

PEER TO PEER SYSTEMS AND BLOCKCHAINS

LAURA EMILIA MARIA RICCI

Anno accademico 2022/23
CdS INFORMATICA
Codice 261AA
CFU 6

| Moduli | Settore | Tipo | Ore | Docente/i |
|----------------------|---------|---------|-----|--------------------------|
| SISTEMI PEER TO PEER | INF/01 | LEZIONI | 48 | LAURA EMILIA MARIA RICCI |

Obiettivi di apprendimento

Conoscenze

Al termine del corso, lo studente acquisirà conoscenze in merito alla progettazione di sistemi peer to peer e di sistemi basati su blockchain.

Modalità di verifica delle conoscenze

Per l'accertamento delle conoscenze saranno svolte delle due prove in itinere, un midterm ed un final term. Infine sarà svolto un progetto finale.

Capacità

Al termine del corso:

- lo studente saprà sviluppare una applicazione distribuita
- lo studente saprà sviluppare smart contract
- lo studente conoscerà diversi meccanismi di consenso

Modalità di verifica delle capacità

Sarà svolto un progetto finale per la verifica della acquisizione delle capacità

Comportamenti

- Lo studente potrà acquisire e/o sviluppare sensibilità alle problematiche relative all'uso di criptomonete

Modalità di verifica dei comportamenti

- Il mid term e final term dovranno essere accompagnati da brevi relazioni

Prerequisiti (conoscenze iniziali)

- Reti di Calcolatori
- Algoritmica
- Conoscenza di almeno un linguaggio di programmazione

Indicazioni metodologiche

- sito di e-learning contenente materiale didattico
- progetto didattico
- il corso è tenuto in lingua inglese

Programma (contenuti dell'insegnamento)

Introduction to the course
Peer to Peer

- Peer to Peer (P2P) systems: general concepts
- Unstructured Overlays: Flooding, Random Walks, Epidemic Diffusion
- Structured Overlays: Distributed Hash Tables (DHT), Routing on a DHT, IPFS

Case Studies:

- BitTorrent as a Content Distribution Network
- KAD implementation of the Kademia DHT

Cryptocurrencies and Blockchains

- basic concepts: basic cryptographic tools (digital signatures, cryptographic hash, Merkle trees,...)
- blockchains: definition
- distributed consensus: definition

the Bitcoin blockchain

- Bitcoin mining mechanism: Nakamoto consensus
- pseudoanonymity: traceability and mixing
- the Bitcoin P2P Network

Ethereum

- structure of the blockchain and consensus mechanism
- programming smart contracts with Solidity

Applications of blockchains:

- NFT
- supply chain
- Self Sovereign Identity

Improving Scalability

- Bitcoin Lightning Network
- Interledger Protocols

Further Consensus mechanisms

- Proof of Stake
- Proof of Space
- Byzantine consensus

Bibliografia e materiale didattico

Materiale fornito dal docente e presente sul sito di e-learning

Indicazioni per non frequentanti

Le slide presentate durante le lezioni sono pubblicate su web, sul sito del corso.
<https://elearning.di.unipi.it/course/view.php?id=218>

Modalità d'esame

Progetto + Orale.

Pagina web del corso

<https://elearning.di.unipi.it/course/view.php?id=295>

Note

Nessuna

Ultimo aggiornamento 06/01/2023 23:54