



Posudek oponenta závěrečné práce

Student: Lukáš Dang
Oponent práce: Ing. Josef Gattermayer, Ph.D.
Název práce: FITCOIN: struktura peněženky
Obor: Webové a softwarové inženýrství

Datum vytvoření: 3. 9. 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: Druhou část bodu zadání "Popište strukturu peněženky kryptoměny Bitcoin, případně i dalších kryptoměn, pokud se u nich tato struktura podstatně liší." jsem v práci nenašel. Existují kryptoměny, jejichž struktura se od struktury Bitcoinu podstatně liší. Hlubší studium více peněženek by taktéž umožnilo se vyvarovat chybám viz 3. Nepísemná část, přílohy. | |
| Hodnotící kritérium: | Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F): |
| 2. Písemná část práce | 100 (A) |
| 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 odlišené 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: K písemné části práce nemám výtky, dobrá forma, citace. | |
| Hodnotící kritérium: | Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F): |
| 3. Nepísemná část, přílohy | 70 (C) |
| 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: Nenašel jsem, jakým způsobem jsou privátní klíče šifrovány. Předpokládám tedy, že šifrovány nijak nejsou, což považuji při použití DB technologií za značně riskantní. Bylo by vhodné mít master klíč (uložený mimo databázi), kterým by byly šifrovány jednotlivé privátní klíče, aby nebyly uloženy v databázi v plain textu. | |
| 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 možnost nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky. | |
| Komentář: Pro produkční použití peněženka použitelná kvůli chybějící enkrypci privátních klíčů není, ale účel studia principů kryptoměn práce plní. | |

| Hodnotící kritérium: | Způsob hodnocení – nehodnotí se |
|--|--|
| 5. Otázky k obhajobě | |
| <i>Popis kritéria:</i> Uvedte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odřádkami). | |
| <i>Otázky:</i> 1) Navrhněte princip šifrování privátních klíčů v peněžence. 2) Popište strukturu peněženky Trinity kryptoměny IOTA. | |
| Hodnotící kritérium: | Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F): |
| 6. Celkové hodnocení | 70 (C) |
| <i>Popis kritéria:</i> 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. | |
| <i>Text hodnocení:</i> Část jednoho bodu zadání nebyla úplně splněna, v návrhové části se vyskytuje bezpečnostní chyba. Pokud obojí student dostatečně jasně vysvětlí u obhajoby není problém hodnocení zvýšit, pokud nikoliv je na diskuzi, jestli bylo zadání splněno. Zbytek práce považuji za kvalitní jak po formální, rešeršní, návrhové i implementační stránce. | |

Podpis oponenta práce: