UNIVERSITEIT GENT

Studiefiche

Vanaf academiejaar 2020-2021

Blockchain: technologie en applicaties (E034150)

Wegens Covid19 kan mogelijk afgeweken worden van de onderwijs- en evaluatievormen. Dergelijke afwijkingen zullen via Ufora worden gecommuniceerd.

Cursusomvang (nominale waarden; effectieve waarden kunnen verschillen per opleiding)

Studiepunten	Studietijd	Contacturen
3.0	90 u	15.0 u

Aanbodsessies en werkvormen in academiejaar 2020-2021

A (semester 1)	Engels	Gent	microteaching	2.5 u
			hoorcollege	12.5 u
			groepswerk	1.25 u

Lesgevers in academiejaar 2020-2021

De Sutter, Bjorn	TW06	Verantwoordelijk lesgever

Aangeboden in onderstaande opleidingen in 2020-2021	stptn	aanbodsessie
Master of Science in de informatica	3	A
Master of Science in de ingenieurswetenschappen: computerwetenschappen	3	A
Master of Science in Computer Science Engineering	3	A
Uitwisselingsprogramma informatica (niveau master)	3	A

Onderwijstalen

Engels

Trefwoorden

blockchain, consensusmanagement, gedecentralizeerde registers, Bitcoin, Ethereum, smart contracts, attacks and defenses, cryptocurrencies

Situering

- Blockchaintechnologie, zoals die gebruikt wordt voor cryptomunten zoals Bitcoin and Ethereum, maar ook voor andere doeleinden, draagt het potentieel om een nieuwe ICT-revolutie teweeg te brengen, net zoals de vorige revoluties van internetconnectiviteit en het Internet of Things.
- In dit domein loopt de praktijk vandaag voor op de theorie. Systemen met blockchaintechnologie worden al ingezet, terwijl veel fundamentele vragen met betrekking tot privacy, schaalbaarheid, en beveiliging nog niet beantwoord zijn. Ondanks deze observatie en het gebrek aan theoretische fundamenten en modellen is het belangrijk dat afstuderende ingenieurs de kerntechnologie en de relevante concepten meester zijn, en het potentieel ervan onderkennen.
- Blockchaintechnologie is gerelateerd aan cryptografie (cryptografische primitieven vormen de kern van blockchainbeveiliging), aan gedistribueerde systemen (als een vorm van gedistribueerde registers waarvan de inhoud op een gedistribueerde manier gecontrolleerd wordt), en aan computerbeveiliging (aangezien het vaak gaat om het opbouwen van vertrouwen tussen elkaar niet vertrouwende partners).
- Dit opleidingsonderdeel met een focus op de onderliggende concepten en toepassingen van blockchaintechnologie is daarom complementair met de bestaande cursussen over informatiebeveiliging, parallel en gedistribueerd programmeren en rekenen, en softwarehacking- en protectie.

Inhoud

- Algemene introductie, waaronder:
  - basisconcepten: het probleem van de Byzantijnse generaals, publieke gedecentraliseerde transactieregisters, bewijs van werk/aandeel/capaciteit, eerlijke meerderheid, onveranderlijkheid, hashfuncties, Merklebomen, transactieblokken, blockchains, rollen en separatie in consensusmanagement;
  - types blockchains: met en zonder permissie;
  - gedistribueerde consensusmechanismes;

    - transparanties, censuur, anonimiteit, pseudonimiteit, niet-aaneensluitbaarheid, nul-kennisbewijzen.
- Bitcoin: Nakamotoconsensus, delvers, portefeuilles, addressen en andere datastructuren, hashpuzzels, langste-kettingregel, concrete implementaties en algoritmes, dubbel spenderen: aanvallen en verdedigingen, consensusmanagement, netwerk- en communicatiemanagement, roddelprotocol, verenigd delven, tools voor muntbeheer, gebruikerservaring en beveiliging, pseudonimiteit vs. anonimiteit.
- Alternatieve blockchaininfrastructuur en -consortia, register met permissies, legale vereisten en regulering, toegangscontrole.
- Data in blockchains: vertrouwde partijen, interplanetaire database, datavalidatie met behulp van orakels.
- Ethereum: slimme contracten, Ethereum virtuele machine, beveilingsproblemen van slimme contracten, programmeertalen ervoor
- Alternatieven om te delven: clouds, processor- en acceleratorarchitecturen, prestaties en energieconsumptie, schaalbaarheid, duurzaamheid, vertrouwde software (in enclaves), bewijs van nuttig geleverd werk, bewijs van verlopen tijd.
- Applicaties in diverse domeinen: energiemarkten; notariaat, kadaster en andere publieke diensten; medische dossiers; bewijzen van scholing; management van vliegtuigmaatschappijen - vluchten - passagiers - annulaties; Internet of Things; financiële producten; verzekeringen; productieketens; voedingsketens;

Begincompetenties

- De studenten worden verondersteld de inhoud van het vak Computerarchitectuur onder de knie te hebben.
- De studenten worden verondersteld de basiskennis uit de computerwetenschappen op het vlak van datastructuren, programmeertalen, computernetwerken, en besturingssystemen te beheersen.

Eindcompetenties

1. Diepgaand begrip van onderliggende concepten, opgeloste problemen, applicaties en open vragen van blockchains.
2. Kennis van de technologische fundamenten van blockchains.
3. Overzicht van alternatieve technologieën voor basiscomponenten van blockchains
4. Diepgaand begrip van mogelijke beveiligingsproblemen, aanvallen, en verdedigingstechnieken.
5. Inzicht in het potentieel van blockchaintechnologie tot disruptie in verschillende industrietakken, en voor nieuwe applicaties en businessmodellen.
6. Het kunnen onderscheiden van scenario's waarin blockchaintechnologie een belangrijke rol kan spelen en scenario's waarin dat allicht niet kan.

Creditcontractvoorwaarde

Toelating tot dit opleidingsonderdeel via creditcontract is mogelijk mits gunstige beoordeling van de competenties

Examencontractvoorwaarde

Dit opleidingsonderdeel kan niet via examencontract gevolgd worden

Didactische werkvormen

Groepswerk, hoorcollege, microteaching, online discussiegroep, zelfstandig werk

Toelichtingen bij de didactische werkvormen

- De lesgever neemt alle hoorcolleges voor zijn rekening. Als het aantal studenten dat de hoorcolleges wil bijwonen binnen mag in het toegewezen lokaal, dan gaan de hoorcolleges on campus door. Zoniet worden ze vervangen door live online lessen.
- Studenten zullen in kleine groepen actuele gevalstudies, beste praktijken, en de geavanceerde technische aspecten van blockchains bestuderen en daarover presentaties voorbereiden en daarmee les geven aan elkaar. De lesgever begeleidt hen bij de studie en de voorbereiding van de presentaties.
- Op Ufora krijgen de studenten kleine taken waarvoor ze zelfstandig allerlei bronnen moeten raadplegen.

Leermateriaal

- Dia's lessen (gratis)
- Bijkomende nota's en publicaties aan kopieerkost.

Referenties

- Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
- Een brede waaier aan online bronnen.

Vakinhoudelijke studiebegeleiding

- Online discussiefora.

- Feedback op online taken die zelfstandig opgelost worden en Q&A daarover in volgend hoorcollege.
- Contact via chat, mail en opendeurbeleid.
- Mogelijkheid tot vragen stellen voor en na de hoorcolleges.
- Begeleiding door de docent van het groepswerk in meerdere bijeenkomsten waarin hun vooruitgang besproken wordt.

Evaluatiemomenten

periodegebonden en niet-periodegebonden evaluatie

Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode

Schriftelijk examen met open vragen

Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Schriftelijk examen met open vragen

Evaluatievormen bij niet-periodegebonden evaluatie

Mondeling examen, peer-evaluatie

Tweede examenkans in geval van niet-periodegebonden evaluatie

Examen in de tweede examenperiode is enkel mogelijk in gewijzigde vorm

Toelichtingen bij de evaluatievormen

Niet-periodegebonden evaluatie: peer-evaluatie, mondeling examen: studentenpresentaties
Voor de niet-periodegebonden evaluatie worden de presentaties van studenten over de opgegeven onderwerpen beoordeeld. Zowel de kwaliteit als de inhoud van de presentaties worden daarvoor in rekening gebracht. Peer-evaluatie wordt als extra input gebruikt om de finale score te bepalen.

Eindscoreberekening

De niet-periodegebonden evaluatie telt mee voor 1/5 van de punten. Studenten dienen 10/20 te halen voor zowel de niet-periodegebonden evaluatie als voor de periodegebonden evaluatie om te kunnen slagen voor dit vak. Indien de berekende totaalscore in dit geval toch een cijfer van 10/20 of meer zou zijn, dan wordt dit teruggebracht tot een totaal van 9/20.

Faciliteiten voor werkstudenten

Mogelijkheid tot vrijstelling van aanwezigheid met vervangende opdracht na overleg met verantwoordelijke lesgever. Mogelijkheid tot mondeling examen met schriftelijke voorbereiding op ander tijdstip binnen het academiejaar. Mogelijkheid tot feedback na afspraak tijdens en na kantooruren.