DOKTORANTŪROS STUDIJŲ DALYKO SANDAS

Dalyko pavadinimas	Mokslo kryptis (šaka) kodas	Fakultetas	Institutas
Blokų grandinių technologijos	07T	Matematikos ir informatikos fakultetas	Duomenų mokslo ir skaitmeninių technologijų institutas

Studijų būdas	Kreditų skaičius ECTS	Studijų būdas	Kreditų skaičius
paskaitos	1	konsultacijos	1
individualus	4	seminarai	1

Dalyko anotacija

Anotacija: Tai išsamus blokų grandinių technologijų kursas, padedantis doktorantams aukštu lygiu suprasti blokų grandinių sistemas ir jas supančią ekosistemą. Kurso tikslas – atnaujinti žinias apie pagrindinius principus (kriptografiją, konsensusą, išmaniuosius kontraktus, viešąsias ir konsorciumų grandines) bei jas papildyti šiuolaikinėmis tendencijomis: antrojo sluoksnio (Layer-2) spartinimo sprendimais, nulinio žinių įrodymo metodais, DeFi mechanizmais bei aktualiais saugumo ir ekonominiais iššūkiais. Studentai išmoks kritiškai vertinti protokolus, taikyti įgytas koncepcijas eksperimentiniuose palyginimuose bei atlikti diegimo užduotis.

Dalyko temos:

1. Įvadas į kriptografiją (Remigijus Paulavičius ir Ernestas Filatovas)
   - Maišos funkcijos (įskaitant atsparumą kolizijoms, įsipareigojimo schemų intuiciją).
   - Maišos nuorodos ir duomenų struktūros: Merkle medžiai ir jų variantai (Merkle-Patricia).
   - Skaitmeniniai parašai: viešieji / privatieji raktai; slenkstiniai parašai (koncepcijos).
2. Blokų grandinių pagrindai (Remigijus Paulavičius ir Ernestas Filatovas)
   - Blokų grandinės kilmė ir ekosistemos evoliucija.
   - Tradicinių transakcijų sistemų trūkumai (pasitikėjimas, audituojamumas, atsiskaitymai).
   - Didžiosios knygos (ledger) modeliai: UTXO prieš sąskaitų modelį (account-based).
   - Bitcoin ir blokų grandinių ištakos.
   - Blokų grandinių taikymai: finansai, logistika, sveikatos apsauga, daiktų internetas (IoT).
3. Kaip veikia „Blockchain“ technologija? (Remigijus Paulavičius ir Ernestas Filatovas)
   - Bloko struktūra ir transakcijos ciklas (mempool, įtraukimas, patvirtinimai, reorganizacijos).
   - Grandinės augimas: blokų susiejimas, šakų pasirinkimas (fork-choice) ir galutinumas (tikimybinis prieš deterministinį).
   - Konsensusas ir dalyvavimas: PoW, PoS, BFT, DAG; kasėjų ir patvirtintojų (validator) vaidmenys bei techninė įranga.
   - PoS delegavimas (staking): patvirtintojų parinkimas arba delegavimas, atlygiai ir baudos (slashing), „staking“ fondai (įskaitant likvidaus „staking“ koncepciją).
   - Išmanieji kontraktai: vykdymo modelis (EVM arba WASM), mokesčiai (gas), būsena ir saugyklos, orakulai.
   - Saugumas ir valdymas: protokolų ir kontraktų grėsmės (51 % ataka, cenzūra, „long-range“ atakos, „reentrancy“, tiltai, MEV); viešieji prieš privačius pasitikėjimo modelius.
4. Viešųjų blokų grandinių įgyvendinimas (Remigijus Paulavičius ir Ernestas Filatovas)
   - Bitcoin ir Ethereum vystymas ir veikimas (klientai, testiniai tinklai).
   - Išmanieji kontraktai ir decentralizuotos programėlės (Ethereum): žetonai (tokens), NFT, Web3 pagrindai.
   - Decentralizuotų finansų (DeFi) apžvalga: AMM (DEX), skolinimas ir skolinimasis, stabilizuotosios valiutos (stablecoins) – mechanizmai ir rizikos.
   - Maksimali išgaunama vertė (MEV) ir praktinės implikacijos (front-running, sandwiching).
   - Tarpgrandininiai tiltai ir sąveika (pasitikėjimo modeliai, dažniausios klaidos).
5. Antrojo sluoksnio (Layer-2) sprendimai ir spartinimas (Remigijus Paulavičius ir Ernestas Filatovas)
   - Spartinimo iššūkiai: pralaidumas, vėlinimas, mokesčiai, būsenos (state) augimas.

- Mokėjimų ir būsenos kanalai (idėja, ginčų sprendimas).
- „Rollups“: optimistiniai prieš ZK „rollups“ (sukčiavimo įrodymai prieš validumo įrodymus).
- Duomenų prieinamumas (data availability) ir modulinės blokų grandinės idėja (vykdymas vs konsensusas vs DA).
- L2 saugumo prielaidos: sekvenceriai, atsparumas cenzūrai, „escape hatches“ mechanizmai.

6. Privatumas ir nulinio žinių įrodymo metodai (Remigijus Paulavičius, Ernestas Filatovas ir Saulius Masteika)
   - Privatumo tikslai blokų grandinėse: anonimiškumas, konfidencialumas, atitiktis.
   - ZK (nulinio žinių įrodymo) pagrindai: kas įrodoma (pagrįstumo/intuicijos aspektai), schemos kaip apribojimai (koncepcija).
   - SNARK/STARK palyginimas (patikima parengtis, įrodymo kūrimo ir patvirtinimo sąnaudos).
   - ZK taikymai: privatūs pervedimai, tapatybė ir kredencialai, ZK „rollups“, skaičiavimai su įrodymais (ZKVM idėja).
7. Postkvantinė kriptografija ir blokų grandinių atsparumas (Remigijus Paulavičius ir Ernestas Filatovas)
   - Postkvantiniai skaitmeniniai parašai (perėjimas nuo elipsinių kreivių prie NIST standartizuotų PQC algoritmų).
   - Kvantiniams kompiuteriams atsparūs konsensuso mechanizmai (PoW ir PoS saugumo prielaidų vertinimas kvantinėje aplinkoje).
   - Migracijos strategijos („kvantiškai saugus“ esamų didžiųjų knygų perėjimas).
   - Postkvantiniai ZK įrodymai: skirtingų įrodymo sistemų (SNARKs vs STARKs) kvantinio pagrįstumo analizė.
8. Konsorciumų ir verslo blokų grandinės (Remigijus Paulavičius ir Ernestas Filatovas)
   - „Hyperledger“ tipo grandinės: „Fabric“ architektūra, kanalai, patvirtinimo (endorsement) taisyklės.
   - „Hyperledger Fabric“ tipo grandinių kūrimas (chaincode, diegimas, testiniai tinklai).
   - Hibridinės architektūros.
   - Saugumo ir atitikties aspektai verslo diegimuose.
9. Investavimas ir kriptovaliutų rinkų analizė (Saulius Masteika)
   - Kriptovaliutų rinkos ir rinkos mikrostruktūros pagrindai.
   - Automizuotų prekybos mechanizmų (ATM) technologiniai sprendimai: architektūra, likvidumo ir atsiskaitymų srautai, KYC-AML atitiktis, operacinės ir saugumo rizikos.
   - Rizikos veiksniai: kintamumas, likvidumas, stabilizuotųjų valiutų, tiltų ir valdymo rizikos.
   - Portfelio formavimas ir vertinimas (rizika įvertinantys rodikliai, apribojimai).
   - Aukšto dažnio prekybos (HFT) algoritmai.
   - Intelektualios sprendimų paramos sistemos kriptovaliutų rinkoms (signalai, prognozavimas, rinkos režimų aptikimas).

Praktinės užduotys: eksperimentiškai palyginti pirmaujančius viešuosius ir privačius (konsorciumų) blokų grandinių tinklus bei atlikti programavimo užduotis juos konfigūruojant ir kuriant taikomąsias programas. Parinkti tinkamiausią blokų grandinės tipą nurodytam panaudojimo atvejui ir įdiegti koncepcijos įrodymą (PoC) testiniame tinkle. Įgyvendinti ir įvertinti paprastą antrojo sluoksnio (Layer-2) sprendimą (pvz., kanalą arba „rollup“ tipo transakcijų grupavimą) bei sukurti minimalų nulinio žinių įrodymo komponentą (pvz., bazinį įrodymo patvirtinimą). Formuoti ir valdyti kriptovaliutų investicinius portfelius, taikyti intelektualius sprendimų paramos metodus ir testuoti HFT strategijas kontroliuojamoje atgalinio testavimo (backtesting) aplinkoje.

Pagrindinė literatūra

1. Antonopoulos, A. M., & Harding, D. A. (2023). Mastering Bitcoin: Programming the open blockchain (3rd ed.). O'Reilly Media. https://github.com/bitcoinbook/bitcoinbookAntonopoulos, A. M., Osuntokun, O., & Pickhardt, R. (2021). Mastering the Lightning Network: A second layer blockchain protocol for instant Bitcoin payments. O'Reilly Media. https://github.com/lnbook/lnbook.
2. Antonopoulos, A. M., Wood, G., Parisi, C., Mazza, A., & Pozzolini, N. (2025). Mastering Ethereum: Implementing smart contracts (2nd ed.). O'Reilly Media. https://github.com/ethereumbook/ethereumbook
3. Bashir, I. (2023). Mastering blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3 (4th ed.). Packt Publishing. https://www.packtpub.com/en-eg/product/mastering-blockchain-fourth-edition-9781803241067

4. Ethereum Foundation. (2025, October 22). Maximal extractable value (MEV). Ethereum.org. https://ethereum.org/developers/docs/mev/
5. Ethereum Foundation. (2025, November 18). Scaling. https://ethereum.org/developers/docs/scaling/
6. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering: Design principles and practical applications. Wiley Publishing, Inc.
7. Hyperledger Fabric documentation (Release 2.5). https://hyperledger-fabric.readthedocs.io/en/release-2.5/
8. Lavin, R., Liu, X., Mohanty, H., Norman, L., Zaarour, G., & Krishnamachari, B. (2024). *A survey on the applications of zero-knowledge proofs*. *arXiv*. https://doi.org/10.48550/arXiv.2408.00243
9. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
10. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.
11. Rebello, G. A. F., Camilo, G. F., de Souza, L. A. C., Potop-Butucaru, M., de Amorim, M. D., Campista, M. E. M., & Costa, L. H. M. K. (2024). A survey on blockchain scalability: From hardware to layer-two protocols. *IEEE Communications Surveys & Tutorials*, *26*(4), 2411–2458. doi:10.1109/COMST.2024.3376252
12. Torralba-Agell, A., & Pérez-Solà, C. (2025). Security assumptions in permissionless blockchains and layer 2 scalability solutions: A comprehensive taxonomy. *Blockchain: Research and Applications*, 100388. doi:10.1016/j.bcra.2025.100388
13. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549 (7671), 188–194. doi:10.1038/nature23461.
    National Institute of Standards and Technology. (2024). *Post-Quantum Cryptography Standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA)*. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography

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

Doktorantūros komiteto teikimu patvirtinta fakulteto/instituto taryboje 20__ m.__ mėn.__d. , protokolo Nr.
Tarybos pirmininkas

Pastaba: jei doktorantūros teisė bus suteikta kartu su kita institucija, tvirtinama ne fakulteto taryboje , o jungtinėje komisijoje.