POSUDEK BAKALÁŘSKÉ PRÁCE

Oponent práce

Autor práce: Tomáš Šrail

Název tématu: Kryptoměny a jejich využití širší veřejností

Dodržení minimálního přípustného rozsahu práce		☒ ano	☐ ne
Splnění bodů zadání	☒ úplně	☐ částečně	☐ nesplněno
Případný komentář: ---			

	Předmět hodnocení	Nadprůměrné	Průměrné	Podprůměrné
1	Formulace cílů a metodika zpracování práce	☒	☐	☐
2	Logická struktura a členění práce	☐	☒	☐
3	Rozsah a úroveň použitých zdrojů, bibliografické citace (dle platné ČSN ISO), poznámkový aparát	☐	☒	☐
4	Jazyková, stylistická úroveň a formální úprava práce	☒	☐	☐
5	Kvalita zpracování tématu práce	☒	☐	☐
6	Formulace vlastních závěrů, vlastní přínos autora práce	☒	☐	☐
7	---	☐	☐	☐

Doplnění hodnocení, připomínky, dotazy:

Autor ve své závěrečné práci seznamuje čtenáře s problematikou kryptoměn a předkládá základní informace o šifrování a principech, které využívají, technickém vybavení, které je s nimi spojeno, a rovněž popisuje konkrétní nejznámější a nejvyužívanější kryptoměny. V závěru práce se pak věnuje dotazníkovému šetření na téma možnosti využití kryptoměn širší veřejností u nás.

První kapitolu věnuje autor popisu vlastností běžně používaných peněz a srovnání s jejich virtuálními protějšky. Taktéž přináší náhled do problematiky šifrování, se kterým jsou kryptoměny nerozlučně spjaty. Kapitola je pojata jako stručný náhled na danou problematiku, což je v souvislosti s komplexností tématu a kritérii pro tvorbu bakalářské práce rozhodně v pořádku. Téma je popsáno věcným a zajímavým způsobem. Chybí zde snad jen vysvětlení pojmu „altcoin" jako jakékoli jiné alternativní měny po nástupu Bitcoinu a poznámka, že se s nimi čtenář setká později. Nicméně Dogecoin, který je uveden společně s Litecoinem jako nejúspěšnější, již bohužel v práci dále zmíněn není. Oproti tomu je pak ve třetí kapitole zmíněn Ether, ačkoli není uveden v této kapitole.

Ve druhé kapitole jsou podrobněji popsány kryptologické techniky v souvislosti s kryptoměnami, zmíněny principy šifrování a vysvětleny nejdůležitější pojmy, které jsou s kryptoměnami spojené, jako např. hashovací funkce, decentralizovaná síť, transakce, bloky, blockchain, těžba jednotek a další. Poněkud neuceleně působí, že některé pojmy jsou zmiňovány již v první podkapitole, ačkoli by bylo z hlediska zvolené struktury možná vhodnější je zařadit do následující kapitoly s názvem Pojmy. Snad vlivem úprav textu se vytratily správné kroky vedoucí k výsledku d=59 v kapitole 2.1.1 týkající se šifrování RSA. Kapitola 2.1.2 Metoda eliptických křivek uvádí zkratku ECC (Elliptic-curve cryptography), která není uvedena ve zkratkách v úvodu práce a z textu lze získat pocit, že je zaměnitelná s metodou ECDSA. Zaznít by ovšem mělo, že ECDSA (Elliptic Curve Digital Signature Algorithm) je varianta algoritmu pro digitální podpis, která ECC využívá. Tabulka 1 v této kapitole avizuje porovnání bezpečnosti šifer, ale následně není uvedeno, co z uvedených hodnot vyplývá. Na škodu je horší kvalita obrázků 2, 6 a 7, které jsou kvůli tomu jen obtížně čitelné.

Třetí kapitola se již týká popisu dvou konkrétních kryptoměn: Bitcoinu a Litecoinu. Kromě jejich

