UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA SISTEMA BITCOIN IN ALTERNATIVNIH MOŽNOSTI UPORABE BITCOIN TEHNOLOGIJE NA FINANČNEM PODROČJU

Ljubljana, maj 2016 DEJAN MEKIĆ

IZJAVA O AVTORSTVU

Spodaj podpisani Dejan Mekić, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor magistrskega dela z naslovom Analiza sistema Bitcoin in alternativnih možnosti uporabe Bitcoin tehnologije na finančnem področju, pripravljenega v sodelovanju s svetovalcem prof. dr. Matejem Marinčem.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega magistrskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 17. maja 2016 Podpis avtorja: _____

KAZALO

UVOD **1**
1 ANALIZA SISTEMA BITCOIN **4**
1.1 Procesi/Dogodki, ki so pripeljali do razvoja Bitcoina 4
1.1.1 Zgodovina prvih poskusov vzpostavitve kriptografskih virtualnih valut 4
1.1.2 Začetki Bitcoina 5
1.2 Sistem Bitcoin 6
1.2.1 Principi, na katerih temelji tehnologija sistema Bitcoin 6
1.2.1.1 Kriptografija 7
1.2.1.2 Zgoščevalna funkcija in zgoščena vrednost 11
1.2.1.3 Merklovo drevo 12
1.2.1.4 Omrežje vsak z vsakim 13
1.2.1.5 Odprtokodnost 14
1.2.2 Omrežje Bitcoin 14
1.2.3 Ključi, naslovi in denarnice 16
1.2.4 Rudarjenje 17
1.2.5 Veriga blokov 20
1.2.6 Transakcije 25
2 BITCOIN KOT VALUTA **29**
2.1 Definicija in sheme virtualnih in kriptografskih valut 29
2.2 Funkcije bitcoina kot valute 32
2.2.1 Menjalni posrednik 32
2.2.2 Obračunska enota 36
2.2.3 Hranilec vrednosti 39
2.3 Načini pridobitve bitcoina 40
2.4 Vrste denarnic 42
2.5 Ekonomski vidik 43
2.5.1 Temelji bitcoina v ekonomski teoriji in deflacija 43
2.5.2 Rast stroškov rudarjenja 45
2.5.3 Problem dolgoročnega vzdrževanja nizkih ravni provizij 47
2.6 Zakonodajnopravni vidik 48
2.7 Uporabnost bitcoina 50
2.8 Prednosti in slabosti bitcoina 52
3 SISTEM BITCOIN V SLOVENIJI **53**

3.1 Davčna obravnava bitcoina 53
3.2 Podjetja, ki se ukvarjajo s tehnologijo Bitcoin 55
4 ALTERNATIVNA UPORABA TEHNOLOGIJE BITCOIN NA FINANČNEM PODROČJU 55
4.1 Alternative dokazu o vloženem delu 56
4.2 Kategorije kriptotehnologije 57
4.2.1 Valute 58
4.2.2 Registri sredstev 59
4.2.2.1 Primer registra sredstev 60
4.2.3 Nabori aplikacij 61
4.2.3.1 Primer nabora aplikacij 62
4.2.4 Tehnologija, osredinjena na sredstva 63
4.2.4.1 Menjava valut in nakazovanje sredstev v tujino 63
4.2.4.2 Izvajanje plačil v realnem času 64
4.2.4.3 Izmenjava dokumentarnega gradiva 65
4.2.4.4 Servisiranje sredstev 65
4.2.4.5 Primer tehnologije, osredinjene na sredstva 66
4.3 Različice verige blokov 68
4.4 Trenutno stanje na finančnem področju in izzivi za prihodnost 69
SKLEP 71
LITERATURA IN VIRI 74

KAZALO SLIK

Slika 1: Simetrična kriptografija 7
Slika 2: Kriptografija javnega ključa 8
Slika 3: Napad s posrednikom 9
Slika 4: Proces digitalnega podpisovanja 10
Slika 5: Merklovo drevo 12
Slika 6: Stopnje centralizacije/decentralizacije omrežij 13
Slika 7: Funkcionalnosti deležnikov Bitcoin 15
Slika 8: Razmerje med zasebnim in javnim ključem ter naslovom Bitcoin 16
Slika 9: Primer verige blokov 22
Slika 10: Primer začasne veje blokov v verigi 23
Slika 11: Primer transakcije Bitcoin 26
Slika 12: Podpisovanje transakcij v omrežju Bitcoin 28
Slika 13: Dnevno število transakcij bitcoin med 1. 1. 2010 in 31. 1. 2016 35
Slika 14: Prikaz cene bitcoina v USD med 1. 1. 2011 in 31. 1. 2016 37
Slika 15: Povprečno število transakcij v bloku med 1. 1. 2010 in 31. 1. 2016 45
Slika 16: Hitrost zgoščevanja med 1. 1. 2010 in 31. 1. 2016 46

Slika 17: Skupni dnevni prihodek rudarjev v bitcoinih na podlagi provizij med 1. 1. 2011 in 31. 1. 2016 47
Slika 18: Kategorije kriptotehnologij s podanimi primeri 58
Slika 19: Tržna kapitalizacija kriptografskih valut v USD na 31. 1. 2016 59

KAZALO TABEL

Tabela 1: Prikaz zgoščenih vrednosti za kriptografsko zgoščevalno funkcijo SHA-256 11
Tabela 2: Struktura bloka 20
Tabela 3: Struktura glave bloka 20
Tabela 4: Struktura transakcije 25
Tabela 5: Matrika denarja 30

UVOD

Večina današnjih valut (ki predstavljajo izraz za denarno enoto neke države oziroma območja) sodi k valutam fiat[1]. Valute fiat (na primer evro, ameriški dolar, ruski rubelj …) izdajo določene oblasti in same po sebi nimajo notranje vrednosti (angl. *intrinsic value*). To pomeni, da njihova vrednost ni povezana z vrednostjo neke druge dragocene stvari, kot je na primer zlata. Valute fiat so posledično sprejete izključno zato, ker jih je oblast predpisala za zakonito plačilno sredstvo (angl. *legal tender*), kar pomeni, da se denarna vrednost z izročitvijo valute fiat lahko vedno izpolni.

Pretekle izkušnje so pokazale, da vodenje denarne politike ni dobro izpostaviti političnemu vplivu, saj lahko v tem primeru denarna politika postane namenjena reševanju kratkoročnih finančnih problemov. Kratkoročni finančni problemi se običajno rešujejo s prekomernim izdajanjem valute, s čimer pa se ta razvrednoti in se s tem vanjo posledično izgubi zaupanje (Franco, 2015, str. 5). Vodenje denarne politike je zato običajno zaupano centralni banki. Ena izmed njenih glavnih nalog je zagotavljanje stabilnosti cen, kar posledično podpira tudi gospodarsko rast. S tem sta izdajanje in nadzor denarja v obtoku izključno v domeni centralne banke, kar pomeni, da sta centralizirana. Ker je vrednost valute v veliki meri odvisna od denarne politike centralne banke, je vanjo treba popolnoma zaupati.

Pomemben del obstoječe finančne infrastrukture so tudi plačilni sistemi. Plačilni sistem je skupek plačilnih in drugih instrumentov, bančnih postopkov in značilnih mehanizmov za medbančni prenos denarnih sredstev, ki skupaj omogočajo kroženje denarja ali opravljanje plačilnih storitev (Logar, 1998, str. 23). Temeljna naloga plačilnih sistemov je torej omogočiti poravnavo denarnih obveznosti, ki nastanejo pri poslovanju ekonomskih subjektov. Prek plačilnih sistemov se med bankami kot izvajalci storitev plačilnega prometa izmenjajo informacije o plačilih ter izračunajo medsebojne obveznosti in terjatve (kliring) ter izvede prenos sredstev iz naslova plačil (poravnava). Kliring in poravnava sta potrebna, če plačnik in prejemnik nista komitenta iste banke. V takšnem primeru je v sam proces vpletena tudi centralna banka, ki mora v svojo glavno knjigo (angl. *ledger*) narediti tudi ustrezno zavedbo novega denarnega stanja posamezne banke. Centralna banka mora kot edina institucija za izdajanje denarja in nadzora denarja v obtoku voditi glavno knjigo, v kateri je vodena evidenca lastništva denarja v sistemu. Posledično je tudi glavna knjiga torej centralizirana.

Virtualna valuta je v nasprotju z valuto fiat digitalna predstava vrednosti, ki je ne izda centralna banka in ki je v določenih razmerah lahko uporabljena kot alternativa denarju (European Central Bank, 2015, str. 25). Tako kot valute fiat tudi virtualne valute nimajo notranje vrednosti, vendar pa po drugi strani niso priznane kot zakonito plačilno sredstvo.

[1] Beseda fiat je latinskega izvora in pomeni ukaz, odredbo ali pooblastilo neke avtoritete.

Virtualne valute za vodenje njihovega lastništva prav tako potrebujejo glavno knjigo, v katero se zapisuje lastništvo digitalne valute.

Začetni poskusi vzpostavitve virtualne valute niso našli načina, kako bi se lahko izognili potrebi po centralni instituciji, ki bi vodila glavno knjigo. Centralno institucijo so želeli odstraniti za to, da zaupanje v valuto ne bi bilo odvisno samo od politike ene institucije. Da bi bilo mogoče popolnoma odstraniti potrebo po centralni instituciji, je namreč treba decentralizirati tudi glavno knjigo. To pomeni, da bi bilo treba hrambo glavne knjige pa tudi njeno ustvarjanje razdeliti med več različnih institucij oziroma deležnikov. Ob decentralizaciji glavne knjige pa se pojavi problem morebitnega dvojnega porabljanja (angl. *double-spending*) sredstev.

Dvojno porabljanje sredstev se zgodi, ko uporabnik ista sredstva želi porabiti dvakrat (jih poslati dvema različnima naslovnikoma). Problem dvojnega porabljanja sredstev se po eni strani ob decentralizaciji lahko pojavi zaradi distribuiranega (razvejanega) pretoka informacij (te namreč niso evidentirane samo pri enem deležniku). Vsi deležniki, ki soustvarjajo glavno knjigo, jih zaradi razvejanosti namreč ne prejmejo hkrati. Po drugi strani pa se problem dvojnega porabljanja lahko pojavi zaradi problemov pri doseganju skupnega soglasja deležnikov o tem, katera transakcija je pravilna. To je problematično predvsem ob obstoju sebičnih in zlonamernih udeležencev (Tschorsch & Scheuermann, 2015, str. 1).

Leta 2008 je Satoshi Nakamoto objavil članek, v katerem je predstavil elektronski denarni sistem, ki je kot prvi ob decentralizirani glavni knjigi odpravil problem dvojnega porabljanja. Kot bom pokazal v tem magistrskem delu, to stori tako, da glasovanje o pravilnosti posameznih transakcij ter soustvarjanje in hrambo glavne knjige omogoči vsem deležnikom v sistemu. Zaradi tega razloga glavno knjigo naredi javno. Omenjeno javno glavno knjigo je poimenoval veriga blokov (angl. *blockchain*), ker je sestavljena iz posameznih zaporednih blokov (angl. *block*), v katere so vključene transakcije, ki skupaj tvorijo neprekinjeno verigo. Ker vsem deležnikom v sistemu ni mogoče zaupati, si je dodatno pomagal s kriptografijo (vedo o zaščiti informacij). Od deležnikov, ki soustvarjajo verigo blokov, za vključitev posameznega novega bloka v verigo namreč zahteva rešitev kriptografske uganke (podrobneje je predstavljena v podpoglavju 1.2). Z rešitvijo kriptografske uganke namreč dokažejo, da so jim z iskanjem njene rešitve nastali stroški. S tem pa pokažejo, da so prave in ne samo navidezne identitete.

Omenjeni sistem je poimenoval Bitcoin, valuto, ki jo sistem uporablja za prenos vrednosti, pa prav tako (bitcoin). Da bi se izognil nejasnostim, želim poudariti, da bo pri razlikovanju med sistemom in valuto v celotnem magistrskem delu skladno z jezikovnimi pravili, če bo šlo za ime sistema, to pisano z veliko začetnico (torej Bitcoin), če bo šlo za valuto, pa z malo začetnico (torej bitcoin). Kot sistem Bitcoin prevzema vlogo centralne banke in plačilnega sistema. Njegova namena sta namreč izdajanje in prenos bitcoina kot valute.

Bitcoin kot valuta je torej samo produkt sistema in sredstvo za prenos vrednosti. Definirali bi ga lahko kot virtualno kriptografsko valuto.

Kmalu po vzpostavitvi sistema Bitcoin so se pojavile nove virtualne kriptografske valute, na splošno imenovane alternativni kovanci (angl. *altcoins*), ki pa kljub nekaterim izboljšavam sistema niti približno ne dosegajo priljubljenosti in tržne kapitalizacije bitcoina. Prav tako pa se je tehnologija, na kateri temelji Bitcoin, začela uporabljati na finančnem in nefinančnem področju s ciljem zmanjševanja stroškov in hitrejše izvedbe procesov.

Cilj magistrskega dela je poglobljena in celostna analiza sistema Bitcoin ter alternativnih možnosti uporabe na njem temelječe tehnologije na finančnem področju. Potrditi ali ovreči želim hipotezo, da bitcoin v tem trenutku ne predstavlja najbolje in v polni meri vseh funkcij klasične valute fiat. Po Mankiwu (2011, str. 325) mora dobra valuta opravljati tri glavne funkcije, in sicer: vlogo menjalnega posrednika (angl. *medium of exchange*), obračunske enote (angl. *unit of account*) in hranilca vrednosti (angl. *store of value*), ki bodo podrobneje predstavljene v podpoglavju 2.2. Omenjene funkcije bom preučil z analizo posameznih značilnosti, po katerih se bitcoin razlikuje pri posamezni funkciji v primerjavi s klasičnimi valutami fiat, pri čemer bom hkrati poskušal ugotoviti tudi, ali omenjene razlike lahko pripomorejo k bolj množičnemu sprejetju bitcoina kot valute in posledično njegove uporabe.

Dodatno želim potrditi ali ovreči hipotezo, da ima – ne glede na prihodnost Bitcoina – tehnologija, na kateri temelji Bitcoin, potencial, da postane pomemben del finančnih sistemov (pametne pogodbe, plačilni sistemi, trgovanje s finančnimi instrumenti …).

Magistrsko delo je sestavljeno iz štirih poglavij, dodatno razdelanih v več podpoglavij. V prvem poglavju bom podrobno in celovito analiziral sistem Bitcoin. Na začetku bom na kratko predstavil dogodke in procese, ki so pripeljali do njegovega razvoja. S pomočjo deskriptivnega pristopa bom nato najprej predstavil principe, na katerih temelji tehnologija Bitcoin in za katere menim, da so nujni za razumevanje sistema. Sledila bo podrobna analiza posameznih sestavnih delov Bitcoina. Podrobno poznavanje delovanja Bitcoina kot sistema je namreč nujno za razumevanje bitcoina kot valute. Vse značilnosti bitcoina kot valute namreč izhajajo iz delovanja sistema.

Po analizi sistema bom v drugem poglavju nadaljeval z analizo bitcoina kot valute. Predstavil bom definicijo virtualne in kriptografske valute ter s komparativno metodo prikazal različne sheme virtualnih valut. Funkcijam bitcoina kot valute bom zaradi potrditve ali ovržbe prve hipoteze namenil največ pozornosti. Pri volatilnosti bitcoina kot pomembni značilnosti obračunske enote in hranilca vrednosti, po kateri se bitcoin najbolj razlikuje od klasičnih valut fiat, bom uporabil metodo kompilacije. V nadaljevanju bom predstavil različne mogoče načine pridobitve bitcoina, vrste denarnic (angl. *wallets*),

ekonomski, zakonodajnopravni vidik (v določenih izbranih državah) in njegovo uporabnost. Na koncu poglavja bom povzel njegove prednosti in slabosti.

V tretjem poglavju bom predstavil trenutno stanje sistema Bitcoin v Sloveniji. Poudarek bo predvsem na davčni obravnavi bitcoina v Sloveniji in kratki predstavitvi slovenskih podjetij oziroma njihovih storitev, ki temeljijo na tehnologiji Bitcoin.

V zadnjem poglavju bom najprej predstavil pristope, ki jih uporabljajo nekateri alternativni kovanci. Sledili bosta dve trenutno najrelevantnejši delitvi na Bitcoinu temelječe tehnologije. Prva delitev tehnologije, ki temelji na kriptologiji, bo glede na možnost njene uporabe pri ponudnikih plačilnih storitev (angl. *payment services providers*)[2]. Druga delitev pa bo na tako imenovane različice verige blokov, ki na Bitcoinu temelječo tehnologijo razdelijo glede na širši namen njene uporabe (ustvarjanje in prenos alternativnih kovancev, uporaba na finančnem in nefinančnem področju). Poglavje bom sklenil z opisom trenutnega stanja uporabe na Bitcoinu temelječe tehnologije na finančnem področju in s predstavitvijo izzivov za prihodnost.

Magistrsko delo bom končal s sklepnimi ugotovitvami in spoznanji.

1 ANALIZA SISTEMA BITCOIN

V tem poglavju bom najprej predstavil prve poskuse vzpostavitve kriptografskih valut. Pri vsaki kriptografski valuti bom na kratko predstavil njene značilnosti in pomanjkljivosti. Prvotne kriptografske valute so pomembne za razumevanje pomena Bitcoina in inovativnega pristopa, ki ga Bitcoin prinaša in na podlagi katerega je ta rešil omenjene pomanjkljivosti. Nato bom predstavil začetke Bitcoina.

Sledila bo podrobna analiza sistema Bitcoin, pri čemer bom še pred analizo podrobneje predstavil principe, na katerih temelji Bitcoin. Ti principi so za razumevanje sistema bistvenega pomena.

1.1 Procesi/Dogodki, ki so pripeljali do razvoja Bitcoina

1.1.1 Zgodovina prvih poskusov vzpostavitve kriptografskih virtualnih valut

Za nastanek Bitcoina je izjemno pomembno gibanje Cypherpunk (*cypher* v angleškem jeziku pomeni šifra). Prek omenjenega gibanja so si njegovi člani po elektronski pošti izmenjavali ideje o tem, kako z uporabo kriptografije doseči čim večjo varnost in

[2] Ponudniki plačilnih storitev so institucije, ki posameznikom in podjetjem ponujajo plačilne storitve (banke, poštne institucije z dovoljenjem opravljanja plačilnih storitev, družbe za izdajanje elektronskega denarja in centralne banke).

zasebnost. Večina izmed spodaj omenjenih idej, ki so uporabljene v Bitcoinu, je nastala oziroma bila analizirana ravno v sklopu omenjenega gibanja (Franco, 2015, 161–162).

Leta 1990 je David Chaum ustanovil sistem eCash, ki je s pomočjo kriptografskih protokolov omogočal plačevanje (s priključenostjo v omrežje in brez nje) na način, ki je onemogočal dvojno porabljanje sredstev, vendar pa je za delovanje potreboval centralno institucijo (Nian & Chuen, 2015, str. 8–9).

Leta 1997 je Adam Back (2002, str. 1–8) predstavil metodo za omejevanje nezaželene elektronske pošte, imenovano Hashcash. Pri omenjeni metodi je vsakemu elektronskemu sporočilu v glavo sporočila treba pripeti žeton (angl. *token*), s katerim s pomočjo kriptografije dokaže, da je za oblikovanje sporočila porabil določeno računsko moč in si posledično s tem ustvaril tudi stroške (ustvarjanje tovrstnih nezaželenih sporočil namreč stane). Pri omenjeni metodi torej ne gre za virtualno valuto. Je pa – kot bom pokazal v nadaljevanju – za nastanek Bitcoina pomemben prispevek ravno zgoraj omenjeni dokaz, da je bilo v ustvarjanje elektronskega sporočila vloženo določeno delo.

Leta 1998 sta bili predlagani distribuirani digitalni shemi denarja, imenovani Bitgold (Szabo, 2005) in B-money (Dai, 1998). Oba predloga sta za vodenje evidence uporabljala distribuirano glavno knjigo, kar pomeni, da sta odpravila potrebo po centralni instituciji. Obe rešitvi sta uporabljali zgoraj omenjeni dokaz o vloženem delu, vendar pa se nista opredelili o tem, kako naj se deležniki dogovorijo glede rasti ponudbe denarja v obtoku. Obe rešitvi sta – tako kot pri Bitcoinu – delno anonimni, vendar pa je glavna razlika v tem, da sta izpostavljeni možnosti dvojnega porabljanja sredstev. Omenjena predloga sta bila samo teoretična in v praksi nista nikoli zaživela.

Leta 2004 je Hal Finney predstavil sistem, imenovan Reusable proof of work (v nadaljevanju RPOW), ki je temeljil na Hashcashu, s to razliko, da za izmenjavo žetonov teh ni bilo treba ponovno generirati. Uporabnik najprej kreira žeton. Ko se odloči, da ga bo porabil, pa ga posreduje drugemu uporabniku, ki ga prek strežnika RPOW, da bi se izognil možnosti dvojnega porabljanja, takoj zamenja za nov žeton. Strežnik v tem primeru ne izda novega žetona, ampak samo ponovno uporabi isti žeton. Omenjeni sistem se torej zanaša na centralno institucijo, ki vzdržuje podatkovno bazo porabljenih žetonov (Franco, 2015, str. 167–168).

Nobenemu izmed zgoraj omenjenih pristopov torej ni uspelo onemogočiti možnosti dvojnega porabljanja ob hkratni odsotnosti centralne institucije.

1.1.2 Začetki Bitcoina

Leta 2008 je kmalu po razmahu svetovne gospodarske krize Satoshi Nakamoto na internetu objavil članek z naslovom »Bitcoin: a peer-to-peer electronic cash system«, v katerem je

podal idejno zasnovo za vzpostavitev sistema elektronskega denarja, ki – čeprav onemogoča dvojno porabljanje sredstev – za delovanje ne potrebuje centralne institucije (Nakamoto, 2008, str. 1–9).

Identiteta avtorja za zdaj še ni znana, in to kljub veliko poizkusom razkritja. Prav tako ni znano, ali gre za posameznika ali skupino ljudi (Nian & Chuen, 2015, str. 11). Glede na dozdajšnje objave avtorja, pri katerih je bila uporabljena ednina, bom v tem magistrskem delu v nadaljevanju navajal avtorja, kot da gre za posameznika.

Vzrok za vzpostavitev tovrstnega sistema je – kot kaže – predvsem ideološki. Bitcoin je namreč izrecno zasnovan tako, da ne potrebuje centraliziranega nadzora, in sicer niti za plačevanje niti za kontroliranje ponudbe bitcoinov v obtoku. Posledično je Bitcoin zasnovan tako, da za delovanje ne potrebuje velike stopnje zaupanja deležnikov v neko tretjo osebo oziroma institucijo. Dodatno potrditev glede omenjene predpostavke nam daje tudi besedilo »The Times 03/Jan/2009 Chancellor on brink of second bailout for banks«, ki ga je Satoshi Nakamoto leta 2009 dodal v izvorni blok, na podlagi katerega je bilo ustvarjenih prvih 50 bitcoinov. Omenjeno besedilo se namreč nanaša na članek, ki je bil 3. 1. 2009 objavljen v časopisu The Times. S tem je želel dokazati časovni izvor prvega bloka ter tudi opozoriti na konceptualno razliko med sistemom Bitcoin in delovanjem obstoječih denarnih sistemov (Ali, Barrdear, Clews, & Southgate, 2014a, str. 267).

Kot prva maloprodajna transakcija, izvedena z bitcoini, se šteje nakup dveh pic v vrednosti 10.000,00 bitcoinov, ki je bila izvršena leta 2009. Pri omenjeni transakciji bitcoinov ni prejela picerija, ampak tretja oseba, ki je pice za kupca v piceriji poravnala z ameriškimi dolarji, kupec pa ji je potem transakcijo z bitcoini nakazal na njen račun (Yermack, 2014, str. 6).

Leta 2010 je Satoshi Nakamoto nadaljnji razvoj projekta prepustil fundaciji Bitcoin in se umaknil iz javnosti (Nian & Chuen, 2015, str. 15).

1.2 Sistem Bitcoin

1.2.1 Principi, na katerih temelji tehnologija sistema Bitcoin

Opisal bom glavne principe, na katerih temelji Bitcoin. Teh je pet, in sicer kriptografija, zgoščevalna funkcija (angl. *hash function*) in zgoščena vrednost (angl. *hash*), Merklovo drevo (angl. *Merkle tree*), omrežje vsak z vsakim (angl. *peer to peer network*) in odprtokodnost (angl. *open source*).

1.2.1.1 Kriptografija

Brez kriptografije sistem Bitcoin ne bi obstajal, zato je razumevanje kriptografije izjemno pomembno za razumevanje sistema Bitcoin.

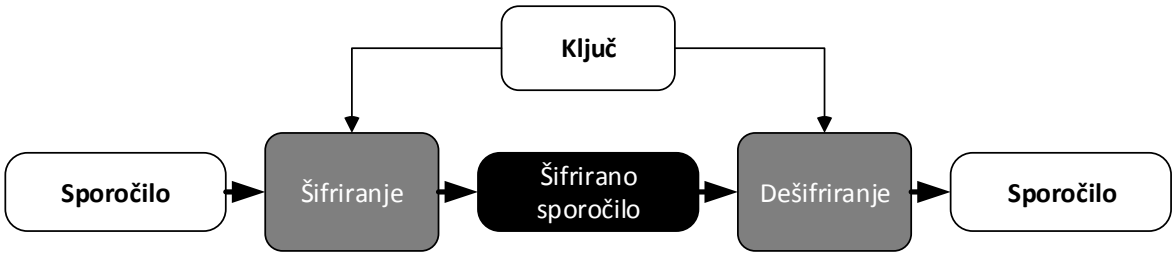
Kriptografija je znanstvena veda varnega komuniciranja ob prisotnosti vsiljivca (angl. *adversary*), ki lahko prestreže, zadrži, blokira ali pa celo spremeni komunikacijo. Veda zajema področje šifriranja, dešifriranja in overitve ter distribucijo ključev (Harvey, 2014, str. 2).

Namen kriptografije je, da s pomočjo matematične znanosti šifriramo in dešifriramo podatke za namene hrambe ali njihovega prenosa na način, da jih bo lahko razbral samo tisti, kateremu so namenjeni. Šifriranje sporočil je pretvorba sporočila v tako obliko (nerazumljiv niz znakov), da ga navadno nepooblaščene osebe ne morejo razumeti. Dešifriranje sporočil pa je ravno nasproten proces. Samo oseba, ki ima v lasti skrivni ključ, lahko podatke dešifrira nazaj v razumljivo obliko (sporočilo).

Poznamo dve vrsti kriptografije, in sicer simetrično in kriptografijo javnega ključa.

Pri simetrični kriptografiji gre za to, da se za šifriranje in dešifriranje uporablja isti ključ. Prikazana je v Sliki 1.

Slika 1: Simetrična kriptografija



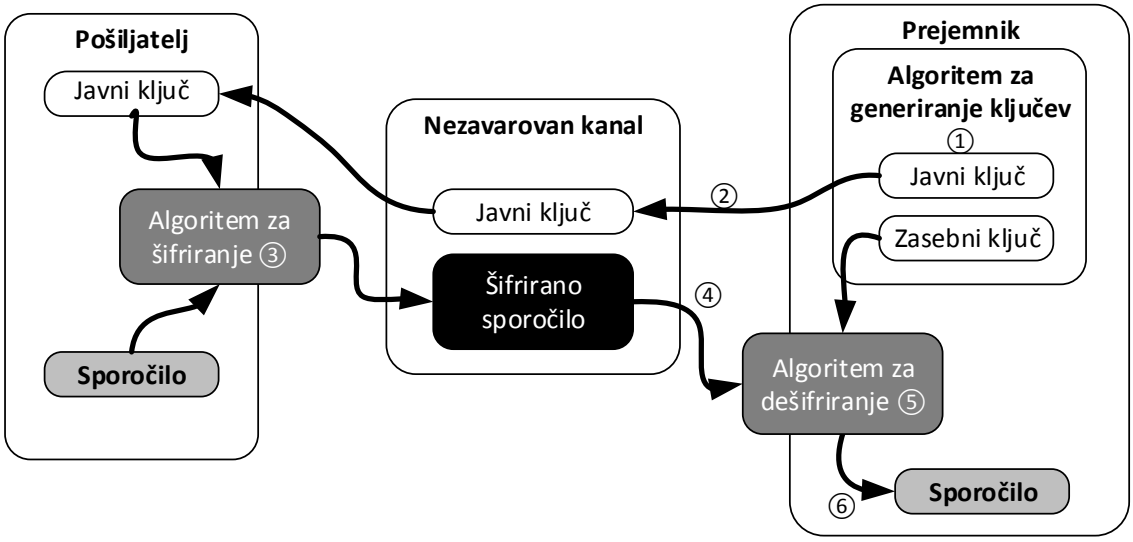
Vir: C. Pacia, Bitcoin explained like you`re five: Part 3 – Cryptography, 2013b.

V praksi to pomeni, da neki čistopis s pomočjo algoritma in ključa pretvorimo v šifrirano besedilo, ki ga brez omenjenega ključa, s katerim so podatki šifrirani, ne moremo prebrati. Za dešifriranje besedila potrebujemo isti ključ, s katerim so bili podatki v osnovi šifrirani. Simetrična kriptografija je dobra za šifriranje podatkov na osebnem računalniku ali pa strežniku, ne pa tudi za komuniciranje. Ker se isti ključ uporablja za šifriranje in dešifriranje, se morata osebi na obeh straneh komunikacije dogovoriti o istem ključu. Glede na to, da se podatki šifrirajo ravno zato, ker menimo, da komunikacijski kanal ni varen, ključa prek omenjenega kanala ne moremo preprosto poslati osebi na drugi strani. Obstajajo sicer metode za varno izmenjavo ključa prek interneta, kot je na primer Diffie-

Hellmanova metoda (Pacia, 2013b), vendar pa je pri tovrstni izmenjavi ključa vseeno treba paziti, da smo prepričani, da ga izmenjujemo s pravo osebo (in ne z nekom, ki se predstavlja, da to je) in da smo s to osebo hkrati povezani v splet – šifriranje in dešifriranje morata torej potekati hkrati. Najbolj priljubljena uporaba kriptografije, ki ima simetričen ključ, je *Advanced encryption standard*. Bitcoin simetrično kriptografijo uporablja samo pri varovanju javnega in zasebnega ključa v uporabnikovi denarnici, ki se uporablja za hrambo omenjenih ključev (Pacia, 2013b).

Kriptografija javnega ključa je bila razvita kot odgovor na pomembno pomanjkljivost simetrične kriptografije – distribucijo ključa. Proces delovanja kriptografije javnega ključa je razviden iz Slike 2.

Slika 2: Kriptografija javnega ključa

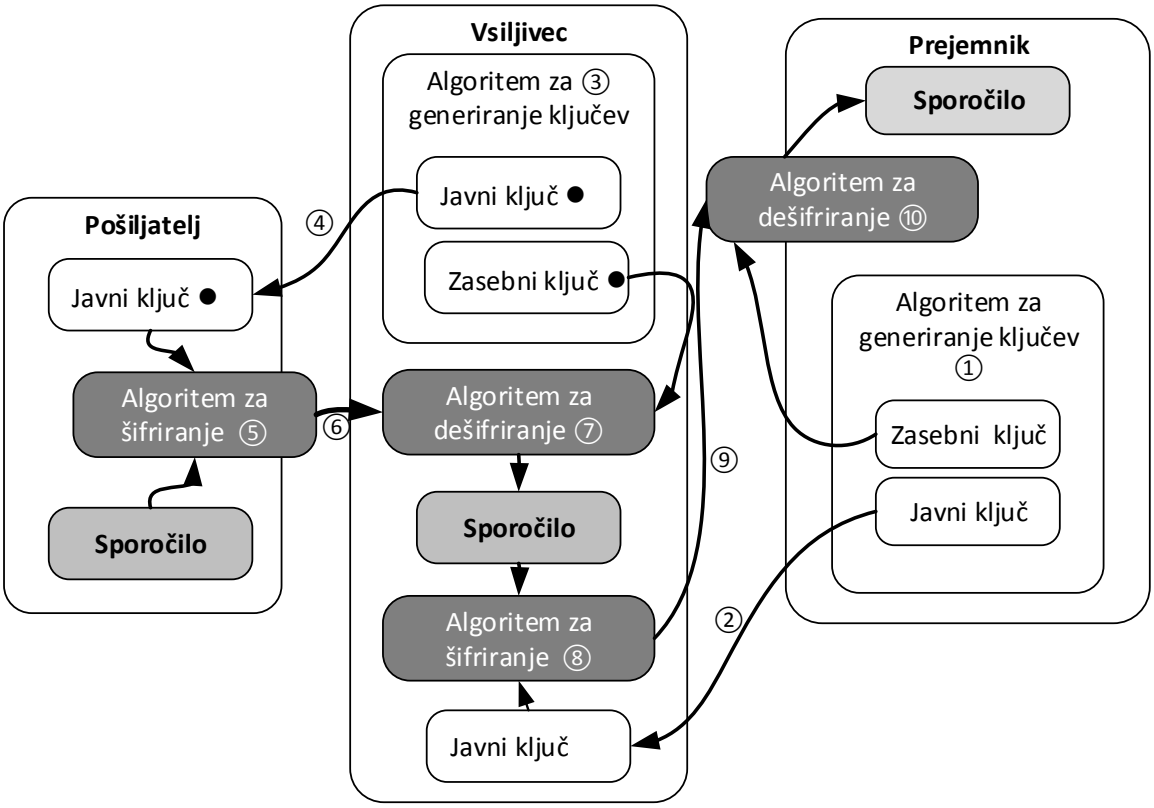


Vir: P. Franco, Understanding Bitcoin Cryptography, Engineering and Economics, 2015, str. 54, slika 5.1.

Prejemnik šifriranega sporočila mora najprej zagnati algoritem za generiranje javnega in zasebnega ključa, ki sta med seboj matematično povezana. Algoritem je sestavljen tako, da je iz javnega ključa zasebni ključ dejansko nemogoče pridobiti. Iz zasebnega ključa pa je javni ključ mogoče pridobiti. Prejemnik nato javni ključ posreduje pošiljatelju sporočila, zasebnega pa obdrži zase. Po prejemu javnega ključa pošiljatelj z njegovo uporabo šifrira želene podatke in jih posreduje prejemniku. Potencialni vsiljivec sicer lahko prestreže sporočilo, vendar pa ga brez zasebnega ključa ne more dešifrirati (Franco, 2015, str. 53). Tako lahko prejemnik javno objavi javni ključ, kdor koli pa mu potem lahko pošlje šifrirano sporočilo, ki ga bo lahko prebral samo on.

Tudi zgoraj omenjeni način ima pomanjkljivost, in sicer možnost napada s posrednikom (angl. *man in the middle attack*), ki je prikazan v Sliki 3.

Slika 3: Napad s posrednikom



Vir: P. Franco, Understanding Bitcoin Cryptography, Engineering and Economics, 2015, str. 54, slika 5.2.

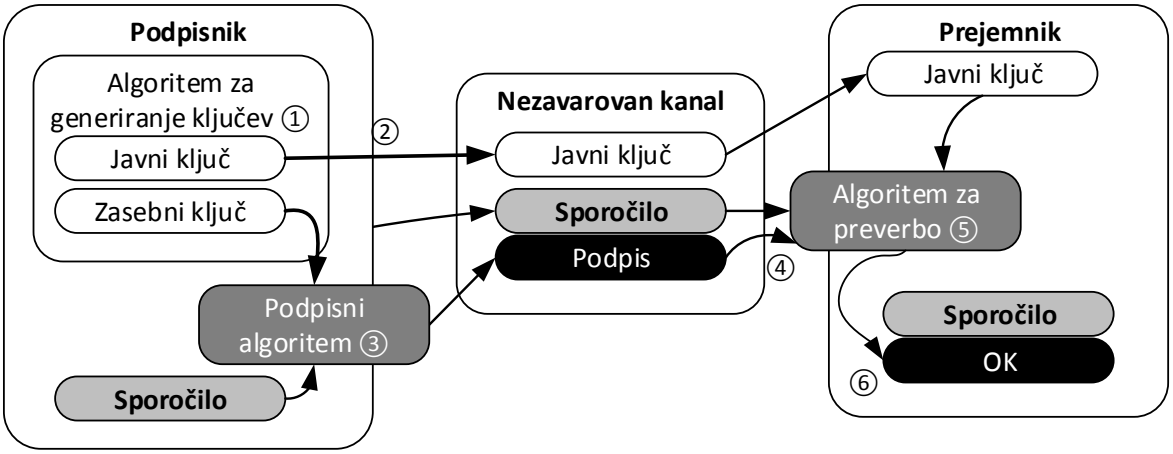
Pri omenjenem napadu posrednik nadzoruje komunikacijski kanal in ima možnost prestrezanja sporočil. Prejemnik sporočila po komunikacijskem kanalu najprej pošlje javni ključ, posrednik pa ga nato prestreže. Namesto da bi pošiljatelju sporočila posredoval originalni javni ključ, posrednik generira nov par zasebnega in javnega ključa ter nov javni ključ posreduje pošiljatelju sporočila, pri čemer ta verjame, da gre za originalni javni ključ prejemnika sporočila. Ko sporočilo pošiljatelj sporočila šifrira z javnim ključem posrednika in ga pošlje po komunikacijskem kanalu, omenjeno sporočilo posrednik spet prestreže in ga dešifrira. To lahko stori, saj ima v lasti zasebni ključ, ki pripada javnemu ključu, s katerim je bilo sporočilo šifrirano. Posrednik nato sporočilo šifrira z originalnim (s prestreženim) javnim ključem prejemnika in mu ga posreduje. Pošiljatelj in prejemnik v takšnem primeru sploh ne vesta, da sta napadena (Franco, 2015, str. 53–55).

Napad s posrednikom se tako lahko izvaja samo zaradi prestrezanja informacij pa tudi za posredovanje napačnih informacij. Omenjenemu napadu se lahko izognemo z varno distribucijo javnega ključa (pri čemer se izgubi namen vzpostavitve kriptografije javnega ključa kot izboljšave pomanjkljivosti simetrične kriptografije), mrežo zaupanja, na kateri temelji program *Pretty good privacy* (ki se lahko uporablja za zavarovanje vsebine elektronske pošte), ter prek overiteljev in izdajateljev digitalnih potrdil, kot je na primer SIGEN-CA (Franco, 2015, str. 55).

Bitcoin sicer ne uporablja opisanega procesa kriptografije javnega ključa, ki se uporablja za šifriranje in dešifriranje podatkov, uporablja pa tehnologijo digitalnih podpisov, ki temelji na kriptografiji javnega ključa. Cilj digitalnih podpisov je zagotoviti, da sporočilo generira podpisnik, da je nespremenjeno in da je podpis neizpodbiten (podpisnik sporočila ne more zanikati, da ga je podpisal). Kriptologija ima poleg šifriranja in dešifriranja podatkov torej pomembno vlogo tudi pri overitvi sporočil (Franco, 2015, str. 56).

Proces digitalnega podpisovanja je razviden iz Slike 4.

Slika 4: Proces digitalnega podpisovanja



Vir: P. Franco, Understanding Bitcoin Cryptography, Engineering and Economics, 2015, str. 57, slika 5.3.

V procesu digitalnega podpisovanja podpisnik s pomočjo algoritma za generiranje para ključev generira javni in zasebni ključ. Javni ključ prek komunikacijskega kanala nato posreduje prejemniku sporočila. Podpisnik nato z zasebnim ključem digitalno podpiše sporočilo in ga skupaj s podpisom posreduje prejemniku. Sporočilo v tem primeru ni šifrirano, ampak samo overjeno. Prejemnik preveri podpis z uporabo javnega ključa. Ob pozitivnem rezultatu lahko z gotovostjo potrdi, da je sporočilo res prišlo od podpisnika (Franco, 2015, str. 57).

Tudi pri zgoraj omenjenem procesu lahko pride do napada s posrednikom, pri čemer se možnosti napada lahko izognemo na isti način kot pri kriptografiji javnega ključa. Pri Bitcoinu do tega sicer ne more priti, ker so javni ključi, kot bom pokazal v nadaljevanju, zavarovani v verigi blokov.

Ena izmed pomembnih lastnosti digitalnih podpisov je, da so podpisani podatki integralni del podpisa. Če bi nekdo podatke kakor koli spremenil, bi se ob preverbi podpisa pojavila napaka. Tako lahko podatke varno prenašamo, ne da bi nas skrbelo, da nam bo kdo ukradel podpis in ga priložil k svojim podatkom (Pacia, 2013b).

Digitalni podpisi so za delovanje sistema Bitcoin ključnega pomena. S podpisom transakcije (z zasebnim ključem) in z njenim razkritjem v omrežju (skupaj z javnim ključem) posamezni deležniki na podlagi naslova, iz katerega prihajajo bitcoini, in priloženega javnega ključa namreč potrdijo lastništvo in veljavnost transakcije ter jo razširijo naprej v omrežju (Pacia, 2013b).

1.2.1.2 Zgoščevalna funkcija in zgoščena vrednost

Zgoščevalna funkcija je algoritem, ki dobi kot vhodno vrednost poljubno dolgo sporočilo, kot izhodno vrednost pa vrne fiksno dolgo binarno vrednost, imenovano zgoščena vrednost. Zgoščena vrednost je za isto vhodno vrednost vedno enaka (Franco, 2015, str. 96).

Osnovni namen zgoščevalne funkcije je torej preoblikovanje poljubno dolgih sporočil v sporočila fiksne, tj. vnaprej določene dolžine.

Kriptografska zgoščevalna funkcija mora imeti po Harveyju (2014, str. 5) naslednje lastnosti:

- kakršna koli sprememba vhodne vrednosti mora kot rezultat producirati popolnoma drugačno izhodno vrednost;
- izhodna vrednost mora imeti vedno enako velikost, ne glede na dolžino vhodne vrednosti;
- enosmernost (iz izhodne vrednosti ni mogoče pridobiti vhodne vrednosti).

V Tabeli 1 je zaradi lažjega razumevanja predstavitev zgoraj omenjenih lastnosti na konkretnem primeru, narejenem s kriptografsko zgoščevalno funkcijo SHA-256 (SHA-256 hash calculator, 2015).

Tabela 1: Prikaz zgoščenih vrednosti za kriptografsko zgoščevalno funkcijo SHA-256

Vhodna vrednost	**Izhodna (zgoščena) vrednost**
EF	3a4db4ee1e59ce1a0a1b9f56bd6d5506d8c204e2f1d501b7a3a4021e6365e8db
EF"	97176e9a181463eba57d543068aad96abc6a05a56eaefbdc924323ad13e2ad46
Ekonomska fakulteta Univerze v Ljubljani	9431038dfa8bdd643ed4afae3c796dc117db727b9c6e1ba1879b738f22116918

Z dodajanjem narekovaja k vhodni vrednosti se je zgoščena vrednost popolnoma spremenila, a hkrati obdržala isto velikost (dolžino – 64 znakov). Enako velja ob uporabi bistveno daljše vhodne vrednosti. Če bi na primer kot vhodno vrednost uporabil celotno

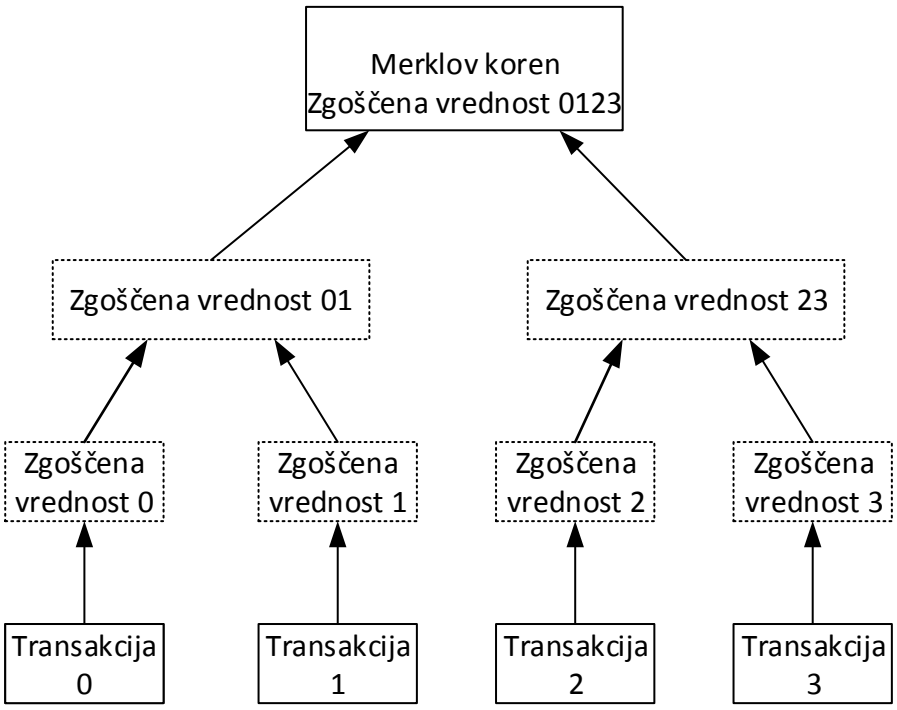
besedilo tega magistrskega dela, bi kot izhodno vrednost prav tako dobil 64 znakov. Iz posamezne izhodne vrednosti pa prav tako ne moremo sklepati, kakšna je bila njena vhodna vrednost.

Največja nevarnost zgoščevalnih funkcij je možnost trka (angl. *collision*). To se lahko zgodi, če bi dve različni vhodni vrednosti kot rezultat dali isto izhodno vrednost. Zaradi tega razloga Bitcoin uporablja zgoščevalno funkcijo SHA256 (v bistvu celo SHA256^2 – kar pomeni, da gre vhodna vrednost dvakrat skozi algoritem), ki ima $2^{256} - 1$ mogočih kombinacij in za katero posledično v praksi ni verjetno, da bi do trka prišlo (Harvey, 2014, str. 5).

1.2.1.3 Merklovo drevo

Merklovo drevo je podatkovna struktura, v kateri vsak vrh drevesa (koren) predstavlja zgoščeno vrednost vseh v paru zgoščenih vrednosti njegovih listov. Prikazano je v Sliki 5.

Slika 5: Merklovo drevo



Vir: C. Pacia, Bitcoin mining explained like you`re five: Part 2 – Mechanics, 2013a.

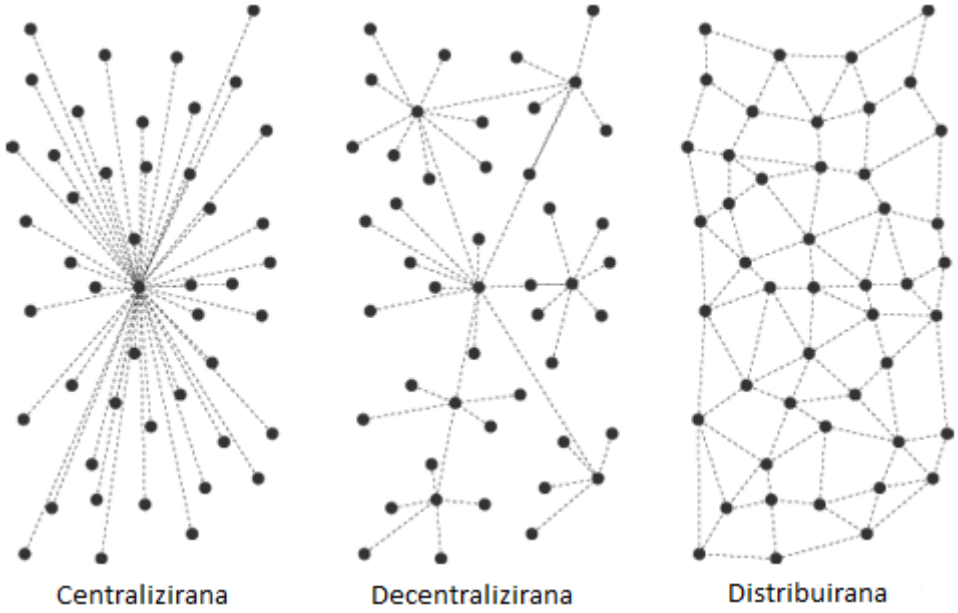
Bitcoin Merklovo drevo uporablja za združevanje transakcij v bloku. Vsaka transakcija Bitcoin je s pomočjo zgoščevalne funkcije spremenjena v zgoščeno vrednost, te pa so potem v paru spojene in s pomočjo zgoščevalne funkcije spremenjene v nove zgoščene vrednosti, dokler ne dobimo Merklovega korena, ki ga – kot bom pokazal v nadaljevanju – deležniki v sistemu Bitcoin uporabijo pri iskanju rešitve kriptografske uganke. Največja

prednost Merklovega drevesa je hitra verifikacija transakcij. Za kriptografski dokaz, da je posamezna transakcija del bloka oziroma Merklovega drevesa, je namreč treba preveriti samo določene dele Merklovega drevesa, kar omogoča hitrejše preverjanje transakcij (Pacia, 2013a). Hkrati pa je Merklovo drevo – kot bom pokazal v točki 1.2.5 – izjemno pomembno tudi za zaščito sistema.

1.2.1.4 Omrežje vsak z vsakim

Po Baran (1964, str. 4) obstajajo tri različne stopnje centralizacije omrežij, ki so prikazane v Sliki 6.

Slika 6: Stopnje centralizacije/decentralizacije omrežij



Vir: P. Baran, On Distributed Communications Networks, Communications Systems, 1964, str. 4.

Centralizirano omrežje je popolnoma odvisno od enega, glavnega deležnika (strežnika) v omrežju. Centralizacija po eni strani omogoča lažjo administracijo, po drugi strani pa zaradi odvisnosti od enega deležnika dela omrežje ranljivejše. Če ima omenjeni deležnik težave, lahko namreč pride do izpada celotnega omrežja.

Decentralizirano omrežje je v nasprotju s centraliziranim omrežjem odvisno od več deležnikov. Za delovanje vseeno potrebuje neko stično točko. Z izpadom večjega števila deležnikov je med njimi posledično prav tako lahko ohromljena komunikacija.

Bitcoin uporablja distribuirano stopnjo omrežja, imenovano omrežje vsak z vsakim, občasno poimenovano tudi kot vrstniško omrežje. Omrežje vsak z vsakim je organizirano kot skupek deležnikov, povezanih v samoorganizirano omrežje. V omrežju vsak z vsakim

imajo lahko nekateri deležniki vlogo odjemalca in strežnika ter so hkrati med seboj povezani. Ob tem ni nujno, da so vsi hkrati povezani s čisto vsemi preostalimi deležniki v omrežju. Takšno omrežje je načelno hitrejše kot klasično omrežje ter tudi zanesljivejše, saj ni podvrženo napadom na specifični lokaciji (Dwyer, 2014, str. 3).

Najbolj znano in prvotno najbolj razširjeno tovrstno omrežje je v preteklosti uporabljal Napster (namenjen nezakoniti izmenjavi glasbe), trenutno pa Bittorrent (namenjen izmenjavi raznovrstnih zakonitih in nezakonitih podatkov).

Zaradi distribuirane oblike omrežja je distribuirana tudi baza podatkov oziroma glavna knjiga, imenovana veriga blokov. Soustvarjajo jo lahko vsi deležniki v sistemu.

1.2.1.5 Odprtokodnost

Bitcoin se zanaša na odprtokodno programsko opremo. Gre za programsko opremo, pri kateri je njena izvorna koda javno dostopna, pri čemer jo dejansko vsak lahko spremeni in uporabi.

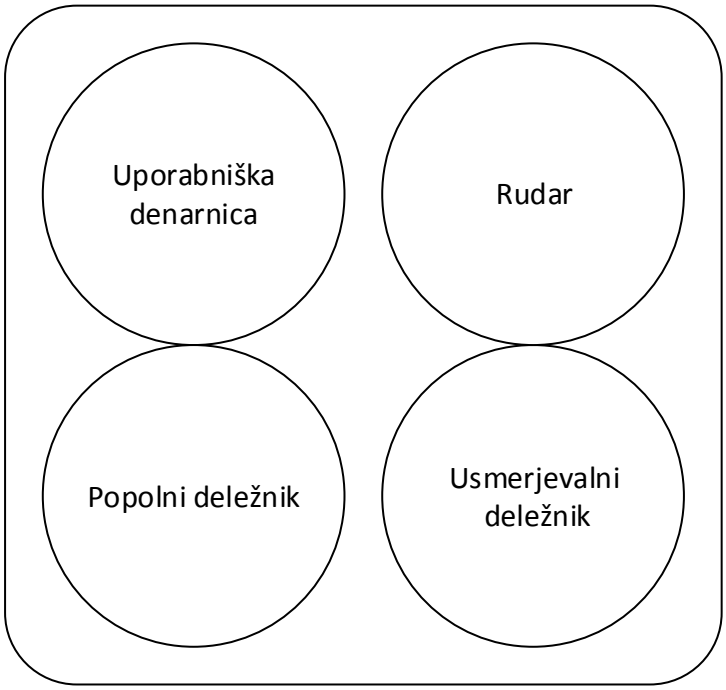
Prednost odprtokodne programske opreme je v tem, da velja za vredno zaupanja, saj ima vsak vpogled v izvorno kodo in lahko torej preveri, kako je spisana (da na primer ne vsebuje škodljivih delov). Poleg tega pa lahko ob nezadovoljstvu uporabnikov nova skupina programerjev na podlagi obstoječe izvorne kode ubere drugačno pot razvoja (ustvari novo programsko opremo, ki temelji na obstoječi, vendar se od nje v določenih delih razlikuje). Pri tem mora imeti za njen uspeh zadostno podporo uporabnikov. Posledično mora, čeprav za razvoj Bitcoina skrbi fundacija Bitcoin (ki ji je Satoshi Nakamoto prepustil razvoj), ob večjih spremembah za njihov konsenz vključiti tudi širšo skupnost (Dwyer, 2014, str. 3–4).

1.2.2 Omrežje Bitcoin

Omrežje Bitcoin je strukturirano kot omrežje vsak z vsakim, kar pomeni, da so si vsi deležniki med seboj enaki (ne obstajajo deležniki, ki bi bili vredni več kot drugi). Vsi deležniki tako nosijo breme nudenja omrežnih storitev. Glavni razlog, zakaj Bitcoin uporablja omrežje vsak z vsakim, je decentralizacija, ki je nujna, če se hočemo izogniti potrebi po centralni instituciji, ki bi vodila glavno knjigo.

Po Antonopoulos (2014, str. 137–139) se izraz omrežje Bitcoin nanaša na skupino deležnikov, ki poganjajo protokol Bitcoin. Čeprav so si deležniki med seboj enaki, pa imajo – odvisno od funkcionalnosti, ki jo podpirajo – lahko različne vloge. Mogoče funkcionalnosti deležnikov so razvidne iz Slike 7.

Slika 7: Funkcionalnosti deležnikov Bitcoin



Vir: A. Antonopoulos, Mastering Bitcoin, 2014, str. 138, slika 6-1.

Vsi deležniki v omrežju Bitcoin vključujejo usmerjevalno funkcijo (lahko pa tudi dodatno – katero oziroma vse izmed preostalih treh). Vsi deležniki namreč preverjajo in razširjajo informacije o posameznih transakcijah in blokih po omrežju ter vzdržujejo povezave z drugimi deležniki.

Nekateri deležniki (imenujejo se popolni deležniki) lokalno hranijo celotno posodobljeno kopijo verige blokov. Takšni deležniki lahko avtonomno preverjajo transakcije brez pomoči drugih deležnikov. Ker je celotna kopija verige blokov velika (saj vsebuje celotno zgodovino transakcij) in se neprestano povečuje, pa večina deležnikov ne hrani celotne kopije verige blokov, ampak se pri transakcijah zanaša na metodo poenostavljenega preverjanja plačil (angl. *simplifed payment verification*). To pomeni, da ti deležniki hranijo samo del posameznega bloka, ne pa tudi transakcij v posameznem bloku. Transakcijo preverijo s pomočjo dokaza Merklove poti, tako da od deležnikov, ki hranijo celotno kopijo, pridobijo ustrezne zgodovinske podatke. Omenjena metoda je podrobneje predstavljena v točki 1.2.5.

Uporabniške denarnice so deležniki, ki lokalno hranijo zasebni ključ, generirajo pare novih zasebnih in javnih ključev (posledično tudi naslovov) ter vodijo stanje bitcoinov deležnika.

Rudarji (angl. *miners*), kot bom pokazal v nadaljevanju, tekmujejo drug z drugim z iskanjem rešitve kriptografske uganke (podrobneje predstavljene v točki 1.2.4), s čimer v verigo blokov dodajajo nove bloke preverjenih transakcij.

1.2.3 Ključi, naslovi in denarnice

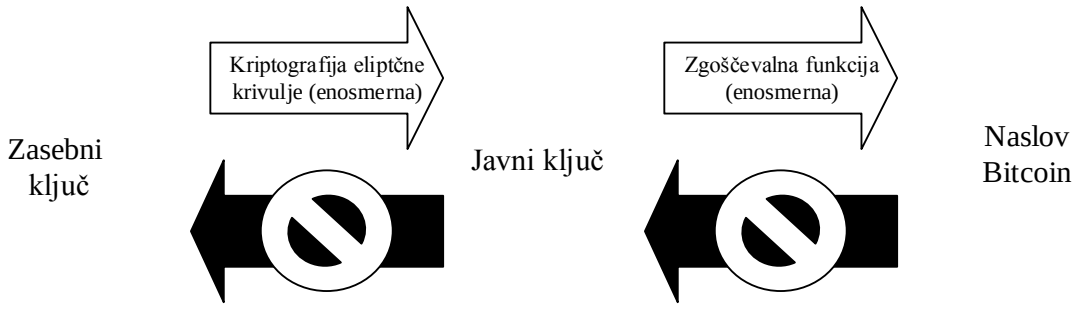
Lastništvo bitcoinov je določeno s pomočjo digitalnih ključev, naslovov Bitcoin in digitalnih podpisov. Digitalni ključi niso hranjeni v verigi blokov ali omrežju, ampak so kreirani in hranjeni v datoteki uporabnika, v preprosti bazi podatkov, imenovani denarnica (Antonopoulos, 2014, str. 61).

Vsaka transakcija, kot bom pokazal v nadaljevanju, za vključitev v verigo blokov potrebuje veljaven digitalni podpis, ki je lahko generiran samo s pomočjo digitalnih ključev (javnega in zasebnega). Oseba, ki ima v lasti digitalne ključe, torej lahko razpolaga z bitcoini na posameznem računu. Zato je izjemno pomembno, da so ključi v denarnici dobro varovani (Antonopoulos, 2014, str. 61).

Kljub uporabi besede denarnica ta torej ne vsebuje bitcoinov. To je zato, ker bitcoini obstajajo izključno v omrežju, v katerem samo menjajo lastništvo. Nameni denarnice so torej le hramba in varovanje digitalnih ključev ter vodenje evidence lastništva bitcoinov na različnih naslovih. Transakcije Bitcoin so posledično torej samo veriga digitalnih podpisov, ki predstavljajo spremembo lastništva bitcoinov (Bheemaiah, 2015, str. 7–8).

Kot je pojasnjeno v točki 1.2.1.1 in razvidno iz Slike 8, digitalni ključi obstajajo v paru, in sicer kot zasebni ter javni ključ, ki sta med seboj matematično povezana. Če imamo v lasti zasebni ključ, lahko iz njega s pomočjo kriptografskega algoritma generiramo javnega, v nasprotni smeri pa to v praksi ni mogoče. Zasebni ključ se uporabi za digitalno podpisovanje transakcij, javni ključ pa za preverjanje podpisa in prejetje transakcij (naslov Bitcoin je namreč zgoščena vrednost javnega ključa).

Slika 8: Razmerje med zasebnim in javnim ključem ter naslovom Bitcoin



Vir: A. Antonopoulos, Mastering Bitcoin, 2014, str. 63, slika 4-1.

Naslov Bitcoin, ki je zapisan v verigi blokov, ni neposredno povezan z dejanskim uporabnikom (iz naslova je namreč nemogoče ugotoviti, komu pripada), vendar pa je za določen naslov mogoče videti celotno zgodovino transakcij tega uporabnika, povezanih s

tem naslovom, kar je lahko problematično, če se naslov poveže (na primer prek IP-naslova[3]) s pravo identiteto uporabnika (na primer pri objavi naslova ob donacijah, interakciji na nakupovalnih straneh in pri menjalnicah z bitcoini). To sta pokazala tudi Reid in Harrigan (2012, str. 15–25), zato je posledično Bitcoin le delno (angl. *pseudonymous*) in ne popolnoma anonimen (Brito & Castillo, 2013, str. 5).

Ron in Shamir (2013, str. 4) zato priporočata, da se za vsako transakcijo generira nov par digitalnih ključev in s tem za boljšo anonimnost posledično vedno uporabi nov naslov Bitcoin.

1.2.4 Rudarjenje

Rudarjenje (angl. *mining*) je proces zbiranja in potrjevanja transakcij (zavedba v verigo blokov) ter izdajanja novih bitcoinov. Proces se imenuje rudarjenje, ker nagrada (angl. *coinbase*), ki jo prejmejo rudarji, simulira padajoče donose, podobno kot pri rudarjenju za plemenitimi kovinami (Antonopoulos, 2014, str. 173).

Ker zaradi decentralizacije ne obstaja centralna entiteta, ki bi vodila evidenco bitcoinov, in ker pretok informacij po distribuiranem omrežju ni hkraten, se morajo deležniki, da bi se izognili možnosti dvojnega porabljanja, med seboj strinjati, katere transakcije so veljavne. Če je večina rudarjev poštena, so vse transakcije, ki jih je večina potrdila, tudi pravilne. Tak način glasovanja o transakcijah pa je lahko podvržen napadu, imenovanem Sybill. Pri napadu Sybill zlonameren deležnik hkrati prek iste strojne opreme vzpostavi več identitet, s katerimi sporoča oziroma glasuje za napačne transakcije (Tschorsch & Scheuermann, 2015, str. 1).

Zaradi tega razloga je Satoshi Nakamoto (2008, str. 3) v proces na podlagi ideje, ki jo je dobil pri Hashcashu, vpeljal tako imenovani dokaz o vloženem delu (angl. *proof of work*), ki ga morajo rudarji opraviti, preden se blok, v katerega so zbrali transakcije (potrjene kot veljavne pri večini deležnikov v omrežju), lahko objavi in doda k prejšnjemu bloku transakcij v verigo blokov. S tem namreč pokažejo, da so v predlog veljavnih transakcij vložili določeno delo oziroma trud, zaradi katerega so jim nastali stroški. Delo je sestavljeno iz reševanja kriptografske uganke, ki umetno poveča računske stroške, potrebne za potrjevanje transakcij. Posledično je možnost potrjevanja odvisna od procesne oziroma računske moči (angl. *hashing power*) in ne od števila deležnikov v omrežju. Glavna predpostavka je torej, da je veliko težje nadzorovati večino računske moči v sistemu kot pa število različnih identitet (deležnikov). Z opravljenim delom namreč deležniki dokažejo, da so prave in ne navidezne identitete (Tschorsch & Scheuermann, 2015, str. 3).

[3] IP-naslov je edinstveno zaporedje števil, ki omogoča, da naprava lahko pošlje in prejme podatke od drugih naprav prek interneta. Z njim je posamezna naprava oziroma njena dostopna točka na internetu predstavljena.

Kot rezultat kriptografske uganke je treba generirati zgoščeno vrednost, ki je manjša od ciljne (ta se zaradi prilagajanja težavnosti skozi čas lahko spreminja). Omenjena zgoščena vrednost nastane iz Merklovega korena (sestavljenega iz zgoščenih vrednosti vseh veljavnih transakcij v bloku), zgoščene vrednosti predhodnega bloka, časovne znamke (angl. *timestamp*), težavnosti (angl. *difficulty*) in naključnega arbitrarnega števila (angl. *nonce*), ki so spuščeni skozi zgoščevalno funkcijo (podrobneje so predstavljeni v točki 1.2.5). Rudar z naključnim spreminjanjem/prilagajanjem omenjenega arbitrarnega števila (drugi podatki so namreč fiksni) in vsakokratnim izvajanjem zgoščevalne funkcije poskuša kot rezultat dobiti zgoščeno vrednost, ki je nižja od ciljne vrednosti. Rešitev uganke (pravilno naključno arbitrarno število) je težko ugotoviti, je pa njeno pravilnost zelo preprosto preveriti, saj je treba na podlagi najdene rešitve uganke in drugih zgoraj omenjenih vrednosti samo oblikovati zgoščeno vrednost, s čimer lahko takoj preverimo njeno pravilnost (Paul, Sarkar, & Mukherjee, 2014, str. 186).

V praksi to pomeni, da mora rudar z naključnim spreminjanjem arbitrarnega števila in izvajanjem zgoščevalne funkcije nad prej omenjenimi vrednostmi kot rezultat dobiti zgoščeno vrednost, ki se začne z vnaprej določenim začetnim številom ničel (na primer rezultat oziroma zgoščena vrednost se mora začeti z desetimi zaporednimi ničlami, nadaljnje vrednosti pa so lahko poljubne). Manjša kot je ciljna vrednost (več začetnih ničel kot rezultat mora imeti zgoščena vrednost), težje je priti do rešitve uganke. Rešitev je mogoče najti samo z naključnim spreminjanjem števila. Za najdbo rešitve je torej treba uporabiti ogromno računske moči (saj je z veliko hitrostjo treba opraviti ogromno poizkusov). Glede na to, da želijo vsi rudarji rešiti zgoraj omenjeno uganko, je verjetnost, da posamezen rudar kot prvi najde rešitev, proporcionalna njegovi računski moči v omrežju. Zaradi stabilnosti in razumnega čakanja na potrditev transakcij se ciljna vrednost (in s tem posledično težavnost) prilagodi vsakih 2.016 ustvarjenih blokov, tako da naj bi v povprečju ustvarjanje posameznega bloka vzelo 10 minut. V povprečju naj bi se ciljna vrednost torej prilagodila vsaka dva tedna. Če so v omenjenem obdobju v povprečju bloki ustvarjeni hitreje kot v 10 minutah, se težavnost poveča, v nasprotnem primeru pa zmanjša (Tschorsch & Scheuermann, 2015, str. 3).

Ob tem se lahko upravičeno vprašamo, zakaj bi rudarji želeli prispevati svoj čas in računsko moč za potrjevanje transakcij tretjih oseb. Vzrok je v nagradi, ki jo rudarji prejmejo za svoje delo (če kot prvi rešijo uganko). Kot nagrado rudar, ki prvi najde rešitev uganke, prejme na novo izdane bitcoine. Bitcoini so torej izdani ob vsaki potrditvi novega bloka in kot nagrada dodeljeni rudarju, ki je našel rešitev kriptografske uganke. Edino na omenjeni način so torej bitcoini izdani in prihajajo v obtok. Izjema je prvotna nagrada, ki je bila podeljena ob oblikovanju izvornega bloka, ki ga je 3. 1. 2009 ustvaril Satoshi Nakamoto. Nagrada se prepolovi vsakih 210.000,00 blokov, kar naj bi bilo ob predpostavki, da je blok v povprečju ustvarjen vsakih 10 minut približno vsaka štiri leta. Na začetku je bila nagrada 50 bitcoinov, trenutno pa znaša 25 bitcoinov (Bheemaiah, 2015,

str. 8–10). Naslednja delitev nagrade (na 12,5 bitcoina) se po podatkih, dostopnih na Bitcoin clock (2016), pričakuje v letošnjem letu (2016) v sredini julija.

Poleg na novo izdanih bitcoinov pa rudar, ki najde rešitev uganke, za nagrado pobere tudi provizije posameznih transakcij, ki so vključene v dotični blok (več o tem v točki 1.2.6). Sistem Bitcoin je zastavljen tako, da bo izdanih samo 21 milijonov bitcoinov. Po zadnjem izdanem bitcoinu bodo kot edina nagrada rudarjem ostale samo provizije posameznih transakcij (Eyal, 2014, str. 2). Večina skupno izdanih bitcoinov bo v obtoku okoli leta 2040 (Ali et al., 2014a, str. 266). Bitcoini so sicer deljivi na osem decimalnih mest, pri čemer je najmanjši mogoči del 0,00000001 BTC imenovan satoshi (Velde, 2013, str. 1). Posledično naj bi bil zadnji del bitcoina izdan leta 2140, ko bo izdanih vseh 20,999.999,98 bitcoinov (Antonopoulos, 2014, str. 174).

V osnovi si je Satoshi Nakamoto (2008, str. 3) zamislil, da bo ena centralno-procesna enota (torej načelno en računalnik) z njeno procesno/računsko močjo predstavljala en glas.

Z večanjem tržne vrednosti bitcoina in posledično večjim zanimanjem za rudarjenje pa je na področju rudarjenja prišlo do napredka pri izvajanju računskih operacij. Na začetku se je računske operacije res izvajalo s centralno-procesno enoto, ki jo najdemo v vsakem osebnem računalniku. Kmalu za tem se je ugotovilo, da je grafični procesor (v računalniku je zadolžen za poganjanje grafike) še primernejši za omenjene operacije. Sledil je razvoj posebne namenske strojne opreme, imenovane F*ield programmable gate array* ter *Application specific integrated circuit* (v nadaljevanju *ASIC*), ki je trenutno v uporabi in ki poleg rudarjenja ne more opravljati drugih nalog (Tasca, 2015, str. 71–72).

Trenutno je rudarjenje dobičkonosno samo z uporabo najnovejše tehnologije. V nasprotnem primeru stroški energije presegajo pričakovani prihodek. Čeprav je pričakovani prihodek od rudarjenja proporcionalen moči uporabljene strojne opreme glede na omrežje, pa je trenutno zaradi ogromne računske moči celotnega omrežja za posameznega rudarja tudi z uporabo najnovejše tehnologije zelo malo verjetno, da bo v naslednjih nekaj letih našel rešitev uganke. Zaradi tega razloga so se posamezni rudarji začeli povezovati v skupine rudarjev (angl. *pools*). Rudar, ki najde rešitev uganke, si namreč nagrado deli s preostalimi rudarji v njegovi skupini (Eyal & Sirer, 2013, str. 4). Nagrada se samodejno proporcionalno razdeli glede na računsko moč posameznega rudarja v skupini. Pričakovan prihodek posameznega rudarja je tako enak, kot če bi rudaril sam, s to razliko, da zaradi večje računske moči celotne skupine v primerjavi s celotno računsko močjo omrežja skupina rešitev najde pogosteje, kot če bi jo iskal sam. To pa posameznemu rudarju omogoča stabilnejši dnevni oziroma tedenski prihodek (Eyal, 2014, str. 3).

V praksi ima večina skupin rudarjev svojega upravljavca. Posamični rudarji se registrirajo pri upravljavcu skupine in zanj rudarijo. Ta dodeljuje naloge, rudarji pa potem iščejo rešitev uganke na podlagi omenjenih nalog. Ko rudar najde rešitev, jo posreduje

upravljavcu, ta pa jo potem objavi v omrežju. Upravljavec se v sistemu Bitcoin obnaša, kot bi bil samostojen rudar. Za nagrado upravljavec dobi na novo izdane bitcoine in jih nato razdeli med rudarje v skupini glede na njihovo računsko moč, ki jo preverja z dodeljevanjem nalog posamičnim rudarjem za doseganje lažjih ciljnih vrednosti od dejanske ciljne vrednosti sistema Bitcoin. Pri tem seveda pobere tudi provizijo (Eyal, 2014, str. 3).

1.2.5 Veriga blokov

Veriga blokov je naraščajoča veriga med seboj povezanih blokov (Franco, 2015, str. 105).

Posamezni blok je neke vrste vsebnik (angl. *container*) podatkovne strukture, v katero so združene transakcije, ki naj bi se dodale v verigo blokov, ki predstavlja neke vrste javno knjigo nakazil (Antonopoulos, 2014, str. 160).

Posamezen blok, kot je bilo pojasnjeno v točki 1.2.4, v verigo blokov doda rudar, ki kot prvi najde rešitev kriptografske uganke. Sestavljen je iz delov, zapisanih v Tabeli 2.

Tabela 2: Struktura bloka

Velikost	Polje	Opis
4 bajte	Velikost bloka	Velikost bloka v bajtih
80 bajtov	Glava bloka	Več polj, ki so del glave bloka
1–9 bajtov	Števec transakcij	Število transakcij
Spremenljiva	Transakcije	Transakcije, ki so zapisane v omenjenem bloku

Vir: A. Antonopoulos, Mastering Bitcoin, 2014, str. 160, tabela 7-1.

Posamezni blok je sestavljen iz štirih podatkov. Velikost bloka in števec transakcij sta opisna podatka. Velikost bloka nam pokaže njegovo velikost v bajtih, števec transakcij pa nam pokaže število transakcij, ki so vključene v blok. Najpomembnejša podatka v bloku sta dejanski seznam posameznih transakcij in glava bloka, ki po velikosti tudi predstavljata glavnino bloka.

Glava bloka (angl. *block header*) je sestavljena iz delov, zapisanih v Tabeli 3.

Tabela 3: Struktura glave bloka

Velikost	Polje	Opis
4 bajte	Različica	Različica programske opreme

se nadaljuje

nadaljevanje

Velikost	Polje	Opis
32 bajtov	Zgoščena vrednost glave predhodnega bloka	Referenca na zgoščeno vrednost predhodnega bloka v verigi blokov
32 bajtov	Merklov koren	Zgoščena vrednost vseh zgoščenih vrednosti skupkov parov transakcij v bloku
4 bajte	Časovna znamka	Približen čas ustvarjanja bloka
4 bajte	Težavnost	Težavnost algoritma za dokaz o vloženem delu
4 bajte	Naključno arbitrarno število	Število, ki ga spreminjamo, dokler ne dobimo prave rešitve uganke

Vir: A. Antonopoulos, Mastering Bitcoin, 2014, str. 161, tabela 7-2.

Glava bloka je torej sestavljena iz treh delov metapodatkov (angl. *metadata*). Prvi del predstavlja zgoščena vrednost predhodnega bloka, ki vsak blok povezuje z njegovim predhodno dodanim blokom v verigo blokov. Drugi del je sestavljen iz težavnosti, časovne znamke in iz naključnega arbitrarnega števila. Tretji del pa predstavlja Merklov koren.

Vsak blok je identificiran z zgoščeno vrednostjo bloka (ki predstavlja rezultat uganke) in višino bloka (angl. *block height*). Zgoščena vrednost bloka je dejansko zgoščena vrednost podatkov glave bloka in predstavlja njegov unikatni identifikator. Višina bloka pa predstavlja njegovo zaporedno številko v verigi blokov. Višina bloka ni njegov unikatni identifikator, saj ima zaradi možnosti več sočasnih vej v verigi blokov, kot bom pokazal v nadaljevanju, več blokov lahko v določenem trenutku hkrati isto višino bloka. Posledično višina bloka ni zapisana v samem bloku (Antonopoulos, 2014, str. 161–162).

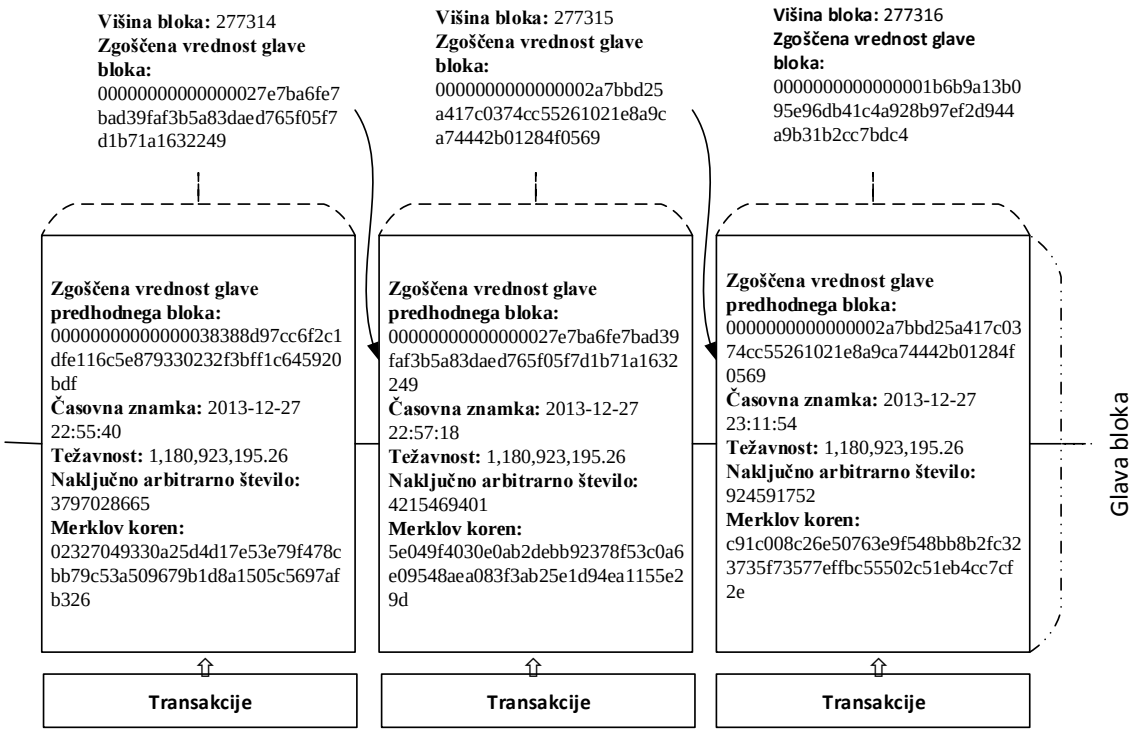
Težavnost je, kot je omenjeno pod točko 1.2.4, določena v algoritmu in se prilagaja vsakih 2.016 blokov. Izračuna se na podlagi časa, ki je bil potreben za ustvarjanje omenjenih blokov, pri čemer podatek dobi iz časovne znamke posameznega bloka. Časovna znamka predstavlja čas začetka iskanja rešitve kriptografske uganke v posameznem bloku in jo doda rudar. Časovna znamka mora biti večja ali enaka mediani zadnjih 11 blokov, pri čemer pa rudarji ne smejo sprejeti bloka, ki bi imel časovno znamko postavljeno več kot 2 uri naprej od njihovega trenutnega časa. Naključno arbitrarno število pa je število, ki ga rudar spreminja (vsi drugi podatki v glavi bloka so namreč v trenutku iskanja rešitve statični). Vsakič, ko ga spremeni, izračuna novo zgoščeno vrednost glave bloka. Če je ta manjša od ciljne vrednosti (rezultat zgoščevanja, torej zgoščena vrednost ima zadostno začetno število ničel), pomeni, da je rudar našel rešitev uganke (Bitcoin developer reference, 2016).

Merklov koren predstavlja zgoščeno vrednost, skupek vseh transakcij v določenem bloku. Namen Merklovega korena je torej ravno to, da ni treba pri vsakem poskusu zamenjave arbitrarnega števila znova iskati zgoščenih vrednosti vseh transakcij, ki bodo vključene v

blok (to bi namreč povečalo potrebo po računski moči in podaljšalo čas za iskanje rešitve). Prav tako pa omogoča hitro preverbo, ali je bila neka transakcija res vključena v določen blok. V primeru n-števila transakcij v določenem bloku se za preverbo transakcije potrebuje samo $2*\log_2(n)$ kalkulacij zgoščenih vrednosti. Posledično to pomeni, da lahko tudi deležniki, ki ne hranijo celotne kopije verige blokov lokalno (njena velikost se namreč neprestano povečuje), hitro preverijo, ali je bila določena transakcija res vključena v neki blok. To storijo tako, da od deležnikov, ki imajo podatke celotnega bloka, zahtevajo samo določene dele Merklovega drevesa tega bloka. Zahtevati morajo tiste dele, ki jih potrebujejo, da lahko najhitreje skupke zgoščenih vrednosti v parih spuščajo skozi zgoščevalno funkcijo, dokler ne pridejo do Merklovega korena. Ta mora biti enak Merklovemu korenu objavljenega bloka, v katerega je vključena dotična transakcija. Podatkom drugih deležnikov lahko zaupajo, saj napačni podatki kot rezultata vseh zgoščevanj namreč ne bi podali prave vrednosti Merklovega korena (Antonopoulos, 2014, str. 164–171).

Iz Slike 9 je razviden primer verige blokov, sestavljene iz treh blokov, pridobljenih na podlagi realnih podatkov.

Slika 9: Primer verige blokov



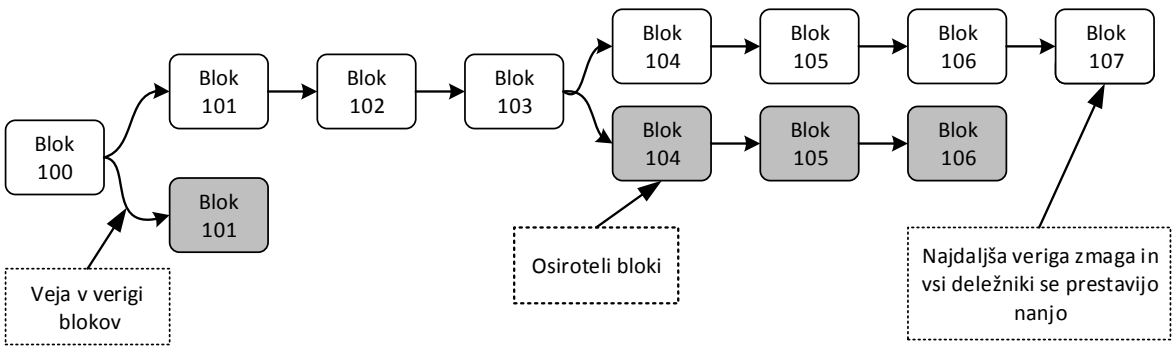
Vir: A. Antonopoulos, Mastering Bitcoin, 2014, str. 165, slika 7-1.

Kot je razvidno iz Slike 9, je zgoščena vrednost glave bloka (poleg tega, da predstavlja rezultat kriptografske uganke) tudi glavni vezni člen, ki med seboj povezuje zaporedne bloke.

Ko rudar najde rešitev uganke, jo objavi in doda v svojo lokalno verigo blokov. Enako po preverbi rešitve in ustreznosti bloka storijo tudi drugi deležniki. Ob dani rešitvi lahko namreč na podlagi vseh podatkov, objavljenih v glavi bloka, z apliciranjem zgoščevalne funkcije preprosto preverijo, ali je ustrezna (tj. da ima rezultat zadostno število začetnih ničel). Ker so posamezni bloki potrjeni in objavljeni v distribuiranem omrežju, se lahko zgodi, da pride do začasnih vej verige blokov. To se lahko zgodi, če dva (ali več) rudarja hkrati (oziroma ob približno istem času) najdeta rešitev vsak svojega bloka. Posamezni rudar v omrežju bo rudarjenje namreč samodejno nadaljeval na podlagi tistega bloka, ki ga je kot prvega prejel kot veljavnega (od preostalih deležnikov). Sporočila in podatki zaradi razvejanosti omrežja namreč ne dosežejo vseh deležnikov hkrati. Sistem Bitcoin takšno situacijo rešuje na podlagi pravila, po katerem se rudarjenje vedno nadaljuje na najdaljši lokalno znani veji. Predpostavlja se namreč, da je bilo za najdaljšo verigo blokov skupno porabljene največ računske moči, kar pomeni, da jo predstavlja večina glasov rudarjev v omrežju. V določenem trenutku se bo namreč gotovo zgodilo, da bodo na eni izmed vej rudarji hitreje prišli do rešitve in objavili nov blok. V takšnem primeru bo ta veja postala daljša, rudarji pa se bodo s krajše verige posledično prestavili na daljšo. Za rudarje krajše verige je namreč bolj smiselno, da se z verige, na kateri delajo (čeprav bi bil del blokov v krajši verigi potrjen z njihove strani), prestavijo na daljšo, saj krajše večina rudarjev zaradi zgoraj omenjenega pravila ne bi nikoli sprejela (večina je namreč ni sprejela kot veljavne). Kar koli »narudarijo« na krajši verigi, je torej zaman, saj ne bo nikoli sprejeto kot veljavno (Ali et al., 2014a, str. 269).

Oportunitetni strošek rudarja je zaradi stroškov električne energije, ki se porabi za rudarjenje, torej prevelik, da bi se mu splačalo nadaljevati rudarjenje na krajši verigi, ki ne bo nikoli sprejeta. Primer začasne veje v verigi blokov je razviden iz Slike 10.

Slika 10: Primer začasne veje blokov v verigi



Vir: P. Franco, Understanding Bitcoin Cryptography, Engineering and Economics, 2015, str. 109, slika 7.8.

S tem ko rudarji s krajše veje preidejo na daljšo vejo, bodo vsi osiroteli bloki, ki so bili del krajše veje, in v njih potrjene transakcije postali neveljavni. Omenjene transakcije so zelo verjetno že del daljše verige. Če niso, pa se bodo vključile v naslednji na novo ustvarjen blok, ki bo del daljše verige.

Ravno zaradi nastanka vej obstaja tudi pravilo, da nagrado v obliki na novo izdanih bitcoinov rudar lahko porabi šele po 100 potrditvah, torej po 100 naknadno ustvarjenih in v verigo blokov sprejetih blokih, od bloka, na podlagi katerega je bila omenjena nagrada prejeta (Antonopoulos, 2014, str. 160).

Pravilo, da se rudarjenje vedno nadaljuje na najdaljši lokalno znani veji, je pomemben element pri spopadanju s poskusom prevar v sistemu Bitcoin. Potencialni napadalec bi namreč moral, če bi želel spremeniti ali odstraniti transakcijo, ki je že dodana v verigo blokov, najprej ponovno rešiti uganko dotičnega bloka. Če spremenimo, odstranimo ali dodamo katero koli transakcijo v bloku (na primer naslov, na katerega naj se pošlje), se namreč spremeni Merklov koren, kar pomeni, da je posledično treba za dotičen blok ponovno najti novo rešitev kriptografske uganke. Merklov koren je namreč del glave bloka, zaradi lastnosti kriptografske zgoščevalne funkcije (če se spremeni samo del vhoda, je izhodni rezultat popolnoma drugačen) pa prej najdeno naključno arbitrarno število ne more več predstavljati rešitve uganke. Ker so bloki med seboj povezani prek zgoščene vrednosti glave bloka (vsak blok ima v glavi bloka tudi zgoščeno vrednost glave njegovega predhodnega bloka), bi moral napadalec poleg omenjenega bloka na novo najti tudi uganko vseh blokov, ki mu sledijo, obenem pa tudi preseči obstoječo verigo blokov (da bi torej napadalčeva postala najdaljša). To bi bilo mogoče samo, če bi imel napadalec več kot 51 % celotne računske moči omrežja, saj bi v nasprotnem primeru večina rudarjev v »originalno« verigo blokov hitreje dodajala nove bloke kot pa on sam (Pacia, 2013a).

Na tem mestu je treba poudariti, da napadalec v obdobju, ko obvladuje večino računske moči omrežja, lahko novim transakcijam samo preprečuje potrditev in izvaja napad dvojnega porabljanja lastnih kovancev. Ne more pa preprečiti pošiljanja novih transakcij v omrežje (te bi bile samo prikazane kot nepotrjene). Prav tako pa tudi ne more spremeniti pravil protokola, ustvariti novih kovancev »iz ničesar« (lahko pa jih prejme kot nagrado iz na novo ustvarjenih blokov), porabiti kovancev, ki mu niso nikoli pripadali, in zase ukrasti kovancev nekoga tretjega (Kaşkaloğlu, 2014, str. 94).

Tovrstni napad bi tudi ob 51- ali večodstotni računski moči v omrežju napadalcu vzel ogromno časa in stroškov (odvisno od tega, koliko globoko v verigi se nahaja transakcija, ki jo želi spremeniti). Zato je načelno bolj smiselno, da računsko moč porabi za rudarjenje novih blokov, na podlagi katerih bo zaradi velikosti njegove računske moči z veliko verjetnostjo redno prejemal nagrado in tudi provizijo.

Ravno zaradi možnosti zgoraj omenjenega napada so skupine rudarjev lahko problematične. Skupina rudarjev namreč v večini primerov sprejme kogar koli. Če skupina postane zelo velika, pa lahko preseže 51 % skupne računske moči v omrežju. To se je v juliju 2014 za en dan tudi zgodilo, ko je skupina, imenovana GHash.IO, ustvarila več kot 50 % blokov v glavni verigi blokov. Takoj po omenjenem dogodku je skupina načrtno zmanjšala skupno računsko moč in se javno zavezala, da je ne bo več presegla (Eyal, 2014, str. 4). Nobenemu izmed poštenih rudarjev namreč ni v interesu, da se zgubi zaupanje v sistem. Cena bitcoina bi padla, s tem pa bi oni sami izgubili največ.

1.2.6 Transakcije

V nasprotju s centraliziranimi digitalnimi valutami knjiga nakazil (veriga blokov), ki jo uporablja sistem Bitcoin, ne vodi računov in stanj posameznih uporabnikov. Hrani pa transakcije (Franco, 2015, str. 77). Transakcije so posledično najpomembnejši del sistema Bitcoin. Vse drugo je načrtovano z namenom, da se transakcije lahko oblikujejo, distribuirajo po omrežju, potrdijo in dodajo v verigo blokov.

Transakcije so podatkovne strukture, ki zakodirajo prenos vrednosti med deležniki v sistemu Bitcoin. Vsaka transakcija je javen vnos v javno knjigo nakazil, imenovano veriga blokov (Antonopoulos, 2014, str. 109). Sestavljene so iz seznama vhodnih in izhodnih delov. Vsaka transakcija ima tudi zgoščeno vrednost, ki predstavlja njen identifikator. Struktura posamezne transakcije je prikazana v Tabeli 4.

Tabela 4: Struktura transakcije

Velikost	Polje	Opis
4 bajte	Različica	Različica pravil, ki jim sledijo transakcije
1–9 bajtov	Števec vhodov	Kaže število vhodnih delov
Spremenljiva	Vhodni deli	Eden ali več vhodnih delov
1–9 bajtov	Števec izhodov	Kaže število izhodnih delov
Spremenljiva	Izhodni deli	Eden ali več izhodnih delov
4 bajte	Časovni zaklep	Časovna znamka ali pa številka bloka

Vir: A. Antonopoulos, Mastering Bitcoin, 2014, str. 111, tabela 5-1.

Izhodni del transakcije je ključni del posamezne transakcije, ki je ob izvedbi transakcije tudi zapisan v verigi blokov. Vsak izhodni del posamezne transakcije je sestavljen iz zneska in naslova prejemnika. Naslov je, kot je pojasnjeno v točki 1.2.3, pridobljen na podlagi javnega ključa. Samo lastnik zasebnega ključa lahko odklene sredstva, hranjena v izhodnem delu posamezne transakcije. Da bi sredstva lahko odklenil, mora lastnik zasebnega ključa transakcijo digitalno podpisati.

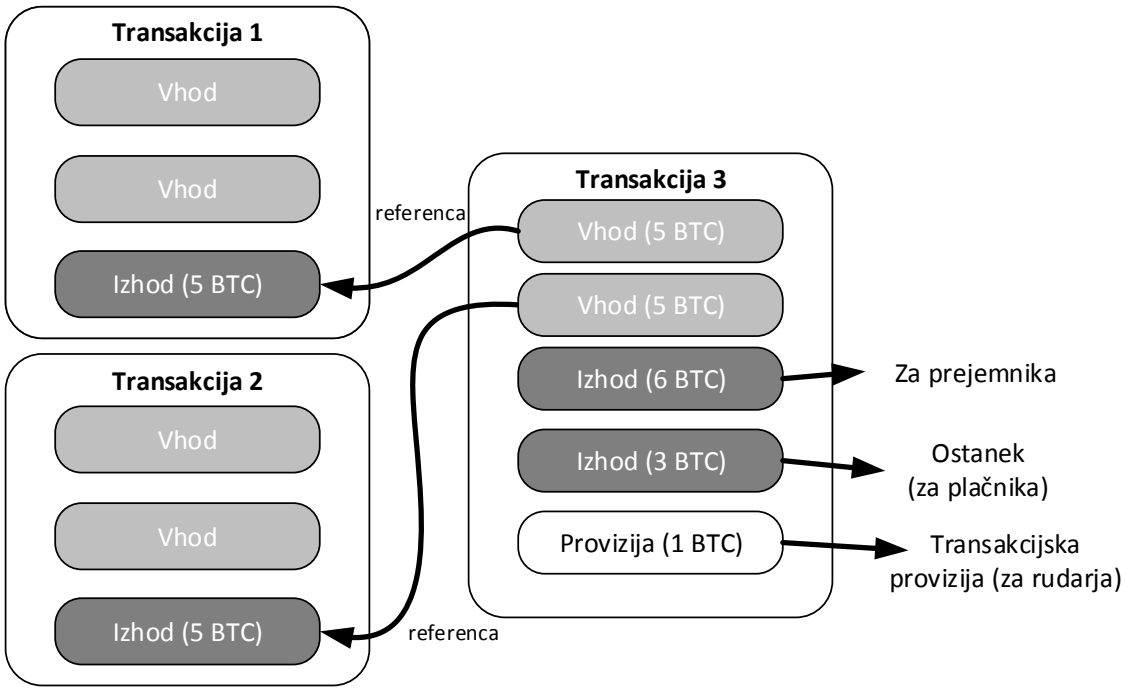
Vsak izhodni del mora biti porabljen v celoti. Ponovno sklicevanje na isti izhodni del se šteje kot poskus dvojnega porabljanja. Bitcoinova programska oprema uporablja predpomnilnik (angl. *cache*) neporabljenih izhodnih delov transakcij (angl. *unspent transaction output*), s pomočjo katerega lahko posamezen deležnik hitro preveri, ali je transakcija veljavna.

Vhodni del posamezne transakcije vsebuje referenco predhodnega izhodnega dela transakcije in digitalni podpis, da se sredstva predhodnega izhodnega dela transakcije lahko porabijo. Če se digitalni podpis ne ujema, je transakcija zavrnjena (Franco, 2015, str. 77).

Časovni zaklep predstavlja najmanjši mogoči čas, za katerega želimo, da se transakcija doda v verigo blokov. Vrednost časovnega zaklepa je vedno privzeta na 0, razen če bi izrecno želeli, da se podobno kot pri čeku določi, kdaj točno naj se izvrši (Antonopoulos, 2014, str. 112).

Primer transakcije, sestavljene iz dveh različnih vhodnih delov, je razviden iz Slike 11.

Slika 11: Primer transakcije Bitcoin



Vir: P. Franco, Understanding Bitcoin Cryptography, Engineering and Economics, 2015, str. 78, slika 6.1.

Kot je razvidno iz Slike 11, je vsak posamezni vhodni del transakcije številka 3 sestavljen iz celotnega izhodnega dela transakcije številka 1 (v vrednosti 5 bitcoinov) in celotnega izhodnega dela transakcije številka 2 (v vrednosti 5 bitcoinov).

Ker se izhodni del predhodne transakcije lahko uporabi samo enkrat, mora vhodni del obstoječe transakcije vedno uporabiti vse kovance izhodnega dela predhodne transakcije. Vhodni del posledično ne specificira, koliko kovancev mora biti porabljenih (prenesenih) v okviru transakcije. Zaradi tega razloga je treba poleg izhodnega dela (v zgornjem primeru v vrednosti 6 bitcoinov), s katerim specificiramo, koliko kovancev želimo porabiti (prenesti na nov naslov), dodati še (vsaj) en izhodni del, s katerim razliko kovancev vrnemo nazaj na svoj naslov (načelno vedno kreiramo novega in ga ne vrnemo na istega). Tako Bitcoin implementira vračilo »drobiža« oziroma ostanka.

Zgoraj omenjena vrednost izhodnega dela je pomembna zato, ker razlika med vsemi vhodnimi in izhodnimi deli v posamezni transakciji samodejno predstavlja provizijo, ki jo za svoje delo (poleg nagrade v obliki na novo izdanih bitcoinov) prejme rudar, ki transakcijo z rešitvijo kriptografske uganke doda v verigo blokov (Tschorsch & Scheuermann, 2015, str. 3–4). V zgornjem primeru bi torej, če bi pozabili definirati vračilo ostanka, rudar namesto enega bitcoina zaslužil štiri bitcoine.

Provizija (poleg nagrade v obliki na novo izdanih bitcoinov) predstavlja pomemben del zaslužka rudarjev. Nagrada, ki jo dobi rudar z vključitvijo bloka v verigo blokov, se namreč približno vsaka štiri leta razpolovi. V prihodnosti bo provizija torej postala edini vir zaslužka rudarjev. Prav tako pa provizija sistem ščiti pred zlorabami v obliki velikega števila hkratnih nezaželenih transakcij (angl. *spam*), s katerimi bi napadalec želel preplaviti omrežje (tovrsten napad bi bil za napadalca namreč drag). Provizija je izračunana na podlagi velikosti transakcije v kilobajtih (ki je odvisna od števila vhodnih in izhodnih podatkov) in ne na podlagi vrednosti transakcije v bitcoinih (Antonopoulos, 2014, str. 118–120).

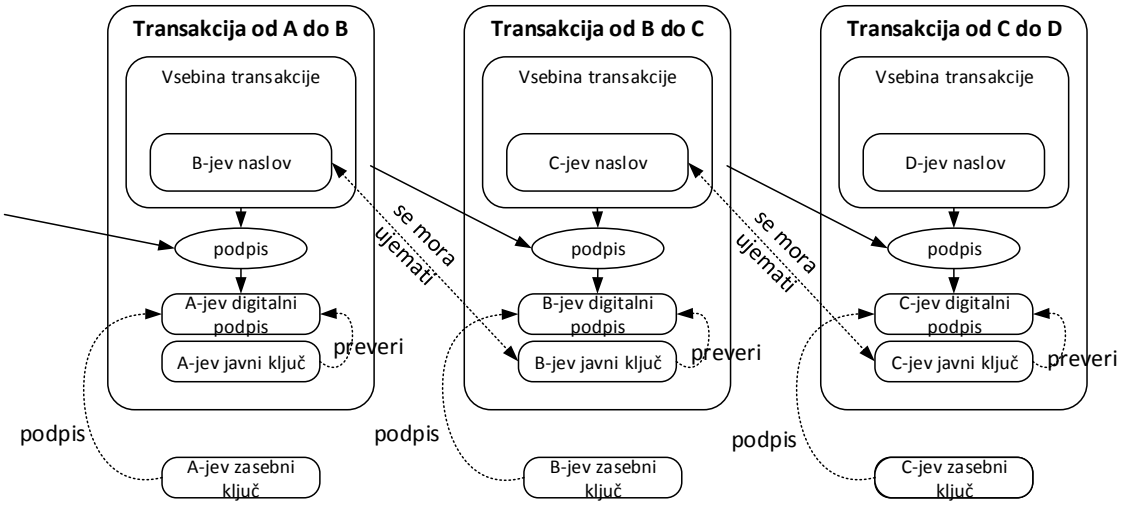
Provizija je trenutno prostovoljna. Posledično je ni nujno določiti, vendar pa pripomore k hitrejši vključitvi transakcije v posamezen blok. Rudarjem posameznih transakcij namreč načelno ni treba vključiti v verigo blokov. S tem ko jim plačamo provizijo, jih spodbudimo, da jo vključijo. V teoriji naj bi popolno konkurenčni rudarji transakcijo vključili, če je provizija večja od mejnih stroškov vključitve. V protokolu je definirano, da je največja velikost posameznega bloka 1 megabajt. Posledično so mejni stroški vključitve nič, če je trenutno nepotrjenih transakcij manj, kot je zanje prostora v trenutno grajenem bloku. Če v trenutno grajenem bloku ni dovolj prostora za vse še nepotrjene transakcije, je bolj smiselno, da rudar dodeli prednost transakcijam, na podlagi katerih bo prejel provizijo. Rudar se tako (dokler v prihodnje v protokolu provizije ne bodo obvezne) lahko nadeja provizij samo ob omejeni velikosti posameznega bloka, saj le tako transakcije (s provizijo) med seboj tekmujejo za čimprejšnjo vključitev v blok (Möser & Böhme, 2014, str. 3).

Trenutno je glede na privzete nastavitve v programski opremi smiselno transakcijo brez provizije poslati, samo če je ta manjša od 1.000,00 bajtov, da je seštevek njenih izhodov vsaj 0,01 bitcoina in da je njena prioriteta dovolj visoka. Prioriteta se izračuna tako, da

seštevek vrednosti vhodnih delov (izraženih v enoti satoshi), pomnoženih z njihovo starostjo (izraženo v številu blokov), delimo z velikostjo transakcije v bajtih. Da ne potrebuje provizije, mora biti izračunana prioriteta posamezne transakcije večja od 57,600.000,00. Ker se vhodni deli z vsako nadaljnjo potrditvijo novega bloka starajo, bo vsaka transakcija (tudi brez provizije) prej ali slej dobila dovolj visoko prioriteto, na podlagi katere jo bo rudar vključil v verigo blokov. Če transakcija nima dovolj visoke prioritete, mora vključevati provizijo, sicer je rudar načelno ne bo dodal v verigo blokov (Bitcoin Wiki Transaction fees, 2016).

Kot je razvidno iz Slike 12, vsako transakcijo, ki jo deležnik podpiše, skupaj z digitalnim podpisom in javnim ključem razširi po celotnem omrežju, pri čemer vsak deležnik, ki jo prejme, preveri, ali je transakcija res veljavna. S pomočjo naslova, s katerega prihajajo bitcoini (to je namreč zgoščena vrednost javnega ključa), najprej preveri, ali je javni ključ, ki je priložen transakciji, pravi (če na podlagi javnega ključa izvede zgoščevalno funkcijo, mora kot rezultat dobiti zgoraj omenjeni naslov). S pomočjo javnega ključa pa potem deležnik preveri še veljavnost podpisa (Shirriff, 2014).

Slika 12: Podpisovanje transakcij v omrežju Bitcoin



Vir: K. Shirriff, Bitcoins the hard way: Using the raw Bitcoin protocol, 2014.

Če transakcija ni veljavna, jo posamezen deležnik zavrne in ne razširi naprej po omrežju. Deležnik preveri, ali je transakcija veljavna, na naslednji način (Franco, 2015, str. 78–84):

- preveri, ali vsak predhodni izhodni del res obstaja in ali res še ni bil uporabljen;
- preveri, ali je seštevek vhodnih delov večji ali enak izhodnim delom;
- preveri, ali so digitalni podpisi vsakega vhodnega dela veljavni.

Šele nato jo rudarji tudi potrdijo z dodajanjem v verigo blokov.

Ker so transakcije med seboj povezane, je za vsako transakcijo oziroma vsak njen del mogoče videti zgodovino – vse do izvora (nagrade ali pa izvornega bloka (ki ga je ustvaril Satoshi Nakamoto), ki sta sestavljena samo iz izhodnega dela).

Za zneske večjih vrednosti je zaradi možnosti začasnih vej, preden lahko z gotovostjo potrdimo, da je bila transakcija res izvršena (če smo na primer v vlogi prodajalca storitve, ki bo poplačan z bitcoini), priporočeno počakati, da je po vključitvi bloka, v katerega je transakcija dodana v verigo blokov, naknadno dodanih še vsaj 6 dodatnih blokov (Pacia, 2013a).

Transakcije Bitcoin sicer omogočajo več fleksibilnosti, kot je samo zgoraj omenjeni prenos kovancev. Bitcoin namreč omogoča skriptiranje (angl. *scripting*), kar posledično transakcijam daje več manevrskega prostora glede njihovih izvršitev in namembnosti. Programski jezik, ki ga uporablja Bitcoin, je osnoven za to, da ne more priti do zlorab. Prenos kovancev z enega na drug naslov je tako samo izvršba najosnovnejše in najpogostejše skripte, ki pa je zadostna za namene tega magistrskega dela. Posledično različnih dodatnih možnosti skriptiranja v tem delu ne bom podrobneje omenjal.

2 BITCOIN KOT VALUTA

V tem poglavju bo kot glavni produkt oziroma namen vzpostavitve sistema Bitcoin predstavljen bitcoin kot valuta.

Najprej bom predstavil definicijo virtualne in kriptografske valute ter različne sheme virtualnih valut. Sledila bo preučitev bitcoina z vidika funkcij, ki jih mora opravljati dobra valuta fiat, in sicer menjalnega posrednika, obračunske enote in hranilca vrednosti. Funkcije bitcoina kot valute bom preučil z analizo posameznih značilnosti, po katerih se bitcoin razlikuje pri posamezni funkciji v primerjavi s klasičnimi valutami fiat. Ob tem bom hkrati poskušal ugotoviti tudi, ali omenjene razlike lahko pripomorejo k bolj množičnemu sprejetju bitcoina kot valute in posledično njegove uporabe.

V nadaljevanju bom predstavil različne mogoče načine pridobitve bitcoina, vrste denarnic, ekonomski, zakonodajnopravni vidik (v določenih izbranih državah) in njegovo uporabnost. Na koncu poglavja bom povzel njegove prednosti in slabosti.

2.1 Definicija in sheme virtualnih in kriptografskih valut

Evropska centralna banka (angl. *European Central Bank*, v nadaljevanju ECB, 2012, str. 13) je na podlagi matrike denarja (Tabela 5) virtualno valuto najprej definirala kot vrsto nereguliranega digitalnega denarja, ki je izdana in običajno tudi regulirana prek njenih razvijalcev ter je sprejeta in v rabi med člani neke virtualne skupnosti.

Tabela 5: Matrika denarja

<table>
<tr><td rowspan="3">Pravni status</td><td>Nereguliran</td><td>Nekatere oblike lokalnih valut</td><td>Virtualne valute</td></tr>
<tr><td rowspan="2">Reguliran</td><td rowspan="2">Bankovci in kovanci</td><td>Elektronski denar</td></tr>
<tr><td>Knjižni denar</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Fizična</td><td>Digitalna</td></tr>
<tr><td colspan="2">Oblika denarja</td></tr>
</table>

Vir: European Central Bank, Virtual currency schemes, 2012, str. 11, tabela 1.

Naknadno je leta 2015 ECB spremenil definicijo virtualne valute, in sicer: »Virtualna valuta je digitalna predstava vrednosti, ki je ne izda centralna banka, kreditna institucija ali pa institucija za izdajanje elektronskega denarja in ki je v določenih razmerah lahko uporabljena kot alternativa denarju« (ECB, 2015, str. 25).

Po mnenju ECB definicija ne sme vsebovati besede »denar«, saj se je pokazalo, da virtualne valute niso dovolj likvidne in množično sprejete, kot mora biti pravi denar. Prav tako so odstranili besedo »nereguliran«, saj so v določenih državah prilagodili zakonodajo in nadzor na način, da vsaj delno pokriva nekatere njene vidike oziroma vidike z njo povezanih storitev. Da bi se izognili napačnim interpretacijam glede teoretičnih omejitev možnosti sprejetja virtualne valute, pa so prav tako odstranili zadnji del stavka prvotne definicije, ki se glasi: »sprejeta in v rabi med člani neke virtualne skupnosti«.

Evropski bančni organ (angl. *European Banking Authority*, v nadaljevanju EBA, 2014, str. 11)[4] podobno kot ECB virtualno valuto definira kot digitalno predstavo vrednosti, ki je ne izda centralna banka oziroma javni organ in ki ni nujno vezana na valuto fiat, vendar pa jo z namenom menjave individualne in pravne osebe lahko hranijo, prenašajo in z njo elektronsko trgujejo.

Bitcoin glede na zgornji definiciji spada med virtualne valute, saj predstavlja določeno vrednost (določeno s ponudbo in povpraševanjem), ne izda ga centralna banka, z njim se elektronsko trguje, prav tako pa se lahko v določenem okolju uporablja kot alternativa denarju.

Glede na interakcijo s pravim denarjem oziroma z realnim gospodarstvom ECB (2012, str. 13–14) razlikuje med tremi mogočimi shemami virtualnih valut:

[4] EBA je neodvisen organ Evropske unije, katerega namen je zagotoviti učinkovito in usklajeno stopnjo ureditve varnega in skrbnega poslovanja ter nadzora v evropskem bančnem sektorju. Njegova splošna cilja sta ohranjati finančno stabilnost v Evropski uniji ter zagotavljati integriteto, učinkovitost in pravilno delovanje bančnega sektorja.

- **zaprto shemo**, pri kateri ni povezave z realnim gospodarstvom; pri tovrstni shemi lahko uporabnik virtualno valuto pridobi in uporablja samo znotraj virtualne skupnosti; tak primer je na primer igra World of Warcraft, pri kateri uporabnik z napredovanjem v igri zasluži kovance, ki jih potem uporablja za nakup raznih dodatkov v sami igri;
- **shemo z enostranskim tokom**, pri kateri je virtualno valuto mogoče kupiti z valuto fiat, ni pa je mogoče zamenjati nazaj za valuto fiat; primer tovrstne sheme so Amazonovi kovanci, ki omogočajo nakup storitev in dobrin v Amazonovem ekosistemu;
- **shemo z dvostranskim tokom**, pri kateri je virtualno valuto po veljavnem tečaju mogoče kupiti in zamenjati z valuto fiat; tovrsten primer je bitcoin.

Peters, Chapelle in Panayi (2014, str. 11–15) pa menijo, da je virtualne valute bolje razvrstiti glede na to, ali gre za centralizirane (imajo enega administratorja) ali pa decentralizirane valute (administracija obstaja skozi soglasje v omrežju). Zadnje imenujejo tudi kriptografske valute, saj pogosto temeljijo na kriptografskih dokazih. Bitcoin tako natančneje lahko definiramo tudi kot kriptografsko virtualno valuto.

Glede na omenjeno razvrstitev jih v večini primerov lahko razlikujemo glede na:

- **razlog obstoja**, pri čemer kriptografske valute obstajajo zaradi uporabe v realnem gospodarstvu, centralizirane virtualne valute pa se uporabljajo samo v sistemu izdajatelja;
- **izdajo v obtok**, pri čemer kriptografske valute postopoma prihajajo v obtok s pomočjo rudarjenja, izdaja centraliziranih virtualnih valut pa je poljubno kontrolirana prek centralnega izdajatelja;
- **denarno politiko**, pri čemer je pri kriptografskih valutah ponudba fiksna, pri centraliziranih virtualnih valutah pa je lahko prilagojena glede na inflacijo (več o tem v točki 2.5.1);
- **možnost korekcije**, pri čemer pri kriptografskih valutah v nasprotju s centraliziranimi virtualnimi valutami izvršenih transakcij ni mogoče popraviti oziroma razveljaviti;
- **mesto hrambe**, pri čemer so kriptografske valute lahko hranjene v eni ali več različnih denarnicah in posledično naslovih hkrati;
- **menjalno razmerje**, ki je pri kriptografskih valutah dvostransko in se spreminja glede na povpraševanje in ponudbo, v nasprotju s centraliziranimi virtualnimi valutami, pri katerih je razmerje enostransko in ga določi izdajatelj;
- **izvor vrednosti**, ki pri kriptografskih valutah v nasprotju s centraliziranimi virtualnimi valutami nastane zaradi mrežnih učinkov (več o tem v točki 2.2.1) in stroškov izdajanja valute;
- **področje uporabe**, pri čemer se kriptografske valute uporabljajo v realnem gospodarstvu, centralizirane virtualne valute pa samo na strani oziroma virtualnem prostoru izdajatelja.

2.2 Funkcije bitcoina kot valute

Po Mankiwu (2011, str. 325) mora dobra valuta (oziroma širše denar) opravljati tri glavne funkcije, in sicer: vlogo menjalnega posrednika, obračunske enote in hranilca vrednosti.

Vse tri funkcije bom preučil z analizo posameznih značilnosti, po katerih se bitcoin razlikuje pri posamezni funkciji v primerjavi s klasičnimi valutami fiat, pri čemer bom poskušal hkrati ugotoviti, ali omenjene razlike lahko pripomorejo k bolj množičnemu sprejetju bitcoina kot valute in posledično njegove uporabe.

2.2.1 Menjalni posrednik

Menjalni posrednik je stvar, ki jo kupec izroči prodajalcu ob nakupu dobrine ali storitve (Mankiw, 2011, str. 325). Uporablja se kot posrednik ob menjavi, da se izognemo nevšečnostim, ki bi sicer nastale ob blagovni menjavi (ECB, 2015, str. 23).

Kot menjalni posrednik se bitcoin od drugih klasičnih valut občutno razlikuje v transakcijskih stroških, hitrosti izvršbe transakcij, anonimnosti in transparentnosti, v tem, da ni zakonito plačilno sredstvo, stroških vzpostavitve sistema za sprejetje kot plačilno sredstvo, mrežnih učinkih, zahtevanem poznavanju delovanja sistema, možnostih glede reševanja težav in pomanjkanju kreditnega trga (Kancs, Ciaian, & Rajcaniova, 2015, str. 7). Vsaka izmed razlik bo v nadaljevanju podrobneje predstavljena.

Transakcijski stroški so pri transakcijah z bitcoini zaradi odsotnosti posrednikov in organov nadzora v primerjavi z drugimi načini plačevanja, kot so na primer plačilne kartice ali pa bančni transferji, nižji za vse deležnike. Plačati je namreč treba samo stroške vzdrževanja sistema (rudarjenja), in sicer s plačilom provizije rudarju, ki je transakcijo dodal v verigo blokov. Povprečni transakcijski stroški naj bi bili nižji od 0,0005 BTC oziroma 1 odstotek vrednosti transakcije. To je manj od 2 do 4 odstotkov, kot znašajo stroški prek spletnih plačilnih sistemov (oziroma manj od 8 do 9 odstotkov, kot znašajo stroški ob nakazilih, ki ne potekajo prek bančnih računov). Ob nakazovanju med državami z različnimi valutami se na ta način prav tako izognemo stroškom konverzije med različnimi valutami. Med članicami Evropske unije zaradi enotnega območja plačil v evrih (SEPA) bitcoinovi nizki transakcijski stroški sicer ne predstavljajo takšne prednosti. Evropska zakonodaja namreč zapoveduje, da morajo biti stroški prenosov med posameznimi članicami v evrih enaki kot znotraj države (EBA, 2014, str. 16–17). Zaradi nizkih transakcijskih stroškov ob plačilu z bitcoini trgovci velikokrat prenesejo na kupca prihranek, ki ga ustvarijo z razliko med transakcijskimi stroški, ki bi sicer nastali pri plačevanju z valuto fiat. Bitcoin je zelo primeren tudi za plačila majhnih vrednosti. Minimalni stroški so v primerjavi z drugimi plačilnimi posredniki namreč zelo nizki. Paypal si na primer vsakič zaračuna 0,30 USD (Lo & Wang, 2014, str. 6–7). Pri bitcoinu, če gre za bitcoin z dovolj veliko prioriteto, plačilo provizije ni potrebno.

Nizki transakcijski stroški torej lahko pripomorejo k bolj množičnemu sprejemu bitcoina kot valute.

Transakcije bitcoinov so **izvršene hitro**. V protokolu je namreč določeno, da naj bi se nov blok v verigo blokov v povprečju dodal vsakih 10 minut, česar se zaradi prilagajanja težavnosti iskanja rešitve kriptografske uganke tudi drži. Za zneske majhnih vrednosti lahko že na podlagi preverbe veljavnosti transakcije to razumemo kot veljavno. Pri zneskih večjih vrednosti pa je zaradi možnosti vej v verigi blokov in posledično rizika njenih razveljavitev smiselno počakati vsaj 6 potrditev v verigo blokov, preden transakcijo z gotovostjo lahko sprejmemo kot dokončno. Pri valutah fiat lahko predvsem pri mednarodnih plačilih zaradi večjega števila posrednikov (centralnih in lokalnih bank) na izvršitev čakamo tudi več dni. Tudi pri plačilih znotraj iste države oziroma denarnega območja se, če gre za plačila med računi različnih bank, pri valutah fiat plačila ne izvršijo takoj ob vnosu v sistem, saj se prenosi med bankami izvršujejo le nekajkrat dnevno.

Sistem Bitcoin v nasprotju s tradicionalnimi plačilnimi sistemi deluje 24 ur na dan. Posledično se v nasprotju s tradicionalnimi plačilnimi sistemi, pri katerih ob nepravočasnem procesiranju transakcij na izvršbo lahko čakamo od enega do več dni (na primer praznik, konec tedna), lahko izvršijo kadar koli (EBA, 2014, str. 17–18).

Hitrost izvršbe transakcij torej lahko pripomore k bolj množičnemu sprejemu bitcoina kot valute.

Sistem Bitcoin je **anonimen** in **transparenten**. V njem so uporabniki namreč predstavljeni samo z naslovi, med katerimi se bitcoini prenašajo. Zaradi odprtokodnosti programske opreme in zapisa vseh transakcij v javno knjigo nakazil pa je tudi transparenten. Transparentnost ga sicer dela le delno anonimnega, saj se lahko, če se z določenim naslovom poveže pravo identiteto uporabnika, javno vidi celotno zgodovino transakcij z omenjenim naslovom. Če je uporabnik previden in za vsako transakcijo generira nov naslov, pa to ne predstavlja tolikšnega problema. Poleg tega pa na trgu obstajajo specializirane storitve (angl. *mixers*), ki združujejo zneske več uporabnikov, ki jih razdelijo na manjše dele in pošljejo na različne naslove, s čimer še dodatno zakrijejo, komu zneski v resnici pripadajo (Böhme, Christin, Edelman, & Moore, 2015, str. 221–222). Ravno anonimnost je v začetni fazi najbolj pripomogla k uveljavljanju bitcoina kot plačilnega sredstva. Najbolj znana tržnica z nezakonitimi storitvami na spletu, imenovana Silk Road, naj bi med svojim delovanja namreč predstavljala skoraj polovico vseh transakcij v omrežju (Yermack, 2014, str. 6).

Plačevanje z valuto fiat (z izjemo poslovanja z gotovino) ni anonimno, saj je lastnik računa, na katerem se nahajajo denarna sredstva, pri banki poznan in ustrezno identificiran. Prav tako pa ni tako transparentno, saj vpogleda v glavno knjigo posamezne poslovne oziroma centralne banke nima vsak.

Anonimnost in transparentnost torej lahko pripomoreta k bolj množičnemu sprejemu bitcoina kot valute.

Bitcoin trenutno nikjer na svetu **ni zakonito plačilno sredstvo**. To pomeni, da njegovo sprejetje (na primer pri prodajalcu storitve) ni obvezno. Prav tako ni nujno, da bo dolžnik svoj dolg lahko poplačal z bitcoini (EBA, 2014, str. 13).

V nasprotju z bitcoinom je valuta fiat v državi oziroma denarnem območju, v katerem je izdana, zakonito plačilno sredstvo.

Dejstvo, da bitcoin ni zakonito plačilno sredstvo, torej ne pripomore k bolj množičnemu sprejemu bitcoina kot valute, saj je odločitev, ali bo sprejel bitcoine kot plačilo, prepuščena vsakemu posamezniku in ni obvezujoča.

Če se deležniki odločijo, da bodo sprejemali oziroma izvajali plačila v bitcoinih, so s tem povezani določeni **stroški vzpostavitve sistema**. Kupci morajo bitcoine pridobiti, kar lahko načelno storijo le z rudarjenjem (ki je drago) ali pa nakupom prek menjalnice, s čimer so povezani stroški nakazila valute fiat na menjalnico, stroški zamenjave za bitcoine in transakcijski stroški prenosa bitcoina (Yermack, 2014, str. 10). Podjetja pa morajo prav tako imeti ustrezno strojno in programsko opremo.

Tudi ob plačevanju z valuto fiat obstajajo določeni stroški vzpostavitve sistema, ki pa so predvsem zaradi standardizirane strojne in programske opreme ter možnosti najema za podjetja nižji. Kupci pa prav tako zaradi prejema plače, socialnih transferov, pokojnine ali pa štipendije v valuti fiat z njo razpolagajo že v osnovi in zato nimajo stroškov pridobitve.

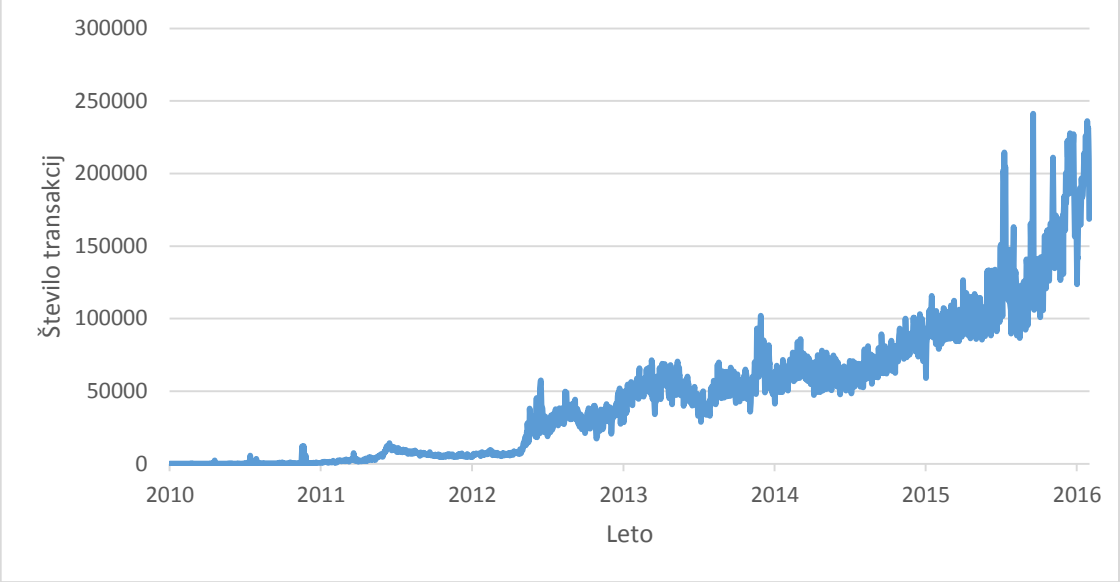
Zgoraj omenjeni začetni stroški torej ne pripomorejo k bolj množičnemu sprejemu bitcoina kot valute.

Teorija **mrežnih učinkov** pravi, da se porabnikova korist z velikostjo omrežja povečuje. Motivacija, da posameznik uporablja neki menjalni posrednik, je odvisna od stopnje njegove sprejetosti med trgovci. Podobno pa prav tako trgovci za plačevanje njihovih izdelkov oziroma storitev večinoma izberejo plačilno infrastrukturo, ki je najpogosteje v uporabi. Za nadaljnjo promocijo in sprejetje inovativnih plačilnih pristopov je tako pomembna dovolj velika kritična masa uporabnikov in tudi trgovcev (Polasik, Piotrowska, Wisniewski, Kotkowski, & Lightfoot, 2015, str. 19). Ravno majhna stopnja sprejetja je po mnenju ECB (2015, str. 23) glavni razlog, da bitcoin ni dober menjalni posrednik.

Leta 2014 je bilo po vsem svetu v povprečju z bitcoinom izvedenih 69.000,00 transakcij dnevno, medtem ko je bilo samo v Evropski uniji dnevno izvedenih 274 milijonov negotovinskih plačilnih transakcij (ECB, 2015, str. 16–17). Kot je razvidno iz Slike 13, se dnevno število transakcij z bitcoinom sicer povečuje. V letu 2015 je bilo povprečno število

dnevnih transakcij namreč 126.000,00, vendar pa to še vseeno predstavlja zanemarljiv delež v primerjavi z valutami fiat.

Slika 13: Dnevno število transakcij bitcoin med 1. 1. 2010 in 31. 1. 2016



Vir: Blockchain Info, 2016.

Problem mrežnih učinkov vsaj na kratek rok zadržuje rast in bolj množično uporabo bitcoina kot valute.

Poznavanje delovanja sistema je zaradi zaupanja v sistem izjemno pomembno. Z vidika uporabnika je sicer izvajanje transakcij zaradi preproste programske opreme preprosto, vendar pa povprečen uporabnik ne pozna, kako sistem Bitcoin deluje s tehničnega vidika. To pa pomeni, da mu mora zaupati.

Tudi pri plačevanju z valutami fiat povprečen uporabnik ne pozna sistema, vendar pa zaupa bančnim institucijam in centralni banki oziroma posredno državi.

Menim, da je nepoznavanje in posledično nezaupanje v sistem eden izmed glavnih razlogov, zakaj bitcoin ni bolj množično sprejet. Večina uporabnikov je poleg tistih, ki bitcoin uporabljajo samo zaradi anonimnosti, ali tehnoloških navdušencev, ali pa oseb, ki jih privlači dejstvo, da bitcoin ni povezan z nobeno oblastjo na svetu (Yermack, 2014, str. 7–8).

Transakcije Bitcoin so ob predpostavki poštenih rudarjev nepovratne in dokončne, kar otežuje **reševanje morebitnih težav**. Ko je transakcija enkrat izvršena, ji ni mogoče oporekati. To je lahko problem, če kupec želi izdelek vrniti ali pa nekega izdelka celo ni prejel, ali če je šlo za zmotno (na primer napačen znesek) ali pa celo nepooblaščeno (če

nam nekdo iz denarnice ukrade zasebne ključe) transakcijo. Kupec v takšnem primeru v nasprotju s plačevanjem z valutami fiat ni zavarovan (Böhme et al., 2015, str. 230). Za trgovce, ki sprejemajo bitcoine, pa je to sicer lahko tudi prednost, saj so zavarovani pred zlorabami, če kupec blago prejme in trdi, da ga ni prejel (EBA, 2014, str. 18).

Odsotnost institucije, prek katere bi se lahko reševale težave, ki lahko nastanejo pri plačevanju z bitcoini, vsaj pri kupcih izdelkov oziroma storitev zavira bolj množično uporabo bitcoina kot valute.

Ena izmed glavnih pomanjkljivosti pri plačevanju z bitcoini je **pomanjkanje kreditnega trga**. Plačilo blaga oziroma storitev je mogoče, samo če imamo na svojih naslovih zadostno število bitcoinov. Na večini trgov je dejstvo, da za nakup ne potrebujemo gotovine oziroma da nam v trenutku nakupa ni treba imeti celotnega zneska vrednosti nakupa na svojem denarnem računu, stalna praksa. Nakup z valuto fiat je v večini primerov namreč mogoč na kredit, ki ga financira prodajalec ali pa banka oziroma plačilne kartice (na primer Visa) in kartice z odloženim plačilom (na primer Diners). Tovrstna možnost je pri plačevanju z bitcoini otežena, saj za zdaj ne obstajajo kreditne kartice, ki bi bile denominirane v bitcoinih. Prav tako pa ne obstajajo niti bančna posojila, izdana v bitcoinih (Yermack, 2014, str. 11). Vzrok, zakaj banke v bitcoinih ne izdajajo posojil, je v tem, da bitcoina ne morejo izdati (ga pridobiti od centralne banke). Lahko ga pridobijo samo na trgu, na katerem pa je količina bitcoina v obtoku omejena. Ob pridobitvi bitcoina na trgu in izdaji posojila v bitcoinih pa bi se zaradi pomanjkanja izvedenih finančnih instrumentov z bitcoini zaradi njegove volatilnosti banke preveč izpostavile valutnemu tveganju.

Pomanjkanje kreditnega trga zavira rast bolj množičnega plačevanja z bitcoini in posledično bolj množičnega sprejetja in uporabe bitcoina kot valute.

2.2.2 Obračunska enota

Obračunska enota je merilo, ki ga uporabljamo za prikaz cen in zapis dolga (Mankiw, 2011, str. 325). Uporablja se kot standardna numerična enota za merjenje vrednosti in stroškov dobrin, storitev, sredstev in obveznosti (ECB, 2015, str. 23).

Kot obračunska enota se bitcoin od valut fiat občutno razlikuje predvsem v deljivosti in cenovni volatilnosti (Kancs et al., 2015, str. 12).

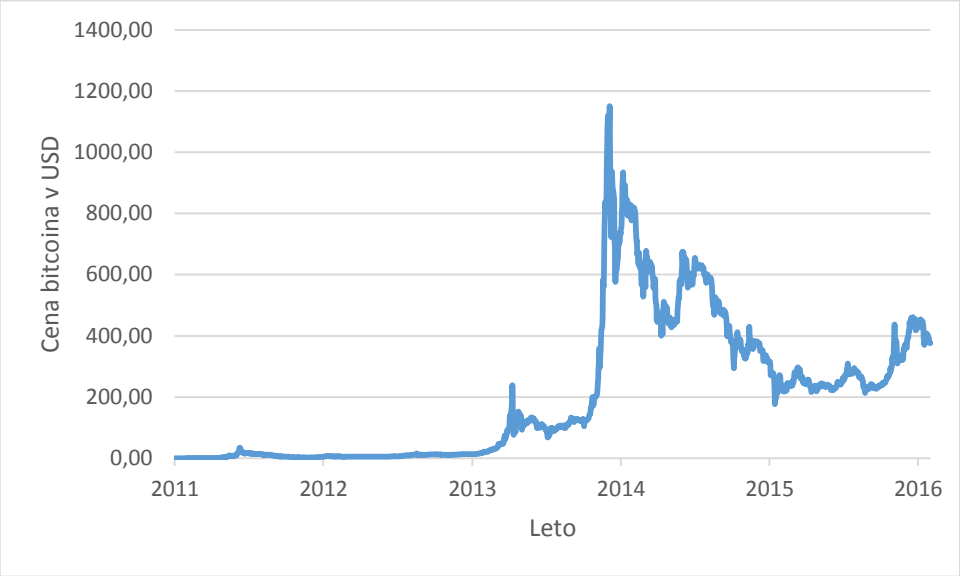
Bitcoin je **deljiv** na osem decimalnih mest. Po eni strani je to lahko prednost, saj ena najmanjša enota bitcoina, s katerim lahko plačujemo, ni nujno celo število. Glede na relativno visoko vrednost enega bitcoina je to po eni strani lahko pozitivno, saj je na ta način mogoče plačati tudi zneske, ki so v danem trenutku manjši od vrednosti enega bitcoina. Po drugi strani pa ima tudi negativno plat, saj je produkte manjših vrednosti (na primer žvečilni gumi, vžigalice, vrečke …) treba prikazati na več decimalnih mest (na

primer 0,005297 BTC). To pa je z vidika kupca lahko problematično, saj si je vrednost, če je ta izražena na več decimalnih mest, težko predstavljati. Še težje pa je takšne zneske med seboj vrednostno primerjati. Z deljivostjo imajo lahko težave tudi prodajalci, saj večina programske opreme zaradi lastnosti valut fiat vodenje omogoča samo na dve decimalni mesti (Yermack, 2014, str. 12–13).

Deljivost bitcoina po eni strani torej pripomore, po drugi pa zaradi težavne predstave vrednosti zavira bolj množično sprejetje kot valute.

Cena bitcoina je izjemno **volatilna**, kar je razvidno iz Slike 14.

Slika 14: Prikaz cene bitcoina v USD med 1. 1. 2011 in 31. 1. 2016



Vir: Blockchain Info, 2016.

Cena se je od leta 2011 pa do konca januarja 2016 vseskozi spreminjala, pri čemer je najnižja v omenjenem obdobju znašala 0,298998 USD, najvišja pa 1.151,00 USD. Bitcoin je začel pridobivati na vrednosti leta 2013, tj. v času ciprske krize, najvišjo vrednost pa je dosegel pred objavo kitajske centralne banke o omejitvah glede poslovanja z omenjeno virtualno valuto za njihove državljane, ki je povzročila padec.

Yermack (2014, str. 14–22) je po primerjavi cene bitcoina v USD v primerjavi z valutami EUR, JPY, GBP, CHF in zlatom v USD ugotovil, da se bitcoin obnaša bolj kot špekulativna naložba in ne kot valuta fiat. Podobno ob primerjavi volatilnosti bitcoina z volatilnostjo ameriškega delniškega trga pokažeta tudi Baek in Elbeck (2015, str. 30–33) z utemeljitvijo, da je trg z bitcoini bolj špekulativen in rizičen od delniškega. Na drugi strani pa Sapuric in Kokkinaki (2014, str. 255–264) opozarjata, da je pri izračunu bitcoinove

volatilnosti treba upoštevati tudi majhen volumen transakcij. Ob njihovem upoštevanju pa je prilagojena volatilnost bitcoina občutno manjša.

Večina študij dejavnikov, ki vplivajo na ceno bitcoina, je ugotovila, da ceno določajo: tržne sile povpraševanja in ponudbe po bitcoinu, njegova privlačnost ter globalno makroekonomsko in finančno stanje, pri čemer Kancs et al. (2014, str. 15–28) po analizi privlačnost bitcoina postavljajo na prvo mesto, takoj za tem pa povpraševanje in ponudbo po bitcoinu, medtem ko globalni dejavniki po njihovem mnenju nimajo bistvenega vpliva na ceno.

Glaser, Haferkorn, Weber in Zimmermann (2014, str. 1410–1415) ugotavljajo, da poročanje medijev o bitcoinu prav tako pomembno vpliva na njegovo ceno. Če gre za negativen zapis, je vpliv na ceno negativen, če gre za pozitiven zapis, pa pozitiven.

Ker se vrednost bitcoina na dnevni ravni v primerjavi z valutami fiat hitro spreminja, bi morali trgovci, ki sprejmejo plačevanje z njim, cene, objavljene v bitcoinih, pogosto preračunavati, kar bi bilo zanje drago, za kupce pa težje razumljivo. Dodaten problem povzroča tudi dejstvo, da se z bitcoinom trguje na različnih menjalnicah. Cene so med njimi v preteklosti variirale tudi do 7 odstotkov (Yermack, 2014, str. 12), ob čemer pa je treba poudariti, da je arbitraža[5] otežena. Hkraten nakup na eni in prodaja na drugi menjalnici zaradi lastnosti sistema Bitcoin namreč nista mogoča. Po nakupu bitcoina na prvi menjalnici bi bilo omenjeni bitcoin, da bi ga na drugi menjalnici lahko prodali, na drugo menjalnico treba namreč najprej prenesti. Ker gre v tem primeru za dve različni menjalnici, bi bila potrebna zavedba omenjene transakcije v verigi blokov (iz naslova Bitcoin prve, na naslov Bitcoin druge menjalnice). Ker pa se blok, v katerega so dodane transakcije v verigo blokov, doda v povprečju vsakih 10 minut, takojšen prenos ni mogoč. Poleg tega pa razlika v ceni bitcoina na posamezni menjalnici lahko izhaja tudi iz različne likvidnosti posamezne menjalnice.

Zaradi razlike v cenah med menjalnicami se trgovci lahko poslužujejo portalov, ki trenutno ceno bitcoina izračunavajo na podlagi indeksa, v katerega je glede na njihov obseg prometa hkrati vključenih več različnih menjalnic. Na ta način pa lahko le delno odpravimo težavo, saj še vedno ni mogoče natančno določiti stroškov pridobitve in odsvojitve bitcoinov (Yermack, 2014, str. 11–12). Večina trgovcev omenjeno težavo rešuje na dva mogoča načina. Po prvem trgovec ceno objavlja samo v lokalni valuti (lahko pa sočasno, kot približek, tudi v bitcoinih). Končna vrednost v bitcoinih pa se prikaže šele ob plačilu. V tem primeru je vrednost v bitcoinih določena glede na ceno, pridobljeno iz že omenjenih portalov (ali pa točno določene spletne menjalnice). Tovrsten način je prijaznejši do kupcev, saj jim bistveno ne spremeni nakupovalne izkušnje, na katero so navajeni. Je pa

[5] Arbitraža ali arbitražna priložnost (dobiček) pomeni možnost kupiti premoženje poceni na enem trgu in ga na kakšnem drugem trgu takoj prodati za višjo ceno. Arbitraža je torej hkratno nakupovanje in prodajanje premoženja z namenom ustvarjanja dobička iz razlike v ceni.

manj primeren za prodajalce, saj jih izpostavlja valutnemu tveganju. Posledično trgovci rajši uporabijo drugo možnost, pri kateri je v proces plačevanja vključen še plačilni posrednik, kot sta na primer Coinbase in BitPay. V transakciji je plačilni posrednik in ne trgovec tisti, ki od kupca prejme bitcoine, jih po trenutno veljavnem tečaju takoj pretvori v lokalno valuto in jo izplača trgovcu. Valutno tveganje za hrambo bitcoinov v daljšem časovnem obdobju ob določeni proviziji ki si jo zaračuna, torej v takšnem primeru nosi plačilni posrednik in ne trgovec. Posledično trgovec lahko sprejme plačilo v bitcoinih, ne da bi ga skrbelo nihanje vrednosti bitcoina v daljšem časovnem obdobju (Luther & White, 2014, str. 5–6).

Zaradi volatilnosti bitcoina načelno trgovci ob vračilu blaga kupcem ne vrnejo protivrednosti v bitcoinih, ampak jim ponudijo samo dobroimetje, ki ga naknadno lahko porabijo samo pri njih (Lo & Wang, 2014, str. 6).

Če povzamem, volatilnost bitcoina ne pripomore k bolj množičnemu sprejetju bitcoina kot valute, vendar pa predvsem z vidika trgovcev zaradi možnosti uporabe plačilnih posrednikov ne otežuje uporabe v tolikšni meri, kot se to zdi na prvi pogled.

2.2.3 Hranilec vrednosti

Hranilec vrednosti je stvar, s katero lahko zdajšnjo kupno moč prenesemo v prihodnost (Mankiw, 2011, str. 325). Posledično se omenjena stvar lahko v danem trenutku shrani in v prihodnosti ponovno pridobi oziroma uporabi (ECB, 2015, str. 23).

Kot hranilec vrednosti se bitcoin od drugih valut fiat občutno razlikuje v tem, da nanj ne delujejo inflacijski pritiski in da je pri njem zelo pomembna kibernetska varnost (Kancs et al., 2015, str. 13). Na tem mestu pa prav tako lahko omenimo tudi že zgoraj omenjeno cenovno volatilnost, ki se zaradi svoje nepredvidljivosti občutneje razlikuje od klasičnih valut fiat (Ali, Barrdear, Clews, & Southgate, 2014b, str. 279).

Valute fiat so večinoma inflatorne, kar pomeni, da se njihova vrednost skozi čas zmanjšuje, kar hkrati zmanjšuje njihovo sposobnost, da funkcionirajo kot hranilec vrednosti. Bitcoin zaradi nadzorovanega vnosa denarja v obtok v nasprotju z valutami fiat državnim institucijam ne omogoča vmešavanja v obliki manipulacije z inflacijo (**ni torej podvržen inflacijskim pritiskom**). Po drugi strani pa bo – glede na to, da bo eventualno v obtoku samo 21 milijonov bitcoinov – ta v prihodnosti najverjetneje podvržen deflacijskim pritiskom (Kancs et al., 2015, str. 13–14). Inflacijski in deflacijski pritiski so podrobneje predstavljeni v točki 2.5.1.

Na kratek rok dejstvo, da bitcoin ni podvržen inflacijskim pritiskom, lahko pripomore k bolj množičnemu sprejetju bitcoina kot valute, vendar pa se to v prihodnje zaradi morebitnih deflacijskih pritiskov lahko spremeni.

Skozi zgodovino je v preteklosti pomemben del obravnavanja valute kot hranilca vrednosti pomenil fizično varovanje pred njeno krajo, in sicer kot skrivanje denarja doma ali pa hrambe v banki. Pri bitcoinu pa je **kibernetska varnost** tista, ki je izjemnega pomena. Kdor ima namreč dostop do uporabnikove denarnice (in posledično zasebnih ključev), je tisti, ki lahko upravlja z bitcoini. Če je denarnica shranjena lokalno na uporabnikovem računalniku, je za varnost odgovoren on sam, če je hranjena pri ponudniku tovrstne storitve, pa omenjeni ponudnik. V obeh primerih je računalnik oziroma dostop do strežnika treba ustrezno zaščititi, s čimer pa so povezani stroški (Yermack, 2014, str. 14). Tudi pri valutah fiat je kibernetska varnost zelo pomembna, vendar pa v njihovem primeru večji del odgovornosti pade na banke, ki so odgovorne za morebitne napade na njihov sistem in so posledično ustrezno zaščitene. Prav tako pa ob spletnem bančništvu ustrezno stopnjo ravni zaščite zahtevajo tudi od svojih komitentov (certifikati, identifikacijske kartice, obvezna menjava gesel …).

Ker je ustrezna kibernetska varnost lahko draga, povprečni uporabniki (predvsem pri lokalni denarnici) niso ustrezno zaščiteni, javni ponudniki storitev pa so še bolj izpostavljeni morebitnim vdorom, kar lahko vodi v krajo in nezaupanje v sistem. Posledično menim, da zahteva za ustrezno kibernetsko varnost negativno vpliva na bolj množično sprejetje bitcoina kot valute.

V točki 2.2.2 omenjena cenovna volatilnost je pri bitcoinu kot hranilcu vrednosti v nasprotju s funkcijo bitcoina kot obračunske enote bolj problematična za bolj množično sprejetje bitcoina kot valute. Da je neka valuta kot plačilo sprejeta v sedanjosti, je namreč odvisno od njene pričakovane vrednosti v prihodnosti, torej pričakovanj glede njene prihodnje sprejemljivosti drugih deležnikov. Ob visoki cenovni volatilnosti pa je vnaprej njeno vrednost oziroma prihodnjo sprejemljivost težko predvideti (Lo & Wang, 2014, str. 11–12). Zaradi velike volatilnosti v bitcoinih ni smiselno varčevati, saj je valuta preveč izpostavljena špekulacijam.

2.3 Načini pridobitve bitcoina

Po Plassarasu (2013, str. 8) je bitcoine mogoče pridobiti na tri načine:

- z zamenjavo za valuto fiat;
- z zamenjavo za blago ali storitve;
- z rudarjenjem.

Zamenjava za valuto fiat (ali pa celo za drugo virtualno valuto) je najpogostejša in se lahko zgodi neposredno med dvema udeležencema v menjavi ali pa prek izbrane menjalnice. Menjalnice bom v nadaljevanju zaradi najpogostejše uporabe tudi podrobneje predstavil. Rudarjenje za povprečnega uporabnika zaradi zahtevne strojne opreme in visokih stroškov ni zanimivo, kot je bilo že podrobneje obrazloženo pod točko 1.2.4. Zamenjava za blago ali

storitve pa prav tako v večini primerov poteka prek trgovcev oziroma plačilnih posrednikov, omenjenih pod točko 2.2.2.

Menjalnica z bitcoini je neke vrste spletni trg, na katerem lahko uporabniki bitcoin ali pa drugo virtualno valuto zamenjajo za valuto fiat oziroma drugo virtualno valuto in nasprotno. Večina jih podobno kot pri tradicionalnih finančnih trgih uporablja dvojno avkcijo s povpraševanjem in ponudbo, za kar si zaračuna provizijo, ki znaša od 0,2 do 2 odstotka (Böhme et al., 2015, str. 220).

V menjalnici lahko uporabnik kupi in proda bitcoine po trenutno veljavnem razmerju glede na želeno valuto. Poleg tega pa jih lahko v menjalnici tudi »hrani« (seveda ne dejansko, ampak posredno prek zasebnega ključa). Ob prodaji mora uporabnik iz svoje denarnice v denarnico, ki jo zanj oblikuje menjalnica, najprej prenesti bitcoine. Uporabnik potem lahko trguje le z bitcoini, ki so dostopni prek denarnice, hranjene pri menjalnici. Posledično to pomeni, da zasebni ključ omenjene denarnice hrani menjalnica, zato je izbira menjalnice, ki ji lahko zaupamo, izjemno pomembna. Nakazila bitcoin v menjalnico in iz menjalnice so zavedena kot transakcije v verigi blokov, medtem ko so transakcije, ki so izvršene v okviru trgovanja na menjalnici, zapisane samo v evidencah dotične menjalnice (Bhaskar & Chuen, 2015, str. 559–560).

Menjalnice so zaradi hrambe ključev podvržene kibernetskim napadom. Moore in Christin (2013, str. 1–7) sta ugotovila, da je pri bolj priljubljenih menjalnicah verjetneje, da bo prišlo do kršitve varnosti. Prav tako sta potrdila domnevo, da je možnost preživetja posamezne menjalnice odvisna od povprečnega števila transakcij, izvedenih na omenjeni menjalnici.

Menjalnica Mt. Gox, ki je leta 2013 predstavljala 70 odstotkov vseh transakcij, izvršenih na menjalnicah, je v svoji zgodovini občutila kar nekaj kibernetskih napadov. Leta 2011 jo je eden izmed napadov stal 8,750.000,00 USD. Februarja 2014 pa je zaradi izgube skoraj 750.000,00 bitcoinov tudi propadla (Bhaskar & Chuen, 2015, str. 563–564).

Večina menjalnic je uradno registrirana, vendar zaradi pomanjkanja ustrezne zakonodaje nenadzorovana (odvisno od države, v kateri so registrirani in v kateri poslujejo). V nasprotju z nadzorovanimi menjalnicami nenadzorovane menjalnice niso podvržene zahtevam po kapitalski ustreznosti. Tovrstne menjalnice tudi niso ustrezno zavarovane, kar je z vidika uporabnikov problematično, če pride do zgoraj omenjenih kršitev varnosti (Bhaskar & Chuen, 2015, str. 569).

2.4 Vrste denarnic

Kot je omenjeno v točki 1.2.3, v denarnicah niso hranjeni bitcoini, ampak zasebni ključi, s pomočjo katerih podpišemo transakcijo Bitcoin in s tem prenesemo lastništvo bitcoinov iz svojega naslova na naslov drugega uporabnika.

Kljub analogiji v imenu med denarnico Bitcoin in fizično denarnico obstajajo pomembne razlike (Franco, 2015, str. 123):

- fizična denarnica vsebuje fizični denar, zato je ni mogoče skopirati, pri denarnici Bitcoin pa je to mogoče. Kdor koli ima v lasti kopijo denarnice, lahko zapravi sredstva, ki jih je mogoče podpisati z njenimi zasebnimi ključi;
- denarnico Bitcoin je mogoče distribuirati skozi več naprav na način, da se za dostop do sredstev zahteva sodelovanje med vsemi omenjenimi napravami. To je mogoče doseči z večkratnim podpisovanjem (angl. *multisignature*);
- pri bitcoinu obstaja možnost denarnic tipa »samo prejem«; tovrstne denarnice hranijo samo javne ključe in naslove ter so namenjene samo preverjanju stanja in transakcij; z njimi podpisovanje transakcij in posledično porabljanje bitcoinov ni mogoče.

Denarnice delimo glede na njihovo povezljivost v internetno omrežje (Pacia, 2013c), in sicer na:

- denarnice, nameščene na napravi, ki je povezana na internet; pravimo jim tudi vroče denarnice (angl. *hot wallet*);
- denarnice, nameščene na napravi, ki ni povezana na internet; pravimo jim tudi hladna shramba (angl. *cold storage*).

Ker je vsaka naprava, ki je povezana v internetno omrežje, potencialno podvržena kibernetskim napadom, je najbolj smiselno, da imamo v denarnicah, ki so povezane na internet, hranjene samo bitcoine, s katerimi operiramo na dnevni bazi. Preostale bitcoine pa hranimo na napravi, ki ni povezana v internetno omrežje (Franco, 2015, str. 123).

Z uporabniškega vidika obstajajo tri vrste denarnic, in sicer: denarnice, katerih programsko opremo si na osebni računalnik naložimo sami (na primer osnovna programska oprema Bitcoin), spletne denarnice in mobilne denarnice (Pacia, 2013c).

Z vidika povprečnega uporabnika so zanimive predvsem spletne denarnice, kot sta Blockchain in Coinbase, s ponujanjem oblačnih storitev. Poleg preproste prijave in upravljanja z uporabnikovimi ključi namreč omogočajo izjemno nizke provizije pri transakcijah, izvedenih med njenimi člani, ter takojšnjo izvršitev tovrstnih transakcij. Tovrstne transakcije namreč niso zavedene v verigi blokov, ampak podobno kot pri menjalnicah samo v evidence spletne denarnice. Tudi pri spletnih denarnicah je treba biti

previden pri izbiri in izbrati takšno, ki ji res zaupamo. V nasprotju z bankami namreč niso ustrezno nadzorovane, prav tako pa tudi ne kapitalsko ustrezne. Ob insolventnosti so sredstva tako izgubljena. Posledično je pomembno, da spletne denarnice večino sredstev oziroma zasebnih ključev prav tako hranijo v denarnicah, ki niso povezane v internetno omrežje (Franco, 2015, str. 131).

2.5 Ekonomski vidik

V tem podpoglavju bom najprej predstavil temelje bitcoina v ekonomski teoriji in probleme, ki se z bitcoinom kot valuto lahko pojavijo zaradi omejene količine denarja v obtoku. Sledila bo utemeljitev razlogov rasti stroškov rudarjenja. Na koncu podpoglavja bo predstavljena tudi problematika dolgoročnega vzdrževanja nizkih ravni provizij.

2.5.1 Temelji bitcoina v ekonomski teoriji in deflacija

Najzanimivejši značilnosti bitcoina z ekonomskega vidika sta nadzorovana rast ponudbe denarja v obtoku (v povprečju se vsakih 10 minut število izdanih bitcoinov poveča, pri čemer se vnos v obtok skozi čas geometrično zmanjšuje, tako da se približno vsaka štiri leta prepolovi) in omejena končna izdana količina bitcoinov (približno 21 milijonov).

Zgornji dve značilnosti sta bili v sistem Bitcoin implementirani z namenom, ki ga je mogoče posredno razbrati iz Nakamotovega (2008, str. 1–9) izvirnega članka in njegovih naknadnih komentarjev, in sicer da bitcoin ni pod neposrednim vplivom denarne politike določene države in političnih odločitev ter posledično ni podvržen nestabilnostim, kot je na primer inflacija.

O inflaciji govorimo takrat, ko pride do splošnega zvišanja ravni cen izdelkov in storitev. Zaradi tega lahko za 1 evro kupimo manj – ali povedano drugače: evro je vreden manj kot pred omenjenim zvišanjem ravni cen.

Bitcoin ima glede na zgornji značilnosti svoje temelje delno v šoli avstrijskih ekonomistov (ECB, 2012, str. 22) in Friedmanovega »k-odstotnega« pravila rasti (Böhme et al., 2015, str. 233).

Šola avstrijskih ekonomistov verjame, da povečana količina denarja v obtoku nedvoumno vodi v povečanje cen in ekonomsko nestabilnost. Zanje inflacija ni povečanje cen, ampak povečanje ponudbe denarja v obtoku. Za deflacijo pa šola avstrijskih ekonomistov meni, da lahko nastane zaradi tehnološkega napredka ali pa zmanjšanja ponudbe denarja v obtoku, pri čemer je problematična samo zadnja. Posledično zagovarjajo fiksno ponudbo denarja. Avstrijska šola je znana tudi po teoriji glede kreiranja denarja, ki je predstavljena v tako imenovanem Misesovem teoremu. Po njem ima valuta danes vrednost, ker njeni imetniki pričakujejo, da jo bodo jutri lahko uporabili za zamenjavo dobrin in storitev. Današnja

vrednost je bila posledično prenesena iz včerajšnje. V preteklosti je posledično valuta morala biti vezana na neko dobrino, od katere je lahko prevzela vrednost. Za valute fiat tej teoriji lahko pritrdimo, glede na to, da so bile v preteklosti vezane na plemenite kovine, kot je na primer zlato. Za bitcoin pa tega ne moremo potrditi, saj ob izdaji ni bil vezan na neko prej določeno vrednost (Franco, 2015, str. 21–22). Prav tako se bitcoin ne sklada z Haykovo denarno teorijo, po kateri vlade ne bi smele imeti monopola nad izdajanjem denarja, ampak bi ga morale v obliki certifikatov izdajati zasebne banke, pri čemer bi se obdržali samo certifikati, ki bi bili najučinkovitejši (ECB, 2012, str. 22). Bitcoina namreč ne izdajajo zasebne banke.

Milton Friedman je leta 1960 predlagal, da bi za nadzorovanje inflacije letna količina denarja morala rasti po vnaprej določenem razmerju (ne glede na cikel, v katerem se gospodarstvo trenutno nahaja). Vsakoletna rast naj bi bila takšna, kot je rast realnega bruto družbenega proizvoda (Peters, Panayi, & Chapelle, 2015, str. 13). V nasprotju z omenjeno teorijo je bitcoinova rast geometrično padajoča (in neodvisna od realnega gospodarstva) in končno omejena.

V takšnem primeru se je treba vprašati, kaj se zgodi, če gospodarstvo raste z drugačno hitrostjo kot količina denarja v obtoku. Ravno fiksna končna količina in počasna rast količine denarja v obtoku sta po mnenju ekonomista Paula Krugmana zaradi možnosti pojava deflacije glavna problema bitcoina, če bi bil ta bolj množično uporabljan (Krugman, 2011).

Barber, Boyen, Shi in Uzun (2012, str. 6) so zaradi pojava morebitne deflacijske spirale ob predpostavki omejene končne količine denarja v obtoku prišli do podobnega zaključka.

Deflacijska spirala je ekonomski pojav, ko neobvladljiva deflacija lahko vodi v propad določene valute. Deflacija pomeni padec splošne ravni cen. Nastane lahko, ko cena blaga in storitev, merjena relativno glede na določeno mero, pade. Ni pa nujno, da nastane zaradi znižanja vrednosti cen določenega blaga ali storitev. Lahko se namreč zgodi, da naraste samo vrednost valute, v kateri so blago ali pa storitve merjeni. Deflacijska spirala se pojavi, ko se vrednost določene valute kot posledica kopičenja (angl. *hoarding*) relativno povečuje glede na vrednost dobrin v določenem gospodarstvu. Valuto posamezniki zadržujejo oziroma kopičijo, ker predpostavljajo, da bodo v prihodnosti lahko kupili več dobrin za manj denarja. Kot posledica se ustvari cikel, v katerem se zaradi pomanjkanja dostopnosti do valute cene dobrin dodatno znižajo, kar še dodatno poveča kopičenje valute (Peters et al., 2015, str. 13).

Ron in Shamir (2013, str. 7) sta ugotovila, da do maja 2012 več kot polovica izdanih bitcoinov še ni bila udeležena v nobeni transakciji, kar bi lahko nakazovalo na kopičenje bitcoinov.

Dodaten problem predstavlja tudi tako imenovano uničenje bitcoinov. Bitcoini sicer ne morejo biti dobesedno uničeni, vendar pa izguba zasebnih ključev (če na primer trdi disk, na katerem so shranjeni, preneha delovati) ob predpostavki, da nimamo varnostne kopije, pomeni, da so izgubljeni za vedno. To pa je enako, kot če bi jih lahko uničili (Barber et al., 2012, str. 7).

Deflatorne valute so problematične, ker (Tasca, 2015, str. 58):

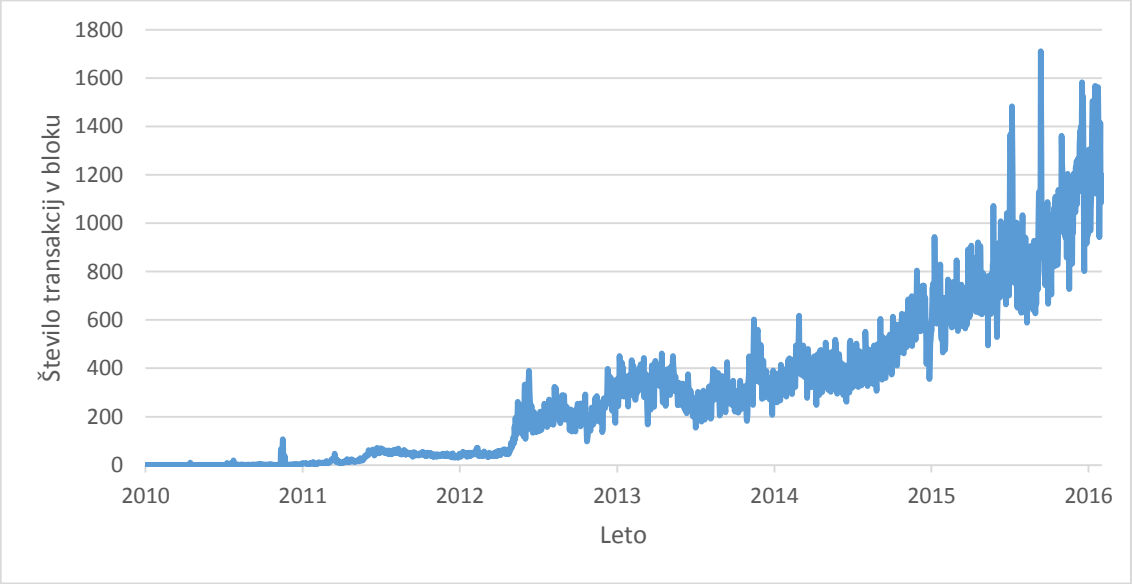
- povzročajo nezaposlenost, saj se plače ne prilagodijo navzdol ter zahtevajo neprestano prilagajanje cen in storitev;
- spodbujajo varčevanje namesto izposojanja (in posledično porabljanja) denarja;
- eventualno postanejo nelikvidne, drage in volatilne, kar jih dela manj uporabne, pri čemer jih je čedalje manj trgovcev pripravljenih sprejeti kot plačilo.

2.5.2 Rast stroškov rudarjenja

Stroški rudarjenja neprestano rastejo. To se dogaja zaradi dveh razlogov, in sicer zaradi povečevanja uporabe bitcoina kot menjalnega posrednika in prevelikega investiranja rudarjev v za rudarjenje namensko strojno opremo (Ali et al., 2014b, str. 282).

Zaradi povečane uporabe bitcoina se povečuje število transakcij v posameznem bloku, kar je razvidno iz Slike 15, in posledično tudi velikost bloka.

Slika 15: Povprečno število transakcij v bloku med 1. 1. 2010 in 31. 1. 2016

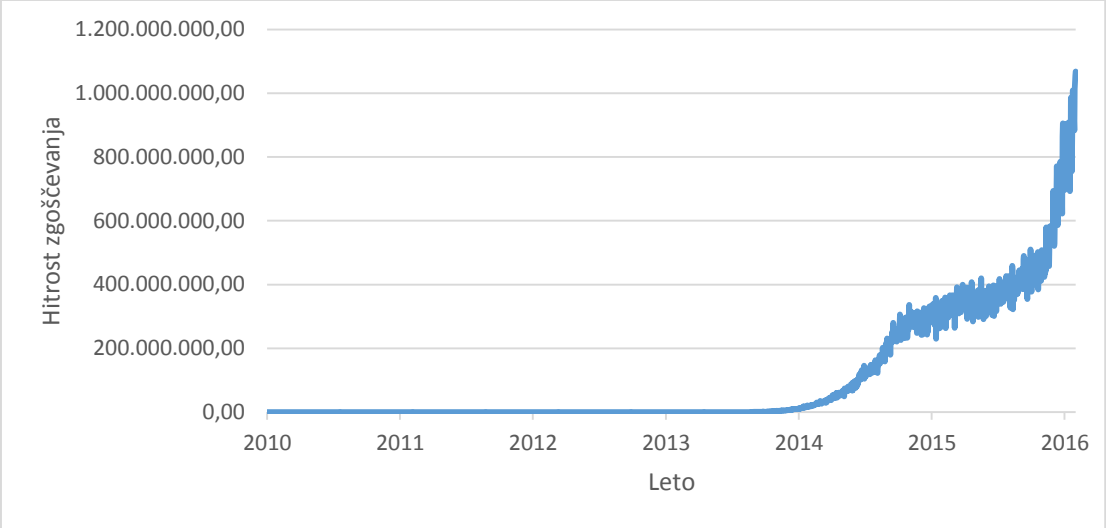


Vir: Blockchain Info, 2016.

Povečano število transakcij in velikost bloka imata neposreden vpliv na stroške rudarjenja, saj rudarji porabijo več pasovne širine njihovega internetnega ponudnika, prav tako pa tudi posreden vpliv na stroške, saj se z večanjem števila transakcij podaljšuje tudi čas vključevanja transakcij v blok prek rudarja. To namreč pomeni, da ima rudar manj časa za rešitev kriptografske uganke. Z večjim številom transakcij pa se veča tudi velikost bloka in s tem čas, da se ga razširi in kot prvega pravilnega sprejme v celotnem omrežju. To pa povečuje verjetnost, da bo blok, ki ga je rudar dodal v verigo blokov, osirotel (da ga bo torej nadomestil blok drugega rudarja, ki je ob istem času našel rešitev uganke, in sicer ob predpostavki, da bo ta postal del daljše verige).

Večja kot je računska moč posameznega rudarja, več prihodka lahko pričakuje, da bo ustvaril. Posledično rudarji neprestano vlagajo v boljšo strojno opremo, ki pa samo povečuje računsko moč celotnega omrežja, katere rast je razvidna iz Slike 16. Posledično se prav tako zaradi zmožnosti prilagajanja povečuje težavnost rudarjenja. Vsak posamezen rudar namreč ne upošteva negativnih učinkov, ki jih bo povzročil z nakupom omenjene strojne opreme na preostale rudarje, ki bodo posledično prav tako bili prisiljeni v nadaljnje investiranje. V teoriji bi tako v hipotetičnem ravnovesju vsi rudarji neučinkovito preveč investirali v novo strojno opremo, za kar pa bi na koncu prejeli isti prihodek (Ali et al., 2014b, str. 282).

Slika 16: Hitrost zgoščevanja med 1. 1. 2010 in 31. 1. 2016



Vir: Blockchain Info, 2016.

Slika 16 predstavlja ocenjeno hitrost zgoščevanja celotnega omrežja med 1. 1. 2010 in 31. 1. 2016. Hitrost zgoščevanja je mera procesne oziroma računske moči omrežja bitcoin, ki nam pove, koliko giga (milijard) zgoščevalnih funkcij je izvedenih vsako sekundo. Kot je razvidno iz Slike 16, se je hitrost zgoščevanja začela povečevati konec leta 2013, tj. z začetkom uporabe za rudarjenje namenske strojne opreme ASIC.

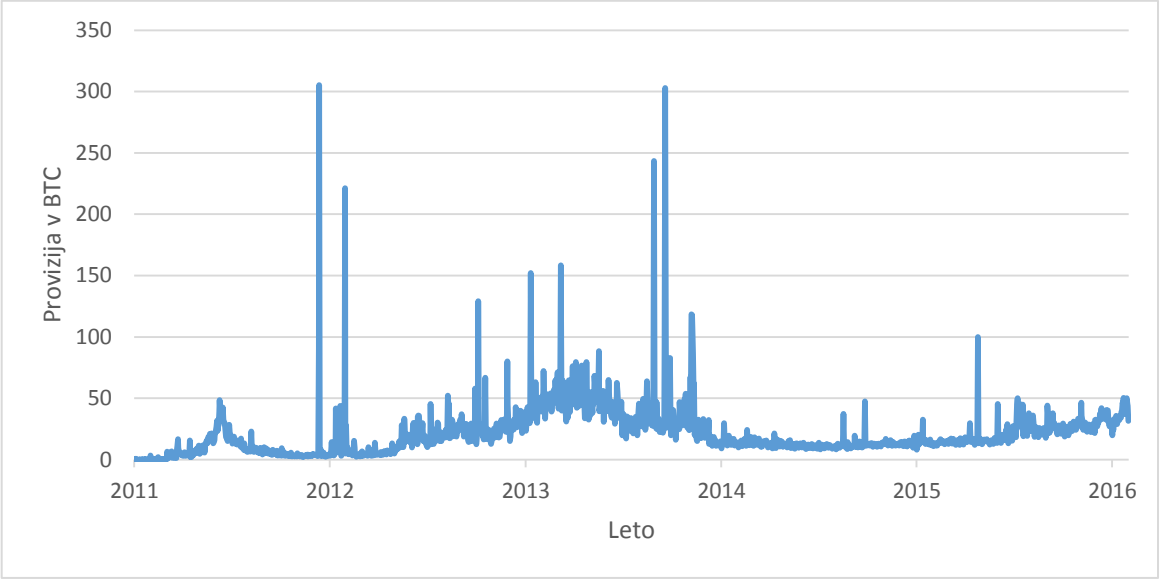
2.5.3 Problem dolgoročnega vzdrževanja nizkih ravni provizij

Posamezen rudar je spodbujen, da v blok doda transakcijo, ki ponuja kakršno koli provizijo. Rudar je namreč na boljšem, če sprejme provizijo, čeprav je ta majhna, kot pa če bi transakcijo izpustil. Čeprav si rudarji želijo, da bi bile provizije višje, se vsak rudar zaveda, da bo tovrstno transakcijo v verigo blokov, če je ne bo on sam, vključil eden izmed preostalih rudarjev. Tudi če bi se vsi rudarji dogovorili, da tovrstnih transakcij ne bi sprejemali, bi se verjetno našel nekdo, ki bi rudaril pod anonimnim imenom in transakcijo vseeno vključil. Za posameznika je torej smiselno, da rudarju dodeli provizijo, vendar ne preveliko. Ob dodelitvi prevelike provizije bi se namreč po nepotrebnem odrekel določeni vrednosti, ki pa mu ne bi prinesla dodatne koristi (Kroll, Davey, & Felten, 2013, str. 12).

Zgoraj omenjeno seveda velja pod predpostavko, da je v danem trenutku transakcij manj, kot pa jih je mogoče vključiti v posamezen blok. Velikost posameznega bloka je namreč približno 1 MB (Möser & Böhme, 2014, str. 3).

Slika 17 prikazuje skupni dnevni prihodek rudarjev v bitcoinih na podlagi provizij.

Slika 17: Skupni dnevni prihodek rudarjev v bitcoinih na podlagi provizij med 1. 1. 2011 in 31. 1. 2016



Vir: Blockchain Info, 2016.

Od zadnjega zmanjšanja nagrade s 50 na 25 bitcoinov, ki se je zgodilo 28. 11. 2012, pa do 31. 1. 2016 je v povprečju skupni dnevni prihodek vseh rudarjev na podlagi provizij znašal 26,11 bitcoina. Če predpostavimo, da bi v omenjenem obdobju v povprečju dnevno moralo biti kreiranih 3.600,00 novih bitcoinov (6 ustvarjenih blokov na uro pomnoženo s 24 ur

pomnoženo s 25 izdanih bitcoinov na blok), lahko vidimo, da so provizije v omenjenem obdobju predstavljale zanemarljiv delež prihodka rudarjev.

Zaradi manjšanja nagrade za rudarje in nizkih provizij se posledično dolgoročno pojavi tudi vprašanje glede ekonomičnosti stroškov rudarjenja. Če bo na dolgi rok za rudarje ceneje kupiti bitcoine, kot pa jih rudariti (oziroma bo, ko nagrade ne bo več, rudar lahko služil samo s provizijami), rudarji ne bodo imeli več motivacije opravljati svojega dela. V takšnem primeru se lahko zgodi, da bo večina rudarjev prenehala rudarjenje. Posledično se bo znižala težavnost rudarjenja, tako da bo določeno število rudarjev sicer verjetno še vedno obstajalo, vendar pa je sistem v takšnem primeru dovzetnejši za morebiten napad. Da bi se temu lahko izognili, bo za vzdrževanje dovolj velike računske moči omrežja rudarje treba ustrezno nagraditi, kar bo mogoče samo z dvigom provizij (Kaşkaloğlu, 2014, str. 93–98).

To pa bi bitcoinu lahko odvzelo eno izmed glavnih konkurenčnih prednosti v primerjavi s plačevanjem z valutami fiat. Dolgoročno bo tako politiko provizij treba nastaviti tako, da bo na eni strani obstajalo zadostno število aktivnih rudarjev, na drugi strani pa provizije ne bodo tako visoke, da bi uporabniki z bitcoinom prenehali plačevati. Tega po mojem mnenju ne bo mogoče prepustiti v uravnavanje samemu sistemu, ampak bo treba omenjeno politiko implementirati v protokolu.

2.6 Zakonodajnopravni vidik

Največ preglavic za ustrezno obravnavo bitcoina z vidika zakonodaje (predvsem regulacije) povzročata dve izmed njegovih glavnih prednosti, in sicer anonimnost in decentralizacija. Virtualne valute za zdaj v nobeni državi na svetu nimajo statusa zakonitega plačilnega sredstva in ne spadajo v definicijo tradicionalnega denarja fiat. To pomeni, da načelno ne morejo biti obravnavane z vidika obstoječe napisane zakonodaje. Posledično so se posamezne države oziroma njihove institucije (centralne banke, različni nadzorni organi …) do bitcoina oziroma virtualnih valut na splošno odzvale vsaka po svoje. V nekaterih primerih tudi različne institucije znotraj iste države bitcoina ne obravnavajo na enak način.

Njihove odzive lahko razvrstimo v štiri kategorije, in sicer: opozorila, izjave in pojasnila glede njihovega zakonitega statusa, odredbe glede licenciranja in nadzora ter izdaje prepovedi uporabe (ECB, 2015, str. 30). Ustrezna regulacija tehnološkemu razvoju po navadi namreč sledi šele čez nekaj let (ECB, 2012, str. 44).

Na podlagi omenjenih odzivov pa lahko posamezne države umestimo v tri mogoče tipe jurisdikcij, in sicer: sovražne, striktne in odprte (Tasca, 2015, str. 47–48).

Med sovražne jurisdikcije spadajo Bangladeš, Bolivija, Kirgizija, Ekvador in Islandija, ki so prepovedale uporabo bitcoina. V Islandiji zaradi leta 2008 postavljenih kapitalskih kontrol sicer velja samo prepoved nakupovanja, ne pa tudi prodajanja bitcoinov (Tasca, 2015, str. 47).

Med striktne jurisdikcije spadajo Kitajska, Tajska, Rusija, Indija, Indonezija, Jordanija, Libanon, Tajvan in Vietnam, pri katerih ima uporaba bitcoina določene omejitve. Kitajska je na primer prepovedala nakup dobrin in storitev z bitcoinom, omogoča pa trgovanje z njim. Menjalnicam, ki so locirane na Kitajskem, je predpisala, da morajo o svojih uporabnikih poročati regulatorju z namenom preprečevanja pranja denarja.

Pri zgoraj omenjenih je treba vzeti v obzir, da kljub stališčem posamezne države prepoved ali omejitev še ne pomeni, da njihovi državljani z bitcoinom tudi v praksi ne morejo trgovati ali pa ga uporabljati za plačilo, saj je to zaradi narave bitcoina in globalne uporabe izjemno težko doseči. Uporabniki so v določeni meri samo omejeni. Na Kitajskem na primer ne morejo v njihovih trgovinah kupovati z bitcoinom, vendar pa to lahko počnejo drugje po svetu (zaradi razširjenosti interneta to namreč ni problem).

V Rusiji so v letu 2015 izdali opozorilo, v katerem so virtualne valute nadomestek denarja, s katerim se lahko igrajo, ne smejo pa ga uporabljati kot plačilno sredstvo. Pričakuje se, da bodo v kratkem uredili zakonodajo na način, da bo tistemu, ki virtualno valuto oblikuje ali pa izda, dodeljena globa (Tasca, 2015, str. 47–48).

Med virtualnim valutam odprte jurisdikcije lahko štejemo Združene države Amerike (v nadaljevanju ZDA), evropske države, Kanado, Japonsko in Avstralijo. Omenjene države se najbolj ukvarjajo s tem, kako opredeliti virtualne valute, in sicer ali kot blago (angl. *commodities*) ali pa kot valute (Tasca, 2015, str. 48).

V ZDA je njihov zvezni organ za preprečevanja finančnega kriminala (angl. *Financial crimes enforcement network*) izdal navodila, v katerih razlikuje med uporabniki, administratorji in izmenjevalci. Uporabniki v nasprotju z administratorji (z izjemo rudarjev, ki virtualno valuto pridobivajo za lasten namen) in izmenjevalcev niso podvrženi registraciji in poročanju. Administratorji in izmenjevalci se obravnavajo kot podjetja, ki se ukvarjajo z denarnimi storitvami in ki so posledično podvržena pravilom, ki veljajo za preprečevanja pranja denarja in skrbnega preverjanja strank. Regulacija se podrobneje razlikuje po posameznih zveznih državah. V New Yorku morajo na primer finančni posredniki zaprositi za licenco, imenovano Bitlicence (Tasca, 2015, str. 48–51). Prav tako so se do bitcoina drugače opredelile ameriške nadzorne institucije. Ameriški davčni urad (angl. *Internal revenue service*) je na primer bitcoin definiral kot lastnino (angl. *property*), Komisija za blagovne terminske posle (angl. *Commodity futures trading commission*) pa kot blago (Parker, 2015).

Situacija v Evropski uniji je precej drugačna v primerjavi z ZDA. Ne obstaja namreč zakon, direktiva ali pa regulativa, kar bi izdala določena institucija, ki bi posebej obravnavala področje virtualnih valut in bi posledično veljala za vse države v Evropski uniji. Prav tako ni jasne definicije, kaj bitcoin je. Decembra 2013 je EBA (Evropski bančni organ, str. 1–3) izdal opozorilo uporabnikom glede kupovanja, hrambe in trgovanja z virtualnimi valutami, julija 2014 (EBA, str. 44) pa še mnenje, v katerem finančne institucije ozavešča ter jim odsvetuje kupovanje, hrambo in trgovanje z virtualnimi valutami. Prav tako je predlagal, da bi menjalnice postale obvezujoče izpolnjevati standarde za preprečevanje pranja denarja in financiranja terorizma, kar pa se na ravni Evropske unije za zdaj še ni zgodilo. Tako je odločitev, kako obravnavati bitcoin in preostale virtualne valute, za zdaj prepuščena posameznim državam. Na Švedskem so na primer objavili, da bitcoin ni valuta, se pa morajo menjalnice registrirati pri finančnem nadzorniku. V Nemčiji so bitcoin opredelili kot obračunsko enoto, ki ni zakonito plačilno sredstvo in se obravnava kot finančni instrument, vendar pa za uporabo, trgovanje in za rudarjenje ne potrebuje odobritve (ECB, 2015, str. 29–31).

2.7 Uporabnost bitcoina

Motivi za uporabo bitcoina so lahko različni. Po Mas in Chuen (2015, str. 443–447) jih lahko razdelimo na motiv po doseganju anonimnosti in priročnosti ter na previdnostni in špekulativni motiv. Dodatno je bitcoin uporaben tudi v državah z omejitvami pretoka kapitala in državah tretjega sveta, ki niso ustrezno pokrite s finančno infrastrukturo.

V osnovi je ravno anonimnost (oziroma delna anonimnost) ena izmed glavnih prednosti bitcoina pred valutami fiat. To se je pokazalo že kmalu po začetku vzpostavitve in delovanja sistema. Kot prvi uporabniki so se namreč pojavili ravno posamezniki, ki so iskali lastnosti, ki so bile drugje težko dosegljive, in sicer večjo anonimnost ob odsotnosti pravil glede nakupov in prodaj storitev in izdelkov. Ob hkratni uporabi omrežja Tor (ki anonimizira uporabnikovo lokacijo in njegovo uporabo internetnega prenosa podatkov) z bitcoinom je namreč mogoče doseči visoko stopnjo anonimnosti. Tako se je na temačnih straneh interneta (angl. *dark web*) februarja leta 2011 pojavila spletna tržnica, imenovana Silk road, na kateri je bil izključno z bitcoinom mogoč nakup nezakonitih dobrin, in sicer predvsem drog. Takoj po pojavu omenjene tržnice naj bi se v naslednjem letu volumen transakcij z bitcoini povečal za 15 milijonov dolarjev. FBI je oktobra 2013 omenjeno tržnico sicer zaprl, vendar pa so se kmalu po tem pojavile nove (Böhme et al., 2015, str. 222–223).

Anonimnost je prav tako zelo uporabna lastnost za igralce iger na srečo. Ena izmed takšnih iger je na primer Satoshi dice, v kateri igralec zmaga, če je številka, ki jo naključno generira igralnica, manjša od številke, na katero je igralec stavil. Med junijem 2012 in majem 2013 naj bi v določenih trenutkih plačila majhnih vrednosti, ki so nastala na podlagi

omenjene storitve, predstavljala celo do 80 odstotkov vseh transakcij v omrežju Bitcoin (Möser & Böhme, 2014, str. 7–10).

Kot sem pokazal v prejšnjih poglavjih, je plačevanje z bitcoinom izjemno priročno. Transakcije je mogoče izvajati 24 ur dnevno, in sicer vse dni v letu. Provizije pri transakcijah so občutno nižje kot pri drugih plačilih, kar je dobro predvsem pri plačilih nizke vrednosti. Priročne lastnosti so tudi hitrost potrjevanja transakcij (predvsem pri plačilih nizke vrednosti) in nizki stroški pri mednarodnih nakazilih. Največjo korist od omenjenih lastnosti imajo trgovci, saj imajo nižje stroške, kot bi jih imeli pri plačevanju s kreditnimi in plačilnimi karticami, poleg tega pa so manj podvrženi morebitnim zlorabam kupcev, ki trdijo, da izdelkov niso prejeli.

Iz previdnostnega motiva lahko bitcoin uporabljajo državljani ekonomsko in politično nestabilnih držav, da se izognejo investicijam, denominiranim v njihovi lokalni valuti. S tem namreč odpravijo riziko zmanjševanja vrednosti njihovega kapitala v lokalni valuti zaradi morebitne visoke inflacije, visoke obdavčitve ali pa celo zaplembe premoženja od države (Mas & Chuen, 2015, str. 444–445).

Hramba oziroma trgovanje z bitcoinom je mogoča/-e tudi zaradi špekulativnih namenov, če menimo, da bo njegova vrednost v prihodnosti narastla. Wu in Pandey (2014, str. 47–51) ugotavljata, da je bitcoin zelo slabo koreliran z drugimi valutami fiat, delniškim, obvezniškim in z nepremičninskim trgom. Posledično bi ga v majhnih količinah lahko hranili zaradi doseganja boljše razpršenosti samega investicijskega portfelja.

Bitcoin je prav tako lahko uporaben v državah z omejitvami pretoka kapitala (Brito & Castillo, 2013, str. 7). Kot primer lahko navedemo obdobje med ciprsko (2012–2013) in grško krizo (2015).

Približno 2,5 milijarde odraslih ljudi na svetu nima dostopa do bančnih storitev. Posledično na primer ne morejo odpreti varčevalnega računa niti pridobiti kreditne kartice. Večina živi v revnih območjih oziroma državah tretjega sveta, v katere banke ne želijo vstopiti, saj te niso dobičkonosne ali pa nimajo postavljene ustrezne infrastrukture. Za plačevanje z bitcoinom v takem primeru ne potrebujejo niti pametnega telefona. Dovolj je, da lahko sprejemajo besedilna sporočila, za izvedbo transakcije pa ga lahko po potrebi na primer začasno priklopijo na računalniško omrežje. Tovrstna zelo razširjena storitev je na primer M-Pesa (ki sicer ne omogoča plačevanja z bitcoini) in je v lasti telekomunikacijskega podjetja Safaricom. BitPesa pa na primer v nasprotju s prej omenjenim ponuja tudi plačevanje z bitcoini iz Kenije in v Kenijo, iz Tanzanije in v Tanzanijo, iz Ugande in v Ugando ter iz Nigerije in v Nigerijo (Vigna & Casey, 2015, str. 186–218).

2.8 Prednosti in slabosti bitcoina

Na podlagi analize sistema Bitcoin in bitcoina kot valute v tem magistrskem delu ugotavljam, da ima bitcoin na podlagi svojih značilnosti prednosti in slabosti. V določenih primerih je neka značilnost lahko hkrati prednost in tudi slabost.

Prednosti bitcoina so:

- odprtokodnost (vsak ima vpogled v izvorno kodo);
- decentralizacija;
- nadzorovana ponudba denarja v obtoku (ni podvržen inflacijskim pritiskom);
- delna anonimnost;
- manjši stroški za trgovce (ni treba plačati provizij posrednikom);
- popoln nadzor uporabnika; ta nima skritih stroškov in nobena tretja oseba mu – razen v primeru kraje zasebnih ključev – bitcoinov ne more zaseči;
- majhni stroški transakcij, kar je pomembno predvsem pri mikrotransakcijah;
- nepovratnost transakcij, kar je prednost za trgovce, ki so sicer podvrženi zlorabam, če kupec kljub prejetju blaga trdi, da ga ni prejel;
- ponarejanje v smislu izdaje novih bitcoinov ni mogoče;
- svoboda plačevanja (plačamo lahko kadar koli in kjer koli);
- hitrost izvršbe transakcij;
- konvertibilnost z valutami fiat in drugimi alternativnimi valutami;
- možnost avtomatizirane in fleksibilne uporabe (pametne pogodbe ...) s pomočjo skriptiranja (Nian & Chuen, 2015, str. 12–13);
- možnost finančne vključenosti za države tretjega sveta in države s kapitalskimi omejitvami.

Slabosti bitcoina so:

- anonimnost (možnost uporabe za nezakonite namene);
- cenovna volatilnost;
- nepovratnost transakcij, kar za uporabnike ob pomanjkanju ustreznega načina za reševanj težav lahko ob zmotnih transakcijah pomeni izgubo bitcoinov;
- podvrženost morebitnim kibernetskim napadom;
- možnost izgube bitcoinov kot posledica izgube zasebnih ključev (izguba gesla do ponudnika spletne denarnice, odpoved trdega diska), zaradi česar je obvezna redna varnostna izdelava kopije zasebnih ključev;
- nereguliranost, kar otežuje možnost preprečevanja pranja denarja in financiranja terorizma;
- nadzorovana ponudba denarja v obtoku (deflacija in kopičenje bitcoinov);
- prevzemanje rizika nasprotnih strank (ob uporabi menjalnic in spletnih denarnic);

- ni zakonito plačilno sredstvo (posledično je stopnja sprejetja nizka);
- odprtokodnost, ki lahko vodi v več vej različice programa (podprtih od različnih razvijalcev) oziroma celo vzpostavitev novih valut, kar lahko posledično destabilizira bitcoin (Kroll & Davey, 2013, str. 17–18);
- moč in možnost odločanja je čedalje bolj centralizirana (fundacija Bitcoin, skupine rudarjev, spletne denarnice in menjalnice), kar je v osnovi ravno nasprotno od osnovnih načel in namena Bitcoina (Gervais, Karame, Capkun, & Capkun, 2014, str. 3–5);
- velika poraba električne energije za rudarjenje.

3 SISTEM BITCOIN V SLOVENIJI

Glede na to, da na ravni Evropske unije za zdaj ni posebne direktive, ki bi urejala virtualne valute, je ureditev oziroma opredelitev prepuščena posamezni državi članici. V Sloveniji glede virtualnih valut nimamo posebne zakonodaje, so se pa do njih opredelile posamezne institucije.

Urad Republike Slovenije za preprečevanje pranja denarja (2014) je izdal obvestilo za zavezance, v katerem pravi, da bitcoin lahko z vidika pranja denarja umestimo v kontekst 16. c-točke 4. člena Zakona o preprečevanju pranja denarja in financiranja terorizma. Ta kot zavezance po omenjenem zakonu določa tudi pravne in fizične osebe, ki v Republiki Sloveniji opravljajo posle v povezavi z dejavnostjo izdajanja in upravljanja drugih plačilnih sredstev, pri čemer ne gre za plačilno storitev skladno z zakonom, ki ureja plačilne storitve in sisteme. Zavezanci morajo zaradi odkrivanja in preprečevanja pranja denarja pri opravljanju svojih dejavnosti izvajati naloge, določene v omenjenem zakonu in na njegovi podlagi sprejetih predpisih. Po omenjenem zakonu je tako zavezanec vsak, ki se ukvarja s trgovanjem oziroma z izdajanjem virtualne valute. V omenjenem obvestilu je omenjeno tudi stališče Banke Slovenije, ki pravi, da bitcoin ni elektronski denar, kot to določa Zakon o plačilnih storitvah in sistemih, niti tuja valuta oziroma deviza, kot to določa Zakon o deviznem poslovanju. Posledično bitcoina Banka Slovenije ne nadzoruje.

Največ obvestil oziroma pojasnil je izdala Finančna uprava Republike Slovenije (v nadaljevanju FURS), ki bodo podrobneje predstavljena v naslednjem podpoglavju.

3.1 Davčna obravnava bitcoina

FURS je v povezavi z bitcoinom posegel na tri področja, in sicer na davčno obravnavo dohodka, davčno potrjevanje računov in obravnavo provizije pri prodaji bitcoinov.

V pojasnilu, številka 4210-11634/2013 (FURS, 2013), je obrazložil, da se bitcoin ne šteje za denarno sredstvo po 7. točki 4. člena Zakona o plačilnih storitvah in sistemih. Prav tako pa se bitcoin ne šteje za finančni instrument.

Davčna obravnava dohodka, doseženega pri trgovanju/poslovanju, je po omenjenem pojasnilu odvisna od okoliščin posameznega primera. Treba je namreč ugotoviti, kdo dosega dohodek in za katere vrste dohodek v posameznem primeru gre (dohodek iz izdaje bitcoinov, kupovanja in prodajanja bitcoinov, izplačilo drugega dohodka v bitcoinih).

Skladno s 15. členom Zakona o dohodnini (v nadaljevanju ZDoH-2) se kakršen koli dohodek, ki ga fizična oseba dobi izplačanega v bitcoinih, obdavči kot dohodek, prejet v naravi. Višina dohodka v evrih se določi tako, da se upošteva vrednost bitcoina v evrih v času, ko je dohodek prejet (FURS, 2013).

Zanimivo je, da kapitalski dobiček, dosežen pri trgovanju z bitcoini, ni obdavčljiv. FURS je to utemeljil z določbo, da se dohodnina ne plača od dobička iz kapitala od odsvojitve premičnin (razen izjem, med katere pa bitcoin ne spada). Bitcoin po interpretaciji FURS-a torej spada med premičnine. Dohodek, ki ga fizična oseba doseže z rudarjenjem, se obdavči po 105. členu ZDoH-2, pri čemer pa se višina dohodka v evrih prav tako določi glede na vrednost bitcoina v evrih, ko je bil dohodek prejet. FURS bo narudarjene bitcoine sicer lahko zaznal le prek ugotavljanja povečanja premoženja (Ahtik, 2014, str. 291–292).

Če fizična oseba bitcoinski dohodek ustvari pri opravljanju dejavnosti, se dobiček iz poslov trgovanja z bitcoini ali dohodek iz rudarjenja obdavčuje kot dohodek iz dejavnosti po določbah ZDoH-2. Davčna osnova od dohodka iz dejavnosti je dobiček, ki se ugotovi kot razlika med prihodki in odhodki, doseženimi v povezavi z opravljanjem dejavnosti. Za ugotovitev prihodkov in odhodkov pa se uporabljajo predpisi o obdavčitvi dohodkov pravnih oseb. FURS ugotavlja, da Zakon o davku od dohodkov pravnih oseb nima izrecne odločbe za davčno obravnavo dohodkov, povezanih s poslovanjem oziroma trgovanjem z bitcoini. Uporabljale pa naj bi se siceršnje določbe omenjenega zakona o dobičku. Te torej veljajo tudi za bitcoine. Računovodska obravnava naj bi bila tako odvisna od primera do primera (Ahtik, 2014, str. 291).

FURS (2015a, str. 123) je v okviru pogostih vprašanj in odgovorov glede davčnega potrjevanja računov pojasnil, da se v okviru Zakona o davčnem potrjevanju računov bitcoin obravnava kot gotovina, saj naj bi med plačilo z gotovino spadali tudi drugi, podobni načini plačila. Posledično morajo zavezanci pri plačilu z bitcoinom prav tako uporabljati davčno blagajno.

FURS je 7. 12. 2015 spremenil svoje stališče glede obravnave provizije pri prodaji bitcoinov po Zakonu o davku na dodano vrednost (v nadaljevanju ZDDV-1). Pred omenjenim pojasnilom je veljalo stališče, da provizija, ki je zaračunana za nakup bitcoinov

v zameno za evre, ne more biti oproščena skladno s 4. d-točko 44. člena ZDDV-1, saj bitcoin ne predstavlja zakonitega plačilnega sredstva. Provizija za opravljeno storitev menjave pa je namreč predmet obdavčitve z davkom na dodano vrednost (v nadaljevanju DDV). FURS je spremenil omenjeno stališče, saj je bilo namreč ugotovljeno, da bitcoin na podlagi sodbe Sodišča Evropske unije v zadevi C-264/14 (Skatteverket proti Davidu Hedquistu) predstavlja neposredno plačilno sredstvo med subjekti, ki ga sprejmejo, zato je transakcija menjave v povezavi z njo, ki se šteje za opravljanje storitev za plačilo, oproščena plačila DDV. Izhajajoč iz zadevne sodbe, je zato treba provizijo, ki je zaračunana za nakup bitcoinov v zameno za evre, oprostiti plačila DDV. Sprememba stališča velja od sprejetja sodbe naprej in nima retroaktivnega učinka (FURS, 2015b).

3.2 Podjetja, ki se ukvarjajo s tehnologijo Bitcoin

S tehnologijo Bitcoin se ukvarja tudi nekaj v Sloveniji ustanovljenih podjetij, in sicer predvsem na področju menjave bitcoina prek spletne menjalnice, plačevanja z bitcoinom in dviga bitcoinov prek bankomatov.

Leta 2011 je bila v Sloveniji ustanovljena spletna menjalnica Bitstamp, ki še danes spada med največje menjalnice po prometu z bitcoinom na svetu. Leta 2013 je bil njen sedež sicer prestavljen v Veliko Britanijo.

Cashilla je plačilni posrednik in platforma za plačevanje z bitcoini, ki ima tudi bančno licenco za izvrševanje bančnih transakcij za območje SEPA. Omogoča nakazovanje bitcoinov neposredno iz denarnice uporabnika na določen bančni račun. Podjetje je ustanovljeno v Češki republiki, saj jim je uspelo pridobiti bančno licenco češke centralne banke, medtem ko poslujejo iz Slovenije.

Bitnik je družba, ki upravlja z enosmernimi bankomati Bitcoin (mogoč je samo nakup), podjetje Grecom pa z dvosmernimi, kar pomeni, da sta prek njega mogoča nakup in tudi prodaja bitcoinov.

4 ALTERNATIVNA UPORABA TEHNOLOGIJE BITCOIN NA FINANČNEM PODROČJU

V tem poglavju bom najprej predstavil alternativne pristope za potrjevanje transakcij, ki se razlikujejo od Bitcoinovega tako imenovanega dokaza o vloženem delu in ki so v uporabi pri nekaterih alternativnih kovancih.

Sledila bo delitev tehnologije, ki temelji na kriptologiji in jo je podalo Bančno združenje za evro (angl. *Euro Banking Association*)[6], in sicer glede na možnost njene uporabe pri ponudnikih plačilnih storitev. Razdeljena bo v štiri kategorije, pri čemer bo vsaka izmed njih predstavljena teoretično in tudi na konkretnem primeru. Omenjeni delitvi bo sledila tudi splošnejša delitev, in sicer glede na različico verige blokov.

Poglavje bo sklenjeno s prikazom trenutnega stanja na finančnem področju in z izzivi za prihodnost.

4.1 Alternative dokazu o vloženem delu

Dokaz o vloženem delu, ki ga za potrjevanje transakcij uporablja bitcoin, ima naslednje slabosti (Lee, 2015, str. 27–28):

- rudarjenje zahteva velik računski napor, za katerega je porabljene ogromno električne energije; sistem je namreč zasnovan tako, da je zloraba zaradi porabe procesne moči (in posledično energije) in možnosti prilagajanja težavnosti izjemno draga; zaradi večanja uporabe bitcoina se povečuje število rudarjev in posledično tudi računske moči omrežja, to pa povzroča, da se zaradi možnosti spreminjanja povečuje tudi težavnost in prek te poraba električne energije;
- donosi rudarjev, ki vzdržujejo sistem, so padajoči; približno vsaka štiri leta se namreč nagrada v obliki na novo izdanih bitcoinov, ki predstavlja večinski delež rudarjevih prihodkov, prepolovi; na dolgi rok posledično obstaja možnost, da bi to zaradi zmanjšanja interesa za rudarjenje ogrozilo sistem; to sicer ni gotovo, saj se bo ustrezno prilagodila tudi težavnost rudarjenja in s tem se bodo zmanjšali tudi stroški;
- možnost napada 51 %, ki je bil podrobneje predstavljen v točki 1.2.5.

Kot odgovor na zgoraj omenjene pomanjkljivosti so se s pojavom alternativnih kovancev pojavili tudi alternativni pristopi za potrjevanje transakcij.

Pri dokazu o deležu (angl. *proof of stake*) deležniki v nasprotju z dokazom o vloženem delu nove bloke skujejo (angl. *minting*) in ne narudarijo. Kovanje ne zahteva velike procesne moči, ker je verjetnost skovanja novega bloka odvisna od deleža, ki ga ima deležnik v sistemu. Omenjeni delež je izmerjen z mero, imenovano starost kovancev (angl. *coin age*). Starost kovancev je izračunana kot število kovancev, pomnožena z njihovo starostjo, torej z obdobjem, od katerega so bili nazadnje porabljeni – odkar so torej v lasti trenutnega deležnika (King & Nadal, 2012, str. 1–5). Omenjeni koncept v osnovi prav tako izhaja iz Bitcoina, in sicer iz določanja prioritet transakcijam.

[6] Bančno združenje za evro je organizacija, ki članom zagotavlja forum za razpravo o bančnih vprašanjih in preučevanje bančnih tem, zlasti v povezavi z uporabo evra in poravnavo transakcij v evrih.

Posledično je dokaz o deležu prijaznejši do okolja (porabljene je malo energije), manj centraliziran (saj imajo vsi obstoječi lastniki kovancev ekonomsko iniciativo za kovanje) in dražji za izvedbo tako imenovanega napada 51 % (saj bi moral imeti napadalec večinski delež omenjenih kovancev, hkrati pa bi posledično delal škodo samemu sebi). Glavni problem dokaza o deležu je rešljivost situacije ob pojavu različnih vej verige blokov. Če imajo deležniki sredstva v več vejah hkrati, jim je tudi ob majhnem deležu namreč v interesu, da kovanje še naprej nadaljujejo na vseh vejah. Dodaten problem predstavlja tudi možnost dvojnega porabljanja, ki ga je pri dokazu o deležu lažje izvesti (Patterson, 2015a). Primera alternativnih kovancev, ki uporabljata dokaz o deležu, sta na primer peercoin in NXT.

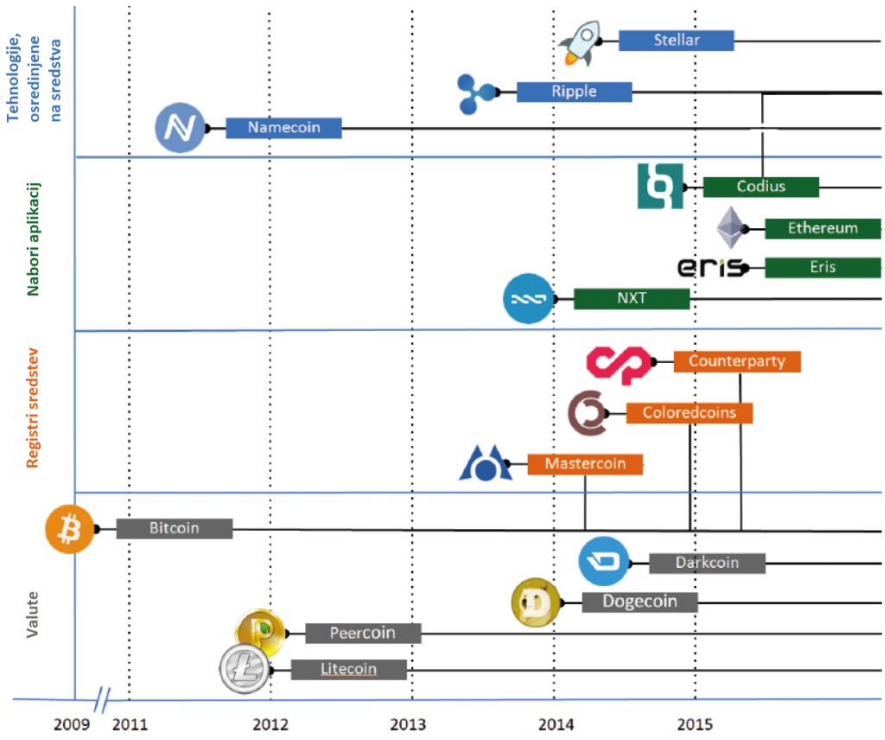
Poleg dokaza o deležu obstaja še nekaj manj znanih konceptov, ki pa so v večini primerov samo teoretični (oziroma je pri določenem alternativnem kovancu uporabljen samo del koncepta). Dokaz o aktivnosti (angl. *proof of activity*) je koncept, ki hkrati uporablja dokaz o vloženem delu in dokaz o deležu. Dokaz o uničenju (angl. *proof of burn*) namesto porabe energije deluje po principu uničevanja alternativnih kovancev, tako da jih pošlje na naslov, s katerega jih ni več mogoče unovčiti. Z uničenjem kovancev si zagotovi možnost nadaljnjega rudarjenja (več kovancev kot uniči, večja je verjetnost, da bo ustvaril nov blok). Dokaz o kapaciteti (angl. *proof of capacity*) pa kot omejen vir uporablja prostor na trdem disku (odmerjen v megabajtih). Več prostora, kot je dodeljenega, večja je verjetnost rešitve uganke (Patterson, 2015b).

4.2 Kategorije kriptotehnologije

V zadnjih nekaj letih so pojavile različne na kriptologiji temelječe tehnologije (v nadaljevanju kriptotehnologije), ki so prepoznane kot ena izmed večjih informacijskotehnoloških inovacij, s potencialom, da izboljšajo obstoječo arhitekturo sistemov in procese v industriji, ki se ukvarjajo z digitalnimi transakcijami. Kriptotehnologija je kombinirana uporaba različnih kriptografskih tehnik v decentraliziranem oziroma distribuiranem omrežju z namenom oblikovanja distribuirane in soglasne glavne knjige (angl. *distributed consensus ledger*), poznane tudi kot veriga blokov. Tovrstna glavna knjiga omogoča skupno oblikovanje, razvijanje in vodenje evidence enotnega zbirališča transakcij oziroma drugega zaporednega niza dogodkov prek deljenega omrežja brez potrebe po vzdrževanju in administraciji centralne institucije (Euro Banking Association, 2015, str. 4–6).

Bančno združenje za evro (Euro Banking Association, 2015, str. 4) je kriptotehnologije glede na njihovo možnost uporabe z vidika ponudnikov plačilnih storitev razdelilo v štiri kategorije, in sicer: valute (angl. *currencies*), registre sredstev (angl. *asset registry*), nabore aplikacij (angl. *application stacks*) in tehnologije, osredinjene na sredstva (angl. *asset-centric technologies*), ki so na konkretnih primerih razvidne v Sliki 18.

Slika 18: Kategorije kriptotehnologij s podanimi primeri



Vir: *Euro Banking Association, Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios: An exploration for transaction banking and payments professionals, 2015, str. 5, slika 1.*

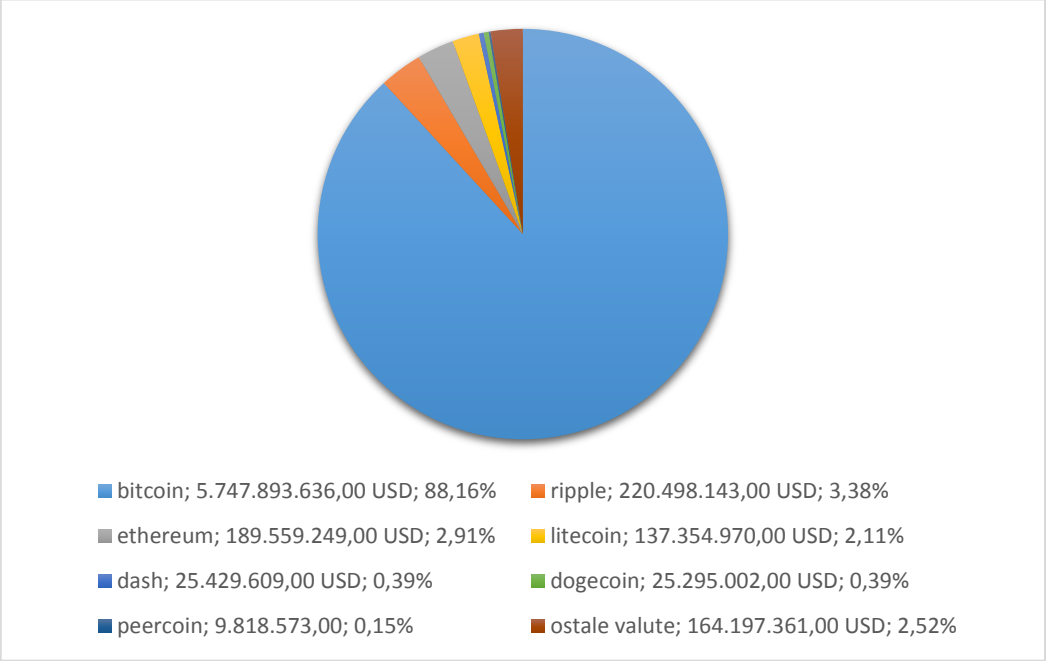
V nadaljevanju bom omenjene kategorije podrobneje predstavil. Največji poudarek izmed omenjenih štirih kategorij bom dal zadnji kategoriji, saj je potencialno najzanimivejša za uporabo za ponudnike plačilnih storitev v kratkoročnem obdobju. Vzrok je v tem, da se lahko poleg pospešitve obstoječih procesov in zmanjšanja kompleksnosti v nasprotju z drugimi tremi tehnologijami že zdaj integrira z obstoječim informacijskim in s pravnim sistemom ter sredstvi (z valutami, vrednostnimi papirji …).

4.2.1 Valute

Prva veriga blokov je bila kot revolucionarna inovacija predstavljena v sistemu Bitcoin, katerega glavni produkt je valuta bitcoin. Za razumevanje principa delovanja kriptotehnologij je razumevanje delovanja sistema Bitcoin in lastnosti bitcoina kot valute bistvenega pomena.

Kot je razvidno iz Slike 19, je po Coin market cap (2016) bitcoin na dan 31. 1. 2016 predstavljal 88,16-odstotni delež celotne tržne kapitalizacije (v USD) izmed vseh 503 na omenjeni strani evidentiranih kriptografskih valut.

Slika 19: Tržna kapitalizacija kriptografskih valut v USD na 31. 1. 2016



Vir: Coin market cap, 2016.

Bitcoin po tržni kapitalizaciji kljub nekaterim njegovim pomanjkljivostim in pojavu alternativnih kovancev še vedno predstavlja najpomembnejšo kriptografsko valuto. Omenjeno lahko pripišemo dejstvu, da je bitcoin kot prvi uspešno odpravil možnost dvojnega porabljanja ob odsotnosti centralne institucije in da je posledično na trgu tudi prisoten najdlje.

4.2.2 Registri sredstev

Registri sredstev za registracijo sredstev uporabljajo obstoječe javne glavne knjige (verige blokov), ki so v osnovi namenjene samo izdaji in evidenci lastništva specifičnih kovancev oziroma valut (na primer bitcoina). Z vključitvijo majhne transakcije ob njeni navezavi na obstoječe sredstvo (vrednostne papirje, prevozno sredstvo, nepremičnine itn.) je tako lastništvo omenjenega sredstva javno zapisano v verigi blokov. Za registracijo sredstva tako ne potrebujemo centralne institucije, ki bi vodila evidenco. Lastnik zasebnega ključa omenjene javne zavedbe je tako posledično tudi lastnik omenjenega sredstva. Fizično sredstvo se sicer lahko izgubi ali pa ukrade, vendar pa lastništva nad njim brez zamenjave naslova, ki si lasti valuto (prek izvedbe in zabeležbe njene transakcije v verigi blokov), uradno ni mogoče uveljavljati. Trenutno se neko sredstvo na transakcijo veže tako, da se v transakcijo doda podatke (omogočeno je namreč skriptiranje), ki sicer niso potrebni za potrjevanje transakcije. Problem, ki se pojavi s takšnim načinom zavedb, je v tem, da vplivajo na zmogljivost omrežja. Z dodajanjem za potrjevanje nepotrebnih podatkov se namreč veča velikost transakcije in posledično se potrebuje tudi večja procesna moč za

njeno potrjevanje. Tovrstna množična uporaba pa bi omrežje prav tako preplavila s transakcijami, ki bi zaradi omejene velikosti posameznega bloka lahko podaljšale čas potrjevanja transakcij, ki so v resnici namenjene za prenos vrednosti dotične valute in za katero je v osnovi namenjena tovrstna veriga blokov. Z vidika bančne industrije imajo registri sredstev zato bolj omejeno uporabno vrednost (Euro Banking Association, 2015, str. 7–8).

Po mnenju Bančnega združenja za evro pa imajo registri sredstev potencial za zmanjšanje stroškov upravljanja in revizije.

4.2.2.1 Primer registra sredstev

Primeri registrov sredstev so: Counterparty, Mastercoin in Colored coins. Zadnje bom tudi podrobneje predstavil.

Bitcoin je naredil revolucijo v do takrat znanem načinu izdajanja denarja in elektronskega izvajanja plačil z izdajanjem valute, ki je hranjena in distribuirana elektronsko ob hkratni odsotnosti potrebe po centralni instituciji. Cilj projekta Colored coins je omenjene lastnosti prenesti in uporabiti tudi na druge vrste sredstev (torej poleg valut). Colored coins bi v slovenski jezik lahko prevedli kot obarvani kovanci, pri čemer pa je treba poudariti, da gre pri »obarvanju« samo za metaforo in ne za dejansko asociacijo z določeno barvo. V praksi lahko »barvo«, s katero označimo določen kovanec in po kateri se kovanec razlikuje od drugih, na primer predstavljata posebna oznaka kovanca in unikatna zgoščena vrednost. Osnovna ideja je, da lahko s tem, ko obarvamo oziroma označimo določen bitcoin (natančneje se dejansko obarva izhodni del transakcije Bitcoin), nanj vežemo lastništvo določenega realnega sredstva, katerega vrednost je neodvisna od dejanske tržne vrednosti obarvanega bitcoina, na katerega je sredstvo vezano. Vsakokratni lastnik obarvanega bitcoina je tako hkrati tudi lastnik sredstva, ki je na ta bitcoin vezano. Primer sredstev so lahko na primer obveznice, delnice, plemenite kovine ali blago (Rosenfeld, 2012, str. 1–9).

Colored coins uporabljajo Bitcoinovo obstoječe omrežje, pri čemer posledično izkoristijo vse njegove tehnološke prednosti. V osnovi je Bitcoinov programski jezik, imenovan skriptiranje, namenjen za podprtje izmenjave bitcoinov. Dodatno pa omogoča, da se v verigi blokov hranijo tudi manjše količine metapodatkov. Uporabnik določeno sporočilo (na primer opis sredstva, količina, izdajatelj …) najprej konvertira v šestnajstiško (angl. *hexadecimal*) vrednost, to pa potem v naslov Bitcoin. Ko nekdo prenese bitcoine na omenjeni naslov, se ta informacija za vedno zapiše v verigo blokov. Za generiranje omenjenih naslovov in nadaljnje sledenje sredstev je potrebna uporaba za to namenskih denarnic, kot so na primer Coinprism, Colu in Coinspark. Transakcije pa morajo prav tako slediti določenim pravilom, da so lahko zaznane pri »barvno ozaveščenih« deležnikih v omrežju (Tasca, 2015, str. 79–80).

Pravila algoritma so naslednja (Rosenfeld, 2012, str. 8):

- vhodni in izhodni deli transakcij so razvrščeni po barvah, s tem da morajo biti neobarvani kovanci vedno na koncu;
- isto zaporedje barv mora biti uporabljeno za vhodne in izhodne dele transakcij;
- za vsako barvo mora biti skupna vrednost njenih vhodnih delov enaka skupni vrednosti njenih izhodnih delov; samo neobarvani kovanci imajo vhodni del lahko večji od izhodnega.

Colored coins se lahko na primer uporabljajo (Rosenfold, 2012, str. 1) pri:

- pametnem lastništvu, pri čemer se lastništvo fizičnega sredstva (mobilni telefon, vozilo, nepremičnina) prenaša prek obarvanih kovancev, ki lastniku omogočajo dostop in uporabo sredstva;
- vrednostnih papirjih, pri čemer podjetje izda obarvane kovance, ki predstavljajo vrednostne papirje; morebitne dividende, obresti in glasovalne pravice pa se tako samodejno prenesejo na lastnike obarvanih kovancev;
- deterministični pogodbah, pri katerih lahko oseba ali pa podjetje izda pogodbo, s katero specificira izplačilo v prihodnosti.

4.2.3 Nabori aplikacij

Nabori aplikacij so rezultat nenehnega iskanja uporabnosti tehnologije verige blokov za namene, ki so širši od samo možnosti kreiranja virtualnih valut. Med seboj se razlikujejo glede na njihov fokus. Glavni fokus katerega koli nabora aplikacij je postati platforma za razvoj in izvedbo celovitih aplikacij, ki delujejo nad decentraliziranim ali pa distribuiranim omrežjem, kot je na primer Bitcoinovo (Euro Banking Association, 2015, str. 8–9).

Z omenjenimi celovitimi aplikacijami so mišljene distribuirane avtonomne organizacije (angl. *distributed autonomous organizations*, v nadaljevanju DAO). DAO so najkompleksnejša oblika do zdaj poznane decentralizirane avtomatizacije. Najpreprostejša in prva oblika DAO je bil Bitcoin. Kompleksnejše oblike tovrstnega koncepta so avtonomni agenti, pametne pogodbe, decentralizirane aplikacije in decentralizirane organizacije. Kot DAO si lahko predstavljamo organizacijo, ki glede na vnaprej določena pravila na podlagi decentralizirane, transparentne, varne in javno revidirane odprtokodne programske opreme, ki je distribuirana prek računalnikov določene interesne skupine, deluje popolnoma avtonomno. Deluje lahko torej brez dodatnega človeškega nadzora oziroma vmešavanja – z izjemo človeškega napora, ki je bil vložen v njeno kreiranje (Tasca, 2015, str. 85–86).

Po mnenju Bančnega združenja za evro omenjena tehnologija lahko predstavlja priložnost za katerega koli udeleženca trga, ki se ukvarja s plačili, še posebej pa v povezavi z

ustvarjanjem novih produktov in s prilagodljivostjo ter z možnostjo njihove dodatne razčlembe.

4.2.3.1 Primer nabora aplikacij

Primeri naborov aplikacij so: NXT, Eris, Codius in Ethereum. Zadnjega bom tudi podrobneje predstavil.

Osnova ideja Ethereuma izhaja iz koncepta Colored coins, ki ga poizkuša nadgraditi. Glavna omejitev Colored coins izhaja iz njihove odvisnosti od Bitcoina (saj temelji na njegovi verigi blokov; kot žeton, prek katerega se prenaša lastništvo, uporablja bitcoin kot valuto). Z dodajanjem novih blokov v verigo blokov njena velikost neprestano raste. Za namene potrjevanja transakcij Bitcoin vsem deležnikom ni treba lokalno hraniti celotne kopije, saj se za dokaz, da je bila določena transakcija vključena v blok, lahko uporabi poenostavljeno preverjanje plačil, omenjeno v točki 1.2.5. Pri Colored coins to ni mogoče, saj ni dovolj, da ugotovimo, ali je bila določena transakcija res vključena v verigo blokov. Transakciji je namreč treba slediti vse do njenega izvornega obarvanja. Naslednja omejitev Colored coins izhaja iz omejitev programskega jezika, ki ga ta uporablja. Omenjeni jezik namreč ni Turing popoln (angl. *Turing complete*), kar pomeni, da so možnosti programiranja zelo omejene (ne podpira na primer zank). Tretja pomanjkljivost pa izhaja iz dejstva, da preplavlja omrežje Bitcoin z nepotrebnimi dodatnimi transakcijami (Buterin, 2014).

Ethereum je izboljšal zgoraj omenjene omejitve, saj gre za odprtokodno platformo, ki temelji na lastni verigi blokov in uporablja lasten programski jezik Turing popoln. Posledično se lahko sprogramirajo kakršna koli pravila. Prav tako uporablja lastno valuto, imenovano ether, ki je namenjena predvsem plačevanju transakcijskih provizij. Za rudarjenje trenutno uporablja prilagojen dokaz o vloženem delu, ki zmanjšuje možnost izkoriščanja prednosti namenske opreme za rudarjenje (kot je na primer ASIC). V prihodnosti obstaja možnost, da bo, kar se tiče rudarjenja, prešel na dokaz o deležu. Izdaja etherja ni omejena samo na en mehanizem. Na začetku je bil ether namreč izdan prek množičnega financiranja (angl. *crowdfunding*)[7]. Tako je bilo izdanih 60,102.216,00 ethrov. Naknadno pa je bil ustvarjen in ustanovnim članom ter prvim podpornikom alociran še 0,099-kratni količnik sredstev, zbranih prek množičnega financiranja. Ista količina pa je bila izdana in alocirana tudi za namene dolgoročnih rezerv z namenom pokrivanja stroškov in nagrad za nadaljnji razvoj projekta. Vsako leto bo prek rudarjenja na novo ustvarjena 0,26-kratna količina omenjenega zneska. V nasprotju z bitcoinom ether ni končno omejen, njegova rast pa je od določenega trenutka naprej neskončna in linearna (Ethereum white paper, 2015).

[7] Množično financiranje je skupen nastop posameznikov s finančno podporo določenemu projektu. V zameno za podporo posameznik ceneje in hitreje pride do izdelka oziroma storitve, ki jo je s podprtjem pomagal zagnati.

Ethereum je namenjen ustvarjanju decentraliziranih aplikacij. Omenjene aplikacije lahko samodejno komunicirajo z drugimi decentraliziranimi aplikacijami in posledično niso odvisne od določene kontrolne točke. S finančnega vidika je namenjen predvsem formuliziranim pametnim pogodbam, pri čemer pa te niso samo pogodbe med dvema strankama, ampak so neke vrste avtonomni agenti, simulirani prek verige blokov. Vsaka pogodba ima svojo lastno skripto, ki se aktivira vsakič, ko je nanjo poslana transakcija. Poleg pogodb se lahko na primer uporablja tudi za večkratno podpisne založne račune (angl. *multisignature escrows*), varčevalne račune (pri katerih je dvig sredstev mogoč le postopoma), igre na srečo in oblikovanje novih virtualnih valut (Buterin, 2014).

4.2.4 Tehnologija, osredinjena na sredstva

Pri tehnologiji, osredinjeni na sredstva, gre za tehnologijo, namenjeno za izmenjavo digitalne predstave obstoječih sredstev (valut, kovin, vrednostnih papirjev …). Zaupanje je v nasprotju z bitcoinom (ki temelji na rudarjenju in verigi blokov) organizirano neposredno med udeleženci. Ob tem morajo imeti nekateri izmed udeležencev, kot so na primer visokolikvidne borze, za izmenjavo digitalnih sredstev vlogo vzdrževalca trga (angl. *market maker*), nekateri pa prehodnih točk (angl. *gateway*), ki skrbijo za konverzijo med digitalnim in realnim svetom. Večinoma se uporablja deljena ter zasebna in ne javna glavna knjiga. Med zaupanja vrednimi deležniki se lahko uveljavijo ekskluzivne pogodbe za izmenjavo sredstev, s čimer se ponudniki plačilnih storitev tako lahko izognejo izpostavljanju rizika, ki bi sicer lahko nastal ob brezvestnih tretjih osebah (Euro Banking Association, 2015, str. 9–10).

Bančno združenje za evro (Euro Banking Association, 2015, str. 10) z vidika ponudnikov plačilnih storitev navaja štiri mogoče načine uporabe tehnologije, osredinjene na sredstva, in sicer: menjavo valut in nakazovanje sredstev v tujino (angl. *foreign exchange and remittances*), izvajanje plačil v realnem času (angl. *real-time payments*), izmenjavo dokumentarnega gradiva (angl. *documentary trade*) in servisiranje sredstev (angl. *asset servicing*).

4.2.4.1 Menjava valut in nakazovanje sredstev v tujino

Tehnologije, osredinjene na sredstva, lahko ob odsotnosti potrebe po hkratni vpletenosti različnih ponudnikov plačilnih storitev ter obstoječega klirinškega in poravnalnega mehanizma valutno trgovanje in nakazovanje sredstev pospešijo in naredijo učinkovitejše. Če hoče manjša evropska banka, ki ponuja transakcije z različnimi valutami, sredstva stranke nakazati v ZDA, mora to storiti prek večje banke, ki ima pri določeni banki v ZDA odprt račun nostro[8]. Omenjena ameriška banka po prejemu denarja potem denar nakaže na drugo ameriško banko, ki jo je izbral prejemnik sredstev. Vsak dodaten člen v verigi

[8] Račun nostro je račun domače banke, odprt pri tuji banki, prek katerega se opravljajo storitve.

posrednikov podaljša čas, poveča riziko in doda stroške k omenjenemu procesu. Kompleksnost in riziko se dodatno povečata pri valutnih parih, ki imajo medsebojno nizko likvidnost. Podobno velja za nakazovanje sredstev v bančno podhranjene družbe (na primer v države tretjega sveta), v katerih dodaten problem predstavlja tudi pomanjkanje ustrezne infrastrukture (na primer podružnic in bankomatov).

Ob izvedbi omenjenih transakcij prek distribuirane soglasne glavne knjige lahko določeni ponudniki plačilnih storitev v različnih jurisdikcijah opravljajo vlogo prehodnih točk. Prehodna točka objavi digitalno sredstvo, kot zavarovanje oziroma jamstvo pa hrani sredstva v valuti fiat ali pa vrednostnih papirjih. Ko prehodne točke (ponudniki plačilnih storitev) vzpostavijo medsebojno zaupanje, lahko med seboj trgujejo v realnem času. Pri tem lahko uporabijo tudi vzdrževalce trga, ki lahko po potrebi zagotovijo ustrezno likvidnost (Euro Banking Association, 2015, str. 11).

Tovrsten pristop ima po mnenju Bančnega združenja za evro (Euro Banking Association, 2015, str. 11) za vse udeležence tri ključne prednosti:

- pozicije vseh sodelujočih ponudnikov plačilnih storitev v različnih razredih sredstev so v medsebojni povezavi vzdrževane v realnem času;
- tehnična pridružitev med različnimi jurisdikcijami je lahko cenejša;
- nižji stroški za vzdrževanje, upravljanje, zagotavljanje varnosti in za revizije tovrstnega omrežja v primerjavi z naraščajočimi stroški v obstoječem omrežju ob hkratnem doseganju podobne stopnje zaupanja.

4.2.4.2 Izvajanje plačil v realnem času

Obstoječi proces izvajanja plačil je rezultat evolucije. Če želimo znotraj istega ponudnika plačilnih storitev izvesti plačilo med dvema različnima računoma, se procesiranje in poravnava izvedeta znotraj samega ponudnika (na primer znotraj določene banke). Posledično tovrsten premik sredstev med računi ne spremeni skupnega denarnega stanja omenjenega ponudnika plačilnih storitev. Ob izvedbi plačila med računi dveh različnih ponudnikov plačilnih storitev pa se to spremeni. Zaradi zahtev po zadostnih kapitalskih rezervah morajo ponudniki plačilnih storitev spremembe v bilancah neprestano spremljati in jih ustrezno upravljati. Podobno velja za mednarodna plačila, pri katerih kliring in poravnavo med seboj izvajajo centralne banke. Na proceduralni ravni omenjeni proces zahteva zahtevno koordinacijo za različne resurse intenzivnih korakov, predvsem z organizacijskega vidika in vidika obdelovalne zmogljivosti. Omenjeni koraki se večinoma ne izvajajo konstantno, ampak samo nekajkrat dnevno, in sicer v različnih ciklih. Posledično so plačila pogosto izvršena šele nekaj dni po njihovi sprožitvi. To še posebej velja, če presežemo presečno uro za izvršitev nakazila znotraj istega dne, če mora plačilo potovati po kompleksnih poteh, ob plačevanju v drugi valuti in če katera izmed bank v

verigi zaradi praznika ali pa konca tedna ne obratuje (Euro Banking Association, 2015, str. 13).

Ob obstoju distribuirane soglasne glavne knjige, pri kateri bi bila centralna banka edini vzdrževalec trga in podpornik digitalne obveznosti z valutami fiat, bi bilo lahko med sodelujočimi ponudniki plačilnih storitev omogočeno neprekinjeno poravnavanje obveznosti. Kot rezultat bi moralo iti skozi postopek kliringa manj sredstev. Povečanje učinkovitosti in frekvence klirinških ciklov pa posledično eventualno vodi v takojšnje izvajanje plačil, k čemur na primer stremi tudi ECB (Euro Banking Association, 2015, str. 12–13).

4.2.4.3 Izmenjava dokumentarnega gradiva

Večina ponudnikov plačilnih storitev je nadgradila obstoječe sisteme ter sprejela digitalizacijo in avtomatizacijo, vendar pa njihova logika in logistika še vedno temeljita na podlagi ravnanja s fizičnimi dokumenti, ki mu pravimo tudi dematerializacija (na primer skeniranje fizičnih kopij in arhiviranje digitalnih). Posledično različni ponudniki plačilnih storitev še vedno niso izkoristili digitalizacije in avtomatizacije v polni meri. Procesi izmenjave dokumentarnega gradiva, ki na primer nastanejo pri odpiranju računa, odprtju akreditiva (angl. *letter of credit*)[9] in potrdilih, povezanih z njim, so – čeprav si delijo osnove elemente – različni ter ločeni na postopkovni ravni in ravni informacijske tehnologije (Euro Banking Association, 2015, str. 14).

Današnje dokumentarne naloge bi bilo s pomočjo kriptotehnologije mogoče dodatno avtomatizirati. Ob akreditivih bi omenjeno lahko realizirali s pomočjo denarnic, ki delujejo na podlagi večkratnih podpisov (angl. *multi-signature wallets*) in s popolnoma transparentnim procesom za vse udeležence (banko, prodajalce in kupce). Kupčeva banka bi v tovrstno denarnico deponirala sredstva in ključ razdelila med vse udeležence. Prenos sredstev bi se samodejno izvedel, ko bi kupec s skeniranjem kode QR[10] potrdil prejeto pošiljko. Avtomatizacijo procesa za izvedbo pogojnega plačila bi s tem lahko dvignili na višjo raven in posledično zmanjšali potrebo po stroških, povezanih z varnostjo in nadzorom (Euro Banking Association, 2015, str. 14–16).

4.2.4.4 Servisiranje sredstev

S servisiranjem sredstev so po mnenju Bančnega združenja za evro (Euro Banking Association, 2015, str. 16) v povezavi z distribuirano soglasno glavno knjigo mišljene tri stvari:

[9] Akreditiv je najvarnejši plačilni instrument, saj pomeni samostojno in nepreklicno obvezo banke, da bo prodajalcu plačala za pravočasno predložitev pravilnih, v akreditivu navedenih obveznosti.
[10] Koda QR je matrična oziroma dvodimenzionalna črtna koda, ki lahko v nasprotju s klasično črtno kodo shranjuje vse vrste besedilnih znakov (spletne naslove, besedila, številke …).

- ustvarjanje sredstev (na primer valut, obveznic, delnic, plemenitih kovin ...);
- omogočanje trgovanja med različnimi partnerji, kot so banke oziroma druge institucije, ki se ukvarjajo s trgovanjem;
- eventualna likvidacija vlagateljeve pozicije.

Proces servisiranja sredstev je kompleksen zaradi koordinacije, ki je potrebna med vsemi interesnimi skupinami, kot so: investitorji, skrbniške banke in drugi posredniki. Interakcija med vsemi interesnimi skupinami je postala kompleksna zaradi obstoječih sistemov, ki so podvrženi napakam, in draga, saj posamezniki v skupini ne uporabljajo iste glavne knjige. Pomanjkanje enotne platforme za servisiranje sredstev namreč vodi v okolje, v katerem sočasno obstajajo različni protokoli, različne platforme za izmenjavo in nezanesljivi načini za doseganje končnih rešitev. Enotno in standardizirano omrežje, v katerem bi bilo sredstva mogoče ustvarjati in tudi trgovati z njimi, bi prek možnosti oblikovanja in spreminjanja stanja v skupni in deljeni glavni knjigi lahko odpravilo zgoraj omenjene težave (Euro Banking Association, 2015, str. 16–17).

4.2.4.5 Primer tehnologije, osredinjene na sredstva

Primeri tehnologije, osredinjene na sredstva, so: Stellar, Namecoin in Ripple. Zadnjega bom tudi podrobneje predstavil.

Ripple je odprtokoden in decentraliziran bruto poravnalni sistem, menjalnica valut in omrežje za nakazovanje sredstev v tujino. Razvija in vzdržuje ga zasebno podjetje Ripple Labs. Ripple podpira prenos različnih vrst sredstev, in sicer: valut fiat, virtualnih valut, blaga itn. Če hoče uporabnik pristopiti k sistemu, mora aktivirati svoj račun, tako da svoja sredstva prek prehodne točke konvertira v zadolžnico (angl. *i owe you*). Prehodne točke so posebni deležniki (predvsem spletne finančne storitve), ki Ripplovo omrežje povezujejo s preostalim svetom. Opravljajo vlogo skrbništva in skrbijo za dvig realnih sredstev. Po omrežju se izmenjujejo in prenašajo samo zadolžnice. Zadolžnica dobi vrednost iz dogovora prehodne točke, da bo izpolnila obvezo, ki jo ta predstavlja (Tasca, 2015, str. 89).

Valuta ripple, ki jo uporablja sistem, ne predstavlja omenjene zadolžnice in ni povezana s prehodno točko. V nasprotju z večino preostalih virtualnih valut je prav tako ni treba uporabiti kot menjalnega posrednika. Namesto menjalnega posrednika ripple v osnovi namreč opravlja dve drugi izjemno pomembni funkciji. Prva je ta, da sistem Ripple brani pred zlorabami v obliki nezaželenih transakcij. Ripple namreč zahteva, da vsak račun vzdržuje obvezno rezervo v vrednosti dvajset ripplov. Dodatno je ob vsaki transakciji tudi uničenih 0,00001 rippla (ne gre za zaslužek nekoga, ampak za dejansko uničenje valute). Če bi v prihodnje cena rippla preveč narastla (ali padla), je omenjeni količini mogoče ustrezno uravnati, za kar pa je potrebno zadostno število glasov upravljavcev strežnikov. Druga funkcija pa je ta, da se jo lahko (ni pa nujno) uporabi za povezavo med nelikvidnimi

pari valut. Če je vsaka valuta likvidna z ripplom, je posledično likvidna tudi z vsemi preostalimi valutami. Valuta ripple ni ustvarjena s procesom rudarjenja, ampak je bila v omejenem obsegu (100 milijard) izdana ob zagonu protokola. Ripple Labs ima z namenom vzdrževanja in potencialnega zaslužka namen zadržati 25 odstotkov omenjene količine (20 odstotkov so obdržali tudi lastniki), preostalo pa razdeliti med vzdrževalce trga, prehodne točke in uporabnike. Pri tem proces razdeljevanja ni definiran in je za zdaj popolnoma v domeni podjetja, ki jih razdeljuje po lastni presoji (Ripple, 2014, str. 14–16).

V osnovi je Ripple distribuirana baza podatkov z glavno knjigo, ki transakcije potrjuje in zaznava v realnem času (vsakih nekaj sekund) in hkrati samodejno posodablja stanja uporabnikov v katerem koli sredstvu. Ko se zgodi sprememba v glavni knjigi, se strežniki, ki so povezani v Ripplov protokol, medsebojno strinjajo, da bodo posodobili vsak svojo kopijo glavne knjige. V nasprotju z večino preostalih kriptografskih protokolov Ripple ne temelji na doseganju soglasja s procesom rudarjenja. Ripplov protokol namreč uporablja novo komponento, imenovano unikatni seznam deležnikov (angl. *unique node list*). Vsak strežnik (deležnik) v Ripplovem omrežju vzdržuje seznam drugih strežnikov, ki jim zaupa. Kadar koli je potrebno soglasje, deležnik o mnenju povpraša strežnike, ki so na njegovem seznamu. V nasprotju z Bitcoinom, pri katerem se rudarji vsakič posvetujejo z vsemi deležniki v omrežju, Ripple upošteva samo mnenje strežnikov, ki so na njegovem seznamu. Ker vsi deležniki ne uporabljajo istega seznam strežnikov, katerim zaupajo, je število deležnikov, ki glasuje o določeni transakciji, lahko zelo veliko. Strežnik sprejme transakcijo, če jo je sprejelo vsaj 80 odstotkov strežnikov na njegovem unikatnem seznamu strežnikov. Tako Ripple uspešno preprečuje morebitne veje v njegovi glavni knjigi (Tasca, 2015, str. 89–90).

Če želi ameriško uvozno podjetje prek sistema Bitcoin izvesti plačilo evropskemu izvoznemu podjetju, mora prek ameriške banke v spletno menjalnico najprej nakazati USD in jih zamenjati za bitcoine. Bitcoine mora nato poslati na naslov Bitcoin evropskega izvoznega podjetja. Evropsko izvozno podjetje pa jih potem prek spletne menjalnice pretvori v EUR in nakaže na svoj denarni račun, odprt pri evropski banki. Ker je v tem primeru kot menjalnega posrednika treba uporabiti bitcoin, sta podjetji zaradi enournega čakanja po izvršitvi transakcije izpostavljeni njegovi volatilnosti. Pri Ripplu je zgoraj omenjena transakcija izvedena v nekaj sekundah, prav tako pa ripple ni treba uporabiti kot menjalnega posrednika. Ameriška banka se poveže neposredno v omrežje Ripple in sproži transakcijo iz USD v EUR. Vzdrževalci trga (banke, hedge skladi itn.) nato med seboj tekmujejo za izvršbo transakcije z objavo menjalnega razmerja EUR / USD, pri čemer Ripple samodejno izbere najugodnejšega ponudnika. Izbrani vzdrževalec trga nato kupi USD od ameriške banke in proda EUR evropski banki (Ripple, 2014, str. 8–9).

