Review of Master's Thesis

Student: Tamaškovič Marek, Bc.
Title: Fast, Scalable and DoS-Resistant Proof-of-Stake Consensus Protocol Based on an Anonymization Layer (id 22623)
Reviewer: Veselý Vladimír, Ing., Ph.D., DIFS FIT BUT

1. Assignment complexity — **more demanding assignment**

Zadáním se jedná o mírně obtížnější práci. Sestávalo se z dvou netriviálních částí, a to: 1) nastudování si proof-of-stake algoritmů (pro zajištění konsensu) a útoků na ně (v na blockchainu postavených distribuovaných systémech), a 2) principů směrování paketů v overlay anonimizačních sítích (jako Tor, I2P). Z těchto domén měl pak student zkombinovat to nejlepší a implementovat prototyp odolný vůči DoS na klíčové uzly.

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

Zadání bylo ve všech bodech splněno. Aktuální stav představuje prototyp, u kterého došlo ke kritické reflexi, z níž vyplynulo, že např. výkonnostní metriky jako počet transakcí za sekundu by šlo ještě vylepšit využitím kompilovaného programovacího jazyka.

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

Práce má 53 stran textu v husté LaTeXové šabloně, 59 stran i s pomocnými provozy. V rámci na fakultě vzniklého počítadla http://standardpages.herokuapp.com/standardpages/ má 68,8 normostran, 98% textu a 2% obrázků.
Dle výše uvedeného je tedy mírně pod hranicí obvyklého rozmezí DP.

4. Presentation level of technical report — **90 p. (A)**

Práce je logicky strukturovaná a její (pod)kapitoly odrážejí body zadání. Na vhodných místech je patrné správné použití UML, což libovolné jinému informatikovi usnadňuje případnou práci s výstupy.

5. Formal aspects of technical report — **80 p. (B)**

Práce je psána v angličtině, což jistě přispěje k potenciálně větší čtenářské obci, která by mohla z výstupy dále pracovat. Co se jazykové a typografické stránky týče, tak se v práci vyskytuje již rušivější (přesto ale stále malé) množství překlepů či tiskařských šotků, např:
* použití československých a nikoli anglických uvozovek;
* elementy přetékající standardní okraje stránky (např. Table 3.1 a 3.2);
* chybějící interpunkce při porušování SVOMPT pravidla.

6. Literature usage — **75 p. (C)**

Student v práci cituje z dostatečného (69 pramenů) množství relevantních zdrojů, kde nezanedbatelnou část z nich tvoří i vědecké články. Některé citace mají oproti ostatním špatný či neúplný formát (např. chybějící datum citace, více bibliografických metadat jednoznačně identifikující pramen), a to třeba [68], [60], [35], [15], [51], [67].

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

Implementačním výstupem je prototypová implementace vlastního proof-of-stake algoritmu v jazyce Python. Řádově se jedná o jednotky souborů s desítkami/stovkami autorských řádků.
Co se testování týče, tak mě aktuální stav implementace přijde složitý na programatické a opakovaně deterministické (kvůli použití RNG) testování; student v tomto očekával ale součinnost s jinou kvalifikační prací, která nakonec nebyla odevzdána.
Za pochvalu však stojí zdárné využití Metacentra sdružení CESNET k testování v masivnějším měřítku.

8. Utilizability of results

Výstupy prototypu jsou rozhodně zajímavé, rozšiřující stávající poznatky. Návrh aktuálního prototypu si dokáži představit jako torzo frameworku, na který by bylo možné nabalovat nové algoritmy a testovat je. Student má podle všeho PhD ambice, a tak jej bude pravděpodobně dále rozšiřovat, stejné jako je v plánu výsledky dále diseminovat i formou plnohodnotné vědecké publikace.

9. Questions for defence

- Podařilo se dosáhnout primárního cíle práce (tj. DoS ochrany leadera). Další metou je zvýšení propustnosti množství transakcí za sekundu o řád; z aktuálních 766 tx/s na potenciálních 2000+ tx/s. Jak by toho šlo docílit?

10. Total assessment — **89 p. very good (B)**

Práce je pro mě na pomezí výborně (A) a velmi dobře (B). Nechávám na komisi a výsledku závěrečné obhajoby popasovat se s finální známkou. Nejlepší stupeň hodnocení sráží pár šotků v textové části a neohrabanost použití

stávající implementace za účelem programatického testování; i tak ale kolega Tamaškovič zpracoval obtížnější práci nad obvyklý průměr.

In Brno 8 June 2021

Veselý Vladimír, Ing., Ph.D.
reviewer