COMP6452 Software Architecture for Blockchain Applications
Week 10 Tutorial

David Zhang
d.zhang@unsw.edu.au

Yue Liu
yue.liu13@unsw.edu.au

Term 2, 2021

Theory sub-session

The final exam will be 24-hour take-home exam. It takes up 35% of the final mark of the course. You will receive a research paper in the field of blockchain software architecture. The real questions and points in the exam will be similar with but different from the sample questions given below. We expect you to write around 1500 words for these questions in total.

This theory sub-session will get you prepared for the final exam.

Xiwei Xu, Qinghua Lu, Yue Liu, Liming Zhu, Haonan Yao, and Athanasios V. Vasilakos. "Designing blockchain-based applications a case study for imported product traceability". In: *Future Generation Computer Systems* 92 (2019), pp. 399–406. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2018.10.010**. URL:** https://primoa.library.unsw.edu.au/permalink/f/11jha62/TN_cdi_swepub_primary_oai_DiVA_org_ltu_71483

- What is the problem that the research aims to solve? (2 marks, approx. 100 words)

  Since blockchain is an emerging technology which is still at an early stage of development, there is limited experience on applying blockchain to real-world software applications. We share our experience of building originChain. By using blockchain and designing towards security, originChain provides transparent tamper-proof traceability data with high availability and enables automated regulatory-compliance checking and adaptation in product traceability scenarios.

- Why this problem is significant and what are the causes of the problem? (8 marks, approx. 250 words)

Due to the properties and limitations of blockchain, the technology does not fit all the use cases. First, blockchain has limited storage capability since it contains a full history of all the transactions across all participants of the blockchain network. Second, blockchain applications might have sensitive data, but the information on blockchain is designed to be accessible to all the participants. Third, since all the smart contracts can be called by all the blockchain participants by default, a permission-less function might be triggered by unauthorized users accidentally, which becomes a vulnerability of blockchain-based applications.

- What is the architecture design of the solution? Include diagrams to demonstrate. (10 marks, approx. 300 words)

  UI layer, management layer, data layer (off-chain), and blockchain layer (on-chain). Blockchain is used as a software connector that contains both data and business logic. (can elaborate on what services / detailed components in each layer)

- How the study is evaluated? (10 marks, approx. 300 words)

  Qualitative analysis on adaptability regarding upgradability of data/service contracts, and dynamic binding between different parties. Quantitative analysis on the performance of writing and reading data to blockchain and database.

- Are there any design trade-off made? Any new problem introduced by the solution? (3 marks, approx. 100 words)

  On-chain / off-chain data storage; smart contract design and blockchain size.

  The two main limitations of blockchain, including performance and privacy, need to be considered. Performance of the system depends on deployment of the blockchain. In originChain, due to low writing throughput because of the large granularity of traceability information, limited throughput of blockchain is not the main concern. However, the data on blockchain is publicly accessible to all the participants of the blockchain network, the private data (for example, the information of customers) should not be stored on-chain.

- Are there any improvements can be done on this research? (7 marks, approx. 300 words)

  Performance: If using consortium blockchain, can consider improving the gas limit / block size.