2IN1510 – Understanding blockchain

Instructors: Marc-Antoine Weisser
Department: INFORMATIQUE
Language of instruction: FRANCAIS
Campus: CAMPUS DE PARIS - SACLAY
Workload (HEE): 45
On-site hours (HPE): 27,00
Elective Category : Fundamental Sciences
Advanced level : Yes

Description
The objective of this course is to understand the blockchain technology, to be able to explain it, to know in which context to use it and why it is not adapted in all contexts.

Quarter number
Intensive week SG6

Prerequisites (in terms of CS courses)
Good knowledge of the basics of Python 3.

Syllabus
The course is divided into 5 major parts.

I. Introduction to the blockchain and cryptographic elements
- The shared ledger
- Block chaining
- One-way function

II. Implementation of the blockchain
- Proof of work
- Nodes and miners
- Composition of a transaction
- Initialization of a chain
- Composition of a block
- Validation process

III. Advanced concepts
- Mining
- Crypto risk
- Other proofs

- Smart Contract
- Consensus
- Fork of the chain and resolution

IV. issues
- Pool and governance
- Vulnerabilities
- Ethics and legal

V. TP
- Implementation of a simple blockchain in Python
- Proposal of an application integrating it

Class components (lecture, labs, etc.)
- Lectures: 6x3h
- TP: 3x3h

Grading
Validation on the TP and a report.

Resources
- Lectures
- Practical Work
- Reading of support and synthesis

The courses and supervision of TP are provided by Marc-Antoine Weisser.

Learning outcomes covered on the course
At the end of this course, the student will be able to understand how works a shared ledger using blockchain technology, to know its possibilities, its issues and its limitations. The student will have acquired:
- basic elements of asymmetric cryptography (one-way function, hashing, public key and private key, etc.);
- the fundamental elements of blockchain technology (block chaining, proof of work, nodes, mining, composition of a block, etc.);
- some extensions and alternatives (proof of stake, smart contract, consensus, ...);
- the stakes (security, governance, vulnerability, ...).

Learning outcomes:
- Know the principles of asymmetric cryptography
- Understand how blockchains work
- Implement a blockchain

- Distinguish the relevant use cases of a blockchain
- Design an application implementing a blockchain

Description of the skills acquired at the end of the course

C1.1: Examine problems in their entirety and beyond their immediate parameters. Identify, formulate and analyse the scientific, economic and human dimensions of a problem

C1.4 : Design, detail and corroborate a whole or part of a complex system.