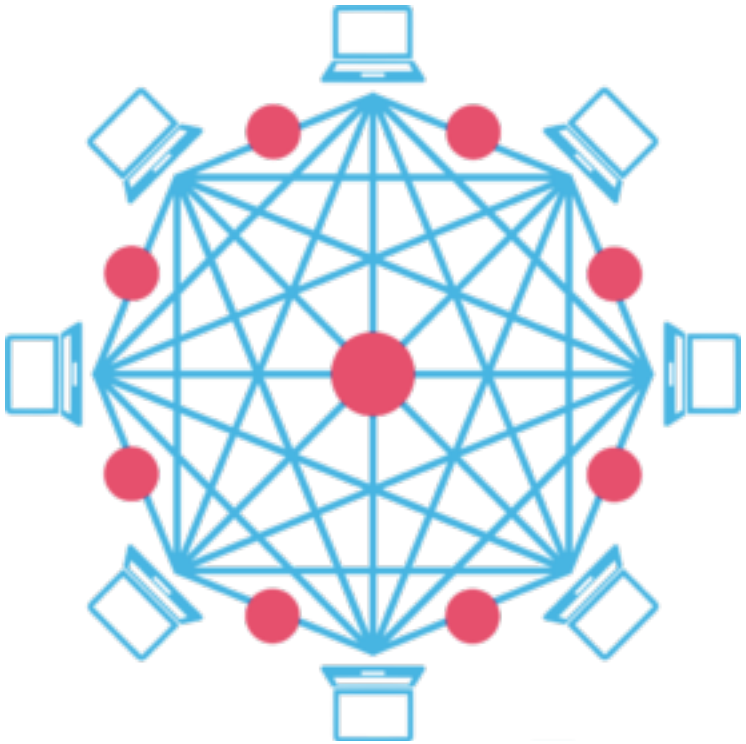
Be Selfish and Avoid Dilemmas

Fork After Withholding Attacks on Bitcoin

Y. Kwon, D. Kim, Y. Son, E. Vasserman, Y. Kim. CCS 2017.

Simon Bienz

Blockchain



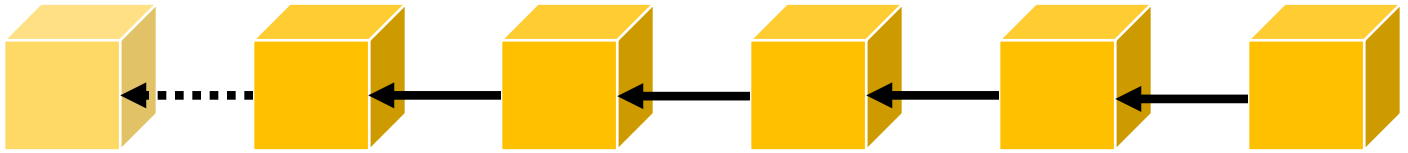
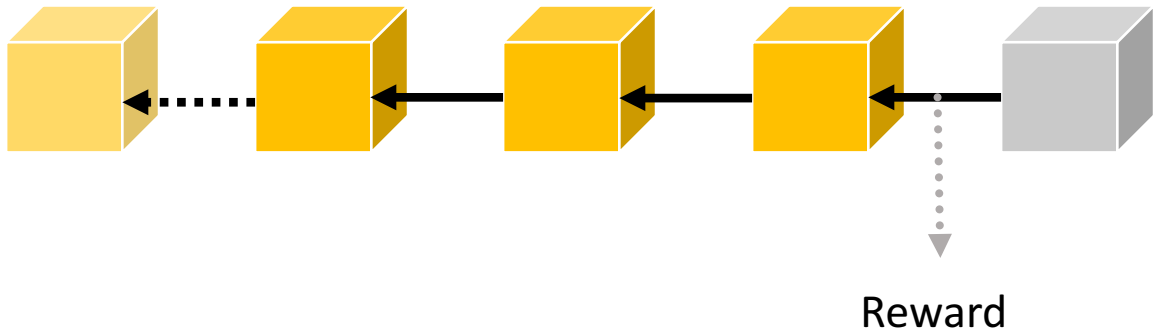
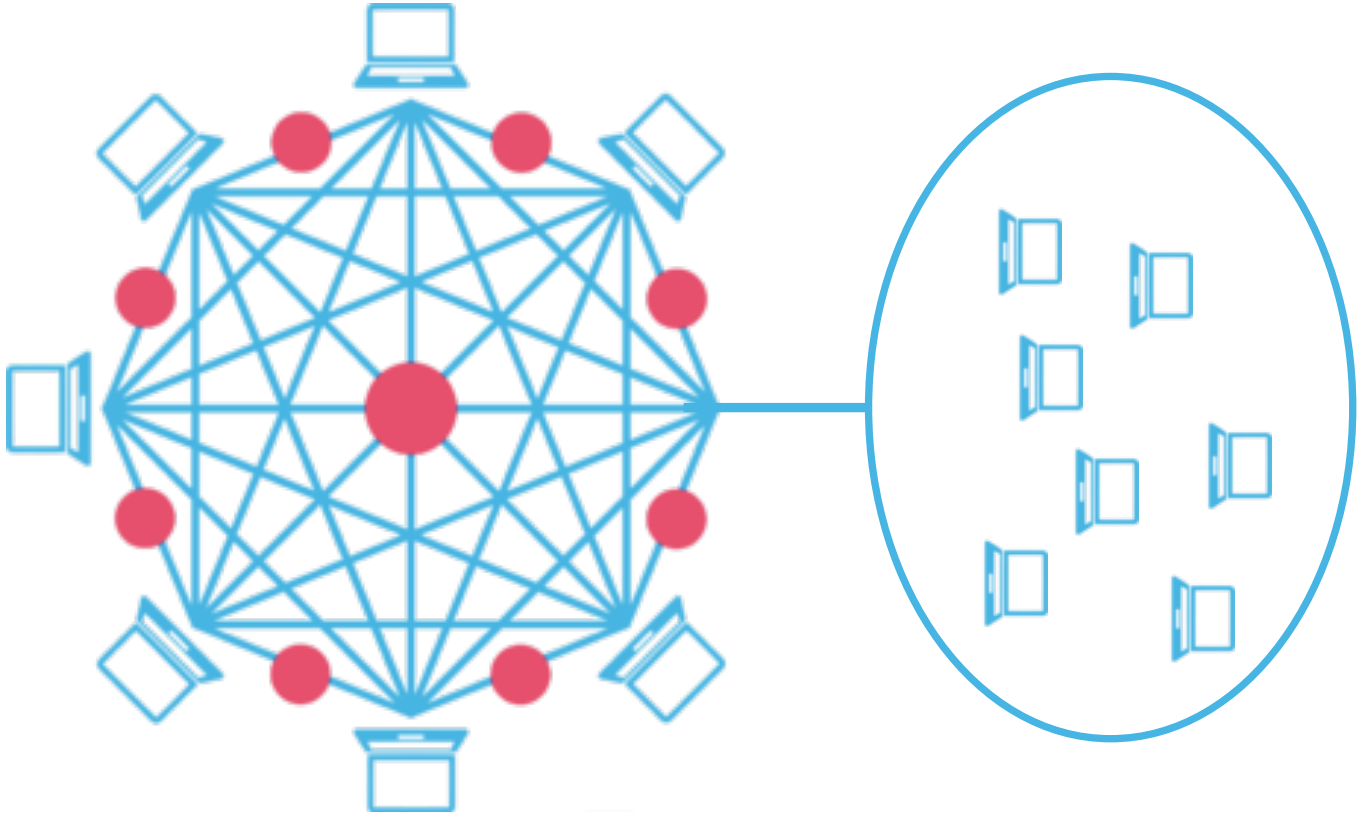


Image: https://d2omlh28jsv4r7.cloudfront.net/wp-content/uploads/2016/09/image-4-276x300.png

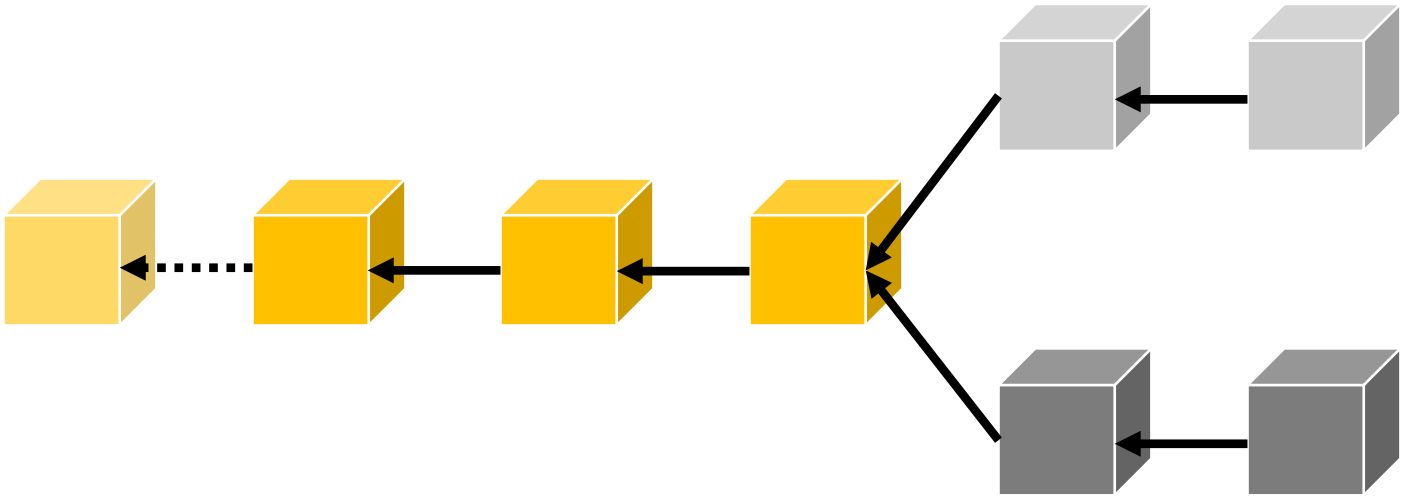
Blockchain: Mining



Mining Pools



Blockchain: Fork

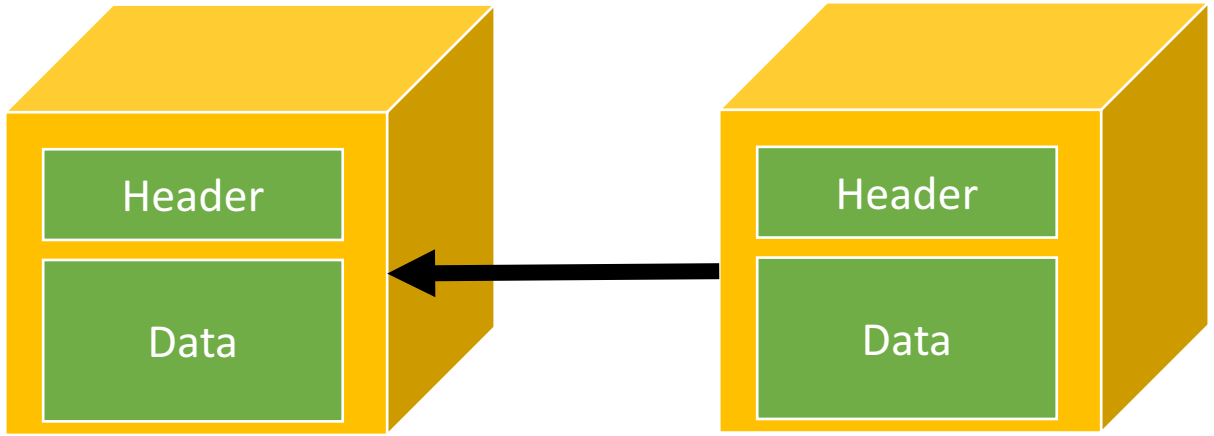


Bitcoin

- Digital currency
- Completely peer-to-peer
- Transactions verified by nodes
- Underlying blockchain acts as ledger
- Coins created by mining

Image: https://bitcoin.org/img/icons/opengraph.png

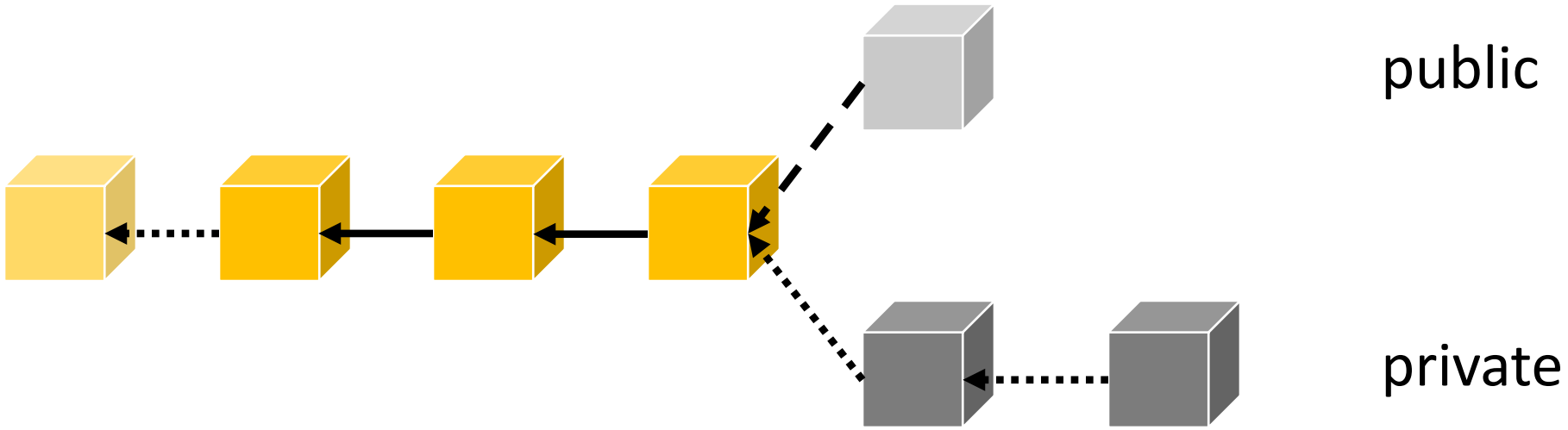
Bitcoin: Block



Header: Merkle root of data + hash(*previous header*) + Nonce

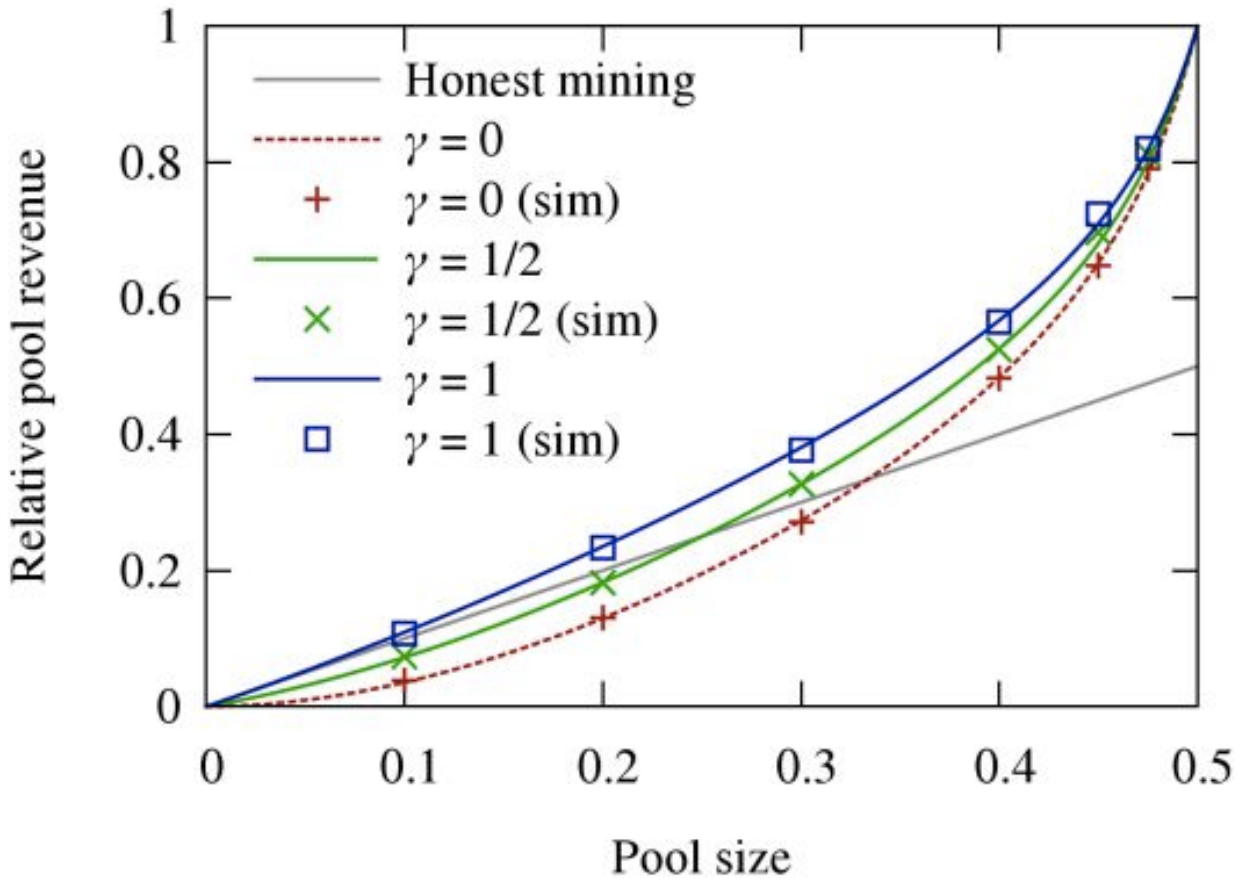
Data: Transactions

Selfish Mining



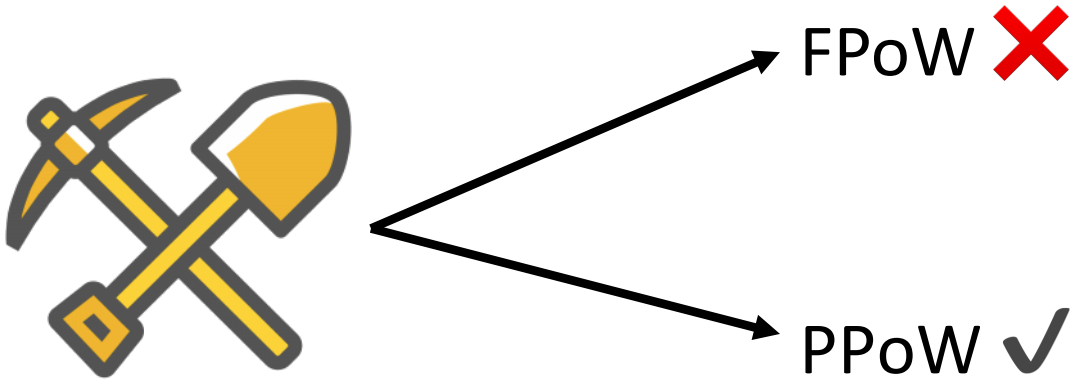
Create Fork intentionally

Selfish Mining: Reward



Majority Is Not Enough: Bitcoin Mining Is Vulnerable; Ittay Eyal and Emin Gun Sirer; 2014;

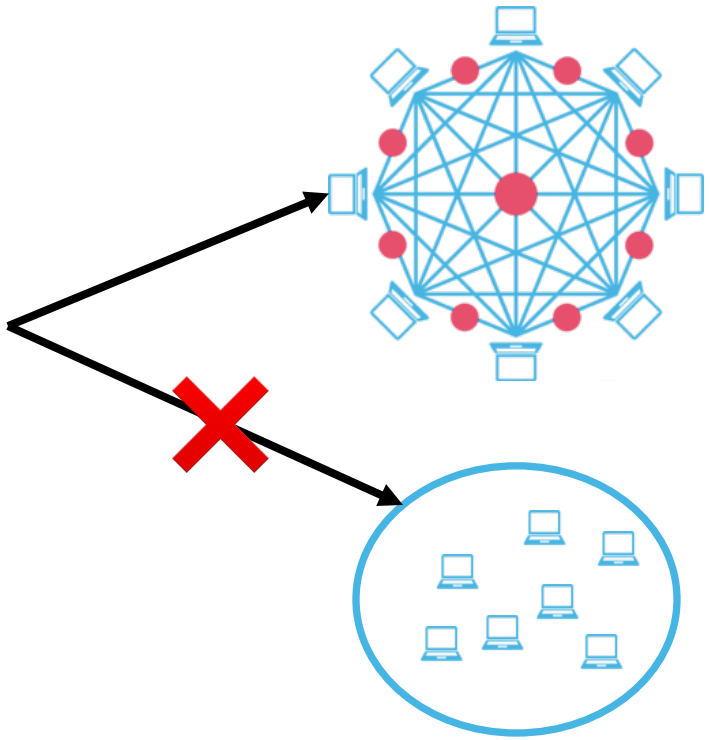
Block Withholding Attack



Loss for the attacked pool

Image: https://www.buybitcoinworldwide.com/wp-content/uploads/2017/02/i1000-_0000_Vector-Smart-Object-300x300.png

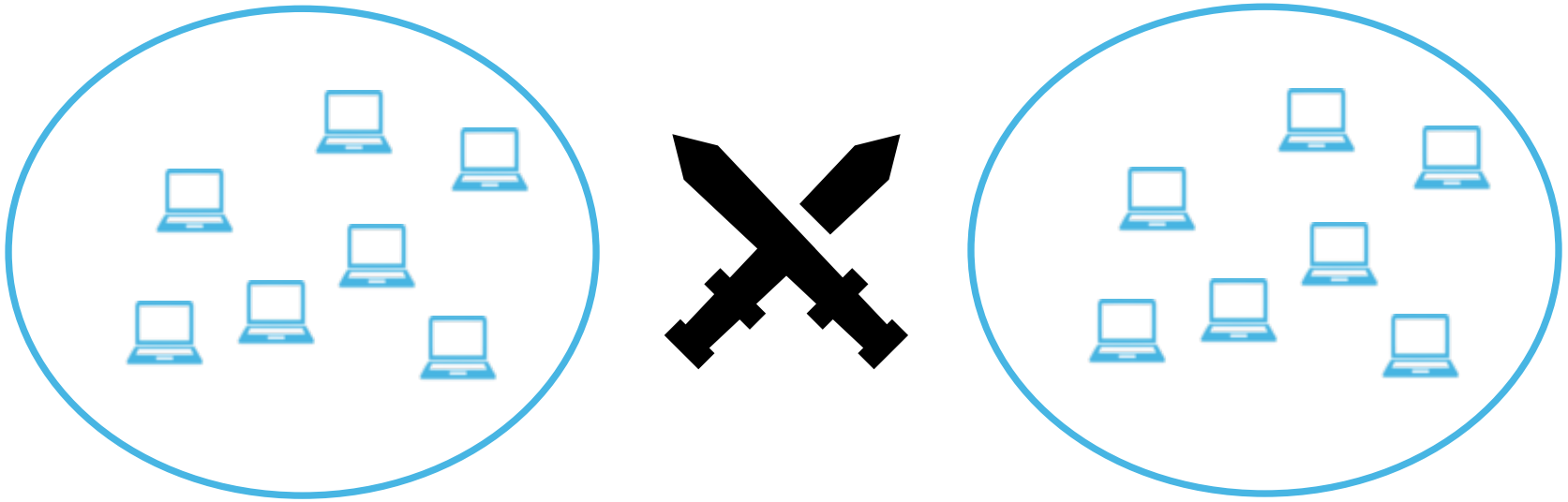
Block Withholding Attack



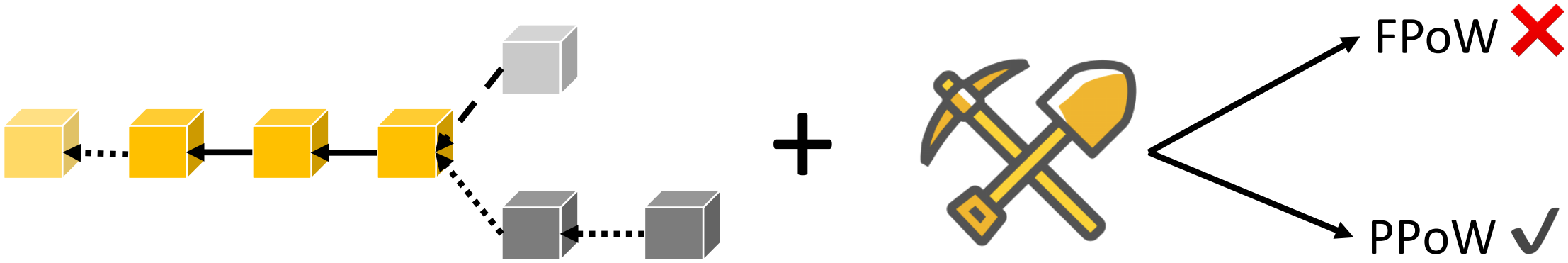
Loss for pool + reward for attacker

Image: https://www.buybitcoinworldwide.com/wp-content/uploads/2017/02/i1000-_0000_Vector-Smart-Object-300x300.png

BWH: Attacker’s Dilemma

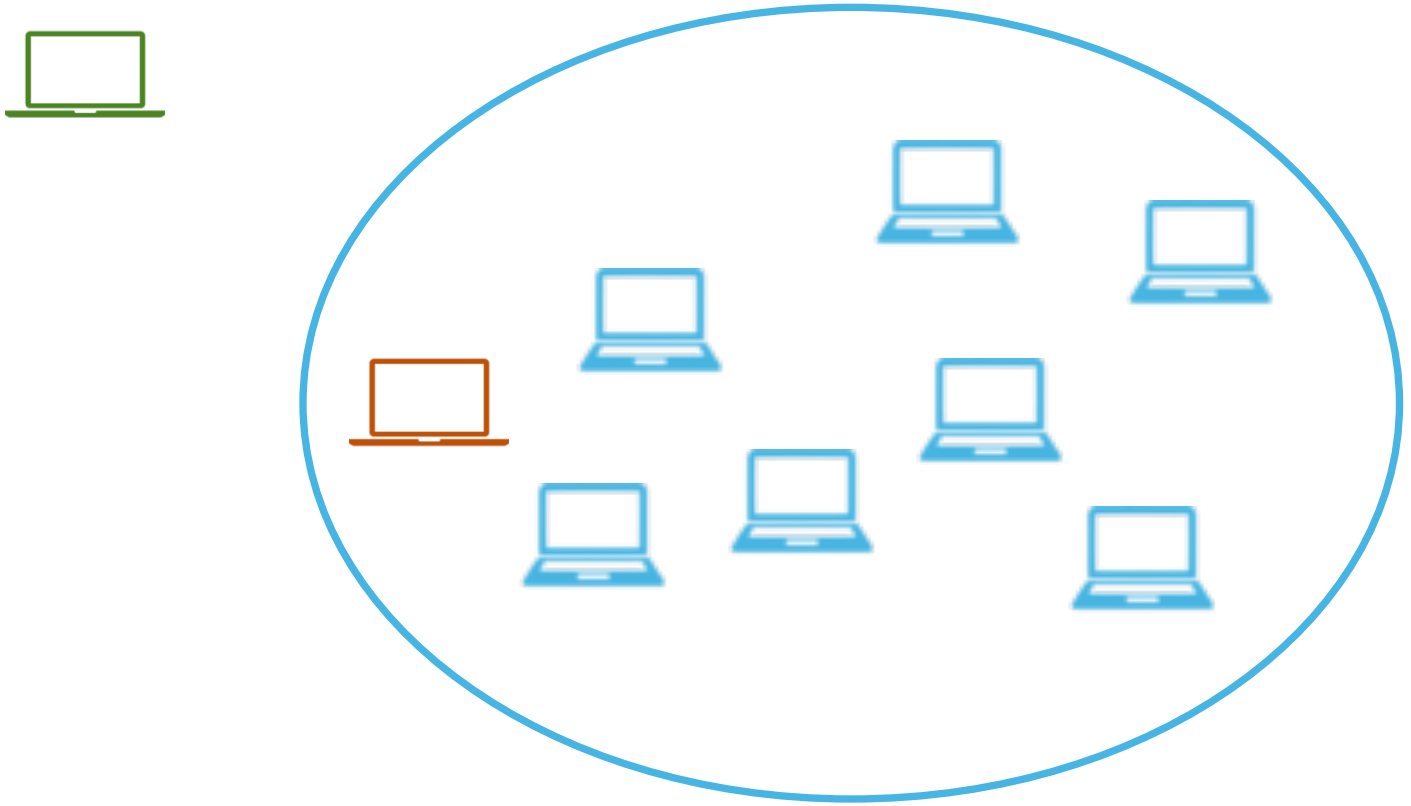


Fork After Withholding Attack



FAW: Attacking One Pool

FAW: Attacking One Pool



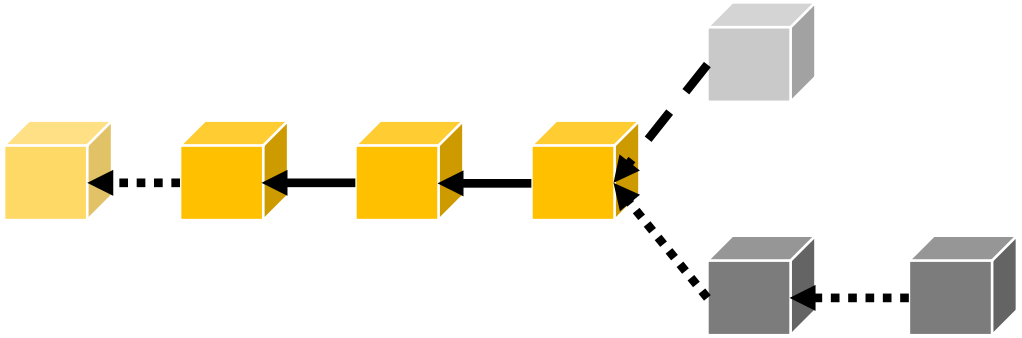
Innocent Miner

Infiltration Miner

no immediate FPoW propagation

FPoW holding + 2nd Block found

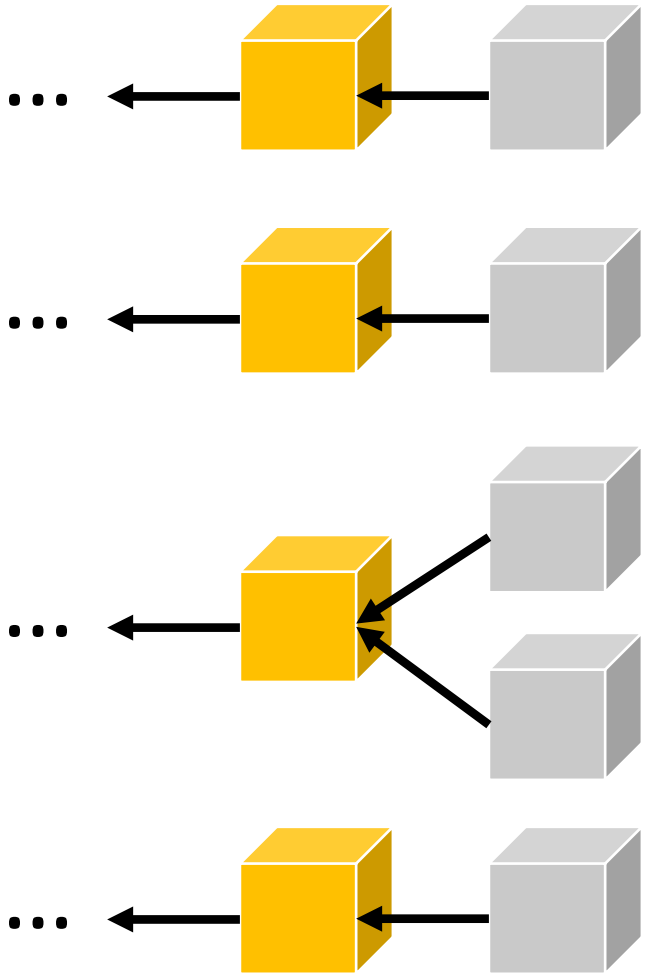
1) miner outside:



2) honest miner: FPoW ❌

3) own innocent miner: FPoW ❌

Reward Attacker



attacker innocent mining

honest miner in pool

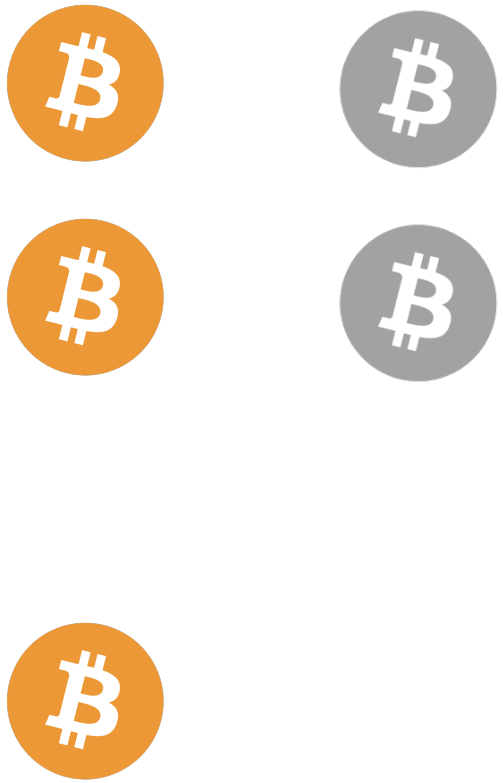
other miner

attacker infiltration

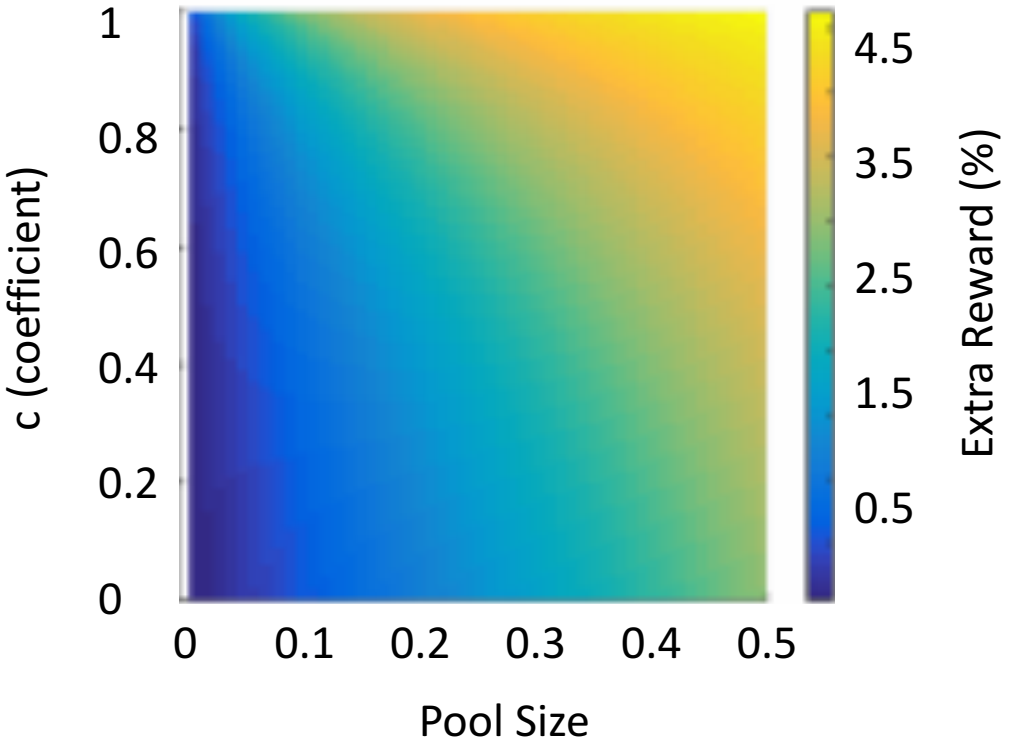
other miner

FAW

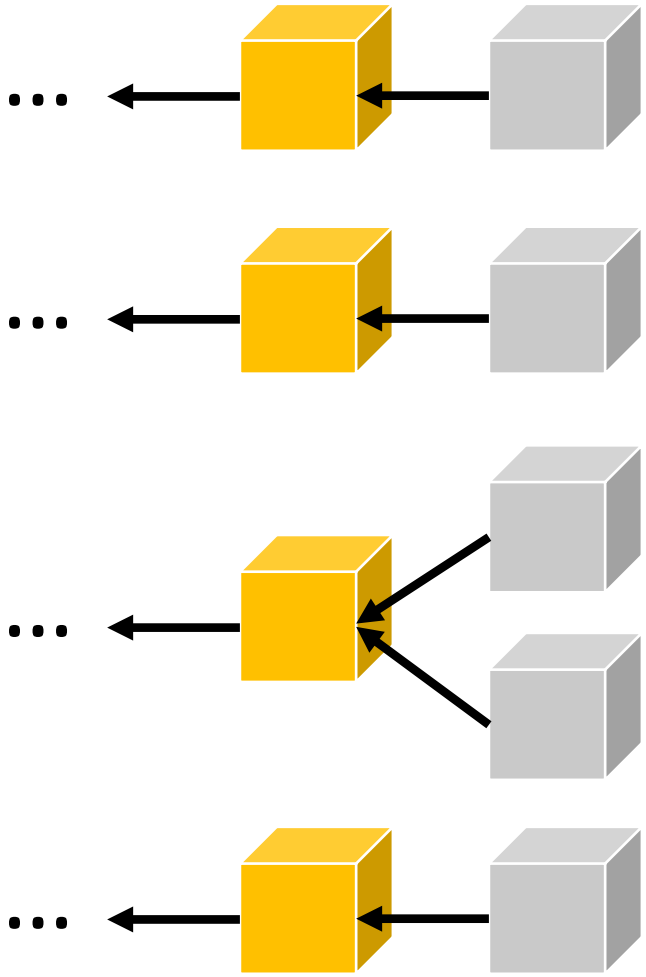
BWH



Reward Attacker



Reward Pool



attacker innocent mining

honest miner in pool

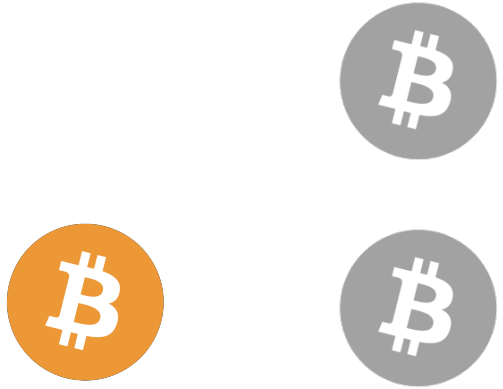
other miner

attacker infiltration

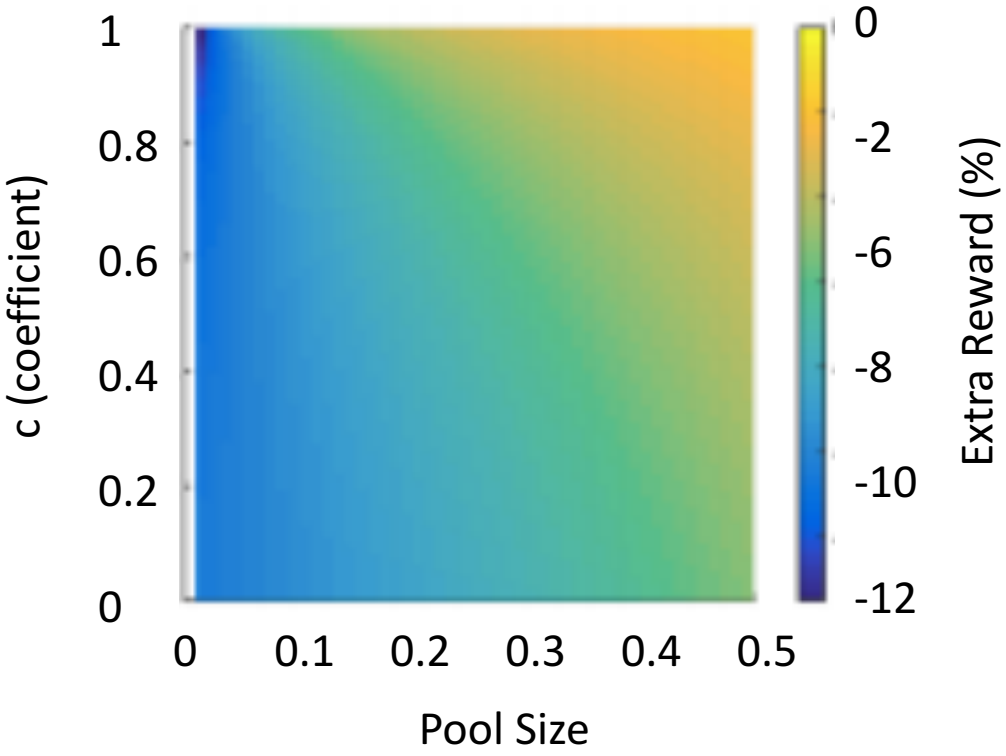
other miner

FAW

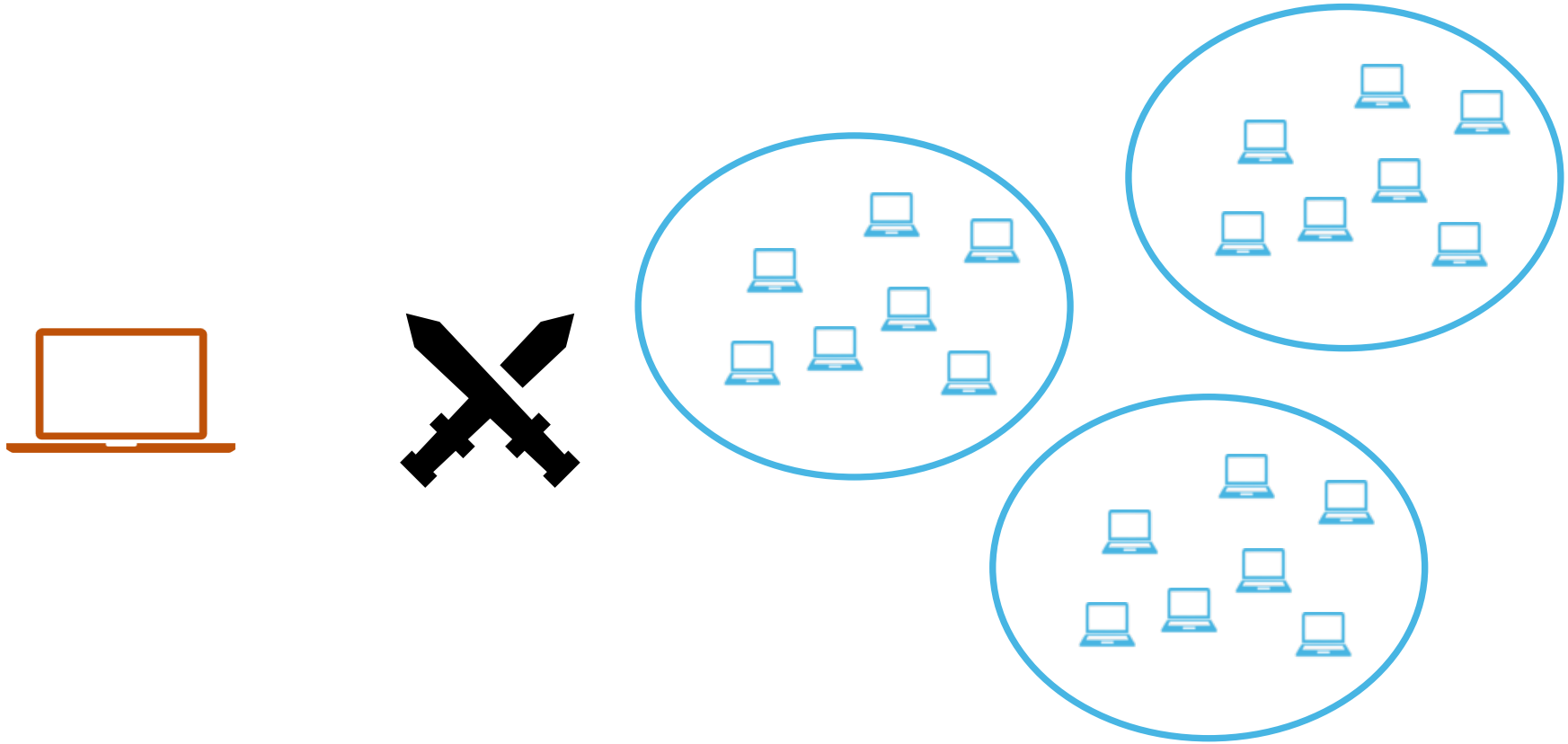
No Attack



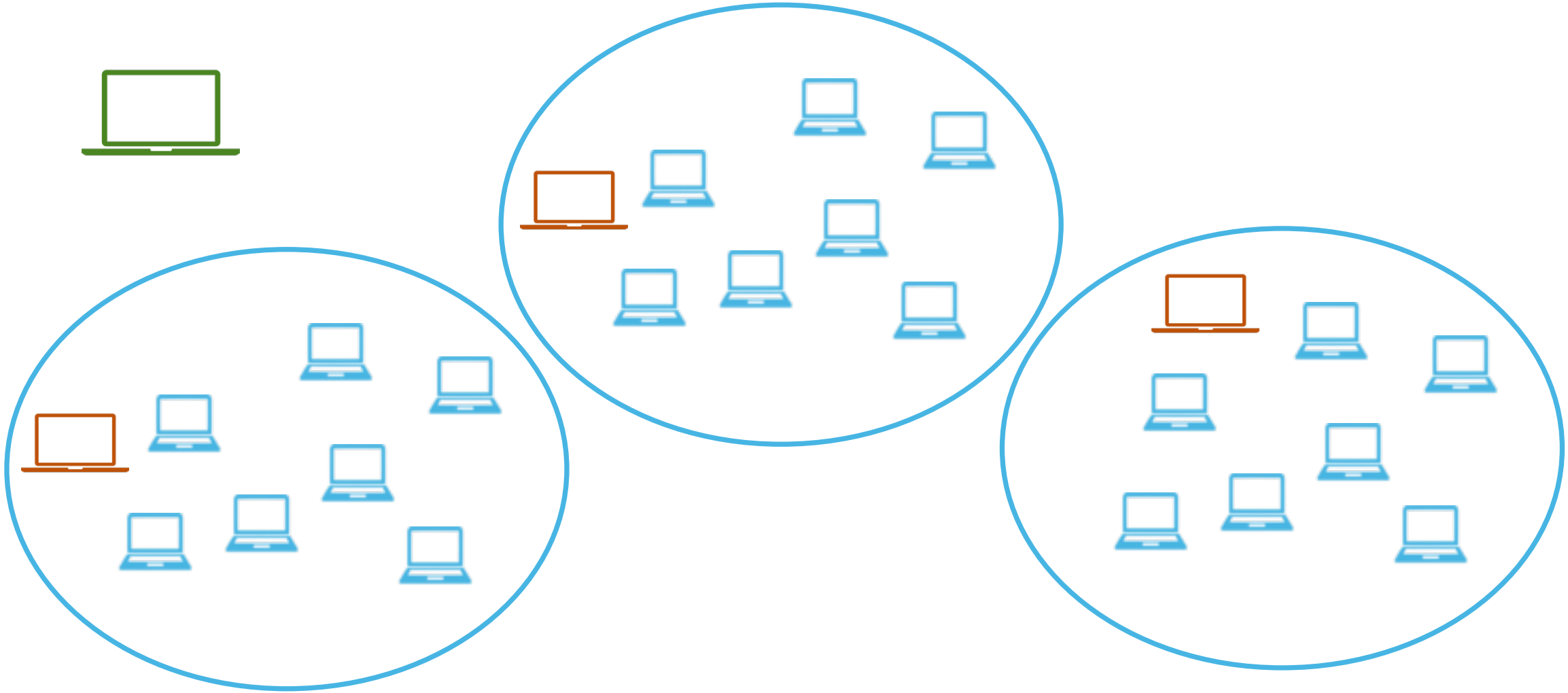
Pool Reward


1
0.8
0.6
0.4
0.2
0
c (coefficient)
0
0.1
0.2
0.3
0.4
0.5
Pool Size
0
-2
-6
-8
-10
-12
Extra Reward (%)

FAW: Against Multiple Pools



FAW: Against Multiple Pools



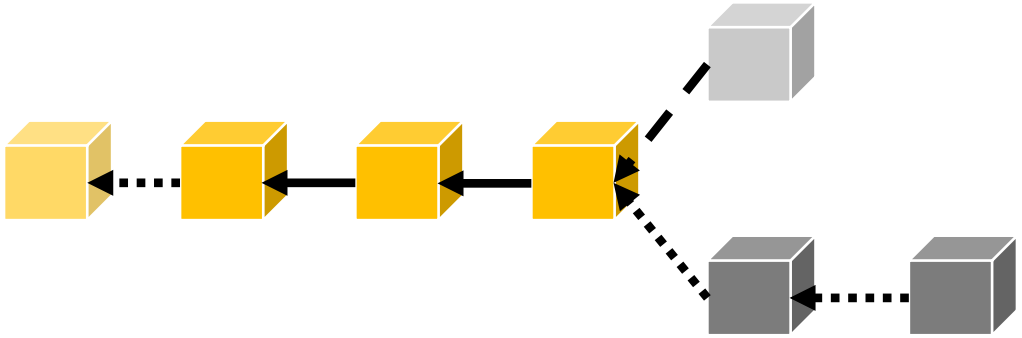
Innocent Miner

Infiltration Miner

no immediate FPoW propagation

FPoW holding + 2nd Block found

1) miner outside:



