DOKTORANTŪROS STUDIJŲ DALYKO SANDAS

Dalyko pavadinimas	Mokslo kryptis (šaka) kodas	Fakultetas	Institutas, katedra
Blokų grandinių technologijos	Informatikos inžinerija, 07T	MIF	DMSTI, Blokų grandinių technologijų grupė

Studijų būdas	Kreditų skaičius ECTS	Studijų būdas	Kreditų skaičius
paskaitos	1 (pavasario sem.)	konsultacijos	1
individualus	4	seminarai	1

Dalyko anotacija

Anotacija: Tai yra išsamus „Blockchain“ (blokų grandinių) technologijos kursas, padedantis suprasti pačią technologiją ir visą ekosistemą. Šio kurso tikslas – įsigilinti į „Blockchain“ pagrindus ir veikimo principus bei taikyti juos realizuojant „Blockchain“ sprendimus.

Dalyko temos:

1. Įvadas į kriptografiją
    - Kriptografinės maišos (angl. Hash) funkcijos
    - Maišos rodyklės ir duomenų struktūros: *Merkle tree*
    - Skaitmeniniai parašai: privatusis ir viešasis raktai
2. Blockchain pagrindai
    - Blockchain kilmė ir atsiradimo priežastys, Bitcoin priešistorė
    - Dabartinių transakcijų (sandorių) sistemų trūkumai
    - Viešas transakcijų žurnalas
    - Bitcoin’o ir „Blockchain“ atsiradimas
    - „Blockchain“ taikymai: finansai, valdymas, logistika, sveikatos priežiūra, daiktų internetas.
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
    - Išmaniosios sutartys (*Smart Contracts*)
    - Saugumas
    - Privatieji ir viešieji „blockchain“
4. Įvairių tipų „blockchain“ tinklų naudojimas, tobulinimas ir programavimas
    - *Bitcoin* ir *Ethereum* tipo „blockchain“ tinklų programavimas
    - *AWS Blockchain* šablonai
    - *„Hyperledger*: *Linux Foundation*“ projektas: *Hyperledger-Fabric* sistema ir jos naudojimas.
    - Testavimo tinklų naudojimas
5. Investavimas bei kriptografinių valiutų rinkų analizė
    - Kriptografinių valiutų biržos
    - ATM technologiniai sprendimai
    - HFT algoritmai prekyboje
    - Intelektualios sprendimų paramos sistemos kriptografinių valiutų rinkose

Praktinės užduotys: eksperimentiškai palyginti populiariausius viešuosius ir privačius „blockchain“ tinklus, atlikti programavimo užduotis skirtas šių tinklų kūrimui ir tobulinimui. Nustatyti tinkamą „blockchain“ tipą duotam taikymui. Pritaikyti „blockchain“ duotam taikymui testiniame tinkle. Formuoti ir valdyti kriptografininių valiutų investicinius portfelius, taikyti intelektualias sprendimų paramos sistemas kriptografinių valiutų rinkose, testuoti HFT algoritmus.

Pagrindinė literatūra

1. Andrew Miller, Arvind Narayanan, Edward Felten, Joseph Bonneau, ir Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (2017). https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf https://www.coursera.org/learn/cryptocurrency
2. Andreas Antonopoulos ir Gavin Wood. *Mastering Ethereum: Building Smart Contracts and Dapps* (2018) https://github.com/ethereumbook/ethereumbook
3. Andreas Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain* (2017). https://github.com/bitcoinbook/bitcoinbook
4. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf
5. Ferguson, Niels, Bruce Schneier, ir Tadayoshi Kohno. *Cryptography engineering: design principles and practical applications* (2012).
6. AWS Blockchain Templates Resources: https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-dg.pdf
7. Video mokomoji medžiaga: *IBM Blockchain Foundation for Developers:* https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers

Konsultuojančiųjų dėstytojų vardas, pavardė	Mokslo laipsnis	Svarbiausieji darbai mokslo kryptyje (šakoje) paskelbti per pastaruosius 5 metus
Remigijus Paulavičius	dr.	• Qi Chen, **R. Paulavičius**, S. García-Muñoz, C.S. Adjiman (**2018**) An Optimization Framework to Combine Operable Space Maximization with Design of Experiments. *AIChE Journal*, DOI: 10.1002/aic.16214 • **R. Paulavičius**, L. Chiter, J. Žilinskas (**2018**) Global optimization based on bisection of rectangles, function values at diagonals, and a set of Lipschitz constants. *Journal of Global Optimization* 71 (1), p. 5-20 doi:10.1007/s10898-016-0485-6 • L. Stripinis, **R. Paulavičius**, J. Žilinskas (**2017**) Improved scheme for selection of potentially optimal hyper-rectangles in DIRECT. *Optimization Letters*, doi:10.1007/s11590-017-1228-4 • J. Mockus, **R. Paulavičius**, D. Rusakevičius, D. Šešok, J. Žilinskas (**2017**) Application of Reduced-set Pareto-Lipschitzian Optimization to truss optimization. *Journal of Global Optimization* 67 (1), p. 425-450 doi:10.1007/s10898-015-0364-6 • **R. Paulavičius**, P-M. Kleniati, C.S. Adjiman (**2016**) Global optimization of nonconvex bilevel problems: implementation and computational study of the Branch-and-Sandwich algorithm. *Computer Aided Chemical Engineering*, 38, p. 1977-1982. • **R. Paulavičius**, J. Žilinskas (**2016**) Advantages of simplicial partitioning for Lipschitz optimization problems with linear constraints. *Optimization Letters* 10 (2), p. 237–246 doi:10.1007/s11590-014-0772-4 • **R. Paulavičius,** J Žilinskas (**2014**) Simplicial global optimization. 137 p., ISBN 978-1-4614-9092-0, Springer, doi: 10.1007/978-1-4614-9093-7

		• **R. Paulavičius**, Y.D. Sergeyev, D.E. Kvasov, J. Žilinskas (**2014**) Globally-biased DISIMPL algorithm for expensive global optimization. *Journal of Global Optimization* 59 (2), p. 545-567 doi:10.1007/s10898-014-0180-4 • **R. Paulavičius**, J. Žilinskas (**2014**) Simplicial Lipschitz optimization without the Lipschitz constant. *Journal of Global Optimization* 59 (1), p. 23-40 doi: 10.1007/s10898-013-0089-3
Ernestas Filatovas	dr.	• F. Orts, **E. Filatovas**, G. Ortega, O. Kurasova, E. M. Garzón (**2018**) Improving the energy efficiency of SMACOF for multidimensional scaling on modern architectures. *The Journal of Supercomputing*, 1–13, online, doi: 10.1007/s11227-018-2285-x. • **E. Filatovas,** A. Lančinskas, O. Kurasova, J. Žilinskas (**2017**) A preference-based multi-objective evolutionary algorithm R-NSGA-II with stochastic local search. *Central European Journal of Operations Research*, Springer, Vol. 25(4), 859–878, doi: 10.1007/s10100-016-0443-x. • J. J. Moreno, G. Ortega, **E. Filatovas**, J. A. Martínez, E. M. Garzón (**2017**) Using low-power platforms for Evolutionary Multi-Objective Optimization algorithms. *The Journal of Supercomputing*, *Springer*, Vol. 73(1), 302–315, doi: 10.1007/s11227-016-1862-0. • T. Petkus, J. Tichonov, **E. Filatovas**, V. Jakštys (**2017**) Quality assessment of high-resolution images with small distortions after compression. *Baltic journal of modern computing.* Vol. 5(2), 206–220, doi: 10.22364/bjmc.2017.5.2.04. • G. Ortega, **E. Filatovas,** J. A. Martínez, E. M. Garzón, L. G. Casado (**2016**) Non-dominated sorting procedure for Pareto dominance ranking on multicore CPU and/or GPU. *Journal of Global Optimization*, Springer, Vol. 69(3), 607–627, doi: 10.1007/s10898-016-0468-7. • **E. Filatovas,** D. Podkopaev, O. Kurasova (**2015**) A Visualization Technique for Accessing Solution Pool in Interactive Methods of Multiobjective Optimization. *International Journal of Computers Communications & Control*, Vol. 10(4), 508–519, doi: 10.15837/ijccc.2015.4.1672. • **E. Filatovas,** O. Kurasova, K. Sindhya (**2015**) Synchronous R-NSGA-II: an extended preference-based evolutionary algorithm for multi-objective optimization. *Informatica*, Vol. 26(1), 33–50, doi: 10.15388/informatica.2015.37.
Saulius Masteika	dr.	• Krikščiūnienė, Dalia; Sakalauskas, Virgilijus; Strigūnaitė, Sandra; **Masteika, Saulius**. Project performance evaluation by modified analytic hierarchy process model // Transformations in business and economics. ISSN 1648-4460. (**2015**), Vol. 14, no. 1(34), p. 192-211. Social Sciences Citation Index (Web of Science); Science Citation Index Expanded (Web of Science)] • Lopata, Audrius; Ambraziūnas, Martas; Veitaitė, Ilona; **Masteika, Saulius**; Butleris, Rimantas. SysML and UML models usage in knowledge based

		MDA process // Elektronika ir elektrotechnika. Kaunas : Technologija. ISSN 1392-1215. (**2015**), Vol. 21, iss. 2, p. 50-57. [DB: Scopus; Science Citation Index Expanded (Web of Science); Current Abstracts; INSPEC; VINITI] • Driaunys, Kęstutis; **Masteika, Saulius**; Sakalauskas, Virgilijus; Vaitonis, Mantas. An algorithm-based statistical arbitrage high frequency trading system to forecast prices of natural gas futures // Transformations in business and economics, ISSN 1648-4460. **(2014)**, Vol. 13, no. 3, p. 96-109. [DB: Social Sciences Citation Index (Web of Science); e-Jel (nenaudotinas); EconLit; IBSS; Science Citation Index Expanded (Web of Science)] • Plikynas, Darius; Bašinskas, Gytis; Kumar, Pravin; **Masteika, Saulius**; Kežys, Darius; Laukaitis, Algirdas. Social systems in terms of coherent individual neurodynamics: conceptual premises, experimental and simulation scope // International journal of general systems. Abingdon : Taylor & Francis. ISSN 0308-1079. (**2014**), vol. 43, no 5, p. 434- 469. (Web of Science); Zentralblatt MATH (zbMATH); Compendex; Scopus;Science Citation Index Expanded (Web of Science)] • Raudys, Aistis; Plikynas, Darius; **Masteika, Saulius**. Novel automated multi-agent investment system based on simulation of self-excitatory oscillations // Transformations in business and economics. ISSN 1648-4460. (**2014**), Vol. 13, no. 2, p. 78-90. (Web of Science); e-Jel (nenaudotinas); EconLit; IBSS; Science Citation Index Expanded (Web of Science)] • **Masteika, Saulius**; Driaunys, Kęstutis; Rutkauskas, Aleksandras Vytautas. Historical data formation for back test and technical analysis in North American futures market // Transformations in business & economics. ISSN 1648-4460. (**2013**), Vol. 12, no. 1A, p. 473-488. • Vaitonis, Mantas; **Masteika, Saulius**. Statistical arbitrage trading strategy in commodity futures market with the use of nanoseconds historical data // Information and software technologies, ICIST 2017, - Book series: Communications in Computer and Information Science. Vol 756. ISSN 1865-0929, eISSN 1865-0937. Cham : Springer, (**2017**). ISBN 9783319676418. eISBN 9783319676425. p. 303-313. • Vaitonis, Mantas; **Masteika, Saulius**. Research in high frequency trading and pairs selection algorithm with Baltic region stocks // Information and software technologies: ICIST 2016, Ser.: Communications in computer and information science. ISSN 1865-0929. Vol. 639. Cham : Springer International Publishing Switzerland, (**2016**). ISBN 9783319462530. p. 208-217. • **Masteika, Saulius**; Vaitonis, Mantas. Quantitative research in high frequency trading for natural gas futures market // Business Information Systems

		Workshops : BIS 2015 International Workshops, Poznań, 2015, revised papers. Series: Lecture Notes in Business Information Processing, Vol. 228 / Editor : Witold Abramowicz. ISSN 1865-1348. Berlin : Springer, (**2015**). • Plikynas, Darius; **Masteika, Saulius**. Agent-based nonlocal social systems: neurodynamic oscillations approach // Social computing and social media : 6th international conference, SCSM (B) : proceedings. - Book series: Lecture notes in computer science. Vol. 8531. • Plikynas, Darius; **Masteika, Saulius**; Bašinskas, Gytis; Kezys, Darius; Kumar, Pravin. Group neurodynamics: conceptual and experimental framework // Advances in Cognitive Neurodynamics (IV) Springer Netherlands, (**2015**). ISBN 9789401795470 p. 15-20. • **Masteika, Saulius**. Informacijos blokų grandinėlės technologija keičia mūsų kasdienybę // Spectrum. Vilnius : Vilniaus universiteto leidykla. ISSN 1822-0347. 2015, Nr. 2, p. 30-33. • **Masteika, Saulius**. Virtuali valiuta - žaisminga idėja ar reali alternatyvios pinigų rinkos užuomazga? // Spectrum. ISSN 1822-0347. 2013, nr. 2, p. 30-31. • Vaitonis, Mantas; **Masteika, Saulius**. Research in high frequency statistical arbitrage strategies applied to microsecond and nanosecond information // 9th International workshop on Data Analysis Methods for Software Systems (DAMSS), (**2017**). Vilnius : VIlniaus universitetas, • Vaitonis, Mantas; **Masteika, Saulius**. Computerized high frequency trading of nanoseconds in futures market // Data analysis methods for software systems (**2016**). Vilnius : Vilniaus universiteto leidykla, 2016. ISBN 9789986680611. p. 62-63. • Vaitonis, Mantas; **Masteika, Saulius**. High frequency statistical arbitrage strategy engineering and algorithm for pairs trading selection // Data analysis methods for software systems (**2015**). Vilnius : Vilniaus universiteto leidykla, ISBN 9789986680581. p. 51-52.