Report:
IACR Summer School on Blockchain Technologies
Corfu – 2016

C Carr
NTNU

May – June 2016

1 Overview of the Event

The event took place on the island of Corfu from 30 May 2016 to 2 June 2016. It was designed to inspire and showcase research in Blockchain and Bitcoin like cryptocurrencies. Overall, there was high attendance rate at all lectures and most were well received.

2 Talks

2.1 Bitcoin overview (Joe)

Introductory talk to kick of the school, focusing on an overview of Bitcoin, from both a technical and a practical standpoint.

2.2 Scaling Bitcoin securely (Aggelos)

Presents a framework for formal analysis of Bitcoin and Blockchain like protocols, which tries to capture what they refer to as a general class of adversaries.

2.3 Consensus (Roger)

Presented somewhat of an overview of the history of consensus protocols. Talk went on to focus on fault tolerance within distributed systems, specifically focusing on consensus protocols Paxos and Zyzzyva.

2.4 Mining (Joe)

A focus on the technical challenges of the Bitcoin consensus and transaction affirmation method, what is commonly referred to as mining. The talk looks at hardware, and its evolution, contrasting that with "physical" gold mining

and its development. There is an undercurrent of addressing the mining pool concern which is rather significant within the ‘Blockchain community.

2.5 Cryptographic e-cash (Jan)

A look back at the different flavours of crypto e-cash, which is a refreshing approach in the context of the modern distributed digital cash, that is separate, and in some ways ignores, the research conducted towards the currently politically dangerous ideas of centralised systems.

2.6 Anonymity in cryptocurrencies (Foteini)

Lectures on the mounting issues concerning anonymity in Bitcoin, being that it is not very strong and it is causing problems. Takes a deep look into the areas of tumbling and mixing services to see what if they offer any form of anonymity whatsoever.

2.7 Cryptography on the blockchain (Vassilis)

Describing how one can use the Blockchain – or a Blockchain – to achieve other interesting results, such as an ability to do a secure online lottery system. They use some formal models with the assumption that Bitcoin behaves in a standard way, in order to get some results, before relaxing that assumption in order to show that there are still useful cryptographic applications even in cases where Bitcoin has malicious users.

2.8 Short talks

Collection of accepted short talks given by participants, which included academic ideas as well as presentations from industry.

2.9 Decentralisation as a privacy-enhancing technology (George)

Talk focuses on the considerable benefits that can come from a truly decentralised system, before addressing the issues that surround the area.

2.10 Bitcoin de-anonymization in practice (Adam)

Talk from a start up about their journey, offering some interesting insights into what has been happening on the Bitcoin transaction graph, and providing some further results into practical discussion of how you would go about deanonymising users of the network.

2.11 Breakout sessions

Session inspired for designers to get hands on with the technology, including a toy cryptocurrency developed specifically for the event called corfu coin.

2.12 Anonymous online marketplaces (Nicolas)

Highlighting the concerns that Bitcoin and other problems that arise with an anonymous (pseudo-anonymous) distributed system like Bitcoin.

2.13 The Bitcoin economic ecosystem (Rainer)

Rainer focused on the financial incentives behind Bitcoin, providing some insight as to why it was so successful in the first place, making the case that it is better to have a system that incentives early adopters, although it remains to be seen if this will help with the long term sustainability.

2.14 Regulation in Bitcoin (Jerry)

Presentations from a legal perspective. The main message here was that Bitcoin has never been unregulated, and has in fact always come under some regulatory framework, since the first practical application. Mostly, the talk described the ways that Bitcoin has come up against regulation and how burdensome it can become on trading platforms.

2.15 Alternatives to Blockchains (Sarah)

Delves into the murky area between *fully decentralised* and transparent recording of data and the traditional behind-closed-doors approach that is apparent in centralised banking. The talk focuses on the developments in these areas and discusses the growing work on other areas, such as alternative *proof-of-x* schemes.