香港浸會大學理學院
HKBU Faculty of Science

DEPARTMENT OF COMPUTER SCIENCE

PhD Degree Oral Presentation

PhD Candidate:	Mr. ZHANG Ce
Date	28 July 2023 (Friday)
Time:	10:00 am – 12:00 nn (35 mins presentation and 15 mins Q & A)
Venue:	1) DLB637, 6/F, David C Lam Building, Shaw Campus 2) ZOOM (Meeting ID: 929 5534 1846) (The password and direct link will only be provided to registrants)
Registration:	https://bit.ly/bucs-reg (Deadline: 6:00 pm, 27 July 2023)

Collaborative On-Chain and Off-Chain Data Processing Techniques for Blockchain Systems

Abstract

Blockchain technology has gained significant attention for its innovative and transformative potential in various industries such as finance and IoT. It offers a new solution for trusted storage and computation services through its immutability and consensus protocol. However, directly storing large-sized general data (e.g., images, documents, PDF files) on the blockchain is not scalable. To address this challenge, prior research has proposed a hybrid storage blockchain architecture, which involves on-chain and off-chain nodes to collaboratively process the blockchain data. Specifically, raw data is stored off-chain while its digest is kept on-chain for notarization. The integrity of the data retrieved from off-chain storage is ensured through the authentication of on-chain digests. Although this approach works well for simple key-value queries, it lacks support for commonly used queries such as range queries and keyword search queries.

Apart from the trusted storage service, the blockchain system itself also faces storage scalability issues due to the replication of transaction histories and ledger states. To address this challenge, prior works have introduced the concept of a stateless blockchain, which also follows the on-chain and off-chain collaboration paradigm. In a stateless blockchain, ledger states and transaction executions are moved off-chain to specific nodes, while only short commitments of ledger states are maintained on-chain, reducing the on-chain workload. However, existing stateless blockchains are primarily designed for cryptocurrencies and do not support smart contract functionality.

To address the aforementioned issues, in this dissertation, we explore novel collaborative on-chain and off-chain data processing techniques for blockchain systems. We first study authenticated range queries and keyword search queries in the hybrid storage blockchains. The key challenge lies in designing an authenticated data structure (ADS) that can be efficiently maintained by the blockchain, where a unique gas cost model is employed. For range queries, we propose a novel ADS called GEM2-tree, which is both gas-efficient and capable of supporting authenticated range queries. We further propose an optimized structure, GEM2*-tree, to reduce maintenance costs without significantly sacrificing query performance. For keyword search queries, we propose the Suppressed Merkle inverted (Merkleinv) index, which securely maintains a partial ADS structure on-chain using a logarithmic-sized cryptographic proof. Additionally, we introduce the Chameleon inverted (Chameleoninv) index, leveraging the chameleon vector commitment to achieve a constant maintenance cost. The performance of the proposed ADSs is validated through theoretical analysis and empirical evaluation.

Moreover, we propose SlimChain, a novel stateless blockchain system that enables scalable transaction processing with smart contract capabilities. To realize SlimChain, we propose new schemes for off-chain smart contract execution, on-chain transaction validation, and state commitment. We also present optimizations to reduce network transmissions and a novel sharding technique to further enhance system scalability. Extensive experiments are conducted to validate the performance of SlimChain.

***** ALL INTERESTED ARE WELCOME *****