Comparing Quantitatively Layer 1 Security

How to Compare PoW Blockchains?

Bitcoin   Ethereum   Litecoin   Dogecoin

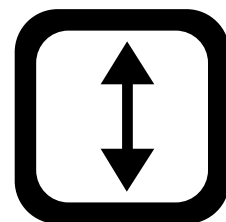# How to Compare PoW Blockchains?

Bitcoin   Ethereum   Litecoin   Dogecoin

- 2 parameters

  ▷ Block generation ⏳

  ▷ Block size

How to Compare PoW Blockchains?

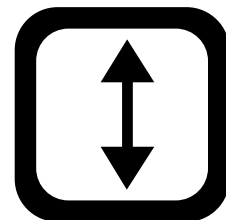| Bitcoin	Ethereum	Litecoin	Dogecoin
10 min	**15 sec**	**2.5 min**	**1 min**

- 2 parameters

  ▷ Block generation

  ▷ Block size

How to Compare PoW Blockchains?

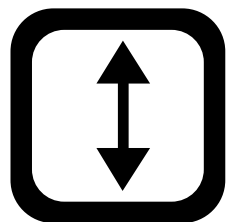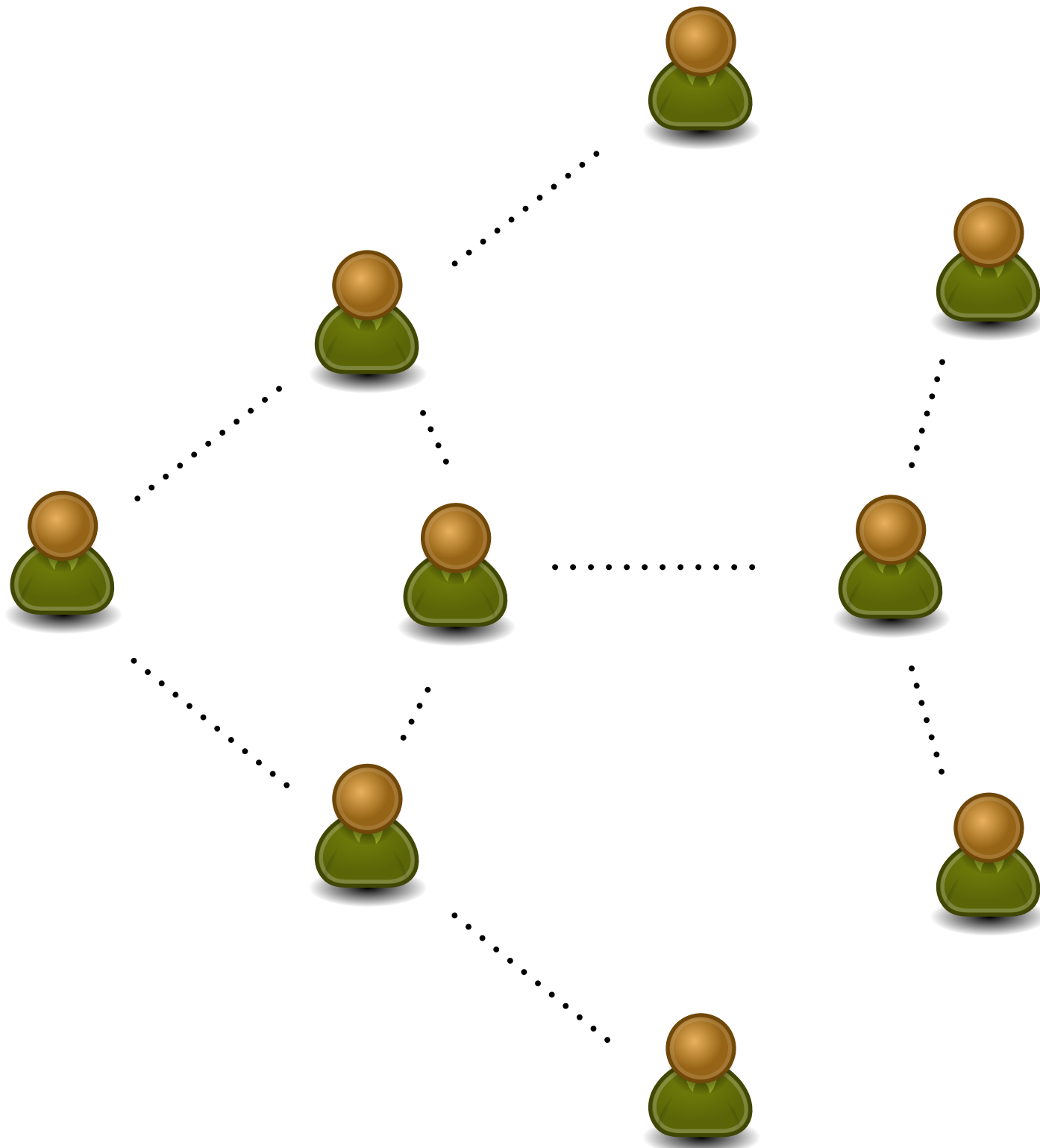| Bitcoin	Ethereum	Litecoin	Dogecoin
10 min	**15 sec**	**2.5 min**	**1 min**

- 2 parameters

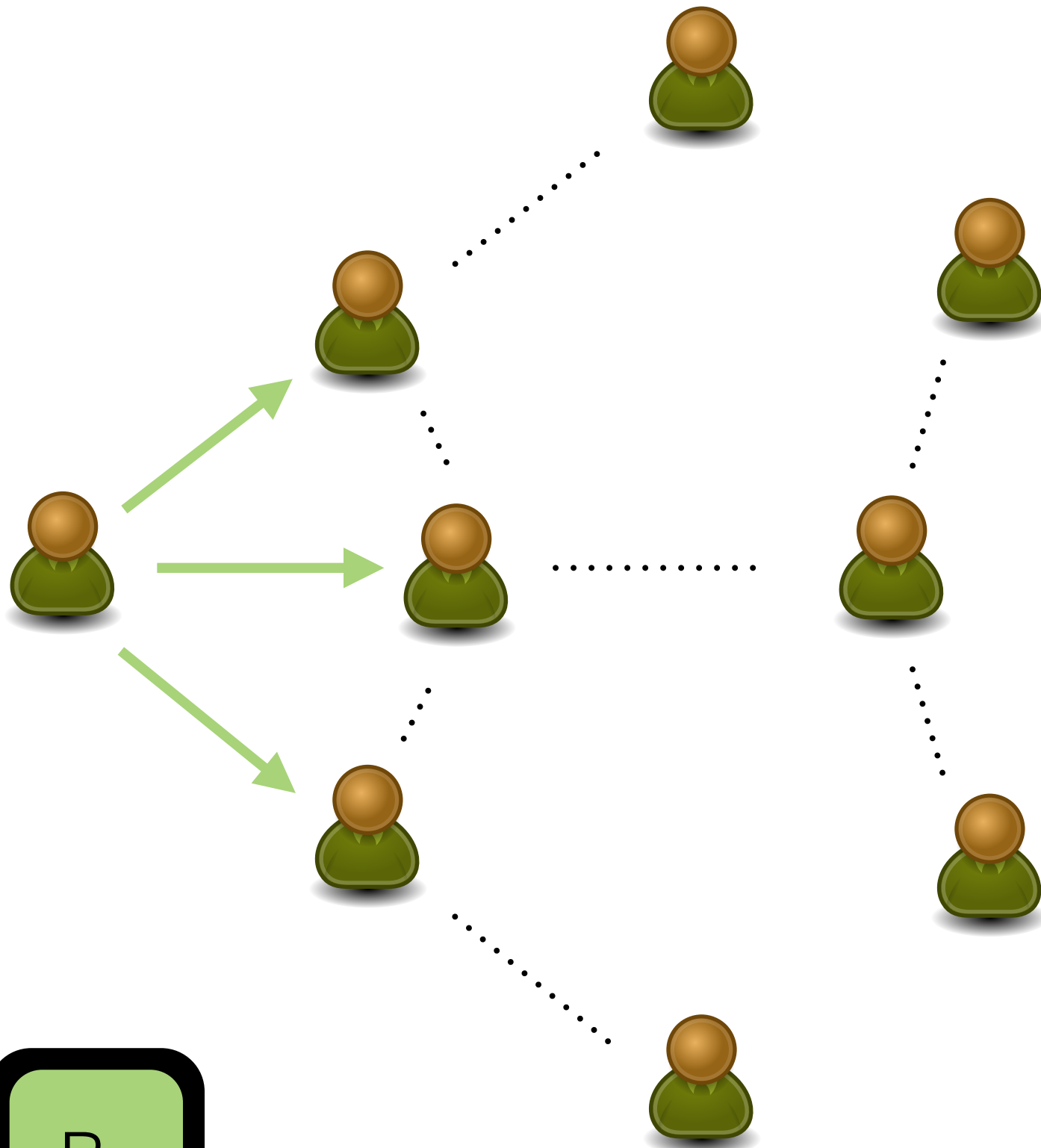⧗ Faster block generation ➡ Faster payments

