BitCoin
Projektna naloga pri predmetu kriptografije in teorije kodiranja 2

Jernej Azarija

28. marec 2012

Povzetek

V dani projektni nalogi je predstavljen monetarni sistem *BitCoin.* BitCoin je prvi sistem virutalnega denarja, ki zagotavlja anonimnost transakcij, decentralizirano vodenje računov in hkrati preprečuje napade z dvojno potrošnjo sredstev. V projektni nalogi obravnavamo tehnični aspekt navedenih lastnosti.

1 Uvod

Pojem denarja presega meje projektne naloge in se zliva na področje antropologije, vendar je za namene popolnosti potrebno omeniti tudi nekaj konceptov iz tega področja. Na denar danes gledamo kot na objekt s pripisano materialno vrednostjo, ki ga lahko uporabimo kot menjalno sredstvo za dobrine in storitve. Pri tem se takoj postavi vprašanje: 'Kdo določa vrednost, denarja?'. Zgodovinsko gledano je bil denar[1] vezan na zlato [2]. Določena količina dolarjev je ustrezala točno določeni količini zlata.

Do leta 1971 je Ameriška centralna banka zagotavljala ustrezno količino zlata za vsak dolarski bankovec. Po letu 1971 so zaradi potrebe inflacije in deflacije ukinili takoimenovan zlati standard - vrednost denarja je obvisela v zraku. Posledice takšnega ravnanja so vidne skozi zgodovino v obliki fluktuacij tečajev dolarja in posledično svetovnega gospodarstva. Danes pa se

[1]Za primer vzemimo ameriški dolar, čeprav je isto veljalo tudi za druge 'stare' valute kot je npr. švicarski frank.

te posledice omenja predvsem v povezavi s 'finančno krizo', kjer se ogromni dolgovi poplačujejo s tiskanjem nekritega denarja.

Ko je govora o denarju, ne gre brez omembe institucij, tesno povezanih z denarjem - bank. V toku let so banke izgubile primarno funkcijo hranjenja in varovanja denarja ter se prestrukturirale v institucije, ki plemenitijo lastnen kapital, državi pa pomagajo pri vodenju evidence o državljanih. V kolikor želi bralec zares začutiti pomembnost, ki ga anonimni monetarni sistem prinaša, mora sam pri sebi odgovoriti na spodnja vprašanja:

- Kaj določa vrednost denarju?
- Kakšen vpliv ima družba na inflacijo/deflacijo denarja? Ali ga sploh ima?
- Zakaj delodajalci nakazujejo denar zgolj na bančne račune?
- Zakaj morajo transakcije nad 10000€ potekati zgolj preko bank?
- Ali se zavedam, da ima banka pravico, da mi v vsakem trenutku zapre moj bančni račun in zaseže razpoložljiva sredstva?

V kolikor bralec ni začutil pomembnosti zgornjih vprašanj potem zanj BitCoin ne prinaša novosti in je iz praktičnega stališča neuporaben. V primeru, da so zgornja vprašanja vzbudila zavedanje o represiji, ki jo montarni in bančniški sistem izvajata, potem mu BitCoin prinaša tudi koristi. Na kratko lahko lastnosti BitCoin-a povzamemo s spodnjimi alinejami:

- Odprava vmesnega posrednika. Transakcije sredstev se opravljajo brez posrednikov.
- Popolna anonimnost transakcij. Za transakcijo med Alenko in Bojanom vesta samo Alenka in Bojan.
- Vrednost denarja je striktno določena z ponudbo in povpraševanjem. Z drugimi besedami - inflacijo oz. deflacijo ni možno neposredno manipulirati.

Zgoraj omenjene točke ne predstavljajo bistvene tehnološke zanimivosti dokler ne vzamemo v zakup, da mora vsak smiseln monetarni sistem omogočati tudi varnost. Lepota BitCoin-a se skriva ravno v implementaciji zgoraj navedenih lasnosti in hkratnem zagotavljanju varnosti ter integritete bilans uporabnikov. V nadaljevanju so opisani mehanizmi delovanja, ki omogočajo zgoraj opisane storitve.

2 Delovanje BitCoin omrežja

V tem odseku je opisano delovanje omrežja BitCoin. Predpostavili bomo, da se celotno dogajanje vrši v nekem *p2p* omrežju, v katerem si vozlišča izmenjujejo podatke. Opis delovanja določenih aspektov sistema je poenostavljen, podrobnosti pa so dopolnjene v 3. razdelku kjer obravnavamo varnostne vidike BitCoin-a.

Za začetek bomo opisali osnovne gradnike omrežja.

2.1 Transakcije

Celotno delovanje BitCoin omrežja temelji na transakcijah. Pojem *kovanca* (coina) je definiran šele na višjih nivojih (v aplikacijah) kot posebna vrsta transakcije. Za lažje razumevanje predpostavimo sledeč (nepopolen, a za trenutno znanje primeren) scenarij:

- Bojan je opisan s trojko $(A_b, (PU_b, PR_b))$ kjer je A_b njegov BitCoin naslov[2], (PU_b, PR_b) pa javni/privatni ključ nekega kriptosistema za podpisovanje.[3]
- Alenka je opisan s trojko $(A_a, (PU_a, PR_a))$ definirano analogno kot v Bojanovem primeru.

Recimo, da želi Bojan Alenki kreditirati x enot denarja, pri čemer obstaja v omrežju evidenca o tem[4], da ima Bojan dana sredstva.

Bojan ustvari transakcijo v kateri sta (med drugim) dve meta komponenti: Bojanov podpis in naslov A_a. Podpis je potreben, da se dejansko preveri, da je zahtevo po transakciji izvršil Bojan.[5] Ustvarjanje nove transakcije je shematično prikazano tudi na Sliki 1.

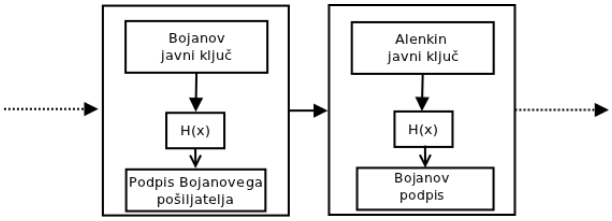
Bojan transakcijo pošlje po *p2p* omrežju BitCoin sistema, tako, da lahko vsako vozlišče omrežja evidentira transakcijo med Bojanom in Alenko.

[2]Kot bomo videli, je naslov ponavadi kar vrednost neke zgoščevalne funkcije aplicirane na PU_b

[3]V trenutni implementacij je uporabljen *ECDSA* [3].

[4]Kako je evidenca implementirana, bomo videli kasneje.

[5]Opomba. V dejanski implementaciji BitCoin sistema, so na tem mestu lahko dodane tudi dodatne informacije in zahteve, ki določajo pod kakšnimi pogoji se lahko transakcija izvede [4].



Slika 1: Slika prikazuje tvorjenje novih transakcij v BitCoin omrežju. Iz slike je razvidno, kako transakcije na naraven način tvorijo seznam vseh transakcij prek reference na polje $h(x)$, ki predstavlja vrednost neke razpršilne funkcije aplicirane na starševski transakciji.

2.2 Decentralizirano evidentiranje transakcij

V prejšnjem razdelku smo videli strukturo transakcije in kako nastane transakcija med dvema uporabnikoma. [6] Vprašanje, kako omrežje ve, da je transakcija ne mestu in kako je evidentiran seznam vseh transakcij, smo pustili odprto.

Vprašanje ima zelo preprost odgovor v kolikor dopuščamo možnost centra zaupanja C. Vsako zahtevano transakcijo pošlje Bojan $C-$ju, katerega naloga je, da vodi evidenco vseh transakcij. V kolikor je Bojanova zahteva veljavna, se Alenki (prek centra C) kreditira ustrezno količino denarja, opravljeno transakcijo pa posodobi v seznam, ki ga C hrani.

