Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Peter Korošec

# Varnost in anonimnost pri plačevanju s spletno valuto Bitcoin

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Mentor: doc. dr. Mojca Ciglarič

Ljubljana 2016

*Besedilo je oblikovano z urejevalnikom besedil LaTeX.*

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Pojasnite problematiko spletnih plačil in motivacijo za nastanek digitalnih valut. Osredotočite se na pojem anonimnosti in na možne načine njenega zagotavljanja. Preučite in opišite način delovanja spletne valute in sistema Bitcoin. Pojasnite kriptografsko ozadje in mehanizme, ki pri plačevanju zagotavljajo varnost, zaupnost in anonimnost. Glede na to poiščite možne napade na transkacije Bitcoin in na njegov mehanizem hranjenja in distribucije podatkov. Izberite napad, ki se vam zdi najbolj izvedljiv in ga simulirajte v svoji pilotni postavitvi majhnega okolja Bitcoin. Komentirajte težavnost izvedbe, možne protiukrepe in realnost grožnje, ki jo napad predstavlja za trgovce, ki sprejemajo plačila s to spletno valuto.

# Izjava o avtorstvu diplomskega dela

Spodaj podpisani Peter Korošec sem avtor diplomskega dela z naslovom:

*Varnost in anonimnost pri plačevanju s spletno valuto Bitcoin*

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 12. februarja 2016 Podpis avtorja:

*Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za pomoč in nasvete pri izdelavi diplomskega dela. Zahvaljujem se tudi staršema in vsem ostalim, ki so me podpirali tekom študija.*

# Kazalo

# Seznam uporabljenih kratic

| kratica | angleško | slovensko |
|---|---|---|
| **BTC** | bitcoin | bitcoin |
| **P2P** | peer-to-peer | Od točke do točke |
| **USD** | United States Dollar | Ameriški dolar |
| **SHA** | Secure Hash Algorithm | Varni hash algoritem |
| **VPN** | Virtual Private Network | Virtualno zasebno omrežje |
| **IP** | Internet Protocol | Internetni protokol |

# Povzetek

V diplomski nalogi je predstavljen digitalni plačilni sistem Bitcoin. Opisana je kriptografija, na kateri je sistem zasnovan. Predstavljeno je delovanje in kratka zgodovina sistema. Večji poudarek je na oceni anonimnosti pri plačevanju z Bitcoinom in na zagotavljanju varnosti pri izvedbi transakcij. V sklopu anonimnosti je opisan nivo prikrivanja identitete, ki ga zagotavlja sistem in dodatni mehanizmi in opozorila, ki so potrebni za anonimno plačevanje. V sklopu varnosti so naštete potencialne ranljivosti sistema Bitcoin, izpostavljena je šibka točka pri sprejemanju hitrih plačil, ki napadalcem omogoča izvedbo tako imenovanega double-spending napada. Praktično je prikazano, kako je možno brez posebnih orodij z odprtokodno programsko opremo, ki jo razvija Bitcoin skupnost sama, izvesti napad.

**Ključne besede:** Bitcoin, anonimnost, dvakratna poraba.

# Abstract

This thesis presents the digital payment system Bitcoin. It describes the cryptography on which the system is based. Presented are the short history of the system and the principles of how it works. Highlighted are the state of anonymity that the system provides while making payments and the safety it guarantees while executing transactions. Within the context of anonymity, the state of masking the users identity within the payment system is described, together with warnings and mechanisms to better hide the users identity. Considering the safety of Bitcoin transactions, potential vulnerabilities of the system are listed. Exposed is a weakness, while accepting fast payments, that enables attackers the execution of the double-spending attack. Practically it is demonstrated, how to execute the attack without special tools, with the use of opensource software recomended and developed by the Bitcoin community.

**Keywords:** Bitcoin, anonymity, double-spending.

# Poglavje 1

# Uvod

Bitcoin je elektronski plačilni sistem, ki je bil prvič opisan v članku Satoshija Nakamota leta 2008. Bitcoin se zanaša na digitalne podpise za dokazovanje lastništva valute in na javno bazo transakcij za preprečevanje napadov z dvakratno porabo. Zgodovina transakcij se deli med uporabniki P2P omrežja in se validira s pomočjo "proof-of-work" sistema.

Cilj diplomske naloge je raziskati delovanje Bitcoin sistema in varnostnih mehanizmov, ki jih uporablja, ter ugotoviti stopnjo varnosti, anonimnosti in zasebnosti, ki jo ponuja. Namen je tudi identificirati znane napade in enega izmed njih reproducirati v laboratorijskem okolju, da se ugotovi težavnost izvedbe napada.

V naslednjem poglavju so opisane kriptografske metode, na katerih temelji Bitcoin. V tretjem poglavju sta predstavljena Bitcoin sistem in istoimenska valuta na splošno. Opisano je delovanje sistema in potek izvajanja transakcij, skupaj s kratko zgodovino valute. Četrto poglavje je namenjeno pregledu anonimnosti pri izvajanju Bitcoin transakcij in načinom za ohranjanje anonimnosti. V petem poglavju so naštete ranljivosti sistema in opisani nekateri napadi. Izpostavljena je situacija, ko trgovec sprejema Bitcoin v sklopu hitrih plačil - ko je čas med menjavo plačila in blaga ali storitve kratek. Takrat je trgovec izpostavljen napadu z dvakratno porabo. Praktično je prikazana izvedba napada s pomočjo programske opreme Bitcoin Core. Prikazana je

uspešnost napada v povezavi z različnimi dejavniki in predlaganih je nekaj možnih protiukrepov.

# Poglavje 2

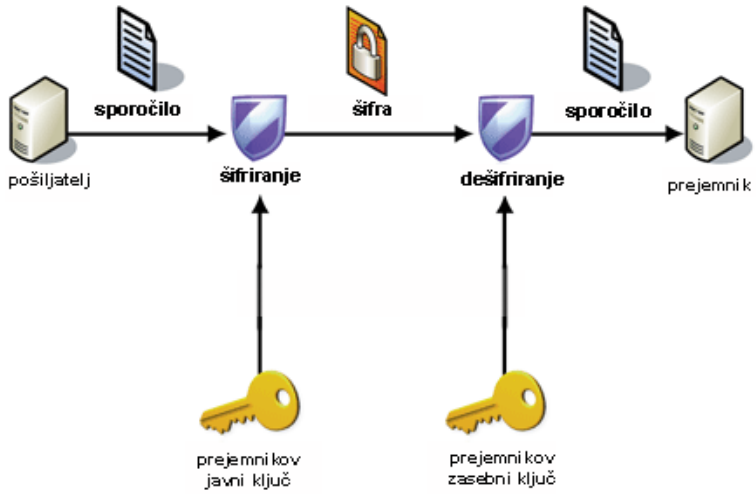
# Kriptografija

Kriptografija je veda, ki se ukvarja z načini vzpostavljanja varne, tajne komunikacije. Varna komunikacija zagotavlja zaupnost in integriteto sporočila, omogoča avtentikacijo in zagotavlja operacijsko varnost. Zaupnost v tem kontekstu pomeni, da lahko sporočilo razume le oseba, ki ji je bilo namenjeno. Zagotavljanje integritete pomeni, da lahko zaznamo morebitno spremembo ali popačenje sporočila med pošiljanjem. Avtentikacija napadalcu onemogoča, da se izdaja za pošiljatelja. Prejemnik želi biti prepričan s kom komunicira. Operacijska varnost pa je zagotavljanje same zmožnosti komuciranja. Gre torej za konstrukcijo in analizo protokolov, ki morebitnemu napadalcu onemogočajo prisluškovanje, prirejanje sporočil ali motenje komunikacije. Moderno kriptografijo delimo na simetrično in asimetrično. Pri simetrični pošiljatelj in prejemnik sporočila uporabita enak ključ za šifriranje in dešifriranje sporočila. Pri asimetrični sta ključa različna.

Kriptografija predstavlja temelj za delovanje sistema Bitcoin. Bitcoin imenujejo tudi prva delujoča kriptovaluta. [11] Pri Bitcoinovih transakcijah se uporablja ECDSA algoritem. Algoritem uporablja kriptografijo eliptičnih krivulj, enega izmed pristopov k asimetrični kriptografiji. Pri Bitcoin rudarjenju se uporablja Hashcash algoritem, ki temelji na kriptografskih hash funkcijah. [15]

## 2.1 Kriptografija javnega ključa

Asimetrično kriptografijo imenujemo tudi kriptografijo javnega ključa. Pri kriptografiji z javnim ključem ima vsak sodelujoči dva različna ključa. Javnega, ki je znan vsem in zasebnega, ki ga pozna le on. Pošiljatelj najprej pridobi javni ključ prejemnika. Sporočilo šifrira s pomočjo znanega enkripcijskega algoritma in z javnim ključem. Prejemnik šifrirano sporočilo dešifrira s zasebnim ključem in znanim algoritmom. Ključa in algoritem so torej izbrani tako, da lahko z zasebnim ključem dešifriramo sporočilo, ki je bilo šifrirano z javnim. Velja tudi obratno. Z javnim ključem lahko dešifriramo sporočilo, ki je bilo šifrirano z zasebnim. Kriptografija javnega ključa tako omogoča varno komunikacijo brez izmenjave vnaprej dogovorjenega gesla. [35]

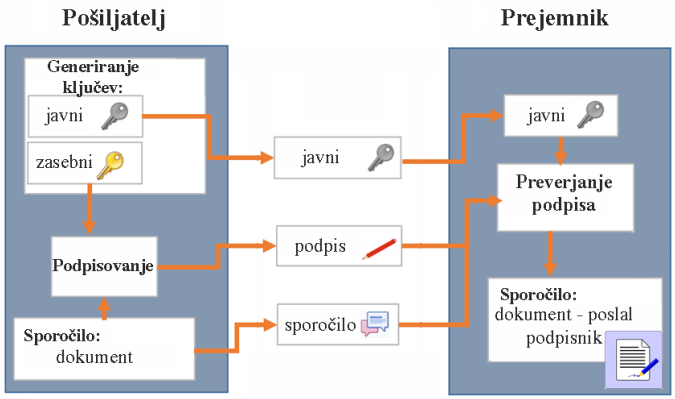



Slika 2.1: Kriptografija z javnim ključem

## 2.2 Digitalni podpisi

Digitalni podpis je kriptografska tehnika za dokazovanje avtentičnosti in integritete sporočil. Veljaven digitalni podpis prejemniku zagotavlja, da je sporočilo poslal znan prejemnik in da med pošiljanjem ni bilo spremenjeno.

Prav tako pošiljatelj ne more trditi, da sporočila ni poslal (če je njegov zasebni ključ res skriven). Digitalni podpisi temeljijo na asimetrični kriptografiji. Digitalni podpis sloni na treh algoritmih. Algoritem za generiranje ključev ustvari par javnega in zasebnega kjuča, vrne naključni zasebni ključ iz nabora možnih ključev in pripadajoči javni ključ. Algoritem za podpisovanje iz sporočila in zasebnega ključa ustvari podpis. Algoritem za potrjevanje podpisa na podlagi sporočila, podpisa in javnega ključa sporočilo potrdi ali zavrže.




Slika 2.2: Digitalno podpisovanje

Elliptic Curve Digital Signature Algorithm (ECDSA), ki ga za digitalno podpisovanje transakcij uporablja Bitcoin, je varianta Digital Signature Algorithm (DSA). [19] ECDSA deluje podobno, pomaga si z zakonitostmi eliptičnih krivulj. Algoritem je podrobno opisan v [9].

### 2.2.1 DSA

Algoritem za generiranje ključev je sestavljen iz dveh delov. V prvem delu se določijo parametri, ki jih bo algoritem uporabljal. V drugem se na podlagi parametrov generirajo ključi.

**Izbira parametrov:**

- izbira kriptografske zgoščevalne funkcije - Bitcoin uporablja SHA-256
- določitev parametrov $L$ in $N$, števili predstavljata bitni dolžini $p$ in $q$, izbira vpliva na kriptografsko moč digitalnega podpisa, daljši števili dajeta boljšo zaščito, standard priporoča vrednosti $L = 2048$, $N = 256$
- izbira L-bitnega praštevila $p$
- izbira N-bitnega praštevila $q$, tako, da velja $q$ je delitelj $p - 1$
- izbira parametra $g$, velja: $g = h^{(p-1)/q} \bmod p$, kjer je $(1 < h < p - 1)$, če je rezultat 1, postopek ponovimo z drugim številom $h$

**Generiranje ključev:**

- naključna izbira števila $x$, $0 < x < q$
- izračun $y = gx \bmod p$
- javni ključ je $y$
- zasebni ključ je $x$

Parametri in javni ključ so znani uporabnikom sistema, zasebni ključ je skriven. Predpostavimo, da je H - zgoščevalna funkcija in m - originalno sporočilo.

**Podpisovanje:**

- naključna izbira vrednosti $k$, $0 < k < q$
- izračun $r = (g^k \bmod p) \bmod q$, če je $r = 0$ ponovimo z drugim $k$
- izračun $s = k^{-1}(H(m) + xr) \bmod q$, če je $s = 0$ ponovimo z drugim $k$
- podpis je nabor $(r, s)$

Pri podpisovanju torej pošiljatelj šifrira sporočilo (ki je bilo prej zgoščeno s hash funkcijo) s svojim zasebnim ključem. Pridobi podpis sestavljen iz r in s. Sporočilo pošlje skupaj s podpisom.

**Preverjanje podpisa:**

- če $0 < r, s < q$ zavrni podpis
- izračun $w = s^{-1} \bmod q$
- izračun $u1 = H(m)w \bmod q$
- izračun $u2 = rw \bmod q$
- izračun $v = ((g^{u1}y^{u2}) \bmod p) \bmod q$
- podpis je veljaven, če je $v = r$

Prejemnik dešifrira podpis z javnim ključem pošiljatelja. Pridobi zgoščeno obliko sporočila. Potem sporočilo, ki ga je prejel skupaj s podpisom, zgosti z isto zgoščevalno funkcijo kot pošiljatelj. Če se zgoščeni vrednosti ujemata, je podpis veljaven. Sporočilo, ki ga je prejel je enako sporočilu, ki ga je pošiljatelj podpisal.

## 2.3 Kriptografske zgoščevalne funkcije

Zgoščevalna (hash) funkcija vhodnim podatkom priredi niz znakov fiksne dolžine, imenovan hash - zgoščena vrednost. Kriptografska zgoščevalna funkcija mora izpolnjevati dodaten kriterij. Praktično neizvedljivo je reproducirati originalno sporočilo, če poznamo hash. [35] Idealna kriptografska zgoščevalna funkcija ima poleg tega še naslednje lastnosti:

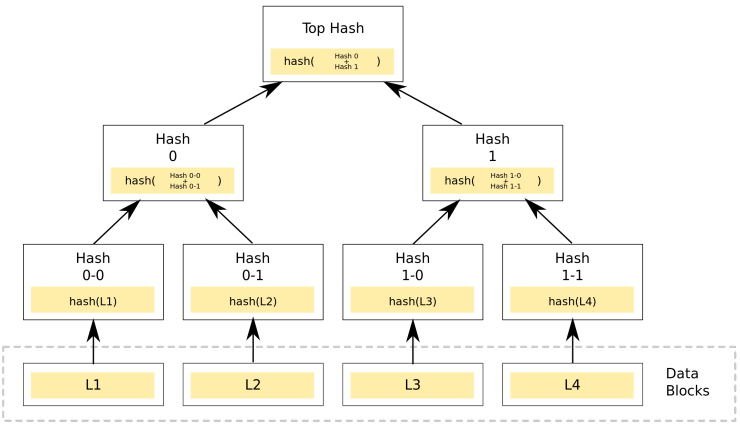
- izračun hasha je enostaven za poljubno sporočilo
- praktično neizvedljivo je najti dve različni sporočili, ki vrneta enak hash

- praktično neizvedljivo je spremeniti sporočilo, ne da bi se spremenil hash

Bitcoin za svoje delovanje uporablja SHA-256 in RIPEMD-160 funkciji. [15] Večino časa se uporablja SHA-256, RIPEMD-160 se uporabi le v primeru, ko je zaželjen krajši hash. SHA 2 je skupina kriptografskih zgoščevalnih funkcij, ki jih je razvila ameriška vladna agencija NSA. SHA-256 je ena izmed šestih funkcij iz te skupine. Oznaka 256 predstavlja bitno dolžino hasha, ki ga funkcija vrne. Funkcija je podrobno opisana v [20].

## 2.4 Merklova drevesa

Merklovo drevo ali hash drevo je v kriptografiji drevo, pri katerem vsako vozlišče, ki ni list, vsebuje hash svojih otrok. Omogoča učinkovito verifikacijo vsebine velikih podatkovnih struktur. S pomočjo korena je mogoče preveriti veljavnost vseh ostalih hashev v drevesu. Pri Bitcoinu se uporablja za združevanje vseh transakcij znotraj enega bloka podatkov v en sam hash.




Slika 2.3: Primer Merklovega drevesa [16]

## 2.5 Algoritem Hashcash

Proof-of-work je podatek, ki ga je težko (računsko zahtevno in časovno potratno) ustvariti, enostavno pa ga je preveriti in ugotoviti, ali ustreza določenim zahtevam. Bitcoin v ta namen uporablja algoritem Hashcash.

Hashcash je predlagal Adam Black leta 1997 z namenom, da bi omejil nezaželjeno elektronsko pošto. Ideja je bila, da se v glavo elektronskega sporočila doda Hashcash proof-of-work, ki dokazuje, da je pošiljatelj porabil določeno količino procesorskega časa za pošiljanje sporočila. Na ta način bi otežil pošiljanje velikega števila elektronskih sporočil "spammerjem".

Kasneje je Satoshi Nakamoto prirejeno različico uporabil pri Bitcoin sistemu. Algoritem temelji na kriptografskih zgoščevalnih funkcijah in izkorišča njihove lastnosti. Cilj algoritma je generirati hash (niz znakov), določene oblike. V ta namen se sporočilu dodaja žeton, številska vrednost, imenovana "nonce", ki se v vsaki iteraciji poveča, dokler dobljeni niz znakov ne ustreza zahtevam. Niz se mora začeti z vnaprej določenim številom ničel. Z zahtevanim številom ničel je možno nadzorovati računsko zahtevnost iskanja prave vrednosti, medtem ko za validacijo zadostuje izračun ene zgoščevalne funkcjie. Kot zgoščevalna funkcija se pri Bitcoinu uporablja SHA-256, ki se za dodatno varnost uporabi dvakrat zaporedoma (izračuna se hash hasha). Zahtevnost pa se regulira tako, da je povprečni čas iskanja žetona 10 minut. [18, 14]

# Poglavje 3

# Splošno o bitcoinu

## 3.1 Digitalne valute

Digitalne valute so medij za menjavo, ki temelji na internetu in omogoča takojšnje izvajanje transakcij in prenos lastništva brez upoštevanja državnih mej. Delijo se na virtualne valute in kriptovalute. [46] Virtualne valute fizično ne obstajajo in niso namenjene za kupovanje fizičnih dobrin. Za oskrbo in upravljanje z denarjem skrbijo razvijalci virtualnega okolja, v katerem se valuta uporablja. Primer je denar v spletni igri. Kriptovalute se za svoje delovanje zanašajo na kriptografijo in nimajo centralne avtoritete. Lahko se uporabljajo za kupovanje fizičnih dobrin.

Najpopularnejše so Bitcoin, Litecoin in Ripple. Litecoin je tehnično skoraj enak Bitcoinu. Nastal je kot veja Bitcoin-Qt odjemalca. Od Bitcoina se razlikuje v nižji težavnosti za izračun bloka, večjem maksimalnem številu enot in kriptografski zgoščevalni funkciji, ki jo uporablja. Ripple je sistem, ki omogoča pošiljanje denarja in trgovanje z valutami. V nasprotju z Bitcoinom Ripple za svoje delovanje potrebuje sodelovanje finančnih ustanov. Ripple med seboj direktno povezuje različne finančne ustanove in omogoča pošiljanje najrazličnejših nosilcev vrednosti (od valut do minut v mobilnem omrežju) z nizkimi provizijami in visoko hitrostjo. [7]

Idejo digitalnega denarja je prvi predstavil David Chaum leta 1983. Leta

1990 je ustvaril podjetje DigiCash. Istoimenski plačilni sistem je za anonimizacijo transakcij uporabljal kriptografske protokole. 1996 se je pojavil e-gold, ki je temeljil na zlatu. Uporabniki so poslali fizično zlato in v zameno na račun prejeli "e-gold". [32] Prvi je opisal koncept kriptovalute Wei Dai leta 1998 na cyberphunks seznamu za elektronsko pošto. Predstavil je idejo denarja, ki bi za svoj nastanek in transakcije uporabljal kriptografijo. [12]

## 3.2 Motivacija in nastanek

Oktobra leta 2008 je Satoshi Nakamoto objavil članek z naslovom **Bitcoin: A Peer-to-Peer Electronic Cash System**. V njem je opisal idejo elektronskega denarja, ki omogoča direktna plačila preko spleta brez posredovanja finančne ustanove:

*"Trgovanje na spletu se skoraj popolnoma zanaša na finančne ustanove, ki delujejo kot zaupanje vredne tretje osebe za procesiranje elektronskih plačil. Popolnoma nepovratne transakcije niso možne, ker finančne institucije ne morejo preprečiti razreševanja sporov med udeleženci transakcij.*

*Cena reševanja sporov povečuje ceno transakcij in s tem omejuje minimalno praktično velikost transakcije. Manjka možnost opravljanja nepovratnih plačil za nepovratne storitve. Z možnostjo povrnitve transakcije se povečuje potreba po zaupanju.*

*Potreben je elektronski plačilni sistem, ki bazira na kriptografskem dokazovanju namesto na zaupanju in omogoča izvajanje transakcij med posamezniki ali ustanovami brez potrebe po mediaciji zaupanja vredne institucije."* [40]

Nekaj mesecev kasneje je izšla prva verzija plačilnega sistema Bitcoin.

## 3.3 Zgodovina

Pomembni dogodki od nastanka Bitcoina do danes:

- 31. 10. 2008 - Satoshi Nakamoto objavi prvi članek o Bitcoinu [40]

- 3. 1. 2009 - Nakamoto ustvari prvih 50 bitcoinov in zažene plačilno omrežje [13]
- 12. 1. 2009 - Hall Finney prejme 10 bitcoinov od Nakamota v prvi Bitcoin transakciji [13]
- 15. 8. 2010 - zaznana in izkoriščena je bila ranljivost protokola, v transakciji se generira preko 184 milijonov bitcoinov, v nekaj urah transakcijo zaznajo in izbrišejo, napaka na protokolu se odpravi; "edina večja varnostna napaka v zgodovini Bitcoina" [45]
- oktober 2012 - BitPay beleži preko 1000 trgovcev, ki sprejemajo Bitcoin kot plačilno sredstvo [30]
- februar 2013 - Coinbase beleži prodajo bitcoinov v vrednosti milijona ameriških dolarjev v enem mesecu [37]
- oktober 2013 - v Kanadi je postavljen prvi Bitcoin bankomat [39]
- november 2013 - kitajsko podjetje BTC China prevzame japonski Mt. Gox in evropski Bitstamp, postane največji trgovec z Bitcoinom (glede na promet) [41]
- 19. 11. 2013 - cena bitcoina se povzpne na 900 USD (Mt. Gox) po zasedanju ameriškega senata, kjer je Bitcoin predstavljen kot legitimna finančna storitev [2]
- 5. 12. 2013 - Kitajska banka prepove uporabo Bitcoina finančnim institucijam [34]
- februar 2014 - Mt. Gox, eden izmed največjih trgovcev z Bitcoinom, naznani bankrot [17]
- 26. 1. 2015 - Coinbase postane prvi reguliran trgovec z Bitcoinom v 25 ameriških zveznih državah [44]

## 3.4 Kdo je Satoshi Nakamoto?

Satoshi Nakamoto je oseba (ali skupina oseb), ki je razvila Bitcoin protokol in programsko opremo Bitcoin Core. [40] Ni znano ali gre za pravo ime ali psevdonim. Nakamoto je po izdaji Bitcoina nadaljeval z razvojem programske opreme in protokola skupaj z drugimi razvijalci do sredine leta 2010. Nato je predal repozitorij izvorne kode in domene, povezane z Bitcoinom, drugim članom Bitcoin skupnosti in prenehal s sodelovanjem na projektu. [29] Njegova identiteta do danes ni znana. Iz javne baze transakcij (tako imenovanega blockchaina) je razvidno, da Nakamotove znane Bitcoin denarnice vsebujejo okoli milijon Bitcoinov, ki so imele v začetku 2016 vrednost okoli 400 milijonov ameriških dolarjev. [36]

## 3.5 Zasnova sistema

Bitcoin je decentraliziran (brez centralnega administratorja) plačilni sistem, ki temelji na konceptu Proof-Of-Work. Gre za P2P omrežje, katerega uporabniki lahko med seboj direktno izvajajo plačila. Računalniki na omrežju preverjajo pravilnost izvedenih transakcij in jih beležijo v javno dostopno podatkovno bazo, imenovano block chain. Pri transakcijah sistem uporablja valuto, imenovano bitcoin (BTC) (bitcoin pisan z majhno začetnico se nanaša na valuto, z veliko na celoten sistem). Bitcoini nastajajo in so dodeljeni uporabnikom omrežja kot nagrada za procesiranje in beleženje transakcij v bazo - block chain. Postopek imenujejo "mining". Transakcije se v bazo dodajajo v blokih. Ko je potrjenih dovolj transakcij, se te zberejo v blok, ki se ga doda v bazo. Hkrati z nastankom bloka nastane vnaprej določeno število novih bitcoinov.

**Prednosti:**

- hitra in preprosta plačila
- plačevanje je možno kadarkoli, kjerkoli je dostop do spleta, brez birokratskih omejitev, praznikov, mej, ...

- nižji stroški transakcij: pri prejemanju provizij ni, pri pošiljanju po želji - provizija vpliva na hitrost potrditve transakcije

**Slabosti:**

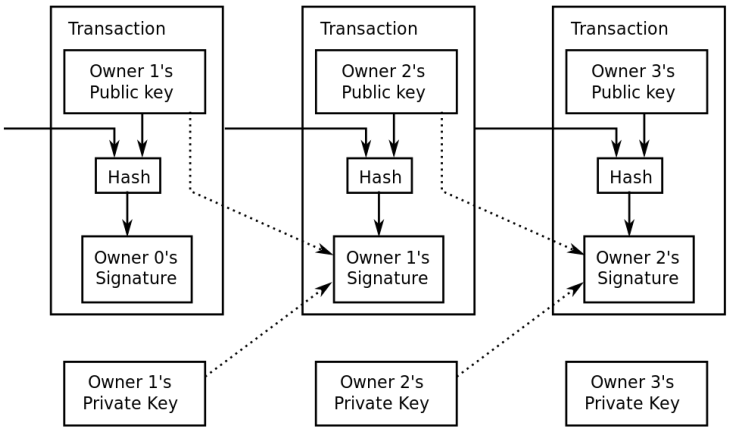
- nestabilnost valute: cena bitcoina stalno močno niha, zato ni primerna za hranjenje denarja
- stopnja sprejemanja: število podjetij, ki sprejema plačilo v Bitcoinih, je še vedno relativno majhno
- transakcije so nepovratne: vračilo sredstev je možno le v primeru, da jih je prejemnik pripravljen vrniti

### 3.5.1 Transakcije

Elektronska plačila se izvajajo v obliki transakcij med uporabniki omrežja. Uporabnika v transakcijah predstavlja Bitcoin naslov (Bitcoin address). Vsak uporabnik ima lahko poljubno število različnih naslovov. Naslov predstavlja par javnih in zasebnih kriptografskih ključev. Par ključev se uporablja za prenos lastništva bitcoinov med različnimi naslovi.

Transakcija vsebuje digitalno podpisan hash tistega bloka, kjer so bili bitcoini nazadje prenešeni, skupaj z javnim ključem prejemnika transakcije. Tako lahko bitcoinom sledimo preko transakcij do bloka, kjer so bili na novo ustvarjeni. Transakcija je potrjena, ko je vključena v blok v bazi. Pri transakciji ima pošiljatelj možnost vključiti provizijo. S strani pošiljatelja je provizija prostovoljna, vendar pa “Bitcoin minerju“ transakcije ni potrebno vključiti v na novo izračunan blok. Danes se številne transakcije obdelajo brez provizij, v prihodnosti pa naj bi provizije nadomestile novonastale bitcoine kot nagrado za ”minerje”. Provizija vpliva na vrstni red, po katerem se nepotrjene transakcije dodajajo v na novo izračunane bloke. Tako lahko uporabnik s provizijo zagotovi, da bo transakcija izvedena hitreje. Za povprečno transakcijo provizija znaša 0.0001 BTC ne glede na število poslanih bitcoinov. [23]

Kadar je izhod ene transakcije uporabljen kot vhod v drugo transakcijo, se mora vhod porabiti v celoti. V primeru, da je vrednost vhoda višja od zneska, ki ga uporabnik želi plačati, se generira dodaten Bitcoin naslov, na katerega se pošlje višek.




Slika 3.1: Povezave med transakcijami [24]

### 3.5.2 Veriga blokov

"Block chain" je javna porazdeljena podatkovna baza, na katero se zanaša plačilni sistem Bitcoin. Fizično je shranjena na računalnikih uporabnikov omrežja. Za delovanje Bitcoin denarnica potrebuje svojo lokalno kopijo ali vsaj del verige blokov. Vse potrjene transakcije od začetka delovanja omrežja so shranjene v verigi blokov. Integriteto in kronološki vrstni red transakcij v bazi sistem zagotavlja s pomočjo kriptografije. Za vzdrževanje in gradnjo baze skrbijo računalniki v omrežju, postopek pa je imenovan "mining" - rudarjenje. Bitcoin rudarji stalno oprezajo za novimi transakcijami in jih zbirajo v skupine, imenovane bloki. Blok vsebuje transakcije in informacijo, ki blok povezuje z prejšnjim blokom v bazi. Približno vsakih deset minut se nov blok doda v bazo.

| BLOCK #370124 | |
|---|---|
| Number Of Transactions | 1470 |
| Output Total | 8,260.18422886 BTC |
| Estimated Transaction Volume | 1,943.78255977 BTC |
| Transaction Fees | 0.31402517 BTC |
| Height | 370142 (Main Chain) |
| Timestamp | 2015-08-16 16:49:52 |
| Received Time | 2015-08-16 16:49:52 |
| Relayed By | F2Pool |
| Difficulty | 52,699,842,409.35 |
| Bits | 404020484 |
| Size | 878.826171875 KB |
| Version | 3 |
| Nonce | 762969971 |
| Block Reward | 25 BTC |

Slika 3.2: Primer bloka iz block chaina [4]

### 3.5.3 Rudarjenje

Bitcoin rudarjenje je postopek upravljanja verige blokov. Uporabnik omrežja lahko da na razpolago svoj procesorski čas za kreiranje novih blokov. Kot pogoj, da nastane nov blok in ga omrežje sprejme, mora ta vsebovati tako imenovani proof-of-work. V ta namen se podatkom pripne naključna vrednost - žeton. Žeton vstopi v zgoščevalno funkcijo skupaj s časovnim žigom, hashem prejšnjega bloka in korenom Merklovega drevesa vseh transakcij v bloku. Smisel pripenja žetona podatkom je, da se hash, ki ga funkcija vrne ob dodajanju različnih vrednosti nepredvidljivo spremeni. Ker Bitcoin zah-

teva hash posebne oblike (začeti se mora z določenim številom ničel), Bitcoin minerji iščejo ustrezen žeton s poskušanjem. Težavnost poskušanja se prilagaja z zahtevanim številom ničel v hashu. Ko član omrežja najde proof-of-work, ustvari nov blok. Vanj vključi izračunan hash, vse nepotrjene transakcije, ki jih hrani lokalno in dodatna polja. Novo ustvarjen blok doda v block-chain in spremembo posreduje po omrežju. Težavnost izračuna (kako računsko zahtevno je najti hash pod določeno vrednostjo) je določeno kot globalna spremenljivka v Bitcoin omrežju. Vsakih 2016 izračunanih blokov se težavnost prilagodi, glede na hitrost izračuna preteklih blokov. [8] Omrežje cilja na vrednost, ki omogoča izračun novega bloka približno vsakih 10 minut. Kot nagrado za novonastali blok uporabnik, ki ga je izračunal, prejme nagrado v obliki novonastalih bitcoinov in morebitnih provizij, ki so jih plačali pošiljatelji. V času pisanja z vsakim blokom nastane 25 bitcoinov. Število novonastalih bitcoinov se približno vsaka 4 leta razpolovi, dokler ne bo v obtoku 21 milijonov bitcoinov.

| Hashes | |
|---|---|
| Hash | 00000000000000000130a1683f9deda4ae46cd88545ad9ca74f2f4f42f59d0300 |
| Previous Block | 00000000000000002c551476cf97fe40d5b0251b1e4eea295bafcce5fb3cd30 |
| Next Block | 00000000000000000b3de5a1623e531fd54fec1f0f7c1625a1cd1b4ddef96238 |
| Merkle Root | bc7d40acd5d5be416e902dd12f2ac1063cd5df78b60fdc6a8eac2479518abed9 |

Slika 3.3: Pripadajoči hashi bloka # 370142 [4]

### 3.5.4 Bitcoin denarnice

Bitcoin denarnica hrani podatke o lastništvu bitcoinov, potrebne za izvajanje transakcij. Lastništvo bitcoinov pomeni, da uporabnik razpolaga z bitcoini na določenem naslovu. Vsako transakcijo mora pošiljatelj digitalno podpisati z ustreznim zasebnim ključem. V osnovi je Bitcoin denarnica zbirka uporabljenih ključev.

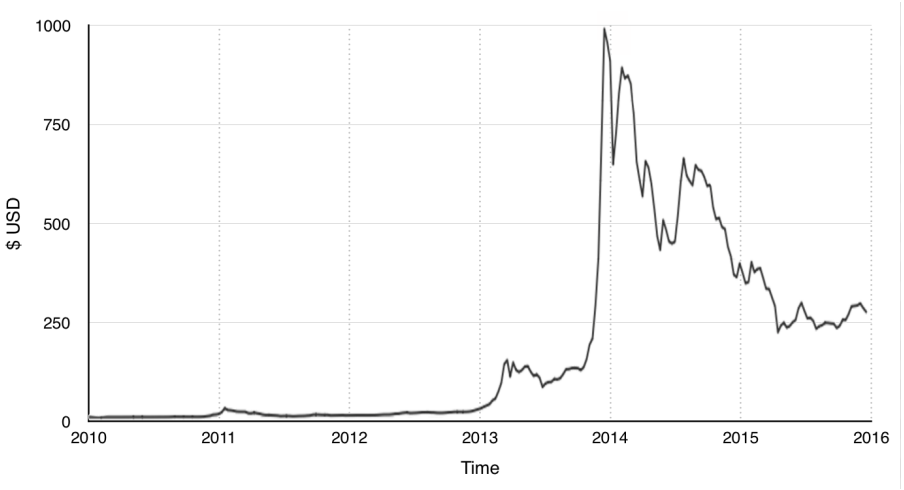
Obstajo različne vrste denarnic. Programske denarnice se poleg hranjenja

ključev priklopijo na omrežje in omogočajo izvajanje transakcij. Denarnice v obliki strojne opreme omogočajo izvajanje transakcij, če jih priklopimo na računalnik, in varnejše hranjenje ključev, brez povezave s spletom, ko jih odklopimo. Spletne denarnice so podobne, le da ključe hrani ponudnik namesto uporabnika in so ponavadi enostavnejše za uporabo. Obstajo tudi fizične denarnice, katerih namen je še večja varnost. Ključe hranijo zapisane na predmetu, kot naprimer fizični kovanec ali papir.

## 3.6 Ekonomsko stališče

Ekonomisti opisujejo denar kot sredstvo za hranjenje vrednosti, obračunsko enoto in medij za menjavo. Čeprav Bitcoin na nek način zadošča vsem trem kriterijem, ga finančne institucije še vedno ne sprejmejo kot zakonito valuto. Pogosto ga opisujejo kot kriptovaluto, virtualno valuto ali digitalni denar. Težavo predstavlja visoka volatilnost - hitro, vsakodnevno nihanje cene bitcoina. Volatilnost omejuje uporabnost Bitcoina kot zanesljivo sredstvo za hranjenje vrednosti in obračunsko enoto. Trgovci, ki sprejemajo bitcoine, za računovodstvo uporabljajo drugo valuto. [47]

Trgovanje z bitcoini je možno ali na spletnih izmenjavah, ki omogočajo nakup in prodajo, ali direktno med dvema posameznikoma. Enota, ki jo uporablja Bitcoin sistem, se imenuje bitcoin. Kot oznako se uporablja BTC ali XBT. Manjši zneski, ki se alternativno uporabljajo kot enote, so milibitcoin (0.001 BTC), mikrobitcoin (0.000 001 BTC) in satoshi (0.000 000 001 BTC).




Slika 3.4: Gibanje cene BTC/USD [3]

## 3.7 Povezava s kriminalom

V medijih se Bitcoin stalno pojavlja v povezavi z različnimi kriminalnimi dejavnostmi. Največ pozornosti je pritegnila spletna stran Silk Road. Spletni črni trg, ki je bil znan predvsem po prodaji ilegalnih drog, je obratoval od februarja 2011, dokler ga ni ameriški FBI zrušil na začetku oktobra 2013. Spletna stran, ki je letno zabeležila transakcije v vrednosti okoli 15 milijonov ameriških dolarjev, je trgovala z bitcoini. Ocenjujejo, da je bilo v času delovanja spletne strani 5-9% vseh bitcoin transakcij povezanih s Silk Roadom. [31] Tik po zaprtju Silk Roada je cena bitcoina padla za 25%. [47]

V kratki bicoinovi zgodovini je bila popularna tudi kraja. Če napadalec pridobi zasebni ključ za dostop do žrtvinega Bitcoin naslova, lahko bitcoine s tega naslova prenese drugam in čeprav bitcoinom lahko sledimo po naslovih, nadaljnih transakcij ni možno blokirati ali jih vrniti prvotnemu lastniku. Bitcoin se omenja tudi v povezavi s pranjem denarja, različnimi Ponzijevimi sistemi in nezakonitim Bitcoin miningom s pomočjo botnetov. V času pisanja na nizozemskem iščejo "Bitcoin bomberja", ki zahteva odkupnino v bitcoinih, da preneha z bombnimi napadi in grožnjami. [21]

## 3.8 Celoten potek transakcije

Branko je spletni trgovec, ki se je odločil, da bo kot plačilo sprejemal Bitcoin. Alenka je kupec, ki želi kupovati pri Branku.

Branko in Alenka imata oba na svojih računalnkih nameščene Bitcoin denarnice. Denarnice omogočajo kreiranje različnih Bitcoin naslovov. Naslov je niz znakov, kot naprimer "1Ebb8NfVmKMoGuMJCAEbVMv2dX8GnzgxSa". Vsak naslov ima svoje stanje bitcoinov.

Brako s pomočjo denarnice ustvari nov naslov in ga sporoči Alenki. Ko je Branko ustvaril naslov, je v resnici generiral nov kriptografski par ključev, javnega in zasebnega. Če transakcijo podpiše z zasebnim ključem, ki ga pozna samo on, lahko drugi potrdijo veljavnost transakcije z javnim ključem, ki je poznan vsem. Brankov nov naslov predstavlja unikatni javni ključ. Pripadajoči zasebni ključ pa hrani Brankova denarnica.

Alenka naroči svojemu Bitcoin odjemalcu, da bi rada prenesla znesek nakupa na Brankov naslov. Alenkina denarnica hrani zasebne ključe za vse njene naslove. Bitcoin odjemalec podpiše transakcijo z zasebnim ključem naslova, s katerega Alenka pošilja. Vsakdo v omrežju lahko potrdi, da bitcoine res pošilja lastnik naslova, s pomočjo ustreznega javnega ključa.

