中山大學
SUN YAT-SEN UNIVERSITY

MVCom: Scheduling Most Valuable Committees for the Large-Scale Sharded Blockchain

Huawei Huang, Zhenyi Huang, Xiaowen Peng, Zibin Zheng, Song Guo*
School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou, China
*Department of Computing, The Hong Kong Polytechnic University, Hong Kong.

Presentation for ICDCS 2021

Introduction

Elastico [1] : a sharding-based blockchain system

Partition the blockchain network nodes into smaller committees

Committees collaboratively process disjoint sets of transaction

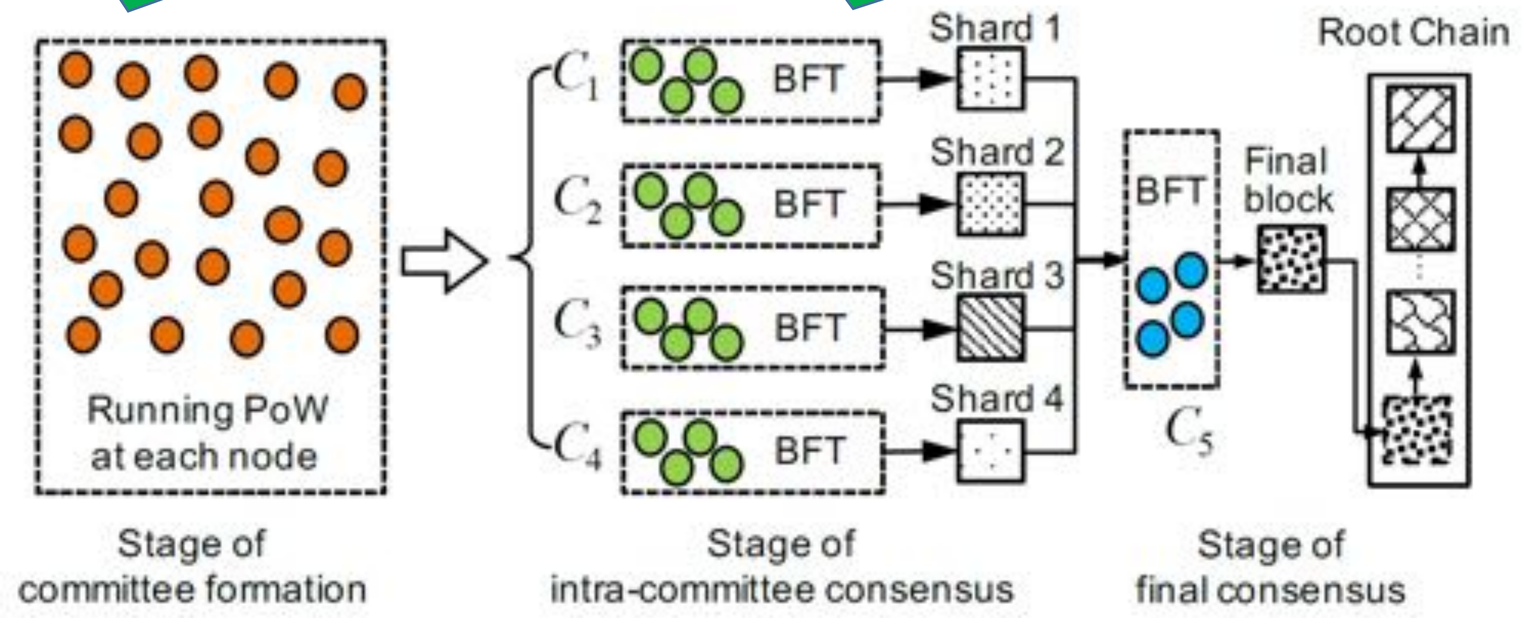


Fig. 1. Each epoch of sharding protocol (e.g., Elastico [1]) includes three major stages: committee formation, intra-committee consensus, and the final consensus.

[1] Luu, L. , et al. “A Secure Sharding Protocol For Open Blockchains.” the 2016 ACM SIGSAC Conference *on* CCS, 2016.

Motivation

Why would we study the committee's scheduling?

- The *two-phase* latency in Elastico is unbalanced
- The committee-formation latency is much longer than the consensus latency
- Some straggler committees will slow down the block formation

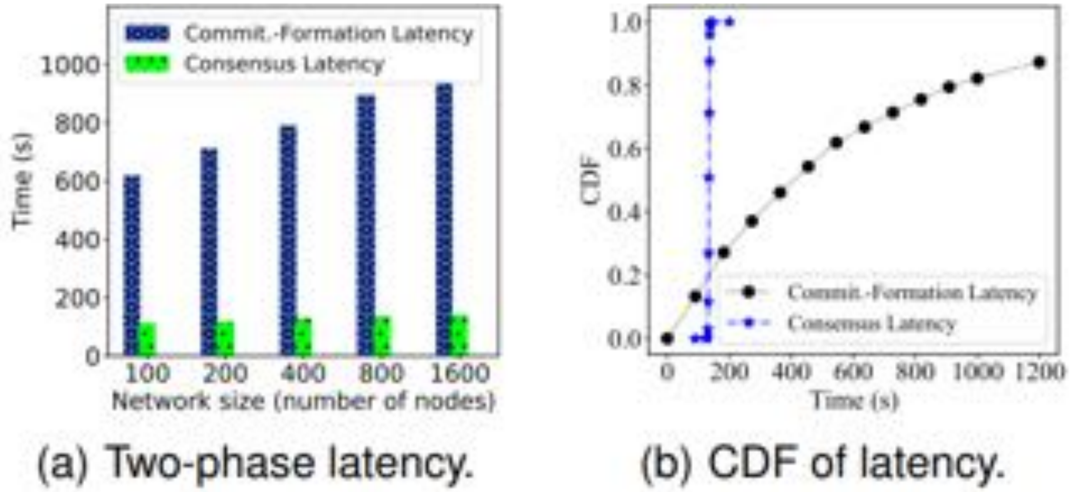
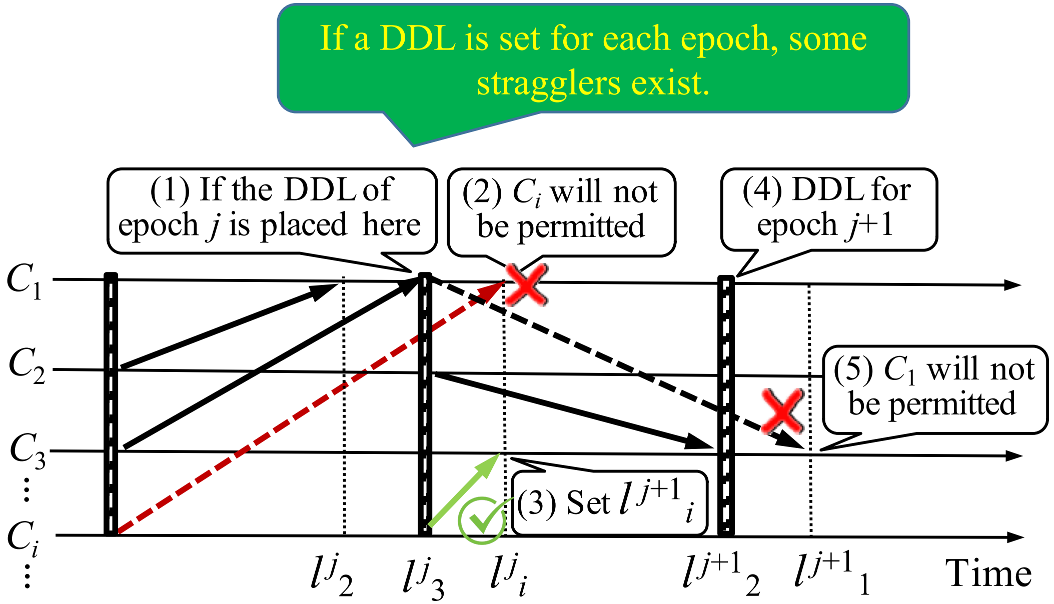


Fig. 2. *Two-phase* latency in the Elastico protocol, including *committee-formation* latency and *intra-committee consensus* latency.



Suppose C_1 and C_3 are *final committees* of epoch *j* and *j*+1, respectively.

Fig. 3. Handling the *two-phase latency* across 2 successive epochs.

