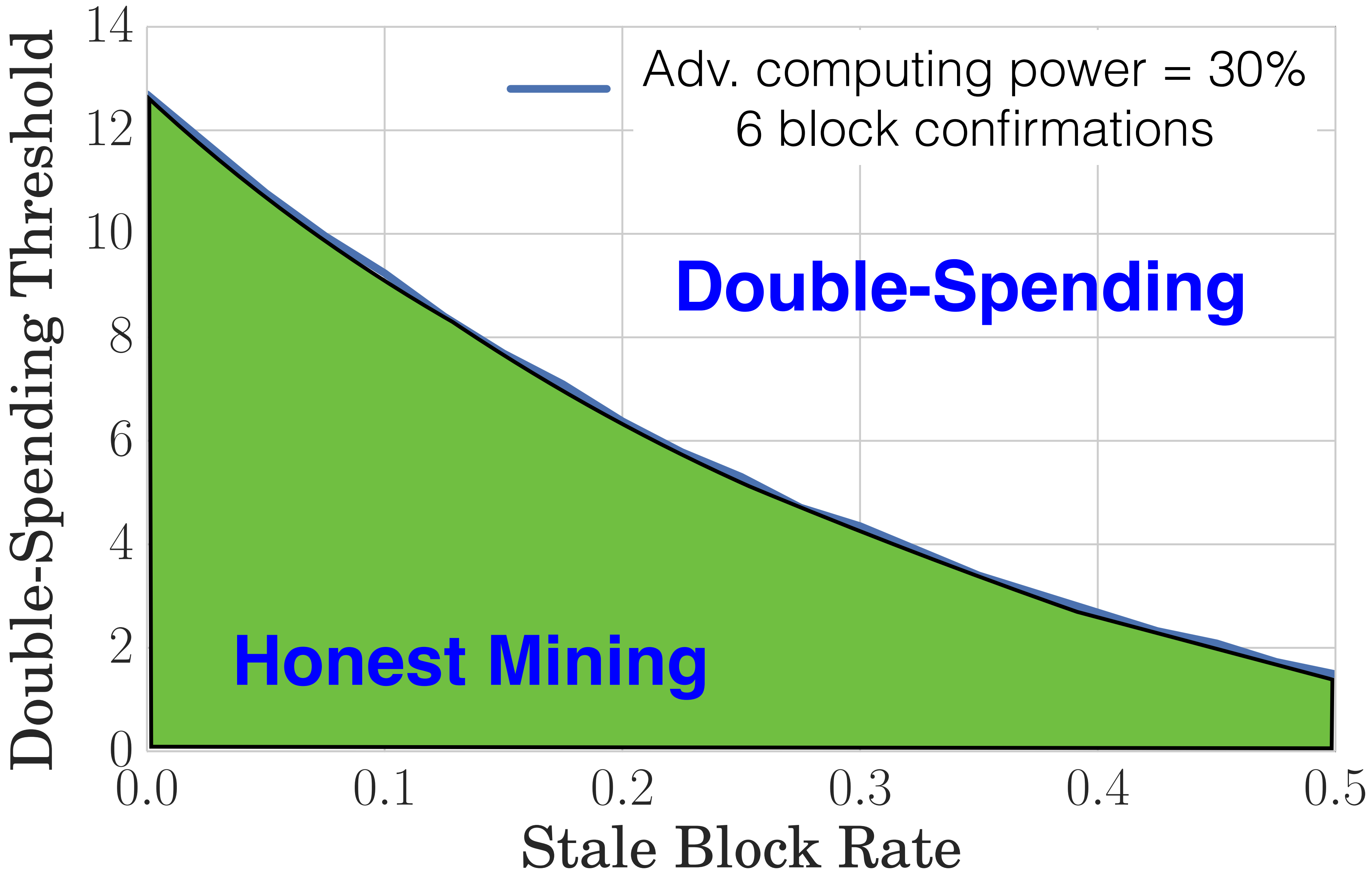
Double-Spending Threshold

Profitability depends on transaction value.



Double-Spending Threshold

Profitability depends on transaction value.



Double-Spending Defence - Confirmation Time

Ethereum

Bitcoin

Double-Spending Defence - Confirmation Time

	Ethereum	Bitcoin
Block confirmations	37	6

Double-Spending Defence - Confirmation Time

	Ethereum	Bitcoin
Block confirmations	37	6

30% of the total computing power

Double-Spending Defence - Confirmation Time

	Ethereum	Bitcoin
Block confirmations	37	6
	about **10 minutes**	about **60 minutes**

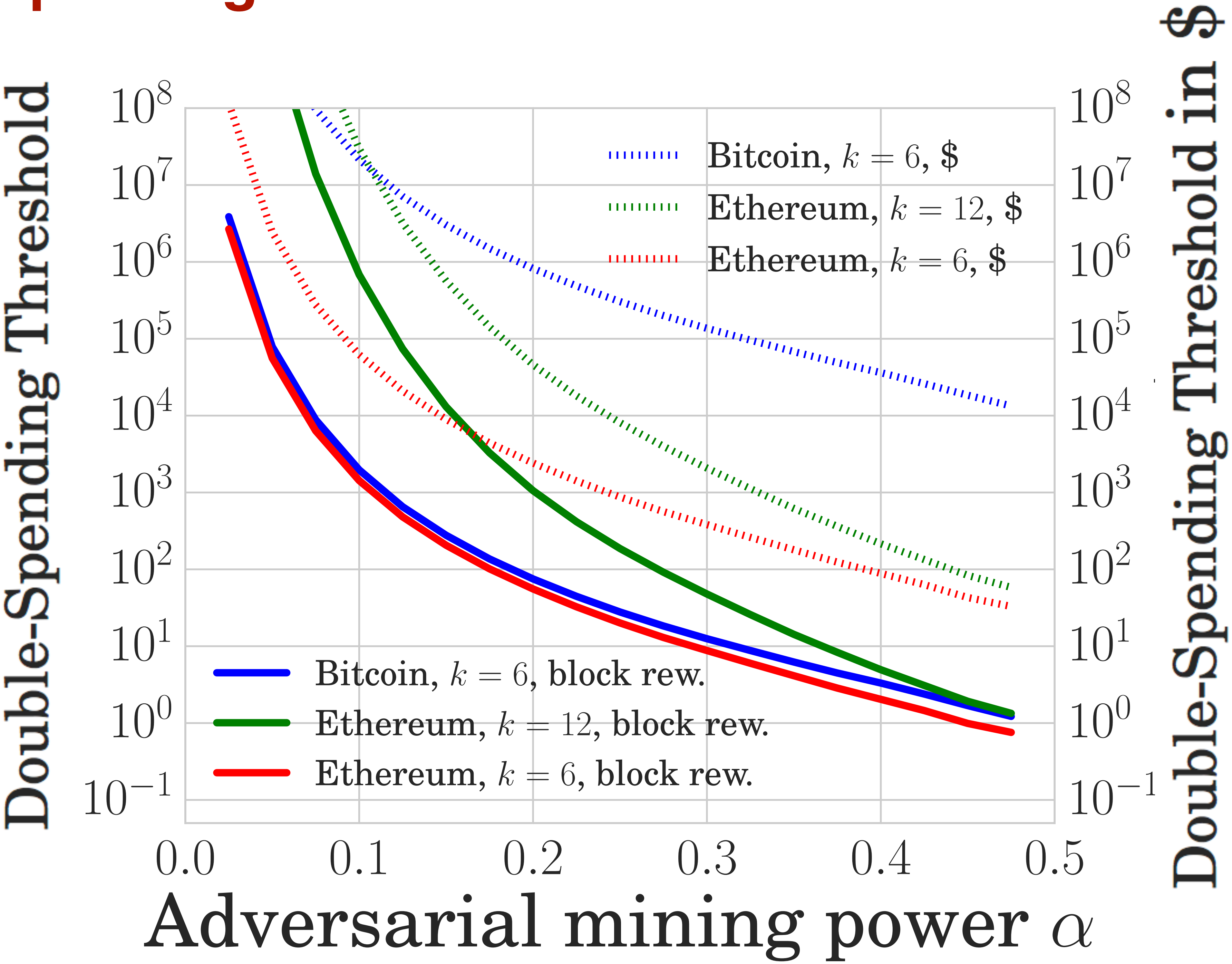
30% of the total computing power

Double-Spending Defence - Confirmation Time

	Ethereum	Bitcoin	Litecoin	Dogecoin
Block confirmations	37 about **10 minutes**	6 about **60 minutes**	28 about 70 minutes	47 about 47 minutes

30% of the total computing power

Double Spending Bitcoin vs. Ethereum



Double-spending resistance of
Ethereum (k in {6,12}) vs. Bitcoin (k=6)