Posudek oponenta diplomové práce

Student: Borčík Filip, Bc.
Téma: Testování bezpečnosti a výkonu Proof-of-Stake Protokolů pomocí simulace (id 22846)
Oponent: Veselý Vladimír, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Cílem práce bylo vytvořit simulační modely pro proof-of-stake algoritmy k udržení konsensu distribuovaného systému a integrovat je do simulátoru NS-3. Svou povahou se tedy jedná o náročnější zadání - student musel proniknout jak do fungování netriviálního a velice robustního simulátoru diskrétních událostí, tak do jádra principů blockchainových technologií.

2. Splnění požadavků zadání **zadání splněno**

Všechny body zadání byly splněny. Co se implementace týče, tak byly vytvořeny simulační modely a porovnáno jejich chování pro algoritmy Algorand, Casper FFG a Gasper.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Práce má 62 stran textu v husté LaTeXové šabloně, 75 stran i s pomocnými provozy. V rámci na fakultě vzniklého počítadla http://standardpages.herokuapp.com/standardpages/ má 102,29 normostran, 99% textu a 1% obrázků.
Dle výše uvedeného je tedy mírně nadnormativní vůči obvyklém rozmezí DP.

4. Prezentační úroveň předložené práce **95 b. (A)**

Práce je logicky strukturovaná a její (pod)kapitoly odrážejí body zadání. V práci je vyvážené množství detailů k souvisejícím informacím a i díky si zachovává čtivost. S povděkem kvituji krátké leč poctivé srovnání existujících simulátorů pro blockchainové technologie v Kapitole 4.

5. Formální úprava technické zprávy **85 b. (B)**

Práce je psána ve slovenštině, i proto gramatickou stránku věci nejsem sto schopen správně posoudit. Co se týče typografie, anotování obrázků a diagramů, tak se zdá býti bez prohřešků. Nicméně osobně bych preferoval:
* nemíchat zkrácené a nezkrácené identifikátory, v tomto případě Obr. 2.5 avšak v textu obrázek 2.5;
* u některých obrázku zvětšit velikost písma anotací (např. právě Obr. 2.5).

6. Práce s literaturou **80 b. (B)**

Student v práci cituje z opravdu velkého (95 pramenů) množství relevantních zdrojů, které tvoří majoritně online whitepapery souvisejících technologií. Některé citace mají oproti ostatním špatný či neúplný formát (např. chybějící datum citace, více bibliografických metadat jednoznačně identifikující pramen), a to třeba [95], [28], [29].

7. Realizační výstup **95 b. (A)**

Implementačním výstupem jsou simulační modely v C/C++ a scénáře pro nástroj NS-3. Řádově se jedná o jednotky souborů s desítkami/stovkami autorských řádků. Výstupem testovací/analytické fáze je pak cca tucet excelovských souborů se zpracovanými výsledky sloužícími k případné reprodukci a znovuověření výsledků. Pozornost si zaslouží i testování a provoz nástroje v podmínkách Metacentra sdružení CESNET.

8. Využitelnost výsledků

Výstupy simulátoru jsou zajímavé a potrvzují/rozšiřují domněnky stran fungování proof-of-stake algoritmů v rozsáhlejších peer-to-peer sítích.
Autor sám sice nemá ambice ve vývoji pokračovat dále, ale navrhnul a připravil vše tak, aby pro jiného/nového uživatele bylo snadné simulátor dále rozšířit. Dokáži si proto představit, že se může jednat o nástroj, který relevantní vědecká komunita bude dále zušlechťovat.

9. Otázky k obhajobě

- Porovnejte Váš nástroj SimPoS s jeho předchůdcem Bitcoin Simulator (zmiňte i případné bugfixy či rozšíření stran paralelizovatelnosti).

10. Souhrnné hodnocení **90 b. výborně (A)**

Posuzovanou práci hodnotím stupněm A, kde oceňuji obě nedílné součásti - jak teoretickou tak praktickou - které není vždy úplně snadné dotáhnout do ekvivalentně výtečného stavu. Kolegovi Borčíkovi se to však podařilo.

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

V Brně dne: 8. června 2021

Veselý Vladimír, Ing., Ph.D.
oponent