



Posudek oponenta závěrečné práce

Student: Vladislav Khomchenko
Oponent práce: Ing. Josef Gattermayer, Ph.D.
Název práce: Možnosti komerčního využití technologie blockchain
Obor: Webové a softwarové inženýrství

Datum vytvoření: 10. 6. 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: Návrh implementace si představuji jinak. | |
| 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: Překlep hned v úvodu "s technického pohledu" Musel jsem hledat, co znamená "haš". Opravdu to znamená i český překlad hash. Jinak formálně v zdařilé. | |
| 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: Nebyly. | |
| Hodnotící kritérium: | Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F): |
| 4. Hodnocení výsledků, jejich využitelnost | 40 (F) |
| 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:

5.2 Nevýhody technologie

Pro oba zmiňované problémy existují řešení, možná bylo vhodné diskutovat. Problém 5.2.3. se netýká bezpečnosti technologie blockchain jako takové, ale bezpečnosti centralizovaného úložiště privátních klíčů, což s technologií blockchain nemá nic společného. 5.2.4. je již úplná spekulace, blockchain rozhodně není "klíčovým nástrojem pro podvodníky", není citován žádný zdroj co toto tvrdí.

8.1 Analýza požadavků

F7: Odkud se vzal požadavek na privátní blockchain? V zadání práce není, privátní blockchain neposkytuje oproti běžné databázi téměř žádné výhody.

Mezi nefunkčními požadavky chybí specifikace, kolik mají (mohou) dané transakce stát a kolik mají obsluhovat uživatelů. To ovlivňuje volbu technologie.

8.7 Volba implementačního jazyka

Shrnout celou kapitolou, která má určit technické řešení do jednoho odstavce, který doporučí jazyk C++, protože se jedná o "kvalitní programovací jazyk" je naprosto nedostatečné. Zde měla následovat řešese vhodných blockchainových implementací - Ethereum, Tezos, KIN, Hyperledger. Poté měl teprve následovat návrh architektury, který je zde proveden "na slepo", tudíž neodpovídá případné implementaci. Teprve poté se měl řešit programovací jazyk s přihlédnutím k tomu, co která blockchain implementace nabízí za knihovny.

Celé to mělo vypadat např. takto - <https://github.com/ETHLend/Documentation/blob/master/ETHLendWhitePaper.md>.

Hodnotící kritérium:

Způsob hodnocení – nehodnotí se

5. Otázky k obhajobě

Popis kritéria:

Uvedte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Jaký konkrétní blockchain byste zvolil pro implementaci a proč?

Jak by vypadala architektura aplikace pro tento blockchain?

Jaké by byly konkrétně náklady na provoz (cena v GAS či jiné měně) za jednu uzavřenou půjčku?

Jak by vypadaly základní smart contracty?

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:

Analytickou část práce považuji za velice zdařilou, hodnotil bych B. Návrhová část není ale opřena o žádnou analýzu technologie a je proto zcela nedostatečná z pohledu SW inženýrství. Dle návrhové části by mělo být možné začít implementovat SW dílo, což zde opravdu možné není. Samostatně bych hodnotil za F, působí dojmem že byla práce odevzdána v půlce.

Podpis oponenta práce: