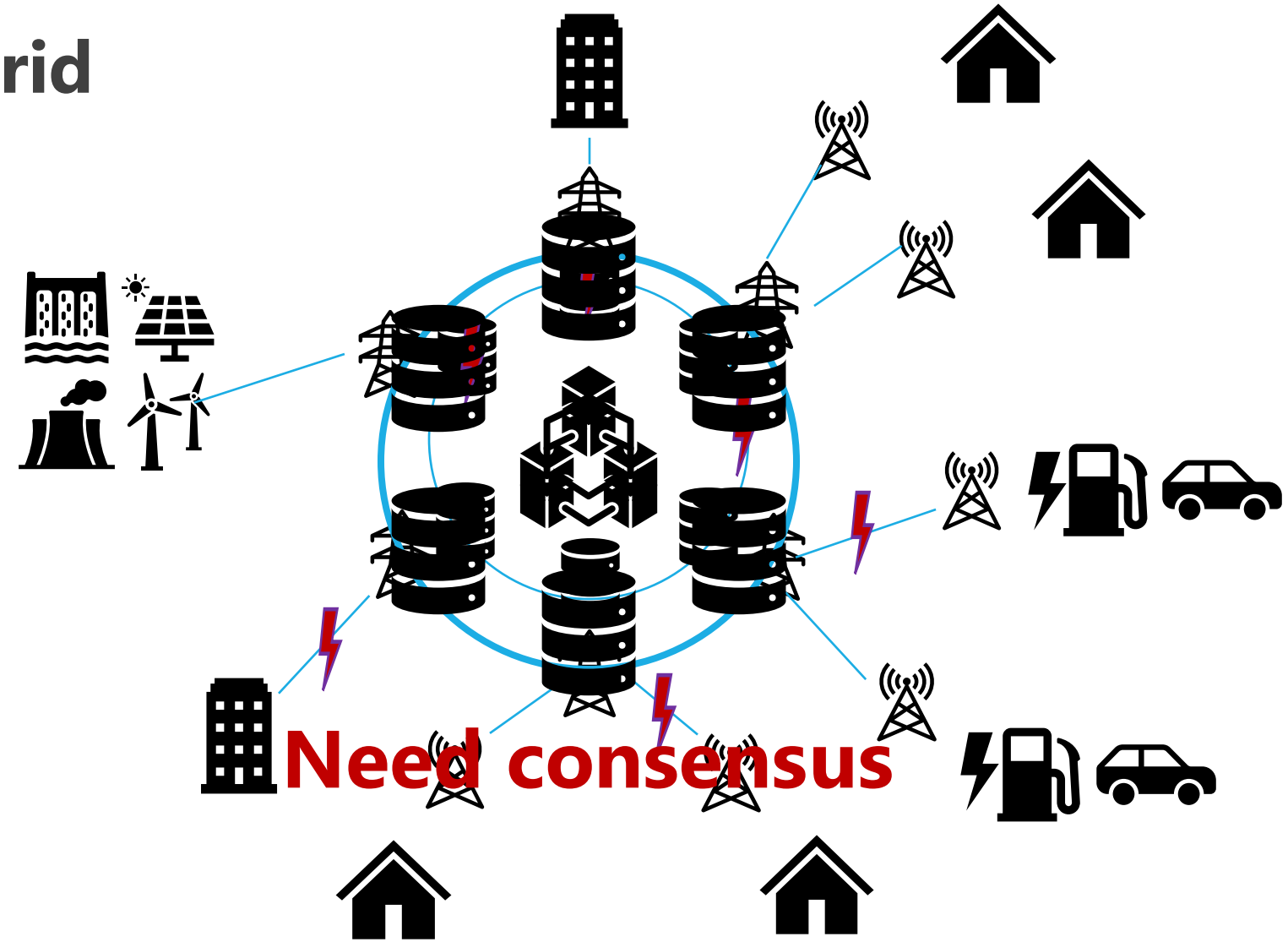
Blockchain Algorithms with Random Committee Selection

2025/2/4

Institute of Science Tokyo, Défago Lab.
Yusuke ICHIKI（市来優典）

Background

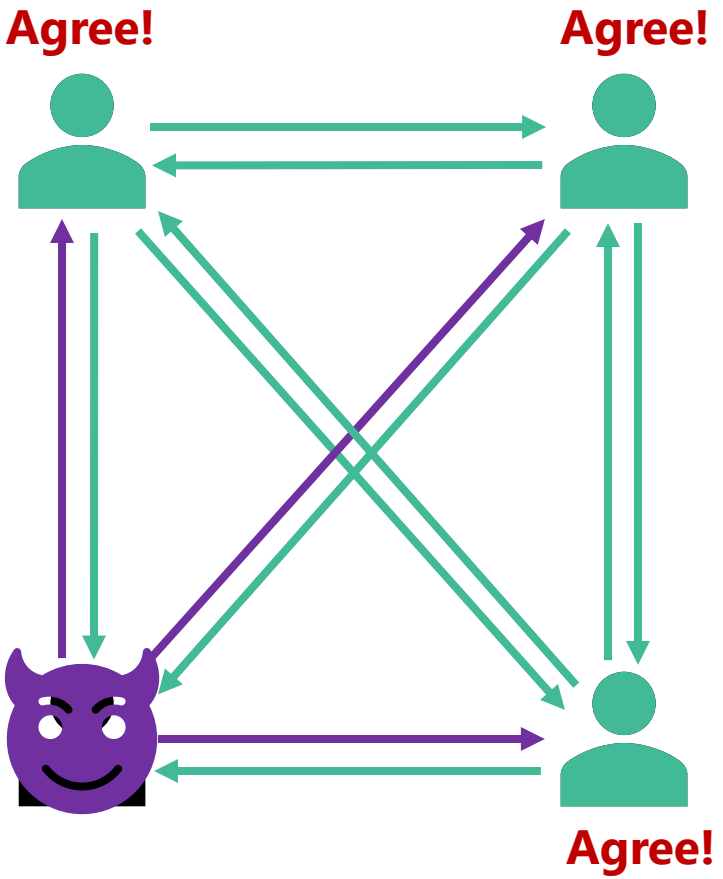
Microgrid



Problem

Byzantine Fault Tolerance[12,3]

- **Unpredictable & malicious** behavior
- **Consensus** even with faulty nodes



[12] L. Lamport+. *TOPLAS*, 1982.
[3] M. Castro+. *ACM Trans. Comput. Syst.*, 2002.

Problem

Byzantine Fault Tolerance[12,3]

- **Unpredictable & malicious** behavior
- **Consensus** even with faulty nodes

In larger systems, degrade

- Network overhead
- Resource consumption
- Latency

[12] L. Lamport+. *TOPLAS*, 1982.
[3] M. Castro+. *ACM Trans. Comput. Syst.*, 2002.

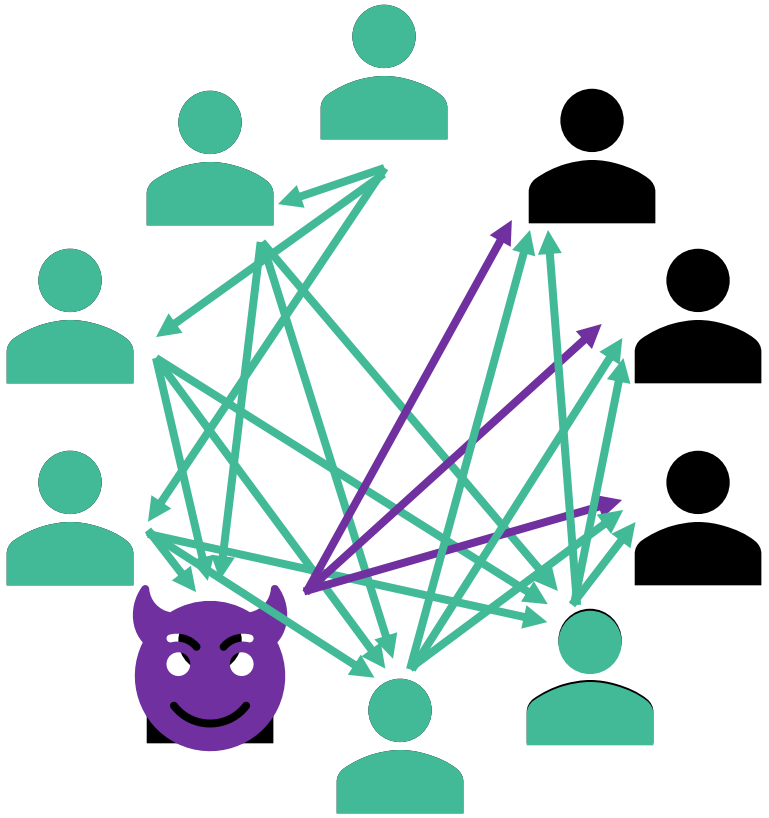
Motivation

By selecting a committee,

- Reduce communication overhead
- Decrease computational cost
- Improve latency

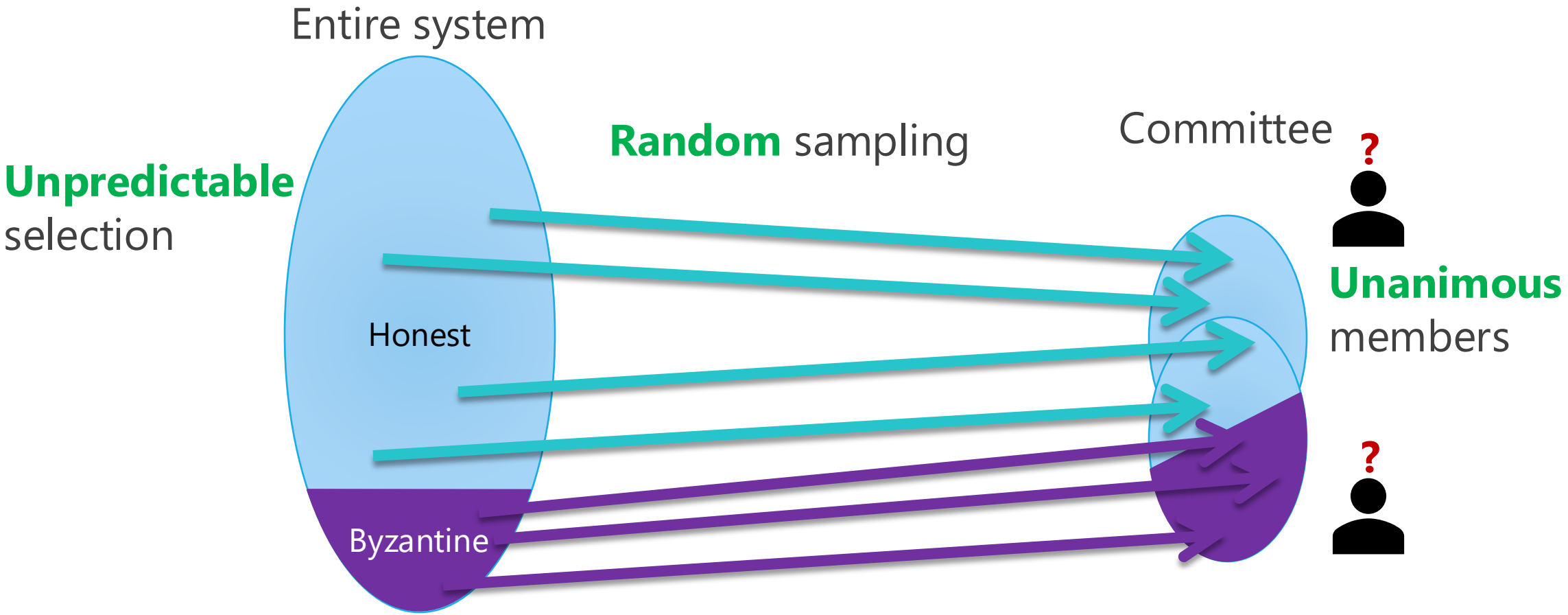
There are risks such as

- Majority of **malicious nodes**
- Target for **attacks**
- Selecting **bias**



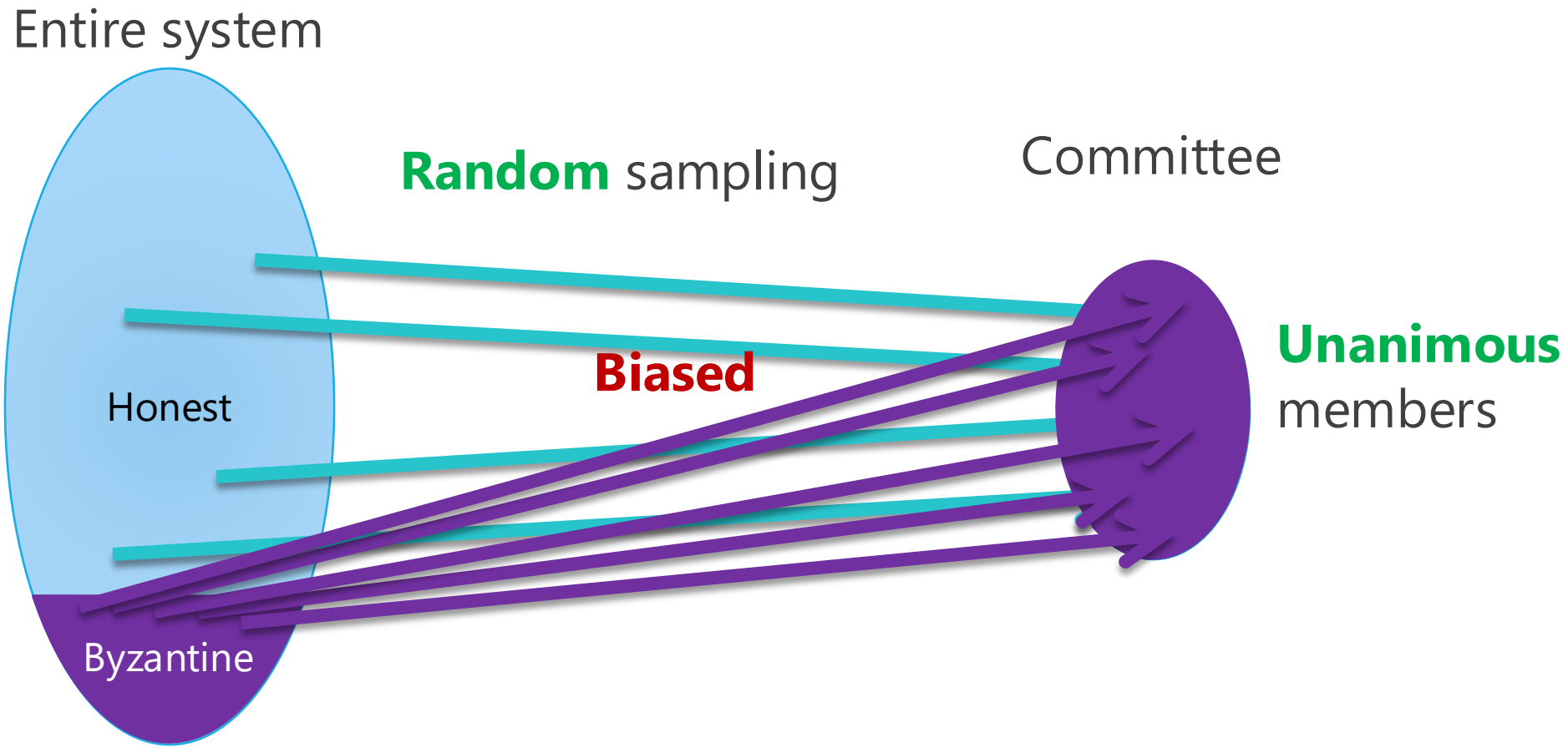
Motivation

Committee selection



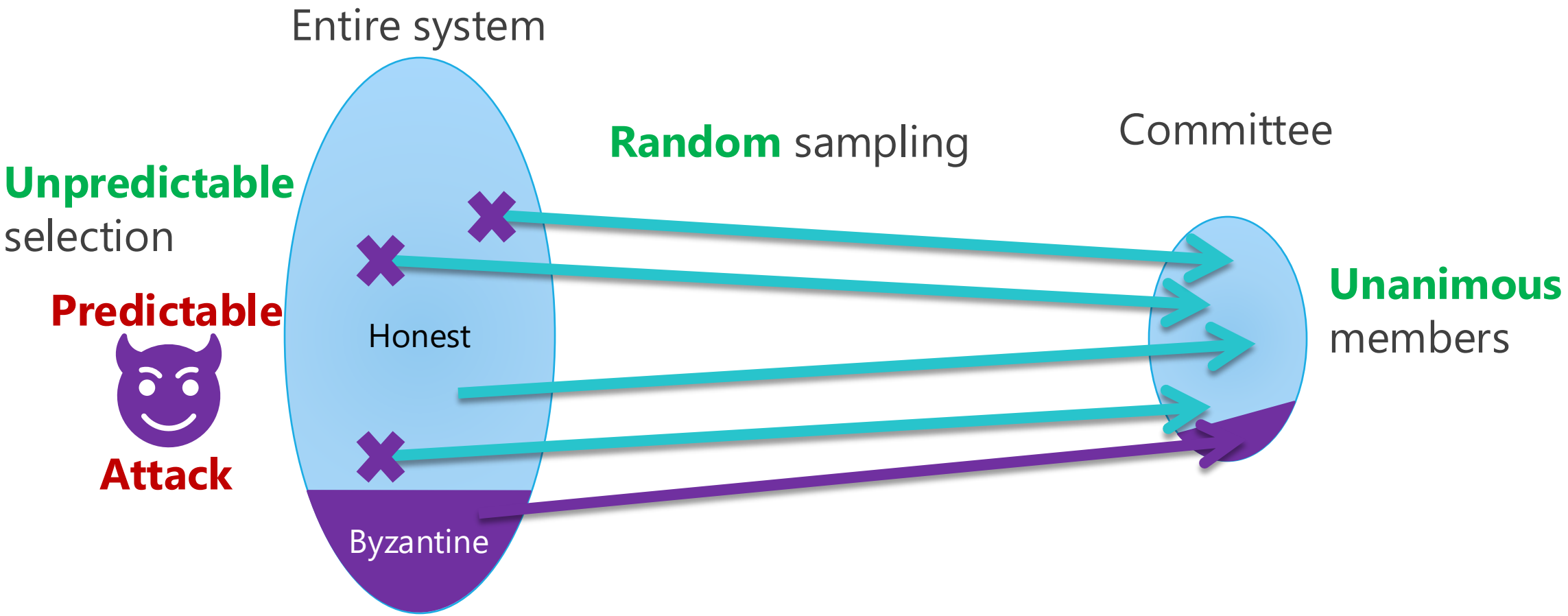
Motivation

Committee selection



Motivation

Committee selection



Related Work

Committee selection mechanisms for blockchain

Committee selection	Predictability	Committee members	Message complexity
Round robin[3]	Deterministic and highly **predictable**	**Fixed size and unanimous**	**Computed locally**
Probabilistic selection[4]	**Unpredictable**	**Cannot be fixed**	Depends on BFT algorithms
This work: Random beacon[7]	**Unpredictable before beacon generated**	**Fixed size and unanimous**	**Depends on BFT algorithms**

[3] M. Castro+. *ACM Trans. Comput. Syst.*, 2002. [4] J. Chen+. *TCS*, 2019. [7] D. Galindo+. *2021 EuroS&P*, 2021.

Research Questions

RQ1: How to apply **random, unanimous, and unpredictable** committee selection?

- RQ1.1: Delegate selection for **verification**
- RQ1.2: 〃 for **block proposal**

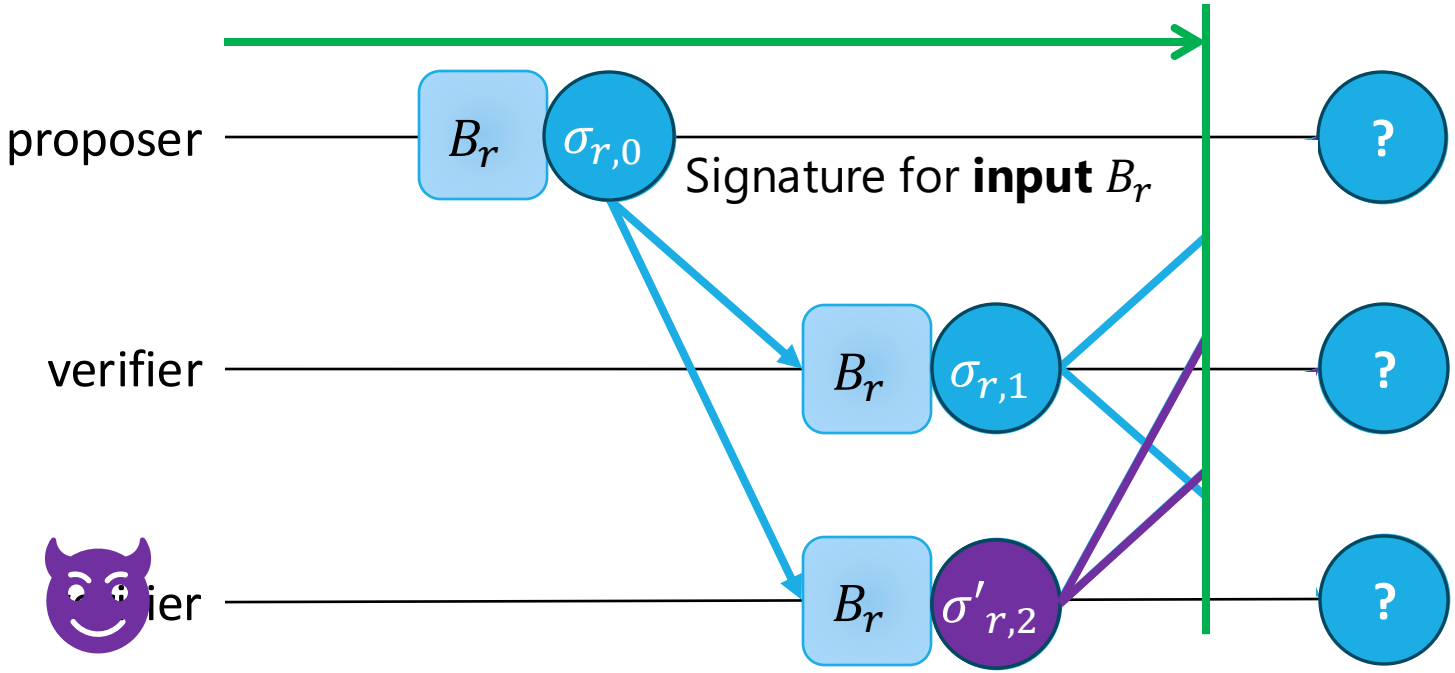
RQ2: How to improve **scalability** and **performance**?

- RQ2.1: **Large systems** by using committee selection
- RQ2.2: **Processing speed** of transactions

Combine Random Beacon

What is random beacon[13]?

- Mechanism for generating unbiased and random numbers
- Verifiable with signatures



Collect signatures

Output (random number) σ_r

Properties for B_r & σ_r

- Unpredictability
- Consistency
- Robustness
- Uniqueness

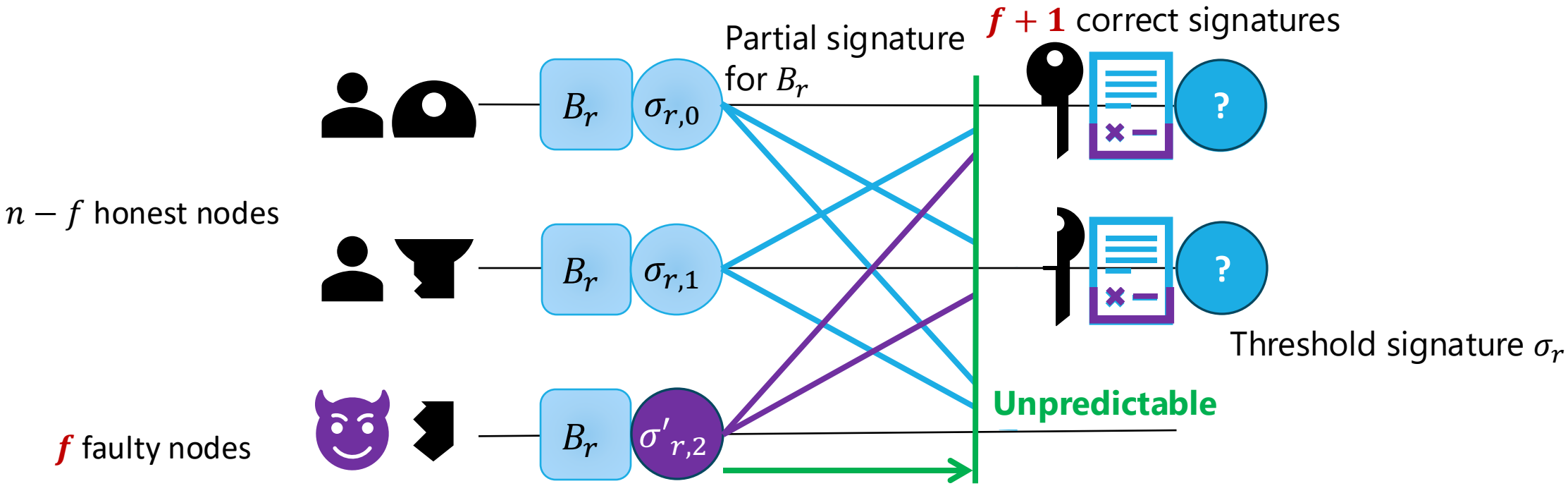
Single unique σ_r for each B_r

[13] J. Liao+. *The 54th DSN*, 2024.

Signature Scheme

How to secure randomness and unpredictability?

- Utilize a threshold signature scheme[7]

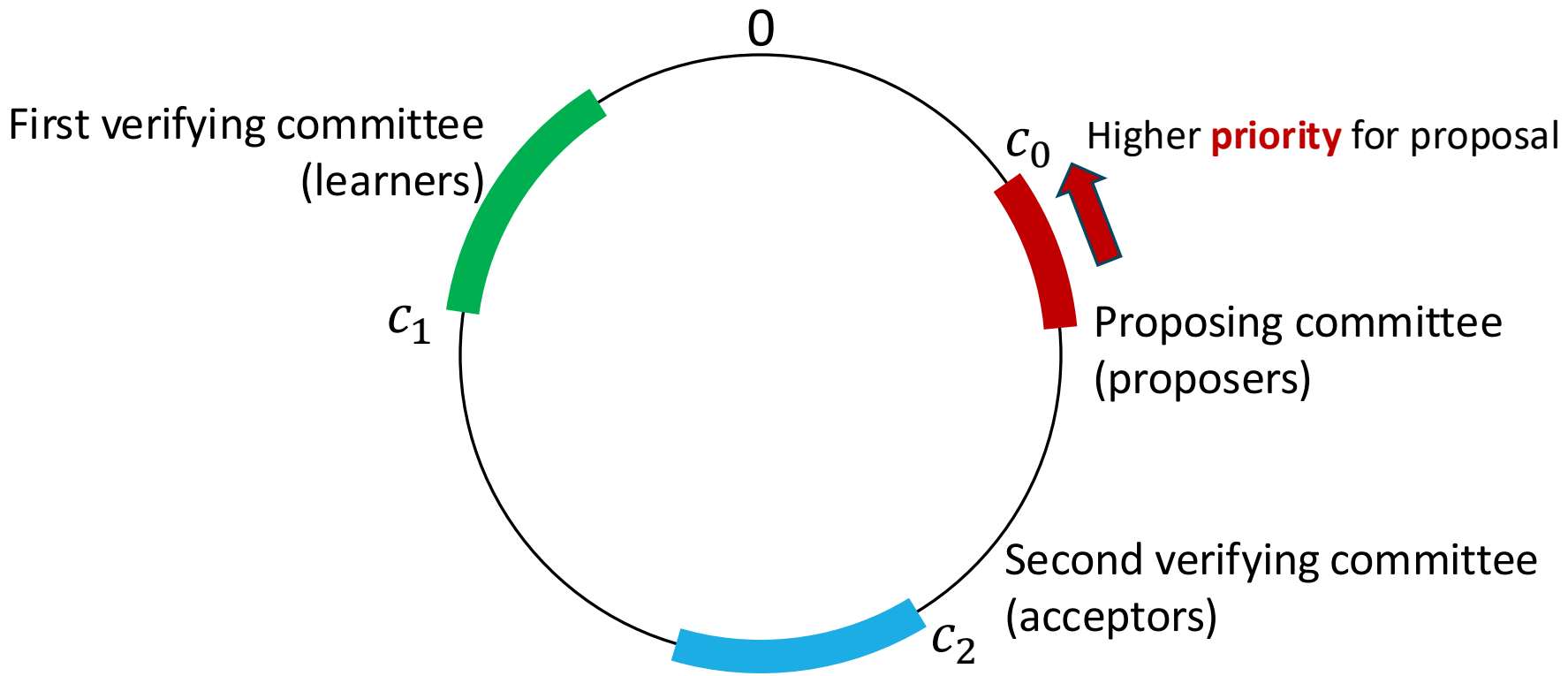


[7] D. Galindo+. *2021 EuroS&P*, 2021.

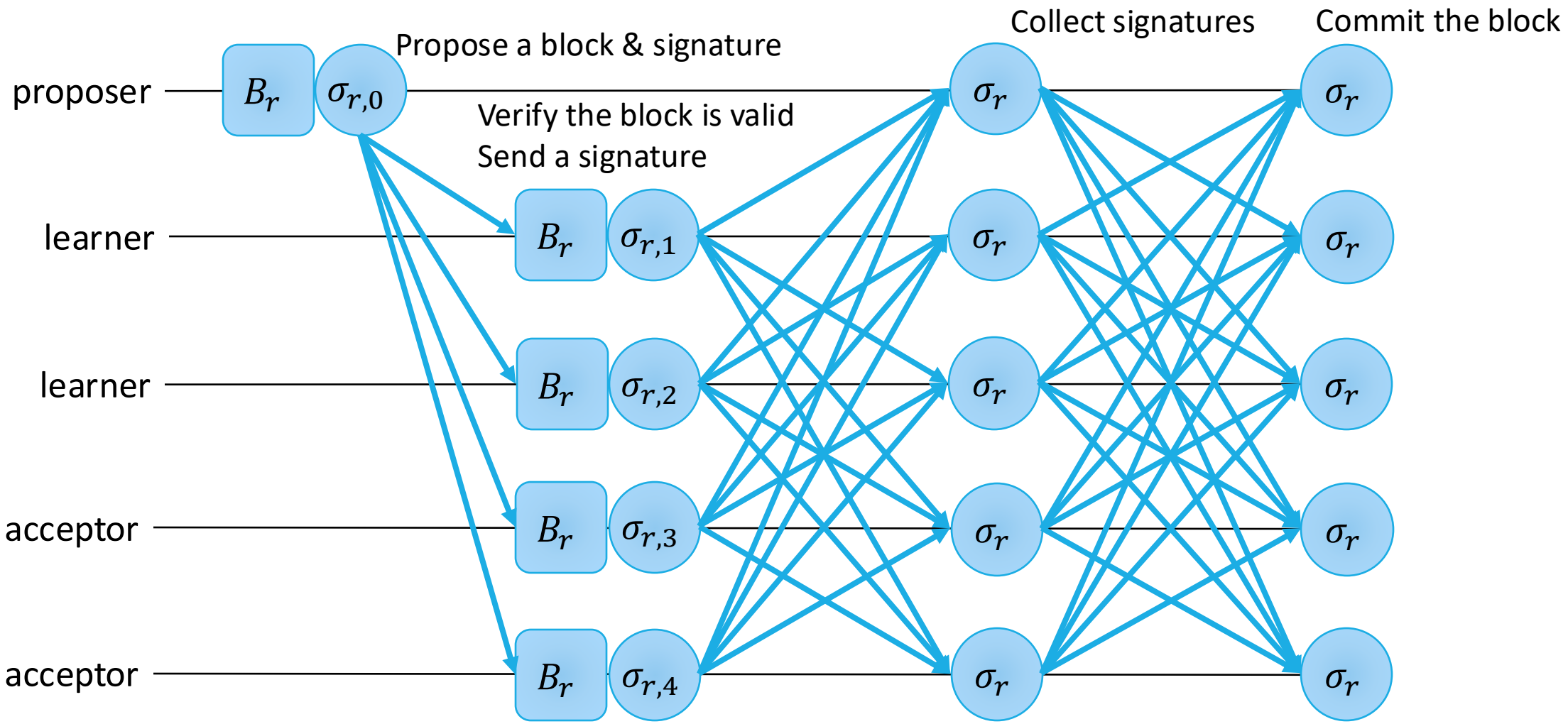
Committee Selection

Select committees from random beacon's output

- Use **uniformly random** numbers: $c_k = H(r, \sigma_{r-1}, k)$

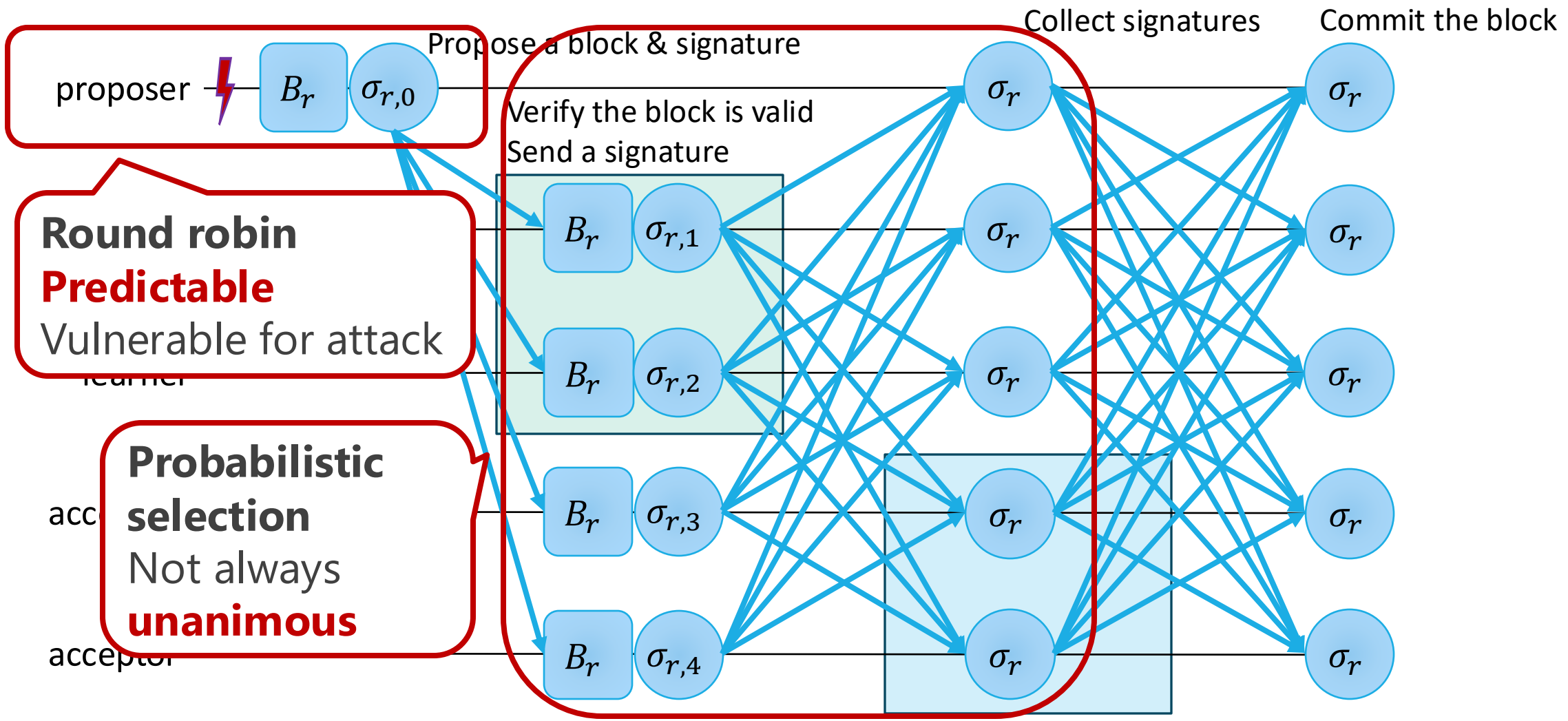


Existing committee selection[3,4]



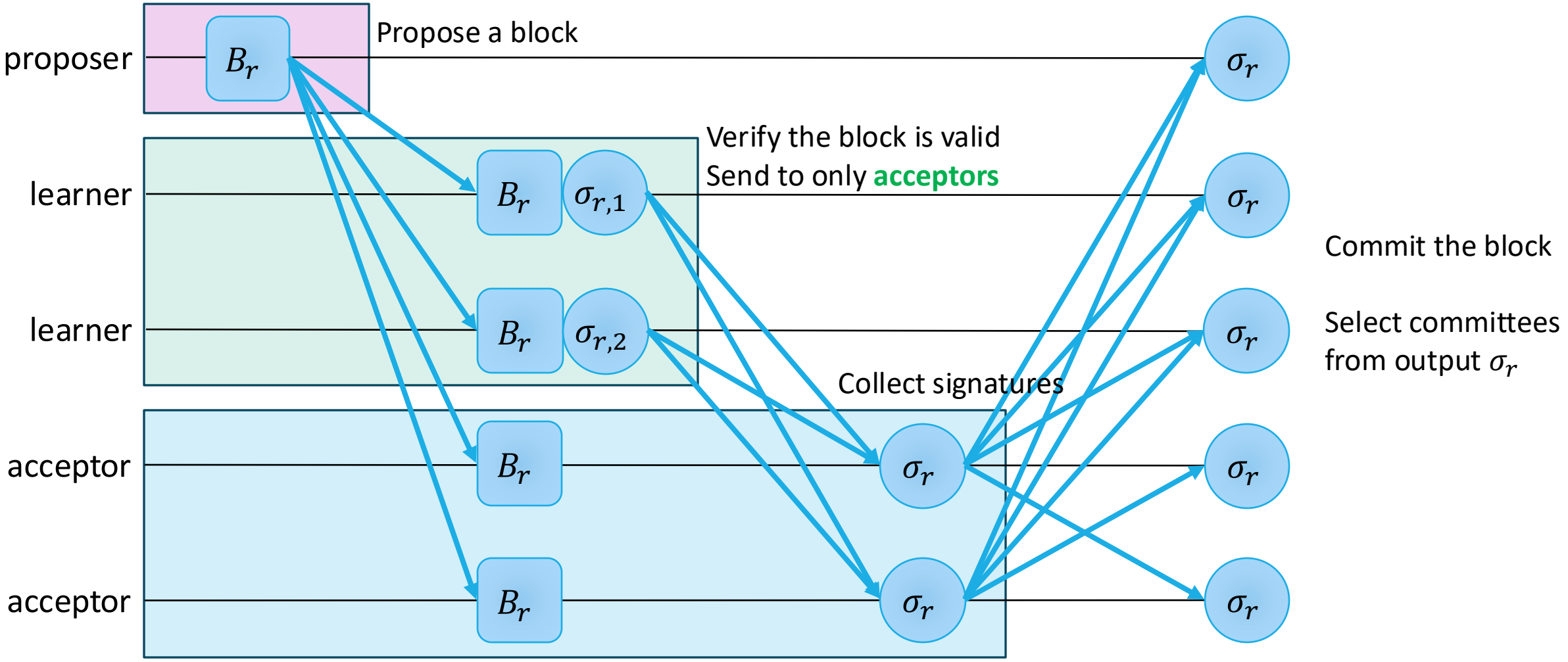
[3] M. Castro+. *ACM Trans. Comput. Syst.*, 2002. [4] J. Chen+. *TCS*, 2019.

Existing committee selection[3,4]

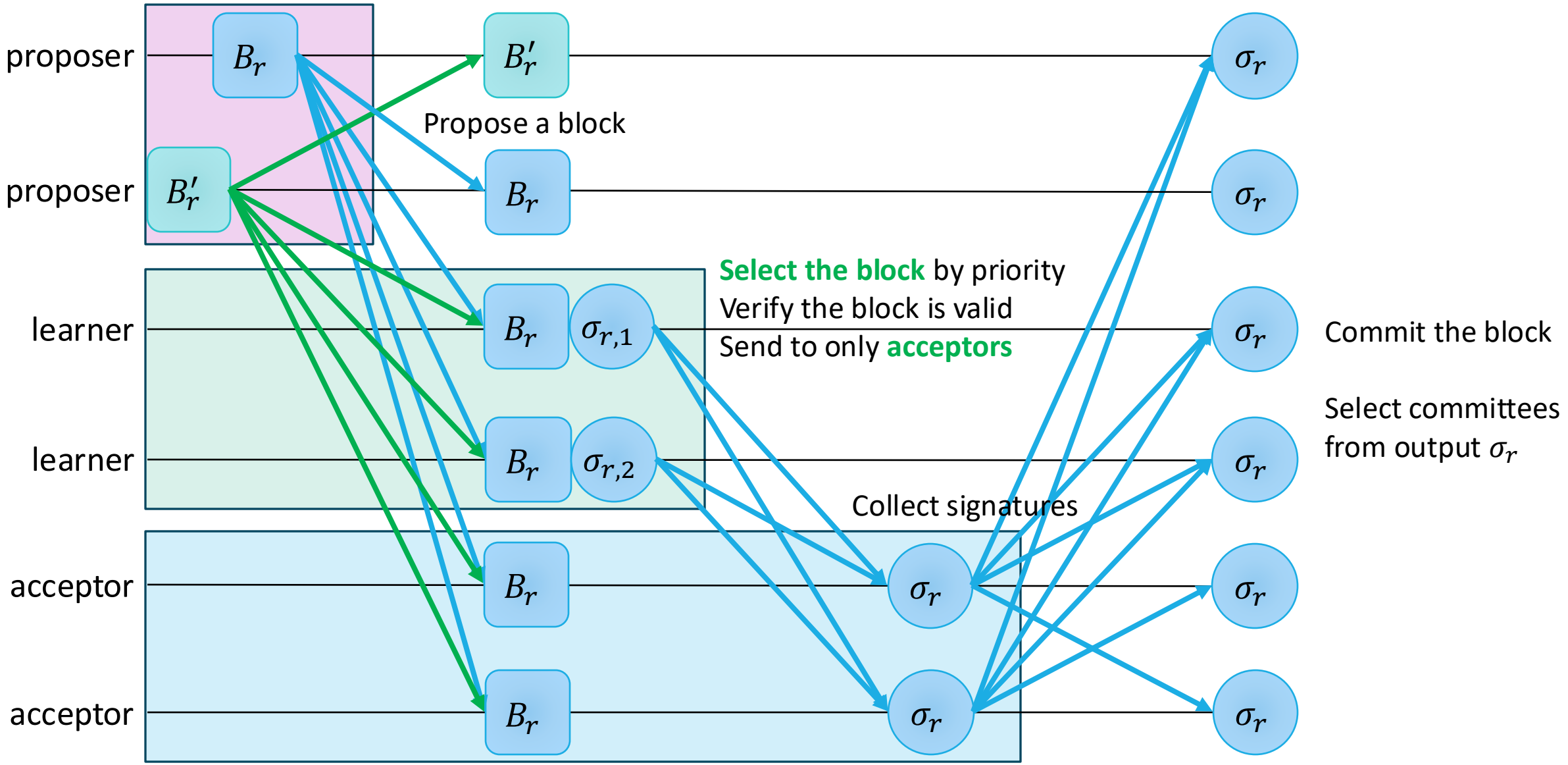


[3] M. Castro+. *ACM Trans. Comput. Syst.*, 2002. [4] J. Chen+. *TCS*, 2019.

Approach


proposer
learner
learner
acceptor
acceptor
B_r
Propose a block
B_r
$\sigma_{r,1}$
Verify the block is valid
Send to only acceptors
B_r
$\sigma_{r,2}$
B_r
B_r
Collect signatures
σ_r
σ_r
σ_r
σ_r
σ_r
σ_r
σ_r
Commit the block
Select committees from output σ_r

Approach


proposer
proposer
learner
learner
acceptor
acceptor
B_r
B'_r
Propose a block
B'_r
B_r
Select the block by priority
Verify the block is valid
Send to only acceptors
B_r
$\sigma_{r,1}$
B_r
$\sigma_{r,2}$
Collect signatures
B_r
B_r
σ_r
σ_r
σ_r
σ_r
σ_r
σ_r
σ_r
Commit the block
Select committees from output σ_r

Research Questions

RQ1: How to apply random, unanimous, and unpredictable committee selection?

- ☑ Combine **random beacon** with BFT algorithms
  - Only do committees enter consensus process, i.e., **less messages**.

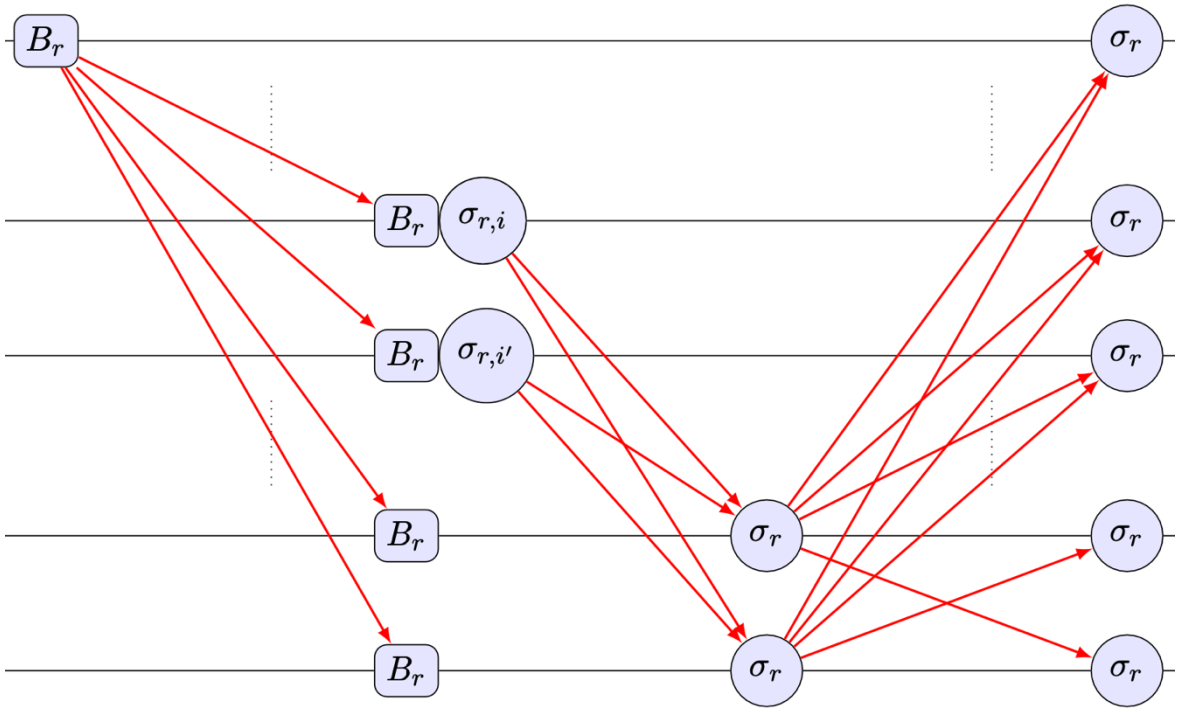
RQ2: How to improve scalability and performance?

- Evaluate performance of committee selection in a large system

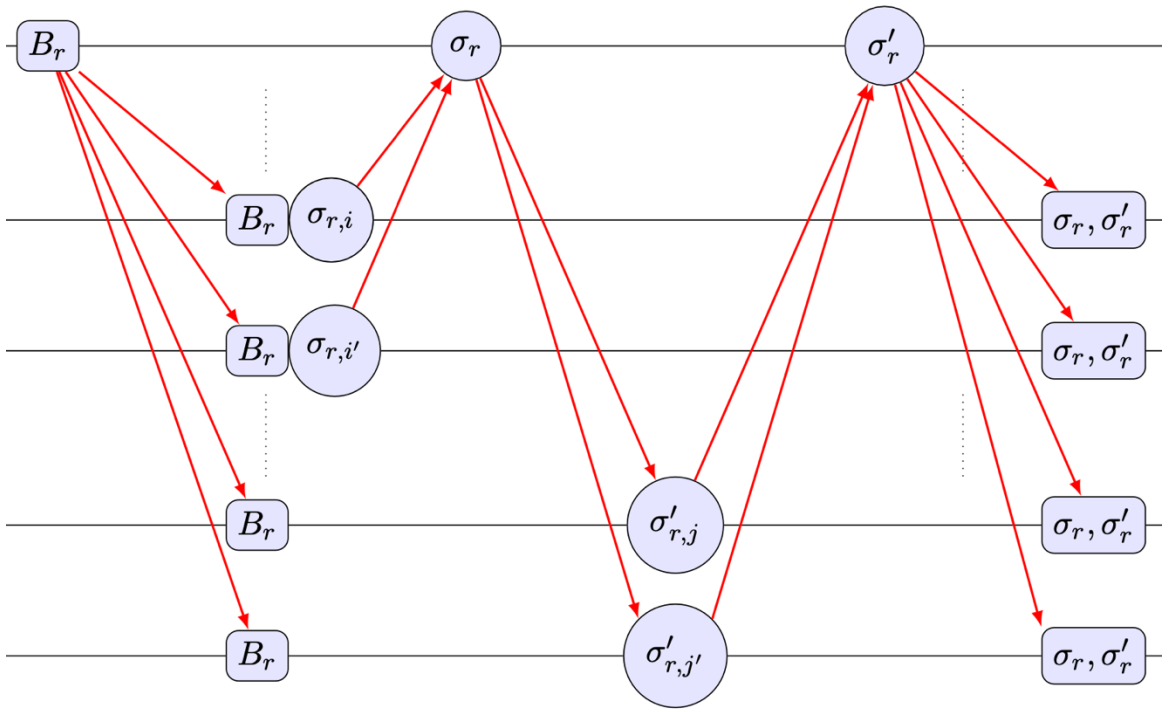
Evaluation

BFT algorithms used in simulation

PBFT[3]: $O(n^2)$ messages



HotStuff-2[14]: $O(n)$ messages

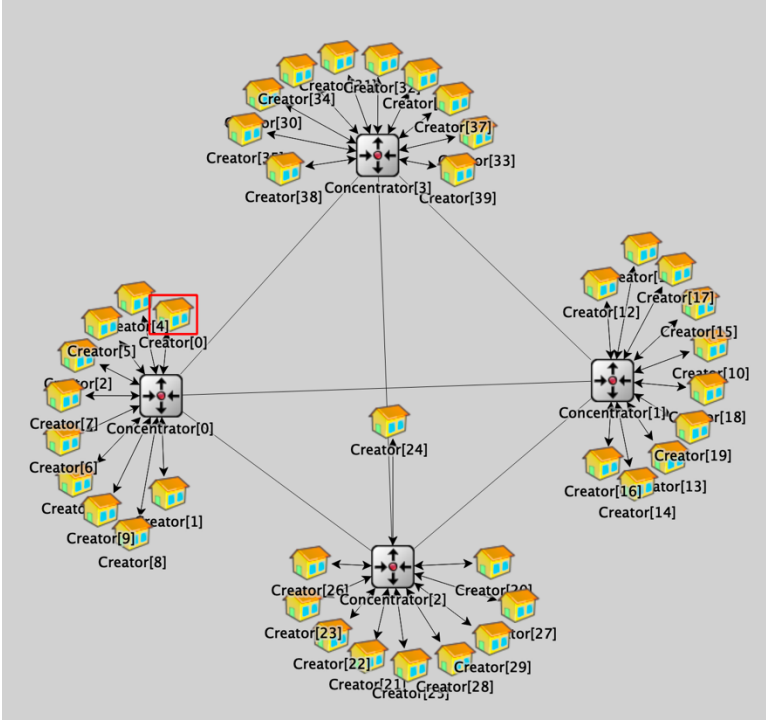


[3] M. Castro+. *ACM Trans. Comput. Syst.*, 2002.
[14] D. Malkhi+. *Cryptology ePrint Archive*, 2023.

Evaluation

Simulation settings: microgrid system[1]

- Parameters
  - **1000 smart meters:** record trades and send information
  - **10%** are faulty
  - **Transaction size:** 512 bytes
  - **Block size:** 64 KB ~ 16 MB
- Metrics
  - **Throughput:**
    Rate at which the system commits transactions
  - **Latency:**
    Delay between block proposal and finalization



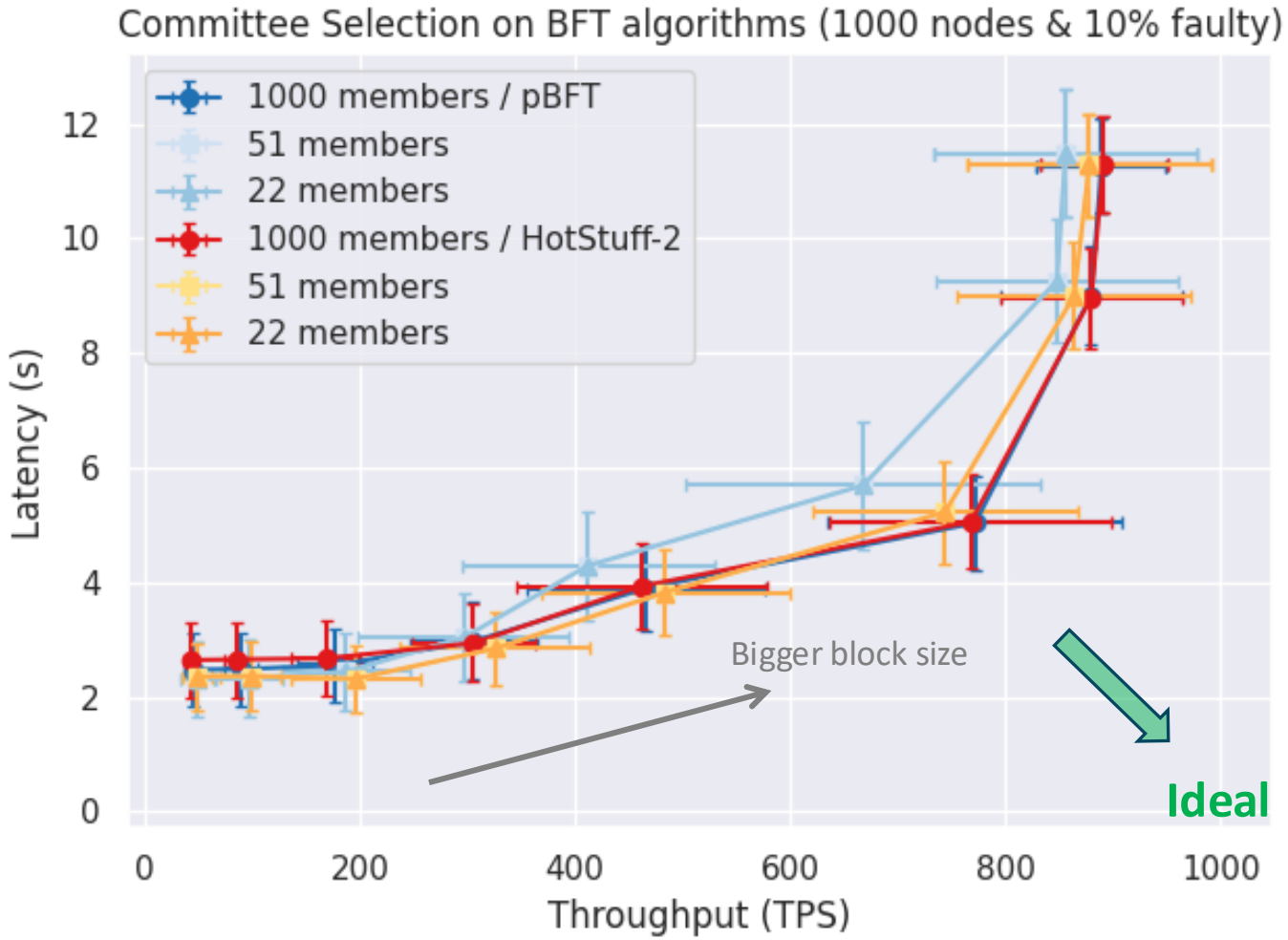
Simulation on OMNeT++[16]

[1] D. Bian+. *IET Communications*, 2019.
[16] OMNeT++. https://omnetpp.org, 2024.

Results

Verifying committee selection

- **Less messages**, but…
- Committee **does not impact** on speed due to faulty proposers.
- What about multiple proposers?

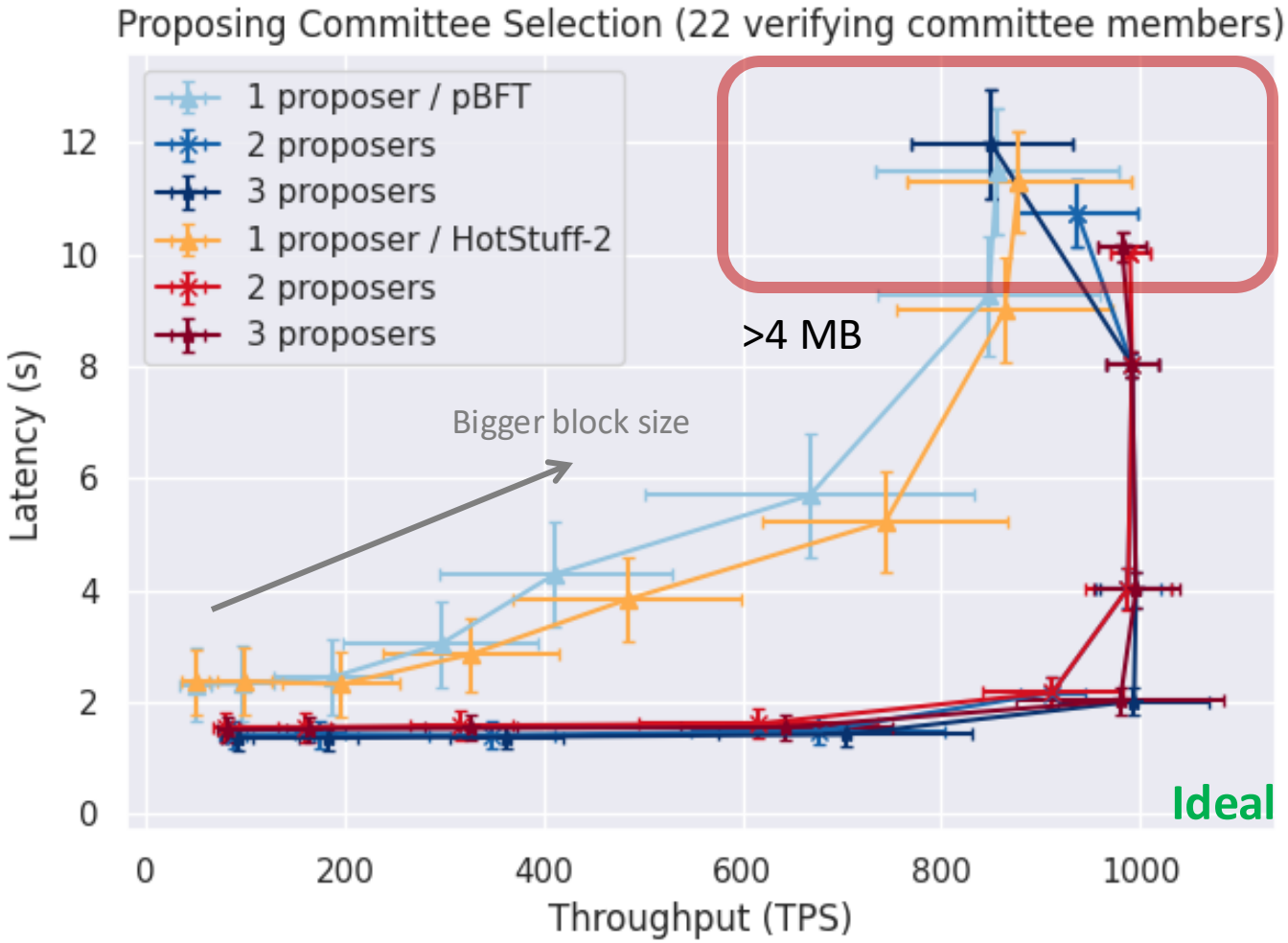


Results

Proposing committee selection

- Improve on both **throughput** & **latency**
- Less timeouts

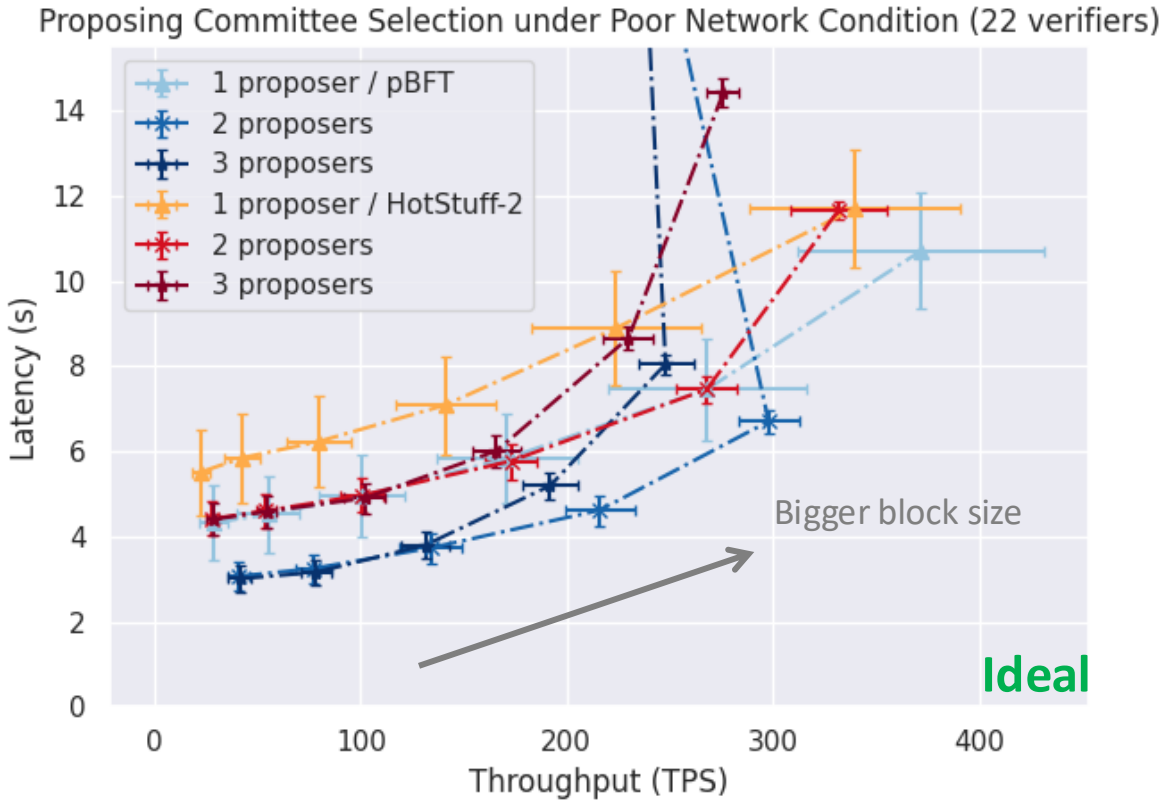
- Performance differs when block size >4 MB.
- **Network overhead** for proposals?



Results

Under poor network condition

- Impact of block size gets **bigger** as num. of proposers is bigger.
- **Network overhead** makes verification difficult
- Maximum size for consensus depends on **compexity** of BFT algorithms.



Conclusion

RQ1: How to apply random, unanimous, and unpredictable committee selection?

- ☑ Combine **random beacon** with BFT algorithms
  - Only do committees enter consensus process, i.e., **less messages**.

RQ2: How to improve scalability and performance?

- ☑ Scalability improves with **verifying committee selection**.
- ⚠ Performance improves with **multiple proposers** with **a good network condition**.

Open Question

- **Overhead** for reorganizing a round from timeout is heavy. How to **reduce** it?

Appendix

Approach

Combine random beacon with BFT algorithms

Select committees from random beacon's output

- $H(\cdot)$: Hash function
- P_r: proposing committee, n_P: size of P_r
- $V_{r,1}, V_{r,2}$: verifying committees, n_V: size of $V_{r,1}, V_{r,2}$
- $$\begin{cases} P_r = \{c_0 \bmod n, \dots, (c_0 + n_P - 1) \bmod n\} \\ V_{r,1} = \{c_1 \bmod n, \dots, (c_1 + n_V - 1) \bmod n\} \\ V_{r,2} = \{c_2 \bmod n, \dots, (c_2 + n_V - 1) \bmod n\} \end{cases} \left(c_k = H(r, \sigma_{r-1}, k)\right)$$

Evaluation

Committee size

- When $n = 1000$ and $f = 100$,
- Size for two verifying committees with one in a million chances of corruption in the same round, is ≥ 22.
- Size for either of the committees with one in a million chances of corruption, is ≥ 51.