UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Smart Contracts, Bitcoin e Blockchain Technology

2526-1-FSG02A002

Obiettivi formativi

- Conoscenza e capacità di comprensione
  Conoscere e comprendere il funzionamento delle principali tipologie di blockchain, degli smart contracts. Comprendere le principali implicazioni giuridiche, sociali e finanziarie connesse all'uso delle blockchain e criptovalute.

- Conoscenza e capacità di comprensione applicate
  Saper scegliere la miglior tipologia di blockchain per un determinato scopo.

- Autonomia di giudizio
  Saper valutare i rischi e le potenzialità connesse all'uso di soluzioni basate su blockchain.

- Abilità comunicative
  Saper interagire con esperti informatici e amministratori per comprendere e discutere l'adozione di strumenti basati sulla blockchain.

- Capacità di apprendere
  Saper valutare criticamente nuovi strumenti basati sulla blockchain, valutandone l'utilità, le criticità e le implicazioni giuridiche.

Contenuti sintetici

Nozioni e concetti alla base del funzionamento delle blockchain, delle criptovalute, e degli smart contract. Semplici esempi pratici di creazione di criptovalute e smart contract.

Programma esteso

- Introduzione alle blockchain: motivazioni, tipi di blockchain, e loro applicazioni
- Blockchain basate sulle transazioni: Bitcoin e altre criptovalute
- Crittografia asimmetrica: cifratura, firme digitali, funzioni di hash
- Gli exchange, e i wallet
- Gli script di Bitcoin
- Blockchain basate su account: Ethereum
- Differenze tra la blockchain di Bitcoin e la blockchain di Ethereum
- Criptovalute: esempi pratici e attualità
- Introduzione agli smart contract: cosa sono, possibili utilizzi e limitazioni
- La tokenizzazione. Token fungibili e non fungibili (NFT).
- Algoritmi di consenso

Prerequisiti

- Competenze di base in matematica (livello scuola secondaria di secondo grado).
- Capacità di leggere semplici testi in inglese.

Metodi didattici

- 21 lezioni da 2 ore svolte in modalità erogativa (in italiano) in presenza.
- Disponibilità delle registrazioni delle lezioni.

Modalità di verifica dell'apprendimento

La verifica dell'apprendimento verrà effettuata per mezzo di una prova scritta a domande aperte. Non sono previste prove in itinere.
Le domande saranno di ordine generale e saranno volte alla verifica della comprensione sia degli aspetti teorici connessi alle tematiche affrontate durante il corso, sia delle loro implicazioni pratiche. Essenziale sarà dimostrare di aver compreso i principali vantaggi e limiti delle tecnologie discusse a lezione, nonché di essere in grado di scegliere lo strumento più adatto al supporto di alcune comuni esigenze in ambito giuridico.
Attenzione verrà inoltre data alla proprietà di linguaggio e alla capacità di rielaborazione personale.

Testi di riferimento

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
  Può essere (legalmente) scaricato da: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

Sustainable Development Goals