Posudek oponenta bakalářské práce

Student: Jacko Martin
Téma: Decentralizovaný biometrický autentizační systém (id 25056)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno**

Všechny body zadání byly splněny v dostatečné kvalitě.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Rozsah technické zprávy odpovídá požadavkům na bakalářskou práci.

4. Prezentační úroveň předložené práce **75 b. (C)**

Logická struktura práce je na velmi dobré úrovni. Autor vhodným způsobem představuje řešenou problematiku a technologie potřebné k porozumění větších detailů. V kap. 2 a 3 mohl zpracovat i konkrétní představitele biometrických autentizačních systémů a blockchainové protokoly resp. diskutovat jejich podstatné parametry. V části popisující návrh a implementaci chybí několik podstatných částí jako je diskuze volby Etherea, diskuze vlivu ceny gas na celý systém, detailnější popis smartkontraktu a informací uložených v blockchain. Chybí větší diskuze k dopadům použití blockchainu (jeho režii apod), což mělo být asi jádro práce a diskuze možnosti reálného nasazení.

5. Formální úprava technické zprávy **75 b. (C)**

Jazyková a stylistická stránka práce i úroveň typografie je na velmi dobré úrovni. Práce obsahuje jen minimum chyb. Obrázek 2.1 je anglicky a ve špatném rozlišení.

6. Práce s literaturou **75 b. (C)**

Odkazované zdroje jsou relevantní tématu a vhodně vybrány.

7. Realizační výstup **85 b. (B)**

Realizační výstup je na dobré úrovni. Proof-of-koncept zapracování blochainu je funkční, testování je dobře zpracováno. Hlavní výtku mám k návrhu celého řešení. Autor přidal nutnost asymetrické kryptografie v prvním kroku uživatele, čímž se z řešení stala defacto vícefaktorová autentizace a navíc nebezpečně využitá (uživatel se vzdává svého soukromého klíče ve prospěch MainModule, žádné solení při ukládání klíčů apod). Diskutabilní je i navržené zapojení hybridního šifrování a využití smartkontraktu pro běžný zápis do blockchainu. Chválím naopak snahu využít existujících standardů, např. pro formát authentizačního řetězce.

8. Využitelnost výsledků

Vzhledem k vysoké abstrakci nevidím žádné další využití simulátoru.

9. Otázky k obhajobě

1. Vysvětlete nutnost použití smartkontraktu pro zápis do blockchain a popište co vše se zapisuje.
2. Jaká je režie navrženého protokou v kontextu blockchain (potřebný gas, ..)?
3. Ethereum jste vybral z důvodu škálovatelnosti. Je to vhodný parametr? Očekáváte velké počty autentizací, resp. tolik souběžných vstupů?

10. Souhrnné hodnocení **75 b. dobře (C)**

Kvalitu práce snižují chybějící textové části a chyby v návrhu, naopak implementace je na velmi dobré úrovni.

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

V Brně dne: 29. května 2022

Malinka Kamil, Mgr., Ph.D.
oponent