

## DOKTORANTŪROS STUDIJŲ DALYKO SANDAS

Dalyko pavadinimas	Mokslo kryptis, kodas	Fakultetas	Institutas, katedra, mokslo grupė
Blokų grandinių technologijos	Informatikos inžinerija (T 007)	Matematikos ir informatikos fakultetas	Duomenų mokslo ir skaitmeninių technologijų institutas, Blokų grandinių technologijų grupė
Studijų būdas	Kreditų skaičius ECTS	Studijų būdas	Kreditų skaičius
paskaitos	1	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 (Remigijus Paulavičius ir Ernestas Filatovas)
  - Kriptografinės maišos (angl. Hash) funkcijos
  - Maišos rodyklės ir duomenų struktūros: *Merkle tree*
  - Skaitmeniniai parašai: privatusis ir viešasis raktai
2. Blockchain pagrindai (Remigijus Paulavičius ir Ernestas Filatovas)
  - 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? (Remigijus Paulavičius ir Ernestas Filatovas)
  - 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 (Remigijus Paulavičius ir Ernestas Filatovas)
  - *Bitcoin* ir *Ethereum* „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 (Saulius Masteika)
  - 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 kriptografinių 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://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. D. Hellwig, G. Karlic, and A. Huchzermeier, *Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology*. Springer International Publishing, 2020.
6. Ferguson, Niels, Bruce Schneier, ir Tadayoshi Kohno. *Cryptography engineering: design principles and practical applications* (2012).
7. AWS Blockchain Templates Resources: <https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-dg.pdf>
8. Hyperledger Fabric documentation: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/>
9. Internetinis kursas: *Introduction to Hyperledger Blockchain Technologies*:  
<https://www.edx.org/course/introduction-to-hyperledger-blockchain-technologie>
10. Internetinis kursas: *Hyperledger Sawtooth for Application Developers*  
<https://www.edx.org/course/hyperledger-sawtooth-for-application-developers-2>

Konsultuojančiųjų dėstytojų vardas, pavardė	Mokslo laipsnis	Svarbiausieji darbai mokslo kryptyje (šakoje) paskelbti per pastaruosius 5 metus
Remigijus Paulavičius	dr.	<a href="http://www.elaba.mb.vu.lt/dmsti/?aut=Remigijus+Paulavi%C4%8Dius">http://www.elaba.mb.vu.lt/dmsti/?aut=Remigijus+Paulavi%C4%8Dius</a>
Ernestas Filatovas	dr.	<a href="http://www.elaba.mb.vu.lt/dmsti/?aut=Ernestas+Filatovas">http://www.elaba.mb.vu.lt/dmsti/?aut=Ernestas+Filatovas</a>
Saulius Masteika	dr.	<a href="https://www.researchgate.net/profile/Saulius_Masteika">https://www.researchgate.net/profile/Saulius_Masteika</a>