Incentive Analysis of Bitcoin-NG, Revisited

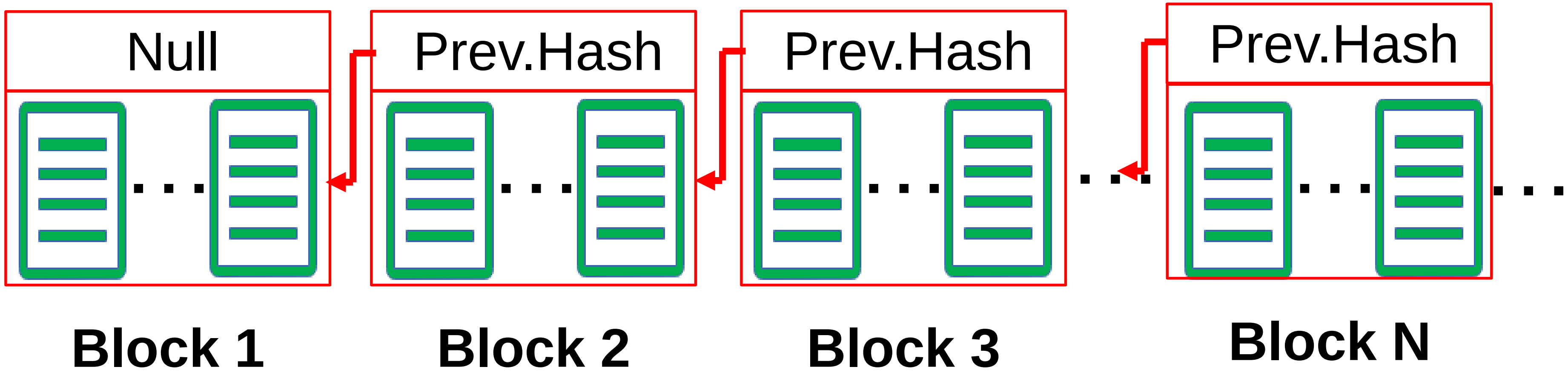
Jianyu Niu, Ziyu Wang*, Fangyu Gai, and Chen Feng

School of Engineering, University of British Columbia (Okanagan Campus)

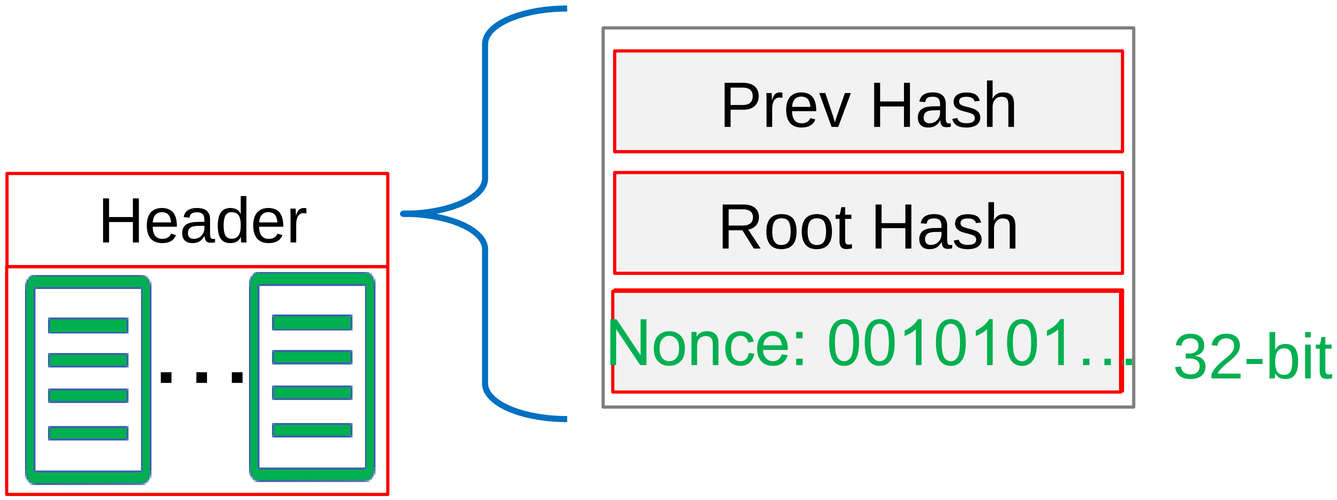
*School of Cyber Science and Technology, Beihang University

Blockchain

In 2008, Nakamoto invented blockchain and Bitcoin

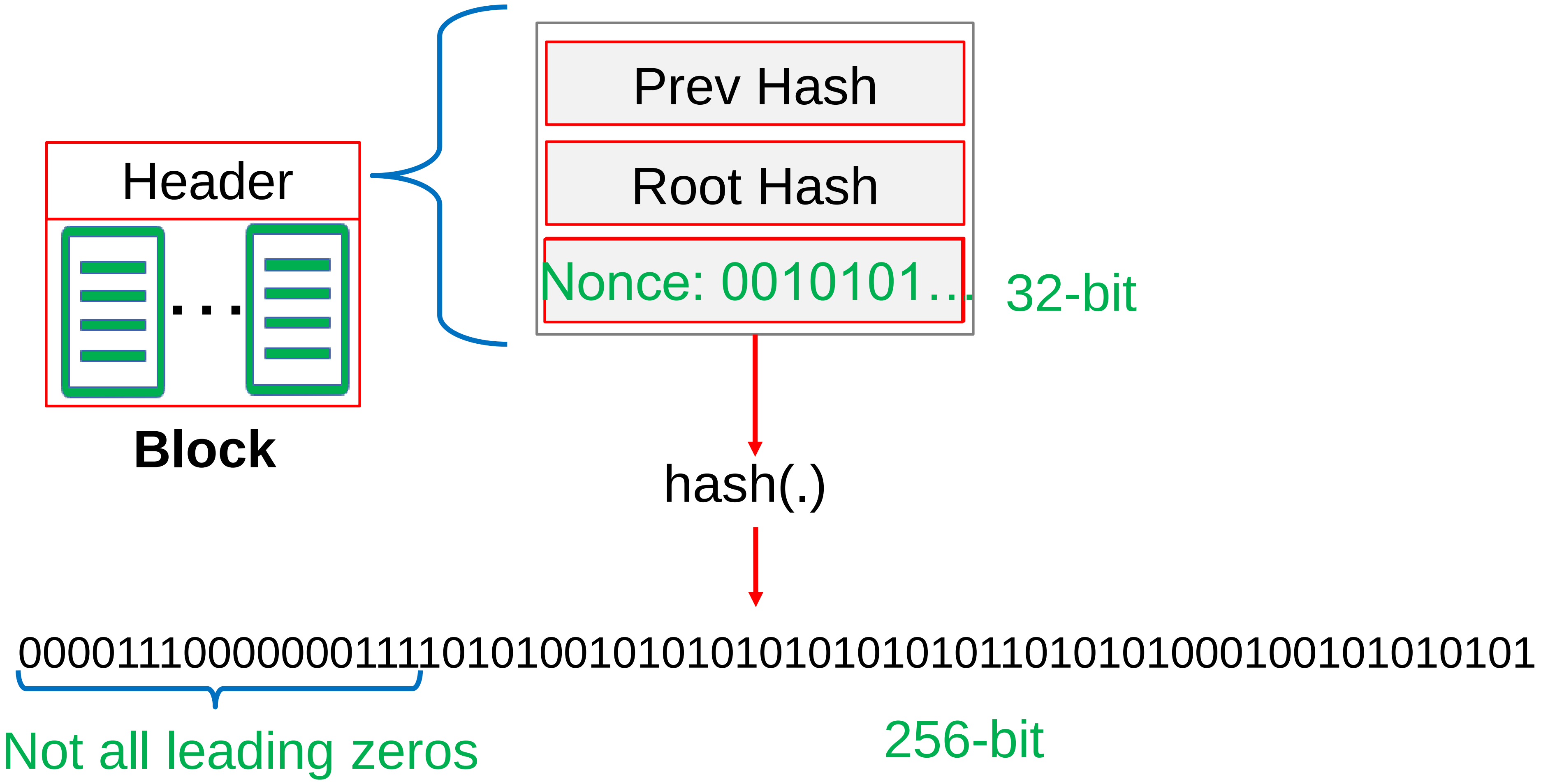


Proof-of-Work

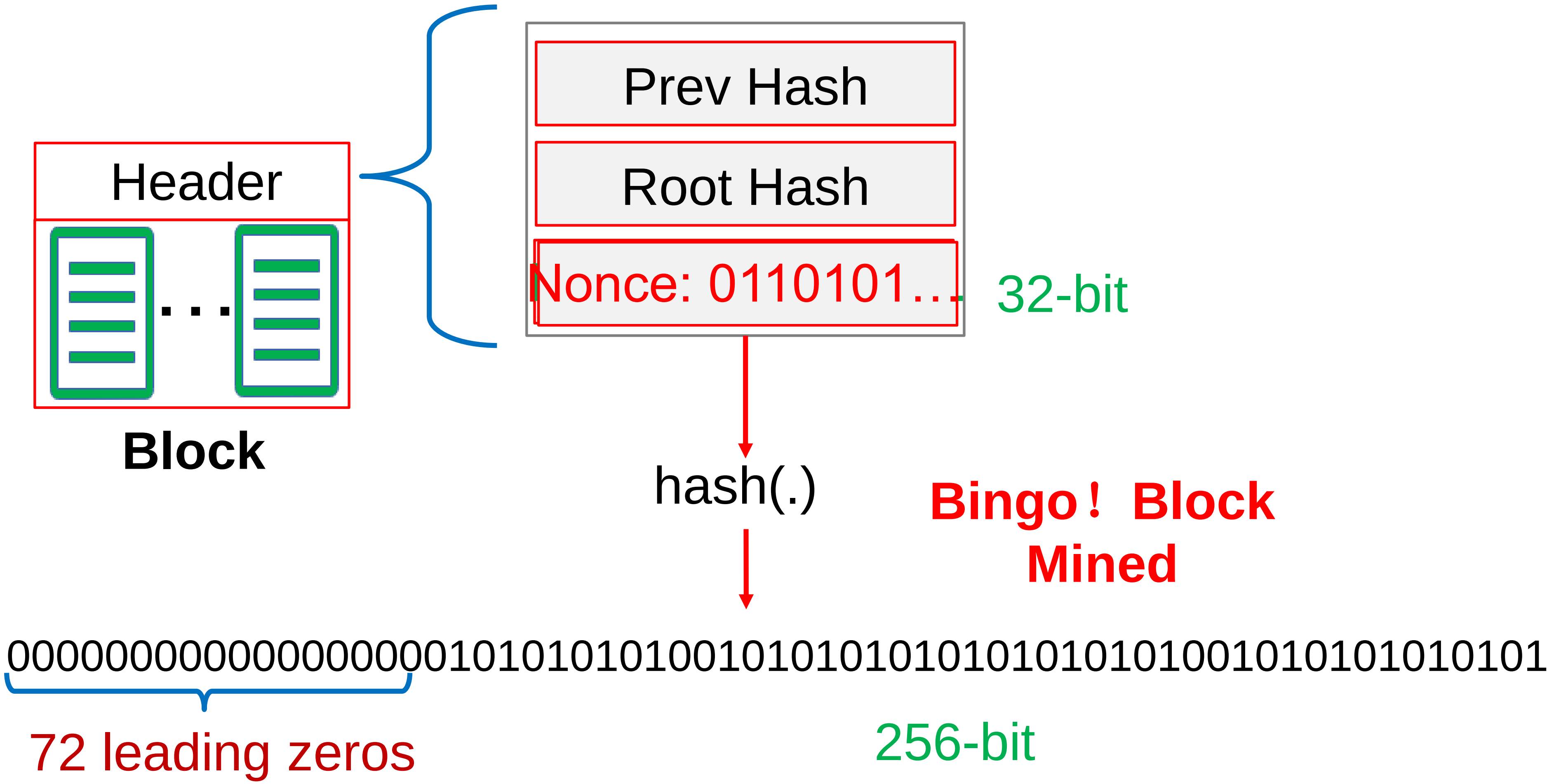


Block

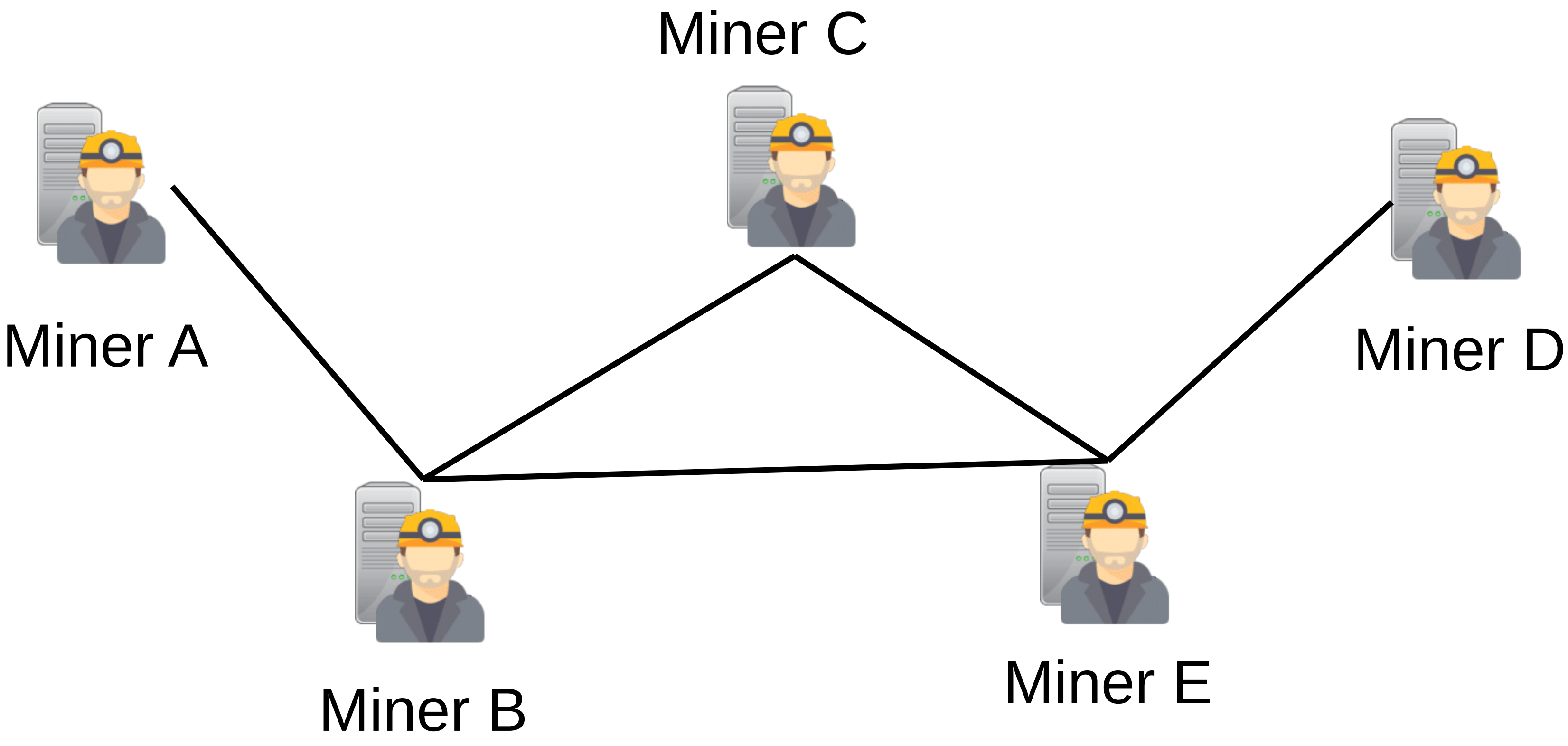
Proof-of-Work



Proof-of-Work

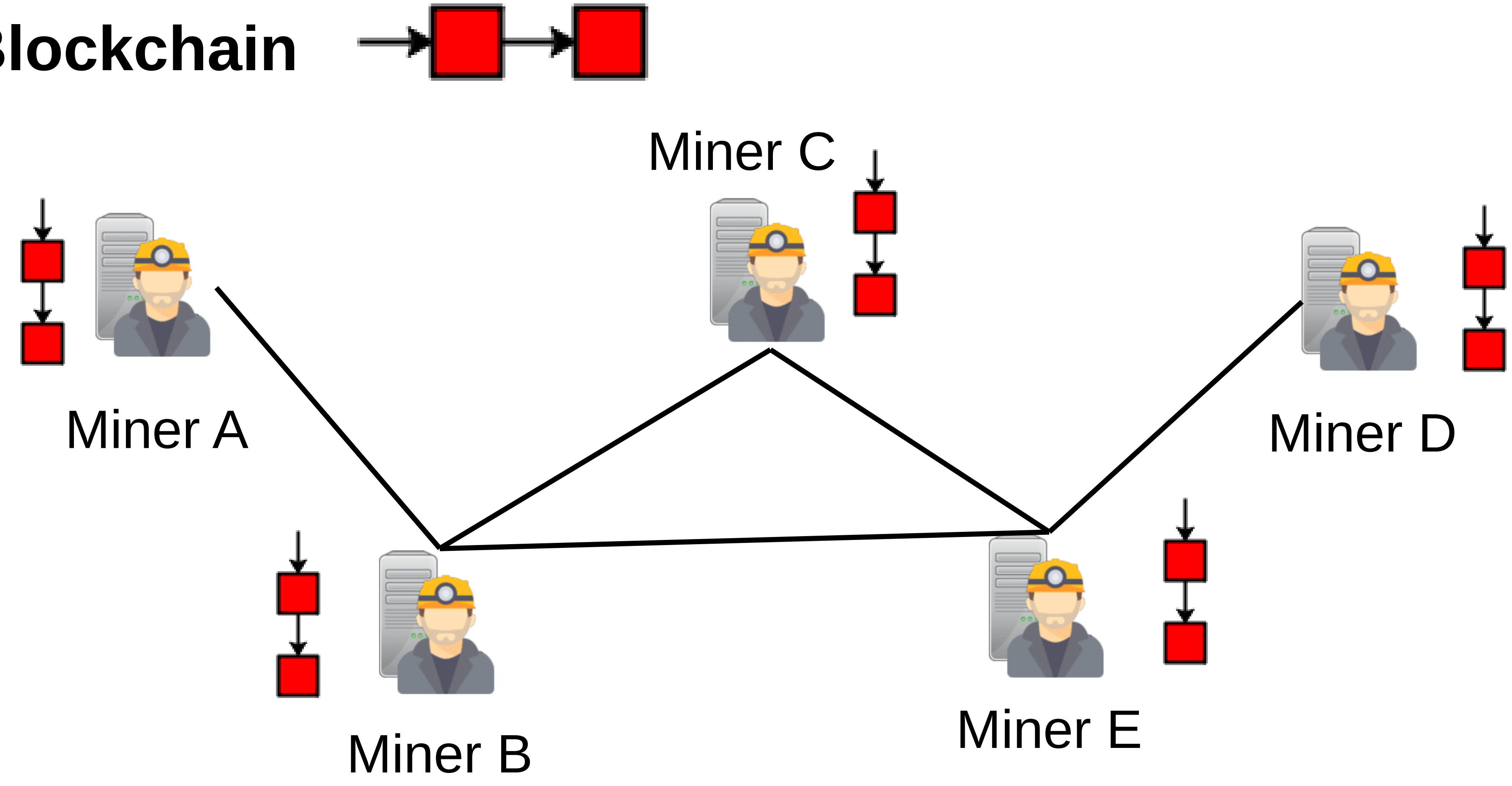


Mining

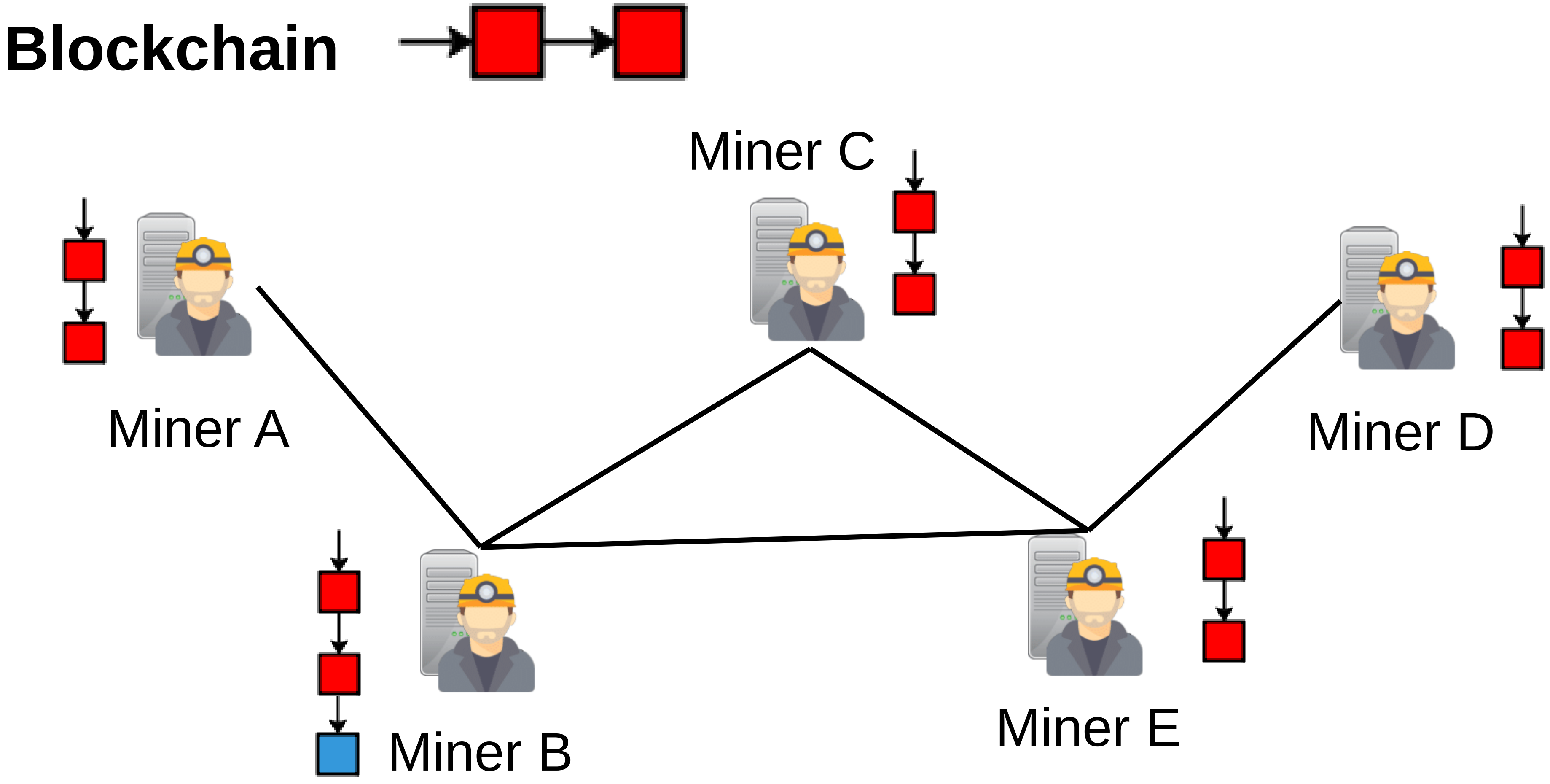


Mining

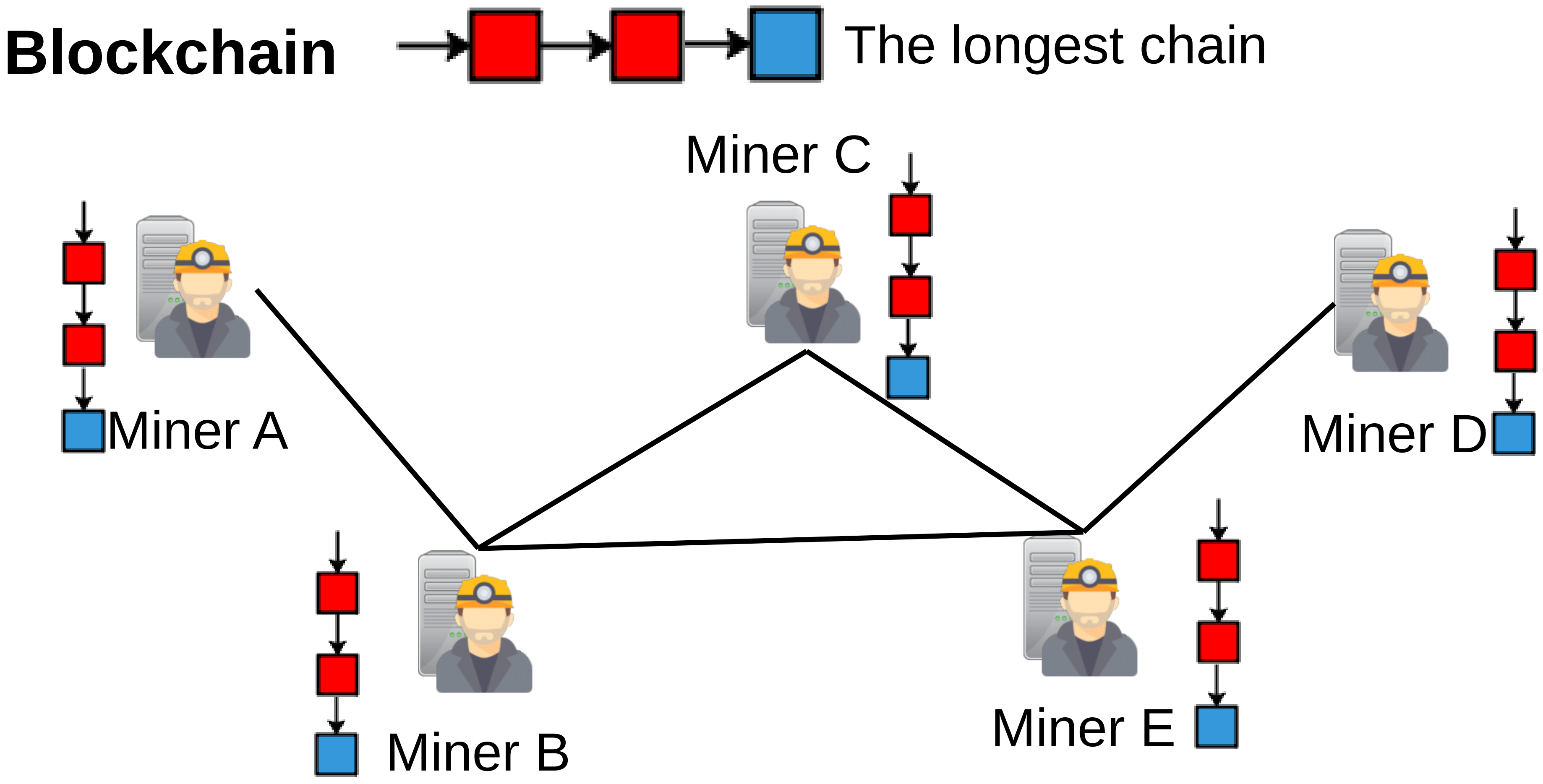
Blockchain



Mining

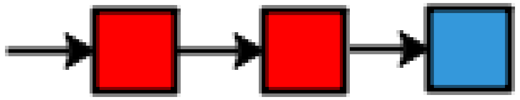


Mining

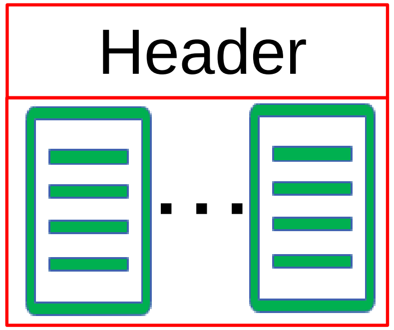

Blockchain
The longest chain
Miner A
Miner B
Miner C
Miner D
Miner E

Incentive for Mining

- Block reward
- Transaction fees



The longest chain



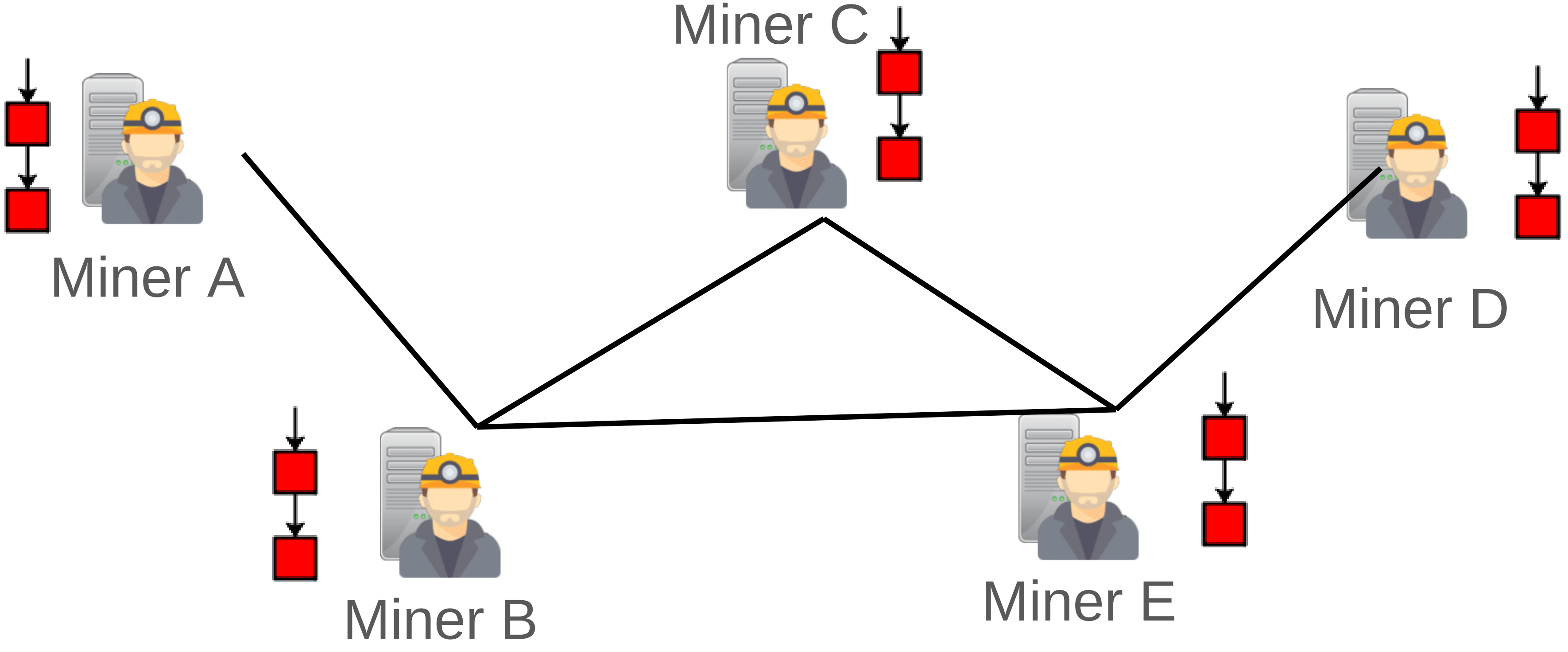
Fairness: wins proportional to computation power

Speed-Security Tradeoff

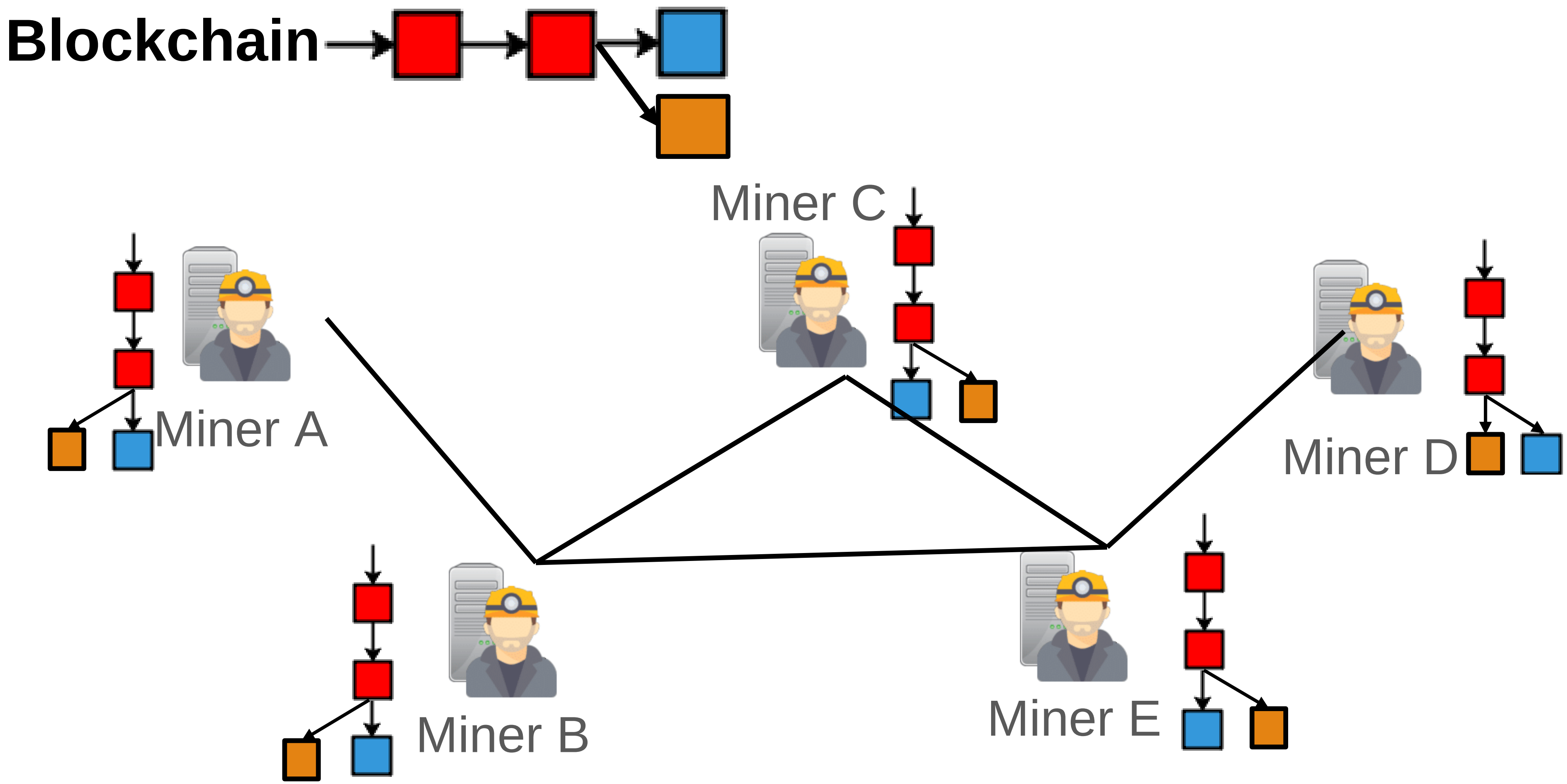
Low throughput ~7 txs per second (Blocks are mined every 10 minutes)

Speed-Security Tradeoff

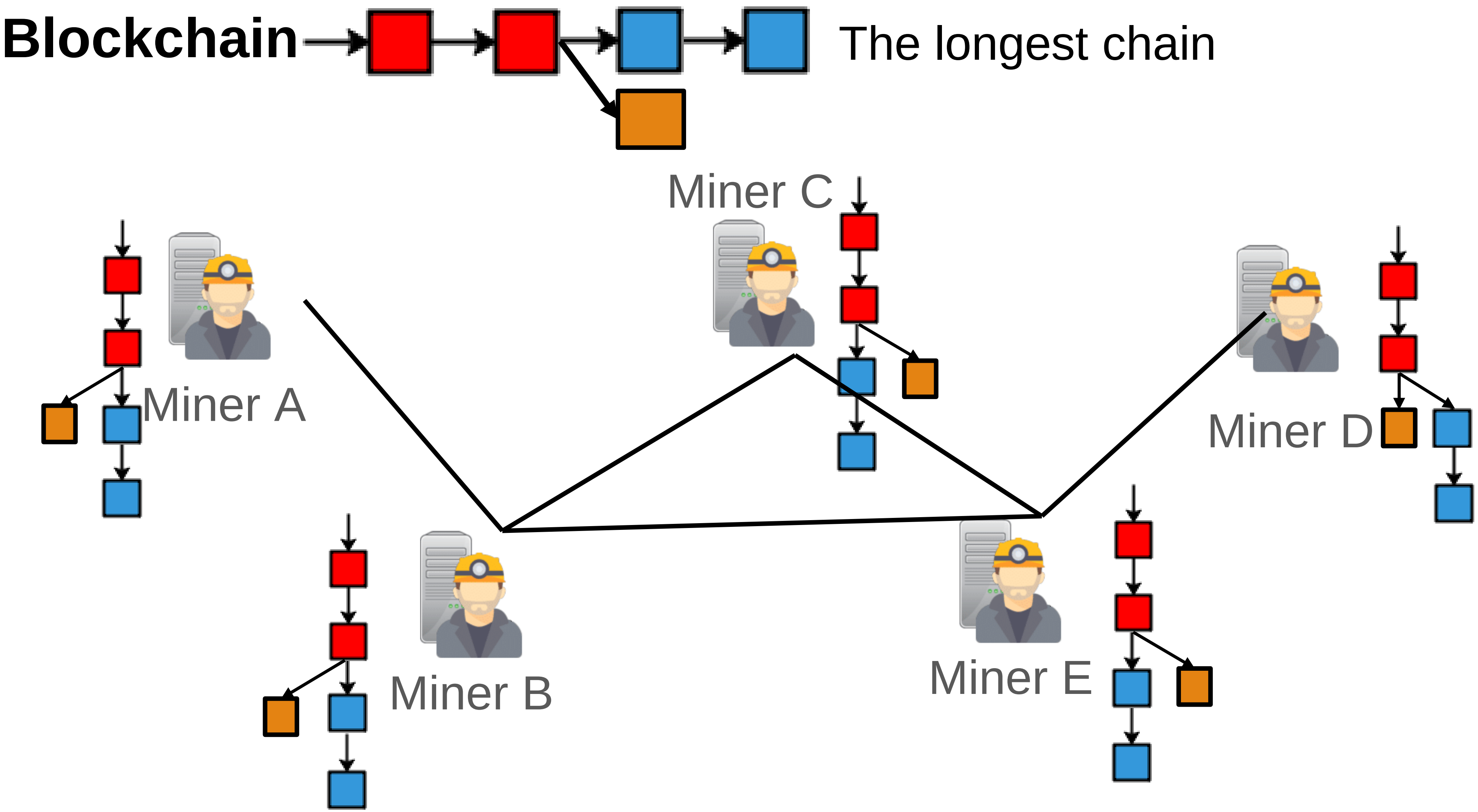
Blockchain



Speed-Security Tradeoff

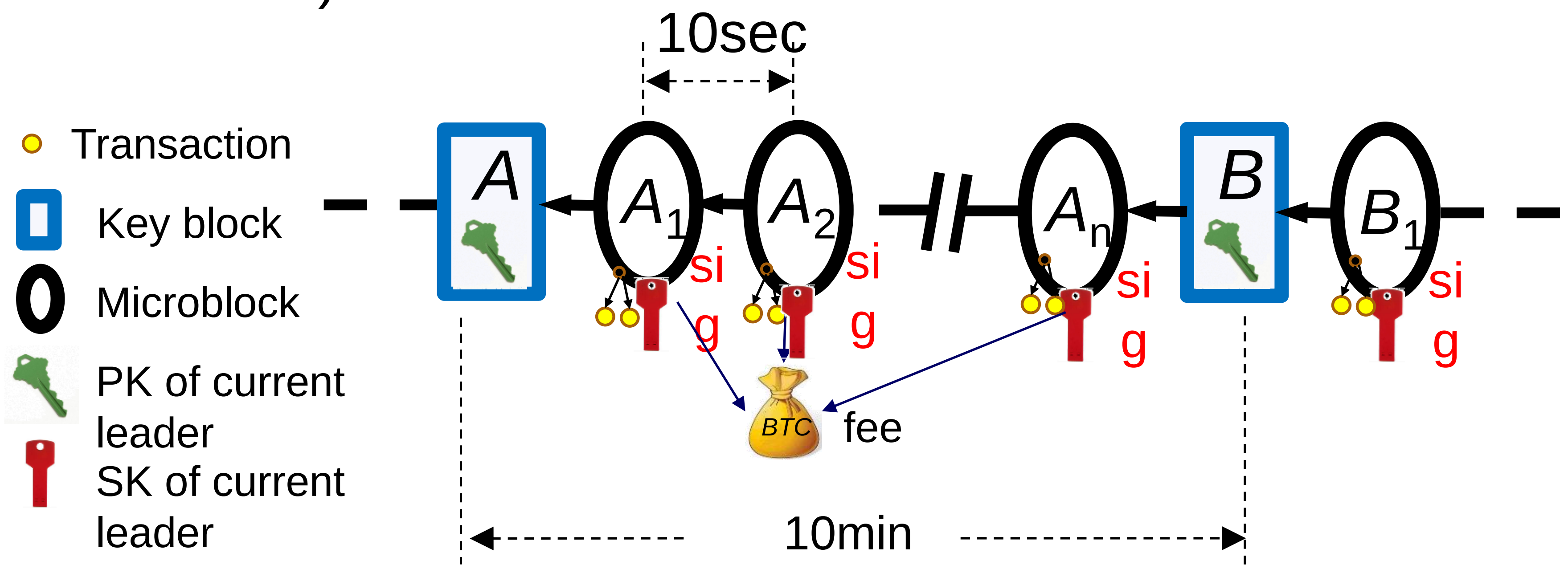


Speed-Security Tradeoff



Bitcoin-NG (Next Generation)

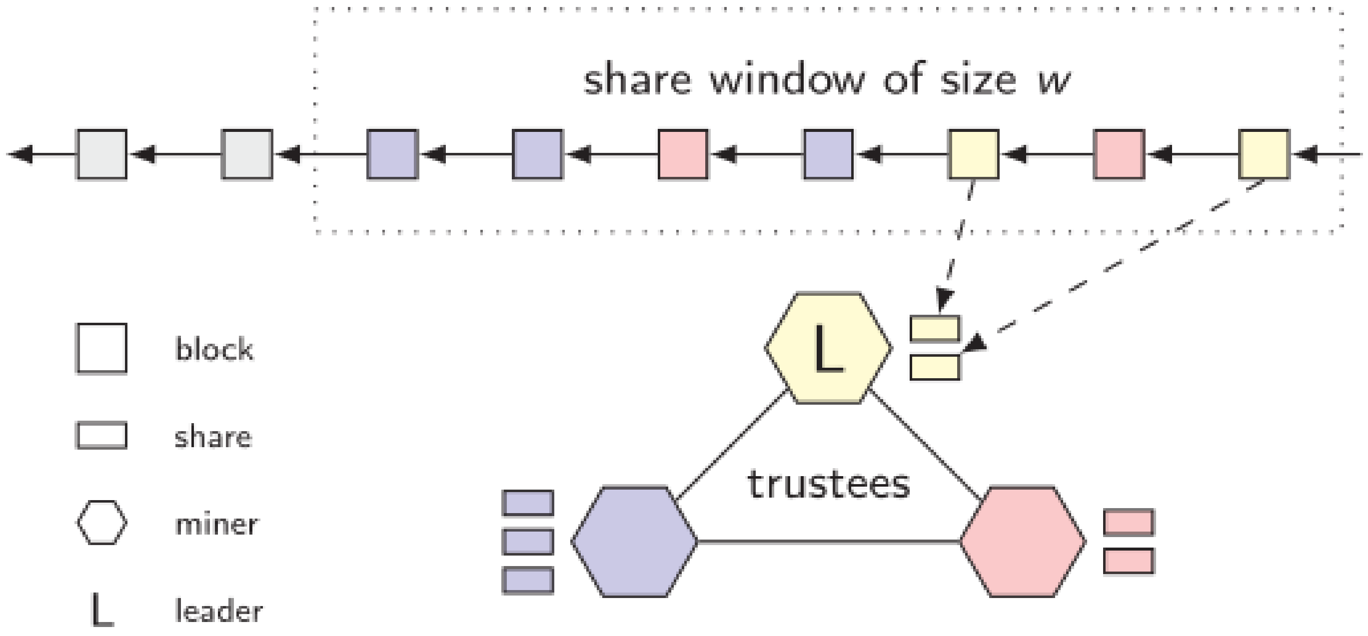
- Bitcoin-NG: A scalable blockchain protocol (NSDI 2016)
- Bitcoin-NG elects a leader by PoW (Key block creator), who can sign several microblocks efficiently (transactions are in microblocks).



Bitcoin-NG decouples leader election with transaction ordering

Next-Generation Blockchains

- Byzcoin (Usenix Security 2016)

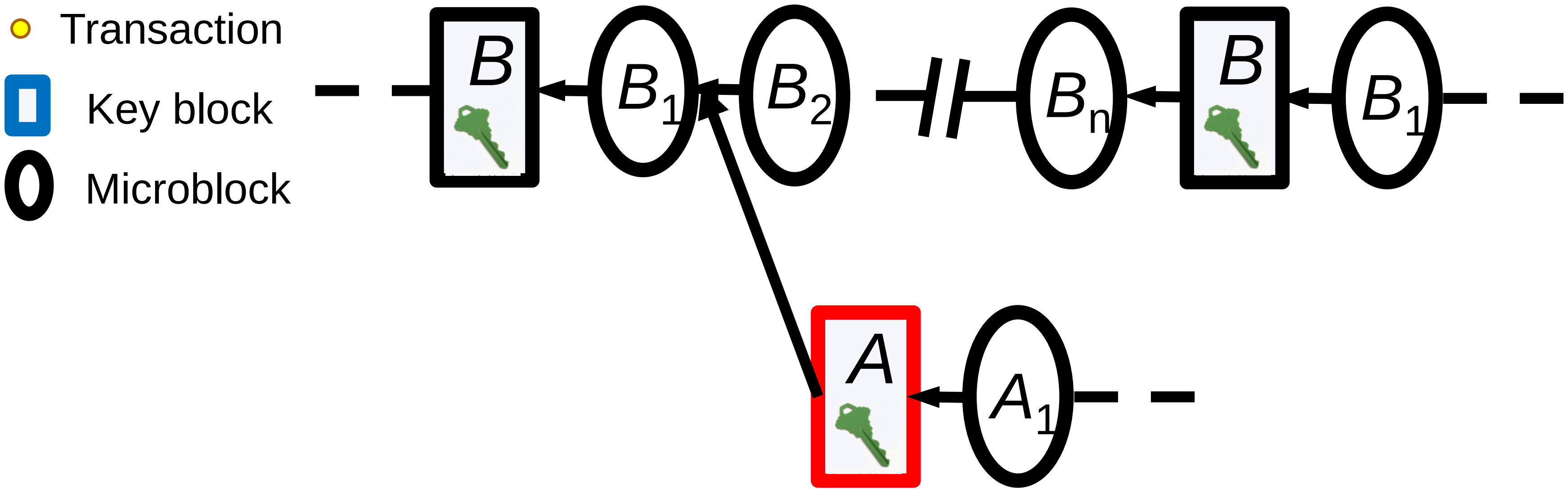


- Prism (CCS 2019), Hybrid Consensus (DISC 2017)

Bitcoin-NG Incentives

Longest chain extension attack

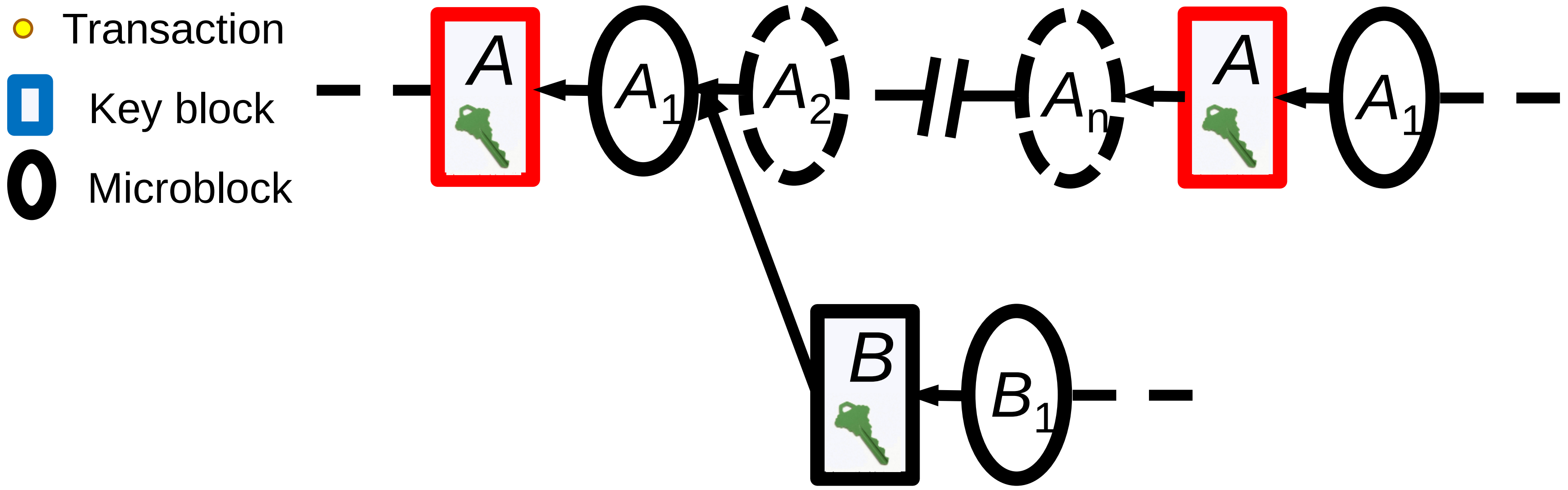
- The adversary rejects some (or all) microblocks and mines directly on the last accepted block;
- Incentivized if transaction fees in microblocks go primarily to the first key-block owner.



Bitcoin-NG Incentives

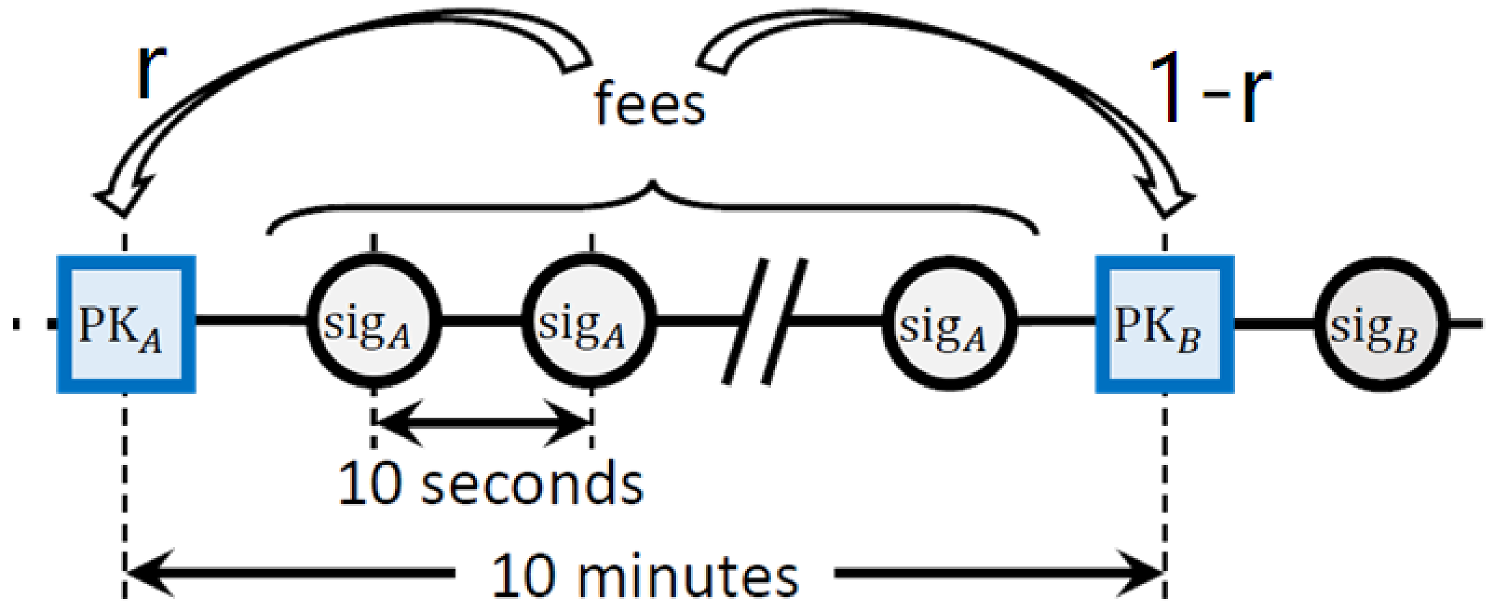
Transaction inclusion attack

- The adversary keeps the last several microblocks private;
- Incentivized if transaction fees in microblocks go primarily to the second key-block owner.

