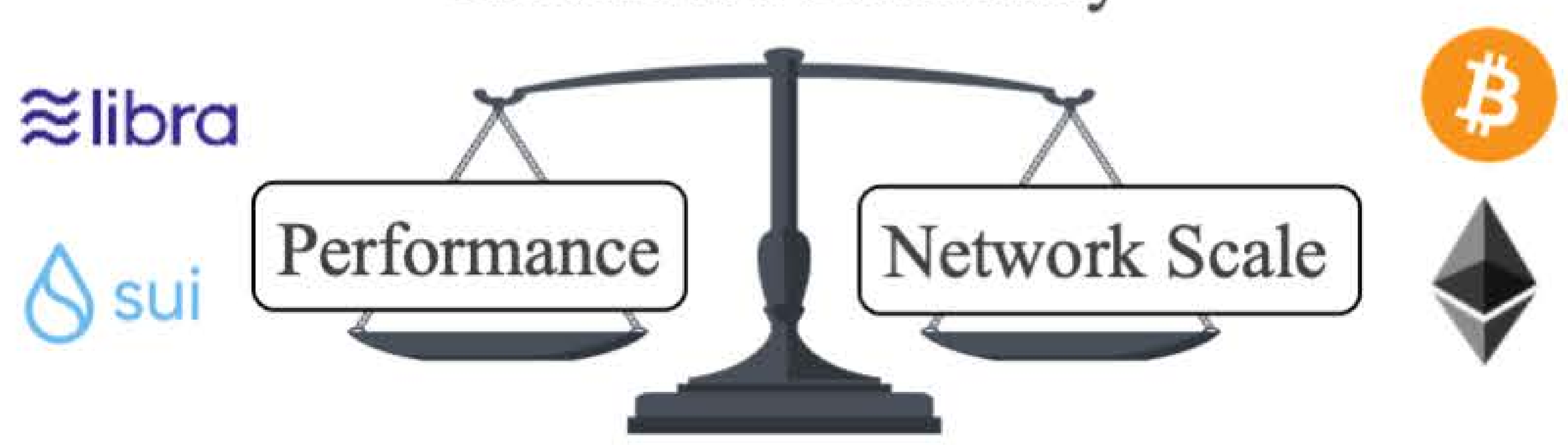
CERIAS
The Center for Education and Research in Information Assurance and Security

Sharding SMR with Optimal-size Shards for Highly Scalable Blockchains

Jianting Zhang[1], Zhongtang Luo[1], Raghavendra Ramesh[2], Aniket Kate[1,2]
[1]Purdue University, [2]Supra Research