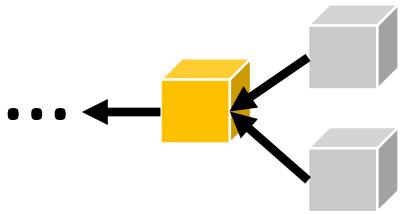
2) honest miner: FPoW ❌

3) own innocent miner: FPoW ❌

Reward Attacker

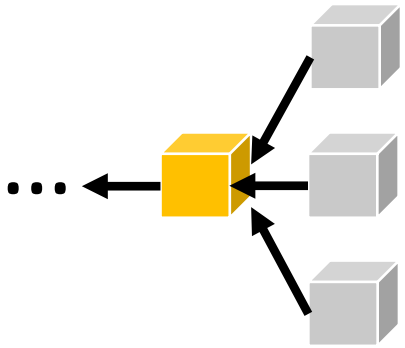
attacker innocent mining

honest miner in pool



other miner

attacker infiltration



other miner

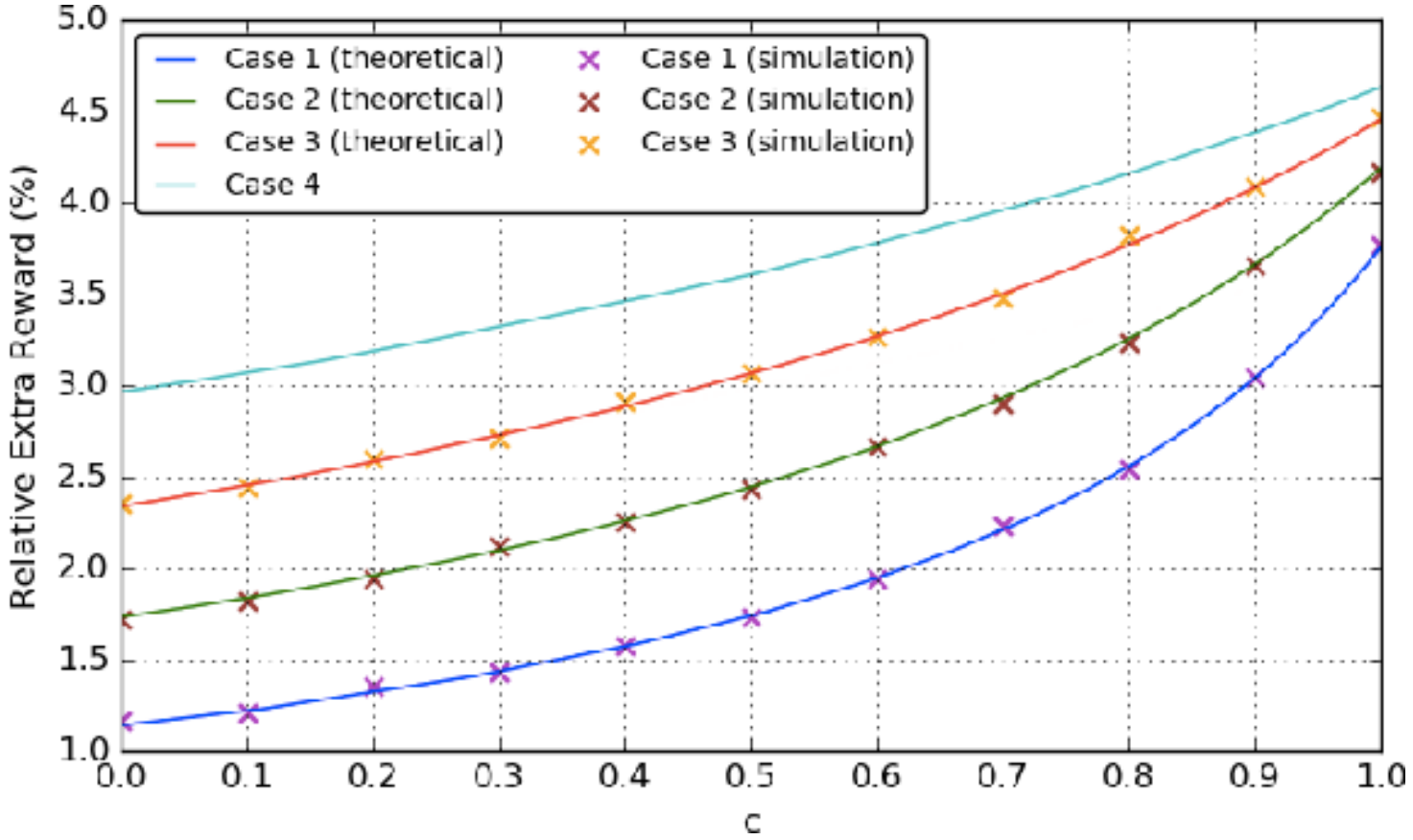
attacker infiltration pool 1

attacker infiltration pool 2

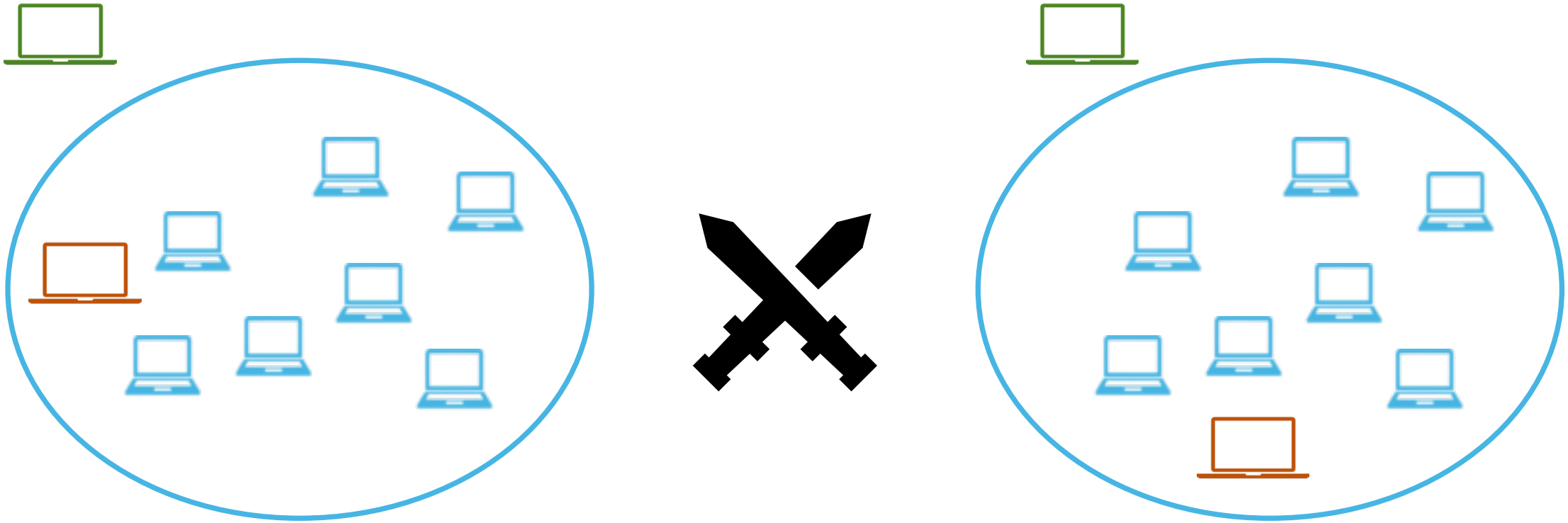
FAW

BWH

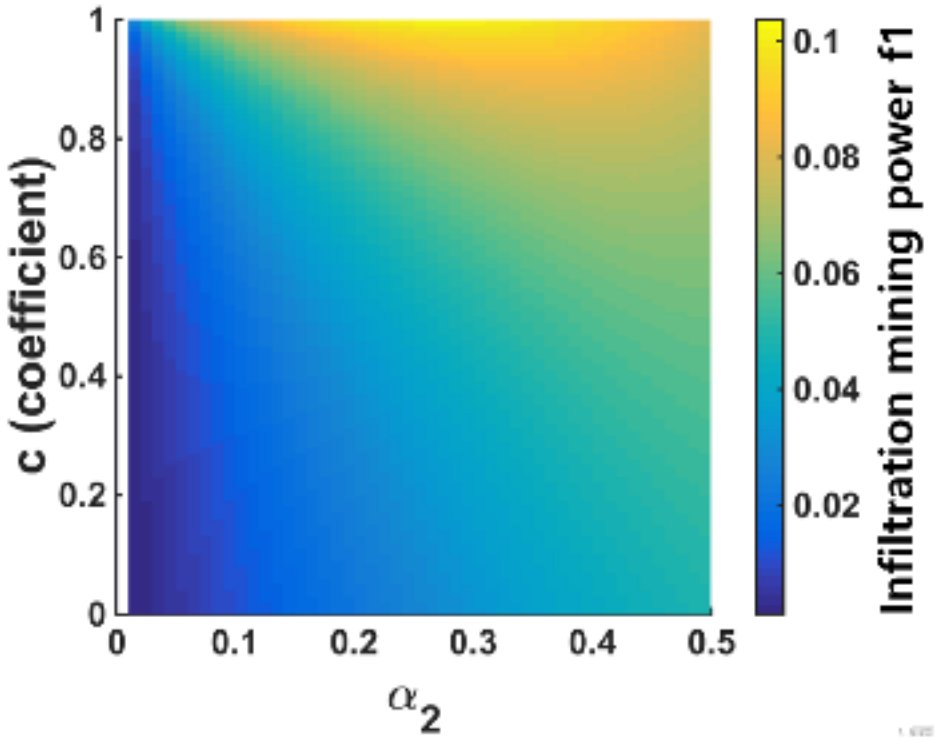
Reward Attacker



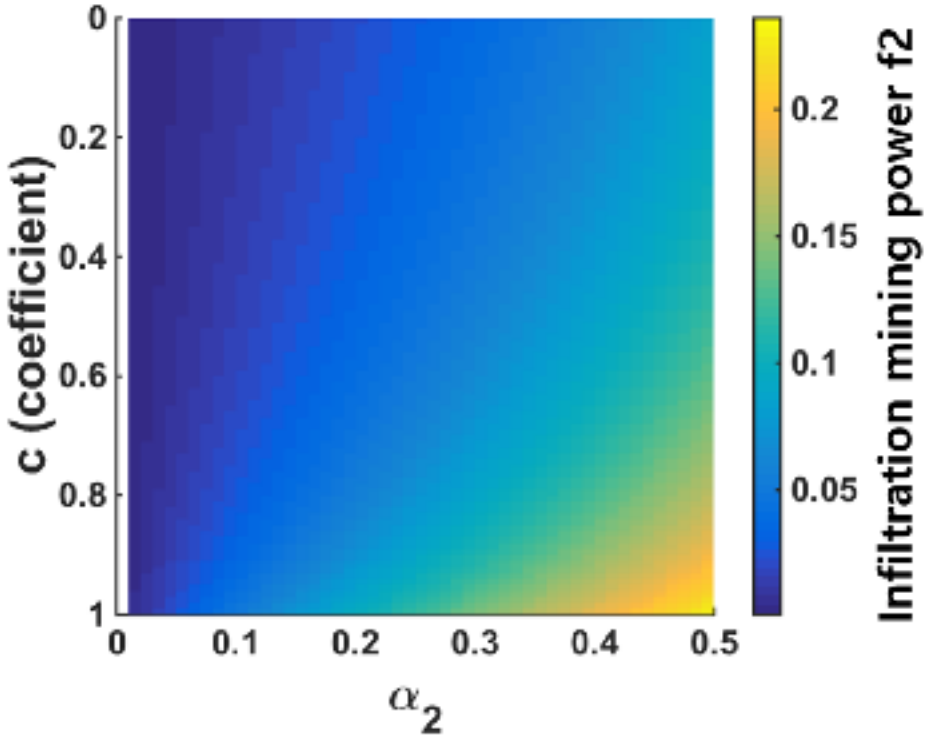
FAW: Attack Game



Attack Game

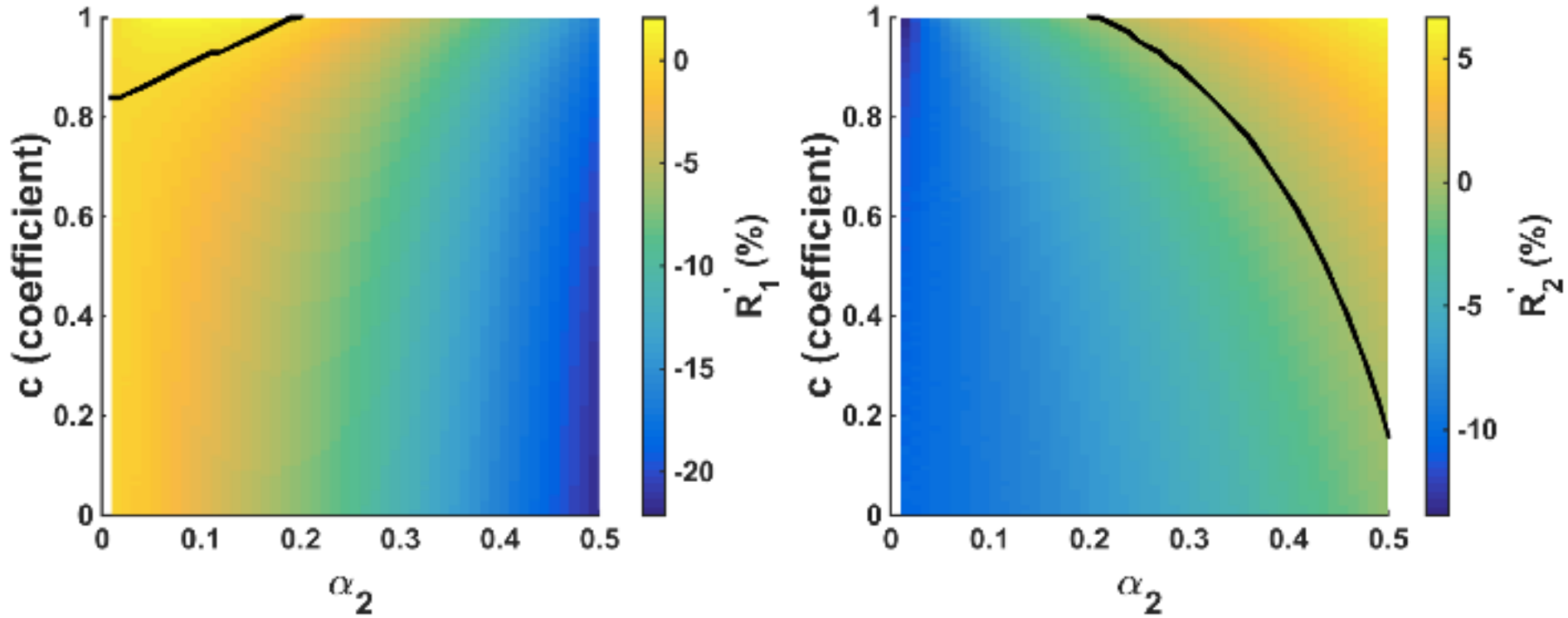


Pool 1 Infiltration Power

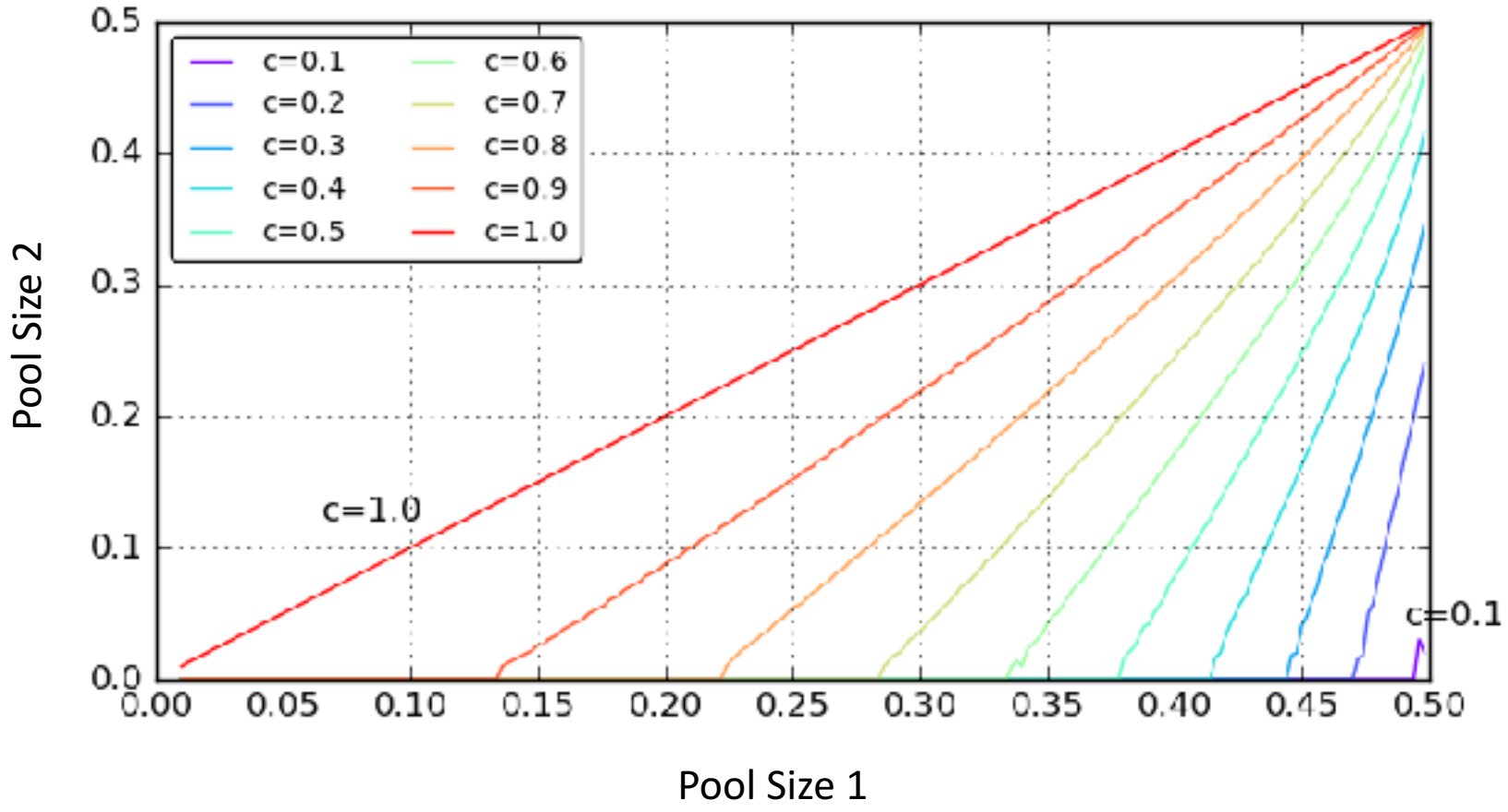


Pool 2 Infiltration Power

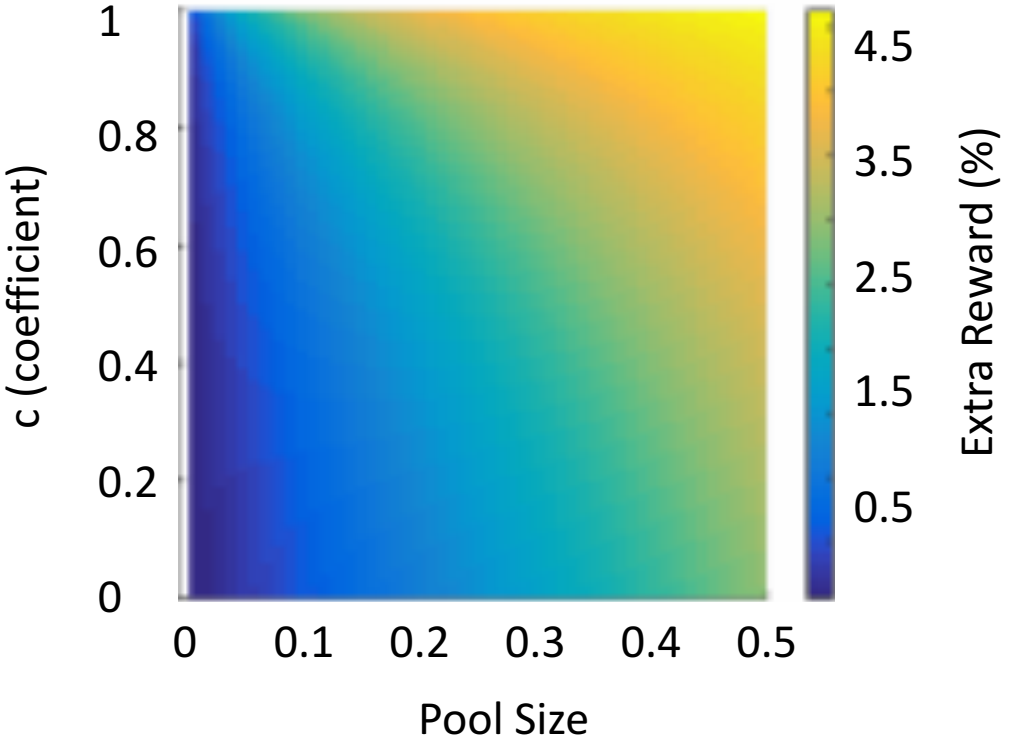
Attack Game

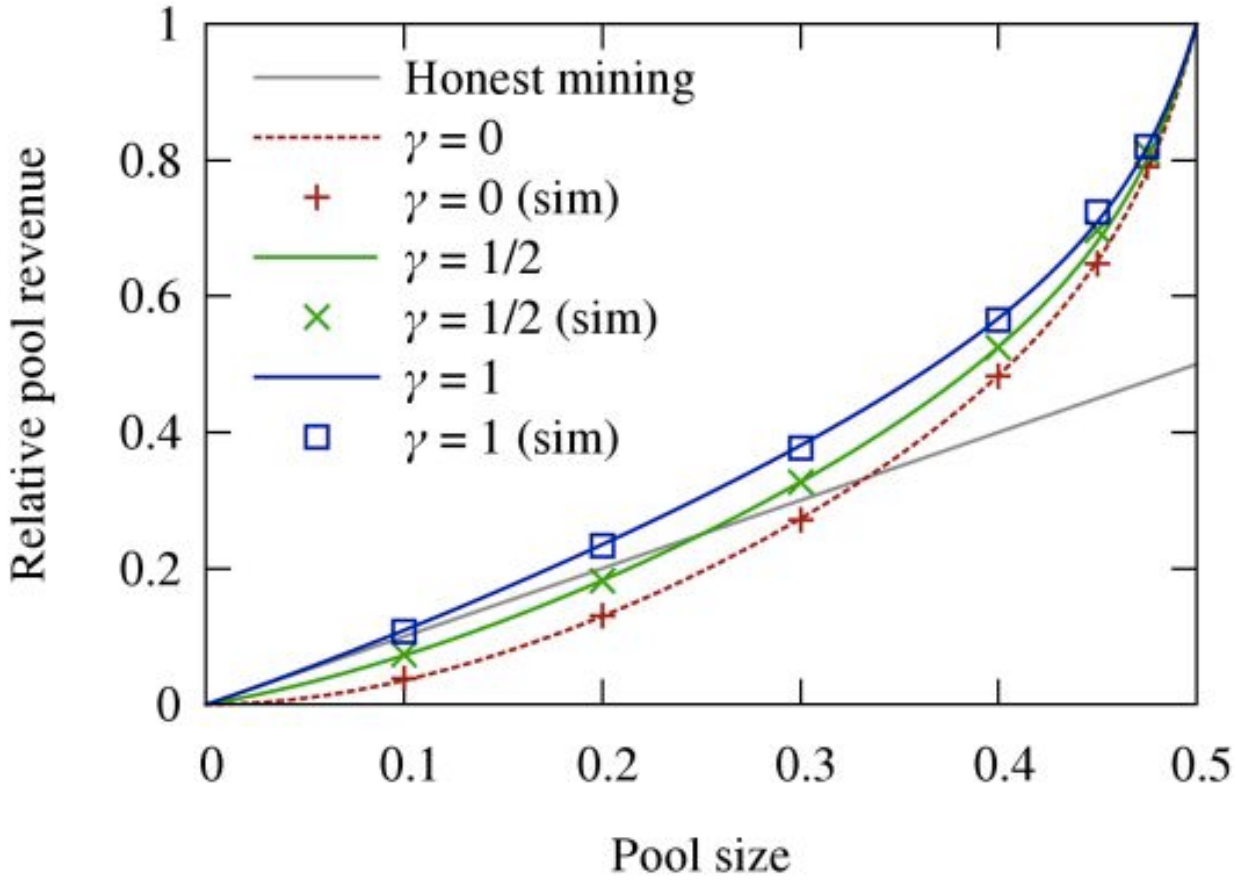

c (coefficient)
1
0.8
0.6
0.4
0.2
0
0
0.1
0.2
0.3
0.4
0.5
α_2
0
-5
-10
-15
-20
$R_1^{'}$ (%)
c (coefficient)
1
0.8
0.6
0.4
0.2
0
0
0.1
0.2
0.3
0.4
0.5
α_2
5
0
-5
-10
$R_2^{'}$ (%)

Network Capability