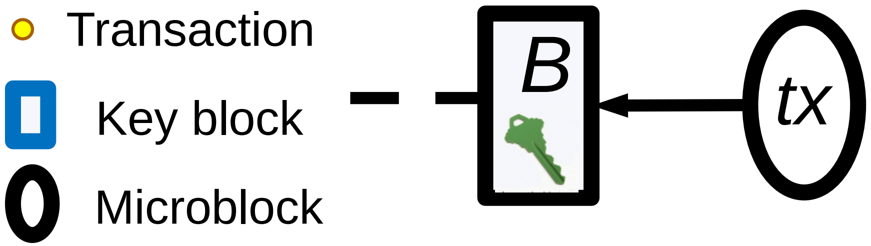


Bitcoin-NG Incentives

The transaction fee distributed rate r

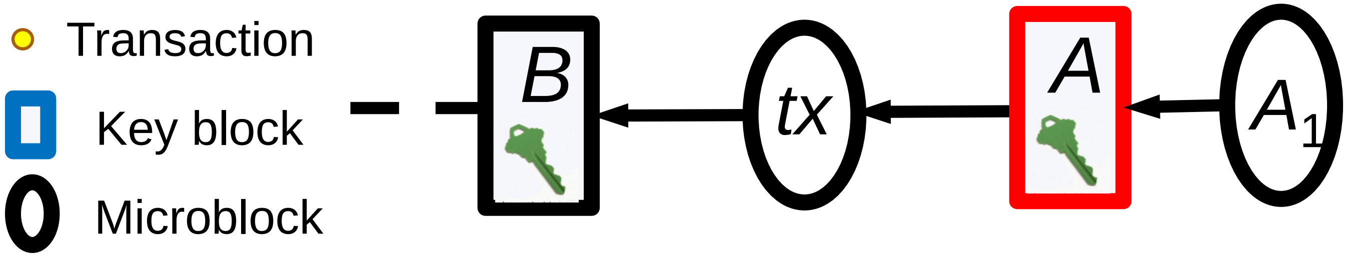


Existing Incentive Analysis



A simple case of the longest chain extension attack

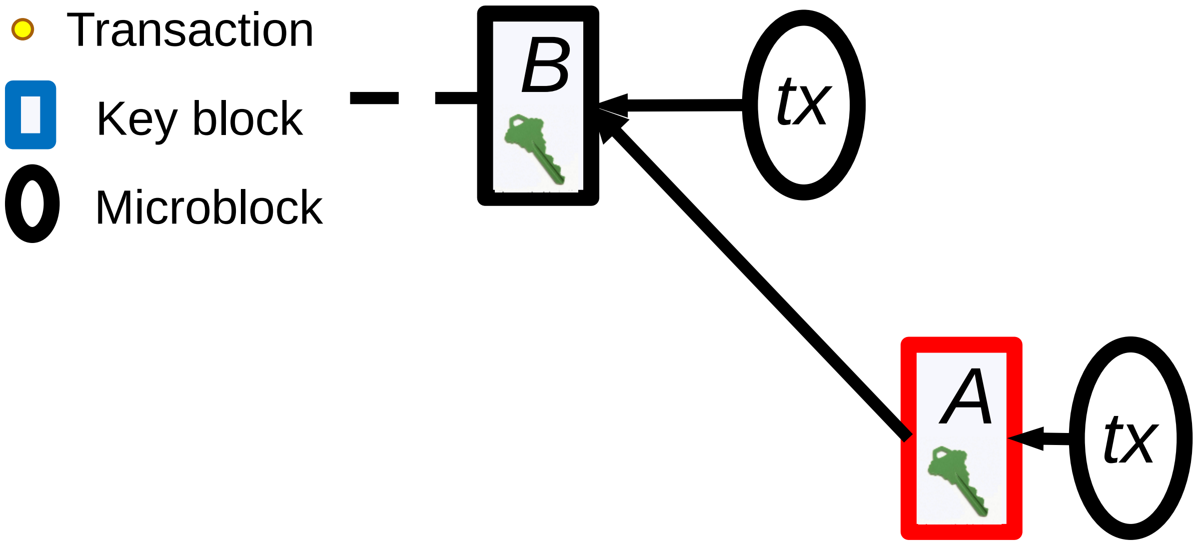
Existing Incentive Analysis



$$\overbrace{\alpha \times (100\% - r)}^{\text{Mine on microblock}}$$

A simple case of the longest chain extension attack

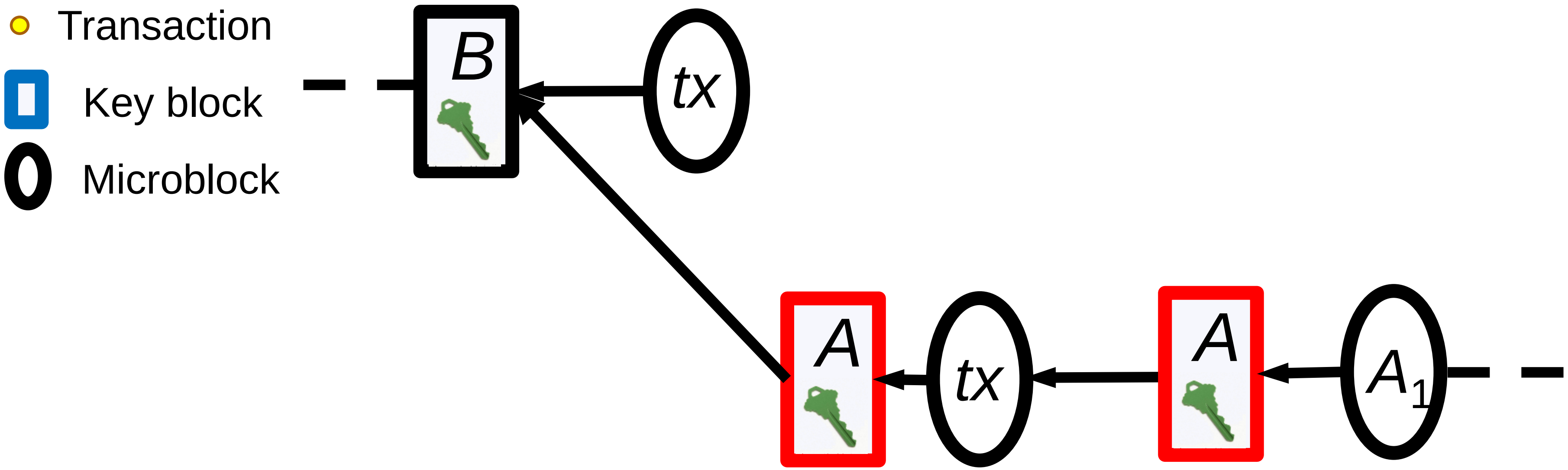
Existing Incentive Analysis



$$\underbrace{}_{}\overset{\text{Mine next key block}}{\alpha \times r} \qquad \overbrace{\alpha \times (100\% - r)}^{\text{Mine on microblock}}$$

A simple case of the longest chain extension attack

Existing Incentive Analysis



$$\overbrace{\alpha \times r}^{\text{Mine next key block}} + \overbrace{\alpha^2 \times (100\% - r)}^{\text{Mine the third key Block}} < \overbrace{\alpha \times (100\% - r)}^{\text{Mine on microblock}}$$

A simple case of the longest chain extension attack

Existing Incentives Analysis

- **Resisting longest chain extension attack**

$$\underbrace{\alpha \times r}_{\text{Mine next key block}} + \overbrace{\alpha^2 \times (100\% - r)}^{\text{Mine the third key Block}} < \overbrace{\alpha \times (100\% - r)}^{\text{Mine on microblock}}$$

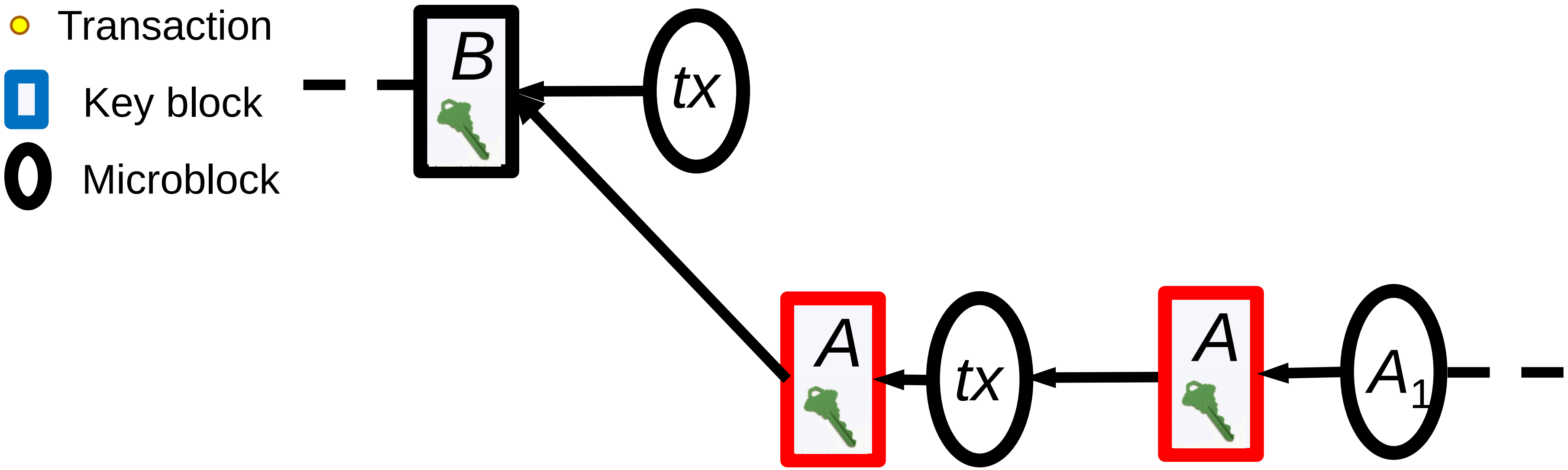
- **Resisting transaction inclusion attack**

$$\overbrace{\alpha \times 100\%}^{\text{win 100\%}} + \overbrace{(1-\alpha) \times \alpha \times (100\% - r)}^{\text{Lose 100\%,but mine after txn}} < r$$

The transaction fee distributed rate r should be:

$$1 - \frac{1-\alpha}{1+\alpha-\alpha^2} < r < \frac{1-\alpha}{2-\alpha}$$

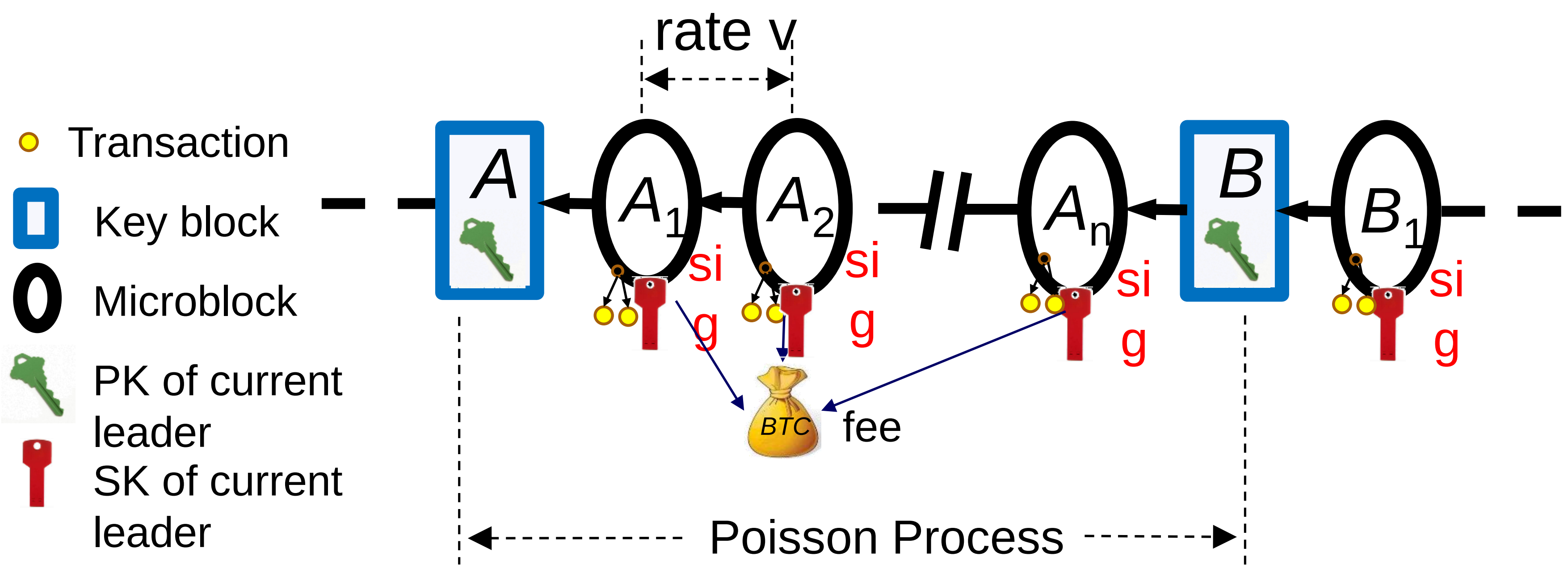
Limitations



$$\overset{\text{Mine next key block}}{\alpha \times r} + \overbrace{\alpha^{2} \times (100\% - r)}^{\text{Mine the third key Block}} < \overbrace{\alpha \times (100\% - r)}^{\text{Mine on microblock}}$$

Without considering the network capacity

Our Analysis Model

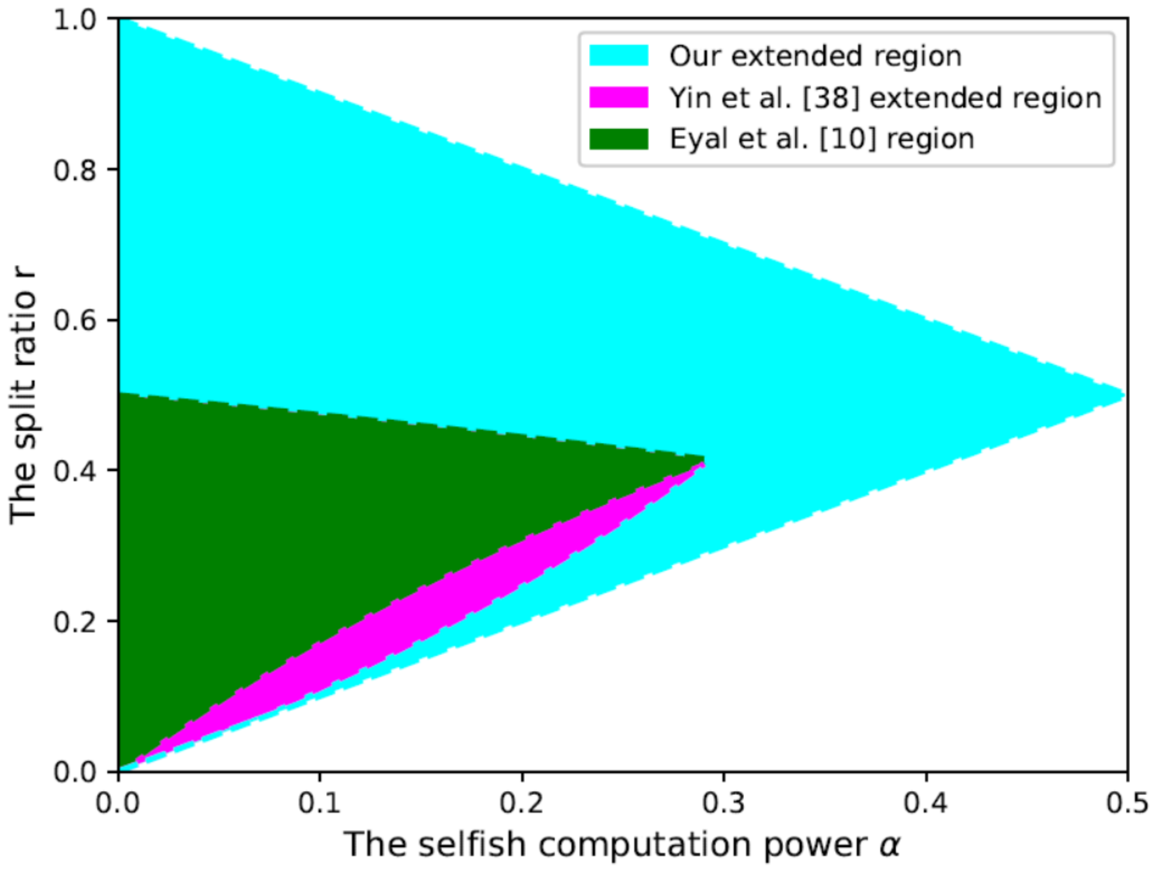


Incentive Analysis with Network Capacity

Consider the revenue for the adversary in a time interval t

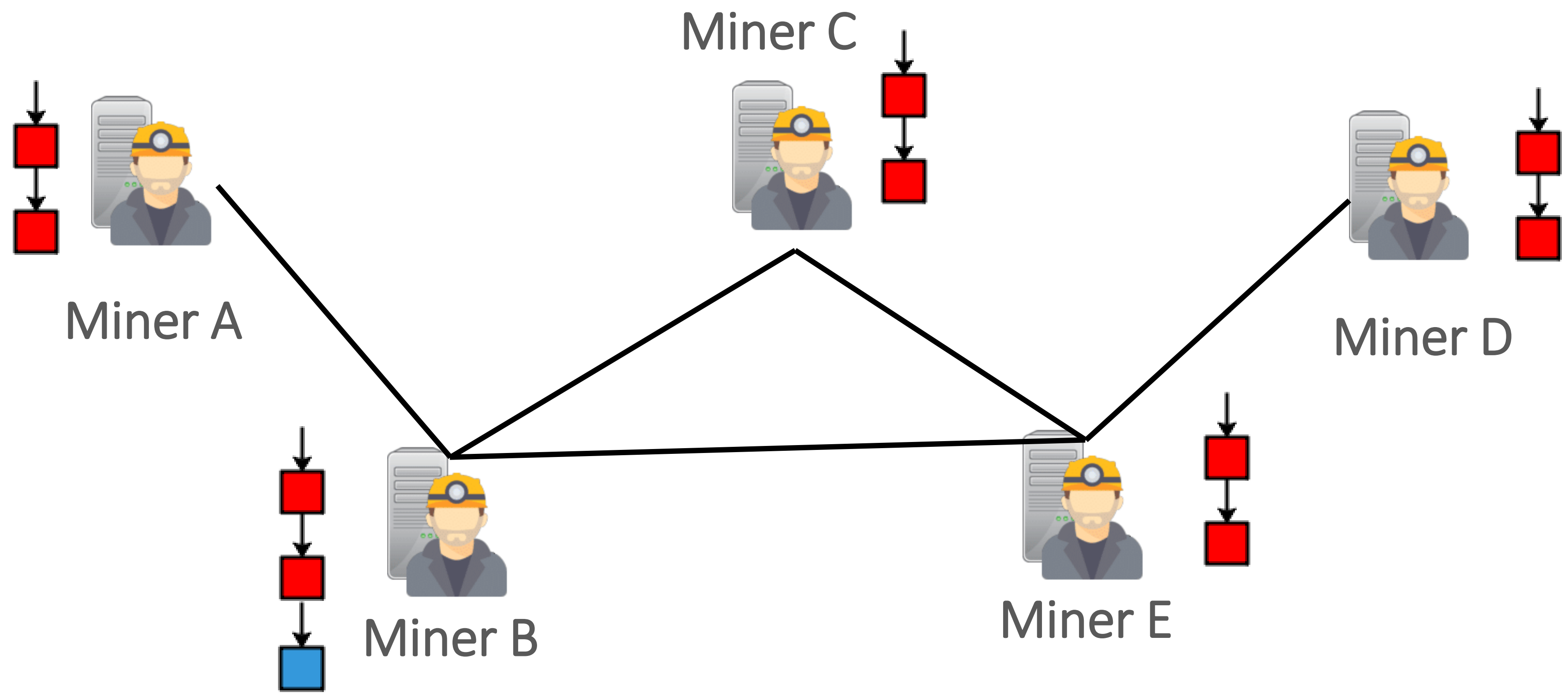
$$u = \lim_{t \to \infty} \frac{r_a(t) + t_a(t)}{r_a(t) + r_h(t) + t_a(t) + t_h(t)}$$

Incentive Analysis with Network Capacity



$$\alpha < r < \beta$$

Key Block Selfish Mining



If selfish miners control more than 23.21% of computation power, it obtain a revenue larger than their fair share.

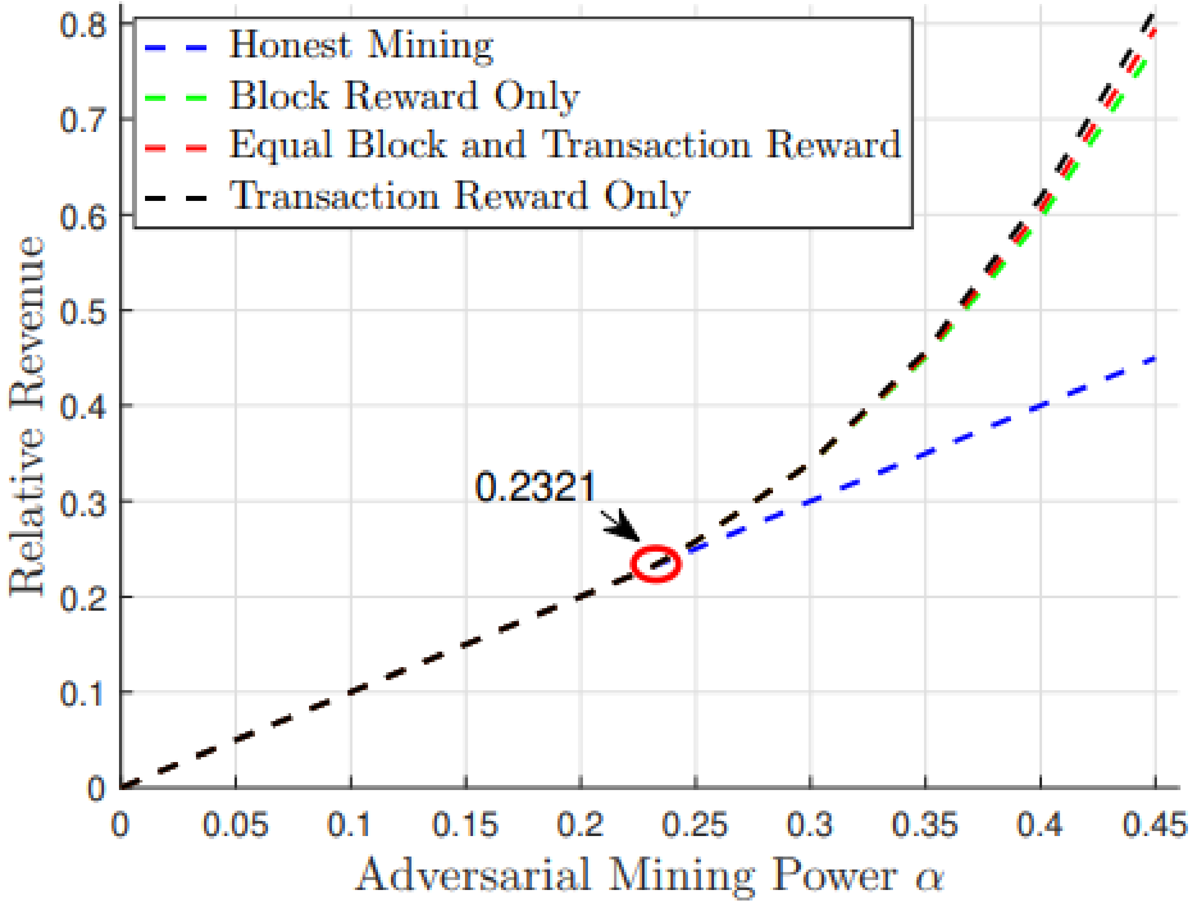
MDP Model

TABLE I
STATE TRANSITION AND REWARD MATRICES FOR THE OPTIMAL SELFISH MINING.

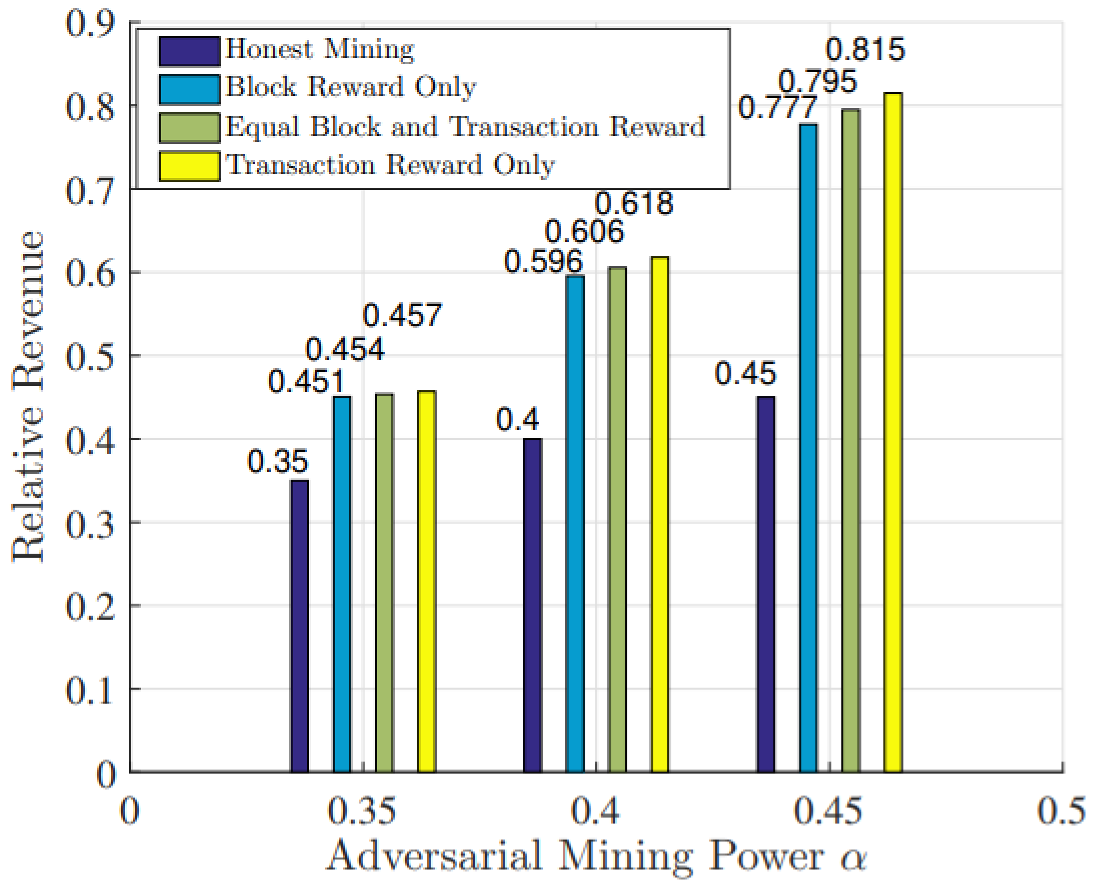
State × Action	State	Probability	Reward	Condition
$(l_a, l_h, \cdot, S_h)$, adopt	$(1, 0, \text{noTie}, H_{\text{in}})$	α	$(l_h, l_h, 0, 0)$	–
$(l_a, l_h, \cdot, S_p)$, adopt	$(0, 1, \text{noTie}, H_{\text{in}})$	$1-\alpha$	$(l_h, l_h - 1 + (1-r), 0, r)$	
$(l_a, l_h, \cdot, \{H_{\text{in}}, H_{\text{ex}}\})$, adopt			$(l_h, l_h - 1, 0, 0)$	
$(l_a, l_h, \cdot, S_h)$, adoptE	$(1, 0, \text{noTie}, H_{\text{ex}})$	α	$(l_h, l_h, 0, 0)$	–
$(l_a, l_h, \cdot, S_p)$, adoptE	$(0, 1, \text{noTie}, H_{\text{ex}})$	$1-\alpha$	$(l_h, l_h - 1 + (1-r), 0, r)$	
$(l_a, l_h, \cdot, \{H_{\text{in}}, H_{\text{ex}}\})$, adoptE			$(l_h, l_h - 1, 0, 0)$	
$(l_a, l_h, \cdot, H_{\text{ex}})$, override	$(l_a - l_h, 0, \text{noTie}, S_p)$	α	$(0, 0, l_h + 1, l_h + 1)$	$l_a > l_h$
$(l_a, l_h, \cdot, H_{\text{in}})$, override	$(l_a - l_h - 1, 1, \text{noTie}, S_p)$	$1-\alpha$	$(0, r, l_h + 1, l_h + (1-r))$	
$(l_a, l_h, \cdot, \{S_p, S_h\})$, override			$(0, 0, l_h + 1, l_h)$	
$(l_a, l_h, \cdot, H_{\text{ex}})$, overrideH	$(l_a - l_h, 0, \text{noTie}, S_h)$	α	$(0, 0, l_h + 1, l_h + 1)$	$l_a > l_h$
$(l_a, l_h, \cdot, H_{\text{in}})$, overrideH	$(l_a - l_h - 1, 1, \text{noTie}, S_h)$	$1-\alpha$	$(0, r, l_h + 1, l_h + (1-r))$	
$(l_a, l_h, \cdot, \{S_p, S_h\})$, overrideH			$(0, 0, l_h + 1, l_h)$	
$(l_a, l_h, \text{noTie}, \cdot)$, wait	$(l_a + 1, l_h, \text{noTie}, *)$	α	$(0, 0, 0, 0)$	–
	$(l_a, l_h + 1, \text{noTie}, *)$	$1-\alpha$		
$(l_a, l_h, noTie, H_{\text{in}})$, match	$(l_a + 1, l_h, \text{tie}, H_{\text{in}})$	α	$(0, 0, 0, 0)$	$la \geq l_h$
$(l_a, l_h, \text{tie}, H_{\text{in}})$, wait	$(l_a - l_h, 1, \text{noTie}, S_p)$	$\gamma(1-\alpha)$	$(0, r, l_h, l_h - 1 + (1-r))$	
	$(l_a, l_h + 1, \text{noTie}, H_{\text{in}})$	$(1-\gamma)(1-\alpha)$	$(0, 0, 0, 0)$	
$(l_a, l_h, noTie, H_{\text{ex}})$, match	$(l_a + 1, l_h, \text{tie}, H_{\text{ex}})$	α	$(0, 0, 0, 0)$	$la \geq l_h$
$(l_a, l_h, \text{tie}, H_{\text{ex}})$, wait	$(l_a - l_h, 1, \text{noTie}, S_p)$	$\gamma(1-\alpha)$	$(0, 0, l_h, l_h - 1)$	
	$(l_a, l_h + 1, \text{noTie}, H_{\text{ex}})$	$(1-\gamma)(1-\alpha)$	$(0, 0, 0, 0)$	
$(l_a, l_h, \text{noTie}, \{S_p, S_h\})$, match	$(l_a + 1, l_h, \text{tie}, *)$	α	$(0, 0, 0, 0)$	$la \geq l_h$
$(l_a, l_h, \text{tie}, \{S_p, S_h\})$, wait	$(l_a - l_h, 1, \text{noTie}, S_p)$	$\gamma(1-\alpha)$	$(0, 0, l_h, l_h)$	
	$(l_a, l_h + 1, \text{noTie}, *)$	$(1-\gamma)(1-\alpha)$	$(0, 0, 0, 0)$	
$(l_a, l_h, \text{noTie}, H_{\text{in}})$, matchH	$(l_a + 1, l_h, tie', H_{\text{in}})$	α	$(0, 0, 0, 0)$	$la \geq l_h$
$(l_a, l_h, tie', H_{\text{in}})$, wait	$(l_a - l_h, 1, \text{noTie}, S_h)$	$\gamma(1-\alpha)$	$(0, r, l_h, l_h - 1 + (1-r))$	
	$(l_a, l_h + 1, \text{noTie}, H_{\text{in}})$	$(1-\gamma)(1-\alpha)$	$(0, 0, 0, 0)$	
$(l_a, l_h, noTie, H_{\text{ex}})$, matchH	$(l_a + 1, l_h, \text{tie}', H_{\text{ex}})$	α	$(0, 0, 0, 0)$	$la \geq l_h$
$(l_a, l_h, \text{tie}', H_{\text{ex}})$, wait	$(l_a - l_h, 1, \text{noTie}, S_h)$	$\gamma(1-\alpha)$	$(0, 0, l_h, l_h - 1)$	
	$(l_a, l_h + 1, \text{noTie}, H_{\text{ex}})$	$(1-\gamma)(1-\alpha)$	$(0, 0, 0, 0)$	
$(l_a, l_h, noTie, \{S_p, S_h\})$, matchH	$(l_a + 1, l_h, \text{tie}', *)$	α	$(0, 0, 0, 0)$	$la \geq l_h$
$(l_a, l_h, \text{tie}', \{S_p, S_h\})$, wait	$(l_a - l_h, 1, \text{noTie}, S_h)$	$\gamma(1-\alpha)$	$(0, 0, l_h, l_h)$	
	$(l_a, l_h + 1, \text{noTie}, *)$	$(1-\gamma)(1-\alpha)$	$(0, 0, 0, 0)$	
$(l_a, l_h, \text{tie}', \cdot)$, revert	$(l_a, l_h, \text{tie}, *)$	1	$(0, 0, 0, 0)$	–
$(l_a, l_h, \cdot, S_h)$, revert	$(l_a, l_h, *, S_p)$	1	$(0, 0, 0, 0)$	$l_h = 0$
$(l_a, l_h, \cdot, H_{\text{ex}})$, revert	$(l_a, l_h, *, H_{\text{in}})$	1	$(0, 0, 0, 0)$	$l_a = 0$

$*$ denotes the state element remains the same in the state transition.

Joint Incentive Analysis



Joint Incentive Analysis



Thank you!