4.3 Različice verige blokov

Bitcoin je s svojim konceptom delovanja spremenil pogled na finančno industrijo in obstoječo finančno infrastrukturo. Do pojava Bitcoina je bila potreba po centralni instituciji, ki vodi in nadzoruje transakcije ter stanja posameznikov, namreč nekaj samoumevnega. Za zdaj sicer še ni povzročil bistvenih sprememb v delovanju finančnega sistema, je pa spremenil način razmišljanja in nakazal nove možnosti nadaljnjega razvoja finančne tehnologije. Kmalu po njegovem nastanku se je zaradi njegove odprtokodnosti in njegovih pomanjkljivosti pojavilo ogromno drugih alternativnih kovancev, ki so poizkušali izboljšati njegov princip delovanja. Hkrati pa so se iz njegovih idej razvile tudi druge alternativne možnosti uporabe tehnologije, na kateri temelji.

Posledično se je pojavila tudi potreba po ustreznem razvrščanju na novo razvitih tehnologij. Eno izmed mogočih razvrstitev na kriptologiji temelječe tehnologije je glede na njihovo uporabnost pri ponudnikih plačilnih storitev podalo Bančno združenje za evro. Na kriptologiji temelječe tehnologije je Bančno združenje za evro razdelilo v štiri kategorije, in sicer: valute, registre sredstev, nabore aplikacij in tehnologije, osredinjene na sredstva (Euro Banking Association, 2015, str. 4).

Najpomembnejša inovacija Bitcoina je veriga blokov in zato na njeni osnovni logiki delovanja temeljijo tudi preostale kriptografske valute in kriptografske tehnologije, katerih namen je v večini primerov prav tako zmanjšati število posrednikov (posledično tudi stroškov) in odvisnost od centralne institucije. S tega vidika je smiselna delitev novih s kriptografijo povezanih tehnologij in principov na različice verige blokov, pri čemer vsaka različica predstavlja namen oziroma področje, na katerem se omenjena veriga blokov lahko uporablja.

V tem kontekstu je na izraz veriga blokov potrebno treba širše kot samo na princip delovanja verige blokov v sistemu Bitcoin. Nanjo je treba gledati kot na distribuirano glavno knjigo, ki prek oblike soglasja in zaupanja v sistem vodi in vzdržuje pravilno evidenco zapisov ter bilanco stanj. Večina novejših distribuiranih glavnih knjig namreč na primer sploh ne uporablja rudarjenja niti ne dodaja transakcij v posamezen blok. Kljub temu pa ime veriga blokov ostaja v splošni uporabi za vse tehnologije, ki temeljijo na kriptografiji; njihova glavna cilja sta decentralizacija in znižanje stroškov.

S tega vidika Swan (2015, str. 1–52) omenjene tehnologije razdeli v tri kategorije, in sicer glede na različico verige blokov:

- veriga blokov 1.0, kamor spadajo alternativni kovanci in z njimi povezani plačilni sistemi;
- veriga blokov 2.0, kamor spadajo v financah mogoče uporabe omenjene tehnologije, ki presegajo samo osnovne plačilne transakcije z alternativnimi kovanci (vrednostni

papirji, izvedeni finančni instrumenti, pametno lastništvo, pametne pogodbe, posojila, hipoteke …);
- veriga blokov 3.0, kamor spadajo možnosti uporabe omenjene tehnologije na nefinančnem področju (uprava, zdravstvo, znanost, umetnost, literatura, kultura …).

Pri tem želim ponovno poudariti, da gre pri zgoraj omenjenih različicah samo za fiktivno številčno različico posamezne verige blokov, saj ne gre za nadgradnje v smislu, da izhajajo iz iste izvorne kode. Višja različica v tem primeru torej ne pomeni izboljšane različice nekega protokola oziroma programske opreme, ampak posamezna različica predstavlja samo namen njene uporabe na finančnem in tudi nefinančnem področju.

Glede na zgornjo delitev verige blokov na posamezne različice (glede na namen njene uporabe) bi po mojem mnenju v različico verige blokov 1.0 lahko uvrstili prvo izmed štirih kategorij, na katere je Bančno združenje za evro razdelilo različne vrste kriptotehnologije, in sicer valute. V različico 1.0 namreč spadajo alternativni kovanci in z njimi povezani plačilni sistemi. Preostale tri kategorije, na katere je Bančno združenje za evro razdelilo različne vrste kriptotehnologije, in sicer: registre sredstev, nabore aplikacij in tehnologije, osredinjene na sredstva, pa bi po mojem mnenju lahko uvrstili v različico verige blokov 2.0. V različico verige blokov 2.0 namreč spadajo v financah mogoče uporabe omenjene tehnologije, ki presegajo samo osnovne plačilne transakcije z alternativnimi kovanci.

4.4 Trenutno stanje na finančnem področju in izzivi za prihodnost

V zadnjih dveh letih je ogromno ključnih svetovnih finančnih institucij začelo vlaganje, preučevanje in testiranje tehnologije, ki temelji na verigi blokov. Omenjene institucije preizkušajo lastne rešitve in tudi rešitve različnih obstoječih ponudnikov (Ripple, Ethereum, Stellar, Hyperledger, Eris …).

Eno izmed njih je podjetje R3, ki vodi konzorcij 42 pomembnih svetovnih vodilnih bančnih institucij, kot so: Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J. P. Morgan, Royal Bank of Scotland, State Street, UBS, The Bank of New York Mellon, Morgan Stanley itn. Pred kratkim je 40 izmed bank v omenjenem konzorciju izvedlo testiranja različice verige blokov, ki jih ponujajo Chain, Eris Industries, Ethereum, IBM in Intel. Ocenjevali so prednosti in slabosti posamezne tehnologije na podlagi zagona pametnih pogodb, ki so bile programirane za izdajo, sekundarno trgovanje in zapadlost komercialnega zapisa ter kratkoročnega dolžniškega vrednostnega papirja, pri čemer rezultati testa niso javno objavljeni (Smith, 2016).

Depository Trust & Clearing Corporation (v nadaljevanju DTCC)[11] je januarja 2016 izdal poročilo, v katerem je preučil možnosti uporabe tehnologije verige blokov na področju finančnih storitev, ki so potrebne po sklenitvi posla s finančnimi instrumenti (predvsem kliringom in poravnavo vrednostnih papirjev). DTCC meni, da bi varna in distribuirana glavna knjiga s pomočjo popolne in sledljive zgodovine transakcij za določena sredstva, ki so deljena in dostopna samo med zaupanja vrednimi deležniki, lahko pripomogla k izboljšavam na operativni ravni, prav tako pa tudi k zmanjševanju rizika in stroškov, povezanih s poravnavo, skrbništvom in s kliringom.

DTCC (2016, str. 13–17) meni, da je možnosti uporabe omenjene tehnologije z vidika izboljšanja obstoječe infrastrukture in procesov smiselno raziskati predvsem na področjih:

- upravljanja z glavnimi podatki (angl. *master data management*), kot so informacije o posameznih entitetah, sredstvih, delovnih dneh in praznikih;
- izdaje in servisiranja sredstev oziroma vrednostnih papirjev;
- potrjevanja sklenjenih poslov in pogodb (angl. *trade/contract validation*) ter vodenja (angl. *record*) evidence in uparjanja (angl. *match*) kompleksnejših sredstev, za katere trenutno ne obstajajo dobre rešitve;
- netiranja in kliringa;
- upravljanja zavarovanj (angl. *collateral management*);
- poravnave.

Kljub zgoraj omenjenim potencialno mogočim izboljšavam pa DTCC (2016, str. 18) opozarja, da omenjena tehnologija še ni dozorela in da posledično še ni dovolj dokazana, da bi jo v trenutni obliki že bilo mogoče umestiti v obstoječe okolje. Tako kot pri vsaki novi tehnologiji se bo ta sčasoma izboljšala. Izboljšave pa bodo mogoče le z izvajanjem eksperimentov ter posledično z učenjem na njihovih napakah in uspehih. Ob tem pa ni nujno, da se bo na koncu izkazalo, da je omenjena tehnologija res najprimernejša za vsa zgoraj omenjena področja.

V poročilu zato DTCC (2016, str. 18) preostale obstoječe deležnike v finančni industriji tudi poziva k skupnemu sodelovanju pri raziskovanju in razvoju tehnologije.

[11] DTCC je v ZDA ustanovljena družba, ki se ukvarja finančnimi storitvami, potrebnimi po sklenitvi posla s finančnimi instrumenti (na borzi ali pa neposredno med strankami). Finančnim trgom ponuja predvsem storitve kliringa in poravnave ameriških finančnih instrumentov, hkrati pa opravlja tudi vlogo njihovega skrbnika.

SKLEP

Bitcoin je izjemno zanimiva in aktualna tema, ki zahteva znanje iz ekonomije in tudi poznavanje pravnega področja, kriptografije, teorije iger, psihologije in računalništva (Bheemaiah, 2005, str. 3).

V tem magistrskem delu sem tako poleg preučevanja Bitcoina z ekonomskega vidika in posledično njegove obravnave z vidika valute posegel tudi na vsa druga zgoraj omenjena področja. Vzrok je v tem, da je za razumevanje vseh značilnosti Bitcoina in revolucionarnega načina razmišljanja, ki ga Bitcoin prenaša, potrebno detajlno poznavanje sistema Bitcoin in tudi vseh področij, na katera posega. Podrobno poznavanje Bitcoina pa je s teoretičnega vidika izjemno pomembno za razumevanje konceptov tehnologij, ki temeljijo na Bitcoinovih idejah in za katere menim, da imajo prihodnost za uporabo na finančnem področju.

Na podlagi ugotovitev prvega poglavja magistrskega dela lahko potrdim hipotezo, da bitcoin v tem trenutku ne predstavlja najbolje in v polni meri vseh funkcij klasične valute in s tem otežuje bolj množično sprejetje bitcoina kot valute. Kljub nekaterim pozitivnim lastnostim bitcoina kot menjalnega posrednika v primerjavi z valutami fiat (nizki transakcijski stroški, hitrost izvršbe transakcij, anonimnost in transparentnost) ima namreč tudi negativne lastnosti (ni zakonito plačilno sredstvo, začetni stroški vzpostavitve sistema za sprejetje kot plačilno sredstvo, mrežni učinki, zahtevano poznavanje delovanja sistema, pomanjkanje možnosti reševanja težav, pomanjkanje kreditnega trga). Njegova deljivost ima po eni strani pozitiven, po drugi strani pa skupaj s cenovno volatilnostjo negativen učinek na bolj množično sprejetje bitcoina kot obračunske enote. Na kratek rok dejstvo, da nanj ne delujejo inflacijski pritiski, sicer vpliva pozitivno, vendar pa se zaradi omejene končne količine bitcoina v obtoku dolgoročno to lahko izkaže tudi kot negativno, saj obstaja velika nevarnost pojava deflatornih učinkov (predvsem ob pridobitvi pomembnejšega deleža kot valute v svetovnem gospodarstvu), ki na valuto delujejo negativno. Prav tako pa bitcoinu kot hranilcu vrednosti ne pripomoreta niti zahteva po kibernetski varnosti niti visoka cenovna volatilnost. Omenjenemu dognanju potrjuje tudi ECB (2015, str. 23–24), ki ugotavlja, da nobena trenutno znana virtualna valuta ne izpolnjuje vseh treh omenjenih funkcij denarja v polni meri.

Pomembnost bitcoina in virtualnih valut na splošno potrjuje tudi dejstvo, da so se definicij virtualnih valut lotile različne regulatorne institucije, kot so: lokalni davčni uradi, različni regulatorni organi in centralne banke, pri čemer pa se razlikujejo pristopi med državami in tudi različnimi organi znotraj iste države. Moje mnenje je, da sta za to področje potrebni natančnejša definicija ter uvedba ustrezne zakonodaje in regulacije. V evropskem prostoru bi bilo to najbolje urediti na ravni Evropske unije, na kar pa bo verjetno treba počakati še nekaj časa, saj običajno zakonodaja tehnološkemu razvoju sledi z nekajletnim zamikom.

V Sloveniji so se do Bitcoina opredelile različne državne institucije. V največji meri se je do tega opredelila Finančna uprava Republike Slovenije, katere obravnava je odvisna od okoliščin posameznega primera. Po eni strani pravi, da bitcoin ni denarno sredstvo ali pa finančni instrument, po drugi strani pa ga uvršča med gotovino oziroma njej podobna plačilna sredstva ter celo premičnino. To samo potrjuje moje mnenje glede potrebe po vzpostavitvi ustrezne zakonodaje glede virtualnih valut na ravni celotne Evropske unije. Začetni mrzlici Bitcoin so se pridružila tudi nekatera mlada slovenska podjetja, med katerimi je najuspešnejša predvsem spletna menjalnica Bitstamp, ki velja za eno izmed največjih in najbolj priznanih na svetu.

Lee (2015, str. 1) meni, da je bitcoin za denarne transferje naredil isto, kar je elektronska pošta naredila za pošiljanje pošte. Ali bo to res tako, bo pokazal čas.

V zadnjih mesecih je med deležniki v skupnosti Bitcoin aktualna predvsem problematika, povezana z velikostjo bloka, katere velikost je ohranjena še iz originalnega koncepta. Zaradi povečanega števila transakcij se namreč dogaja, da nekatere transakcije niso pravočasno procesirane. Posledično so se pojavile zahteve po povečanju velikosti posameznega bloka, s čimer pa se ne strinjajo vsi deležniki. Takšna situacija bi lahko eventualno vodila v razdelitev skupnosti (in protokola) v dve za stalno popolnoma ločeni veji Bitcoina, vsaka s povsem svojo različico programske opreme. V takšnem primeru pa bi bilo glede na njegov osnovni idejen koncept celo mogoče argumentirati, da se je Bitcoin izkazal kot neuspel projekt.

Ne glede na to, kaj se bo z Bitcoinom zgodilo v prihodnosti, pa je moje mnenje, da ima tehnologija, na kateri temelji Bitcoin, prihodnost na finančnem področju. Tehnologija na osnovi Bitcoina prinaša nove možnosti za inovacije, na podlagi katerih bo mogoč nastanek novih pa tudi izboljšanje (predvsem zmanjšanje stroškov in povečanje hitrosti izvršbe) obstoječih produktov in sistemov. To dokazujejo vlaganja in testiranja omenjene tehnologije največjih svetovnih igralcev v finančni industriji pa tudi pojav družb in novih produktov, ki se z njo ukvarjajo. S tem potrjujem tudi drugo hipotezo, da ima – ne glede na prihodnost Bitcoina – tehnologija, na kateri temelji Bitcoin, potencial, da postane pomemben del finančnih sistemov. Nova tehnologija, tako imenovana druga različica verige blokov, z Bitcoinom namreč ni neposredno povezana, saj je od njega samo vzela nekatere idejne koncepte, jih nadgradila in razširila njihovo uporabnost, ki presega oblikovanje in prenos vrednosti virtualnih valut.

Moje mnenje je, da bo omenjena tehnologija v prihodnosti igrala pomembno vlogo predvsem pri medsebojnem povezovanju velikih finančnih igralcev (bank, skrbniških bank, borz, klirinških in poravnalnih agentov) z namenom nižanja stroškov in učinkovitejše poravnave sredstev. Prav tako pa bo omogočala, da bodo omenjene institucije svojim strankam lahko ponudile nove in inovativne produkte (predvsem na področju izdaje in trgovanja s finančnimi instrumenti). V nasprotju z Nakamotovo osnovno idejo o odstranitvi

finančnih posrednikov in centralnih institucij pa bo po mojem mnenju omenjena tehnologija najbolj koristila prav njim. Težko si je namreč predstavljati, da bi te dovolile njihovo iztisnitev iz finančnega sistema oziroma da bi privolile v zmanjšanje njihove vloge v njem. Posledično jim je zato tudi v interesu, da tehnologijo razvijajo v svoj prid, namesto da delujejo proti njej.

Za uspeh omenjene tehnologije bo ključnega pomena, da bodo finančne institucije k razvoju tehnologije in posledično postavitvi standardov znotraj določenega finančnega področja pristopile enotno, saj v nasprotnem primeru po mojem mnenju ne bo mogoče doseči glavnih namenov, zaradi katerih sploh želimo vpeljati omenjeno tehnologijo. Ob hkratnem obstoju različnih distribuiranih glavnih knjig na določenem področju oziroma v različnih fazah določenega procesa (na primer poravnave vrednostnih papirjev) namreč ne bi bilo mogoče zmanjšati niti obstoječe kompleksnosti sistema in tudi ne stroškov na najnižjo mogočo raven.

Izjemnega pomena pa je tudi vključitev regulatorjev v proces razvoja omenjene tehnologije. Brez ustrezne podpore oziroma odobritve regulatorjev uporaba omenjene tehnologije ne bo mogoča. Tudi regulatorjem je sicer v interesu, da so v proces vključeni, saj ta lahko pripomore k njihovemu boljšemu delovanju. Distribuirana glavna knjiga namreč omogoča vpogled v zgodovino vseh transakcij, ki so popolnoma in lahko preverljive. Regulator bi bil lahko na primer takoj opozorjen ob poizkusu izvedbe določene transakcije, ki bi bila zaradi določenih razlogov zavrnjena. Od posamezne banke bi lahko na primer zahteval izboljšanje količnika neporavnanih plačil ali pa ustreznejše obvladovanje operativnih tveganj. S pomočjo tovrstne tehnologije bi regulator lažje zaznal, kdaj se določena banka znajde v težavah, in posledično hitreje ustrezno ukrepal. Tako bi regulator lahko posledično močno okrepil svojo preventivno funkcijo (Barnes, 2016).

Menim, da sem z omenjenim delom prispeval k razumevanju pomembnosti poznavanja in razumevanja virtualnih valut in konceptov, ki jih te prinašajo v obstoječe delovanje posameznih finančnih sistemov. Prav tako pa sem nakazal, kam bi lahko v prihodnje šla razvoj in uporaba omenjene tehnologije, ki temelji na virtualnih valutah in hkrati presega njihovo področje, s čimer sem postavil temelje za diskusijo in morebitna nadaljnja raziskovanja omenjenega področja.

LITERATURA IN VIRI

1. Ahtik, M. (2014). Nekateri pravnoekonomski vidiki navideznih valut. V M. Damjan (ur.), *Pravo v informacijski družbi* (str. 273–296). Ljubljana: GV Založba.
2. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014a). Innovations in Payment Technologies and the Emergence of Digital Currencies. *Bank of England Quarterly Bulletin 2014 Q3*. Najdeno 15. julija 2015 na spletnem naslovu http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf
3. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014b). The economics of digital currencies. *Bank of England Quarterly Bulletin 2014 Q3*. Najdeno 15. julija 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2499418
4. Antonopoulos, A. (2014). *Mastering Bitcoin*. b. k.: O`Reilly.
5. Back, A. (2002, 1. avgust). Hashcash - A denial of service counter-measure. Najdeno 15. januarja 2016 na spletnem naslovu http://www.hashcash.org/papers/hashcash.pdf
6. Baek, C., & Elbeck, M. (2015). Bitcoins as an investment or speculative vehicle? A first look. *Applied economic letters*, *22*(1), 30–34.
7. Baran, P. (1964). On Distributed Communications Networks, Communications Systems, *IEEE Transactions*, *12*(1).
8. Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better – How to make bitcoin a better currency. Najdeno 1. julija 2015 na spletnem naslovu http://elaineshi.com/docs/bitcoin.pdf
9. Barnes, D. (2016, marec). One good reason not to buy a jetcar. Najdeno 18. marca 2016 na spletnem naslovu http://securities.bnpparibas.com/quintessence/key-themes/changing-technology/one-good-reason-not-to-buy-a-jet.html
10. Bhaskar, N., & Chuen, D. (2015). Bitcoin exchanges. V D. Chuen (ur.), *Handbook of digital currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (str. 559–573). b. k.: Academic Press.
11. Bheemaiah, K. (2015, 3. februar). Why business schools need to teach about the Blockchain. Najdeno 3. oktobra 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2596465
12. *Bitcoin clock*. Najdeno 31. januarja 2016 na spletnem naslovu http://bitcoinclock.com/
13. *Bitcoin developer reference*. Najdeno 2. januarja 2016 na spletnem naslovu https://bitcoin.org/en/developer-reference
14. *Bitcoin Wiki Transaction fees*. Najdeno 5. januarja 2016 na spletnem naslovu https://en.bitcoin.it/wiki/Transaction_fees
15. *Blockchain Info*. Najdeno 10. februarja 2016 na spletnem naslovu https://blockchain.info/
16. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. Najdeno 13. avgusta 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2495572

17. Brito, J., & Castillo, A. (2013). Bitcoin – A primer for policymakers. *Policy. Summer2103/2014*, *29*(4), 3–12.
18. Buterin, V. (2014, 24. januar). Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. Najdeno 10. novembra 2015 na spletnem naslovu https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211
19. *Coin market cap*. Najdeno 2. februarja 2016 na spletnem naslovu http://coinmarketcap.com/
20. Dai, W. (1998). B-money. Najdeno 15. januarja 2016 na spletnem naslovu http://www.weidai.com/bmoney.txt
21. Depository Trust & Clearing Corporation. (2016, januar). Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape. Najdeno 18. marca 2016 na spletnem naslovu http://www.dtcc.com/~/media/Files/PDFs/DTCC-Embracing-Disruption.pdf
22. Dwyer, G. (2014, 8, maj). The Economics of Bitcoin and Similar Private Digital Currencies. Najdeno 10. decembra 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434628
23. *Ethereum White paper*. Najdeno 28. novembra 2015 na spletnem naslovu https://github.com/ethereum/wiki/wiki/White-Paper
24. Euro Banking Association. (2015, 11. maj). Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios: An exploration for transaction banking and payments professionals. Najdeno 5. novembra 2015 na spletnem naslovu https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf
25. European Banking Authority. (2014, 4. julij). EBA Opinion on "Virtual currencies". Najdeno 20. oktobra 2015 na spletnem naslovu https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
26. European Central Bank. (2012, oktober). Virtual currency schemes. Najdeno 15. oktobra 2015 na spletnem naslovu https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
27. European Central Bank. (2015, februar). Virtual currency schemes – a further analysis. Najdeno 15. oktobra 2015 na spletnem naslovu https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
28. Evropski bančni organ. (2013, 12. december). Opozorilo uporabnikom v zvezi z navideznimi valutami. Najdeno 20. oktobra 2015 na spletnem naslovu https://www.eba.europa.eu/documents/10180/598420/EBA_2013_01030000_SL_TRA.pdf
29. Eyal, I., & Sirer, E. (2013, 01. november). Majority is not enough: Bitcoin mining is vulnerable. Najdeno 18. avgusta 2015 na spletnem naslovu http://arxiv.org/abs/1311.0243

30. Eyal, I. (2014, 26. november). The Miner`s Dilemma. Najdeno 18. avgusta 2015 na spletnem naslovu http://arxiv.org/abs/1411.7099
31. Finančna uprava Republike Slovenije. (2013, 23. december). Davčna obravnava poslovanja z virtualno valuto po ZDoh-2 in ZDDPO-2. Najdeno 6. maja 2016 na spletnem naslovu www.racunovodstvo.net/pojasnila/priloga/4835/4210-11634-2013.pdf
32. Finančna uprava Republike Slovenije. (2015a, julij). Davčno potrjevanje računov. Pogosta vprašanja in odgovori. Najdeno 20. januarja 2016 na spletnem naslovu http://www.fu.gov.si/fileadmin/Internet/Nadzor/Podrocja/Davcne_blagajne_in_VKR/Vprasanja_in_odgovori/Vprasanja_in_odgovori_1_izdaja_Davcno_potrjevanje_racunov.pdf
33. Finančna uprava Republike Slovenije. (2015b, 7. december). Obravnava provizije pri prodaji "bitcoinov" po ZDDV-1. Najdeno 20. februarja 2016 na spletnem naslovu http://www.fu.gov.si/fileadmin/Internet/Davki_in_druge_dajatve/Podrocja/Davek_na_dodano_vrednost/Novice/2015/Obravnava_provizije_pri_prodaji_bitcoinov_po_ZDDV-1.pdf
34. Franco, P. (2015). *Understanding Bitcoin Cryptography, Engineering and Economics.* b. k.: Wiley.
35. Gervais, A., Karame, G., Capkun, S., & Capkun, V. (2014). Is Bitcoin a Decentralized Currency. Najdeno 10. septembra 2015 na spletnem naslovu https://eprint.iacr.org/2013/829.pdf
36. Glaser, F., Haferkorn, M., Weber, M., & Zimmermann, K. (2014). How to Price a Digital Currency? Empirical Insights on the Influence of Media Coverage on the Bitcoin Bubble. *MKWI 2014 (Paderborn) & Banking and Information Technology, 15*(1), 1404–1416.
37. Harvey, C. (2014, 17 maj). Cryptofinance. Najdeno 10. decembra 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438299&rec=1&srcabs=2424516&alg=1&pos=1
38. Kancs, D., Ciaian, P., & Rajcanilova, M. (2015). The digital agenda of virtual currencies: Can bitcoin become a global currency?. Najdeno 15. novembra 2015 na spletnem naslovu http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97043/the%20digital%20agenda%20of%20virtual%20currencies_final.pdf
39. Kaşkaloğlu, K. (2014). Near Zero Bitcoin Transaction Fees Cannot Last Forever. Najdeno 15. oktobra 2015 na spletnem naslovu http://www.decentralgroup.com/archive_files/96cd6f6067fcbaf5e3947d071aa688fb.pdf
40. King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Najdeno 20. januarja 2016 na spletnem naslovu https://www.peercoin.net/assets/paper/peercoin-paper.pdf

41. Kroll, J., Davey, I., & Felten, E. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Najdeno 13. avgusta 2015 na spletnem naslovu https://www.cs.princeton.edu/~kroll/papers/weis13_bitcoin.pdf
42. Krugman, P. (2011, 7. september). Golden Cyberfetters. Najdeno 15. januarja 2016 na spletnem naslovu http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/
43. Lee, L. (2015, 05. september). New Kids on the blockchain: How bitcoin`s technology could reinvent the stock market. Najdeno 10. novembra 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2656501
44. Lo, S., & Wang, J. (2014, 4. september). Bitcoin as Money? Najdeno 10. avgusta 2015 na spletnem naslovu http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.6701&rep=rep1&type=pdf
45. Logar, R. (1998). *Plačilni sistemi: kaj je dobro vedeti o njih*. Ljubljana: Zveza računovodij, finančnikov in revizorjev Slovenije.
46. Luther, W., & White, L. (2014, 5. junij). Can Bitcoin Become a Major Currency?. Najdeno 10. septembra 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604
47. Mankiw, G. (2011). *Principles of Macroeconomics* (6th ed.). b. k.: South-Western Cengage Learning.
48. Mas, I., & Chuen, D. (2015). Bitcoin-Like protocols and Innovations. V D. Chuen (ur.), *Handbook of digital currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (str. 417–451). b. k.: Academic Press.
49. Moore, T., & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. Najdeno 10. novembra 2015 na spletnem naslovu http://fc13.ifca.ai/proc/1-2.pdf
50. Möser, M., & Böhme, R. (2014, 26. oktober). Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. Najdeno 30. septembra 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2530843
51. Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic cash system. Najdeno 10. julija 2015 na spletnem naslovu https://bitcoin.org/bitcoin.pdf
52. Nian, L., & Chuen, D. (2015). Introduction to Bitcoin. V D. Chuen (ur.), *Handbook of digital currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (str. 5–30). b. k.: Academic Press.
53. Pacia, C. (2013a, 2. september). Bitcoin mining explained like you`re five: Part 2 – Mechanics. Najdeno 15. avgusta 2015 na spletnem naslovu https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/
54. Pacia, C. (2013b, 7. september). Bitcoin explained like you`re five: Part 3 – Cryptography. Najdeno 15. avgusta 2015 na spletnem naslovu https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/

55. Pacia, C. (2013c 29. september). Bitcoin explained like you`re five: Part 4 – Securing your wallet. Najdeno 1. februarja 2016 na spletnem naslovu https://chrispacia.wordpress.com/2013/09/29/bitcoin-explained-like-youre-five-part-4-securing-your-wallet/
56. Parker, L. (2015, 19. september). Bitcoin is Officially a Currency, Property, Money, and Now a Commodity. Najdeno 5. februarja 2016 na spletnem naslovu http://bravenewcoin.com/news/bitcoin-is-officially-a-commodity-first-cftc-ruling-against-a-bitcoin-options-trading-platform/
57. Paterrson, R. (2015a, 18. avgust). Alternatives for Proof of Work, Part 1: Proof Of Stake. Najdeno 20. januarja 2016 na spletnem naslovu https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/
58. Paterrson, R. (2015b, 26. avgust). Alternatives for Proof of Work, Part 2: Proof of Activity, Proof of Burn, Proof of Capacity, and Byzantine Generals. Najdeno 20. januarja 2016 na spletnem naslovu https://bytecoin.org/blog/proof-of-activity-proof-of-burn-proof-of-capacity/
59. Paul, G., Sarkar, P., & Mukherjee, S. (2014). Towards a more democratic mining in bitcoin. *Lecture notes in computer science,* 2014(8880), 185–203.
60. Peters, G., Chapelle, A., & Panayi, E. (2014, 4. september). Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective. Najdeno 10. oktobra 2015 na spletnem naslovu http://arxiv.org/abs/1409.1451
61. Peters, G., Panayi, E., Chapelle, A. (2015, 19. avgust). Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. Najdeno 15. februarja 2016 na spletnem naslovu http://arxiv.org/abs/1508.04364
62. Plassaras, N. (2013, 7. april). Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. Najdeno 15. julija 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419
63. Polasik, M., Piotrowska, A., Wisniewski T., Kotkowski, R. & Lightfoot, G. (2015, 31. avgust). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. Najdeno 15. februarja 2016 na spletnem naslovu http://www.tandfonline.com/doi/full/10.1080/10864415.2016.1061413
64. Reid, F., & Harrigan, M. (2012, 7. maj). An Analysis of Anonymity in the Bitcoin System. Najdeno 15. avgusta 2015 na spletnem naslovu http://arxiv.org/abs/1107.4524
65. Ripple. (2014, november). The Ripple protocol: A deep dive for Finance Professionals. Najdeno 10. novembra 2015 na spletnem naslovu https://ripple.com/files/ripple_deep_dive_for_financial_professionals.pdf
66. Ron, D., & Shamir, A. (2013). Quantitative analysis of the full Bitcoin transaction graph. Najdeno 15. avgusta 2015 na spletnem naslovu https://eprint.iacr.org/2012/584.pdf
67. Rosenfeld, M. (2012, 4. december). Overview of Colored Coins. Najdeno 10. novembra 2015 na spletnem naslovu https://bitcoil.co.il/BitcoinX.pdf

68. Sapuric, S., & Kokkinaki, A. (2014, 1. oktober). Bitcoin is volatile! Isn`t that right? Najdeno 10. februarja na spletnem naslovu http://link.springer.com/chapter/10.1007/978-3-319-11460-6_22
69. *SHA-256 hash calculator*. Najdeno 27. decembra 2015 na spletnem naslovu http://www.xorbin.com/tools/sha256-hash-calculator
70. Shirriff, K. (2014). Bitcoins the hard way: Using the raw Bitcoin protocol. Najdeno 25. januarja 2016 na spletnem naslovu http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html
71. Smith, T. (2016, 3. marec). R3 completes trial of five cloud-based emerging blockchain technologies with 40 bank consortium members. Najdeno 5. marca 2016 na spletnem naslovu http://r3cev.com/press/2016/3/3/r3-completes-trial-of-five-cloud-based-emerging-blockchain-technologies-with-40-bank-consortium-members
72. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. b. k.: O`Reilly.
73. Szabo, N. (2005, 27. december). Bit gold. Najdeno 15. januarja 2016 na spletnem naslovu http://unenumerated.blogspot.si/2005/12/bit-gold.html
74. Tasca, P. (2015, 7. september). Digital currencies: Principles, trends, Opportunities, and Risks. Najdeno 15. novembra 2015 nas spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657598
75. Tschorsch, F., & Scheuermann, B. (2015). Bitcon and beyond: A technical Survey on Decentralized digital currencies. Najdeno 15. novembra 2015 na spletnem naslovu https://eprint.iacr.org/2015/464.pdf
76. Urad Republike Slovenije za preprečevanje pranja denarja. (2014, 22. januar). Virtualna valuta bitcoin – obvestilo za zavezance. Najdeno 5. januarja 2016 na spletnem naslovu http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Bitcoin_obvestilo.pdf
77. Velde, F. (2013). Bitcoin: a primer. Najdeno 15. julija 2015 na spletnem naslovu https://www.cs.princeton.edu/courses/archive/fall14/cos109/bitcoin.primer.pdf
78. Vigna, P., & Casey, M. (2015). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*. New York: St. martin`s Press.
79. Wu, C., & Pandey V. (2014). The value of bitcoin in enhancing the efficiency of and investors`s portfolio. *Journal of financial planning*, *27*(9), 44–52.
80. Yermack, D. (2014, 1. april). Is bitcoin a real currency? An economic appraisal. Najdeno 15. julija 2015 na spletnem naslovu http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599&rec=1&srcabs=2438299&alg=1&pos=3