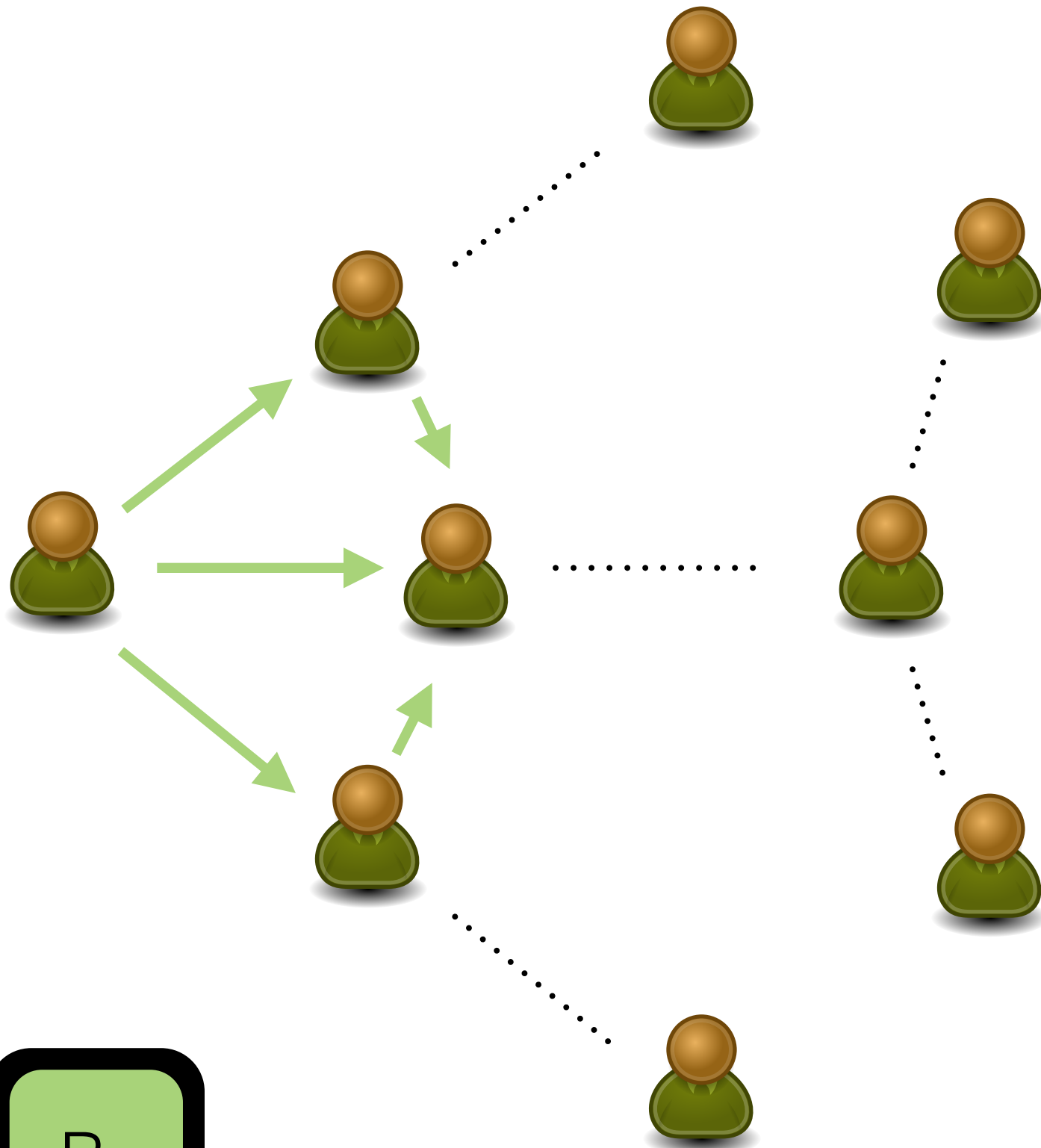⇕ Bigger block size ➡ More throughput/ Slower propagation

Mining and Forks

Mining and Forks

B₁
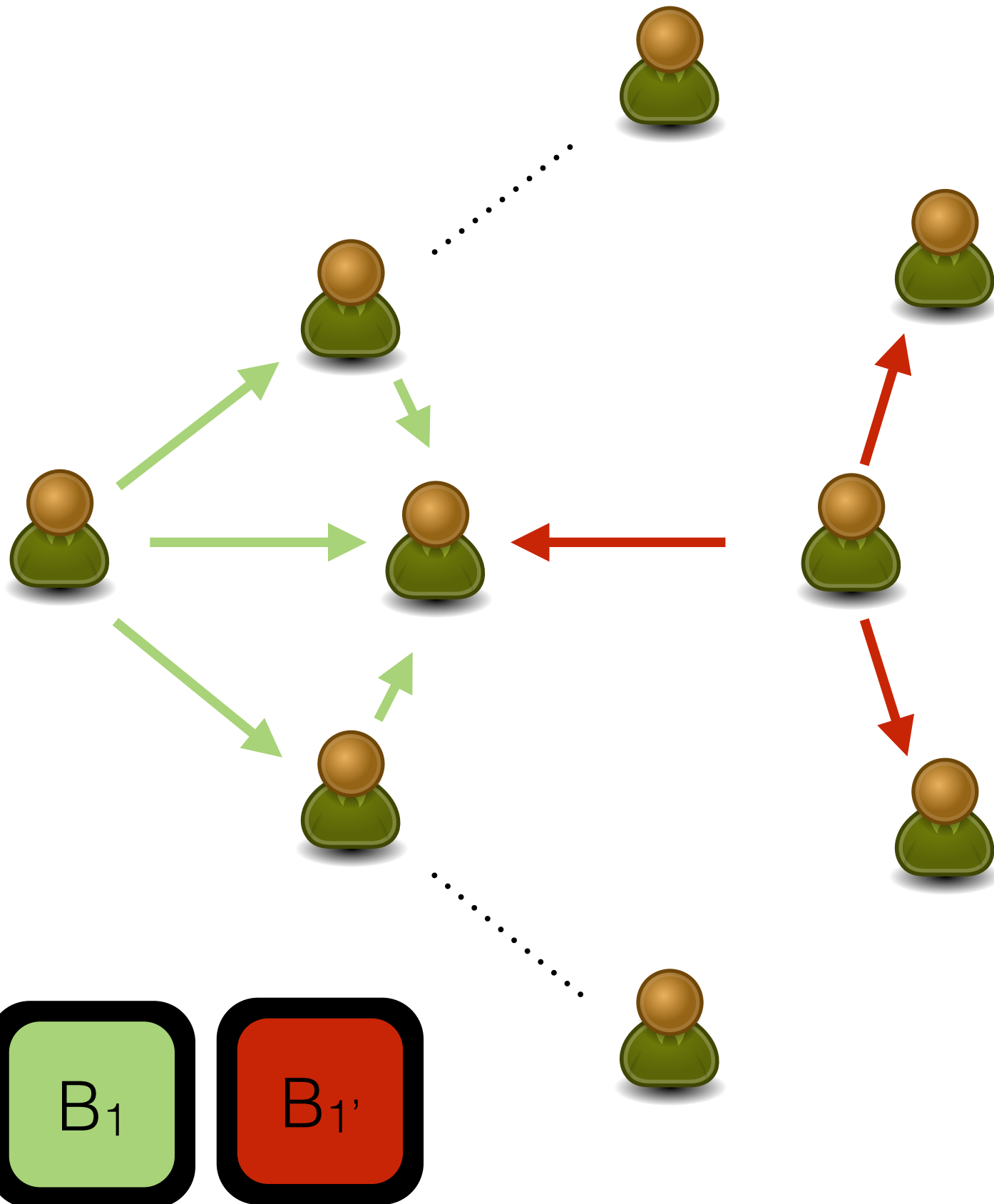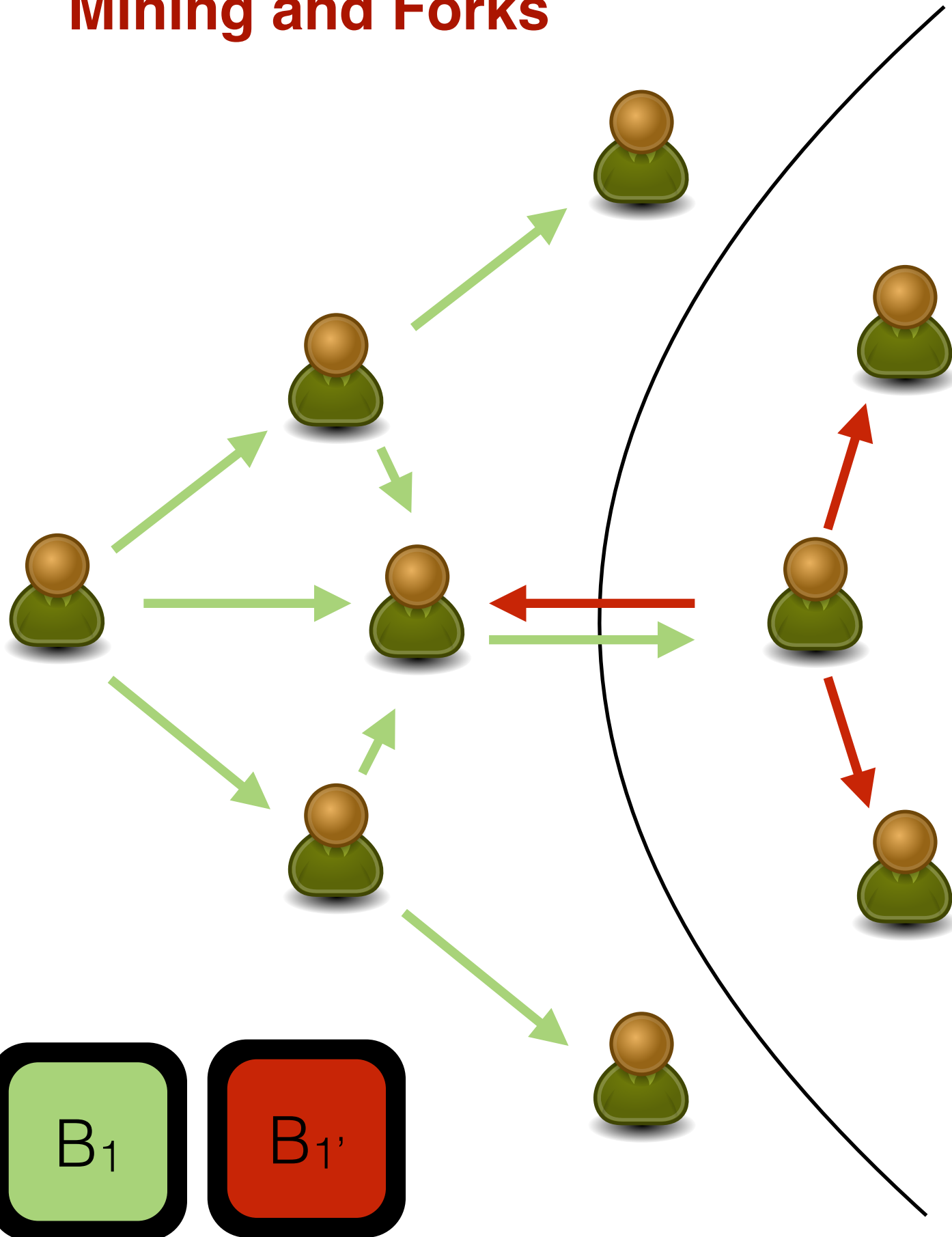
Mining and Forks

B₁

3

Mining and Forks

B₁ B₁'

Mining and Forks

B₁ B₁'

Mining and Forks

B₁ B₁'

Mining and Forks

Stale blocks = lost efforts

B_1 $B_{1'}$

3

Mining and Forks

Stale blocks = lost efforts

B_1 B_1'
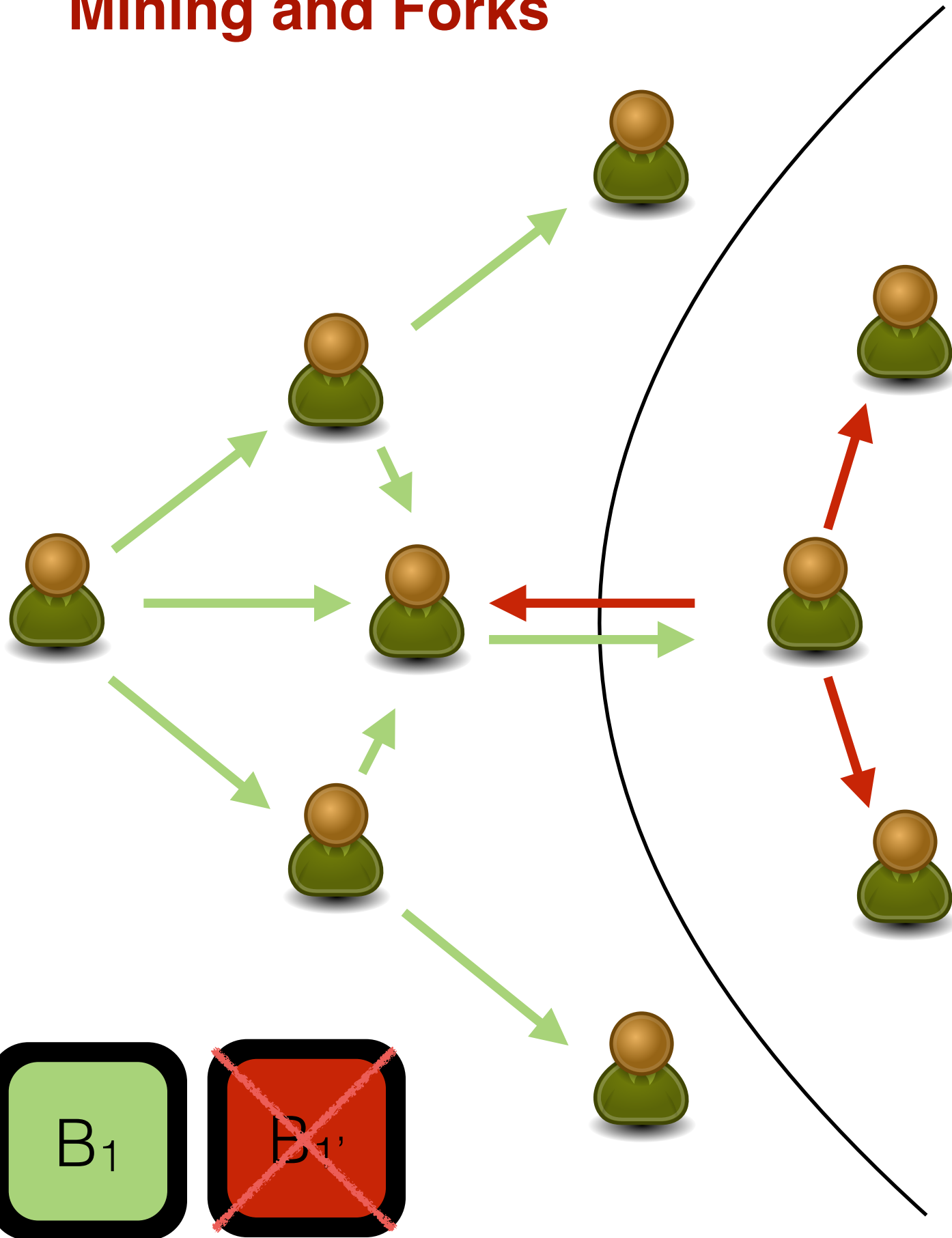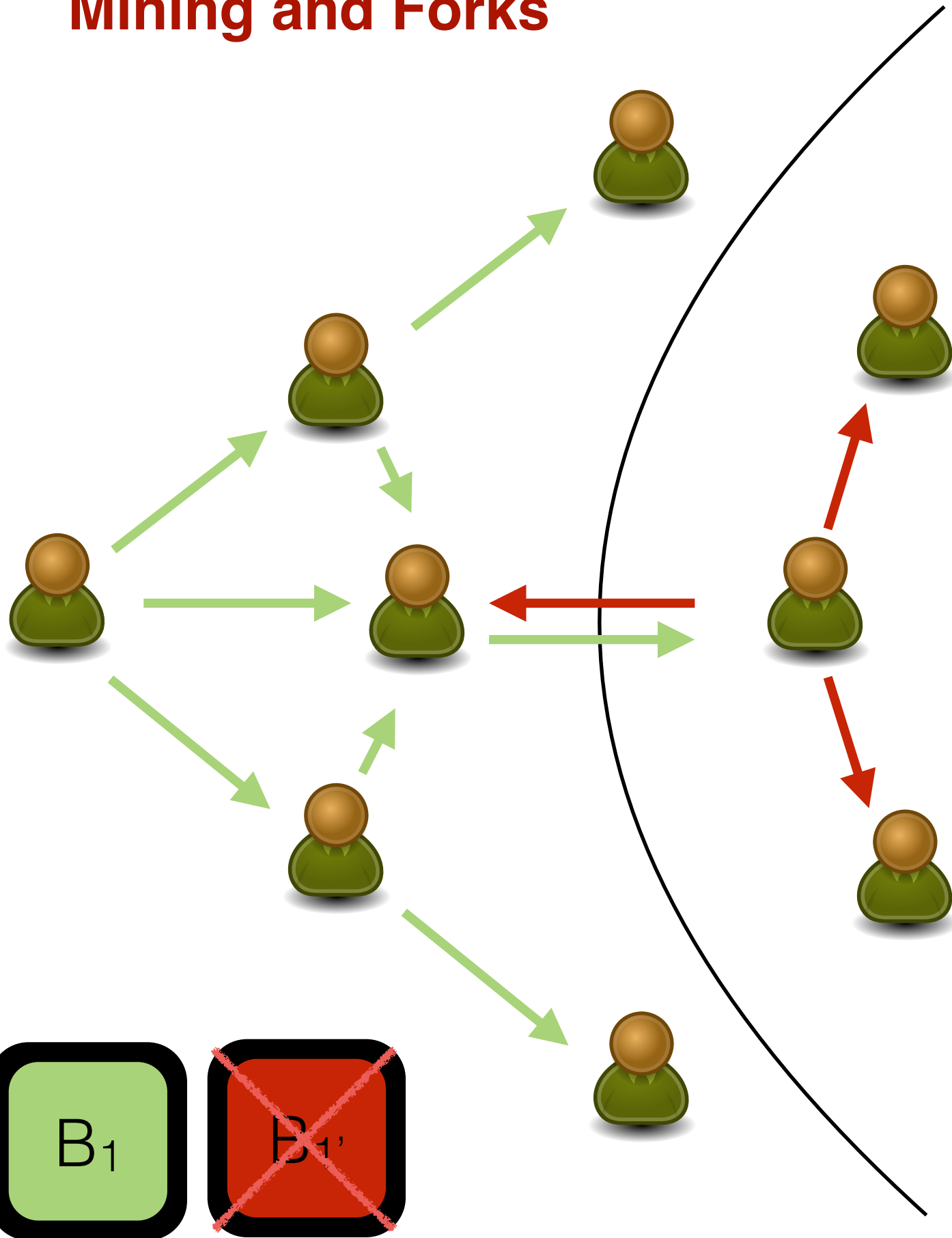
Mining and Forks
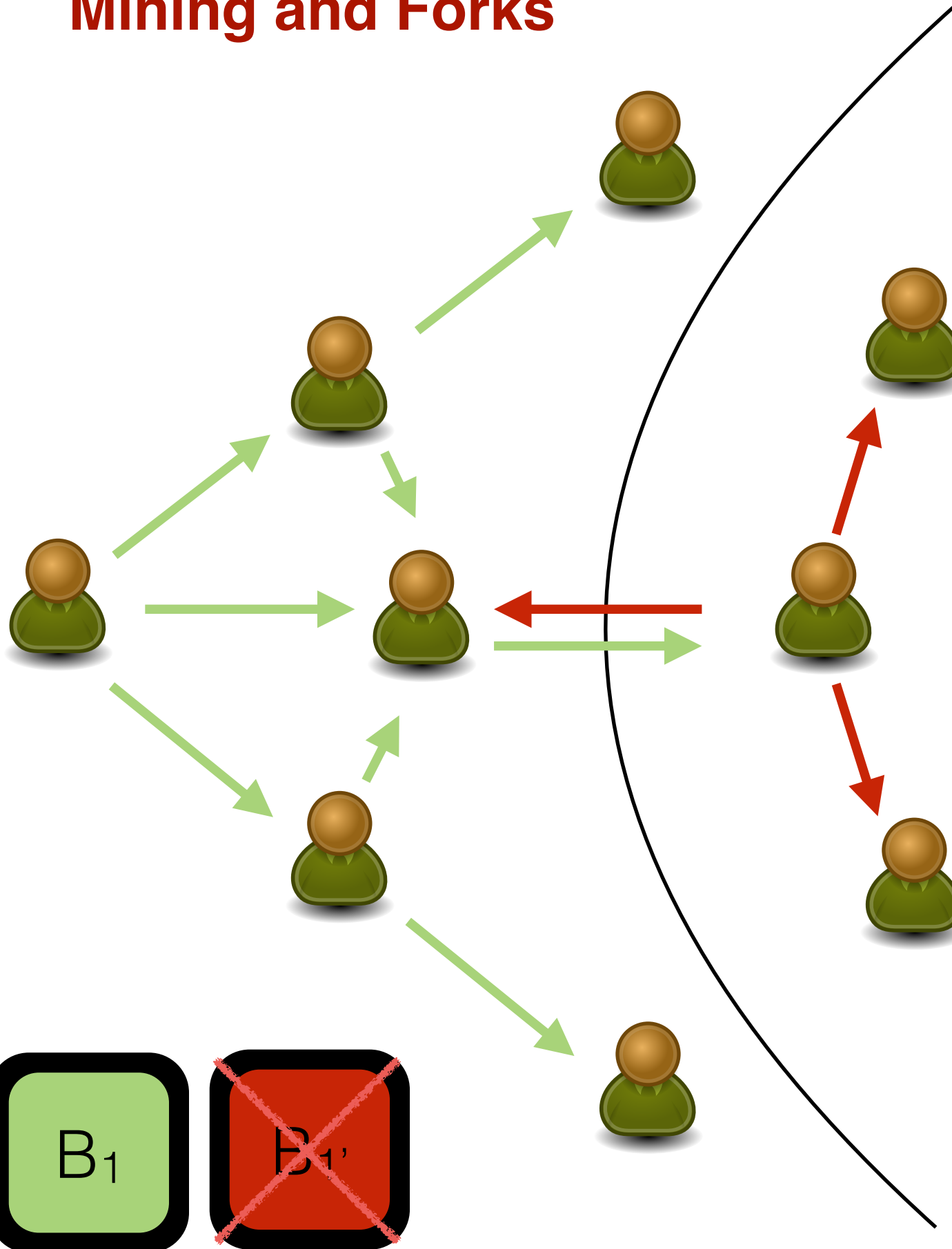
Stale blocks = lost efforts

Stale Block rates

Bitcoin	Litecoin
0.4%	0.3%

Dogecoin	Ethereum
0.6%	6.8%

B_1 $B_{1'}$

Security vs. Scalability in Blockchains

Block generation

Block size

Croman et al., FC'16
Sapirshtein et al., FC'16
Sompolinsky et al., FC'15
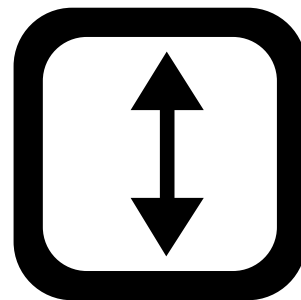Garay et al., Eurocrypt '15

Security vs. Scalability in Blockchains
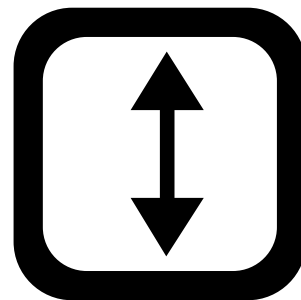
Block generation

Block size → Bigger →

Croman et al., FC'16
Sapirshtein et al., FC'16
Sompolinsky et al., FC'15
Garay et al., Eurocrypt '15

Security vs. Scalability in Blockchains

Block generation

Block size

Bigger

Slower propagation

less security

Croman et al., FC'16
Sapirshtein et al., FC'16
Sompolinsky et al., FC'15
Garay et al., Eurocrypt '15
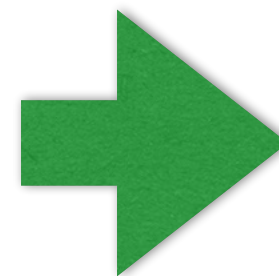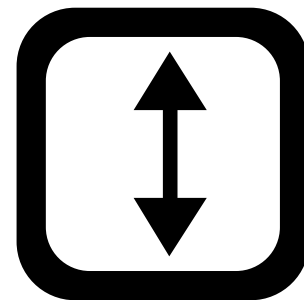
Security vs. Scalability in Blockchains

Block generation — Faster → Faster payments

Block size — Bigger → Slower propagation

→ **less security**

Croman et al., FC'16
Sapirshtein et al., FC'16
Sompolinsky et al., FC'15
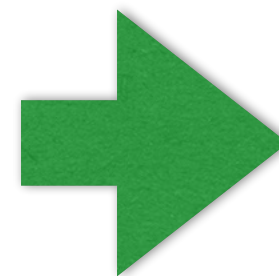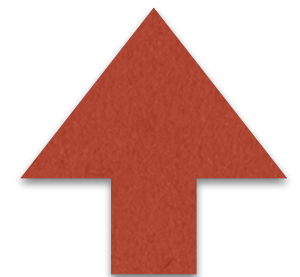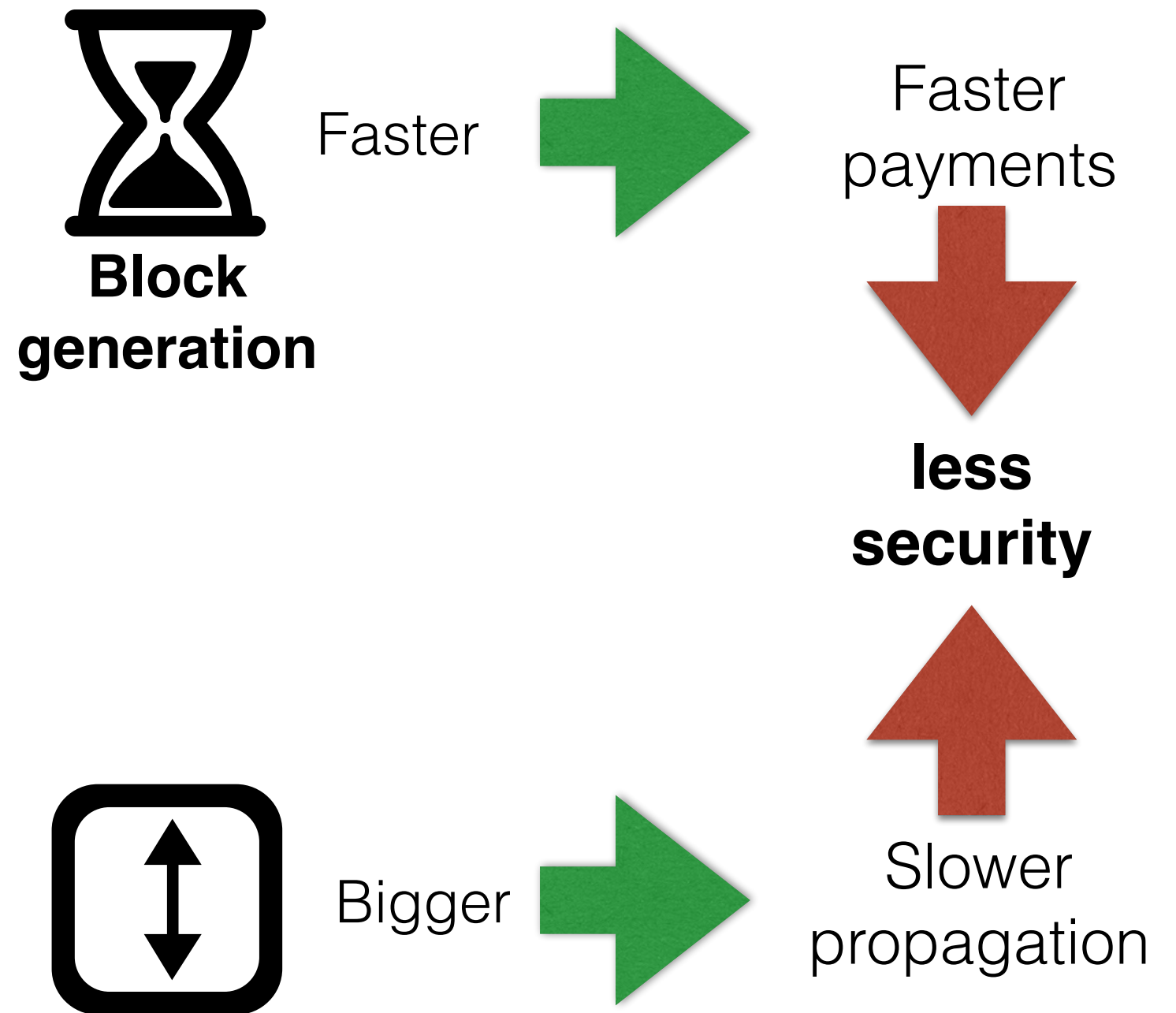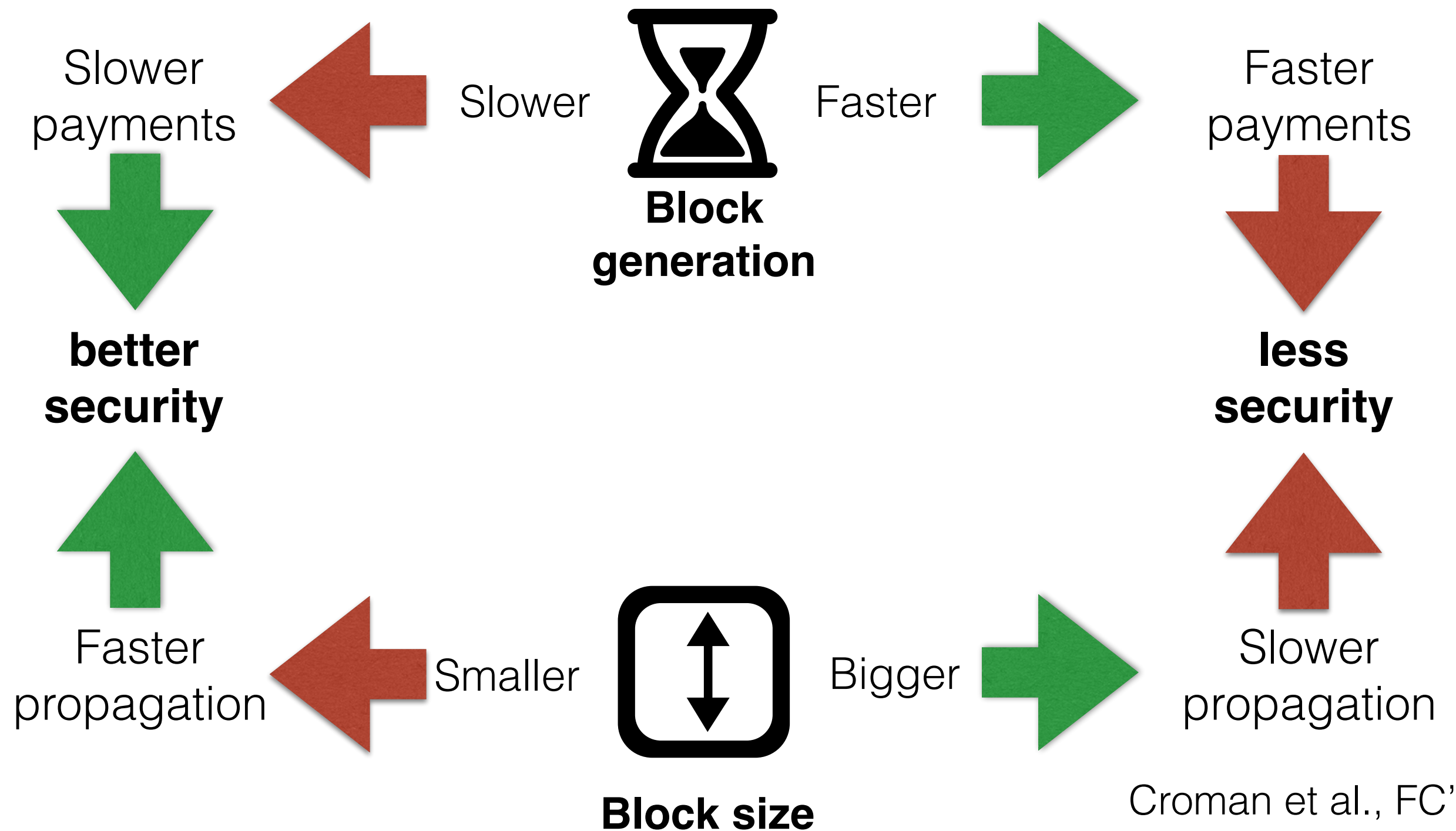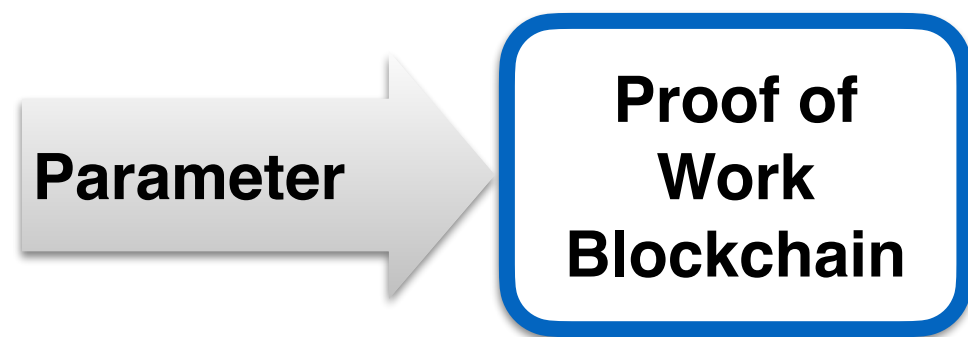Garay et al., Eurocrypt '15

Security vs. Scalability in Blockchains

Slower payments

better security

Slower ← Block generation → Faster

Faster payments

less security

Faster propagation

Smaller ← Block size → Bigger

Slower propagation
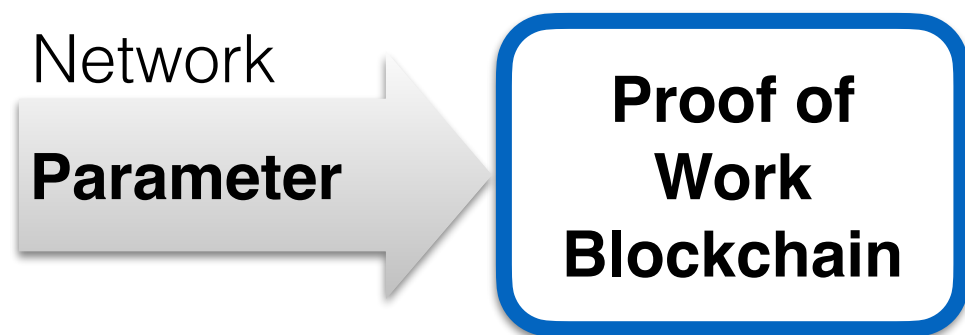
Croman et al., FC'16
Sapirshtein et al., FC'16
Sompolinsky et al., FC'15
Garay et al., Eurocrypt '15

Comparing PoW Blockchain Security

Parameter → **Proof of Work Blockchain**

Comparing PoW Blockchain Security

Network

Parameter

Proof of Work Blockchain

Comparing PoW Blockchain Security

Network

Parameter

Consensus

Proof of Work Blockchain

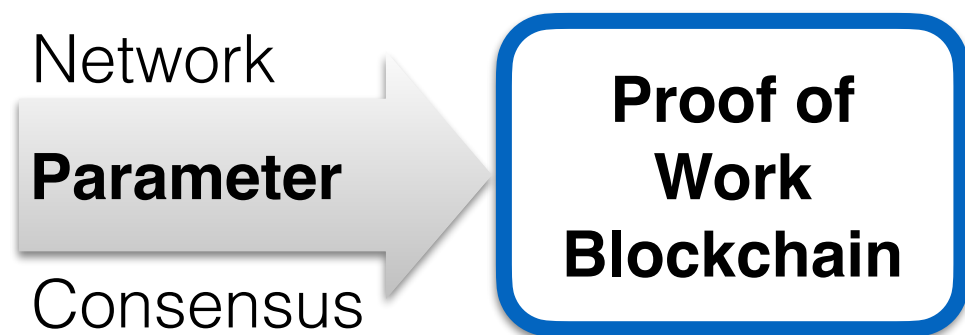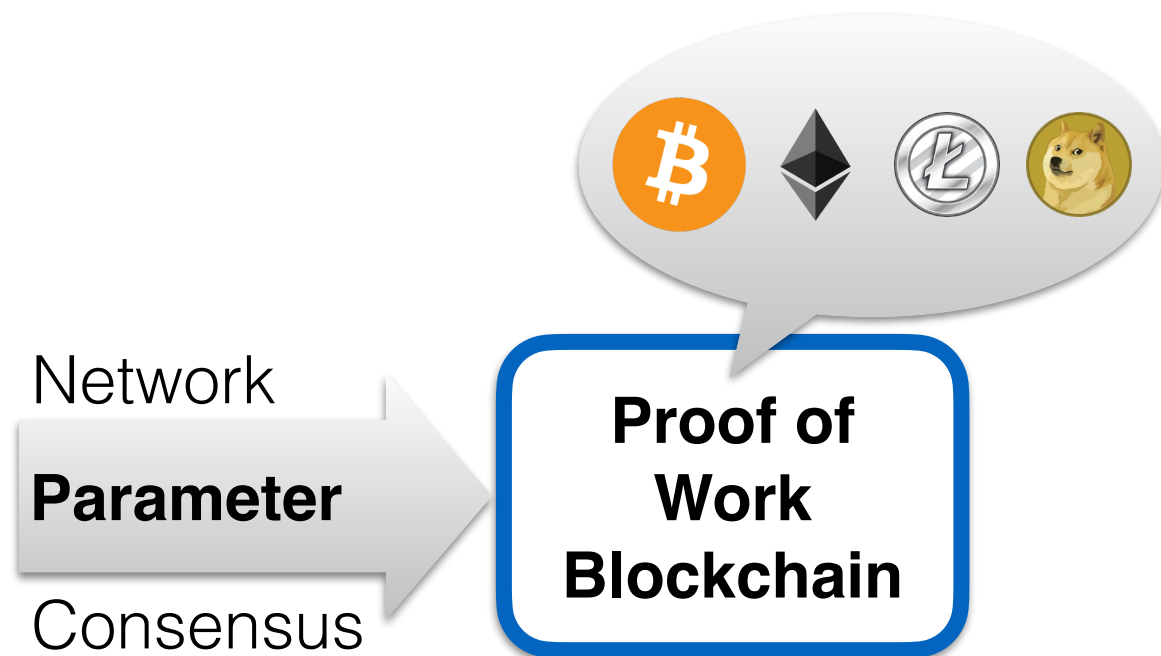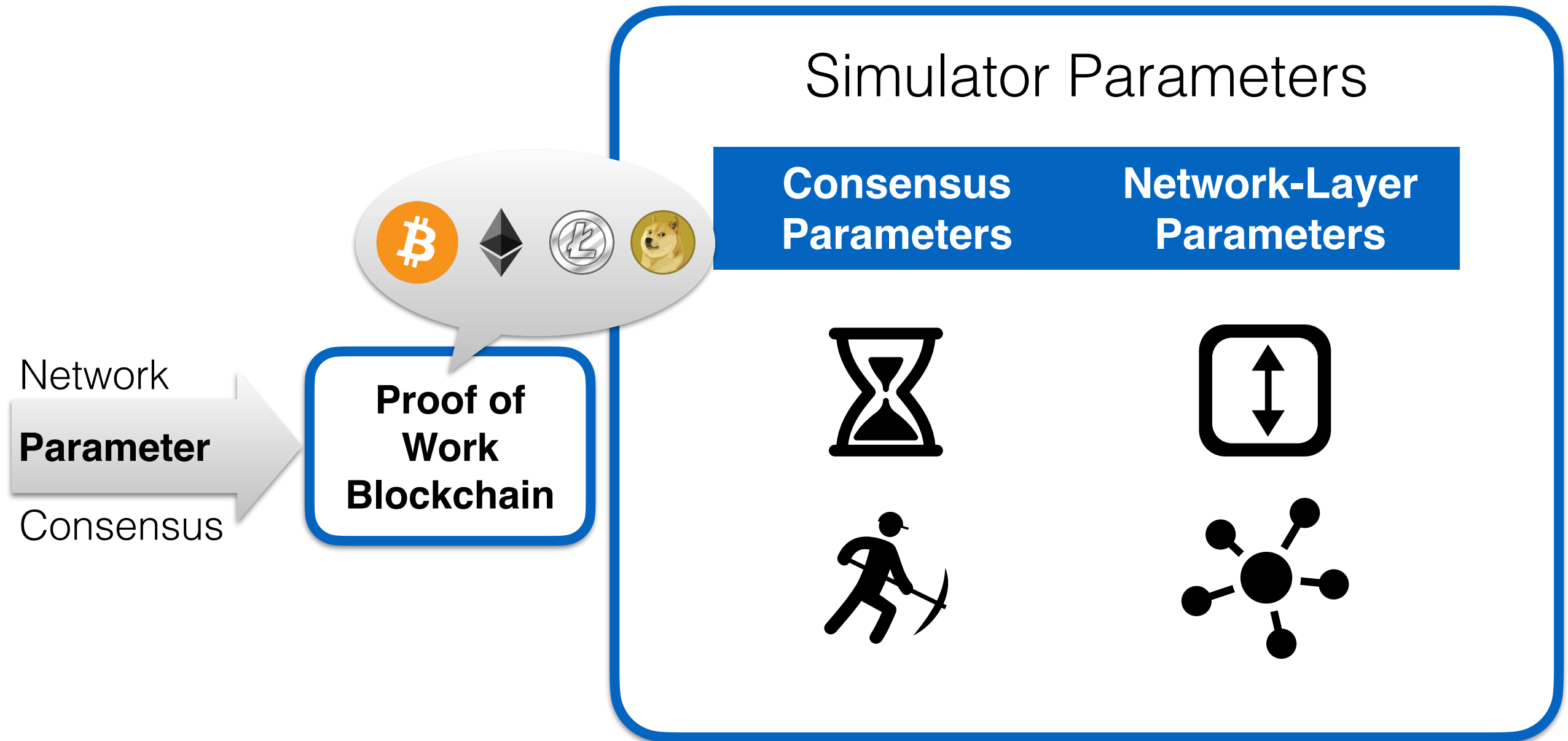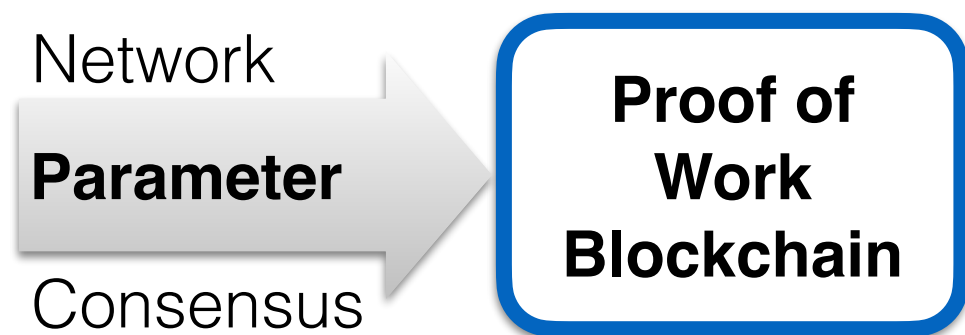# Comparing PoW Blockchain Security

Network

Parameter

Consensus

Proof of Work Blockchain

Comparing PoW Blockchain Security

Comparing PoW Blockchain Security

Network

Parameter

Consensus

Proof of Work Blockchain

Comparing PoW Blockchain Security

Network

Parameter

Consensus

Proof of Work Blockchain

Stale Block Rate

Comparing PoW Blockchain Security

Network

Parameter

Consensus

Proof of Work Blockchain

Stale Block Rate

Markov Decision Process

Comparing PoW Blockchain Security

Attacks

Network **Parameter** Consensus

Proof of Work Blockchain

Stale Block Rate
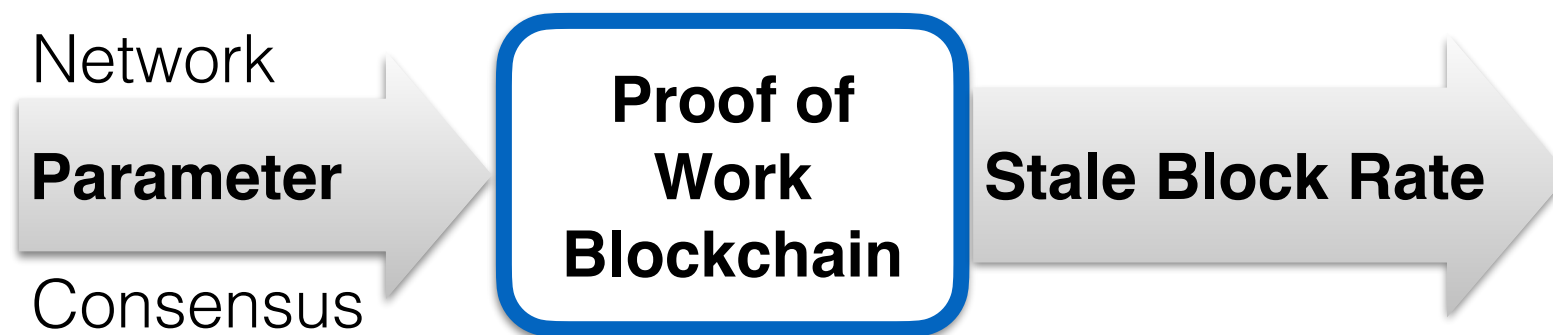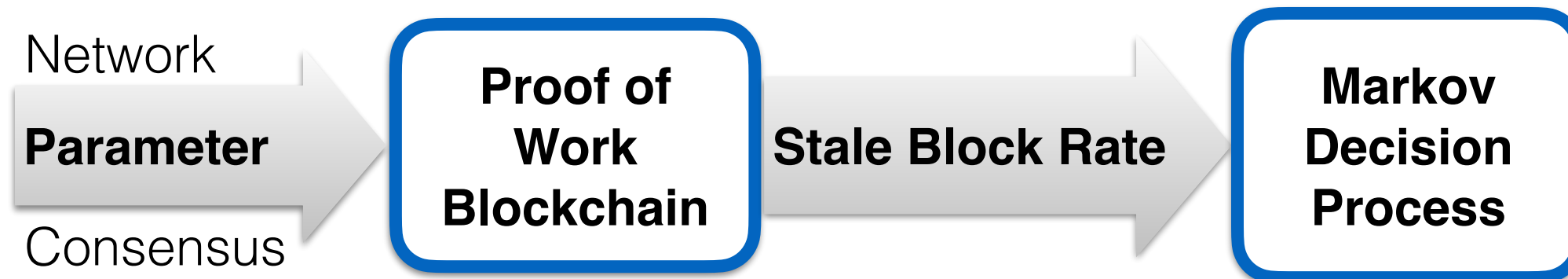
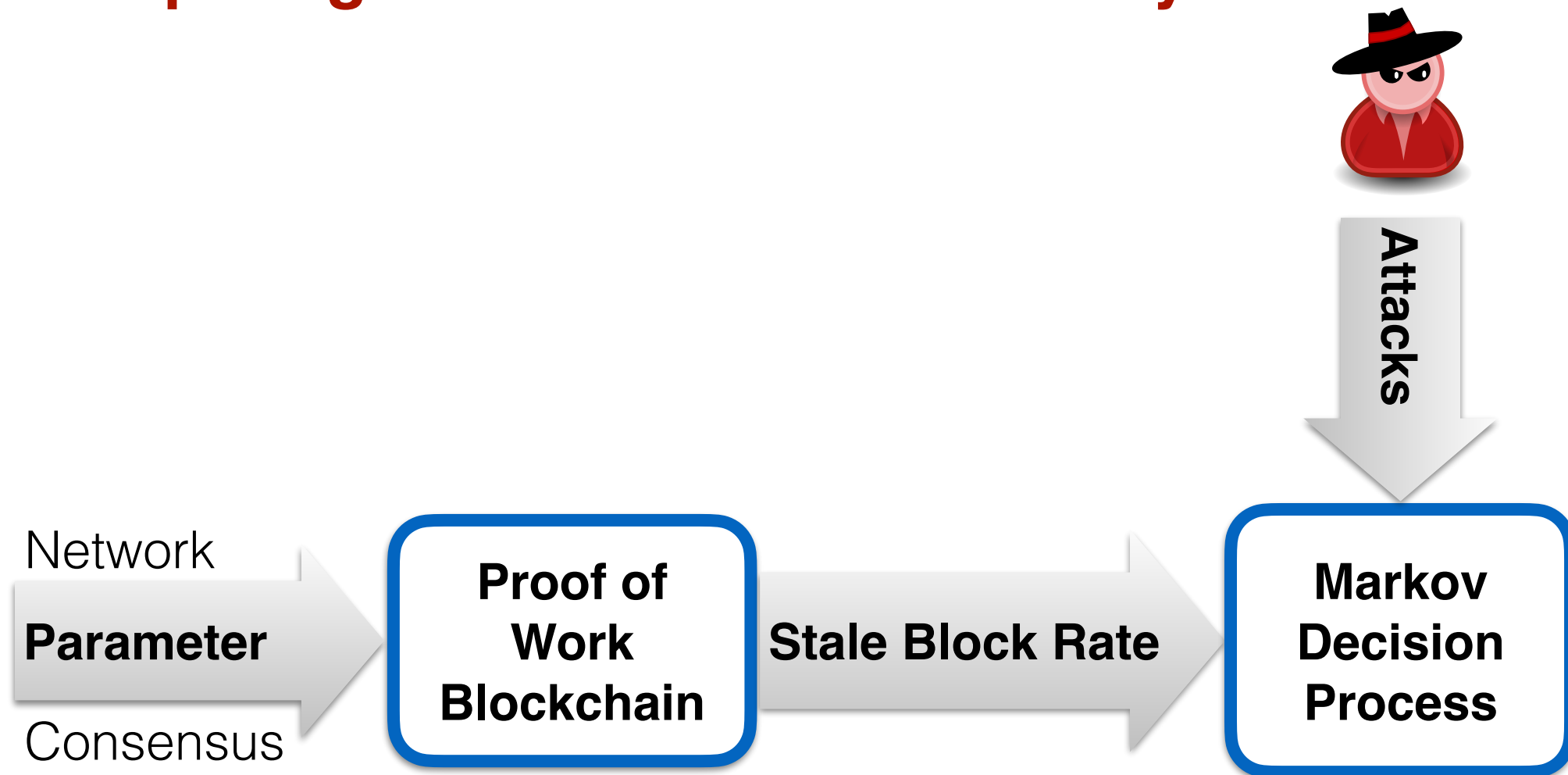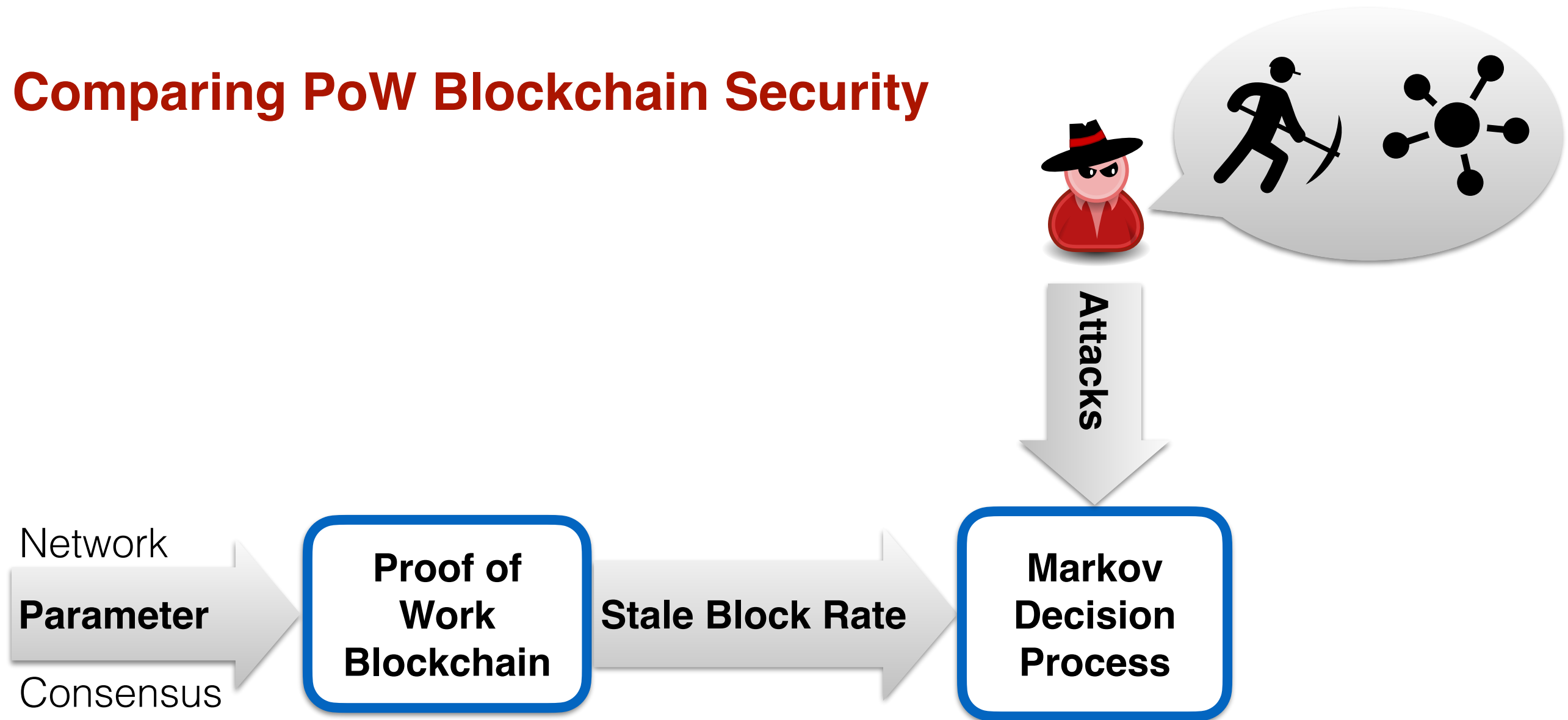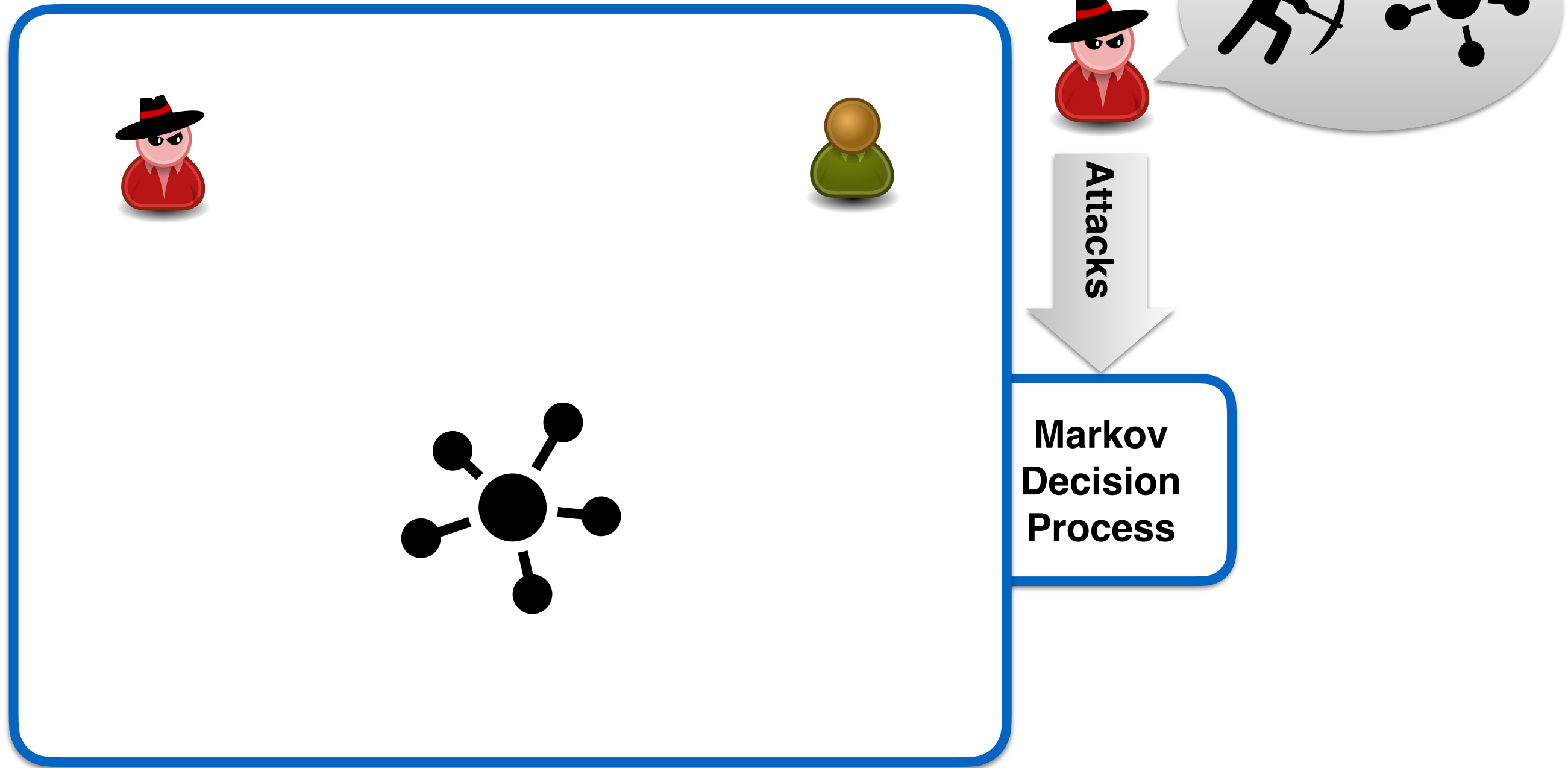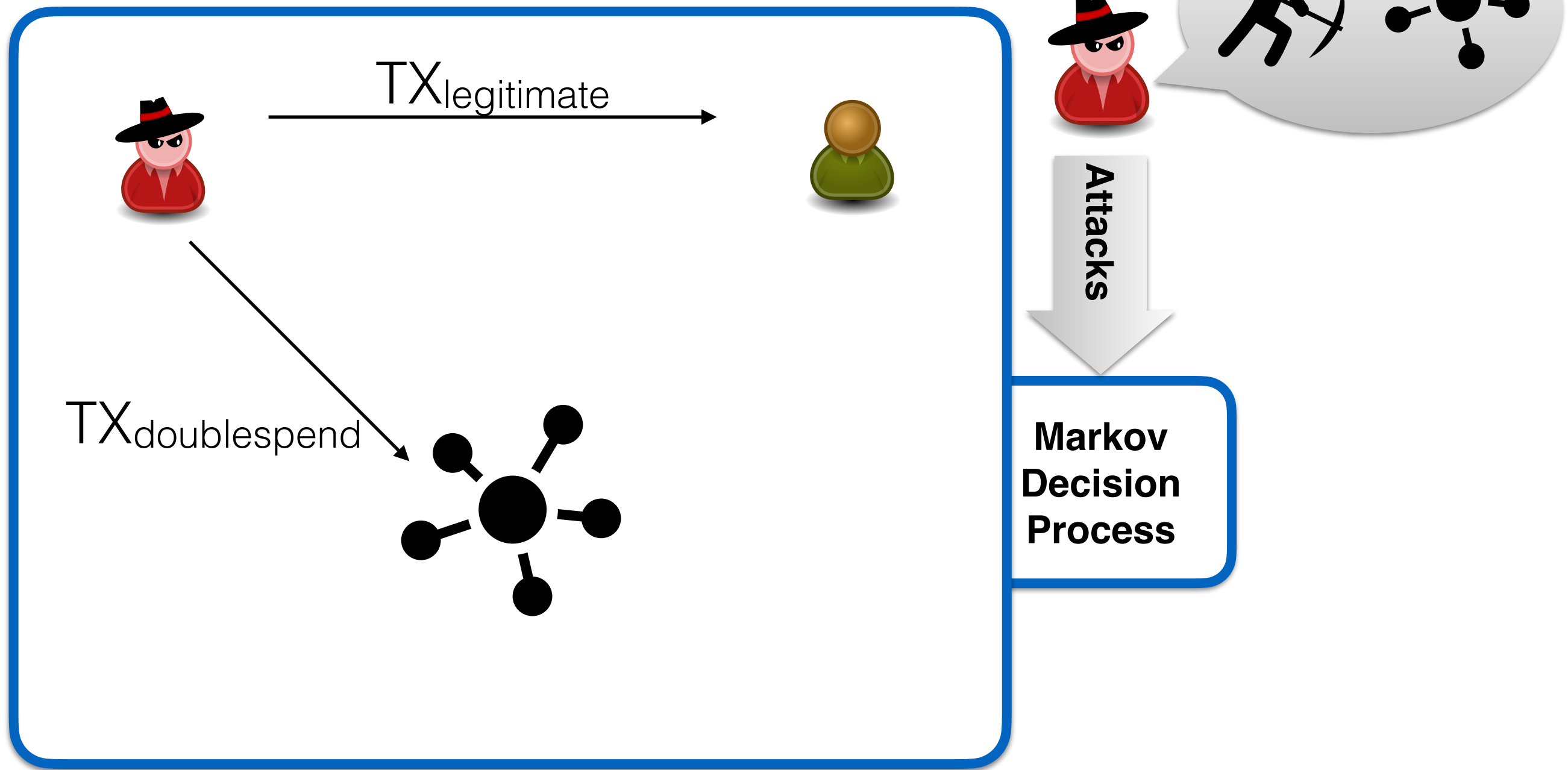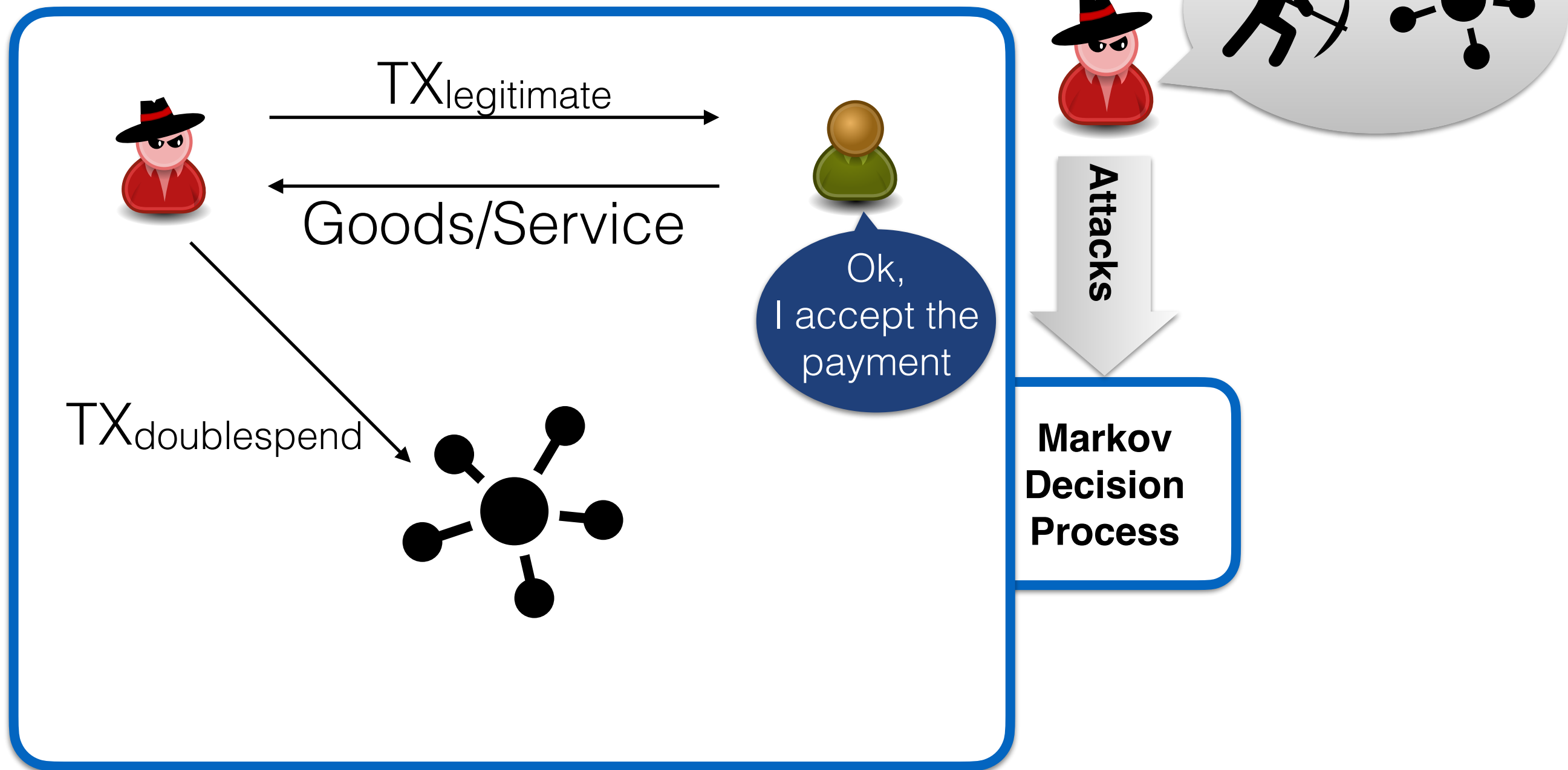**Markov Decision Process**

Comparing PoW Blockchain Security

Comparing PoW Blockchain Security

Comparing PoW Blockchain Security

TX$_{legitimate}$

TX$_{doublespend}$

Attacks

Markov Decision Process

Comparing PoW Blockchain Security

Comparing PoW Blockchain Security

TX$_{legitimate}$

Goods/Service

TX$_{doublespend}$

TX$_{legitimate}$

Ok, I accept the payment

Attacks

Markov Decision Process

Comparing PoW Blockchain Security

TX~legitimate~

Goods/Service

TX~doublespend~   TX~legitimate~

Ok, I accept the payment

Majority accepts TX~doublespend~

Attacks

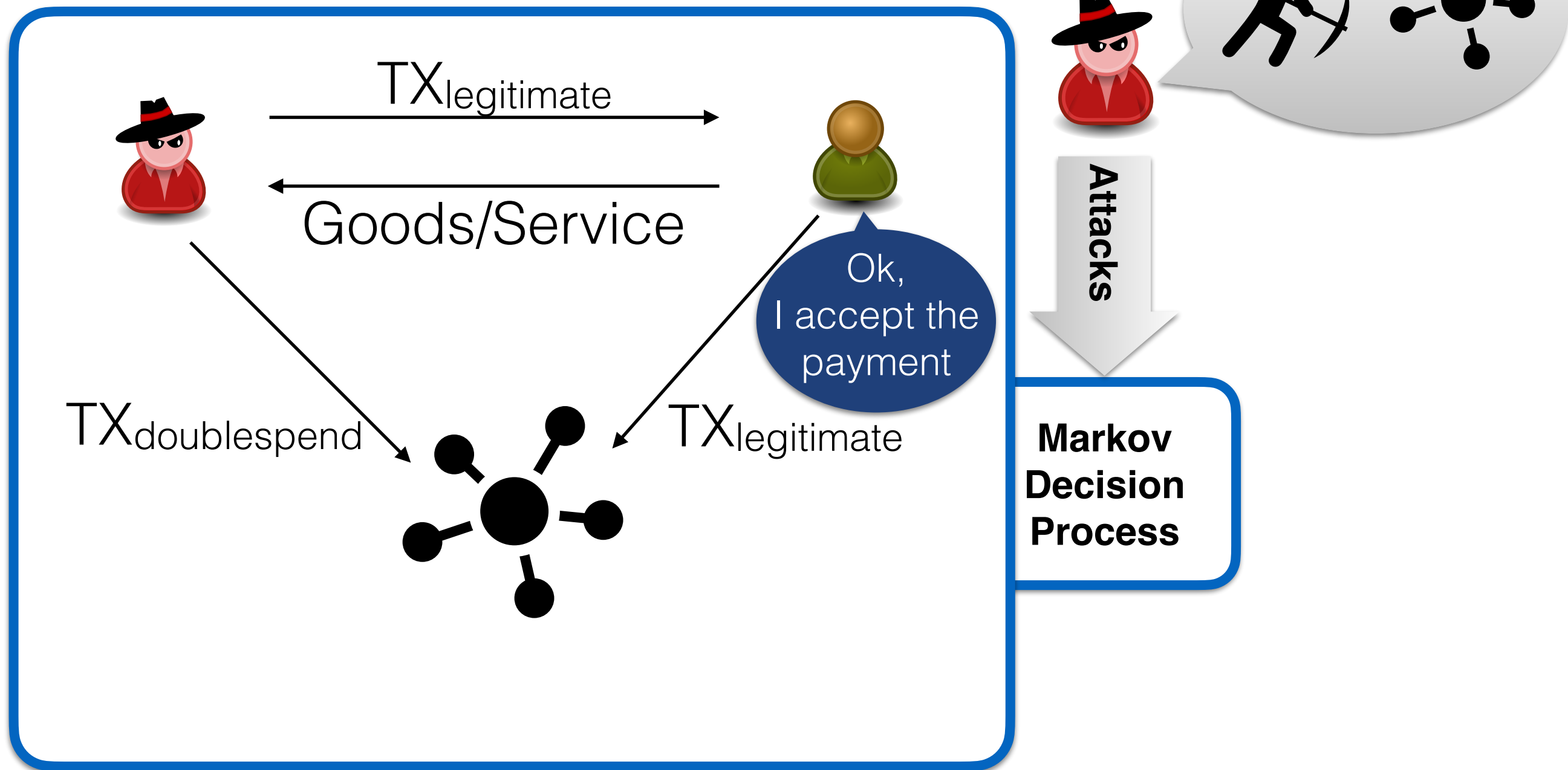**Markov Decision Process**
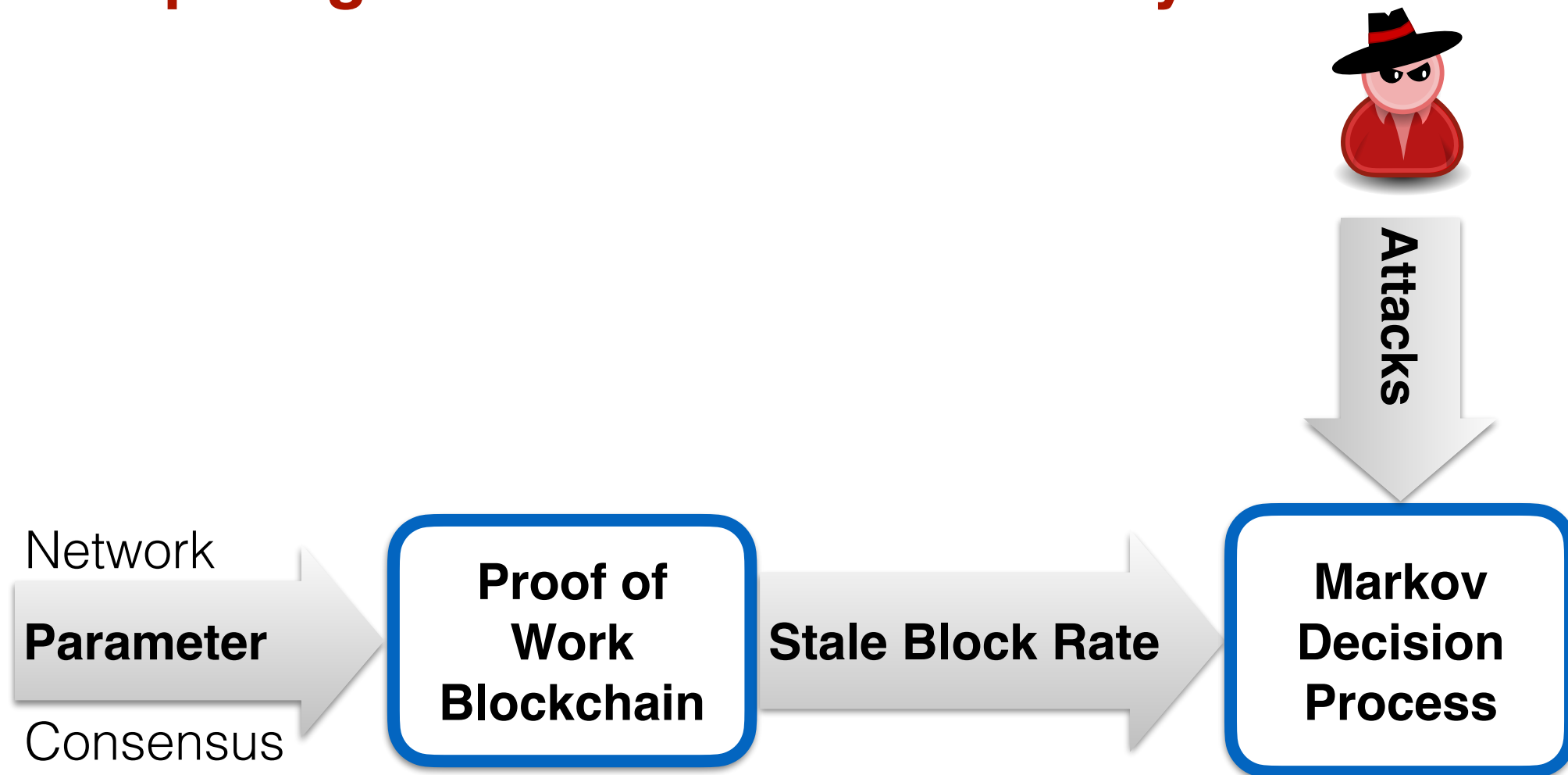
Comparing PoW Blockchain Security

Comparing PoW Blockchain Security

Comparing PoW Blockchain Security