



## Lecture Plan

### 1) Identification

**Course: Blockchain and Cryptocurrencies Technologies**

**Credits: 45h**

**Online: 22h Onsite: 23h**

**Professors :** **Jean Everson Martina**  
**Ricardo Felipe Custodio**  
**Thais Bardini Idalino**

### 2) Prerequisites

Students must have programming skills. Some prior familiarity with cryptography may be helpful, but all necessary background will be covered in class.

### 3) Aim

Cryptographic Primitives. Blockchain concepts and protocols. Cryptocurrencies and non-financial applications running on blockchains. Smart contracts development.

### 4) Objectives

#### General Objectives :

Understand the concepts of the blockchain ecosystem. Distinguish between financial and non-financial applications on blockchains. Learn how to develop decentralized applications.

#### Specific Objectives:

- Understand security primitives as a way of yielding security
- Understand how blockchains provide distributed storage and reach consensus
- Describe how transactions can be used to transfer assets on blockchains
- Use cryptographic means to identify transacting users
- Comprehend how cryptocurrencies and non-financial applications work on blockchains
- Create and deploy smart contracts to conceive as autonomous, conflict-free applications

### 5) Course Outline

- Cryptographic Primitives.
  - Hash functions
  - Asymmetric cryptography
- Blockchain concepts
  - Assets
  - Wallets

- Transactions
- Blocks and linked lists based on hashing
- Mining and Proof of Work
- Nodes and distributed consensus
- Blockchain Properties
  - Anonymity
  - Consensus
  - Post-Quantum Integrity
  - Resilience
- Blockchain applications
  - Cryptocurrencies: Bitcoin and altcoins
  - Non-financial applications: notarial services, name registry and message exchange
- Smart contracts development on Ethereum
  - Use cases: voting, record keeping, digital identities
  - Ethereum Virtual Machine
  - Hyperledger Fabric
- Project Development
  - Infrastructure for conducting experiments
  - Deploying experiment
  - Reporting experiments

## 6) Methodology

This will be a project-oriented course intended to give students theoretical knowledge but also hands-on experience. We will see the basic building blocks necessary to build blockchains and perform all the cryptography needed. We will then cover all the key concepts behind cryptocurrencies with the focus of understanding how they work and how they disrupt current models. We will study a series of known applications for blockchains and its related technologies.

The first part of the course will be taught and explanatory. This part of the course will happen mostly asynchronously using pre-recorded classes following the pandemic regulations in place by the university. It aims at explaining the innards of the technology of blockchains and cryptocurrencies. The second part of the course will focus primarily on student projects, carried out individually or in small teams. This part will involve more synchronous classes. A typical project may involve:

- Coming up with a specification for a particular system using the technologies seen in the first part and performing a detailed analysis of its properties; or
- Extending or adapting an existing cryptocurrency system for achieving different goals targeted for specific applications.
- Conducting a theoretical study of the relationship between several models studied before.

A selection of candidate projects will be provided, but students are encouraged to propose their own.

Lectures will be given in English to broaden the outreach of the course and to facilitate access to standard material of the area such as books, articles and manuals of the tools. Also the course may be joined by international partners under cooperation agreements with UFSC, where credits are interchangeable. A second but no least important reason for the Lecture to be conducted in English is

that experts on the field will be invited to speak in some guest lectures. Guest Lectures will be limited to three throughout the semester and will cover some tools and techniques from the viewpoint of its creators.

## **7) Evaluation**

The evaluation will be conducted over a final technical report written by the students, together or not with their research supervisors or the course professor. This technical report will be constructed over the semester with oversight of the course professor.

The technical report will be assessed using standard strategies used to evaluate conference papers. The technical reports will be evaluated over their readability, adherence to the proposed topic, contribution, coherence of the experimentation conducted and the results achieved.

Technical reports will be graded using the standard grading system for the PPGCC program and will be the final grade achieved by the student. Technical reports with a pass mark should be fit for submission to the main conferences in the area of security protocols, formal methods or foundations of computer security.

## **8) Schedule**

To be defined at the beginning of the semester with the students.

## **9) Bibliography**

- **The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, William Mougayar, 2016, 209pp**
- **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Don Tapscott, 2016, 268pp**
- **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Arvind Narayanan; Joseph Bonneau; Edward Felten; Andrew Miller; Steven Goldfeder, 2016, 328pp**
- **Bitcoin and Cryptocurrency Technologies. Nayaran, Arvind et al. Online:**
- **<http://bitcoinbook.cs.princeton.edu>**
- **Solidity. Online: <https://solidity.readthedocs.io/en/latest/index.html>**
- **A Blockchain Platform for the Enterprise - Hyperledger Fabric <https://hyperledger-fabric.readthedocs.io/en/release-2.2/>**