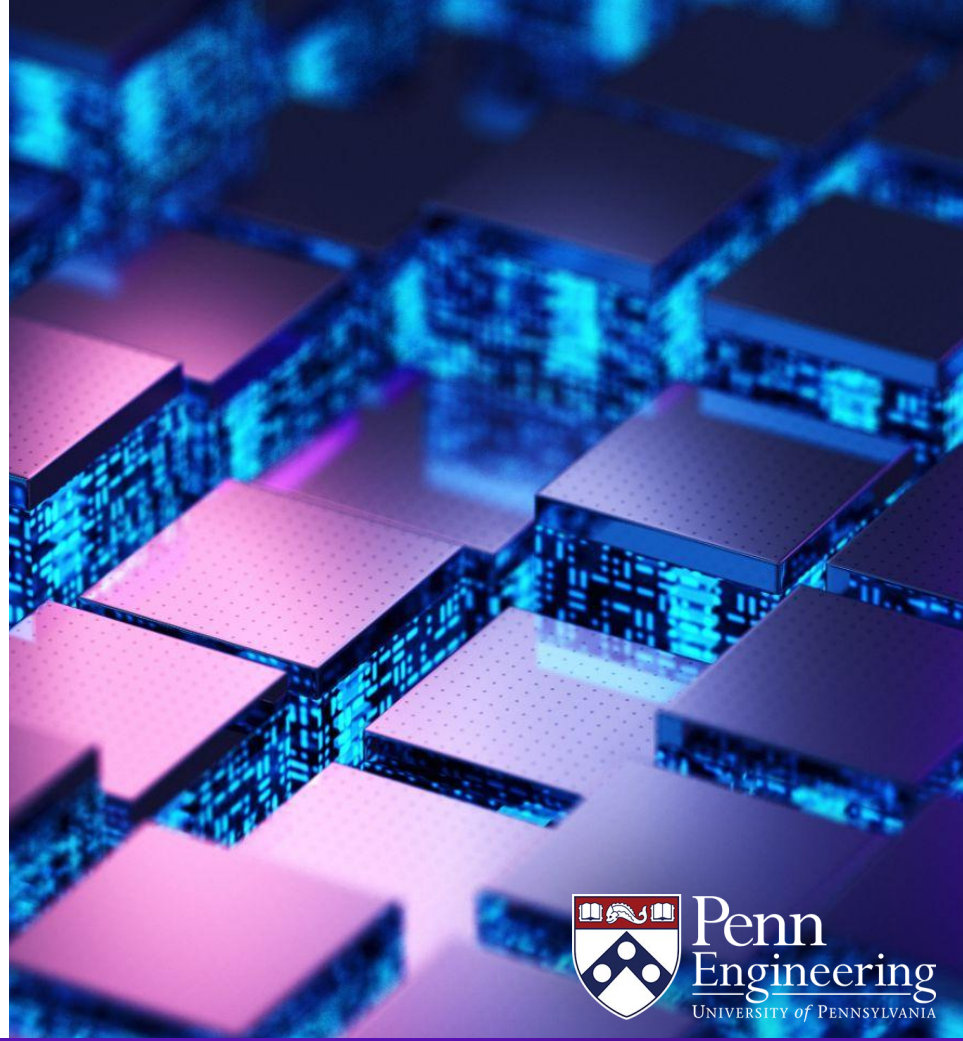
EAS 5830: BLOCKCHAINS

Selfish Mining

Dr. Brett Hemenway Falk



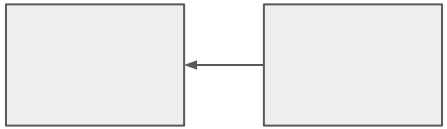
Majority is not Enough: Bitcoin Mining is Vulnerable

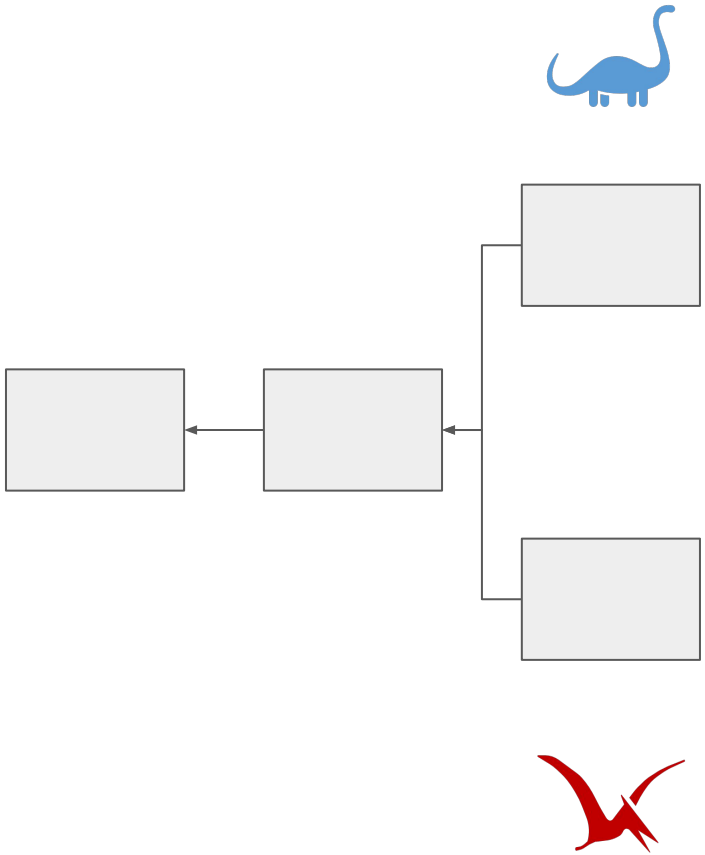
Ittay Eyal and Emin Gün Sirer

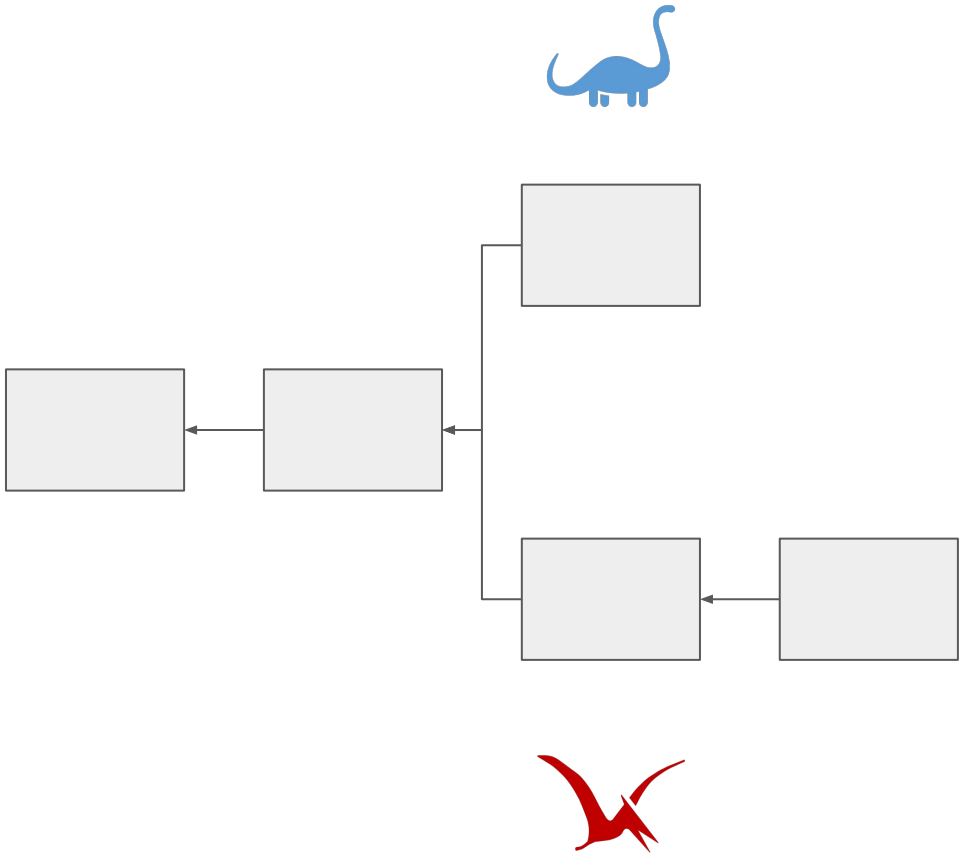
Department of Computer Science, Cornell University
ittay.eyal@cornell.edu, egs@systems.cs.cornell.edu

Basic Security Analysis

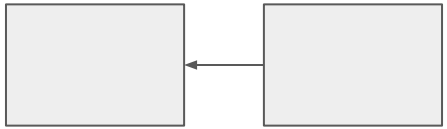
- **Protocol**:
  - Always mine on the longest chain
    - In the event of a tie, mine on the block you saw first
  - Always publish block as soon as you mine it
- **Analysis**:
  - If an attacker ignores the blocks of the honest miners
    - Only mines on their own fork
  - Attack is successful if attacker controls a majority of the stake





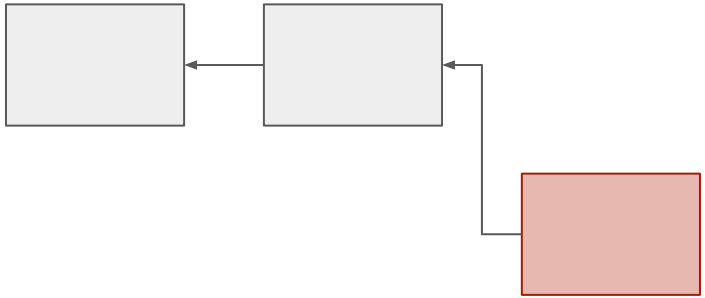


Honest miners



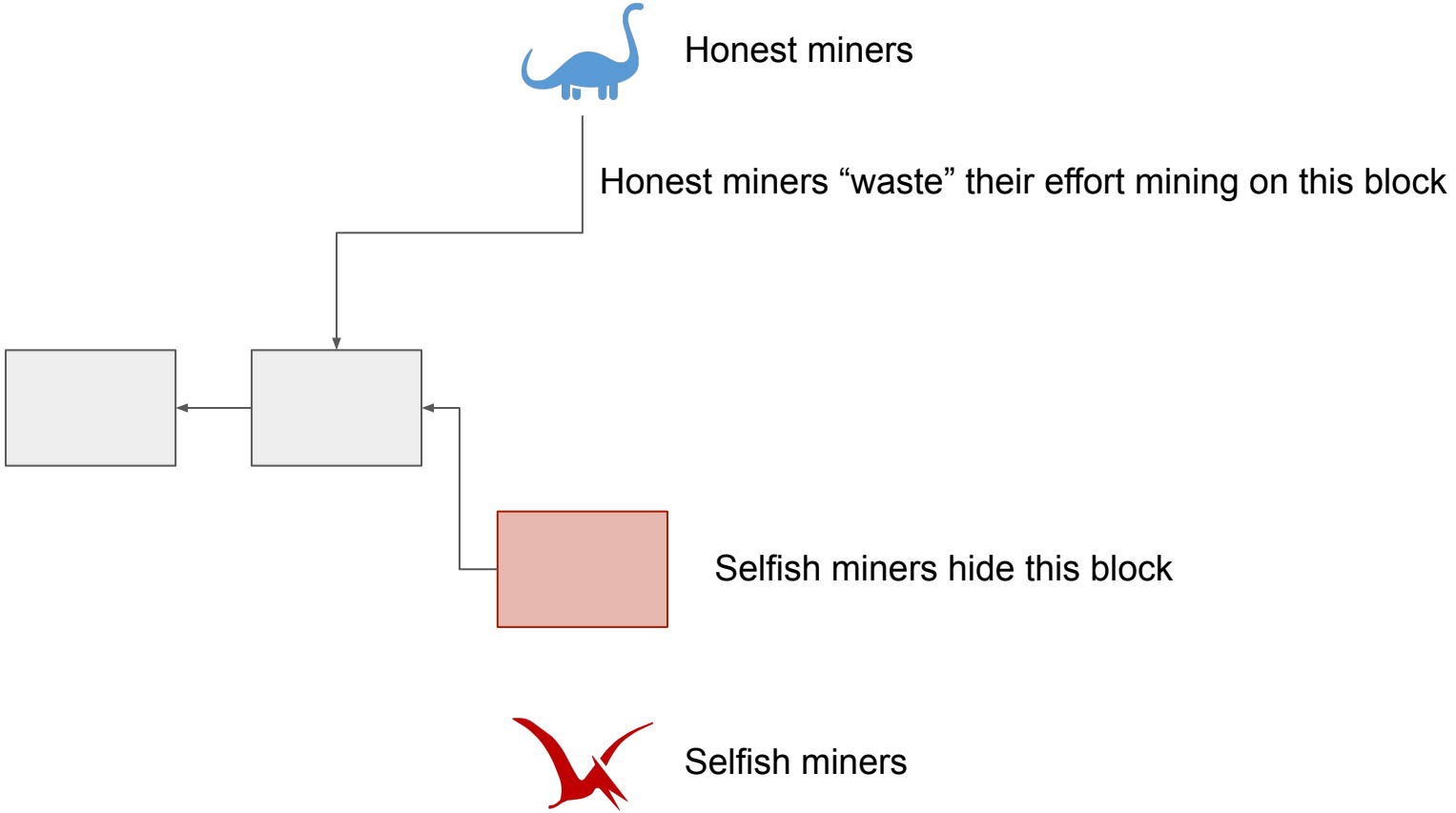
Selfish miners

Honest miners



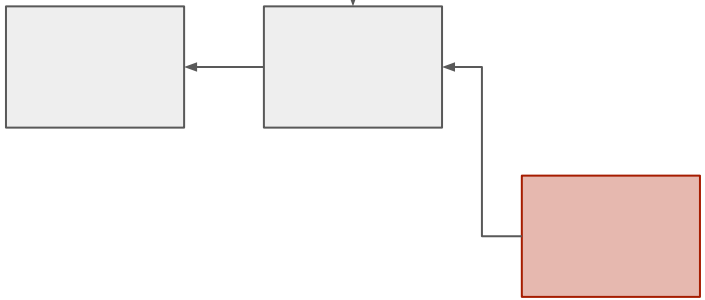
Selfish miners hide this block

Selfish miners


Honest miners
Honest miners “waste” their effort mining on this block
Selfish miners hide this block
Selfish miners

Honest miners

Honest miners “waste” their effort mining on this block



Intuition:
If you can make honest miners “waste” their effort Selfish miner effectively has a larger fraction of the mining power

Selfish miners hide this block

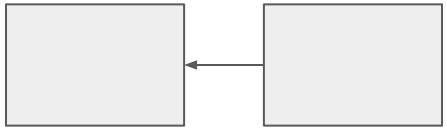
Selfish miners

Warmup

Honest miners

Assume:

- Selfish miners have better connectivity than honest miners
- Selfish miners can propagate blocks faster than honest miners



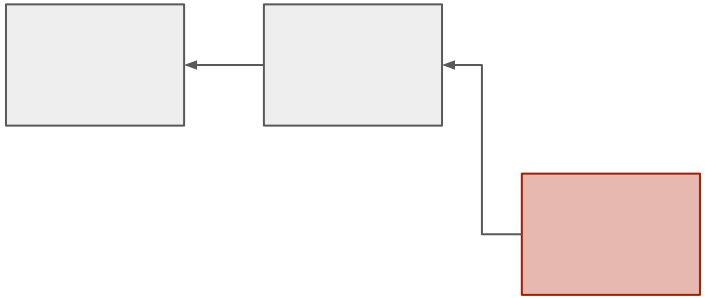
Selfish miners

Warmup

Honest miners

Assume:

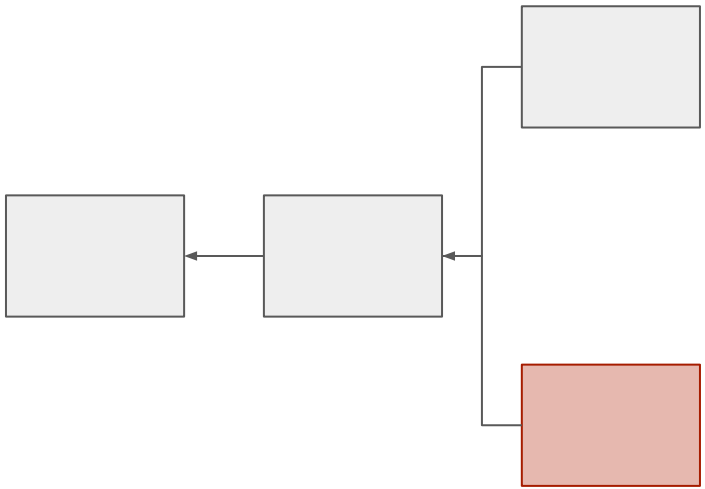
- Selfish miners have better connectivity than honest miners
- Selfish miners can propagate blocks faster than honest miners



