STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Blokų grandinių technologijos	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantys: 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 (angl. *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.
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.	6				4		10	8	Įvairių tipų „blockchain“ testavimas ir jų modifikavimas
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.	10				10		20	20	

Išmaniosios sutartys (*Smart Contracts*). Saugumas. Privatieji ir viešieji „blockchain“. Bitcoin tipo „blockchain“ tinklo programavimas.									
4. **Įvairių tipų „blockchain“ realizacijos**: Ethereum tipo „blockchain“ tinklo programavimas. *AWS Blockchain* šablonai. „*Hyperledger: Linux Foundation*“ tipo „blockchain“ tinklo programavimas. Testavimo tinklai.	10				14		24	25	
5. 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 1-3 temas. Maksimalus įvertis už puikiai atliktas užduotis yra 10 balų (atitinkantys 20 % bendrojo svorio). Skiriami papildomi balai (iki 20 % maksimalaus įverčio svorio) kai užduotys atsiskaitomos anksčiau nurodytų terminų.
Antrasis laboratorinis darbas	20	Semestro metu	Studentams skiriamos užduotys, apimančios 4 temos Ethereum „blockchain“ tinklo programavimą. Maksimalus įvertis už puikiai atliktas užduotis yra 10 balų (atitinkantys 20 % bendrojo svorio). Skiriami papildomi balai (iki 20 % maksimalaus įverčio svorio) kai užduotys atsiskaitomos anksčiau nurodytų terminų.
Trečiasis laboratorinis darbas	20	Semestro metu	Studentams skiriamos užduotys, apimančios 4 temos *Hyperledger* „blockchain“ tinklo programavimą. Maksimalus įvertis už puikiai atliktas užduotis yra 10 balų (atitinkantys 20 % bendrojo svorio). Skiriami papildomi balai (iki 20 % maksimalaus įverčio svorio) kai užduotys atsiskaitomos anksčiau nurodytų terminų.
Egzaminas (raštu)	40	Egzaminų sesijos metu	Egzaminą laikyti leidžiama semestro metu surinkus ne mažiau, nei minimalų 15 balų skaičių, atitinkantį 50 % laboratoriniams darbams skirtojo svorio. Egzamino metu galima surinkti iki 10 balų, kurie atitinka 40 % galutinio įvertinimo. Egzamino metu studentas turi pateikti praktinį pateiktos užduoties sprendimą, motyvuojant naudojamų priemonių efektyvumą, bei analizuojant alternatyvius užduoties sprendimo būdus.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privaloma literatūra				
Andrew Miller, Arvind Narayanan, Edward Felten, Joseph Bonneau, Steven Goldfeder	2017	Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction		Princeton University Press. https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf https://www.coursera.org/learn/cryptocurrency
Andreas Antonopoulos	2017	Mastering Bitcoin: Programming the Open Blockchain	2nd Edition	O‘Reilly, https://github.com/bitcoinbook/bitcoinbook
Andreas Antonopoulos, Gavin Wood	2018	Mastering Ethereum: Building Smart Contracts and Dapps		https://github.com/ethereumbook/ethereumbook
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
Amazon	2018	AWS Blockchain Templates Resources		https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-dg.pdf
IBM	2018	IBM Blockchain Foundation for Developers		https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers

COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
Blockchain technologies	

Lecturer(s)	Department(s) where the course unit (module) is delivered
Coordinator: PhD. Remigijus Paulavičius, PhD. 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	3th 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, investigation of various types of blockchains.
2. **Blockchain fundamentals.** Origin of the blockchain. Drawbacks of the current transactions systems. Ledger. Bitcoin. Blockchain applications: finance, logistics, health, Internet-of-Things.	6				4		10	8	
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.	10				10		20	20	

4. **Development of other popular blockchains.** Development of the Ethereum-type blockchain. AWS Blockchain templates. Development of the Hyperledger-type blockchain. Testnets.	10				14		24	25	
5. 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	Individual works are assigned to students covering topics 1-3. The maximum score for the assignment is 10 points (this corresponds 20% of the total weight). Students can receive bonus points (up to 20% of the maximum score) when tasks are successfully defended before the deadline.
The second laboratory work	20	During the semester	Individual works are assigned to students covering development of the Ethereum-type blockchain from topic 4. The maximum score for the assignment is 10 points (this corresponds 20% of the total weight). Students can receive bonus points (up to 20% of the maximum score) when tasks are successfully defended before the deadline.
The third laboratory work	20	During the semester	Individual works are assigned to students covering development of the Hyperledger-type blockchain topic 4. The maximum score for the assignment is 10 points (this corresponds 20% of the total weight). Students can receive bonus points (up to 20% of the maximum score) when tasks are successfully defended before the deadline.
Written examination	40	During the exams session	The final exam is allowed to take if the minimum qualifying mark (equal to 15 points; equivalently to 50% of the total score from laboratory works). During the exam, students can collect up to 10 points, which corresponds to 40% of the final assessment. In the examination, the student must provide a practical solution to the actual problem, and provide motivation for the used tools.

Author	**Year of publication**	**Title**	**Issue of a periodical or volume of a publication**	**Publishing place and house or web link**
Compulsory reading				
Andrew Miller, Arvind Narayanan, Edward Felten, Joseph Bonneau, Steven Goldfeder	2017	Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction		Princeton University Press. https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf https://www.coursera.org/learn/cryptocurrency
Andreas Antonopoulos	2017	Mastering Bitcoin: Programming the Open Blockchain	2nd Edition	O'Reilly, https://github.com/bitcoinbook/bitcoinbook
Andreas Antonopoulos, Gavin Wood	2018	Mastering Ethereum: Building Smart Contracts and Dapps		https://github.com/ethereumbook/ethereumbook
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
Amazon	2018	AWS Blockchain Templates Resources		https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-dg.pdf
IBM	2018	IBM Blockchain Foundation for Developers		https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers