ETH zürich

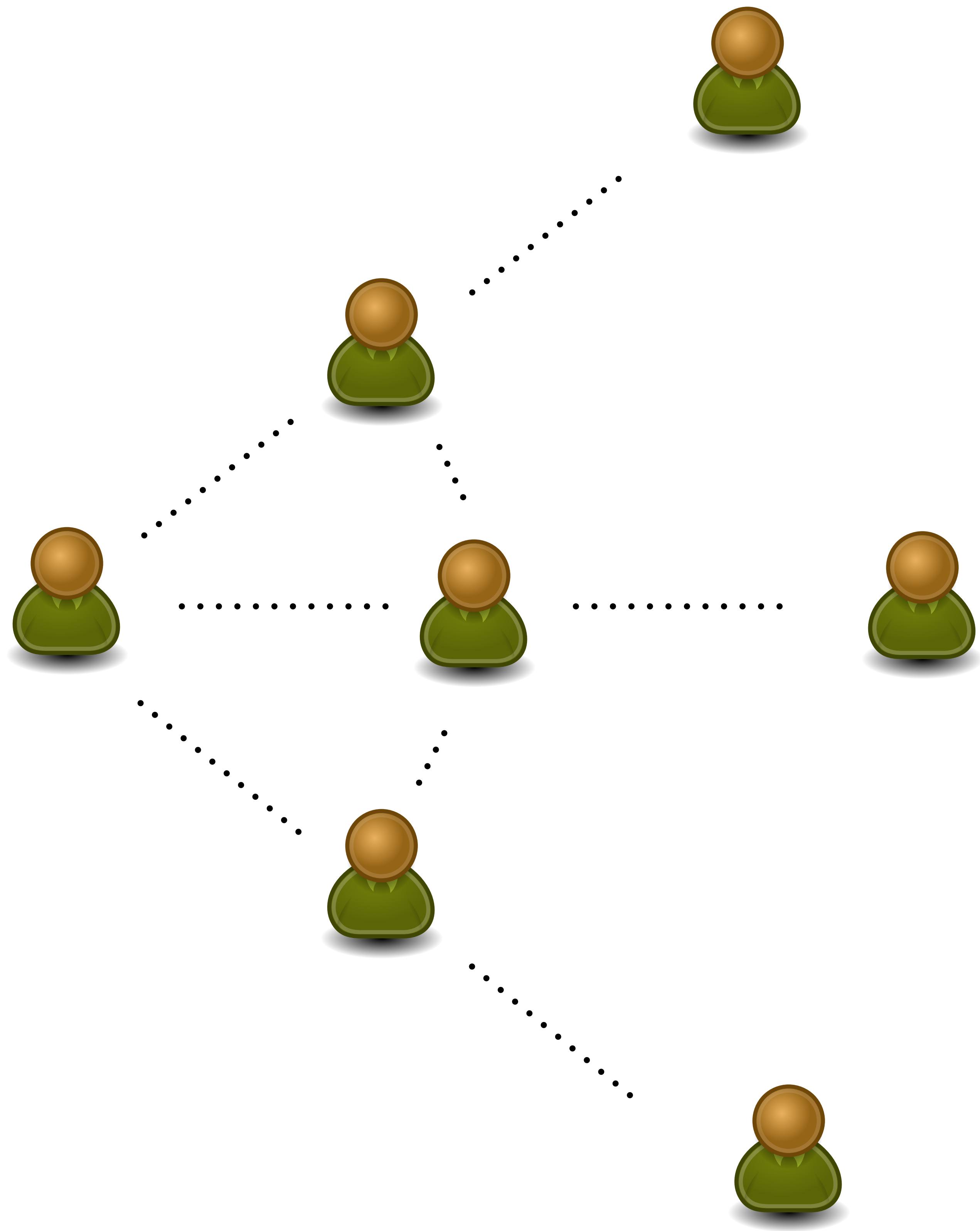
On the Security and Scalability of Proof of Work Blockchains

Arthur Gervais

ETH Zurich

Scaling Bitcoin 2016 - Milan

Broadcast of transactions/blocks

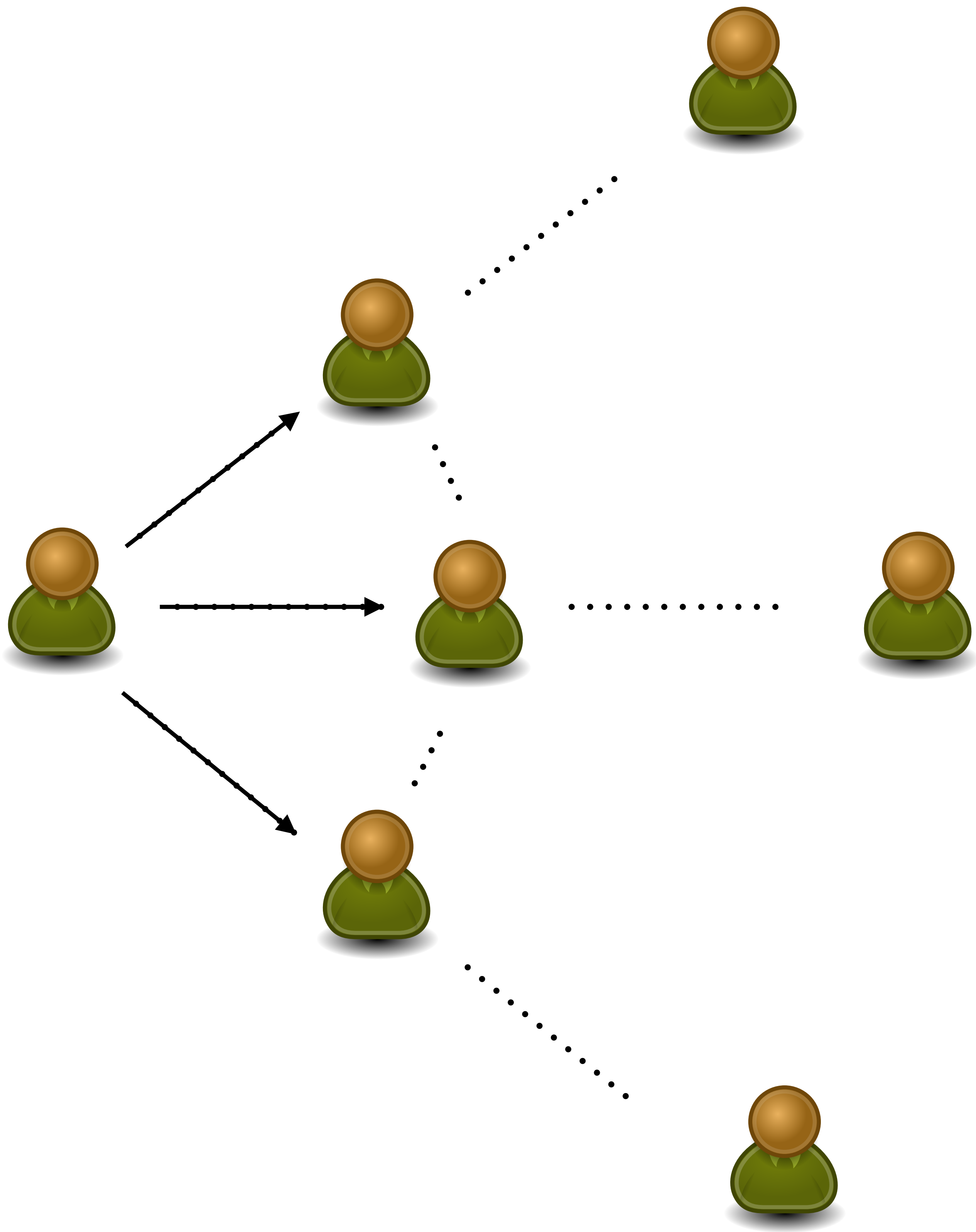


- All transactions, blocks need to be broadcast into the whole network

- Larger blocks
  - ➡ slower propagation
  - ➡ increased consensus latency

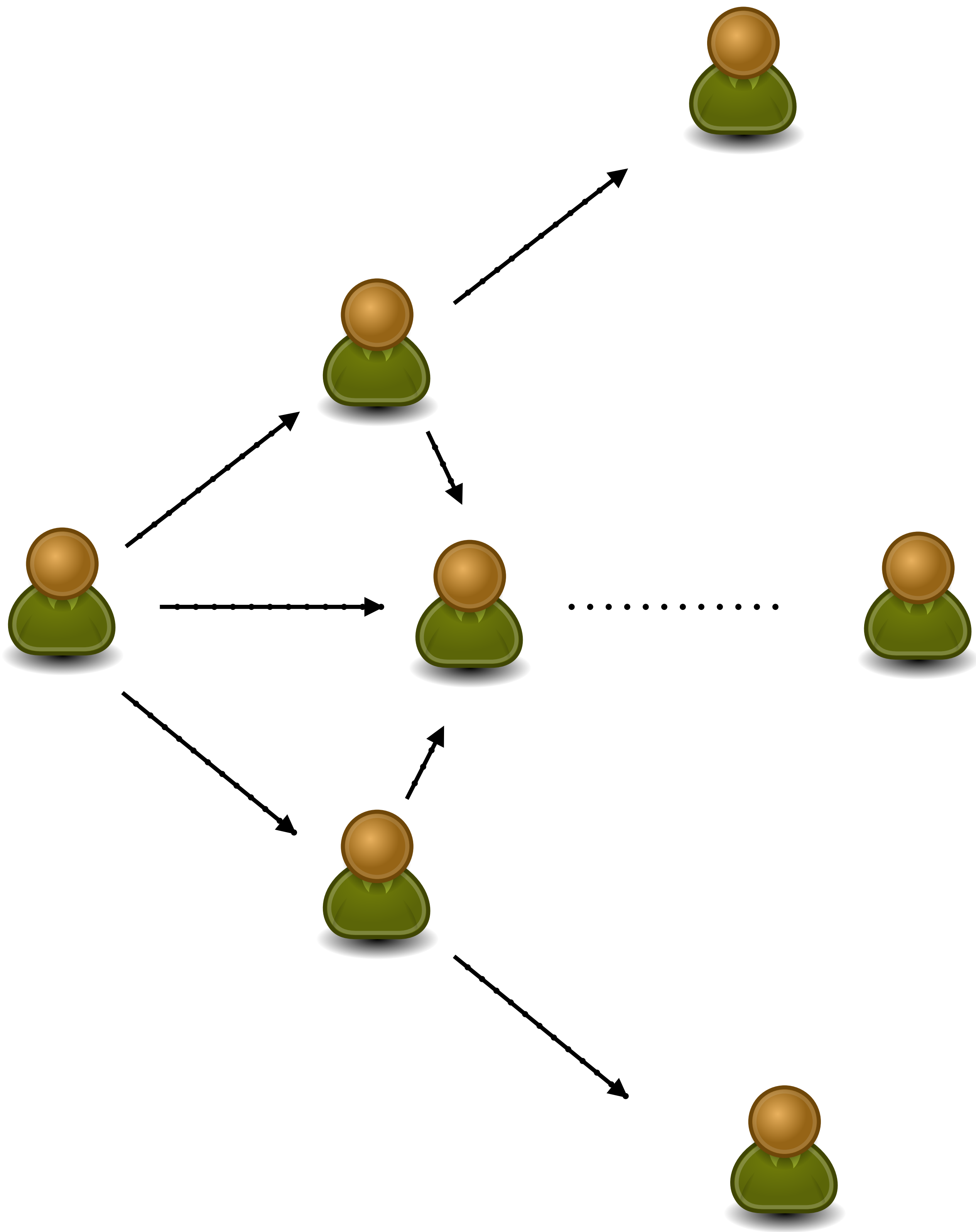
- Risks of network partition (stale blocks…)

Broadcast of transactions/blocks



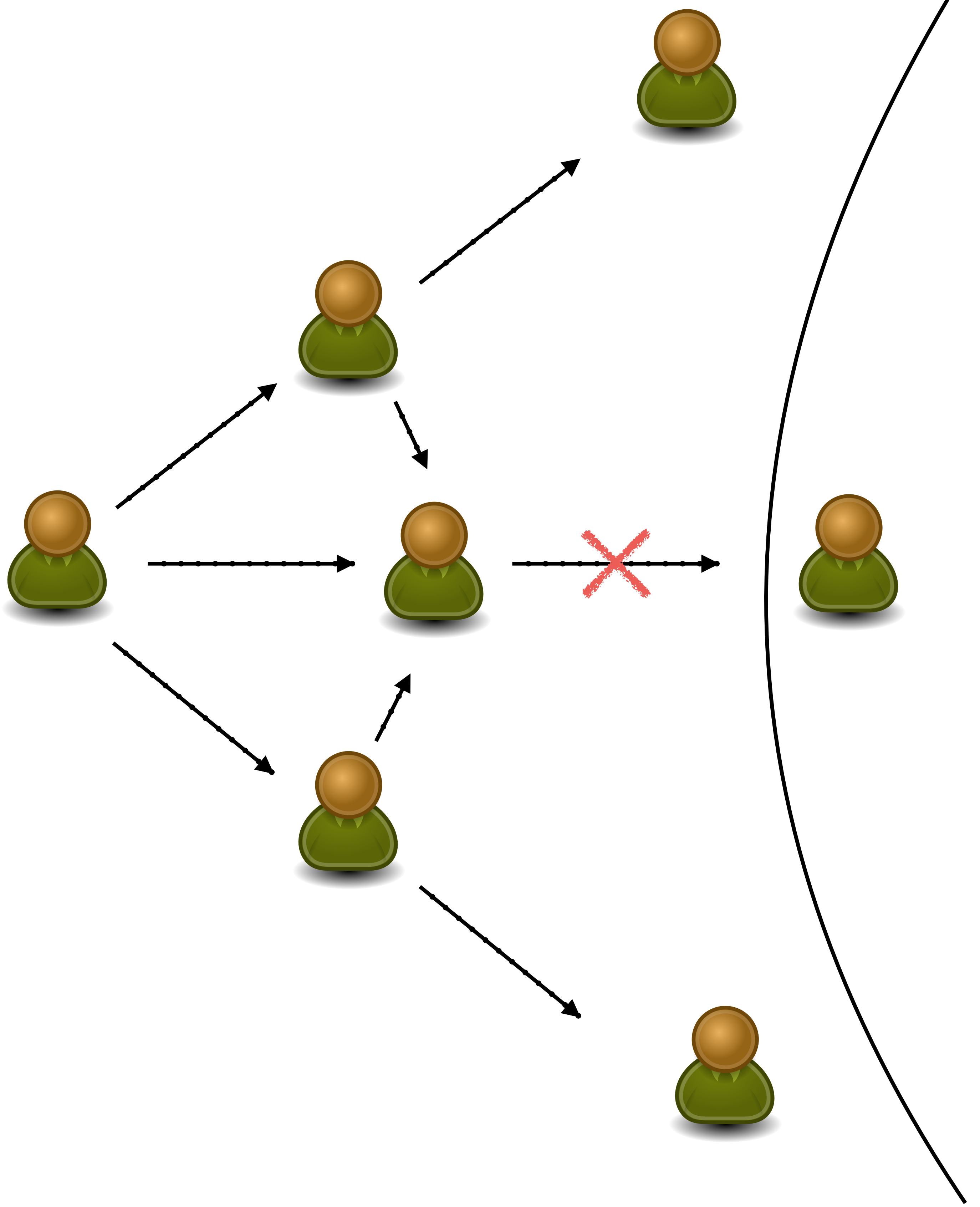
- All transactions, blocks need to be broadcast into the whole network
- Larger blocks
  → slower propagation
  → increased consensus latency
- Risks of network partition (stale blocks...)

Broadcast of transactions/blocks



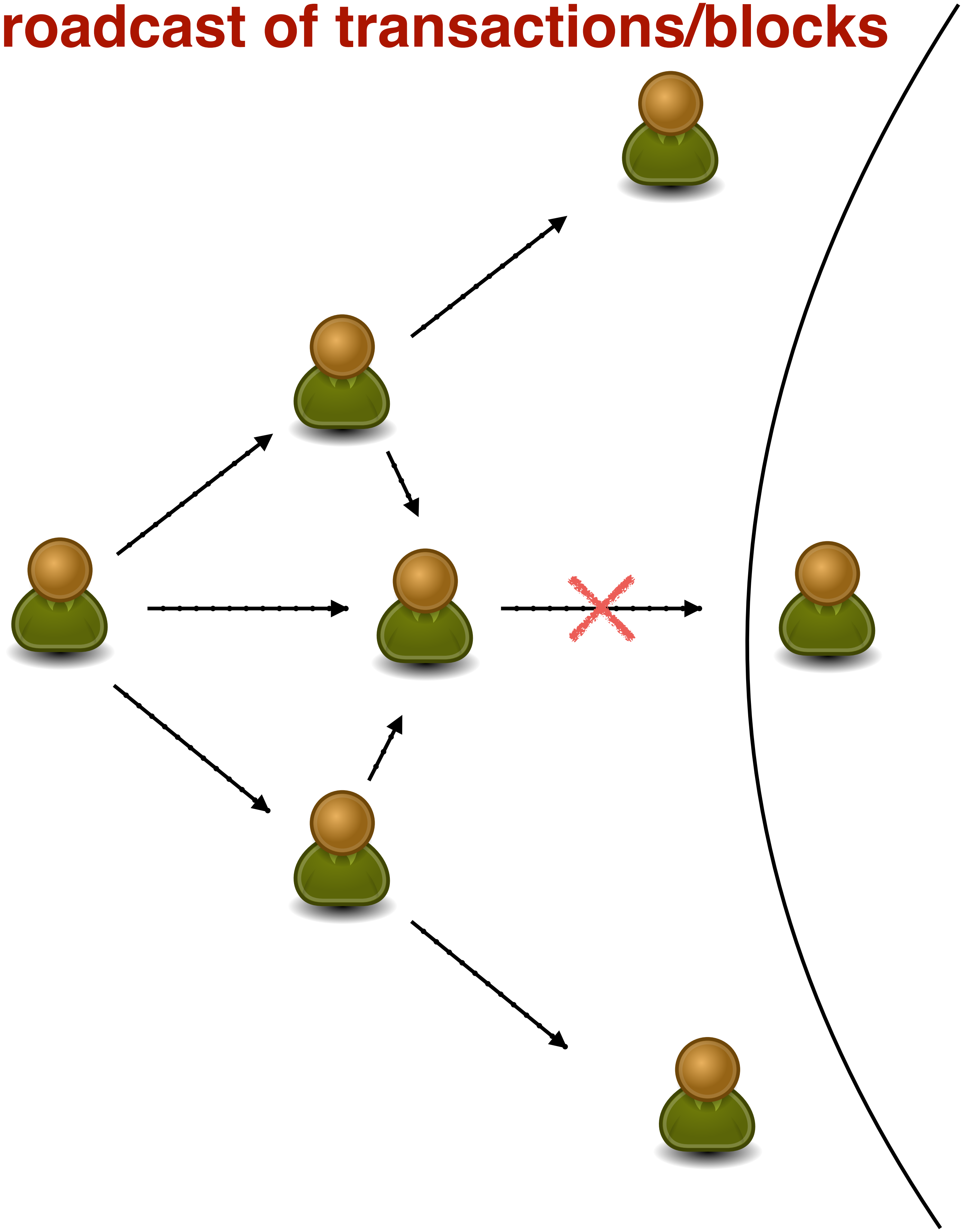
- All transactions, blocks need to be broadcast into the whole network
- Larger blocks
  - → slower propagation
  - → increased consensus latency
- Risks of network partition (stale blocks…)

Broadcast of transactions/blocks



- All transactions, blocks need to be broadcast into the whole network
- Larger blocks
  - → slower propagation
  - → increased consensus latency
- Risks of network partition (stale blocks…)

Broadcast of transactions/blocks



- All transactions, blocks need to be broadcast into the whole network
- Larger blocks
  - → slower propagation
  - → increased consensus latency
- Risks of network partition (stale blocks…)

Selfish Mining

Denial of Service

Double Spending

Which one is a better Blockchain?

10 minutes	2.5 minutes	1 minute	20 seconds

Which one is a better Blockchain?

10 minutes | 2.5 minutes | 1 minute | 20 seconds

Faster block generation → Faster payments

Bigger block size → More payments / slower propagation

Which one is a better Blockchain?

10 minutes | 2.5 minutes | 1 minute | 20 seconds

Faster block generation → Faster payments

Bigger block size → More payments / slower propagation

	Bitcoin	Litecoin	Dogecoin	Ethereum
Propagation Time	8.7 s	1.02 s	0.85 s	0.5 - 0.75 s
Medium Block size	534.8 KB	6.11 KB	8 KB	1.5 KB

Contributions

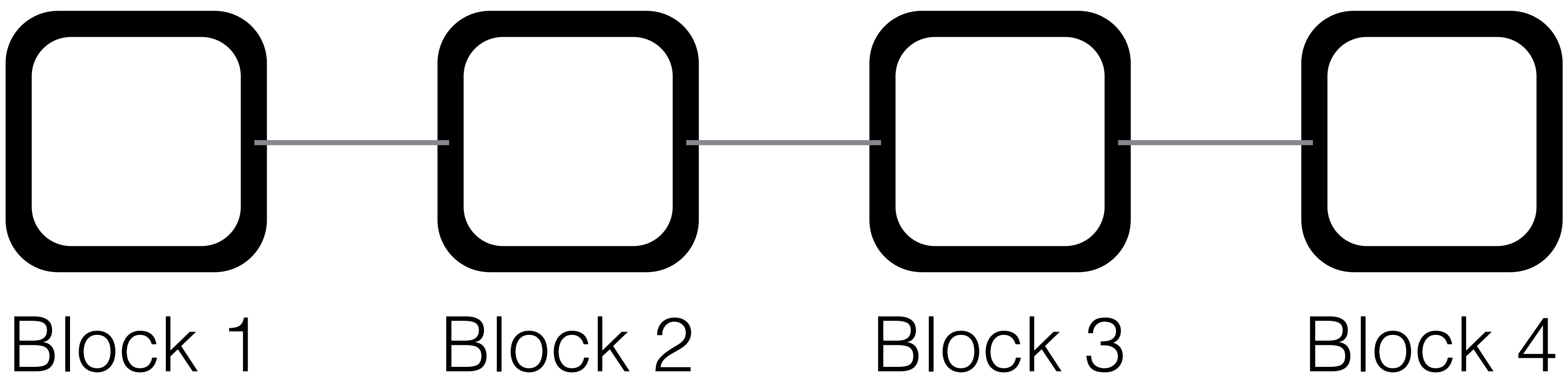
Quantitative Framework

- Compare security of PoW blockchains
- Account for double-spending and selfish mining
- Determine the optimal adversarial strategies
- Provide # of secure confirmations depending on tx value
- Increasing throughput without penalizing security

Open Source Bitcoin Simulator

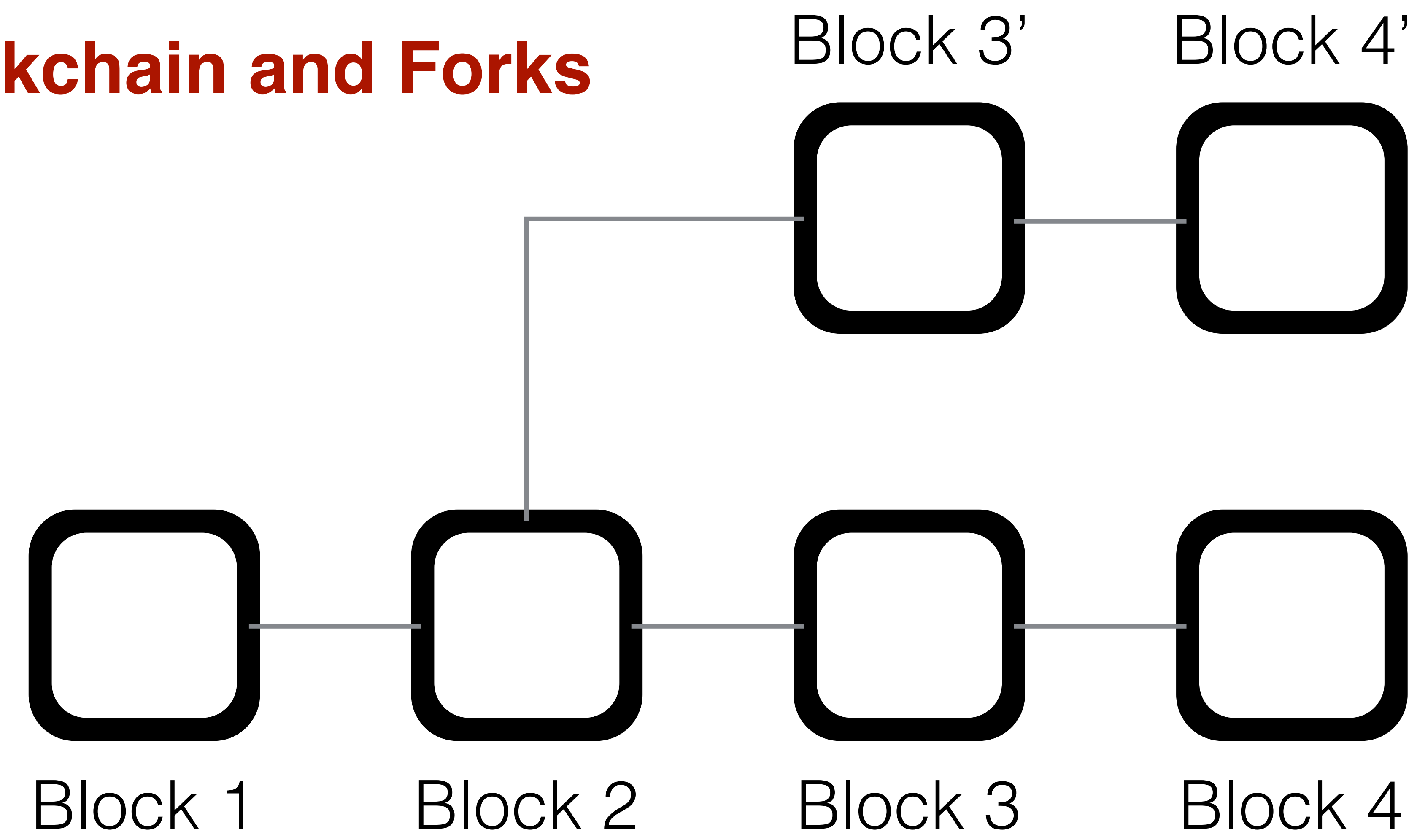
- Realistic simulation of network and blockchain properties
- Flexible reparametrization
- Scalable to thousands of nodes
- Open Source and documented

Blockchain and Forks

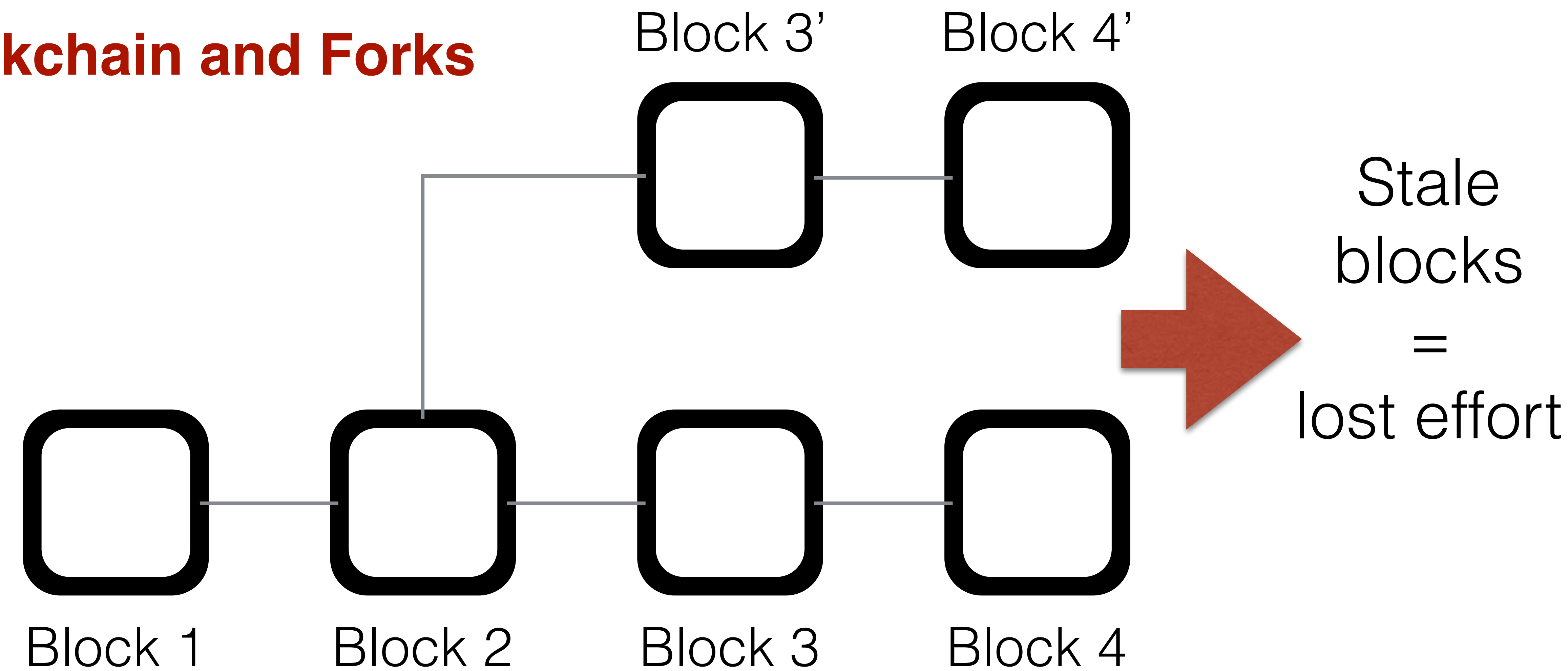


ETH zürich

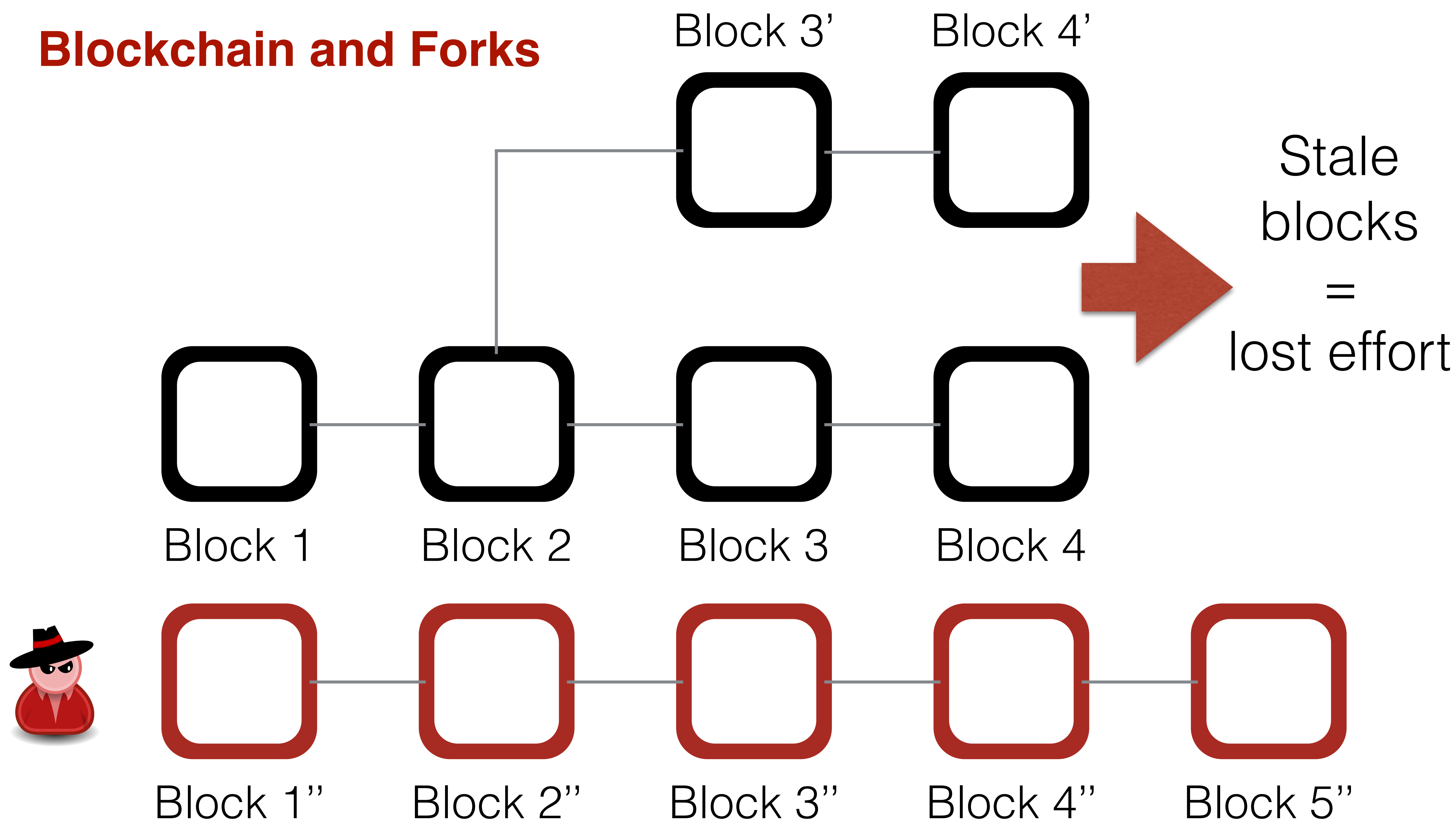
Blockchain and Forks



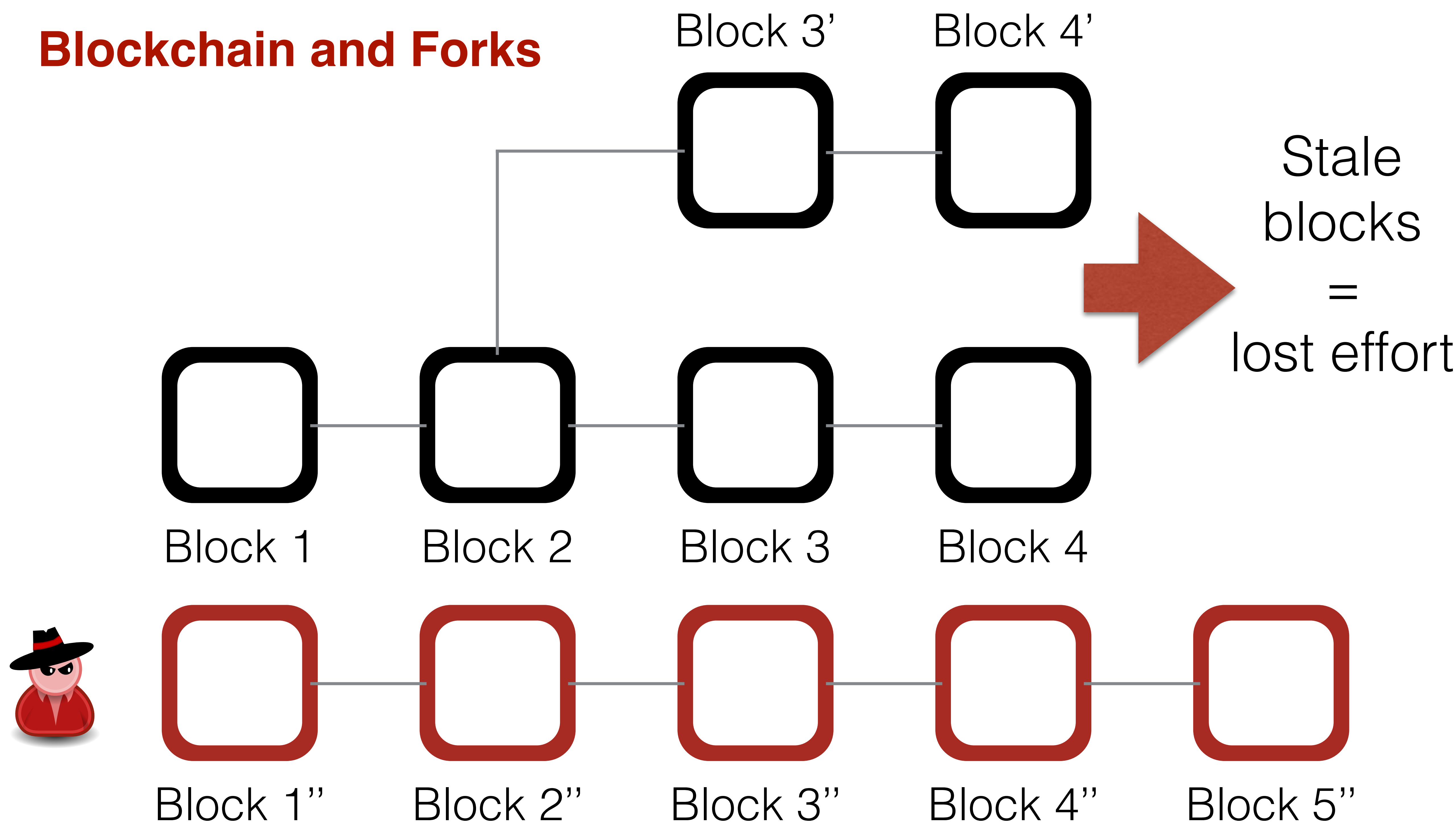
Blockchain and Forks



Blockchain and Forks



Blockchain and Forks



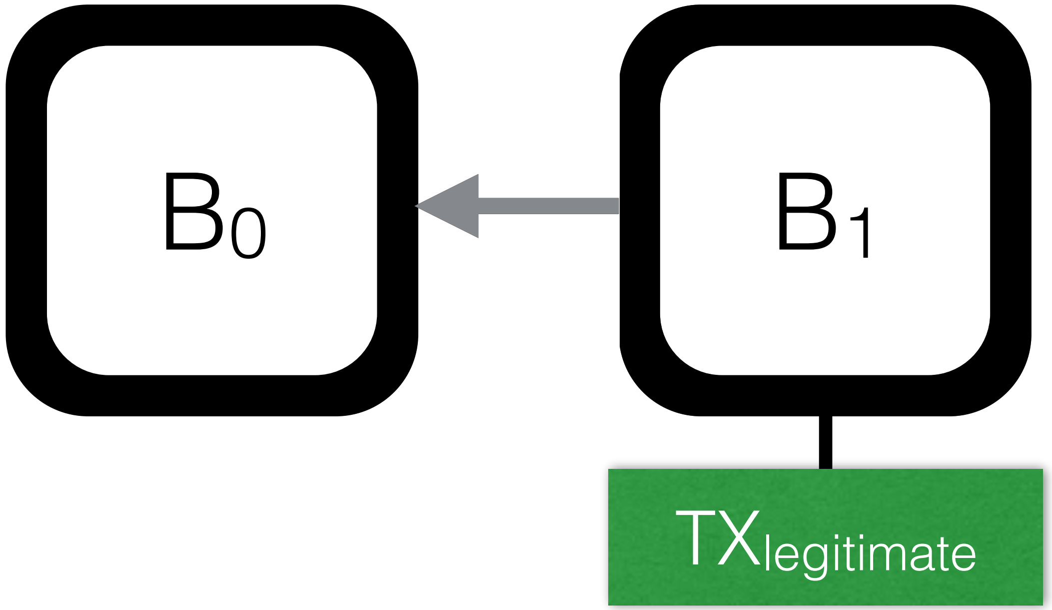
Stale Block rates

Bitcoin	Litecoin	Dogecoin	Ethereum
0.41%	0.273%	0.619%	6.8%

Double Spending

$TX_{legitimate}$ - Pays the vendor

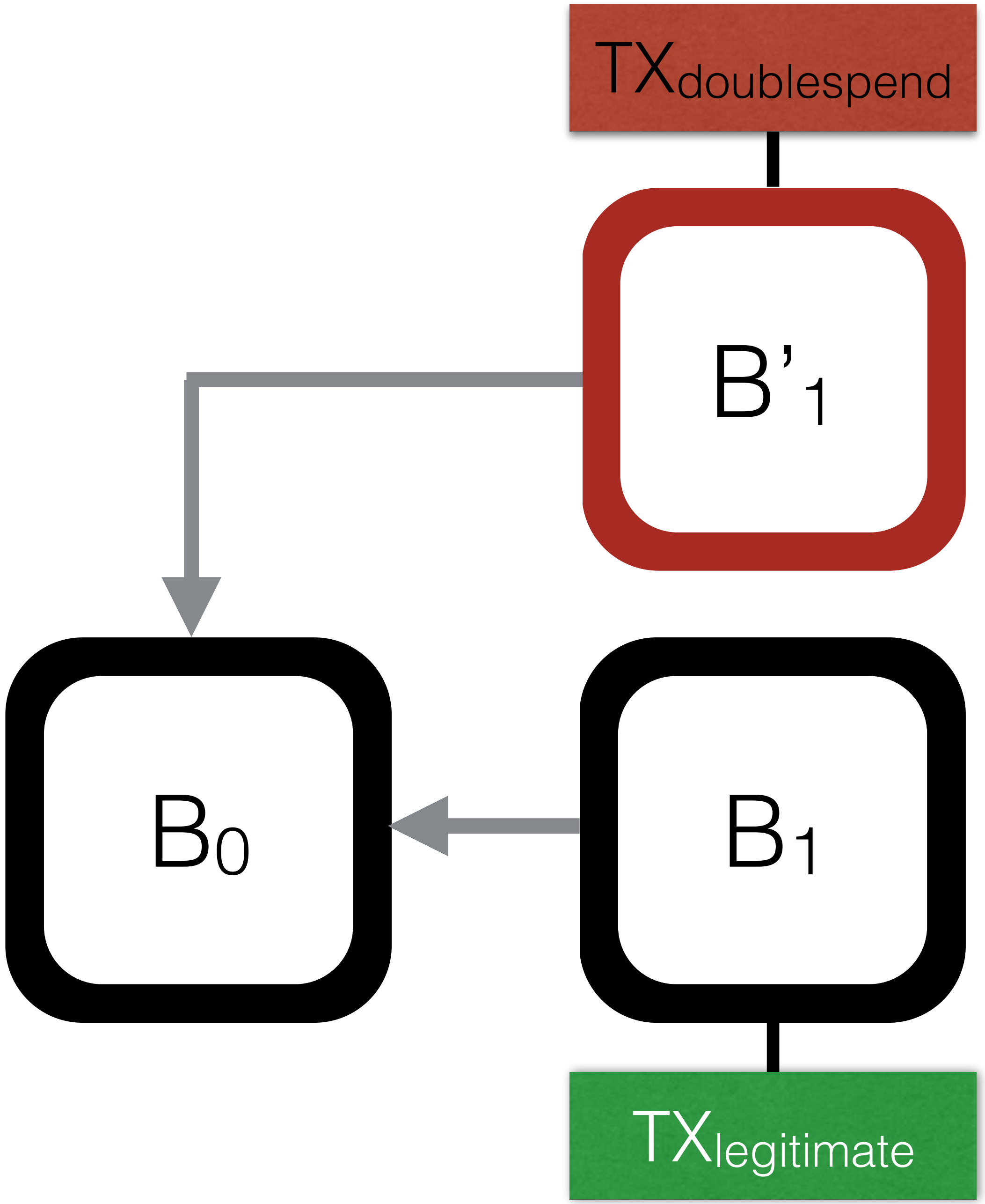
$TX_{doublespend}$ - Pays the adversary



Double Spending

$TX_{legitimate}$ - Pays the vendor

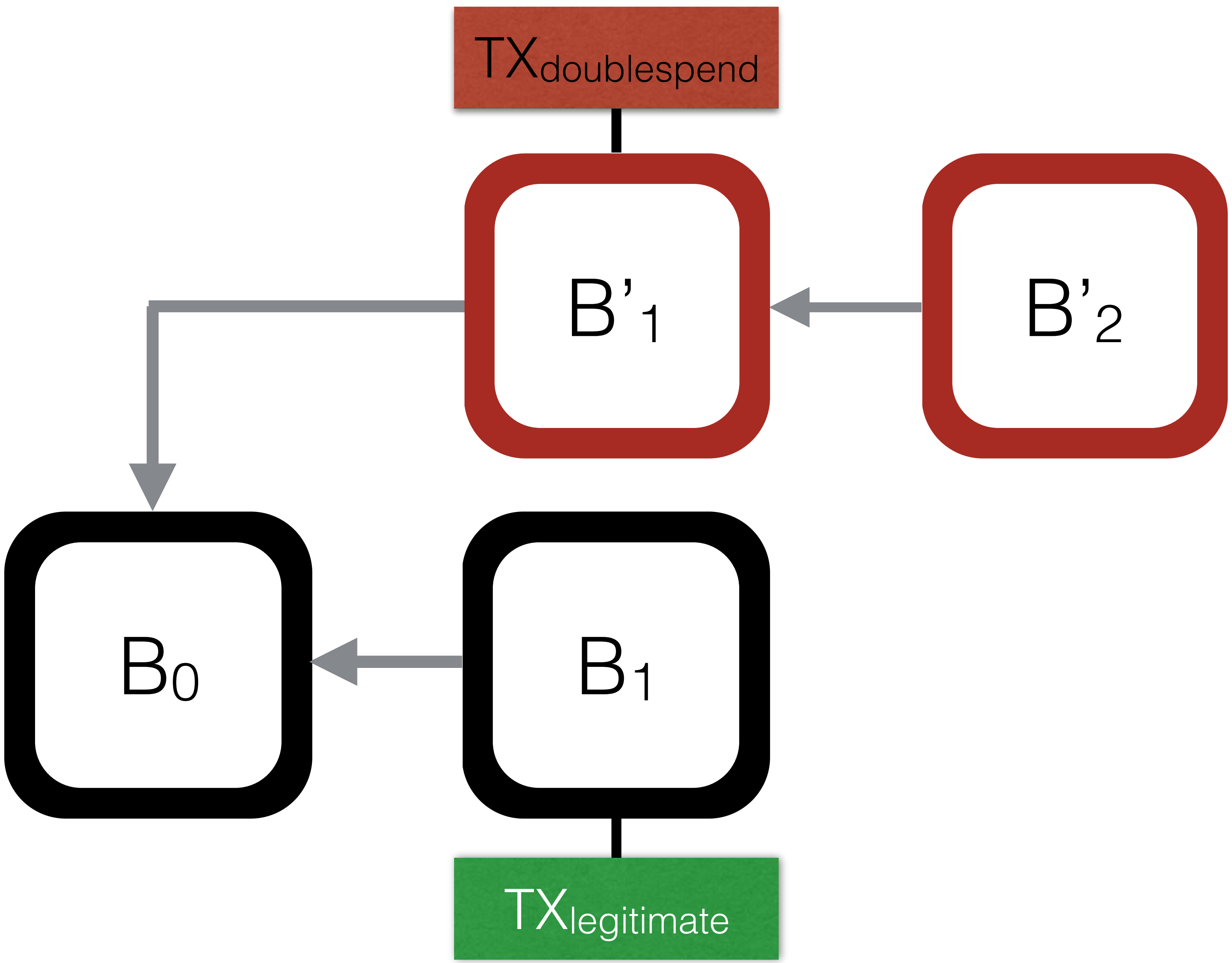
$TX_{doublespend}$ - Pays the adversary



Double Spending

$TX_{legitimate}$ - Pays the vendor

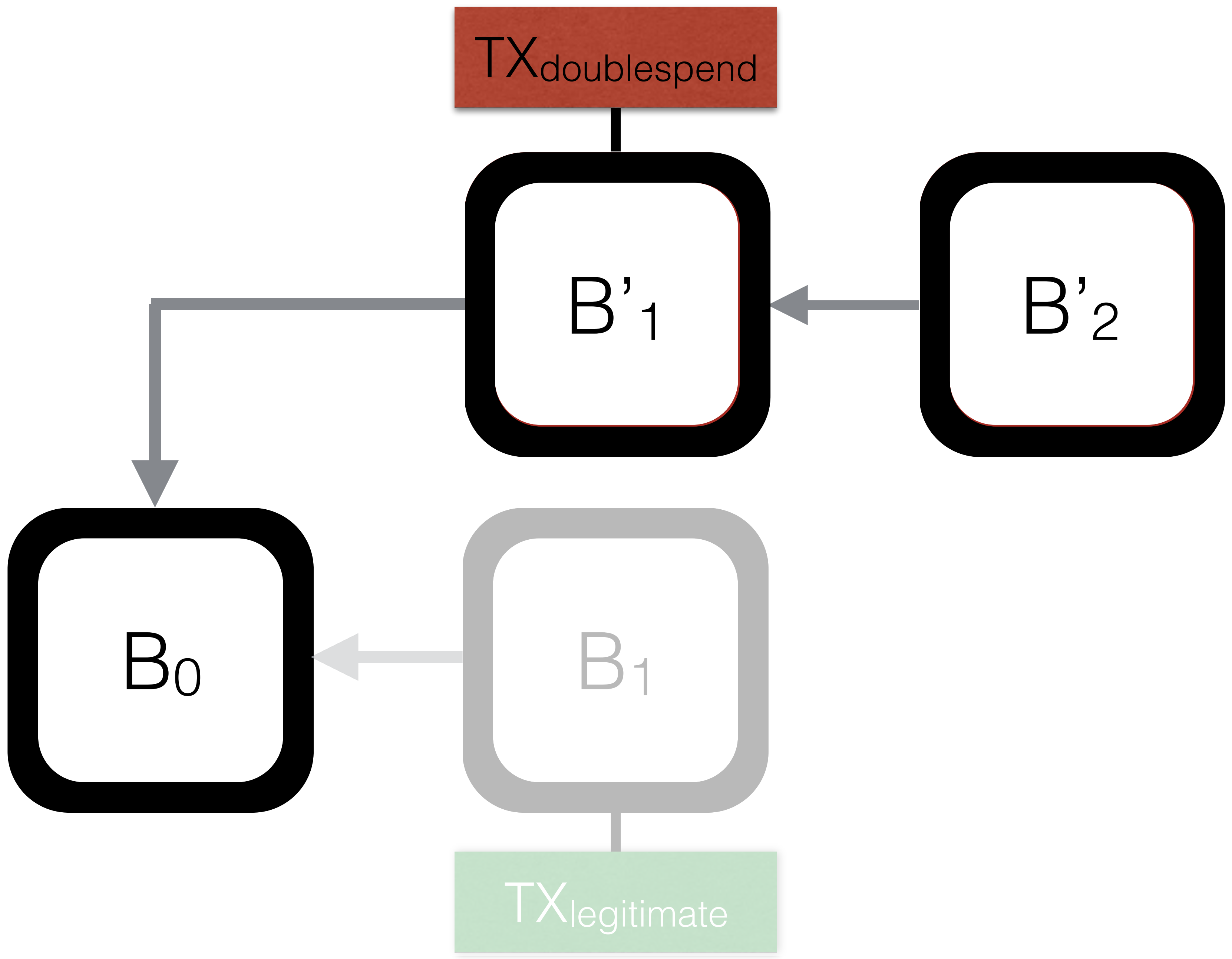
$TX_{doublespend}$ - Pays the adversary



Double Spending

$TX_{legitimate}$ - Pays the vendor

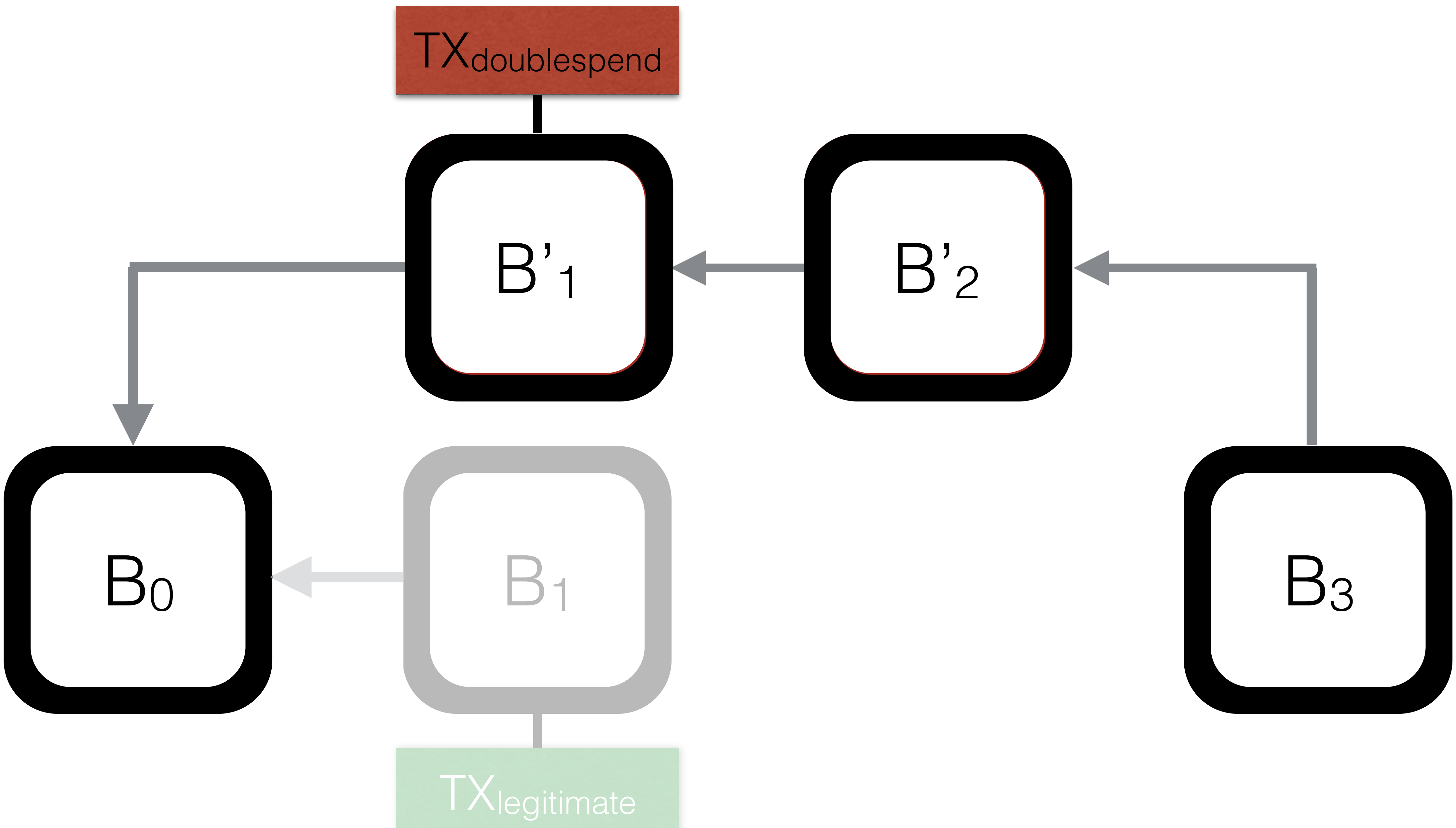
$TX_{doublespend}$ - Pays the adversary



Double Spending

$TX_{legitimate}$ - Pays the vendor

$TX_{doublespend}$ - Pays the adversary



What is Selfish Mining? [Eyal and Sirer]

- Instead of publishing, keep a block private
- Release block to compete

➡ Other miners will perform wasteful computations

➡ Adversary looses block rewards

Selfish Mining vs. Double Spending

Selfish Mining

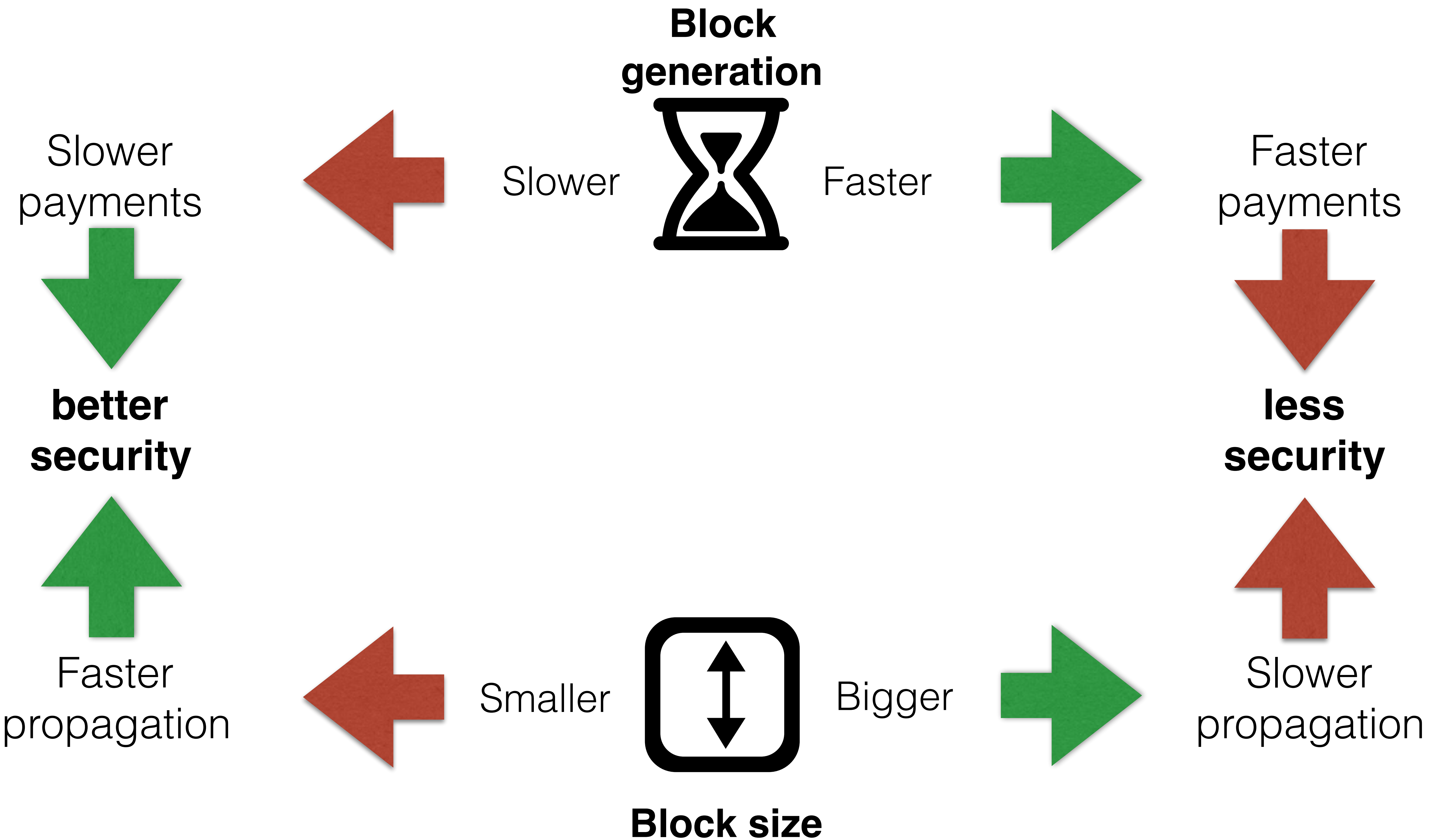
- Increases **relative** reward
- Not necessarily rational

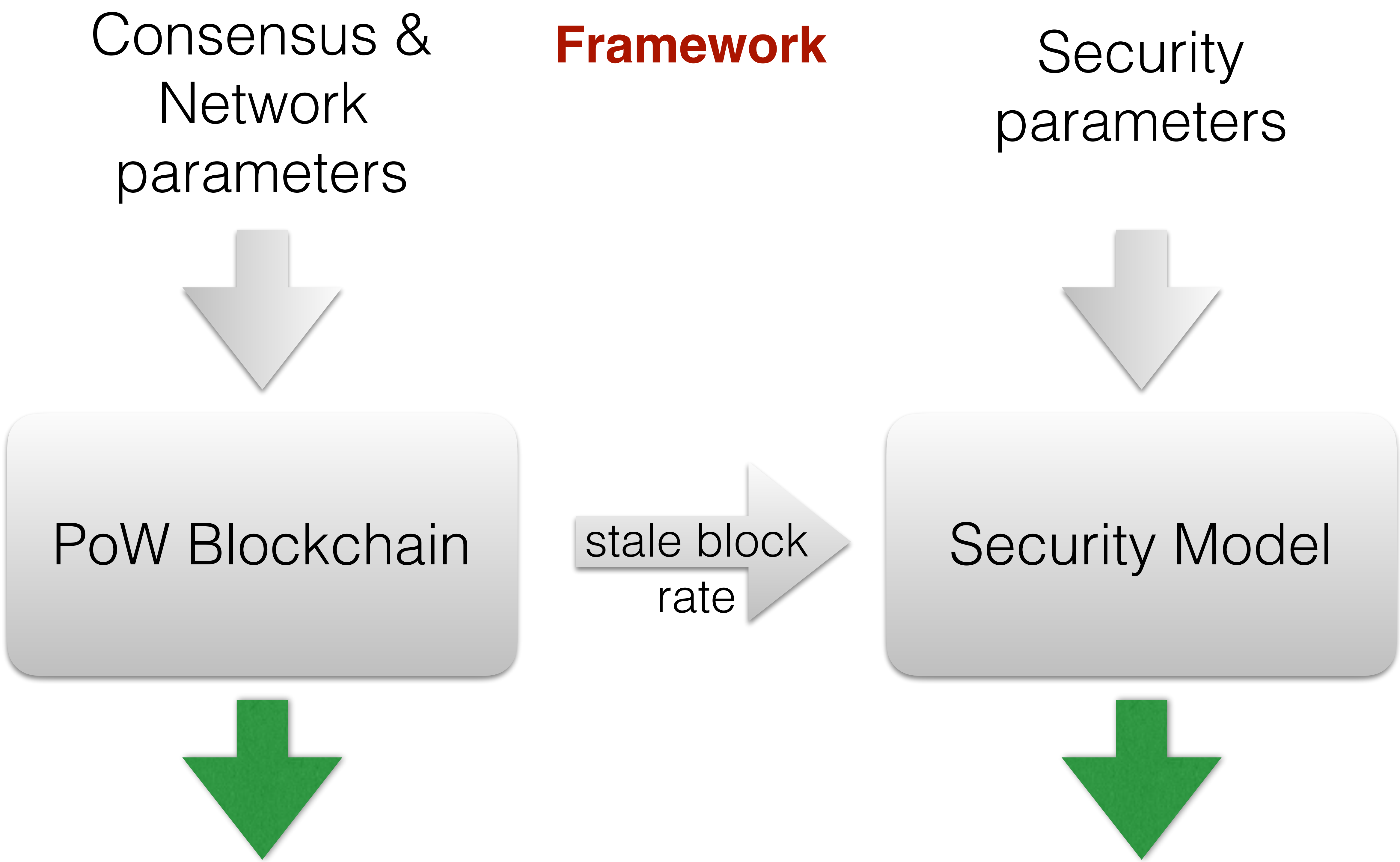
Double Spending

- Increase **absolute** reward
- Economically rational adversary

⇒ Consider them independently

Towards a better Blockchain

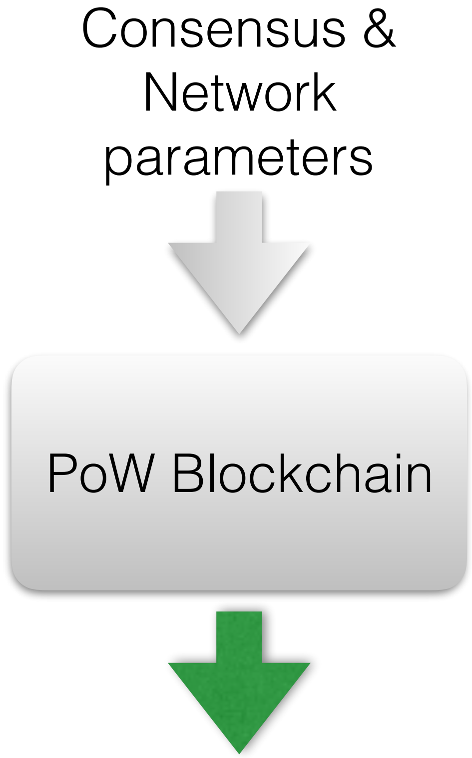




- Block propagation times
- Throughput

- Optimal adversarial strategy
- Security characteristics

PoW Blockchain



- **Stale block rate**
- Block propagation times
- Throughput

Blockchain instance can be

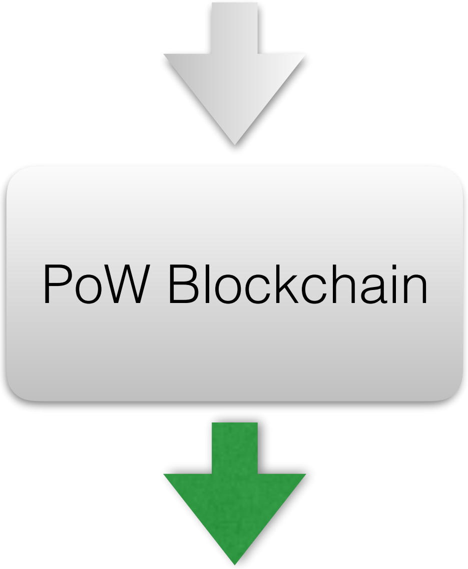
- A **real** blockchain (e.g. Bitcoin, Ethereum)
- **Simulated** blockchain

Simulator captures (**Open Source**)

Consensus parameter	Network-Layer Parameters
Block interval distribution	Block size distribution
Mining power dist.	Geographical distribution of nodes/miners
	Number of connections of nodes/miners
	Propagation Protocol

PoW Blockchain

Consensus & Network parameters



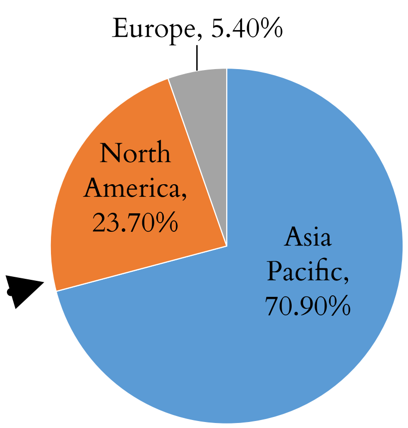
- **Stale block rate**
- Block propagation times
- Throughput

Blockchain instance can be

- A **real** blockchain (e.g. Bitcoin, Ethereum)
- **Simulated** blockchain

Simulator captures (**Open Source**)

Consensus parameter	Network-Layer Parameters
Block interval distribution	Block size distribution
Mining power dist.	Geographical distribution of nodes/miners
	Number of connections of nodes/miners
	Propagation Protocol



PoW Blockchain

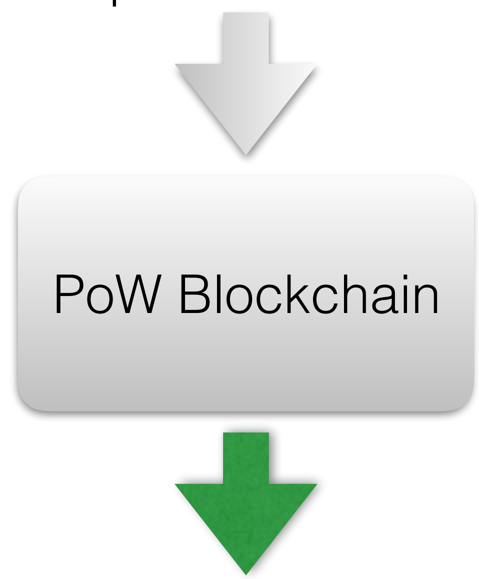
Blockchain instance can be

- A **real** blockchain (e.g. Bitcoin, Ethereum)
- **Simulated** blockchain

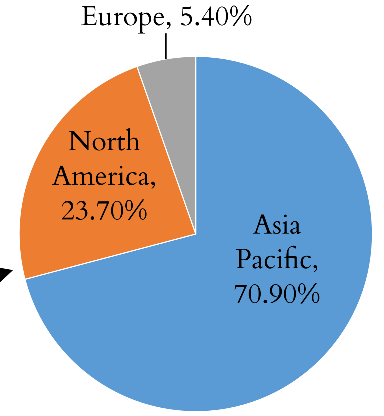
Simulator captures (**Open Source**)

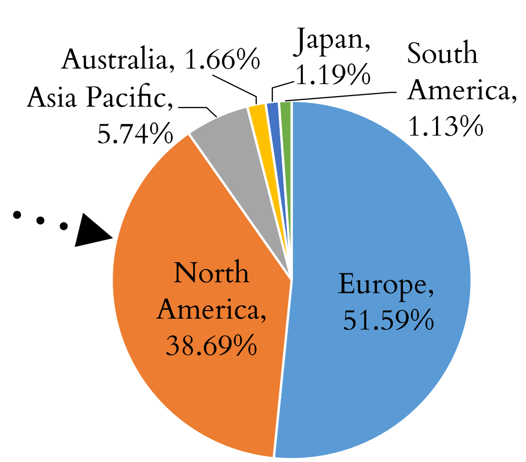
Consensus parameter	Network-Layer Parameters
Block interval distribution	Block size distribution
Mining power dist.	Geographical distribution of nodes/miners
	Number of connections of nodes/miners
	Propagation Protocol

Consensus & Network parameters



- **Stale block rate**
- Block propagation times
- Throughput

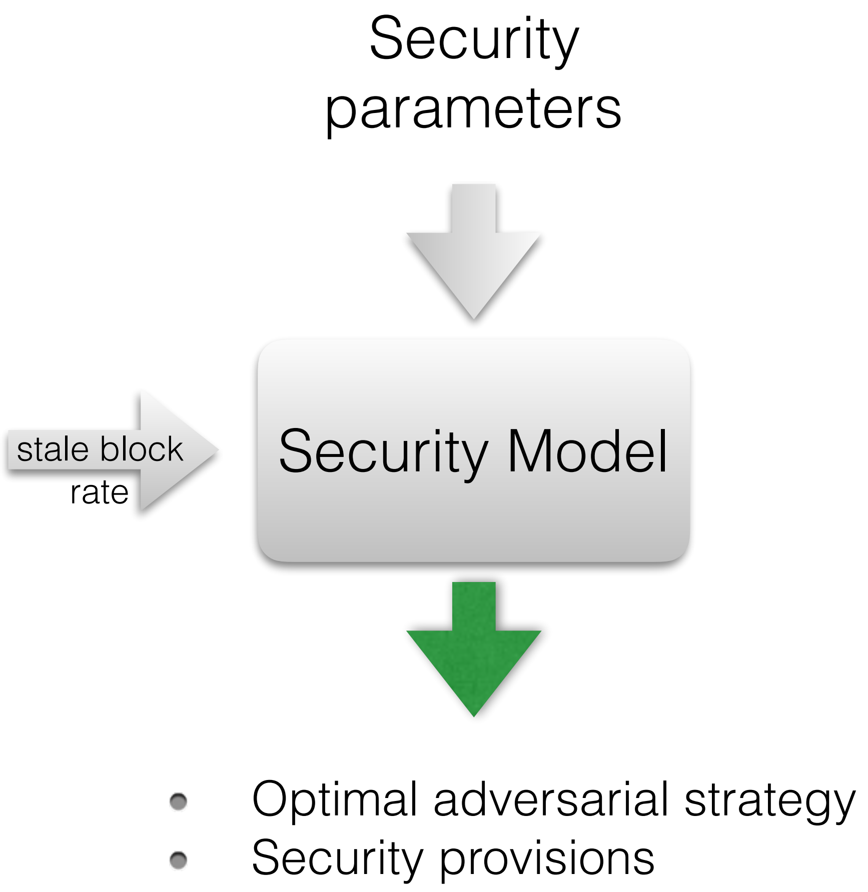




Security Model

Captures **optimal adversarial** strategies

- for Selfish Mining
- for Double Spending
- based on **Markov Decision Processes**



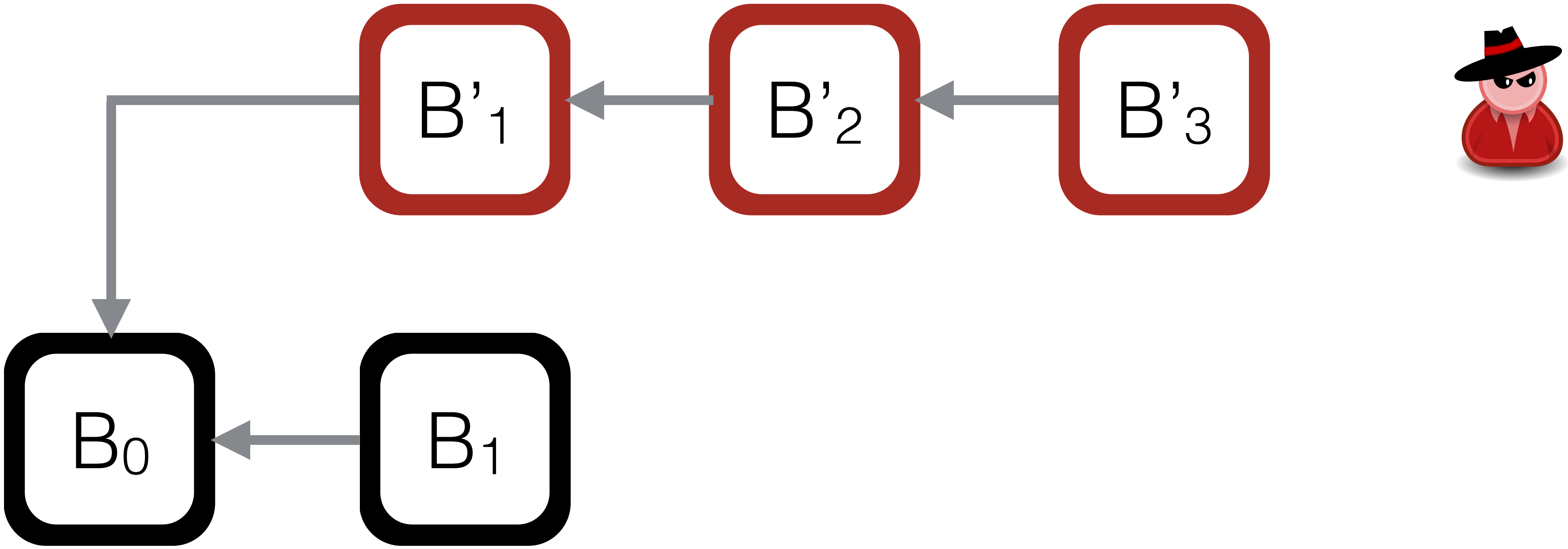
Security Parameters

- Adversarial mining power
- Stale block rate
- Connectivity of the adversary
- Impact of eclipse attacks
- Mining costs
- Number of required confirmations

Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space

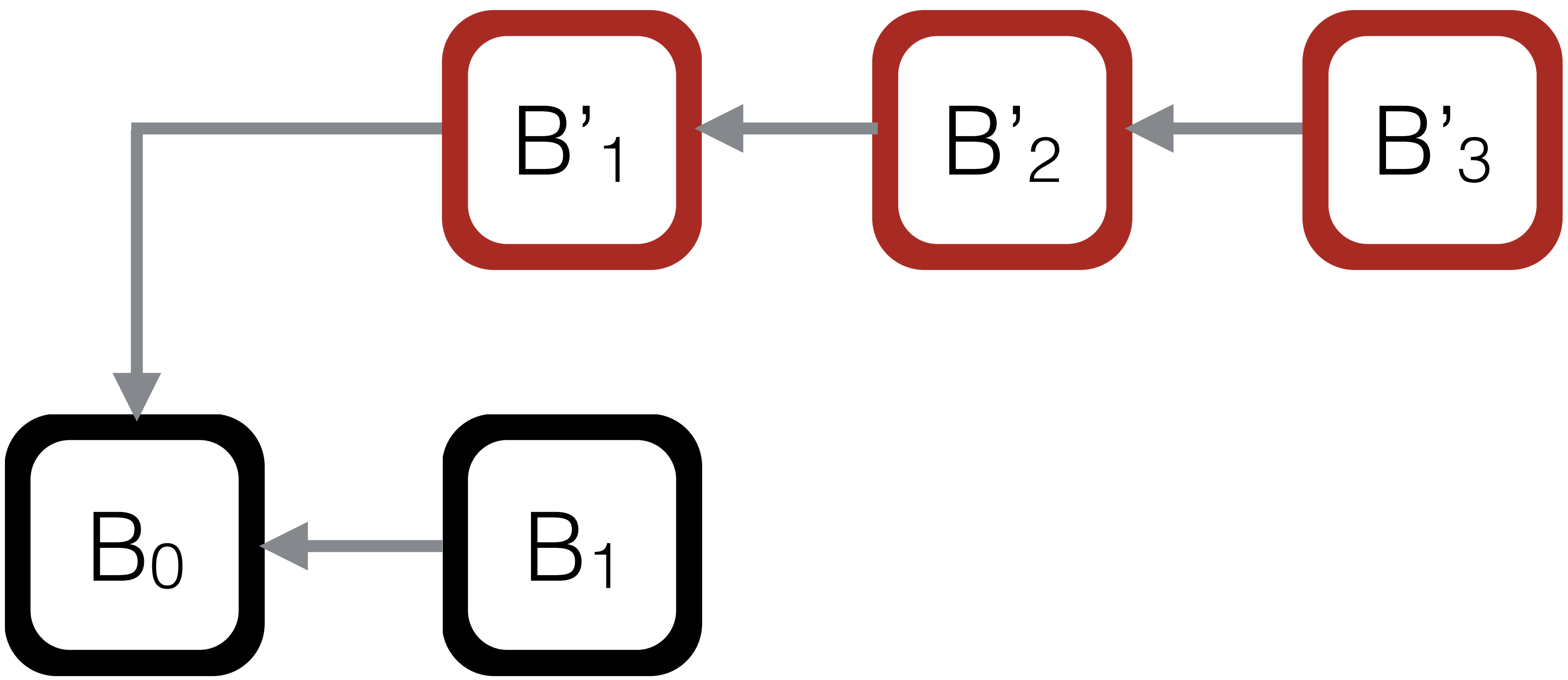


State: (3, 1)

Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space

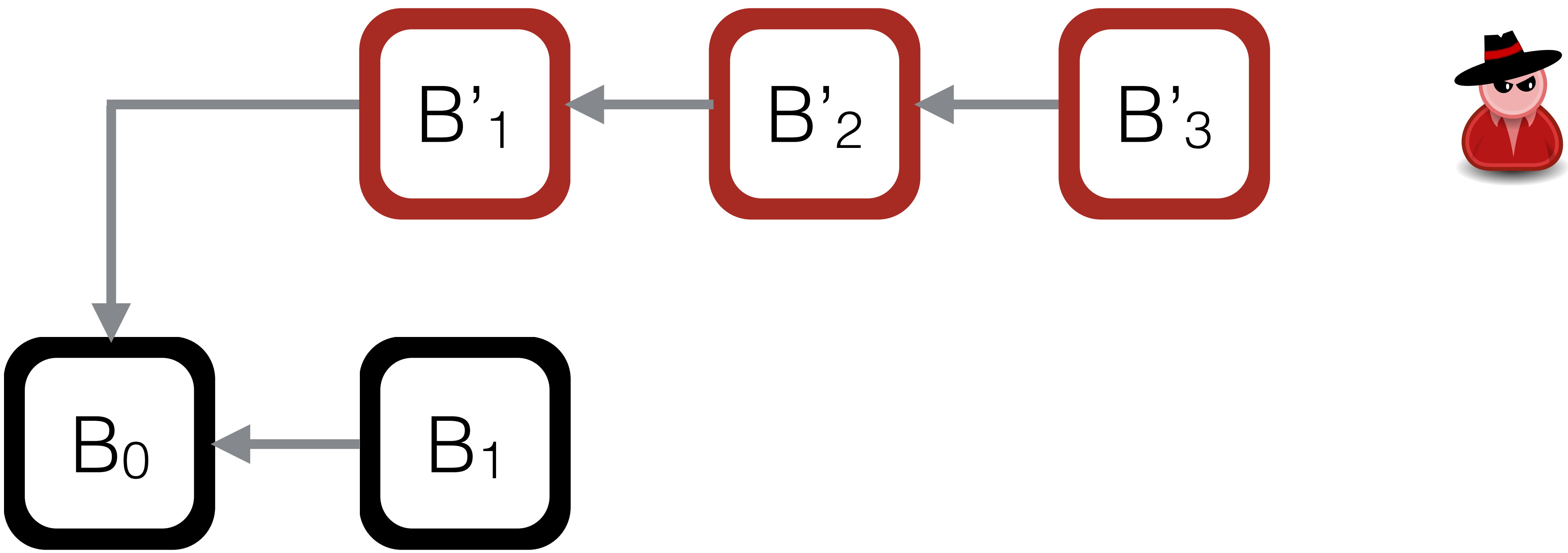


State: (3, 1)

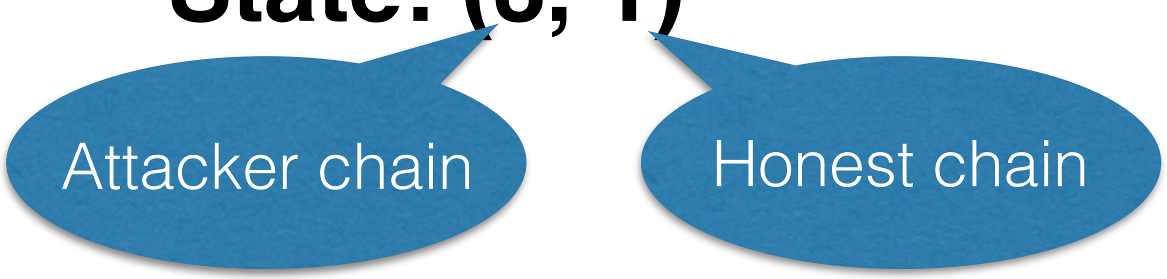
Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space



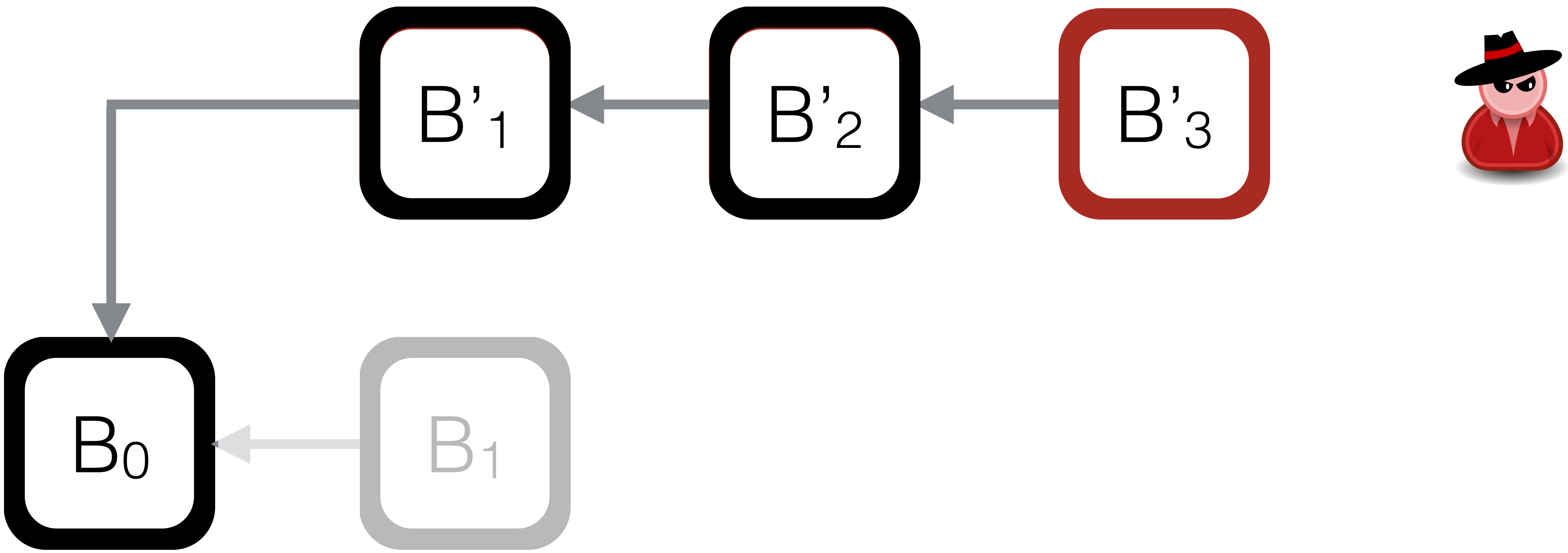
State: (3, 1)



Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space



State: (3, 1)

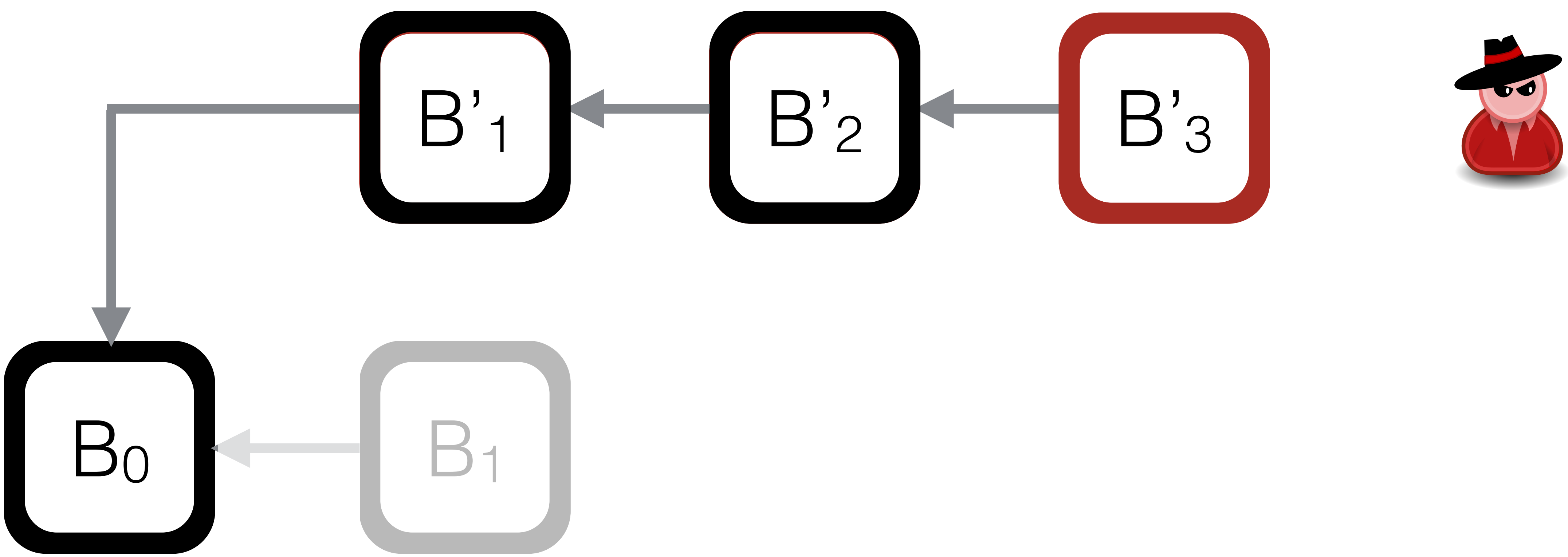
Attacker chain

Honest chain

Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space

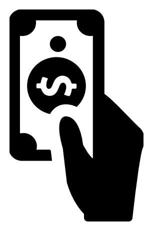


State: (3, 1)

Attacker chain

Honest chain

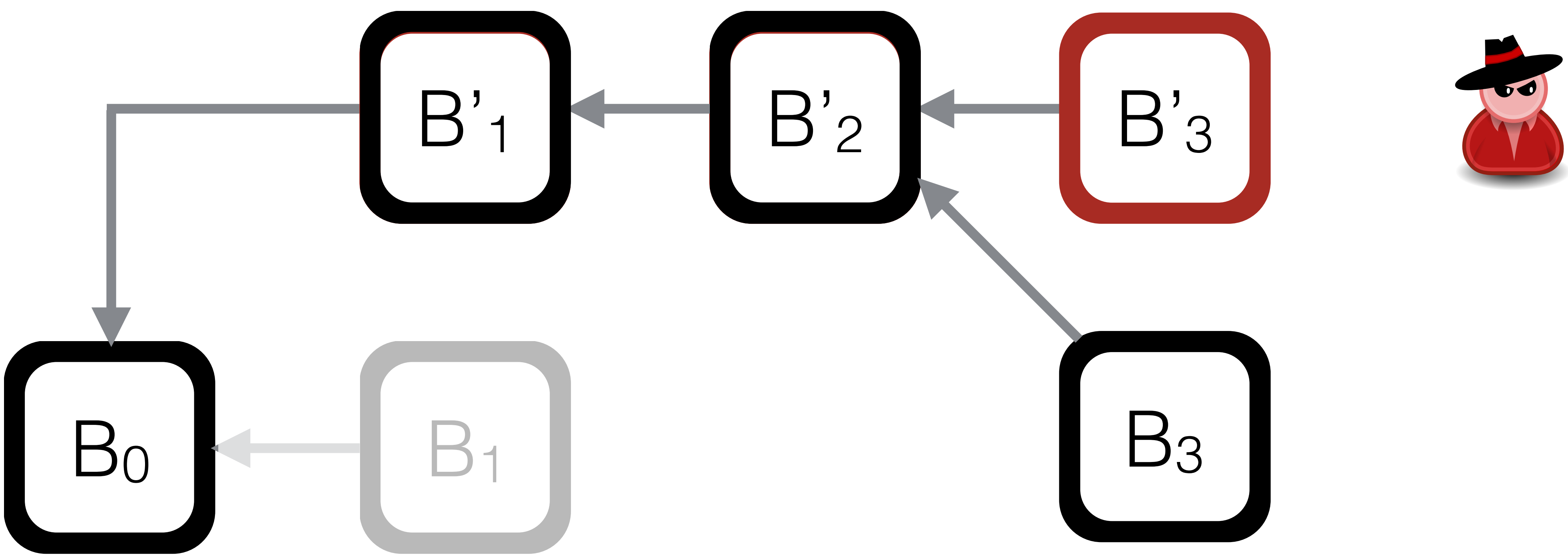
Reward for adversary: 2



Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space



State: (3, 1) → (1, 1)

Attacker chain

Honest chain

Reward for adversary: 2

How many confirmations required to match security?

	Ethereum	vs.	Bitcoin
Stale block rate	6.8 %		0.41 %

How many confirmations required to match security?

vs.

smaller block rewards

higher stale block rate

Stale block rate	6.8 %	0.41 %

How many confirmations required to match security?

	Ethereum	vs.	Bitcoin
	smaller block rewards		
	higher stale block rate		
Stale block rate	6.8 %		0.41 %
Matching Block confirmations, 30% adversary	37 12.4 minutes		6 60 minutes

Litecoin would require 28, and Dogecoin 47 block confirmations respectively to match the security of 6 Bitcoin confirmations.

Increasing throughput?

Based on Simulator results

- 1 MB blocks
- 1 Minute Block interval

Increasing throughput?

Based on Simulator results

- 1 MB blocks
- 1 Minute Block interval

→ Stale block rate does not increase substantially

Increasing throughput?

Based on Simulator results

- 1 MB blocks
- 1 Minute Block interval

→ Stale block rate does not increase substantially

→ **From 7 tps to 60 tps, without sacrifising security**

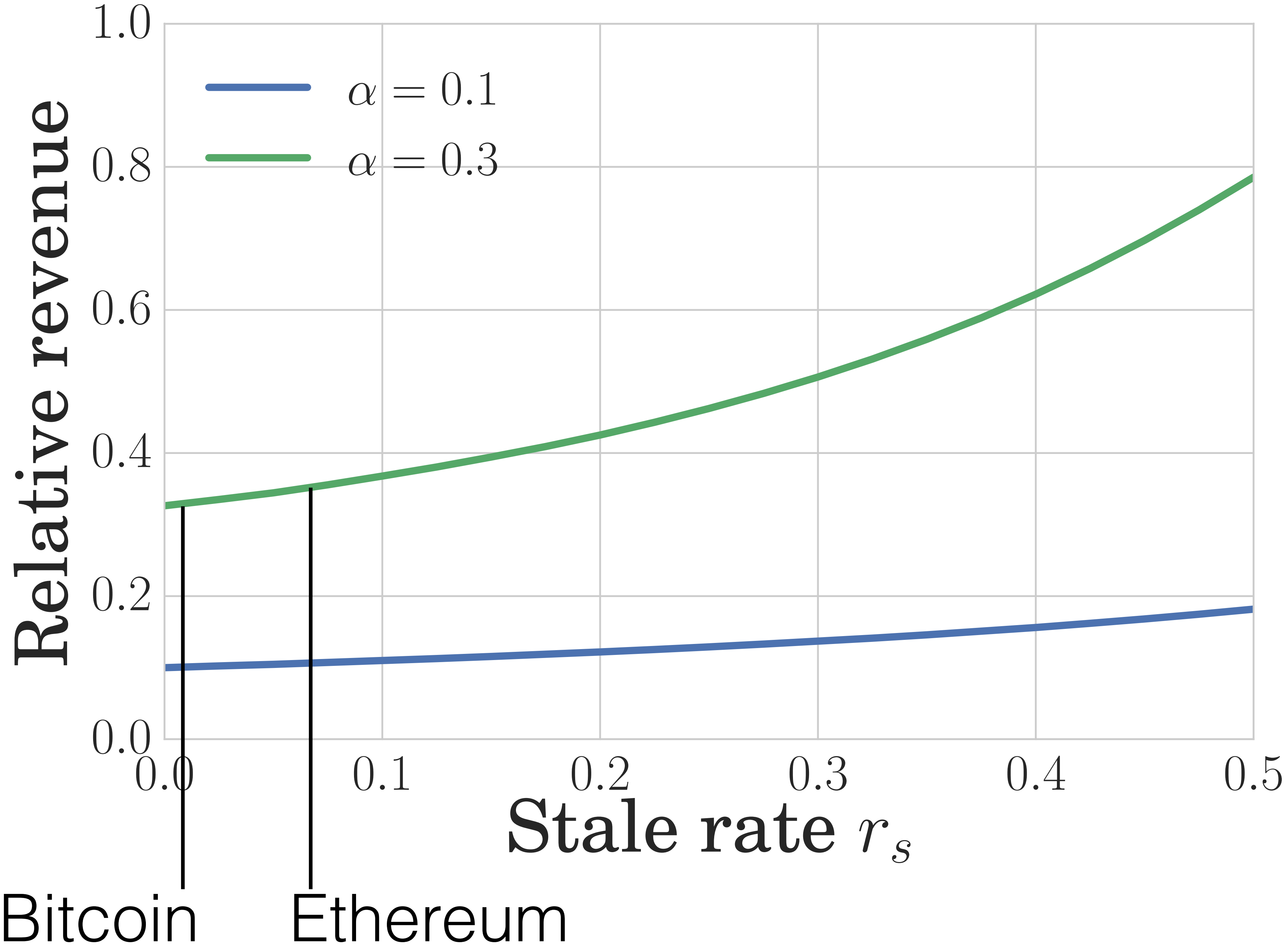
Selfish Mining under constant difficulty

Mining 1000 blocks

- 30 % selfish miner mines 209 blocks, instead of 300! (under optimal strategy)
- Eyal and Sirer's strategy yields on average 205.8 blocks

→ Selfish Mining yield fewer block rewards than honest mining.

Influence of Stale Block rate on Selfish Mining

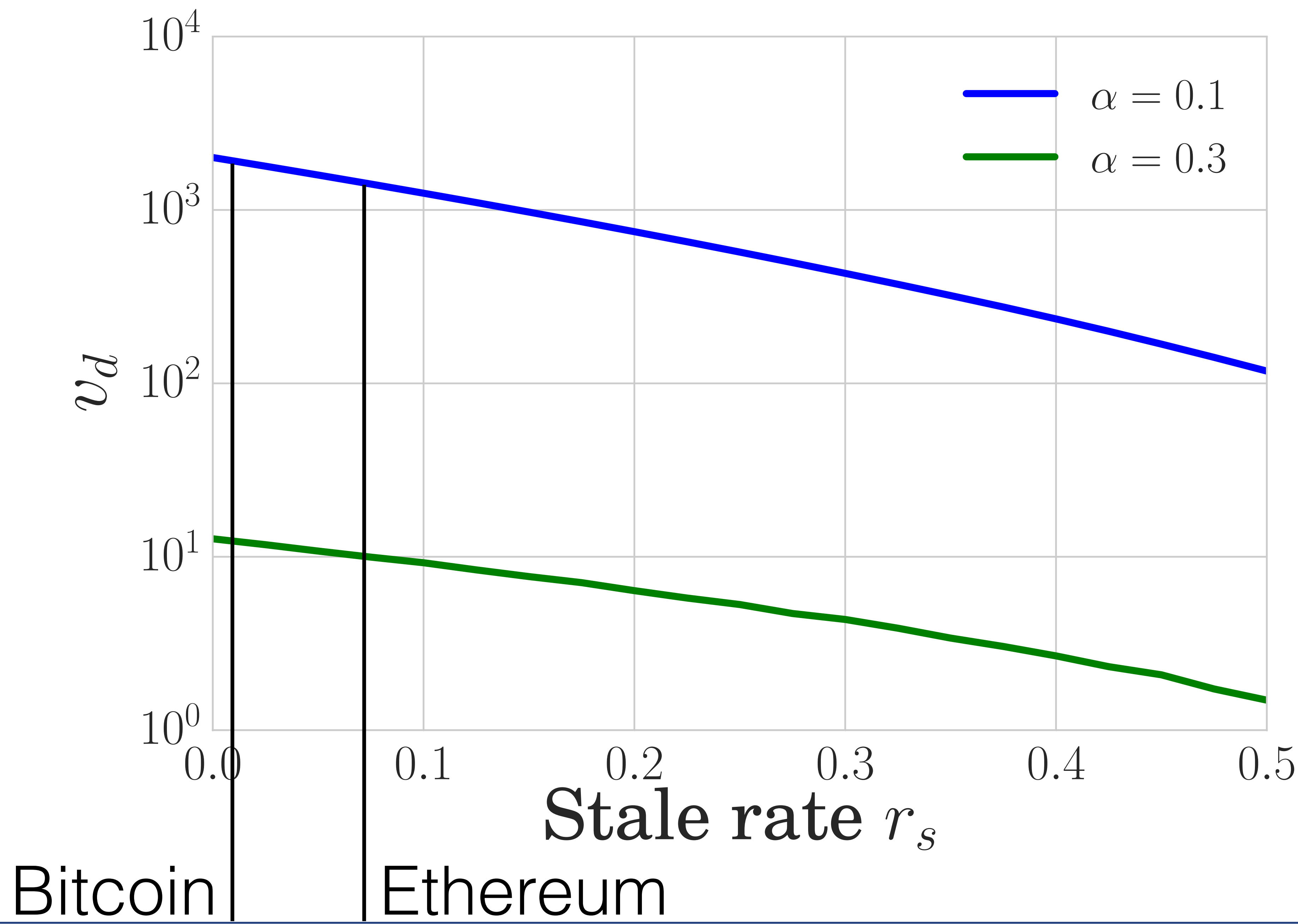


The higher the stale block rate the higher the relative revenue

Double-Spending

Profitability depends on transaction value

- Quantifying resilience using minimum v_d, s.t. double-spending is profitable

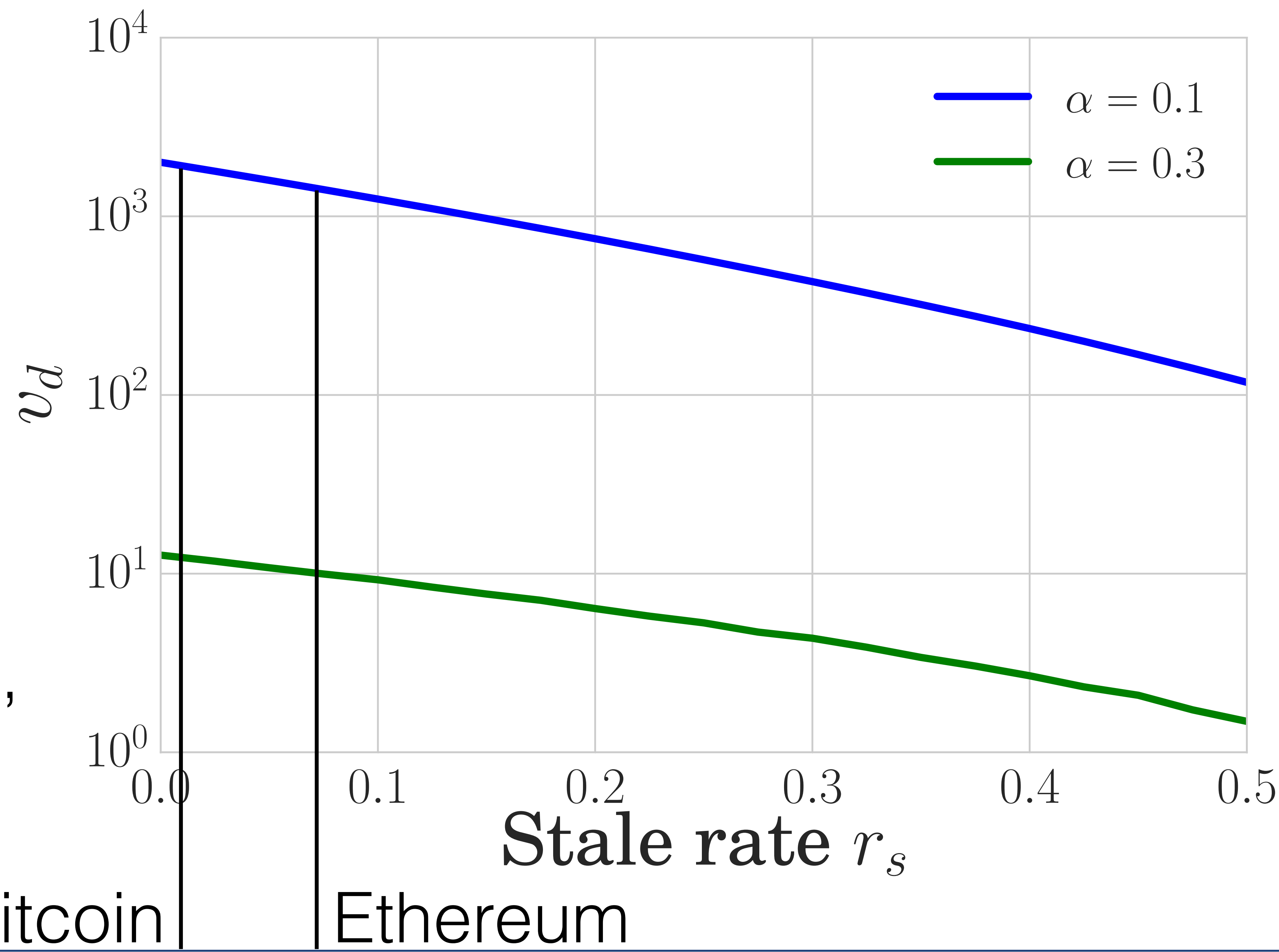


Double-Spending

Profitability depends on transaction value

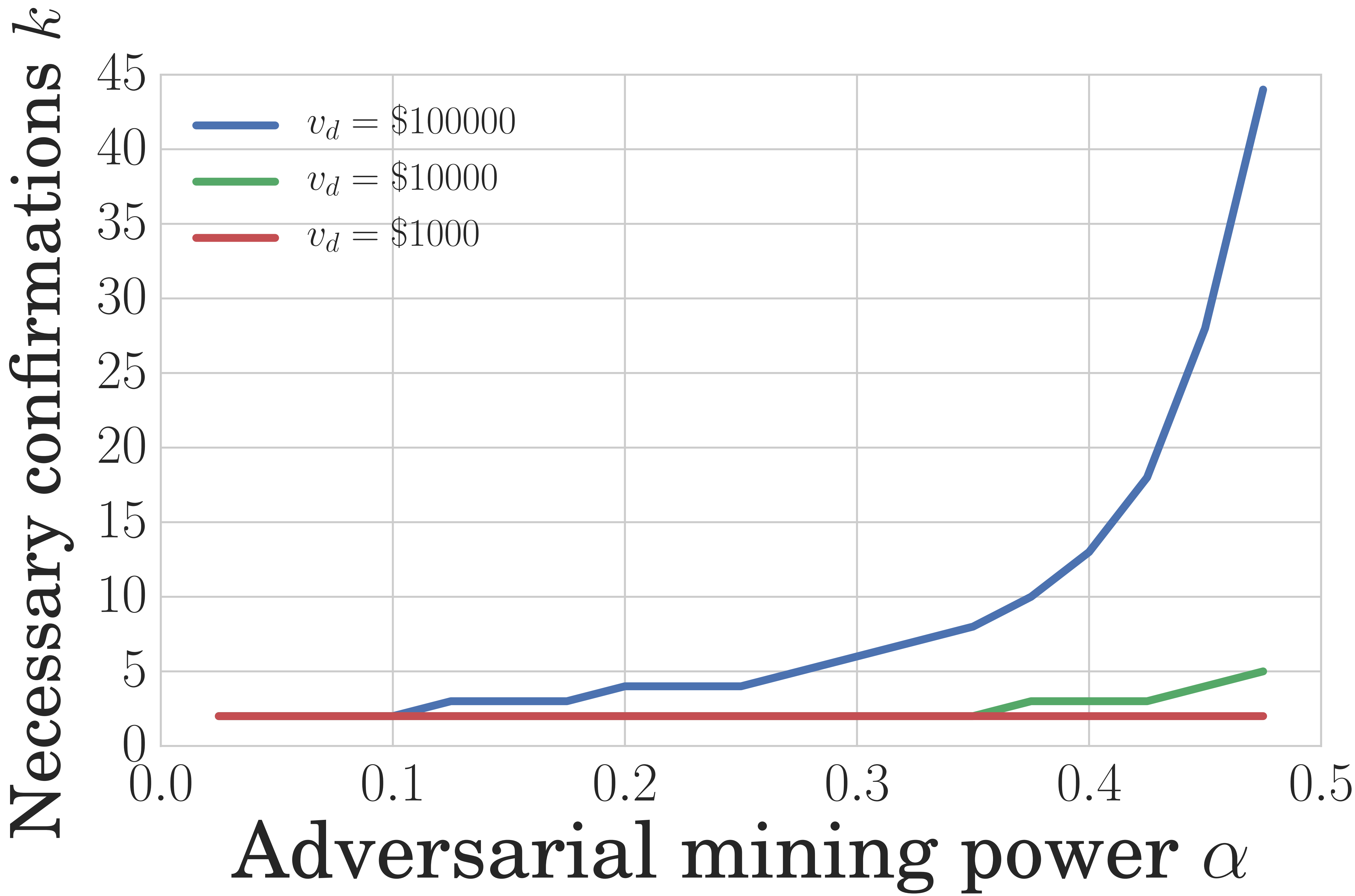
- Quantifying resilience using minimum v_d, s.t. double-spending is profitable

Threshold at which double-spending is more profitable than honest mining



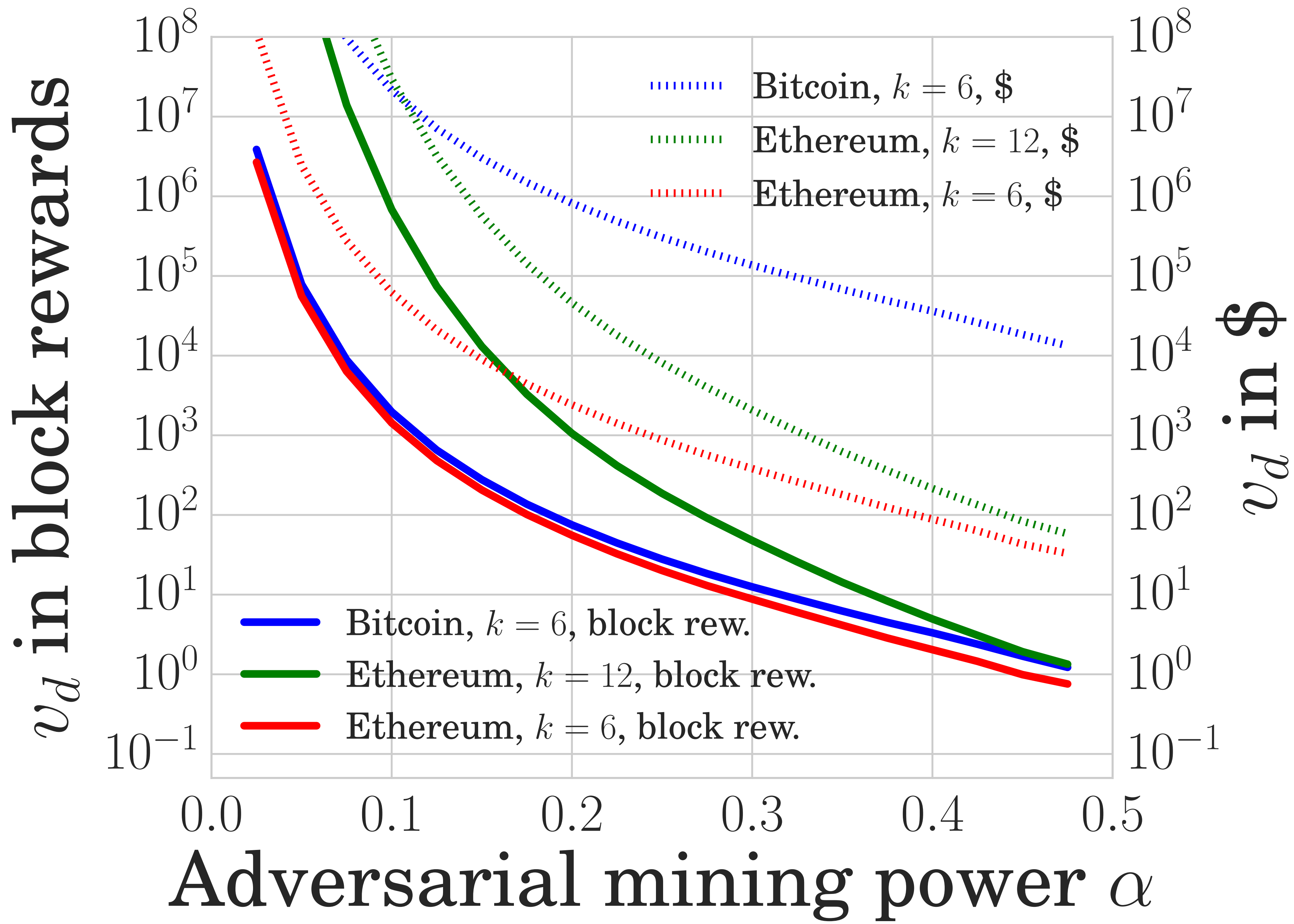
The higher the v_d, the better

Number of required confirmations (Bitcoin)



ETH zürich

Double Spending Bitcoin vs. Ethereum



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

Block reward impact

For a fixed transaction value

- We show that the higher the block reward (e.g., in USD), the more resilient it is against double-spending

Merchant can vary the # of confirmations depending on the transaction value

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Block confirmation equivalence

6 Bitcoin = 37 Ethereum (20 sec)
= 28 Litecoin (2.5 min)
= 47 Dogecoin (1 min)

The higher the block reward in USD, the more resilient against double spending

Summary

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Block confirmation equivalence

6 Bitcoin = 37 Ethereum (20 sec)
= 28 Litecoin (2.5 min)
= 47 Dogecoin (1 min)

The higher the block reward in USD, the more resilient against double spending

Good block size/interval

1 MB block and
1 Minute block interval

+60 transactions/s
without scarifying security

(instead of Bitcoin 7 tps)

ETH zürich

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Thank you!

Block confirmation equivalence

6 Bitcoin = 37 Ethereum (20 sec)
= 28 Litecoin (2.5 min)
= 47 Dogecoin (1 min)

The higher the block reward in USD, the more resilient against double spending

Good block size/interval

1 MB block and
1 Minute block interval

+60 transactions/s
without scarifying security

(instead of Bitcoin 7 tps)

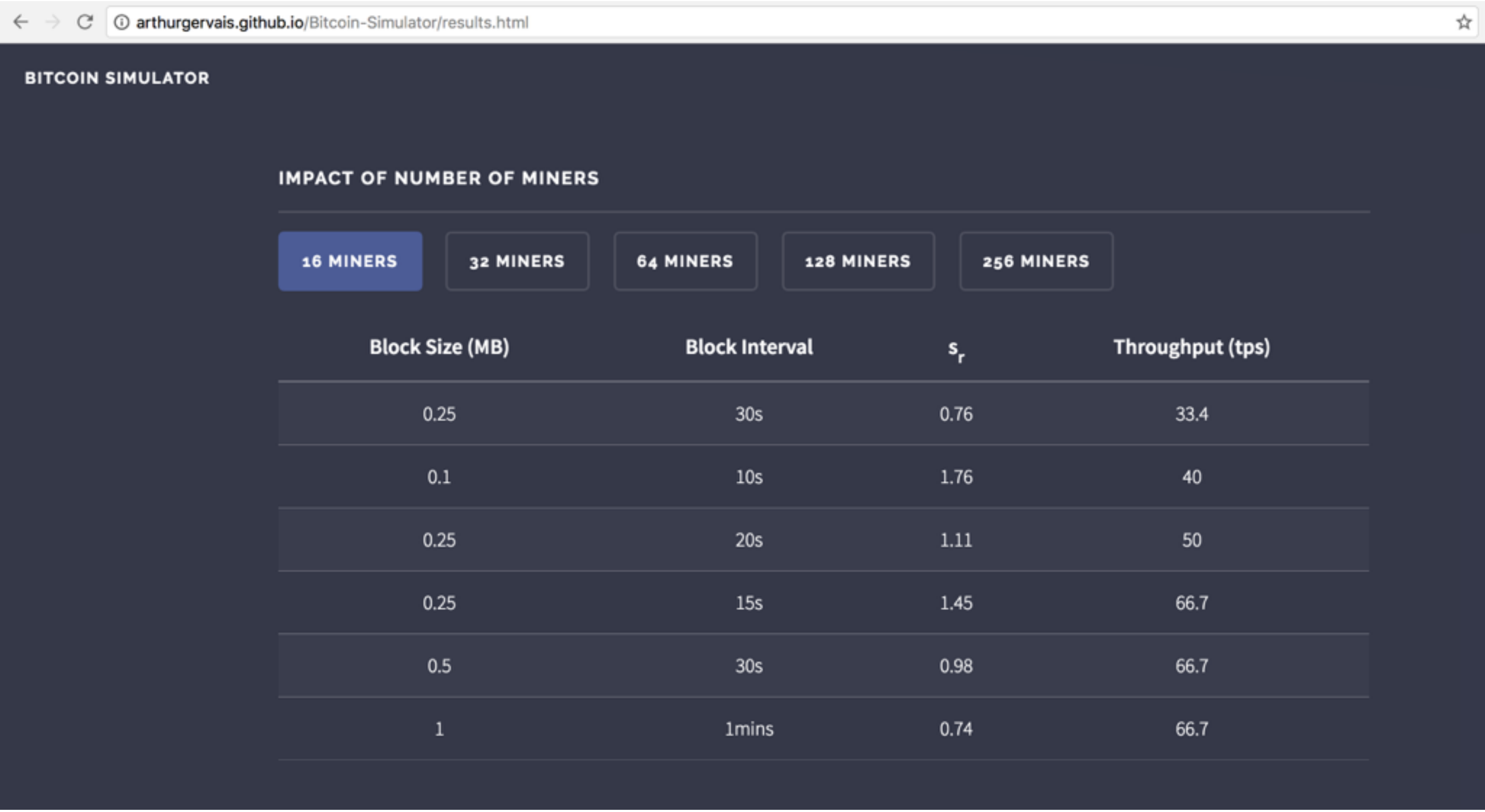
arthurgervais.github.io/Bitcoin-Simulator/results.html

BITCOIN SIMULATOR

IMPACT OF BLOCK GENERATION INTERVAL

STANDARD

Interval	t_{mean} (s)	t_{median} (s)	$t_{10\%}$ (s)	$t_{25\%}$ (s)	$t_{75\%}$ (s)	$t_{90\%}$ (s)	s_r	Bandwidth (kbps)
25 mins	61.23	35.73	18.43	24.15	52.59	91.02	1.72%	14.14
10mins	25.83	14.7	7.87	10.14	21.29	35.47	1.51%	14.26
2.5mins	6.83	4.18	2.52	3.06	5.76	9.12	1.82%	14.51
1mins	3.02	2.08	1.43	1.65	2.68	3.76	2.15%	14.71
30s	1.81	1.43	1.07	1.2	1.77	2.3	2.54%	15.39
20s	1.45	1.21	0.95	1.05	1.45	1.83	3.20%	16.12
10s	1.09	1	0.8	0.88	1.13	1.38	4.77%	17.67
5s	0.93	0.89	0.73	0.79	0.97	1.13	8.64%	21.03
2s	0.85	0.84	0.68	0.74	0.91	1	16.65%	31.44
1s	0.84	0.82	0.67	0.71	0.89	0.97	26.74%	49.83



arthurgervais.github.io/Bitcoin-Simulator/results.html

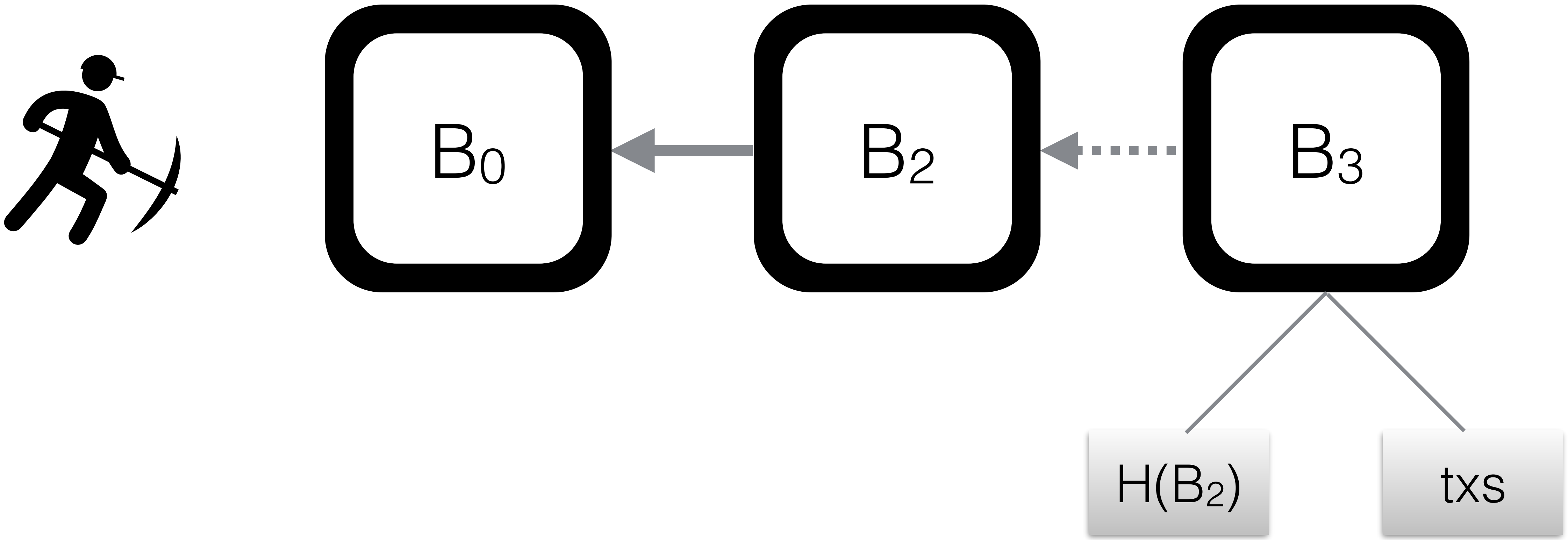
BITCOIN SIMULATOR

IMPACT OF NUMBER OF MINERS

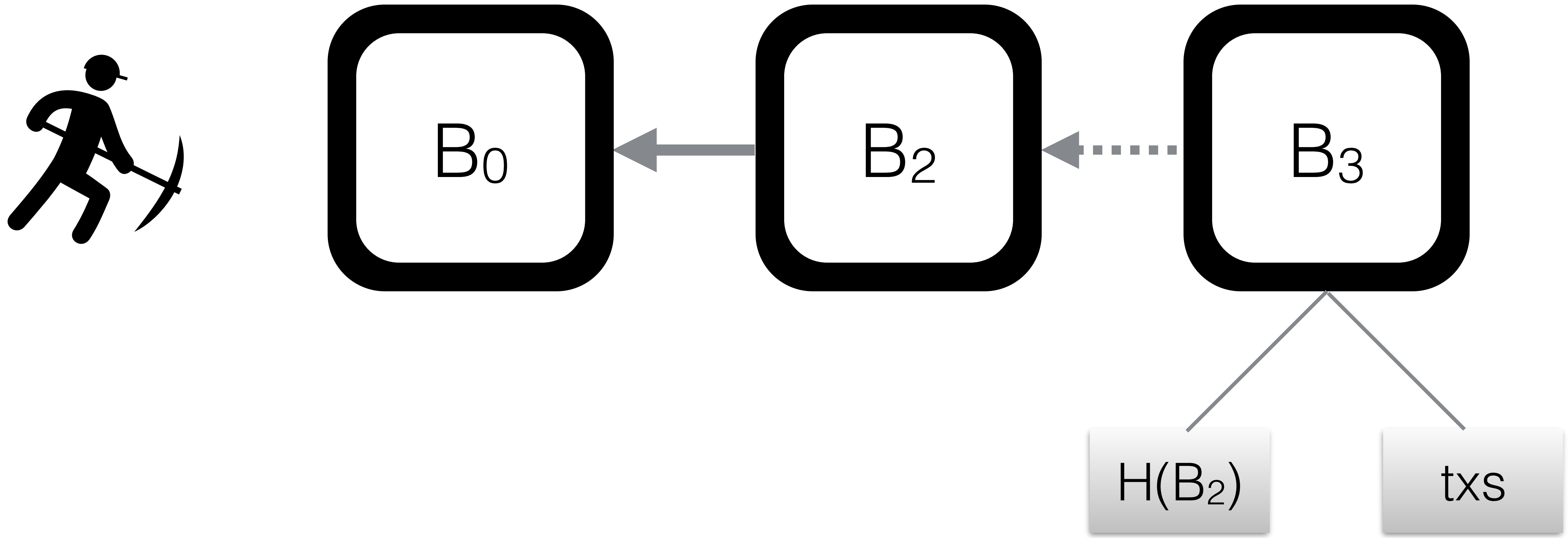
16 MINERS | 32 MINERS | 64 MINERS | 128 MINERS | 256 MINERS

Block Size (MB)	Block Interval	s_r	Throughput (tps)
0.25	30s	0.76	33.4
0.1	10s	1.76	40
0.25	20s	1.11	50
0.25	15s	1.45	66.7
0.5	30s	0.98	66.7
1	1mins	0.74	66.7

Proof of Work Blockchains



Proof of Work Blockchains



Mining

- Find Nonce N, s.t. $H(H(B_3)|txs|N) < target$