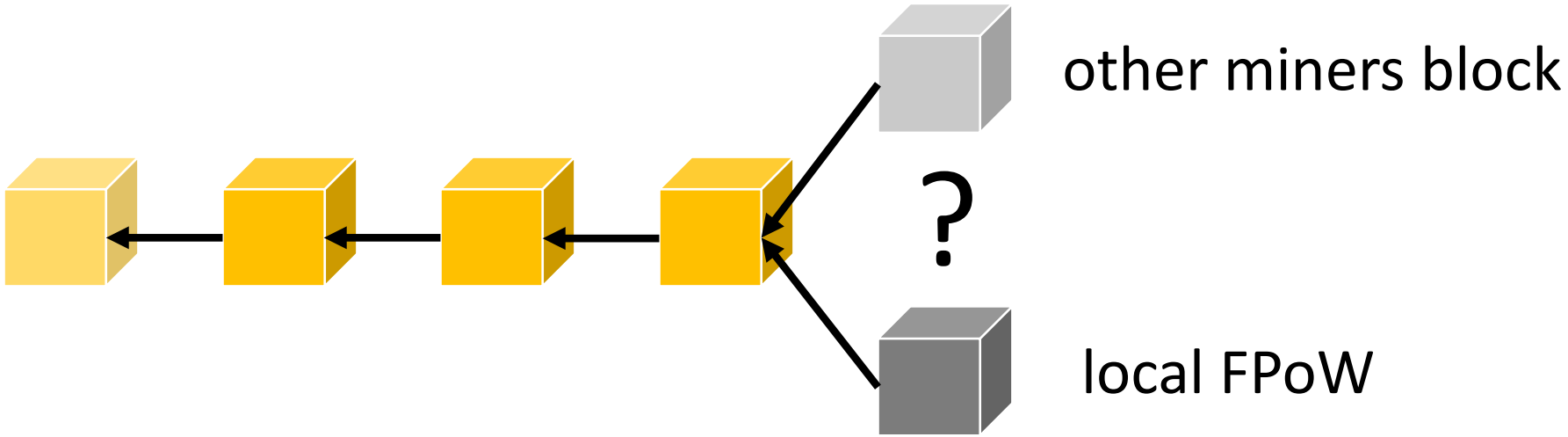


FAW vs Selfish Mining



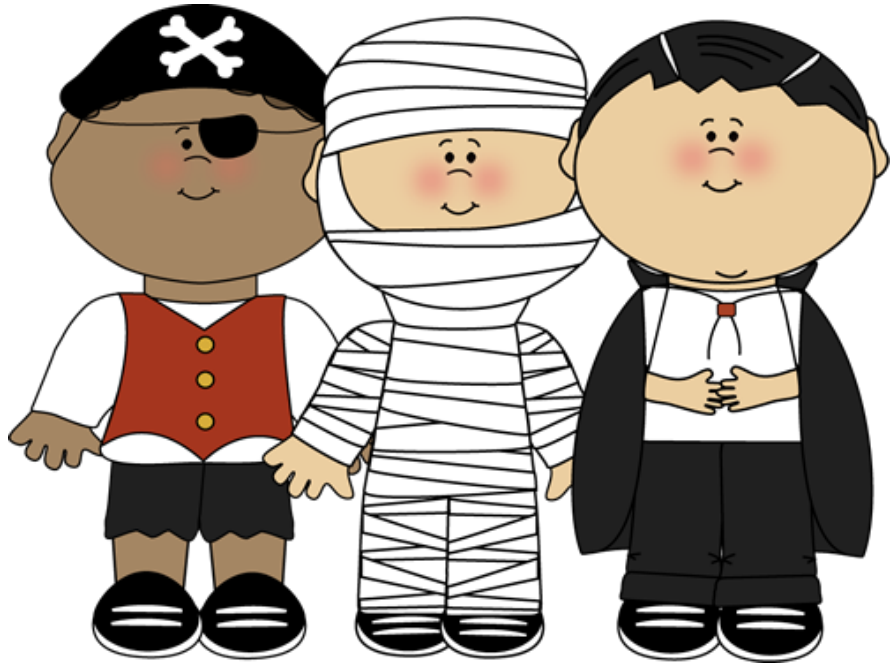


Rational Manager



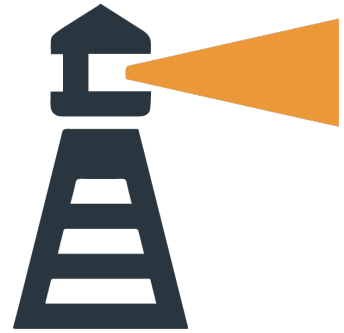
Detecting Attacks

VS



FAW: Countermeasures

- Two phase protocol
  Eyal, Rosenfeld
- beacon
- honey pot
  Eyal
- joining fee
  Eyal, Luu et al.
- bonus



Conclusions

- reward lower bounded by BWH
- rather small gain compared to selfish mining
- gain possible single miner / small pools
- no attackers dilemma
- attack harder to detect