UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

DIPLOMSKO DELO

BITCOIN - DENAR PRIHODNOSTI?

Ljubljana, november 2015 MILAN MILOŠEVIĆ

IZJAVA O AVTORSTVU

Spodaj podpisani Milan Milošević, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor diplomskega dela z naslovom Bitcoin - denar prihodnosti?, pripravljenega v sodelovanju s svetovalcem prof. dr. Alešem Berk Skokom.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo diplomskega 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 diplomskem 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 diplomskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 11.11.2015 Podpis avtorja:_____

KAZALO

KAZALO SLIK

UVOD

V vsakdanjem življenju se nenehno srečujemo z denarjem. V današnji družbi je denar tako samoumeven del gospodarstev, da z njim vsakodnevno rokujemo, kljub temu pa večinoma ne vemo, kaj konkretno zapisane vrednosti na bankovcih predstavljajo in od kod izvirajo. Denar je bistvo gospodarstva, je tisto, kar simbolizira trgovsko strukturo, znotraj katere operiramo. Posledično monetarni sistem predstavlja temelj današnjih gospodarstev in je zato ključni del naše družbe.

Skozi zgodovino lahko opazujemo številne spremembe oblik denarja in spreminjanje njegovih funkcij. Povečana stopnja medsebojne povezanosti, ki jo omogoča internet, je vplivala tudi na naravo finančnih transakcij. Z razvojem socialnih medijev, programske opreme in pametnih tehnologij smo priča novim oblikam denarja, ki se raztezajo onkraj tradicionalnih plačilnih sredstev in vladno garantiranih valut, saj finančno poslovanje danes vključuje tudi mobilna plačila ter digitalne in virtualne valute.

Glede na to, da že obstajajo virtualni svetovi, je bilo samo vprašanje časa, kdaj se bo pojavil tudi virtualni monetarni sistem, ki bo dopolnil obstoječi monetarni red. Pravi digitalni denar združuje področji ekonomije in kriptografije, prav preplet teh dveh področij pa je botroval nastanku Bitcoina, ki predstavlja prvi popolnoma decentraliziran sistem digitalnih plačil. Namesto da bi se zanašal na odločitve ljudi, za Bitcoinom stojijo enostavna matematična pravila, ki določajo in vodijo sistem, ki je veliko bolj sofisticiran od obstoječega monetarnega sistema.

Namen diplomskega dela je raziskati, ali se lahko Bitcoin uveljavi na globalni ravni in nadomesti tradicionalne valute na področju plačil. Glede na to, da ima Bitcoin kratko zgodovino in je njegov status v naši družbi ter nadaljnji razvoj še v povojih, bom Bitcoin umestil v trenutni finančni sistem in poskušal ugotoviti, kakšne možnosti ima za spremembo svetovnega sistema plačil. Temeljni cilj diplomskega dela je predstaviti Bitcoin, ga primerjati s tradicionalnimi valutami ter pokazati, kje se skriva največji potencial t.i. digitalne kriptovalute.

Glavne metode dela, ki sem jih uporabil pri pripravi diplomskega dela, slonijo na analizi sekundarnih virov, predvsem strokovne literature tujih avtorjev člankov, prispevkov in drugih virov z najnovejšimi informacijami iz preučevanega področja. Za opis denarja in Bitcoina sem uporabil deskriptivno metodo, s pomočjo katere sem predstavil tematiki skozi zgodovinski pogled. Za primerjavo prednosti in slabosti Bitcoina sem uporabil komparativno metodo, s pomočjo katere so predstavljene ključne pozitivne in negativne značilnosti Bitcoina.

Diplomsko delo je razdeljeno na pet poglavij. V uvodu sem opredelil cilj diplomskega dela in podal metode preučevanja ter navedel strukturo dela. V prvem poglavju sem opredelil funkcije in oblike denarja, kjer je poudarek na digitalni obliki denarja, ki je bistvena za razumevanje obravnavane problematike. V drugem poglavju sem opredelil Bitcoin, in sicer tako, da sem predstavil osnovne elemente, na katerih temelji. Glede na to, da je kriptografija bistvo sistema, na katerem je Bitcoin osnovan, v nadaljevanju predstavim tudi

kriptografijo in samo delovanje sistema. Tretje poglavje je namenjeno primerjavi prednosti in slabosti Bitcoina, kjer sem se osredotočil na primerjavo konkretnih pozitivnih in negativnih lastnosti, ki jih Bitcoin prinaša. V četrtem poglavju se posvečam potencialom, ki jih Bitcoin ponuja danes in v prihodnosti, tako kot sistem valute kot tudi decentraliziran sistem digitalnih plačil. Zadnji del je namenjen sklepu, v katerem povzemam glavne ugotovitve diplomskega dela. Za lažje branje in razumevanje Bitcoina se v prilogi nahaja slovar s ključnimi termini, ki so povezani z Bitcoinom.

1 DENAR

Preden se posvetim Bitcoinu in njegovi umestitvi v trenutni sistem, bom najprej definiral denar in opredelil njegove oblike. Za razumevanje delovanja denarja je potrebno le-tega umestiti v družbeni kontekst in razložiti njegov namen, od kod izhaja njegova vrednost in kakšne so njegove relacije s stvarmi, ki nas obkrožajo.

Denar je mehanizem, preko katerega se na trgu skozi sili ponudbe in povpraševanja nenehno vzpostavlja ravnotežje. Glavna funkcija denarja je pošiljanje zgodnjih in primernih signalov o vrednosti dobrin in storitev, tako da skozi spremembe cen odstranjuje odvečne zaloge ponudbe ali povpraševanja. Trgi so redko popolni in v praksi tudi denar ne more odstraniti vseh negotovosti, kljub temu pa noben drug mehanizem ne vzpostavlja ravnotežja tako dobro kot prav denar (Davies, 2002, str. 29-30). Denar poenostavi osnovno človeško gospodarsko potrebo po menjavi. Vse gospodarske transakcije temeljijo na dejstvu, da si oseba A želi nekaj, kar ima oseba B in je slednja pripravljena to stvar prenesti osebi A, če nazaj dobi nekaj, kar si želi sama. Očitno je, da mora veljati obojestranska povezava, torej ne samo, da si oseba A želi, kar oseba B ponuja, ampak tudi, da si oseba B želi, kar ponuja oseba A. Denar je najboljša oblika orodja take menjave. Je ureditev, skozi katero posameznik usmerja svojo delovanje in lastnino, da bi dosegel cilje, ki jih drugače ne bi mogel doseči neposredno. Kljub vsemu učinkovitost denarja ne gre iskati v fizičnih prednostih posamezne oblike denarja, temveč se njegova učinkovitost kaže predvsem v prednostih široke uporabe kljub njegovim snovnim omejitvam (Simmel, 2005, str. 210).

Današnji monetarni sistem temelji na sprejemanju denarja kot zakonitega plačilnega sredstva. Medij izmenjave v obliki kovanega in papirnatega denarja, ki ga ljudje sprejemajo kot plačilno sredstvo, v osnovi izvira iz družbenega prepričanja, da je to legitimno plačilno sredstvo in ga zato kot takega večina ljudi tudi jemlje. Kljub temu da papirnati denar nima uporabne vrednosti, ga sprejemamo kot plačilno sredstvo, saj pričakujemo, da ga bodo sprejeli tudi vsi ostali. To praktično pomeni, da ima plačilno sredstvo takšno vrednost, kakršno mu jo ljudje pripišejo (Friedman, 1994, str. 18). Denar je torej dogovor, ki se krepi skozi zaupanje ljudi v gospodarski in pravni sistem posamične državne ureditve. Samuelson in Nordhaus (2002, str. 489) trdita, da denarja ne uporabljamo zaradi njegove neposredne koristnosti – njegova vrednost je v tem, kaj

oziroma koliko lahko z njim kupimo. Tudi onadva potrjujeta, da je vrednost denarja stvar družbenega dogovora.

Pred letom 1971 so bile vse pomembnejše svetovne valute direktno ali indirektno vezane na blago, kar pomeni, da je država zagotavljala menjavo svoje valute v zlato. Po 15. avgustu 1971 pa je predsednik ZDA Richard M. Nixon preko monetarnega sporazuma Bretton-Woods prekinil obveznost ZDA, da spreminja dolarje v zlato po fiksni ceni 35 USD na unčo zlata. Od takrat naprej ni bila nobena pomembnejša svetovna valuta več vezana na blago. Papirnati denar torej nima nobene vrednosti kot blago, temveč njegovo vrednost, koliko lahko nekdo kupi s papirnatim denarjem, določata ponudba in povpraševanje. Denar predstavlja vsako stvar, ki je splošno sprejeta za izmenjavo dobrin ali storitev. Denar ni sprejet kot stvar za porabo, temveč kot nekaj, kar predstavlja začasno obliko nakupne moči, da bi le-ta bila kasneje porabljena za nakup drugih stvari oz. dobrin (Friedman, 1994, str. 22-23).

1.1 Funkcije denarja

Funkcije denarja olajšajo razumevanje koncepta denarja in ga umestijo v finančni kontekst. Denar je ogrodje finančne strukture in zato je potrebno razumeti, zakaj so te funkcije pomembne, da bi denar dobro opravljal namen plačilnih sredstev.

Morda je najboljši kazalnik bistva denarja njegova sposobnost primerjave relativne vrednosti katerekoli izmed stotine tisočih stvari in storitev. Hkrati pa denar primerjavo različnih vrednosti zagotavlja z minimalnimi stroški (Davies, 2002, str. 16). Vendar pa si denarja ne želimo zaradi njega samega, saj kovancev za preživetje ne moremo pojesti, ampak ga uporabljamo kot pripomoček pri trgovanju in menjavi (Samuelson & Nordhaus, 2002, str. 472). V skoraj vseh tržnih transakcijah v našem gospodarstvu je denar uporabljen kot posrednik v menjavi za nakup storitev ali dobrin. Uporaba denarja kot posrednika v menjavi podpira gospodarsko učinkovitost z minimiziranjem transakcijskih stroškov (Mishkin, 2004, str. 45).

Denar kot hranilec vrednosti tudi "skladišči" nakupno moč skozi čas. Hranilna vrednost hrani nakupno moč od trenutka prejetega prihodka, dokler ni porabljena. Hranilna funkcija je koristna zato, ker večina od nas ne želi porabiti vsega prihodka takoj ob prejetju, ampak šele takrat, ko se pojavi konkretna potreba (Mishkin, 2004, str. 47).

Sama vrednost denarja izhaja iz tega, da je določena stvar splošno sprejet posrednik menjave, mera vrednosti ali enota za shranjevanje vrednosti. Denar torej omogoča preproste in hitre transakcije, enotno določanje cen in preprosto hranjenje vrednosti skozi čas, to pa so tudi glavne tri funkcije denarja. Posrednik pri menjavi je prva in zagotovo najpomembnejša funkcija denarja. To praktično pomeni, da denarja nimamo zaradi denarja samega, ampak ker ga želimo potrošiti za stvari, ki si jih želimo. Obračunska mera oziroma mera vrednosti je druga funkcija denarja, kar pomeni, da je denar enota, s pomočjo katere

merimo vrednost drugih stvari. Denar kot hranilec vrednosti predstavlja tretjo funkcijo, pomeni pa, da hrani vrednost skozi čas (Samuelson & Nordhaus, 2002, str. 473).

