



# Posudek oponenta závěrečné práce

**Oponent práce:** Mgr. Martin Jureček, Ph.D.  
**Student:** Bc. Lukáš Böhm  
**Název práce:** Rozšíření nástroje Woke  
**Obor / specializace:** Počítačová bezpečnost  
**Vytvořeno dne:** 30. května 2022

## Hodnotící kritéria

### 1. Splnění zadání

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

Všetky body zo zadania považujem za splnené.

### 2. Písemná část práce

70/100 (C)

Práce je dobre členená a má odpovedajúci rozsah. V prvej kapitole je dobre spracovaný úvod do Etherea. V 2. kapitole je zbytočne obširne rozpísaná špecifikácia programovacieho jazyka Solidity. Bolo by vhodné, aby sa časť kapitoly venovala možným bezpečnostným zraniteľnostiam smart kontraktov a prípadne popisu nejakej zraniteľnosti/chyby, ktorá bola využitá v reálnom svete. Popis nástrojov je v 3. kapitole pekne spracovaný. Pri nástroji Slither mi chýbalo, aké bezpečnostné zraniteľnosti vie odhaliť – aspoň vymenovanie zopár z nich. Takisto by bolo vhodné uviesť, aké sú všeobecné možnosti automatickej analýzy smart kontraktov z hľadiska bezpečnosti.

Zoznam ďalších nedostatkov:

- niektoré pojmy uvedené v práci sú definované až neskôr v texte (napr. vytěžení, Wei, gas) a niektoré pojmy nie sú v práci presne definované (napr. mempool, exekučné prostredie I) a nakoniec niektoré pojmy v práci nie sú definované vôbec (napr. RLP je uvedené len v zozname skratiek).
- obrázky nie sú uvedené v texte.
- odkaz [9] má uvedeného ako autora T. T. a uvedený link je v nesprávnom tvare, link na stránku u zdroja [17] nefunguje.
- preklepy: zdrojový kód, Ethereum, limitaca, následjící, ... str. 20: "Během vykonávání inicializačního (chýba slovo KÓDU) existuje adresa... neobsahuj (chýba E)..."
- text častokrát siaha až za okraj
- odkazy na jednotlivé sekcie sú v texte uvedené len číslom a občas nie je na prvý pohľad

jasné, či ide o číslo sekcie alebo nie, napr. str. 49 (...hlavičky 4.2.2 ...) alebo str. 50 (...LSP 4.2.1.).

### **3. Nepísemná časť, prílohy**

85 /100 (B)

Implementácia LSP servera do nástroja Woke je vykonaná prehľadne a správne. Škoda, že v rámci 4. kapitoly nebola implementovaná aspoň analýza/detekovanie nejakej jednoduchšej bezpečnostnej chyby.

### **4. Hodnocení výsledků, jejich využitelnost**

90 /100 (A)

Autor naimplementoval LSP server, ktorý bude následne používaný v nástroji Woke. Táto funkcionálnosť (LSP server) určite patrí do jadra nástroja Woke a je prerekvizitou pre vývoj jeho ďalších častí a funkcionálností.

### **Celkové hodnocení**

75 /100 (C)

Na základe popisu Ethera a príslušných nástrojov pre vývoj smart kontraktov si myslím, že autor problematike rozumie. Text práce obsahuje relatívne dosť nedostatkov, vid' zoznam vyššie. Taktiež v práci chýba popis konkrétnych bezpečnostných chýb a nie sú uvedené možnosti automatickej analýzy/vyhľadávania týchto chýb. Celkovo hodnotím prácu známku C.

### **Otázky k obhajobě**

1. Aké sú možnosti automatickej analýzy smart kontraktov z hľadiska bezpečnosti?
2. Na str. 55 je v posledných 2 vetách stručne spomenutý plán na automatický detektor chýb a ďalšie funkcionality. Môže autor uviesť podrobnosti?

## **Instrukce**

### **Splnění zadání**

Posudte, 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, posudte 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 posudte, 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. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, 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.