Review of Master's Thesis

Student: Slávka Samuel, Bc.
Title: Mobile Cryptocurrency Wallet Based on zk-SNARKs and Smart Contracts (id 23223)
Reviewer: Perešíni Martin, Ing., DITS FIT BUT

1. Assignment complexity — **more demanding assignment**

Diplomová práca sa zaoberá problematikou mobilnej peňaženky (odľahčeného klienta) na prácu s kryptomenami. Prácu hodnotím ako **náročnejšiu**, pretože študent si musel naštudovať princípy blockchain technológií, musel sa oboznámiť s progamovými princípmi smart kontraktov a využiť inovatívne kryptografické konštrukty ako zk-SNARKs.

2. Completeness of assignment requirements — **assignment fulfilled**

Zadanie považujem za **splnené**, študent zanalyzoval danú problematiku, oboznámil sa s validáciou, podpisovaní blokov v blockchaine a rôznych schémach, ako sú schnorr, pixel, BLS podpisy a zero knowledge dôkazy: zk-SNARK, zk-STARK. Študent navrhol aplikačný rámec pozostávajúci z klienta (mobilný aplikácia), servera a samotného blockchainu s ktorým sa interaguje (smart kontrakty). Študent následne implementoval samotný framework v podobe mobilného klienta napísaného v ReactJS a naimplementoval smart kontrakty v Solidity s využitím knižnice Zokrates na overovanie hlavičiek blockchainu. Po implementácii študent svoju prácu vyhodnotil, čiastočne ju porovnal s inými existujúcimi riešeniami a diskutoval o problémoch týkajúcich sa najmä požiadaviek na výpočtový výkon. Pozitívne hodnotím aj vypracovanie práce v anglickom jazyku.

3. Length of technical report — **within minimum requirements**

Rozsah technickej správy je približne 60 normostrán. Dĺžka práce je teda **mierne nad minimálnym** očakávaným rozsahom diplomovej práce. V technickej správe sú uvedené relevantné informácie, ale mohlo ich byť viac.

4. Presentation level of technical report — **85 p. (B)**

Práca má logickú štruktúru, poradie kapitol je vhodne zvolené a celkovo je práca napísaná **zrozumiteľne** pre čitateľa. Moje výhrady sa týkajú toho, že na niektoré obrázky nie sú odkazy (obrázok 2.1), obrázok 4.1 a 4.2 obsahuje štylistické chybky, poznámky pod čiarou sú nefunkčné (url, strana 14), v niektorých pasážach chýbal plynulý prechod medzi textom a na konci kapitol by mohlo byť menšie zhrnutie pre lepšiu orientáciu a prioritizáciu dosiahnutých výsledkov. Práca by tiež mohla byť rozsiahlejšia a zachádzať do zaujímavejších detailov (priestor na to tam je).

5. Formal aspects of technical report — **85 p. (B)**

Text práce je napísaný v **angličtine**. Jazyková úroveň práce je dobrá. Z typografického hľadiska nemám k práci žiadne výhrady.

6. Literature usage — **95 p. (A)**

Študent využíva relevantné zdroje, čerpá informácie z webových stránok a príručiek dostupných na internete a z odbornej literatúry. Jediné mínus vidím v tom, že citácie mohli byť vo väčšom množstve, napriek tomu hodnotím prácu s literatúrou ako **uspokojivú**.

7. Implementation results — **90 p. (A)**

Realizačný výstup práce **splnil** špecifikáciu. Výstupom implementácie je vytvorenie aplikačného frameworku pozostávajúceho z klienta (mobilnej aplikácie), servera a smart kontraktov, ktoré sú nasadené na blockchaine. Študent musel implementovať riešenie vo viacerých programovacích jazykoch, ako napríklad ReactJS, Solidity + knižnica Zokrates a iné. Okrem samotnej implementácie študent overil funkčnosť riešenia a analyzoval požiadavky na výpočtový výkon. Samotný kód vyzerá byť v poriadku.

8. Utilizability of results

Vo výsledkoch tejto práce vidím potenciál. Ide o zaujímavý koncept mobilného klienta, ktorý zrejme nemá konkurenčné riešenia a stálo by za to takéhoto klienta rozšíriť a prípadne aj zverejniť.

9. Questions for defence

1. Kde všade sa podľa vás dajú zk-SNARK, zk-STARK využiť v blockchainoch?
2. Ako by sa dala ďalej zlepšiť veľkosť batchu (počet hlavičiek) a má to vplyv len na výpočtový výkon alebo hrá úlohu aj spotreba gas-u (a jeho cena)?

10. Total assessment — **85 p. very good (B)**

Študent splnil všetky povinné body zadania. Práca dosahuje kvality z hľadiska prevedenia, spracovania a úpravy textu, len mierne zaostáva v rozsahu. Práca bola napísaná v anglickom jazyku a jazyková úroveň napísaného

textu je dobrá, čo hodnotím pozitívne. Realizácia je zaujímavá a má potenciál. Celkovo hodnotím výsledok ako **nadpriemerný** a navrhujem študentovi známku **B**.

In Brno 1 June 2022

Perešíni Martin, Ing.
reviewer