STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Blokų grandinių technologijos	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantys: prof. dr. Remigijus Paulavičius dr. Ernestas Filatovas	Matematikos ir informatikos fakultetas Duomenų mokslo ir skaitmeninių technologijų institutas

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Pasirenkamas

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	3 semestras	Lietuvių/Anglų

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Procedūrinis programavimas, Objektinis programavimas, Algoritmai ir duomenų struktūros, Duomenų bazių valdymo sistemos	**Gretutiniai reikalavimai (jei yra):**

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	133	64	69

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos

Modulio tikslas – įsigilinti į blokų grandinių technologijos (angl. *blockchain*) pagrindus ir veikimo principus bei taikyti juos realizuojant „blockchain“ paremtus sprendimus.

Studijų programos bendrosios kompetencijos (BK):
- Asmeniniai įgūdžiai (**BK1**).
- Žinios ir supratimas (**BK2**).

Studijų programos dalykinės kompetencijos (DK):
- Sprendimų analizė (**DK3**).
- Sprendimų projektavimas ir įgyvendinimas (**DK4**).
- Technologijų taikymas (**DK5**).
- Tyrimai ir duomenų analitika (**DK6**).

Dalyko (modulio) studijų siekiniai	Studijų metodai	Vertinimo metodai
Gebės suprasti blokų grandinių („blockchain“) koncepciją.	Paskaitos, probleminis dėstymas, grupės diskusija, atvejų analizė, pavyzdžių analizė, savarankiškas darbas, konsultacijos, laboratoriniai darbai.	Laboratorinių darbų atlikimas bei rezultatų gynimas, egzaminas raštu (atvirojo, pusiau atvirojo bei uždarojo tipo klausimai ir užduotys).
Gebės taikyti blokų grandinių veikimo principus decentralizuotose P2P srityse.		
Gebės planuoti ir atlikti tiriamojo pobūdžio „blockchain“ eksperimentus, vertinti rezultatus, jais remiantis daryti išvadas.		
Gebės parinkti efektyvius „blockchain“ tipus priklausomai nuo taikymų srities ir/ar uždavinio specifikos, pritaikyti sistemų projektavimo žinias realizuojant „blockchain“ paremtus sprendimus.		

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. **Įvadas į kriptografiją.** Kriptografinės maišos (*hash*) funkcijos. Maišos rodyklės ir duomenų struktūros: *Merkle tree*. Skaitmeniniai parašai: privatusis ir viešasis raktai.	6				4		10	6	Literatūros analizė, pratybos ir laboratoriniai darbai: įvairių tipų

