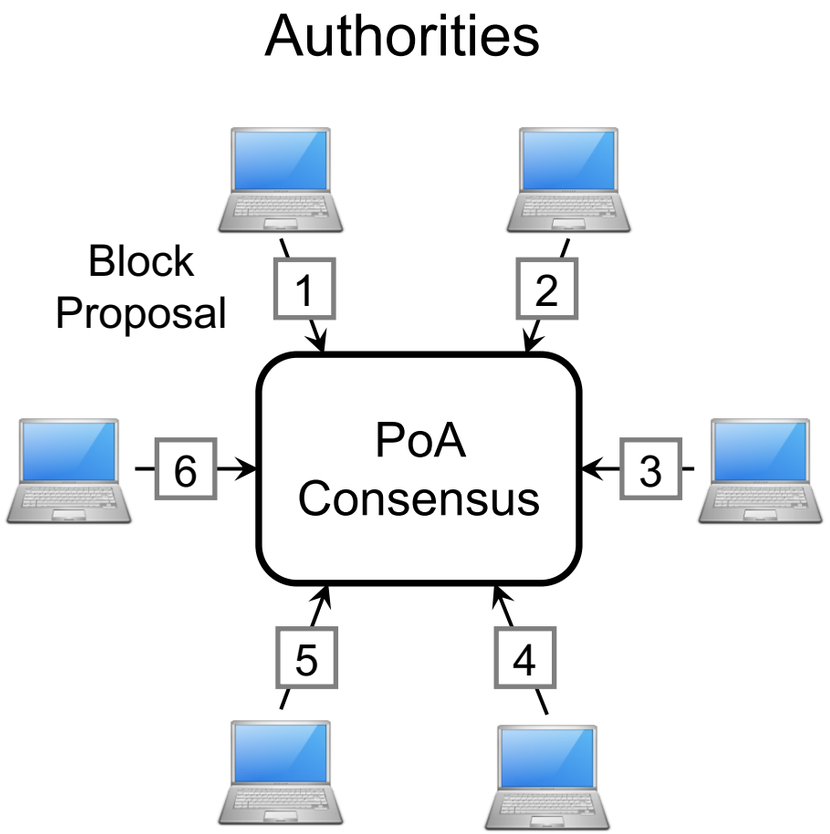
Enhancing Ethereum PoA Clique Network with DAG-based BFT Consensus

Yongrae Jo and Chanik Park

Pohang University of Science And Technology

Proof of Authority (PoA)



- Consensus for permissioned blockchain
  - Only a few messages for block agreement
  - Efficient than proof-of-work (PoW)

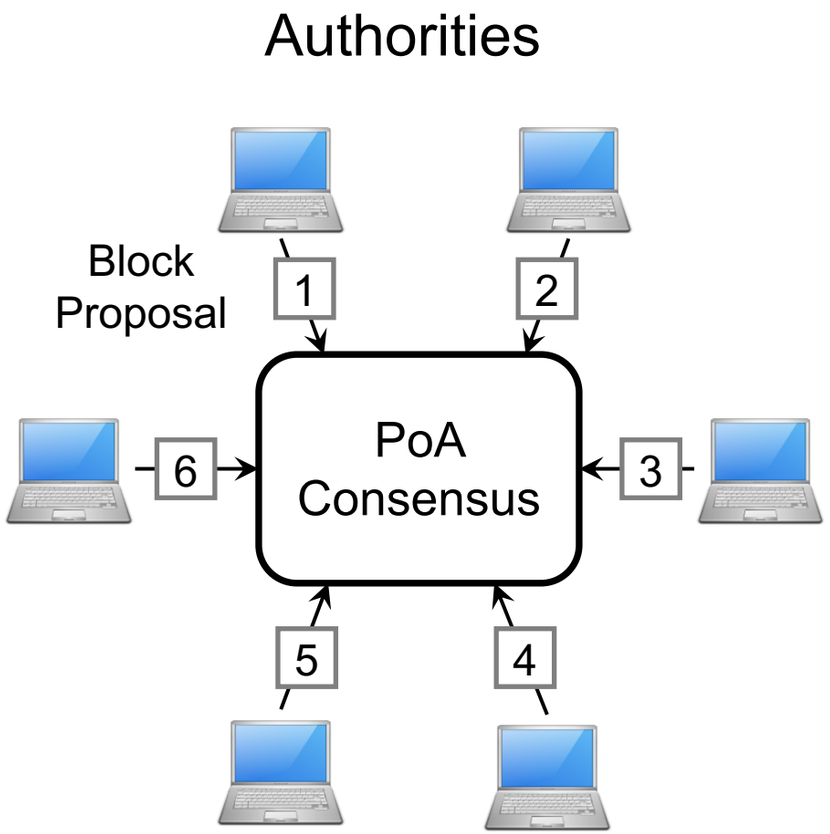
BNB CHAIN

CONSENSYS

Go Ethereum

HYPERLEDGER BESU

Proof of Authority (PoA)



- Consensus for permissioned blockchain
  - Only a few messages for block agreement
  - Efficient than proof-of-work (PoW)

BNB CHAIN

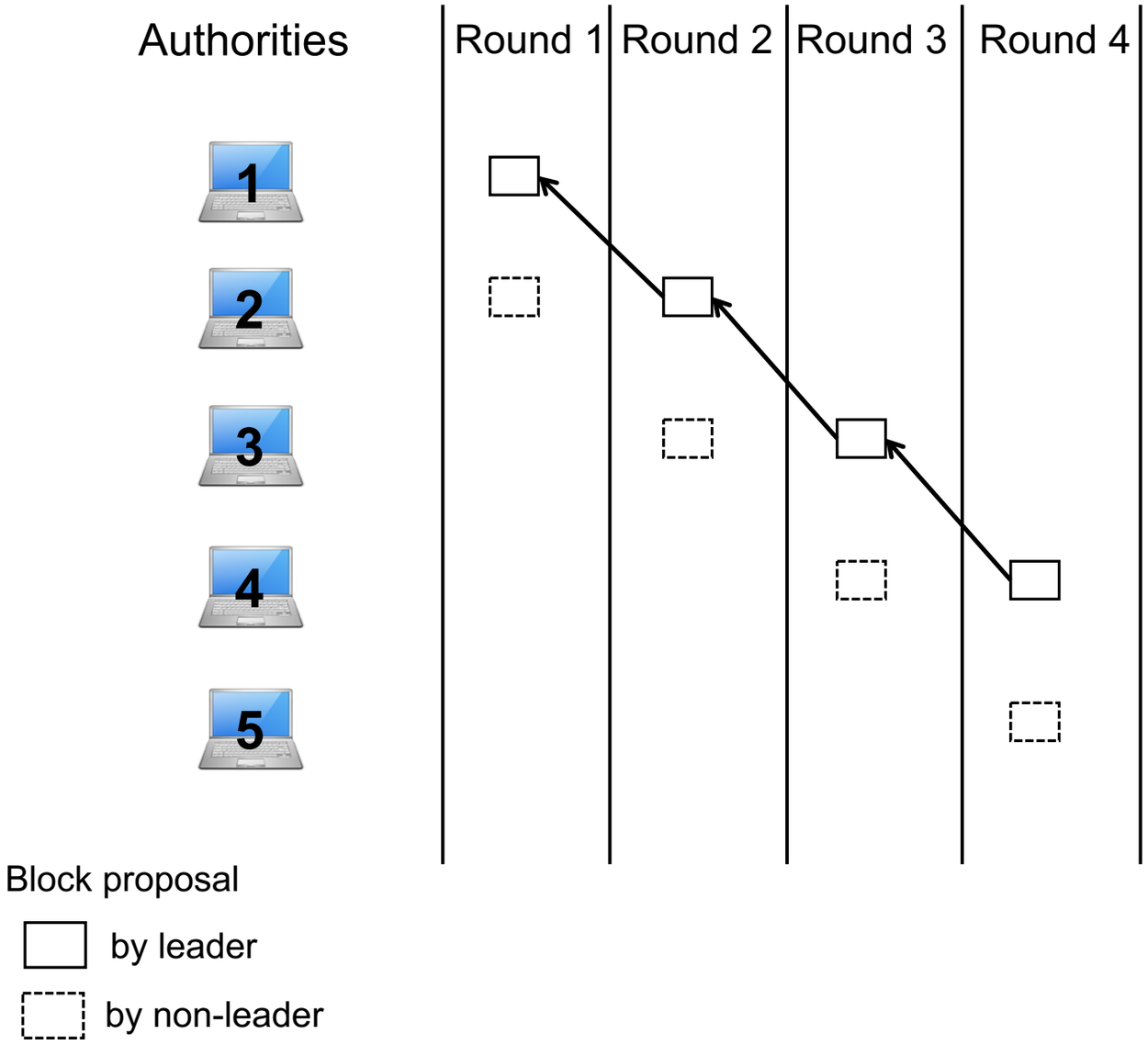
CONSENSYS

Go Ethereum

→ **Clique** (our focus)

