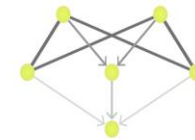


האוניברסיטה העברית בירושלים  
THE HEBREW UNIVERSITY OF JERUSALEM



**DAG**labs

A novel BlockDAG platform

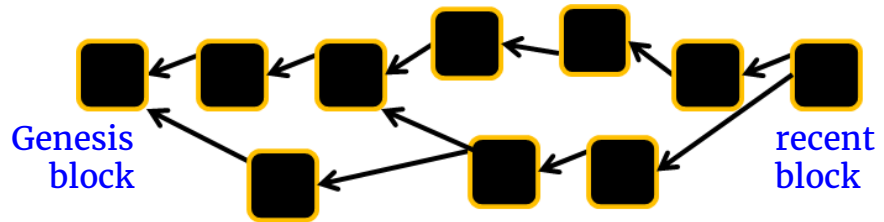
# Incentives and Trade-offs in Transaction Selection in DAG-based Protocols

Yonatan Sompolinsky and Yoad Lewenberg  
Scaling Bitcoin, Stanford

# Background

---

- Directed Acyclic Graph of blocks (blockDAG)
- [Inclusive Blockchain Protocols](#), Financial Crypto '15, Lewenberg, Sompolinsky, and Zohar
- Modification and scaling up of Layer 1
- Orthogonal to Layer 2 solutions

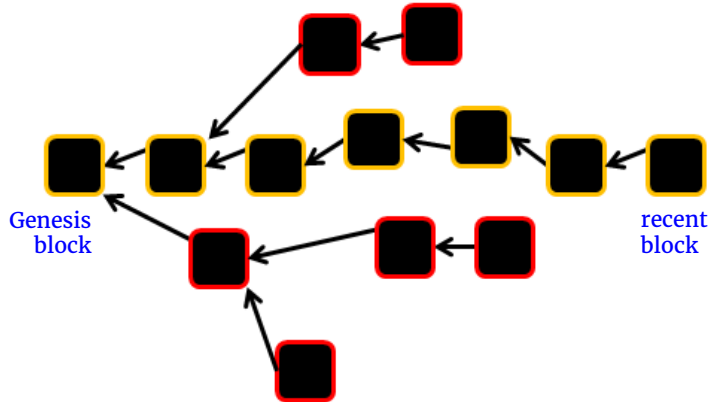


# Blockchain vs BlockDAG

----

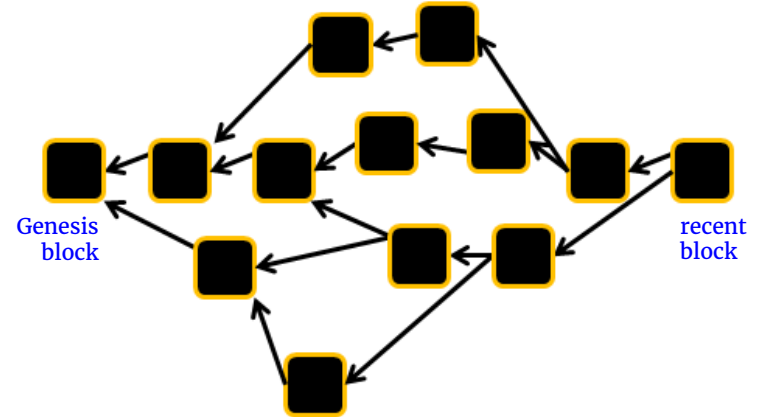
Chain paradigm:

1. maintain single chain
2. ignore the rest
3. forks rare



DAG paradigm:

1. maintain entire graph
2. consider all blocks
3. forks common



# The BlockDAG paradigm

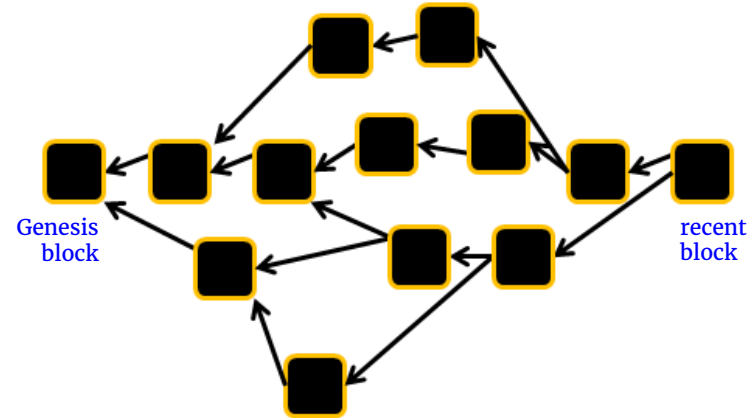
---

more information  
possibly implies:

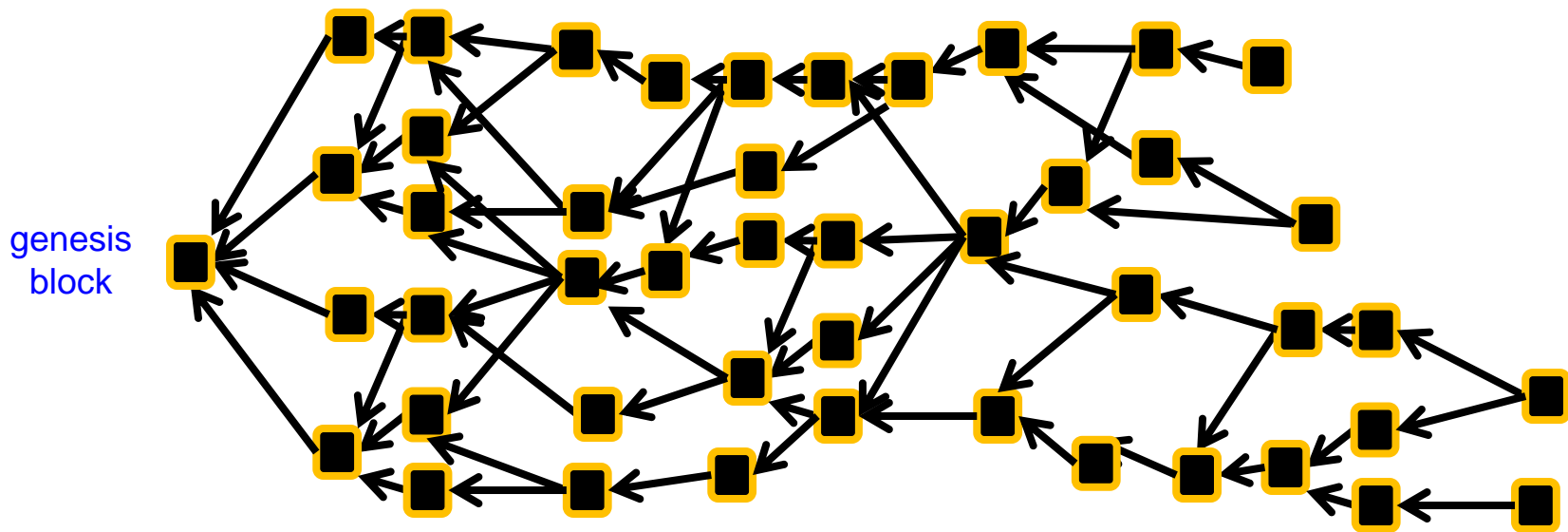
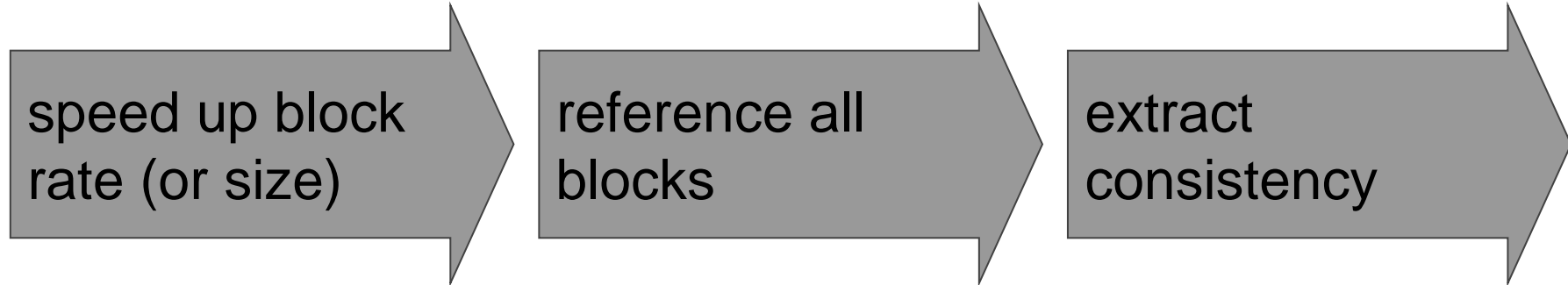
- more security
- more scalability
- more fairness

DAG paradigm:

