DOCTORAL (PHD) STUDIES

COURSE UNIT DESCRIPTION

Course unit title	Scientific areas	Faculty	Institute, department
Blockchain technologies	07T	Mathematics and Informatics faculty	Institute of Data Science and Digital Technologies

Study method	Number of credits	Study method	Number of credits
Lectures	1	Consultations	1
Individual works	4	Seminars	1

Summary

Annotation: This is a comprehensive blockchain technology course that helps PhD students understand blockchain systems and the surrounding ecosystem at an advanced level. The aim of this course is to refresh core principles (cryptography, consensus, smart contracts, public vs consortium chains) and extend them with modern developments: Layer-2 scaling, zero-knowledge proofs, DeFi mechanisms, and current security/economic challenges. Students will learn to critically evaluate protocols and to apply the concepts in experimental comparisons and implementation tasks.

Content:

1. **Introduction into cryptography** (Remigijus Paulavičius ir Ernestas Filatovas)
   - Hash functions (incl. collision resistance, commitment intuition)
   - Hash pointers and data structures: Merkle tree and variants (Merkle-Patricia)
   - Digital signatures: private/public keys; threshold signatures (concepts)
2. **Blockchain fundamentals** (Remigijus Paulavičius ir Ernestas Filatovas)
   - Origin of blockchain and the evolution of the ecosystem
   - Drawbacks of traditional transaction systems (trust, auditability, settlement)
   - Ledger models: UTXO vs account-based
   - Bitcoin and blockchain origins
   - Blockchain applications: finance, logistics, healthcare, Internet-of-Things
3. **How blockchain technology works?** (Remigijus Paulavičius ir Ernestas Filatovas)
   - Block structure and transaction lifecycle (mempool, inclusion, confirmations, reorgs)
   - Chain growth: linking blocks, fork-choice, and finality (probabilistic vs deterministic)
   - Consensus and participation: PoW, PoS, BFT, DAG; mining versus validation roles and hardware
   - PoS staking: validator selection or delegation, rewards or penalties, slashing, staking pools (including liquid staking concept)
   - Smart contracts: execution model (EVM or WASM), gas or fees, state or storage, oracles
   - Security and governance: protocol and contract threats (51%, censorship, long-range, reentrancy, bridges, MEV); public versus private trust models
4. **Public blockchain implementations** (Remigijus Paulavičius ir Ernestas Filatovas)
   - Bitcoin and Ethereum development and operations (clients, testnets)
   - Smart contracts and decentralized applications (Ethereum): tokens, NFTs, Web3 basics
   - Decentralized finance (DeFi) overview: AMMs (DEX), lending/borrowing, stablecoins (mechanisms + risks)
   - Maximal Extractable Value (MEV) overview (front-running/sandwiching) and practical implications
   - Cross-chain bridges and interoperability (trust models, common failures)

5. **Layer-2 solutions and scalability** (Remigijus Paulavičius ir Ernestas Filatovas)
    - Why scaling is hard: throughput, latency, fees, state growth
    - Payment/state channels (idea, dispute resolution)
    - Rollups: optimistic vs ZK rollups (fraud proofs vs validity proofs)
    - Data availability and modular blockchain idea (execution vs consensus vs DA)
    - L2 security assumptions: sequencers, censorship resistance, escape hatches
6. **Privacy and zero-knowledge proofs in blockchain** (Remigijus Paulavičius, Ernestas Filatovas, Saulius Masteika)
    - Privacy goals in blockchains; anonymity vs confidentiality vs compliance
    - ZK basics: what is proven (soundness/zero-knowledge intuition), circuits as constraints (conceptual)
    - SNARK/STARK trade-offs (trusted setup, prover cost, verification cost)
    - ZK applications: private transfers, identity/credentials, ZK rollups, proof-carrying computation (ZKVM idea)
7. **Post-Quantum Cryptography and Blockchain Resilience** (Remigijus Paulavičius ir Ernestas Filatovas)
    - Post-Quantum Digital Signatures (Transitioning from Elliptic Curves to NIST-standardized PQC algorithms)
    - Quantum-Resistant Consensus Mechanisms (Evaluating the security assumptions of PoW and PoS in a post-quantum environment)
    - Migration Strategies ("Quantum-safe" transition of existing ledgers)
    - Post-Quantum ZK-Proofs Exploring the quantum-soundness of different proof systems (SNARKs vs. STARKs)
8. **Consortium/enterprise blockchains and development** (Remigijus Paulavičius ir Ernestas Filatovas)
    - Hyperledger-type blockchains: Fabric architecture, channels, endorsement policies
    - Development of the Hyperledger Fabric-type blockchain (chaincode, deployment, test networks)
    - Hybrid architectures
    - Security and compliance considerations in enterprise deployments
9. **Investing and analysis of cryptocurrency markets** (Saulius Masteika)
    - Cryptocurrency markets and market microstructure basics
    - ATM technological solutions: architecture, liquidity/settlement flow, compliance/KYC-AML considerations, operational/security risks
    - Risk factors: volatility, liquidity, stablecoin/bridge/governance risks
    - Portfolio formation and evaluation (risk-adjusted metrics, constraints)
    - HFT algorithms for trading
    - Intelligent decision support systems for crypto markets (signals, forecasting, regime detection)

Practical tasks: Experimentally compare leading public and private (consortium) blockchain networks and complete programming assignments for their setup and application development. Select the most suitable blockchain type for a given use case and deploy a proof-of-concept on a testnet. Implement and benchmark a simple Layer-2 solution (e.g., channel or rollup-style batching) and prototype a minimal zero-knowledge proof component (e.g., basic proof verification). Form and manage cryptocurrency investment portfolios, apply intelligent decision support methods, and test HFT strategies in a controlled backtesting environment.

Main literature

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 Application*s, 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.
14. 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

Lecturer(s) (name, surname)	Science degree	Main publications
Remigijus Paulavičius	PhD	http://www.elaba.mb.vu.lt/dmsti/?aut=Remigijus+Paulavi%C4%8Dius
Ernestas Filatovas	PhD	http://www.elaba.mb.vu.lt/dmsti/?aut=Ernestas+Filatovas
Saulius Masteika	PhD	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.