Posudek oponenta bakalářské práce

Student: Mračna Štefan
Téma: Decentralizovaný autentizační systém založený na blockchainu (id 24761)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Přestože se evidentně jedná o výzkumné téma, vzhledem k obecnosti zadání a tím získané volnosti při řešení hodnotím témat jako průměrné.

2. Splnění požadavků zadání **zadání téměř splněno**

Všechny body zadání byly splněny v alespoň základní kvalitě.

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

Rozsah technické zprávy odpovídá požadavkům na bakalářskou práci.

4. Prezentační úroveň předložené práce **63 b. (D)**

Práce je převážně psána jako souvislý nestrukturovaný text, ve kterém se hůře orientuje a zpětně vrací k podstatným faktům. Na druhou stranu je solidně psaný, dobře se čte, obsahuje všechny podstatné informace (i když většina je popsána jen na obecné úrovni) a ukazuje dobré pochopení všech oblastí. Z metodického hlediska mi chybí ukázka konkrétních biometrických systémů a jejich designu pro lepší porovnání s navrženým řešením. Popis navrženého systému je podán obtížně stravitelnou formou s minimem schémat. Není jasné, co všechno a proč se ukládá do blockchainu. Nijak nejsou odůvodněny designová rozhodnutí ani možné alternativy (např. proč zrovna PBFT).
Součástí řešení je i testování výkonnosti simulátoru, kdy jsou testovány různé parametry útoku. Chybí větší diskuze k dopadům použití blockchainu, což mělo být asi jádro práce.

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

Jazyková a stylistická stránka práce i úroveň typografie je na dobré úrovni. Nicméně práce obsahuje menší množství gramatických a obsahových chyb, jako je např. nekonzistence terminologie v obrázcích a textu (viz obr 2.5.) a 3.1 (čip vs. otisk prstu).

6. Práce s literaturou **75 b. (C)**

Odkazované zdroje jsou relevantní tématu a vhodně vybrány.

7. Realizační výstup **63 b. (D)**

Tím, že nikde nejsou blíže specifikovány funkční a nefunkční požadavky na řešení, tak nebylo jasné, co přesně mělo vlastně vzniknout. Realizační výstup je pak ve výsledku simulátor chování biometrického systému, který v jedné své části využívá blockchain. Implementace odpovídá návrhu, ale v podstatě všechny komponenty systému byly silně abstrahovány - není využit žádný reálný blockchain protokol, všechny uzly a jejich chování jsou simulovány atd. Dále nedošlo k použití žádný knihoven, které mohly usnadnit implmentaci (blockchain, merklovy stromy atd.), což vedl k velmi simplistickému pojetí celé práce, kdy se většina funkcionality abstrahovala. Nekorektní je i implementace mempoolů a pojetí transakcí a bloků, kdy oproti blochainovým principům je zde blok použit jen jako logické ohraničení a systém pracuje s jednotlivými transakcemi ještě před jejich zveřejněním v bloku. Simulátor je nicméně funkční, součásti je i implementace testů.

8. Využitelnost výsledků

Vzhledem k vysoké abstrakci nevidím žádné další využití simulátoru.

9. Otázky k obhajobě

1. Vaše simulace předpokládá množství decentralizovaných uzlů, které implementují komparátory. Vysvětlete, jak by to mělo fungovat v reálném nasazení v kontextu, který v práci popisujete (tedy vstupní dveře).
2. V části 2.2.3 tvrdíte, že nad daty uloženými v blockchain má uživatel větší kontrolu než v centralizovaném řešení. Data jsou tímto ovšem veřejná pro účastníky protokolu, takže se uživatel kontroly de facto vzdává. Vysvětlete.
3. Využil jste PBFT jako reprezentanta blochain protokolů. Proč zrovna tento protokol a jaké jsou jiné alternativy?

10. Souhrnné hodnocení **69 b. uspokojivě (D)**

Student si kreativně zpřesil poměrně obecné zadání a své návrhy implementoval. Některá designové rozhodnutí jsou diskutabilní, velké možství věcí je abstrahováno a zjednodušeno. Práce mohl dosáhnout větší kvality, kdyby vše nebylo tvořeno na zelené louce.

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