HYPERLEDGER BESU

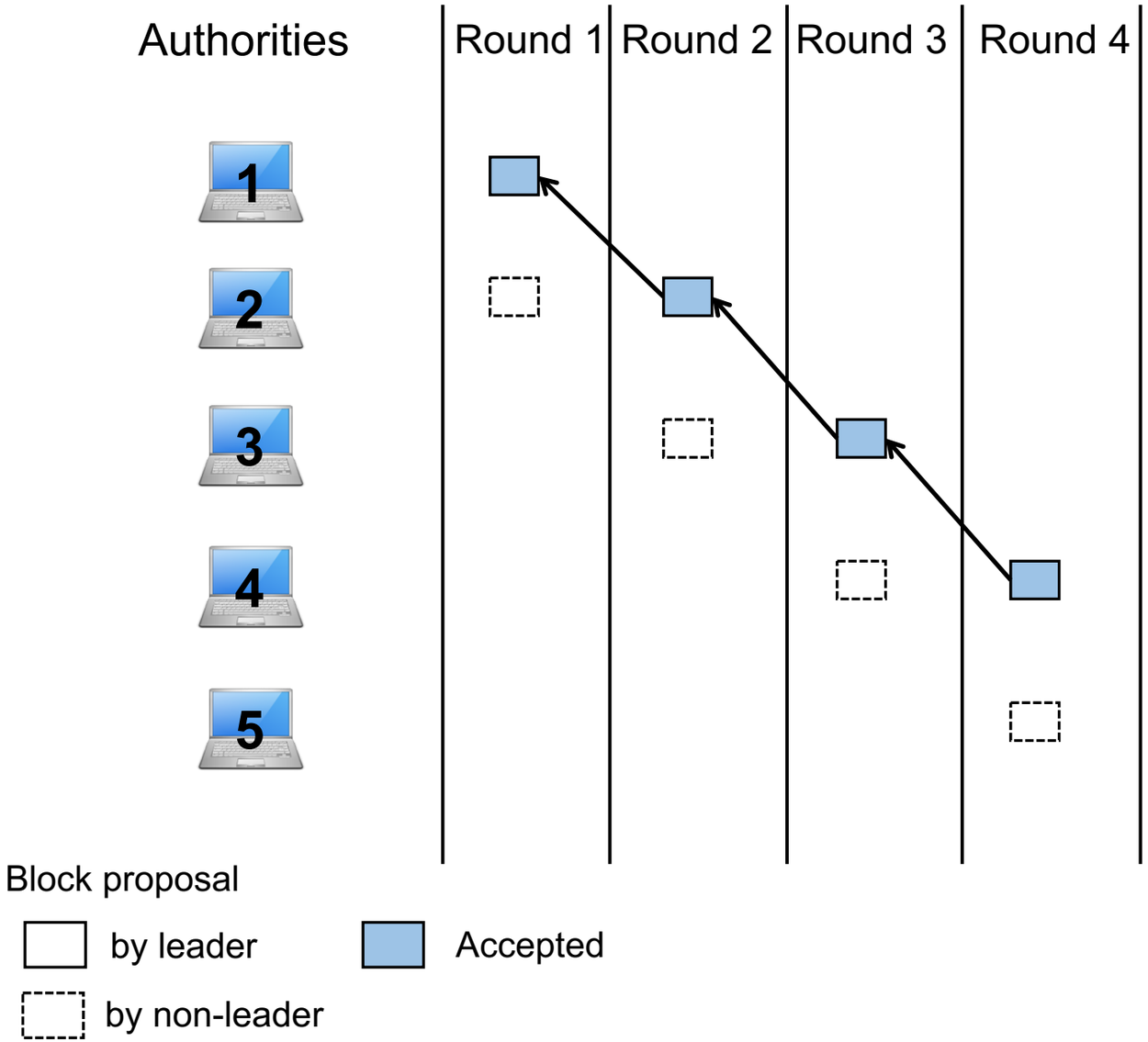
PoA Clique: An Illustration



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with <u>random delays</u>

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

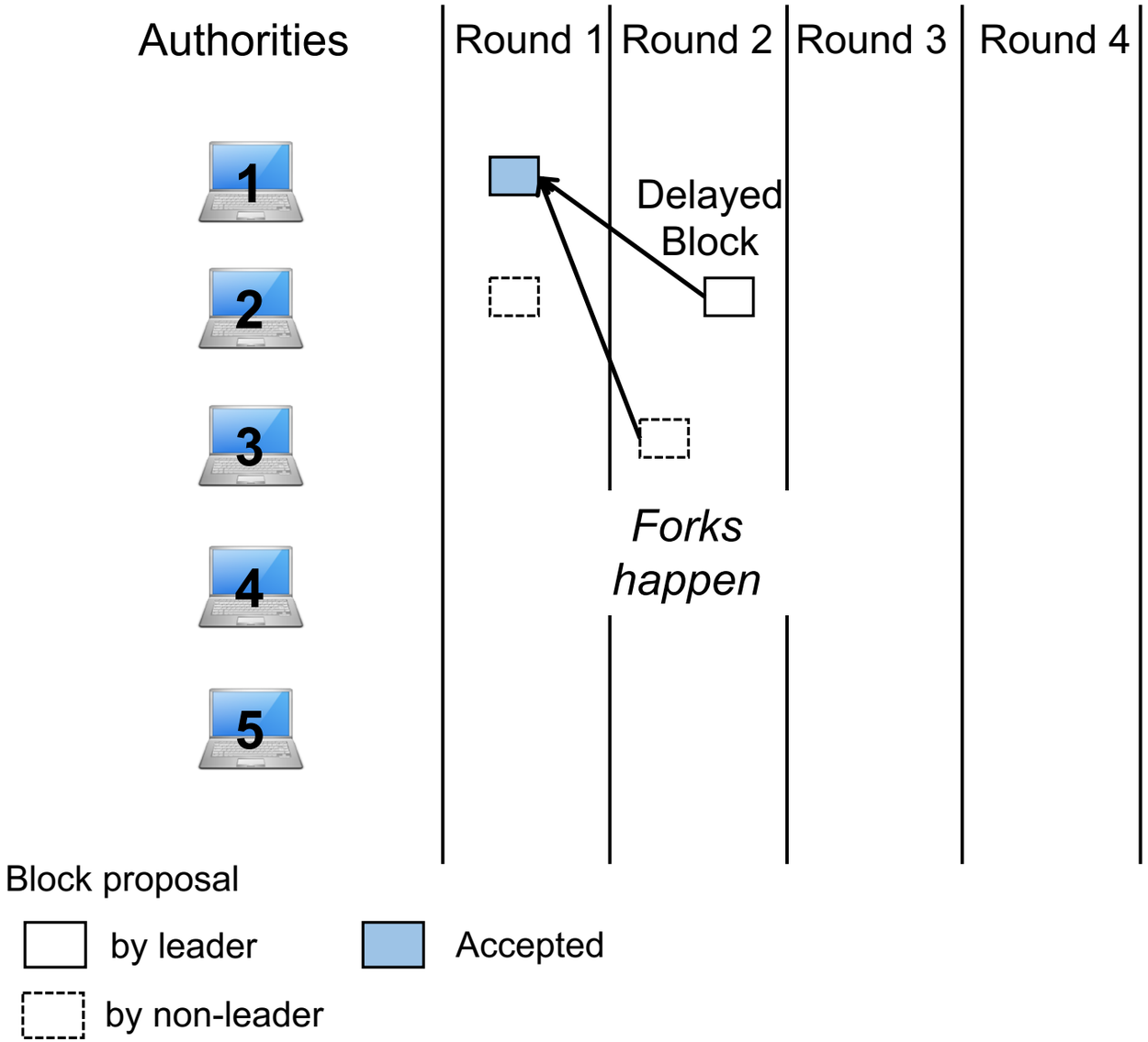
PoA Clique: An Illustration



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with <u>random delays</u>
- Single block acceptance in a round
  - Normal: a leader block

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

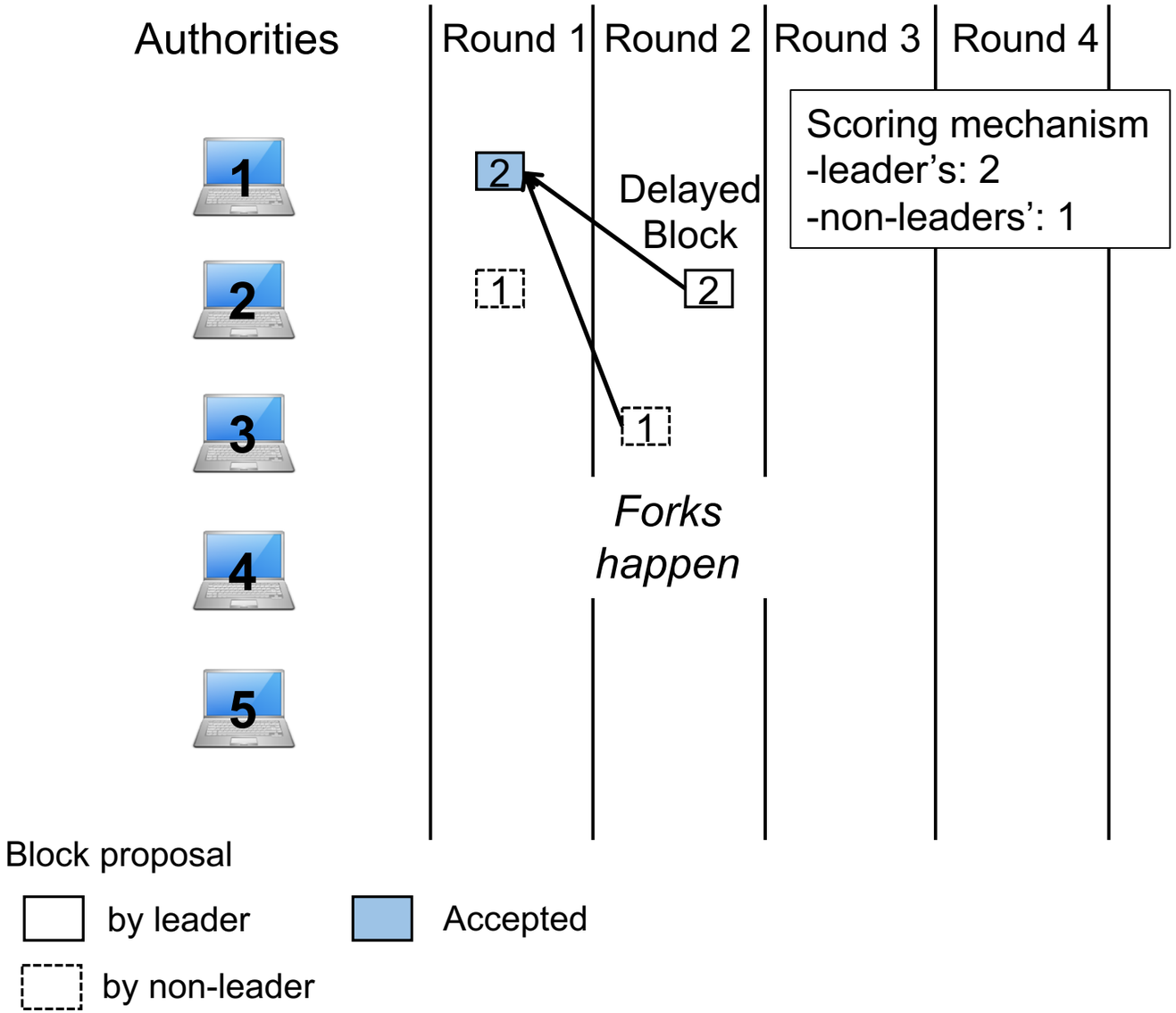
PoA Clique: An Illustration



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with random delays
- Single block acceptance in a round
  - Normal: a leader block

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

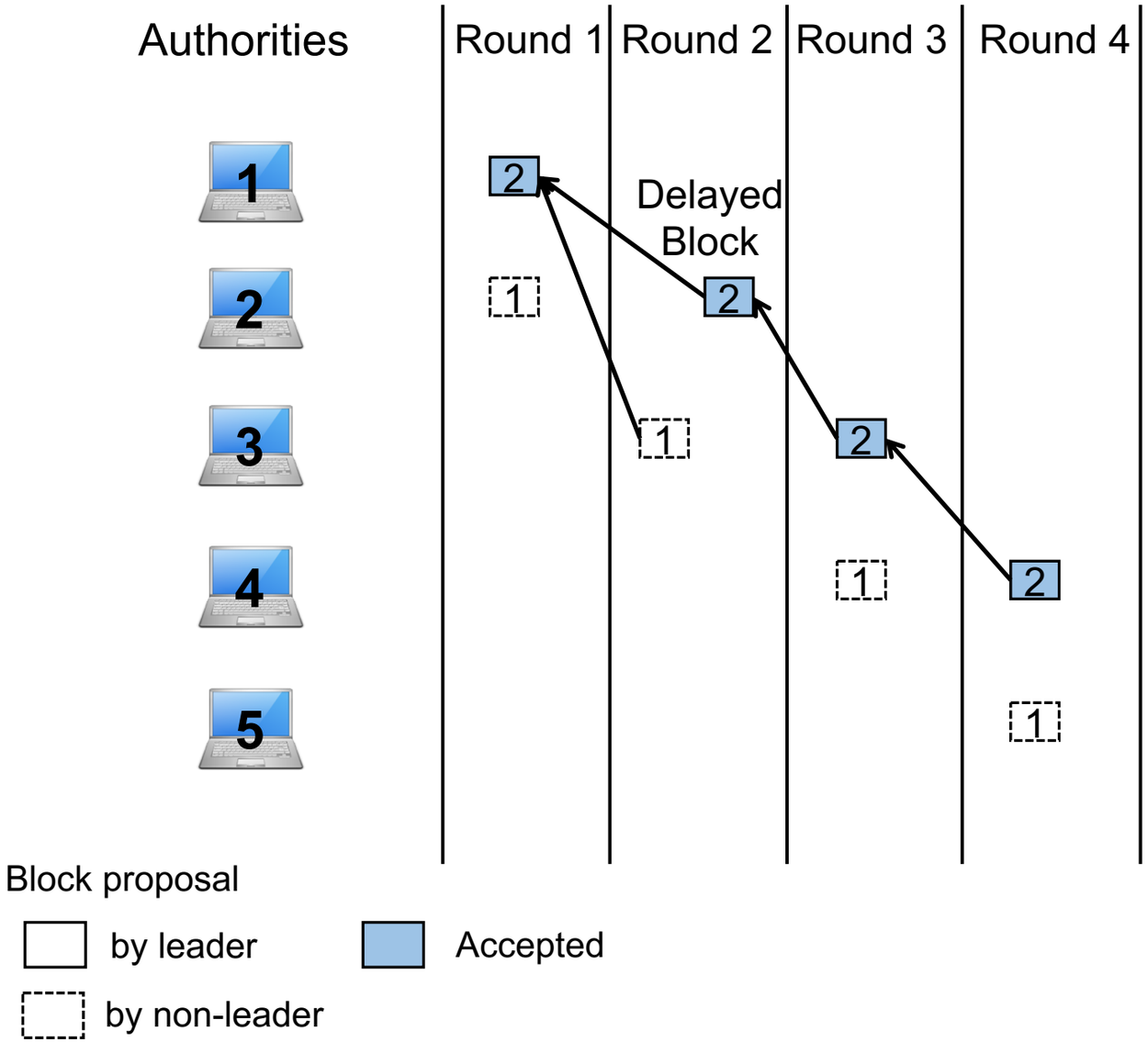
PoA Clique: An Illustration



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with random delays
- Single block acceptance in a round
  - Normal: a leader block
  - Forks: a highest scored chain

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

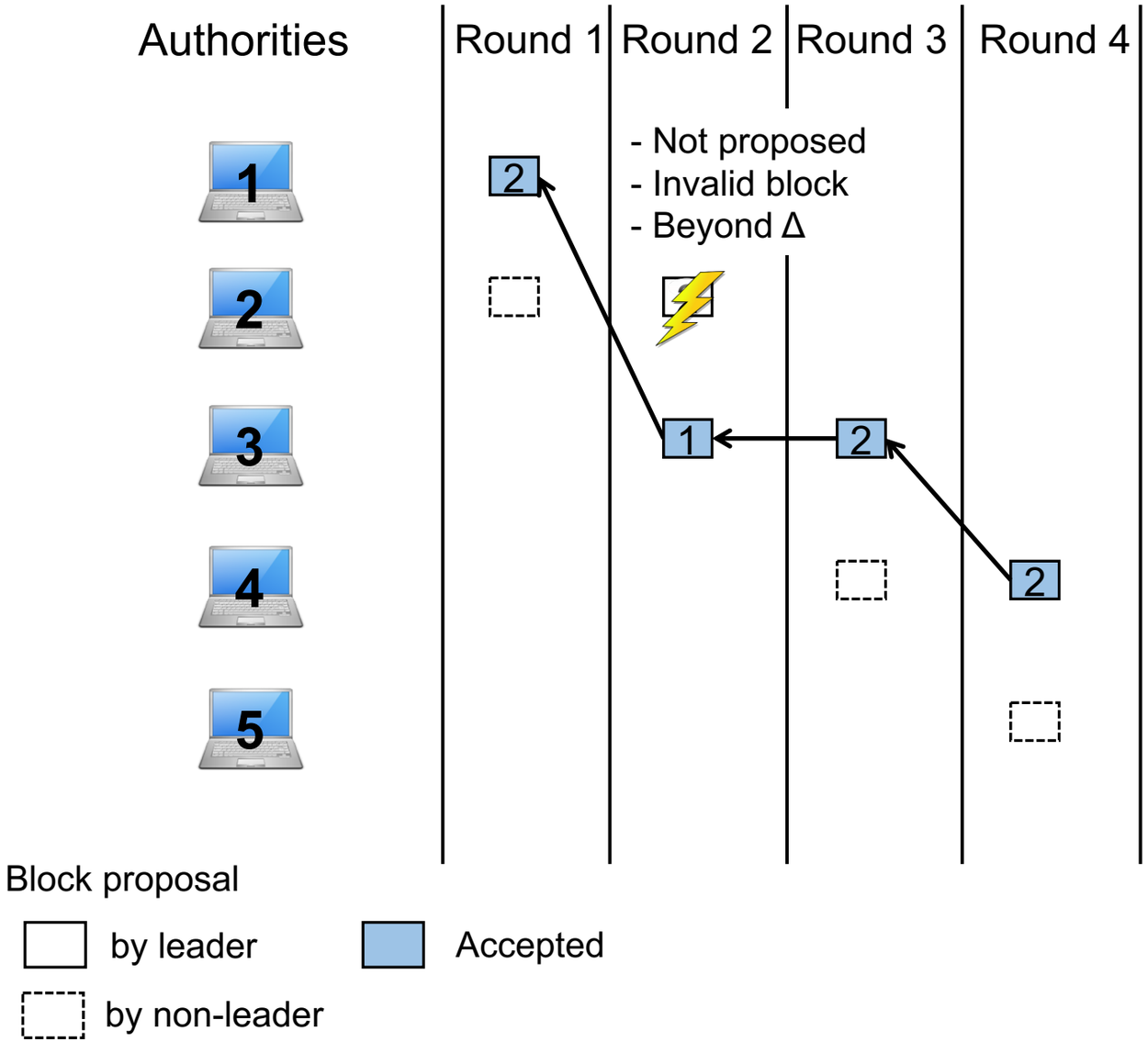
PoA Clique: An Illustration



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with random delays
- Single block acceptance in a round
  - Normal: a leader block
  - Forks: a highest scored chain

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

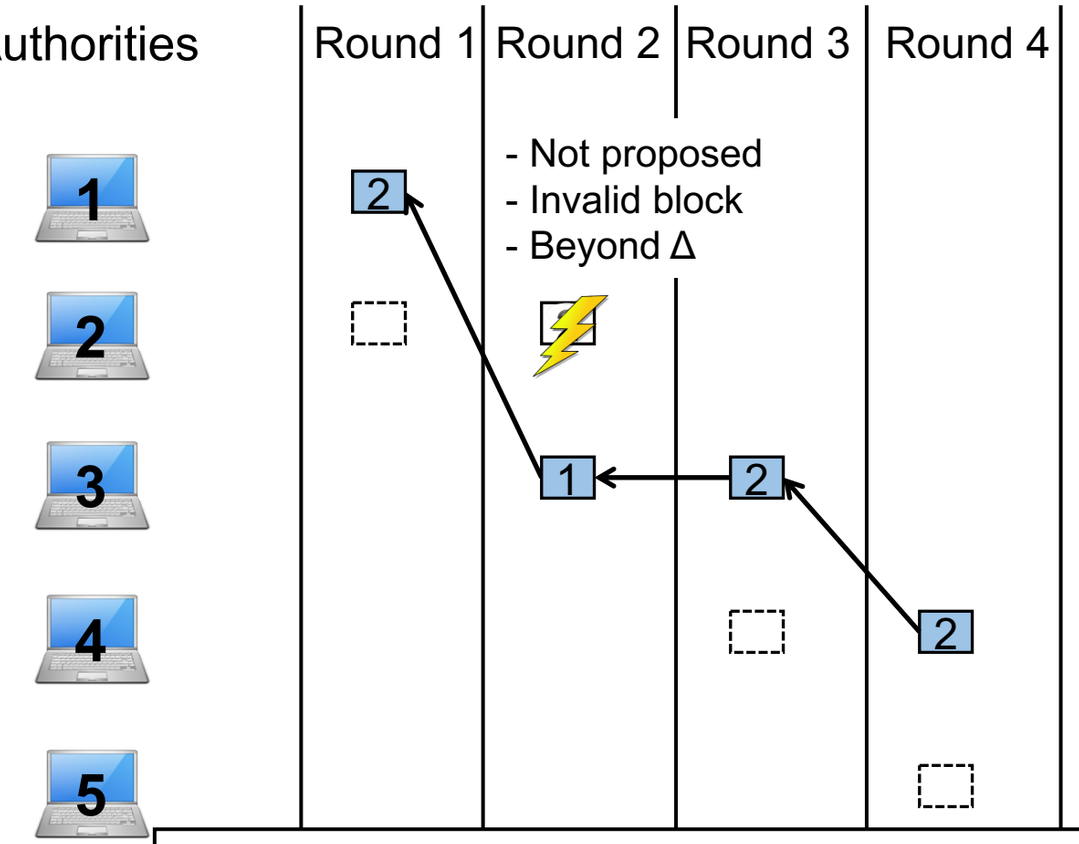
PoA Clique: An Illustration



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with random delays
- Single block acceptance in a round
  - Normal: a leader block
  - Forks: a highest scored chain

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

PoA Clique: Issues



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with random delays
- Single block acceptance in a round
  - Normal: a leader block
  - Forks: a highest scored chain

Multiple block proposals, but a single block acceptance

Block proposal

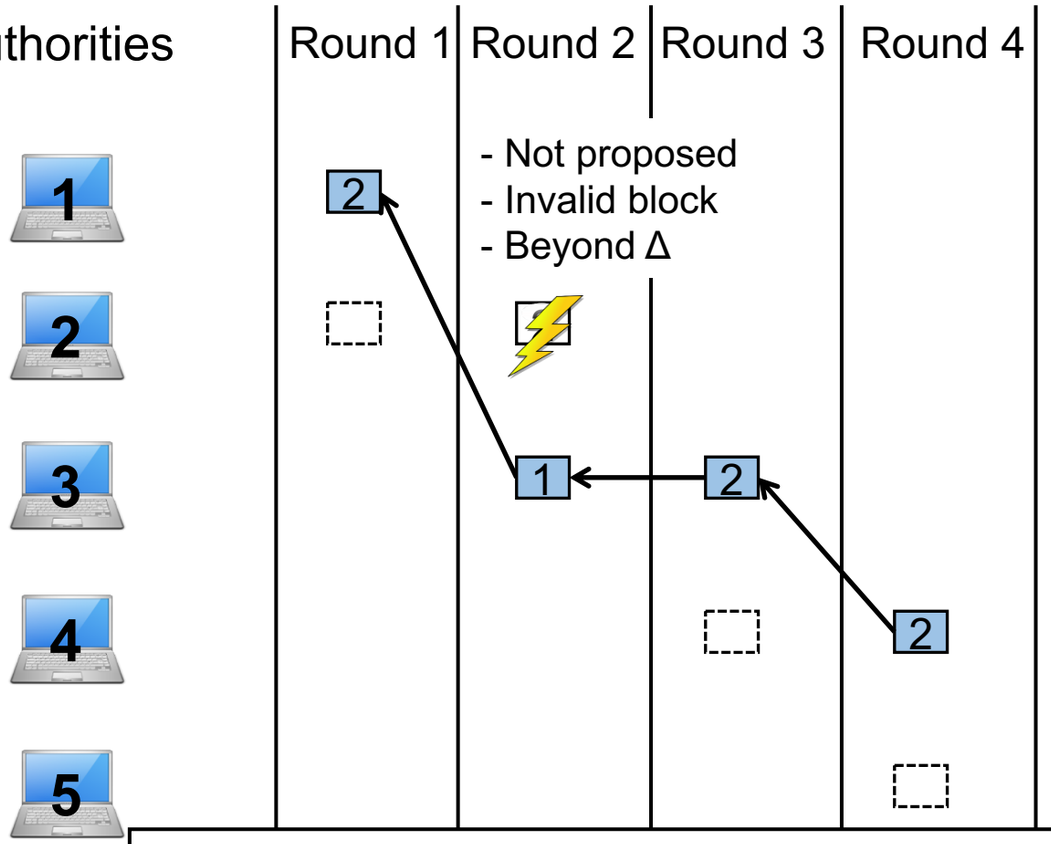
by leader

by non-leader

Accepted

*#non-leaders = up to $\left\lceil \frac{N}{2} \right\rceil - 2$

PoA Clique: Issues



- Round-based
  - (rotating) leader & round timeout Δ
- Multiple block proposals in a round
  - by a leader
  - by non-leaders* with <u>random delays</u>
- Single block acceptance in a round
  - Normal: a leader block
  - Forks: a highest scored chain

Multiple block proposals, but a single block acceptance

Block proposal

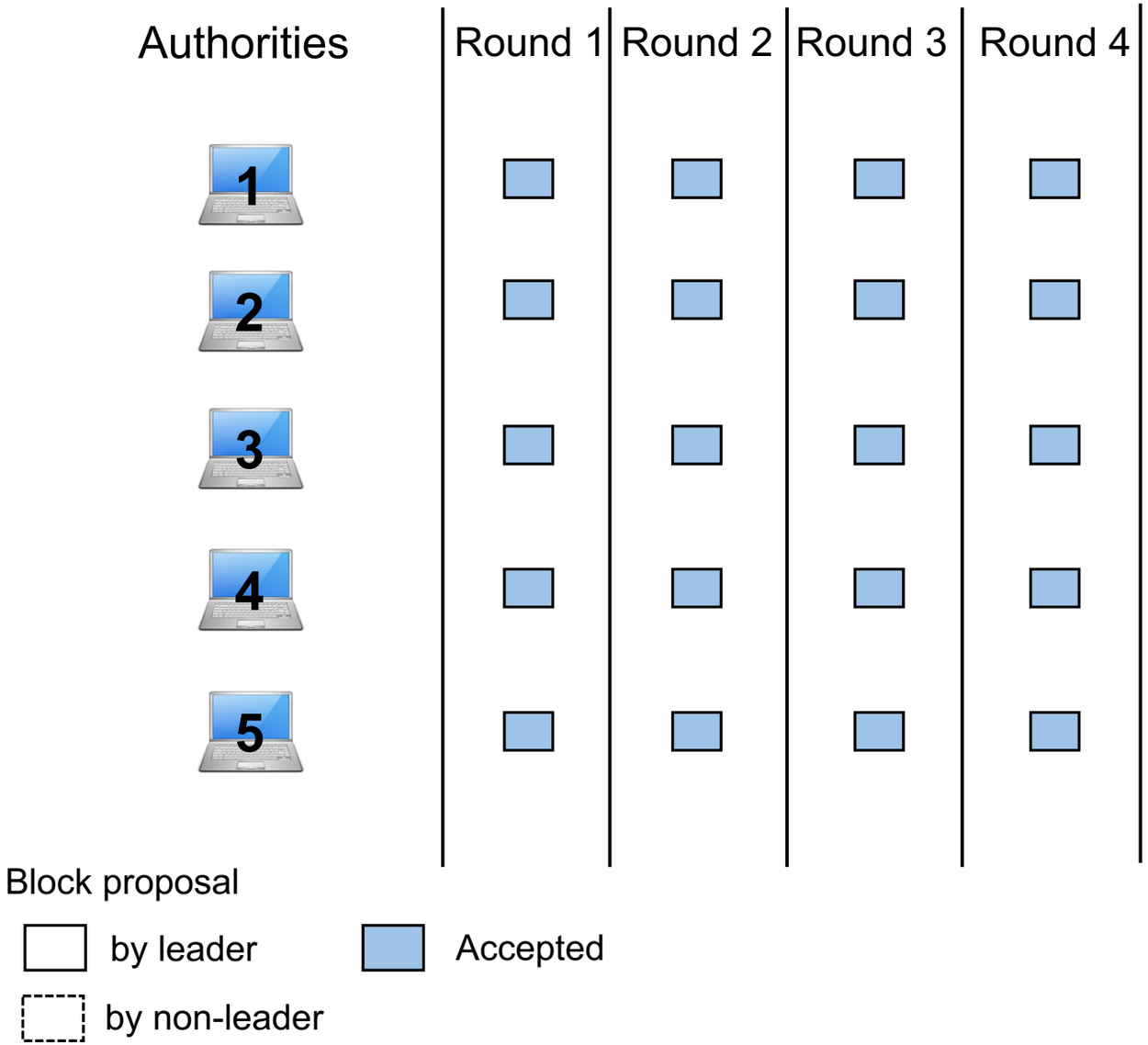
by leader

by non-leader

Limited throughput & Wasted resources

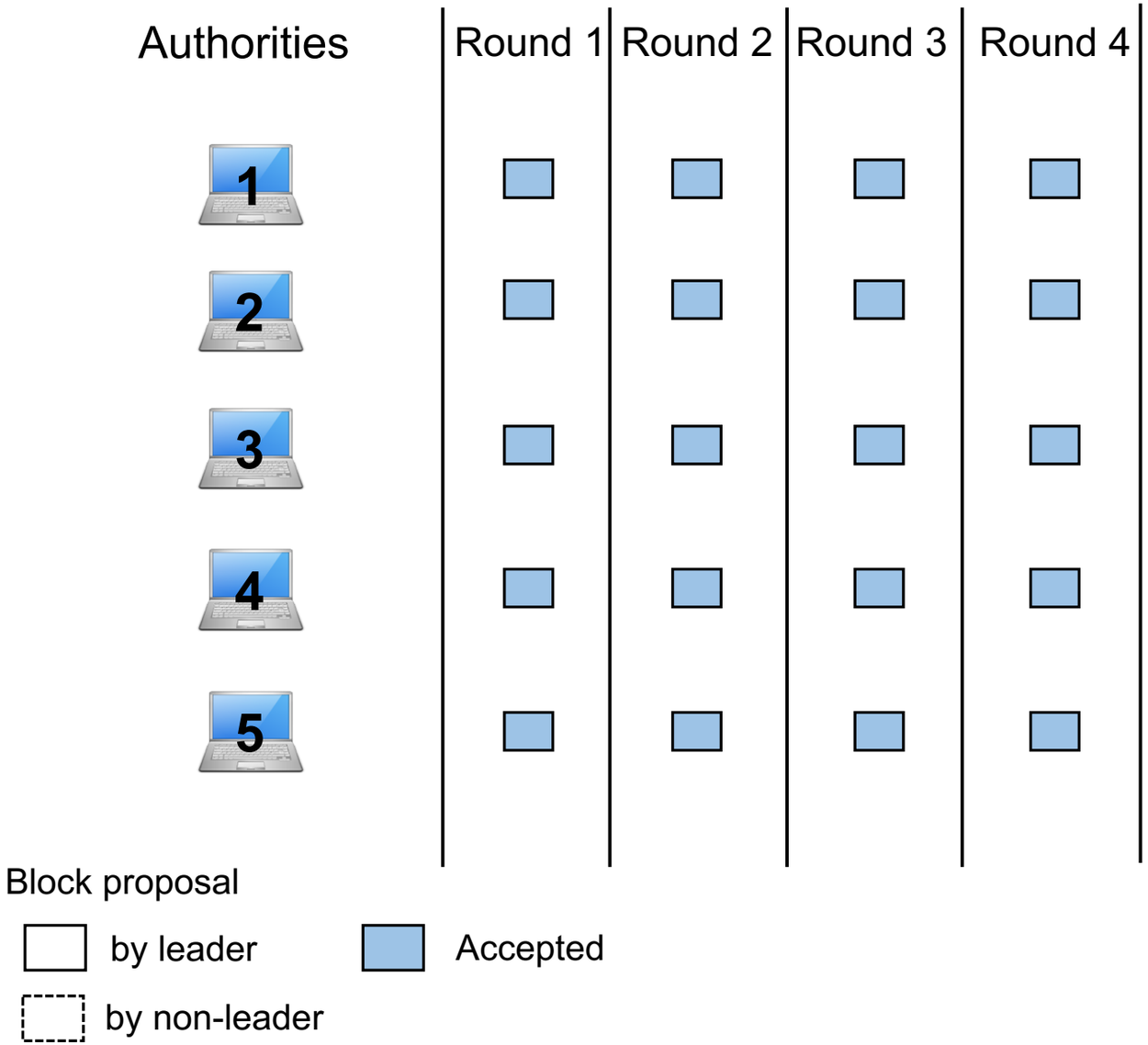
to $\left\lceil \frac{N}{2} \right\rceil - 2$

Our Idea



- Round-based
  - leader-less & round timeout Δ
- Multiple block proposals in a round
  - By all authorities
- Multiple block acceptance in a round
  - Normal: (consistent) all proposed blocks
  - Forks: (consistent) total order

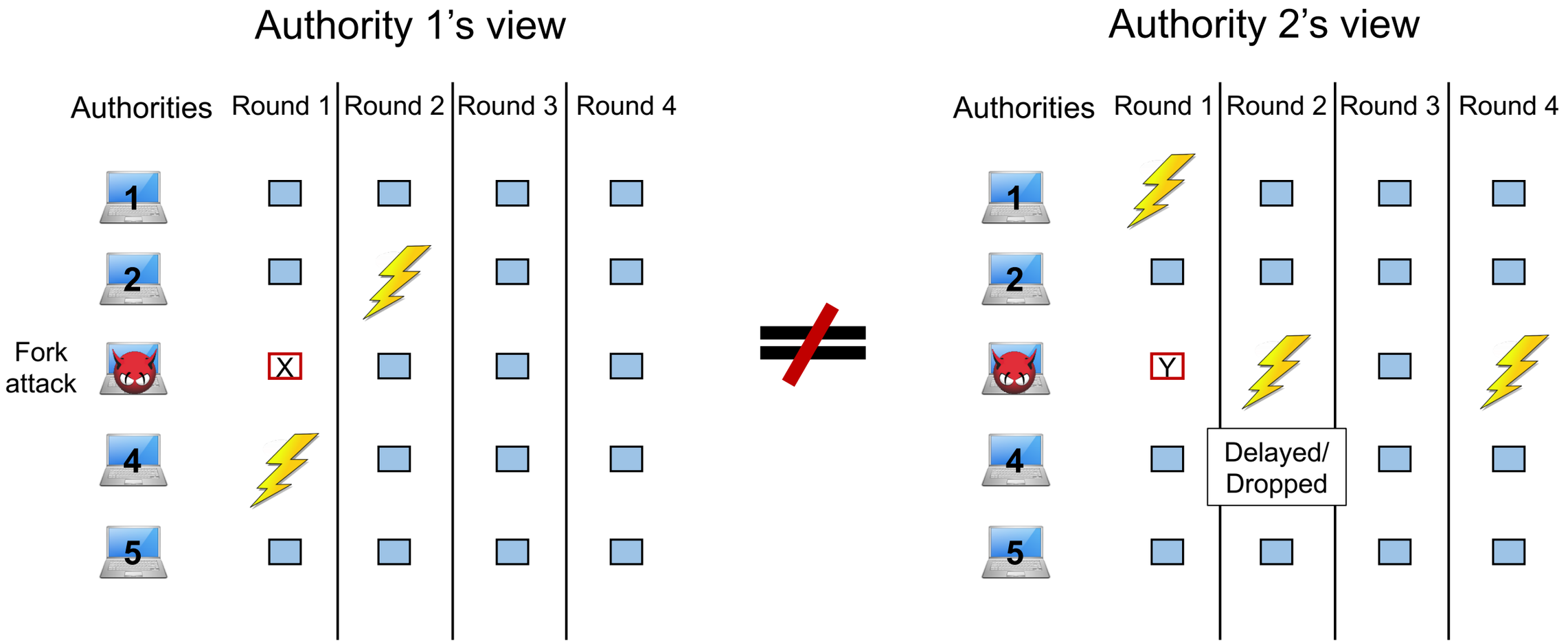
Our Idea



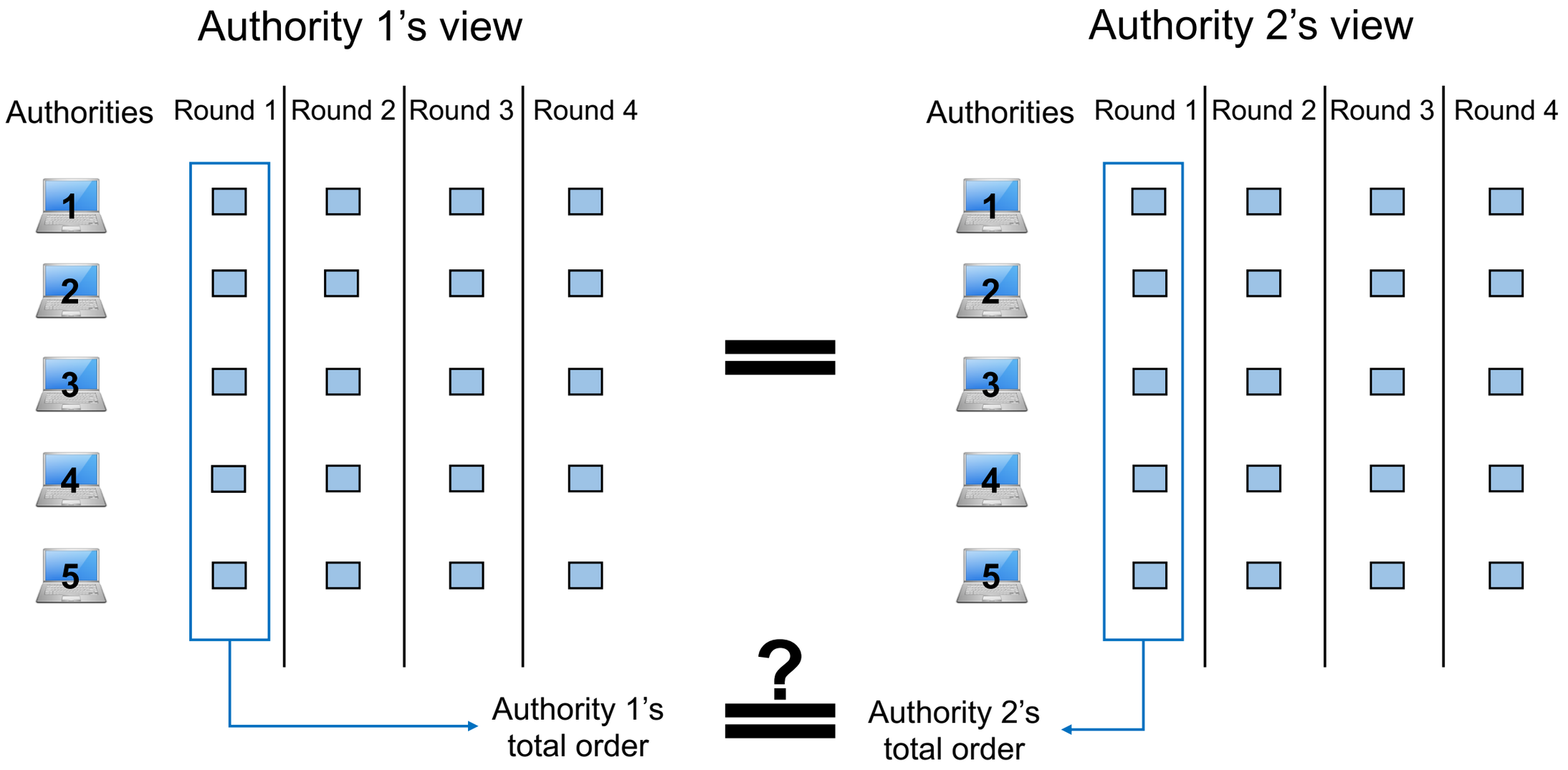
- Round-based
  - leader-less & round timeout Δ
- Multiple block proposals in a round
  - By all authorities
- Multiple block acceptance in a round
  - Normal: (consistent) all proposed blocks
  - Forks: (consistent) total order

Challenges

Challenge (1) Consistent view across nodes

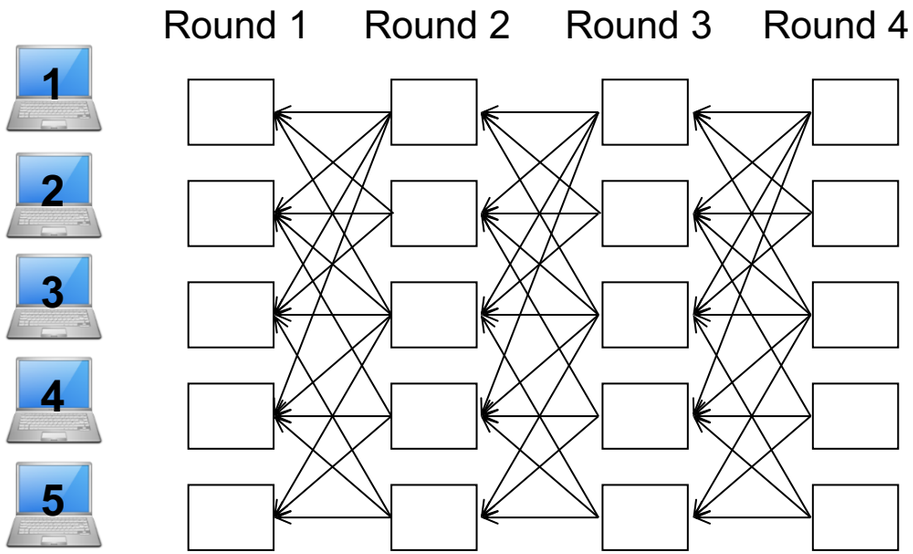


Challenge (2) Consistent total ordering

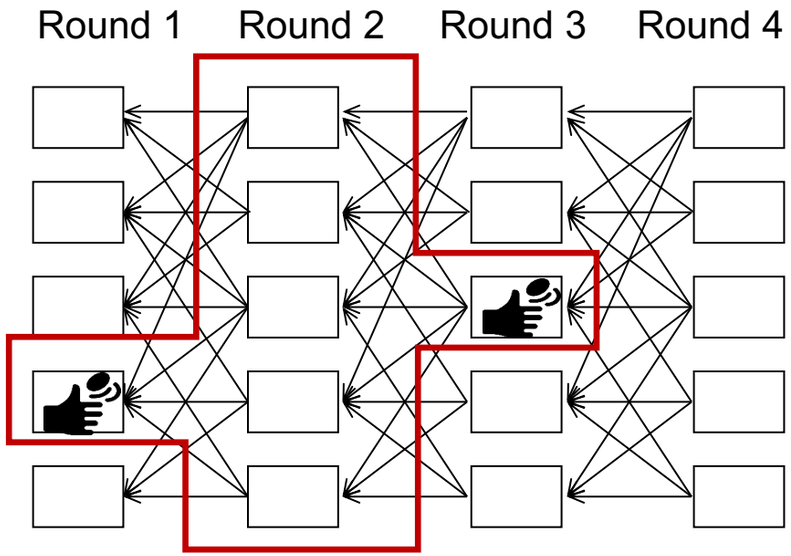


DAG-based BFT Consensus

DAG Mempool



Consensus



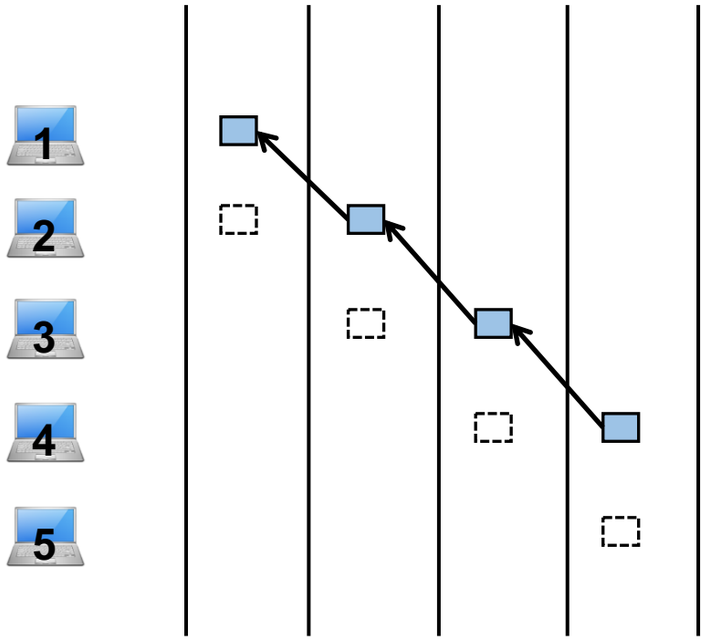
- Consistent blocks across nodes
- Reliable block distribution
- Parallel block proposals & Acceptance

- Consistent total order
- Local & deterministic
- (shared) randomness

Contributions

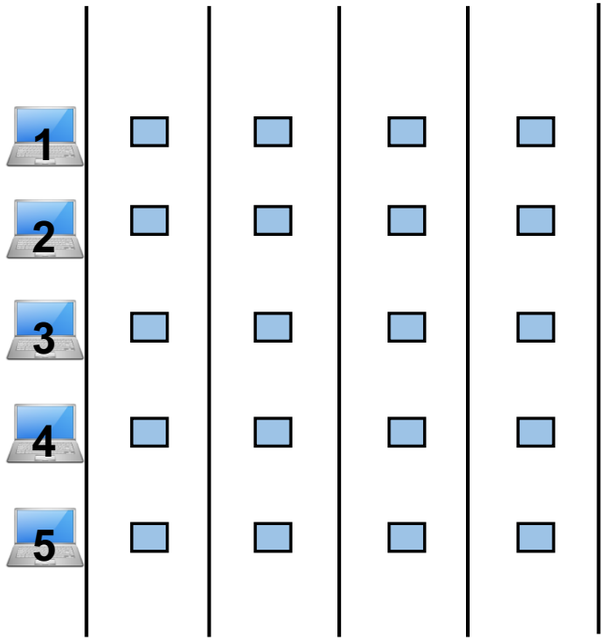
PoA Clique

Single Block Acceptance

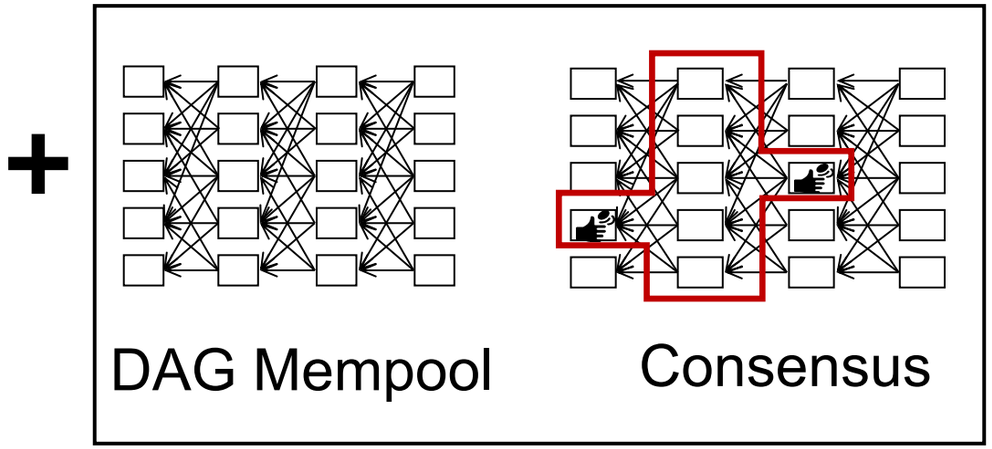


DaPoA

Multiple Blocks Acceptance



DAG-based BFT Consensus

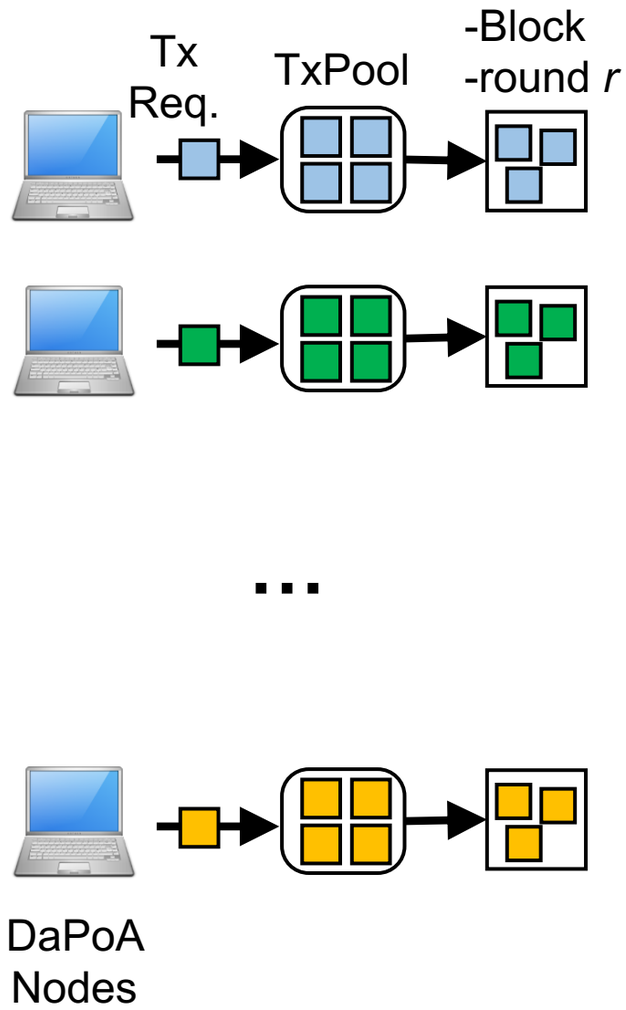


achieves 2.47x higher throughput, 5.76x lower latency than Clique

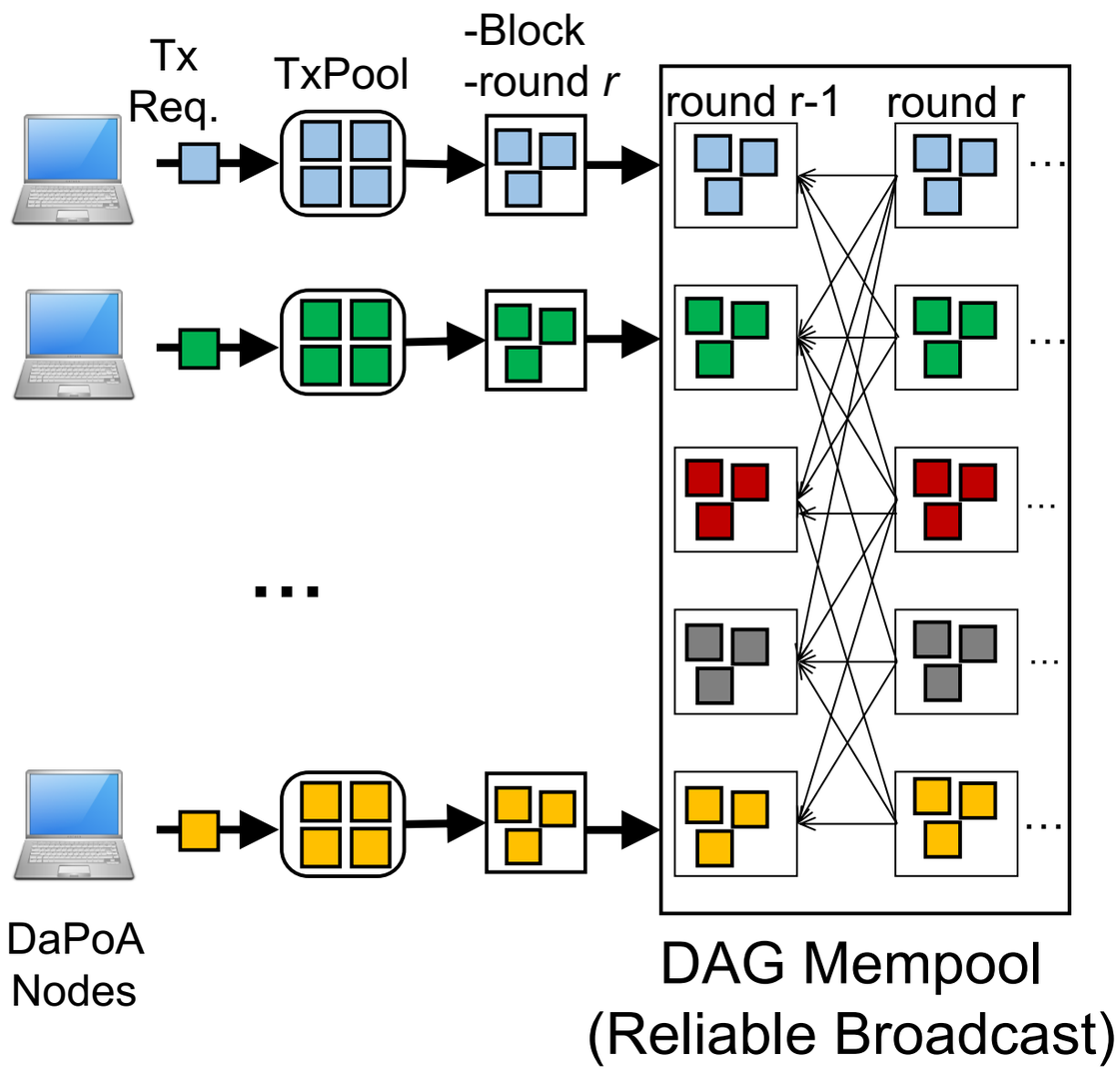
Assumptions

- A consortium blockchain
  - Known Identities
  - Members operates DaPoA node
  - Clients submit Txs to a trusted node
  - f Byzantine members out of $3f+1$ members
- Partially asynchronous network
  - unknown time bound Δ
- Crypto cannot be subverted

DaPoA: Operations

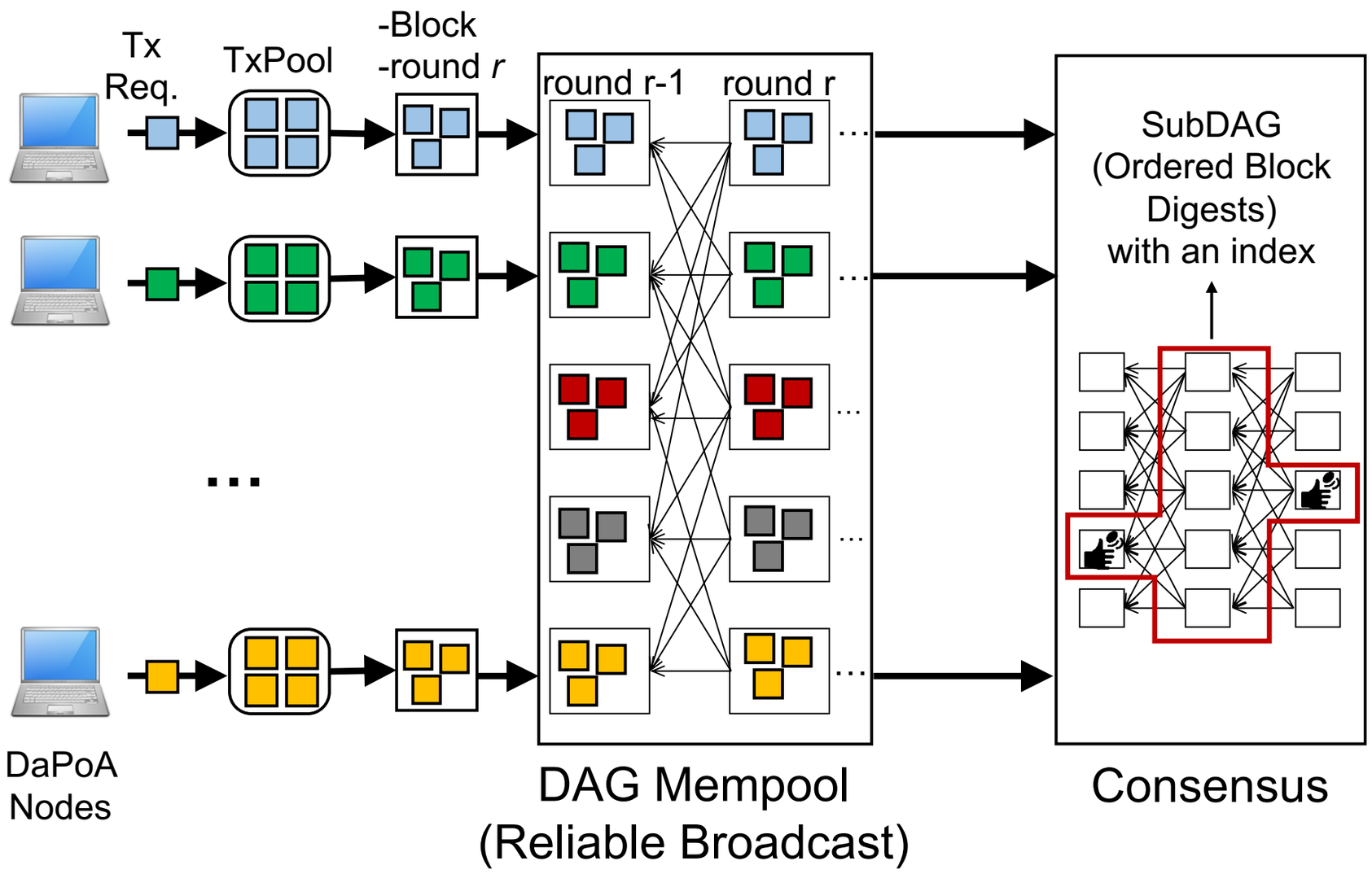


DaPoA: Operations



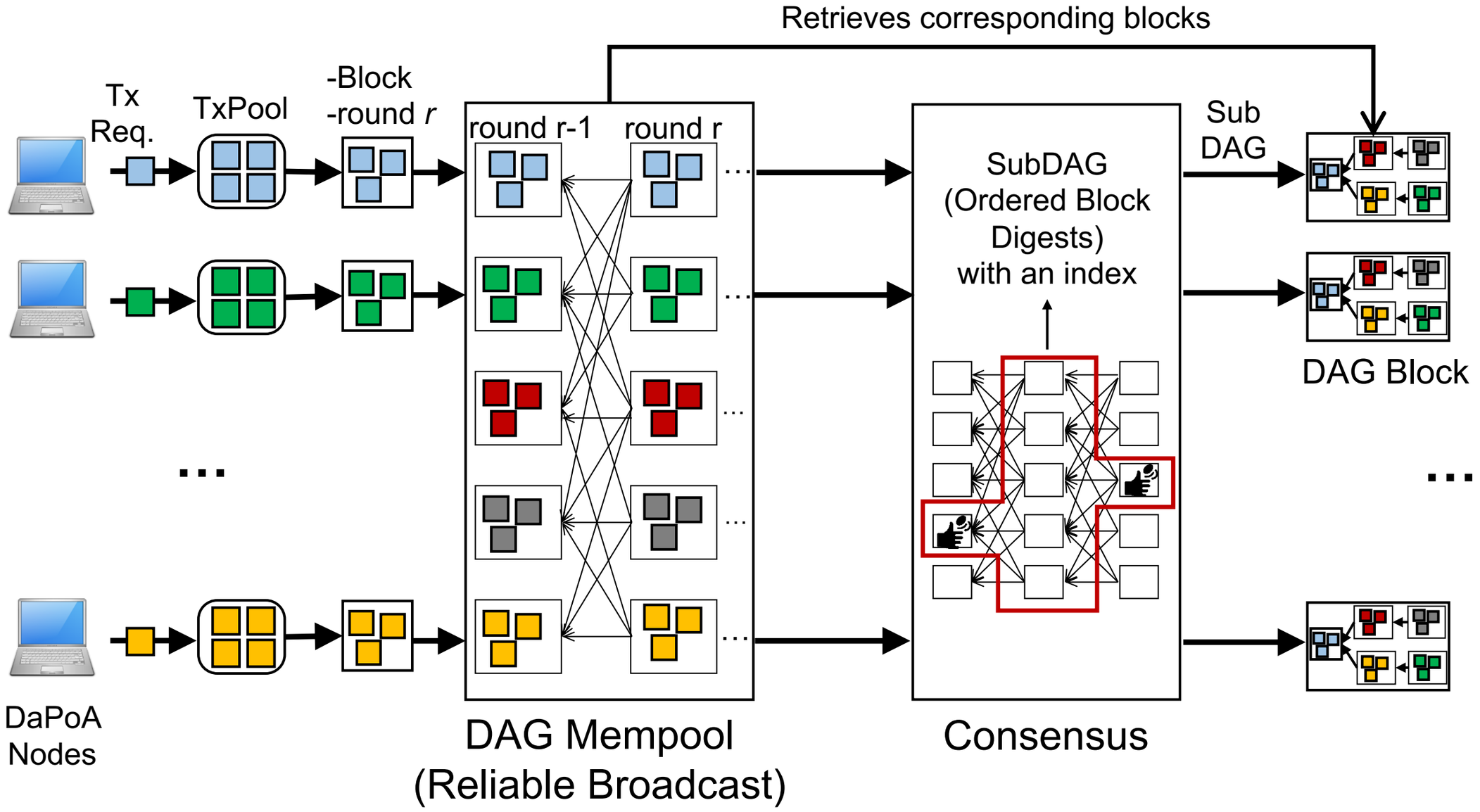
- Reliable block replication across nodes
- Consistent block views
- Multiple block proposals & acceptance