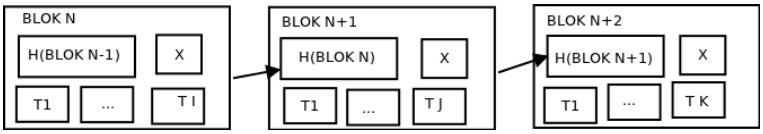
Vsaka taka rešitev pa je seveda ekvivalentna današnjemu sistemu, kjer C predstavlja banko. Obstajajo tudi elektrosnke različice takšnih sistemov, npr. *PayPal* ali *Skrill.*

Decentralizirana rešitev, ki jo uporablja BitCoin temelji na uporabi koncepta o *dokazanem delu* (proof of work system [5, 6]). Ideja je, da celotno p2p omrežje sodeluje pri gradnji seznama transakcij, ta seznam pa ima strukturo, ki onemogoča enostavno izgradnjo seznama. Vsakič, ko se uporabnik pojavi v omrežju, pošlje zahtevo po seznamu transakcij in sprejme najdaljši veljaven[7] seznam, ki mu nato služi za evidenco dosedanjih transakcij.

V praksi ima seznam strukturo kot jo prikazuje Slika 2. Element seznama je blok B, ki hrani nek seznam transakcij, vrednost razpršilne funkcije h aplicirano na trenutno zadnjem bloku iz najdaljšega seznama , hkrati pa mora blok vsebovati takšno število X, da se razpršena vrednost bloka $B - h(B)$

[6] Dobro se je zavedati, da to ni edini način, kako lahko nastane transakcija.

[7] Veljavnost seznama je podrobneje opisana v sekciji 3.2.



Slika 2: Na sliki je prikazna struktura seznama blokov (angleško *block chain*). Vsak naslednji blok je odvisen od prejšnjega, zato je pri generiranju novega elementa v seznamu, potrebno upostevati kakšen je zadnji element seznama.Vsako vozlišče hrani skupno verzijo takšnega seznama.

začne z predpisanim številom ničel k.

Ker se domneva, da ima iskanje takega števila X časovno kompleksnost eksponentnega reda v k, predstavlja iskanje novega bloka računski izziv v katerem sodelujejo vsa vozlišča p2p omrežja. V kolikor bi napadalec želel manipulirati seznam transakcij, bi po računski zmogljivosti moral konkurirati računski zmogljivosti celotnega omrežja.

2.3 Delovanje omrežja

Z dosedaj povedanim, lahko strnemo delovanje BitCoin omrežja na sledeče alineje

1. Zahteve po novih transakcijah se konstantno pošiljajo vsem vozliščem omrežja
2. Vozlišča zbirajo transakcije in jih 'zapakirajo' v blok B
3. Vsako vozlišče išče ustrezno glavo X, da bo blok B veljaven element najdaljšega seznama
4. Ko neko vozlišče najde ustrezno glavo za B, razpošlje (broadcasting) B vsem vozliščem
5. Vozlišča preverijo veljavnost bloka - to je, da so vse transakcije v B veljavne, inda B zares dopolnjuje trenutno najdaljši seznam,
6. Vozlišča sprejmejo blok B tako, da ga dodajo v lastnen seznam najdaljšega bloka in računajo nove bloke, ki v glavi vsebujejo razpršeno vrednost bloka B, kot je to prikazano na Sliki 2

V kolikor bi v 4. koraku dve vozlišči našli veljavno glavo za nek novi blok, se lahko zgodi, da določena vozlišča omrežja dobita oba bloka v različnih vrstnih redih. V takšnem primeru vozlišče nadaljuje na razširjevanju seznama, ki za zadnji element vsebuje prvo dobljeni blok $B1$, drugi blok $B2$ pa shrani za primer, ko bo seznam, ki za zadnji elemenet vsebuje $B2$, prevladal. Konflikt bo razrešilo vozlišče, ki bo naslednje našlo veljaven blok za nov sklop transakcij, saj bo ta novi blok hranil tudi informacijo o predhodnem bloku, ki bo $B1$ ali $B2$.

2.4 Rudarjenje BitCoin-ov

Kot smo do sedaj povedali, se zahteve po transakcijah pošiljajo v p2p omrežje, vozlišča jih enkapsulirajo v bloke in iščejo ustrezno glavo bloka, ki razširja najdaljši znan seznam blokov. Argument za varnost takšnega sistema temelji na predpostavki, da je moč iskanja ustreznih blokov celotnega omrežja večja od moči individualenga napadalca.

Seveda se pri takem sistemu poraja vprašanje, zakaj bi vozlišča v omrežju sploh iskala ustrezne glave blokov?

Odgovor leži v konvenciji, da v vsakem veljavnem bloku B, prva transakcija kreditira 50 BitCoin-ov najditelju glave B. Z iskanjem ustreznih glav si torej vozlišča v omrežju prisvojijo plačilo. Dejstvo, da imajo BitCoin-i tudi realno vrednost v vseh trenutno priznanih valutah, [8] je sprožil pojav takoimenovanega *BitCoin rudarjenja* (BitCoin mining) [7, 8, 9].

Naj omenimo, da je število BitCoinov navzgor omejeno,[9] kar bi lahko povzročalo težavo ob iztrošenju vseh BitCoinov in posledičnemu vpadu motivacije rudarjenja. Rešitev predstavlja uvedba provizije pri transakciji s katero bi si vozlišča zagotovila profit pri iskanju pravilnih blokov.

3 Varnost

V tem razdelku obravnavamo varnostni aspekt BitCoin sistema. Veliko vprašanj, ki so ostala odprta še iz Razdelka 2, razjasnimo v tem odseku na praktičnih primerih. Predstavljeni so možni načini napada in ustrezne tehnične omejitve povezane z napadi.

[8] Na dan pisanja je vrednost enega BitCoina $5.26.

[9] Izračuni ocenjujejo, da bo zgornja meja dosežena približno leta 2033.

3.1 Zasebnost

Za razliko od današnjega modela bank, so pri BitCoin sistemu vse transakcije javne. Za zasebnost transakcij se lahko poskrbi na drugem nivoju in sicer pri politiki upravljanja ključev sistema za podpisovanje. Za ustrezen nivo anonimnosti je priporočeno, da uporabniki tretirajo javni ključ kriptosistema na enak način kot zasebni. Pri transakcijah pa navedejo le naslov za transakcijo, ki je kar razpršilna vrednost javnega ključa.

Poleg tega, se za dodatno varnost priporoča generiranje novega BitCoin ID-ja (t.j, novega para (zasebni, javni ključ)) za vsako transakcijo.

V BitCoin omrežju je možno slediti toku vsakega BitCoina [12], zato je potreba po varnem hranjenju zasebnega in javnega ključa zelo pomembna. Praktični napotki kako doseči maksimalno anonimnost znotraj BitCoin omrežja so obravavani v [11].

3.2 Kreiranje novega neodvisnega najdaljšega seznama blokov

Predpostavimo scenarij, ko nek napadalec želi ustvariti seznam blokov $S = B_1 \mapsto B_2 \mapsto \cdots \mapsto B_n$, tako da bo S najdaljši veljaven seznam v omrežju. Da bi omrežje S sprejelo kot veljaven seznam, mora vrednost razpršilne funkcije aplicirane na $h(B_i)$ $(1 \leq i \leq n)$ vsebovati k_i ničel, kjer k_i ni konstanta ampak je odvisna od $B_1, \ldots, B_{i-1}$.

Na vsakih 2016 blokov se izračuna koliko časa t je bilo potrebnega[10] za generiranje predhodnih 2015, blokov na osnovi tega pa se določi vrednost k_i, tako da se predhodno vrednost k_{i-1} pomnoži z razmerjem trajanja dveh tednov in t.

Torej, če t_w označuje čas trajanja enega tedna, izraženega v istih enotah kot t, lahko izračunamo k_{i+1} na sledeči način:

$$f = t_w/t,$$
$$k_{i+1} = k_i * f.$$

Vsak seznam blokov S, ki ne ustreza zgoraj opisanim zahtevam, ni veljaven in je posledično zavrnjen s strani vozlišč $p2p$ omrežja.

