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.

Motivation

Why would we study the committee’s scheduling?

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

Fig. 2. \textit{Two-phase} latency in the Elastico protocol, including \textit{committee-formation} latency and \textit{intra-committee consensus} latency.

Fig. 3. Handling the \textit{two-phase latency} across 2 successive epochs.
Problem Formulation

➢ Offline-version formulation

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:

- \( x_{ij}^j = 0/1 \): committee \( i \) is selected or not.
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.

\[ f \xrightarrow{q_{f,f'}} f' \]

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

\[ f \xrightarrow{q_{f',f}} f'' \]

 typically each feasible solution follows a general state machine.

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

---

Real-time message exchange between committees and algorithm

\[
\text{Algorithm: } f = \max \arg \ U_f \{ f_1, f_2, \ldots, f_n \}
\]

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

---

Typically, each feasible solution follows a general state machine.

---

Algorithm Design
Theorem 1: The convergence time boundary of SE algorithm

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

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

and

$$t_{\text{mix}}(\epsilon) \leq 4|I^j|(|I^j|^2 - |I^j|) \exp[\frac{3}{2} \beta (U_{\text{max}} - U_{\text{min}}) + \tau] \cdot \left[\ln \frac{1}{2\epsilon} + \frac{1}{2} |I^j| \ln 2 + \frac{1}{2} \beta (U_{\text{max}} - U_{\text{min}})\right]. \quad (13)$$
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 $F \setminus G$, 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

\[
\|q^*u^T - \tilde{q}u^T\| \leq \max_{g \in \mathcal{G}} U_g,
\]

where \(\max_{g \in \mathcal{G}} U_g\) (denoted by \(\tilde{U}_{\text{max}}\)) 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

Results

- Effect of the # of Parallel Threads (denoted by $\Gamma$)

$\Gamma$ is defined as the # of distributed parallel execution threads in SE algorithm.

![Graph showing convergence of Stochastic-Exploration (SE) algorithm under different $\Gamma$](image)

Fig. 8. Convergence of Stochastic-Exploration (SE) algorithm under different $\Gamma$ ($\Gamma$ 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 $\alpha$ (the weight of the number of TXs) = 1.5, and $\Gamma = 1$. 
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

Fig. 11. Convergence of algorithms with a fixed set of committees, while varying $|J| = \{500, 800, 1000\}$, and fixing $\alpha = 1.5, \gamma = 10, C = 1000 \times |J|$.

Fig. 12. Convergence of algorithms with a fixed set of committees, while varying $\alpha = \{1.5, 5, 10\}$, and fixing $|J| = 50, \gamma = 25, C = 50,000 (50K)$. 
Results (cont.)

- Effect of Varying $\alpha$ under Two Cases.
- $\alpha$ is the weight of the # of TXs.

Case 1: given a fixed set of arrived committees

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