

Posudek oponenta diplomové práce

Student: Drozda Tomáš, Bc.
Téma: Forenzní analýza sítě Bitcoin (id 18964)
Oponent: Grégr Matěj, Ing., UIFS FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**
Zadání považuji za obtížnější. Protokol používaný sítí Bitcoin je sice vcelku jednoduchý, nicméně tvorbu algoritmu pro správné shlukování nad velkou datovou sadou považuji za vcelku náročnou.
- 2. Splnění požadavků zadání** **zadání splněno**
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
- 4. Prezentační úroveň předložené práce** **90 b. (A)**
Vůči prezentační úrovni technické zprávy nemám výhrady. Jednotlivé kapitoly na sebe navazují, jejich rozsah je adekvátní a pro čtenáře pochopitelný.
- 5. Formální úprava technické zprávy** **80 b. (B)**
Typografická úroveň práce je kvalitní, našel jsem pouze chybějící referenci na straně 43. Vše ostatní je kvalitně typograficky upraveno. S mými znalostmi sloveštiny nemám k jazykové stránce práce připomínky.
- 6. Práce s literaturou** **75 b. (C)**
V práci jsou využívány citace v souladu se zvyklostmi a normami. Výhradu bych měl pouze k výběru pramenů. Zde mi chybí více vědeckých prací, které se danou problematikou zabývají a které by mohly analýzu práce rozšířit - např. [1], [2] a další.
[1] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *Financ. Cryptogr. Data Secur. 17th Int. Conf.*, 2013.
[2] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network," *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS 14*, pp. 15-29, 2014.
- 7. Realizační výstup** **90 b. (A)**
Realizační výstup využívá jazyk PHP, framework Laravel a NoSQL databázi MongoDB. Výsledkem je webová aplikace, která umožňuje procházet jednotlivé transakce, bloky a adresy používané v síti Bitcoin. Aplikace je funkční a lze do budoucna dále rozšířit.
- 8. Využitelnost výsledků**
Současné nástroje, které podobnou analýzu poskytují, jsou již často nedostupné nebo přešly na komerční verzi. Výsledky práce lze tedy využít v praxi pro analýzu transakcí a adres sítě Bitcoin. Větší využitelnost by aplikace měla kdyby umožňovala analyzovat další kryptoměny.
- 9. Otázky k obhajobě**
-
- 10. Souhrnné hodnocení** **90 b. výborně (A)**
Práce představuje nástroj pro analýzu transakcí, adres a bloků, které obsahuje blockchain síť Bitcoin. Aplikace je použitelná, splňuje zadání a je programována tak, aby do budoucna umožňovala rozšíření o další kryptoměny. Celkově doporučuji hodnotit práci jako výbornou (A).

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

V Brně dne: 3. června 2016

.....
podpis