Posudek oponenta diplomové práce

Student: Handzuš Jakub, Bc.
Téma: Semi-centralizovaná kryptoměna založená na blockchainu a trusted computing (id 23528)
Oponent: Veselý Vladimír, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání — značně obtížné zadání

Svou povahou se dle mě jedná o značně obtížné zadání, kde teoretická část je široce rozkročená napříč technologiemi a praktická implementace v sobě kombinuje:

1. trusted computing programování (v Intel SGX);
2. integrální prvky blockchainových technologií (na C/C++ postavená dynamicky se rozšiřující platforma vedoucího Aquareum);
3. návrh komunikačního protokolu zabezpečeného kryptografií (s ohledem na paranoiu v chování v komunikaci zúčastněných stran).

Cílem práce bylo navázat na vývoj subsystému v platformě Aquareum a rozšířit komunikační model cílící na synchronizaci stavu např. mezi bankovními institucemi, pro které může trusted computing představovat klíčovou vlastnost.

2. Splnění požadavků zadání — zadání splněno

Všechny body zadání byly splněny. I když aktuální prototyp řeší jen kus celého návrhu, tak studentova část implementace zdárně pokrývá všechny práci vytyčené cíle.

3. Rozsah technické zprávy — je v obvyklém rozmezí

Práce má 53 stran textu v husté LaTeXové šabloně, 59 stran i s pomocnými provozy. V rámci na fakultě vzniklého počítadla http://standardpages.herokuapp.com/standardpages/ má 89,57 normostran, 99% textu a 1% obrázků.
Dle výše uvedeného je tedy v obvyklém rozmezí DP.

4. Prezentační úroveň předložené práce — 90 b. (A)

Práce je logicky strukturovaná a její (pod)kapitoly jasně kopírují jednotlivé body zadání. Práce je čtivá; některé koncepty (např. Intel SGX v kapitole 2.1) jsou vysvětlovány stravitelně, ač se ve spoustě případů jedná o téma na samostatnou knihu.

5. Formální úprava technické zprávy — 85 b. (B)

Práce je psána ve slovenštině, i proto gramatickou stránku věci nejsem sto schopen správně posoudit. Co se týče typografie, anotování obrázků a diagramů, tak se zdá býti bez prohřešků. Nicméně osobně bych preferoval:

- nemíchat zkrácené a nezkrácené identifikátory, například Obr. 4.4 avšak v textu obrázek 4.4;
- u některých obrázku zvětšit velikost písma anotací (např. LockTransfers[] v Obr. 5.1), protože v tištěné podobě by mohly být těžko čitelné.

6. Práce s literaturou — 80 b. (B)

Student v práci cituje z dostatečného (57 pramenů) množství relevantních zdrojů, kde nezanedbatelnou část z nich tvoří i vědecké články. Některé citace mají oproti ostatním špatný či neúplný formát (např. chybějící datum citace, více bibliografických metadat jednoznačně identifikující pramen), a to třeba [38], [45], [1], [3], [4] a [5].

7. Realizační výstup — 90 b. (A)

Implementačním výstupem jsou:

- desítky souborů v C/C++ s desítkami až stovkami autorských řádků zdrojového kódu rozšiřujících platformu Aquareum;
- soubory smart kontraktů v jazyce Solidity;
- soubory s jednotkovými testy v různých jazycích (Python, JavaScript).

Student výrazně autorsky přispěl jak k rozvoji komunikačního schématu mezi aktéry, tak platformy Aquareum samotné.

8. Využitelnost výsledků

Práce studenta navazuje na práci jeho vedoucího (který obhospodařuje Aquareum) a dá se tak očekávat

diseminace výstupů.
Za největší přínos považuji, že student "prošlápnul pěšinu" využití trusted computingu za použití Intel SGX v doméně blockchainových technologií, takže dalším přispěvatelům Aquarea to půjde již snadněji.

9. Otázky k obhajobě

- Rozveďte detailněji testování popsané v kapitole 6.5. Můžete se zaměřit na nástroje třetích stran a jejich vzájemné skloubení.

10. Souhrnné hodnocení **90 b. výborně (A)**

Práci hodnotím jako výbornou (tedy stupněm A). Kolega Handzuš byl v poměrně krátkém čase (alespoň dle mě na toto téma) schopen se zorientovat v trusted computingu a blokchainových technologiích, proniknout do jejich konkrétních zástupců (Intel SGX a Aquareum). Následně pak přispěl k návrhu a implementaci dynamicky bujícího kódu Aquarea, kde své rozšíření podrobil kritické debatě ohledně bezpečnostních vlastností.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 8. června 2021

Veselý Vladimír, Ing., Ph.D.
oponent