Universitat Autònoma de Barcelona

2023/2024

Tecnologia Blockchain i Criptomonedes

Codi: 105072
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502441 Enginyeria Informàtica	OT	4	1

Professor/a de contacte

Nom: Jordi Herrera Joancomarti

Correu electrònic: jordi.herrera@uab.cat

Idiomes dels grups

Podeu accedir-hi des d'aquest enllaç. Per consultar l'idioma us caldrà introduir el CODI de l'assignatura. Tingueu en compte que la informació és provisional fins a 30 de novembre de 2023.

Equip docent

Cristina Perez Sola

Prerequisits

Per a cursar aquesta assignatura és necessari haver superat les assignatures d'Informació i Seguretat (IS) i la de Fonaments de Tecnologia de la Informació (FTI), que introdueix diferents conceptes importants a tenir consolidats per a cursar l'assignatura de TBC. En concret:

- FTI consolida els coneixements de criptografia que els estudiants han obtingut en l'assignatura d'IS.
- L'algorisme de signatura de l'ElGamal, que s'estudia a FTI, és la base de l'algorisme ECDSA que es fa servir en la majoria de criptomonedes i que es tracta en l'assignatura de TBC.
- A FTI s'expliquen alguns atacs de mala implementació d'algorismes de signatura digital que poden donar lloc a robatoris de criptomonedes, temes que es tracten a l'assignatura de TBC.
- A FTI s'expliquen en detall el funcionament i les propietas de les funcions hash, que són crucials en la implementació i la seguretat de la tecnologia blockchain.
- L'últim tema d'FTI és una introducció a la tecnologia blockchain i a les criptomonedes. Un tast que serveix per donar una base inicial amb la qual després es treballarà a l'assignatura TBC.

Objectius

Els objectius d'aquesta assignatura són:

- Entendre els conceptes teòrics de la tecnologia blockchain
- Comprendre el funcionament de les criptomonedes

- Entendre com funcionen els Bitcoin, des d'un punt de vista tècnic
- Entendre el concepte d'smart contract.
- Entendre la diferència entre una blockchain basada en UTXO i una basada en comptes.
- Conèixer alguns del mecanismes d'escalabilitat de la tecnologia blockchain

Competències

- Adquirir hàbits de pensament.
- Adquirir hàbits de treball personal.
- Capacitat per a seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de la organització, amb els criteris de cost i qualitat identificats.
- Capacitat per concebre, redactar, organitzar, planificar, desenvolupar i signar projectes en l'àmbit de l'enginyeria informàtica que tinguin per objecte la concepció, el desenvolupament o l'explotació de sistemes, serveis i aplicacions informàtiques.
- Capacitat per dissenyar, desenvolupar, avaluar i assegurar l'accessibilitat, l'ergonomia, la usabilitat i la seguretat dels sistemes, serveis i aplicacions informàtiques, així com de la informació que gestionen.
- Capacitat per dissenyar, desenvolupar, seleccionar i avaluar aplicacions i sistemes informàtics, assegurant-ne la fiabilitat, la seguretat i la qualitat, d'acord amb els principis ètics i la legislació i la normativa vigents.

Resultats d'aprenentatge

1. Desenvolupar la capacitat d'anàlisi, síntesi i prospectiva.
2. Dissenyar les solucions informàtiques que permetin integrar a un sistema distribuït les necessitats d'accessibilitat i seguretat.
3. Dissenyar, desenvolupar, seleccionar i avaluar aplicacions, assegurant la seva fiabilitat i seguretat.
4. Identificar els principals atacs que pot rebre un sistema informàtic, així com els possibles mètodes de protecció, detecció i aplicació de polítiques de seguretat que permetin evitar el dany al sistema o minimitzar la seva repercussió.
5. Incorporar sistemes distribuits de tractament de la informació a una organització per a incrementar la capacitat operativa.
6. Treballar de manera autònoma.

Continguts

Els continguts d'aquesta assignatura són els següents:

1. Conceptes bàsics de tecnologia blockchain
2. Criptografia per a tecnologia blockchain
3. Bitcoin
4. Protocols de segona capa: Lightning Network
5. Ethereum
6. Altres blockchains

Metodologia

L'assignatura s'estructura en sessions de dues hores amb una formulació molt dinàmica on es demanarà als estudiants que intervinguin activament. La tipologia de sessions n'inclourà de contingut més teòric i d'altres més pràctic.

Les sessions de contingut més teòric es basaran en material que el professor prèviament farà arribar als estudiants a través del campus virtual. En base a aquest material, s'estructuraran dos tipologies diferents de sessions. D'una banda, sessions de preguntes i respostes on els estudiants formularan els dubtes que els hagin sorgit del treball previ sobre el material proporcionat. En aquestes sessions, el professor també interpel·larà als estudiants per fer aflorar els aspectes més rellevants del material que s'està treballant. D'altra banda, hi haurà sessions on els estudiants, en grups de dos, presentaran algun estudi més detallat d'algun dels temes tractats a l'assignatura.

Les sessions de contingut més pràctic inclouran tant la resolució de qüestions a mode d'exercicis com la realització de tasques més tècniques on es combinarà l'ús d'eines específiques de l'assignatura (wallets, exploradors de blockchain, compiladors d'smart contracts, etc.) amb el desenvolupament de funcions específiques utilitzant el llenguatge de programació Python.

Competències transversals. En aquesta assignatura es treballaran i avaluaran les següents competències transversals del Grau d'Enginyeria Informàtica:

- T01.02 - Desenvolupar la capacitat d'anàlisi, síntesi i prospectiva: aquesta competència es treballarà de forma més intensa en les sessions més teòriques on els estudiants hauran de demostrar la comprensió dels continguts proposats a través de les preguntes que el professor els proposarà durant les sessions de teoria. També es treballarà aquesta competència en els diferents treballs que els estudiants presentaran al llarg del curs.
- T02.01 Treballar de forma autònoma: aquesta es focalitza en aquelles activitats individuals, com ara la realització dels treballs pràctics que els estudiants faran al llarg del curs.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes pràctiques	25	1	2, 3, 5, 6
Classes teòriques	25	1	1, 4, 5
Tipus: Supervisades			
Tutories i consultes	10	0,4	1, 2, 3, 4, 5
Tipus: Autònomes			
Preparació de les classes pràctiques	25	1	1, 2, 3, 6
Preparació de les classes teòriques	37,5	1,5	1, 4, 5, 6

Avaluació

El model d'avaluació d'aquesta assignatura serà íntegrament d'avaluació continuada. Donat el dinamisme de la mateixa i la implicació que es demana als estudiants en totes les sessions de classe (tant les de caire més teòric com les més pràctiques) el professor tindrà múltiples elements per poder avaluar als alumnes. La participació activa en les classes preguntant dubtes al professor i responent dubtes dels altres estudiants o de

les qüestions del professor suposarà un 20% de la nota de l'assignatura. És per aquest motiu que l'assistència a classe d'aquesta assignatura és obligatòria.

Més enllà de l'avaluació en base a les aportacions en les classes, els estudiants també hauran de lliurar diferents treballs més pràctics que s'aniran proposant al llarg del curs al campus virtual de la UAB, lliuraments que complementaran les evidències d'avaluació de l'estudiant. Aquestes activitats més pràctiques suposaran un 50% de la nota de l'assignatura.

D'altra banda, la presentació del tema que els estudiants faran en les sessions teòriques de l'assignatura també formarà part de les evidències d'avaluació i suposarà un 30% de la nota de l'assignatura.

Per superar l'assignatura caldrà haver superat cada una de les activitats avaluables entenent que les activitats avaluables són: participació a classe, treballs pràctics i presentació. Cada un dels treballs pràctics s'hauran de superar per separat.

En cas de no superar algun dels treballs pràctics es podran recuperar tornant-los a presentar, si bé en aquest cas la nota màxima del treball recuperat que s'obtindrà serà un 5.

En cas de no superar el treballde presentació, caldrà recuperar-lo presentant una versió estesa del mateix treball que serà presentat oralment al professor de l'assignatura.

En cas de no superar l'avaluació de la participació a classe, aquesta no es podrà recuperar.