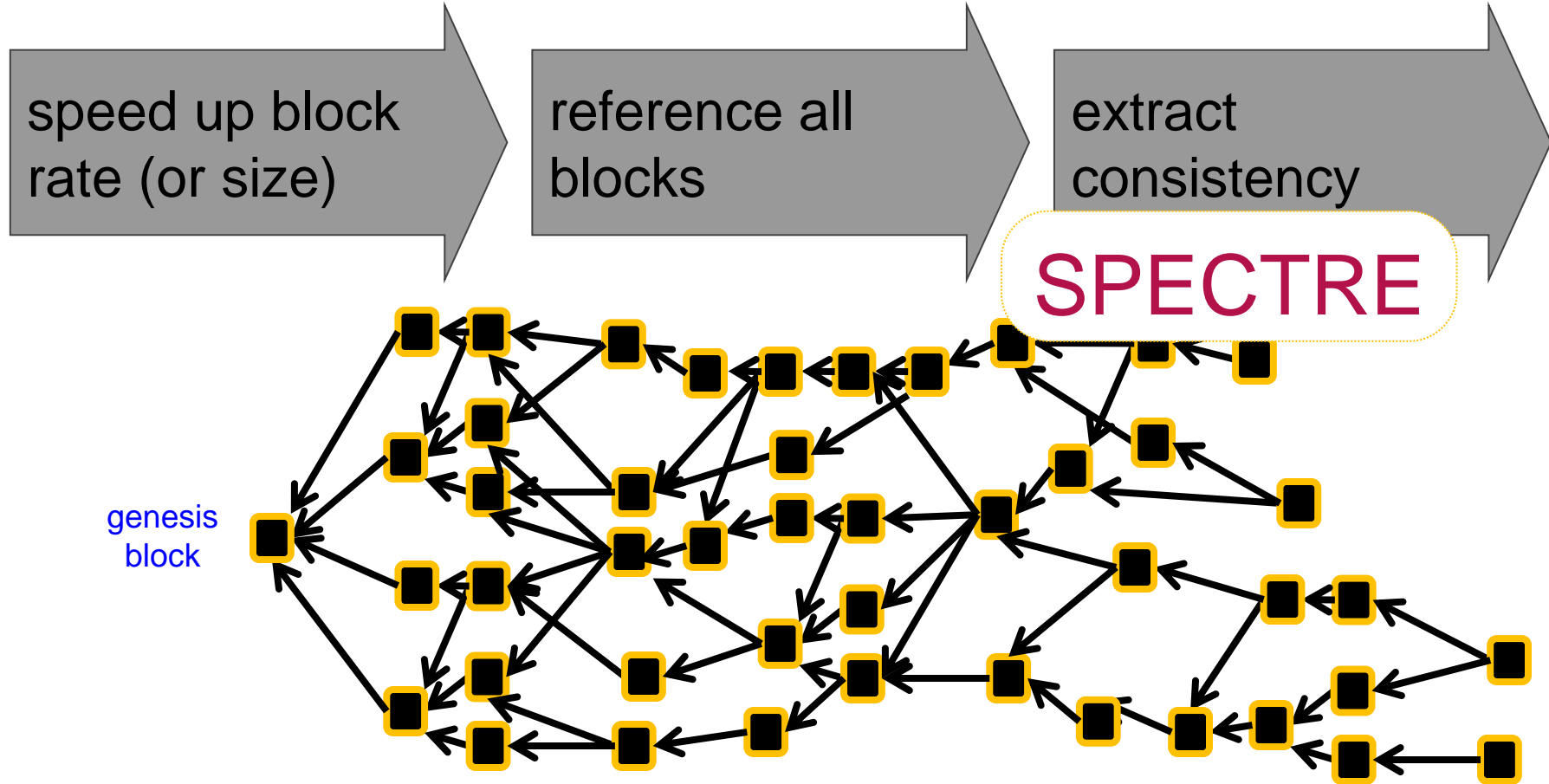
1. maintain entire graph
2. consider all blocks
3. forks common



# Road to scaling up Layer 1



# Road to scaling up Layer 1



# BlockDAG is (only) a paradigm

---

- DAG merely a framework, not a solution
- Not all blockDAGs are created equal
- DAG vs chain like highway vs one-lane road...

# BlockDAG is (only) a paradigm

---

- DAG merely a framework, not a solution
- Not all blockDAGs are created equal
- DAG vs chain like highway vs one-lane road...





# BlockDAG is (only) a paradigm

---

- DAG merely a framework, not a solution
- Not all blockDAGs are created equal
- DAG vs chain like highway vs one-lane road...



# BlockDAG is (only) a paradigm

---

- DAG merely a framework, not a solution
- Not all blockDAGs are created equal
- DAG vs chain like highway vs one-lane road...



# Scaling up Layer 1 -- challenges

---

decentralization

fairness

**throughput &  
confirmation times**

fee structure

POW calculation

**consistency rule**

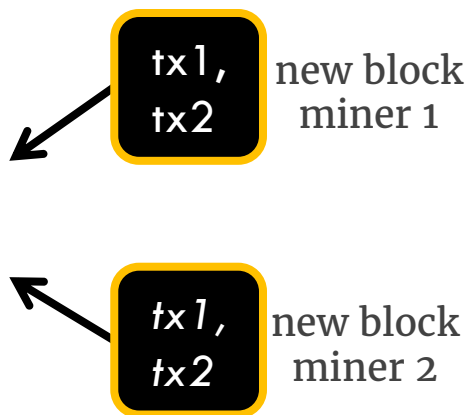
storage

bandwidth utilization

# Two scenarios for DAG throughput

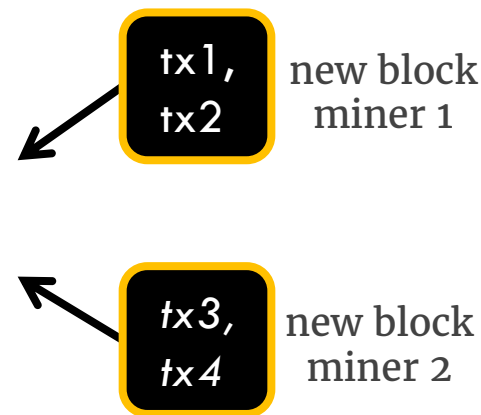
mempool: tx1>tx2>tx3>tx4>... (non-conflicting)

---



tx1,tx2 selected & approved  
tx3,tx4 still in mempool

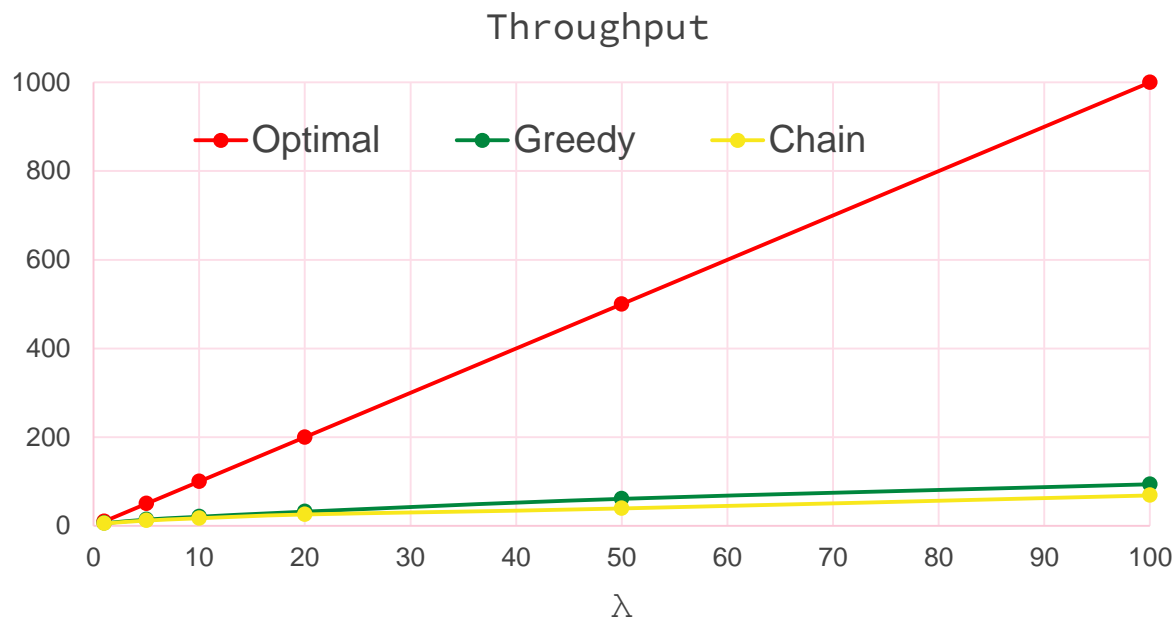
**under utilization**



tx1,tx2,tx3,tx4 selected & approved  
(mempool cleared faster)

**full utilization**

Proposition 1: under naïve/greedy mining,  
DAG throughput  $\approx$  chain throughput



# Key observation / good news

---

*Miners are incentivized to avoid selecting the same txns, and to contribute to throughput increase.*

*Indeed, "collisions" result in loss of fees...*



# The Inclusive Game

---

mempool:  $tx1 > tx2$   
players: miner1, miner2



	<u>miner2 chose tx1</u>	<u>miner2 chose tx2</u>
<u>miner1 chose tx1</u>	$(0.5 * tx1, 0.5 * tx1)$	$(tx1, tx2)$
<u>miner1 chose tx2</u>	$(tx2, tx1)$	$(0.5 * tx2, 0.5 * tx2)$

collision on tx1

collision on tx2

# The Inclusive Game

---

pure strategy: select a txn

mixed strategy: select a txn using randomness



	<u>miner2 chose tx1</u>	<u>miner2 chose tx2</u>
<u>miner1 chose tx1</u>	$(0.5 \cdot tx1, 0.5 \cdot tx1)$	$(tx1, tx2)$
<u>miner1 chose tx2</u>	$(tx2, tx1)$	$(0.5 \cdot tx2, 0.5 \cdot tx2)$

collision on tx1

collision on tx2



# How to “solve” the game

---

level of cooperation

adversarial

selfish

selfish +  
coordination

altruistic

solution:  
Safety Level

solution:  
Nash Equ.

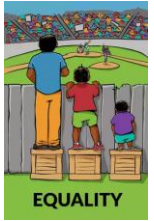
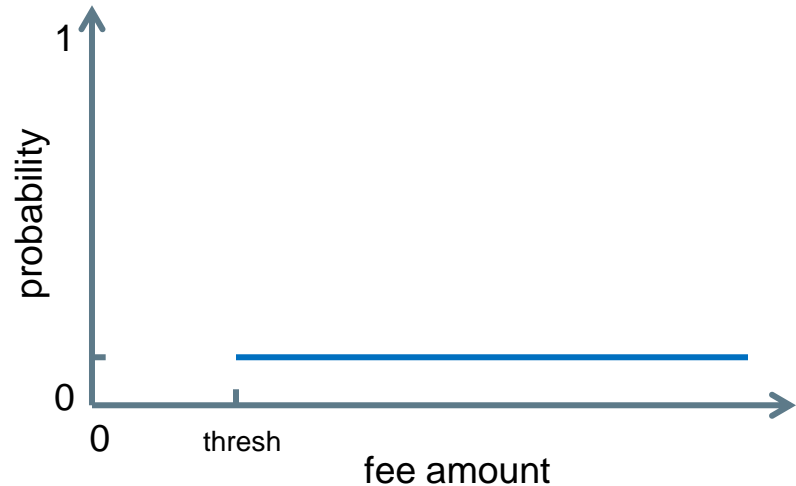
solution:  
Correlated Equ.

solution:  
Max Social  
Welfare

# Max Social Welfare

---

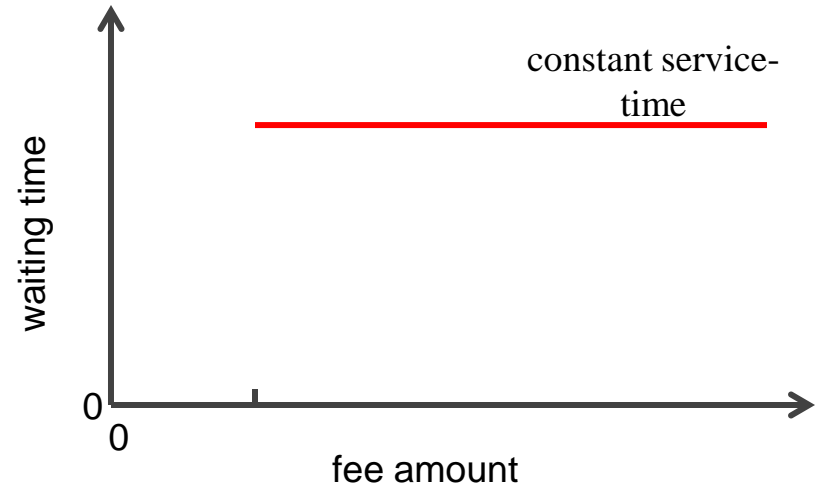
- Solution: select txns uniformly [above capacity threshold]
- No collisions, full utilization
- But there's a catch...



# High throughput is not enough

---

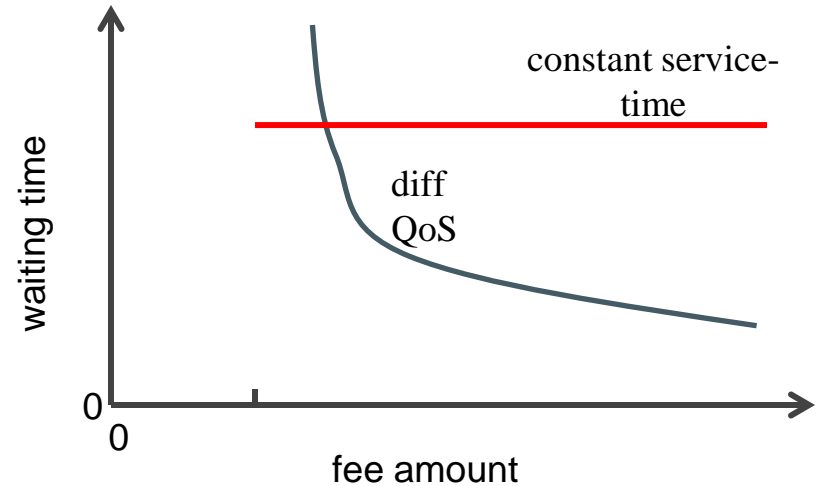
1. Strategically unstable
2. Forces egalitarian waiting times, no QoS levels and preferential treatment



# High throughput is not enough

---

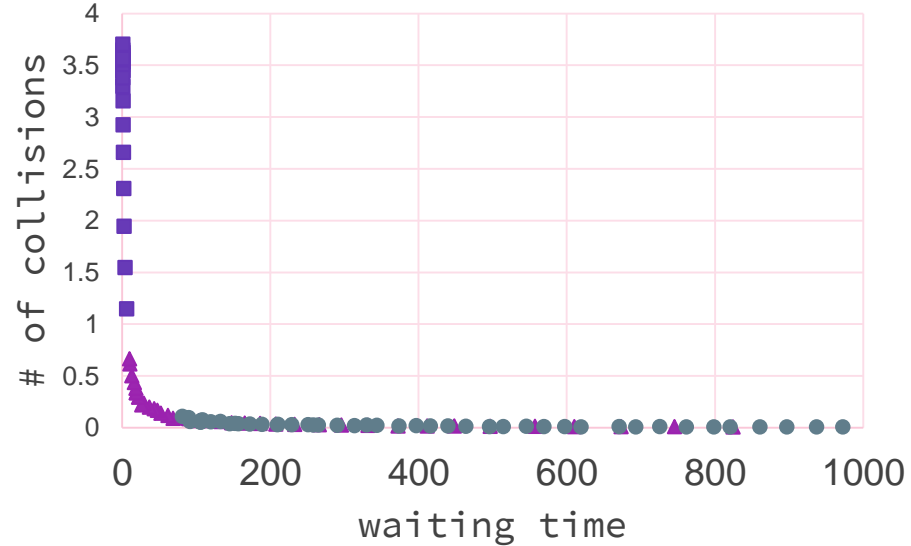
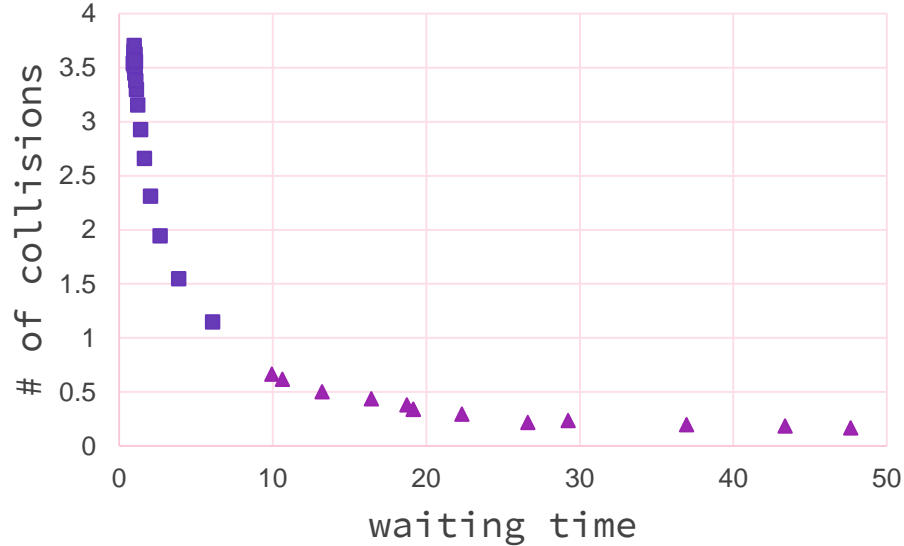
1. Strategically unstable
2. Forces egalitarian waiting times, no QoS levels and preferential treatment



# Trade-off: high utilization vs fast conf. times

---

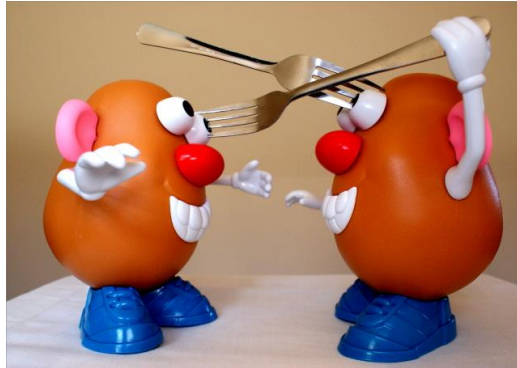
*shorter waiting times  $\rightarrow$  more collisions  $\rightarrow$  lower utilization*



# Nash Equilibrium

----

- Finding Nash usually hard
- Tit-for-tat strategies
- Greedy pools/miners will suffer retaliation (?)



round #1

miner1\miner2	<u>tx1</u>	<u>tx2</u>
<u>tx1</u>	$(0.5 \cdot tx1, 0.5 \cdot tx1)$	$(tx1, tx2)$
<u>tx2</u>	$(tx2, tx1)$	$(0.5 \cdot tx2, 0.5 \cdot tx2)$

round #2

miner1\miner2	<u>tx1</u>	<u>tx2</u>
<u>tx1</u>	$(0.5 \cdot tx1, 0.5 \cdot tx1)$	$(tx1, tx2)$
<u>tx2</u>	$(tx2, tx1)$	$(0.5 \cdot tx2, 0.5 \cdot tx2)$

round #3

miner1\miner2	<u>tx1</u>	<u>tx2</u>
<u>tx1</u>	$(0.5 \cdot tx1, 0.5 \cdot tx1)$	$(tx1, tx2)$
<u>tx2</u>	$(tx2, tx1)$	$(0.5 \cdot tx2, 0.5 \cdot tx2)$

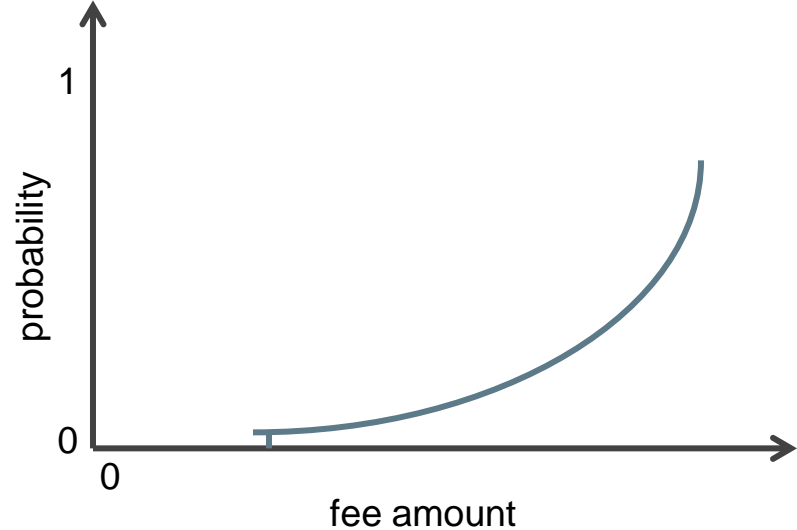
# Nash Equilibrium (myopic)

---

- Assigns high probability to high paying txns
- Not too greedy: top txns not necessarily selected

**Theorem 6.** Suppose the memory buffer consists of  $k_l$  transactions with fee  $v_l$  ( $1 \leq l \leq n$ ). Denote the individual transactions by  $w_1, \dots, w_m$ , which are sorted in descending order of their fees. Denote the index of  $v(w_i)$  by  $l(w_i)$ . The marginal probability  $p_i := \frac{q_{l(w_i)}}{k_{l(w_i)}}$  ( $1 \leq i \leq m$ ) defines a symmetric equilibrium in the single-shot inclusive-F game, where:

$$- q_l = \begin{cases} k_l \cdot \min\left(f^{-1}\left(\frac{c_{k_{max}}}{v_l}\right), 1\right) & 1 \leq l \leq k_{max} \\ 0 & k_{max} < l \leq n \end{cases}$$
$$- \forall 1 \leq l \leq n: G_l(z) := \sum_{h=1}^l k_h \cdot \min\left(f^{-1}\left(\frac{z}{v_h}\right), 1\right) - b$$
$$- k_{max} := \max\{k \leq n \mid \forall l \leq k : G_l(v_l) \leq 0\}$$
$$- c_{k_{max}} \text{ is the root of } G_{k_{max}}.$$



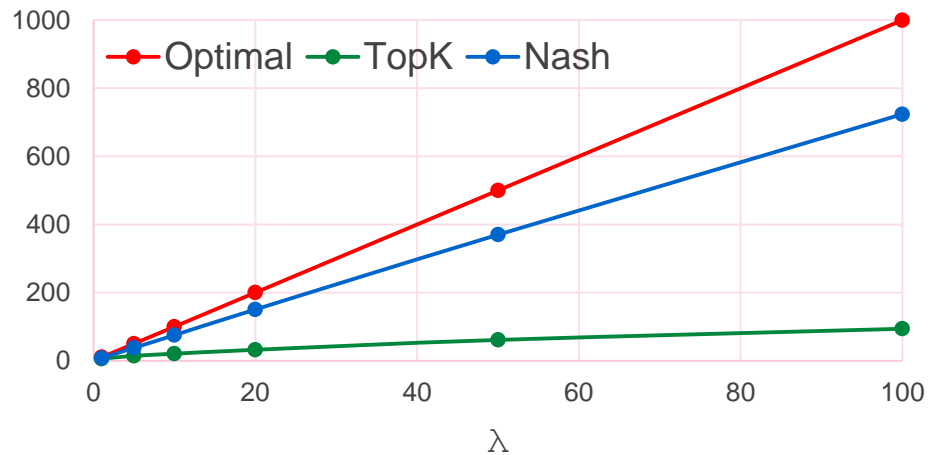
# Throughput under Nash

Throughput of: DAG + greedy mining (green)

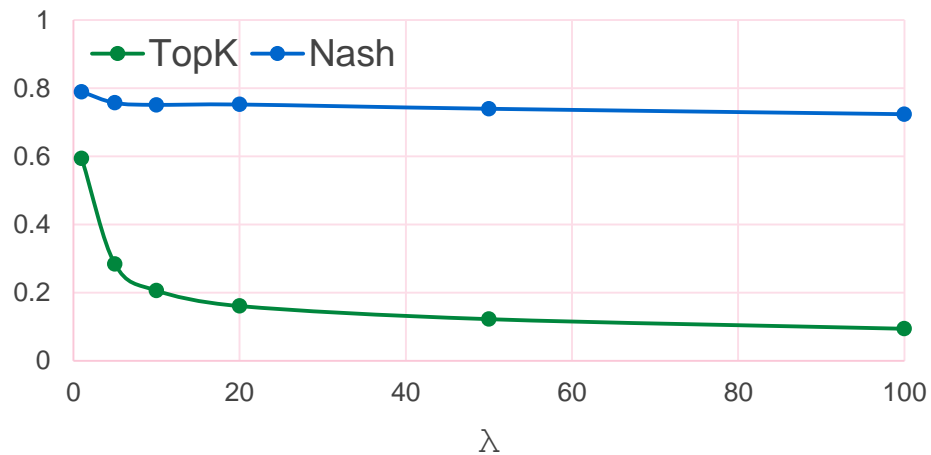
DAG + Nash Equ. (blue)

