

Posudek práce

předložené na Přírodovědecké fakultě JU

- | | |
|--|--|
| ☐ posudek vedoucího | ☒ posudek oponenta |
| ☐ bakalářské práce | ☒ diplomové práce |

Autor/ka: **Bc. Jakub Zimmer**

Název práce: Analýza současných kryptoměn se zaměřením na Bitcoin, zajištění výnosu z trestné činnosti

Studijní program a obor: Aplikovaná informatika

Rok odevzdání: 2018

Jméno a tituly vedoucího/opponenta: **RNDr. Libor Dostálek**

Pracoviště: Ústav aplikované informatiky

Kontaktní e-mail: dostalek@prf.jcu.cz

Odborná úroveň práce:

- ☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

- ☐ téměř žádné ☒ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

- ☐ originální ☐ původní i převzaté ☒ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

- ☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

- ☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

- ☐ téměř žádné ☒ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Tečka na konci názvu práce se opravdu nepíše!

Celková úroveň práce:

- ☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Jedná se o netriviální kompilaci s navrženými řešeními. Chybí mi nějaká praktická úloha.

Případné otázky při obhajobě a náměty do diskuze:

Kdy se v souvislosti s bitcoinem používá symetrická a kdy asymetrická kryptografie?

Práci

☒ doporučuji

☐ nedoporučuji

uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:

☐ výborně ☒ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích



Posudek práce

předložené na Přírodovědecké fakultě JU

☐ posudek vedoucího
☐ bakalářské práce

☒ posudek oponenta
☒ diplomové práce

Autor/ka: Bc. Jakub Zimmer
Název práce: Analýza současných kryptoměn se zaměřením na Bitcoin, zajištění výnosu z trestné činnosti.
Studijní program a obor: Aplikovaná informatika
Rok odevzdání: 2018

Jméno a tituly ~~vedoucího~~/opponenta: Ing. Marta Vohnoutová
Pracoviště: Katedra informatiky
Kontaktní e-mail: mvohnoutova@jcu.cz

Odborná úroveň práce:

☒ vynikající ☐ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

☐ téměř žádné ☒ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

☐ originální ☒ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

☒ téměř žádné ☐ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

☒ vynikající ☐ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/opponenta

Autor předkládá vyspělou poměrně rozsáhlou práci na velmi zajímavé současné téma. Autor píše čtivým stylem, jazyková úprava i přes hrubou chybu a několik chybějících čárek je velmi dobrá. Uvítala bych v některých případech jiný způsob hodnocení a srovnávání než je volně psaný text, kde jsem se časem začala trochu ztrácet. Mám na mysli formu přehledových tabulek, kde by byly určeny srovnávací kritéria a pokud by se vyskytly neporovnatelné vlastnosti, mohly by být uvedeny zvlášť nebo do tabulky jako poznámka. Dále stejné údaje jsou v jednotlivých kapitolách uvedeny na různých místech – např. uvedení tržní hodnoty jednou na konci, jindy na začátku kapitoly apod. V práci mi chyběl slovníček pojmů a odkazy, kde by bylo možné si případně o aktuálně popisovaném tématu přečíst více.

Při čtení je poznat, že autorovi dalo vypracování mnoho práce a je zde množství velmi zajímavých údajů.

Přes připomínky považuji předloženou práci za jednu z nejlepších a dávám na zvážení přihlásit tuto práci za soutěž o Cenu děkana za nejlepší diplomovou práci.

Případné otázky při obhajobě a náměty do diskuze:

1. K Merkle Tree – uvádíte, že transakce zapisované do Merkle Tree přibývají rychlým tempem, podle Vámi přiloženého obrázku by však každá přidaná transakce změnila kořenovou hodnotu v Merkle Tree, což je prakticky nemožné. Víte, jakým způsobem se tedy přidávání transakcí do Merkle Tree a přepočítání jeho kořenové hodnoty řeší?
2. Fork v Blockchain – jakým způsobem zabránit tomu, aby se za odmítnutý blok neřadily další (zdravé) transakce, existuje nějaké alespoň částečné řešení?
3. Vysvětlíte principy Proof of Work a Proof of Stake a jejich rozdíly.

Práci

☒ doporučuji

☐ nedoporučuji

uznat jako diplomovou/~~bakalářskou~~.

Navrhuji hodnocení stupněm:

☒ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/opponenta:

V Českých Budějovicích