Withhold block

Selfish miners

Warmup



Withhold block

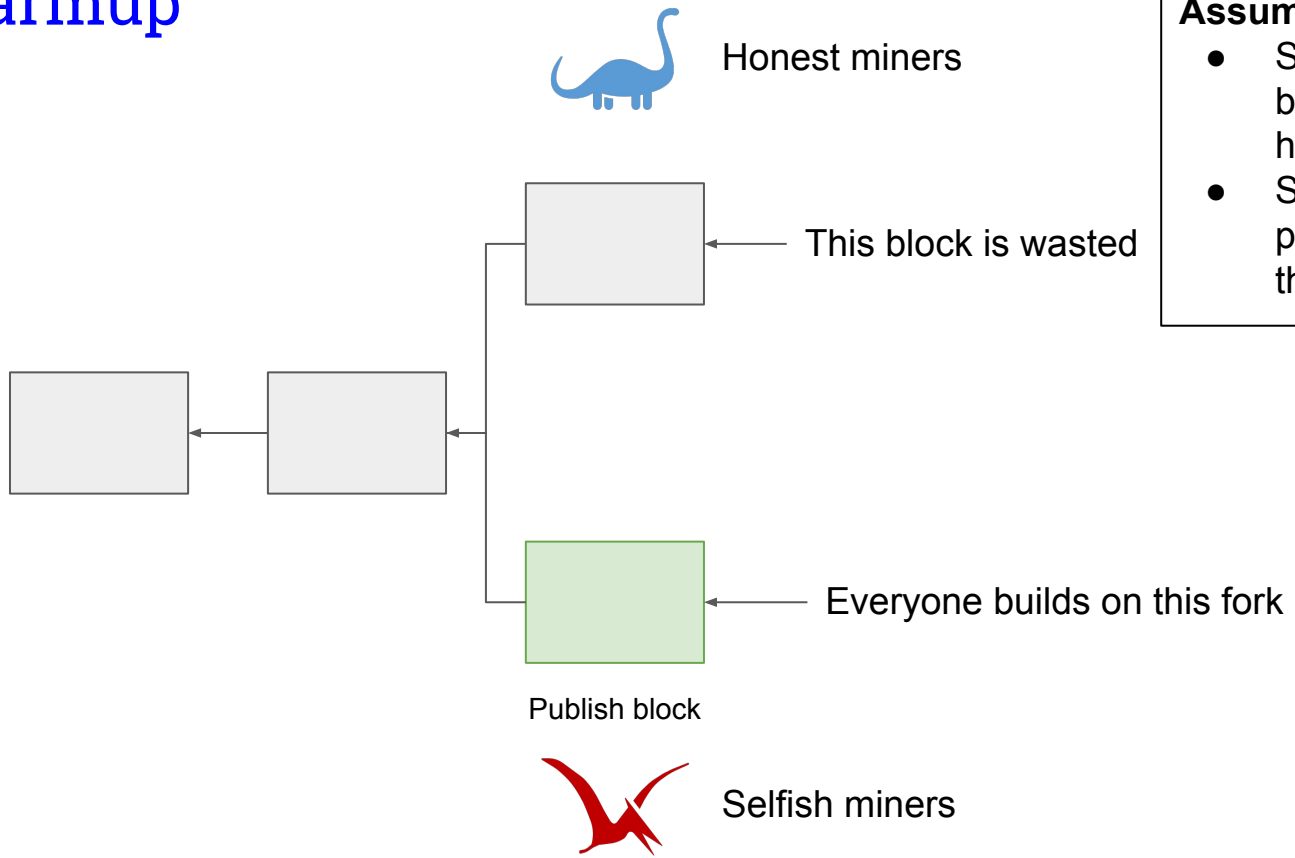
Honest miners

Selfish miners

Assume:

- Selfish miners have better connectivity than honest miners
- Selfish miners can propagate blocks faster than honest miners

Warmup



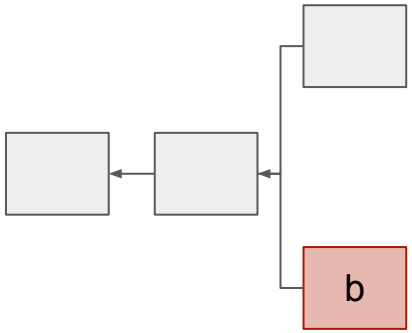
Assume:

- Selfish miners have better connectivity than honest miners
- Selfish miners can propagate blocks faster than honest miners

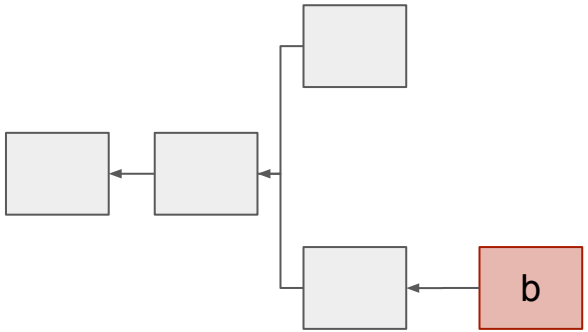
General strategy

- Assume selfish miner controls α-fraction of hash power
- In the case of a tie, a γ-fraction of honest nodes build on selfish-miner's block
  - Warmup was the case $\gamma = 1$
- Strategy
  - If selfish miner has a block b at height h, publish it if:

Case 1: Honest miners catch up



Case 2: Block is "pivotal"



Selfish mining

Theorem:

If $\alpha > ⅓$, following the selfish mining strategy leads to more profit for the selfish miner than following the “honest” strategy

Follow ups

- Majority is not Enough: Bitcoin Mining is Vulnerable
- Optimal Selfish Mining Strategies in Bitcoin
- Undetectable Selfish Mining