SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA INFORMATIKY
A INFORMAČNÝCH TECHNOLÓGIÍ

Návrh zadania diplomovej práce

Finálna verzia do diplomovej práce [1]

Študent:

Meno, priezvisko, tituly: Lukáš Častven, Bc.
Študijný program: Inteligentné softvérové systémy
Kontakt: xcastven@stuba.sk

Výskumník:

Meno, priezvisko, tituly: Kristián Košťál, doc. Ing. PhD.

Projekt:

Názov:	Návrh riešení využívajúcich dôkazy s nulovým vedomím v Ethereum ekosystéme
Názov v angličtine:	Designing Zero-Knowledge Proof Solutions in Ethereum ecosystem
Miesto vypracovania:	Ústav počítačového inžinierstva a aplikovanej informatiky, FIIT STU
Oblasť problematiky:	blockchain, kryptografia, kryptomeny, dôkazy s nulovým vedomím

Text návrhu zadania[2]

Zero-knowledge proofs (ZKPs) are a new cryptographic primitive in applied cryptography with applications in multiple industries, including Web3, supply chains, and the Internet of Things. By verifying the authenticity of information without disclosing its content, ZKPs improve privacy, security, and efficiency in digital systems. Current use cases include decentralized identity (Worldcoin), private transactions (stealth address schemes or blockchains like Zcash and Monero), secure and scalable Layer-2s (ZkSync, Scroll) voting systems, IoT networks, and supply chain management.

Examine existing solutions, proposals, and trends in this domain. Analyse a specific challenge discovered through the related work. Design a solution to address the challenge. Implement and test the solution on Ethereum (or a Layer-2) blockchain network. Evaluate and compare results with existing approaches. Discuss findings and contributions. Conclude with novelty, scientific findings, and future research directions.

[1] Vytlačiť obojstranne na jeden list papiera

[2] 150-200 slov (1200-1700 znakov), ktoré opisujú výskumný problém v kontexte súčasného stavu vrátane motivácie a smerov riešenia

Literatúra[3]

- Ulrich Haböck, David Levit, Shahar Papini. Circle STARKs. Cryptology ePrint Archive, 2024, https://eprint.iacr.org/2024/278.
- Jeremy Bruestle, Paul Gafni, and the RISC Zero Team. RISC Zero zkVM: Scalable, Transparent Arguments of RISC-V Integrity. Risc0. Retrieved January 11, 2024 from https://dev.risczero.com/proof-system-in-detail.pdf.

Vyššie je uvedený návrh diplomového projektu, ktorý vypracoval(a) Bc. Lukáš Častven, konzultoval(a) a osvojil(a) si ho doc. Ing. Kristián Košťál, PhD. a súhlasí, že bude takýto projekt viesť v prípade, že bude pridelený tomuto študentovi.

V Bratislave dňa 1.6.2025

Podpis študenta	Podpis výskumníka

Vyjadrenie garanta predmetov Diplomový projekt I, II, III

Návrh zadania schválený: áno / nie[4]

Dňa: .....

Podpis garanta predmetov

[3] 2 vedecké zdroje, každý v samostatnej rubrike a s údajmi zodpovedajúcimi bibliografickým odkazom podľa normy STN ISO 690, ktoré sa viažu k téme zadania a preukazujú výskumnú povahu problému a jeho aktuálnosť (uveďte všetky potrebné údaje na identifikáciu zdroja, pričom uprednostnite vedecké príspevky v časopisoch a medzinárodných konferenciách)

[4] Nehodiace sa prečiarknite