Slovenská technická univerzita v Bratislave Fakulta informatiky a informačných technológií

Ilkovičova 2, 842 16, Bratislava 4

Transakcia (Dokumentácia)

BlockPay
Blockchain Busters

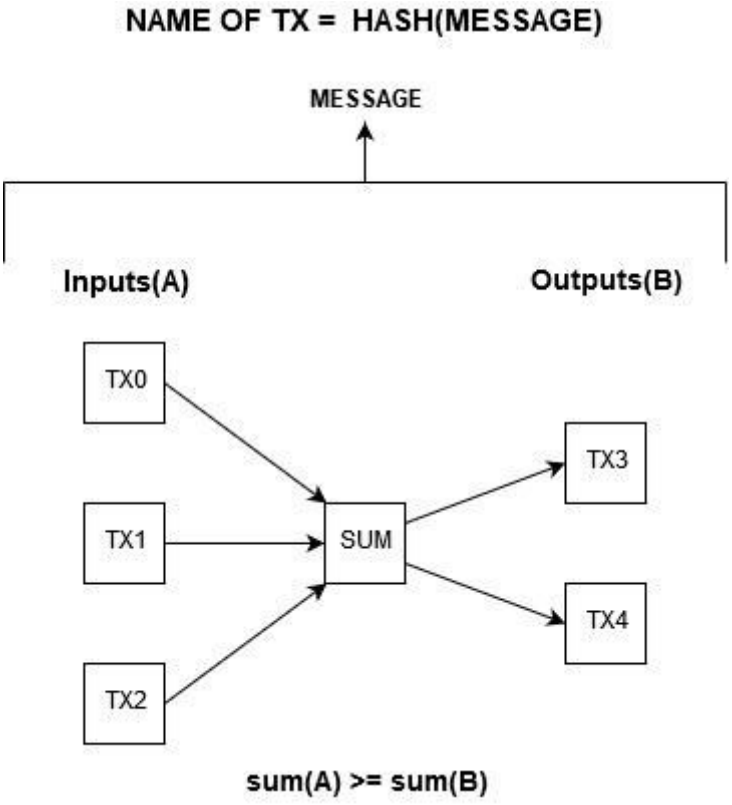
Tímový projekt
Tím č. 20
Vedúci: Ing. Kristián Košťál
fiittim201920@gmail.com

Vypracoval: Vladimír Bernolák

1. Základný formát Bitcoin transakcie

Bitcoin transakciu je možno popísať ako podpísaný balíček dát, ktorý je vysielaný do siete a v prípade, že je úspešne overený, môže byť zaradený do bloku v Bitcoin blockchain. V momente zadania prevodu vytvorí peňaženka klienta správu s názvom Bitcoin transakcia. Táto správa je odoslaná a ďalej šírená peer2peer blockchain sieťou.

Objekty transakcie, ktoré určujú odosielateľa a prijímateľa môžeme označiť ako vstupy a výstupy.



Vstupy sú tie, ktoré do transakcie prinášajú hodnotu. Entita alebo odosielateľ, ktorý túto transakciu uskutočňuje však tieto zdroje priamo fyzicky nevlastní. Svoje vlastníctvo potvrdí privátnym kľúčom, ktorý prislúcha verejnému kľúču daného vstupu (najčastejší typ overenia). Tieto vstupy sú tvorené výstupmi z predošlých transakcií.

