FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Posudek oponenta závěrečné práce

| | |
|---|---|
| **Student:** | Jaroslav Pešek |
| **Oponent práce:** | Ing. Josef Gattermayer, Ph.D. |
| **Název práce:** | Aplikace technologie Blockchain v chytrých konktraktech |
| **Obor:** | Bezpečnost a informační technologie |

**Datum vytvoření:** 10. 6. 2019

| *Hodnotící kritérium:* | *Způsob hodnocení – následující škálou 1 až 4:* |
|---|---|
| **1. Splnění zadání** | *1=zadání splněno,*<br>*2=zadání splněno s menšími výhradami,*<br>***3=zadání splněno s většími výhradami,***<br>*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:*
Práce odevzdána, ale v praxi by to moc nefungovalo.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **2. Písemná část práce** | *80 (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:*
Hned v úvodu dvě věty považuji za mírně přehnané či nepravdivé:
"Decentralizovane? aplikace v ra?mci internetu zaz?i?vaji? v posledni?ch letech mimor?a?dny? rozmach."
"Te?ma jsem si zvolil, nebot? technologie blockchain je velmi mlada?"

Úvod do kapitoly 2.4 Transakce je více formou deníkového zápisu než technického textu.

Formální chyby:
Strana 23 - nevhodně použité odrážky (chybí interpunkce), je takto v celé práci.
Strana 34 - "jiný tip otázek"

Minianalýza ostatních kryptoměn se smart contracty srovnává pouze dle tržní kapitalizace. To rozhodně není důvodem, proč vybrat pro danou aplikaci Ethereum.
Zváženy měly být minimálně následující faktory: transakční náklady, možnosti smart contractů v daném jazyce, podpora vývojářských nástrojů,

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **3. Nepísemná část, přílohy** | *50 (E)* |

*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:*
Zvažování ring signatures považuji pro use-case volby na FITu za overkill. Každá identita zastupovaná veřejným klíčem je anonymní dokud není svázána s konkrétní osobou - identity se dají vygenerovat i jednorázově pouze pro účel volby,

Je rozdíl mezi osobními údaji (přímá identifikace jednotlivce) a digitální stopou. Celá polemika ohledně GDPR na straně 42 stojí na citaci akademické práce, ale implementátory nařízení jsou vždy národní úřady jednotlivých členských států. Nelze se tedy držet rigidního výkladu, že veřejný klíč = osobní data.

Proof of concept na straně 43 v podstatě popírá vhodnost volby dané kryptoměny (která nebyla zdůvodněna). Kvůli transakčním poplatkům je vytvořen privátní blockchain, čímž se automaticky ztrácí jakékoliv výhody blockchainu. Tady přestala práce defacto dávat smysl.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Hodnocení výsledků, jejich využitelnost** | *50 (E)* |

*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:*
Aplikace jak je navržena by nikdy nefungovala (privátní blockchain), nebo za cenu naprosto neadekvátních nákladů (mainnet).

| *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:*
Proč jste zvolil pro aplikaci měnu Ethereum? Vyčíslete přesně GAS náklady na jedny volby do AS na FITu v prostředí mainnet. Pokud z nějakého důvodu trváte na Ethereu, popište, jak provoz aplikace zlevnit (jiný než mainnet blockchain nepřipadá v úvahu neboť se poté nejedná o blockchain). Hint - Plasma, Raiden.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **6. Celkové hodnocení** | *50 (E)* |

*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:*
Cílem práce bylo udělat teoretickou rešerši, nalézt vhodný use case a provést prototypovou implementaci distribuované aplikace.

Teorie tvoří sice značnou část práce, avšak mezi popisovanou kryptografií a implementací SW díla je ještě obrovský kus práce, který zůstal víceméně nepokryt.

Chybí základní rešerše, pomocí kterých nástrojů (kryptoměn, jejich nadstaveb atd.) docílit daného use-casu. Výsledkem toho vznikne Ethereum aplikace, o které sám autor tvrdí, že by byla na provoz drahá, tudíž ji nemá smysl provozovat na veřejném blockchainu. To by mělo být dostatečné varování, že je něco špatně. Na technické univerzitě by neměly vznikat práce typu "děláme blockchain, protože je to cool, i když to nedává smysl".

Inženýrsky zajímavých řešení daného problému je přitom spousta a většina z nich leží právě v oblasti, kterou práce nepokrývá.

Pokud mělo být ale cílem práce převážně zorientování se v kryptografii, na které stojí technologie blockchain, tak je moje kritika nerelevantní a jsem pro výrazně lepší hodnocení.

Podpis oponenta práce: