The 1st International Summer School on Security Privacy for Blockchains and Distributed Ledger Technologies

Shuang Wu , NTNU

Octomber 2019

1 Overview

The 1st International Summer School on Security Privacy for Blockchains and Distributed Ledger Technologies is hold in Vienna from 2nd September to 5th September, it is organised by members of TU Wien (Vienna University of Technology), Princeton University, and SBA Research.

The four days programme includes lectures and hackthons. With my personal experience, it provided a good combination of presentations with different technical level and hand-on session. The topics of the presentations are mainly published researches and projects with high-impact. For example, there are several talks about off-line payment channel, state channel, proof of space and so on. In they morning we have two talks, each one is one hour and half long, the topics are more technical relevant while during afternoon we have talks given by people working in industry, they introduce their project, give hackthon seession. This arrangement is reasonable apart from the duration of each topic is too long, it is hard to continuously keep focus on the presentation for one hour and half.

2 Talks

The talks on the first day are mainly about payment channels and scalability via off-line channels. Pedro Moreno-Sanchez from TU Wien gave a talk about their current research on multi-hop payment channel protocol, they found an attack on Hash time lock contract (a payment protocol deployed in Lightning network), they give a solution and deploy it in Lightning network, Kzen network and Comit network, which is very interesting talk. There is also a economic talk about the blockchain influence from economic perspective, it impressed me because even though it is economy relevanted but it was still very technical, it was embedded with a lot of mathematic theories, interesting but hard to follow.

On Tuesday Christian Cachin from university of Bern gave a talk about the security foundation on Blockchain, includes chain consistency, liveness and so on, followed by Angelo De Caro from IBM research talked about permissioned blockchains.

During Wednesday Sebastian Faust from TU Darmstadt gave a talk about state channel. They built a protocol that allows users to build payment channel by utilising the existing payment channels among other users, therefore the users won't be bothered by creating a new channel every time. Sebastian also showed us how they use UC model to prove the security of the protocol, it is a very technical part but very interesting.

The first talk on Thursday was given by Hubert Ritzdorf from ChianSecurity, his topic was about formal verification on smart contract, it is not a relatively new topic, but very practical and interesting. They use formal verification tool to analyse the security of the smart contract. The most interesting talk of the summer school for me is given by Krzysztof Pietrzak from IST Austria, he talked about a new consensus protocol using proof of space instead of proof of work, the idea is to share a big file to server and ask the server return a certain content of the file later. They introduce a way to proof that the server indeed stores the file, this is with the help of verifiable delayed function, which is also a hot topic recently.

There are also talks from industry about building web interface to use cryptocurrency, Bitpanda, Algorand along with their hackthons.

3 Summary

In my opinion, it is a very good summer school with good talks and good organisation, you can learn useful information and meet interesting people there as well. I recommend this summer if you want to find a valuable blockchain summer school to join in.