FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Jiří Havrusevič
Oponent práce:	Ing. Jiří Buček, Ph.D.
Název práce:	Peněženka pro FitCoin
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 15. 6. 2020

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:
Student splnil zadání bez výhrad.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

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:
Písemná práce je logicky členěna, přehledná a s poměrně malým počtem chyb. Práci by prospělo důkladnější vysvětlení kontextu začlenění do celého projektu Fitcoin včetně předpokládaných situací, kdy budou volány studentovy funkce. V práci také chybí přehledný diagram, který by obrazovou formou osvětlil jednotlivé komponenty.

Matematické vzorce v kapitole pojednávající o eliptických křivkách by zasloužily pečlivější sazbu a přehlednější značení, obsahují také překlepy. Například na str. 9 vzorec pro souřadnice součtu dvou bodů P1+P2 je nejasný, zřejmě obsahuje překlep (místo = je tam -).

V kapitole 2.4.3 na str. 15 dole je nedokončená věta o digitálním podpisu.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*89 (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:
Přílohou jsou zdrojové soubory v jazyce C. Některé soubory jsou asi výsledkem práce jiných studentů, ale to není zřejmé z jejich obsahu. Studentem vytvořené soubory také nejsou označeny jménem autora. Student by měl své zdrojové soubory vždy podepsat, případně vyznačit změny do převzatých souborů. Styl psaní kódu zdá se dobrý, student se snaží ošetřovat všechny mezní situace. Student svůj kód povětšinou přiměřeně komentuje, i když např. funkce syncfreshtx by si zasloužila komentář podrobnější.

V implementaci mi chybí funkčnost digitálního podepisování transakcí, ale to je zřejmě předmětem jiné souběžné práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*85 (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:
Výsledky studentovy práce vypadají funkční, a lze předpokládat, že přispívají svým dílem k rozvoji projektu FitCoin.

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:
Vaše funkce getsec je volána zatím pouze z loadkeys, kde je její výsledek záhy zahozen. Odkud předpokládáte, že se ještě bude volat?
Proč je na některých místech vyhrazeno pro jméno adresáře jen 128 znaků? (To je málo.)

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*89 (B)*

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:
Student prokázal schopnost samostatné tvůrčí práce. Práci doporučuji k obhajobě a navrhuji klasifikovat velmi dobře.

Podpis oponenta práce: