FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Filip Volf
Oponent práce:	doc. Ing. Štěpán Starosta, Ph.D.
Název práce:	A miner for FITCOIN
Obor:	Teoretická informatika

Datum vytvoření: 10. 6. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	*1=zadání splněno,* ***2=zadání splněno s menšími výhradami,*** *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Bod 6 zadání ukládá vytvořit dokumentaci implementace. Kapitolu 5 nelze považovat za dokumentaci k implementaci, neobsahuje ani seznam metod/funkcí apod.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*65 (D)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Kapitoly 1 až 3 shrnují teoretický základ potřebný pro zbytek práce. Výběr témat mi přijde dobrý, avšak logická návaznost není zdařilá. Text je často lepen z citací a poměrně přesných parafrází, což ve výsledku zhoršuje návaznost - např. důležitá část 3.6 o samotném těžení, kde jsou termíny používány před jejich vysvětlením (to např. platí i o termínu "double spending") a celkově je text místy nejasný. Text obsahuje drobné nepřesnosti a odvážná tvrzení - např. na straně 17 se píše "Only the owner of the secret key can generate such signatures and spend the funds".

Kapitoly 4 až 6 jsou stručnější a zasloužily by doplnit detaily. V kapitole 4 není jasně označeno, co je již hotovo, a co bylo se má v této práci dodělat. Z části 4.1.3 to vypadá, že Fitcoin Miner je již hotový - tak proč jej dělat? Celkově je popis stávajícího návrhu Fitcoin příliš stručný - důležité informace musí čtenář hádat z popisu struktury bloku na straně 38. V tomto popisu se například píše, že se hashuje celý blok "Prev is the SHA256 digest of its parent block.", což není pravda (dle implementace). Popis implementace v kapitole 5 obsahuje nejasnosti u důležitý kroků (vizte Otázky k obhajobě).

Práce je psána v anglickém jazyce, obsahuje malé množství překlepů a gramatických chyb vyjma interpunkce, ta je naopak v naprosté většině případů zcela špatně. Vše se zdá být řádně ocitováno a zdroje jsou adekvátní. Na straně 3 chybí zdroj ("[?]").

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (B)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:

Přílohy obsahují celou stávající implementaci Fitcoin, tedy i výstupy jiných závěrečných prací. Nelze poznat, co přesně bylo v rámci práce uděláno. I po rozkrytí této otázky za pomoci školitele lze zdrojový kód těžko hodnotit, protože je velmi ovlivněn existujícími částmi. Obsahuje rozumné množství komentářů. Vznikají otázky, zda jsou dobře ošetřeny všechny extrémní situace (např. přetečení u změně hodnoty "target").

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*80 (B)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Implementace je funkční a doplňuje další nutnou část pro fungování Fitcoin, zasloužila by ovšem lepší dokumentaci a možná revizi volby proměnné "target" (vizte Otázky k obhajobě).

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

1. Na straně 42 se píše "Merkle root is utilized in several different ways in cryptocurrencies. In Fitcoin it's only purpose as of now is to simplify the process of hashing a block. " Vysvětlete, jak je tento strom použit při hashování bloku.
2. A) Vysvětlete, jak (za jakých předpokladů) má Algoritmus 4 zajistit podmínku, aby vytěžení každého bloku trvalo konstantní čas? B) Jak je tomu u prvních 12 bloků?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*72 (C)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Text práce trpí špatnou návazností a občasným výskytem nepřesností. Vlastní tvořivá práce je popsána příliš stručně a je těžké odlišit, co už bylo uděláno, a co je vytvořeno v této práci. Celkově je implementace funkční, i když s drobnými nedostatky.

Podpis oponenta práce: