

Titulació	Tipus	Curs
Enginyeria Informàtica	OP	4

Professor/a de contacte

Nom : Jordi Herrera Joancomarti

Correu electrònic : jordi.herrera@uab.cat

Equip docent

Domènec Madrid Hernández

Ghazaleh Keshavarzkalhori

Idiomes dels grups

Podeu consultar aquesta informació al [final](#) del document.

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 propietats 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 dels mecanismes d'escalabilitat de la tecnologia blockchain

Resultats d'aprenentatge

1. 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.
2. Dissenyar, desenvolupar, seleccionar i avaluar aplicacions, assegurant la seva fiabilitat i seguretat.
3. Desenvolupar la capacitat d'anàlisi, síntesi i prospectiva.
4. Treballar de manera autònoma.
5. Incorporar sistemes distribuïts de tractament de la informació a una organització per a incrementar la capacitat operativa.
6. Dissenyar les solucions informàtiques que permetin integrar a un sistema distribuït les necessitats d'accessibilitat i seguretat.

Continguts

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

Activitats formatives i Metodologia

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

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. En aquestes sessions els estudiants hauran de portar el seu portàtil a l'aula.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, perquè l'alumnat completi les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura.

Avaluació

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	1
Presentació oral d'un tema	30	1	0,04	1, 2, 3, 4, 5, 6

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 caràcter 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, els estudiants (en grups de dues persones) hauran de preparar un treball de l'assignatura que presentaran en les sessions teòriques i que també formarà part de les evidències d'avaluació, amb un pes del 30% de la nota de l'assignatura.

Per superar l'assignatura caldrà haver superat cada una de les activitats avaluable, entenent que les activitats avaluable són: la participació a classe, les pràctiques i la presentació del treball.

Cada una de les pràctiques s'haurà de superar per separat. En cas de no superar alguna de les pràctiques, aquesta només es podrà recuperar en cas que la nota obtinguda hagi estat superior a 3,5 i caldrà tornar-la a presentar. En aquest cas, la nota màxima de la pràctica recuperada serà un 5. Si una de les pràctiques té una nota inferior a 3,5 ja no es podrà recuperar.

En cas de no superar el treball de presentació, aquest no es podrà recuperar.

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

Un cop avaluades cada una de les parts (participació a classe, pràctiques o presentació del treball), en cas que una no quedi aprovada encara hi haurà la possibilitat de superar l'assignatura per mitjà d'un examen final oral. Aquest examen final suposarà el 80% de la nota. El 20% de la nota de participació a classe continuarà essent la que s'ha obtingut al llarg del curs.

No es contempla cap mena de convalidació de cap de les activitats avaluable 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.

Aquesta assignatura estableix una política d'ús restringit de les tecnologies d'intel·ligència artificial (IA). Es permet l'ús de tecnologies d'Intel·ligència Artificial (IA) exclusivament en tasques de suport, com la cerca bibliogràfica o d'informació, la correcció de textos, les traduccions, o la consulta de documentació sobre funcions o llibreries de programari. Tanmateix, no està permès utilitzar la IA per generar íntegrament la solució d'una pràctica, ni per escriure funcions completes o fragments de codi substancials. L'estudiant haurà d'identificar clarament quines parts han estat generades amb aquesta tecnologia i especificar les eines emprades. La no transparència de l'ús de la IA en aquesta activitat avaluable es considerarà falta d'honestedat acadèmica i pot comportar una penalització parcial o total en la nota de l'activitat, o sancions majors en casos de gravetat.

Els alumnes que aconseguixin 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 deshonestedat acadèmica, 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. El protocol de "sol·licitud de reprogramació d'activitats d'avaluació" es troba disponible al web de l'Escola d'Enginyeria i és aplicable en els casos descrits als criteris i instruccions d'avaluació del centre.

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.

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; 3d Edition. (2023) ISBN: 978-1098150099
- 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.

Grups i idiomes de l'assignatura

La informació proporcionada és provisional fins al 30 de novembre.

A partir d'aquesta data, podreu consultar l'idioma de cada grup a través d'aquest [enllaç](#). Per accedir a la informació, caldrà introduir el CODI de l'assignatura

Tipus de docència	Grup	Idioma	Semestre	Torn
(PAUL) Pràctiques d'aula	450	Català	primer quadrimestre	matí-mixt