2. **Blockchain pagrindai**. Blockchain kilmė ir atsiradimo priežastys. Dabartinių transakcijų (sandorių) sistemų trūkumai. Viešas transakcijų žurnalas. *Bitcoin*. „Blockchain“ taikymai: finansai, valdymas, logistika, sveikatos priežiūra, daiktų internetas.	4				2		6	4	„blockchain“ testavimas ir jų modifikavimas; išmaniųjų sutarčių ir decentralizuotų aplikacijų kūrimas.
3. **Kaip veikia „blockchain“ technologija?** Bloko struktūra. Blokų įtraukimas į „blockchain“. Konsensuso algoritmai: *Proof-of-Work, Proof-of-Stake, Byzantine Fault Tolerance, Directed Acyclic Graphs* ir kt. Kasyba: mazgai, sudėtingumas, algoritmai, aparatūrinė įranga ir pan. „Blockchain“ išsišakojimai. Saugumas. Privatieji ir viešieji „blockchain“. Bitcoin tipo „blockchain“ tinklo programavimas.	8				8		16	16	
4. **Viešojo tipo „blockchain“ realizacijos ir taikymai.** Išmaniosios sutartys (*Smart Contracts*). Decentralizuotos aplikacijos kūrimas *Ethereum* „blockchain“ tinkle. *Ethereum* testavimo tinklai. *Ethereum* tinklo žetonai (*tokens*), nepakeičiami žetonai (*non-fungible tokens*, NFT), decentralizuoti finansai (*decentralized finance*, DeFi), Web3.	8				10		18	20	
5. **Konsorciomo tipo „blockchain“ realizacijos ir taikymai.** „*Hyperledger: Linux Foundation*“ tipo „blockchain“ tinklai. *Hyperledger Fabric* tinklo paleidimas. Decentralizuotos aplikacijos kūrimas *Hyperledger Fabric* tinkle.	6				8		14	13	
6. **Pasiruošimas egzaminui ir egzamino laikymas**.								10	
Iš viso	**32**				**32**		**64**	**69**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Pirmasis laboratorinis darbas	20	Semestro metu	Studentams skiriamos užduotys, apimančios 1 temą. Maksimalus įvertis už puikiai atliktas užduotis yra 10 balų (atitinka 20 % bendrojo įvertinimo). Skiriami papildomi balai (iki 20 % maksimalaus įvertinimo) už papildomas užduotis, o taip pat ir kai užduotys atsiskaitomos anksčiau nurodytų terminų.
Antrasis laboratorinis darbas	20	Semestro metu	Studentams skiriamos užduotys, apimančios 2-3 temas: *Bitcoin* tipo „blockchain“ tinklo programavimą ir informacijos iš *Bitcoin* tinklo išgavimą bei interpretavimą programiniu būdu. Maksimalus įvertis už puikiai atliktas užduotis yra 10 balų (atitinka 20 % bendrojo įvertinimo). Skiriami papildomi balai (iki 20 % maksimalaus įvertinimo) už papildomas užduotis, o taip pat ir kai užduotys atsiskaitomos anksčiau nurodytų terminų.
Trečiasis laboratorinis darbas	30	Semestro metu	Studentams skiriamos užduotys, apimančios 4 temą: decentralizuotos aplikacijos kūrimas *Ethereum* „blockchain“ tinkle. Maksimalus įvertis už puikiai atliktas užduotis yra 10 balų (atitinka 30 % bendrojo įvertinimo). Skiriami papildomi balai (iki 30 % maksimalaus įvertinimo) už papildomas užduotis, o taip pat ir kai užduotys atsiskaitomos anksčiau nurodytų terminų.
Egzaminas (raštu)	30	Egzaminų sesijos metu	Egzaminą laikyti leidžiama semestro metu surinkus ne mažiau 50 % laboratoriniams darbams skirtojo įverčio ($\geq$ 3,5). Egzamino metu galima surinkti iki 10 balų, kurie atitinka 30 % galutinio įvertinimo. Egzamino metu studentas turi pateikti praktinį pateiktos užduoties sprendimą, motyvuojant naudojamų priemonių efektyvumą, bei analizuojant alternatyvius užduoties sprendimo būdus. Egzaminas taip pat gali būti laikomas eksternu, kai už atliktus laboratorinius darbus surinkta ne mažiau 50 % laboratoriniams darbams skirtojo įverčio.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privaloma literatūra				
Imran Bashir	2023	Mastering Blockchain:Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3	4rd Edition	Packt, https://www.packtpub.com/product/mastering-blockchain-fourth-edition/9781803241067
Andreas Antonopoulos	2023	Mastering Bitcoin: Programming the Open Blockchain	3rd Edition	O‘Reilly, https://github.com/bitcoinbook/bitcoinbook
Andreas Antonopoulos, Gavin Wood	2018	Mastering Ethereum: Building Smart Contracts and Dapps	1st Edition	O'Reilly, https://github.com/ethereumbook/ethereumbook

Matt Zand, Xun Wu, Mark Anthony Morris	2021	Hands-On Smart Contract Development with Hyperledger Fabric V2	1st Edition	O'Reilly, https://www.oreilly.com/library/view/hands-on-smart-contract/9781492086116/
Nakamoto, Satoshi	2008	Bitcoin: A peer-to-peer electronic cash system		https://bitcoin.org/bitcoin.pdf
Papildoma literatūra				
Ferguson, Niels, Bruce Schneier, Tadayoshi Kohno	2012	Cryptography engineering: design principles and practical applications		Wiley Publishing
Coursera	2019	Blockchain Specialization		https://www.coursera.org/specializations/blockchain#courses

COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
Blockchain Technologies	

Lecturer(s)	Department(s) where the course unit (module) is delivered
Coordinator: Prof. Dr. Remigijus Paulavičius, Dr. Ernestas Filatovas **Other(s):**	Faculty of Mathematics and Informatics Institute of Data Science and Digital Technologies

Study cycle	Type of the course unit (module)
First	Optional

Mode of delivery	Period when the course unit (module) is delivered	Language(s) of instruction
Face-to-face	3rd semester	Lithuanian

Requirements for students	
Prerequisites: Procedural programming, Object Oriented Programming, Algorithms and Data Structures, Database Management Systems	**Additional requirements (if any):**

Course (module) volume in credits	Total student's workload	Contact hours	Self-study hours
5	133	64	69

Purpose of the course unit (module): programme competences to be developed

The purpose of the course is to teach blockchain principles and techniques and apply them for real-world blockchain-based solutions.

Common study program competencies:

- Personal skills (**BK1**).
- Knowledge and understanding (**BK2**).

Specific study program competencies:

- Solution analysis (**DK3**).
- Solution design and implementation (**DK4**).
- Technology application (**DK5**).
- Research and data analytics (**DK6**).

Learning outcomes of the course unit (module)	Teaching and learning methods	Assessment methods
Ability to comprehend blockchain concept.	Lectures, working in a group, group discussion, case studies, individual work, consultations, laboratory works, learning through dedicated web pages.	Assessment of laboratory works, written exam (open, semi-open and closed questions and tasks).
Ability to apply blockchain principles for decentralized P2P networks.		
Ability to design and implement blockchain-based solutions, to evaluate the obtained results, and to draw conclusions.		
Ability to select and apply appropriate blockchain system depending on the application and/or problem specifics, apply system development skills to blockchain-based solutions.		

Content: breakdown of the topics	Contact hours							Self-study work: time and assignments	
	Lectures	Tutorials	Seminars	Exercises	Laboratory work	Internship/work placement	**Contact hours**	**Self-study hours**	**Assignments**
1. **Introduction into cryptography.** Hash functions. Hash pointers and data structures: *Merkle tree*. Digital signatures: private and public keys.	6				4		10	6	Analysis of the literature, exercises and laboratory works: testing and

2. **Blockchain fundamentals.** Origin of the blockchain. Drawbacks of the current transactions systems. Ledger. Bitcoin. Blockchain applications: finance, logistics, health, Internet-of-Things.	4				2		6	4	modifying different types of blockchains; developing smart contracts and decentralized applications.
3. **How blockchain technology works?** The structure of the block. Connecting blocks. Consensus algorithms: *Proof-of-Work, Proof-of-Stake, Byzantine Fault Tolerance, Directed Acyclic Graphs* and others. Mining: nodes, complexity, algorithms, hardware. Blockchain forks. Smart contracts. Security. Private and public blockchains. Development of the Bitcoin-type blockchain.	8				8		16	16	
4. **Public blockchain implementations and applications**. Smart Contracts. Building a decentralized application on the Ethereum blockchain. Ethereum test networks. Ethereum network tokens, non-fungible tokens (NFTs), decentralized finance (DeFi), Web3.	8				10		18	20	
5. **Implementations and applications of the consortium-type blockchain**. Hyperledger: Linux Foundation type blockchain networks. Hyperledger Fabric network. Building a decentralized application on the Hyperledger Fabric.	6				8		14	13	
6. **Preparation for the exam and taking the exam**.								10	
Total	**32**				**32**		**64**	**69**	

Assessment strategy	**Weight, %**	**Deadline**	**Assessment criteria**
The first laboratory work	20	During the semester	Students are given assignments covering Topic 1. The maximum score for the assignments is 10 points (equivalent to 20% of the overall mark). Additional points (up to 20% of the maximum mark) are awarded for additional assignments, as well as when assignments are submitted before the specified deadlines.
The second laboratory work	20	During the semester	Students are given assignments covering Topics 2 and 3: programming a Bitcoin-like blockchain network and extracting and interpreting information from the Bitcoin network programmatically. The maximum score for the assignments is 10 points (equivalent to 20% of the overall mark). Additional points (up to 20 % of the maximum mark) will be awarded for additional assignments, as well as when assignments are submitted before the specified deadlines.
The third laboratory work	30	During the semester	Students are given assignments covering Topic 4: Developing a decentralized application on the Ethereum blockchain. The maximum score for the assignments is 10 points (equivalent to 30% of the overall mark). Additional points (up to 30 % of the maximum mark) will be awarded for additional assignments, as well as when assignments are submitted before the specified deadlines.
Written examination	30	During the exam session	The exam is allowed to be taken with a score of at least 50% (≥3.5) of the grade given for the laboratory work during the semester. Up to 10 points may be obtained in the examination, corresponding to 30% of the final mark. In the examination, the student must provide a practical solution to the problem presented, motivating the effectiveness of the tools used and analyzing alternative solutions to the problem. The examination may also be taken externally when at least 50 % of the marks awarded for the laboratory work have been obtained.

Author	**Year of publication**	**Title**	**Issue of a periodical or volume of a publication**	**Publishing place and house or web link**
Compulsory reading				
Imran Bashir	2023	Mastering Blockchain:Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3	4rd Edition	Packt, https://www.packtpub.com/product/mastering-blockchain-fourth-edition/9781803241067
Andreas Antonopoulos	2023	Mastering Bitcoin: Programming the Open Blockchain	3rd Edition	O'Reilly, https://github.com/bitcoinbook/bitcoinbook
Andreas Antonopoulos, Gavin Wood	2018	Mastering Ethereum: Building Smart Contracts and Dapps	1st Edition	O'Reilly, https://github.com/ethereumbook/ethereumbook

Matt Zand, Xun Wu, Mark Anthony Morris	2021	Hands-On Smart Contract Development with Hyperledger Fabric V2	1st Edition	O'Reilly, https://www.oreilly.com/library/view/hands-on-smart-contract/9781492086116/
Nakamoto, Satoshi	2008	Bitcoin: A peer-to-peer electronic cash system		https://bitcoin.org/bitcoin.pdf
Optional reading				
Ferguson, Niels, Bruce Schneier, Tadayoshi Kohno	2012	Cryptography engineering: design principles and practical applications		Wiley Publishing
Coursera	2019	Blockchain Specialization		https://www.coursera.org/specializations/blockchain#courses