Problem Formulation

- Offline-version formulation

$$\textbf{MVCom}: \max\ U = \sum_{j\in J}\sum_{i\in I^j}(\alpha\cdot x_i^j s_i^j - \Pi_i^j) \qquad (2)$$

$$\text{s.t.} \quad \sum_{i\in I^j} x_i^j \geq N_{\min},\ \forall j\in J. \qquad (3)$$

$$\sum_{i\in I^j} x_i^j s_i^j \leq \hat{C},\ \forall j\in J. \qquad (4)$$

$$\text{Variables: } x_i^j \in \{0,1\}, \forall i\in I^j, \forall j\in J. \qquad (5)$$

The objective function: to maximize a joint utility

- max: # of TXs included in permitted committees
- min: cumulative age of those TXs

Constraints:

- Requirement of the minimum # of committees
- Capacity of the final block: no more than the maximum # of TXs included in the final block

Decisions:

- x^j_i = 0/1: committee *i* is selected or not.

Algorithm Design

The Stochastic Exploration (SE) algorithm:

- Online distributed algorithm
- Adopting Stochastic Exploration (SE) technique
- Two major phases when designing the Algorithm:
  - log-sum-exp approximation
  - implementation of Markov Chain.

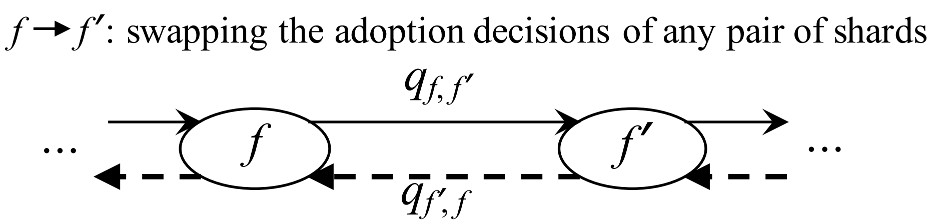


Fig. 4. Transition between two adjacent states (i.e., solutions).

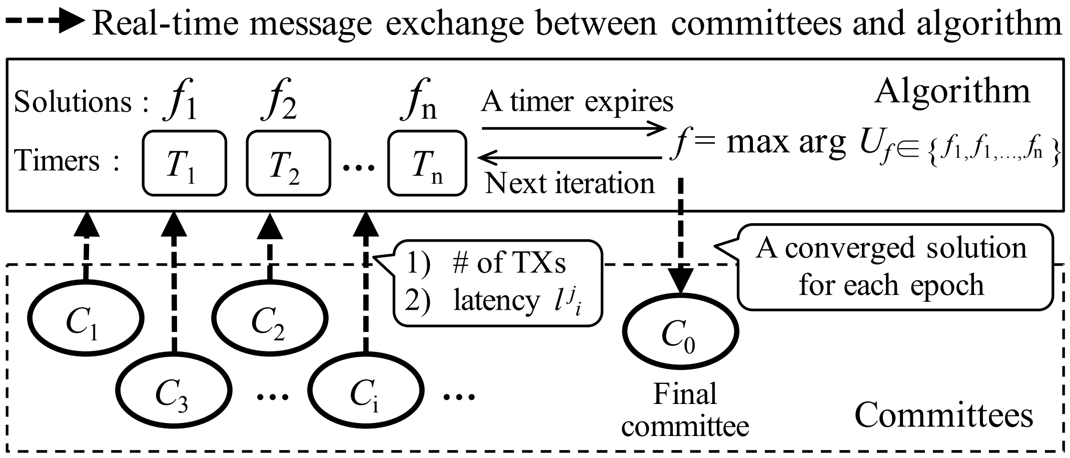


Fig. 5. Interactions between the committee and the distributed algorithm.

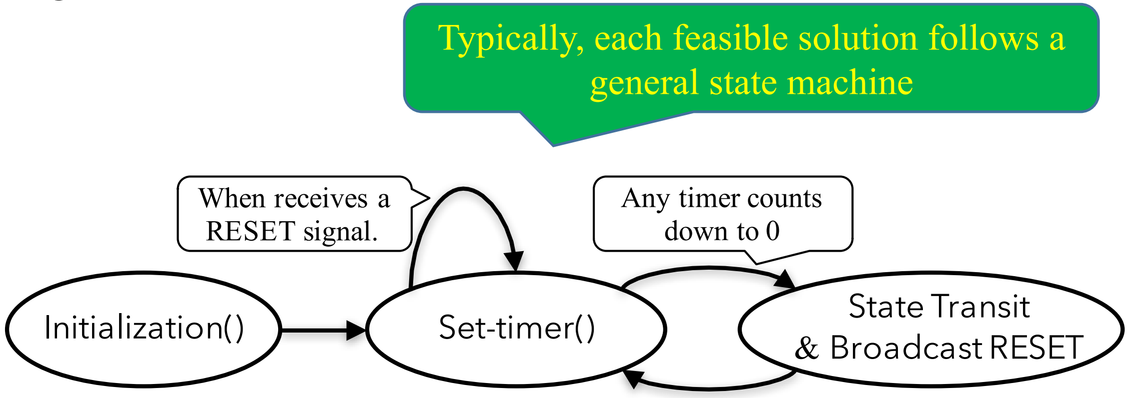


Fig. 6. State machine for each parallel feasible solution.

Algorithm Design (cont.)

Theorem 1: The convergence time boundary of SE algorithm

Theorem 1: *Given a set of member committees, and let* $U_{\max} = \max_{\forall f \in \mathcal{F}} U_f$, $U_{\min} = \min_{\forall f \in \mathcal{F}} U_f$, *the mixing time* $t_{mix}(\epsilon)$ *for each epoch of the constructed Markov chain in Algorithm 1 is bounded by:*

$$t_{mix}(\epsilon) \geq \frac{\exp[\tau - \frac{1}{2}\beta(U_{\max} - U_{\min})]}{|I^j|^2 - |I^j|} \ln \frac{1}{2\epsilon}, \qquad (12)$$

and

$$t_{mix}(\epsilon) \leq 4^{|I^j|}(|I^j|^2 - |I^j|) \exp[\frac{3}{2}\beta(U_{\max} - U_{\min}) + \tau] \cdot [\ln \frac{1}{2\epsilon} + \frac{1}{2}|I^j| \ln 2 + \frac{1}{2}\beta(U_{\max} - U_{\min})]. \qquad (13)$$

Analysis of Committee’s Failure

- **Committee may fail**
- **We then have the following two questions**
  - Q1: Can we still use the proposed stochastic-exploration algorithm when a member committee fails? – Through experiments
  - Q2: What is the performance perturbation brought by the failed committee? – Through Theorem 2

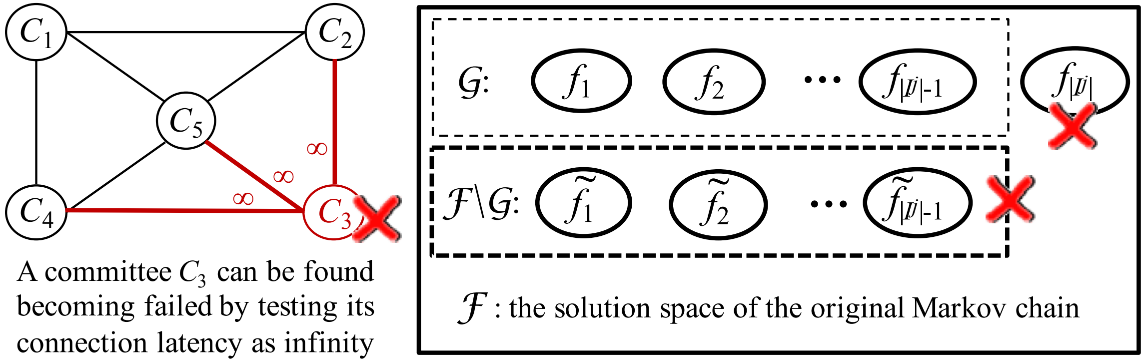


Fig. 7. Suppose that C_3 fails due to an attack or a network failure, its connection latency can be tested as infinity. Thus, the original solution space should be trimmed by eliminating all states that relates to C_3. That is, in space $F\backslash G$, every single trimmed state f_n ($n = 1, 2, ..., |I| - 1$) associates with the failed committee C_3.

Committee's Failure (cont.)

- **To answer the following question, we give Theorem 2**
  - Q2: What is the performance perturbation brought by the failed committee?

Theorem 2: *Suppose that a single committee fails during the running of Algorithm 1, the performance perturbation is bounded by*

$$\|\boldsymbol{q}^{*}\boldsymbol{u}^{T} - \tilde{\boldsymbol{q}}\boldsymbol{u}^{T}\| \leq \max_{g\in\mathcal{G}} U_g, \tag{19}$$

where $\max_{g\in\mathcal{G}} U_g$ (denoted by $\tilde{U}_{\max}$) represents the utility under the best solution in the new state space $\mathcal{G}$.

Performance Evaluation

Experiment Setup:

- Replay the real-world Bitcoin TXs [2].
- 1378 transaction blocks
- For each epoch, blocks are divided into different groups to simulate the transaction shards.
- In each shard, the total number of TXs is accumulated together from all blocks included.

Baseline algorithm:

- SA：Simulated Anneal algorithm
- DP：Dynamic Programming
- WOA：Whale Optimization Algorithm

[2] J. Wu, J. Liu, W. Chen, H. Huang, Z. Zheng, and Y. Zhang, “Detecting mixing services via mining bitcoin transaction network with hybrid motifs,” IEEE Trans. on Systems, Man, and Cybernetics: Systems, pp. 1–13, 2021

Results

- Effect of the # of Parallel Threads (denoted by **Γ**)

Γ is defined as the # of distributed parallel execution threads in SE algorithm.

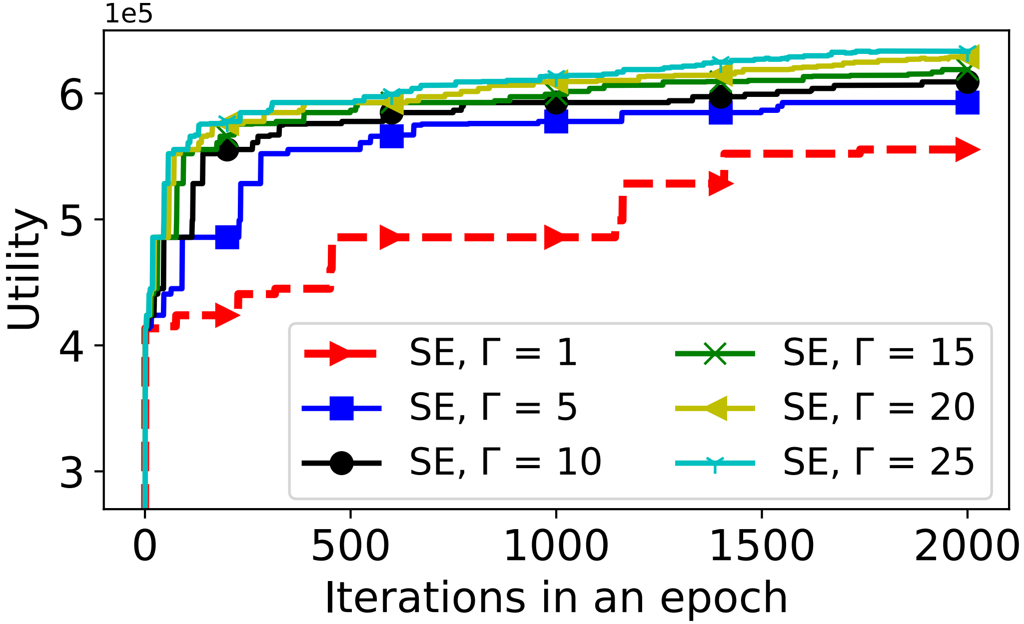
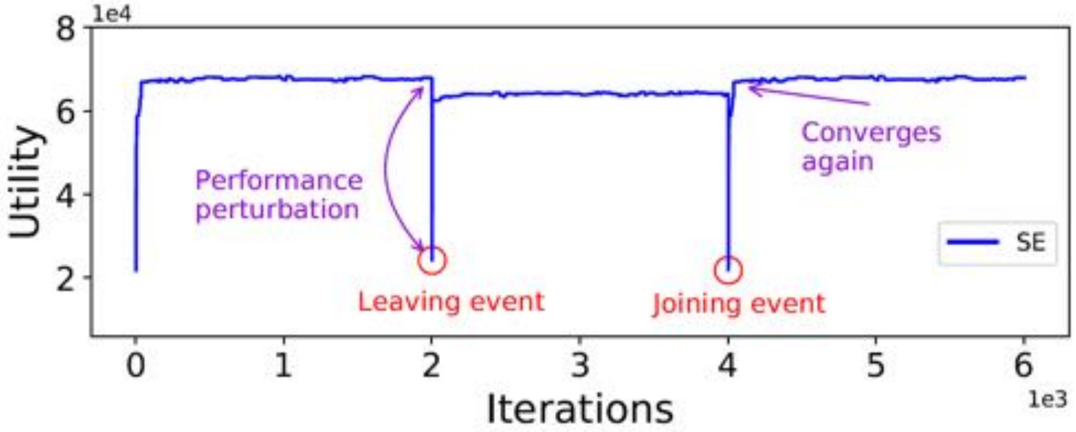


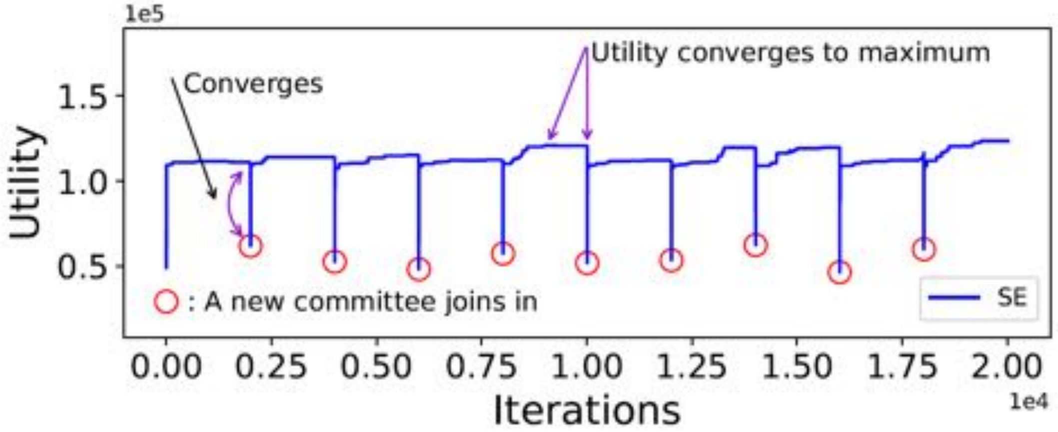
Fig. 8. Convergence of Stochastic-Exploration (SE) algorithm under different Γ (Γ is defined as the number of distributed parallel execution threads).

Results (cont.)

- Dynamic Event Handling



(a) Committee's leaving & joining, $|I^j|$=50, $\hat{C}$=40K.



(b) Committee's consecutive joining, $|I^j|$=100, $\hat{C}$=80K.

Fig. 9. Results of dynamic-event handing, with parameters α (the weight of the number of TXs) = 1.5, and $\Gamma = 1$.

Results (cont.)

➢ Valuable Degree of Algorithms

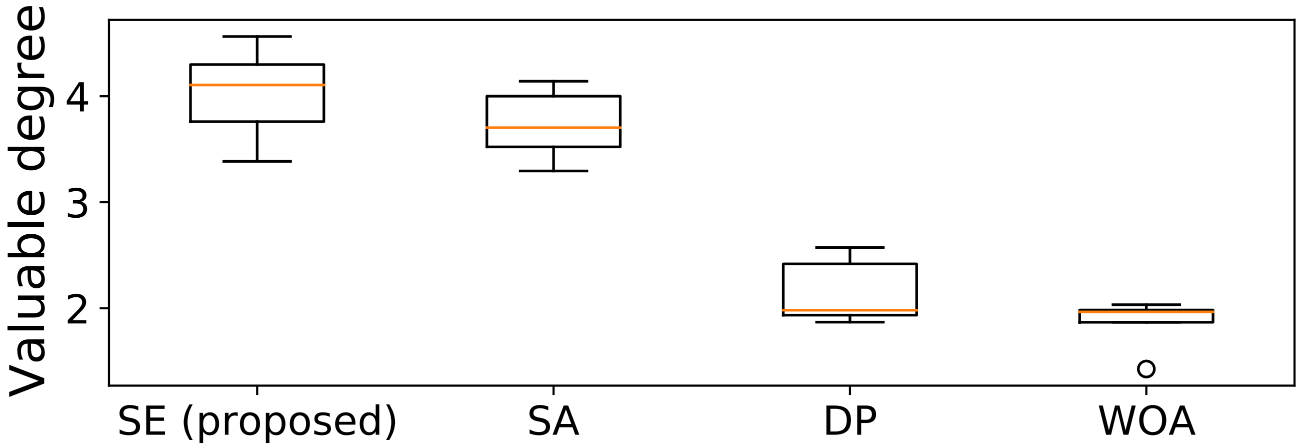
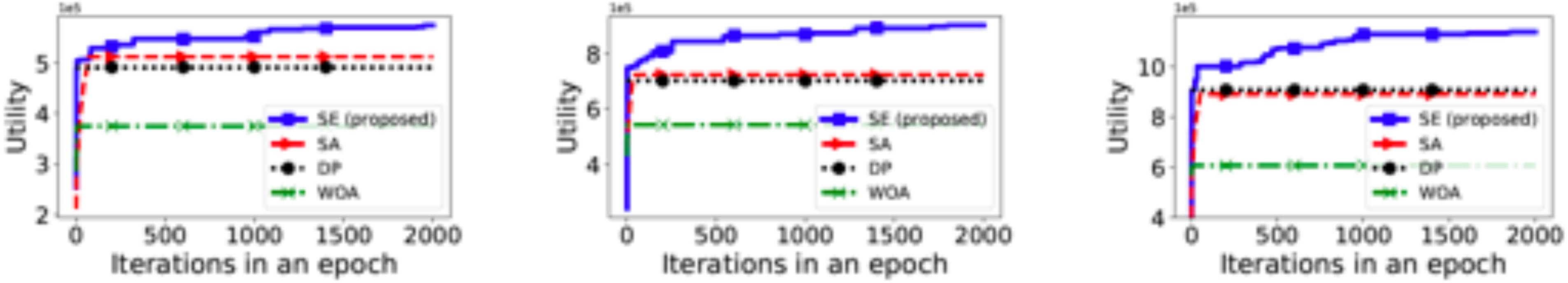


Fig. 10. Algorithm's Valuable Degree, which is defined as the numerical ratio dividing the total number of processed TXs by the cumulative age of the TXs packaged in the permitted shards.

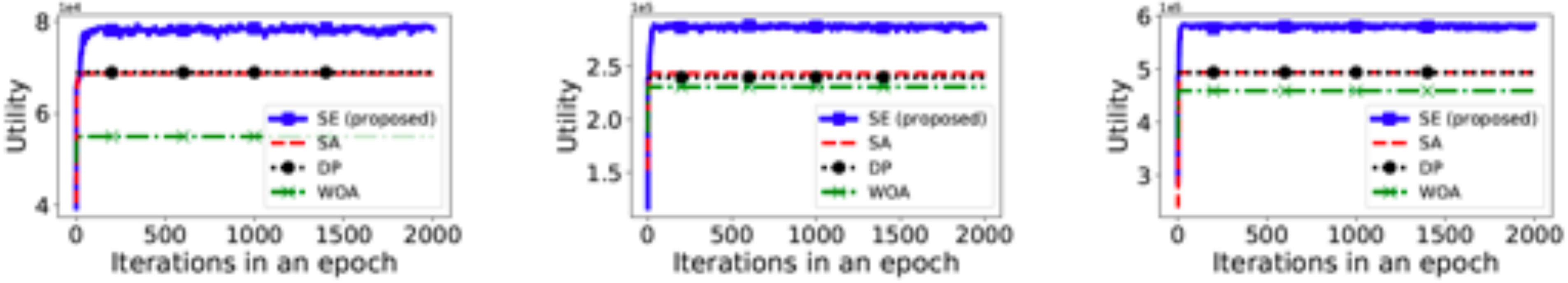
Results (cont.)

➢ Convergence performance under varying parameters



(a) $|I^j|$=500, $\hat{C}$=0.5 million, α=1.5 (b) $|I^j|$=800, $\hat{C}$=0.8 million, α=1.5 (c) $|I^j|$=1000, $\hat{C}$=1 million, α=1.5

Fig. 11. Convergence of algorithms with a fixed set of committees, while varying $|I^j| = \{500, 800, 1000\}$, and fixing α=1.5, Γ= 10, $\hat{C}$ = 1000 $\times|I^j|$

