Sharding SMR with Optimal-size Shards for Highly Scalable Blockchains

Jianting Zhang¹, Zhongtang Luo¹, Raghavendra Ramesh², Aniket Kate¹,²

¹Purdue University, ²Supra Research

Introduction

Blockchain Scalability

Performance | Network Scale

- Blockchain scalability is evaluated by performance and network scale.
- With more nodes joining in, a scalable blockchain system is expected to handle more transactions.

Key Observations

Obs1: Blockchains rely on state machine replication to maintain a ledger securely, performing the repeated tasks:
1. Dissemination (data availability);
2. Ordering;
3. Execution
- Tasks 1&3: resource-intensive but 1/2 fault tolerance
- Tasks 2: resource-saving but only 1/3 fault tolerance
Obs2: The larger the fault tolerance a shard achieves, the smaller the size of the shard is needed.

Blockchain Sharding

Nodes are divided into shards

Ideal sharding:
- Small shard size
- Multiple shards
- High performance

Actual sharding:
- Large shard size
- Few shards
- Limited performance

- Sharding scales a blockchain by dividing nodes into shards for parallel execution.
- Efficiency-security dilemma: large shards are required to guarantee security.

Our Solution

\[ f_s + f_L < 1 \]
\[ f_s > f_L \]

Certify Module

Execute Module

\[ f_S + 2f_L < 1 \]
\[ f_S = f_L \]

Global order

Byzantine Fault Tolerance Consensus

Processing Shards

Idea: deconstructing SMR to create more lightweight shards.
- Ordering-processing sharding scheme: one ordering shard performs the ordering task and multiple processing shards perform the dissemination and execution tasks.
- Safety-liveness separation: trade liveness threshold \( f_L \) for larger safety threshold \( f_S \), create much smaller shards.

Evaluations

\[ m \text{-shard size}; k \text{-shard number}; \]

The total number of nodes \( n \) [SOTA, Ours]

\[
\begin{array}{cccccccc}
\text{m} & 20 & 38 & 49 & 57 & 57 & 60 & 63 & 63, 24 \\
\text{k} & 20, 13 & 57, 22 & 60, 24 & 63, 24 & 63, 24 & 63, 24 & 63, 24 \\
\end{array}
\]

More details