DAG + optimal utilization (red)

Throughput

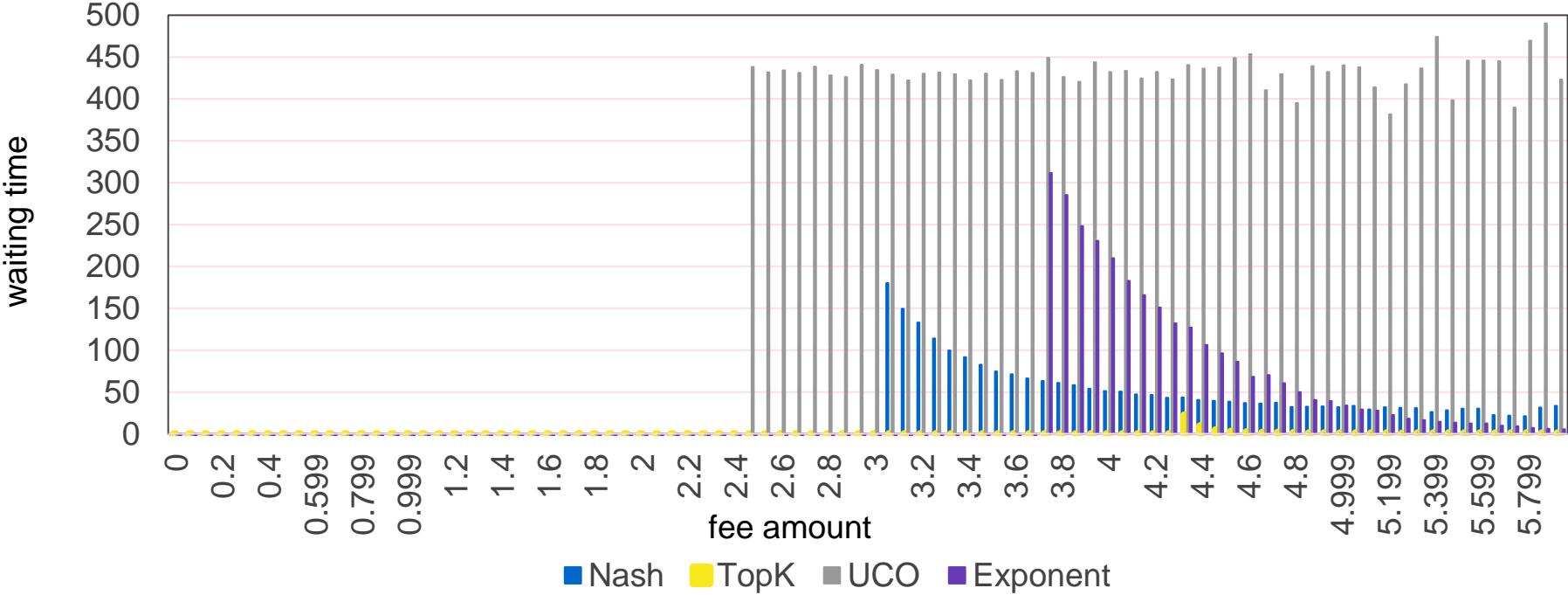


Utilization





# QoS levels



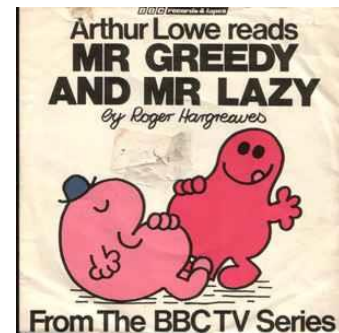
# Correlated Equilibrium / asymmetric Nash

- 
- Can we do better by somehow coordinating between miners?
  - Preliminary results: yes, higher throughput
  - Coordination mechanism: using prvs blocks' randomness
  - Future work



# Scaling and incentives

---



- Strategic mining in Bitcoin -- sophisticated, risky  
in DAG -- easy (but also marginal)
- Decisions more granular: *which txns to select?*  
*how fast to release blocks?*
- “Lazy” selfish mining -- miner is lazy in information sharing, does not contribute reasonable bandwidth

When implementing  
BlockDAG protocols --  
incentives *really* matter

“Bitcoiners of the world, unite!  
You have nothing to lose but your chains!”