Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav inteligentních systémů (UITS) Akademický rok 2021/2022

Zadání diplomové práce

Student: **Holub Juraj, Bc.**
Program: Informační technologie
Obor: Kybernetická bezpečnost
Název: **Testování bezpečnosti a výkonu Proof-of-Stake Protokolů pomocí simulace**
Security and Performance Testbed for Simulation of Proof-of-Stake Protocols
Kategorie: Bezpečnost

Zadání:

1. Seznamte se s existujícími proof-of-stake protokoly a jejich populárními hybridními variantami. Vytvořte si přehled o existujících simulačních nástrojích, které jsou orientovány na simulaci konsenzuálních protokolů pro blockchain.
2. Vytvořte teoretické srovnání těchto protokolů z hlediska propustnosti, škálovatelnosti, bezpečnosti, soukromí, odolnosti vůči selhání, dostupnosti a dalších vlastností. V oblasti bezpečnosti zohledněte všechny známé existující zranitelnosti proof-of-stake protokolů, jakož i ty obecné.
3. Zvolte aspoň tři protokoly (včetně Harmony a Solana) a implementujte je jako součást simulačního nástroje.
4. Porovnejte vybrané protokoly pomocí výsledků získaných ze simulací. Experimentujte se simulací různých hrozeb.
5. Na základě výsledků simulace a teoretické analýzy navrhněte několik vylepšení, které můžete ověřit pomocí vytvořeného simulačního nástroje.

Literatura:

- Homoliak, Ivan, et al. "The security reference architecture for blockchains: Towards a standardized model for studying vulnerabilities, threats, and defenses." *arXiv preprint arXiv:1910.09775* (2019).
- Yakovenko, Anatoly. "Solana: a new architecture for a high performance blockchain v0. 8.14." (2021).
- Harmony Team. "Harmony Technical Whitepaper", https://harmony.one/whitepaper.pdf
- Aoki, Y., Otsuki, K., Kaneko, T., Banno, R. and Shudo, K., 2019. SimBlock: a blockchain network simulator. arXiv preprint arXiv:1901.09777.

Při obhajobě semestrální části projektu je požadováno:

- Body 1 a 2.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Homoliak Ivan, Ing., Ph.D.**
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1. listopadu 2021
Datum odevzdání: 18. května 2022
Datum schválení: 3. listopadu 2021