Posudek diplomové práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce	David Surma
Název práce	Analýza blockchainu používaného pro Bitcoin
Rok odevzdání	2023
Studijní program	Informatika **Studijní obor** Umělá inteligence

Autor posudku	Ing. David Hartman, Ph.D. **Role** vedoucí
Pracoviště	Informatický ústav Univerzity Karlovy

Text posudku:

Realizace celého životního cyklu kryptoměn včetně některých vlastností jako je anonymita představuje velmi zajímavé pole zkoumání z pohledu teoretické realizace jednotlivých procesů, ale i z pohledu datové analýzy odpovídajícího systému. Bitcoin je jedním z nejstarších systémů tohoto typu s největším počtem uživatelů, který má za sebou jak fázi velkého rozšíření, tak i některé větší krize. Tím představuje zajímavý systém z pohledu analýzy. Tento systém má mnohé výhody, které se ovšem při zneužití mohou stát velmi nebezpečným nástrojem. Příkladem může být anonymita celého řešení. Ať již na pohled koukáme z pohledu odkrytí anonymity či se zájmem o její zachování, je prozkoumání síly této vlastnosti zajímavým tématem.

Kolega David Surma se ujal tohoto úkolu velmi svědomitě. V prvé řadě zevrubně představil celou oblast s důrazem na často chybějící formální pohled s ohledem na cíl práce a tím je právě indetifikace anonymizovaných identifikátorů adres skrze datově orientované metody. Kromě teoretického úkolu správně identifikoval zmiňovaný problém a nastínil jeho řešení v literatuře včetně možných metod strojového učení ovšem s ohledem na často chybějící učící data. U těchto řešení následně popsal slabé stránky a zmapoval tak celý problém do úrovně identifikace chybějícího poznatku.

Z výše zmiňovaných metod se autor nejvíce zaměřil na metody navrhující heuristiky vedoucí k vhodným klustrováním odpovídajícího systému. U těchto identifikoval problémy a následně navrhl řešení jak tyto problémy vylepšit. Následně identifikoval možná budoucí rozšíření. Výsledky by tedy bylo možné použít jak z pohledu samotné metody realizující daný úkol, tak i pomocné metody jiných analytických metod analýzy daného systému.

Student během zpracování pracoval velmi samostatně a veškeré znalosti o systému byl schopen získat a ozkoušet osobně. Provedl rešerši metod a shrnul poznatky o daném systému do pěkného teoretického popisu. Zrealizoval získání dat i samotnou tvorbu analytického pipeline, která prováděla testy. Bohužel ke konci práce byl cítit mírný nedostatek času hlavně s ohledem na velké množství,

v některých případech slepých, testů, které bylo nutné provést. Tím je práce hlavně v druhé části méně rigorózní a popis není toliko detailní. Také by určitě bylo ideální mít více reprezentativních a více popsaných testů.

I přes výše zmíněné nedostatky se jedná o velmi kvalitní a zajímavou práci, která rozhodně splnila své zadání. Celkově by práce mohla by být dobrým zdrojem pro mnohé další pokračující v tomto výzkumu.

Práci doporučuji k obhajobě.

Práci nenavrhuji na zvláštní ocenění.

V Praze dne 5. 6. 2023

Podpis: