Posudek oponenta bakalářské práce

Autor/autorka práce: **Martin Procházka**

Název práce: **Bezpečné předávání zpráv s využitím Blockchainu**

Obsah práce

V první, teoretické, části práce je popsána motivace vzniku této práce a jsou představeny jednotlivé dále používané technologie. V druhé, praktické, části je popsán nově navržený systém, jeho implementace, postup nasazení a provedené funkční testy. Tato část práce je zpracována přehledně a jednotlivé části zde lépe logicky navazují. Celkový počet stran práce je vyšší než je obvyklé u bakalářských prací, což zjevně bylo nutné s ohledem na komplexnost zvoleného řešení.

Kvalita řešení a dosažených výsledků

Výsledný software je funkční a splňuje primární cíl zadání, tedy umožnit zabezpečenou komunikaci s využitím blockchainu. Zdrojové kódy jsou logicky členěné, bohužel jsem v nich nenašel ani náznak komentářů. Stejně tak postrádám popis adresářové struktury či alespoň hlavičky souborů, která by rychleji objasnily význam jednotlivých souborů. Zdrojové kódy obsahuji i vzorové konfigurační soubory, které ale opět nejsou nijak dokumentovány a není ani zřejmé kde a jak se tvoří klíče, které obsahují. Výsledná práce umožňuje zapezbečenou komunikaci, ale části navrženého řešení by, s ohledem na bezpečnost, bylo vhodné lépe promyslet. Například použití potvrzovacích kódů by mělo být časové omezené. Déle by bylo vhodné při validacích zohledňovat IP adresu původního požadavku či místo předávání ověřovacích údajů emailem využít jinou metodu, například mobilní aplikaci. Součástí práce jsou i testovací scénáře, bohužel jsou zaměřené jen na funkčnost aplikace, ale nijak neřeší bezpečnostní stránku, tedy prokázání nenapadnutelnosti komunikace či jednotlivých částí aplikace.

Formální úroveň

Práce je logicky členěna a jednotlivé technologie jsou dobře popsané. Co v práci v některých místech postrádám, je jasnější zdůvodnění výběru jednotlivých technologií a jejich provázání. V práci se vyskytují kapitoly bez textu, například kapitola 4 Ethereum, kde by právě vysvětlení přítomnosti této kapitoly bylo velice přínosné.

Práce s literaturou

Téměř všechny použité zdroje jsou elektronické, což je s ohledem na zvolené téma pochopitelné, ale rozsah 13 bodů literatury, s ohledem na množství zmínovaných technologií mi nepřijde dostatečný. Zároveň je nepříjemné, že odkaz na literaturu se nevyskytuje vždy u prvního odkazu, ale následně v textu, což je pro čtenáře nepřehledné.

Splnění zadání

Splněno s menšími výhradami. Myslím, že poslední bod zadání a tedy analýza bezpečnostních rizik by si zasloužila více prostoru a predevším začlenění do realizovaných testu.

Dotazy k práci

- Nebylo by vhodné, aby hlasování o důvěryhodnosti ověřovací autority bylo povinné a vynucovalo se hlasování při změně účastníků?
- Je při jednotlivých operacích ve vašem řešení zohledňována časová platnost zpráv a případně vazba operace na IP adresu, kde požadavek původně vznikl ? Pokud ne, bylo složité vaše řešení o tyto prvky rozšířit ?
- Proč byl jako ověřovací kanál zvolen email, který jak píšete nedovoluje implementovat ověřovací autoritu v rámci Etherea. Jak složité by bylo email nahradit například mobilní aplikací ?

Navrhuji hodnocení známkou **velmi dobře** a práci doporučuji k obhajobě.

V Plzni 27.5.2021 Ing. Luboš Matějka, Ph.D.