

Posudek oponenta diplomové práce

Student: Anton Matyáš, Bc.
Téma: Heuristiky pro deanonymizaci v sítích kryptoměn (id 21564)
Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

- 1. Náročnost zadání** **průměrně obtížné zadání**
Cílem práce je navrhnout vhodné heuristiky, které by mohly částečně pomoci při deanonymizaci transakcí. Práci považuji celkově za průměrně obtížnou.
- 2. Splnění požadavků zadání** **zadání splněno**
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
Práce je rozsahově spíše kratší, nicméně z hlediska popisu je vše popsáno věcně a srozumitelně.
- 4. Prezentací úroveň předložené práce** **80 b. (B)**
Práce je logicky členěna, kapitoly na sebe navazují a celkově je text práce pro čtenáře pochopitelný.
- 5. Formální úprava technické zprávy** **70 b. (C)**
Jazyková práce obsahuje větší množství chyb - zejména chybějící velké písmena na začátcích vět.
- 6. Práce s literaturou** **75 b. (C)**
V rámci práce jsou citovány především internetové zdroje a základní informace ke kryptoměnám. Ocenil bych nastudování většího množství článků, které se zabývají danými heuristikami a deanonymizací.
- 7. Realizační výstup** **80 b. (B)**
V rámci práce vznikla jednoduchá aplikace pro vyhledávání a deanonymizaci transakcí, Za hlavní výstup práce považuji ale sadu testů, které byly provedeny při snaze vytvořit potřebné heuristiky.
- 8. Využitelnost výsledků**
Výstupy práce lze dále využít a integrovat do nástrojů vznikajících v rámci projektu TARZAN.
- 9. Otázky k obhajobě**
 - Jaká je časová a výpočetní náročnost heuristik použitých v rámci deanonymizace?
- 10. Souhrnné hodnocení** **80 b. velmi dobře (B)**
Cílem práce bylo pokusit se navrhnout heuristiky, které by umožnili deanonymizaci transakcí v kryptoměnových sítích. Použité techniky jsou sice vcelku přímočaré, nicméně se ukazuje, že v základní podobě mohou fungovat. Text práce je až na občasné chybějící velké písmena na začátcích vět čitelný a realizační výstup dále použitelný, Celkově hodnotím práci jako velmi dobrou (B).

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

V Brně dne: 7. června 2019

Grégr Matěj, Ing., Ph.D.
oponent