Blockchainy a decentralizované aplikace (BDA)

Korelace BTC transakcí vůči poskytnutému datasetu

Daniel Konečný (xkonec75)
Vysoké učení technické v Brně
Fakulta informačních technologií

5. května 2022

1 Implementace

Projekt je implementovaný v jazyce Python 3.10 za použití knihoven:

- psycopg2 – pro práci s PostgreSQL databází;
- requests – pro práci s Blockbook API;
- datetime – pro práci s časovými značkami, rozdíly mezi časy apod.;
- a dalších základních knihoven.

2 Korelační metoda

Ke korelaci je využita hodnota posílaného bitcoinu (resp. cena zboží) a čas dělící objednávku a schválení bloku s kandidátní transakcí. Rozdíl ceny je uvedený ve sloupci price_diff a čas dělící objednávky v minutách je uvedený ve sloupci heuristics výstupního CSV souboru.

Pro korelaci se uvažují transakce z bloků až hodinu před provedením objednávky (z důvodu možného nepřesně uvedeného času vytěžení bloku) a dále až 24 hodin po uskutečnění objednávky. Tyto transakce se očistí o ty, které nejsou validní, např. coinbase transakce, či transakce s nějakým skriptem. Dále se neuvažují mince, které se vrací v rámci transakce na jednu ze vstupních adres (jako zbylé mince po neutracení celého UTXO).

Jako kandidátní transakce k dané objednávce jsou uvažovány pouze ty, které se liší maximálně o 10 satoshi, tedy o hodnotu která mohla vzniknout nějakým nepřesným zaokrouhlením. Při korelaci jsou uvažovány všechny možné varianty produktu v ceně přesně v době objednávky. Vyberou se ty, ke kterým je nalezena kandidátní transakce podle dříve uvedených podmínek.

3 Implementace

Pro získání bloků s kandidátními transakcemi, které by mohly odpovídat nákupu daného produktu jsem využil dodatečné tabulky databáze. Tato tabulka obsahuje čísla bloků s jejich časem vytěžení. Tato informace se nedá nijak přesně vypočítat či odvodit, je ji tedy třeba získat přímo z blockchainu. Při prvním spuštění aplikace se taková tabulka vytvoří se všemi potřebnými informacemi (může trvat i několik hodin) a následně už se pouze používá. Při potřebě aktualizace o nové bloky se to také provede, tato možnost však není defaultně zapnutá, neboť pracujeme s datasetem s fixním časovým obdobím.

Aplikaci je možné spustit ve dvou režimech. První demonstruje korelaci konkrétního počtu objednávek, které se náhodně vyberou z databáze. Druhý provede korelaci na konkrétním produktu objednaném v konkrétním čase. Bližší informace ke spuštění jsou uvedeny v přiloženém README.md.

4 Dosažené výsledky

Aplikace je schopná nalézt kandidátní transakce, které se liší maximálně o 10 satoshi, většinou však i takové, které se liší pouze o 1 satoshi.