Gregor, Gašper in Gorazd so Bitcoin minerji. Njihovi računalniki stalno zbirajo nove transakcije in jih združujejo v bloke. Njihovi računalniki v ta namen računajo kriptografske zgoščevalne funkcije. Kriptografske zgoščevalne funkcije pretvorijo vhodne podatke v alfanumerični niz znakov fiksne dolžine imenovan hash. Že majhne spremembe v vhodnih podatkih vrnejo zelo različen hash. Tako je skoraj nemogoče ugotoviti, kateri vhodni podatki vrnejo specifičen hash. Da je možno iz enakih podatkov dobiti različne hashe, Bitcoin uporablja tako imenovani "nonce". Gre za naključno številsko vrednost, ki se pripne vhodnim podatkom. Sprememba številke drastično spremeni vrnjeni hash. Vsak blok vsebuje hash, ki nosi informacijo o preteklih transakcijah. Računalniki minerjev računajo hashe iz kombinacije hasha prejšnjega bloka, hasha novih transakcij in "nonce"vrednosti. Računanje hasha je računsko trivialno, vendar pa Bitcoin sistem zahteva, da ima hash po-

sebno obliko. Konkretno, hash vrednost se mora začeti z določenim številom ničel. V ta namen iščejo "nonce", ki bo vrnil hash ustrezne oblike. Ker ni načina, da bi predvideli katera vrednost bo vrnila pravi hash, so prisiljeni generirati hashe z različnimi "nonce" vrednostmi, dokler ne najdejo ustrezne. Vsak blok vsebuje posebno transakcijo, ki dodeli nove bitcoine minerju, ki je uspel izračunati hash. Če torej izračun uspe Gašperju, je v njegovi denarnici ustvarjen nov naslov, ki hrani novonastale bitcoine.

S časom se za blok, v katerem je Alenkina transakcija, dodajajo novi bloki. Če bi kdo želel spremeniti vsebino tega bloka, bi moral na novo izračunati vrednost, ki jo je izračunal Gašper in posledično izračunati vse bloke, ki so bili dodani od takrat. Ker je iskanje "nonce"vrednosti računsko zahtevno in se stalno dodajo novi bloki, so takšne spremembe skoraj nemogoče. [42]

# Poglavje 4

# Anonimnost

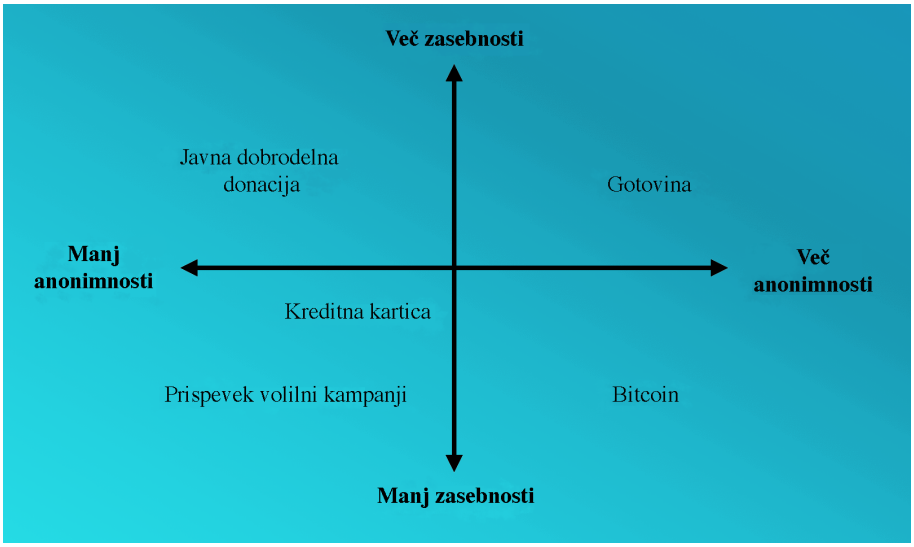
## 4.1 Anonimnost/zasebnost

V kontekstu finančnih transakcij lahko ločujemo med anonimnostjo in zasebnostjo. Transakcijo imenujemo anonimno, če nihče (razen udeležencev) ne ve, kdo v transakciji sodeluje. Transakcijo imenujemo zasebno, če nihče ne ve, kaj je bilo kupljeno in za kakšen znesek. [38] Gotovina ali menjava blaga je primer zasebnega in anonimnega načina plačevanja. "Transakcija"ni nikjer zabeležena, le udeleženca poznata podrobnosti nakupa. Nasprotno kreditna kartica ni ne anonimna ne zasebna. Ponudnik kartice razpolaga z vsemi podatki o plačevanju. Pri dobrodelnih donacijah se lahko razkrije ime donorja, ne pa nujno tudi donirani znesek. Takšna transakcija je zasebna, ni pa anonimna. Bitcoin pa je znotraj svojega sistema popolnoma anonimen, ni pa zaseben.

## 4.2 Je Bitcoin anonimen?

Bitcoin je pogosto opisan kot način za anonimno izvajanje transakcij, ker omogoča pošiljanje in prejemanje bitcoinov brez razkrivanja osebnih podatkov. [38], [1] V resnici pa je za prikrivanje identitete potrebno vložiti precej truda. Med tehničnimi uporabliki Bitcoina vlada prepričanje, da anonimnost

ni eden glavnih razvojnih ciljev sistema. [43] Bitcoinove transakcije so javno in trajno shranjene v omrežju. Sistem za izvajanje transakcij uporablja psevdonime - Bitcoin naslove. Če se psevdonim poveže z osebnimi podatki uporabnika, je možno z uporabnikom povezati vse izvedene transakcije. Blockchain, baza v kateri so zavedene vse transakcije, je javno dostopna. Vsakdo lahko dostopa do podatkov o transakcijah in stanju bitcoinov za posamezen naslov. Uporabnik je zato anonimen le, dokler ga ni možno povezati z naslovom, ki ga uporablja. Številni uporabniki že prvi nakup bitcoinov opravijo preko popularnih spletnih izmenjav, ki zahtevajo registracijo uporabnika. Na takšen način že pri vstopu v trgovanje z Bitcoinom povežejo svoj naslov z osebnimi podatki. Uporabnik, ki želi ostati anonimen, mora bitcoine pridobiti na drugačen način. Dve možnosti sta privatna transakcija ali nagrada za mining.




Slika 4.1: Anonimnost/zasebnost različnih načinov plačevanja

## 4.3 Najpogostejši načini izgube anonimnosti

- objava svojega imena in Bitcoin naslova na spletu; samoumevno, vendar se pogosto dogaja zaradi želje po donacijah, npr. osebni blog s pravim imenom in naslovom ali podpis v forumih s pravim imenom, vsakdo na spletu lahko spremlja stanje in transakcije objavljenega naslova

- trgovanje z bitcoini na spletnih izmenjavah; izmenjave, ki omogočajo trgovanje z uradnimi valutami morajo v skladu z zakonodajo od uporabnikov zahtevati registracijo, ponavadi s kopijami osebnih dokumentov, spletna izmenjava hrani podatke o vseh uporabljenih naslovih

- kupovanje z bitcoini; včasih je ob nakupu težko prikriti identiteto, potrebno je navesti svoje ime ali naslov za pošiljanje, trgovec posledično pridobi povezavo bitcoin naslova z identiteto

- spletne denarnice ali "lahke"denarnice, ki ne hranijo blockchaina lokalno; lahke denarnice nimajo svoje kopije blockchaina, zato opravljajo poizvedbe na strežnik, kjer se baza nahaja, poizvedbe razkrijejo naslove, ki pripadajo denarnici in IP naslov administratorju strežnika, prav tako spletne denarnice v celoti obstajajo na strežniku in so ponavadi povezane s telefonsko številko ali e-mail naslovom

- uporaba Bitcoina brez VPN-ja ali TOR-a; bitcoin nima vgrajene enkripcije pri oddajanju transakcij v omrežje, internetni ponudnik lahko promet prestreže in ugotovi katere transakcije pripadajo IP naslovu, za skrivanje IP naslova je potrebna uporaba dodatne programske opreme npr. TOR-a ali VPN omrežja, alternativa je uporaba javnega WiFi omrežja [22]

## 4.4 Ohranjanje anonimnosti

Za izboljšanje anonimnosti sistema je Nakamoto že v originalnem članku, kjer je prvič predstavil Bitcoin, predlagal, da se za vsako transakcijo uporabi nov naslov. [40] Prejemnik torej vsakič, ko želi prejeti plačilo, generira nov naslov in ga sporoči plačniku. Na tak način bi preprečili, da se različne transakcije povežejo z istim lastnikom. Še vedno pa so problematične transakcije z večimi vhodi, ki črpajo bitcoine iz večih naslovov. Čeprav uporabnik prejema plačila na različne naslove, v trenutko, ko izvede transakcijo, ki črpa bitcoine z večih uporabljenih naslovov, izda, da vsi uporabljeni naslovi pripadajo isti denarnici, torej skupnemu lastniku.

## 4.5 Mešalni servisi (Mixing service)

“Umazane“ bitcoine, takšne, ki niso več anonimni in jih je možno povezati z lastnikom, je možno spet ”očistiti”. Ponudniki Bitcoin mešalnih servisiv v zameno za provizijo ponujajo menjavo umazanih bitcoinov za druge - ponavadi bitcoine drugih uporabnikov storitve in na tak način prekinejo povezavo v verigi transakcij. Storitev deluje na način, da vzdržuje bazen - večjo vsoto bitcoinov, pridobljeno od uporabnikov storitve. Uporabnik ustvari račun na njihovi spletni strani in prenese bitcoine, ki jih želi očistiti, na njihov naslov. V zameno prejme bitcoine iz bazena ponudnika na novo generiran naslov. Čez čas ponudnik bitcoine, ki jih je uporabnik prvotno prenesel, doda v bazen. Za še boljšo anonimnost je možno počakati nekaj časa, preden se prevzamejo novi bitcoini in jih razbiti na manjše in različno velike vsote ter jih prenesti na različne naslove. Težavo pri storitvah te vrste predstavlja zaupanje, saj mora uporabnik poslati bitcoine brez zagotovila, da jih bo dobil nazaj. Uspešnost storitve je odvisna od količine bitcoinov, ki jih uporabnik želi očistiti in prometa, ki ga ima storitev. Manjši, kot je promet in večja kot je vsota za čiščenje, večja je verjetnost, da uporabnik dobi vrnjene sam svoje bitcoine. Mešanje večjih vsot denarja na takšen način je seveda sporno, ker omogoča pranje denarja. [27]

# Poglavje 5

# Varnost - Napadi

## 5.1 Ranljivosti

BitcoinWiki razvršča ranljivosti Bitcoin omrežja na tri kategorije, glede na nevarnost, ki jo po njihovem mnenju predstavljajo. [25]

**Neproblematično:**

- premajhno število bitcoinov: trenutno je v obtoku 15 milijonov bitcoinov (število se še povečuje do planiranih 21), transakcije pa operirajo z natančnostjo osmih decimalk, v primeru da število enot za plačevanje ne bi zadostovalo, povečanje natančnosti ne bi predstavljalo problema

- generiranje ogromnega števila naslovov: število naslovov ne vpliva na delovanje omrežja, kolizije so malo verjetne, saj so naslovi 160 bitni, kar predstavja dovolj različnih naslovov, da ima vsak zemljan na voljo 2.15*10^38 različnih naslovov

- generiranje veljavnih blokov z nižjo težavnostjo: napadalec se lahko popolnoma loči od ostalega omrežja in generira svojo vejo blokov z nižjo težavnostjo kot ostalo omrežje, bloki bi bili za njega popolnoma veljavni, a bi bili uničeni ob združitvi s celotnim omrežjem, omrežje za

veljavno vejo vedno vzame tisto, ki predstavlja večjo skupno računsko zahtevnost

**Verjetno neproblematično:**

- zlom kriptografije: SHA-256 se danes smatra za zanesljivo kriptografsko funkcijo, po potrebi ne bi bilo težko preiti na drug algoritem

- segmentacija omrežja: sistem deluje tudi z minimalno povezavo med dvema deloma segmentiranega omrežja, ob združitvi popolnoma ločenih delov prevlada daljši blockchain, transakcije krajšega so še vedno veljavne, izgubijo le število potrditev

- napadalec ima veliko računsko moč: napadalec, ki nadzira več kot polovico računske moči omrežja, ima nadzor nad tem, katere transakcije bodo vključene v blockchain, lahko transakcijam prepreči potrditve, ostalim uporabnikom preprečuje generiranje veljavnih blokov, poljubno razveljavlja svoje transakcije, ne more pa razveljaviti drugih transakcij, preprečiti pošiljanje transakcij, operirati z bitcoini, ki mu ne pripadajo. Zaradi omejenega nadzora nad omrežjem, ki ga napad omogoča in velike računske moči, ki je potrebna, se zdi napad malo verjeten. Napad je možno izvesti z manjšim odstotkom računske moči, vendar uspešnost napada z znižanjem odstotka drastično pada.

- "spamming transakcij": pošiljanje transakcij sam sebi večkrat zaporedoma je enostavno, in lahko preprečuje vključevanje v bloke ostalim transakcijam. Takšen napad bi bil za napadlaca drag, saj je prioriteta vključevanja odvisna od provizije pri posamezni transakciji. Prav tako prioriteta narašča s starostjo nepotrjene transakcije. Napadalcu slej kot prej zmanjka denarja.

- Finney napad: različica dvakratne porabe, ki zahteva sodelovanje Bitcoin minerja. Podrobneje opisana v nadaljevanju.

**Mogoče problematično:**

- kraja denarnice: Bitcoin denarnice se privzeto hranijo nešifrirane, zato so zanimiva tarča za krajo, novejše izdaje omogočajo enkripcijo
- sledenje zgodovini bitcoinov: bitcoinom je možno slediti po blockchainu in naslove povezati z identiteto uporabnika
- Sybil napad: napadalec lahko zapolni omrežje z odjemalci pod njegovim nadzorom, posledično lahko izolira poštenega odjemalca od ostalega omrežja, kar olajša nekatere druge napade
- Denial of service napad: pošiljanje velike količine podatkov odjemalcu lahko prepreči procesiranje transakcij, nekaj mehanizmov za preprečevanje je vgrajenih, a napredni napadi verjetno vseeno predstavljajo nevarnost
- nelegalna vsebina v block chainu: v transakcije je možno vključiti poljubne podatke, polni odjemalci (rudarji) pa imajo lokalno kopijo blockchaina, kar lahko povzroči probleme z zakonodajo

## 5.2 Dvakratna poraba

"Double spending" je zmožnost večkratne porabe digitalnega denarja. V nasprotju s fizičnim denarjem je možno elektronske datoteke, ki predstavljajo elektronski denar, podvajati. Ker transakcija ne izbriše podatkov o denarju na strani plačnika, so za preprečevanje dvakratne porabe potrebni dodatni mehanizmi. Klasični elektronski plačilni sistemi se zato zanašajo na tretjo osebo - centralno avtoriteto, kateri zaupajo in katera potrjuje ali zavrača transakcije. Bitcoin se proti double spendingu ščiti s pomočjo block chaina, kjer se vodi evidenca zgodovine transakcij.

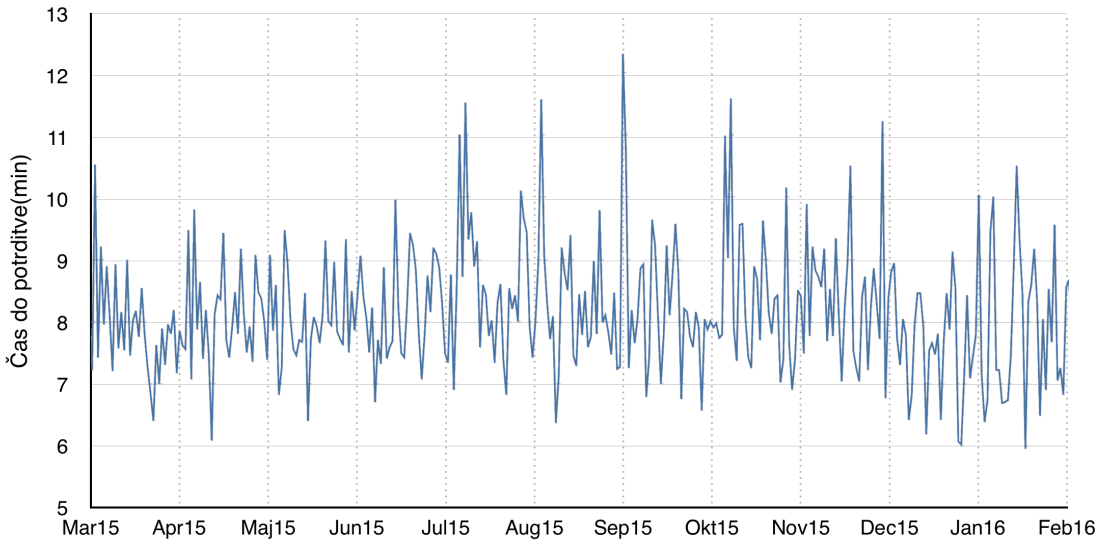
Ko je transakcija vključena v nov blok blockchaina, je potrjena. Število potrditev v kontekstu Bitcoina predstavlja število blokov, ki so bili dodani od vključno bloka, ki vsebuje transakcijo. Če je neka transakcija dodana v nov blok, za tem blokom pa sta se dodala še dva nova bloka, ima ta transakcija 3

potrditve. Ko je transakcija enkrat potrjena, nevarnosti za double spending ni več. Blockchain ne bo sprejel transakcije z vhodi, ki so bili že zapravljeni.

Bitcoin protokol je proti double spendingu torej dobro zaščiten. Tudi BitcoinWiki omenja varianto double spendinga le v kategoriji ranljivosti "Probably not a problem". Kljub temu pa je stanje drugačno pri tako imenovanih hitrih plačilih.

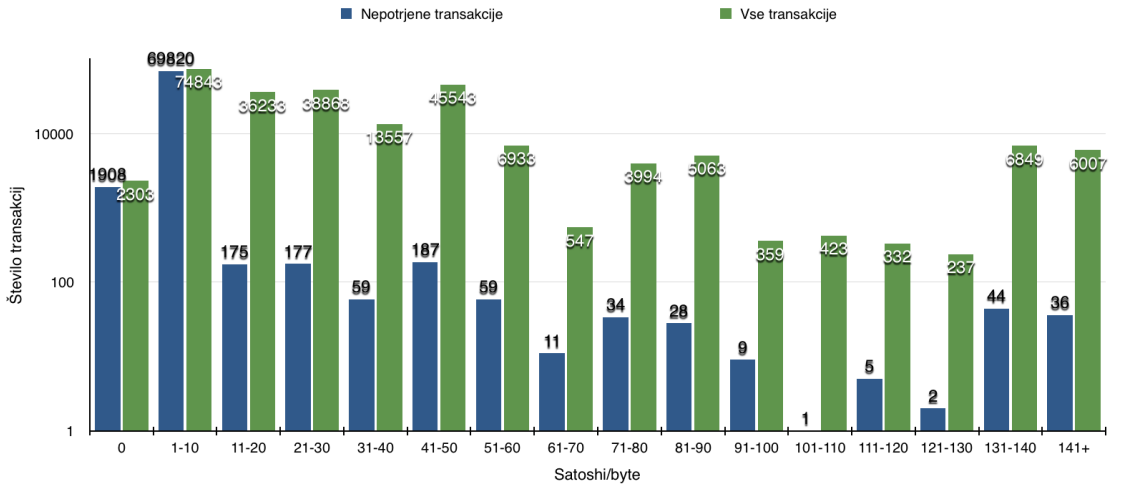
### 5.2.1 Hitra plačila in Bitcoin

Kot hitra plačila označujemo plačevanje pri storitvah, pri katerih se izmenjava plačila in blaga zgodi v časovnem razmiku nekaj minut. Primer predstavljajo nakup v supermarketu, drive-in restavracije, avtomati ali kava/napitki za s seboj. Če ponudniki takšnih storitev želijo uporabljati Bitcoin kot plačilno sredstvo, se ne morejo zanašati na potrjevanje transakcij, ker je čas potreben za potrditev, predolg.




Slika 5.1: Čas, potreben za prvo potrditev transakcije v zadnjem letu, velja le za transakcije s provizijo. [5]

Iz slike 5.1 je razvidno, da večina transakcij potrebuje 7-10 minut za prvo potrditev. Ker Bitcoin omrežje stalno prilagaja težavnost generiranja novih blokov in ohranja čas med sosednjima najdenima blokoma pri približno desetih minutah, se ta čas tudi v prihodnje ne bo bistveno spremenil. Graf velja le za transakcije, ki vključujejo provizije. Za transakcije brez provizij je čas do prve potrditve še daljši, saj imajo nižjo prioriteto pri vključevanju v naslednji najden blok.




| Delay \ Fee | 0 | 1-10 | 11-20 | 21-30 | 31-40 | 41-50 | 51-60 | 61-70 | 71-80 | 81-90 | 91-100 | 101-110 | 111-120 | 121-130 | 131-140 | 141+ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Blocks | 8-inf | 0-6 | 0-1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Time (min) | 60-inf | 0-80 | 0-30 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 | 0-25 |

Slika 5.2: Vpliv provizije na čas, potreben za potrditev transakcije. Graf kaže primerjavo med vsemi transakcijami zadnjih 24 ur in še nepotrjenimi transakcijami, v tabeli je prikazan povprečni zamik do prve potrditve. [6]

V posamezni vrstici slike 5.2 zgornji stolpec prikazuje število nepotrjenih transakcij v nekem trenutku, spodnji pa število potrjenih v zadnjih 24-ih urah. Transakcije s provizijo, nižjo od 10 satoshijev na bajt transakcije, potrebujejo občutno daljši čas za potrditev kot ostale. Najcenejša provizija, ki zagotavlja hitro potrditev transakcije, je v trenutku nastanka grafa 11-20 satoshijev na bajt transakcije.

Ker stranke po plačilu seveda ne želijo čakati še dodatnih 10 minut na potrditev, so se trgovci, ki sprejemajo Bitcoin kot plačilno sredstvo, prisiljeni zanašati na transakcije brez potrditev. Če trgovec sprejema transakcije brez potrditev (o transakciji je obveščen takoj, ko je ta poslana, prikaže se kot "0/unconfirmed"), je izpostavljen dvakratnemu zapravljanju.

## 5.3 Vrste napadov z dvakratno porabo

V času, dokler transakcija ni sprejeta v blockchain, lahko zlonamerna stranka bitcoine, zapravljene v prvotni transakciji, porabi še enkrat. Iste bitcoine uporabi kot vhod v drugo transakcijo. Če je kasneje v blockchain sprejeta druga transakcija namesto prve, je plačilo trgovcu zavrnjeno.

### 5.3.1 Tekmovalni napad (Race attack)

Predpostavljamo, da ima napadalec napravo, na kateri teče Bitcoin odjemalec in trgovec sprejema nepotrjene Bitcoin transakcije kot plačilo. Napadalec želi od trgovca pridobiti storitev, brez da bi za njo plačal. Poskušal bo bitcoine ki jih je poslal kot plačilo trgovcu, zapraviti še enkrat. Uporabil jih bo kot vhod v transakcijo, ki jo bo poslal sam sebi. Napadalec nadzoruje le nekaj odjemalcev v omrežju, vsi ostali so pošteni. Računska moč napadalca ne presega računske moči ostalega omrežja, zato napadalec ne more vstavljati nepravilnih blokov. Napadalec prav tako ne sodeluje v procesu iskanja novih blokov (rudarjenju). Ko je transakcija potrjena v blok, je napadalec ne more več spreminjati. Napadalec nima dostopa do naprave ali zasebnih kriptografskih ključev trgovca, pozna pa njegov IP naslov. Bitcoin naslovi, ki jih bo uporabil napadalec, ne zadoščajo za njegovo identifikacijo. Čeprav bo zlonamerno obnašanje napadalca v prihodnosti (po tem ko je že pridobil storitev) zaznano, njegova identiteta ne bo razkrita.

Napadalec torej izda dve transakciji z istima vhodoma. Ena predstavlja plačilo trgovcu, druga le pošlje bitcoine na drug naslov pod njegovim nadzorom. Da napad uspe, se morata izpolniti dva pogoja.

1: Trgovčev odjemalec mora najprej sprejeti pravilno transakcijo (plačilo trgovcu), drugače z njegove strani izgleda, kot da plačilo ni bilo izvedeno.

2: Druga transakcija (plačilo samemu sebi) mora biti sprejeta v naslednji blok.

Če sta transakciji poslani v omrežje hitro ena za drugo, imata podobni verjetnosti, da sta sprejeti v naslednji blok. Odjemalci transakcije neprestano periodično oddajajo v omrežje. Bitcoin odjemalci ne bodo sprejeli transakcije z istimi vhodi, kot jih že ima druga transakcija v njihovem pomnilniku. Prvemu pogoju lahko napadalec zadosti tako, da se napadalec priklopi na trgovčevega odjemalca kot direktni sosed. Bitcoin protokol sprejema vhodne povezave, če število povezav ne presega določene meje. Če napadalec pošlje prvo transakcijo kot direktni sosed trgovca, drugo pa kmalu za tem z drugega odjemalca, ki ni direktni sosed, bo trgovec zagotovo najprej prejel prvo transakcijo. Med drugo transakcijo in trgovcem je vsaj en skok v omrežju več kot pa med trgovcem in prvo. Drugemu pogoju je težje zadostiti. Ker sta transakciji poslani z različnih lokacij v omrežju, se po omrežju širita različno hitro. Večje število odjemalcev, ki prejme zlonamerno transakcijo, pomeni večjo verjetnost, da bo ta vključena v blok - večjo verjetnost za uspeh napada. Transakciji tekmujeta (tekmovalni napad) med seboj, ko se širita po omrežju. Na uspeh napada vpliva časovni zamik med transakcijama, povezanost trgovca in napadalca (več povezav - hitrejše širjenje) in topologija omrežja. [33]

### 5.3.2 Finney napad

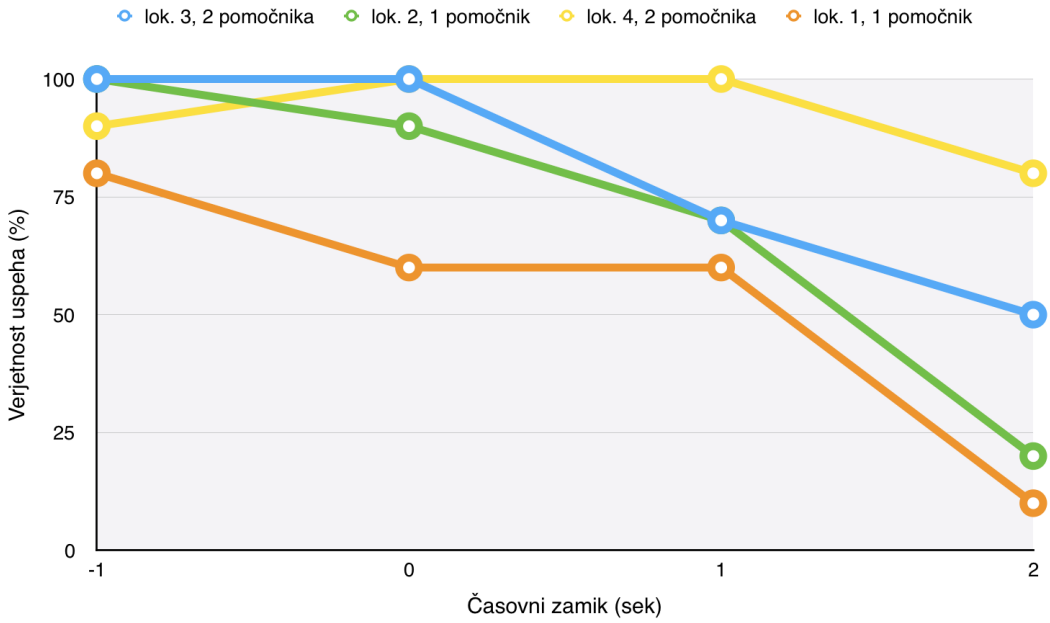
Napad je poimenovan po Hallu Finneyu (prvi prejemnik Bitcoin transakcije), ki je prvi opozoril nanj. Gre za vrsto dvakratne porabe, ki zahteva sodelovanje pri iskanju novih blokov. Napadalec poskuša izračunati nov blok. V blok, ki ga išče, doda transakcijo, v kateri pošilja vsoto bitcoin na svoj naslov. Ko najde nov blok, ga ne pošlje takoj naprej v omrežje. Najprej iste bitcoine uporabi za nakup storitve pri nekem trgovcu, ki sprejema hitra plačila. Ko

je pridobil storitev, izračunan blok odda v omrežje in transakcija za nakup pri trgovcu je v naslednjem bloku zavrnjena. Napad ne uspe, če v času od izračuna novega bloka do pridobitve storitve trgovca preostalo omrežje najde naslednji blok. V tem primeru napadalec izgubi v transakciji zapravljene bitcoine in nagrado za najden blok. Zaradi težavnosti iskanja novih blokov so priložnosti za izvedbo napada redke. Prav tako ni možno napovedati, kdaj bo naslednji blok najden, kar dodatno otežuje izvedbo napada. Ob visoki vrednosti bitcoina je nagrada 25 bitcoinov za najden blok dovolj velika, da je napadalec ne želi tvegati. [26]

Obstaja še nekaj drugih vrst napadov z dvakratno porabo. Napad z grobo silo (Brute force) in večinski (Majority) napad se zanašata na veliko računsko moč. Če napadalec generira bloke hitreje, kot preostalo omrežje, lahko gradi svojo vejo blockchaina in ob združitvi krajšo vejo razveljavi. Večinski napad je pravzaprav napad z grobo silo z računsko močjo, večjo od polovice moči celotnega omrežja. Večinski napad je vedno uspešen, z manjšanjem deleža računske moči pa uspešnost hitro pada. Te dve vrsti napadov sta v praksi težko izvedljivi zaradi ogromne računske moči, ki bi bila potrebna. Še ena vrsta je "vector76" napad, ki je kombinacija tekmovalnega in Finney napada. Omogoča ponovno zapravljanje bitcoinov iz transakcije, ki že ima eno potrditev. Slabost je, da napadalec v tem primeru vedno žrtvuje en izračunan blok. Pri vrednosti enega bitcoina 410 evrov (januar 2016), bi napadalec moral žrtvovati 410 * 25 = 10250 evrov. Več o ostalih napadih v [10]. V praksi se zato najlažje izvedljiv zdi tekmovalni napad.

### 5.3.3 Uspešnost tekmovalnega napada

Eksperimentalni rezultati, ki so jih dosegli Karame, Androulaki in Capkun leta 2012 [33], kažejo na veliko uspešnost tekmovalnih napadov dvakratne porabe:




| Lokacija, # Povezav trgovca | # Pomočnikov | Časovni zamik | Uspešnost |
|---|---|---|---|
| **Azija-Pacifik 1, 125** | 2 | 0 s | 100% |
| **Azija-Pacifik 1, 8** | 2 | 1 s | 100% |
| **Azija-Pacifik 2, 125** | 2 | 0 s | 100% |
| **Azija-Pacifik 2, 125** | 2 | 1 s | 100% |
| **Severna Amerika 1, 8** | 1 | 0 s | 100% |
| **Severna amerika 1, 40** | 1 | -1 s | 100% |

Slika 5.3: Graf: Uspešnost napada pri različnih časovnih zamikih med transakcijama, trgovec ima 125 povezav. Tabela: Zbrane so kombinacije lokacije trgovca, števila njegovih povezav, števila pomočnikov napadalca in časovnega zamika, pri katerem so dosegli 100% uspešnost napada. [33]

Vsaka točka v zgornjem grafu predstavlja 10 izvedenih napadov. Prikazani so rezultati za 4 trgovce na različnih lokacijah. Dve izmed lokacij sta se nahajali v Severni Ameriki, dve pa v azijsko-pacifiškem območju. Število pomočnikov predstavlja število odjemalcev pod napadalčevim nadzorom, ki širijo drugo transakcijo.

Rezultati kažejo, da napad z dvakratno porabo skoraj zagotovo uspe v primeru, da trgovec ne uporabi nobenih protiukrepov in napadalec pozna njegov IP naslov. Bitcoin je do začetka leta 2013 omogočal tudi transakcije z uporabo IP naslovov namesto Bitcoin naslovov. Z verzijo Bitcoin Core programske opreme 0.8.0 so podporo odstranili. Predpostavka o znanem IP naslovu izhaja iz tega.

V članku Have a Snack Pay with Bitcoins [28], je opisan podoben eksperiment, kjer pa trgovec uporabi več protiukrepov in napadalec ne pozna trgovčevega IP naslova. Uspešnost napada je bila v tem primeru nižja od 0,1%. V eksperimentu trgovec ni sprejemal vhodnih povezav do svojega odjemalca, prejetih transakcij ni posredoval naprej po omrežju, uporabil je časovni okvir v katerem je bil obveščen o morebitnih konfliktnih transakcijah in povezan je bil z velikim številom odjemalcev v omrežju. Povprečno je bil povezan s 1024 odjemalci. Med njimi je naključno izbral podmnožico, od katere je pridobil vhodne transakcije in jih preverjal za morebitne konflikte. Najprimernejši izmerjen časovni okvir je bil 6,29 sekund, in najprimernejša velikost podmnožice 37.

## 5.4 Simulacija napada

Izmed napadov z dvakratno porabo je najzanimivejši tekmovalni napad. V nasprotju s Finney ali vector76 napadom, tekmovalni napad ni odvisen od uspešnega rudarjenja. Priložnost za napad se zato ne pojavi le v trenutku izračunanega bloka. Napadalcu tudi ni potrebno tvegati relativno visoke nagrade, ki jo v vsakem primeru prejme ob izračunanemu bloku. Prav tako ne potrebuje posebne računske moči, kot bi jo potreboval pri napadu z grobo silo. Priložnost za izvedbo tekmovalnega napada je prisotna vedno, kadar ima napadalec dostop do trgovca, ki sprejema hitra plačila. Napadalec potrebuje le napravo, na kateri je nameščen Bitcoin odjemalec.

V nadaljevanju je prikazana praktična izvedba tekmovalnega napada z namenom ugotavljanja težavnosti izvedbe napada.

### 5.4.1 Uporabljene tehnologije - Bitcoin core

Bitcoin core je paket programske opreme, ki služi kot odjemalec za Bitcoin P2P omrežje. Vključuje programa bitcoind in bitcoin-qt. Bitcoind upravljamo s pomočjo ukazne vrstice. Teče v ozadju, kot demon, in čaka na ukaze. Bitcoin-qt pa ima grafični uporabniški vmesnik za isti namen. Bitcoin core temelji na originalni referenčni kodi Satoshija Nakamota. Služi kot Bitcoin denarnica in omogoča upravljanje z bitcoin naslovi in pošiljanje/prejemanje transakcij. Verzija programa, s katero je bila izvedena simulacija je BitcoinCore v0.11.2.0. Uporabljeni ukazi so podrobno opisani v Bitcoin Developer Reference (`https://bitcoin.org/en/developer-reference#bitcoin-core-apis`).

### 5.4.2 Izvedba

Simulacija je bila izvedena na virtualki z operacijskim sistemon Ubuntu 14.04, na kateri je bil nameščen Bitcoin Core. Bitcon Core omogoča regtest način delovanja, ki je namenjen razvoju in testiranju Bitcoin aplikacij. V regtest načinu delovanja se Bitcoin odjemalec ne poveže na P2P omrežje, ampak

sam lokalno vzdržuje svojo verzijo blockchaina, ki je na začetku prazna. V tem načinu je uporabniku na voljo dodaten ukaz - generate, s katerim lahko generira poljubno število novih blokov in jih doda v blockchain. Generate ukaz v generiran blok doda vse nepotrjene transakcije, ki se nahajajo v pomnilniku odjemalca in na naslov v uporabnikovi denarnici nakaže nagrado za najden blok. Nagrada v regtest načinu še vedno znaša 50 bitcoinov (na pravem omrežju je trenutno 25).

Za potrebe simulacije zaženemo štiri različne bitcoin odjemalce in jih povežemo med seboj. Na isti napravi lahko zaženemo poljubno število odjemalcev, vendar mora vsak teči v svojem direktoriju, kjer se nahaja datoteka z parametri za zagon in direktorij regtest, kamor se bo shranjevala podatkovna baza in datoteke, ki jih za delovanje potrebuje Bitcoin denarnica.


Slika 5.4: Direktorij, kjer so se nahajali odjemalci

Vsak izmed direktorijev vsebuje datoteko *bitcoin.conf*, v kateri so nastavitve za regtest način delovanja, vrata, na katerih bo odjemalec poslušal in nastavitve, ki omogočajo odjemalcu sprejemanje ukazov med delovanjem. Vse štiri datoteke so med seboj enake, le vsak izmed odjemalcev posluša na različnih vratih. *bitcoin.conf* trgovca:

```
# regtest
regtest=1
```

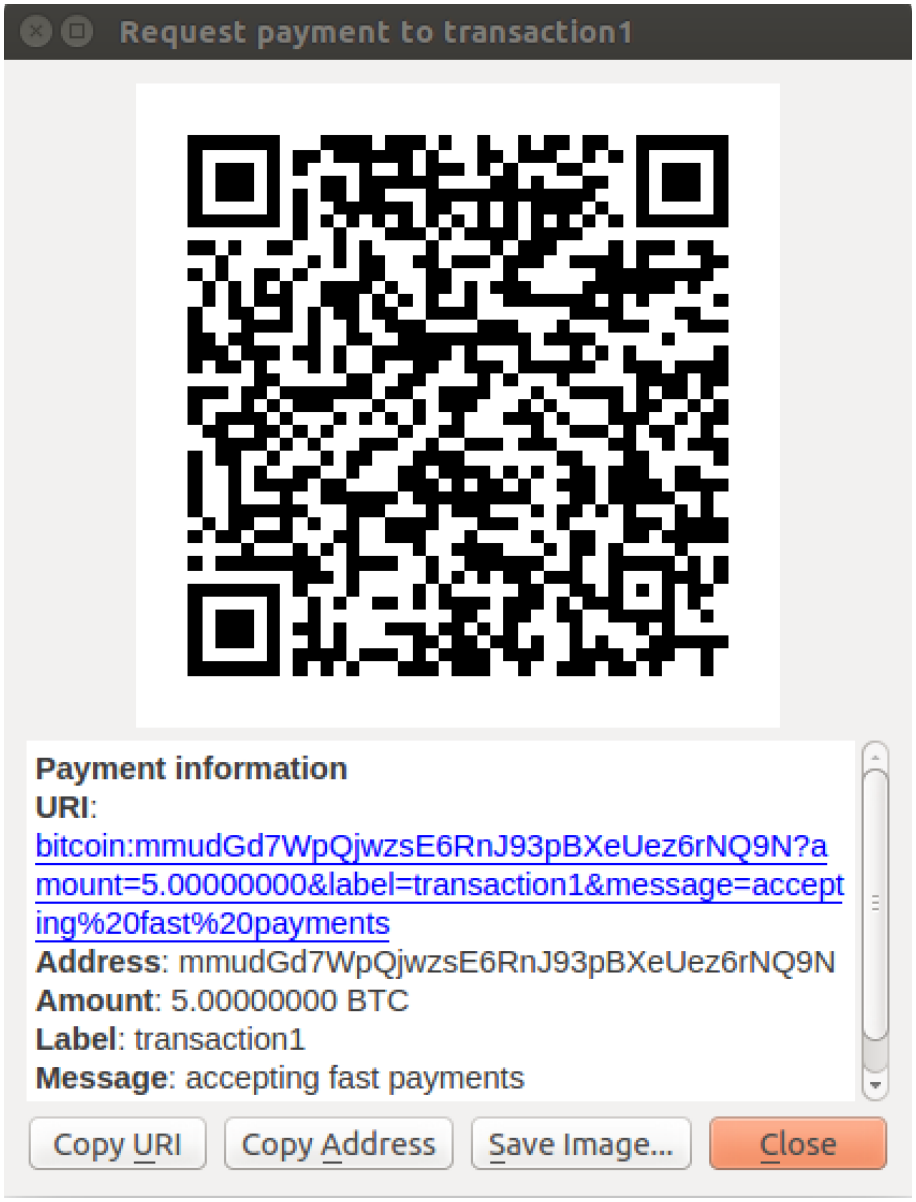
```
dnsseed=0
upnp=0
# listen on ports
port=19020
rpcport=19021

# accept RPC commands
#(for controlling a running Bitcoin process)

server=1
# rpc username and password must be set
rpcuser=admin3
rpcpassword=123
```

Naslednji ukazi v bash lupini zaženejo napadalca in trgovca. Pri napadalcu generiramo 101 blok blockchaina, kar nam da na razpolago 50 bitcoinov, ki jih prejmemo kot nagrado za prvi novonastali blok. Novi bitcoini "dozorijo" šele, ko so 100 blokov globoko v verigi blokov. Gre za zaščitni mehanizem, ki preprečuje zmedo v primeru, da bi se novonastali blok razveljavil, pripadajoči bitcoini pa bi že bili porabljeni v transakcijah. Napadalec, ki pozna IP naslov trgovca, se nanj direktno poveže. (V našem primeru se seveda vsi nahajajo lokalno, na različnih vratih)

```
pero@ubuntu:~/bitsim$ bitcoind -daemon
-datadir=attacker;

pero@ubuntu:~/bitsim$ bitcoind -daemon -datadir=vendor;

pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=attacker
 generate 101;
```

```
pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=attacker
  addnode 127.0.0.1:19020 add;
```

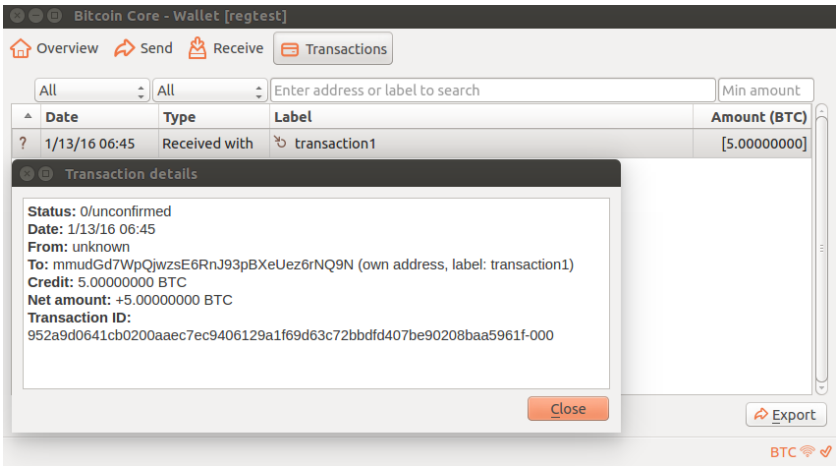
Trgovec ustvari nov Bitcoin naslov, na katerega želi prejeti plačilo in ga sporoči napadalcu. Napadalec nanj nakaže ustrezen znesek bitcoinov. Ker trgovec sprejema hitra plačila, odda blago takoj, ko mu odjemalec sporoči, da je transakcija prispela, čeprav še nima potrditev.



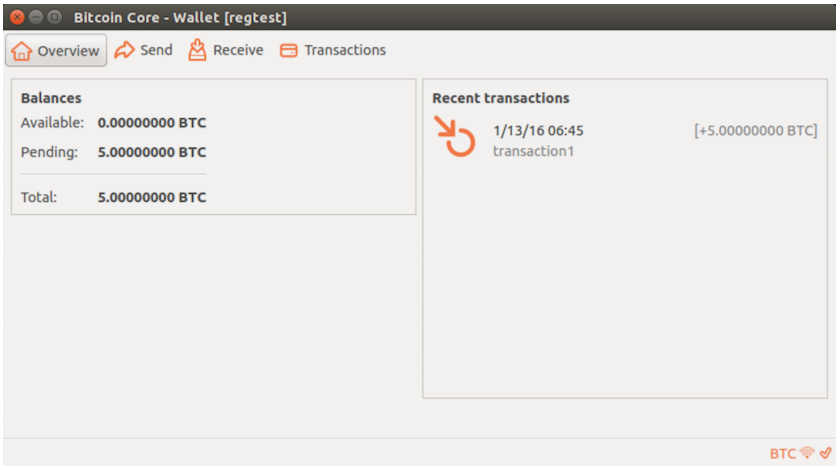

Slika 5.5: Trgovec ustvari nov naslov, na katerega želi prejeti plačilo

Izvedba plačila:

```
pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=attacker
 sendtoaddress mmudGd7WpQjwzsE6RnJ93pBXeUez6rNQ9N 5;
```



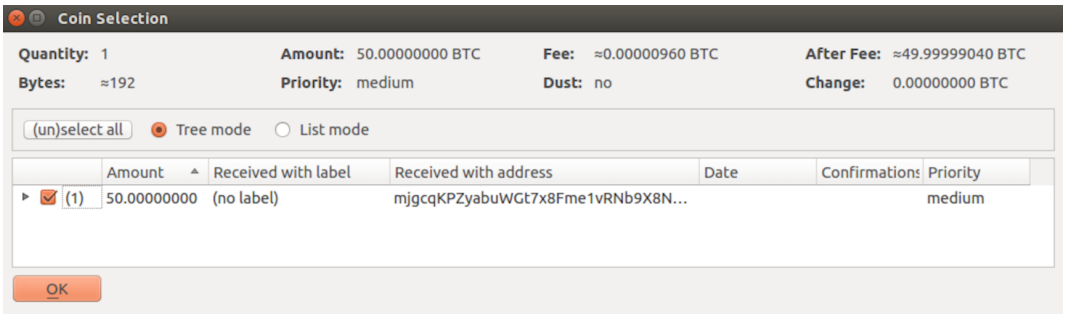

Slika 5.6: Trgovec prejme nepotrjeno transakcijo v nekaj sekundah




Slika 5.7: Trgovec prejetih bitcoinov še ne more zapraviti, vendar vidi, da bi naj prispeli

Skoraj istočasno napadalec pošlje še eno transakcijo z istimi vhodi kot jih je imela prvotna. Transakcijo pošlje z druge lokacije v Bitcoin omrežju. Napadalec izvozi zasebni ključ naslova, ki je služil kot vhod v prvo transakcijo in ga uvozi v drugo denarnico (to lahko stori vnaprej, pred izvedbo plačila). Sama denarnica ne dopušča ponovnega zapravljanja istih bitcoinov. Denarnica lokalno vodi evidenco o stanju bitcoinov na posameznih naslovih uporabnika in stanje aktualizira ob vsaki transakciji. Če zasebni ključ uvozimo v drugo denarnico, pa se stanje na naslovu, ki mu ključ pripada, prebere iz verige blokov, kjer še vedno velja stanje pred pošiljanjem transakcije. Ukaz *dumpprivkey* kot argument sprejme naslov, katerega ključ želimo in pripadajoči ključ vrne. Dobljeni ključ uvozimo z *importprivkey*. Pred tem zaženemo rudarja in drugega odjemalca napadalca ter ju povežemo. Rudarja povežemo še s trgovcem.

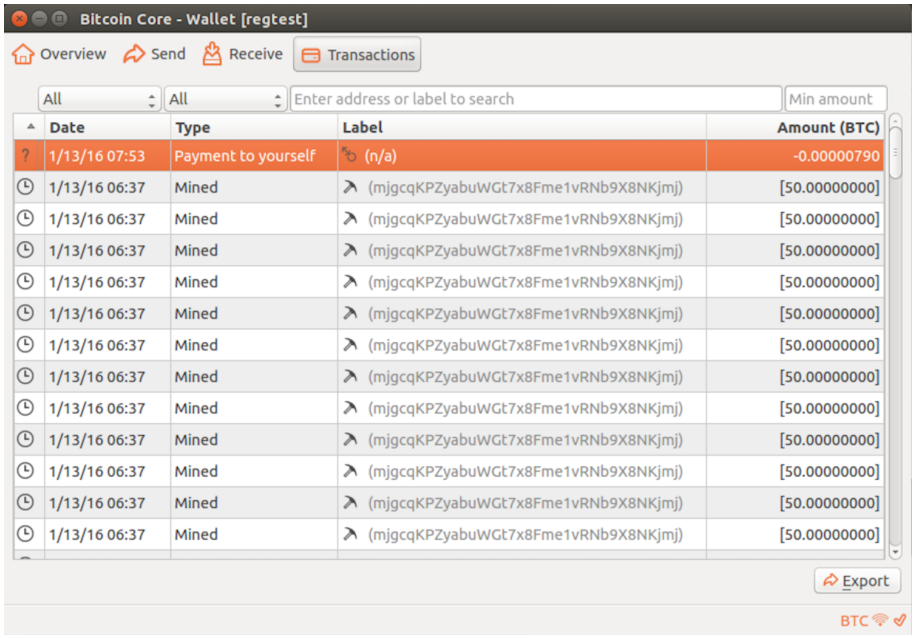
```
pero@ubuntu:~/bitsim$ bitcoind -daemon
-datadir=attacker2;

pero@ubuntu:~/bitsim$ bitcoind -daemon -datadir=miner;

pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=miner
addnode 127.0.0.1:19020 add;

pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=miner
addnode 127.0.0.1:19030 add;

pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=attacker
dumpprivkey mjgcqKPZyabuWGt7x8Fme1vRNb9X8NKjmj;

pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=attacker2
importprivkey
cQzVe7S6UCCYVbpmJpMg314kLTHHA6B2EAcgENNvzGggZTvitHFG;
```



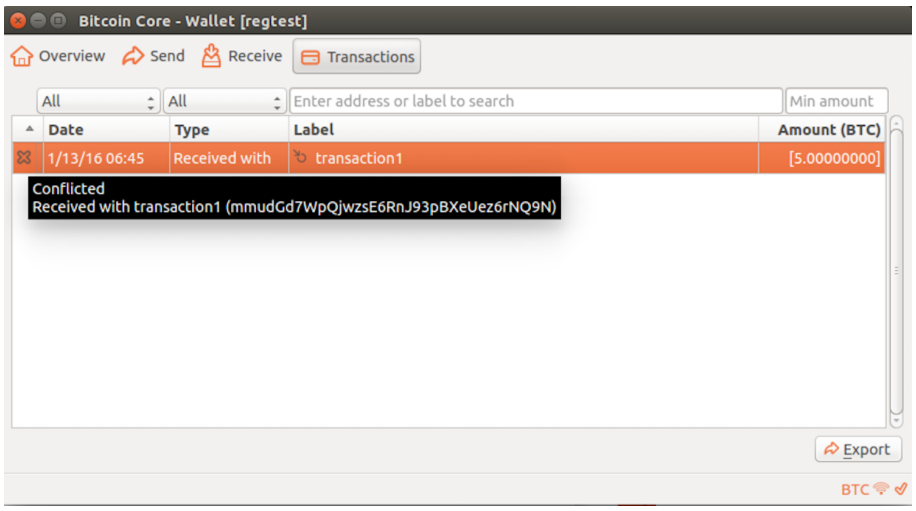

Slika 5.8: Napadalec za vhod v transakcijo izbere isti naslov kot prvič, stanje na naslovu je ponovno 50 bitcoinov, ker je bil ključ za ta naslov ponovno uvožen.

Trgovčev odjemalec drugo transakcijo zavrne brez opozorila. Odjemalec Bitcoin rudarja najprej sprejme drugo transakcijo. Če najde nov blok, jo bo vključil. Ukaz *getrawmempool* nam pokaže identifikacijske številke transakcij v pomnilniku. Tako se lahko prepričamo, da je v pomnilniku minerja res druga transakcija. Rudar generira nov blok in ga odda v omrežje.

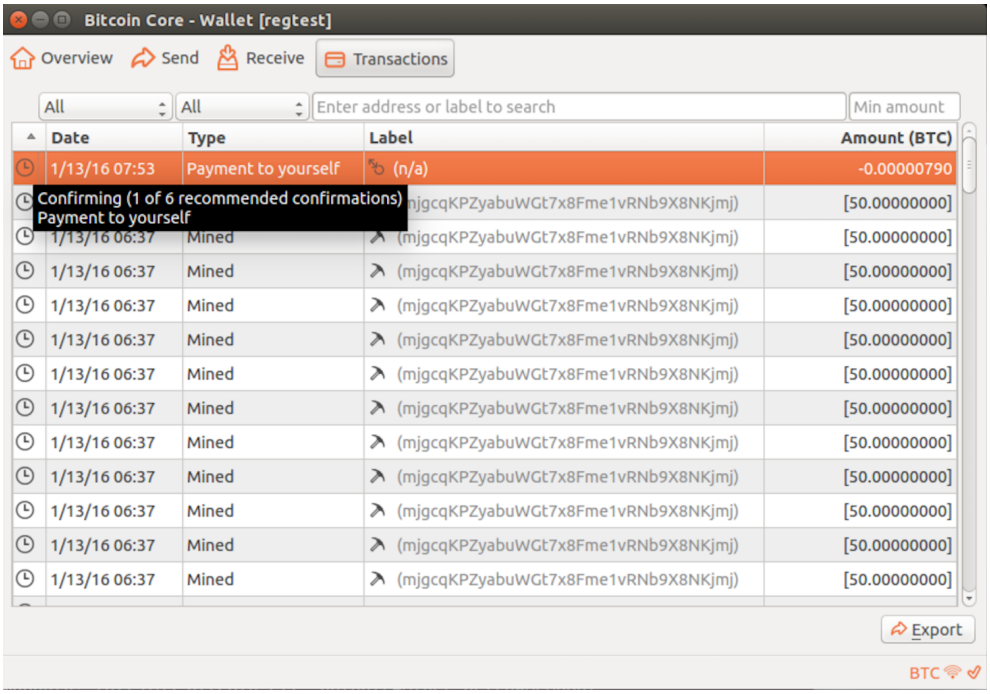
```
pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=miner
 getrawmempool;
[a63577a2f876790e5a8e3505f3f16a12fd92e720-
-2ea3c1c93b8e7602af9b92ba]

pero@ubuntu:~/bitsim$ bitcoin-cli -datadir=miner
 generate 1;
```




Slika 5.9: Stanje pri napadalcu, preden je najden naslednji blok. Druga transakcija je označena kot *"payment to self"*.




Slika 5.10: Stanje pri trgovcu po novem bloku. Plačilo je zavrnjeno, napad je uspel.




Slika 5.11: Stanje pri napadalcu po novem bloku. Druga transakcija je sprejeta. Znesek je negativen zaradi provizije.

Izvedba napada je relativno enostavna in za anonimnega napadalca ne predstavlja nobenega tveganja. Privzete nastavitve Bitcoin odjemalcev ne zadoščajo za preprečevanje napadov z dvakratno porabo. V nasprotju trgovec, ki se zaveda nevarnosti in se ustrezno zaščiti, lahko grožnjo napada z dvakratno porabo skoraj popolnoma izniči.

## 5.5 Možni protiukrepi

BitcoinWiki za preprečevanje napadov z dvakratno porabo trgovcem priporoča, da onemogočijo vhodne povezave do njihovega Bitcoin odjemalca, izhodne povezave pa izbirajo ročno in s previdnostjo. Na takšen način se napadalcu onemogoči, da se na trgovca priklopi direktno, kar mu oteži zagotavljanje prvega pogoja za uspeh napada - da trgovec prejme pošteno transakcijo najprej. [10].

Bitcoin odjemalec lokalno generira napako, ko prejme transakcijo, katere vhodi so že bili porabljeni. Težava je v tem, da je ne sporoči uporabniku. Z modifikacijo obstoječih odjemalcev bi lahko dosegli, da se v okviru nekaj sekundnega časovnega intervala po prejetju transakcje uporabnika opozori o morebitnih konfliktnih transakcijah. Zaradi hitrosti propagiranja transakcij po Bitcoin omrežju bi moral trgovec počakati le nekaj sekund, pred izdajo blaga stranki, da prepreči napad. Daljši, kot bi bil časovni interval, manjša bi bila verjetnost napada. Napad lahko še vedno uspe, če vsi sosedi v omrežju trgovca najprej sprejmejo pošteno transakcijo. V tem primeru nepoštena transakcija nikoli ne pride do trgovca, saj jo zavrnejo že njegovi sosedi.

Boljša rešitev bi bila, da trgovec v omrežju nadzoruje še nekaj odjemalcev na različnih lokacijah, ki mu direktno sporočajo prejete transakcije. Na tak način trgovec v nekem časovnem okvirju pred izdajo blaga spremlja transakcije v večjem kosu omrežja in je o morebitnem poskusu napada obveščen z večjo verjetnostjo. Z zadostnim številom opazovalcev se lahko trgovec torej dobro zaščiti pred napadi z dvakratno porabo, kar pa za trgovca seveda pomeni dodatne stroške vzdrževanja večjega števila odjemalcev v omrežju.

Še boljša rešitev, ki bi prav tako zahtevala nadgradnjo obstoječih Bitcoin odjemalcev, pa bi bila sporočanje konfliktov v omrežje. Če bi vsi pošteni odjemalci ob prejetju konfliktne transakcije po omrežju razširili opozorilo, bi bil trgovec o poskusu napada zagotovo pravočasno obveščen. Prav tako rešitev od trgovca ne zahteva dodatnih stroškov in napadalec se ji ne more izogniti. Povečala bi se le obremenjenost omrežja. [33]

# Poglavje 6

# Sklepne ugotovitve

Čeprav je Bitcoin v medijih pogosto predstavljen kot popolnoma anonimna valuta, ki omogoča izvajanje transakcij v tajnosti, povprečen uporabnik skoraj nikoli ni popolnoma anonimen. Znotraj transakcij so uporabniki res imenovani le z naslovi, s katerimi upravljajo njihove Bitcoin denarnice, vendar je prikrivanje povezave med identiteto uporabnika in naslovi, ki jih uporablja težavno. Spletne Bitcoin menjalnice, kjer večina uporabnikov omrežja prvič pridobi valuto, zahtevajo identifikacijo. S podatki, ki jih imajo na voljo menjalnice je možno slediti toku bitcoinov in deanonimizirati velik delež uporabnikov. Mešalni servisi, spletne storitve, ki lahko prekinejo verigo transakcij deanonimiziranih bitcoinov, večinoma niso zaupanja vredni, ne jamčijo vračila sredstev in niso primerni za večje vsote bitcoinov. Povezave med naslovi je zato težko prikriti, če so bile pripadajoče identitete kadarkoli razkrite. Idealno uporabnik, ki želi ostati anonimen uporablja le bitcoine, ki jih je pridobil z rudarjenjem, v transakcijah vedno uporablja novo generirane naslove in pri transakcijah na vhodu ne uporablja večih naslovov naenkrat (da jih ne poveže med seboj). Velika nihanja v vrednosti bitcoina za uporabnike, ki razpolagajo z velikim številom kovancev predstavlja tveganje, ki ga ni možno odpraviti brez menjave bitcoinov za stabilno valuto. Ravno pri menjavi valut pa je težko ohranjati anonimnost, predvsem, če gra za večje vsote denarja. Bitcoin torej znotraj svojega sistema res nudi anonimnost, vendar

pa je možno z uporabo zunanjih informacij razkriti večino Bitcoin naslovov.

S stališča varnosti je bitcoin dobro zasnovan. Dokler je večina omrežja poštena, proof-of-work shema skrbi za pravilnost izvajanja in beleženja vseh transakcij v sistemu. Ker poznavanje zasebnega ključa Bitcoin naslova absolutno in nepovratno omogoča upravljanje z bitcoini na pripadajočem naslovu, je potrebna pazljivost pri upravljanju in hranjenju Bitcoin denarnic. V primeru kraje je uporabnik nemočen, čeprav lahko svoje bitcoine spremlja po nadaljnih transakcijah. Gre za zavestno odločitev snovalcev sistema in za varovanje svoje denarnice uporabnik odgovarja sam. Šibka točka, ki je posledica proof-of-work mehanizma, je časovni okvir, dolg okoli 10 minut, v katerem je možno poslano transakcijo razveljaviti - izvesti napad z dvakratno porabo. Privzete nastavitve Bitcoin sistema ne zadoščajo za preprečevanje napada. Pri sprejemanju hitrih plačil so trgovci, ki se ustrezno ne zaščitijo, v tem času izpostavljeni napadom. Napad z dvakratno porabo je relativno enostavno izvesti in za anonimnega napadalca ne predstavlja nobenega tveganja, tudi v primeru, da napad ne uspe. Trgovec, ki je previden in sprejme ustrezne protiukrepe, pa se lahko proti napadom z dvakratno porabo zelo dobro zaščiti. Bitcoin je torej primeren tudi za sprejemanje hitrih plačil (naprimer na avtomatih za napitke), če se uporabnik zaveda nevarnosti napada in se ustrezno zaščiti.

# Literatura


[1] Anonymity, bitcoin simplified. http://bitcoinsimplified.org/learn-more/anonymity/. Povzeto: 22. 8. 2015.

[2] Bbc news - 'legitimate' bitcoin's value soars after senate hearing, bbc. http://www.bbc.com/news/technology-24986264. Povzeto: 15. 8. 2015.

[3] Bitcoin price chart. http://www.coindesk.com/price/. Povzeto: 15. 8. 2015.

[4] block 370142. https://blockchain.info/block/000000000000000130a1683f9deda4ae46cd88545ad9ca74f2f4f42f59d0300. Povzeto: 27. 12. 2015.

[5] Cointape. https://blockchain.info/charts/avg-confirmation-time. Povzeto: 28. 12. 2015.

[6] Cointape. http://www.cointape.com. Povzeto: 28. 12. 2015.

[7] Crypto-currency market capitalizations. http://coinmarketcap.com. Povzeto: 20. 9. 2015.

[8] Difficulty, bitcoin wiki. https://en.bitcoin.it/wiki/Difficulty. Povzeto: 15. 8. 2015.

[9] Digital signature standard (dss), federal information processing standards publication. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf. Povzeto: 15. 10. 2015.

[10] Double-spending, bitcoinwiki. hhttps://en.bitcoin.it/wiki/Double-spending. Povzeto: 3. 1. 2016.

[11] Drug market moving quickly online, global user survey finds, south china morning post. http://www.scmp.com/news/world/article/1482245/drug-market-moving-quickly-online-global-user-survey-finds. Povzeto: 30. 8. 2015.

[12] Faq. https://bitcoin.org/en/faq. Povzeto: 20. 9. 2015.

[13] Hal finney received the first bitcoin transaction. here's how he describes it. the washington post. https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/. Povzeto: 15. 8. 2015.

[14] Hashcash, bitcoinwiki. https://en.bitcoin.it/wiki/Hashcash. Povzeto: 15. 10. 2015.

[15] How bitcoin works. https://en.bitcoin.it/wiki/How_bitcoin_works. Povzeto: 30. 8. 2015.

[16] Merkle tree. https://en.wikipedia.org/wiki/Merkle_tree#/media/File:Hash_Tree.svg. Povzeto: 27. 12. 2015.

[17] Mtgox bitcoin exchange files for bankruptcy, bbc. http://www.bbc.com/news/technology-25233230. Povzeto: 15. 8. 2015.

[18] Proof of work, bitcoinwiki. https://en.bitcoin.it/wiki/Proof_of_work. Povzeto: 20. 10. 2015.

[19] Protocol documentation. https://en.bitcoin.it/wiki/Protocol_documentation. Povzeto: 10. 10. 2015.

[20] Secure hash standard (shs), federal information processing standards publication. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Povzeto: 15. 10. 2015.

[21] Serial bomber demands bitcoin ransom after planting explosives at supermarkets, mirror. http://www.mirror.co.uk/news/technology-science/technology/serial-bomber-demands-bitcoin-ransom-6250202. Povzeto: 17. 8. 2015.

[22] Top seven ways your identity can be linked to your bitcoin address. https://bitcoinhelp.net/know/more/top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address. Povzeto: 30. 8. 2015.

[23] Transaction fees, bitcoin wiki. https://en.bitcoin.it/wiki/Transaction_fees. Povzeto: 15. 8. 2015.

[24] transactions. https://upload.wikimedia.org/wikipedia/commons/thumb/c/ce/Bitcoin_Transaction_Visual.svg/1000px-Bitcoin_Transaction_Visual.svg.png. Povzeto: 27. 12. 2015.

[25] Weakneses, bitcoin wiki. https://en.bitcoin.it/wiki/Weaknesses. Povzeto: 15. 10. 2015.

[26] What is a finney attack?, bitcoin.stackexchange. http://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack. Povzeto: 29. 12. 2015.

[27] What is bitcoin fog? http://www.bitcoinfog.com. Povzeto: 30. 8. 2015.

[28] Tobias Bamert, Christian Decker, Lennart Elsen, Roger Wattenhofer, and Samuel Welten. Have a snack, pay with bitcoins. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pages 1–5. IEEE, 2013.

[29] Bianca Bosker. Gavin andresen, bitcoin architect: Meet the man bringing you bitcoin (and getting paid in it), huffposttech. http://www.huffingtonpost.com/2013/04/16/gavin-andresen-bitcoin_n_3093316.html. Povzeto: 15. 8. 2015.

[30] Brian Browdie. Bitpay signs 1,000 merchants to accept bitcoin payments, american banker. http://www.americanbanker.com/issues/177_176/bitpay-signs-1000-merchants-to-accept-bitcoin-payments-1052538-1.html. Povzeto: 15. 8. 2015.

[31] Nicolas Christin. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*, pages 213–224. International World Wide Web Conferences Steering Committee, 2013.

[32] Ken Griffith. A quick history of cryptocurrencies bbtc — before bitcoin. https://bitcoinmagazine.com/12241/quick-history-cryptocurrencies-bbtc-bitcoin/. Povzeto: 20. 9. 2015.

[33] Ghassan Karame, Elli Androulaki, and Srdjan Capkun. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *IACR Cryptology ePrint Archive*, 2012:248, 2012.

[34] Leo Kelion. Bitcoin sinks after china restricts yuan exchanges, bbc. http://www.bbc.com/news/technology-25428866. Povzeto: 15. 8. 2015.

[35] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach (6th Edition)*. Pearson, 6th edition, 3 2012.

[36] Alec Liu. Bitcoin mints its first billionaire: Its inventor, satoshi nakamoto, motherboard.vice.com. http://motherboard.vice.com/blog/bitcoin-mints-its-first-billionaire-satoshi-nakamoto. Povzeto: 15. 8. 2015.

[37] Sean Ludwig. Y combinator-backed coinbase now selling over $1m bitcoin per month, venture beat. http://venturebeat.com/2013/02/08/coinbase-bitcoin/. Povzeto: 15. 8. 2015.

[38] Adam Ludwin. How anonymous is bitcoin? a backgrounder for policymakers, coindesk. `http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/`. Povzeto: 22. 8. 2015.

[39] Robert McMillan. Take a tour of robocoin, the world's first bitcoin atm, wired. `http://www.wired.com/2013/10/bitcoin_atm_gallery/`. Povzeto: 15. 8. 2015.

[40] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1(2012):28, 2008.

[41] Lomas Natasha. As chinese investors pile into bitcoin, china's oldest exchange, btc china, raises $5m from lightspeed, techcrunch. `http://techcrunch.com/2013/11/18/btc-china-series-a/`. Povzeto: 15. 8. 2015.

[42] Morgen E. Peck. Bitcoin: The cryptoanarchists' answer to cash. `http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash`. Povzeto: 24. 8. 2015.

[43] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on*, pages 1318–1326, Oct 2011.

[44] Jon Russel. Coinbase is opening the first regulated bitcoin exchange in the u.s., techcrunch. `http://techcrunch.com/2015/01/25/coinbase-us-bitcoin-exchange/`. Povzeto: 15. 8. 2015.

[45] Matt Sawyer. The beginners guide to bitcoin – everything you need to know, monetarism. `http://www.monetarism.co.uk/the-beginners-guide-to-bitcoin-everything-you-need-to-know/`. Povzeto: 9. 4. 2014.

[46] Andrew Wagner. Digital vs. virtual currencies. https://bitcoinmagazine.com/15862/digital-vs-virtual-currencies/. Povzeto: 15. 9. 2015.

[47] David Yermack. Is bitcoin a real currency? an economic appraisal. Working Paper 19747, National Bureau of Economic Research, December 2013.