INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

DPT INFORMATIQUE
COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
INSA Campus LyonTech - 7 Avenue Jean Capelle
Batiment Blaise Pascal - 69621 VILLEURBANNE
Phone 0472438892
Web site : http://if.insa-lyon.fr

Conferences and Seminars

Blockchain

IDENTIFICATION

CODE : IF-5-S1-EC-OT4
ECTS : 6.0

HOURS

Lectures :	0.0 h
Seminars :	64.0 h
Laboratory :	0.0 h
Project :	0.0 h
Teacher-student contact :	64.0 h
Personal work :	64.0 h
Total :	128.0 h

ASSESSMENT METHOD

Presentation, demo, and deliverables of the project

TEACHING AIDS

TEACHING LANGUAGE

English

CONTACT

M. BETTINGER Matthieu
matthieu.bettinger@insa-lyon.fr
M. HASAN Omar
omar.hasan@insa-lyon.fr

AIMS

The objective of this course is to introduce the fundamental concepts of blockchain, which will include cryptographic foundations. Moreover, advanced security concepts such as secure multi-party computation will be covered.

CONTENT

1) Cryptographic foundations
- Cryptographic hash functions
- Message digests
- Commitment schemes
- Hash data structures, Merkle trees
- Digital signatures
- Public keys as identities

2) Blockchain
- Decentralization
- Distributed ledger
- Distributed consensus
- Cryptocurrencies
- Mining, proof of work, proof of stake
- Immutability

3) Smart contracts
- Turing complete code execution on blockchain
- Virtualization, Ethereum virtual machine
- Fairness, guaranteed execution of conditional code
- Transactions (deposit, execute, transfer)

4) Introduction to distributed application development
- Environment setup
- P2P network setup
- Development in Solidity
- Java APIs, Web3J, RPCs, GETH
- Deployment
- Remotely accessing smart contract functionality

5) Student project
- Blockchain-specific requirements definition
- Student project proposals
- Project initiation and management
- Design, development, testing on blockchain platform

6) Secure multiparty computation
- Secure protocols
- Homomorphic encryption
- Zero-knowledge proofs
- SMPC applications

BIBLIOGRAPHY

[1] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
[2] Ethereum Homestead Documentation. http://www.ethdocs.org/en/latest/
[3] Web3j 3.5.0 Documentation. https://web3j.readthedocs.io/en/latest/