Proof of Work and Blockchains

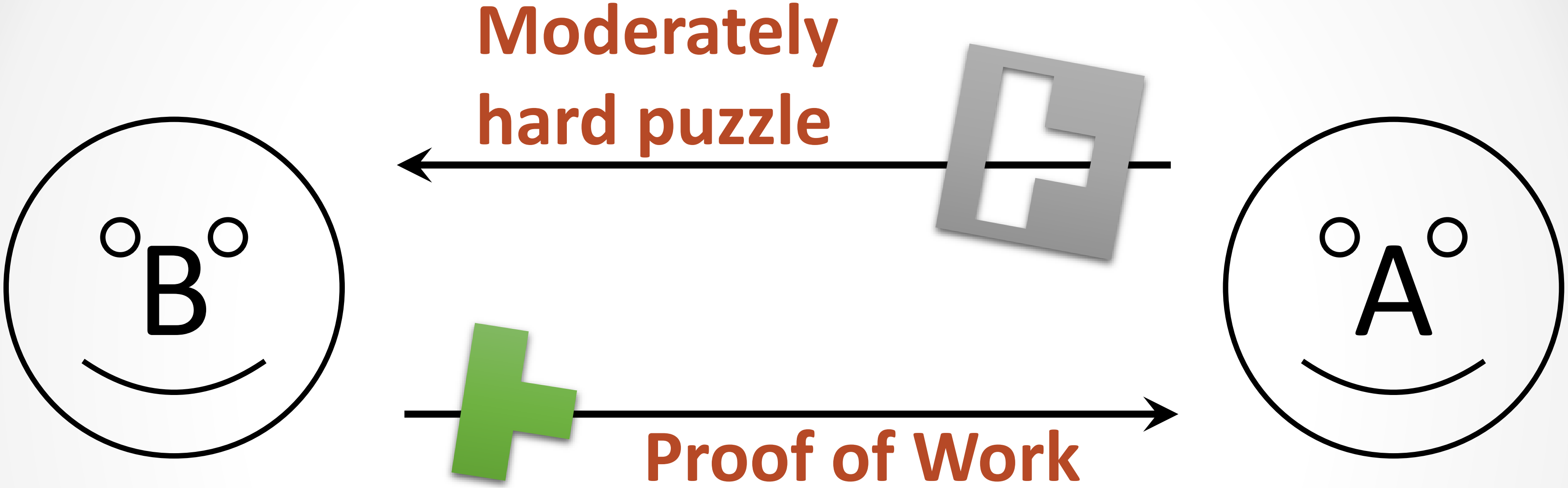
Ittay Eyal

Computer Science, Cornell University

The Initiative for Cryptocurrencies and Contracts (IC3)

Distributed Cryptocurrencies and Consensus Ledgers, July 2017

Proof of Work



Moderately hard puzzle

Proof of Work

- Challenger provides puzzle
- Solver expends resources to solve puzzle

Proof of Work

A variety of uses [Jakobbson+Juels'99]

- Spam protection [Dwork+Naor'92]
- construction of digital time capsules [Goldschlag+Stubblebine'89, Rivest+'96]
- Server access metering [Franklin+Malkhi'97]
- (D)DoS protection [Juels+Brainard'99]
- Digital money minting [Rivest+Shamir'01]
- Sybil protection [Apsnes'15]

… but botnets?

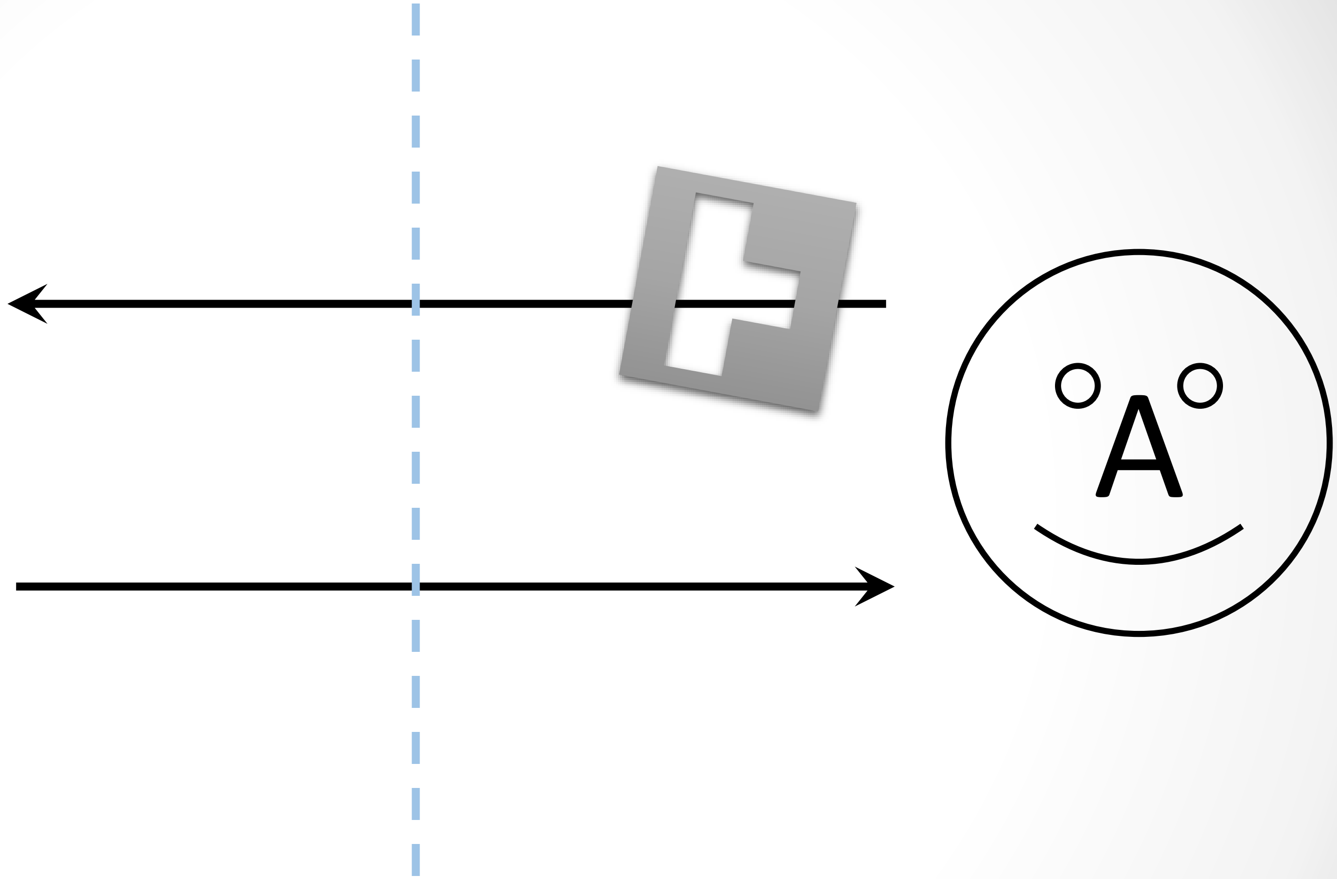
How Hard?

Phone?

Laptop?

Server?

Datacenter?



PoW for Blockchains

- Bitcoin [Nakamoto’08]:

  PoW for Sybil protection,

  With a trick:

  direct monetary compensation

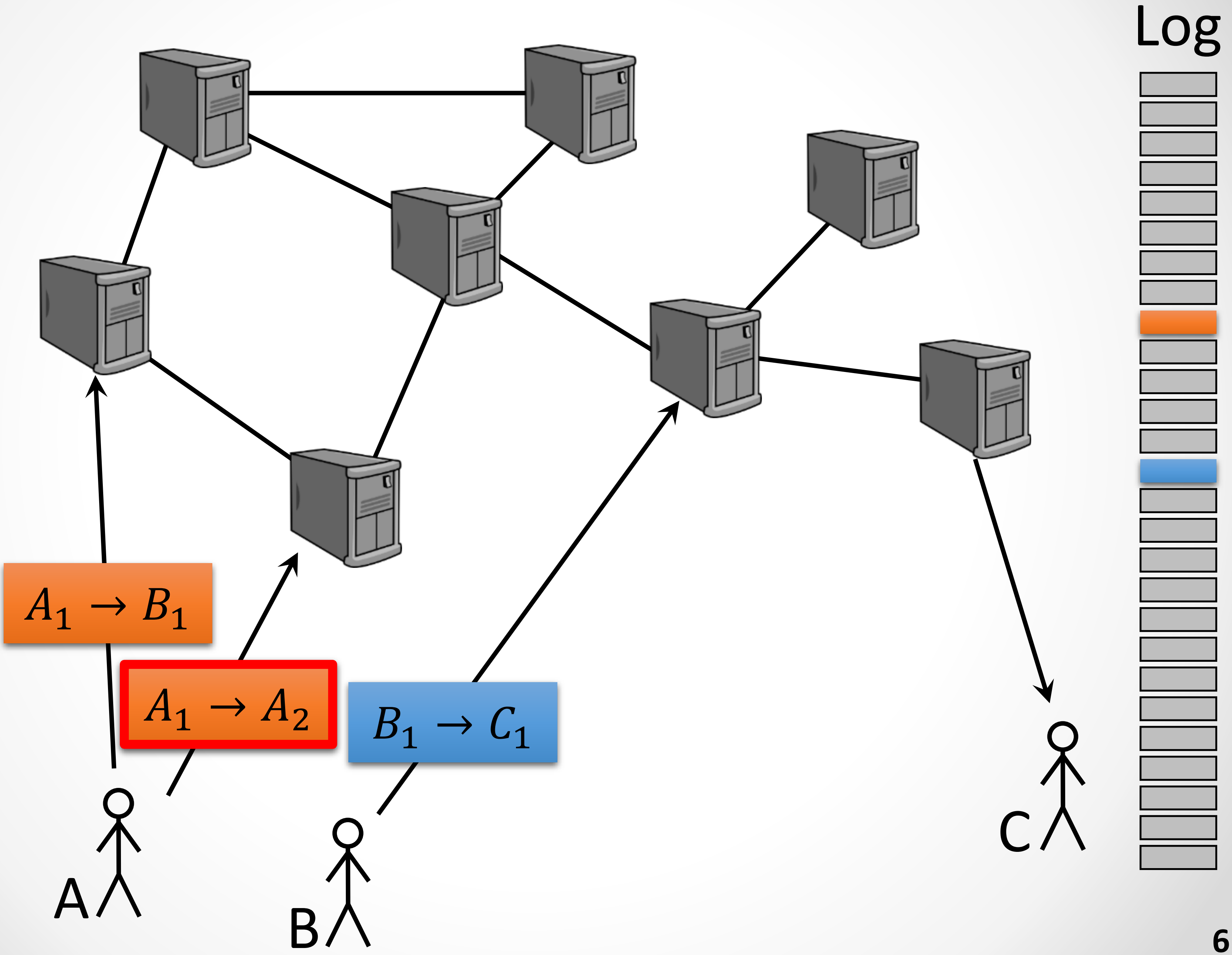
- The result:

  Wildly successful and incredibly robust

  But also:

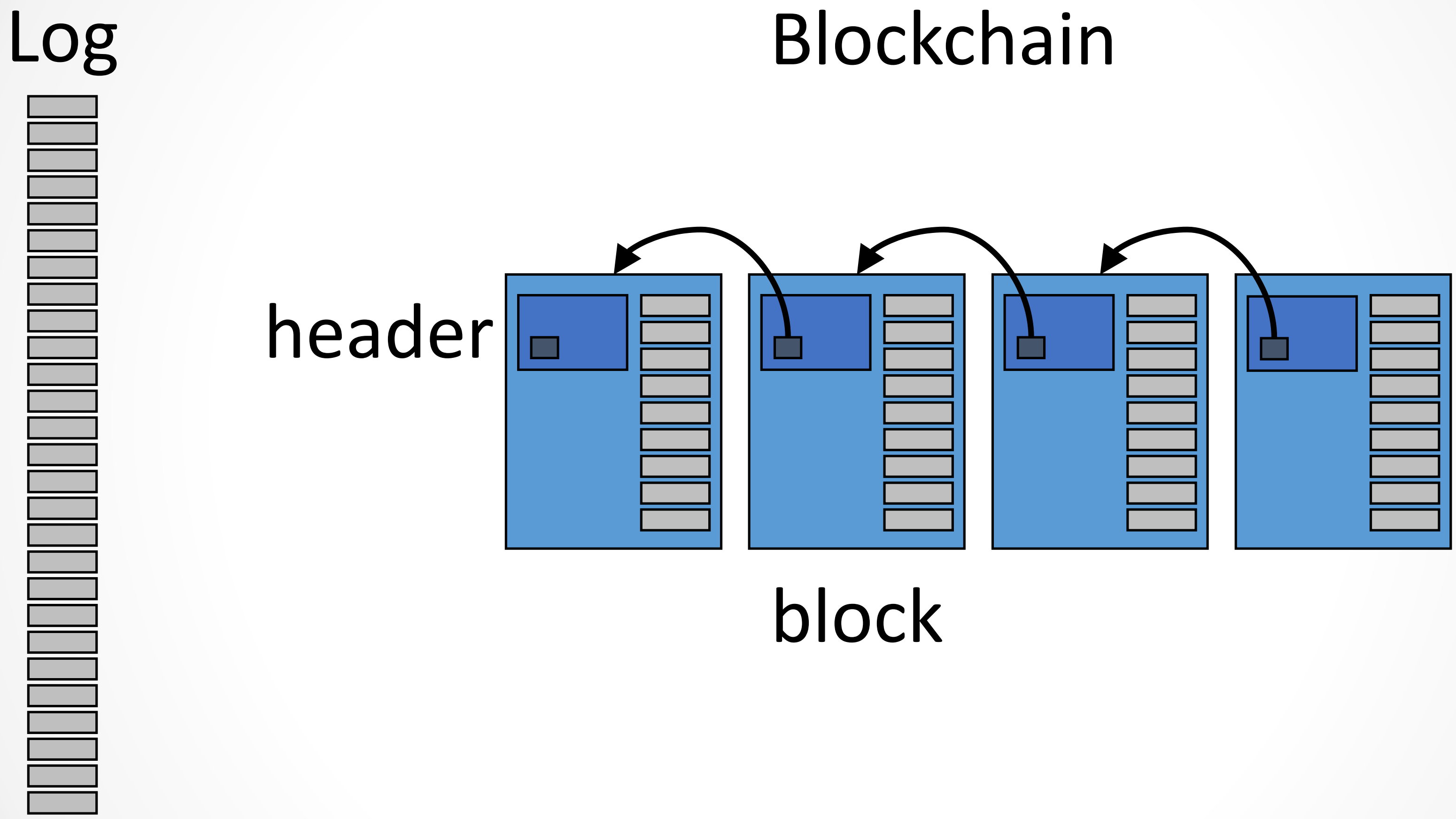
  some surprising properties

A Replicated State Machine



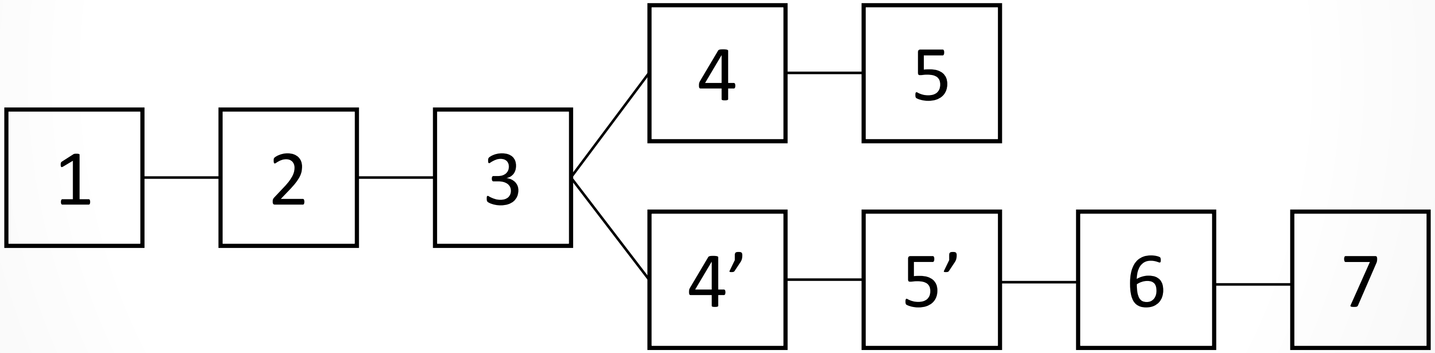
Ittay Eyal, July '16

The Blockchain



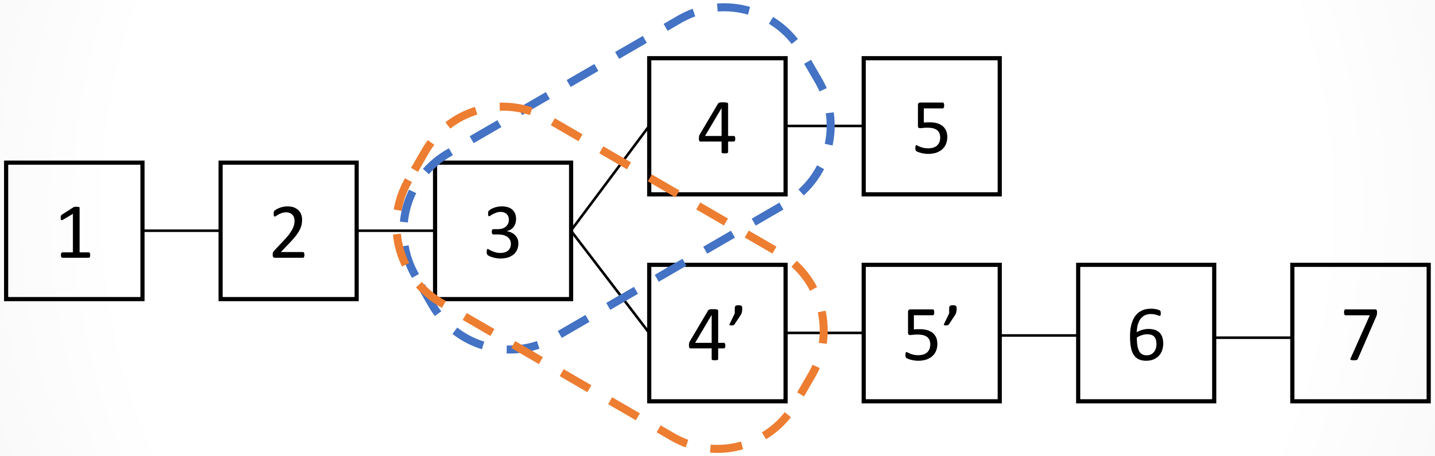
PoW for Blockchains

- Log in blocks
- Solve puzzle to add block
- Get prize per block
- On a fork (a natural event), stronger side wins



Basic Operation

- Puzzle is a function of current and previous block. (e.g., their hash smaller than target)



- Real-world participation cost
- Burn real-world resources, committing to a state machine history

PoW in a Blockchain

- Block every set interval (10min, 15sec)
- Automatically adjusting difficulty
  ==> a lottery of sorts
  ==> bustling mining industry

PoW in a Blockchain

- Block every set interval (10min, 15sec)
- Automatically adjusting difficulty

  ==> a lottery of sorts

  ==> bustling mining industry

Bitcoin

prize decay ==> FOMO at work

Also finite supply, deflation

Waste?

- Real-world waste
  - Compute power (sha256 ^2)
    Really power (Watts)
  - Less useless (Primecoin)
  - Storage [Miller+’14]
  - Hardware (PoET)

- No real-world waste
  - Permissioned (Hyperledger, Stellar), or
  - Pending formal discussion (Proof of Stake)

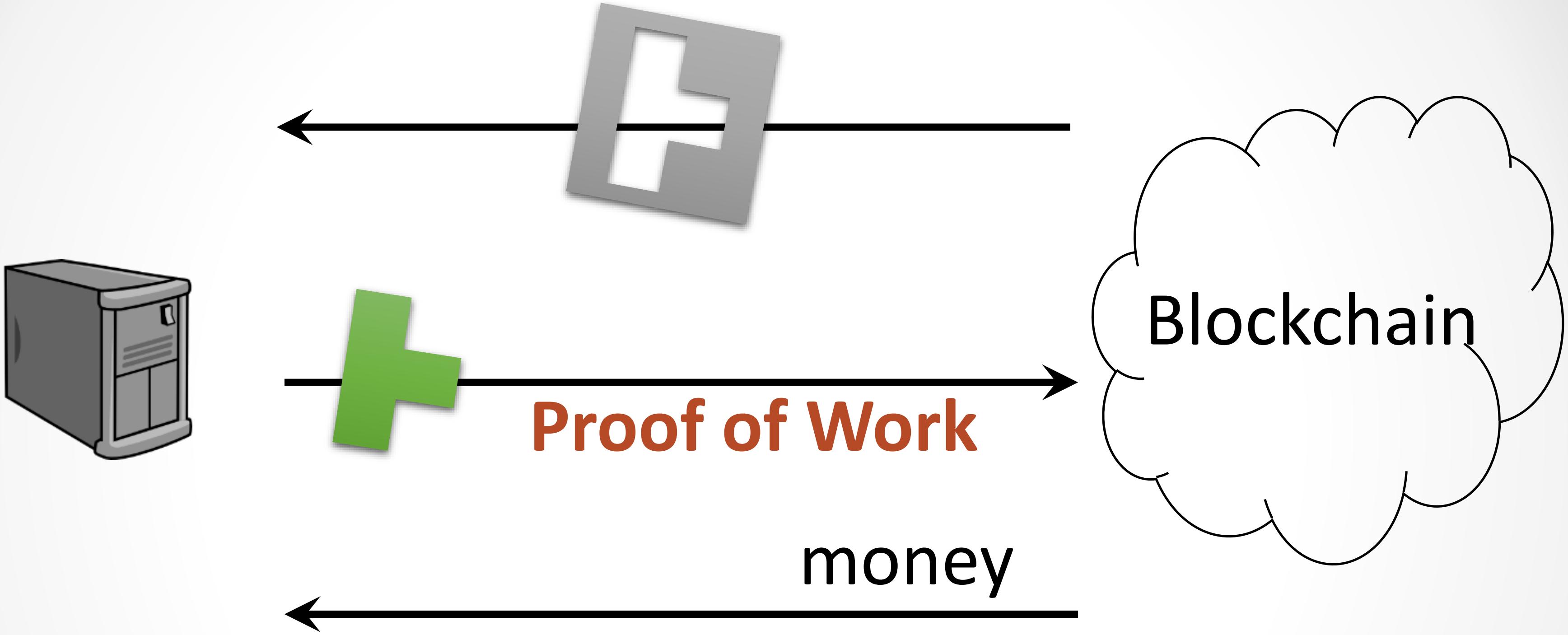
Resilience

- Surprisingly stable
  - Strategic mining
    (Selfish mining etc. not seen in the wild)

- Few blockchain alternatives
  - GHOST +variants (Ethereum, DECOR) [Sompolinsky+Zohar’15, Lewenberg+’15]
  - Bitcoin-NG +variants (Hybrid consensus, Byzcoin)

Pooled Mining

Blockchain Mining



Blockchain

Proof of Work

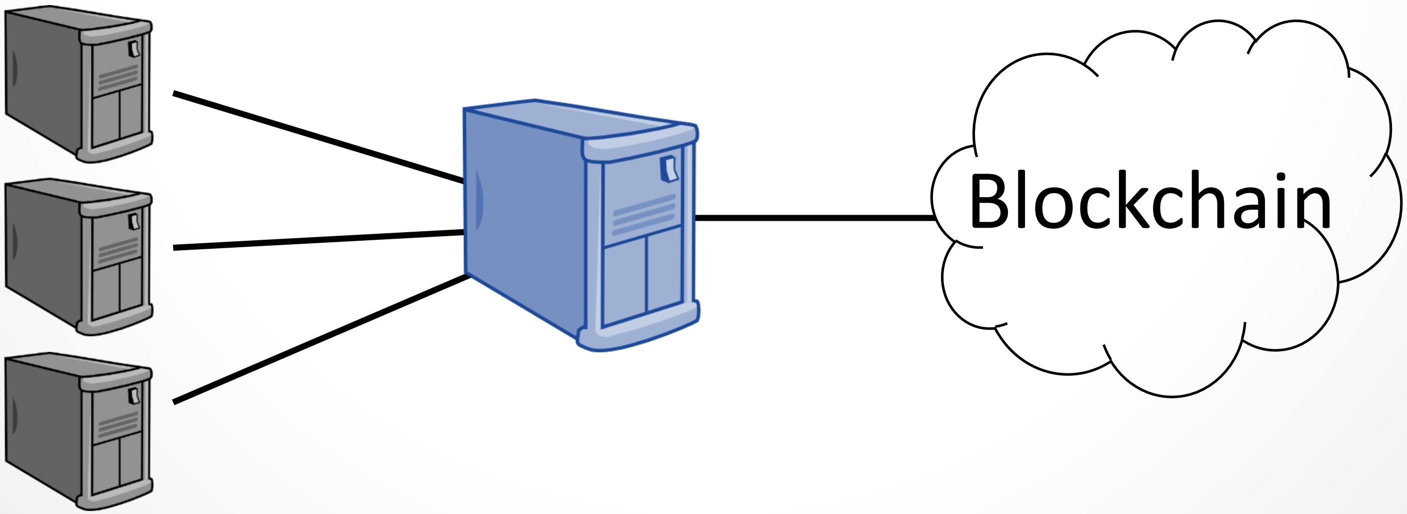
money

Constant rate : globally updated Difficulty

Pooled Mining

Many miners
Constant PoW rate } ⇒ Long time to win

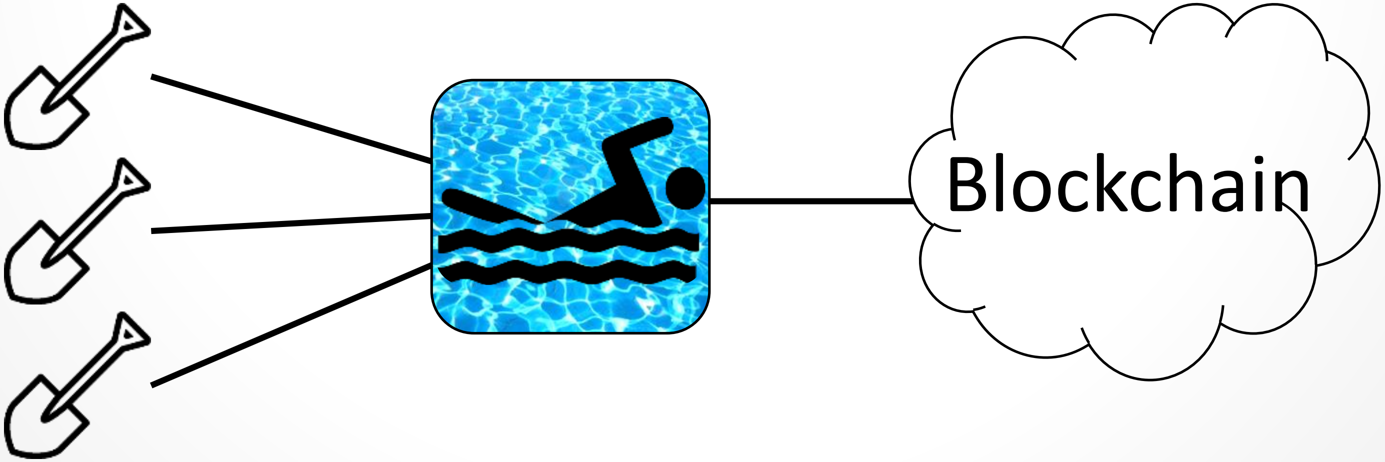
Miners form **pools**



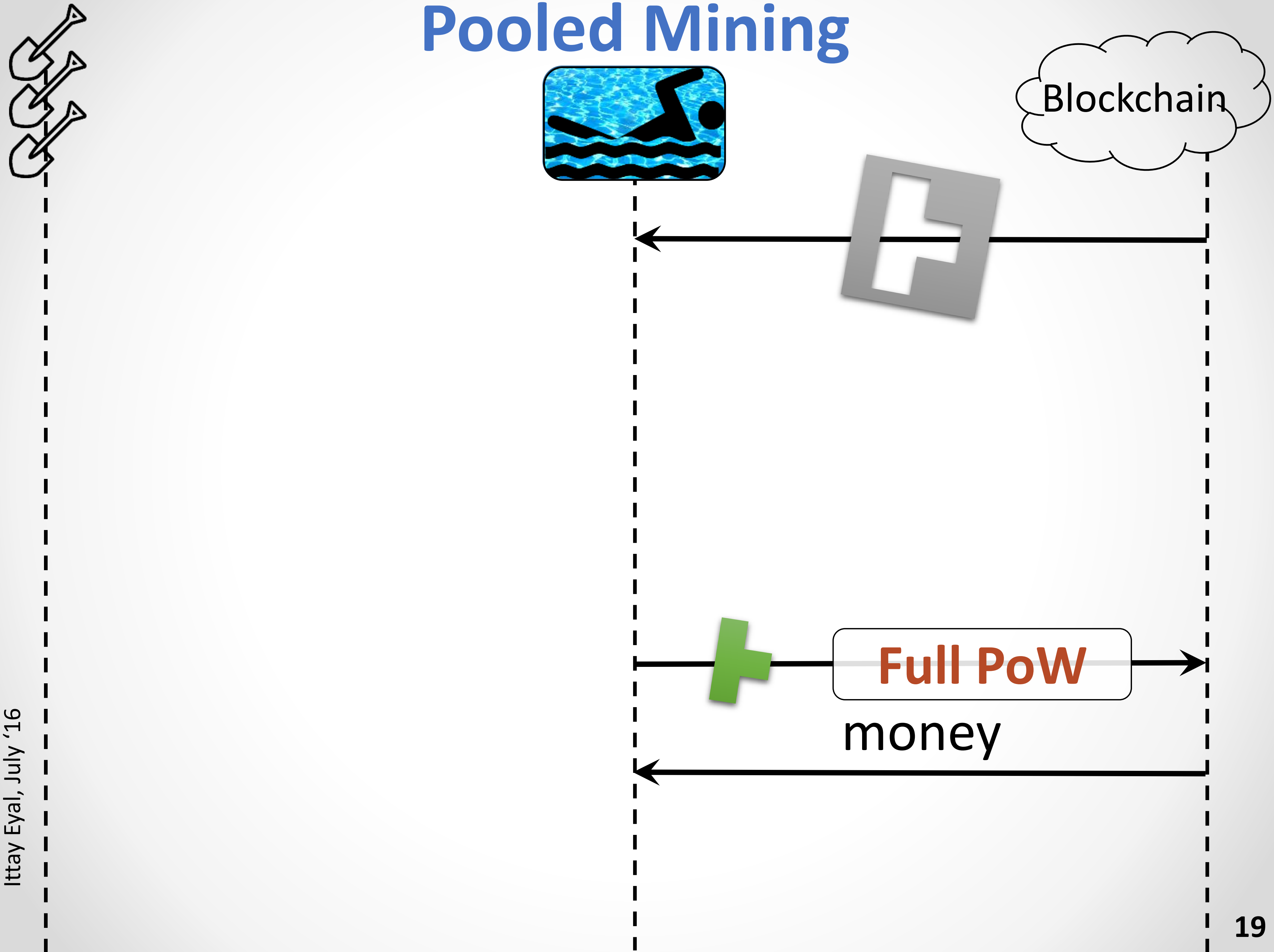
Pooled Mining

Many miners
Constant PoW rate } ⇨ Long time to win

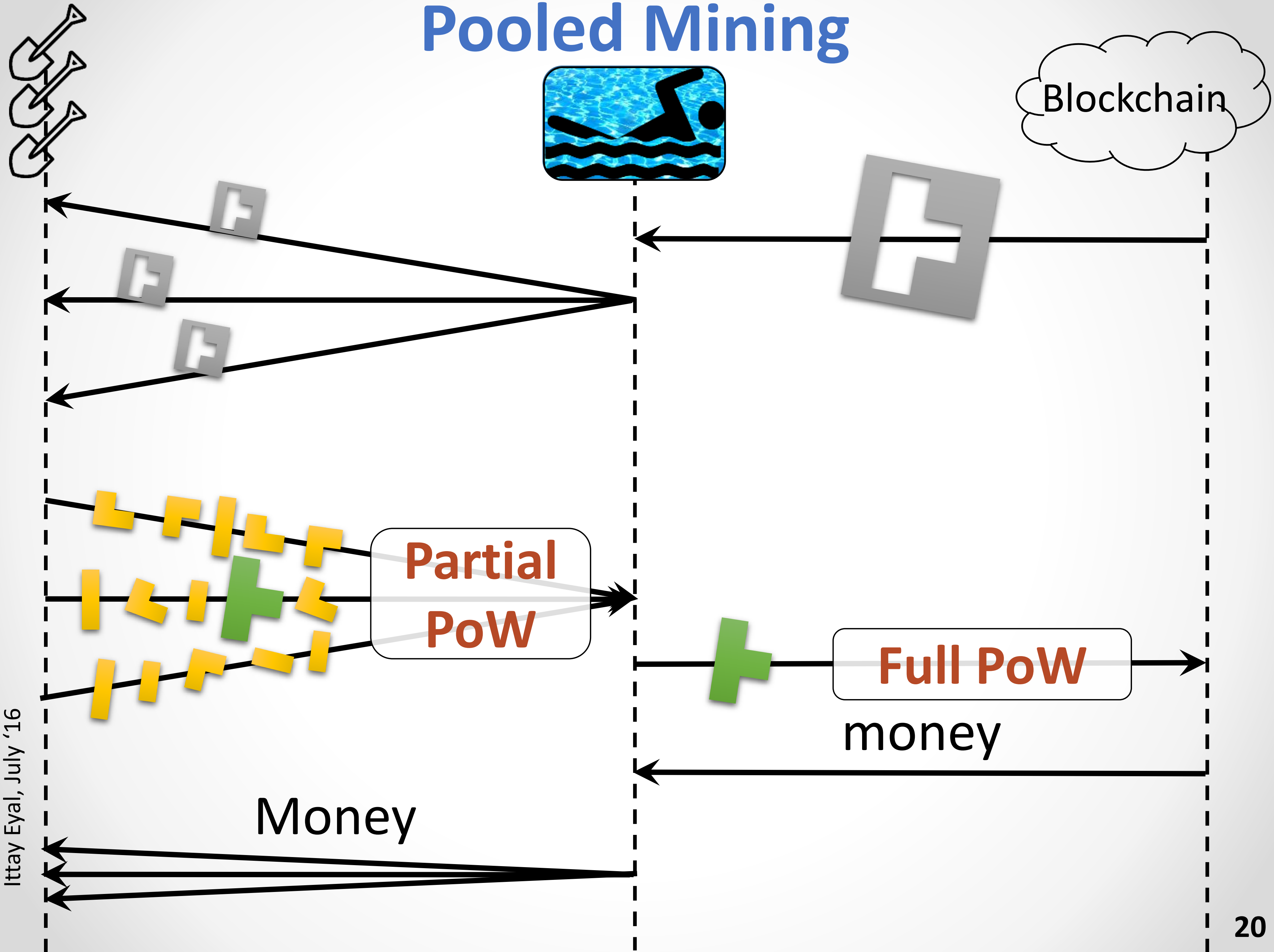
Miners form **pools**



Pooled Mining



Pooled Mining



Blockchain

Partial PoW

Full PoW

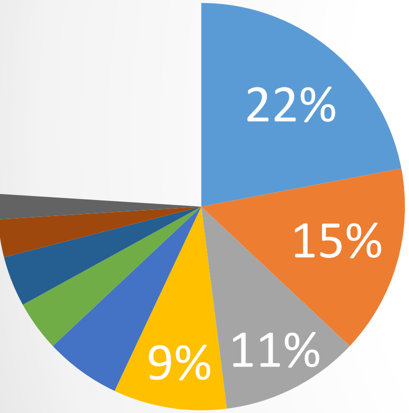
money

Money

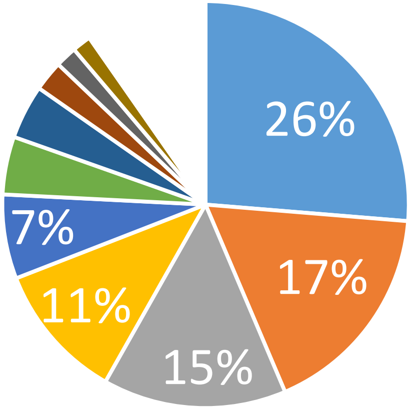
Ittay Eyal, July '16

Open Pools and Centralization

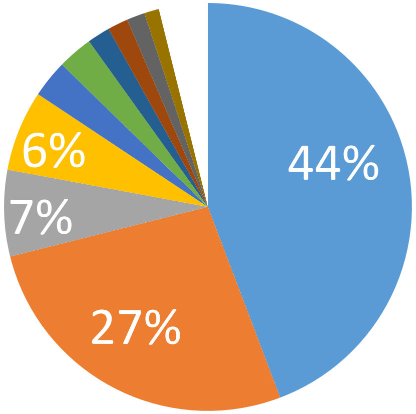
- Miners form pools
- Largest are **open pools**
- Lead to centralization



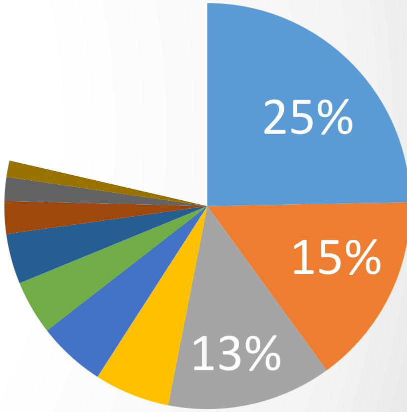
Bitcoin
April 2015



Ethereum
July 2016



Dogecoin
January 2014



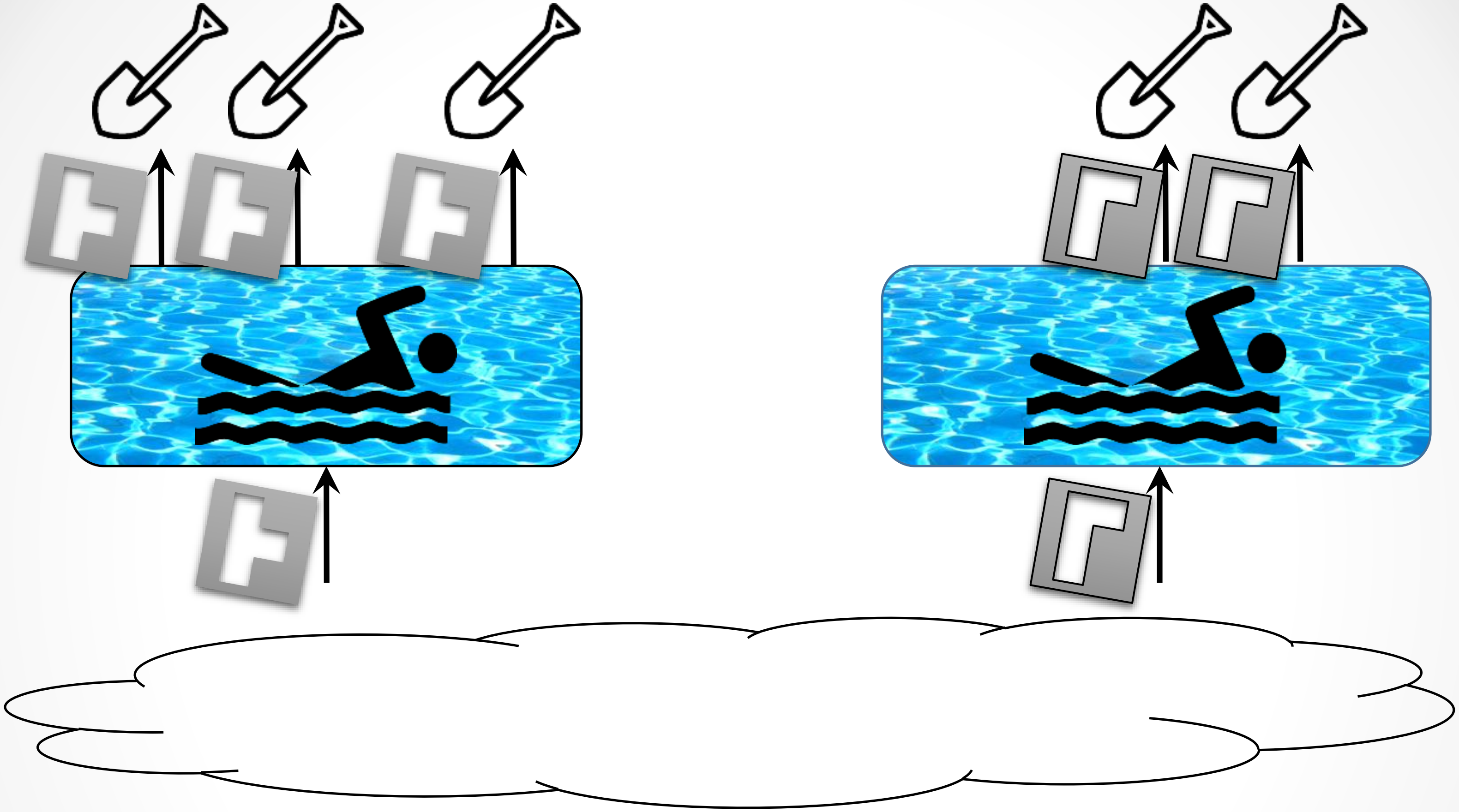
Litecoin
April 2015

A threat to the blockchain's basic premise

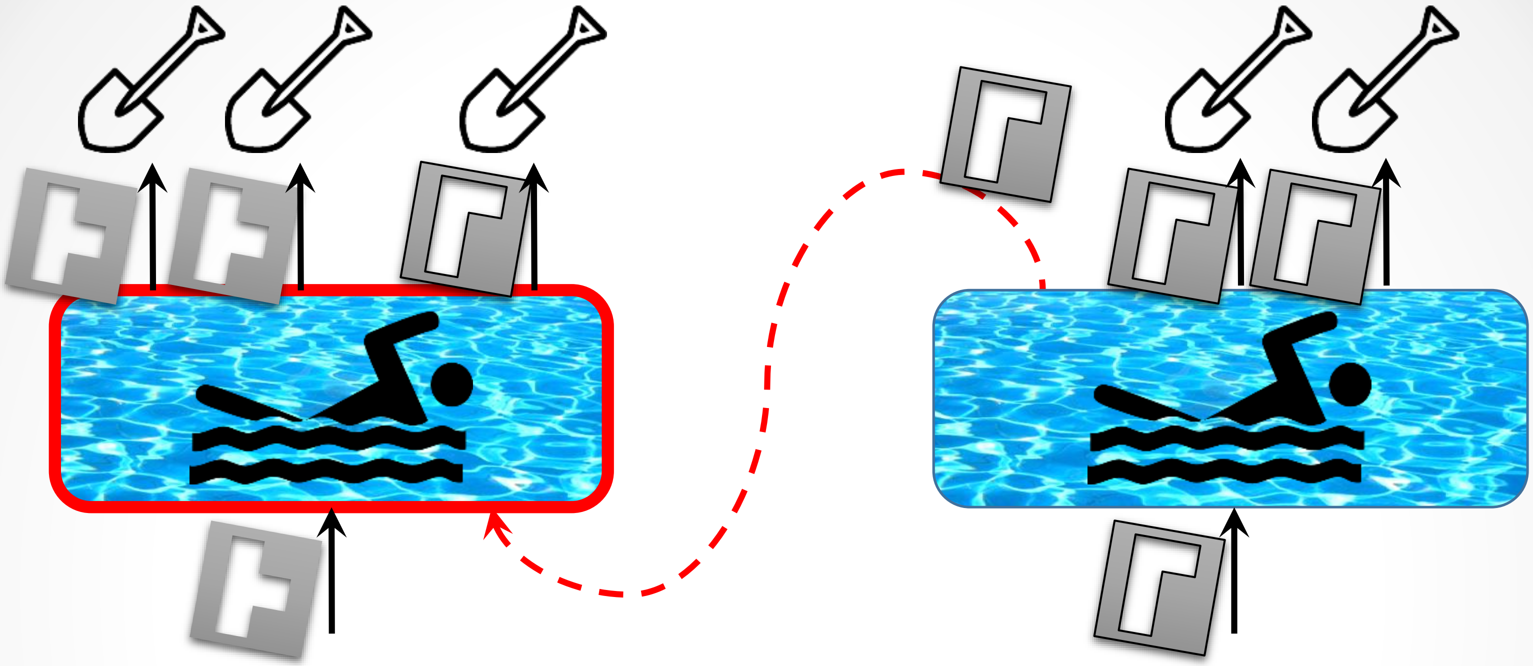
Pool Block Withholding

Oakland'15

Pool Block Withholding



Pool Block Withholding

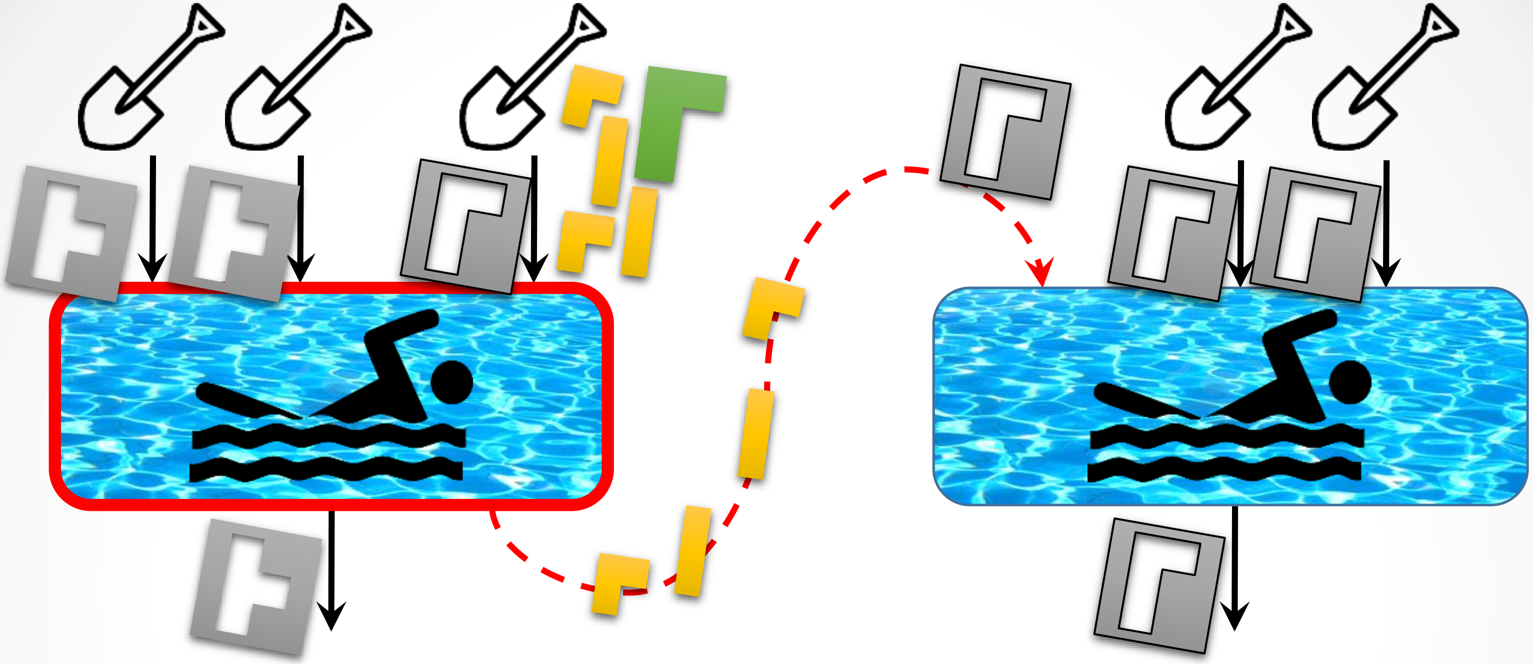


Attacker:

- Registers as standard miner
- Uses some miners as moles

Ittay Eyal, July '16

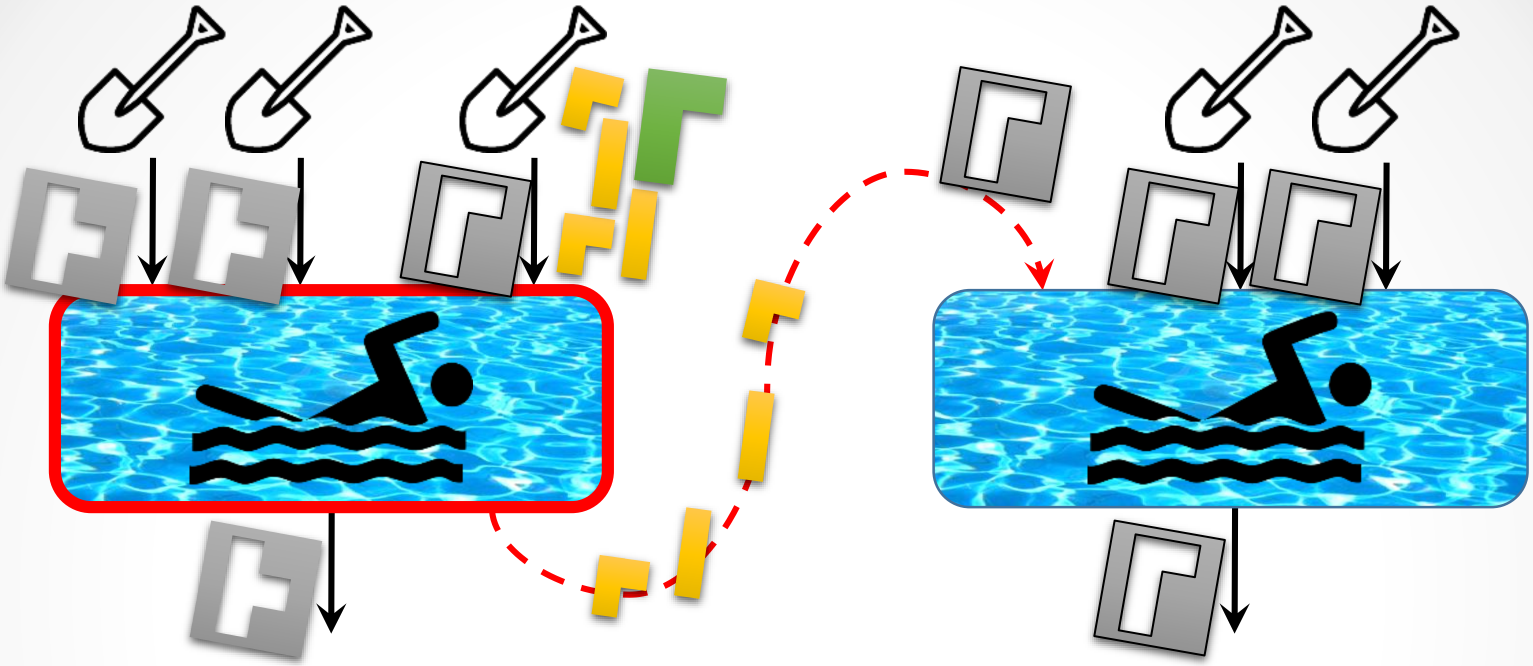
Pool Block Withholding



Attacker:

- Registers as standard miner
- Uses some miners as moles
- Drops full PoW

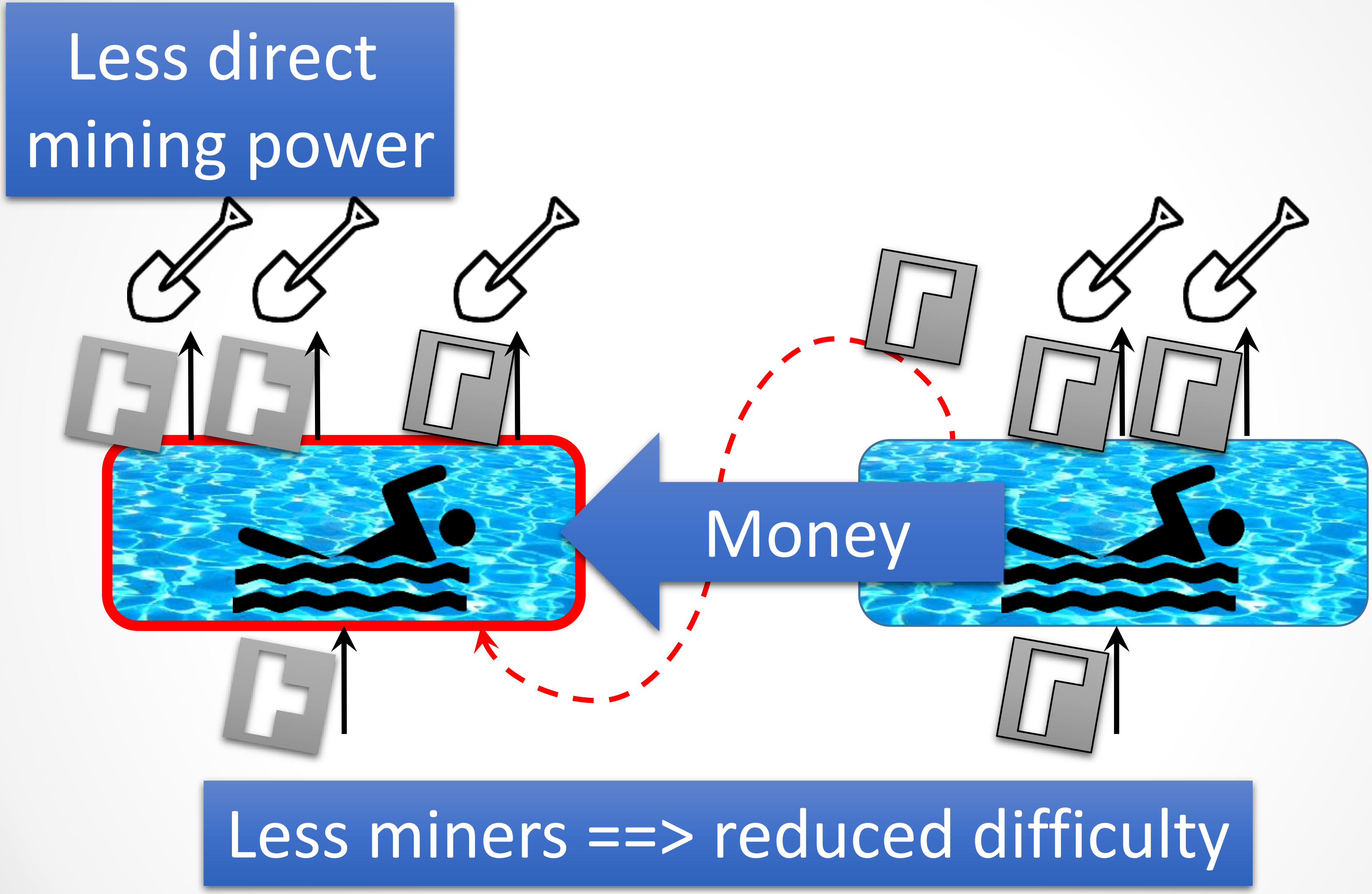
Pool Block Withholding



Attacker:

- Registers as standard miner
- Uses some miners as moles
- Drops full PoW

Factors influencing revenue



Less direct mining power

Money

Less miners ==> reduced difficulty

Ittay Eyal, July '16

π

The Pool Game

Goal

Maximize ***revenue density***

Round

One pool updates infiltration rates

The Pool Game

Goal

Maximize ***revenue density***

Round

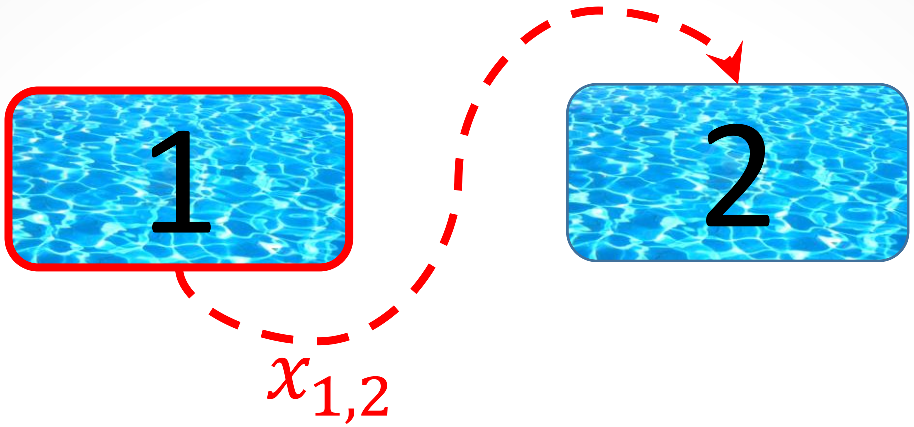
One pool updates infiltration rates

Analysis

- Stable state (equilibrium)
- Generic (any pool size)

Analysis

One Attacker

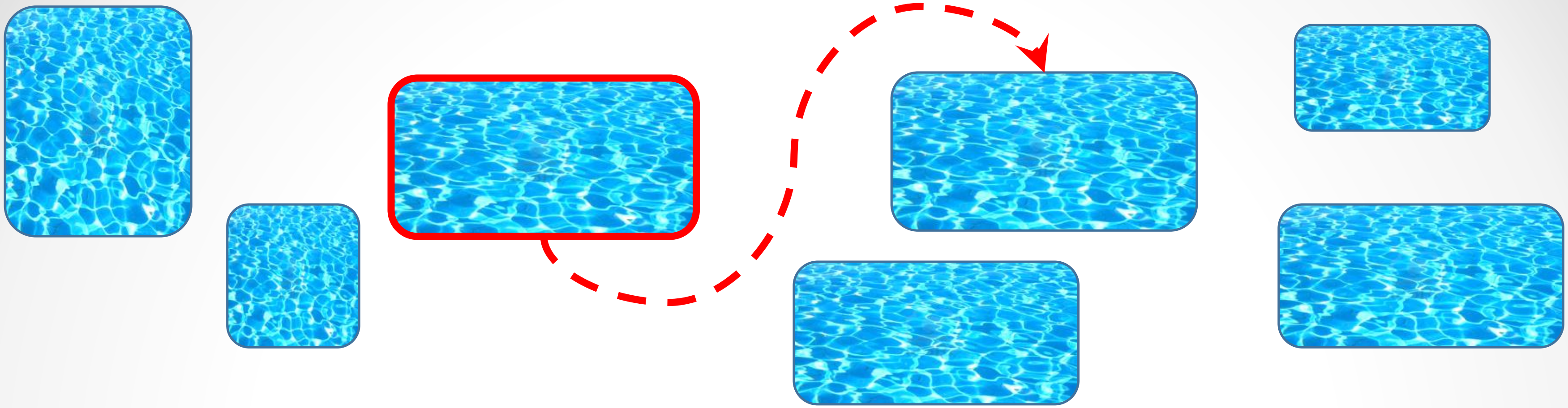


Game progress:

One round – attacker optimizes $r_1(x_{1,2})$

Dominant strategy: Attack

Honest pool mining is not an equilibrium



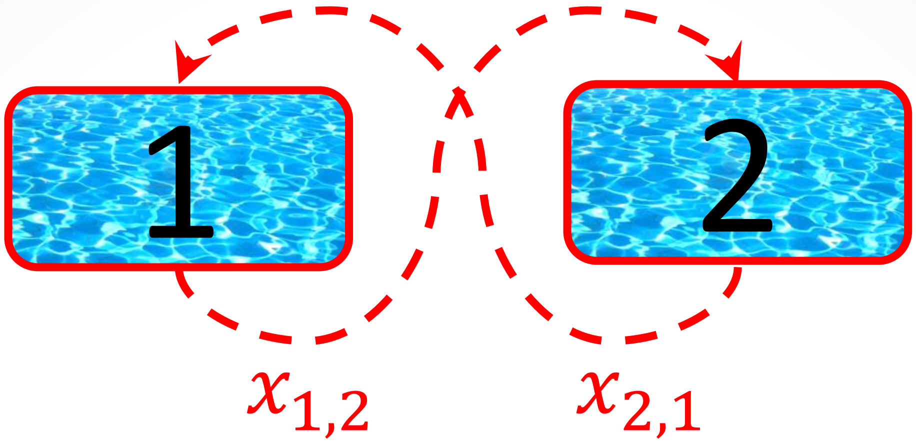
In general:

Honest pool mining is not an equilibrium

(For any two pools, one should attack)

Ittay Eyal, July '16

Two Attackers



Game progress

Repeatedly:

1. Pool 1 optimizes $r_1(x_{1,2}, x_{2,1})$
2. Pool 2 optimizes $r_2(x_{2,1}, x_{1,2})$

A single feasible equilibrium point

The Miner’s Dilemma

When both pools are minorities of any size:

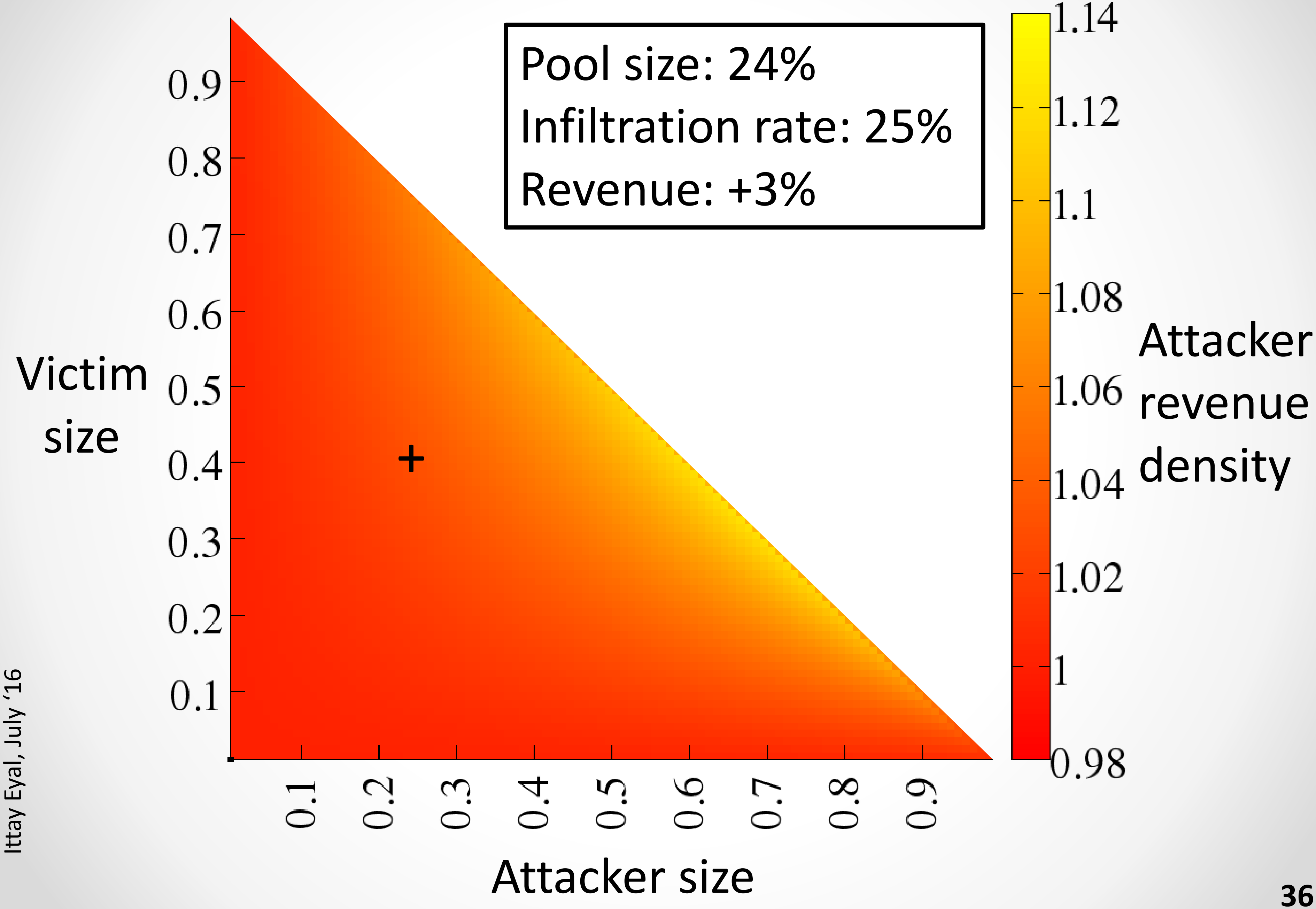
		pool 1	
		NO ATTACK	**ATTACK**
pool 2	**NO ATTACK**		
	ATTACK		

The Miner’s Dilemma

When both pools are minorities of any size:

		pool 1	
		NO ATTACK	ATTACK
pool 2	NO ATTACK	😐 😐	
	ATTACK		

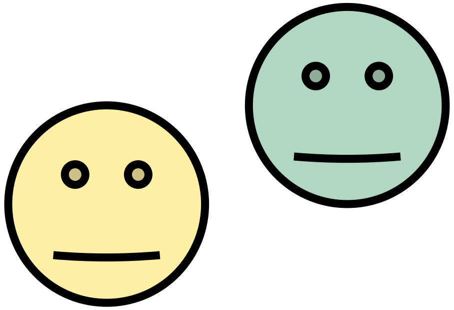
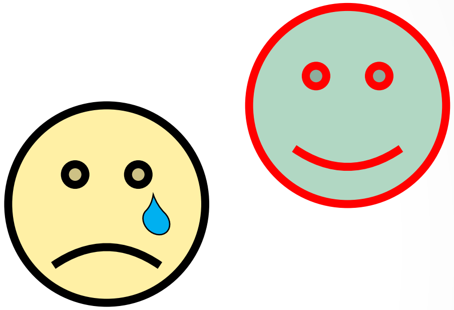
One Attacker



Ittay Eyal, July '16

The Miner’s Dilemma

When both pools are minorities of any size:

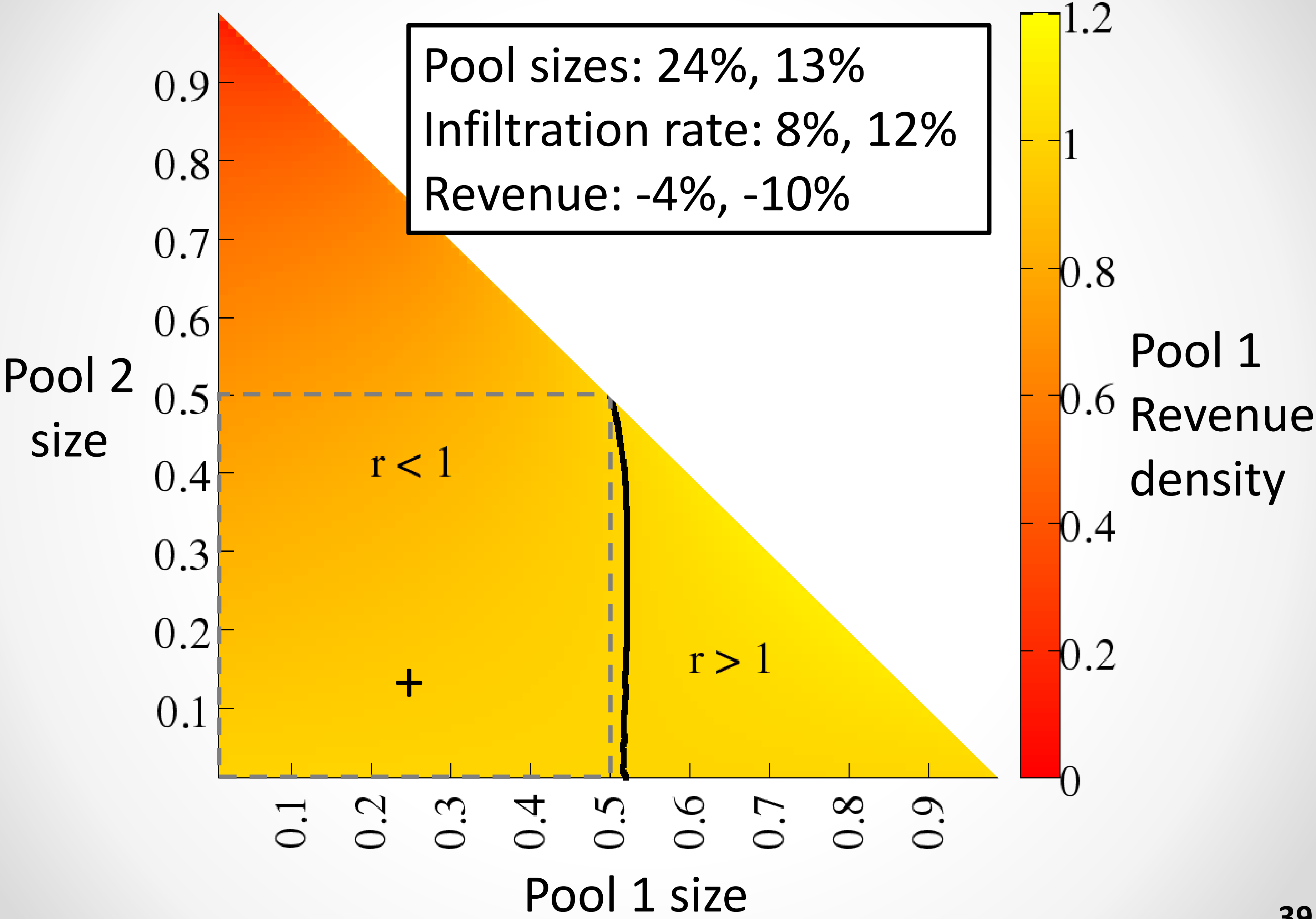
		pool 1	
		NO ATTACK	ATTACK
pool 2	NO ATTACK		
	ATTACK		