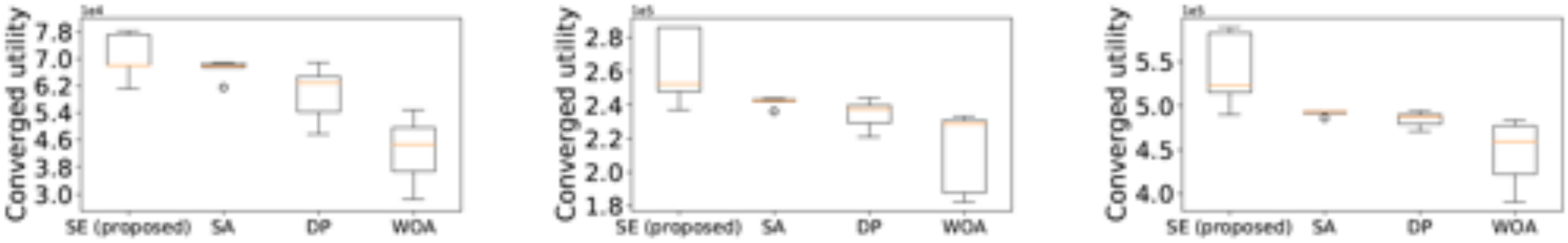


(a) $|I^j|$=50, $\hat{C}$=50K, α=1.5 (b) $|I^j|$=50, $\hat{C}$=50K, α=5 (c) $|I^j|$=50, $\hat{C}$=50K, α=10

Fig. 12. Convergence of algorithms with a fixed set of committees, while varying $\alpha = \{1.5, 5, 10\}$, and fixing $|I^j|$=50, Γ= 25, $\hat{C}$=50,000 (50K).

Results (cont.)

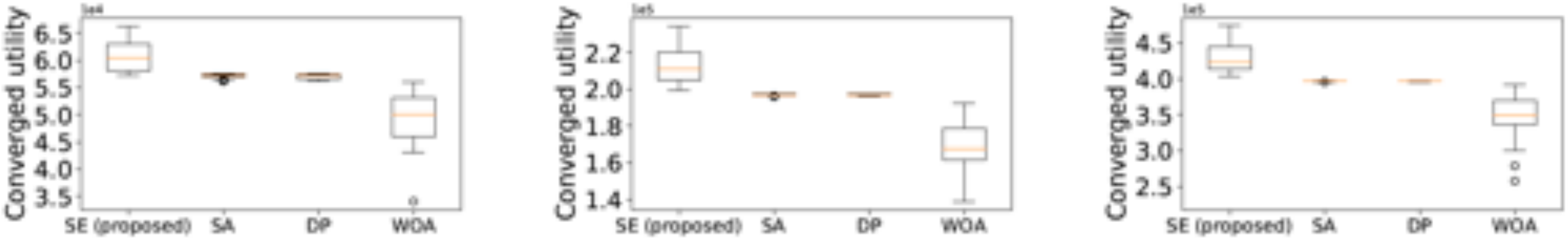
- ➢ Effect of Varying α under Two Cases.
- ➢ α is the weight of the # of TXs.



(a) $|I^j|$=50, $\hat{C}$=50K, α=1.5 (b) $|I^j|$=50, $\hat{C}$=50K, α=5 (c) $|I^j|$=50, $\hat{C}$=50K, α=10

Fig. 13. Distribution of the converged utilities with a fixed set of committees, while varying $\alpha = \{1.5, 5, 10\}$, and fixing $|I^j|$=50, Γ= 25, $\hat{C}$=50,000 (50K).

Case 1: given a fixed set of arrived committees



(a) $|I^j|$=50, $\hat{C}$=40K, α=1.5 (b) $|I^j|$=50, $\hat{C}$=40K, α=5 (c) $|I^j|$=50, $\hat{C}$=40K, α=10

Fig. 14. Online execution with committee's consecutive joining events, while varying $\alpha = \{1.5, 5, 10\}$, and fixing $|I^j|$=50, Γ= 25, $\hat{C}$=40,000 (40K).

Case 2: with 23 committee's consecutive joining events

Contribution and Conclusion

- We focus on the committee’s scheduling for the large-scale sharded blockchain.
- We propose an online distributed SE algorithm that can schedule the most valuable committees for the sharded blockchain.
- The algorithm can also handle the dynamic joining and leaving events of member committees.
- The theoretical convergence time and the performance perturbation brought by committee’s failure are also analyzed rigorously.
- The trace-driven simulations results show that the proposed SE algorithm can select the most valuable committees to participate in the final committee.

Thanks

HuangLab@SYSU http://xintelligence.pro/

Email: huanghw28@mail.sysu.edu.cn