DaPoA: Operations

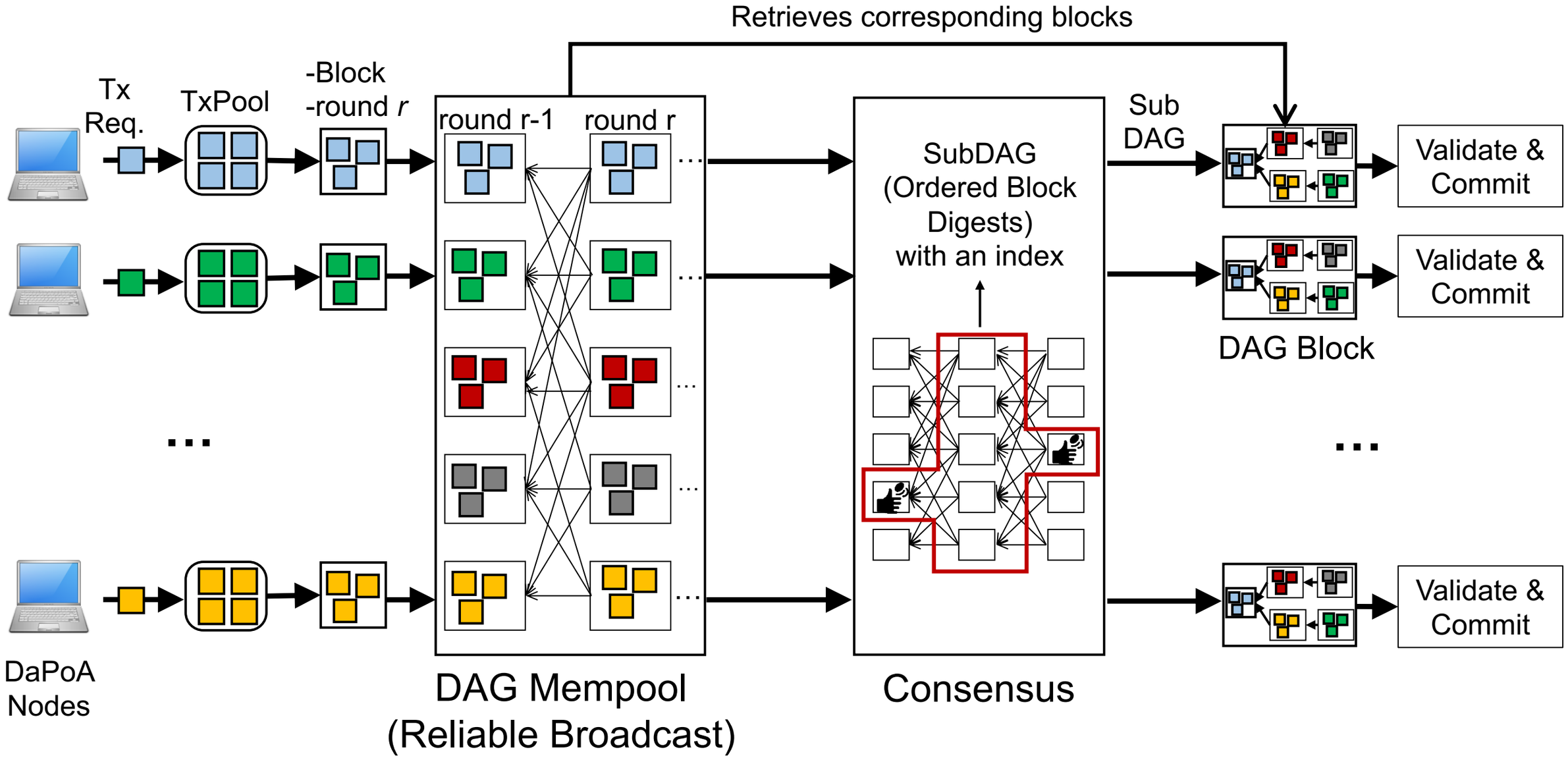


- Consistent total order
- Local & Deterministic
- Based on a shared randomness

DaPoA: Operations

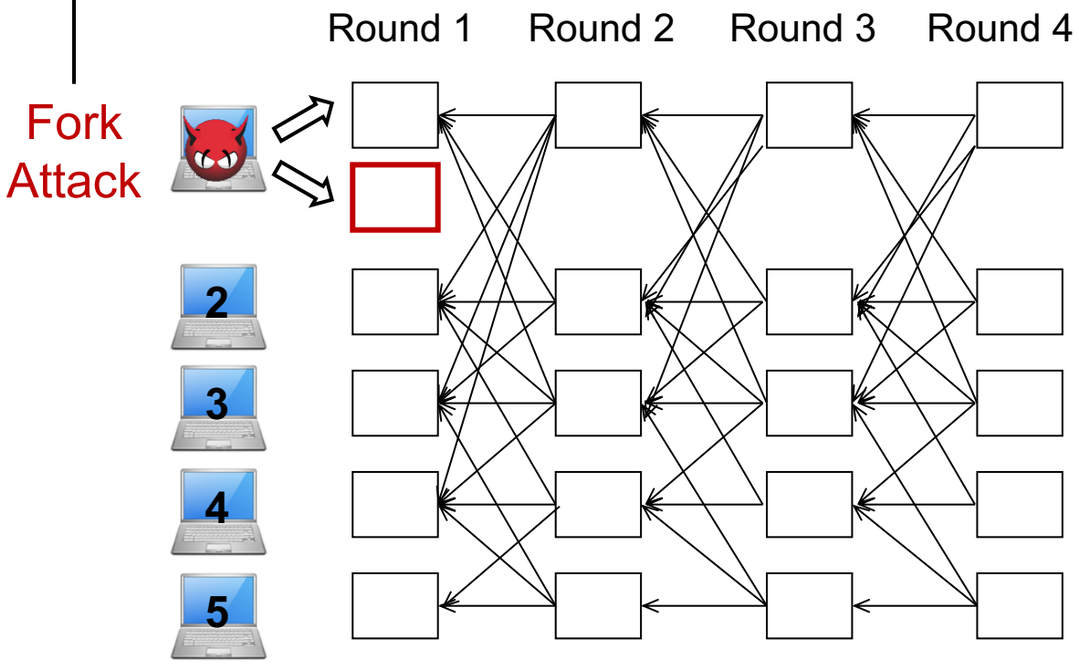


DaPoA: Operations

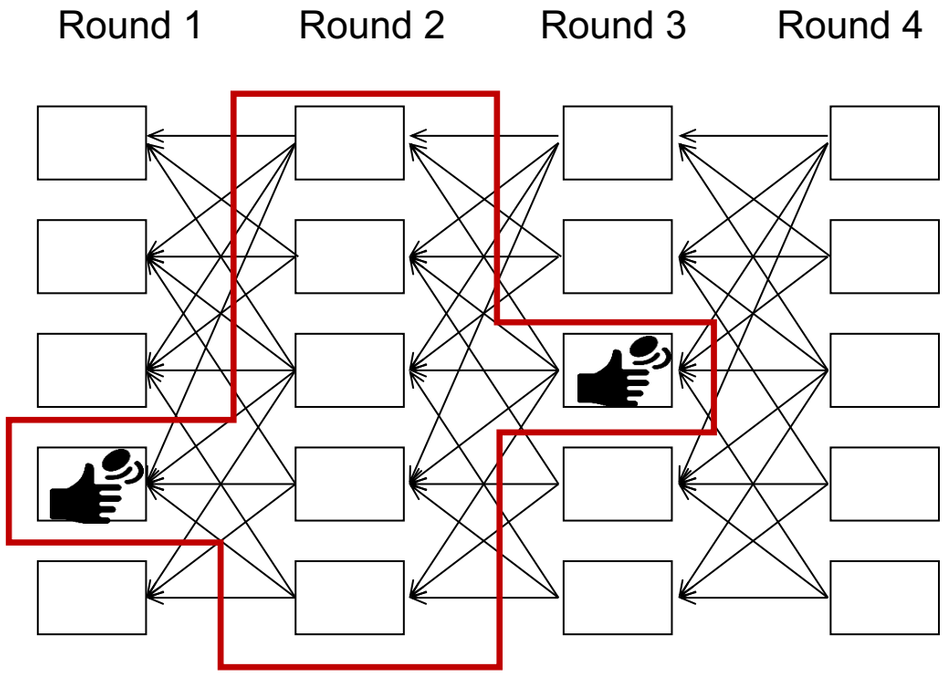


Security Analysis

Accept a proposal with 2f+1 votes from the next round



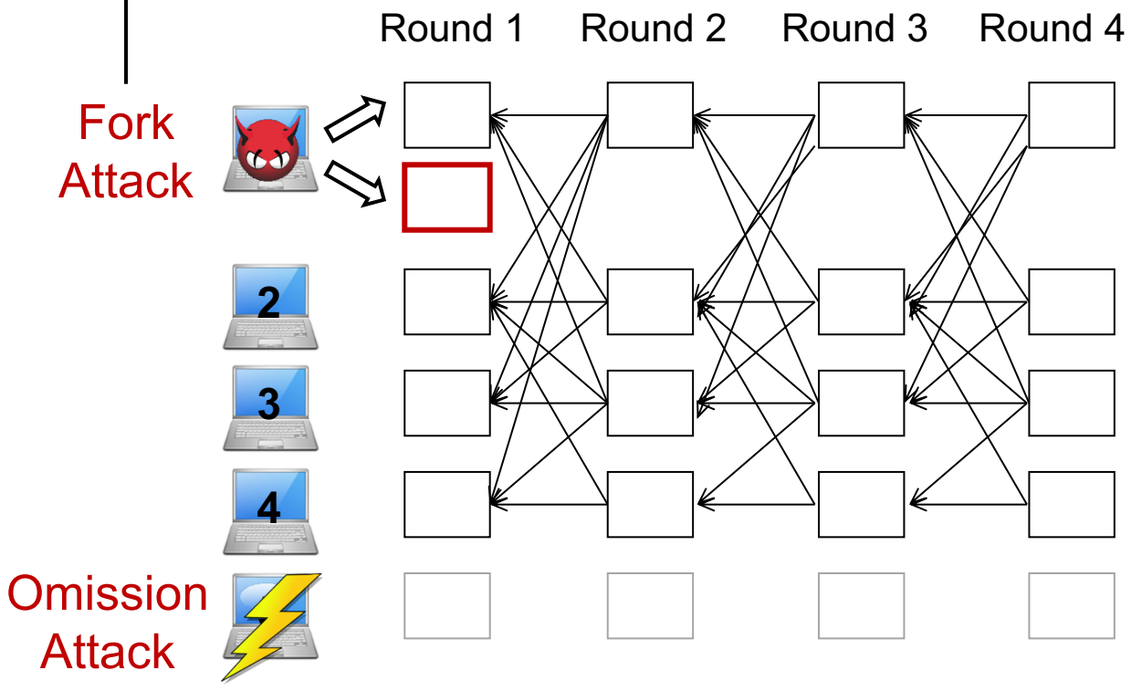
DAG Mempool



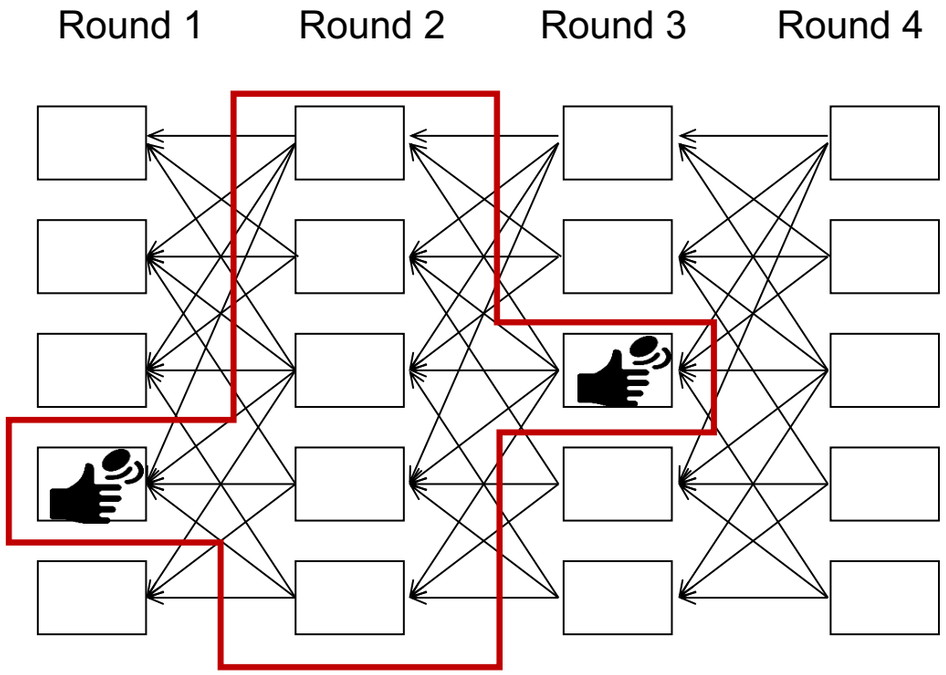
Consensus

Security Analysis

Accept a proposal with 2f+1 votes from the next round



DAG Mempool

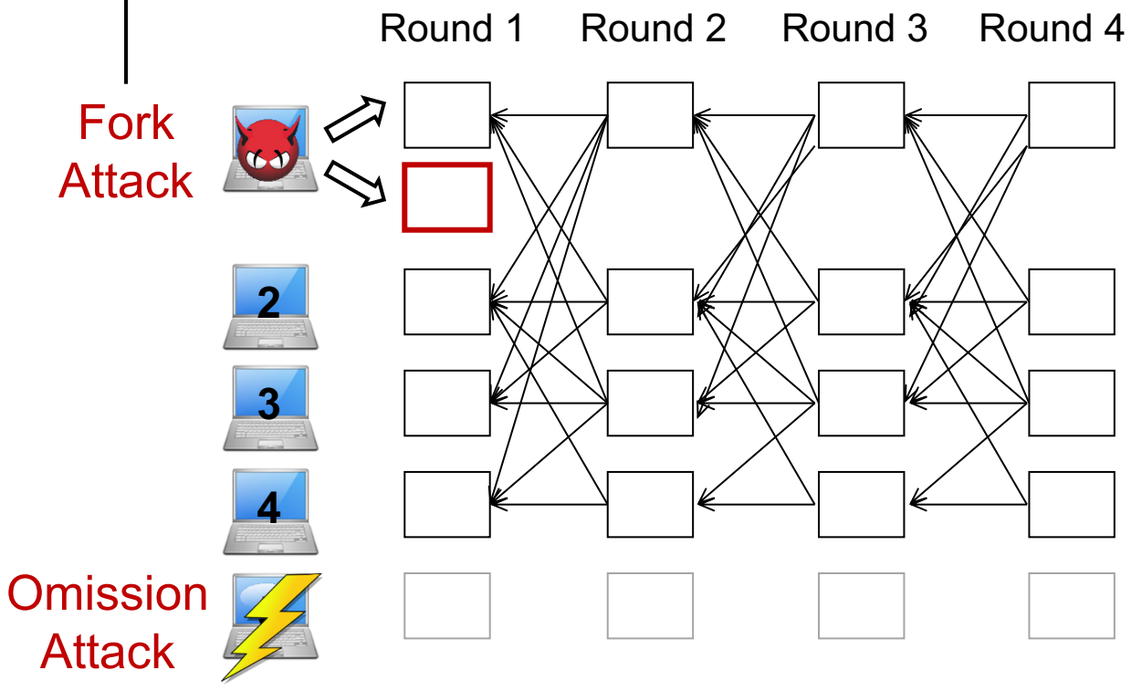


Consensus

Round advances despite f failures

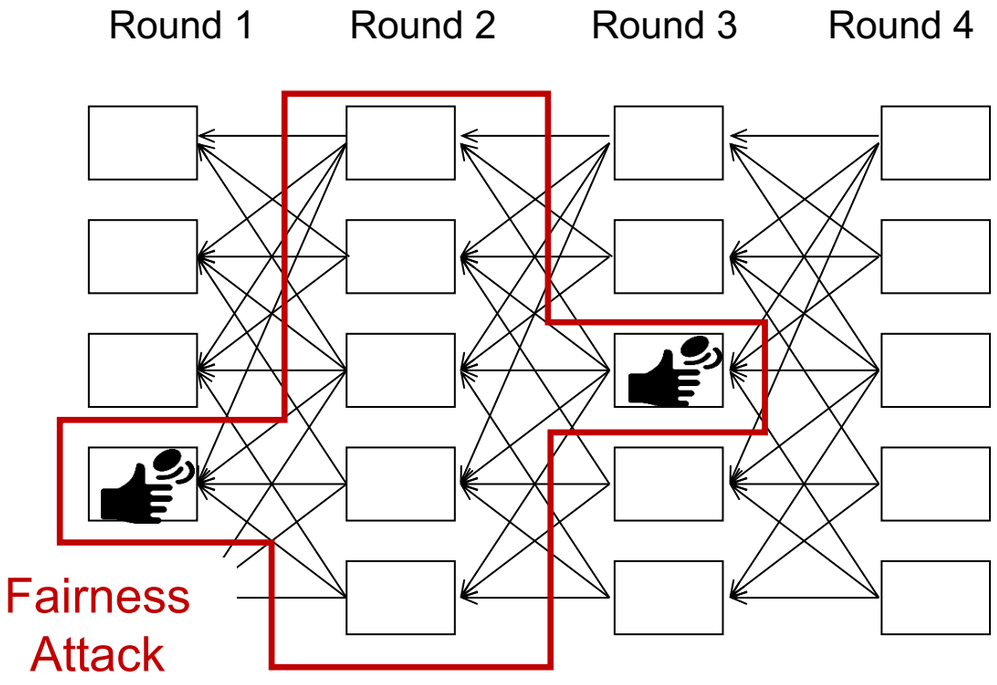
Security Analysis

Accept a proposal with 2f+1 votes from the next round



DAG Mempool

Round advances despite f failures



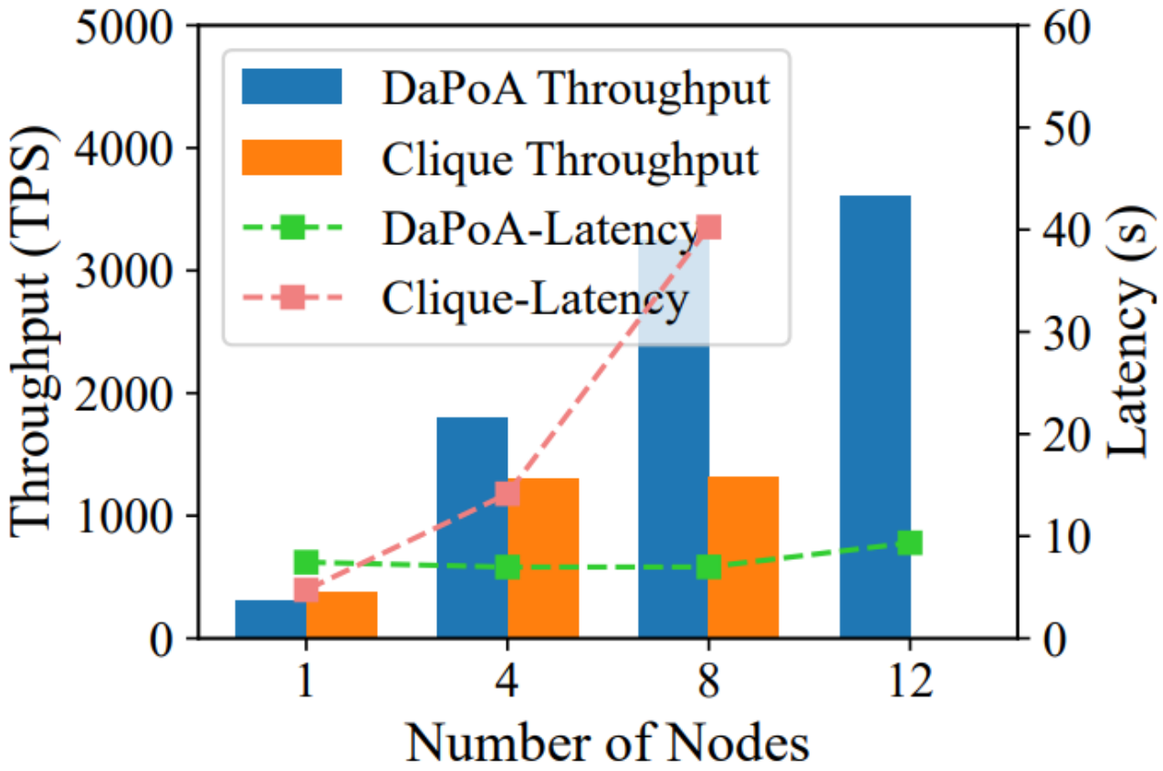
Consensus

Ordering based on a shared randomness

Evaluation: vs. Clique

- Implement DaPoA based on Ethereum Geth*
- Narwhal/Tusk** for DAG BFT
- Benchmark using Hyperledger Caliper
- Hardware: AMD Ryzen 3990X CPU, 256 GB RAM

Parameters
- Simple payment contract
- TX confirmation blocks: 2
- Block Period: 1
- Gaslimit: 10^9
- DAG BFT (Batch Size: 2MB, 1 worker, 1 primary)
- Send rate: 700

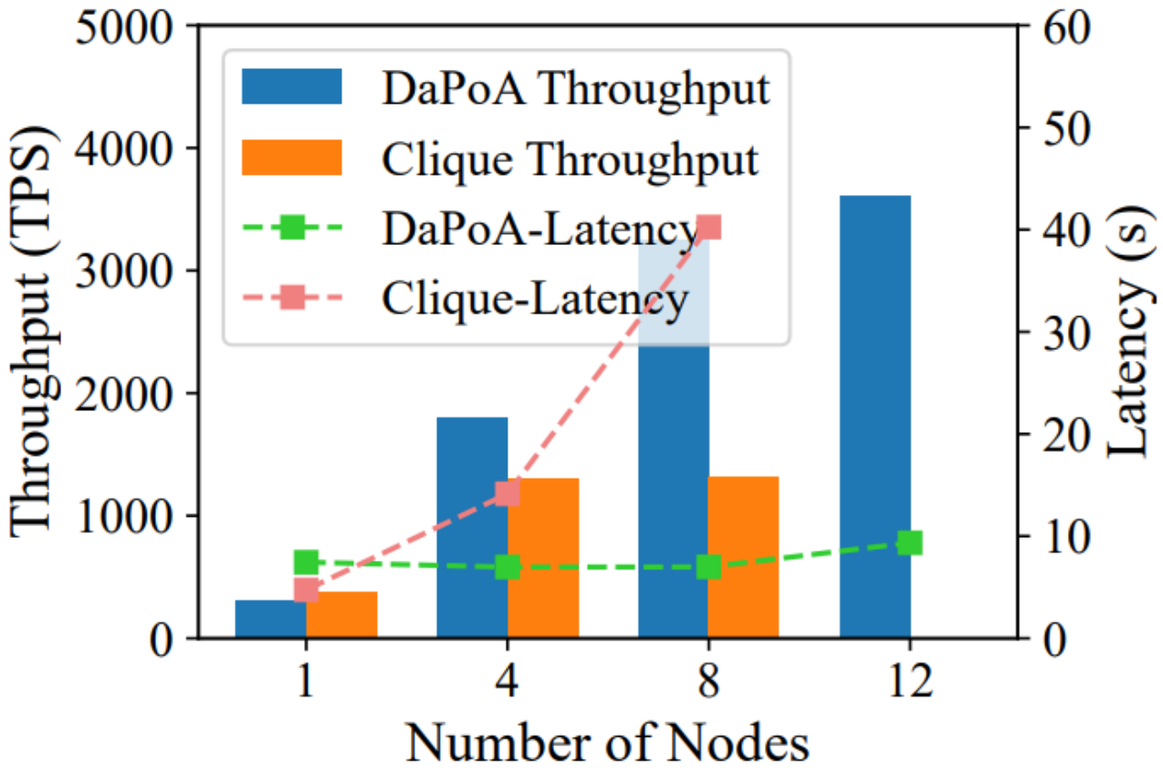


*https://github.com/ethereum/go-ethereum
**https://github.com/facebookresearch/narwhal

Evaluation: vs. Clique

- Implement DaPoA based on Ethereum Geth*
- Narwhal/Tusk** for DAG BFT
- Benchmark using Hyperledger Caliper
- Hardware: AMD Ryzen 3990X CPU, 256 GB RAM

Parameters
- Simple payment contract
- TX confirmation blocks: 2
- Block Period: 1
- Gaslimit: 10^9
- DAG BFT (Batch Size: 2MB, 1 worker, 1 primary)
- Send rate: 700



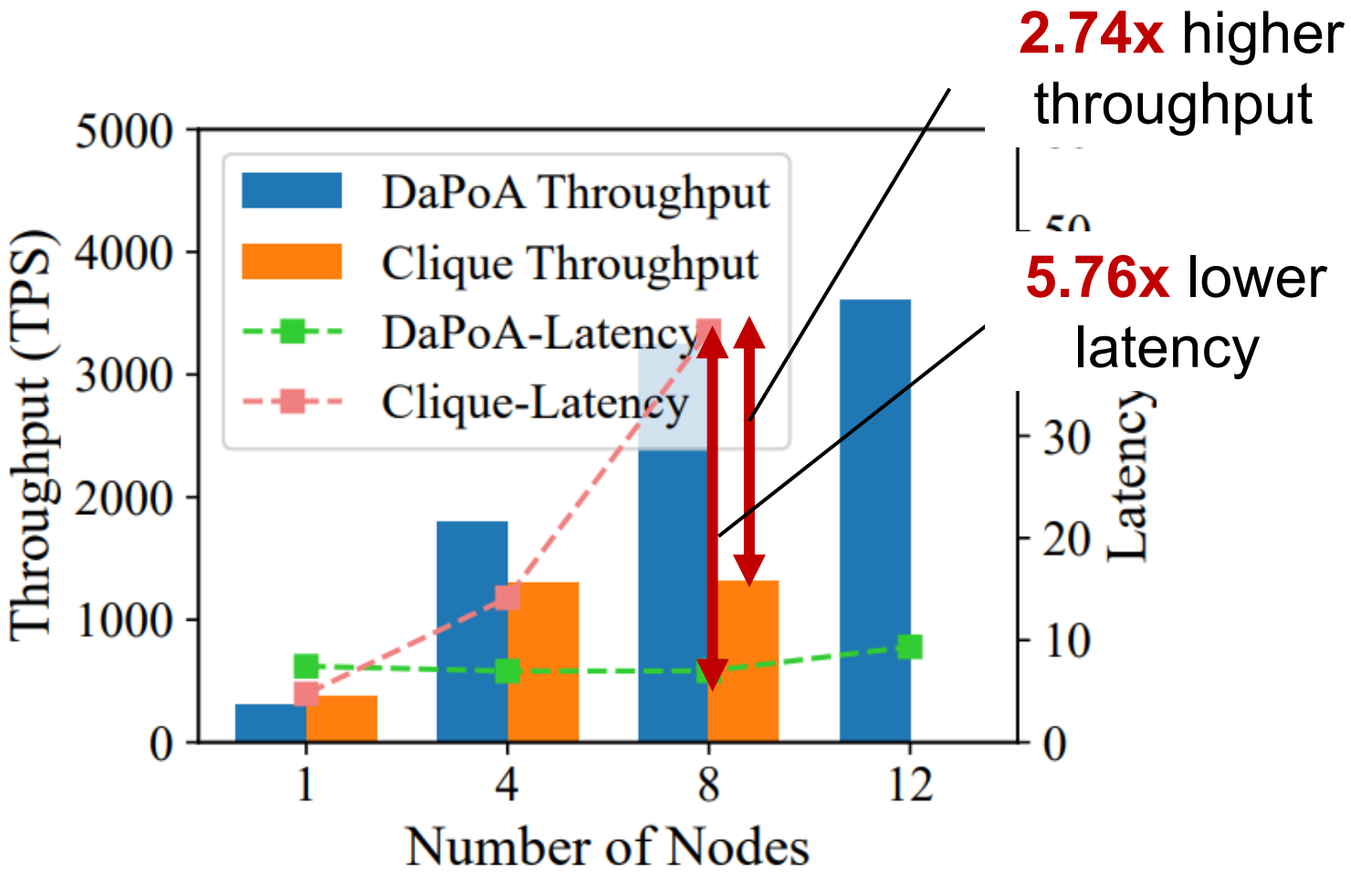
⇨ DaPoA scales better

*https://github.com/ethereum/go-ethereum
**https://github.com/facebookresearch/narwhal

Evaluation: vs. Clique

- Implement DaPoA based on Ethereum Geth*
- Narwhal/Tusk** for DAG BFT
- Benchmark using Hyperledger Caliper
- Hardware: AMD Ryzen 3990X CPU, 256 GB RAM

Parameters
- Simple payment contract
- TX confirmation blocks: 2
- Block Period: 1
- Gaslimit: 10^9
- DAG BFT (Batch Size: 2MB, 1 worker, 1 primary)
- Send rate: 700



DaPoA scales better

*https://github.com/ethereum/go-ethereum
**https://github.com/facebookresearch/narwhal

Conclusion

DaPoA

- An effort to enhance Ethereum Clique for performance scalability
  - Multiple block acceptance
- Leveraging DAG-based BFT consensus
  - A consistent block view across nodes using DAG mempool.
  - A consistent block ordering using local consensus based on shared randomness