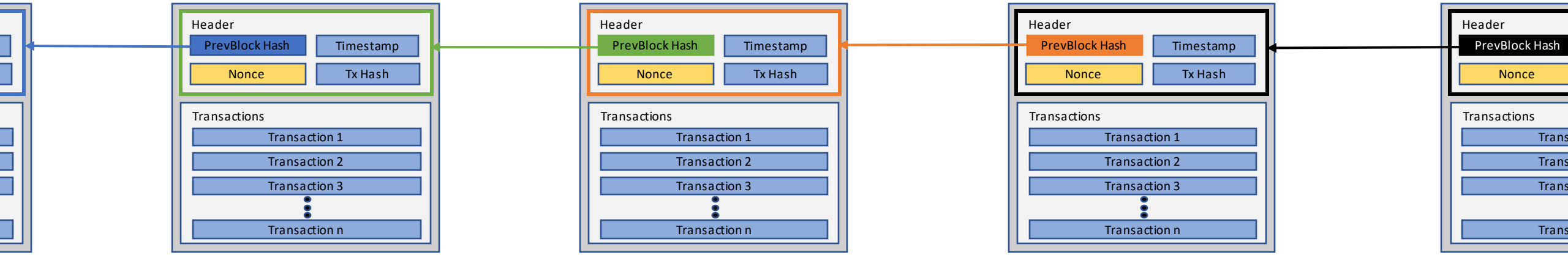
Bitcoin-NG

CS 839 – Kai Mast

Nakamoto Consensus so far



(Some block content is not shown for brevity)

- Leaders are elected by solving the PoW puzzle (finding a correct nonce value)
- Each block contains transactions
- In Bitcoin, blocks are big (1Mb) and infrequent (every 10 minutes)
  - Set to reduce likelihood of forks
  - Throughput is about 4 transactions/second and latency about 1hr

Bitcoin-NG

- Published in 2016 at NSDI
- Authors are Ittay Eyal, Adem Efe Gencer, and Emin Gün Sirer
- High-Level idea: Split leader election from proposing transactions
- Protocol used by multiple real-world blockchains, e.g., aeternity

Ittay Eyal
(Technion and IC3)

Adem Efe Gencer
(LinkedIn)

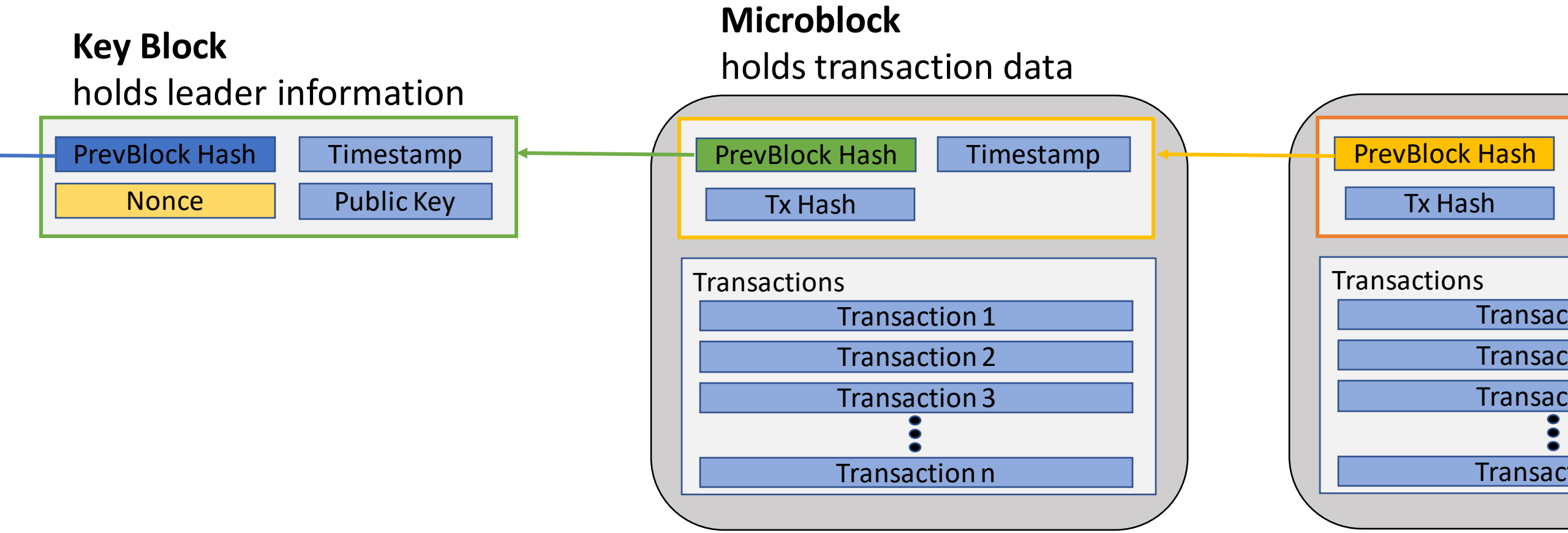
Emin Gün Sirer
(Cornell, Ava Labs,
and IC3)

Bitcoin-NG: Intuition

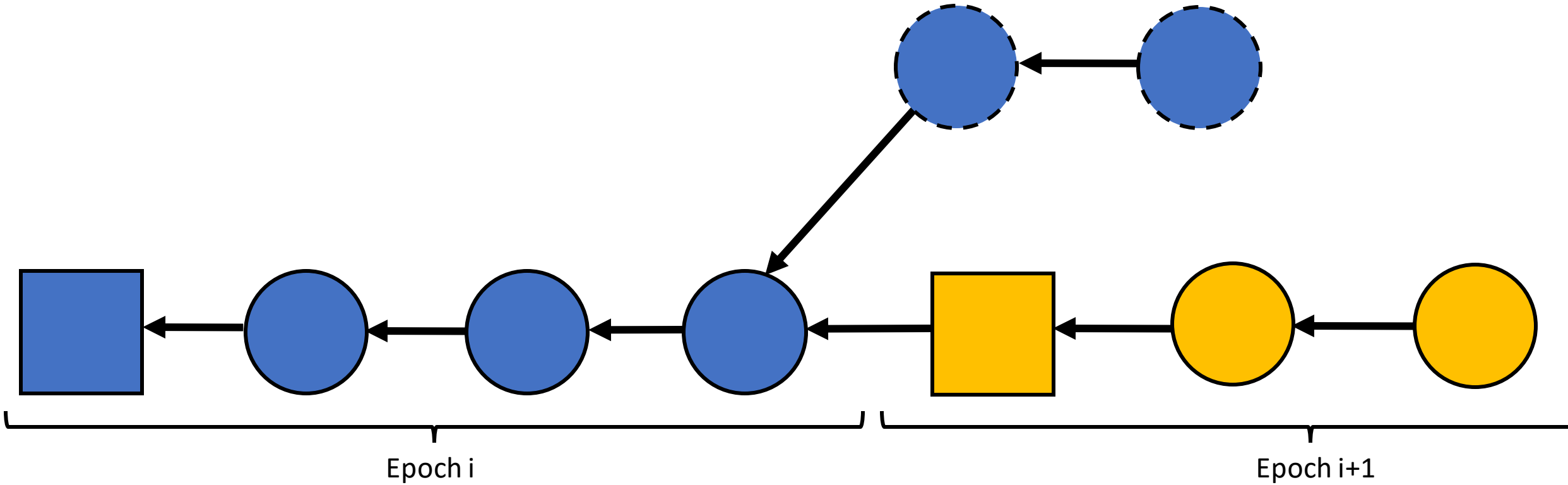
Idea: Separate leader election from block generation

- Key blocks contain leader information
- Once a key block is mined, the leader stays in power until the next key block is mined
- A leader can continuously publish microblocks, which contain transactions, during their tenure
  - Allows leveraging the entire bandwidth of the leader

Key Blocks vs. Microblocks

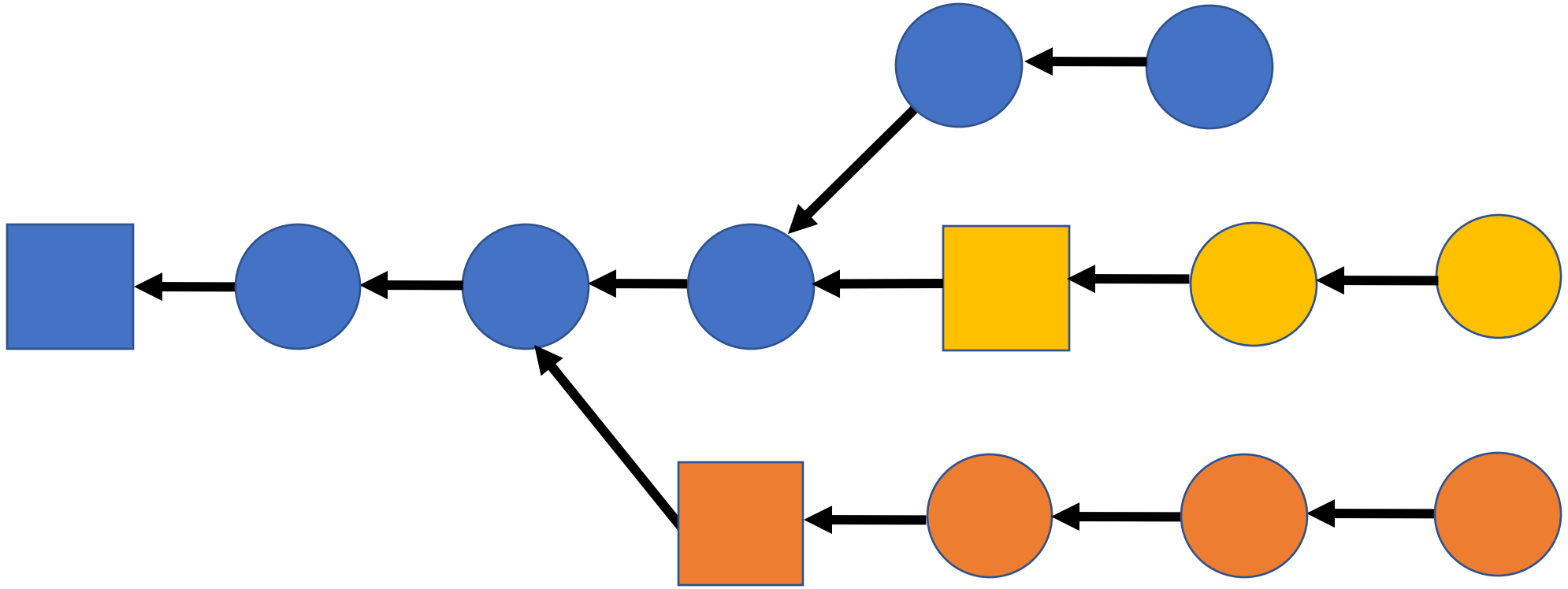


Blockchain Structure: Microblock Forks



Forks do not undo the entire epoch, but only the last few microblocks!

Blockchain Structure: Key Block Forks



Like in Bitcoin, concurrent leaders can exist and chains can be forked at any time

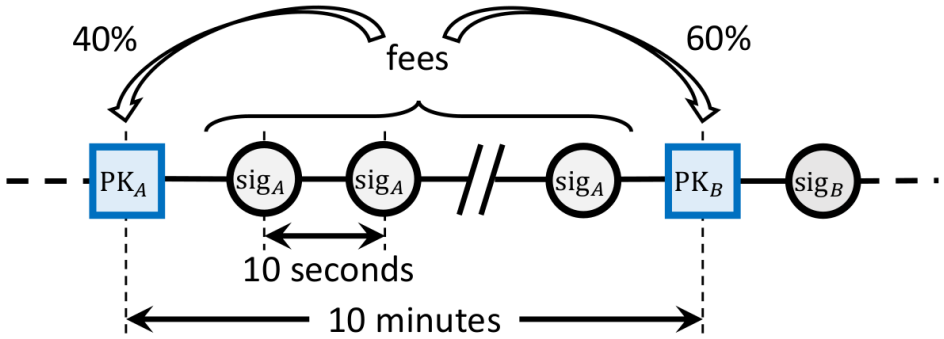
Incentive Structure

Problem:

- Microblocks do not count towards chain weight/length
- The next miners might exclude microblocks so they, reinclude the block's transactions

Solution:

- Split fee between current and next leader
- Next leader needs to get most of the reward (60%) to be incentivized to include the transaction



Transaction Fee Split: Case 1

$$\overbrace{\alpha \times 100\%}^{\text{Win } 100\%} + \overbrace{(1-\alpha) \times \alpha \times (100\% - r_{\text{leader}})}^{\text{Lose } 100\%\text{, but mine after txn}} < r_{\text{leader}} \quad \alpha{=}0.25 \quad r_{\text{leader}} > 37\%$$

- Miner might want to hide the microblock and only mine on it themselves
- In the best case, they win the full transaction fee
- If they lose, the miner can still mine on top of another miner's microblock that contains the transaction

Transaction Fee Split: Case 2

$$\overbrace{r_{\text{leader}}}^{\text{Place in microblock}} + \overbrace{\alpha(100\% - r_{\text{leader}})}^{\text{Mine next key block}} < \overbrace{100\% - r_{\text{leader}}}^{\text{Mine on existing microblock}}, \quad \alpha{=}0.25 \quad r_{\text{leader}} < 43\%$$

- Miner might want to mine on an older microblock and include the block's content in their own microblock
- In the best case, they win the leader fraction of the fee, or even the full fee if they mine the next two key blocks
- Transaction fee share of the current leader must be **less** than that of the next

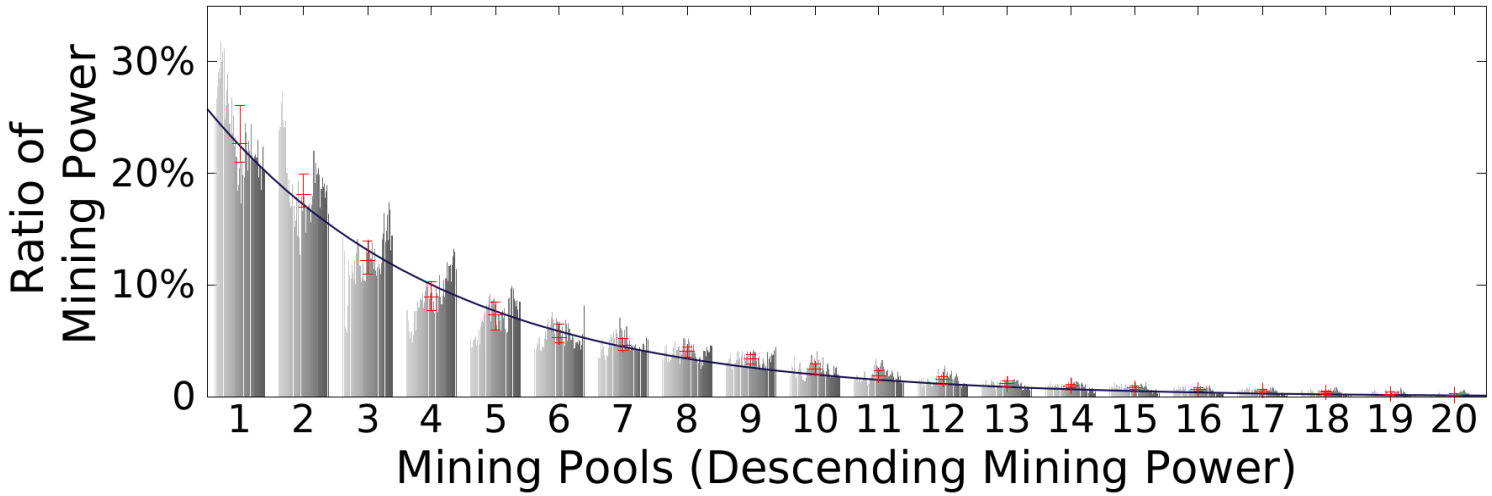
Microblock Fork Prevention

Problem: Malicious miners might publish conflicting microblocks

- If a conflicting microblock is published, punish the miner using a *poison transaction* (similar to a fraud proof in plasma)
- A poison transaction contains a reference to the first block in an invalid microblock branch, i.e., one that is created by two competing microblocks not a key block
- Poison transactions must be published in within the block's maturity window (before block reward can be spent)
- The malicious leader then loses all of the block rewards

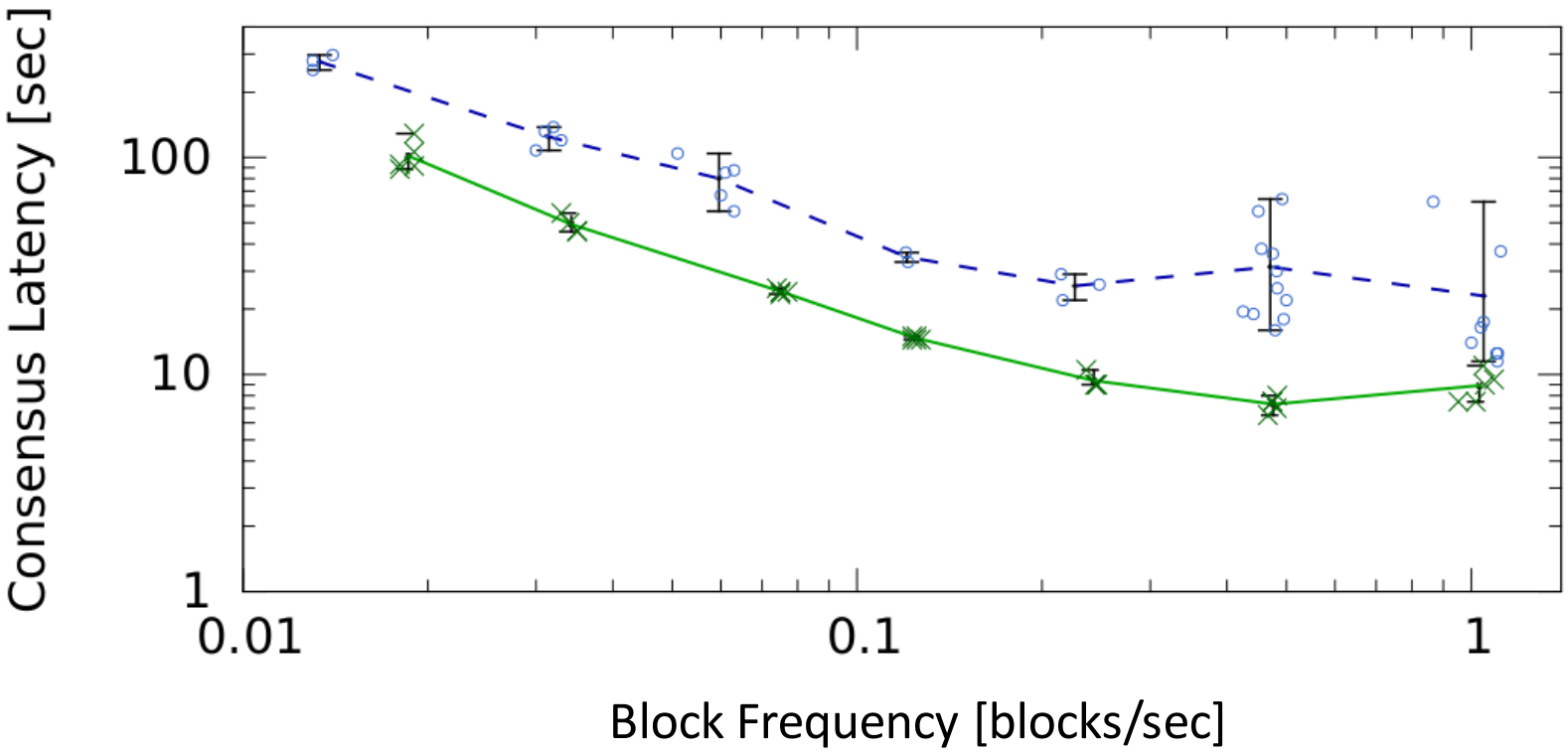
Experimental Setup

- Large scale evaluation with 1000 nodes
- Mining is simulated using a random function
- Each node is connected to 5 peers at random
- Latencies and mining powers are assigned based on the distribution observed in the real Bitcoin network



