GHENT UNIVERSITY

Course Specifications

Valid as from the academic year 2023-2024

Blockchain Technologies and Applications (E034150)

Course size *(nominal values; actual values may depend on programme)*

Credits 3.0 **Study time 90 h**

Course offerings and teaching methods in academic year 2023-2024

A (semester 1)	English	Gent	group work
			lecture
			peer teaching

Lecturers in academic year 2023-2024

De Sutter, Bjorn	TWO6	lecturer-in-charge

Offered in the following programmes in 2023-2024	crdts	offering
Master of Science in Computer Science	3	A
Master of Science in Computer Science Engineering	3	A
Master of Science in Information Engineering Technology	3	A
Exchange Programme in Computer Science (master's level)	3	A
Exchange Programme Information Engineering Technology	3	A

Teaching languages

English

Keywords

blockchain, consensus management, decentralized ledgers, Bitcoin, Ethereum, smart contracts, attacks and defenses, cryptocurrencies, anonimiteit

Position of the course

- Blockchain technology, as used for cryptocurrencies such as Bitcoin and distributed smart contract computing such as Ethereum has the potential to facilitate the next wave of ICT innovation, following the previous waves of Internet connectivity and the Internet of Things. it is important that graduating students know the core technology and concepts, as well as their potential.
- Blockchain technology relates to cryptography (as cryptographic primitives are used extensively to secure the blockchains), to distributed computing (as a blockchain is a distributed ledger and blocks are added to the chain and validated in a distributed manner), and computer security, as it inherently evolves around building trust among untrusting partners.
- A course focused on the fundamental concepts technologies underlying blockchains, and on the applications thereof can hence complement the existing courses on information security, databanks, parallel and distributed programming and computing, and software hacking and protection.

Contents

- General introduction and overview, including cryptographic primitives, first cryptocurrencies, cryptographic puzzles; properties of currencies, additional properties of electronic decentralized currencies vs. centralized fiat financial institutions; record keeping in a blockchain; concensus, proof-of-work, mining; immutability, honest majority; short history of bitcoin; bitcoin issues and alternative coins; smart contracts as an extension of cryptocurrencies.
- Bitcoin core technology: used hash function, Merkle trees, blockheaders and chaining, block difficulty, digital signatures, ECDSA, address generation, UTXO, transactions, bitcoin scripts, proof of burn, P2PKH vs P2SH, multisignatures, practical payments (escrow transactions, green addresses, micro-payments), lock time, distributed implicit concensus algoritm,

incentives for miners (comparison to game theory and fault tolerance), peer-to-peer network, replacy-by-fee, lightweight nodes, bitcoin improvement proposals
- Alternative cryptocurrencies and payment systems: altcoins, scalability solutions: segregated witness, lightning network, sharding; initial coin offerings
- Cryptocurrency day-to-day use: key storage alternatives, hot & cold storage, splitting and sharing keys, online wallets, exchanges, hierarchically deterministic wallets, transaction fees, fee bumping
- Bitcoin mining and proof of work: miner's tasks, mining difficulty, block creation, mining hardware, energy and sustainability, pooled mining, pool payment schemes
- Attacks on proof-of-work consensus algorithms: double spending attacks, censorship attacks, selfish mining, stubborn mining, pool cannibalization, eclipse attacks, possible defenses
- Ethereum: design goals, main technical features, types of accounts, network state, smart contracts, deterministic termination, transactions, ethers and gas, network state machine, Ethereum virtual machine, smart contract programming, Solidity, example contracts, vulnerabilities and exploits, basic smart contract use cases: smart assets, public registries, proof-of-existence, incentivization & crowdfunding, prediction markets; limitations; when to consider using blockchains
- Alternative consensus mechanism: Proof of stake, chain-based PoS, Byzantine Fault Tolerance PoS, Nothing at stake problem and potential solutions (slashing), attacks: attack on finality, liveness denial attacks, censorship attacks, stake grinding attacks, data unavailability, bribing attacks; cryptoeconomic security margin, alternative algorithms: proof of useful work, proof of elapsed time, proof of capacity, proof of activity, delegated proof of stake, delegated Byzantine Fault Tolerance; Peercoin, Ethereum Slasher & Casper
- Anonymity: definition of fundamental concepts, raison d'être, transaction graph analysis, transaction clustering, de-anonymization, taint analysis, mixing, centralized and decentralized mixers, privacy sensitive altcoins (Zcash, Monero, Dash), zero-knowledge proofs, relation to other anonymization technology (TOR, VPN)
- Enterprise blockchain: Hyperledger, Consensys, Enterprise Ethereum Alliance
- Public sector blockchain applications: use in NGOs and world-governing bodies; self-sovereign identity, land registry platforms
- Private sector blockchain applications: insurance, supply chain tracking, fintech, automotive, decentralized marketplaces, decentralized autonomous organizations

Initial competences

A basic understanding of data structures, programming languages and computer networks is expected.

Final competences

1 Deep understanding of underlying concepts, problems solved, applications, and open issues of blockchains, including decentralized and distributed ledgers of transactions as well as consensus mechanisms.
2 Understanding technological foundations of blockchains.
3 Overview of alternative technologies for basic components of blockchains.
4 Deep understanding of potential security issues, attacks, and defenses.
5 Understanding potential of blockchains to disrupt industries and to drive new applications and business models.
6 Differentiate scenarios that cannot benefit from blockchain technology (against the hype) from those that can.

Conditions for credit contract

Access to this course unit via a credit contract is determined after successful competences assessment

Conditions for exam contract

This course unit cannot be taken via an exam contract

Teaching methods

Group work, Lecture, Independent work, Peer teaching

Extra information on the teaching methods

- Core material will be presented in lectures by the lecturer on campus.
- In small groups, students will study current use cases, best practices, and advanced technical aspects of block chains and present that to each other as microteaching, i.e., as short peer presentations on campus. The lecturer advises them during the studying and the preparation of the presentation.
- On Ufora, the students are weekly given small individual assignments for which they have to consult sources of information on their own, and answer short, simple questions with short

answers.

Learning materials and price

- Lecture slides (free)
- Additional notes & papers at copying cost

References

- Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
- A myriad of online sources.

Course content-related study coaching

- Online discussion forum
- Feedback on online assignments and Q&A about them in next lecture.
- Contact via chat, mail and an open door policy.
- Question time before and after each lecture.
- Lecturer advises student group work in preparation of microteaching, meeting multiple times to discuss their progress.

Assessment moments

end-of-term and continuous assessment

Examination methods in case of periodic assessment during the first examination period

Written assessment with open-ended questions

Examination methods in case of periodic assessment during the second examination period

Written assessment with open-ended questions

Examination methods in case of permanent assessment

Oral assessment, Participation, Peer and/or self assessment, Assignment

Possibilities of retake in case of permanent assessment

examination during the second examination period is possible in modified form

Extra information on the examination methods

Permanent evaluation: peer presentations
The students study in group a concrete given topic from the domain, give a presentation about it to their fellow students, and provide notes to the presentation slides so that the fellow students can study the main content afterwards. Both the quality of the given presentation (form, content, accuracy, enthusiasm, style, ...) and that of the notes (accuracy, conciseness, focus, ...) are taken into account to determine the points, as well as the commitment and how well the students have acquired the necessary knowledge. This is evaluated during the supervisory contact moments, and during and after the presentation. Peer assessment is used to evaluate cooperation within groups, as well as the quality of the presentations given. The teacher takes the peer assessment into account in the final grading.
Permanent evaluation: online participation
Weekly, students are given small individual assignments on the online learning platform that require them to consult online resources to briefly answer simple questions. The students are assessed here mainly on participation: it is enough that the submitted answers show that the students have made the necessary effort.
Second chance permanent evaluation: paper
The student will be given an individual assignment to write a paper and give a presentation on a concrete specified sub-work from the domain, and to do the necessary coursework for this. The student will receive limited guidance. Both the quality of the presentation (form, content, accuracy, enthusiasm, style, ...) and that of the paper (accuracy, conciseness, focus, ...) are taken into consideration to determine the points.
Second chance permanent evaluation: online participation
The student is given a number of small individual assignments on the online learning platform for which he must consult online sources, so that he can answer simple questions briefly. The student is mainly assessed on participation: it is sufficient that the submitted answers show that the student has made the necessary effort.
Periodic evaluation:
Theoretic exam with closed book, mostly with open questions but more closed questions can also occur.

Calculation of the examination mark

The permanent evaluation determines 20% of the total mark, of which 5% for the online participation, and 15% for the peer presentations.
Students can only pass the course if they achieve at least 10/20 for the permanent evaluation and 10/20 for the end-of-term exam. In case this requirement is not met, but the computed weighted score is 10/20 or more, the final score is reduced to 9/20.

Facilities for Working Students

Option to be freed from presence in labs with alternative assignment after consultation with the responsible teacher. Option for oral exam with written preparation at another time in the academic year. Option for feedback by appointment during and after business hours.