Universität Zürich[UZH]

UZH Blockchain Center

Blockchain & DLT Research Group

Agent-Based Modelling of Blockchain Consensus

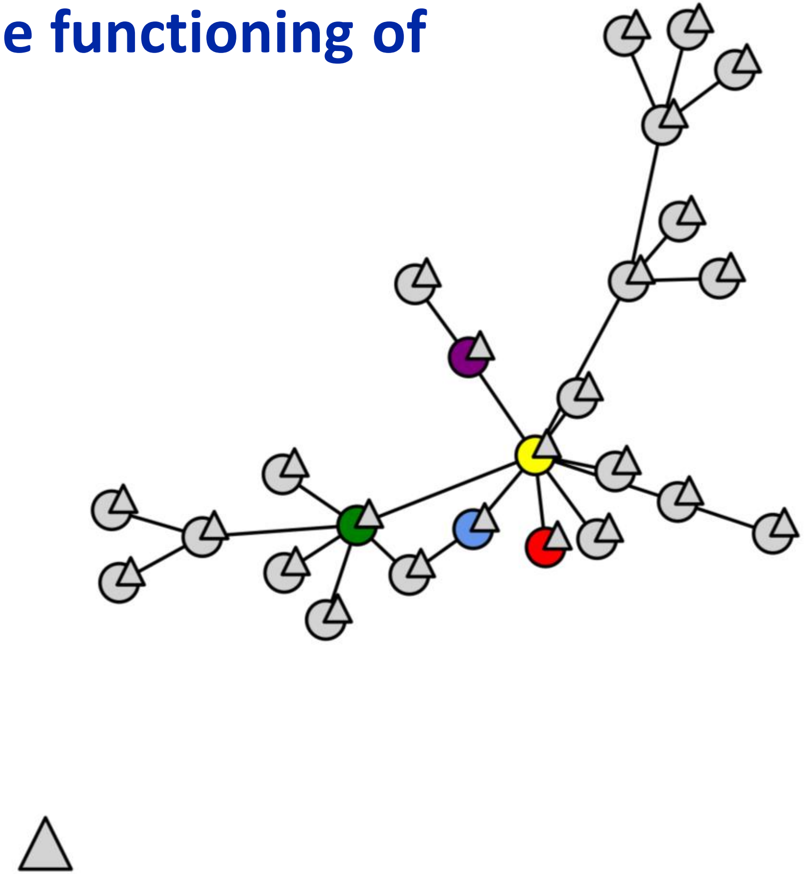
Benjamin Kraner, Nicolò Vallarano, Sheng-Nan Li, Caspar Schwarz-Schilling, Claudio J. Tessone

Claudio Tessone

Blockchain & Distributed Ledger Technologies

UZH Blockchain Center

Consensus is fundamental for the functioning of blockchains

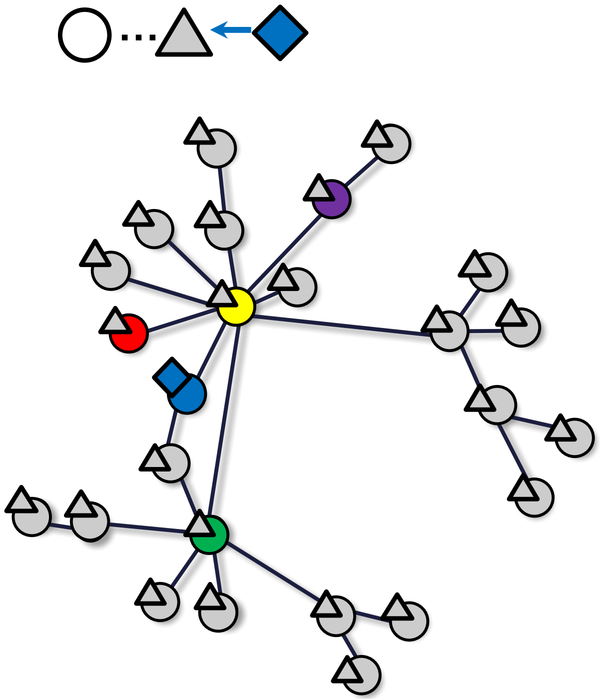


Protocols can only be designed under very stylised conditions: Negligible transmission time of blocks, simplified tolopogies, simple agent behaviour,etc

Agent-based modelling is a technique that allows to expand tremendously the knowledge we have on the functioning and robustness of consensus protocols

PoW Consensus

Consensus in P2P network – symmetry of information



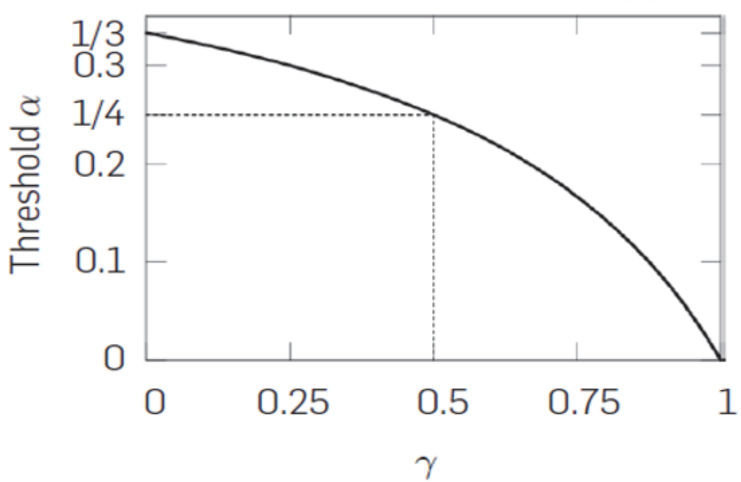
What happens if miners deviate to withhold information of mined block, instead of immediately propagating it?

He has advantage to mine next block before anybody else!

Selfish Mining (SM) Attack

Eyal and Sirer 2014 [1]

A miner (pool) keeps his mined block private and selectively publishes it depending on the relative length of private branch.



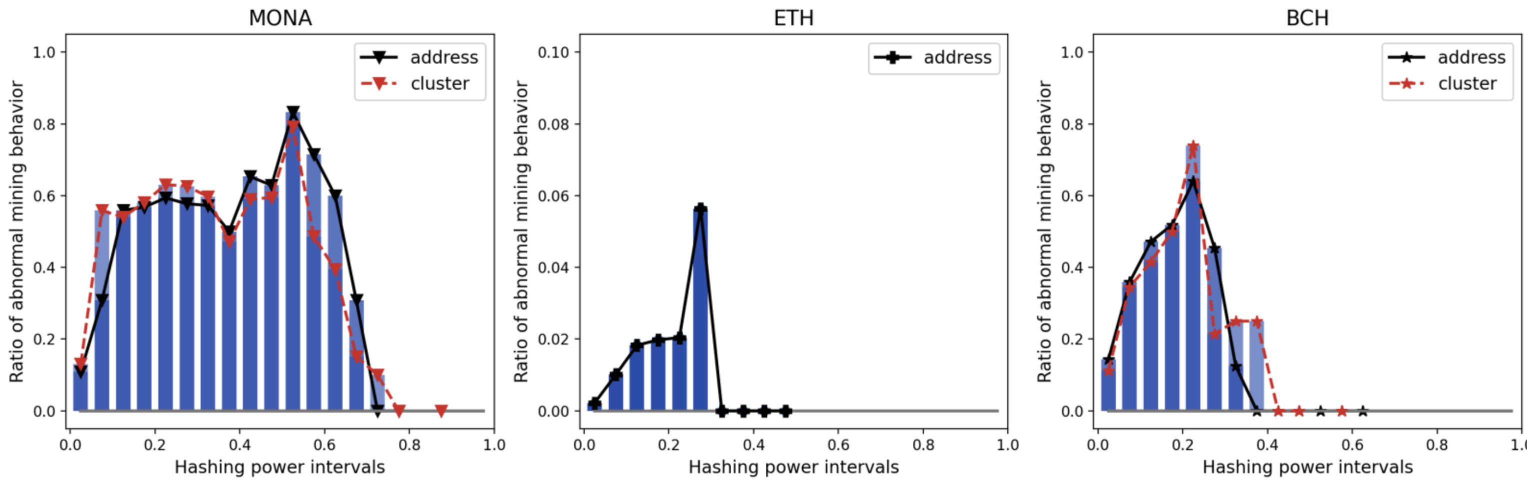
For a given γ (propagation factor), a pool of size α could obtain a revenue more than he expected, in the range:

$$\frac{1-\lambda}{3-2\lambda} < \alpha < \frac{1}{2}$$

Over $\frac{2}{3}$ of the participants need to be honest to defense SM attack. The majority (51%) is not enough.

[1] Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable,"

Motivation of Selfish behaviour



- Ratio of abnormal miners in different power intervals in MONA, ETH and BCH.
- When the mining power is below a certain value, the motivation of doing SM trends to increase with the higher power.

Agent-Based Modelling of Selfish Mining

- Agents
  - Set of N miners. A miner is either selfish or honest.
  - Miners' hashing power α follows various distributions (uniform random, power-law, exponential)
  - *"Longest chain rule"*: Miners adopt the received block if it has greater height.
    - Honest miners immediately share the accepted or mined blocks.
    - Selfish miners strategically share blocks.

Agent-Based Modelling of Selfish Mining

- P2P network
  - Topology: Uniform Random, Erdos-Renyi, Barabási-Albert
  - Events: happen as independent Poisson processes, and the interval time follows exponential distributions.
    - Block creation: at a constant rate, τ^{-1}
    - Block propagation: at a constant rate via each edge, $E_a\tau_{nd}^{-1}$

Agent-Based Modelling of Selfish Mining

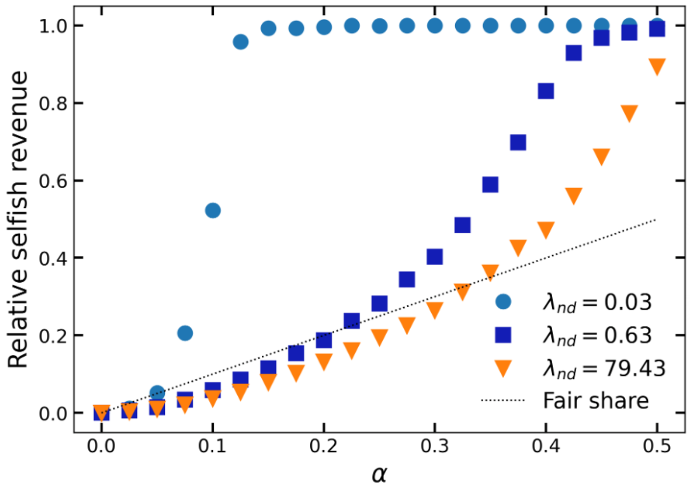
- Evolution

Over time, by **Gillespie algorithm**[1], select next event and increase time. The total transition rate:

$$\xi = \tau^{-1} + E_a \tau_{nd}^{-1}$$

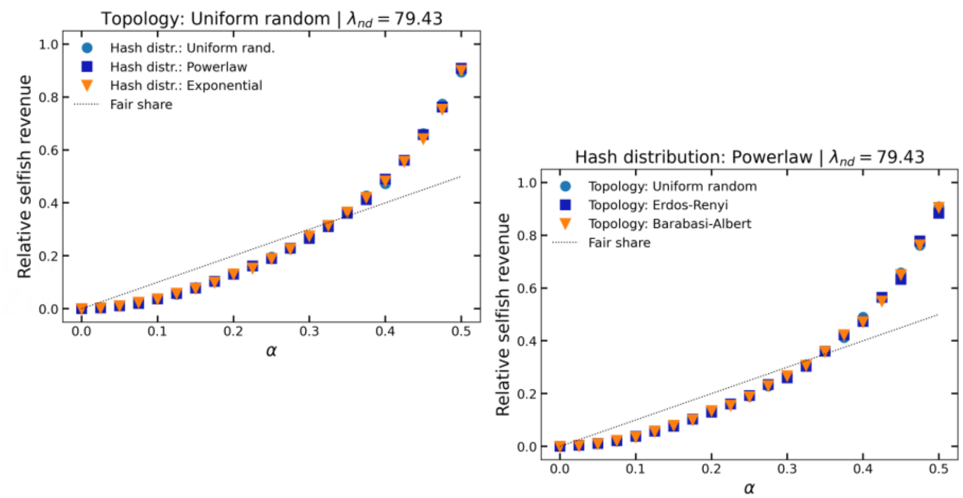
- Next event is selected with the probability :
  - τ^{-1}/ξ , new block is mined.
  - $E_a \tau_{nd}^{-1}/\xi$, block is gossiped from a node to all the peers

Profitable of Selfish Mining



- Reward share of selfish miners with different power α under different levels of the network delay.

(Larger $\lambda_{nd} = \tau_{nd}^{-1}$ reflects a lower network delay)

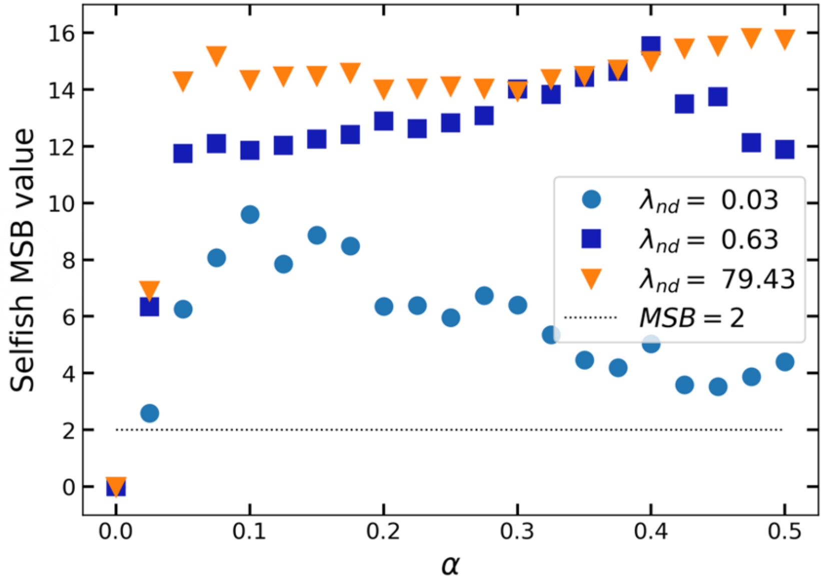


- Reward share of selfish miners with different power α in different network topologies.

Selfish mining is always more profitable for exceeding 1/3 of total mining power. And results are robust among different network topologies.

Detection of Selfish Miners

- Identify the selfish miners by our ***MSB*** method.



Selfish Miners are efficiently identified by our MSB index.

Summary

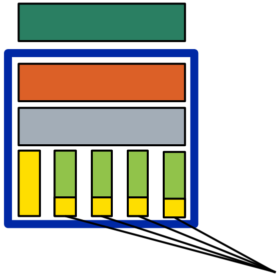
Network delay could affect the profitability of Selfish mining strategy.

Selfish miner indeed has significantly high probability of mining blocks in a row.

PoW in consensus in absence of block rewards

Agent-Based Model - Agent

- Agents
  - set of N miners.
  - Miners' hashing power π_i follows exponential distribution
  - Each miner holds an own memory pool of the current unconfirmed transation(Txs) at time t, $U_i(t)$
  - Ultimatum game strategy set, $S_i = (p_i, q_i)$



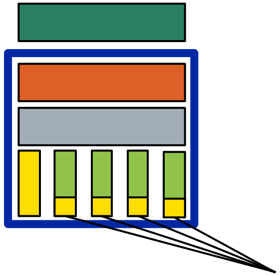
Agent-Based Model - Strategy

Ultimatum Game: When ***mining*** a block b, as proposer, the miner needs to decide how many transactions (Txs) he will include,

Offering Strategy:

- $\boldsymbol{p_i}$**,** a share of unconfirmed Txs from his current memory pool, $U_i(t)$
- limited by block size maximum

$$\theta_b = \min(\lfloor p_i U_i(t) \rceil, \theta^{max})$$



p_i, share of Tx

Agent-Based Model - Strategy

Ultimatum Game: When receiving a block b**,** as a responder, the miner evaluates its fairness to accept or decline,

- **Accepting Strategy:**
  - Accept, if share of the memory pool consumed by the block lower than accepting strategy, q_i .