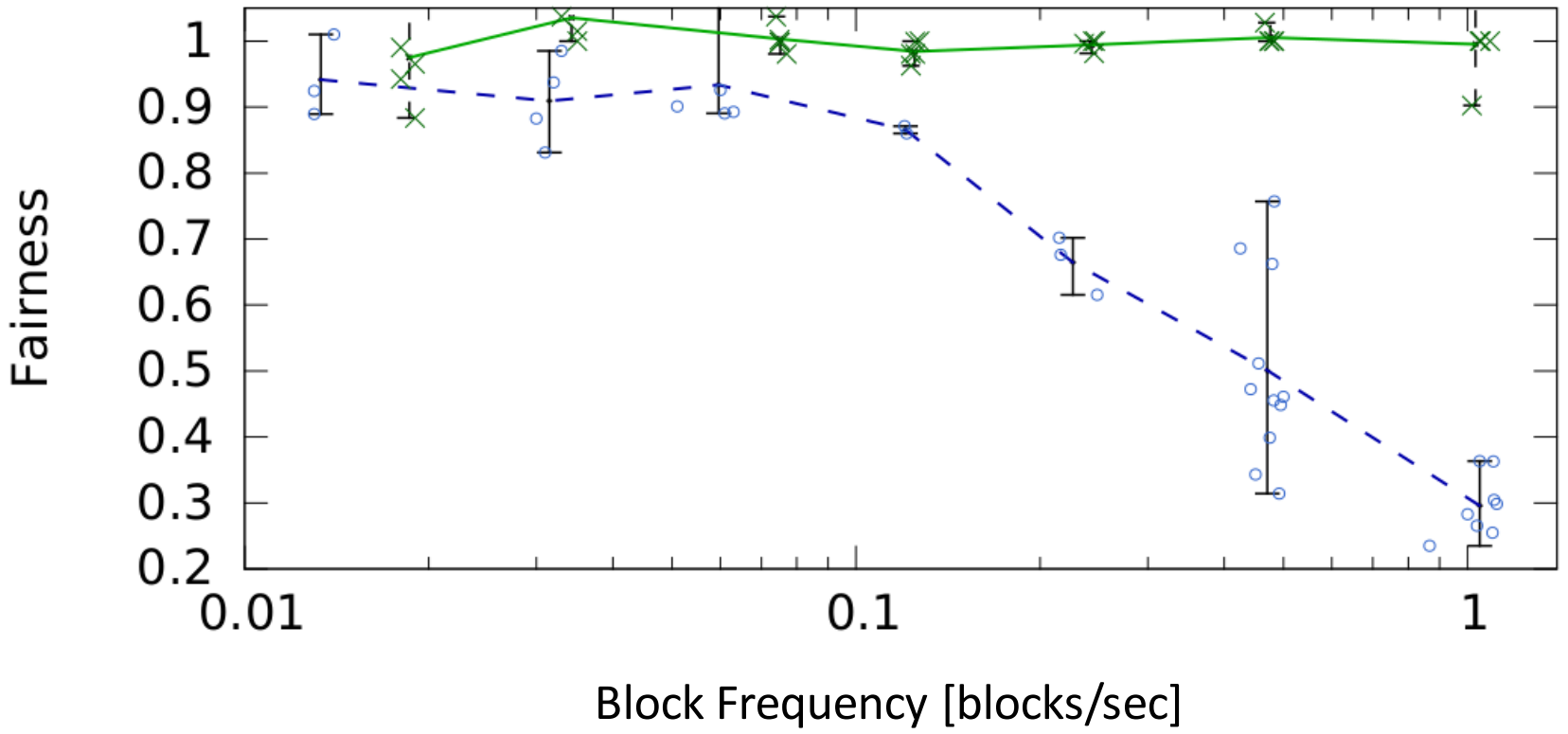
Evaluation: Consensus Delay

How long does it take for the majority of network to "see" a block?



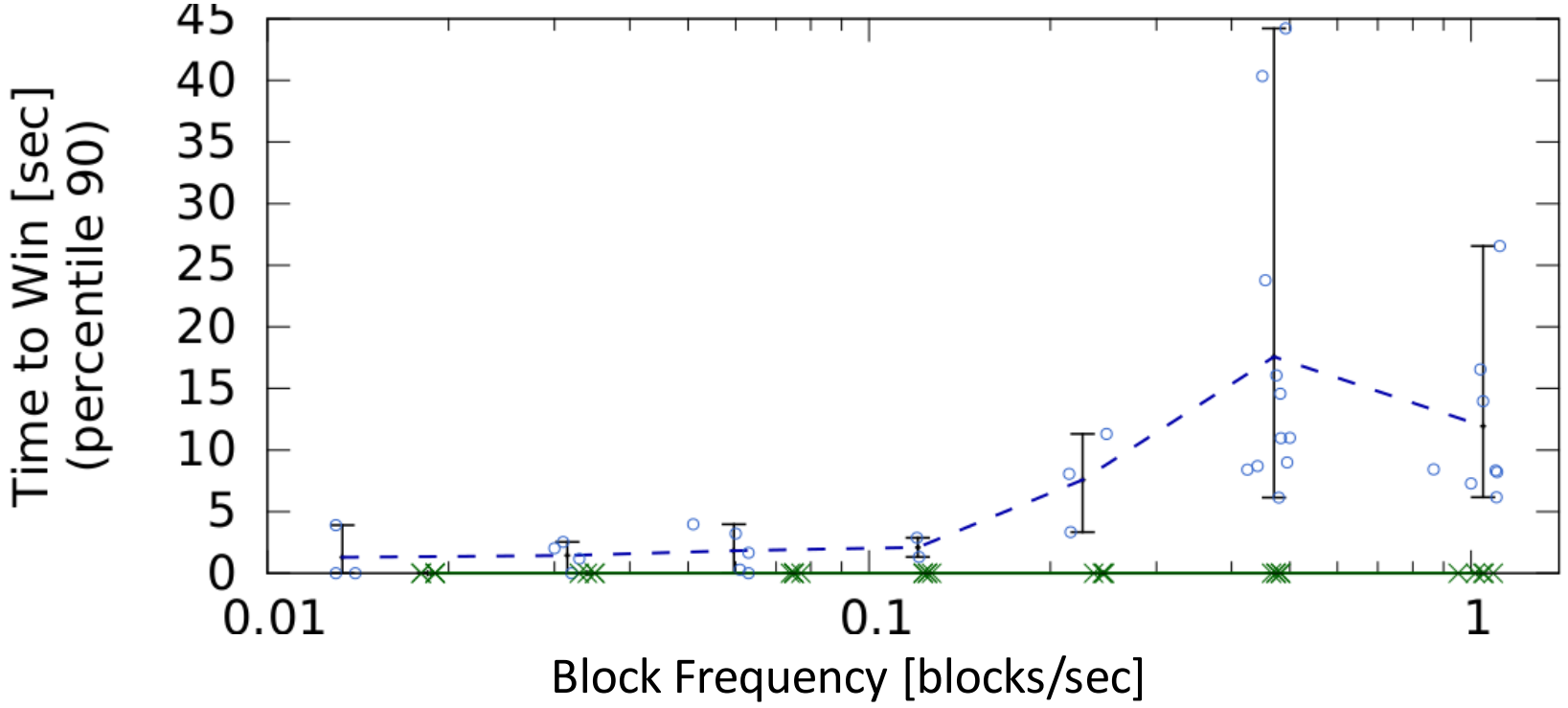
Evaluation: Fairness

What fraction of blocks are not generated by the largest miner?



Evaluation: Time to Win

How long does it take until a new block is part of the longest chain?