The Miner’s Dilemma

When both pools are minorities of any size:

		pool 1	
		NO ATTACK	ATTACK
pool 2	NO ATTACK	😐 😐	😢 🙂
	ATTACK	🙂 😢	

Two Attackers

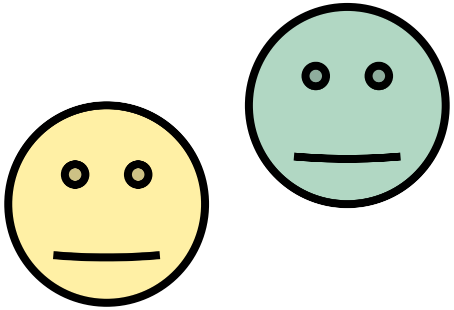
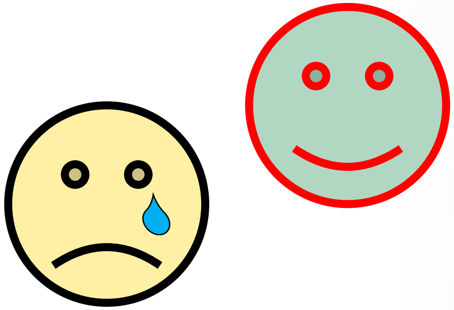
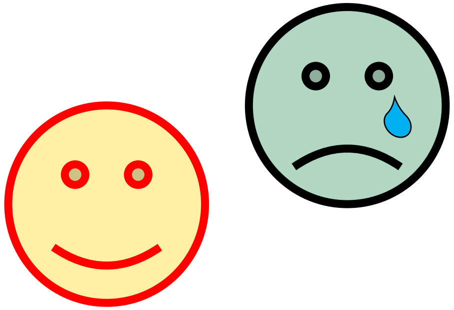
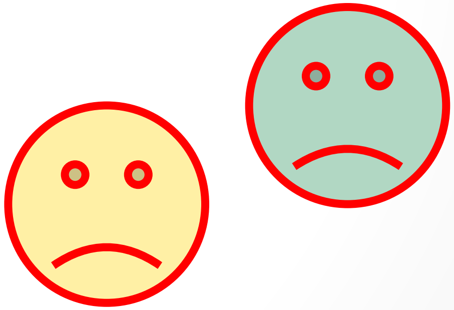

Pool sizes: 24%, 13%

Infiltration rate: 8%, 12%

Revenue: -4%, -10%

The Miner’s Dilemma

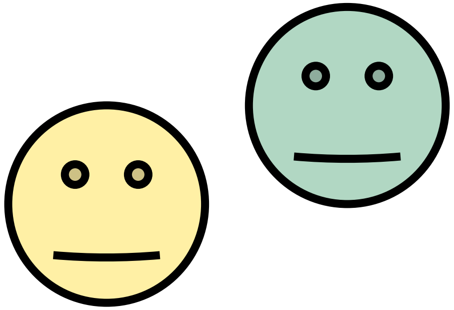
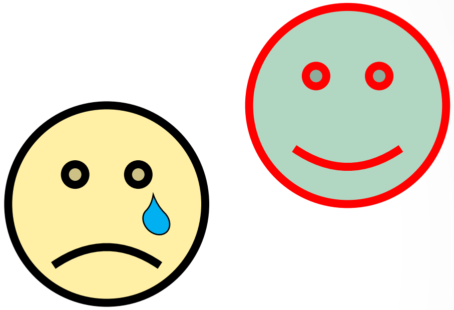
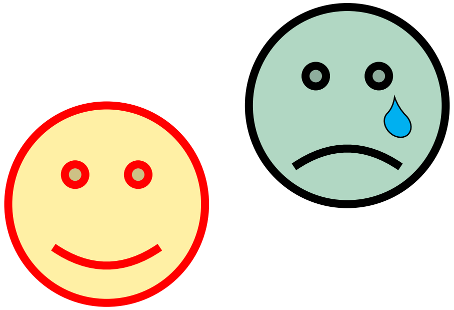
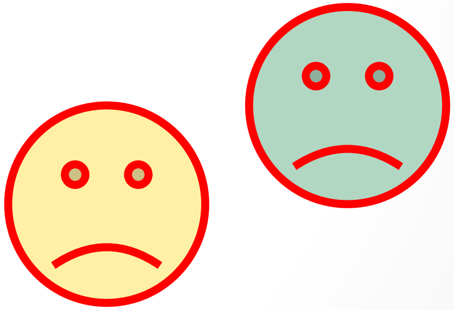
When both pools are minorities of any size:

		pool 1	
		NO ATTACK	ATTACK
pool 2	NO ATTACK		
	ATTACK		

The Miner’s Dilemma

When both pools are minorities of any size:

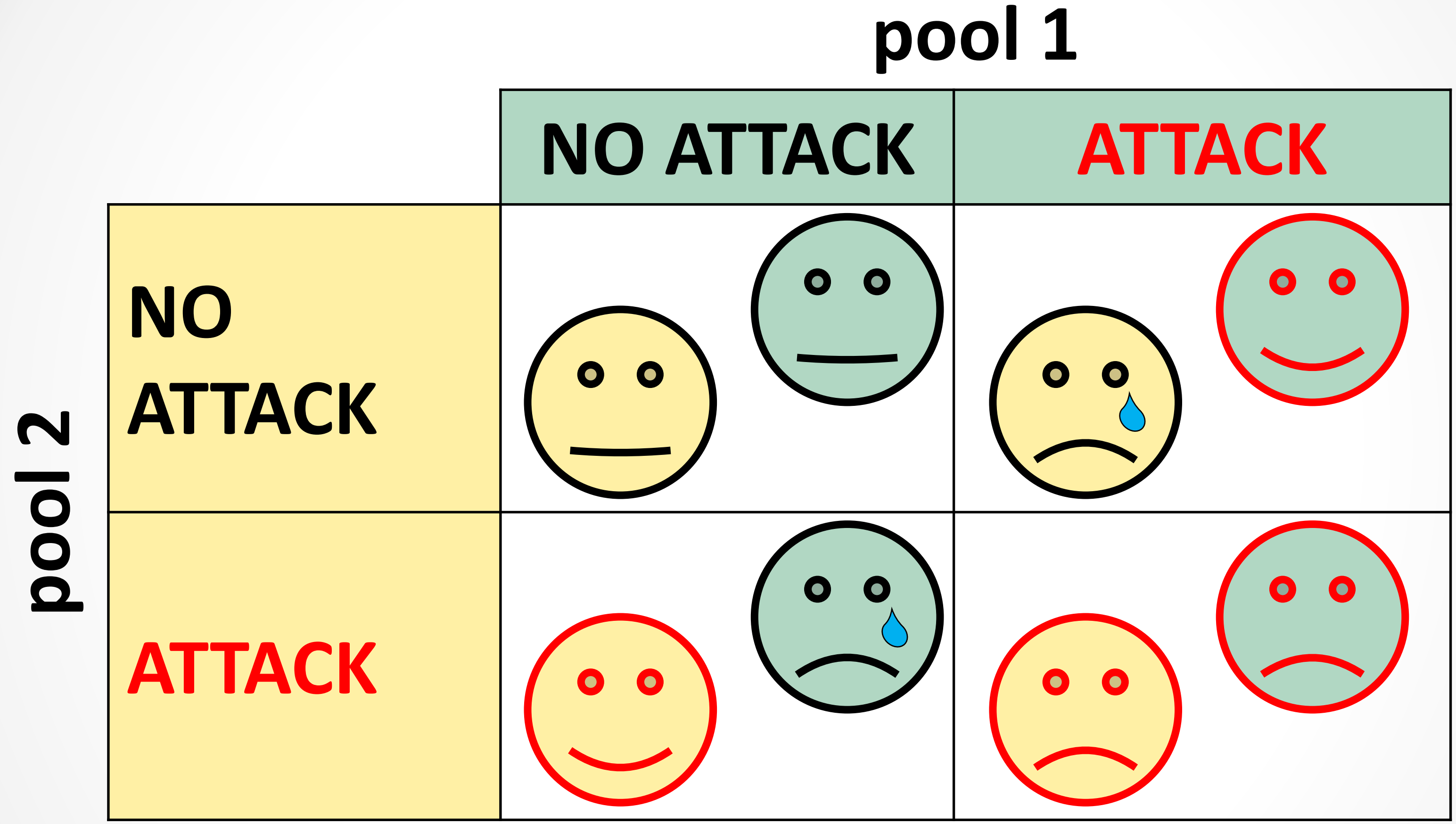
pool 1

		NO ATTACK	ATTACK
pool 2	**NO ATTACK**		
	ATTACK		

This is good

The Miner's Dilemma

When both pools are minorities of any size:



pool 1

		NO ATTACK	ATTACK
pool 2	NO ATTACK		
	ATTACK		

Iterated game with unbounded rounds ==>

Possible non-equilibrium stable state

Countermeasures

- Detection

Does not work

Countermeasures

- Detection

Does not work

- Bonus for full PoW / seniority

Reduces revenue homogeneity

Countermeasures

- Detection

Does not work

- Bonus for full PoW / seniority

Reduces revenue homogeneity

- Honey pot

Wastes resources

Countermeasures

- Detection

Does not work

- Bonus for full PoW / seniority

Reduces revenue homogeneity

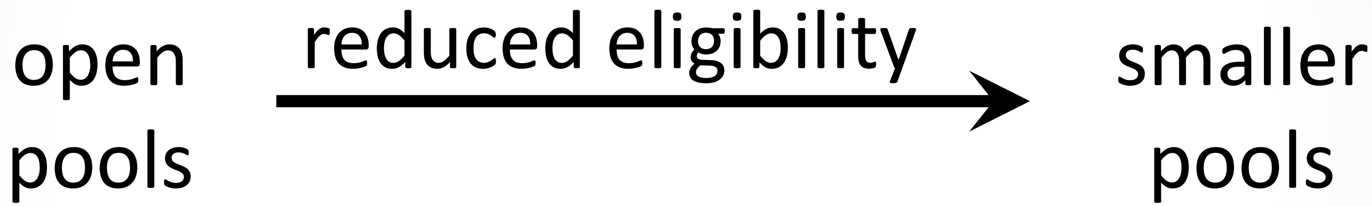
- Honey pot

Wastes resources

- Out of band enforcement

Implies small trust circles

System Health



open pools

reduced eligibility

smaller pools

Conclusion

- Proof of work: cornerstone of open blockchains
  - Some waste
  - Effective security
    (being proven in retrospect)

- Architecture leads to surprising properties
  - The miner’s dilemma
  - Pooled mining
  - Industrial mining
  - Selfish mining
  - Non-standard proof-of-work
  - Proof of work outsourcing
  - Proof of work in face of chain forks