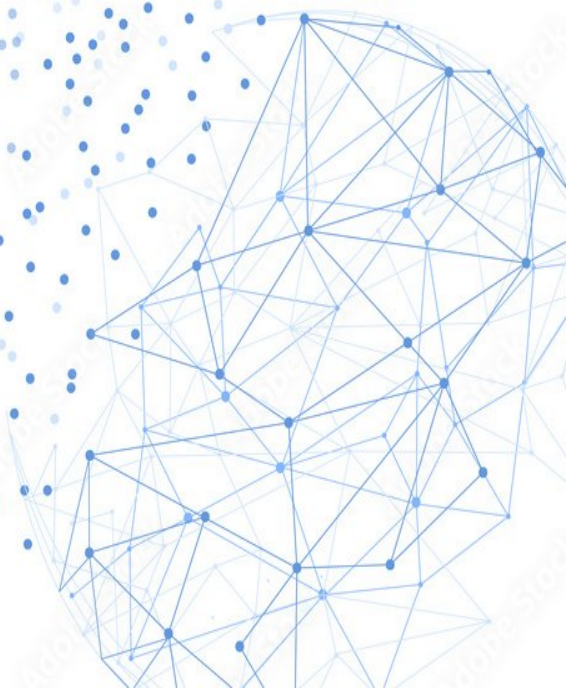
An Optimized Consortium Blockchain for Medical Information Sharing

Course : CS540 (Blockchain)



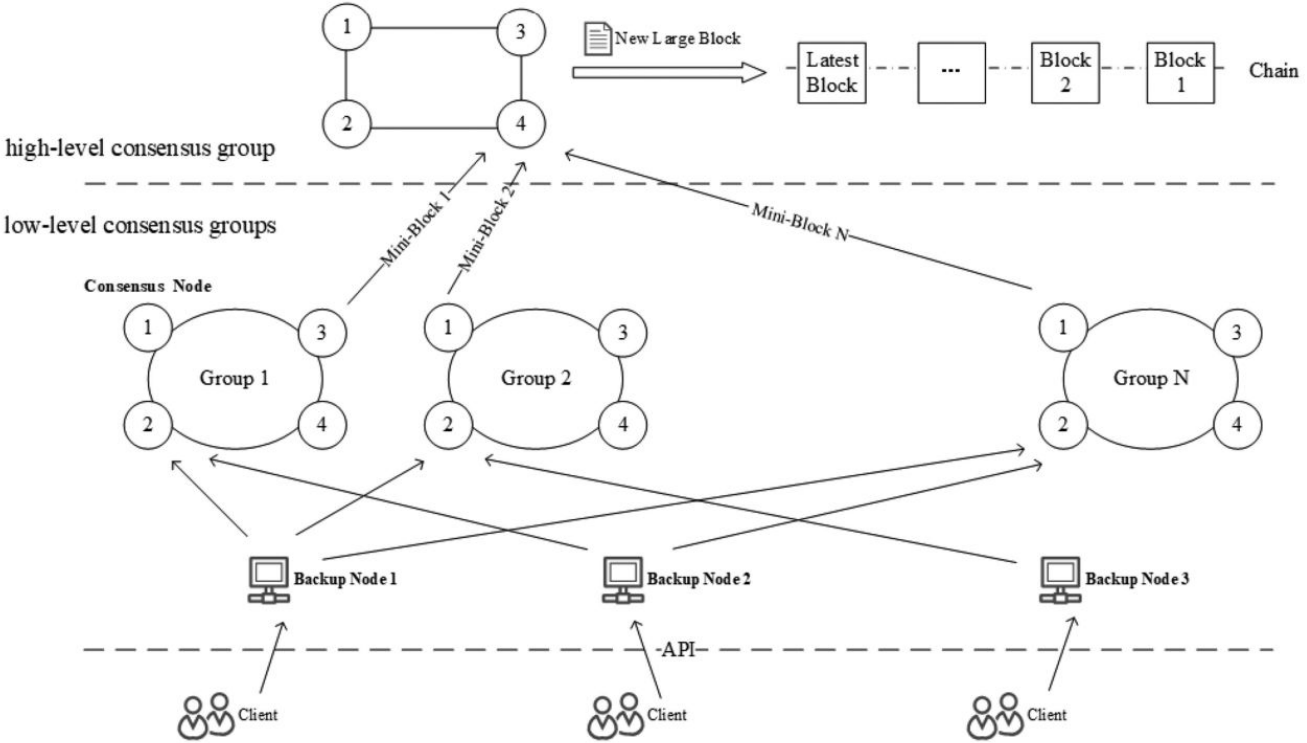
Course Instructor : Dr. Sujata Pal

Sahil Pathak : sahil.23csz0005@iitrpr.ac.in
Raghav Patidar : 2020csb1115@iitrpr.ac.in
Rohan Khanna : 2020csb1117@iitrpr.ac.in
Vijay Dwivedi : 2020csb1140@iitrpr.ac.in
Nikhil Rastogi : 2021mcb1240@iitrpr.ac.in

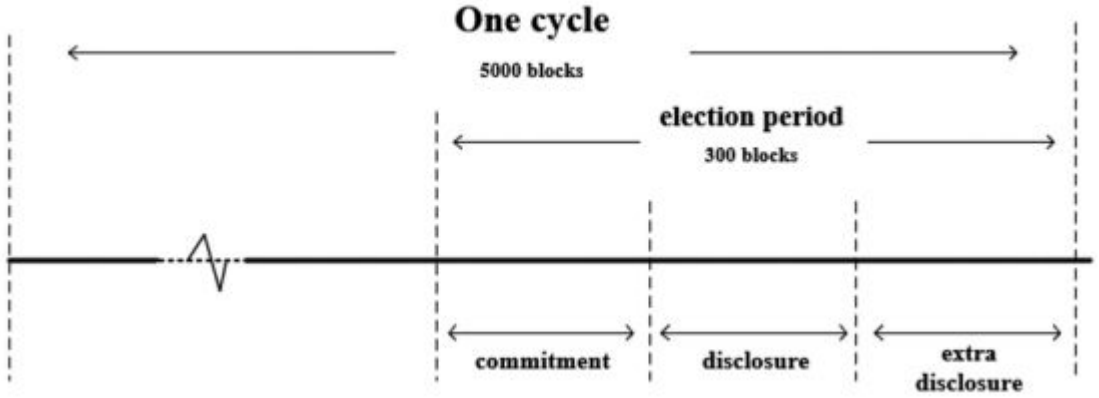
Introduction

- Design a **medical information sharing platform** and its business process using consortium blockchain.
- **Two-layer architecture:** Improve the consortium blockchain by splitting the nodes into two layers: a low-level consensus group (LCG) and a high-level consensus group(HCG). Split the transactions. When the number of transactions increases, only a subset of the CNs are needed to verify the transactions.
- Implement consensus algorithm in the LCG derived from Zyzzyva as done in the paper.
- Design a **VRF mechanism** for selecting the CNs from many verified nodes.
- **Performance Evaluation:** Measure and analyze the performance of the blockchain-based medical information sharing. Improve the application to implement it on public blockchain.

Structure of Blockchain



VRF Mechanism



Analysis of Blockchain

Introduction:

- Our blockchain employs a two-layer structure and innovative sharding technology to redefine scalability.

Sharding Technology:

- Traditional consensus methods involve all nodes in transaction verification.
- Sharding allows a subset of nodes to verify transactions, optimizing efficiency.

Node Efficiency:

- Each node is relieved from verifying all transactions, enhancing overall efficiency
- As the consensus group size grows, Transaction Per Second (TPS) scales linearly.

Analysis : Safety, Liveness, and Fault Tolerance

Safety and Liveness:

- Sharding technology enhances scalability and TPS but introduces challenges in safety and liveness.
- Maintaining a secure and responsive network is crucial for blockchain functionality.

MBFT's Approach:

- In our blockchain, the MBFT consensus algorithm is employed.
- A re-election mechanism is strategically designed to balance performance, scalability, and fault tolerance.

Fault Tolerance in MBFT:

- Despite scalability improvements, MBFT maintains a fault tolerance of 1/3.
- The re-election mechanism ensures continuous operation even in the presence of faulty nodes.