Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Marko Pucelj

Bitcoin

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentor: viš. pred. dr. Aljaž Zrnec

Ljubljana, 2014

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Marko Pucelj, z vpisno številko **63080202**, sem avtor diplomskega dela z naslovom:

Bitcoin

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom viš. pred. dr. Aljaža Zrneca,
- 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 v zbirki "Dela FRI".

V Ljubljani, dne 21. oktobra 2014 Podpis avtorja:

Zahvalil bi se mentorju viš. pred. dr. Aljažu Zrnecu za dobre nasvete in motivacijo pri delu.

Posebej bi se rad zahvalil tudi staršem ter vsem ostalim, ki so mi tekom študija stali ob strani.

Kazalo

Seznam uporabljenih kratic in simbolov

IKT - Informacijsko-komunikacijska tehnologija
EU - European Union; Evropska unija
BTC - Bitcoin
USD - United States Dollar; Ameriški dolar
P2P - Peer to peer
ECDSA - Elliptic Curve Digital Signature Algorithm; Algoritem eliptičnih krivulj za digitalno podpisovanje
RIPEMD - RACE Integrity Primitives Evaluation Message Diges
SHA - Secure Hash Algorithm; Varni Hash Algoritem
QR - Quick Response (code); Hitro odzivne (kode)
FPGA - Field-programmable gate array; Programabilni niz vrat
ASIC - Application-specific integrated circuit; Aplikacijsko specifično integrirano vezje

Povzetek

V diplomskem delu je opisan Bitcoin skupaj s kratko zgodovino denarja. Opisane so glavne značilnosti bitcoina, kako se trguje in kako hrani to kriptovaluto. Prav tako je narejena primerjava med bitcoinom in fiat valutami. Primerjava se prvenstveno dotika vprašanja, ali je bitcoin lahko prepoznan kot prava valuta in sredstvo za izmenjavo. Primarno se osredotočamo na ključne lastnosti, ki omogočajo trgovanje v dani valuti. Primerja se stabilnost valut, kako varno je trgovanje z njimi ter kakšen je nadzor nad trgovanjem. Vse to so faktorji, ki vplivajo na sprejem valute s strani ljudi in vlad ter spremenijo nekaj, kar samo po sebi nima realne vrednosti v sredstvo, ki drži vrednost in se lahko v njem trguje.

Ključne besede:

bitcoin, hash, fiat, valuta, transakcija, menjalnica, rudarjenje, denar, vrednost, zaupanje, kriptovaluta

Abstract

The diploma thesis presents bitcoin together with a brief history of money. It describes the main features of bitcoin, how it is traded and how kept. A comparison is also made to modern fiat currencies. The comparison primarily addresses the question of whether bitcoin can be recognized as a real currency and means of exchange. The primary focus is on key features, that allow trade in a given currency. Comparisons are made on the stability of the currency, how safe it is for trading and how well regulated it is. All of these are factors that affect the recognition of a currency from the people and it's governments while also changing something that in itself holds no real value into an asset with value that can be traded with.

Keywords:

bitcoin, hash, fiat, currency, transaction, exchange, mining, money, value, trust, cryptocurrency

Poglavje 1

Uvod

Izjemen tok sprememb, ki se pospešeno dogaja v zadnjem obdobju, ključno spreminja mnoge izmed naših dosedanjih utečenih navad oz. načinov izvajanja naših vsakodnevnih nalog, tako na delovnem mestu kot v zasebnem življenju.

Sodobne informacijske in komunikacijske tehnologije so sočasno posledica in vzrok za te spremembe. So vir novih poslovnih procesov in eden izmed ključnih podpornih procesov poslovnim procesom ter zasebnemu načinu življenja vsakega posameznika.

Iluzorno bi bilo pričakovati, da spremembe ne bi doletele tudi način trgovanja in s tem v povezavi tudi način plačevanja dobrin. Tako se le ta iz klasičnega načina blagovne menjave na tržnici oz. preko dobavnih verig (veletrgovina, skladiščenje, trgovina na drobno s pomočjo sodobnih logističnih podpornih procesov) postopoma spreminja v mešan način dobavljanja blaga in storitev preko spletne trgovine (spletna trgovina oz. ponudba nadomešča nekdanjo kataloško). Temu seveda sledi tudi bančno poslovanje oz. način plačevanja storitev, ki danes v glavnem poteka brezgotovinsko preko spletnih portalov, kar tudi bistveno spreminja bančne poslovne procese in s tem povezano obvezno izvedbo prenove poslovnih procesov.

Logično nadaljevanje družbenih sprememb, ki jih povzroča revolucija

IKT[1], je umik posameznikov v virtualni svet, kar zopet povzroča tržno nišo za ustvarjalce virtualnega (oz. namišljenega) vzporednega sveta, v katerega se vključijo posamezniki, kar posledično prinese povsem novo obliko družbenega življenja v to vključenega posameznika.

Glede na to, da že obstajajo virtualni (vzporedni) svetovi, je bilo samo vprašanje časa, kdaj se bodo pojavili tudi virtualni monetarni sistemi, ki bodo (delno) nadomestili oz. dopolnili obstoječi monetarni red. Tako je med drugimi nastala tudi virtualna valuta Bitcoin. Le-ta je skozi krizo pridobival na vrednosti, ker ni bil vezan na nobeno centralno banko.

Namen diplomskega dela je predstavitev valute Bitcoin, posameznih strokovnih mnenj, ki so se pojavila ob njegovi vedno večji razširjenosti (predvsem je tu poudarek na nadzorne organe, kot so centralne banke, davčne uprave ipd.) in ob tem analizirati njegove prednosti ter slabosti v primerjavi s klasičnimi valutami.

Na osnovi tega je postavljena naslednja hipoteza: Bitcoin je valuta, ki bo s časom v veliki meri povsem legalno zamenjala obstoječe valute in bo postala pomemben dejavnik v globalizaciji svetovnega gospodarstva.

[1]IKT - Informacijsko-komunikacijska tehnologija

Poglavje 2

BITCOIN

2.1 Zgodovina denarja

2.1.1 Nedenarna izmenjava

Denar je del naše civilizacije že tisočletja. Svoj obstoj dolguje potrebi človeka, da opravlja trgovanje v bolj fleksibilni obliki, kot je bilo tako, ko so se razvile prve civilizacije in organizirana trgovina. Pred tem so ljudje živeli v majhnih skupnostih, kjer je prevladovala ekonomija podarjanja (ang. gift economy) ali blagovna menjava (ang. barter). Prva sloni na tem, da se posamezniku oziroma skupini podari dobrino oziroma uslugo brez dogovora o vračilu nagrad. Idealno je, da se hkrati izvaja več takih transakcij, tako da usluge oziroma dobrine krožijo v skupini. [8]

Hkrati pa je potekala tudi blagovna menjava. Tu je posameznik ali skupina svoj presežek dobrin poskušal zamenjati za dobrino, ki mu je primanjkovala. Pomanjklivost tega sistema leži v njegovi rigidnosti. [15] Če je posameznik želel dobiti dve kravi, imel pa je štiri ovce, ki jih je lahko oddal, je moral najprej najti posameznika, ki je potreboval ovce in imel krave, nato pa še, da ni za ti dve kravi zahteval več, kakor je imel prvi posameznik. [15]

2.1.2 Pojav denarja

Zaradi svojega pomena kot surovina za izdelavo orodji je anatolski obsidian postal prva dobrina, s katero se je veliko trgovalo. Trgovanje z anatolskim obsidianom se je izvajalo v kameni dobi, okoli 12.000 pr. Kr. [10] Razvoj organizirane trgovine v 9. tisočletju pr. Kr. pa je njegovo uporabo kot sredstvo za trgovanje razširil po tedaj znanem svetu. Prav tako se je kot neke vrste denar oz. prej omenjena blagovna menjava okoli tega tisočletja razširila uporaba žita in govedi. Pomembnost žita kot valute je še posebno razvidna v jeziku, kjer izraz zrno zlata pomeni majhno količino zlata.

V začetku se je trgovalo s stvarmi, ki so imele največjo uporabo in zanesljivost v smislu ponovne uporabe in preprodaje – njihova tržnost. Tako so, v kmetijskih skupnostih stvari, ki so bile potrebne za učinkovito produkcijo žitaric in vzgojo živine najlažje dobile na denarnem pomenu za neposredno menjavo. Z izboljšanjem življenjskih razmer in zapolnitvijo osnovnih potreb človeka po obstoju se je delitev dela povečala. Ustvarila so se nova področja in dejavnosti za reševanje bolj kompleksnih težav. Z bolj specifičnimi zahtevami ljudi je izmenjava dobrin in uslug potekala čedalje bolj neposredno, saj je fizični razkol med dobavitelji in povpraševalci zahteval uporabo medija, ki je bil skupen vsem skupinam.

Trgovanje, kjer je kot denar služila vrsta kovine, se je pojavilo v 3. tisočletju pr. Kr. Tako je v Sardiniji, enem izmed glavnih območij, kjer so pridobivali anatoljiski obsidian le-tega zamenjala trgovina z bakrom in srebrom. Kovine so kot sredstvo za trgovanje prevladale nad drugimi sredstvi (govedo, žito, lupine školjk), saj so hkrati odporne, prenosljive in se z lahkoto razdelijo na manjše dele [16].

Prva omemba enote za denar izhaja iz 3. tisočletja pr. Kr. Srebrnik (ang. shekel) je prvotno bila enota za težo hmelja. En shekel je pomenil 180 zrn oziroma 11 gramov. Preko Babiloncev [16] se je ta enota prenesla v današnji Izrael, od kjer izhaja prvi zapis te enote v Biblji. [13]

2.1.3 Denar kot dobrina

Moderni kovanci so se razvili iz trgovanja z blagom, kjer so odstranili del prodajanega blaga, da je ustrezal vrednosti, ki je bila določena. V primeru, da se je trgovalo s srebrom, so tako ostali izrezki, ki so se s časom razvili v kovance. Prvi zlati kovanci v Grčiji so bili narejeni v Lydii okoli leta 700 pr. Kr. [1] Tehtali so med 8.42 in 8.75 gramov.

Prvi znani vladar v Sredozemlju, ki je uradno določil standarde za težo in denar, je bil Pheidon, kralj Argosa v 7. stoletju pr. Kr. Kovanje denarja se je tako pojavilo v tem časovnem obdobju v mestih Male Azije, od koder se je v 5. stoletju pr. Kr. razširilo v sedanjo Grčijo in južno Italijo. Prvi kovan (žigosan z oznako avtoritete v obliki slike ali besed) denar je Stater iz elektruma (naravna zlitina srebra in zlata) z žigom želve. Narejen je bil na otoku Aegina.

Slika 2.1: Želvji Stater iz Aegine

Ostali kovanci narejeni iz elektruma so bili v večjih količinah izdelani okoli leta 650 pr. Kr. v Lydii. [16] Od tam se je uporaba kovancev razširila na bližnja mesta v regiji in v celinsko Grčijo ter Perzijski imperij. Z odkritjem preizkusnega kamna[1] se je uporaba naturalnega denarja baziranega na kovinah in kovancih, razširila, saj se je vsaka mehka kovina lahko testirala za čistost. To je dovolilo posamezniku, da je ocenil količino te kovine v kepi. Tako se je utrdila uporaba zlata kot valute in se razširila iz Male Azije v

[1] ang. touchstone. Orodje za preizkušanje žlahtnih kovin.

preostali svet. Zlato je namreč mehka kovina, ki se jo težko pridobi in se jo lahko skladišči.

Ker pa je uporaba takega sistema še vedno zahtevala poznavanje matematike in uporabo kar nekaj korakov, so proces poenostavili z uvedbo standardiziranih kovancev. Ti so bili predhodno stehtani in legirani[2]. Če je prodajalec poznal poreklo kovanca, uporaba merilnega kamna ni bila potrebna. Kovanci so bili ponavadi kovani v zelo varovanem procesu s strani vlade. Kovani kovanec je bil nato žigosan s simbolom, ki je zagotavljal težo in vrednost valute. Zlato in srebro je tako postalo primarno sredstvo za trgovanje skozi celotno zgodovino.

V mnogih jezikih je beseda za srebro še zdaj sinonim za denar. In čeprav sta bili ti žlahtni kovini najbolj pogosto uporabljeni za kovanje kovancev, so ponekod uporabljali tudi druge kovine, bodisi iz političnih razlogov[3] bodisi zaradi pomanjkanja zlata ali srebra [4].

V Evropi so znova začeli kovati zlate kovance v 14. stoletju in to kot posledico križarskih vojn[5]. V štirianjstem stoletju je Evropa masovno opustila srebro kot valuto v korist zlatu. [18] Tako je leta 1328 Dunaj prenesel svojo kovaštvo srebra v zlato. [18]

Toda zaradi hkratnega obstoja treh različnih vrst kovancev (zlati, srebrni in bakreni) so nastale težave. Angleški in španski trgovci so cenili zlato bolj kot srebro, večina sosedov pa je cenila srebro bolj kot zlato. To je imelo za posledico, da je angleška, na zlatu bazirna guinea, pridobivala na vrednosti nasproti na srebru bazirani kroni v letih od 1670 do 1680. Posledično je bilo srebro ukinjeno zaradi dvomljivih količin zlata, ki so prihajale v Anglijo v tako velikih količinah, da jih nobena druga evropska država ne bi delila. Ta učinek se je še poslabšal, ker azijski trgovci zlata niso cenili tako kakor

[2]ang. alloying. Vsebnost zlata v zlitini je bila predhodno določena.

[3]V Šparti so uporabljali železne kovance in na ta način odvračali svoje državljane od zunanjega trgovanja.

[4]V zgodnjem sedemnajstem stoletju so na Švedskem uporabljali "denarne plošče". To so bile velike plošče kovane iz bakra, dolge in široke 50 centimetrov ali več ter žigosane z indikacijo njihove vrednosti.

[5]Prvi, ki je to prakso znova prenesel v Evropo, naj bi bil Friderik II

evropski trgovci. Zlato je zapuščalo Azijo, srebro pa Evropo v količinah, ki so evropske opazovalce skrbele.

Sistem so stabilizirali s pomočjo zagotovil nacionalnih bank, da bodo zamenjale denar v zlato po fiksnih tarifah. Toda zaradi tega je Banka Anglije v 3. desetletju 17. stoletja tvegala nacionalno finančno katastrofo, ker so stranke zahtevale, da se v času krize njihov denar zamenja v zlato. Banko so na koncu rešili londonski trgovci s finančnimi zagotovili.

Nov korak v evoluciji denarja je bila sprememba dojemanja kovancev iz enote teže v enoto vrednosti.

2.1.4 Zadolžnice in bankovci

Papirnat denar je bil prvič uporabljen na Kitajskem v 11. stoletju, kjer so ga trgovci uporabljali kot dobropis namesto večjih količin bakrenih kovancev, ki jih je bilo nepraktično prevažati pri velikih transakcijah. To ni nadomestilo kovancev v celoti, ampak sta se obe sredstvi uporabljali hkrati. Centralna vlada je opazila ekonomsko prednost papirnatega denarja in izdala monopolne pravice za izdajanje teh certifikatov depozitnim trgovinam. Do dvanajstega stoletja je količina izdanih bankovcev znašala 26 milijonov nizov denarnih kovancev.

VEevropo so zgodbe o denarju iz papirja prinesli v 13. stoletju popotniki, kot sta Marco Polo in William of Rubruck. [21] [20] V Italiji in Flandriji so zaradi nevarnosti in nepraktičnsti prevažanja večjih količin denarja trgovci začeli uporabljati zadolžnice[6], ki so bile nekakšen predhodnik bankovcev. [9] V začetku so bile te osebno podipisane, vendar so kmalu postale pisne odredbe za plačilo zneska imetnika le teh.

Prve bankovce je v letu 1661 izdal Stockholms Banco, ki je predhodnik Banke Švedske. Zamenjali so bakrene plošče, ki so se do tedaj uporabljale kot plačilno sredstvo. Banki je sicer v letu 1664 zmanjkalo kovancev za odkup vseh bankovcev, kar je imelo za posledico zaprtje banke.

[6] ang. promissory note

Banke so kmalu začele izdajati svoje bankovce, ki so se uporabljale na precej podoben način kakor današnji od vlad izdan denar. Dokler niso vlade standardizirale izdajo bankovcev in prenesle monopol na eno banko, je vsaka banka izdajala svoje, kar je imelo za posledico, da bankovci niso bili veljavni povsod. Banka Anglije je to pravico dobila leta 1694, v ZDA pa je FED[7] to pravico dobil leta 1913. Do nedavno so te od vlad avtorizirane valute bile vrsta reprezantivnega denarja, saj so bile vsaj delno podprte s srebrom in zlatom in so vsaj teoreticno lahko zamenljive s srebrom in zlatom.

2.1.5 Digitalne valute

Z uvedbo računalnikov in interneta se je trgovanje v čedalje večji meri odvijalo s pomočjo elektronskih transakcij. IBM in American Airlines sta skupaj razvili SABRE – popolnoma delujoč sistem za rezervacijo letov. Telefonski kabli so bili povezani na terminale na letališču, rezervacije pa so se prvič v zgodovini delale na podlagi kredita. Leta 1970 so se vse evropske banke povezale z z osrednjimi računalniki[8]. S koncem devetdesetih let prejšnjega stoletja se je razširila uporaba elektronskih čekov in pametnih kartic. Le te so uporabljale kriptografijo javnega ključa za izvajanje transakcij.

Leta 1990 je David Chaum ustanovil DigiCash Inc., ki je bila pionir na področju digitalnih valut. Njihove transakcije so bile unikatne v tem, da so ponujale popolno anonimnost zaradi vrste kriptografskih protokolov, ki jih je razvil Chaum. Leta 1998 je podjetje zaradi bankrota kupil eCash Technologies, ki ga je leta 2002 prevzel InfoSpace. eCash je z uporabo kriptografije zagotavljal anonimnost pri trgovanju. Uporabljal je slepe podpise in s tem dosegel nepovezljivost med plačevano in plačano transakcijo. Glede na lastnosti transakcije se je ločilo med povezanimi in nepovezanimi transakcijami. V ZDA je ta sistem uvedla le Mark Twain banka, sistem pa je bil opuščen leta 1997, ko je to banko prevzela banka Mercantile. Podobno kakor kreditne kartice, je bil sistem za uporabnike zastonj, medtem ko so trgovci plačevali

[7] Federal Reserve System kar pomeni federalna rezerva

[8] angl. mainframe

transakcijsko provizijo. [26]

2.1.6 Bitcoin - Uvodni pregled dogodkov

Leta 2008 je avtor pod psevdonimom Satoshi Nakamoto objavil članek, v katerem je opisal Bitcoin protokol. Leta 2009 se je postavila prva Bitcoin mreža preko prvega odprtokodnega klienta, Bitcoin pa je postal prva praktično implementirana kriptovaluta. Leta 2010 so se na forumu bitcointalk prvič pogajali o ceni bitcoin transakcij. Ena bolj opaznih transakcij je bila pica v vrednosti 10000 BTC[9]. 6. avgusta so zaznali prvo ranljivost v Bitcoin protokolu. Transakcije niso bile pravilno preverjene preden so se vključile v transakcijski dnevnik, kar je omogočilo ustvarjanje neomejenega števila bitcoinov. 15. avgusta se je ta ranljivost zlorabila, ko se je ustvarilo preko 184 milijonov novih bitcoinov. Transakcija je bila odkrita, njen zapis izbrisan iz transakcijega dnevnika, ranljivost pa odpravljena. To je bila do sedaj edina odkrita ranljivost Bitcoin protokola.

Leta 2011 so Wikileaks in druge organizacije začela sprejemati bitcoine kot donacije. Konec leta 2011 je vrednost bitcoina strmoglavila iz $30 na $2. Oktobra 2012 je BitPay poročal, da več kot tisoč trgovcev sprejema Bitcoin.

Leta 2013 se je transakcijski dnevnik začasno razdvojil v dva neodvisna dnevnika z različnimi pravili, kako naj se transakcije sprejemajo. Mt. Gox[10] je začasno ukinil trgovanje z bitcoini, zaradi česar je devizni tečaj padel za 23 odstotkov, preden se je zopet vrnil na prejšnje stanje. Aprila 2013 je bitcoin pridobil na razpoznavnosti, ko so storitve, kot so OkCupid in Foodler začele sprejemati bitcoin kot veljavno plačilno sredstvo. [3]

[9] BTC - bitcoin

[10] Spletna menjalnica za trgovanje, sprva s kartami, kasneje pa z bitcoini.

2.2 Bitcoin protokol

Bitcoin je digitalna kriptovaluta, ki je bila prvič omenjena na papirju, napisanem leta 2008 pod psevdonimom Satoshi Nakamoto. Opisan je kot P2P elektronski sistem denarja, ki eliminira potrebo po tretji stranki oz. po sistemu baziranem na zaupanju. Namesto tega bitcoin uporablja elektronski sistem plačevanja ki temelji na kriptografskem dokazu. To ima za posledico, da lahko pri transakciji sodelujeta obe stranki neposredno. Ustvarjanje in transakcije bitcoinov potekajo po odprtokodnem kriptografskem protokolu, kjer je vsak bitcoin razdeljen na do osem decimalnih mest, kar tvori 100 milijonov manjših enot, imenovanih satoshi. Procesiranje transakcij bitcoina poteka preko t. i. bitcoin rudarjev/strežnikov, ki jih lahko postavi vsakdo. Ti strežniki potrjujejo transakcije tako, da jih zapišejo v »knjigo«, ki se posodablja in arhivira. Preko tega arhiviranja se kot izplačilo za narejeno delo kujejo novi bitcoini. [22]

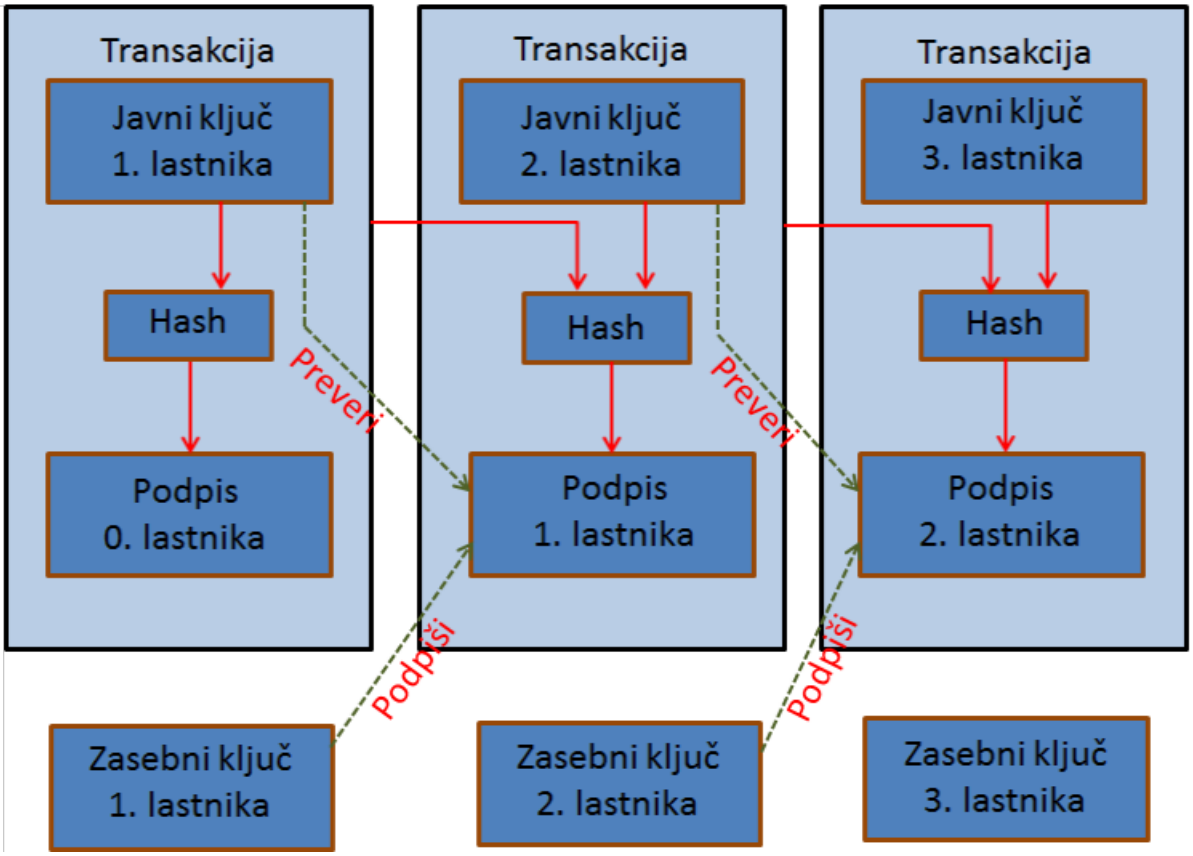
Bitcoin kovanci so definirani kot veriga digitalno podpisanih transakcij, ki so se začele pri njegovi kreaciji. Vsak lastnik bitcoin prenese do naslednjega lastnika tako, da ga digitalno prepiše na naslednjega lastnika v Bitcoin transakciji. Če hoče prejemnik preveriti verigo lastništva, lahko samo pogleda vse prejšne transakcije. Ta t. i. verižni blok je distribuiran preko P2P[11] tehnologije za izmenjavo datotek, ki je podobna BitTorrentu[12].

Mreža žigosa transakcije tako, da jih vključi v bloke. Le-teh ni mogoče modificirati brez da se znova naredi vso delo, ki je bilo potrebno, za privedbo do tega spremenjenega bloka. Ker je mreža bazirana na P2P tehnologiji, zahteva minimalno strukturo za izvanjanje in delitev transakcij. Sporočila se oddajajo po principu "best effort"[13]. Ob priklopu na Bitcoin mrežo vozlišče prenese in preveri nove bloke iz drugih vozlišč ter jih doda v svojo lokalno kopijo verige blokov. [22]

[11] Peer-to-peer. Vozlišča so neposredno povezana

[12] Protokol za prenos datotek preko peer-to-peer mreže

[13] Vozlišča se priklopijo oziroma odklopijo po volji



Slika 2.2: Transakcija Bitcoinov

2.2.1 Bitcoin naslov

Bitcoin naslov je hash javnega dela para ECDSA[14] ključev. Naslovi oz. javni ključi in njim pripadajoči privatni ključi so shranjeni v denarnici. Pri izvedbi transakcije na določen naslov mora denarnica za ta naslov imeti privatni ključ. V primeru da ga nima, so bitcoini, povezani s to transakcijo, izgubljeni. Tak primer je, če se obnovi denarnica na čas, ko le ta ni imela naslova, na katerega so bili poslani bitcoini. Ob izgubi denarnice so izgubljeni vsi bitcoini, ki so bili na tej denarnici. Naslov predstavlja izvor in destinacijo transakcije pri trgovanju z bitcoinom.

Bitcoin naslov ima dolžino do 34 znakov. Le-ti so lahko številke, velike črke ali pa male črke. Izjeme so črke O, I, i in številka 0, da se prepreči vizualna dvoumnost. Naslovi, krajši od štirintrideset znakov, so posledica številk, ki se začnejo z 0. Ko se ničle opustijo, kodiran naslov nastane krajši. V teoriji je lahko najmanjši naslov dolžine do 27 znakov.

Za hitro preverjanje veljavnosti naslova se uporablja kontrolno vsoto. Leta je sestavljena iz različnih znakov znotraj naslova. Tako se lahko tipografske napake avtomatično najdejo in naslov zavrne. Kontrolne vsote prav tako dovolijo Bitcoin programski opremi, da ne zavrne naslovov, krajših od 34 znakov.

Bitcoin omogoča ustvarjanje več različnih naslovov, ki so vezani na denarnico. Vsak je popolnoma neodvisen, prav tako pa ne obstaja t. i. "Glavni naslov". Pri vsaki novi transakciji se za boljšo varnost in povečano stopnjo zasebnosti pogosto uporablja nov naslov.

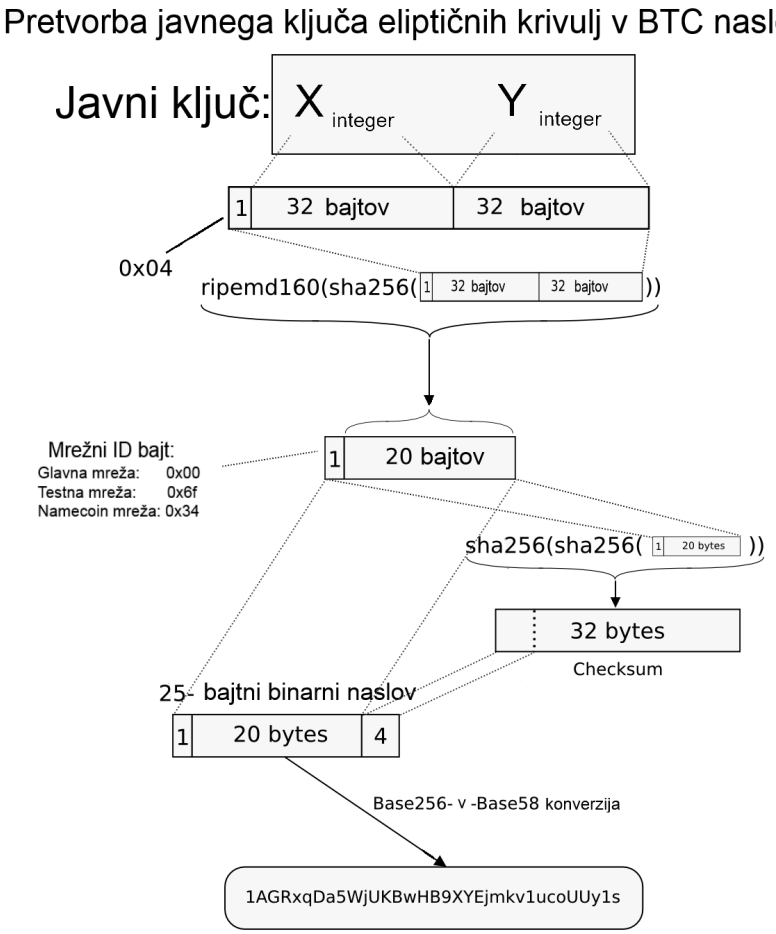
Pridobitev naslova

Uporabnik lahko naslov pridobi na več načinov. Lahko ga pridobi preko spletne strani, kakor je naprimer Bitcoin-Qt, lahko mu ga dodeli menjalnica ali ponudnik spletnih denarnic. Lahko pa ga generira uporabnik sam z uporabo zastonj programske opreme. Generirani so tako, da se vzame na-

[14] Algoritem eliptičnih krivulj za digitalno podpisovanje.

ključno številko in na njej izvede matematične operacije, iz katerih dobimo par javnih/zasebnih ključev. Po pridobitvi para ključev se izračuna sledeče:

Bitcoin naslov/Javni ključ = Verzija združena z RIPEMD-160(SHA-256(javni ključ))
Kontrolna vsota = Prvi štirje bajti od SHA-256(SHA-256(hash ključa))
Bitcoin Naslov = Base58Encode(Hash ključ združen s Kontrolno vsoto) [22]



Slika 2.3: Transakcija Bitcoinov

Povprečen namizni računalnik lahko generira več tisoč naslovov na minuto. Tako serijsko generiranje ključev je uporabno na primer pri spletnih trgovinah, ki imajo možnost nakupa v bitcoinih.

Vrsta Bitcoin naslova

Obstaja več različnih vrst Bitcoin naslovov, ki se ločijo s predpono. Vsaka vrsta ima svoj namen, predpona pa omogoča hitro razpoznavo tega namena.

Decimalna verzija	**Vodilni simbol**	**Uporaba**	**Primer kriptiranega ključa**
0	1	Hash javnega ključa bitcoina	17VZNX1SN5NtKa8U QFxwQbFeFc3iqRYhem
5	3	Hash skripte bitcoina	3EktnHQD7RiAE6uz Mj2ZifT9YgRrkSgzQX
48	L	Hash javnega ključa litecoina	LhK2kQwiaAvhjWY7 99cZvMyYwnQAcxkarr
52	M or N	Hash javnega ključa namecoina	NATX6zEUNfxfvgVw z8qVnnw3hLhhYXhgQn
111	m or n	Hash javnega testnet ključa bitcoina	mipcBbFg9gMiCh81 Kj8tqqdgoZub1ZJRfn
128	5	Hash privatnega ključa bitcoina	5Hwgr3u458GLafKBgxtssHSPqJ nYoGrSzgQsPwLFhLNYskDPyyA
196	2	Hash testnet skripte bitcoina	
239	9	Hash privatnega testnet ključa bitcoina	92Pg46rUhgTT7romnV7iGW6W 1gbGdeezqdbJCzShkCsYNzyyNcc

Navadni naslov se uporablja za standardne transakcije, hash skripte [15] pa pri posebnih vrstah transakcij. Namen je premakniti odgovornost dobave

[15] P2SH - pay to script hash.

pogojev odkupa transakcije od pošiljatelja do kupca. To prinaša korist tako, da lahko pošiljatelj financira poljubne transakcije z uporabo 20 bitnega hasha.

Litecoin in namecoin sta kriptovaluti, ki bazirata na bitcoin protokolu in uporabljata enako logiko za določitev naslovov. Testnet je testno okolje, v katerem se izvaja testiranje novih funkcionalnosti in odpravo hroščev na bitcoin protokolu.

Validiranje Bitcoin naslova

Naslov je veljaven, če je določene dolžine, ima samo dovoljene karakterje in se začne z ena ali tri. Ker pa je možno, da je naslov krajši, saj se vodeče ničle brišejo, se uporablja posebne skripte. En primer tega je spodnja Unix Shell skripta:

```
1  #include <stdio.h>
2  #include <string.h>
3  #include <openssl/sha.h>
4
5  const char *coin_err;
6  #define bail(s) { coin_err = s; return 0; }
7
8  int unbase58(const char *s, unsigned char *out) {
9    static const char *tmpl = "123456789"
10     "ABCDEFGHJKLMNPQRSTUVWXYZ"
11     "abcdefghijkmnopqrstuvwxyz";
12   int i, j, c;
13   const char *p;
14
15   memset(out, 0, 25);
16   for (i = 0; s[i]; i++) {
17     if (!(p = strchr(tmpl, s[i])))
18       bail("bad␣char");
19
```

```
20      c = p - tmpl;
21      for (j = 25; j--; ) {
22        c += 58 * out[j];
23        out[j] = c % 256;
24        c /= 256;
25      }
26
27      if (c) bail("address too long");
28    }
29
30    return 1;
31  }
32
33  int valid(const char *s) {
34    unsigned char dec[32], d1[SHA256_DIGEST_LENGTH], d2[
       SHA256_DIGEST_LENGTH];
35
36    coin_err = "";
37    if (!unbase58(s, dec)) return 0;
38
39    SHA256(SHA256(dec, 21, d1), SHA256_DIGEST_LENGTH, d2);
40
41    if (memcmp(dec + 21, d2, 4))
42      bail("bad digest");
43
44    return 1;
45  }
46
47  int main (void) {
48    const char *s[] = {
49      "1Q1pE5vPGEEMqRcVRMbtBK842Y6Pzo6nK9",
```

```
50      "1AGNa15ZQXAZUgFiqJ2i7Z2DPU2J6hW62i",
51      "1Q1pE5vPGEEMqRcVRMbtBK842Y6Pzo6nJ9",
52      "1AGNa15ZQXAZUgFiqJ2i7Z2DPU2J6hW62I",
53      0 };
54    int i;
55    for (i = 0; s[i]; i++) {
56      int status = valid(s[i]);
57      printf("%s:␣%s\n", s[i], status ? "Ok" : coin_err);
58    }
59
60    return 0;
61  }
```

Denarnice

Denarnice so datoteke, ki vsebujejo kolekcijo privatnih ključev in posledično naslovov. Denarnice dovolijo uporabnikom bitcoina pošiljanje bitcoinov, zahtevanje plačila in izračun celotne bilančne vsote vseh naslovov v denarnici. Ob izgubi denarnice uporabnik izgubi vse bitcoine, ki so bili vezani na naslove v njej. Razvili so tri vrste denarnic, in sicer: programske denarnice, spletne denarnice in papirnate denarnice.

Programske denarnice Primer takih denarnic je bitcoin ali Bitcoin-Qt. To je programska oprema, ki se povezuje neposredno na peer-to-peer mrežo. Obstajajo denarnice za iOS ali Android, ki potrebujejo manj računske moči. S pomočjo QR kod poenostavijo transakcije. Prav tako je možno, da storitve, ki jih opravlja aplikacija na standardnem računalniku, opravlja posebna namenska naprava.

Spletne denarnice Te denarnice so bolj kakor navadnim denarnicam podobne bančnim računom ali trgom v realnem času. Vsebujejo naslove, ki

so vezani na posameznega uporabnika in zadržujejo Bitcoine v imenu tega uporabnika. Uporabljajo se na spletnih straneh (npr. Bitstamp, ipd.).

Papirnate denarnice Vsak veljaven Bitcoin naslov je lahko natisnjen na papir in uporabljen za shranjevanje bitcoinov brez povezave. Taka denarnica je varna za uporabo le v primeru, da jo je uporabnik natisnil sam. Če je denarnico dobil kot darilo, nagrado ali kot plačilo, obstaja možnost, da je bil privatni ključ kopiran in obdržan s strani kreatorja, kar bi mu omogočilo dostop do teh sredstev.

Nekatere od takih denarnic skrijejo privatne ključe za pečat[16], ki je odporen na poseganje. Ker pa ni izključeno, da je originalni ustvarjalec papirnate denarnice ohranil oziroma kopiral privatne ključe, je tak način shranjevanja bitcoinov, imenovan tudi "hladno shranjevanje", klasificiran kot nezanesljiv način hranjena bitcoinov.

2.2.2 Transakcije

Transakcije so kriptografsko podpisani zapisi, ki predajo lastništvo na nov naslov. Tranaskcije imajo vhod. To so zapisi, ki referencirajo sredstva iz preteklih transakcij in so kriptografsko podpisani. Samo oseba, ki ima primeren privatni ključ, lahko ustvari pravilen podpis in omogoči, da se transakcija izvede.

Prav tako imajo izhode. To so zapisi, ki določijo novega lastnika prenesenega Bitcoina in ki bodo referencirani kot vnosi v prihodnjih transakcijah, ko se bo ta bitcoin zapravil. Izhod določi, kateri Bitcoin naslov je prejemnik sredstev. [5]

Pri tradicionalih transakcijah lahko posameznik ponovno pošlje Bitcoine, ki jih nima. To v bistvu ustvari več vej transakcijskega drevesa. Bitcoin se temu izogne tako, da morajo vse transakcije biti overjene z rešitvijo računsko

[16]Namen pečata je, da onemogoči dostop do privatnega ključa. Primer je npr. privatni ključ, skrit za geslo, ali privatni ključ, skrit na različnih delih denarnice - Shamirjeva shema za tajno izmenjavo.

težke težave[17], ki se imenuje tudi rudarjenje. Ko se transakcija vključi v blok, dajejo klienti prednost transakciji, ki je porabila največ računske vrednosti. S tem izničijo ostale veje transakcijskega drevesa.

Tipi transakcij

Obstajajo tri vrste transakcij. Ločujejo se glede na, to čemu so namenjene.

Pay-to-PubkeyHash: To je standardna transakcija, ki se izvede, ko pride do izmenjave bitcoinov med dvema naslovoma. Ker je bitcoin naslov samo hash, pošiljatelj ne more poslati popolnega javnega ključa v scriptPubKey. Ko dobitelj unovči bitcoine, ki so mu bili poslani na naslov, prejemnik dobavi tako podpis kakor tudi javni ključ. Skripta tako preveri, če se javni ključ ujema s hashom v scriptPubKey in nato preveri še podpis na javnem ključu.

Pay-to-scriptHash: Namen Pay-to-Script transakcije je, da prestavi odgovornost za oskrbo pogojev za unovčitev transakcije od pošiljatelja sredstev na unovčitelja. Prednost tega pristopa je, da pošiljatelj lahko financira katerokoli poljubno transakcijo, ne glede na to, kako zahtevna je le ta. To naredi z uporabo hasha fiksne dolžine 20 bajtov, ki je dovolj kratek, da se skenira iz QR kode ali kopira.

Coinbase transakcija: To je posebna vrsta transakcije, ki nima vnosov. Ustvari se, ko se preko rudarjenja[18] ustvari nov blok. Zato, ker vsak na novo ustvarjen blok s sabo nosi nagrado na novo kovanih Bitcoinov, prva transakcija tega bloka (z redkimi izjemami) razdeli te Bitcoine vsem vpletenim v potrditvi tega bloka. Poleg teh na novo ustvarjenih bitcoinov je coinbase transakcija prav tako uporabljena za določanje prejemnika transakcijskih provizij, ki so bile plačane v tem bloku. Coinbase transakcije zmeraj vsebujejo izhode, ki kombinirajo seštevek nagrad in transakcijskih provizij,

[17]Izračun hash glave bloka.
[18]Potrjevanje transakcij.

zbranih iz drugih transakcij. Nagrado se lahko podari enemu Bitcoin naslovu ali večim, kakor pri ostalih transakcijah. [5]

Preverjanje transakcij

Pri tradicionalih transakcijah bi lahko posameznik ponovno poslal Bitcoine, ki jih nima. To potencialno lahko ustvari več vej transakcijskega drevesa.

Bitcoin se temu izogne tako, da morajo vse transakcije biti overjene z rešitivijo računsko težke težave[19], ki se imenuje tudi rudarjenje. Ko se transakcija vključi v blok, dajejo klienti prednost transakciji, ki ima največjo računsko vrednost. S tem izničijo ostale veje transakcijskega drevesa.

Večina izhodov Bitcoinov obremeni novo prenesene kovance z enim ESDCA[20] privatnim ključem. Pravi zapis pri vhodih in izhodih tako ni nujno ključ ampak skripta. Bitcoin uporablja prevajalni skriptirni sistem, da odloči, če so bili izhodni kriteriji zadovoljeni. S tem so možne bolj kompleksne operacije, kot so izhodi z dvema ESDCA podpisoma ali sheme z dvema od treh podpisov. Izhod, ki referencira en Bitcoin, je tipičen izhod in vsebuje informacije v obliki skripte, ki potrebuje en ESDCA podpis. Ta skripta določa, kaj mora biti podano, da se sredstva odklenejo kasneje. Ko se v prihodnje zapravi to transakcijo v novem vhodu, mora vhod zagotoviti vse potrebne podatke, da se pogoj, definiran v originalni izhodni skripti, zadovolji. [6]

2.2.3 Razpršitvene funkcije in podpisi

Podpisi

Da trgovanje z Bitcoinom poteka varno, se uporablja sistem digitalnega podpisovanja. To je matematična shema za predstavitev verodostojnosti digitalnega sporočila ali dokumenta. Veljaven podpis prejemniku zagotavlja, da je bilo sporočilo poslano od poznanega pošiljatelja. Ta zagotovila so:

[19] Izračun hash glave bloka.

[20] Algoritem eliptičnih krivulj za digitalno podpisovanje (angl. elliptic curve digital signature algorithm)

- Avtorizacija, kjer lahko prejemnik preveri, ali je pošiljatelj pravi.
- Nezatajljivost, kjer pošiljatelj ne more zanikati podpisa in pošiljanja.
- Celovitost, kjer se zagotavlja, da sporočilo med prenosom ni bilo spremenjeno ...

Podpisovanje sporočil se ponavadi uporablja pri finančnih transakcijah, distribuciji programske opreme in podobnih primerih, kjer je pomembno, da se prepozna ponarejanje in prirejanje.

Preverjanje podpisa v primeru bitcoina poteka tako, da pošiljatelj transakcijo podpiše s svojim privatnim ključem in objavi svoj podpis na Bitcoin mrežo, kjer ga lahko potrdijo s pošiljateljevim javnim ključem.

Bitcoin podpisuje svoje transakcije z uporabo secp256k1 krivulj. Javni kluči so podani kot 04 ¡x¿ ¡y¿, kjer sta x in y 32 bitna big-endian cela števila, ki predstavljajo koordinate točke na krivulji ali v stisnjeni obliki kot ¡znak¿ ¡x¿, kjer je ¡znak¿ 0x02, če je y sod in 0x03, če je lih. Podpisi uporabljajo DER kodiranje, da zapakirajo r in s komponente v enotni tok bajtov. Podpis se izvede v funkciji CECKey()

```
1 // key.cpp
2 CECKey() {
3         pkey = EC_KEY_new_by_curve_name(NID_secp256k1);
4         assert(pkey != NULL);
5     }
```

Podobno kot vsi javni kriptografski sistemi Bitcoin ne podpisuje celotnega sporočila, saj bi to bilo preveč zahtevno. Namesto tega podpiše kriptografski hash sporočila. Ta se izračuna v funkciji SignatureHash.

```
1 // script.cpp
2 uint256 SignatureHash(CScript scriptCode, const CTransaction&
    txTo,
3                       unsigned int nIn, int nHashType)
4 {
```

```
5       // ...
6       // Wrapper to serialize only the necessary parts of the
        transaction being signed
7       CTransactionSignatureSerializer txTmp(txTo, scriptCode, nIn
        , nHashType);
8
9       // Serialize and hash
10      CHashWriter ss(SER_GETHASH, 0);
11      ss << txTmp << nHashType;
12      return ss.GetHash();
13  }
```

Razpršitvena funkcija

Hash ali razpršitvena funkcija je katerikoli algoritem, ki preslika podatke poljubne dolžine v podatke fiksne dolžine. Izhodni podatek se ponavadi imenuje hash, lahko pa tudi hash vrednost, hash koda ali hash vsota. V primeru bitcoina ta uporablja dvojno SHA-256 razpršitveno funkcijo, ki se izračuna v funkciji GetHash():

```
1   // hash.h
2   uint256 GetHash() {
3           uint256 hash1;
4           SHA256_Final((unsigned char*)&hash1, &ctx);
5           uint256 hash2;
6           SHA256((unsigned char*)&hash1, sizeof(hash1), (unsigned
        char*)&hash2);
7           return hash2;
8       }
```

Primer dvojnega SHA256 kodiranja niza "Pozdrav":

Pozdrav
574cdb27dff104270191f4ec5e3c453f9b75a9c0c140462fa25eb8d3e37c7da0

(first round of sha-256)
4a17b3e8b902da79e454d1b7551cac16c7a62eb1c9484d8cf580d3e593b78277
(second round of sha-256) [23]

Ko pa računamo hash Bitcoin naslova uporabimo SHA-256/RIPEMD-160 dvojno razpršitveno funkcijo. Bitcoin naslov je 160-bitni hash javnega/privatnega ECDSA para ključev. Z uporabo kriptografije javnega ključa se lahko podpiše podatke s privatnim ključem in kdorkoli, ki pozna javni ključ, lahko preveri ali je podpis veljaven.

Hash Bitcoin naslova se izračuna v funkciji Hash160():

```
1  // hash.h
2  template<typename T1>
3  inline uint160 Hash160(const T1 pbegin, const T1 pend)
4  {
5      static unsigned char pblank[1];
6      uint256 hash1;
7      SHA256((pbegin == pend ? pblank : (unsigned char*)&pbegin
       [0]), (pend - pbegin) * sizeof(pbegin[0]), (unsigned char*)
       &hash1);
8      uint160 hash2;
9      RIPEMD160((unsigned char*)&hash1, sizeof(hash1), (unsigned
       char*)&hash2);
10     return hash2;
11 }
```

Kodiranje naslova bitcoina z uporabo RIPEMD-160:

Pozdrav
574cdb27dff104270191f4ec5e3c453f9b75a9c0c140462fa25eb8d3e37c7da0
(first round is sha-256)
b14f21166800b1ad897d4e2ce86237dfe37f44a5
(z ripemd-160) [23]

2.2.4 Rudarjenje Bitcoinov

Da se ustvari distributiran žigosan strežnik v obliki P2P mreže, bitcoin uporablja podoben sistem kakor HashCash[21], vendar namesto časopisov in Usenet[22] objav uporablja interent. Delo, ki se izvaja na tem sistemu, se imenuje rudarjenje Bitcoinov.

