Review of Master's Thesis

Student: Hud Jakub, Bc.
Title: Security and Performance Testbed for Simulation of Proof-of-Stake Protocols (id 25093)
Reviewer: Perešíni Martin, Ing., DITS FIT BUT

1. Assignment complexity — **average assignment**

Diplomová práca sa zaoberá problémom simulácie konsenzuálnych protokolov Proof-of-Stake v blockchaine. Prácu hodnotím ako **stredne náročnú**, pretože študent si musel naštudovať princípy konsenzuálnych protokolov v distribuovanej technológii blockchain a zároveň sa musel oboznámiť so simulačnými nástrojmi využívajúcimi blockchain, aby mohol splniť zadanie.

2. Completeness of assignment requirements — **assignment fulfilled**

Zadanie považujem za **splnené**, študent analyzoval problém, oboznámil sa s inovatívnymi Proof-of-Stake konsenzuálnymi protokolmi v blockchaine a preskúmal jednotlivé bezpečnostné alebo výkonnostné nedostatky konkrétnych protokolov. Študent navrhol simulačný nástroj postavený nad sieťovým simulátorom OMNeT++, v rámci ktorého implementoval jednotlivé konsenzuálne protokoly s cieľom vykonať sadu experimentov na preukázanie vlastností. Vykonané experimenty analyzoval a vyvodil závery, ktoré hodnotím pozitívne. Pozitívne hodnotím tiež vypracovanie práce v anglickom jazyku.

3. Length of technical report — **in usual extent**

Rozsah technickej správy je približne 70 normostrán. Dĺžka práce je v rámci **bežného rozsahu** diplomovej práce (bližšie k dolnej hranici). V technickej správe sú uvedené relevantné informácie.

4. Presentation level of technical report — **85 p. (B)**

Práca má logickú štruktúru, poradie kapitol je dobre zvolené a celkovo je práca napísaná **zrozumiteľne**. Jediné výhrady by som mal k obrázku 4.1, ktorý je vložený bez odkazu v texte, to isté platí aj pre vložené Algoritmy, kapitola 5 je príliš krátka a bolo by vhodné ju spojiť priamo s kapitolou 6 alebo ju rozšíriť a doplniť o relevantnejší text, prípadne tabuľku, a potom sú tu len drobné štylistické nedostatky, medzery a "prázdne strany", ale inak v poriadku. Na druhej strane oceňujem peknú štruktúru textu a príjemné čítanie, chválim aj odkazy v citáciách na konkrétne jednotlivé strany.

5. Formal aspects of technical report — **90 p. (A)**

Práca je napísaná v **anglickom** jazyku. Jazyková úroveň je kvalitná. Z typografického hľadiska nemám k práci žiadne výhrady.

6. Literature usage — **95 p. (A)**

Študent použil relevantné zdroje, čerpal informácie z webových stránok a príručiek dostupných na internete a z odbornej literatúry. Jedinou drobnosťou je, že v predloženom texte sa akosi rozpadli odkazy v citáciách, napr. citácie 4,5,16,20,... Prácu s literatúrou hodnotím **kladne**.

7. Implementation results — **90 p. (A)**

Študent implementoval simulačný nástroj a odovzdal ho ako softvérové dielo, ktoré **spĺňa špecifikáciu** zadania. Výstupom implementácie je rozšírenie nástroja sieťového simulátora OMNeT++ o Proof-of-Stake konsenzuálne protokoly v distribuovanom prostredí blockchainu. Okrem samotnej implementácie študent taktiež navrhol a vykonal sadu experimentov pri ktorých sledoval bezpečnostné a výkonnostné vlastnosti jednotlivých protokolov. Na záver vyvodil výsledky z experimentov. Samotný kód vyzerá byť v poriadku.

8. Utilizability of results

Vo výsledkoch tejto práce vidím potenciál, ktorý by teoreticky mohol byť aj publikovaný. Ide o prácu, ktorá má pridanú hodnotu v tom, že v súčasnosti je ťažké systematicky porovnávať existujúce konsenzuálne protokoly Proof-of-Stake, pretože každý si ich testuje vlastným spôsobom. Neexistuje jednotný spôsob, ako to urobiť, a často sú niektoré údaje o protokoloch zavádzajúce, takže sa jedná o zaujímavé dielo ako sa pokúšať porovnávať vlastnosti jednotným spôsobom.

9. Questions for defence

1. Aké ďalšie vylepšenia PoS protokolov by ste navrhli?
2. Čo považujete za najväčšiu nevýhodu Hedera Hashgraph, hoci sa zdá byť najlepšou voľbou?

10. Total assessment — **90 p. excellent (A)**

Študent splnil všetky povinné body zadania. Práca dosahuje kvalitu z hľadiska rozsahu, úpravy textu (s výnimkou drobných chýb) a prevedenia. Práca bola napísaná v anglickom jazyku a jazyková úroveň napísaného textu je dobrá, čo hodnotím pozitívne. Realizácia je určite prínosná a má potenciál. Celkovo hodnotím výsledok

ako **výborný** a navrhujem študentovi známku **A**.

In Brno 1 June 2022

Perešíni Martin, Ing.
reviewer