香港浸會大學理學院

HKBU Faculty of Science

DEPARTMENT OF COMPUTER SCIENCE

MPhil Degree Oral Presentation

MPhil Candidate:	Mr. Yang Ji
Date	January 10, 2023 (Tuesday)
Time:	10:00 am – 12:00 nn (35 mins presentation and 15 mins Q & A)
Venue:	Zoom ID: 929 0093 5008 (The password and direct link will only be provided to registrants)
Registration:	https://bit.ly/cs-ereg (Deadline: 1:00pm, January 9, 2023)

Towards Secure, Efficient, and Versatile Blockchain Light Clients

Abstract

Recent years have witnessed the prosperity of blockchain technology which seeks to build a decentralized ledger by removing trusted third parties. Light clients have been widely used in blockchain systems to support lightweight nodes by synchronizing and verifying block headers only. However, there are two major limitations with the current light client design. First, with the ever-increasing blockchain size, the cost for light clients to process and store all the block headers would soon become prohibitively high. Second, only simple queries can be supported by light clients due to the limited functionality of block headers.

To address these issues, this thesis aims to propose DCert, a novel decentralized certification framework, to enable superlight clients with constant storage and state validation costs. The main idea is to leverage a trusted enclave (e.g., Intel SGX) to recursively certify the entire history of the blockchain. With DCert, the blockchain integrity can be easily validated by superlight clients with a secure certificate. Furthermore, to support rich verifiable queries on light clients, DCert can be extended to certify authenticated indexes for different types of queries on an as-needed basis. While DCert is compatible with existing blockchain systems, its security is guaranteed by the trusted enclave. Our benchmark-based empirical study shows that DCert incurs a small certification overhead, yet it is capable of supporting efficient verifiable queries with a constant storage size of 2.97 KB and a constant bootstrapping time of 0.14 ms.

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