FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Gattermayer, Ph.D.
Student:	Ihor Salov
Název práce:	Crypto pro FITCoin
Obor / specializace:	Webové a softwarové inženýrství, zaměření Softwarové inženýrství
Vytvořeno dne:	24. srpna 2021

Hodnotící kritéria

1. Splnění zadání

[1] zadání splněno
▸ **[2] zadání splněno s menšími výhradami**
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Závěr bodu 2. "Proveďte rešerši knihoven v jazyce C, které takový podpis implementují." je příliš krátký a nezdůvodňuje výběr, pro čtenáře nemá tím pádem rešerše příliš velkou informační hodnotu.

2. Písemná část práce

60 / 100 (D)

Strana 1:
- Nepovažuji za vhodný zdroj pro velikost market cap článek zpravodajské agentury (lepší použít zdroj z kterého čerpají, např. coinmarketcap.com).
- "Přítomnost hash řetězců a digitálních podpisů téměř úplně vylučuje jakékoli zpětné manipulace" je dost vágní tvrzení, existuje např. 51% attack.

Kapitola Analýza kryptografických knihoven na 10 stránkách rozebírá detaily jednotlivých implementací, avšak samotné porovnání (Zvolené řešení) je popsáno pomocí tří vět. Chybí zde jakékoliv porovnání (tabulka, dané parametry), samotná volba je zdůvodněna velice vágně.

Strana 31:
- Za odrážkami chybí tečka.

Rozsah práce 31 řídkých stran je dostatečný, avšak nikoliv vyčerpávající.

3. Nepísemná část, přílohy 90 /100 (A)

Jelikož mi nepřišla pozvánka do repozitáře dokážu hodnotit pouze na základě snipetů kodů. Zde jsem žádné problémy nezaznamenal. Zvolil bych jednodušší jazyk na implementaci než C, avšak to je součástí zadání.

4. Hodnocení výsledků, jejich využitelnost 70 /100 (C)

Výsledné řešení prošlo základními testy, avšak není zde žádná zmínka o nasazení do projektu FITCoin.

Celkové hodnocení 60 /100 (D)

Zadání nebylo příliš obtížné, vzhledem k tomu je práce zbytečně stručná a místy nepřesná. Závěr rešeršní části nezdůvodňuje finální výběr knihovny. Všechny body zadání jsou splněny.

Otázky k obhajobě

1) Jak je výsledek práce integrován do řešení FITCoin?
2) Proveďte nad Vaším lokálním FITCoin blockchainem 51% útok a zpětně zmanipulujte již provedené transakce. S postupem a výsledkem seznamte komisi.

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.