Posudok oponenta na bakalársku prácu:
**Lucie Deptová: Virtuální měna Bitcoin**

Cieľom predloženej práce bol popis virtuálnej meny a platobného systému Bitcoin. Práca obsahuje veľmi stručný úvod často obmedzený výlučne na základné definície. Nasledujú kapitoly vysvetľujúce Bitcoin adresy, Bitcoin transakcie, bloky a ťažbu Bitcoinov. Práca končí výpočtom pravdepodobnosti dvojitého uplatnenie (double-spending) jednej virtuálnej čiastky (výstupu jednej transakcie).

Hlavný cieľ práce, ucelený popis virtuálnej meny a platobného systému Bitcoin, bol naplnený. Autorke sa výklad jednotlivých prvkov systému podaril a práca je aj napriek roztrieštenosti a zložitosti zdrojov prehľadná a dobre čitateľná. Text ale nie je ani zďaleka úplný popis systému Bitcoin a ponecháva stále veľa nejasností a nezodpovedaných otázok. Detailnejší popis by ale znamenal značné rozšírenie už tak obšírnej práce.

Negatívne hodnotím viacero nepresností, ktorých sa autorka dopustila a to väčšinou v úvode práce. Príkladom sú nepresný popis podpisovej schémy Elgamal na strane 6 ($H$ sa tu používa ako zobrazenie z $\{0,1\}^*$ do celých čísiel ale aj ako zobrazenie z grupy $G$ do celých čísiel), chybný popis DSA na strane 7 (v DSA sa nepracuje s $G = \mathbb{Z}_p^*$ ale iba s jej vlastnou podgrupou), alebo chyba v definícii SHA-256 (jej definičným oborom sú binárne reťazce do dĺžky $2^{64} - 1$ a nie $\{0,1\}^*$). V závere práce mi chýba lepšie zdôvodnenie rovnice (5.9) na strane 37, ktoré by autorka mohla doplniť pri obhajobe.

Celkovo je práca na dobrej úrovni. Text má ale skoro výhradne popisný charakter a tak nie je možné hodnotiť jeho matematickú úroveň.

Predloženú prácu doporučujem uznať ako bakalársku a navrhujem ju hodnotiť známkou ...

Praha, 18.6.2014 Michal Hojsík