Introduction to cryptocurrencies

Abstract

The cryptographic currencies (also dubbed the cryptocurrencies) are a fascinating recent concept whose popularity exploded in the last 6-7 years. The most prominent of them is Bitcoin, introduced in 2008 by an anonymous developer using a pseudonym "Satoshi Nakamoto". These currencies quickly gained noticeable attention among the general public, and their economic importance is rapidly growing - the current capitalization of Bitcoin is over 130 billion USD, and the average number of transactions per day is well above 200,000. The security of Bitcoin is based on an assumption that a large fraction of computing power in the system is controlled by the honest parties.

This tutorial will consist of three parts. The goal of the first part (Lecture 1 and 2) is to provide a research-oriented introduction to Bitcoin. We will start with a description of Bitcoin and its main design principles. We will then talk about the mechanics of the mining pools. Finally, we will discuss some of the weaknesses of Bitcoin, including the so-called *selfish mining attack*, and show some ideas for dealing with them.

In the second part (Lecture 3) we will provide an introduction to the so-called *Bitcoin smart contracts*, and give some examples of their applications, including the micropayment systems, and the multiparty lotteries.

In the last part (Lecture 4) we will present some alternative cryptographic currencies, including those that are used in real life (e.g. Litecoin, Ethereum), and those that are currently only academic proposals (e.g. Spacemint, and Permacoin).

Lectures

Lecture 1 Introduction: history of cryptocurrencies, and the reasons behind their success; high-level description of Bitcoin (Proofs of Work, the blockchain and the transaction syntax).

Lecture 2 Bitcoin mining pools and the attacks against them; security of Bitcoin (technical and conceptual errors in the design, the selfish mining attacks, problems with key storage).

Lecture 3 Smart contracts and their applications, the *Lighting* micropayment system, secure lotteries, and other multiparty computation protocols.

Lecture 4 Alternative cryptographic currencies: Litecoin and Ethereum; currencies based on paradigms other than the Proofs of Work (Proofs of Stake and Proofs of Space); currencies with “useful Proofs of Work” (Primecoin, Permacoin); non-outsourceable Proofs of Work.