Korelace BTC transakcí vůči poskytnutému datasetu

Blockchainy a decentralizované aplikace (BDA)

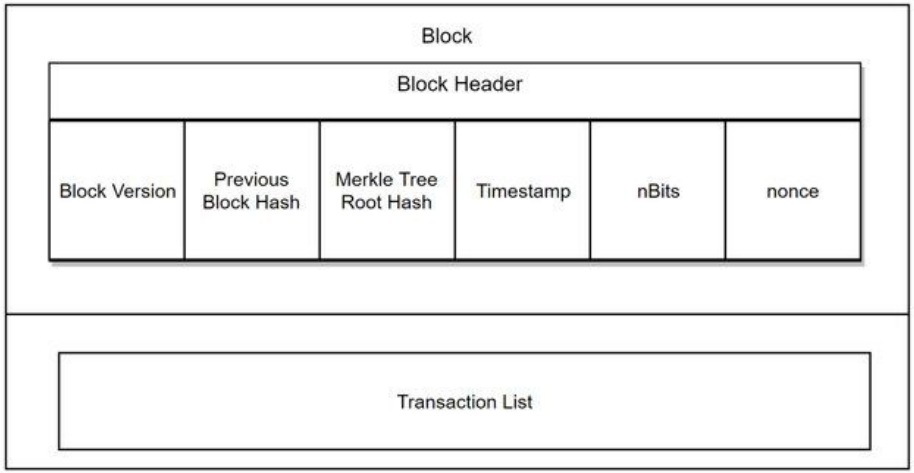
Daniel Konečný (xkonec75)

Cíl projektu

- Korelovat objednávky produktů z darkmarketu s BTC transakcemi
- Datová sada objednávek z darkmarketu
  - Čas objednávky konkrétního produktu
  - Jaké má produkt varianty a jejich ceny v BTC v době objednávky
- Co datová sada neobsahuje
  - Jakou variantu produktu si zákazník objednal
  - Jestli si zákazník neobjednal více produktů, které v rámci jedné objednávky
  - Jestli platil v BTC nebo XMR
  - Kdy a jestli vůbec platba dorazila
- Jaké informace poskytne BTC blockchain
  - Transakce konkrétních částek, jejich formát (více výstupů apod.)
  - Poplatek za transakci
  - Čas vytěžení bloku s transakcí
- Jaké informace nejsou v blockchainu
  - Kdy se transakce objevila v mempoolu
  - Identita uživatele, metadata o něm…

Získání kandidátních bloků s transakcemi

- Na základě času objednávky
- Nemožnost výpočtu čísla bloku z času
- Pomocná tabulka s číslem bloku a časem vytěžení
  - Vytvoří se při prvním spuštění
  - Nekonzistence času vytěžení
- Bloky jednu hodinu nazpět a 24 hodin dopředu



Získání kandidátních transakcí

- Transakce, které se ignorují:
  - Coinbase transakce
  - Transakce obsahující více než přenos peněz z adresy na adresu (třeba skript)
- Výstupy, které se ignorují:
  - Výstup směřující na nějakou ze vstupních adres
  - Výstup s více cílovými adresami

Korelace transakcí s objednávkami

- Uvažuji pouze transakce, které přenáší stejný nebo maximálně o 10 vyšší počet satoshi
- Heuristická funkce
  - Čas schválení bloku od chvíle objednání produktu v minutách – menší je lepší
- Možná další vylepšení heuristické funkce
  - Uvažovat výši poplatku a zahlcení sítě pro odhad, jak dlouho mohla transakce čekat na vytěžení
  - Porovnat kandidátní adresy u produktů od jednoho prodejce na nalezení stejných adres