Theory and Practice of Blockchains 2019

27-29 May, Aarhus University, Denmark

Mayank Raikwar
Norwegian University of Science and Technology

1 Introduction

Theory and Practice of Blockchains 2019 (TPBC19) workshop was held in the Department of Computer Science at Aarhus University, which brought together researchers working on the theory and implementation of blockchains. I am thankful to COINS to support me to attend this workshop. As my Ph.D. research topic is on blockchain and cryptography, this workshop presented different cryptographic concepts used in consensus, security, and privacy of blockchain. In this workshop, I also learned about Game-theoretic aspects of blockchain. I was also introduced to different blockchain specific languages which I was not aware of beforehand. The workshop had interesting talks by well-known cryptographers and researchers. There was a rump session in the workshop as well, which was quite exciting and entertaining. The food was also delicious, and we had workshop dinner as well before the rump session. More details about the program can be found on the website `https://events.au.dk/TPBC19`. Moreover, the campus of Aarhus University was beautiful, and It was pleasant weather as well to explore the beauty of Aarhus. We also got the pass from the workshop to visit *Aros Aarhus Kunstmuseum* which was fascinating, and the city view of Aarhus from the top of Museum was mesmerizing.

2 Workshop

The program of the workshop was divided into the sessions where each session consists of two to three talks. Few of the sessions were only specific to new languages of blockchain, game-theoretic analysis of blockchain and payment channels in the blockchain. Following are the personal highlights from the talks of the workshop :

- **The Tortoise and Hare's Adventures in Space-Time** by Tal Moran: In this talk, Tal Moran talked about the Spacemesh consenus protocol where blockchain is replaced by BlockMesh architecture which is basically a layered DAG creating multiple blocks concurrently in each timestep. However their analysis relies on honest majority of resources.
- **Language Session** In this session, the talks were about new languague for blockchains. Russell O'Connor talked about *Simplicity* language which improves on existing problems on crypto-currency and can be beneficial to be applied on crypto-currency and blockchain platforms. Simon Thompson describes about *Marlowe* language for writing financial contracts on *Cardano* blockchain.

- **Balancing Privacy and Accountability in Blockchain Transactions** by Ivan Damgard: I got the chance to attend the talk by Prof Ivan. I was reading his book *Secure Multiparty Computation and Secret Sharing* for the coursework at NTNU. His approach to apply different approach for identity management and transactions in Blockchains was interesting.
- **Scaling Distributed RSA Modulus Generation with Dishonest Majority** by Muthuramakrishnan Venkitasubramaniam: As in all RSA crypto system, secuity is based on the Modulus. This work presented a way to compute RSA modulus in a distributed fashion so that the RSA cryptsystem used in blockchain can securely compute all the parameters in case of dishonest majority.
- I also enjoyed the talk on security and privacy of payment channel network by Matteo Maffei. As well as, I got to know about the interesting topics such as non-interactive witness indistinguishability (NIWI) which can be applied in cryptcurrency and blokchain.

3 Conclusion

During this workshop, I met many Ph.D. students, Post-docs researchers, and professors and made new connections. I learned many new interesting things in my area of research as well as in different aspects of blockchain. The program was very well organized with few breaks such that It was easy to focus on all the talks and actively participate in QA sessions. Thanks to COINS research school for providing me the opportunity to attend such an event.