INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD
R&D SHOWCASE 2021
Technology, Social Impact

Secure Regenerating Codes for Reducing Storage and Bootstrap Costs in Sharded Blockchain

Introduction

Bitcoin is a decentralized cryptocurrency without a financial institution and Blockchain is a distributed ledger.

Need for Scaling Bitcoin:

- Storage : 330GB and size is increasing (Not good)
- Confirmation Latency: About 1 hour (Not good)
- Security: 50% adversary (Good)

Methods to scale

- **Sharding Approaches**

  Advantages:

  + High Throughput

  + Low latency

  Challenges

  – Higher storage per node

  – Communication cost to new miners is high.

- **Coding-theory approaches**

  Advantages:

  + Lower storage per node

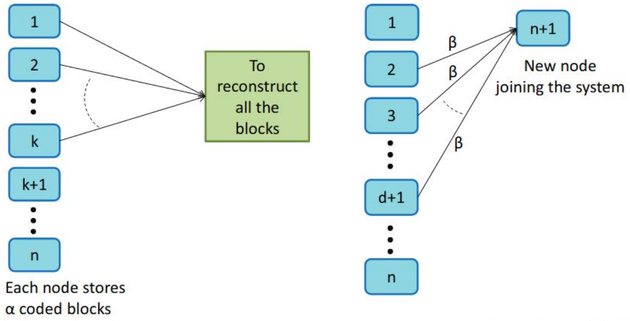
  + Less number of honest nodes to contact for recovery

  Challenges:

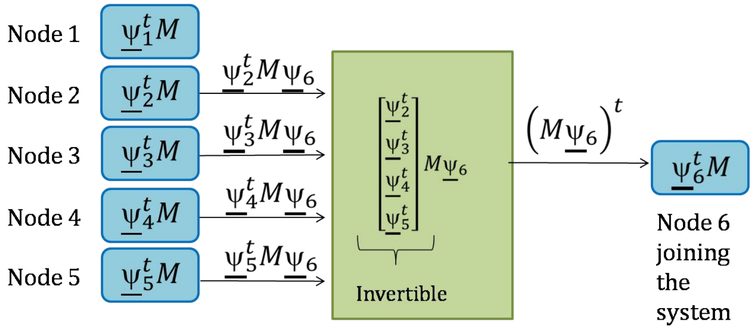
  – Encoding and decoding at every node

Secure Repair Block (SRB) Protocol

Proposed approach can have high throughput, low latency, low storage cost, less communication cost to new miners (new miners to join easily).



Bootstrapping a new node in SRB



Comparison with Existing Schemes

Parameter	Uncoded	SeF	SRB
Storage Overhead	n_S	$(1+\delta)$	$\frac{n_S\alpha}{L}$
Bootstrap Cost	L	$L+O(\sqrt{L}\log^2(L/\delta))$	$\alpha < L$
Security Guarantee	$\frac{n_S}{2}$	$n_S - L - O(\sqrt{L}\log^2(L/\delta))$	$\frac{n_S-\alpha}{2}$

PERFORMANCE COMPARISON OF UNCODED, SEF BASED AND SRB PROTOCOLS FOR SHARDING

- Uncoded/Rapidchain: Higher bootstrap cost and storage
- SeF: New nodes need to decode before mining
- SRB: Start mining with encoded blocks

References

D. S. Gadiraju, V. Lalitha and V. Aggarwal, "Secure Regenerating Codes for Reducing Storage and Bootstrap Costs in Sharded Blockchains," *2020 IEEE International Conference on Blockchain (Blockchain)*, Rhodes, Greece, 2020

Acknowlegement

- This work is in collaboration with Purdue University
- This work was funded by Qualcomm Innovation Fellowship, India 2019

Authors: G.Divija Swetha, V. Lalitha, Vaneet Aggrawal

Signal Processing and Communication Research Center