UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Smart Contracts, Bitcoin e Blockchain Technology

2122-1-FSG01A002

Obiettivi

Comprensione dei principi di funzionamento delle blockchain, delle criptovalute e degli smart contract. Capacità di capire il funzionamento di semplici smart contract. Capacità di scegliere il tipo di blockchain più adatta a seconda della applicazione.

Contenuti sintetici

Nozioni e concetti alla base del funzionamento delle blockchain, delle criptovalute, e degli smart contract. Il corso fornisce inoltre gli strumenti concettuali e teorici che consentono di comprendere il funzionamento delle applicazioni basate su blockchain (DAPPs) presenti sul mercato.

Programma esteso

1. Introduzione alle blockchain: motivazioni, tipi di blockchain, e loro applicazioni
2. Blockchain basate sulle transazioni: Bitcoin e altre criptovalute
3. Crittografia asimmetrica: cifratura, firme digitali, curve ellittiche, funzioni di hash
4. Qualche dettaglio in più su come funziona la blockchain di Bitcoin
5. Gli exchange, e i wallet
6. Gli script di Bitcoin
7. Blockchain basate su account: Ethereum
8. Differenze tra la blockchain di Bitcoin e la blockchain di Ethereum
9. Introduzione agli smart contract: cosa sono, possibili utilizzi e limitazioni
10. Progettazione e implementazione di smart contract in Solidity
11. La sicurezza delle blockchain e degli smart contract
12. La tokenizzazione. Token fungibili e non fungibili (NFT). Gli standard ERC20 e ERC721. Alcuni

aspetti legali della tokenizzazione
13. Algoritmi di consenso
14. Blockchain permissioned, e costruzione di blockchain private per il mondo enterprise
15. Notarizzazione, e memorizzazione di documenti
16. Alcune applicazioni delle blockchain. Architettura e funzionamento di una applicazione decentralizzata (DApp)
17. Side-chains e cross-chains

Prerequisiti

Nessuno.

Modalità didattica

Lezioni in aula, con esempi svolti (dal docente) al computer.

La lingua di erogazione è l'Italiano.

Materiale didattico

Libri:

- 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

Appunti forniti dal docente.

Periodo di erogazione dell'insegnamento

Secondo semestre A.A. 2021-2022

Modalità di verifica del profitto e valutazione

La verifica dell'apprendimento è basata su un colloquio orale avente per oggetto gli argomenti svolti a lezione.

Orario di ricevimento

Su appuntamento