FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Ing. Jiří Martínek, Ph.D.
Katedra informatiky a výpočetní techniky
Fakulta aplikovaných věd
Technická 8, 301 00 Plzeň
Tel.: (+420) 377 632 446
E-mail: jimar@kiv.zcu.cz

Posudek oponenta bakalářské práce

Jakub Burian
Decentralizovaná směnárna v Solidity

Obsah práce
Obsahem práce Jakuba Buriana je na základě analýz a prostudování blockchain distribuovaných databází navrnout a vytvořit vlastní implementaci decentralizované směnárny v jazyce Solidity. Jedná se o práci, která nebyla v akademickém roce 2022/2023 obhájena a byla komisí doporučena k přepracování.

V úvodu a v následné kapitole 2 *Ethereum* autor vysvětluje základní termíny používané v distribuované síti Ethereum. Po přečtení mám ale obavu, že pro čtenáře, který nemá povědomí o fungování blockchainu a souvisejících technologií bude **velmi těžké do textu proniknout** a pochopit vše, co autor popisuje. Chybí mi v teoretické části lepší popis blockchainu, především mechanismu *proof of work*, na kterém je vše založeno. Případně popis *proof-of-stake*, který Ethereum nyní používá.

Postrádám text, který čtenáře postupně provede důležitými pojmy a vysvětlí jejich podstatu, funkci a motivaci. Pomohly by také nějaké vysvětlující obrázky a diagramy, protože mám dojem, že celá druhá kapitola je víceméně seznam sekcí, které se sice snaží vysvětlit zásadní technické pojmy, ale příliš na sebe nenavazují. Následují výhrady a některé výňatky z kapitoly 2.

- V sekci 2.4 se objevuje termín „těžaři“, ačkoliv v předchozím textu vysvětlený tento pojem není.
- Podsekce *2.6.3. Eliptická křivka*; najednou se objeví a čtenář vůbec neví z jakého důvodu se nachází v rámci sekce 2.6 *Transakce*. Navíc je popis eliptických křivek dost obecný, téměř bez matematického formalismu a není ani naznačeno, jak to souvisí s problematikou vysvětlovanou v kapitole 2. Není mi jasné, co chtěl autor říci následující větou: „*Důležitou vlastností eliptických křivek je, že jsou grupami, což znamená, že mají způsob, jak přidávat body na křivce k sobě, aby získaly další bod na křivce.*“. Pokud má autor pocit, že je třeba vysvětlit pojem grupa (což je matematický termín) je dle mého názoru na úrovni dokumentu bakalářské práce potřeba použít formální a exaktní matematický popis.
- V následné části je nevhodně vysázen vzorec pro určení veřejného klíče (konkrétně je použit pro násobení znak „*“, který značí ale konvoluci). Popis algoritmu je matoucí, protože autor nejdříve jako privátní klíč označuje k a o několik řádek níže je privátní klíč najednou p. Z čista jasna se v popisu algoritmu objevují parametry e a n, které nejsou vysvětlené.

Kapitola 3 popisuje programovací jazyk Solidity, ale pouze opět jako výčet jednotlivých vlastností jazyka bez doprovodného textu, který by usnadnil pochopení a motivaci k čemu která podsekce je.

V kapitole 7 *Analýza existujících směnáren* již začíná stěžejní část práce. Čtení této kapitoly bylo dost obtížné, opět by pomohlo nějaké schéma nebo diagram. Podobně jako u kapitoly 2 autor očekává, že všechny potřebné znalosti čtenář práce má. Kapitola 8 popisuje návrh směnárny a popis implementace kapitoly 9 a 10.

Kvalita řešení a dosažených výsledků
Vyvinutý program jsem si nechal předvést studentem. Ukázka proběhla prostřednictvím rozšíření Google Chrome *MetaMask* (krypto peněženka) a front-endu napsaného v Javascriptu. Funkčnost vyvinutého SW (tj. např. vytvoření položek v *Orderbooku*) pokrývají jednotkové testy.

Formální úroveň
Dokument práce byl vytvořen v Google Docs. Vygenerovaný obsah má u položky 8.1 špatné formátování. Objevují se jednopísmenné spojky na konci řádků. Pro vytvoření dokumentu kvalifikační práce bych preferoval a doporučoval LaTeX. V práci se v malé míře vyskytují překlepy.

Reference a práce s literaturou
V referencích se objevují převážně online zdroje, celá řada zdrojů (např. [1], [2], [5], ale i spousta dalších) neobsahují datum citace, což je z hlediska citační normy povinný údaj.

Splnění zadání
Ze zadání a zásad pro vypracování vyplývá, že úkolem je prostudovat a analyzovat existující decentralizované směnárny na blockchainu a navrhnout vlastní řešení. Toto se dle mého soudu **podařilo naplnit**. Nemohu ovšem zcela objektivně posoudit čtvrtý bod zadání (kriticky zhodnoťte dosažené výsledky). Nebylo mi totiž zcela jasné, co s čím porovnávat v tabulce 11.1. Tabulka navíc obsahuje chybně zformátovaná čísla (desetinná čárka jakožto oddělovač řádů). V neposlední řadě mi v práci chybí jasně popsaná využitelnost řešení.

Závěr a hodnocení
Nemám bohužel přístup k původnímu dokumentu bakalářské práce z minulého roku. Nemohu tak zcela posoudit míru přepracování dokumentu, vyplývajícího z doporučení komise. Největší výhrady mám k **(ne)srozumitelnosti dokumentu** a také k **absenci jakéhokoliv obrázku či vysvětlujícího diagramu**. Práce velmi často vyžaduje opakované čtení jednotlivých pasáží a neustálé dohledávání dalších informací. Pro člověka, který nemá povědomí o technologiích jako blockchain a Ethereum bude text s největší pravděpodobností velmi nesrozumitelný.

Ne zcela všemu jsem v práci porozuměl a přestože jsem nejprve uvažoval spíše o známce „nevyhověl“, rozhodl jsem se nakonec pro hodnocení známkou **„dobře“**. Hlavním důvodem pro toto rozhodnutí je to, že jsem vzal v úvahu hodnocení vyvinutého SW, jehož funkcionalitu jsem si nechal Jakubem Burianem předvést. Práci **doporučuji k obhajobě**.

Dotazy k práci

1. Dokážete určit (např. procentuálně) jak velká část textu byla přepracována oproti minulé verzi?
2. Jaký by byl postup, kdybyste vaše vyvinuté řešení chtěl nasadit na Ethereum?

V Plzni dne 27. května 2024

Ing. Jiří Martínek, Ph.D.
(oponent BP)