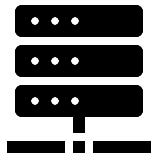


Discussion

- Thoughts on Bitcoin-NG in general?
- How does it affect (de-)centralization?
  - It is fairer and more decentralized than regular Bitcoin
- Is it more vulnerable to denial-of-service attacks?
  - Switching public keys every epoch helps to mitigate DoS attacks

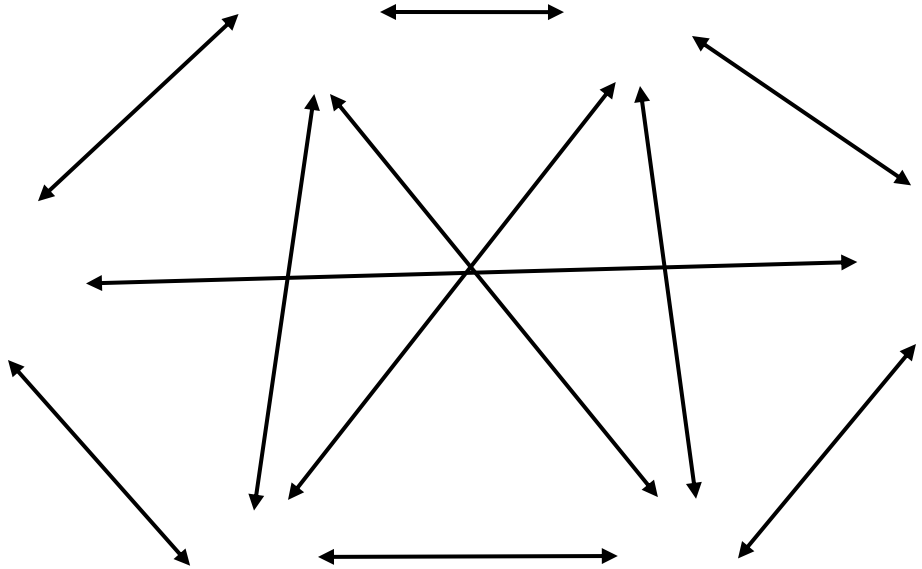
ByzCoin

- **Idea:** Reduce latency by having the last k miners sign off a transaction
- Builds on some ideas from Bitcoin-NG
- Forms the basis for OmniLedger (lecture on 11/2)
- Published in 2016 at USENIX Security
- Authors: Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford (EPFL)



Recap: PBFT

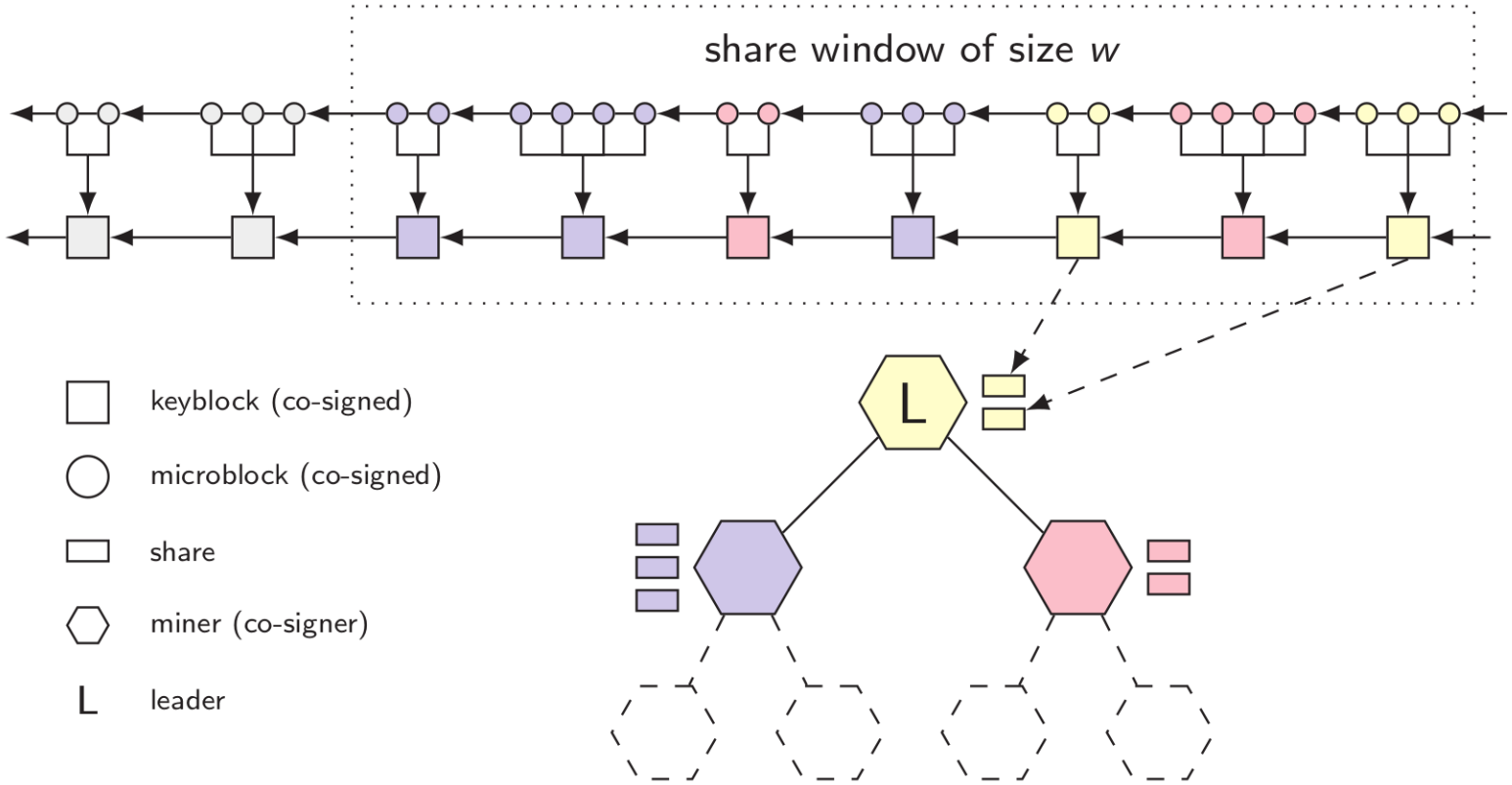
- Leader is elected using a view-change mechanism
- Leader proposes transaction batches
- 2/3 of replicas must sign off transaction batches for them to be accepted



