UNIVERSITEIT GENT

Studiefiche

Vanaf academiejaar 2024-2025

Blockchain: technologie en applicaties (E034150)

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

Studiepunten 3.0 **Studietijd 90 u**

Aanbodsessies en werkvormen in academiejaar 2024-2025

A (semester 1)	Engels	Gent	groepswerk
			peer teaching
			hoorcollege

Lesgevers in academiejaar 2024-2025

De Sutter, Bjorn	TWO6	Verantwoordelijk lesgever

Aangeboden in onderstaande opleidingen in 2024-2025	**stptn**	**aanbodsessie**
Master of Science in Computer Science Engineering	3	A
Master of Science in de industriële wetenschappen: informatica	3	A
Master of Science in de informatica	3	A
Uitwisselingsprogramma industriële wetenschappen: informatica	3	A
Uitwisselingsprogramma informatica (niveau master)	3	A

Onderwijstalen

Engels

Trefwoorden

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

Situering

- Blockchaintechnologie, zoals die gebruikt wordt voor cryptomunten zoals Bitcoin en voor gedistribueerde smart contract computing platformen zoals Ethereum draagt het potentieel om een nieuwe ICT-revolutie teweeg te brengen, net zoals de vorige revoluties van internetconnectiviteit en het Internet of Things. Het is belangrijk dat afstuderende ingenieurs en informatica 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, databanken, parallel en gedistribueerd programmeren en rekenen, en softwarehacking- en protectie.

Inhoud

- Algemene introductie, waaronder cryptografische primitieven, eerste cryptomunten, cryptografische puzzels; eigenschappen van munteenheden, bijkomende eigenschappen van gedecentralizeerde munten; opslaan van transacties in een blockchain; consensus, bewijs van werk, delven; onveranderlijkheid, eerlijke meerderheid, een korte geschiedenis van Bitcoin, problemen met Bitcoin en alternatieve munten; slimme contracten als een uitbreiding van cryptomunten.
- Bitcoin kerntechnologie: gebruikte hashfunctie, Merklebomen, blokheaders en -ketting, moeilijkheid blokken, digitale handtekeningen, ECDSA, generatie adressen, UTXO, transacties, Bitcoin scripts, proof of burn, PKPKH vs P2SH, multihandtekeningen, praktische

betalingen (groene adressen, micro-betalingen, in pand geven), locktijd, gedistribueerd impliciet consensusalgoritme, aansporingen voor delvers (vergelijking met speltheorie en fouttolerantie), peer-to-peernetwerk, replace-by-vergoeding, lichtgewicht knopen, Bitcoin verbetervoorstellen.
- Alternatieve cryptomunten en betalingssystemen: altcoins, schaalbaarheidsoplossingen: segregated witness, lightning network, sharding; initial coin offerings
- Dagelijks gebruik van cryptomunten: opslag van sleutels, koude en warme opslag, het delen en opsplitsen van sleutels, beurzen, hiërarchische deterministische portefeuilles, transactiekosten, vergoedingen verhogen.
- Bitcoin delven en bewijs van werk: taken van de delver, moeilijkheid van het delven, creatie van blokken, hardware om te delven, energieverbruik en duurzaamheid, gezamenlijk delven, betalingsschema's daarvoor.
- Aanvallen op consensusalgoritmes met bewijs van werk: dubbel uitgeven, censuur, zelfzuchtig delven, koppig delven, cannibalisatie, eclipsaanvallen, mogelijke verdedingen.
- Ethereum: ontwerpdoelstellingen, technische eigenschappen, types rekeningen, netwerktoestand, slimme contracten, deterministische terminatie, transacties, ethers en brandstof, Ethereum Virtual Machine, het programmeren van slimme contracten, Solidity, voorbeeldcontracten, kwetsbaarheden en exploits; basistoepassingen: slimme bezittingen, publieke registers, bewijs van bestaan, aanmoedigingen en crowdfunding, voorspellingsmarkten; beperkingen, wanneer blockchains te gebruiken.
- Alternatieve consensusmechanismes: bewijs van belang, kettinggebaseerd bewijs van belang, Byzantine fouttolerantie, niets-te-verliezen-probleem en mogelijke oplossingen (slashing); aanvallen: op finaliteit, censuur, liveness denial, stake grinding, data-onbeschikbaarheid, omkoping, crypto-economische veiligheidsmargel; alternatieve mechanismes: bewijs van nuttig werk, van gewachte tijd, van capaciteit, van activiteit; gedelegeerd bewijs van belang, gedelegeerde Byzantine fouttolerantie; Peercoin, Ethereum Slasher & Casper.
- Anonimiteit: basisbegrippen, noodzaak, analyse van transactiegrafen, transactieclustering, de-anonimizering, spooranalyse, mixing (centraal en decentraal), meer privacygerichte altcoins (Zcash, Monero, Dash), nul-kennisbewijzen, verhouding tot andere privacygerelateerde technologieën (TOR, VPN).
- Blockchain voor ondernemingen: Hyperledger, Consensys, Enterprise Ethereum Alliance
- Blockchaintoepassingen in de publieke sector: NGOs, internationale instellingen, self-sovereign identity, kadasters
- Blockchaintoepassingen in de private sector: verzekeringen, bevoorradings- en verwerkingsketens, financiële instellingen, auto-industrie, gedecentralizeerde marktplaatsen, gedecentraliseerde autonome organizaties.

Begincompetenties

De studenten worden verondersteld de basiskennis uit de computerwetenschappen op het vlak van datastructuren, programmeertalen en computernetwerken te beheersen.

Eindcompetenties

1 Diepgaand begrip van onderliggende concepten, opgeloste problemen, applicaties en open vragen van blockchains, inclusief gedecentraliseerde en gedistribueerde boekhouding van transacties en consensusmechanismes.
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, Zelfstandig werk, Peer teaching

Toelichtingen bij de didactische werkvormen

- De lesgever neemt alle hoorcolleges voor zijn rekening, die normaal gezien altijd op

de campus doorgaan.
- 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 op de campus. De lesgever begeleidt hen bij de studie en de voorbereiding van de presentaties.
- Op Ufora krijgen de studenten individueel wekelijks kleine taken waarvoor ze zelfstandig allerlei bronnen moeten raadplegen en op korte, eenvoudige vragen korte antwoorden moeten geven.

Studiemateriaal

Type: Slides

Naam: Blockchain: technologie en applicaties
Richtprijs: Gratis of betaald door opleiding
Optioneel: nee
Taal : Engels
Aantal slides : 318
Oudst bruikbare editie : 2023-2024
Beschikbaar op Ufora : Ja
Online beschikbaar : Ja
Beschikbaar in de bibliotheek : Nee
Beschikbaar via studentenvereniging : Nee
Bijkomende info: Deze slides worden beschikbaar gesteld in PDF vorm met uitgebreide notities. De slides samen met de notities vormen de syllabus van dit vak.

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

Schriftelijke evaluatie met open vragen

Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Schriftelijke evaluatie met open vragen

Evaluatievormen bij niet-periodegebonden evaluatie

Mondelinge evaluatie, Participatie, Peer en/of self assessment, Werkstuk

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 presentaties
De studenten bestuderen in groep een concreet opgegeven onderwerp uit het domein, geven daarover een presentatie aan hun medestudenten, en bezorgen notities bij de presentatieslides zodat de medestudenten de belangrijkste inhoud achteraf kunnen studeren. Zowel de kwaliteit van de gegeven presentatie (vorm, inhoud, accuraatheid, enthousiasme, stijl, ...) als die van de notities (accuraatheid, bondigheid, focus, ...) worden in overweging genomen om de punten te bepalen, alsook de inzet en hoe goed de studenten de nodige kennis opgedaan hebben. Dat wordt geëvalueerd tijdens de begeleidende contactmomenten, en tijdens en na de presentatie. Er wordt een peer assessment gebruikt om de samenwerking binnen groepen te evalueren, alsook de kwaliteit van de gegeven presentaties. De docent houdt bij de finale kwotering rekening met het peer assessment.

Niet-periodegebonden evaluatie: online participatie

Wekelijks krijgen de studenten kleine individuele opdrachten op het online leerplatform waarvoor ze online bronnen moeten raadplegen, zodat ze eenvoudige vragen kort kunnen beantwoorden. De studenten worden hier vooral op participatie beoordeeld: het volstaat dat uit de ingediende antwoorden blijkt dat de studenten de nodige moeite gedaan hebben.

Tweede kans niet-periodegebonden evaluatie: paper

De student krijgt een individuele opdracht om over een concreet opgegeven onderwerk uit het domein een paper te schrijven en een presentatie te geven, en daarvoor het nodige studiewerk te verrichten. Daarbij krijgt de student beperkte begeleiding. Zowel de kwaliteit van de gegeven presentatie (vorm, inhoud, accuraatheid, enthousiasme, stijl, ...) als die van het paper (accuraatheid, bondigheid, focus, ...) worden in overweging genomen om de punten te bepalen.

Tweede kans niet-periodegebonden evaluatie: online participatie

De student krijgt aan aantal kleine individuele opdrachten op het online leerplatform waarvoor die online bronnen moet raadplegen, zodat die eenvoudige vragen kort kan beantwoorden. De student wordt hier vooral op participatie beoordeeld: het volstaat dat uit de ingediende antwoorden blijkt dat de student de nodige moeite gedaan heeft.

Periodegebonden evaluatie:

Het betreft een theorie-examen met gesloten boek, met grotendeels open vragen, al kunnen er ook gesloten vragen in opduiken.

Eindscoreberekening

De niet-periodegebonden evaluatie telt mee voor 20% van de punten, waarvan 5% voor de online participatie en 15% voor de peer presentaties.
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.