BLOCKCHAIN AND CRYPTOCURRENCIES

Instructor: Julien Prat (CNRS, CREST and Ecole Polytechnique)

Course prerequisites

The course is designed for Master students in Economics or Business. Besides their training in economics and quantitative methods, no specific knowledge about Blockchains is required. Basic programming skills in Python will also be useful.

Course content

The financial industry was until recently a very concentrated sector. This is becoming less and less true as a wave of innovations greatly lowers the barriers to entry and intensifies the degree of competition among providers of financial services. Disruptive technologies are being implemented at an increasing pace, leading to major changes in the realms of payments, lending and borrowing, insurance, wealth management, venture capital.

To understand this revolution, one needs to have a good grasp of technological innovations as well as of the economics of the financial sector. This course will introduce students to both dimensions, allowing them to identify how financial services can be improved with new approaches.

The course will put a strong emphasis on the blockchain protocol because of its disruptive potential, hopefully preparing the audience for the next wave of innovations. We will adopt a hands-on approach with the objective of enabling students to monitor transactions over Bitcoin's blockchain.

On completion of this course, students should understand:

- The ongoing trends in the Fintech industry and their technological underpinnings;
- How cryptographic functions make it possible to secure transactions over a public network;
- Why the blockchain technology can replace third-party certification;
- What are the main differences between the most prominent blockchain infrastructures;
- How the market for cryptocurrencies operates, and critically assess its functions and vulnerabilities;
- What are "smart contracts".

Course structure

1. Introduction to Banking, Fintech and Payment Systems.

2. Basics of Cryptography: Public/private keys, Hash functions…

3. Blockchains: Tamper-evident database, Industrial application of Blockchains (supply chains, payment networks, smart grids, online banking…)

4. Decentralization of the Blockchain under "Nakamoto" consensus: Byzantine general's problem, transactions, mining, Proof-of-work.

5. Using Bitcoin core: How to operate a node in Bitcoin's network

6. The structure of transactions in Bitcoin: UTXOs and Bitcoin Script.

7. Theory of Money and Cryptocurrencies: Credit economy vs. Cash economy, Fundamental analysis of Bitcoin and alternative coins.

8. Smart Contracts: Algorithmic Decision making, Programing self-executing contracts in Bitcoin script, Atomic Swaps.

9. Initial Coin Offerings: Venture Capital, Startups financing, Web 3.0 and decentralized infrastructures.

10. Advanced topics:
    a. New forms of governance;
    b. Alternative protocols: Proof-of-stake;
    c. Zero knowledge proofs and anonymous transactions;
    d. Scaling and Sidechains: Lightning Network, segregated witness…;
    e. Decentralized prediction markets;
    f. External data: Oracles and Internet-of-things.

Literature

The subject being quite new, the literature is still in its embryonic stage. The slides of the course will be self-contained as all the required material will be covered during the lectures. Additional material can be found in the following books:

- *Bitcoin and Cryptocurrency Technologies*, by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder.
- *Mastering Bitcoin: Programming the Open Blockchain*, by Andreas Antonopoulos