ByzCoin Blockchain Structure

Microblock chain contains Transaction data

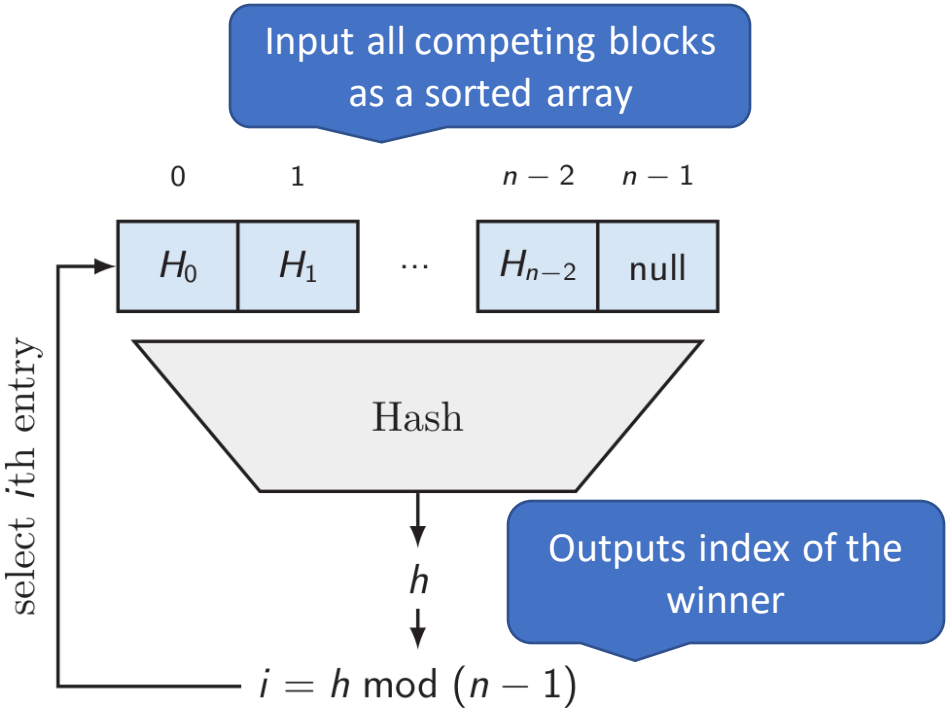
Key block chain contains leader information (can be based on PoW or some other mechanism)



- 2/3 of the quroum need to sign off each microblock
- Quroum membership and voting power is defined by how many key blocks were mined

Leader Election and Conflicting Leaders

- The most recently mined block determines who is the leader
  - Each new key blocks initiates a view change
  - Much easier to implement than PBFT view changes
- The new leader first needs to sign off on the most recent microblocks
  - Requires 2f+2 votes (all previous members and the new one)
- If there are conflicting blocks, a cryptographic hash function serves a tie breaker
  - Tricking the hash function is as hard as finding a new block



Confirmation times in ByzCoin

Transactions are confirmed **almost immediately**

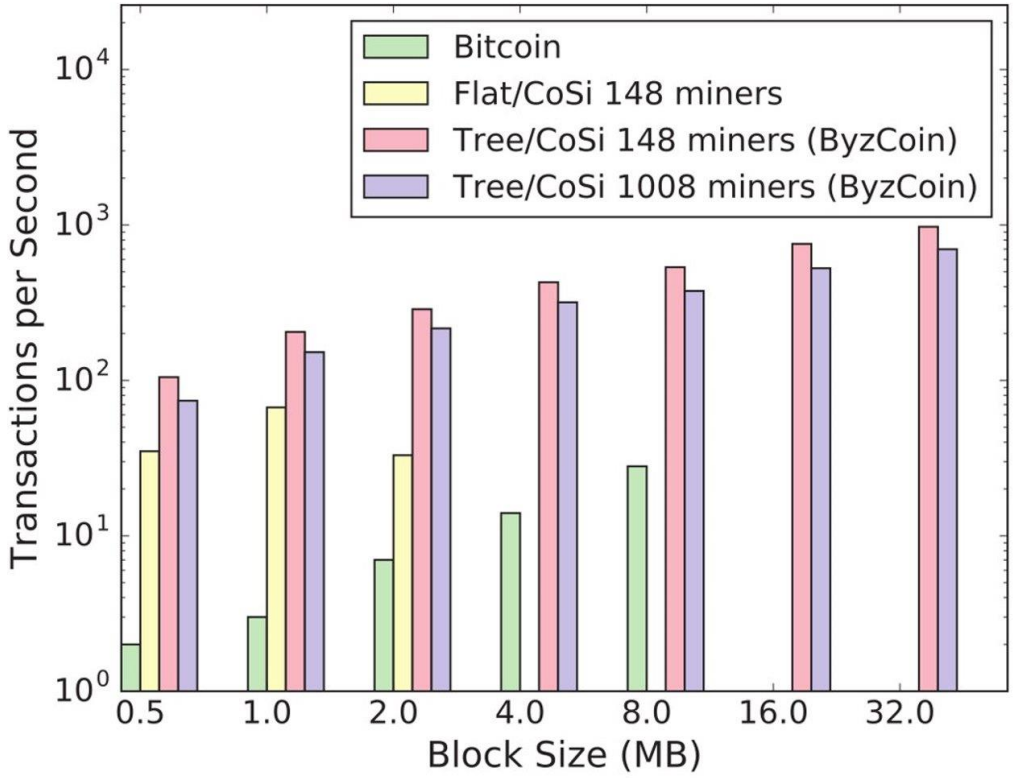
- Assuming a large enough window size, every transaction is immediately signed off by a majority of the mining power
- Transactions are, thus, assumed final as soon as they are included in a microblock