Ob predpostavki, da je časvona kompleksnost iskanja niza x, tako da ima $h(x)$ k ničel, eksponentna v k, predstavlja zgornji mehanizem zelo težavno

[10] Na osnovi časovnih žigov, ki jih vsak blok vsebuje.

prepreko, ki onemogoča izgradnjo popolnoma novega seznama S, s katerim bi napadalec lahko manipuliral poljubne transakcije v omrežju.

3.3 Preprečevanje dvojne potrošnje

Po premisleku iz prejšnjega podrazdelka, je napad, kjer bi napadalec izgradil popolnoma nov seznam blokov, računsko nedosegljiv podvig.[11]

Naslednji možni scenarij, ki bi potencialno ogrožal konsistentnost transakcij predstavlja naslednja situacija:

- Bojan pošlje transakcijo s katero Alenki dodeli nekaj enot denarja
- Vozlišča sprejmejo transakcijo kot veljavno in jo (posredno prek nekega bloka) dodajo v najdaljši seznam blokov S
- Bojan začne na osnovi S delati alternativen seznam blokov, ki bo daljši od trenutno najdaljšega seznama in ne bo vseboval bloka z njegovo transakcijo Alenki

Zgoraj omenjen scenarij je znan pod imenom *problema dvojne potrošnje* (angleško, *double spending problem*). Dirko, v kateri Bojan želi ustvariti najdaljši seznam, ki ne vsebuje njegove transakcije in ustvarjanjem novih veljavnih blokov s strani celotnega omrežja, lahko karakteriziramo z naključnim binomskim sprehodom v 1 dimenziji [10]. Uspeh (tvorba novega bloka) celotnega omrežja predstavimo s korakom za $+1$ enoto naprej, uspeh Bojana pa s korakom za 1 enoto nazaj (-1 naprej.)

Opisan problem lahko modeliramo na sledeč način. Naj bo p verjetnost, da omrežje najde naslednji veljaven blok, q verjetnost da Bojan najde naslednji blok in q_z verjetnost, da Bojan uspe prehiteti omrežje (v gradnji seznama), ob predpostavki, da je dirko začel z zaostankom $z \geq 1$ korakov. Verjetnost q_z lahko tedaj izrazimo kot

$$q_z = (\frac{q}{p})^z$$

Kjer je seveda naša sklep, da je $p < q$, saj je osnovna predpostavka, da je računska zmogljivost celotnega omrežja večja od računske zmogljivosti napadalca (Bojana). Verjetnost Bojanovega uspeha torej eksponentno pada glede na začetni zaostanek dolžine generiranih seznamov.

[11] Ob ustrezni predpostavki, da $P \neq NP$.

q	z
0.10	5
0.15	8
0.20	11
0.25	15
0.30	24
0.35	41
0.40	89
0.45	340

Tabela 1: Tabela prikazuje število blokov z, za katere naj Alenka počaka, da se pojavijo za njeno transakcijo. Vrednost z je določena tako, da bo tedaj verjetnost uspeha Bojanovega napada manjša od 0.001 pri čemur je verjetnost, da Bojan najde novi uspešen blok pred celotnim omrežjem, q.

Ostaja še vprašanje, koliko časa mora Alenki počakati, da lahko varno zaključi, da Bojan ne bo sposoben spremeniti njegove transakcije.

Predpostavimo, da Alenka sprejeme Bojanovo plačilo šele ko je za njeno transakcijo bilo dodanih z novih blokov. Želimo najti z, da bo verjetnost, da bo Bojan uspel spremeniti transakcijo manjša od 0.001.Potencialen napredek Bojana lahko opišemo kot poissonovo distribucijo z matematičnim upanjem

$$\lambda = z\frac{q}{p}.$$

Verjetnost Bojanovega uspeha lahko tedaj izrazimo kot

$$1 - \sum_{k=0}^{z}(\frac{\lambda^k e^{-\lambda}}{k!}(1 - (\frac{q}{p})^{z-k}))$$

Rešitve zgornje enačbe pri verjentosti $p < 0.001$ so strnjene v Tabeli 1, kjer so za različne verjetnosti q predstavljene optimalne vrednosti z.

V praksi se trenutno priporoča vrednost $z = 6$. Velja pa omeniti še, da v kolikor je transakcija med Bojanom in Alenko v vrednosti x BitCoin-ov, potem se pri vrednosti $z \geq x/50$ Bojanu ne splača manipulirati seznama in opehariti Alenko, saj ima pri taki računski sposobnosti večji profit, če pomaga omrežju najti naslednjih z veljavnih blokov in si tako prislužiti $z * 50 > x$ BitCoinov.

3.4 DoS napad

Vpliv DoS napadov na BitCoin omrežje ni dobro raziskano področje. Znano je, da lahko DoS napad na določenega uporabnika sistema BitCoin onemogoča normalno procesiranje transakcij danega uporabnika. BitCoin ima vgrajene mehanizme za preprečevanje takšnih napadov [12], njihova učinkovitost pa ni dobro raziskana. Gavin Andresen, eden izmed glanvih razvijalcev BitCoina, je ze dobro leto nazaj izrazil željo po orodju za testiranje DoS scenarijev BitCoin omrežja [1].

4 Zaključek

Prišli smo v točko, ko se družba sooča z omejitvami trenutnega denarnega sistema, zato je čedalje več ljudi odprtih na alternative. V dani seminarski nalogi je predstavljena ena izmed takšnih alternativ - elektronski monetarni sistem BitCoin.

Ker je z denarjem povezanih veliko goljufij, kraj in zlorab mora vsak dober elektronski sistem temeljiti na dobri varnosti. Konkretno smo za sistem BitCoin obravnavali trenutno znane varnostne mehanizme in ustrezne pomankljivosti. Ker je BitCoin sorazmeroma nov sistem je težko zaključiti z absolutnim odgovorom, ki bi zagovarjal njegovo uporabo. Končen odgovor lahko poda samo en sodnik - čas.

[12] Vozlišče prekine povezavo z vozliščem, ki mu pošilja preveč informacij na določeno časovno enoto.

Literatura

[1] Gavin Andresen, 'Are there any tools for simulating attacks on Bitcoin network?', February 28, 2012, https://bitcointalk.org/index.php?PHPSESSID=850fc7366bc2e00fcb62797cd7ff2772&topic=66537.msg773735#msg773735

[2] Wikipedia, 'Gold Standard', Dostopano 28. marec 2012, http://en.wikipedia.org/wiki/Gold_standard

[3] Elliptic Curve Cryptography, Bundesamt fur Sicherheit in der Informationstechnik, https://www.bsi.bund.de/cae/servlet/.../BSI-TR-03111_pdf.pdf

[4] The BitCoin Wiki, 'Script', Dostopano 28. marec 2012, https://en.bitcoin.it/wiki/Script

[5] Liu, Debin; Camp, L. Jean (2006). 'Proof of Work can work'. Fifth Workshop on the Economics of Information Security.

[6] Wikipedia, 'Proof-of-work system', Dostopano 28. marec 2012, http://en.wikipedia.org/wiki/Proof-of-work_system

[7] We Use Coins, 'About BitCoin mining', Dostopano 28. marec 2012, http://www.weusecoins.com/mining-guide.php

[8] Blockchain, BitCoin pool info,Dostopano 28. marec 2012 , http://blockchain.info/pools

[9] DeepBit, 'Collective mining pool', Dostopano 28. marec 2012, http://deepbit.net/

[10] Wolfram, 'Random Walk–1-Dimensional', Dostopano 28. marec 2012, http://mathworld.wolfram.com/RandomWalk1-Dimensional.html

[11] The BitCoin wiki, 'Staying Anonymous', Dostopano 28. marec 2012, https://en.bitcoin.it/wiki/Anonymity#Staying_Anonymous

[12] The BitCoin wiki, 'Tracing a coin's history', Dostopano 28. marec 2012, https://en.bitcoin.it/wiki/Attacks#Tracing_a_coin.27s_history

[13] Satoshi Nakamoto, BitCoin: A Peer-to-Peer Electronic Cash System, rokopis.