No es contempla cap mena de convalidació de cap de les activitats avaluables per als estudiants repetidors.

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, les irregularitats comeses per un estudiant que puguin conduir a una variació de la qualificació es qualificaran amb un zero (0). Les activitats d'avaluació qualificades d'aquesta forma i per aquest procediment no seran recuperables. Si és necessari superar qualsevol d'aquestes activitats d'avaluació per aprovar l'assignatura, aquesta assignatura quedarà suspesa directament, sense oportunitat de recuperar-la en el mateix curs. Aquestes irregularitats inclouen, entre d'altres:

- la còpia total o parcial d'una pràctica, informe, o qualsevol altra activitat d'avaluació;
- deixar copiar;
- presentar un treball de grup no fet íntegrament pels membres del grup (aplicat a tots els membres, no solament als que no han treballat);

  ús no autoritzat de la IA (p. ex, Copilot, ChatGPT o equivalents) per a resoldre exercicis, pràctiques i/o qualsevol altra activitat avaluable;
- presentar com a propis materials elaborats per un tercer, encara que siguin traduccions o adaptacions, i en general treballs amb elements no originals i exclusius de l'estudiant;

En resum: copiar, deixar copiar o plagiar (o l'intent de) en qualsevol de les activitats d'avaluació equival a un SUSPENS, no compensable i sense convalidacions de parts de l'assignatura en cursos posteriors.

Els alumnes que aconsegueixin el nombre mínim de punts per aprovar l'assignatura, però no hagin assolit la nota mínima en alguna de les activitats d'avaluació, seran avaluats amb una nota final de 4.5. En el cas que no s'hagi aprovat l'assignatura per la qualificació d'un zero d'una activitat per motiu de còpia, la nota final de l'assignatura serà un 3, fet que no permetrà compensar aquesta assignatura.

Finalment, obtindran la qualificació de "No Avaluable" aquells estudiants que no lliurin cap de les activitats pràctiques que es proposin. La participació en alguna d'aquestes activitats d'avaluació suposarà rebre una qualificació diferent de "No Avaluable".

No es farà cap activitat d'avaluació a cap alumne en un horari diferent de l'establert si no és que existeix una causa justificada, s'ha avisat amb anterioritat a l'activitat i el professor ha donat el seu consentiment. En qualsevol altre cas, si un alumne no ha assistit a una activitat, aquesta no es pot recuperar.

Pel que fa a les matrícules d'honor, aquestes es podran concedir a aquells estudiants que hagin superat l'assignatura amb una nota final igual o superior a 9. Donat que el nombre de matrícules d'honor no pot superar el 5% dels estudiants matriculats, es concediran als estudiants amb les notes més altes. En cas d'empat, es podrà requerir als estudiants que realitzin una prova oral per desempatar.

Aquesta assignatura no preveu el sistema d'avaluació única.

Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Activitats pràctiques	50	12,5	0,5	1, 2, 3, 4, 5, 6
Participació a classe	20	14	0,56	4
Presentació oral d'un tema	30	1	0,04	1, 2, 3, 4, 5, 6

Bibliografia

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016). ISBN: 978-0691171692
- Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media; 2nd Edition. (2017) ISBN: 978-1491954386
- Andreas M. Antonopoulos y Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media. (2018) ISBN: 978-1491971949
- C. Pérez Solà i J. Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: https://criptografia.cat/
- Kalle Rosenbaum, Grokking Bitcoin. Manning Publications (2019) ISBN 9781617294648
- Roger Wattenhofer. Blockchain Science: Distributed Ledger Technology. Inverted Forest Publishing; 3rd Edition (2019) ISBN: 978-1793471734
- Andreas Antonopoulos, Olaoluwa Osuntokun, René Pickhardt. Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. O'Reilly Media; 1st edition (January 4, 2022) ISBN: 978-1492054863

Programari

Les sessions de contingut més pràctic inclouran tant la resolució de qüestions a mode d'exercicis com la realització de tasques més tècniques on es combinarà l'ús d'eines específiques de l'assignatura (wallets, exploradors de blockchain, compiladors d'smart contracts, etc.) amb el desenvolupament de funcions específiques utilitzant el llenguatge de programació Python.