FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Bc. Václav Chmel
Vedoucí: práce: Ing. MSc. Martin Jakl
Název práce: Autentizace, autorizace a evidence zařízení pomocí platformy Ethereum
Obor: Webové a softwarové inženýrství

Datum vytvoření: 30. 5. 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:
V sirsim kontextu projektu autentizace pomoci site Ethereum povazuji zadani za splnene. Analyza problemu, identifikace chybejici funkcnosti (sprava uctu na mobilnich zarizenich) a implementace prvni verze ERC 725.
(Z pohledu doslovneho zadani diplomove prace doslo k castecne odchylce, ale to je z casti problem zadani prace a z casti zasadni zmena standardu ERC 725)

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 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:
Rozsah prace odpovida zadani a povazuji ho za vyhovujici. Obzvlaste reserse existujicich technologickych reseni a popis pozadavku je na vysoke urovni.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*75 (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:
Vysledny program AEW odpovida rozsahu diplomove prace. Vhodna volba navrhu reseni, odpovidajici volba stavajicich knihoven, vyuziti open-source. V teto casti prace bohuzel chybi puvodni implementace ERC 725. ERC 725 je standard pro praci s 'identity' na siti Ethereum a tento standard byl pouze ve fazi navrhu (draft).
Student plne implementoval cely standard jako sadu smart-contracts v jazyce Solidity, ovsem nasledne byl cely standard prepsan a tedy implementace pozbyla aktualnosti. To je bezny cyklus vyvoje sw, ovsem implementace mela byt soucasti prilohy pro demonstraci zvladnuti problemu programovani smart-contracts.

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:

Vysledkem je funkci program na spravu Ethereum uctu na platforme Android. Prestoze se vysledna aplikace muze jevit pouze jako 'dalsi' Android penezenka, jedna se o pomerne unikatni program poskytujici ostatnim aplikacim podpis a verifikaci podpisu jako sluzbu.
Uvodni implementace ERC 725 (bohuzel nepublikovana jako soucast diplomove prace) bude slouzit jako zaklad implementace nove verze ERC 725.

Uvedene vysledky jsou kriticke pro pokracovani nase projektu autentizace pomoci site Ethereum (projekt pokracuje nad ramec diplomove prace)

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 samostatné tvůrčí práce (5b).

Komentář:

Student byl aktivni po celou dobu prace a pravidelne konzultoval. Iniciativne vyhledaval odbornou literaturu a open-source projekty, kde se i aktivne podilel v diskusich s ostatnimi uzivateli a autory pouzivanych knihoven.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*80 (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:

Prace dobre demonstruje uskali vyvoje sw. Funkcnost bezne dostupna na jedne platforme (sprava uctu Ethereum pomoci MetaMask v desktop prohlizecich), neni dostupna na ostatnich platformach (kuprikladu mobilni platforma Android). Dale demonstruje uskali vyvoje novych technologii, kdy navrh standardu resi problem (Identity a ERC 725), ale az nasledna implementace odkryje zasadni nedostatky ve standardu, coz vede k jeho zasadni zmene.

Praci hodnotim kladne, pisemna cast a analyza je na vysoke urovni. Prestoze prace castecne nedodala reseni ze zadani (funkcni sadu smart-contracts), umoznuje pokracovani projektu. Odchylka od zadani byla castecne ne zcela vhodnou formulaci zadani a nasledne problemy v uvodni definici standardu ERC 725.

Podpis vedoucího práce: