

Blockchain Algorithms with Random Committee Selection

2024/9/3

Tokyo Institute of Technology, Défago Lab.

市来優典

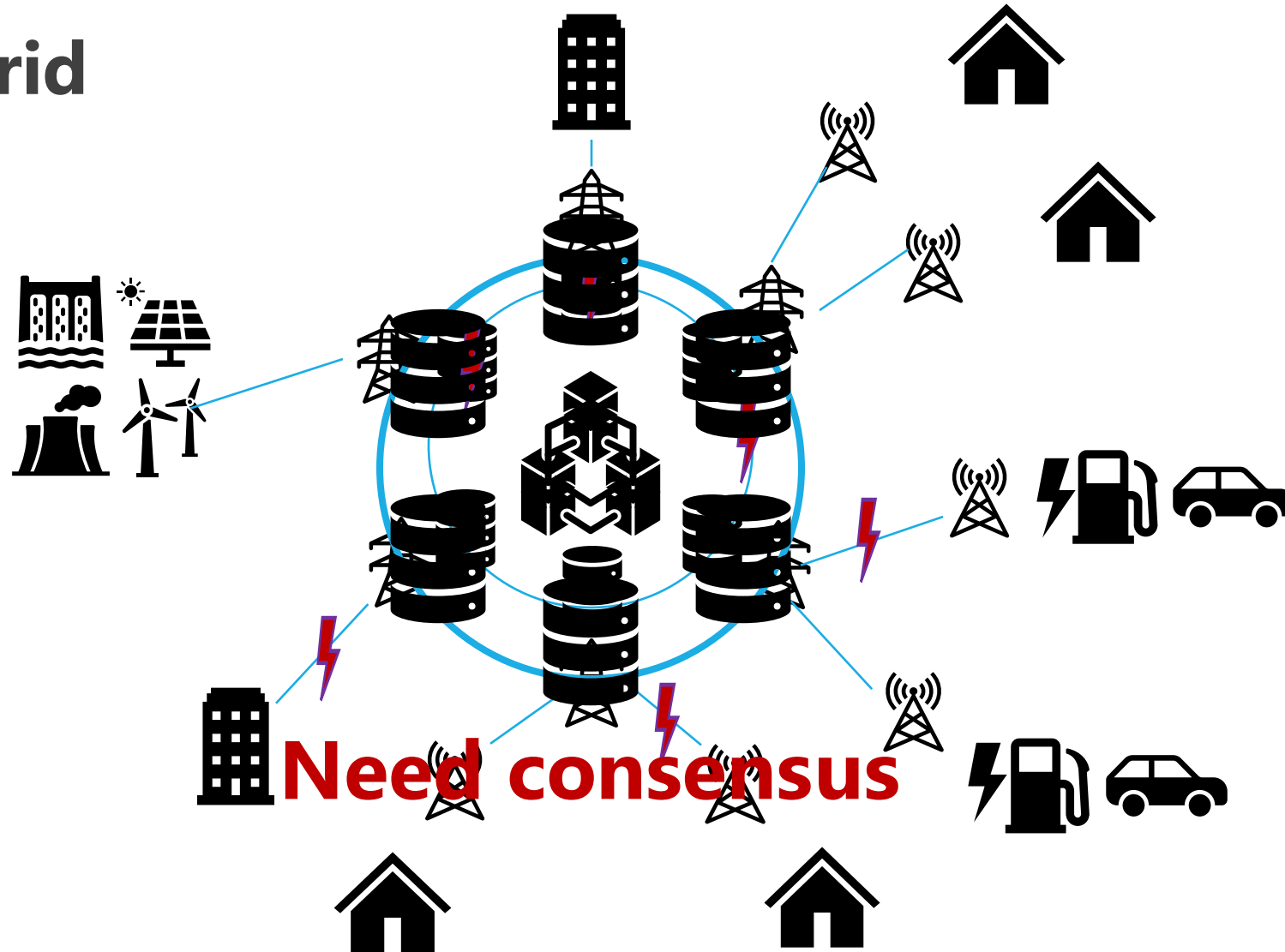
This research explores the integration of decentralized random beacon in Byzantine consensus algorithms to improve scalability through random committee selection. Existing consensus algorithms often encounter challenges regarding network overhead and energy consumption. To address these issues, we propose an approach utilizing random beacon to select committees randomly, unpredictably, and unanimously.

- Background
- Problem
- Motivation
- Related Work
- Research Questions
- Approach
- Progress

Background

4

Microgrid

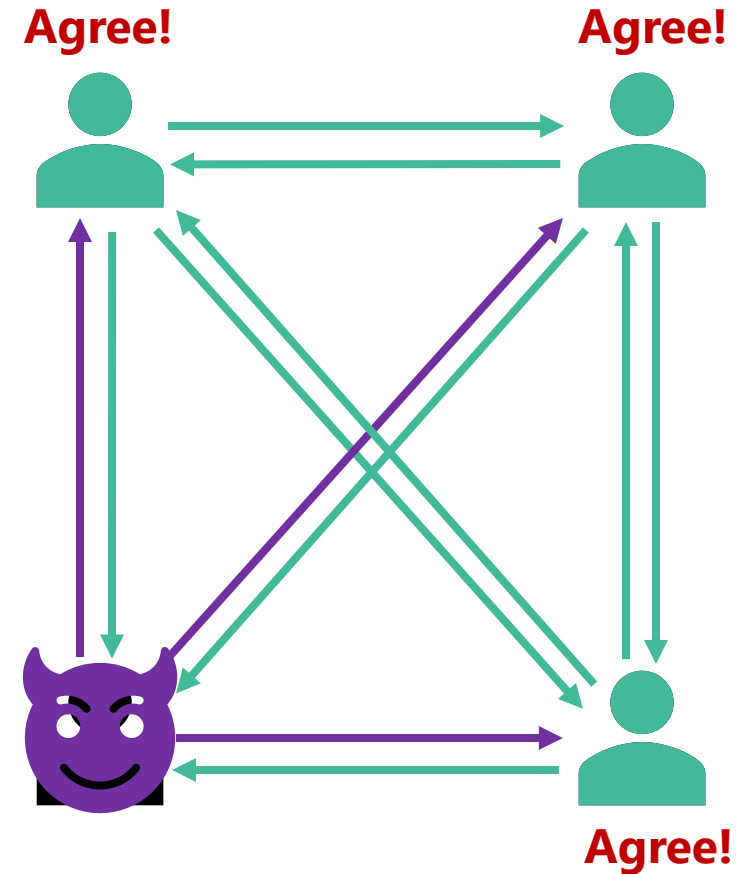


Problem

5

Byzantine Fault Tolerance^[1]

- Some nodes behave in **unpredictable, malicious** manners.
- Goal is to reach consensus while some nodes are faulty.



[1] M. Castro & B. Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* 20, 4, 398–461, 2002.

Byzantine Fault Tolerance^[1]

- Some nodes behave in **unpredictable, malicious** manners.
- Goal is to reach consensus while some nodes are faulty.

In **larger** systems, degrade

- Network overhead
- Resource consumption
- Latency



Motivation

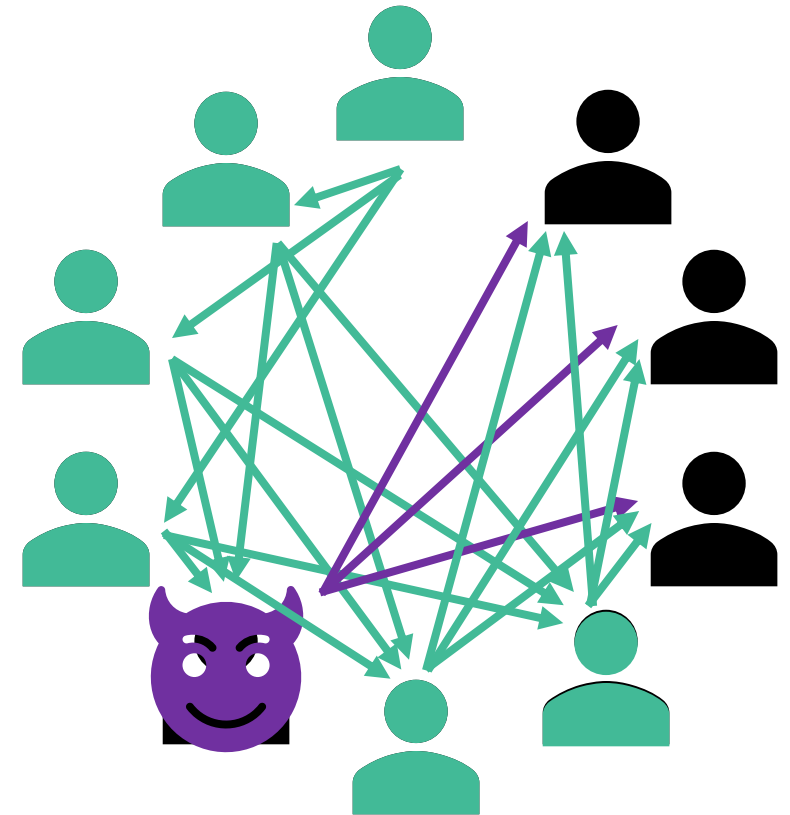
7

By selecting a committee,

- Reduce communication overhead
- Decrease computational cost
- Improve latency

There are risks such as

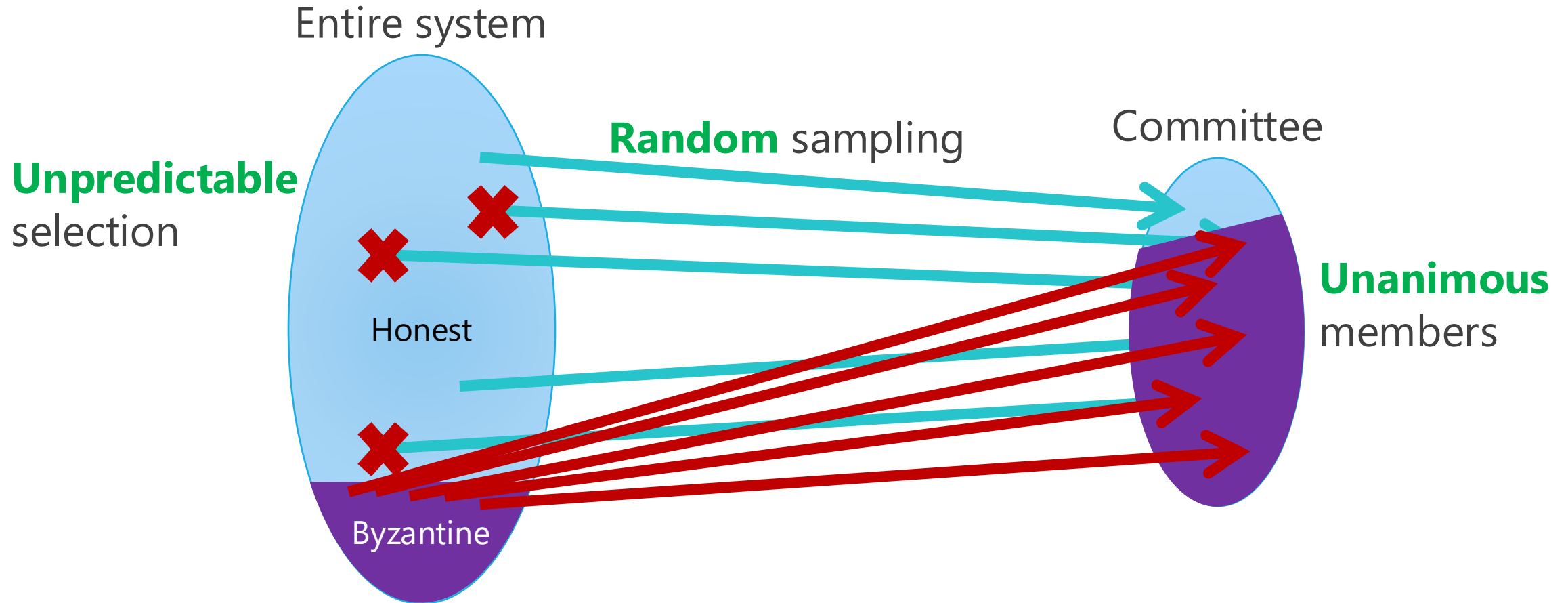
- Majority of **malicious nodes**
- Target for **attacks**
- Selecting **bias**



Motivation

8

Committee selection



Committee selection mechanisms for blockchain

Committee selection	Predictability	Committee size	Message complexity
Predefined order to select leader ^[1]	Deterministic and highly predictable	Fixed size	Computed locally
Cryptographic self-selection ^[2]	Unpredictable	Cannot be fixed	O(kn) k: committee size n: num. of nodes
This work: Decentralized random beacon^[3]	Unpredictable before beacon generated	Fixed size	O(kn)

[2] J. Chen & S. Micali. Algorand: A secure and efficient distributed ledger. *Theoretical Computer Science*, 2019.

[3] D. Galindo, J. Liu, M. Ordean and J. -M. Wong. Fully Distributed Verifiable Random Functions and their Application to Decentralised Random Beacons. *2021 IEEE European Symposium on Security and Privacy*, 2021.

Research Questions

10

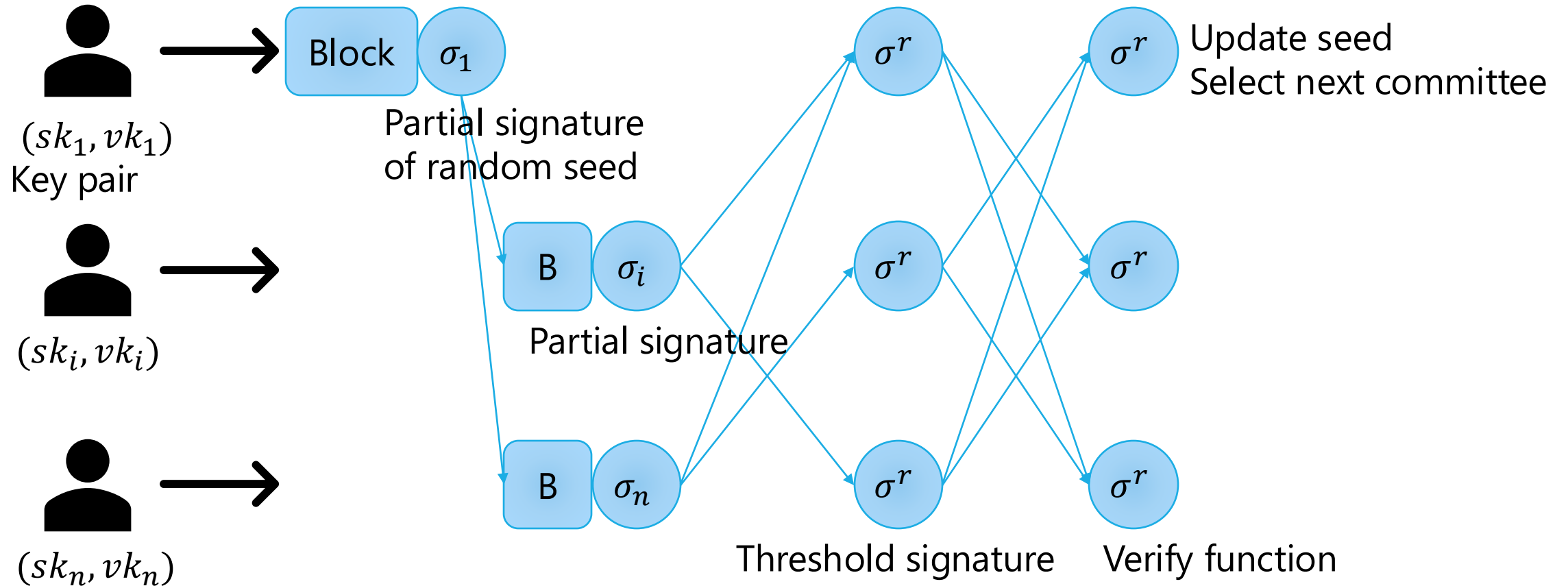
RQ1

- How to apply random, unanimous, and unpredictable committee selection?
 - RQ1.1: Delegate selection for **verification**
 - RQ1.2: Delegate selection for **block proposal**
 - RQ1.3: Both

RQ2

- How to improve decentralization and scalability?
 - What is the ideal size of proposer and verifier committees?

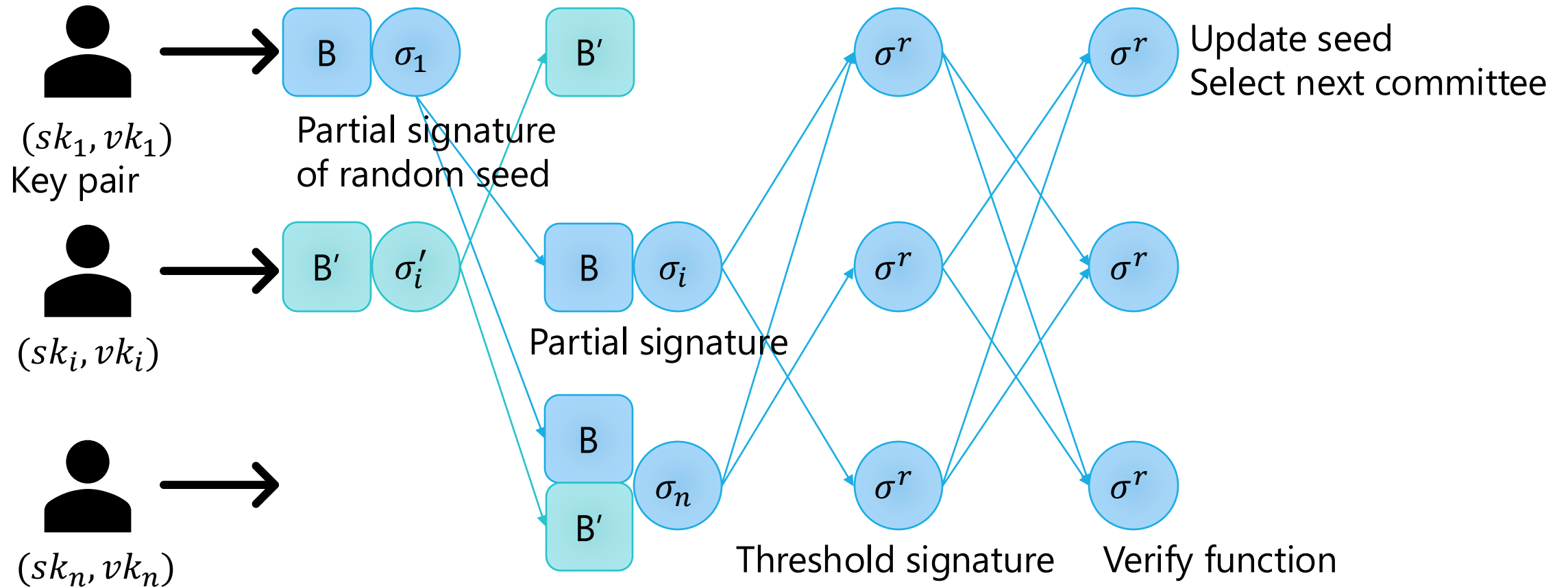
Combine random beacon with consensus^[4]



Approach

12

Multiple proposals into consensus



Research Questions

- ☑ How to apply committee selection?
 - Apply random beacon to both consensus and selection
- ☐ How to improve decentralization and scalability?
 - Simulate a microgrid system with $\geq 5,000$ nodes

	~ August	September	October	November	December	January
Committee selection						
Performance evaluation						
Thesis						