Posudek oponenta diplomové práce

Student: Holub Juraj, Bc.
Téma: Testování bezpečnosti a výkonu Proof-of-Stake Protokolů pomocí simulace (id 25092)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. Náročnost zadání — **průměrně obtížné zadání**

2. Splnění požadavků zadání — **zadání splněno**

Student splnil všechny body zadání na výborné úrovni.

3. Rozsah technické zprávy — **přesahuje obvyklé rozmezí**

Práce téměř překračuje doporučený horní rozsah, protože obsahuje velké množství výsledků experimentů.

4. Prezentační úroveň předložené práce — **90 b. (A)**

Logická struktura práce je na výborné úrovni. Práce velmi detailně představuje jednotlivé pojmy relevantní k zadání. Poskytuje detailně zpracovaný přehled protokolů a útoků na ně. Porovnání existujících simulátorů je důkladné, diskutuje širokou řadu výhod a nevýhod. Volba simulátoru pro další rozšíření je dobře argumentačně podepřena. Asi jedinou výtku mám k stručnému popisu vlastní implementace (nicméně část popisu je součástí dokumentace nástroje na githubu). Významnou částí práce je i popis a vyhodnocení výsledků experimentů.

5. Formální úprava technické zprávy — **95 b. (A)**

Jazyková a stylistická stránka práce i úroveň typografie je na výborné úrovni.

6. Práce s literaturou — **95 b. (A)**

Práce obsahuje větší množství referencí. Odkazované zdroje jsou relevantní tématu a vhodně vybrány.

7. Realizační výstup — **95 b. (A)**

Výstupem je modifikace simulátoru Wittgenstein, který byl rozšířen o podporu protokolů Harmony, Solana a Ouroboros. Vytvořený simulátor je funkční a byl využit k simulaci chování protkolů dle vybraných parametrů. Experimenty jsou rozsáhlé, prokázaly očekáváné zranitelnosti protokolů. Součástí práce byl pak i návrh protiopatření (např. integrace VRF funkce z Algorandu do vše testovaných protokolů za účelem lepší ochrany pro DoS). Funkčnost této úpravy pak byla ověřena dalšími experimenty. Simulace jsou prováděny nad reálnými parametry sesbíranými z dostupných informací o provozu vybraných protokolů.

8. Využitelnost výsledků

Výsledky jsou velmi povedené a jsou využitelné vědeckou komunitou zabývající se simulací blockchain protokolů. Nástroj je veřejně dostupný na githubu.

9. Otázky k obhajobě

-

10. Souhrnné hodnocení — **95 b. výborně (A)**

Práce je výborně zpracována. Implementace je poměrně rozsáhlá, metodika a provedení experimentů je na výborné úrovni. Simulační výsledky ověřující chování protokolů s intgrovanou VRF funkcí mají dle mého názoru i publikační potenciál. Řešení práce je použitelné komunitou. Navrhuji tuto práci na některé z ocenění.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 2. června 2022

Malinka Kamil, Mgr., Ph.D.
oponent