Proces rudarjenja vključuje iskanje vrednosti, ki se začnejo s številko ničelnih bitov, in to po tem, ko se to vrednost dvakrat razprši. Medtem ko se delo, potrebno za iskanje teh številk, eksponentalno povečuje s številom potrebnih prvih nič bitov, se razpršitev z lahkoto preveri tako, da se izvede en krog dveh SHA-256 funkcij. Za žigosano Bitcoin omrežje se najde veljaven dokaz delovanja tako, da se povečuje nonce[23], dokler ni najdena vrednost, ki da razpršitvi bloka potrebno število vodilnih ničelnih bitov Ko je razpršitvena funkcija dosegla veljaven rezultat, se ta blok ne more spremeniti, brez da bi znova naredili vse delo. Ker se kasnejši zapisi oziroma bloki zapišejo po tem bloku, delo, potrebno za spremembo tega bloka vključuje tudi vse naknadne bloke.

Večinsko soglasje v Bitcoinu je predstavljeno v najdaljši verigi, za katero je bilo potrebno opraviti največ napora. Če večino računske moči nadzirajo iskrena vozlišča[24], bo glavna veriga rasla najhitreje in prehitela vse ostale verige. Da bi spremenil prejšni blok, bi napadalec moral znova narediti delo tega bloka, kakor tudi delo vseh blokov po njem. Nato bi moral še dohiteti in prehiteti delo, ki so ga v času, ko je napadalec znova ustvarjal blok, opravila iskrena vozlišča. Verjetnost, da počasnejši napadalec dohiti iskrena ogljišča, se zmanjšuje eksponentalno z vsakim na novo dodanim blokom.

Kot nadomestilo za povečanje strojne moči in različen interes poganjanja vozlišča skozi čas je težavnost odkritja pravilne razpršitve popravljena vsaka dva tedna. Če se bloki generirajo prehitro, se težavnost poveča. Tako je potrebnih več pravilnih razpršitev, da se najde blok in generira nove bit-

[21] HashCash je sistem za omejitev nezaželjene pošte in napadov zavrnitve storitve.
[22] Največja svetovna elektronska oglasna deska.
[23] Številka ali bit, ki se uporabi samo enkrat.
[24] Vozlišča, ki sodelujejo pri kreiranju blokov v glavni verigi.

coine. Bitcoin rudarstvo je konkurenčen podvig. Tak način rudarjenja bitcoinov je pripeljal do "oboroževalne tekme"med različnimi tehnologijami za računanje razpršilnih funkcij: navadni procesorji, najmočnejše grafične procesorske enote, FPGA[25] in ASIC[26]. Pri tem je vsaka naslednja tehnologija zmanjšala dobičkonosnost predhodne. ASIC se vgrajujejo v naprave, ki so namenjene izključno rudarjenju bitcoinov.

Računalniška zmogljivost je pogosto združena v centralni strežnik z namenom, da se zmanjša varianca prihodka rudarja. Samostojni rudarji morajo pogosto čakati dolga obdobja, da lahko potrdijo transakcijski blok in dobijo plačilo. Ko se rudarji združijo, vsi prisotni dobijo del bitcoinov, ko sodelujoči strežnik reši blok. To plačilo je sorazmerno z obsegom dela, ki ga je posamezni rudar prispeval za pomoč pri iskanju bloka.

Proces

Grob pregled procesa za rudarjenje bitcoinov je sledeč:

1. Nove transakcije se oddajo vsem vozliščem.
2. Vsako rudarsko vozlišče zbere nove transakcije v blok.
3. Vsako rudarsko vozlišče dela na potrjevanju svojega bloka.
4. Ko vozlišče najde dokaz dela, blok odda vsem vozliščem.
5. Nove bitcoine pridobi vozlišče, ki je našlo dokaz dela.
6. Vozlišča sprejmejo blok le, če so vse transakcije v njem veljavne in niso še porabljene.

[25]Field programmable array, je integrirano vezje, ki je narejeno tako, da se lahko nastavi po tem ko je proizvedeno (iz strani kupca ali oblikovalca).

[26]Application-specific integrated circuit, je integrirano vezje prilagojeno za točno določeno rabo (v primeru Bitcoin rudarjev za rudarjenje bitcoinov).

7. Vozlišča izražajo svoje sprejemanje bloka tako, da delajo na ustvarjanju novega bloka v verigi z uporabo razpršitve sprejetega bloka kot zadnje razpršitve.

Vozlišča so motivirana, da delajo na razširjanju najdaljše verige, saj v nasprotnem primeru tvegajo, da bo njihovo delo zapravljeno. Če dve vozlišči oddajata dve različni verziji naslednjega bloka hkrati, lahko naslednja vozlišča dobijo enega ali drugega kot prvi blok. V takem primeru delajo na prvem prejetem bloku, drugega pa shranijo v primeru, da postane daljši. Vez bo pretrgana, ko bo najden naslednji dokaz dela in bo ena veja blokov postala daljša. Vozlišča, ki so delala na drugi veji, se v takem primeru preklopijo na daljšo verigo.

Za oddajanje novih transakcij pa ni nujno, da dosežejo vsa vozlišča. V kolikor dosežejo večino vozlišč, se bodo transakcije zapisale v blok. Transakcije blokov so tudi tolerantne na padla sporočila. Če vozlišče ne prejme bloka, bo zahtevalo izgubljeni blok, ko prejme naslednji blok in tako ugotovilo, da je zgrešilo en blok.

Strojna oprema

Rudarjenje bitcoinov je bitka med vse hitrejšimi napravami, ki lahko obdelajo čedalje več hashov na sekundo in vse večji zahtevnosti, ki je potrebna, da se potrdi en blok.

Sprva se je rudarilo s CPE[27], vendar so se kmalu izkazali za prepočasne. Rudarji so posegli po grafičnih karticah, ki so bile veliko hitrejše. Toda s popularnostjo bitcoina je čedalje hitreje rasla tudi zahtevnost, saj je vse več ljudi rudarilo bitcoine. Da bi ostali tekmovalni, so rudarji povezali več grafičnih kartic skupaj in tako pridobili še večjo moč. Toda poraba električne energije, tako za poganjanje samih kartic, kakor tudi za hlajenje, je bila velika. Ker grafične kartice niso namenska tehnologija, je bil njihov izkoristek še vedno povprečen.

[27] centralna procesorska enota.

Rudarji so odgovor na porabo električne energije našli v FPGA čipih, ki so predstavljali le majhno pohitritev nasproti grafičnim karticam, vendar so porabili manj energije. Toda to je bilo le prehodno obdobje.

Februarja 2012 so na trg prišli prvi ASIC bitcoin rudarski stroji. Za razliko od FPGA sistemov, ASIC ni možno spreminjati. Toda za to svojo rigidnost ponudijo 100 krat večjo hitrost obdelovanja hashov, za to pa porabijo manj moči. Ko so začeli prvi ASIC stroji rudariti, so predstavljali tako velik del računske moči, kljub majhnemu številu, da so ostali načini rudarjenja kmalu postali neekonomični. Ker pa gre za strojno opremo, ki je izrecno namenjena rudarjenju bitcoinov, imajo mnogi to za začetek konca oboroževalne tekme [17]. Od tu se ne more trenutno iti nikamor naprej v velikih skokih.

Najmodernejši ASIC stroji, kot so AntMiner S2 (1,000,000 Mhash/s), Avalon3 (800,000 Mhash/s), HashFast Sierra (1,200,000 Mhash/s) in KnC Neptune (3,000,000 Mhash/s) so tako hitri, da naredijo zastarele že prve ASIC stroje (Avalon Batch 1 - 66,300 Mhash/s), v letu 2014 pa so napovedani še hitrejši ASIC stroji (npr. Minerscube 15 - 15,000,000 Mhash/s) [28].

Izbrati pravi stroj za rudarjenje postaja čedalje bolj riskantna naložba, saj se zaradi čedalje večje skupne moči potrjevanja novih blokov težavnost viša vse hitreje, kar pa ima lahko za posledico, da stroj, ki je bil kupljen le nekaj tednov nazaj, ne bo več ekonomsko zadovoljiv. To pa predstavlja problem, saj najnovejše namenske naprave za rudarjenje bitcoinov stanejo tisoč in več evrov.

Rudarjeni bitcoini

Po dogovoru se prva transakcija v bloku obravnava kot posebna transakcija, ki proizvede nove bitcoine, katerih lastnik je ustvarjalec bloka. To doda pobudo za vsa vozlišča, da podpirajo mrežo in zagotavlja način, da

[28] Podroben seznam se nahaja na `https://en.bitcoin.it/wiki/Mining_hardware_comparison`.

kovanci pridejo v obtok, saj ni nikakršnega centralnega organa, ki bi jih izdajal. Stalno in stabilno dodajanje novih kovancev je podobno rudarjem zlata, ki so s porabo sredstev zlato dodali v obtok. V tem primeru se porabljajo računska moč in elektrika. Pobuda je lahko tudi v obliki transakcijskih provizij. Če je izhodna vrednost transakcije manjša kot njena vhodna vrednost, je k pobudni vrednosti bloka v transakciji dodana razlika med vhodno in izhodno vrednostjo transakcije.

2.2.5 Poraba Lokalnih sredstev

Ko je zadnja transakcija kovancev pokopana pod dovolj bloki, se popolnoma porabljene transakcije, ki so bile pred njo, zavržejo z namenom, da se sprazni prostor na disku. Da se lahko to izvede, se razpršitve zapišejo v Merklovo drevo, kjer je v razpršitvi bloka zapisan samo koren drevesa. Stari bloki so lahko nato stisnjeni tako, da se odrežejo veje drevesa. Notranje razpršitve tako ne rabijo biti shranjene. Glava bloka brez transakcij je velika približno 80 bitov. Če vzamemo, da se novi bloki generirajo vsakih deset minut, to pomeni, da se celotna velikost vseh blokov povečuje s 4.2 MB na leto (80 bitov * 6 * 24 * 365 = 4.2 MB). Z računalniškimi sistemi, ki se v letu 2013 prodajajo v povprečju z 6GB RAM-a in Moorovim zakonom, ki predvideva trenutno rast RAM-a s 1.2 GB na leto, shranjevanje podatkov ne bo težava, tudi če morajo biti glave blokov shranjenhttp://images4.fanpop.com/image/photos/19900000/Joker-batman-arkham-city-19914338-1600-900.jpg

2.2.6 Preverjanje plačila

Bitcoin plačila je možno preveriti, ne da bi zaganjali vozlišče s celo mrežo. Uporabnik mora imeti le kopijo glav blokov najdaljše verige, ki se pridobijo tako, da se kliče poizvedbe, dokler ni jasno, da je bila pridobljena najdaljša veriga. Nato se pridobi Merklova veja, ki povezuje transakcijo z blokom, v katerem je žigosana. Transakcijo je možno preveriti le tako, da jo povežeš na mesto v verigi in tako dokažeš, da jo je mrežno vozlišče sprejelo. Kasneje

dodani bloki pa dodatno potrdijo, da jo je mreža sprejela.

Tako je preverjanje zanesljivo, dokler mrežo nadzorujejo iskrena vozlišča, vendar je bolj ranljivo, če mrežo prevzame napadalec. Čeprav lahko vozlišča sama preverijo transakcije, je ta preprosta metoda ranljiva na to, da lahko napadalec pretenta mrežo s svojimi lažnimi transakcijami, dokler premaguje mrežo.

Kot varovalka proti takemu vdoru se pošljejo opozorila po mrežnih vozliščih, ki so zaznale neveljaven blok. Ta opozorila pozivajo uporabnikovo programsko opremo, da prenese celoten blok in preveri opozorjene transakcije, da potrdi njihovo nekonsistenčnost.

2.3 Bitcoin kot valuta

2.3.1 Uporaba

Ker bitcoin sam po sebi ni praktično uporaben kot na primer les, se primarno uporablja kot hranilec vrednosti ali kot menjalno sredstvo.

Hranilec vrednosti je sredstvo, ki je lahko s predvidljivo uporabnostjo shranjeno in kasneje pridobljeno in zamenjano. Pogosto je namen shranjevanje v sredstvih, ki zagotavljajo stagnacijo oz. rast vrednosti v prihodnosti.

Najbolj pogosti hranilci vrednosti v modernih časih so denar, valuta ali blago, kot je npr. finančni kapital ali plemenite kovine.

Menjalno sredstvo pa je medij za izmenjavo dobrin. Včasih so se uporabljale plemenite kovine, dandanes pa je najbolj pogosto menjalno sredstvo fiat valuta[29].

Bitcoin kot hranilec vrednosti

Bitcoin je v zadnji četrtini leta 2013 doživel hitro rast vrednosti zaradi ugodnih razmer na trgu in prepoznave tako s strani držav [25] kakor tudi upo-

[29]Valuta, katere vrednost izhaja iz vladne regulacije ali zakona. Izhaja iz latinske besede fiat ("naj bo")

rabnikov [12]. Valuta je v obdobju od 30. oktobra do 30. novembra skočila iz 204,69 evra na 1.132,00 evra za en bitcoin, kar predstavlja 553.03-odstotno rast. Ta skok in podobni pred njim so bitcoin širši javnosti predstavili kot dobro sredstvo za hranjenje vrednosti, saj je na prvi pogled vrednost vedno rasla.

Slika 2.4: Rast vrednosti Bitcoina v obdobju od 30. 10. 2013 do 30 .11. 2013

Toda ravno ta nestabilnost trga, ki je omogočila tako veliko rast, je botrovala tudi posledičnemu padcu vrednosti. Ob izgubi podpore ene največjih centralnih bank na svetu [7] je vrednost bitcoina močno padla, nakar se je normalizirala v okolici 500 dolarjev za en bitcoin. Zaprtje menjalnice Mt. Gox z začetkom 7. februarja je znova pretreslo trge, ki so se ravno začeli stabilizirati.

Čeprav se ta obdobja rasti in padcev tradicionalno normalizirajo tako, da bitcoin obdrži več kakor pol vrednosti, ki jo je imel v času rasti, so potencialni vlagatelji zaskrbljeni prav zaradi teh velikih nihanj v ceni. Za potrebe hranjena vrednosti se od potencialnega hranilca vrednosti pričakuje stabilnost, ki pa je Bitcoin trenutno ne ponuja.

Bitcoin kot menjalno sredstvo - valuta

Čeprav se bitcoin čedalje bolj pojavlja kot legitimno menjalno sredstvo [30], se spopada z isto težavo, kakor v vlogi hranilne vrednosti.

Zaradi nestabilne vrednosti je trgovanje tvegano, saj se lahko vrednost iz dneva v dan spremeni, kar pa bi pomenilo izgubo na eni ali drugi strani menjave.

Izjema je trgovanje na črnem trgu, kjer se z bitcoini zaradi anonimne narave transakcij veliko trguje, saj je anonimnost cenjena veliko bolj kakor spreminjajoča se vrednost. Tako trgovanje omogoča varen in prikrit prenos sredstev med prodajalcem in kupcem. Ponavadi se trguje orožje in ilegalne vsebine, kot npr.: erotika, cigarete, umetnost, knjige ipd. Največji nelegalni promet predstavlja preprodaja drog [2].

Prav to trgovanje z nelegalno vsebino pa onemogoča priznavanje bitcoina kot valute s strani največjih ekonomij. Ker ne morejo regulirati njegove porabe in slediti denarju so, države soočene s težavami, ki jih predstavlja tako anonimno trgovanje.

Bitcoin v prihodnosti

Težavo pri uveljavi bitcoina kot valute predstavlja težavnost pri plačevanju vsakodnevnih stvari. Transakcije so sicer razmeroma preproste, ko pride do izmenjeve na spletu. Kupovanje na fizičnih lokacijah pa je zamuden proces. Uporabnik mora z mobilnim telefonom posneti QR kodo [31] ali poslati dolg bitcoin naslov preko spletne pošte. Plačevanje z debetnimi karticami, kot so Visa ali Mastercard, je veliko bolj preprosto.

V ta namen sedaj prihajajo prve debetne kartice [32], na katere se lahko nakazuje bitcoine. Predstavljajo nekakšen vmesni korak med tem, da se bitcoin jemlje le kot hranilca vrednosti v to, da se ga uporablja kot valuto.

[30] Seznam podjetji, ki sprejemajo bitcoine: https://en.bitcoin.it/wiki/Trade.

[31] Quick Response Code. Vrsta dvodemnzionalne barkode.

[32] Primer je Xapo (`https://xapo.com/in/campaign/debit/`) ali ANX (`http://debitcard.anxintl.com/`)

V primeru ANX gre za debetno kartico, na katero se nakaže bitcoine, plačuje pa s fiat valutami. Torej gre v osnovi še vedno za navadno debit kartico, le da se lahko na njo nakazuje bitcoine.

Xapo pa je po drugi strani predstavil uradno bitcoin debetno kartico. Transakcije se potrjujejo preko Xapota. Napoved je pri zagovornikih bitcoina bila sprejeta zelo dobro, vendar je kmalu prišlo do zapletov pri transakcijskih provizijah.[14]

Kar to predstavlja za prihodnost bitcoina je da se ga predstavi širšemu občinstvu in uveljavi kot alternativa fiat valutam pri vsakodnevni uporabi. Tako bi preko debetnih kartic ljudje spoznali in začeli zaupati Bitcoinu ter ga uporabljati, najprej morda posredno, nato pa neposredno.

2.3.2 Menjalnice

Nakup bitcoinov je možen brez posrednikov preko neposredne menjave med imetnikom bitcoinov in potencialnim kupcem. Toda večina trgovanja se izvaja predvsem na spletnih menjalnicah.

Obstajajo tržne menjalnice, kjer se nakupna naročila parirajo s prodajnimi naročili. Tak način trgovanja določa ceno bitcoina glede na sam trg. Primeri takih menjalnic so Mt. gox[33], Bitstamp, BTC-E, Bitfinex in BTC China [34].

Če storitev že v osnovi navaja ceno, potem tu ne gre za tržno menjalnico, temveč za menjalnico s fiksno ceno oz. gre za posrednika, ki kupuje in prodaja bitcoine. Taka menjalnica sama določi ceno in je veliko bolj rigidna kakor tržna menjalnica.

Tržne menjalnice delujejo podobno kakor banke. Uporabnik mora ustvariti račun in na njega nakazati bodisi fiat valuto ali bitcoine. Nato preko te menjalnice kupuje in prodaja svoje bitcoine. Vendar na ta način zaupa svoj denar menjalnici, ki s tem sredstvi razpolaga po svoje. Tak način trgovanja, ki temlji na zaupanju, pa je občutljiv na zlorabo, kar se je najbolj očitno po-

[33]V času nastajanja naloge je bil Mt. Gox zaprt.

[34]Poln seznam je dostopen na: `http://bitcoincharts.com/markets/`.

kazalo v primeru zaprtja menjalnice Mt. Gox. Menjalnica je izgubila veliko količino bitcoinov, ki jih je držala, in tako izgubila 744.408 bitcoinov, zaradi česar je šla v stečaj [27].

Tak način zlorabe zaupanja se je pokazal že pri finančnem zlomu iz leta 2008, ko so svetovne banke začele padati ena za drugo. Zaradi slabih posojil in neekonomičnega denarja so porabile več denarja, kot so ga imele na voljo. Ko pa so njihovi upniki in uporabniki zahtevali svoj denar nazaj, je ta denar obstajal samo še na papirju.

Možnost takih zlorab je pri trgovanju z bitcoini zaradi te neregularnosti še na višji ravni. Dokler ne bodo pravila jasna in regulacija trga redna, se znajo zgodbe, kot je Mt. Gox, ponoviti.

Poglavje 3

Primerjava med fiat valutami in bitcoinom

3.1 Razširjenost

Razširjenost valute je njena baza uporabnikov. To so lahko primarni uporabniki, recimo državljani ZDA za dolar, ali sekundarni (valuta se uporablja poleg primarne valute). Večja kot je baza uporabnikov, bolj je valuta priznana in se z njo več trguje, saj je veliko več ljudi pripravljenih trgovati v tej valuti. Posledično je na voljo več dobrin ali storitev, kar naknadno povečuje bazo uporabnikov.

Klasične valute so razširjene po celotnem svetu, saj ima vsaka država ali svojo valuto ali pa valuto monetarne unije (npr. Evroobmočje). Te valute so navadno omejene na meje države, čeprav določene države, ki imajo eno uradno valuto, sprejemajo tudi drugo valuto (evro na Hrvaškem). Menjavo med valutami nadzorujejo banke z javno objavljenimi valutnimi tečaji, ki se spreminjajo glede na ekonomske razmere države, na katero je valuta vezana in na povpraševanje po sami valuti.

Bitcoin je v takem pogledu geografsko bolj razširjen oziroma globalen. Ker ni podvržen nikakršni centralni agenciji, ki bi ga regulirala, je njegova vrednost enaka po celem svetu, vrednost v primerjavi z ostalimi valutami pa

se računa izključno na povpraševanju in trgovanju z bitcoinom. Za razliko od konvencionalnih valut pa je število uporabnikov bitcoina majhno, saj je valuta še mlada, uporabljajo pa jo le ljudje, ki so zainteresirani zanjo (za razliko od navadnih valut, kjer je posameznik primoran trgovati v lokalni valuti). Zaradi svoje anonimne narave pa točno število bitcoin uporabnikov ni znano. Vse številke pa so le ugibanja.

3.2 Stabilnost sistema

Stabilnost sistema pomeni, koliko vrednost valute niha in kako je odporna na finančne šoke. Bolj kot je nestabilna, manjša je verjetnost, da bi jo ljudje dejansko uporabljali za trgovanje, kar vodi v dve smeri:

1. Lahko pride do hiperinflacije, ko valuta izgublja vrednost. To ima za posledico, da se z isto količino denarja lahko kupuje čedalje manj oziroma je dobrina ali storitev čedalje dražja. Na koncu je vrednost valute lahko tako majhna, da je njena uporabnost ničelna.

2. Valuta lahko postane naložba, saj ljudje pričakujejo, da bo njena vrednost še naprej rastla. Z valuto se ne trguje več, valuto pa se kupuje izključno kot naložbo.

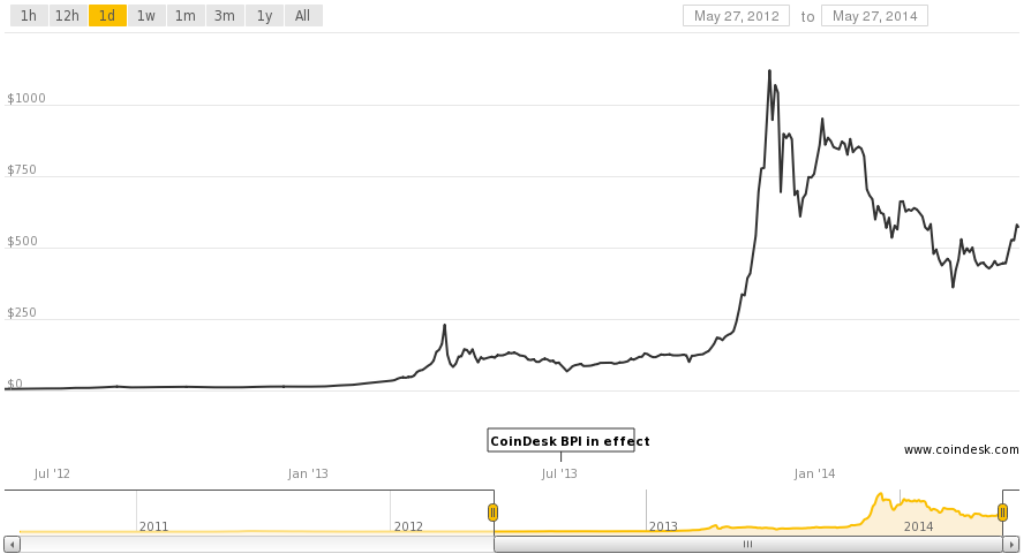
Ker se bitcoin vrednost v večini računa glede na dolar, bomo za vse primerjave uporabili dolar.

3.2.1 Bitcoin

Kljub temu, da bitcoinu vrednost historično narašča, je močno odvisen od finančnih razmer ter drugih dejavnikov (Zaprtje SilkRoada iz strani FBI-ja). Zaradi svoje neregularne vendar precejšne rasti, zaradi česar mu vrednost niha med več deset odstotki, je bitcoin trenutno še vedno nestabilna valuta.

Iz slike 3.2 je razvidno, da je cena rasla razmeroma enakomerno do februarja 2013, ko je začela eksponentalno naraščati, preden je dosegla svoj vrh 9.

4. 2013, ko je narasla na 230 dolarjev za en bitcoin. Nato je strmo padla na več kot polovico svoje prejšne vrednosti, sedaj pa niha v okolici 100 dolarjev za 1 bitcoin



Slika 3.1: Volatilnost Bitcoina

3.2.2 Primerjava z lokalno valuto

V Sloveniji je lokalna valuta evro, saj Slovenija spada v evroobmočje. Njegova stabilnost je bila močno zamajana v zadnjih letih zaradi globalne krize in predvsem krize evroobmočja, ko je veliko bank in držav zašlo v dolgove, ki jih niso bile možne odplačati. Kljub temu cena evra nasproti bitcoinu ne niha za več več deset dolarjev, vendar med 1.3 in 1.5 dolarja za en evro. Taka stabilnost omogoča, da se z evri lahko še naprej trguje tako na lokalni ravni, kakor tudi na globalni. Evro je tako druga največja rezervna valuta. Takoj za dolarjem pa je tudi v količini trgovanja, ki se z njim izvede.

Slika 3.2: Nihanje cene Evra v primerjavi z USD

3.2.3 Primerjava z nadomestno valuto

Nadomestna valuta je katerakoli valuta, ki se uporablja kot alternativa dominantnemu valutnemu sistemu (kot je recimo evro). V to skupino spada tudi bitcoin, kar pomeni, da je celotna skupina teh alternativnih valut precej podobna po stabilnosti sistema, kar pomeni, da je v veliki meri odvisna od trga in omejena na nek manjši del prebivalstva, ponavadi s specifičnim namenom.

Primerjava je težavna, saj je stabilnost sistema neposredno vezan na trg, ki ga valuta pokriva. Ker pa so ti trgi precej manjši od trgov navadnih valut, se finančni šoki ne blažijo tako močno, kar ima za posledico, da je zaupanje veliko manjše in ljudje raje migrirajo svoja sredstva drugam.

3.3 Zaupanje v valuto

Zaupanje v valuto pomeni, kako so ljudje pripravljeni sprejeti valuto in z njo trgovati. Močno je odvisno od stabilnosti valute, saj nihanje vrednosti zmanjšuje zaupanje ljudi v to valuto. Če vrednost valute močno niha, je količina denarja lahko vredna veliko manj ali več naslednji dan. To ima za posledico, da ljudje valuto shranjujejo, saj upajo, da bo njena vrednost še narasla ali pa nočejo trgovati z njo, saj obstaja možnost, da bo njena vrednost padla. To ima občutne posledice na uporabo in razširjenost valute.

3.3.1 Fiat valute

Standardne oz. fiat valute bazirajo svoje zaupanje na tem, da jih zagotavljajo vlade držav, ki jih izdajajo. Ta garancija pomeni, da vlada zagotavlja, da je ta denar dejansko vreden toliko kot pravi. Pred tem je to pomenilo, da si lahko zamenjal denar za zlato, srebro oziroma druge vrsto dobrine, ki je veljala kot zagotovilo za vrednost.

To zagotovilo ima za posledico, da je valuta tako stabilna, kakor je stabilno gospodarstvo države oziroma monetarne unije. V primeru evra je zaupanje v valuto dobro, saj je gospodarstvo v evroobmočju najmočnejše na svetu[1].

3.3.2 Bitcoin

Zaupanje v bitcoin ni veliko, saj je valuta še mlada, njena stabilnost pa majhna. Pot do prepoznave in zaupanja v bitcoin pa otežuje tudi sam princip delovanja te valute. Bitcoin namreč ni vezan na nobeno centralno banko, njegovo vrednost pa zagotavljajo le pravila trga in vloženega dela. Tak sistem v osnovi sledi pravilom prostega trga, toda posledično trpi za nihanji v ceni. V primeru, da pride do pretresa trga, na katerem se trguje primarno z bitcoini, ni nobenih zagotovil, da bo vrednost valute ostala razmeroma ista.

Trenutno se pogosto nakup bitcoinov jemlje kot naložbo v prihodnost. Vrednost zagotavlja predvsem njegova noviteta, redkost in pripravljenost uporabnikov, da trgujejo z njim. Trenutno se v veliki meri trguje špekulativno. Uporabniki jo prodajajo, ker je vrednost na novem vrhuncu, drugi uporabniki pa kupujejo, ker pričakujejo še večjo rast. Tak odnos in nihanje v ceni odvrača poslovne uporabnike in potencialne stranke in zmanjšuje zaupanje v valuto.

[1] V letu 2012, je bdp Evropske unije znašal 16,673,333 miljard USD [24]

3.4 Varnost transakcij

Ena od poglavitnih lastnosti trgovanja je varnost. Ko se izvede transakcija med dvema strankama, je ključnega pomena, da dobrine, tako materialne kakor denarne, varno zamenjajo roke. V nasprotnem primeru vsaj ena od strank ne bo voljna izvajati teh transakcij.

Ko pride do izmenjave materialne dobrine ali storitve, se trg nadzoruje sam. Če stranka kupi dobrino, le-ta pa je v neustreznem stanju, bo ta stranka prenehala kupovati pri tem ponudniku in raje izbrala drugega. Hkrati pa bo svoje izkušnje posredovala drugim potencialnim strankam, ki se zaradi takih informacij morda ne bodo odločile za nakup. Seveda pa obstajajo tudi izjeme, ko ima ponudnik monopol nad trgom.

Denar teh težav nima. Valuta mora biti v ustreznem stanju, sicer ni denar oziroma ne nosi nobene vrednosti. Pri menjavi dobrin za denar in transakcijah je najvažnejša varnost same transakcije. Kar pomeni, da denar varno zamenja roke in se v procesu ne izgubi ali izgubi svojo vrednost.

Denarne transakcije so se razvile kot naraven odgovor nepraktičnosti materialne menjave. V samem začetku je menjava potekala tako, da sta si obe strani izmenjali dobrine osebno ali preko posrednika. Varnost transakcije je bila v takem primeru odvisna od obeh udeležencev transakcije ter zunanjih dejavnikov. Z napredkom družbe in povečanjem količine transakcij so se oblikovali novi načini menjave denarja, kar je privedlo do sedanjih oblik transakcij. Dandanes se transakcije izvajajo neposredno do modema, kar pomeni, da internet ni vpleten v samo transakcijo, ali pa uporabljajo najnovejše kriptografske algoritme. Poleg tega je za izvajanje transakcij pogosto potrebno geslo ali PIN koda.

3.4.1 Varnost transakcij pri trgovanju z Bitcoini

Bitcoin transakcije se izvedejo takoj, nakar se transakcijo preveri na P2P mreži uporabnikov bitcoinov. Več kot je pozitivnih potrdil iz mreže, bolj je verjetno, da je bila transakcija veljavna in zaključena.

Transakcije se ne more razveljaviti z izjemo druge prostovoljne transakcije v enakem znesku iz nasprotne strani. Za razliko lahko pri kupovanju s kreditno kartico prodajalec izgubi denar. To predstavlja težavo, če kupec, ki kupuje z bitcoini, ne dobi kupljenega blaga ali storitve. Države in njihova sodišča so načeloma nenaklonjena uporabnikom bitcoinov, ker valuta ni regulirana in obdavčena. Iz tega razloga je trgovanje z bitcoini priporočljivo samo s preverjenimi prodajalci ali preko uporabe depozitne storitve[2]

Februarja 2014 se je odkrila napaka v Bitcoin sistemu, povezana s transakcijami. Napaka je bila bolj podobna DOS[3] napadu kakor neposrednemu napadu na sredstva. Napadalec je lahko spremenil identifikator oziroma hash transakcije. Tak spremenjen hash ne vpliva na destinacijo ali osnovno vrednost transakcije, vendar sredstva niso varna za sprejem, dokler se transakcija ne potrdi, saj se hashi zanašajo na hashe iz prejšnih transakcij in so lahko spremenjeni, dokler niso potrjeni. Uporabniki bitcoinov lahko tako vidijo svoje transakcije vezane v nepotrjenih transakcijah kar onemogoča menjavo [4].

3.5 Nadzor nad transakcijami

Ljudje smo se združili v skupnosti z namenom, da nam skupnost omogoča lažje in boljše preživetje. Za uspešno delovanje skupnosti potrebujemo organizirano obliko skupnosti, ki se je sčasoma oblikovala v države. Le-te se sicer lahko delijo še na manjše dele (pokrajine, občine ipd.), vse pa potrebujejo za delovanje sredstva. Zato se že od nekdaj pobirajo dajatve. Sprva sicer kot plen pri osvojitvah oz. prisilno s pomočjo profesionalnih pobiralcev davkov, danes pa je to običajno na precej višjem nivoju kot prostovoljna privolitev davkoplačevalcev.

Vendar pri tem prihaja do težav, ker smo ljudje v osnovi razdvojena bitja, ki po eni strani želimo:

[2]Depozitna storitev hrani denar kupca, dokler ne dobi potrdilo o prejemu blaga.
[3]Denial of Service - zavrnitev storitve.

- Iz povsem evolucijskega razloga prenašati svoje gene na svoje potomce, kar iz nas dela egoistične posameznike.

- Po drugi strani iz razlogov preživetja iščemo socialno zaščito v sklopu drugih ljudi, kar nam je ob dvigu inteligence iz mnogih razlogov (za katere se znanost še dandanes ni povsem enoznačno opredelila) omogočilo nadvlado nad drugimi bitji.

Zavedanje o pomenu prispevanja v skupno blagajno je zato lahko pri mnogih posameznikih vprašljivo in se kaže kot izogibanje plačilu dogovorjenih (ponavadi preko parlamentarne procedure) dajatev. Zato morajo državni organi, ki so zadolženi za pobiranje dajatev in nadzor nad izvajanjem dogovorjenih pravil, ustrezno upravljati davčna tveganja (namerna in nenamerna izogibanja plačil dajatev).

Po drugi strani so nekatere dejavnosti prepovedane (npr.: kriminal, prodaja »belega blaga«, mamila, lahko tudi alkohol ipd.), kar sicer ne pomeni, da niso obdavčene (davke se pobira od legalne in nelegalne dejavnosti ...). Zato je ta denar »umazan« in ga kriminalne združbe želijo "oprati".

Do sedaj se je denar škrival"v davčne oaze in to na različne načine kot npr.:

- s pomočjo prenakazovanj (pogosto gre tu za »veriženje« preko različnih računov, da se tako izgubi sled) v države, kjer je zagotovljena bančna tajnost (npr.: Švica, Luxemburg, Bahami ipd.),

- z ustanavljanjem podružnic v davčnih oazah, kjer so nižje (ali celo ničelne) davčne ali carinske stopnje. Pri tem tu ne gre samo za države. Lahko so to samo posamezna območja, kjer zaradi različnih razlogov (ponavadi gre za t. i. "pasivna področja", kot npr.: Livingno v Italiji, Delaware v ZDA ali Kanalski otoki v Združenem kraljestvu ipd.) uvajajo davčne oaze.

Po drugi strani se preko kriminala pridobljeni denar »opere« preko legalne dejavnosti. Najbolj znano je tu gradbeništvo, kjer se z investicijami pogosto

ukvarjajo kriminalne združbe (npr. t. i. mafijske združbe v Italiji, Aziji ipd.), veliko se ga opere v igralništvu in storitveni dejavnosti (gostilne, kavarne, ipd.) [11].

Zato se davčne in carinske uprave trudijo odkrivati davčne in carinske utaje na različne načine. Pri tem se tudi vlade trudijo s poenotenjem carinskega in davčnega sistema (postopno odpravljanje davčnih oaz[4]) ter s pritiski na posamezne države, da odpravijo bančno tajnost. Zelo znan je primer pritisk ameriške federalne davčne uprave na Švico, s katero se je dogovorila za pavšalno odškodnino švicarskih bank, odstranitev davčne tajnosti v Avstriji (kar je pomembno tudi za naše državljane, ki so denar nalagali v avstrijske banke) ipd.

Kaj je ključna ideja pri nadzoru transakcij? Nobena transakcija nad določenim zneskom ne sme biti izvedena, če ni s tem seznanjen tudi ustrezen državni organ. Pri nas so to Urad za preprečevanje denarja ter Davčna in Carinska uprava, pri poslovanju z javnim sektorjem pa tudi vse transakcije nadzoruje Komisija za preprečevanje korupcije. Ob tem je zelo pomembno, da morajo biti javljene vse transakcije znotraj EU[5] in med državami, s katerimi so podpisani posebni sporazumi o izogibanju dvojnega obdavčevanja.

3.5.1 Davčni riziko in pranje denarja pri poslovanju z Bitcoini

V članku Are Cryptocurrencies 'Super' Tax Havens [19] se avtor Omri Y. Marian sprašuje, ali lahko kriptovalute zamenjajo standardne oblike davčnih oaz. Trdi, da je tak izzid pričakovan v prihodnosti zaradi dveh razlogov. Prvi

[4]Tu je zelo aktivna tudi EU.

[5]Tu gre pri bankah za samodejno prijavljanje obresti na bančnih računih in vseh drugih davščin (DDV, davek od dobička ipd.) preko enotnega VIAS sistema. Po drugi strani pa so dolžni na zahtevo ustreznih državnih nadzornih organov poročati o posameznih transakcijah. S tem se poskuša zagotoviti preprečitev izogibanja davčnih obveznosti in pranje denarja (denar, pri katerem je utajen davek, je tudi "umazan denar"in ga seveda utajevalci želijo čim prej "oprati").

je vse večja popularnost kriptovalut, drugi razlog pa je proces transformacije finančnih posrednikov v agente, ki služijo davčnim organom [19].

Kriptovalute imajo enake karakteristike kot davčne oaze (predvsem plačila niso subjekt obdavčitev, anonimnost davkoplačevalcev pa se ohrani), niso pa odvisne od obstoja finančnih posrednikov. Zaradi te prednosti imajo kriptovalute potencial, da porazijo dosedanje uspehe in dosežke vlad v boju proti utaji davkov. Avtor prav tako trdi, da so vlade sicer bitcoinu in ostalim kriptovalutam namenile nekaj pozornosti, vendar do sedaj nisu uspele identificirati akutnost te potencialne težave [19].

Pranje denarja pa je malce drugačno. Ker se vse transakcije zapisujejo v javno knjigo, imenovano blockchain, se lahko vsako transakcijo izsledi nazaj od konca do začetka, kjer se lahko uporabnika identificira glede na naslov, iz katerega so bila sredstva poslana.

Tradicionalna rešitev, ko se "umazan"denar preko transakcij pridruži "čistemu"je za pranje denarja tukaj še posebej pomembna. Tako se preko velikega števila transakcij ustvari žmedo", ki zakrije sledi in oteži sledenje denarju. Tak način pranja denarja pa zahteva, da se transakcije izvajajo preko nekega posrednika, ki transakcije pomeša med sabo.

Na tak način deluje DarkWallet. To je denarnica, ki zagotavlja anonimnost, njen integralni del pa je tudi pranje denarja. Glavni del te denarnice je funkcionalnost CoinJoin, ki naključno izbere dva uporabnika, ki približno isti čas plačujeta, ter njuni transakciji združi v eno kriptirano transakcijo. Tako ni mogoče točno izslediti, iz kje je denar prišel, saj se ob vsaki nadaljni transakciji verjetnost, da je denar res prišel iz naslova, ki ga iščemo, niža z številom transakcij, ki so se izvedle od originalne transakcije. Poleg tega se poslužuje še t. i. Shadow Addressov, ki dodatno varujejo zasebnost uporabnikov. Uporabnik generira ta senčni naslov in ga objavi na spletu kot naslov, na katerega hoče dobivati sredstva. Ko nek drug uporabnik pošlje bitcoine na ta naslov, jih DarkWallet preusmeri na drug naslov, ki predstavlja naključno enkripcijo senčnega naslova. Prvi uporabnik nato z DarkWallet poskenira blockchain iskajoč naslov, ki ga je možno dekriptirati s skritim ključem, ki

ga ima od generacije senčnega naslova, najde plačilo in ga prevzame.

Poglavje 4

Zaključek

Od vsega začetka civilizacije ljudje trgujemo med sabo. In kakor se je razvijala družba in tehnologija skozi čas, se je razvijalo trgovanje. Od osnovne blagovne menjave in lokalnega trga do digitalnih valut in resnično globalnega trga, trgovanje se razvija in evolucira skupaj z nami.

Globalno tržišče, ki je prišlo v ospredje predvsem s prodorom interneta, pa čedalje bolj teži k enotnemu plačilnemu sistemu, ki je neodvisen od lokalnih zakonov ali omejitev. Bitcoin je to svobodo ponujal, prav tako pa je prišel v času enega največjih finančnih zlomov zadnjih desetletij. Zaupanje v fiat valute in finančne inštitucije je padlo, ljudje pa so iskali alternative tem trgom in inštitucijam, ki so jih imeli za koruptirane.

Sprva valuta tehnoloških zanesenjakov, Bitcoin svojo strmo rast dolguje predvsem razmeram na trgu, ki je bil pripravljen sprejeti nekaj povsem novega. Vendar ta uspeh ni bil brez posledic. Število uporabnikov, ki je uporabljalo bitcoin, se je iz dneva v dan večalo, odpirale so se nove menjalnice, vse več ljudi je vzemalo to mlado valuto kot naložbo zaradi volatilne vrednosti, pod drobnogled pa so jo začele vzemati svetovne vlade.

Zaradi svoje decentraliziranosti je bitcoin močno odvisen od razmer na trgu, saj ga ne podpira nobena vlada ali ekonomija. To ga iz stališča stabilnosti naredi bolj podobnega vrednostim papirjem, kar pa ni primerno za valuto, ki zahteva relativno stabilnost.

Bitcoin najverjetneje ni valuta prihodnosti, je pa najbrž korak v pravo smer. Prava digitalna valuta bo poleg lastnosti, ki jih ima Bitcoin potrebovala še blažilec, ki bo vpil nepričakovane spremembe na trgu. Bodisi bo šlo za globalno vlado, ki bo uporabljala enako valuto bodisi bo šlo za kompleksen algoritem, ki bo efektivno blažil nihanja na trgu. Brez tega blažilca bodo te decentralizirane valute ostale le domena avanturističnih vlagateljev in tehnoloških zanesenjakov.

Literatura

[1] I. S. Friedberg A. L. Friedberg. *Gold Coins of the World: From Ancient Times to the Present : an Illustrated Standard Catalog With Valuations*. Coin & Currency Institute, 2009.

[2] James Ball. Silk road: the online drug marketplace that officials seem powerless to stop. `http://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace`. Pridobljeno: 21. 4. 2014.

[3] Bitcoin. `http://en.wikipedia.org/wiki/Bitcoin`. Pridobljeno: 30. 9. 2013.

[4] Danny Bradbury. What the 'bitcoin bug' means: A guide to transaction malleability. `http://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/`. Pridobljeno: 30. 7. 2014.

[5] Timothy Carmody. Money 3.0: How bitcoins may change the global economy. `http://news.nationalgeographic.com/news/2013/10/131014-bitcoins-silk-road-virtual-currencies-internet-money/`. Pridobljeno: 27. 10. 2013.

[6] Certicom Research. *SEC 2: Recommended Elliptic Curve Domain Parameters*, La Baule, France: Suvisoft, 2000.

[7] Alistair Charlton. Chinese ban causes bitcoin value to crash 50 `http://www.ibtimes.co.uk/`

chinese-ban-causes-bitcoin-value-crash-50-1429447. Pridobljeno: 21. 4. 2014.

[8] David J. Cheal. *The Gift Economy*. Routledge, 1988.

[9] Jacques G. Constant. *De geschiedenis van het geld*. Pampus, 1992.

[10] N. H. Demand. *The Mediterranean Context of Early Greek History*. John Wiley & Son, 2011.

[11] Frances DEmilio. Dozens of pizzerias, cafes seized in mafia money-laundering raid in italy. http://www.thestar.com/news/world/2014/01/22/dozens_of_pizzerias_cafes_seized_in_mafia_moneylaundering_raid_in_italy.html. Pridobljeno: 3. 5. 2014.

[12] Chao Deng. Bitcoin market gets a lift from china. http://online.wsj.com/news/articles/SB10001424052702303997604579237913301162066. Pridobljeno: 16. 4. 2014.

[13] F. W. Fairholt F. W. Madden. *History of Jewish coinage, and of money in the Old and New Testament*. B. Quaritch, 1864.

[14] Nermin Hajdarbegovic. Xapo responds to backlash over bitcoin debit card fees. http://www.coindesk.com/xapo-faces-online-backlash-debit-card-fees/. Pridobljeno: 19. 8. 2014.

[15] D. Kinley. *Money: A Study of the Theory of the Medium of Exchange*. Simon Publications LLC, 2003.

[16] S. N. Kramer. *History Begins at Sumer: Thirty-Nine Firsts in Recorded History*. University of Pennsylvania Press, 1981.

[17] Eric Limer. Digital drills: The monster machines that mine bitcoin. http://gizmodo.com/5994446/

digital-drills-the-monster-machines-that-mine-bitcoin.
Pridobljeno: 22. 7. 2014.

[18] E. Miller M. M. Postan. *The Cambridge Economic History of Europe: Trade and industry in the Middle Ages*. Cambridge University Press, 1987.

[19] Omri Y. Marian. Are cryptocurrencies 'super' tax havens? *Michigan Law Review First Impressions*, 112:38–, 2013.

[20] Sergii Moshenskyi. *History of the weksel: Bill of exchange and promissory note*. Cambridge University Press, 2008.

[21] Marco Polo. *The Travels of Marco Polo, a Venetian, in the Thirteenth Century: Being a Description, by that Early Traveller, of Remarkable Places and Things, in the Eastern Parts of the World*. William Marsden, 1818.

[22] Protocol of bitcoin.
http://en.wikipedia.org/wiki/Protocol_of_Bitcoin.
Pridobljeno: 12. 10. 2013.

[23] Protocol specification.
https://en.bitcoin.it/wiki/Protocol_specification.
Pridobljeno: 12. 10. 2013.

[24] Report for selected country groups and subjects.
http://www.imf.org/external/pubs/ft/weo/2013/02/weodata/weorept.aspx?pr.x=33&pr.y=11&sy=2012&ey=2012&scsm=1&ssd=1&sort=country&ds=.&br=1&c=001%2C998&s=NGDPD&grp=1&a=1.
Pridobljeno: 8.10.2013.

[25] Dominic Rushe. Bitcoin hits 700 dollars high as senate stages hearing on virtual currency.
http://www.theguardian.com/technology/2013/nov/18/

bitcoin-risks-rewards-senate-hearing-virtual-currency. Pridobljeno: 16. 4. 2014.

[26] Josh Sturtevant. A brief history of digital currencies. http://blawgconomics.blogspot.com/2012/10/a-brief-history-of-digital-currencies.html. Pridobljeno: 30. 8. 2013.

[27] Rob Wile. Bitcoin exchange mtgox disappears. http://www.businessinsider.com/reports-mtgox-halts-all-trading-2014-2. Pridobljeno: 24. 4. 2014.