UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Smart Contracts, Bitcoin and Blockchain Technology

2122-1-FSG01A002

Aims

Understanding of the principles of operation of blockchains, cryptocurrencies, and smart contracts. Ability to understand the operation of simple smart contracts. Ability to choose the most suitable type of blockchain, depending upon the domain-based application.

Contents

Basic notions and concepts underlying blockchains, cryptocurrencies, and smart contracts. The course also provides the conceptual and theoretical tools that allow the student to understand the operations of blockchain-based applications (DAPPs) which are currently found on the market.

Detailed program

1. Introduction to blockchains: motivations, types of blockchains, and their applications
2. Transaction-based blockchains: Bitcoin and other cryptocurrencies
3. Asymmetric cryptography: encryption, digital signatures, elliptic curves, hash functions
4. Some further details on how Bitcoin works
5. Exchanges and wallets
6. Bitcoin's scripts
7. Account-based blockchains: Ethereum
8. Differences between Bitcoin's blockchain and Ethereum's blockchain
9. Introduction to smart contracts: what they are, possible applications, and limitations
10. Design and implementation of smart contracts in Solidity

11. Security aspects of blockchains and smart contracts
12. Tokenization. Fungible and non-fungible tokens (NFT). The standards ERC20 and ERC721. . Some legal aspects of tokenization
13. Consensus algorithms
14. Permissioned blockchains, and the design of private blockchains for enterprise applications
15. Notarization, and storing documents
16. Some applications of blockchains. Architecture and operation of a decentralized application (DApp)
17. Side-chains and cross-chains

Prerequisites

None.

Teaching form

Lectures in the classroom, with examples performed (by the teacher) on a computer.

The teaching language is Italian.

Textbook and teaching resource

Textbooks:

- Imran Bashir. *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*, 3rd Edition, Packt Publishing, 2020

- Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain,* 2nd Edition. O'Reilly, 2017. https://github.com/bitcoinbook/bitcoinbook
- Andreas M. Antonopoulos, Mastering Ethereum: Building Smart Contracts and Dapps. O'Reilly, 2018. https://github.com/ethereumbook/ethereumbook

Lecture notes provided by the teacher.

Semester

Second semester, Academic Year 2021-2022

Assessment method

The learning assessment is based on an oral colloquium, on the subjects exposed in class during the course.

Office hours

On appointment