



## Hodnocení vedoucího závěrečné práce

**Student:** Matouš Skála  
**Vedoucí práce:** Mgr. Jan Starý, Ph.D.  
**Název práce:** Bitcoin Wallet for Android with TREZOR Hardware Wallet Support  
**Obor:** Teoretická informatika

**Datum vytvoření:** 13. 6. 2018

<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – následující škálou 1 až 4:</i>
<b>1. Splnění zadání</b>	<b><u>1=zadání splněno,</u> 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno</b>
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Práce splňuje všechny body zadání.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>2. Písemná část práce</b>	<b>90 (A)</b>
<i>Popis kritéria:</i> Zhodnotte 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. Zhodnotte 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. Zhodnotte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.	
<i>Komentář:</i> Práce je sepsána pečlivě. Úvodní kapitoly poslouží jako úvod do problematiky kryptoměn, i když obsahují některé drobné chyby (charakteristika podkladového tělesa nemůže být dvě ani tři, diskriminant eliptické křivky by neměl být nulový, stejně tak prvky podpisu R,S by měly být nenulové). Podobně kvalitní popis samotného fungování peněženek pro kryptoměny myslím v češtině neexistuje. Kapitola 3 popisuje podporu hardwarové peněženky TREZOR v různých mobilních peněženkách. Kapitola 4 pak popisuje samotnou vytvořenou aplikaci.  Práce je sepsána kvalitní, i když místy neformální angličtinou.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>3. Nepísemná část, přílohy</b>	<b>100 (A)</b>
<i>Popis kritéria:</i> Die 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	
<i>Komentář:</i> Hlavními výsledky jsou 1. knihovna pro komunikaci Androidu se zařízením TREZOR 2. na této knihovně postavená Android peněženka pro Bitcoin. Díky tomuto oddělení knihovny a aplikace je možné TREZOR použít nejen jako HD peněženku, ale jako obecné kryptografické zařízení (totiž ke správě klíčů, k podpisu předložených dat, atd). Vytvořená peněženka navíc dokáže synchronizovat metadata (account labels) pomocí spojení s dropboxem (kde ukládá tato metadata v zašifované podobě).	

<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>4. Hodnocení výsledků, jejich využitelnost</b>	<b>100 (A)</b>
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Aplikace je plně použitelná a může směle konkurovat existujícím Andorid peněženkám. Řešitel spolupracuje na podpoře TREZORu přímo s výrobcem Satoshi Labs.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – následující škálou 1 až 5:</i>
<b>5. Aktivita a samostatnost studenta</b>	5a: <b>1=výborná aktivita,</b> 2=velmi dobrá aktivita, 3=průměrná aktivita, 4=slabší, ale ještě dostatečná aktivita, 5=nedostatečná aktivita 5b: <b>1=výborná samostatnost,</b> 2=velmi dobrá samostatnost, 3=průměrná samostatnost, 4=slabší, ale ještě dostatečná samostatnost, 5=nedostatečná samostatnost
<i>Popis kritéria:</i> V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatně tvůrčí práce (5b).	
<i>Komentář:</i> Řešitel pracoval od začátku zcela samostatně, systematicky a cílevědomě. Na pravidelné konzultace byl vždy výborně připraven.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>6. Celkové hodnocení</b>	<b>95 (A)</b>
<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> Práce stojí textem i softwarovým zpracováním značně nad průměrem BP. I přes nedostatky v teoretické části si myslím zaslouží nejvyšší hodnocení.	

Podpis vedoucího práce: