ESORICS Workshop
International Workshop on Cryptocurrencies and Blockchain Technology - CBT'17
Travel Report

Christopher Carr

11–15 September 2017, Oslo

1 International Workshop on Cryptocurrencies and Blockchain Technology 2017

This workshop was the First International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2017), which was held in Oslo, on 14 September 2017, in conjunction with the 22nd European Symposium on Research in Computer Security (ESORICS) 2017.

The workshop received 27 submissions that were carefully reviewed by the Program Committee. Each submission received at least three reviews. The Committee selected only six full papers, accepting roughly about 22% and four short papers for presentation.

The papers covered aspects of:

- identity management
- smart contracts
- soft- and hardforks
- proof-of-works
- proof-of-stake
- applications to smart ticketing

1.1 Participation

I was there as an attendant of the workshop which fits directly into my line of research. Some talks were more relevant to my work than others. There was a mix of application focused and theoretical talks.

1.2 Talks and papers

1. Securing Proof-of-Stake Blockchain Protocols, by Wenting Li, Sbastien Andreina, Jens-Matthias Bohli, and Ghassan Karame.
2. Merged Mining: Curse or Cure? by Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter, Artemios G. Voyiatzis, and Edgar Weippl
3. Atomically Trading with Roger: Gambling on the Success of a Hardfork by Patrick McCorry, Ethan Heilman, and Andrew Miller
4. In Code We Trust? Measuring the Control Flow Immutability of All Smart Contracts Deployed on Ethereum by Michael Frwis and Rainer Bhme
5. Who Am I? Secure Identity Registration on Distributed Ledgers by Sarah Azouvi, Mustafa Al-Bassam, and Sarah Meiklejohn
6. A User-Centric System for Verified Identities on the Bitcoin Blockchain by Daniel Augot, Herv Chabanne, Thomas Chenevier, William George and Laurent Lambert
7. Towards a Concurrent and Distributed Route Selection for Payment Channel Networks by Elias Rohrer, Jann-Frederik La, and Florian Tschorsch
8. Graphene: A New Protocol for Block Propagation Using Set Reconciliation by Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr and Brian Levine
9. Short Paper: Revisiting Difficulty Control for Blockchain Systems by Dmitry Meshkov, Alexander Chepurnoy, and Marc Jansen
10. Secure Event Tickets on a Blockchain Bjorn Tackmann

1.3 Interesting Talks

1.3.1 Graphene: A New Protocol for Block Propagation Using Set Reconciliation, by Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr and Brian Levine

This talk was particular interesting as it reduced the overlap of data being sent around the blockchain system. The main idea is to use Bloom filters – used to test weather certain elements are in a set probabilistically – to reduce the amount of extra data needed to effectively transmit blocks around the network.

1.3.2 Secure Event Tickets on a Blockchain, by Bjorn Tackmann

In the paper abstract the author claims "We developed a prototype system in which concert tickets are managed as assets on a blockchain. The system prevents ticket theft as well as fraud such as selling invalid tickets, or selling multiple copies of a ticket, by leveraging the consistency features of the blockchain."

The idea was that one could transfer ownership of a ticket to another person securely using Hyperledger Fabric Technology. This was implemented and a demo was shown. Unfortunately, while this was an interesting talk because of the problem being addressed, the most crucial aspect that was overlooked in their implementation, which is the problem of ticket scalping – where people buy many tickets to an event in order to sell them later for a profit. The solution offered no protection against this, so the entire advantage of a blockchain system was not lost, but severely reduced. On asking about this, no solution was considered.