Incentives in ByzCoin

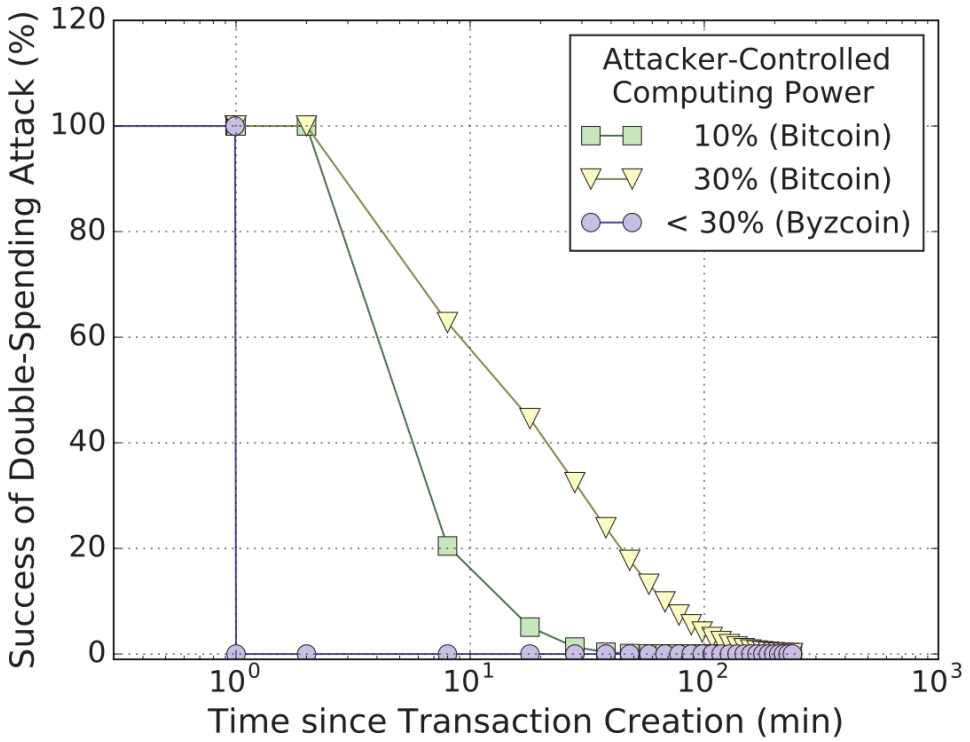
- Block rewards and transaction fees are split between all current committee members
  - Incentivizes members to stay online and available
- No need to split fees between new and old leader, like in Bitcoin-NG
  - Voting after view change ensures the most recent microblock is included

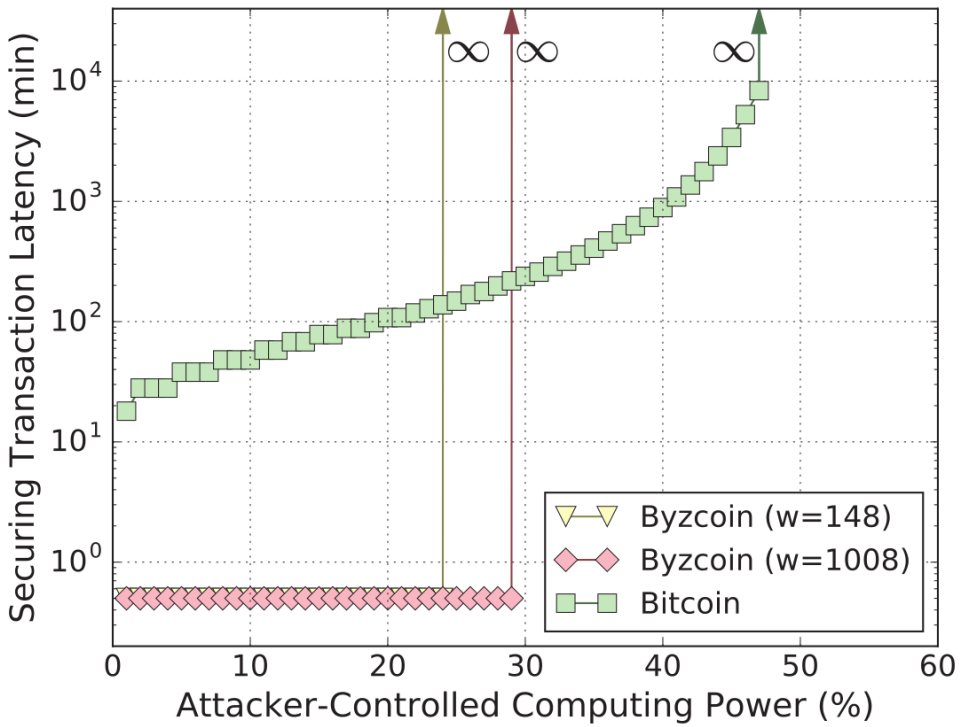
ByzCoin Evaluation

- Evaluation on up to 1008 nodes running on a total of 36 physical machines
- Network is simulated to be wide-area
  - 20ms latency
  - 35Mbps throughput
- Result: About a 100x improvement over Bitcoin in throughput
- Implementation available here: https://github.com/DeDiS/Cothority



ByzCoin Confirmation Delay





Based on formal evaluation, not experimental data!

ByzCoin Discussion

- Thought on the protocol in general?
- What happens if a leader is malicious?
  - Committee will not sign off on blocks
  - Worst case: Not transactions are processed until a new leader is appointed
- Would you build a system using Bitcoin-NG, ByzCoin, or neither?
  - Aeternity uses Bitcoin-NG
  - ByzCoin is the foundation for OmniLedger, a protocol similar to ETH2.0

That's all for today

- Conclusion:
  - Bitcoin-NG increases Bitcoin's throughput and fairness
  - ByzCoin provides virtually instant confirmation
- Next lecture: Oracles and DECO
  - Will be Zoom-only again!