Towards Searchable and Verifiable Blockchain

PI: Prof. XU Jianliang

OBJECTIVES

1. To design a framework for blockchain to alleviate the storage and computing costs of the user and support verifiable Boolean range queries to guarantee the results’ integrity.
2. To design an efficient index structure that supports range queries with integrity assurance in a hybrid-storage blockchain framework.

HIGHLIGHTS

vChain: Enabling Verifiable Boolean Range Queries over Blockchain Databases

- Investigate the verifiable query processing over blockchain databases.
- To support verifiable Boolean range queries, propose an accumulator-based authenticated data structure that enables dynamic aggregation over arbitrary query attributes.
- Design two new indexes to further aggregate intra-block and inter-block records for efficient query verification.
- Develop an inverted prefix tree structure to accelerate the processing of a large number of subscription queries simultaneously.

GEM²-Tree: A Gas-Efficient Structure for Authenticated Range Queries in Blockchain

- Study the authenticated range queries in the hybrid-storage blockchain.
- Leverage the blockchain smart contract and the Service Provider to both maintain the authenticated data structure.
- Design an authenticated data structure GEM²-Tree that can be efficiently maintained by the blockchain in terms of gas cost.
- Propose an optimized structure GEM²*-Tree to further reduce the maintenance cost without sacrificing much the query performance.

SELECTED PUBLICATIONS