$$q_i \geq \frac{\theta_b}{U_i(t)}$$

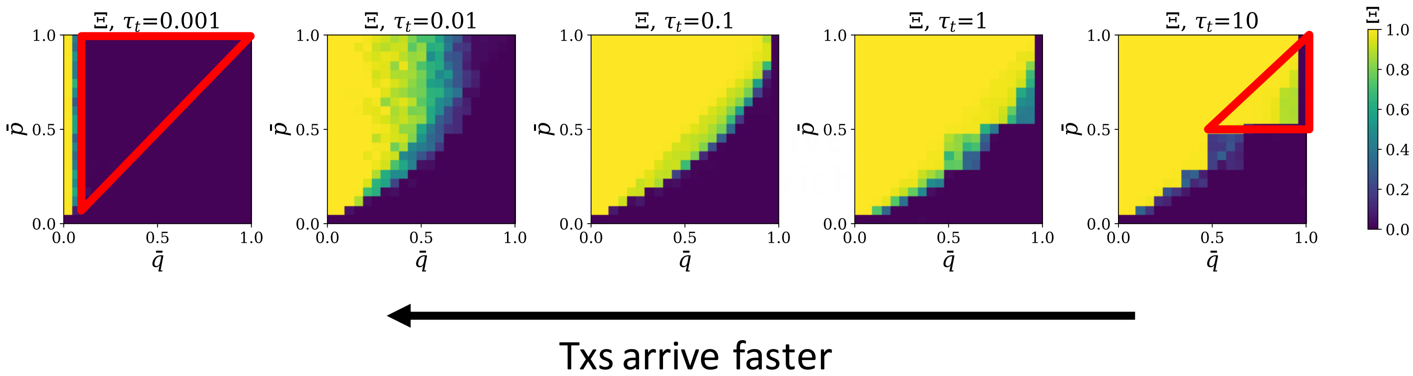
  - Otherwise, decline the block b.

Insight

In absence of block rewards, miners will negotiate over the transaction fees

Global Strategies

Strategies fixed for all nodes: $q_i = \bar{q}\,, p_i = \bar{p}$

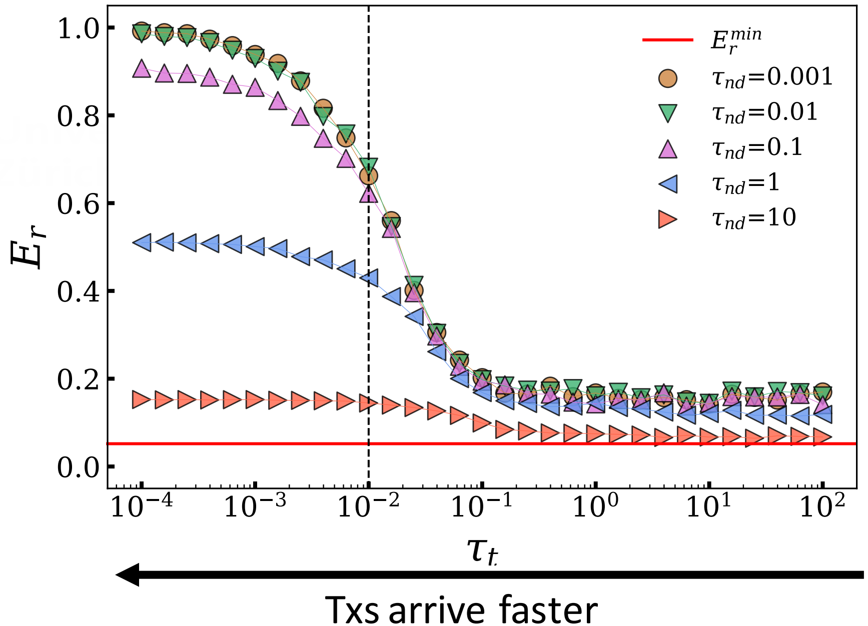


- High supply of transactions enables consensus, even when strategies are not aligned
- Low supply of transactions limits consensus region, as single transaction may lead to unfair block

Random Uniform Strategies

Strategies are randomly assigned following uniform distribution:

$$p_i \sim U(0,1), q_i \sim U(0,1)$$

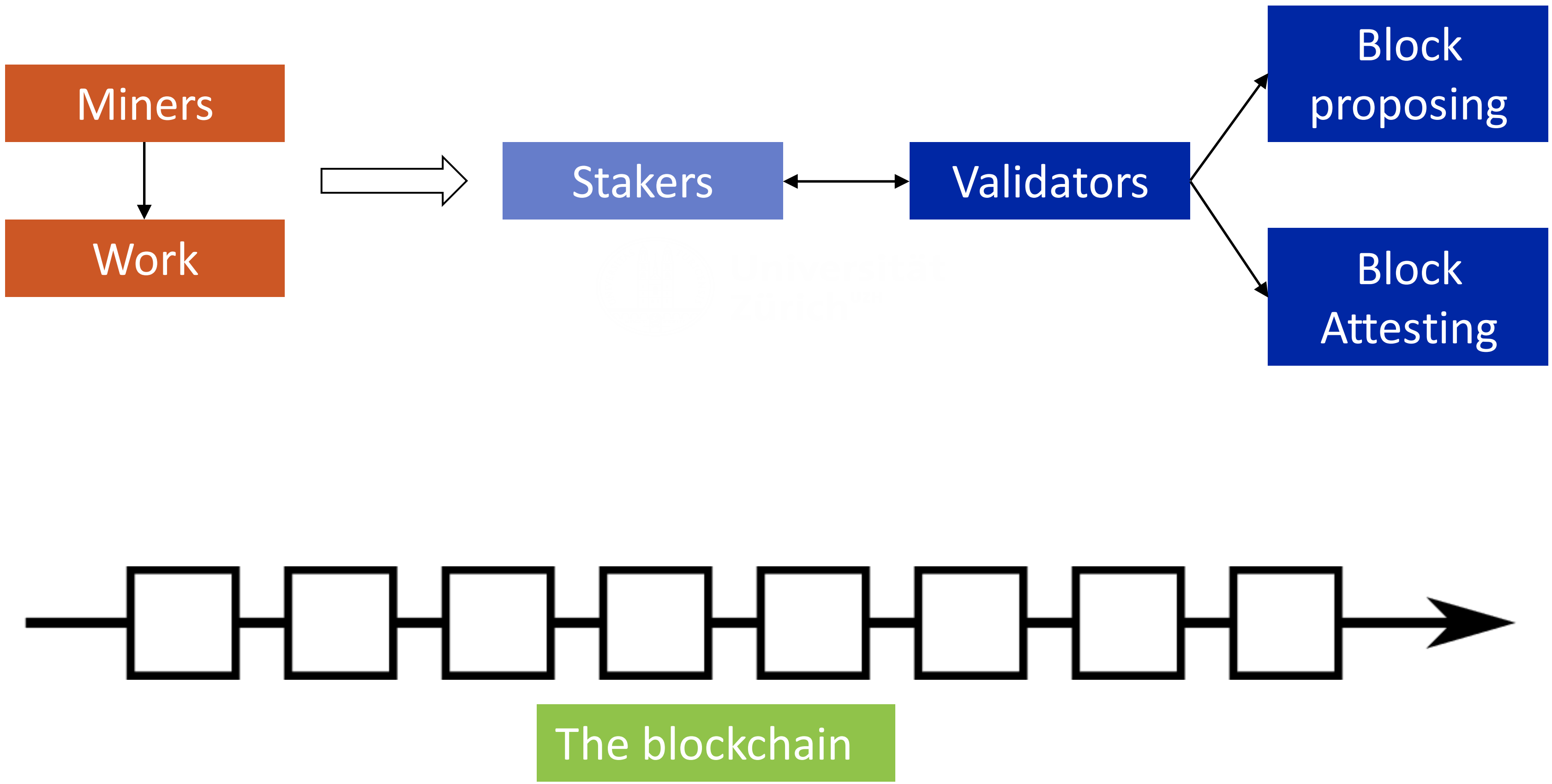


Relative efficiency:

Increasing supply of transaction stimulates the **local** consensus

Ethereum Consensus

Ethereum Proof-of-Stake



The Agents: Ethereum Validators

- The agents represent Ethereum validators
- Agents are assumed to be ***honest***
- Validators are connected in a non-trivial peer-to-peer network
  - We use ***Erdős–Rényi*** random model to generate the peer-to-peer topology
  - The topology is static: nodes and edges do not change

Agents' State

Each agent is characterized by two state variables:

- The collection of received ***blocks***
- The collection of received ***attestations***

Keypoint

At every step, the variables inform the agent's decision on the head of the canonical chain using LMD-GHOST

An event happens when

the state of the system changes

Event Typologies

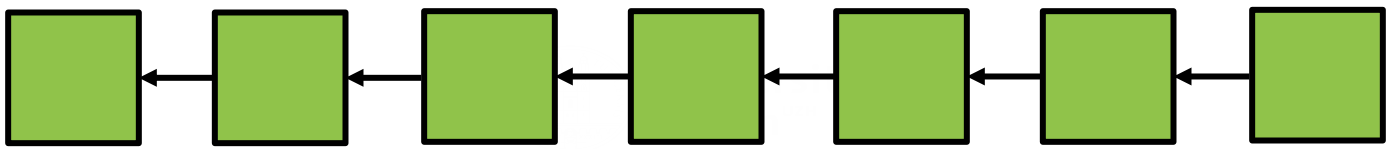
We assume 4 different events, divided in two categories:

- Random time events:
  - Block gossiping :τ_{block}: average gossip event waiting time
  - Attestation gossiping :$\tau_{attestation}$: average gossip event waiting time
- Fixed time events:
  - Block proposal: every T_{slot}(12) seconds
  - Attestation threshold :4 seconds after block proposal

The output of one simulation is a blocktree: the collection of all blocks created during the simulation

The topology of the blocktree serves as an indicator of the consensus efficiency

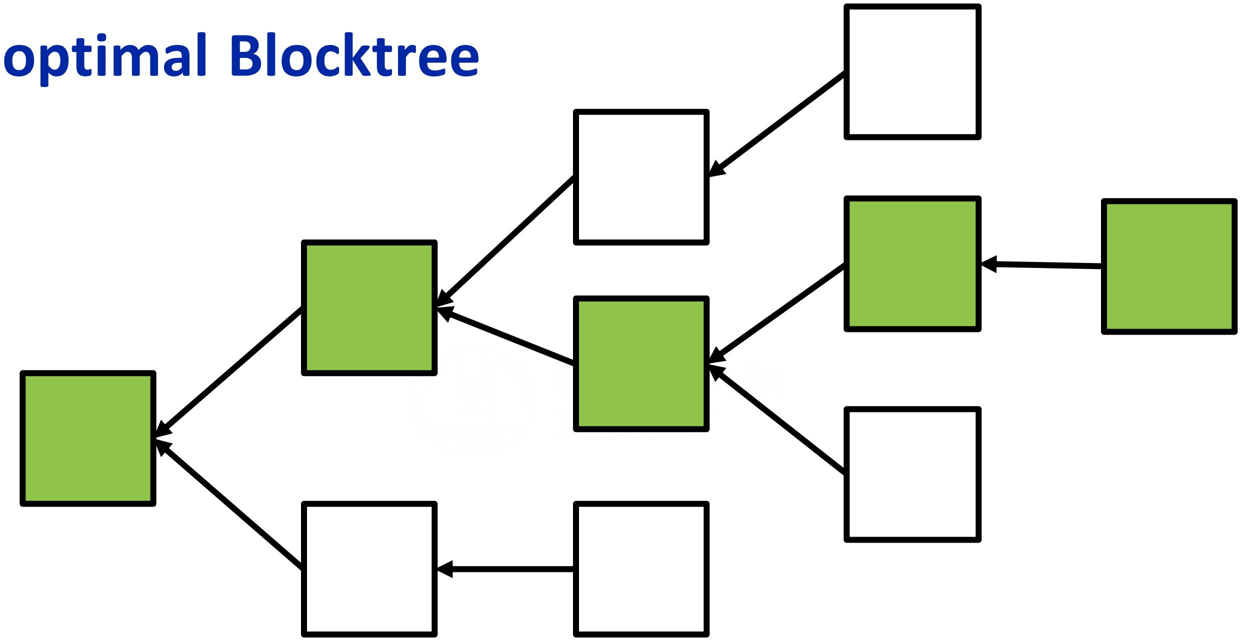
A Sub-optimal Blocktree



No wasted blocks

Canonical chain = Blocktree

A Sub-optimal Blocktree



Wasted blocks

Canonical chain ≠ Blocktree

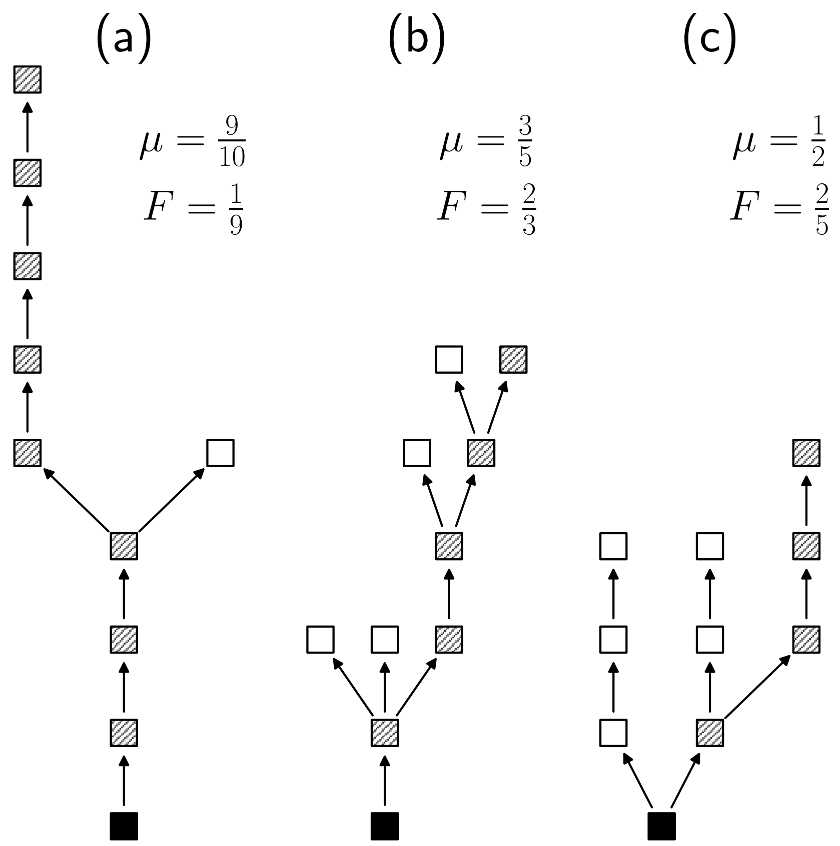
Blocktree Measures

Mainchain rate:

$$\mu = \frac{M}{B} = 1 - \frac{\Theta}{B}$$

Branch ratio:

$$F = \frac{1}{|M|} \sum_{b \in M} \sum_{c \in \Theta} \delta(p(b), p(c))$$



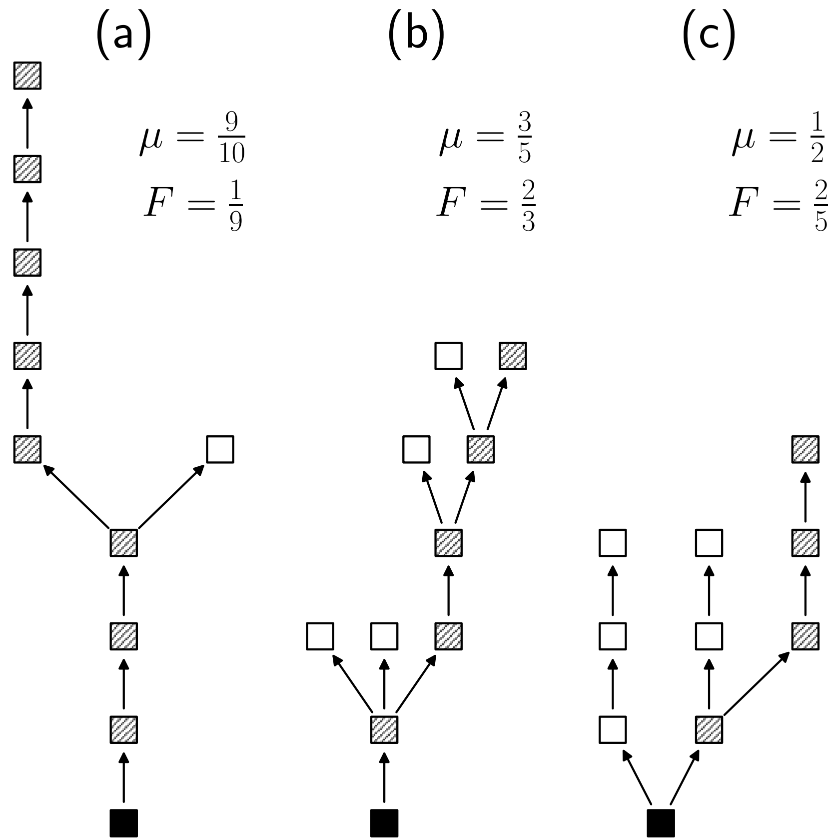
Blocktree Measures

Mainchain rate:

$$\mu = \frac{M}{B} = 1 - \frac{\Theta}{B}$$

Branch ratio:

$$F = \frac{1}{|M|} \sum_{b \in M} \sum_{c \in \Theta} \delta(p(b), p(c))$$



Simulation Parameters

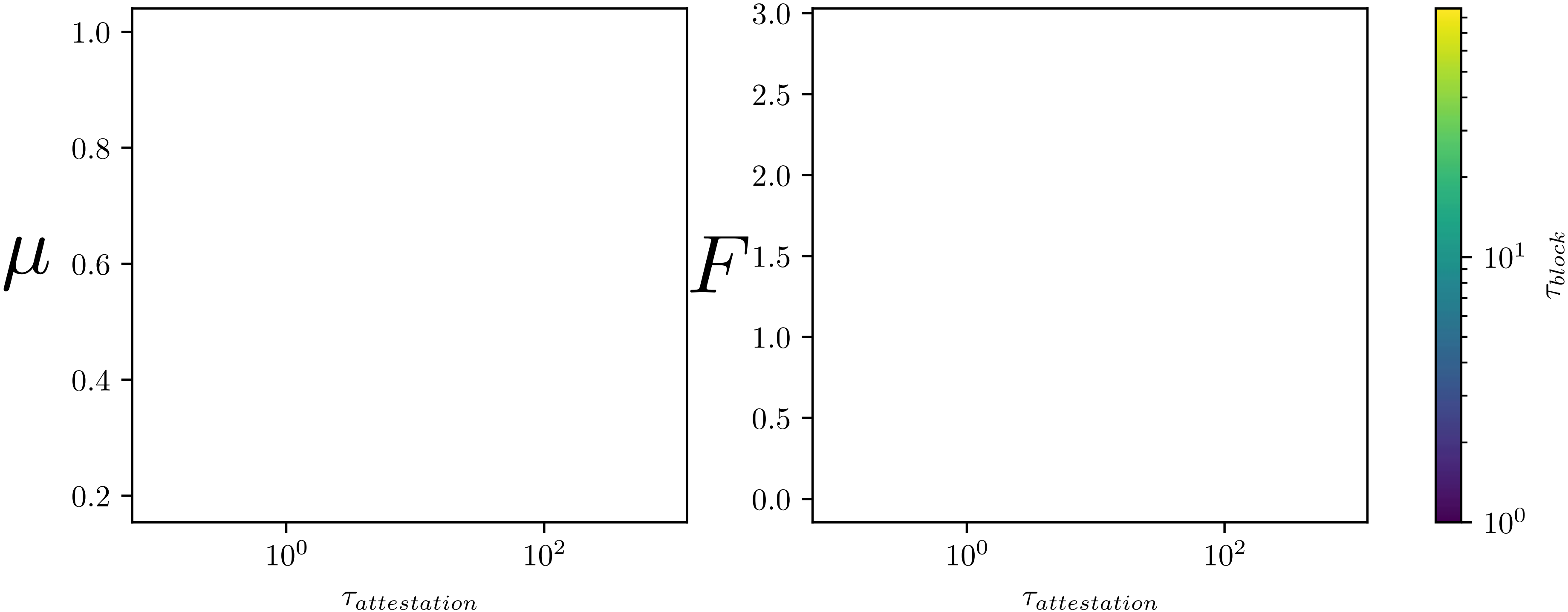
The control parameters of the simulation framework are:

- τ_{block} the block gossip average waiting time
- $\tau_{attestation}$ the attestation gossip average waiting time
- N the size of the peer-to-peer network
- k the average degree of the peer-to-peer network

Results

1. The effect of attestation latency is negligible with respect to block latency
2. Consensus undergoes a phase transition with respect to the control parameter τ_{block}

Attestion Gossip Latency Effect on Consensus



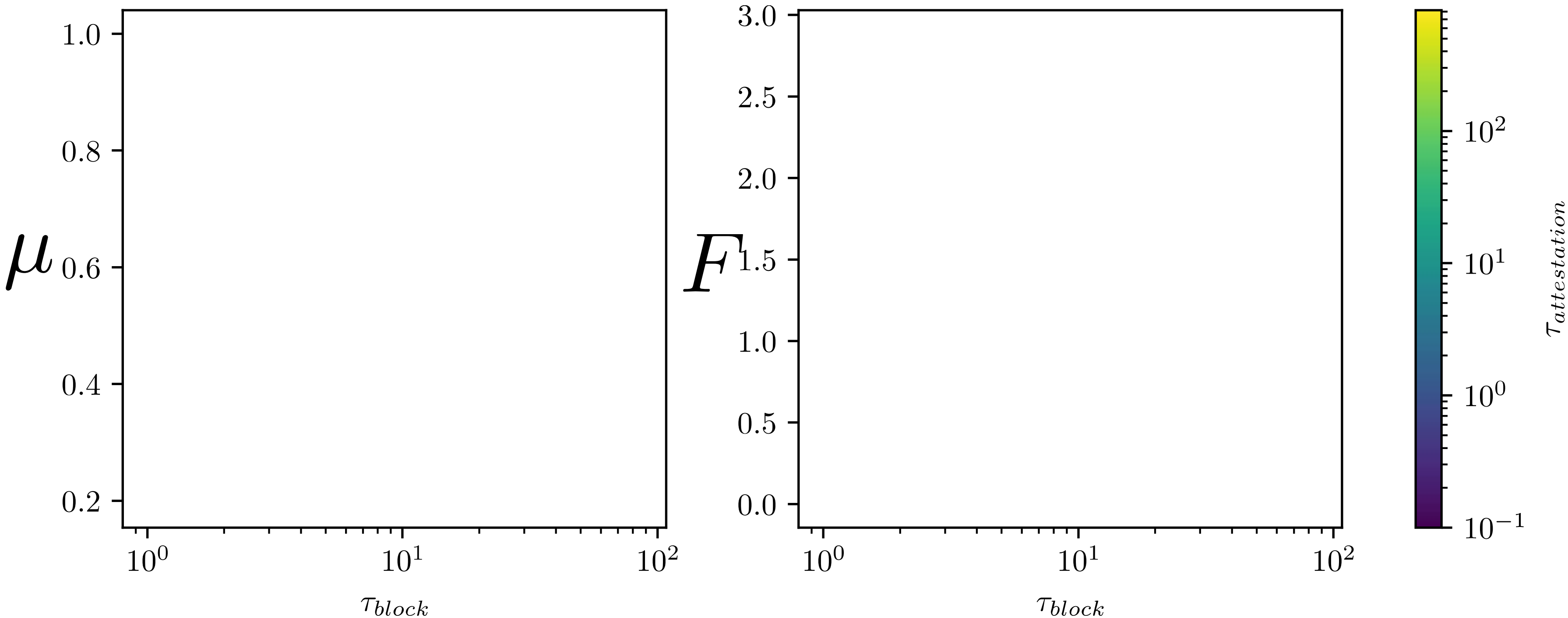
Underlying topology is ER with $N = 128$ and $k = 8$

Results

1. The effect of attestation latency($\tau_{\text{attestation}}$) is negligible with respect to block latency

2. Consensus undergoes a phase transition with respect to the control parameter τ_{block}

Block Gossip Latency Effect on Consensus



Underlying topology is ER with $N = 128$ and $k = 8$

Hypothesis

The system goes out of consensus when the average time for a block to be gossiped to all the agents is larger than the slot time

Can we predict when the system transitions out of consensus?

Out of Consensus: the Phase Transition Threshold

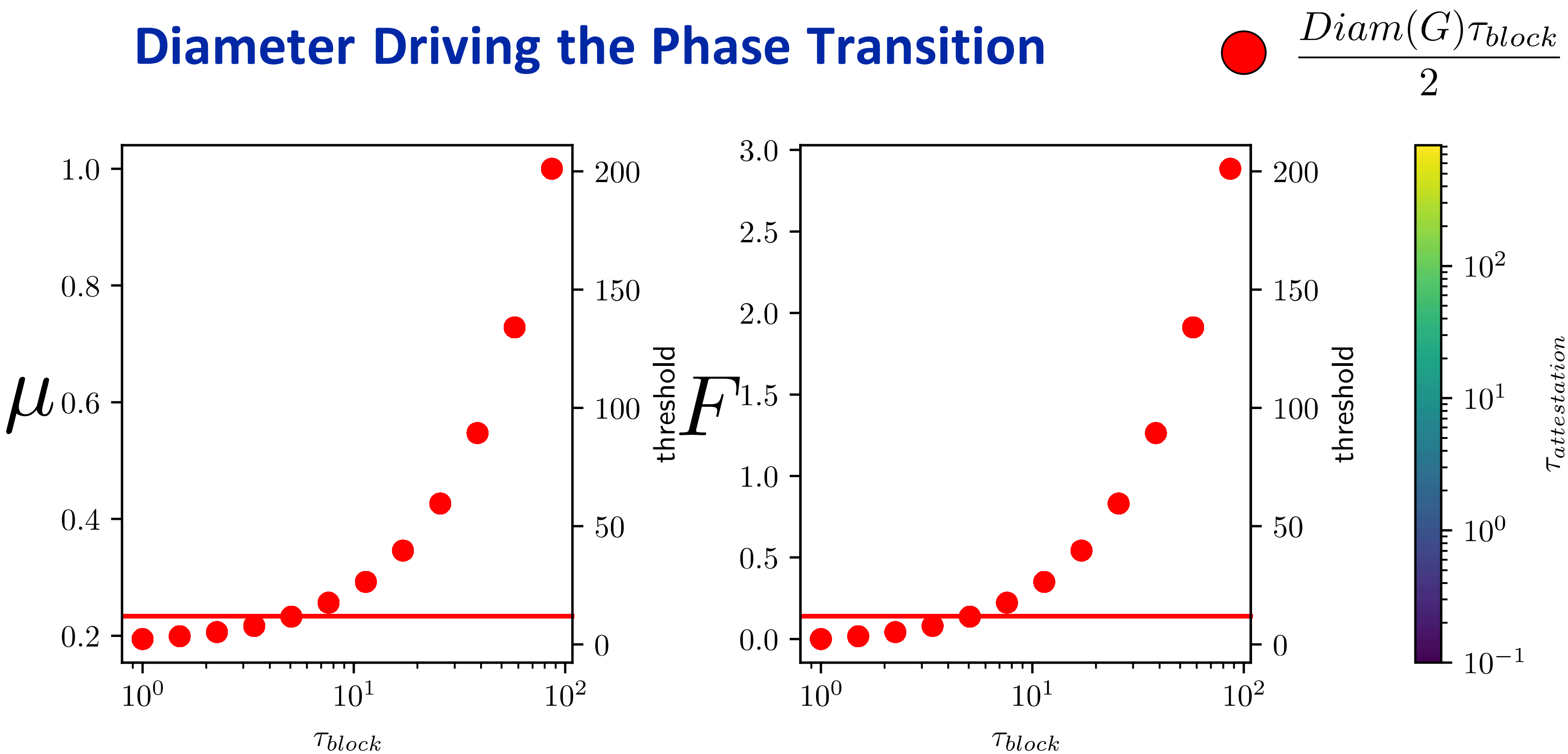
Control parameter

$$\frac{Diam(G)\,\tau_{block}}{2} > T_{slot}$$

Threshold

Diameter

Diameter Driving the Phase Transition



Underlying topology is ER with $N = 128$ and $k = 8$

Conclusion

By measuring the diameter of the peer-to-peer network we are able to predict the block gossip latency threshold which will drive the the system out of Consensus

Vol. 7 (2022)

The Journal of Cryptocurrency and Blockchain Technology Research

LEDGER

ledgerjournal.org

Universität Zürich[UZH]

UZH
Blockchain Center

Blockchain & DLT Research Group

Universität Zürich UZH

UZH Blockchain Center

Blockchain & DLT Research Group

Claudio J. Tessone

Blockchain & Distributed Ledger Technologies

UZH Blockchain Center

@ claudio.tessone@uzh.ch

https://www.blockchain.uzh.ch

in company/uzh-blockchain-center