Posudek bakalářské práce

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

Autor práce:	Daniel Stahr
Název práce:	Sledování obarvených bitcoinů v transakčním grafu
Rok odevzdání:	2014
Studijní program a obor:	Informatika, obecná informatika
Autor posudku:	Mgr. Martin Mareš, Ph.D., oponent
Pracoviště:	Katedra aplikované matematiky

K celé práci	lepší	OK	horší	nevyh.
Obtížnost zadání		X		
Splnění zadání			X	
Rozsah práce			X	

Předmětem práce je rozšíření transakčního systému (kryptografické měny) Bitcoin, které umožňuje část prostředků označit („obarvit“) a sledovat, jak putují transakcemi. Obarvené bitcoiny je pak možné použít k reprezentaci různých komodit.

Samotná myšlenka barvení bitcoinů není nová. Tato práce navazuje na několik předchozích návrhů, které se snaží doplnit barevnou sémantiku bez nutnosti měnit syntaxi bitcoinového protokolu.

Autor navrhuje novou definici transakcí s obarvenými bitcoiny a také software, který prochází graf všech provedených transakcí a sleduje, jak jím obarvené bitcoiny procházejí.

K tomuto úkolu bohužel autor přistoupil poněkud triviálním způsobem, což se odráží jak v malém rozsahu práce, tak v dalších problémech zmíněných níže.

Textová část práce	lepší	OK	horší	nevyh.
Formální úprava		X		
Struktura textu			X	
Analýza			X	X
Vývojová dokumentace		X		
Uživatelská dokumentace		X		

V úvodu práce autor čtenáře seznamuje se základy fungování transakční sítě Bitcoin. Tento úvod je však sepsán dost nepřehledně, zejména proto, že definice transakce následuje až poté, co se delší dobu mluví o blocích transakcí.

Následuje zavedení obarvených bitcoinů, stručný popis jejich aplikací a shrnutí dříve známých definic barevné sémantiky transakcí. Toto shrnutí sice zmiňuje některé výhody a nevýhody jednotlivých definic, ale nedává je do souvislosti s aplikacemi barvení, takže pomíjí, které vlastnosti jsou podstatné a které nikoliv. Taktéž u definic sémantiky chybí jakékoliv citace.

Poté autor navrhuje svůj vlastní protokol (vlastní sémantiku), který je triviální modifikací jednoho z předchozích protokolů a snaží se odstranit některé z jeho nevýhod.

To se daří pouze částečně. Hlavní problém v novém protokolu vidím v nutnosti udržovat globální uspořádání na všech barvách. Toho je snadné dosáhnout v jedné lokální instalaci softwaru, ale při širším využití se to značně zkomplikuje. Práce vůbec neřeší, jakým způsobem se v prostředí s více uživateli zařídí synchronizace přidávání nových barev a přiřazování genesis transakcí k barvám. Taktéž připustíme-li, že k jedné barvě může existovat více genesis transakcí, protokol přestane být stabilní.

Autor také zmiňuje, že stávající protokoly založené na pořadí jsou neintuitivní pro uživatele. S tím souhlasím, ale nemyslím si, že nový protokol by na tom byl výrazně lépe: odstraňuje sice závislost na pořadí vstupů a výstupů transakce, ale nahrazuje ji závislostí na očíslování barev. Jistou útěchou snad je, že počet barev v typické transakci bude v praxi nejspíš menší než počet vstupů a výstupů.

Nový protokol též neřeší diskutovaný problém obarvení poplatků. Ten lze samozřejmě obejít obalením transakce neobarvenými bitcoiny, ale to je u ostatních protokolů zmiňováno jako nevýhoda.

V textu je minimum jazykových a typografických chyb, leč přehledností a zejména důkladností analýzy nevyniká. Nejedno tvrzení postrádá korektní citaci.

Implementační část práce	lepší	OK	horší	nevyh.
Kvalita návrhu			X	X
Kvalita zpracování		X	X	
Stabilita implementace		X		

Druhou částí práce je návrh a implementace programu pro analýzu transakčního grafu a sledování toku obarvených bitcoinů.

Po algoritmické stránce je tento problém triviální: stačí procházet transakční graf v topologickém pořadí a každou transakci vyhodnotit dle definice barevné sémantiky. Přesně to dělá i navržená implementace.

Autor si vybral, že ji naprogramuje v jazyce Python a všechna data uloží do in-memory databáze Redis. Vzhledem k celkovému objemu dat (při současném stavu sítě Bitcoin řádově gigabyty) mi tato volba nepřijde vhodná. Implementace v jazyce C/C++, která by uchovávala všechna data v obyčejných hešovacích tabulkách, by byla výrazně efektivnější a ne o mnoho složitější.

Taktéž postrádam jakékoliv úvahy o možnosti předvýpočtů, jimiž by bylo možné urychlit dotazy na tok obarvených prostředků a přidávání nových barev.

Implementace je tedy značně primitivní, ale jinak solidní a funkční.

Zcela chybí srovnání výkonu s předchozími implementacemi.

Celkové hodnocení: dobře

Práci navrhuji na zvláštní ocenění: ne

V Praze dne 26. srpna 2014

Martin Mareš