FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Gattermayer, Ph.D.
Student:	Kryštof Rašovský
Název práce:	Bezpečnostní analýza consensus protokolů v technologii blockchain
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	11. června 2024

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

2. Písemná část práce 80 /100 (B)

Poznámky mám již k zadání práce:
- blockchain není buzzword, je to technologie stará přes 10 let,
- není pravda, že většina attack vectors jsou na úrovni consensus protokolu (citation needed), v roce 2023 nebyl v top 10 ani jeden (https://www.theblock.co/post/268831/the-10-largest-crypto-hacks-and-exploits-of-2023).

Poznámky k textu:
- blockchain is buzzword nepatří do technického textu (strana 2),
- na straně 19 bych místo víceúrovňových bullets uvítal tabulku nebo diagram,
- "I believe that", " I, therefore, decided", "I consider" nepatří do technického textu (strana 35).

3. Nepísemná část, přílohy 90 /100 (A)

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

Výsledků práce byl dosaženo, ale jejich využitelnost v praxi je hodně teoretická.

Celkové hodnocení 85 /100 (B)

Práce se zabývala zmapováním a simulací hrozeb blockchain sítí (obecně) na úrovni consensus protokolu.

Kapitola Aplikace blockchain technologie se zaměřuje na Smart Cities, ICOs, volby, supply chain. Nic z toho se nepoužívá, jedná se o překonané koncepty (cca rok 2017), student čerpal ze starší literatury. Naopak není vůbec zmíněn use case DeFi (decentralizované finance), který se jako jediný používá (Total Value Locked $102.829b, zdroj: DefiLlama 06/2024).

Věta závěru "The thesis aimed to create a comprehensive security analysis of the blockchain technology, focusing primarily on the consensus layer" je oxymoron. Zaměření práce bylo velice úzké (consensus útoky), nejedná se o "comprehensive security analysis of the blockchain technology".

Cíl práce (jak byl vytyčen) se podařilo splnit, formálně je práce na velice vysoké úrovni. V textu se vyskytuje několik nesrovnalostí, proto B. Obecně práci chybí větší nadhled a propojení s aktuálními trendy vývoje.

Otázky k obhajobě

Popište, jak mohou blockchain protokoly využít consensus protokolu pomocí restakingu (nastudujte např. EigenLayer).

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.