FRing: A Geograph-based P2P Overlay Network for Fast and Robust Blockchain Systems

Haoran Qiu, Tao Ji
Supervised by Dr. Heming Cui

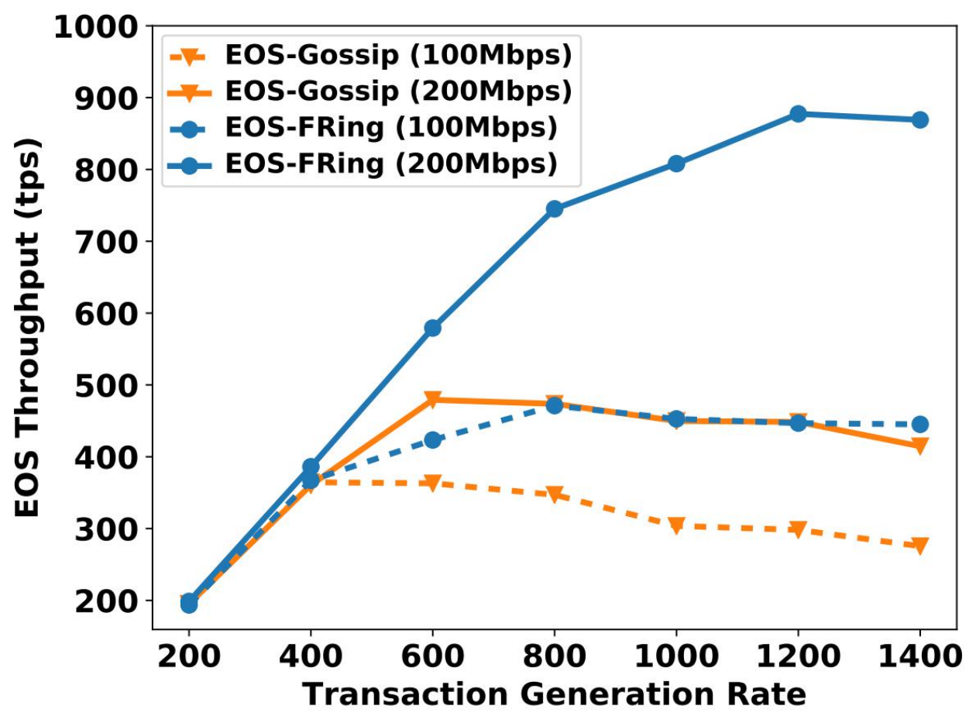
FYP #18006
Department of Computer Science
Faculty of Engineering

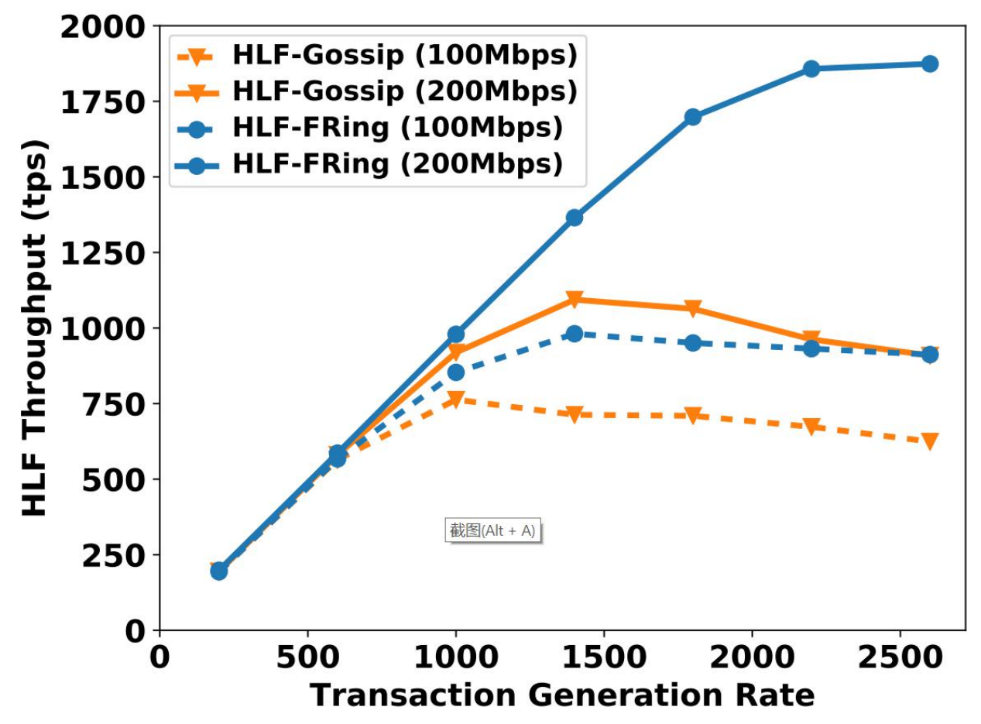
Background

Numerous blockchain systems with various consensus protocols emerges to achieve high transaction rates (2~ 10K tps). However, their underlying P2P network primitives constrain further improvements due to high message redundancy and long broadcast convergence time. The first problem is caused by the excessive robustness of dominant broadcast approach Gossip. All state-of-the-art blockchain systems only tolerate 20-50% node failure while Gossip can withstand up to 90%. The reason for the second problem is that existing broadcast topologies ignore geographical distances among nodes and incur paths with unnecessarily high latency.

Introduction to FRing

We present FRING, a geography-based P2P overlay network for fast and robust broadcast in blockchain systems. FRING has three main features: sufficient robustness, low message redundancy, and fast convergence. To reduce convergence time, FRING forms the network topology by considering geographical proximity. A novel broadcast algorithm based on FRING topology is proposed to lower message redundancy while maintaining sufficient robustness. One major challenge is to eliminate the risk of topology inference by traffic pattern analysis. FRING leverages Intel SGX to guarantee nodes' behavior integrity and incorporates pattern obfuscation to prevent the traffic pattern analysis. Evaluation shows that FRING improved the throughput of EOS and Hyperledger Fabric by up to 2.2X and 2.1X respectively.





Research Problems

Recent studies show that the underlying P2P network layer has become the bottleneck for transaction rate. Current blockchain systems form random P2P networks and predominantly use Gossip as the broadcast mechanism for robustness. For each hop in the broadcast process, a node pushes the message to a randomly chosen subset of its neighbors or pull from the message sender. There are two notorious problems associated with this network solution.

1. Gossip generates **excessive redundant messages** because Gossip is designed for extreme robustness (can tolerate up to 90% node failure). Such redundant messages lead to traffic congestion under high transaction rates.
2. Random network topology causes **unnecessarily long broadcast convergence time** (i.e. time used for a message to cover all nodes in the network).

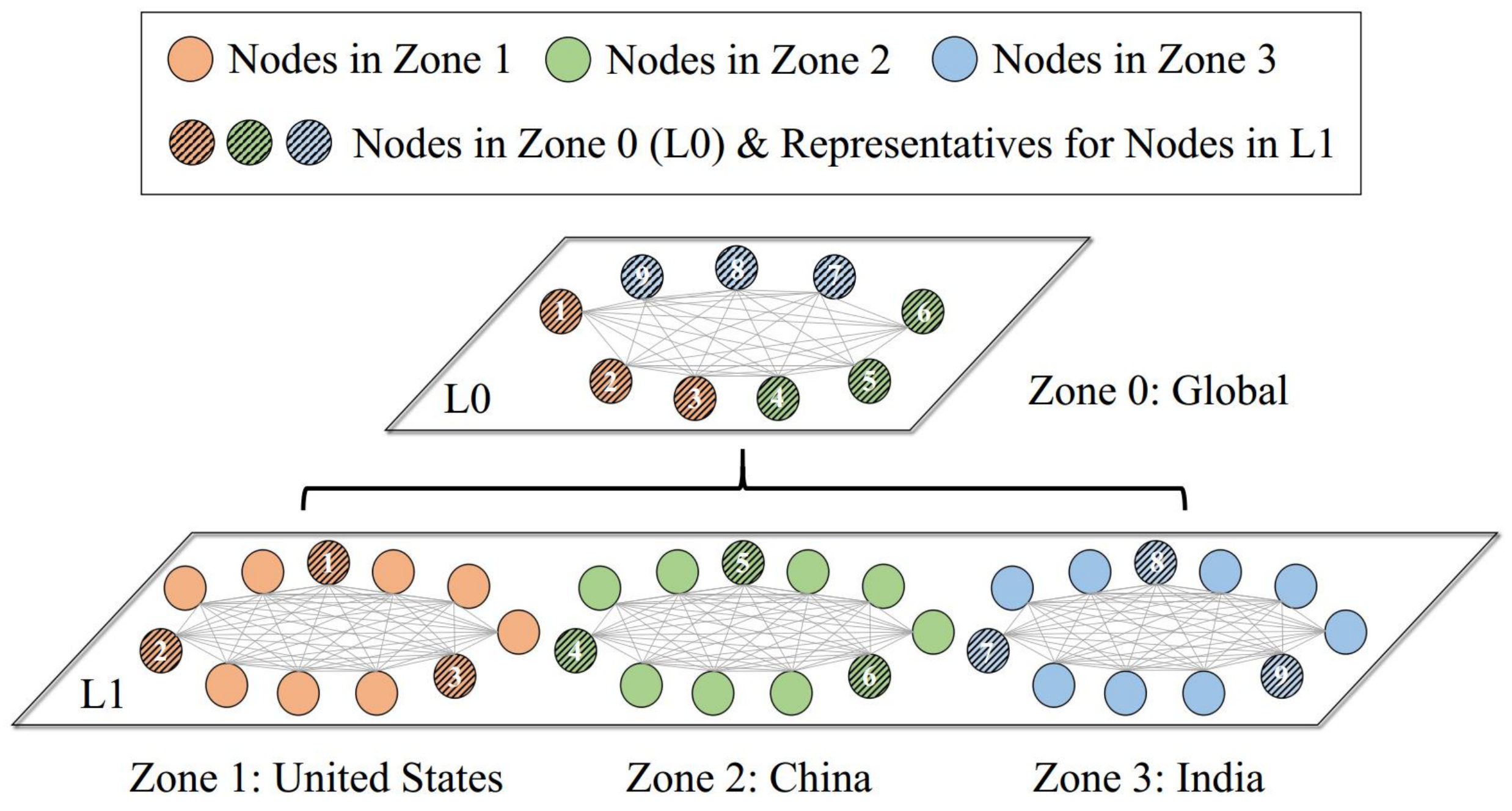
Features of FRing

FRing addresses the two problems with three features:

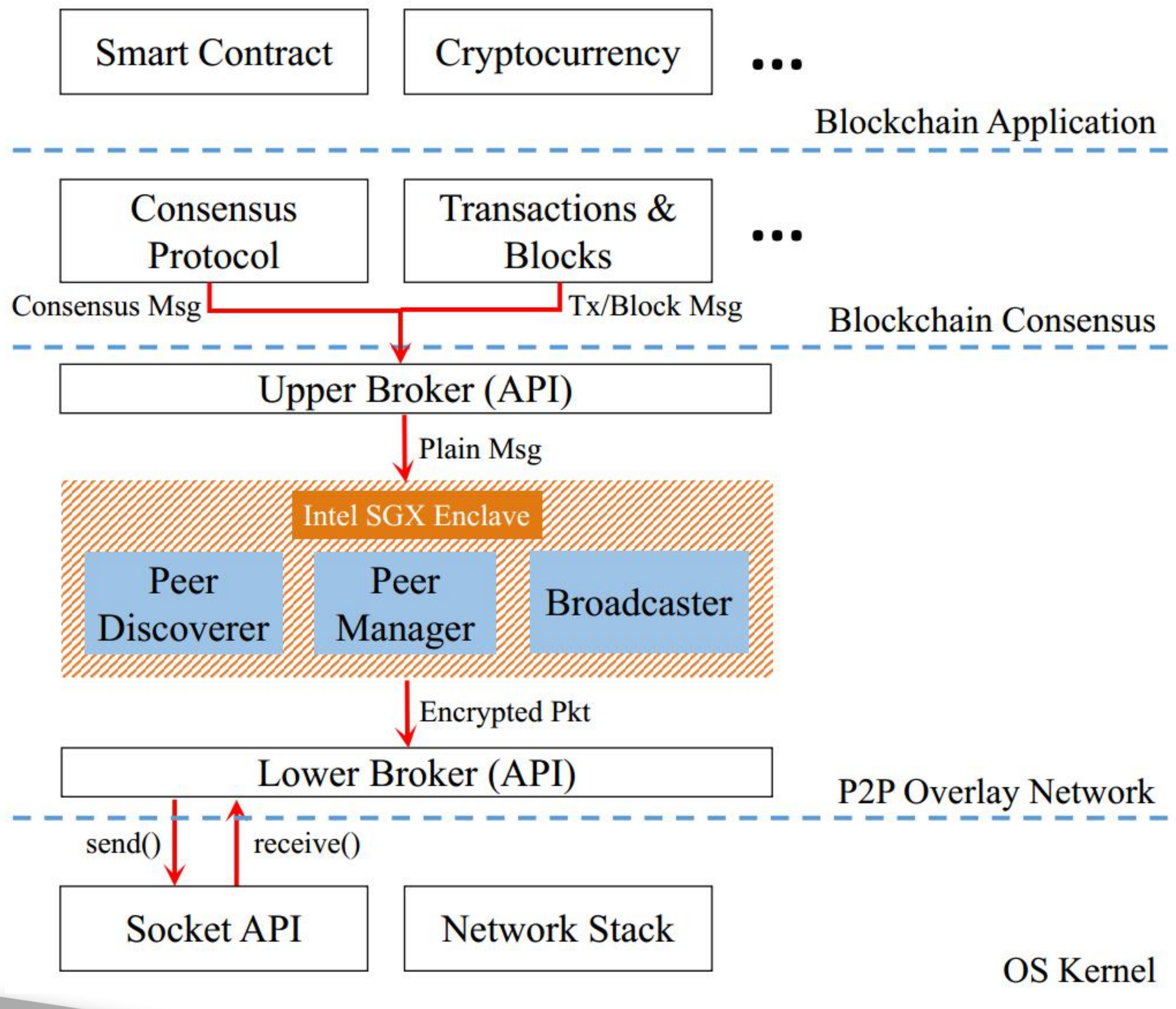
1. **Sufficient robustness**: a broadcast operation can tolerate at least the same portion of node failure as the blockchain consensus protocol;
2. **Low message redundancy**: the messages generated in each broadcast is efficient (O(N)); and
3. **Fast convergence**: the convergence time are short enough so that the accumulation of old messages is reduced effectively;

FRing Topology

Conceptually, the network topology of FRING is a selfmaintained fractal ring structure, where lower level rings (typically formed by inner-region nodes) reside on higher level rings (typically formed by cross-region nodes) in a recursive way. To form this topology, FRING groups all nodes based on their geographical proximity (per-hop latency) at the bottom level. Each group forms a fully-connected ring. FRING selects multiple nodes from each ring to serve as representatives and they form a new ring in the higher level recursively. Finally, there is only one global ring remaining at the top level and all nodes are connected through representatives.

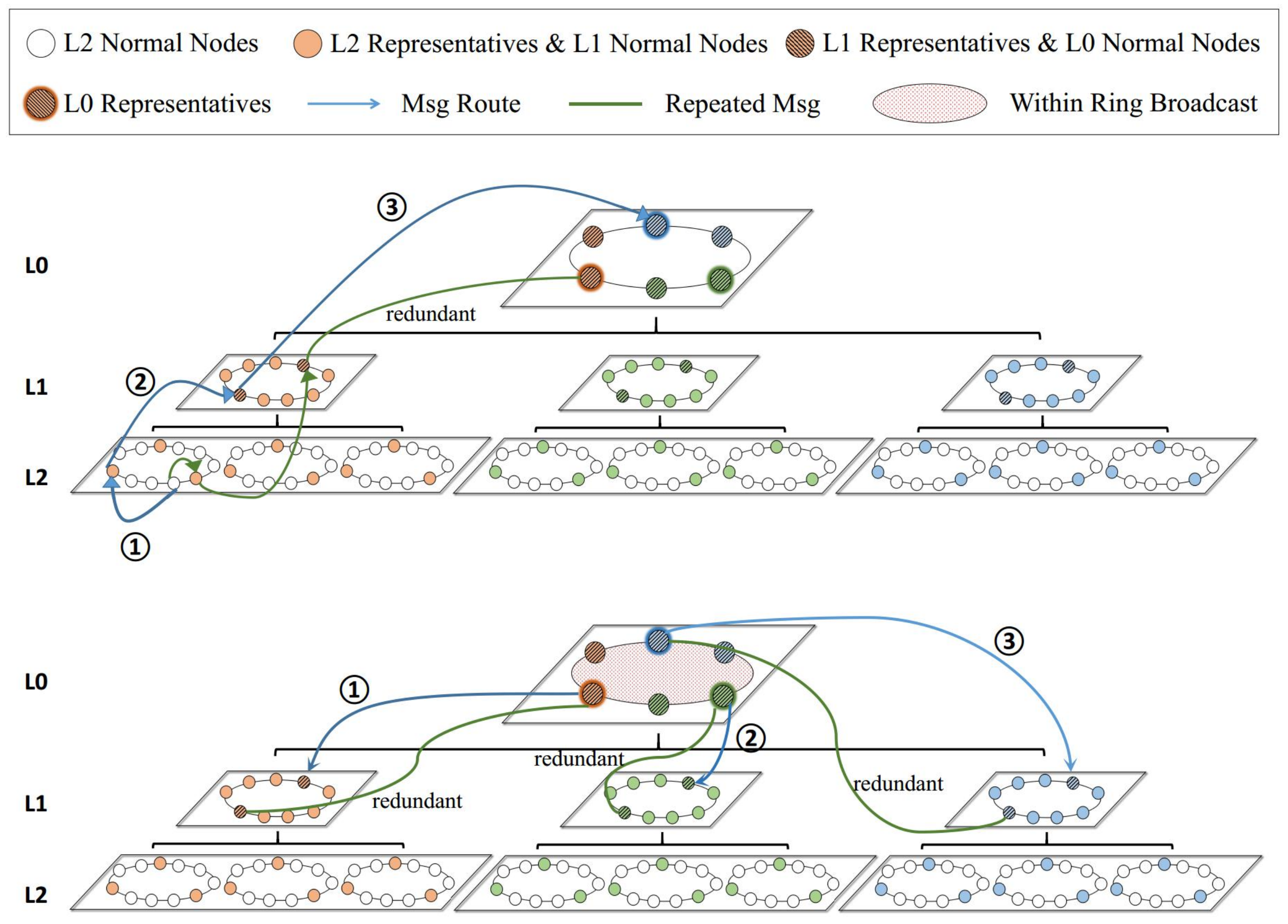


FRing Architecture



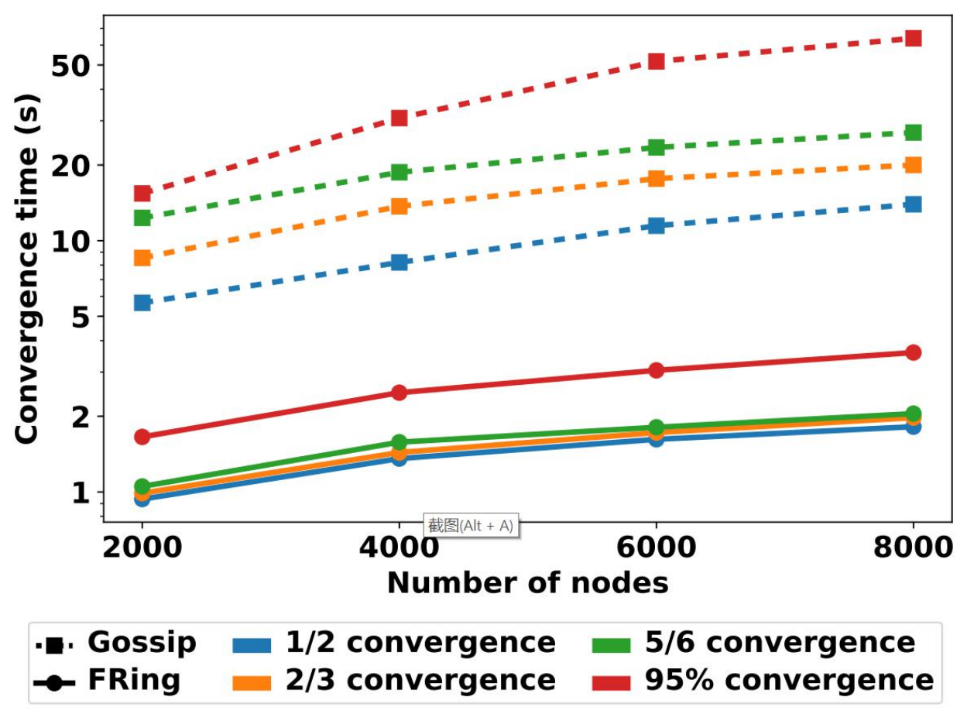
FRing Broadcast Mechanism

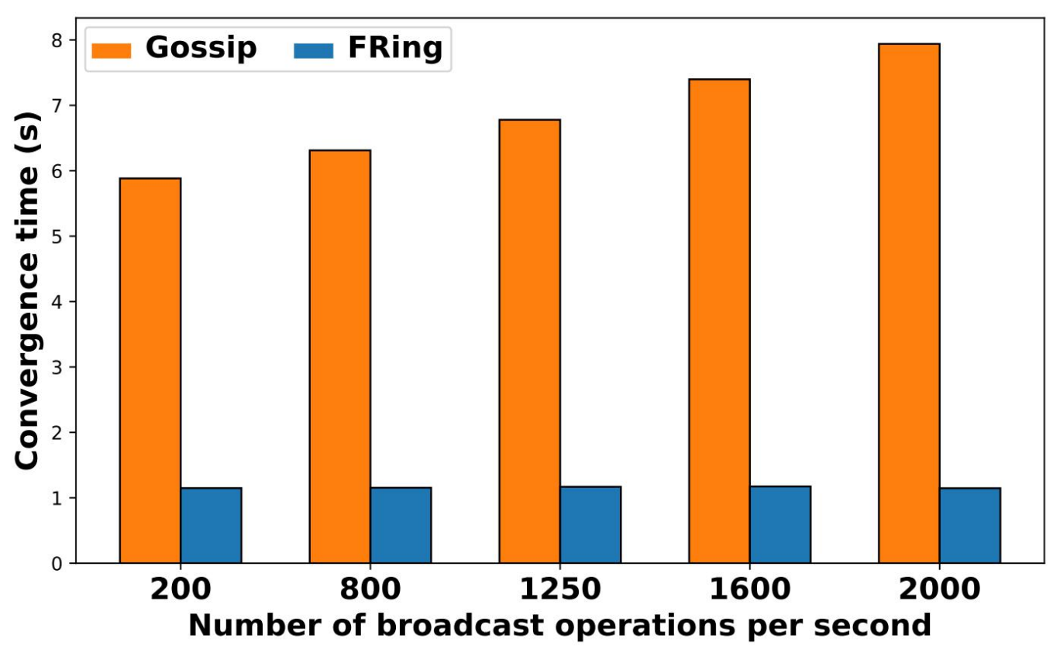
The broadcast mechanism of FRING is devided into three parts: broadcast up, broadcast down, and broadcast within-ring. Broadcast up and down are done with the help of representative nodes. Multiple message paths increase the robustness, which is also parametrized. Broadcast within-ring method is inspired by the distributed k-ary search method which provides O(N) message efficiency. It is done by constructing k-ary spanning trees.

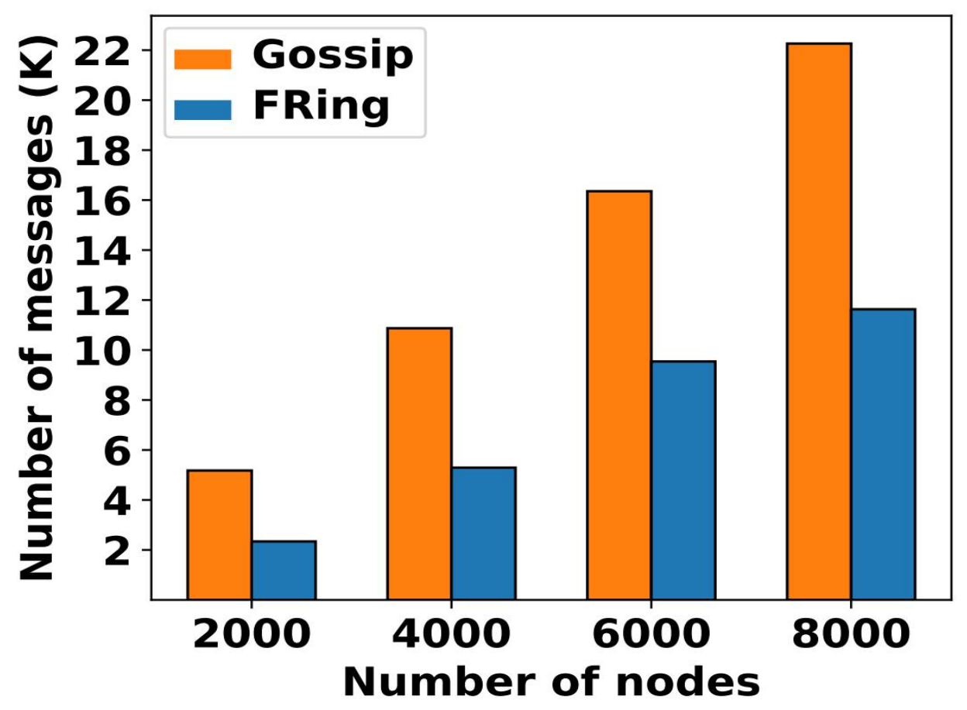


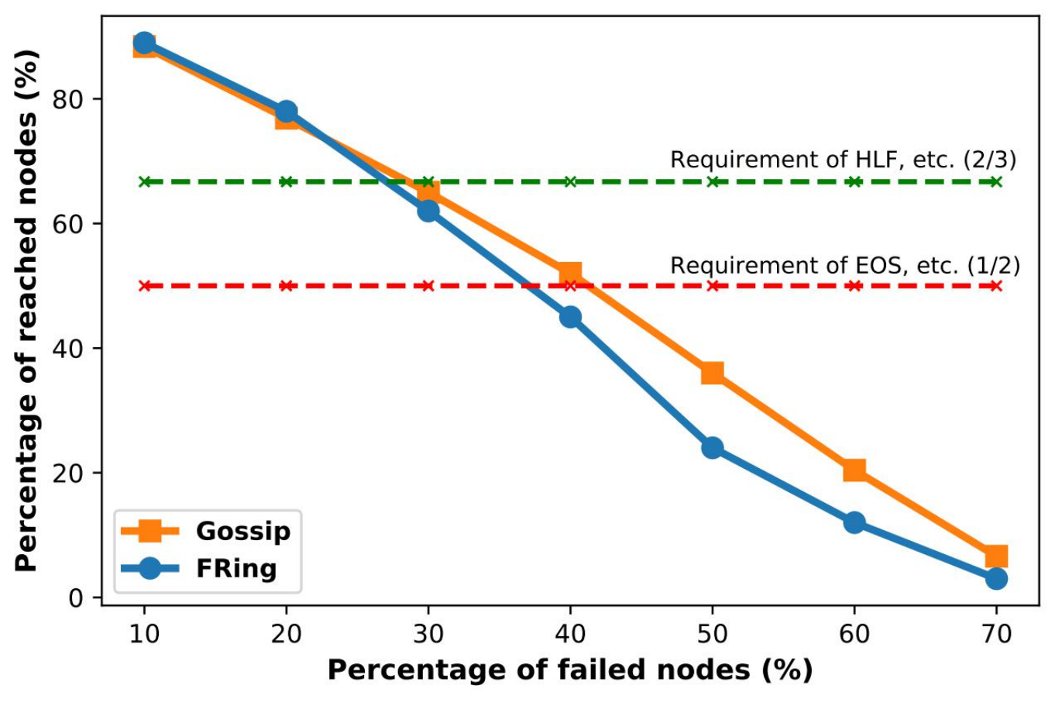
Evaluation Result

We evaluated FRing against Gossip on AWS cloud intensively and evaluation results show that FRing is **efficient** in terms of both convergence time and message complexity. It is also **sufficiently** robust for blockchain systems.









Acknowledgements

This project is supported by Huawei Technologies. Firstly, we would like to thank Dr. Cui for his insightful guidance and feedbacks on our project from time to time. We also want to thank Shixiong Zhao, Xusheng Chen, Ji Qi, and Tsz-on Li for their suggestions on improving the work. We are also grateful for our anonymous reviewers for thoughtful feedback, which helped improve the quality of the project, paper, and presentation.