základních vlastností zde lze nalézt vysvětlení délky průběhu transakcí v závislosti na jejich potvrzování a je popsáno i využití hardware pro těžbu. Jako doplnění ke zmíněným kryptoměnám je velmi krátce uveden rovněž Ether, který má ambice se stát nejen měnou, ale přímo platformou.
Čtvrtá kapitola popisuje technickou stránku využívání kryptoměn, tj. nutné vybavení co se software i hardware týče. Je zde přehledně představeno fungování peněženek, a to jak odlehčených aplikací pro rychlé použití, tak i jejich plnohodnotné verze nebo přímo jejich hardwarové protějšky. Velmi dobře je popsán i hardware a nároky na něj kladené, zejména ty ve spojitosti s těžbou jednotek. Součástí této kapitoly jsou i vcelku nenápadné zásady bezpečné manipulace s kryptoměnami. Tato část by vzhledem k tématu měla být jistě více zdůrazněna a zasloužila by si možná samostatnou kapitolu.
Je vhodné uvést na pravou míru informaci ze strany 33: „Pro potřeby plnohodnotného klienta se nároky na diskový prostor pohybují v řádech desítek GB". Určitě se jedná již o stovky GB, jak vyplývá z textu o pevném disku na následující straně a zejména obrázku instalace Bitcoin Core tamtéž.
Obsáhlost a křížové propojení jednotlivých částí a pojmů tématu bezesporu značně zkomplikovaly členění textu práce. Již přehled úvodních zkratek (kde např. chybí následně používaná RSA či již zmíněná ECC) vybízí k otázce seřazení např. podle abecedy. Orientaci v pojmech by zlepšilo alespoň stručné vysvětlení, orientaci v práci samotné by výrazně napomohlo např. uvedení, kde se s daným pojmem lze setkat. Některé pojmy nejsou ani v samotném textu vysvětleny uspokojivě. Např. pro pojem „obtížnost" z textu na straně 24 vyplývá, že je to „počet nul v řetězci zleva", který ve výsledku umožňuje „rovnoměrné rozložení potvrzování transakcí v čase", ale není zmíněno v jakém řetězci a co vlastně určuje splnění nějaké takové konkrétní podmínky (např. co znamená uvedená obtížnost 17, kterou jeden blok splňuje a druhý nikoli). Na straně 32 je pak uvedena „priorita", která je určena nastavením poplatku za provedení transakce, ale význam není již dále vysvětlen.
Závěrečné dotazníkové šetření je obsaženo v kapitole páté. Autor precizně popisuje jak samotnou přípravu, včetně východisek, předpokladů, tak celý další návazný postup. Soustředí se na výzkumné otázky a hypotézy i na metody sběru informací, respondenty samotné, sestavení dotazníku a jeho vyhodnocení. V textu zde chybí snad pouze informace, kde může čtenář kompletní otázky z dotazníku nalézt (bylo by vhodné toto připomenout např. na konci kapitoly 5.6 popisující tvorbu dotazníku, nebo v kapitole 5.7.2, kde jsou v rámci vyhodnocení odkazovány jednotlivé otázky), a výslednou volbu skupiny respondentů.
Samotné šetření mělo být dle zásad pro vypracování „orientované na jedince, kteří aktivně využívají kryptoměny". To, jak bylo nakonec připraveno a realizováno, tomu sice úplně neodpovídá, ale na druhou stranu je naprosto v souladu s názvem práce a díky pečlivé přípravě i odborně zpracovanému vyhodnocení skýtá možnost kvalitního náhledu na využívání virtuálních služeb běžných bank a také virtuálních měn a povědomí o nich ze strany široké veřejnosti.
Ve vyhodnocení na str. 45 na okamžik sice může být matoucí dvojí odkaz na Graf 4 na následující straně, ale čtenář po nahlédnutí pochopí, že první z odkazů má být na Graf 3.
Závěrem lze konstatovat, že autor efektivně shrnul získané informace a poznatky a předkládá je na odborné úrovni a zároveň srozumitelným a čtivým způsobem. Téma kryptoměn je natolik rozsáhlé, že splnění cíle, „aby čtenář získal komplexní informace z oblasti virtuálních měn", jak je uvedeno v úvodu práce, je v daném rozsahu asi nepříliš reálné. Nicméně jako základní seznámení s tématem je práce více než zdařilá a díky precizně připravenému a provedenému dotazníkovému šetření přináší i zajímavý pohled na vztah veřejnosti k tomuto tématu.

Otázky k obhajobě:
Jakým způsobem byl dosažen výsledek d = 59 při sestavování soukromého klíče v příkladu na str. 14?
Co znamená nějaká konkrétní hodnota obtížnosti a jak se s ní pracuje? (str. 24)
Jak je řešena priorita transakce a s jakým efektem? (str. 32)
Jak probíhal výběr respondentů a kdo byl osloven dotazníkovým šetřením?

Celkové hodnocení práce	☒ **výborně**	☐ **velmi dobře**	☐ **dobře**	☐ **nevyhovující**

Posudek vypracoval: Mgr. Zdeněk Lomička

2.6.2018
Datum

Podpis