



*Dr. Christian Cachin
IBM Research – Zurich
 Säumerstr. 4
CH-8803 Rüschlikon
Switzerland
Phone: +41 44 724 8989
Email: cca@zurich.ibm.com
Web: www.zurich.ibm.com/~cca/*

Rüschlikon, 22. Sep. 2016

Thesis project for Chrysa Stathakopoulou, M.Sc. Student at D-ITET, ETHZ

Distributed cryptography for blockchains

The blockchain data structure, which first appeared in Bitcoin, realizes an immutable record of transactions, maintained collaboratively by all parties in a distributed system. Blockchain implementations achieve this by distributing trust: the data is maintained and controlled by the parties that are only connected over the Internet.

Distributed consensus protocols and cryptographic tools play a crucial role in protocols for building blockchains. The Linux Foundation's Hyperledger Project develops a distributed ledger platform, including one based on Byzantine-fault tolerance from IBM. The goal of this project is to explore the power of distributed cryptosystems in this context.

A threshold (or distributed) cryptosystem distributes the power of a cryptographic scheme (digital signature operation, public-key decryption and so on) over a group of parties in a collaborative and resilient way. No single party alone controls the key, and the scheme always needs enough parties to operate. The Hyperledger fabric already contains a cryptographic security architecture, but no distributed cryptography. In this project a distributed cryptosystem will be developed and integrated with the Hyperledger fabric.

The work will consist of

- 1) design and implementation of a distributed digital signature scheme;
- 2) exploration of protocols for distributed cryptography in Hyperledger fabric;
- 3) (potentially) design and implementation of protocol functions using the distributed cryptosystem.

The project will take be carried out at IBM Research – Zurich, in the time from 17 September 2016 until 17 March 2017, under my guidance. A contract between Chrysa Stathakopoulou and IBM Research GmbH regulates the details of her work inside IBM. Prof. Roger Wattenhofer is responsible for the supervision on behalf of ETH Zurich.

After about three months and again at the end of the project, a the work should be presented at the Computer Engineering and Networks Laboratory (TIK), ETH Zurich.

Sincerely,

Christian Cachin