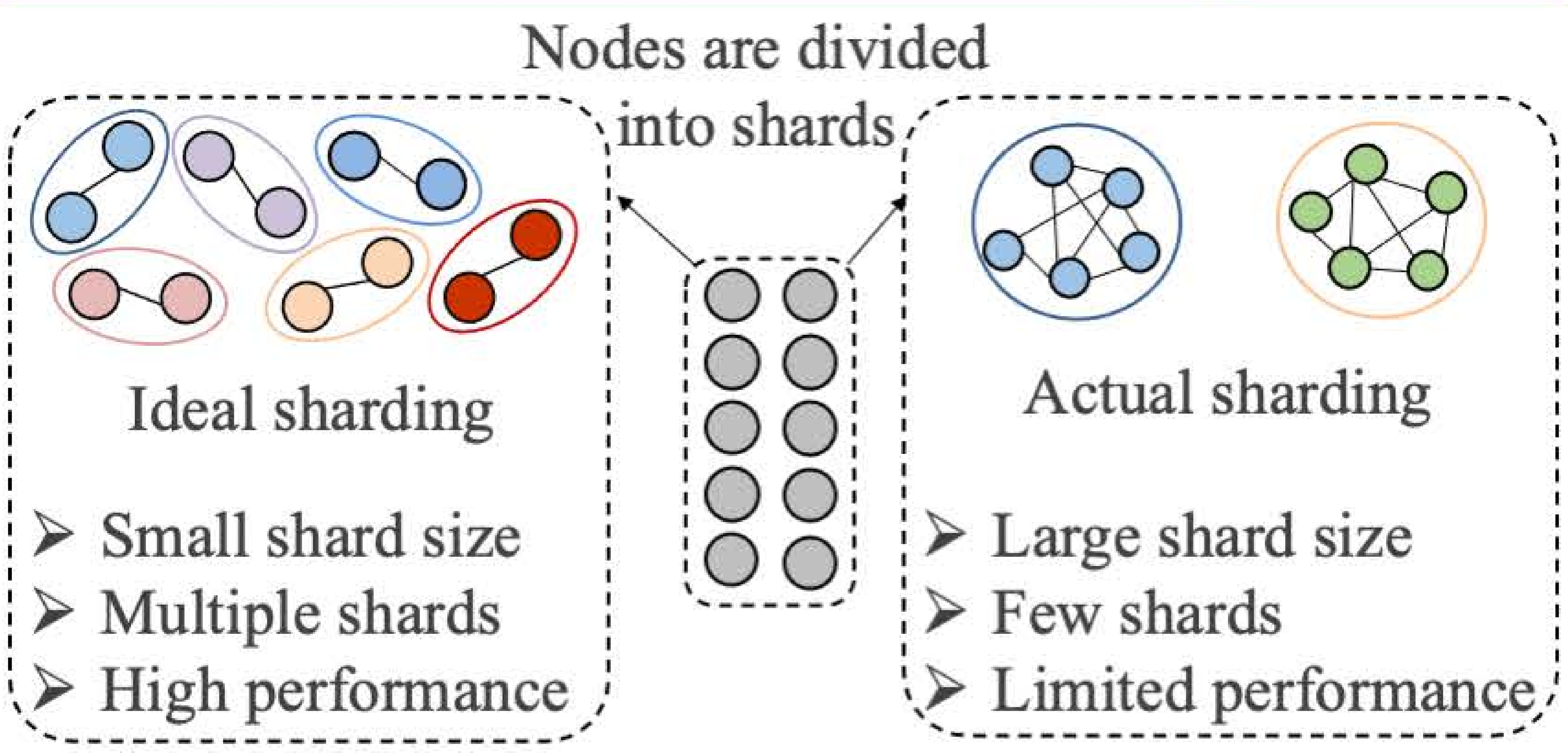
Introduction

Blockchain Scalability



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

Blockchain Sharding



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

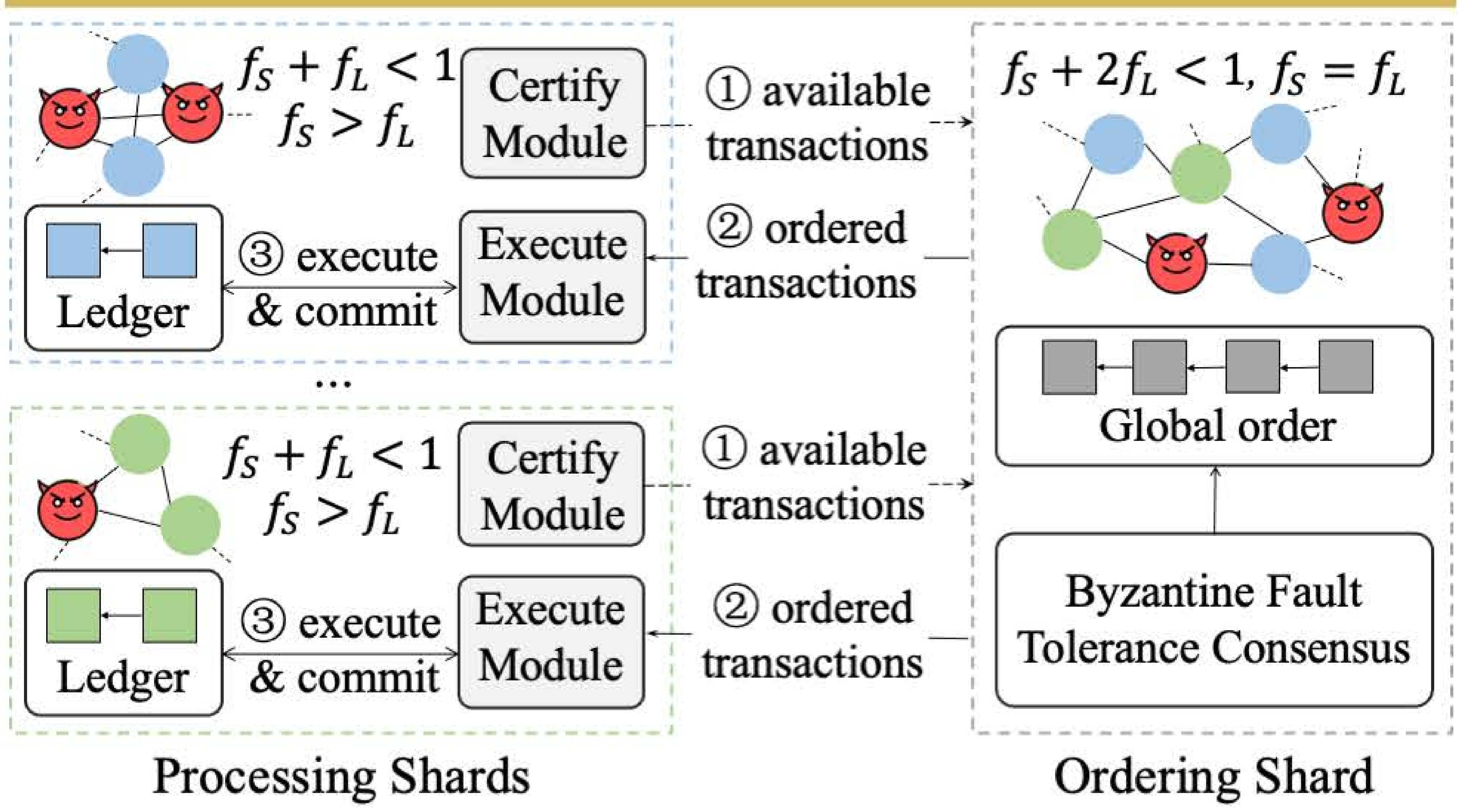
Key Observations

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 ①③: 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.

Our Solution



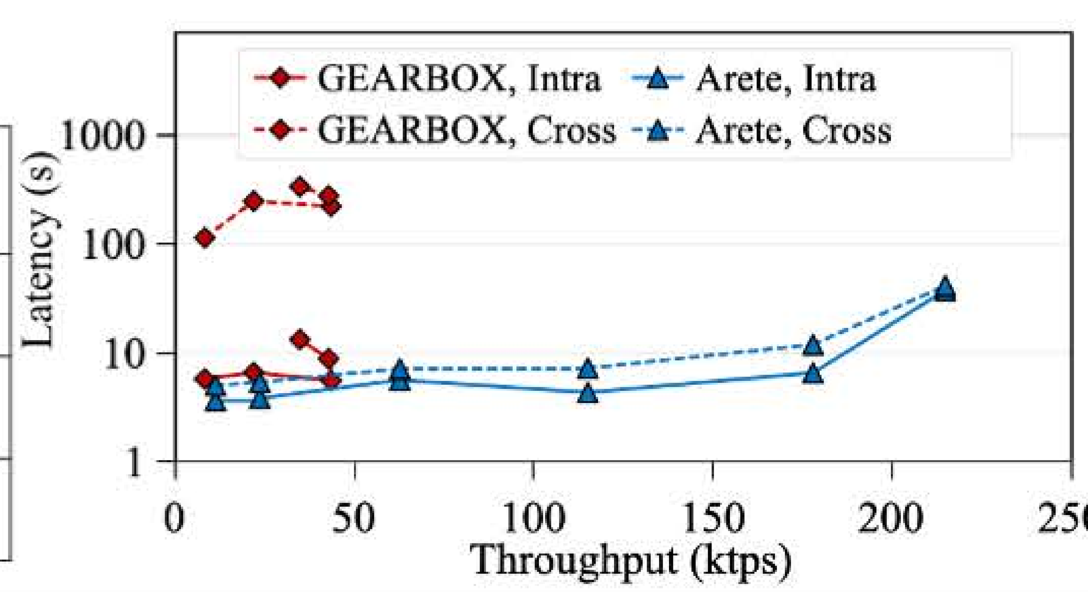
Idea: deconstructing SMR to create more lightweight shards.

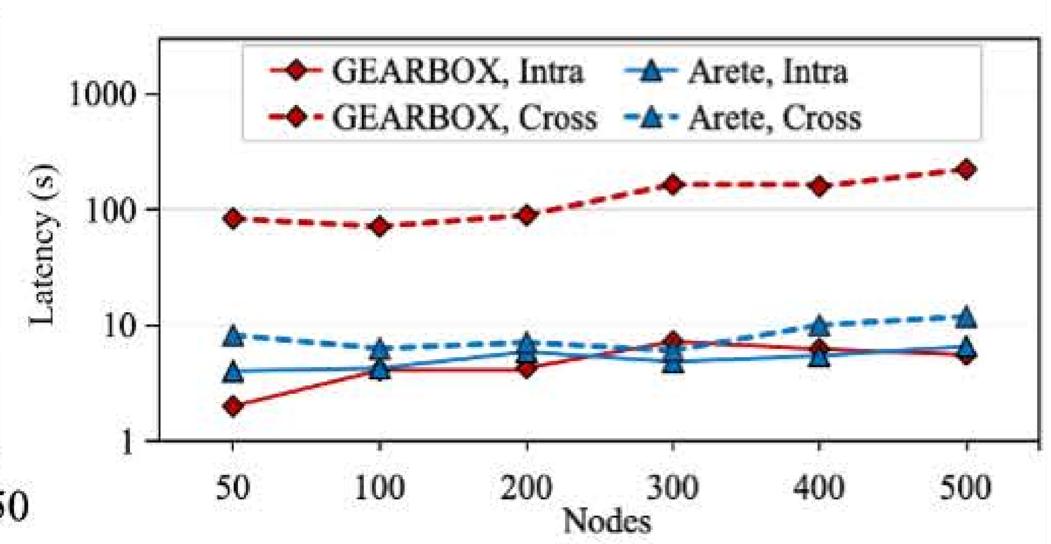
- Ordering-processing sharding scheme: one ordering shard performs the ordering task and multiple processing shards perform the dissemination and execution tasks.
- Safety-liveness separation: trade liveness threshold f_L for larger safety threshold f_S, create much smaller shards.

Evaluations

m-shard size; k-shard number;

	The total number of nodes n [SOTA, Ours]					
	50	100	200	300	400	500
m	20, 13	38, 18	49, 20	57, 22	60, 24	63, 24
k	2, 3	2, 5	4, 10	5, 13	6, 16	7, 20





More details

PURDUE UNIVERSITY

CERIAS