Slovak University of Technology in Bratislava
Ústav počítačového inžinierstva a aplikovanej informatiky

Faculty of Informatics and Information Technologies
Academic year: 2023/2024
Reg. No.: FIIT-16768-116160

BACHELOR THESIS TOPIC

Student: **Lukáš Častven**
Student's ID: 116160
Study programme: Informatics
Study field: Computer Science
Thesis supervisor: Ing. Kristián Košťál, PhD.
Head of department: Ing. Katarína Jelemenská, PhD.

Topic: **Practical usage of Zero-knowledge in different use-cases in blockchains**

Language of thesis: English

Specification of Assignment:

Zero-knowledge proofs (ZKPs) are an exciting breakthrough in applied cryptography that will unlock new use cases across an array of industries, from Web3 to supply chains to the Internet of Things. By verifying the authenticity of information without revealing it, ZKPs can help enhance digital systems' privacy, security, and efficiency. Current use cases are decentralized identity, private transactions, secure and scalable Layer-2s, voting systems, IoT, supply chains, etc. Examine existing solutions and proposals in this domain by conducting state-of-the-art analysis. Propose a system that will utilize Zero-knowledge techniques in some of the existing blockchain networks to enhance its functionality by one of the picked goals. Implement such a solution, which can be done in a smart contract way or as a core network plugin. Potential blockchain networks to use are Polkadot, Kusama, Near, Tezos, Algorand, Moonbeam, Ethereum, etc. Evaluate the implemented solution and compare it with existing ones. Discuss the results and conclude with new findings.

Length of thesis: 40

Deadline for submission of Bachelor thesis: 21. 05. 2024
Approval of assignment of Bachelor thesis: 18. 04. 2024
Assignment of Bachelor thesis approved by: prof. Ing. Valentino Vranić, PhD. – study programme supervisor