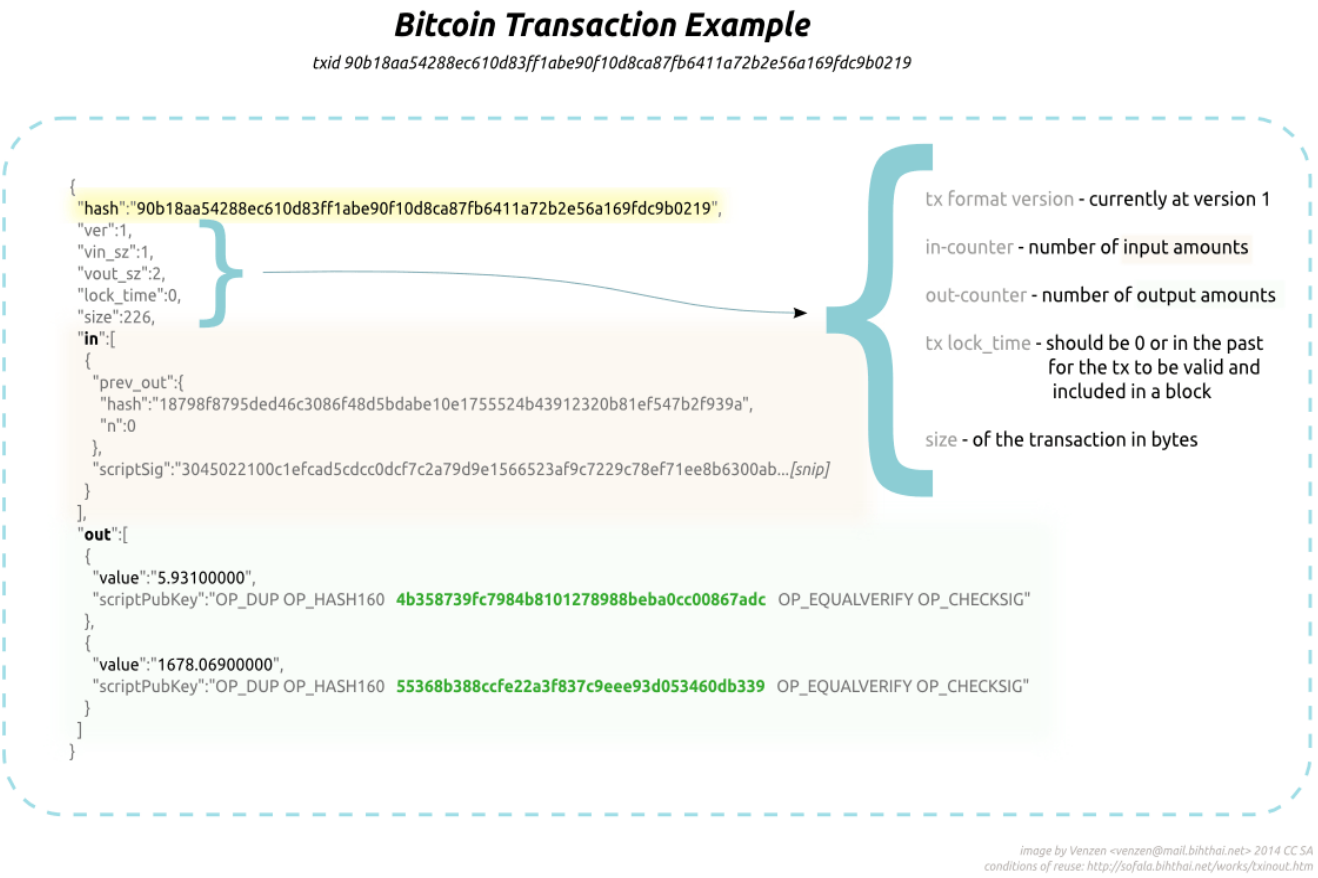
Výstupy je možné smerovať na ľubovoľného účastníka, ktorý následne preukáže svoje právo spomenutým spôsobom. V rámci jednej transakcie môžeme smerovať výstupy na viacerých účastníkov. Hodnota výstupov je poskladaná z hodnôt vstupov, nastať tak teda môže situácia kedy dostupné vstupy prevyšujú hodnotu zamýšľaného výstupu. Do transakcie sa teda zvykne pridať výstup, ktorý sa nazýva výdavok, ten sa nasmeruje späť na zadávateľa transakcie a teda ho môže neskôr

použiť ako ďalší vstup. Zostávajúca prevyšujúca hodnota vstupov oproti výstupom je pripísaná entite, ktorá vyťaží blok v ktorom sa daná transakcia nachádza.

Transakciu ešte dopĺňajú rôzne administratívne polia a ako celok je v danom bloku zapísaná ako hash, ktorý je tvorený dvojnásobným šifrovaním SHA256.

Takto by sa dala popísať štandardná transakcia, výnimku však predstavuje coinbase transakcia, ktorá sa nachádza na začiatku každého bloku. Takáto transakcia neobsahuje vstupy a taktiež by nemala obsahovať výstup typu výdavok. Vstupy do tejto transakcie sú určené odmenou pre entitu, ktorá vyťažila daný blok.

2. Príklad Bitcoin transakcie



Na obrázku môžeme vidieť reálny formát transakcie.

Hlavička obsahuje nasledujúce údaje:

- Identifikátor transakcie v podobe hash
- Verzia formátu transakcie
- Počet vstupov
- Počet výstupov
- Nastavenie najskoršieho času kedy môže byť transakcia vložená do bloku

Časť „**in**“ obsahuje:

- Identifikátory vstupov (v tomto prípade jeden) – transakcia, ktorá previedla práva na odosielateľa („prev_out“)

- Priradenie daného vstupu k výstupu („n:“)
- Potvrdenie o tom, že odosielateľ má vlastnícke práva na daný vstup („scriptSig“)

Časť „**out**“ obsahuje:

- Výstupy s definovanými sumami a podmienkami na autentifikovanie prijímateľov („scriptPubKey“)

Zdroje

[1] Bitcoin Transaction details, Autor: Donald J. Patterson, Ph.D., Dostupné online: https://www.youtube.com/watch?v=Em8nJN8IEes, https://www.youtube.com/watch?v=f9nxuhLSyOg [19.10.2019]
[2] How a Bitcoin Transaction Works, Autor: Venzen Khaosan, Dostupné online: https://www.ccn.com/bitcoin-transaction-really-works/ [19.10.2019]
[3] How does Bitcoin work?, Autor: neuvedený, Dostupné online: https://bitcoin.org/en/how-it-works, [19.10.2019]