Guia docent
200251 - DEB - Enginyeria de Dades i Blockchain

Última modificació: 10/06/2022

Unitat responsable: Facultat de Matemàtiques i Estadística
Unitat que imparteix: 744 - ENTEL - Departament d'Enginyeria Telemàtica.

Titulació: GRAU EN MATEMÀTIQUES (Pla 2009). (Assignatura optativa).

Curs: 2022 **Crèdits ECTS:** 3.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: JOSE LUIS MUÑOZ TAPIA

Altres: Primer quadrimestre:
JOSE LUIS MUÑOZ TAPIA - M-A

CAPACITATS PRÈVIES

Nocions bàsiques de programació.

METODOLOGIES DOCENTS

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores aprenentatge autònom	45,0	60.00
Hores grup gran	15,0	20.00
Hores grup petit	15,0	20.00

Dedicació total: 75 h

CONTINGUTS

Introducció a la criptografia

Descripció:
Introducció a la criptografia bàsica

Objectius específics:
Introducció als algoritmes criptogràfics
Criptografia simètrica
Criptografia asimètrica
Funcions de hash

Dedicació: 5h
Grup gran/Teoria: 1h
Grup mitjà/Pràctiques: 1h
Aprenentatge autònom: 3h

Monedes digitals centralitzades

Descripció:
Monedes digitals centralitzades

Objectius específics:
El problema de la doble despesa.
Signatures a cegues.
Sistemes de pagament anònims amb llibre major centralitzat.

Dedicació: 5h
Grup gran/Teoria: 1h
Grup mitjà/Pràctiques: 1h
Aprenentatge autònom: 3h

Descentralització

Descripció:
Descentralització

Objectius específics:
Introducció i motivació de la descentralització.
Replicació d'estats versus replicació de màquines d'estats.
Protocols de consens.
Sistemes Fail-Stop i Bizantins.
Xarxes síncrones i asíncrones.
L'algoritme fiable, replicat, redundant i tolerant a falles (RAFT).
L'algoritme Practical Byzantine Fault Tolerant (PBFT).

Dedicació: 12h 30m
Grup gran/Teoria: 2h 30m
Grup mitjà/Pràctiques: 2h 30m
Aprenentatge autònom: 7h 30m

Blockchain i Prova de Treball (PoW)

Descripció:
Blockchain i Prova de Treball (PoW)

Objectius específics:
Atacs sybil i consens amb Proof of Work (POW).
La cadena de blocs.
Verificació de transaccions.
Atacs a POW.
Piscines mineres.
Mineria amb circuits integrats d'aplicació específica (ASIC).
Governança i bifurcacions.

Dedicació: 12h 30m
Grup gran/Teoria: 2h 30m
Grup mitjà/Pràctiques: 2h 30m
Aprenentatge autònom: 7h 30m

Coin-based Ledgers

Descripció:
Coin-based Ledgers

Objectius específics:
Unspent Transaction Outputs (UTXOs).
Introductió a Bitcoin.
Bitcoin’s script.
Wallets and Hierarchical Deterministic (HD) wallets.

Dedicació: 12h 30m
Grup gran/Teoria: 2h 30m
Grup mitjà/Pràctiques: 2h 30m
Aprenentatge autònom: 7h 30m

Balance-based ledgers

Descripció:
Balance-based ledgers

Objectius específics:
Principis bàsics dels llibres comptables basats en l'equilibri.
Atacs i contramesures als llibres comptables basats en l’equilibri.
Introducció a Ethereum.
Simulació d’una cadena de blocs d’Ethereum.

Dedicació: 12h 30m
Grup gran/Teoria: 2h 30m
Grup mitjà/Pràctiques: 2h 30m
Aprenentatge autònom: 7h 30m

Smart contracts

Descripció:
Smart contracts

Objectius específics:
Introducció a la programació de contractes intel·ligents.
Teoria bàsica de jocs aplicada als contractes intel·ligents.
Estudi de casos d'ús: compra remota, tokenització, Ofertes inicials de monedes (ICO).

Dedicació: 15h
Grup gran/Teoria: 3h
Grup mitjà/Pràctiques: 3h
Aprenentatge autònom: 9h

SISTEMA DE QUALIFICACIÓ

35% prova parcial i preguntes.
35% Laboratori.
30% Treball final (aquest és un treball que es lliurarà en forma de petit article de recerca i que també serà presentat pels estudiants a classe).

BIBLIOGRAFIA

Bàsica:
- Antonopoulos, Andreas M. Mastering Bitcoin : programming the open blockchain [en línia]. 2nd edition. Beijing: O'Reilly Media, 2017 [Consulta: 30/05/2022]. Disponible a: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=4875878. ISBN 9781491954362.
- Rosenbaum, Kalle. Grokking bitcoin [en línia]. Manning, 2019 [Consulta: 30/05/2022]. Disponible a: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=6642506. ISBN 9781638355977.
- Narayanan, Arvind; Bonneau, Joseph; Felten, Edward. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press, 2016. ISBN 9780691171692.
- Solorio, Kevin; Kanna, Randall; Hoover, David H. Hands-on smart contract development with solidity and ethereum: from fundamentals to deployment [en línia]. O'Reilly Media, 2020 [Consulta: 30/05/2022]. Disponible a: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=5984595. ISBN 9781492045236.