Blago mora izpolnjevati naslednje kriterije, da uspešno opravlja funkcijo denarja (Mishkin, 2004, str. 46):

1. mora biti enostavno standardizirano, kar pomeni, da mora biti vrednost blaga enostavno določljiva,
2. mora biti široko sprejeto,
3. mora biti deljivo, da se ga lahko enostavno razdeli v manjše enote,
4. mora biti enostavno prenosljivo in
5. ne sme biti hitro pokvarljivo.

1.2 Oblike denarja

V zgodovini smo bili priča mnogim oblikam denarja, ki so opravljale osnovne funkcije denarja. Denar je skozi čas spreminjal obliko, saj smo lahko opazovali različne vrste blaga, ki so izpolnjevale ključne kriterije denarja in skozi čas izpodrivale ena drugo. Mishkin (2004, str. 46) ugotavlja, da so imele skozi zgodovino različne oblike denarja, ki so zadovoljile zgoraj navedene kriterije, zelo neobičajne oblike. Raznolikost oblik denarja, ki so se razvile skozi leta, je dokaz domiselnosti človeka, prav tako kot je razvoj orodja in jezika merilo človeškega napredka.

Denar je skozi zgodovino doživel več razvojnih oblik, ki so si sledile v naslednjem vrstnem redu, in sicer je blagovnemu sledil stvarni denar in temu nato kovani denar. Po polnovrednih kovancih je nastal listinski denar, kateremu sta sledila papirnati in knjižni denar (Ribnikar, 1999, str. 12).

Ne glede na to, katero obliko je denar prevzel, najsi so funkcije denarja opravljale školjke, kamni, zlato ali papir, je le-ta moral v vsakem gospodarstvu opravljati tri primarne funkcije. V blagovni menjavi so bile dobrine in storitve menjane direktno za druge dobrine in storitve, kar je posledično vodilo do visokih transakcijskih stroškov, saj so ljudje morali zadovoljiti dvojno naključno hotenje: najti nekoga, ki ima storitev ali dobrino, ki jo mi hočemo, in hkrati najti nekoga z željo po dobrini ali storitvi, ki jo mi ponujamo (Mishkin, 2004, str. 45).

Do iznajdbe denarja je tako prišlo zato, da se je olajšalo trgovanje. Specifičnost denarja je v tem, da omogoča menjavo ceneje, kot bi to opravljale ostale stvari (Ribnikar, 1999, str. 30). S tem se strinja tudi Mishkin (2004, str. 46), ki pravi, da denar povečuje gospodarsko učinkovitost s tem, ko krajša čas, ki bi bil sicer porabljen za izmenjavo dobrin in storitev. Denar je bistven del gospodarstva, je kot mazivo, ki preko nižanja transakcijskih stroškov omogoča bolj tekoče delovanje in na ta način spodbuja specializacijo in delitev dela. Tako učinkovito omogoča ljudem, da se specializirajo za stvari, ki jih počno najbolje.

1.2.1 Tradicionalne oblike denarja

a) Blagovni denar

Sprva je imel blagovni denar posredno denarno funkcijo, pri čemer pa je ohranjal svojo uporabno funkcijo. Sčasoma je blago začelo izgubljati na uporabnosti in je vedno bolj prevzemalo vlogo menjalnega posrednika. Ko je prišlo do procesa dematerializacije, so se ljudje vedno bolj zavedali uporabne vrednosti blaga. Z razširitvijo splošne uporabe blagovnega denarja je le-ta postal okoren menjalni posrednik in so ga zaradi kvarljivosti ter hitre obrabljenosti v vlogi posrednika nadomestile kovine. Te so deljive, homogene, niso kvarljive in hranijo v majhni količini veliko vrednost (Ribnikar, 1999, str. 13).

b) Kovani denar

Z odkritjem kovin je prišlo do nove oblike denarja, in sicer blagovnega denarja v obliki kovin. Tako srebro kot zlato imata notranjo vrednost, kar izvira iz tega, da imata sama po sebi uporabno vrednost, prav zato sta bili skozi čas to tudi najbolj uporabljani kovini. Prednost zlate valute je bila ta, da je imel kovani denar notranjo vrednost. Posledično vladi ni bilo potrebno zagotavljati njene vrednosti, temveč je to skozi ponudbo in povpraševanje po zlatu počel trg sam (Samuelson & Nordhaus, 2002, str. 467). Ko govorimo o notranji vrednosti, moramo razumeti, da v fizičnem svetu pravzaprav nič nima notranje vrednosti. Tudi ko rečemo, da ima zlato notranjo vrednost, je to zaradi tega, ker so mu ljudje določili vrednost zaradi lastnosti, ki jih ima: je relativno redko, ne oksidira, je dober prevodnik elektrike in lepo izgleda (Seaman, 2013, str. 8).

c) Papirnati denar

Kljub dobrim lastnostim kovanega denarja so sčasoma tudi pri kovinah naleteli na slabosti, kot je npr. tehtanje ali merjenje čistosti, kar je podražilo menjavo. Zato so ljudje začeli za zlato, ki je mirovalo pri zlatarju, prejemati potrdila in z njimi poslovati z drugimi ljudmi. Z naraščajočimi potrebami po vse večji količini denarja, se je pogodbeni odnos med zlatarjem in lastnikom zlata spremenil iz hrambene v kreditno pogodbo. To pomeni, da lastnik zlata postane zlatar in se zaveže k izplačilu zlata tiste kakovosti in količine, ki je zapisana na potrdilu imetnika. Ta potrdila so bila predhodniki bankovcev. Zaradi prevelike špekulacije zlatarjev, ki so posojali več zlata, kot so ga imeli, je prihajalo tudi do bankrota posameznih zlatarjev in vlagateljev. Zato se je v področje kreditnih pogodb vmešala država in predpisala načela izdajanja bankovcev ter zagotovila pravico izdajanja denarja le eni banki, ki je postala emisijska oziroma izdajateljska banka (Ribnikar, 1999, str. 18).

Od starodavnih dni do nekaj stoletij nazaj je blagovni denar deloval kot posrednik pri menjavi. Naslednja stopnja je bil papirnati denar. Le-ta je imel na začetku garancijo, da ga je moč zamenjati za plemenite kovine. Sčasoma se je plačilno sredstvo razvilo v *fiat* denar, to je papirnato valuto z odlokom države, da je zakonsko plačilno sredstvo in mora zato biti

sprejeto kot plačilo. Naslednji korak v evoluciji plačilnih sistemov je bil izum čeka, ki je predstavljal veliko novost in izboljšal učinkovitost plačilnega sistema (Mishkin, 2004, str. 49-50). Moderna gospodarstva običajno uporabljajo fiat denar, ki so ga ljudje pripravljeni sprejeti in zamenjati za dobrine in storitve preprosto zato, ker zaupajo centralni oblasti, kar pomeni, da je zaupanje ključen element tega denarnega sistema, predvsem z vidika stabilnosti gospodarstva (European Central Bank, 2012, str. 9-10). Na začetku je bil denar odsev redkosti fizičnih virov, kot sta zlato ali srebro, za katere ga je bilo moč zamenjati. To je denarju dajalo vrednost, saj je nekdo, če je želel ustvariti več denarja, moral zagotoviti tudi več virov. Ta ključna povezava se je ob pojavu fiat denarja prekinila, saj se lahko količina fiat denarja ustvarja brez meja, vrednost namreč ni več vezana na katerikoli vir, temveč izhaja iz zakona.

d) Knjižni denar

Knjižni denar, imenovan tudi žiralni ali depozitni denar, je imetje, ki ga imajo podjetja, ostale institucije ali posamezniki pri poslovnih bankah. Skozi zgodovino so se zvrstile številne oblike denarja, pri večini pa se je pokazala neučinkovitost pri plačevanju večjih zneskov. S pomočjo knjižnega denarja je bilo moč imetje izplačati v gotovini, vendar je lahko posameznik svoj dolg plačal tudi tako, da je dolžni znesek iz svojega računa prenesel na račun svojega upnika (Ribnikar, 1999, str. 20).

1.2.2 Elektronski denar

Tehnične izboljšave posrednikov v izmenjavi so se dogajale že več kot tisočletje. Večinoma je šlo za manjše spremembe, vendar pa smo bili priča tudi dvema velikima spremembama: prva, ko je tiskanje denarja nadomestilo kovanje denarja, in druga, ko je bil izumljen elektronski prenos denarja. Prva sprememba je spodbudila razvoj bančništva, medtem ko druga odpira pot k univerzalnemu in takojšnjemu prenosu denarja (Davies, 2002, str. 649). Papirnati denar je z možnostjo shranjevanja in posojanja denarja odprl razvoj bančništvu in s tem sprožil gospodarski razcvet, medtem ko je internet poleg mnogih sprememb na različnih področjih nakazal tudi možnost nove oblike prenosa denarja in tudi razumevanja denarja na splošno.

Z razvojem na finančnem področju je prišlo do tega, da ima denar mnogo substitutov, in sicer kot menjalni posrednik in tudi kot hranilec vrednosti. S tem ko ga v funkciji menjalnega posrednika nadomeščajo različne finančne oblike, je potrebno imeti v obtoku vse manj denarja (Ribnikar, 1999, str. 29). Razvoj tehnologije in interneta sta omogočili pojav elektronskih plačil. Na spletni strani Banke Slovenije Zakon o plačilnih storitvah in sistemih (Ur.l. RS, št. 58/09, 34/10, 9/11 in 32/12, v nadaljevanju ZplaSS) opredeljuje denar kot shranjeno denarno vrednost v obliki terjatve imetnika elektronskega denarja do izdajatelja elektronskega denarja, ki (Banka Slovenije, 2015):

- je v elektronski obliki,

- jo izda izdajatelj elektronskega denarja na podlagi prejema denarnih sredstev za namen izvrševanja plačilnih transakcij in
- jo kot plačilno sredstvo sprejme oseba, ki ni izdajatelj elektronskega denarja.

Če poenostavimo, lahko rečemo, da je elektronski denar v bistvu elektronski nadomestek za gotovino, ki je shranjen na elektronski napravi in je namenjen elektronskemu plačevanju oziroma izvrševanju plačilnih transakcij (Banka Slovenije, 2015).

V obdobju elektronskega bančništva tradicionalne državne valute počasi postajajo zastarele. Mnogim strankam valuta države v kateri bivajo ne predstavlja edine valute, ki jo uporabljajo. Na trgu danes obstajajo ponudbe raznovrstnih storitev različnih finančnih institucij v različnih konkurenčnih valutah. Medtem ko podjetja ljudem ponujajo veliko izbiro alternativ tradicionalnim valutam, se državnim oblastem kot denarnim monopolistom niža lastna učinkovitost. Monetarna oblast zmeraj poskuša braniti svojo monopolno moč tako, da zagotovi, da se denarna ponudba ustvarja endogeno (Davies, 2002, str. 649-650).

Poznamo dva sistema elektronskega denarja, ki sta prisotna v svetovnih gospodarstvih, in sicer centraliziran in necentraliziran sistem. Centralizirani sistemi delujejo kot posredniki elektronskega denarja, ki uporabnikom omogočajo digitalno menjavo denarja preko svoje banke. Pri decentraliziranem sistemu ni določene avtoritete, ki bi nadzorovala valutni trg. Transakcije so nepovratne za razliko od centraliziranega sistema, kjer se plačilo lahko povrne. Decentralizirani sistemi so lahko manj stabilni od centraliziranih sistemov, saj v osnovi ni standardov za varovanje potrošnikov (Štok, 2012, str. 25-26).

Najbolj znan primer centraliziranega sistema je PayPal, ki deluje kot posrednik pri elektronskih transakcijah. PayPal je mednarodni spletni plačilni sistem, ki procesira milijone plačil dnevno in nudi ljudem bolj učinkovit način pošiljanja denarja. Sistem poteka tako, da posameznik v zameno za prejeto storitev ali dobrino nakaže denar zaupanja vrednemu posredniku - v tem primeru PayPalu, ki za svojo storitev zaračuna določeno provizijo. Tako pošiljatelj kot prejemnik morata imeti odprt račun pri PayPalu in mu posredovati informacije o svojem bančnem računu, da se transakcija lahko uspešno izvede. Centralizirani sistemi imajo znanega ustanovitelja in delujejo pod nadzorom finančnih institucij (PayPal Case Study, 2015).

1.2.3 Virtualni denar

Preden opredelim virtualni denar, je potrebno opredeliti okolje, v katerem ta valuta deluje. Virtualna skupnost je kraj znotraj kibernetskega prostora, kjer posamezniki sodelujejo in sledijo vzajemnim interesom ali ciljem. Obstaja več vrst virtualnih skupnosti, od socialnih omrežij, kot sta Facebook in Twitter, preko skupnosti, ki delijo znanje, npr. Wikipedia in tudi take strani, ki ustvarjajo virtualni svet, kot je Second Life. V nekaterih primerih so te virtualne skupnosti ustvarile in dale v obtok tudi svojo virtualno valuto, ki je namenjena

izmenjavi blaga in storitev, ki jih ponujajo. S tem so virtualne skupnosti ustvarile novo obliko denarja (European Central Bank, 2012, str. 10-11).

Evropska centralna banka v svojem poročilu definira virtualno valuto kot nereguliran digitalni denar, ki je izdan in običajno kontroliran s strani izdajateljev ter je uporabljen in sprejet med člani določene virtualne skupnosti. Virtualne valute se ponavadi lahko kupijo na dva načina (European Central Bank, 2012, str. 13):

a) Prvi način je nakup s pomočjo pravega denarja po predhodno določenem menjalnem tečaju. Virtualna valuta sama navadno nima blagovno podprte vrednosti.
b) Drugi način je povečanje svoje zaloge virtualne valute s sodelovanjem v posebnih dejavnostih, kot je na primer odzivanje na promocije ali oglaševanje.

Danes obstaja veliko vrst virtualnih valut in to področje se hitro razvija, saj zelo hitro nastajajo nove. Znotraj virtualnega denarja ločimo tri kategorije tovrstnega denarja (European Central Bank, 2012, str. 13-16):

a) Zaprta virtualna valuta

Zaprta virtualna valuta ni povezana z realnim gospodarstvom. V praksi to izgleda tako, da uporabniki plačajo določeno članarino, v zameno pa potem lažje pridobivajo virtualni denar, s katerim lahko kupijo določene storitve in dobrine znotraj te virtualne skupnosti, medtem ko tega denarja ne morejo pretvoriti nazaj v katerokoli svetovno valuto. Primer take virtualne valute je virtualno zlato v računalniški igri *World of Warcraft* (v nadaljevanju WoW), kjer si igralci z različnimi članarinami lahko kupujejo različne stvari znotraj igre, medtem ko je prodaja in nakup WoW zlata zunaj igre strogo prepovedana s strani podjetja, ki določa pogoje vsem igralcem WoW okolja.

b) Virtualna valuta z enosmernim tokom

V tem primeru gre za nakup virtualne valute s tradicionalno valuto, pri čemer pa te kupljene virtualne valute ne moremo več zamenjati nazaj v tradicionalne valute, temveč jo lahko porabimo le znotraj tega virtualnega trga. Pri tej valuti je poleg virtualnih dobrin in storitev moč kupiti tudi dobrine in storitve v realnem svetu. Primer take valute ima Facebook, kjer je moč kupiti stvari s pravim denarjem, vendar teh stvari ne moremo prodati in dobiti denarja nazaj.

c) Virtualna valuta z dvosmernim tokom

Virtualna valuta z dvosmernim tokom predstavlja virtualno valuto, kjer je denar moč zamenjati za virtualni denar in ga po potrebi lahko zamenjamo tudi nazaj v realni denar preko menjalnice v realni denar. Primer take valute so Linden dolarji v virtualnem svetu, imenovanem Second Life, kjer obstaja virtualna ekonomija, v kateri uporabniki med seboj kupujejo in prodajajo dobrine in storitve. Prav tako pa je moč prislužene Linden dolarje zamenjati nazaj v ameriške dolarje.

1.2.4 Digitalni denar

Digitalni denar kot povezovalni mehanizem za elektronsko poslovanje temelji na povezanosti gospodarske logike in kriptografije. Napredek v posamezni vedi še ne bo pripomogel k pospešitvi rasti elektronskega poslovanja, zato mora obstajati sinergija obeh omenjenih področij. Na področju kriptografije, ki skrbi za posameznikovo zasebnost in varnost, si trg želi možnosti izbire med različnimi denarnimi ponudniki. Na področju ekonomije pa trg išče najboljšo denarno enoto vrednosti. Denar je življenjska sila gospodarstva, ki simbolizira gospodarsko strukturo, v kateri delujemo (Matonis, 1995, str. 1).

Zasebni digitalni denar mora izpolnjevati naslednjih deset lastnosti (Matonis, 1995, str. 2-3):

1. Varnost mora biti zagotovljena skozi transakcijski protokol. Oseba A mora digitalni denar posredovati osebi B, brez da bi bil kdo od njiju ali kdorkoli drug zmožen spremeniti ali ponarediti elektronski znak.

2. Anonimnost mora jamčiti zasebnost transakcij na več nivojih. Poleg šifriranja je neizsledljivost ena od značilnosti digitalnega denarja. Oseba A in oseba B morata imeti možnost ostati anonimna ob plačevanju in prejemanju plačila, to pomeni, da morajo akterji transakcij imeti možnost biti nevidni z vidika nezmožnosti sledenja transakcijam.

3. Prenosljivost v obliki varnosti uporabe ne sme biti odvisna od fizične lokacije. Denar bi lahko prenesli preko računalniških mrež ali tudi brez njih na prenosljive pomnilniške naprave. Uporabniki bi morali imeti možnost prenašati svoj digitalni denar tudi brez računalniške mreže.

4. Dvosmernost velja, če je digitalni denar moč poslati drugim uporabnikom. Bistveno je, da so plačila preko vrstniškega omrežja možna tudi, če kdo izmed udeležencev nima statusa registriranega trgovca.

5. *Offline* delovanje pomeni, da se transakcije med dvema uporabnikoma lahko izvedejo tudi, če nista med seboj povezana, to pomeni, da za izvedbo plačila ni potreben dostop do strežnika. Oseba A lahko nek znesek prosto posreduje osebi B brez prisotnosti tretje strani, ki bi to transakcijo potrdila.

6. Deljivost elektronskega denarja pomeni, da lahko znesek denarja razdelimo na več manjših delov. Denar mora biti deljiv, kar pomeni, da lahko od določenega zneska porabimo le del.

7. Neomejen rok veljavnosti pomeni, da digitalni denar ne more poteči. Mora zadržati vrednost, dokler ni izgubljen ali uničen. Kdorkoli spravi digitalni denar na varno, ga ima po 10 ali 20 letih še vedno možnost uporabiti.

8. Široka sprejemljivost pomeni, da mora biti digitalni denar dobro poznan in sprejet v ekonomskem prostoru. Primarno je to moč urediti skozi prepoznavnost in zaupanje v izdajatelja.

9. Uporabniku prijazen pomeni, da mora biti elektronski denar enostaven za uporabo, tako za porabo kot tudi za prejemanje denarja. Enostavnost vodi v množično uporabo, le-ta pa k širši sprejetosti. V praksi to pomeni, da uporabniku ni potrebno poznati kriptografije, da bi uporabljal elektronski denar.

10. Svobodna valuta pomeni, da je digitalni denar označen v enotah, ki niso podobne svetovnim valutam. V tem pogledu bi tak denar konkuriral mednarodnemu denarju, izdanemu s strani držav.

Razlika med virtualno valuto in elektronskim denarjem je v tem, da je elektronski denar povezan s tradicionalnim denarjem in ima izdajatelj zakonsko odgovornost do uporabnika, saj so shranjena sredstva izražena v isti enoti kot "realne" valute - npr. evro, ameriški dolar ipd. Iz virtualne valute pa ni vedno možno dobiti nazaj tradicionalno valuto, saj so menjalni tečaji diktirani izključno preko ponudbe in povpraševanja. Podjetje, ki izdaja virtualni denar, ima popoln nadzor nad virtualno valuto, ki se hrani v navidezni obračunski enoti (European Central Bank, 2012, str. 16). Sistemi elektronskega denarja so regulirani in institucije, ki izdajajo plačilna sredstva v obliki elektronskega denarja so pod nadzorom ustreznih institucij. To pa ne velja za sisteme virtualnih valut, kar posledično pomeni, da so tveganja pri slednjih valutah večja.

1.2.4.1 DigiCash

Leta 1990 je David Chaum ustvaril prvo svetovno digitalno valuto, imenovano DigiCash. Skozi koncept "skritih podpisov", ki jih je avtor predstavil že sedem let prej, je postavil sistem, kjer se ob transakciji z DigiCashem lahko zakrije identiteta prejemnika plačila, kot tudi čas in znesek plačila, zato tretja stran - večinoma banka - nima dostopa do teh podatkov. DigiCash je v praksi deloval bolj kot anonimna predplačniška kreditna kartica kot resnično digitalna valuta, saj so plačniki najprej morali denar nakazati na bančni račun, da so potem lahko denar skozi sistem DigiCasha nakazali nekomu drugemu. Kljub vsemu je princip anonimnosti in zasebnosti te digitalne valute spodbudil razmišljanje o tej temi, kar je posledično pripeljalo do pojava Bitcoina (Peng, 2013, str. 8-9).

2 OPREDELITEV BITCOINA

Bitcoin je digitalni denarni sistem, ki je v bistvu zbirka različnih konceptov in tehnologij, ki tvorijo osnovo njegovega "ekosistema". Sistem vključuje tudi valuto, preko katere se vrednost blaga shranjuje in posreduje med udeleženci Bitcoin omrežja (Antonopoulos, 2014, str. 1). Sistem temelji na vrstniški mreži (angl. *peer-to-peer*), podobni omrežju BitTorrent, ki je protokol za izmenjavo datotek, kot so filmi, igre, glasba in druge vsebine na internetu. Bitcoin deluje na globalni ravni in se lahko uporablja kot valuta za vse vrste poslov, najsi zadevajo virtualno ali realno blago in storitve. Bitcoin temelji na decentraliziranem vrstniškem omrežju, kar pomeni, da ne obstaja kakršnakoli finančna ali druga institucija, ki bi sodelovala v transakcijah, saj uporabniki te naloge opravljajo sami (European Central Bank, 2012, str. 21).

Vzrok za nastanek Bitcoina izvira iz potrebe, ki jo je v svojem dokumentu leta 2008 opredelil avtor Satoshi Nakamoto, za katerega še danes ne vemo, kdo pravzaprav je; ta psevdonim najbolj verjetno predstavlja posameznika ali skupino ljudi. Osnovni motiv za izvedbo koncepta Bitcoina je kritika družbene odvisnosti od finančnih institucij na področju elektronskih plačil, saj le-te služijo kot zaupanja vredni posredniki pri postopku plačil. Sistem sicer v osnovi deluje zadovoljivo za večino transakcij, ima pa veliko pomanjkljivost, in sicer to, da temelji na zaupanju. Če želi oseba A nakazati določen znesek osebi B, lahko to stori le preko posrednika, ki mu zaupata obe strani. Zaupanje, ki ga nudi tovrstna finančna institucija, prinese določene transakcijske stroške, ki se jim po mnenju avtorja Bitcoina lahko izognemo. Satoshi Nakamoto predstavi rešitev za elektronski plačilni sistem, in sicer kriptografski dokaz, ki nadomesti vmesnika in s tem omogoči, da lahko stranke direktno, brez dodatnih stroškov poslujejo med seboj (Nakamoto, 2008, str. 1). Do sedaj je transakcija potekala na tak način, da je oseba A preko svojega bančnega računa nakazala osebi B določen znesek za storitev, ki jo je prejela od osebe B. Banka je za svojo storitev zaračunala provizijo, ki se ji po konceptu kriptovalut lahko izognemo in tako omogočimo poslovnima strankama, da poslujeta direktno, brez visokih stroškov provizij.

2.1 Kriptografija in kriptovaluta

Bitcoin je prva svetovna decentralizirana digitalna kriptovaluta. Za razliko od večine obstoječih plačilnih sistemov se ne zanaša na institucije, kot sta vlada ali banka, ki posredujejo transakcije ali izdajajo valuto, temveč temelji na kriptografiji (Clark, 2013, str. 1). Dejansko gre za kriptovaluto, saj je kriptografija integrirana v sistem Bitcoina in zato Bitcoina kot valute ne moremo ločevati od kriptografije.

Kriptografija je znanstvena veda o tajnem, zakodiranem pisanju sporočil in njihovem prebiranju. Cilj je varovanje skrivnosti pred vdori zlonamernih in nepooblaščenih oseb preko zaščite celotnega kriptosistema. Trije najpomembnejši vidiki kriptografije, uporabljeni s strani Bitcoina, so enkripcija in dekripcija, razpršilni algoritem in digitalni

sistemski podpis. Dandanes so algoritmi enkripcije in dekripcije (šifriranje in dešifriranje sporočil) uporabljeni v vsakdanjem življenju. Na strežnikih zagotavljajo osebne in finančne informacije, pošiljajo zavarovane podatke preko interneta in nenazadnje zagotavljajo tudi varnost map na računalniku. Brez enkripcije in dekripcije algoritmov bi bil vsak ukraden podatek zlahka zlorabljen s strani tatov. Razpršilni algoritmi so pogosto uporabljeni za zagotavljanje celovitosti podatkov (Piasecki, 2012, str. 10-13).

Pri Bitcoinu ne obstaja podjetje ali organizacija, ki bi vodila ta sistem, ampak gre za mrežo računalnikov, ki se ji lahko pridruži vsakdo, in sicer tako, da namesti na svoj računalnik ustrezno programsko opremo. To je možno kjerkoli po svetu, tako da posamezni računalniki kolektivno podpirajo mrežo in vzdržujejo sistem. Bitcoin kot tak ni podjetje, saj nima centralnega strežnika in ne obstaja noben posameznik, ki bi bil odgovoren za omrežje ali dogodke, ki se v sistemu Bitcoina zgodijo (Plassaras, 2013, str. 2).

Za Bitcoinom namreč stoji matematično preverljiv sistem; vsakdo si lahko prebere izvorno kodo, po kateri sistem deluje, saj je koda prosto dostopna. Sistem ni lastniški in zato nobena oseba ne more napihniti trga z ustvarjanjem novih kovancev. Glede na to, da ustvarjanje bitcoinov sledi matematičnemu urniku, se že vnaprej pričakuje, da bo končno število kovancev doseženo do sredine naslednjega stoletja. Redkost bitcoinov zagotavlja, da vrednost ne bo oslabljena s politično odločitvijo, da se natisne več denarja, saj se sistema ne da spremeniti in nihče ne more odločiti, da bi izdal več kot 21 milijonov bitcoinov, kar je končno število bitcoinov (Brito & Castillo, 2013, str. 5-7). Bitcoin aplikacijo lahko vsak poganja na domačem računalniku in tako služi kot en člen v celotnem omrežju. Posamezni člen ima realno zelo majhen vpliv, vendar pa skupek vseh uporabnikov po celem svetu tvori izjemno močno in robustno verigo, ki postaja vse močnejša.

2.2 Delovanje Bitcoina

Bitcoin predstavlja nov koncept kriptovalute, ki se ne zanaša na katerokoli oblast ali institucijo in ni z njo na noben način povezan. Bitcoin je v svojem bistvu plačilni sistem, ki skozi matematično preverjen sistem v obliki kriptografije povsem sam upravlja, izdaja, vodi in preverja bitcoine oz. posamezne enote Bitcoin valute.

Prihod interneta je spremenil mnoge interakcije, ki so veljale vrsto let, zato ni čudno, da je temeljito vplival tudi na področje trgovanja. Do sedaj so elektronska plačila potrebovala varnega vmesnega posrednika, kot je npr. Paypal, da potrdi namen in avtentičnost transakcij. Bitcoin je revolucionaren zato, ker razrešuje problem dvojne porabe brez posrednika, kar je predstavljalo največji problem pri uporabi virtualnih plačil, saj je ravno tu v veliki meri prihajalo do zlorab (Peng, 2013, str. 4-5). Problem dvojne porabe v praksi pomeni: če imamo datoteko na našem računalniku in jo pošljemo nekomu drugemu, ta ista datoteka še vedno ostane na našem računalniku in jo lahko nato še enkrat pošljemo naprej drugim naslovnikom z novimi naslovi. Tak način plačevanja je zatorej slab, saj prejemnik nima zagotovila, da je dejansko edini prejemnik plačila.

Problem je torej v tem, da prejemnik plačila ne more verificirati, da eden od lastnikov morda ni dvojno porabil kovancev. Potrebujemo način, ki bo prejemniku nedvoumno zagotavljal, da pošiljatelj ni že prej poslal svojih bitcoinov, tj. da ni podpisal ene od že obstoječih transakcij. Pri Bitcoinu je sistem tak, da je prejšnja transakcija tista, ki šteje, kar pomeni, da nas ne skrbi glede kasnejših poskusov dvojne porabe iste transakcije. Edini način potrditve transakcije je ta, da vemo za vse transakcije. Rešitev bi lahko bila v vpeljavi centralne avtoritete, vredne zaupanja, ali v kovnici, ki bi pri vsaki transakciji preverjala dvojno porabo. Po vsaki transakciji bi kovanec moral biti vrnjen v kovnico, da bi le-ta izdala nov kovanec, in samo kovanci, ki bi bili direktno izdani iz kovnice, bi bili vredni zaupanja, da niso bili porabljeni dvojno. Pri modelu s kovnico bi kovnica morala imeti pregled nad vsemi transakcijami in bi odločila, katera transakcija je prišla prej. Da to dosežemo brez zaupanja vrednega posrednika, morajo biti vse transakcije javno objavljene in potrebujemo sistem, kjer se sodelujoči strinjajo o isti zgodovini, po kateri si transakcije kronološko sledijo (Nakamoto, 2008, str. 2). Zato je Bitcoinov decentralizirani mehanizem brez posrednika tako učinkovit. Za razrešitev morebitnih sporov v sistemu skrbi protokol, ki zagotavlja preverljivost vseh podatkov, ki so javno dostopni vsakomur. Problem pri zgoraj opisani rešitvi s kovnico je ta, da bi bila usoda celotnega monetarnega sistema zopet odvisna od podjetja, ki vodi kovnico, ker bi morala vsaka transakcija iti preko nje tako kot preko banke. Gre torej za neke vrste posrednika, ki bi preverjal in nadzoroval transakcije in s tem nadomestil manjkajoče zaupanje med strankama. To prinese tudi določene stroške, katere želimo zmanjšati ali pa se jim v celoti izogniti.

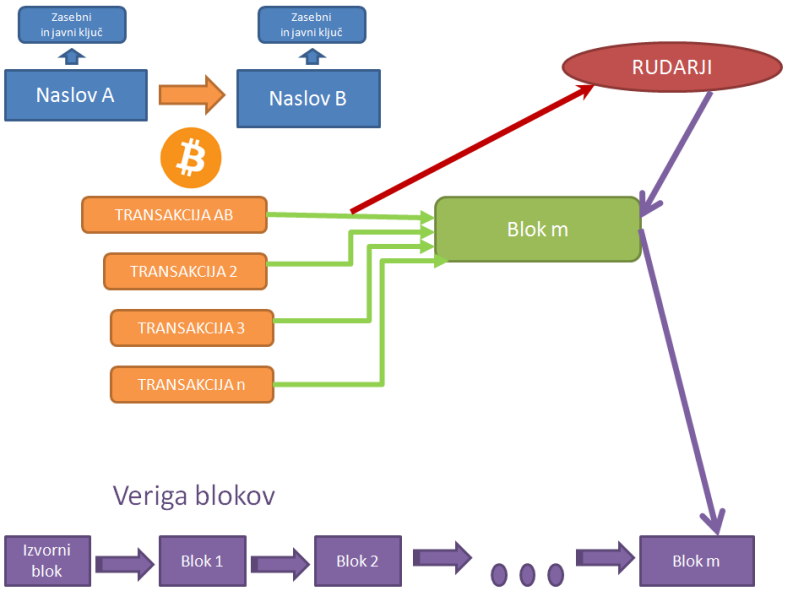
Sterry (2012, str. 8) pravi, da je o Bitcoinu potrebno vedeti tri stvari, in sicer da:

- bitcoini pripadajo naslovom,
- se premikajo iz enega na drug naslov in
- ena oseba lahko ima več naslovov.

Vsak naslov ima svoj zasebni in javni ključ, ki ju potrebuje za prenos bitcoinov iz enega na drug naslov. Ko naslov A (pošiljatelj) pošlje določeno število bitcoinov naslovu B (prejemniku), se opravi transakcija, ki je digitalno podpisana z zasebnim ključem pošiljatelja. Več različnih transakcij se potem v vrstniškem omrežju Bitcoina skozi proces rudarjenja združi v nov blok. Osnovni del Bitcoin sistema je veriga blokov, sestavljena iz skupka transakcij, ki so povezane v enoto, ki se imenuje blok in te enote blokov skupaj tvorijo verigo. Vsak novo ustvarjen blok se doda že ustvarjenemu bloku v verigi, kjer osnovo celotne verige predstavlja izvorni blok oz. prvo nastali blok (Bradbury, 2013, str. 5-6). Rudarjenje je operacija ustvarjanja novih blokov, ki jo opravljajo rudarji. Rudarji rešujejo zahteven kriptografski problem in ko najdejo rešitev, se oblikuje nov blok, ki je nato dodan obstoječi verigi blokov in se shrani v t.i. javno knjigo vseh transakcij, ki beleži vse opravljene transakcije v Bitcoinovi mreži. S tem je transakcija potrjena in nespremenljiva, rudar pa si s tem prisluži nagrado v obliki novo ustvarjenih bitcoinov, ki v letu 2015 znaša 25 bitcoinov. Poleg tega rudarju pripadajo vse pristojbine opravljenih

transakcij v novoustvarjenem bloku (Gup, 2014, str. 55-56). Zgoraj opisan proces poteka transakcij v Bitcoin mreži je prikazan na sliki 1.

Slika 1: Delovanje Bitcoina



Transakcija je enostaven proces premikanja bitcoinov med različnimi Bitcoin naslovi. Gre za podobno stvar kot pri bančnem prenosu. Bitcoini so določeni z naslovom, kot je številka bančnega računa, ki je ključna za prejemanje plačil. V primerjavi s številko kreditne kartice se Bitcoinov naslov uporablja na drugačen način. Pri transakciji s kreditno kartico stranka priskrbi informacijo, ko plača, saj prodajalec vzame številko naše kartice, ko potegne kartico skozi terminal. Pri Bitcoinu pa je postopek obraten, saj prodajalec poda svojo informacijo in nam pokaže svoj naslov, ko pride čas za plačilo.

Za sodelovanje v vrstniškem omrežju potrebujemo odprtokodni računalniški program, ki vsakemu uporabniku dodeli svoj naslov. Vse transakcije so digitalno podpisane in decentralizirano shranjene v omrežju, kar preprečuje ponarejanje in ponovno uporabo kovancev. Sistem Bitcoin nima banke ali kakršnegakoli nadzornega organa, ki bi nadzoroval količino kovancev v obtoku, kajti kovanci nastajajo z reševanjem časovno zahtevnega, a predvidljivega matematičnega problema. Slednje preprečuje ponarejanje in ponovno uporabo kovancev, to pa pomeni, da rešuje največji problem digitalnih plačil - dvojno porabo (Nakamoto, 2008, str. 1-2).

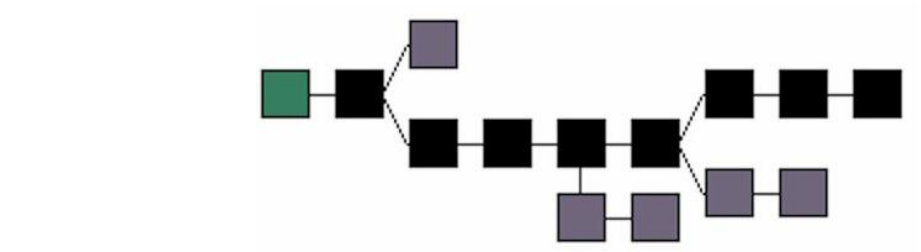
Bitcoin ima v sebi vgrajeno matematično uganko, katero je možno rešiti samo s pravilnim zaporedjem znakov. Rudarjenje poenostavljeno pomeni računalnik, ki je preko interneta konstantno povezan z Bitcoin omrežjem in ki ves čas poskuša rešiti problem z iskanjem pravilnega zaporedja znakov, dokler ne reši uganke. Ti računalniki, ki konstantno ugibajo iskana zaporedja, hkrati delajo še to, kar je bistveno za Bitcoin omrežje - preverjajo in potrjujejo transakcije in gradijo prej omenjeni seznam ter ga zavarujejo, da ostane tak kot je in ga zato ni mogoče samovoljno spreminjati. Rudarji to delajo predvsem zaradi

nagrade, vendar pa ob tem hkrati vzdržujejo tudi omrežje in mu dajejo varnost (Antonopoulos, 2014, str. 3). Torej, tudi če izpade elektrika na celotnem kontinentu, bo omrežje živelo naprej, saj je sistem razporejen po celem svetu in je skoraj nemogoče onemogočiti celotno omrežje.

Bitcoinov protokol vključuje vgrajene algoritme, ki regulirajo funkcijo rudarjenja skozi celotno mrežo. Zahtevnost problema, ki ga morajo rudarji rešiti, je dinamično prilagojena, tako da nekdo najde pravilno rešitev v povprečju vsakih deset minut, ne glede na to, koliko rudarjev dela na problemu v danem trenutku. Protokol rudarjem razpolovi nagrado na približno vsaka 4 leta (Grinberg, 2011, str. 163).

Prejemnik plačila potrebuje dokaz, da se je v času vsake transakcije večina rudarjev strinjala, da je bila ta transakcija izvršena. Da se to zgodi, tj. da so transakcije sprejete in dodane v blok, pa skrbi vsak rudar v Bitcoinovi mreži, ki sledi malemu številu enostavnih matematičnih pravil. Mreža rudarjev je bistveni del sistema, ki ga sestavljajo posamezniki, ki skozi potrjevanje transakcij ustvarjajo nove bloke, hkrati pa pomagajo mreži Bitcoina, da funkcionira in se krepi (Segendorf, 2014, str. 74-75). Interakcija med rudarji vodi v pojav posebnega obnašanja, kjer se ne dvomi o zaupanju v vsakega posamičnega rudarja, saj različni rudarji z medsebojno interakcijo skupaj tvorijo mrežo zaupanja.

Slika 2: Veriga blokov v vrstniškem omrežju Bitcoin



Vir: Clark, C., Bitcoin Internals, 2013, str. 32.

Legenda: Zeleni kvadrat - izvorni blok
Črni kvadrat - veljavni blok
Sivi kvadrat - osiroteli blok

Na zgornji sliki imamo prikazanih več konfliktnih transakcij v decentraliziranem sistemu, ki so označeni s sivo barvo. Vsi klienti preverjajo veljavnost transakcij, a to ni dovolj, saj občasno hkrati pride do nastanka večih blokov, ki se razrešijo tako, da se upošteva največja vložena količina dela, ki je bila vložena v posamezni blok, kar je v bistvu *Proof of Work (*v nadaljevanju PoW*).* PoW je posrednik protokola, preko katerega lahko nekdo dokaže, da je bil v proces pridobivanja bitcoinov vložen velik računalniški napor za odkrivanje zahtevane rešitve. Tako se v primeru neodločenih situacij veriga nadaljuje tam, kjer je bilo opravljenega več dela in vključenih transakcij. Na sliki številka 2 lahko vidimo primer verige, kjer je potrjena blokovna veriga označena s črnimi kvadratki, medtem ko so osiroteli bloki, torej bloki, ki se ne nadaljujejo, označeni s sivo barvo. Zanimivo je, da je ves ta proces decentraliziran in ne obstaja neka centralna avtoriteta, ki bi vplivala na ta

proces, saj gre namreč za izključno matematični proces. Bitcoinov protokol določa, da je pravilna zgodovina transakcij potrjena s strani daljše verige blokov v mreži, tj. verige z največ vložene računalniške moči. Uporabniki zmeraj delajo na tem, da podaljšajo vejo s trenutno najdaljšo verigo blokov, ki ima korenine iz izvornega bloka, torej prvonastalega bloka v verigi, na sliki označenega z zeleno barvo. Druge, krajše veje in neveljavni bloki pa so s strani mreže ignorirani (Clark, 2013, str 31-32).

Veriga blokov je mehanizem, ki preprečuje dvojno porabo, saj je ekvivalent javni knjigi vseh preteklih transakcij, ki je distribuirana vsem uporabnikom vrstniškega omrežja Bitcoina. Vsaka nova transakcija se preveri glede na že obstoječo verigo blokov, s tem se zagotovi, da prej porabljeni kovanci ne morejo biti porabljeni še enkrat. Enkrat ko je transakcija potrjena, se doda k obstoječi verigi blokov potrjenih transakcij. Vrstniško omrežje deluje kot neke vrste posrednik in zagotavlja, da ne prihaja do dvojne porabe in s tem posledično tudi do zlorab (De Feis & Patterson, 2014, str. 1).

Bitcoin je veriga digitalnih podpisov, ki kaže pot kovancev skozi Bitcoinov ekosistem. Vsak blok, ki je na sliki 2 narisan kot kvadrat, vsebuje informacije o prejšnjih transakcijah. Takoj ko je rudar sposoben ustvariti nov blok in ga pripne obstoječi verigi, to tudi naredi. Verigo je potrebno po tem še potrditi, o čemer pa odločajo vsi ostali člani vrstniškega omrežja, in sicer gre za preverjanje prejšnjih transakcij in PoW. Po potrditvi verige jo začno uporabljati nova vozlišča v mreži in na to verigo pripenjati nove bloke (Kroll, Davey & Felten, 2014, str. 4-5).

PoW rešuje problem določanja reprezentativnosti sprejemanja odločitve večine. Če bi večina uporabnikov odločala na osnovi IP (angl. *Internet Protocol*) naslova (en IP naslov je en glas), bi bila podvržena zlorabi, da bi se nek uporabnik lahko razporedil na več IP. PoW je v bistvu ena centralna procesna enota, ki ustreza enemu glasu. Večinska odločitev je predstavljena kot najdaljša veriga, ki ima vložen največji računalniški trud. Če je večina moči centralne procesne enote kontrolirana s strani poštenih vozlišč, bo poštena veriga rasla najhitreje in bo tako prehitela vse konkurenčne verige. Za spremembo prejšnjih blokov bi moral napadalec spremeniti PoW konkretnega bloka kot tudi vse bloke za njim, da bi ujel ter prehitel delo poštenih rudarjev, kar je zelo zahtevno, a ne povsem nemogoče (Nakamoto, 2008, str. 3).

Vsak blok ima vključenih več transakcij, ki se s pomočjo rudarja ali rudarjev vključijo v verigo blokov. Transakcija je digitalno podpisana izjava s strani enega uporabnika drugemu, ko uporabnik A želi poslati bitcoine s svojega naslova na naslov uporabnika B (Kroll, Davey & Felten, 2014, str. 5-6). Pri tem je potrebno opozoriti, da uporabniki delujejo pod psevdonimi in ne uporabljajo pravih imen, se pravi, da potek javnih transakcij med uporabniki vidimo kot zaporedje številk.

Bitcoin je v osnovi digitalni zapis v javni knjigi, ki beleži lastništvo v Bitcoinovem sistemu. Javna knjiga beleži lastništvo z uporabo digitalnih naslovov, brez da bi razkrivala resnične identitete. Lastništvo je odvisno od tega, ali ima uporabnik v posesti poleg javnega ključa tudi zasebni digitalni ključ, ki daje lastniku ekskluzivno pravico, da pošlje

bitcoine na drug naslov. Lastnik lahko porabi bitcoine za nakup dobrin ali storitev od kogarkoli, ki jih je pripravljen sprejeti (Böhme, Christin, Edelman, & Moore, 2015, str. 215-216). Tehnologija konceptov javnih in privatnih ključev je že znana, saj je uporabljena predvsem pri poslovanju s spletnimi bankami, kjer svojo identiteto dokažemo skozi certifikat, preden smemo vstopiti v sistem in opraviti želene transakcije. Bitcoin je ta koncept nadgradil tako, da je omrežje decentraliziral, kar pomeni, da namesto centralne avtoritete, kot je recimo banka, za ta sistem skrbi javna veriga blokov, za katero skrbijo vsi računalniki v mreži.

Sistem Bitcoina ni centraliziran, zato tudi ni nadzora nad tem valutnim trgom, saj deluje v okolju, kjer ni bank in centralne lokacije za upravljanje s tem navideznim denarjem. Vendar to ne pomeni, da so bitcoini lahko ustvarjeni brez vloženega dela, saj imajo fiksno ponudbo denarja in so zavarovani skozi kriptografske algoritme. Bitcoine lahko smatramo kot digitalno verzijo zlata. Možno jih je zamenjati za blago, storitve in tradicionalne valute. Glede na svoje značilnosti, bitcoini ponujajo veliko nižje stroške transferjev med uporabniki kot tradicionalni elektronski transferji, hkrati pa nudijo uporabnikom visoko stopnjo anonimnosti (Salmon, 2013, str. 1).

Gotovina je nepreklicna, saj ko nekomu izročiš denar, ga sam ne poseduješ več. Ko je enkrat prišlo do prenosa, nihče več ne more jamčiti, da boš gotovino dobil nazaj. Transakcije z Bitcoinom so prav tako nepreklicne kot transakcije z denarjem. Tisti trenutek, ko so bitcoini poslani na drug naslov, je plačilo nemogoče ustaviti (Sterry, 2012, str. 25). Bitcoin onemogoča, da bi prišlo do dvojne porabe: ko pošljemo Bitcoine na drug naslov, le-ti zapustijo našo posest in niso več naši. To je predstavljalo velik izziv za digitalno valuto, saj pred Bitcoinom to še ni bilo izvedljivo. Po uspešno poslani datoteki drugemu uporabniku je ta datoteka še vedno ostala na našem računalniku in je obstajala možnost, da se to datoteko pošlje še enkrat. Bitcoinu pa je s pomočjo kriptografije in PoW uspelo razrešiti problem dvojne porabe in nepreklicnosti.

V primerjavi s tradicionalnimi valutami so bitcoini popolnoma virtualni. Uporabniki lahko z bitcoini počno vse, kar lahko počno tudi s tradicionalnimi valutami, se pravi bodisi kupujejo bodisi prodajajo dobrine ali pošiljajo denar drugim uporabnikom. Bitcoine je moč kupiti ali prodati, kot tudi zamenjati za drugo valuto na specializiranih borzah (Antonopoulos, 2014, str. 1).

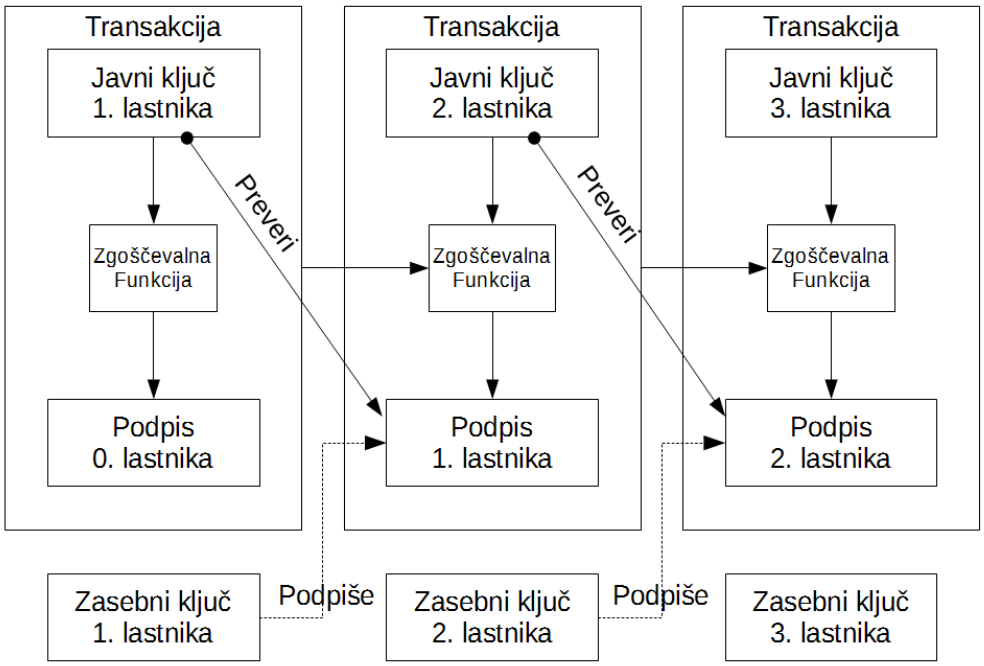
Bitcoini so ustvarjeni z reševanjem kriptografskih problemov, povezanih z ustvarjanjem blokov in zagotavljanjem PoW. Reševanje problema zahteva veliko računalniških virov in je zlahka preverljivo, kar zagotavlja, da so bloki ustvarjeni približno vsakih deset minut. Za nagrado ustvarjanja veljavnega bloka njegov ustvarjalec prejme nagrado v fiksnem znesku novih kovancev. Bitcoini imajo fiksno ponudbo kovancev in ne morejo biti ustvarjeni brez dela, zato se smatrajo kot digitalna verzija zlata. Lahko se jih zamenja za dobrine, storitve in tradicionalne valute, le da bitcoini ponujajo veliko nižje stroške pošiljanja denarja med ljudmi kot tradicionalni elektronski transferji, hkrati pa nudijo uporabnikom visoko stopnjo anonimnosti (Piasecki, 2012, str. 9).

Prenos bitcoinov poteka tako, da kupec doda naslov trgovca, pri katerem želi nekaj kupiti, nato pa transakcijo podpiše s svojim zasebnim ključem. Zaradi uporabe asimetričnih šifrirnih ključev se podpisa kupca ne da ponarediti in se po končanem zgoraj opisanem postopku spremeni lastništvo bitcoinov. Bitcoini nato potujejo po omrežju, kjer njihova vozlišča preverjajo šifrirane podpise, kar se na koncu zaključi s potrditvijo transakcije (Štok, 2012, str. 32).

Ko izvedemo transakcijo v Bitcoin omrežju, se odločimo, kolikšen del bomo namenili za transakcijske stroške. Vrednost, ki jo določimo sami, bo pripadla rudarju, ki bo rešil naslednji blok. Ta rudar bo dobil nagrado 25 bitcoinov (toliko trenutno znaša nagrada), poleg tega pa bo pobral še transakcijske stroške, ki so mu jih namenili uporabniki v svojih transakcijah. Če transakciji ne bomo namenili nikakršne pristojbine, obstaja možnost, da bodo rudarji našo transakcijo nekaj časa ignorirali, ker bodo v svoj blok raje vključili transakcije, ki vsebujejo neko pristojbino (Kroll, Davey & Felten, 2014, str. 12-13). Ko bo poteklo nekaj časa in bo transakcij malo, bodo rudarji vzeli tudi našo transakcijo, ki je brez pristojbine ne bi in jo vključili v blok ter jo s tem potrdili. Posledično to pomeni, da nižji kot je transakcijski strošek, ki ga določimo, dlje bo transakcija potrebovala, da se potrdi.

Transakcija je zapis v Bitcoin omrežju, kjer pošiljatelj iz svojega naslova pošlje določeno število bitcoinov drugemu uporabniku na njegov naslov. To stori tako, da s pomočjo svojega digitalnega ključa podpiše zgoščevalno funkcijo (angl. *Hash*) in s tem preda lastništvo svojih bitcoinov novemu naslovu. Vsak Bitcoin naslov vsebuje javni in zasebni ključ, s pomočjo katerih uporabnik opravlja transakcije, pri čemer zasebni ključ predstavlja lastnika določenega naslova, kjer ima vsak naslov točno en zasebni ključ. Zgoščevalna funkcija je matematični postopek, ki s pomočjo posebnega algoritma šifrira izvirno sporočilo. Z združevanjem večih transakcij nastane blok, ki je javno objavljen v javni knjigi, s tem pa se tudi potrdi prenos bitcoinov iz enega na drug naslov (Blundell-Wignall, 2014, str. 8). Bitcoini so definirani kot veriga digitalno podpisanih transakcij, kjer vsak lastnik bitcoine prenese naslednjemu lastniku tako, da s svojim zasebnim ključem digitalno podpiše javni ključ naslednjega lastnika. Na spodnji sliki lahko vidimo, kako poteka opisana transakcija v Bitcoinovi mreži.

Slika 3: Potek transakcij v Bitcoinu



Vir: Nakamoto, S., Bitcoin: A Peer-to-peer Electronic Cash System, 2008, str. 2.

Rešitev se v povprečju najde vsakih deset minut s strani nekoga, ki je sposoben potrditi transakcije preteklih desetih minut in je zato nagrajen z novimi bitcoini. Ustvarjanje bitcoinov je v bistvu globalno tekmovanje, ki ga lahko primerjamo z izdajanjem denarja s strani centralnih bank. Razlika med tema sistemoma je ta, da pri slednjem o izdajanju denarja odločajo zgolj centralne banke, medtem kot pri ustvarjanju bitcoinov sodelujejo vsi udeleženci mreže. Zanimivo pri sistemu Bitcoina je, če omrežje zazna, da se bitcoini prehitro ustvarjajo, to pomeni, da je težavnost problema premajhna. Sistem sam od sebe to zazna in dvigne težavnost matematičnih problemov toliko, da se rešljivost približa predvidenemu času desetih minut (Barber, Boyen, Shi & Uzun, 2012, str. 4-5).

Enkrat ko je porabljena procesorska moč za reševanje posameznega bloka, ta blok ne more več biti modificiran brez spreminjanja PoW vseh prejšnjih blokov. To občutno zmanjšuje verjetnost dvojne porabe, saj bi morali za ta konkretni blok spremeniti vse prej potrjene transakcije v verigi blokov in vse bloke, ki so bili potrjeni za njim. Da bi to naredili uspešno in hkrati prehiteli stekajoče se transakcije vseh poštenih uporabnikov v mreži, je zelo malo verjetno, kajti za ponarejanje bloka bi potrebovali več procesne moči kot celotna mreža Bitcoina skupaj. Prvi uporabnik, ki reši problem, pripne nov blok k obstoječi verigi blokov in si hkrati za nagrado prisluži novo pridobljene bitcoine. To je edini način, kako se lahko pridobijo novi bitcoini in se dodajo v monetarno bazo Bitcoina. Nove transakcije so hkrati posredovane vsem uporabnikom in grupirane v obliki novega bloka (Gervais, Karame, Capkun & Capkun, 2014, str. 1).

Transakcijska nagrada in možnost pridobivanja novih bitcoinov je primarna spodbuda za rudarje, da prispevajo procesno moč in vzdržujejo avtentičnost mreže Bitcoina. Nagrada se razpolovi vsakih 210.000 blokov transakcij, dokler ne postane praktično nemogoče izkopati nove bitcoine (Antonopoulos, 2014, str. 177-178). Rudarjenje oziroma pridobivanje Bitcoinov lahko primerjamo s pridobivanjem zlata. Na začetku je bilo zlata na voljo več, zato so bile izkopane količine večje. S tem ko se je vse več ljudi odločalo za izkopavanje zlata, je bilo potem izkopanega zlata v relativnem smislu vse manj. Na začetku je bila torej nagrada relativno večja kot skozi čas, ko je postalo zlato relativno redkejša dobrina. S tem ko ga je bilo težje izkopati, je nagrada hkrati postajala vse manjša.

Podoben proces poteka tudi pri bitcoinih. Na začetku je bila potrebna relativno majhna računalniška moč, da se je razrešil matematični problem, s katerim si je rudar pridobil nagrado v vrednosti 50 bitcoinov, danes pa je potrebno za rudarjenje bitcoinov vložiti ogromno računalniške moči. Iz začetnih 50 bitcoinov se je nagrada po približno 4 letih razpolovila na 25 bitcoinov in tako se bo nadaljevalo tudi v prihodnje. V naslednjem ciklu se bo nagrada zopet znižala, takrat bo nagrada znašala 12,5 bitcoinov. Po matematičnem izračunu je vsota razpolovitev končno število, kar posledično pomeni, da obstaja tudi končno število bitcoinov, ki znaša 21 milijonov bitcoin kovancev (Rice, 2013, str. 1).

Ko je Satoshi Nakamoto ustvaril platformo Bitcoina, je določil maksimalno število bitcoinov na osnovi zgornjega izračuna. Zadnji satoshi, ki je najmanjša enota Bitcoina, naj bi bil pridobljen leta 2140. Po tem bo sistem kot spodbudo rudarjem lahko ponudil le transakcijske stroške v obliki pristojbin. Enkrat ko bo pridobljen zadnji satoshi, pa rudarji ne bodo več nagrajeni skozi novo pridobljene bitcoine. Nagrajeni bodo le skozi pristojbine, ki jih bodo uporabniki ponudili za potrditev svojih transakcij. Ko se bodo nagrade znižale, bodo pristojbine postale pomembne, saj bo tisti, ki bo poskušal potrditi blok, za vključitev transakcije v blok prejel nagrado v obliki pristojbin. Tisti, ki bodo ponudili višje pristojbine, bodo imeli več možnosti za potrditev svoje transakcije (Antonopoulos, 2014, str. 178).

Sčasoma postaja reševanje problema vse težje in nagrada vse manjša, posledično pa se bo povečal tudi vpliv transakcijskih stroškov, ki bodo dodatna motivacija za rudarje, da bodo nadaljevali s svojim delom kljub majhni nagradi (Brito & Castillo, 2013, str. 6-7). To ne pomeni, da se bodo stroški transakcij čez čas povečevali. Če bi se Bitcoin uveljavil kot substitut tradicionalnega denarja, bi število transakcij v desetih minutah postalo bistveno višje, kajti že v tem trenutku se v vsak blok združi nekje od dvajset do tisoč transakcij, potem bi bilo le-teh še mnogo več. S tem bi imeli več majhnih pristojbin na transakcijo in bi se tako tudi rudarjem povečala nagrada in motivacija, da rudarijo še naprej.

Zaenkrat so pristojbine nepomembne, ko pa bo potekalo veliko transakcij in bo obstajalo malo rudarjev, ki bodo želeli potrjevati transakcije, bo višina pristojbin sila pomembna. Takrat bodo uporabniki, ki bodo želeli uporabljati Bitcoin sistem, morali paziti na višino pristojbin, da bodo le-te spodbujale rudarje, da bodo še naprej ohranjali sistem (Kroll, Davey & Felten, 2014, str. 13).

V sistem Bitcoina so tako vključene tudi ekonomske spodbude. Transakcijske pristojbine in možnost pridobivanja novih bitcoinov spodbuja rudarje, da svojo računalniško moč ponudijo Bitcoin sistemu. Glede na to, da skupnost Bitcoina raste in problemi postajajo vse težji, se bo produkcijsko razmerje med vloženo računalniško močjo in pridobljenimi bitcoini skozi čas zniževalo (Barber, Boyen, Shi & Uzun, 2012, str. 2-3).

V Bitcoinovi ekonomiji se globalno ravnotežje doseže, ko je skupna rudarska nagrada v dolarjih na sekundo enaka globalnim stroškom rudarjenja. Dokler to razmerje še ni doseženo in je nagrada višja kot stroški, bodo uporabniki nadaljevali z rudarjenjem bitcoinov in Bitcoinov sistem bo ostal stabilen. Konsenz protokola Bitcoin mora sprejeti vsak, ki vstopi v sistem. To pomeni, da morajo rudarji nadaljevati najdaljšo verigo blokov. V splošnem Bitcoin protokol ni samo-izvršilen, saj se zanaša na pripravljenost uporabnikov, da sprejemajo pravila sistema in ekonomske nagrade, ki so vključene v ta sistem (Kroll, Davey & Felten, 2014, str. 7-9).

2.3 Kronologija pomembnejših dogodkov

Satoshi Nakamoto (2008, str. 1) v svojem izvlečku razloži koncept in temelje Bitcoina, zaradi katerih ima ta kriptovaluta tak potencial. Dandanes se trgovanje preko interneta zanaša predvsem na storitve zaupanja vrednih posrednikov za procesiranje elektronskih plačil, kot je recimo PayPal. Centraliziran sistem, kot je PayPal, načeloma deluje dovolj dobro, kljub temu pa je slabost tega modela ta, da temelji na zaupanju. To pomeni, da so v transakcije vključeni posredniki, ki morajo zagotavljati večjo stopnjo zaupanja. S tem ko hranijo podatke o vseh članih transakcij, res nudijo uporabnikom večjo stopnjo varnosti, vendar pa to hkrati poveča transakcijske stroške in zato omeji ekonomičnost manjših zneskov.

Bitcoin ima sicer kratko zgodovino, vendar se je od leta 2008 do danes zgodilo veliko mejnikov, ki so pomembno vplivali na dosedanji potek razvoja te virtualne valute. V nadaljevanju so navedeni najpomembnejši dogodki od začetka Bitcoina do danes (History of Bitcoin, 2015):

2008

- 18. avgusta 2008 je bila registrirana spletna stran z naslovom Bitcoin.org.
- 31. oktobra 2008 je bil objavljen dokument s strani posameznika ali skupine pod psevdonimom Satoshi Nakamoto, ki predstavi koncept Bitcoina.

2009

- 3. januarja 2009 je bil ustvarjen izvorni blok (angl. *Genesis Block*) Bitcoina, ki je začetni blok, na katerega se pripenjajo novi bloki najdaljši verigi blokov.
- Kmalu za tem objavijo Bitcoin programsko opremo verzija 0.1, ki vključuje sistem, po katerem bo maksimalno število ustvarjenih bitcoinov 21 milijonov.

- 12. januarja 2009 je prišlo do prve Bitcoin transakcije, ki je bila opravljena med Satoshi Nakamotom in Hal Finneyjem, kriptografskim aktivistom.
- 5. oktobra 2009 je prišlo do prvega menjalnega tečaja t.i. *New Liberty Standard*, ki je postavil vrednost bitcoinov na 1 USD = 1.309,03 BTC. Razmerje je bilo osnovano na ceni elektrike, ki je bila potrebna za delovanje računalnika, da ustvari bitcoine.

2010

- 6. februarja 2010 je bila ustanovljena prva Bitcoin borza.
- 17. julija 2010 se ustanovi borza MtGox, ki sčasoma postane najpomembnejša svetovna borza za trgovanje z bitcoini.
- 6. novembra 2010 tržna vrednost Bitcoina preseže 1 milijon ameriških dolarjev. Vrednost na MtGoxu je dosegla 0,50 USD/BTC.

2011

- Leta 2011 začne poslovati Silk Road, ki postane največja spletna trgovina za droge in druge nelegalne storitve.
- 28. januarja 2011 je bilo ustvarjenih 25% vseh možnih bitcoinov, kar znaša 5,25 milijonov bitcoinov.
- 9. februarja 2011 je Bitcoin na MtGoxu prvič dosegel valutno pariteto 1 USD/BTC.
- 23. marca 2011 je Bitcoin prvič dosegel pariteto z evrom.

2012

- 15. novembra 2012 je spletno podjetje Wordpress začelo sprejemati bitcoine kot način plačila, kar pomeni, da so Bitcoin kot način plačila začela sprejemati podjetja.
- 28. novembra 2012 se je zgodil razpolovitveni dan (angl. *Halving Day*) - s tem dnem se je nagrada za blok razpolovila. Iz takratnih 50 bitcoinov na blok je po novem nagrada za novoustvarjeni blok znašala 25 bitcoinov.

2013

- 18. marca 2013 je FinCEN (angl. *Financial Crimes Enforcement Network, United States Department of the Treasury*) definirala svojo pozicijo do virtualnih valut.
- 28. marca 2013 je tržna kapitalizacija Bitcoina dosegla 1 milijardo USD.
- 2. oktobra 2013 je FBI (angl. *Federal Bureau of Investigation*) zaprl Silk Road, razvpito tržnico z nezakonitimi dobrinami in storitvami, ter zasegel bitcoine v vrednosti 3,6 milijonov USD.
- 14. oktobra 2013 je največji kitajski spletni iskalnik Baidu začel kot prvi iskalnik sprejemati bitcoine.
- 19. novembra 2013 je vrednost bitcoina presegla 1000 USD.

2014

- 28. februarja 2014 je največja Bitcoin borza MtGox bankrotirala, pri čemer je prišlo do izgube 744.408 bitcoinov v protivrednosti 436 milijonov USD.
- 11. aprila 2014 je kitajska banka (angl. *People Bank of China*) uradno sporočila, da Kitajska ne bo prepovedala Bitcoina.
- 18. julija 2014 je računalniško podjetje Dell objavilo, da bo začelo sprejemati bitcoine.
- 23. septembra 2014 Paypal objavi partnerstvo z Bitcoinom.
- 11. decembra podjetje Microsoft doda možnost plačevanja z bitcoini za Xbox igre in telefonske vsebine.

Danes, dne 19.6.2015, znaša vrednost bitcoina 246,95 USD. Trenutno je v obtoku v skupni vrednosti 14,29 milijonov USD bitcoinov, celotna tržna kapitalizacija pa znaša 3,52 milijard USD (Blockchain, 2015).

2.4 Razširjenost Bitcoina

Klasične valute so razširjene po celotnem svetu, saj ima vsaka država svojo valuto ali pa valuto monetarne unije. Te valute so navadno omejene na meje držav, čeprav določene države, ki imajo eno uradno valuto, sprejemajo tudi druge valute. Menjavo med valutami nadzorujejo banke z javno objavljenimi valutnimi tečaji, ki se spreminjajo glede na ekonomske razmere, na katere je valuta vezana. Bitcoin je v tem pogledu geografsko bolj razširjen oziroma globalen, saj ni podvržen nikakršni centralni agenciji, ki bi ga regulirala. Zato je njegova vrednost enaka po celem svetu, vrednost v primerjavi z ostalimi valutami pa se računa izključno glede na povpraševanje in ponudbo bitcoinov.

Hitrejši razvoj in težnja po zmanjševanju stroškov silita denar, da se transformira v vse bolj optimalno obliko za uporabnike. Tako kot je že Ribnikar (1999, str. 13) ugotovil, smo bili priča transformaciji denarja iz blagovne oblike, preko kovanega denarja do papirnatega denarja. Čez čas je prišlo do popolne dematerializacije denarja, kar smo videli ob prihodu knjižnega denarja. Vendar proces dematerializacije še ni zaključen, saj se tudi to področje razvija in še naprej spreminja.

Danes smo priča mnogim inovacijam in naglemu razvoju različnih oblik denarja (Samuelson & Nordhaus, 2002, str. 467). Razvoj denarja poteka v smeri bolj učinkovite oblike, ki bo olajšala transkacije med uporabniki, bodisi skozi zmanjšanje stroškov uporabe bodisi skozi hitrejše in lažje potrjevanje transakcij. Evolucija denarja tako poteka v smeri bolj optimalne denarne oblike.

V primerjavi s tradicionalnimi valutami je trenutno število uporabnikov Bitcoina relativno nizko, saj je valuta še mlada. Število ljudi, ki so zainteresirani za Bitcoin, bodisi skozi uporabo ali trgovanje, pa se vendarle povečuje. Zaradi svoje anonimne narave točno število Bitcoin uporabnikov ni znano.

2.5 Regulacija Bitcoina

Uporabniki in investitorji Bitcoina so bili v sistem privabljeni zaradi potenciala, ki jim ga le-ta ponuja kot valuta. Po drugi strani pa Bitcoin kot digitalni plačilni sistem ponuja nove možnosti tudi na področju bančništva in trgovanja. Zaradi decentralizirane narave in neodvisnosti od centralnih oblasti so oblasti in regulatorji upravičeno zaskrbljeni nad stopnjo tveganja, ki ga predstavlja ta kriptovaluta. Za večjo veljavo v družbi bi moral Bitcoin postati bolj stabilen, širše sprejet in se redno uporabljati tudi v gospodarstvu ter bi predvsem moral pridobiti več zaupanja tako držav, gospodarstev kot tudi posameznikov (Deloitte, 2014, str. 5). Kombinacija vse večje sprejetosti Bitcoina v širšo javnost in njegov potencial za kriminalno zlorabo je spodbodel pomembnejše svetovne agencije, da bolj podrobno preučijo, kako opredeliti in posledično tudi regulirati Bitcoin.

Najodmevnejši dogodek s področja uporabe bitcoinov je bilo poslovanje spletne strani Silk Road, ki je bila t.i. eBay za droge, s to razliko, da je stran Silk Road večinoma ponujala nezakonite dobrine. Šlo je za spletno tržnico, kjer so uporabniki prodajali in kupovali različne vrste prepovedanih drog, orožje, ponarejene dokumente, idr. Silk Road se je skrivala na t.i. temnem internetu, ki deluje preko Tor orodja, zato oblastem več let ni uspelo najti lokacije strežnika. Trgovci in kupci so za plačila uporabljali izključno bitcoine, kar je policiji še dodatno otežilo delo (Dorit & Shamir, 2013, str. 1-3). Prav ta dogodek je spodbudil pozornost večjih regulatornih organov, da so aktivneje pristopili k preučevanju Bitcoina in konkretneje opredelili svoja stališča do te in tudi drugih kriptovalut.

Uporabniki Silk Roada so dostopali do strani s pomočjo Tor mreže, ki skrije IP naslov uporabnika in s tem omogoči anonimnost identitete. Uporabniki so lahko na ta način kupovali prepovedana mamila, ponarejene dokumente in druge nelegalne storitve, kot je recimo naročanje umorov, ne da bi jih bilo moč izslediti. Edino plačilno sredstvo na spletni strani Silk Road je bil bitcoin. V času delovanja je stran Silk Road ustvarila več kot 9,5 milijonov bitcoinov dohodkov in zaslužila 600.000 bitcoinov skozi provizije (De Feis & Patterson, 2014, str. 1-2). Stran je uspešno delovala več kot 2 leti, potem pa je ameriški preiskovalni urad FBI 1. oktobra 2013 aretiral Rossa Ulbrichta, glavnega človeka, ki je vodil Silk Road. V času, ko je bila kazenska ovadba izdana, je to znašalo 1,2 milijarde USD v dohodkih in 80 milijonov USD v provizijah. Med februarjem 2011 in julijem 2013 je imela stran Silk Road 957.079 uporabnikov po celem svetu (Peng, 2013, str. 27).

Vzrok za hitro sprejemanje Bitcoina na svetovni ravni gre iskati v njegovih dobrih tehničnih lastnostih: v učinkoviti rešitvi dvojne porabe preko PoW, nepreklicnosti transakcij, sposobnosti poenostavitve transakcij preko meja z minimalnimi transakcijskimi stroški s skoraj takojšnjo potrditvijo, idr. (Peng, 2013, str. 32). Nenadni porast uporabe sistema Bitcoin v letu 2012 so sprožili Evropejci, in sicer prebivalci tistih držav, ki jih je finančna kriza najbolj prizadela, na primer v Španiji in na Cipru. Varčevalci teh držav so se zaradi nastalih razmer bali za svoje prihranke in so zato z zamenjavo evrov v bitcoine želeli svoje prihranke kar se da najbolje zavarovati. Varčevalci na ta način sporočajo, da svoj denar raje prenesejo v sistem Bitcoin, kot da bi ga zaupali bankam z dolgoletnimi

tradicijami. Enako velja tudi glede državnih trezorjev in to kljub temu, da so se v sistemu Bitcoin v preteklosti že zgodili številni napadi hekerjev. Navedena ugotovitev kaže na to, da ljudje v bančni sektor vse manj zaupajo (Plassaras, 2013, str. 13).

Zaradi vse večje razširjenosti Bitcoina in atraktivne rasti vrednosti se je od njegovega nastanka zgodilo več kraj bitcoinov, največja pa je vplivala celo na bankrot največje svetovne menjalnice Bitcoina. 28. februarja 2014 je največja Bitcoin menjalnica Mt. Gox sporočila, da je zaradi pomanjkljivosti v sistemu poleg 100.000 svojih bitcoinov izgubila še vseh 750.000 bitcoinov od uporabnikov. Takratna vrednost 1 bitcoina je znašala 565 USD, kar pomeni, da je šlo za izgubo v protivrednosti 480 milijonov USD, kar je predstavljalo 7% vseh bitcoinov v obtoku (Takemoto & Knight, 2014). Sam sistem Bitcoina je varen, medtem ko ima okolje, v katerem deluje, polno pasti. Prav zato je za varovanje bitcoinov pred izgubo ali krajo odgovoren vsak lastnik sam. Tudi v zgornjem primeru se je izkazalo, da so težave nastale zaradi neprimerne varnosti sistema Mt. Goxa in ne zaradi pomanjkljivosti v zasnovi sistema Bitcoin. Zaradi tovrstnih primerov se postavlja vprašanje, ali bi bilo moč tovrstne kraje zmanjšati, če bi bilo poslovanje z bitcoini regulirano.

Zaradi transakcij, ki so opravljene pod psevdonimi, ima zakonodaja večje težave pri zaznavanju nezakonitih aktivnosti in ugotavljanju resničnih identitet uporabnikov. Prva, ki je sprožila formalne smernice za regulacijo Bitcoina, je bila ameriška agencija FinCEN. Regulativne smernice so obravnavale virtualne valutne menjalnice enako kot zahteve proti pranju denarja za tradicionalne denarne pošiljatelje, kot je recimo mednarodna mreža za pošiljanje denarja po vsem svetu Western Union (Peng, 2013, str. 33). Decentraliziran sistem Bitcoina bi deloval najbolje takrat, ko bi bila stopnja regulacije čim manjša. V primeru pretiranih posegov institucij v sistem, v smislu obdavčevanja ali omejevanja uporabe bitcoinov, bi se to odražalo na celotnem trgu in zato Bitcoin ne bi mogel delovati optimalno. Po drugi strani pa je potrebno opredeliti standarde glede poročanja o poslovanju s to valuto in spopadanja s problematiko pranja denarja.

Po FinCEN-u so se opredelitve do Bitcoina lotile tudi ostale večje svetovne finančne institucije. Ameriški davčni urad IRS (angl. *Internal Revenue Service*) še vedno ni prilagodil svojih davčnih regulativ za virtualne valute. Virtualne valute imajo veliko karakteristik, ki so zaželene v okolju davčnih oaz in ta možnost izogibanja davkom zagotovo doda davčnemu uradu večjo motivacijo, da bi reguliral kriptovalute. Na osnovi obstoječih pravil IRS opredeljuje, da posamezniki s prodajanjem dobrin ali zagotavljanjem storitev preko plačil z bitcoini ustvarijo dohodek in ga zato morajo prijaviti (IRS, 2015). To v osnovi pomeni, da vlada ZDA obravnava Bitcoin kot lastnino in ne kot valuto, kar pomeni, da obdavčuje bitcoine na enak način kot delnice. Zakonodaja na področju Bitcoina še ni povsem natančno definirana, kljub temu pa se s tem, ko vse več institucij definira svoj odnos do virtualnih valut, stanje vse bolj kristalizira.

Ameriški preiskovalni urad FBI je sredi leta 2013 razčlenil možnosti uporabe bitcoinov in njegove posledice. Najpomembnejša ugotovitev te organizacije je, da Bitcoin predstavlja

še enega izmed medijev za izvedbo transakcij, kar pomeni, da se bo skupina za pregon kriminalitete znotraj FBI ukvarjala tudi s tem, kako se lahko bitcoine uporablja za nezakonite aktivnosti, kot je pranje denarja, nakup otroške pornografije, hazardiranje, trgovino z ljudmi, saj želi zavarovati uporabnike pred zlorabami. FBI pri uporabi Bitcoina skrbi predvsem potencialna možnost financiranja terorističnih organizacij in podobnih kriminalnih organizacij preko bitcoinov (Federal Bureau of Investigation, 2012, str. 5-10).

V drugi polovici leta 2013 je svoje poročilo o Bitcoinu javnosti posredovala tudi Evropska centralna banka (v nadaljevanju ECB), v katerem so prvič ocenili potencial virtualnih valut na ekonomijo in posledice, ki jih le-te lahko povzročijo. Primarna skrb ECB je varovanje nizke inflacije v evro območju, zato so se pri svojem poročilu osredotočili predvsem na možnost motenj v gospodarstvu, ki bi jih Bitcoin in druge virtualne valute utegnile prinesti. Ugotovili so, da je s trenutnim tečajem in celotnim denarnim agregatom, vpliv Bitcoina na ekonomijo zanemarljiv. V Evropski uniji trenutno ni mogoče ugotoviti pravnega statusa Bitcoina. Po direktivi 2009/110/EC ga je sicer moč uvrstiti med elektronski denar, čeprav ne izpolnjuje vseh pogojev za uvrstitev v to kategorijo (European Central Bank, 2012, str. 16-19).

V veliki večini držav sveta status Bitcoina še ni definiran, v nadaljevanju je razložena spodnja slika, ki nazorno prikazuje področja regulacije Bitcoina v letu 2015.

Slika 4: Regulacija Bitcoina

Vir: Merkletree, 2015.

Legenda: Zeleno območje - dovoljen
Rumeno območje - pogojno dovoljen
Rdeče območje - prepovedan
Modro območje - nedefiniran status

Sodeč po viru Merkletree, uporaba Bitcoina v tem trenutku ni prepovedana in je posledično dovoljena v državah, ki so na sliki 4 označene z zeleno barvo. Državni regulatorji imajo v teh državah podobno stališče glede sprejemanja Bitcoina, vendar seveda obstajajo razlike od države do države. Medtem ko v nekaterih državah še nimajo dovolj podrobno opredeljenih regulativ, da bi pravno opredelili Bitcoin, imajo v drugih državah takšne zakone, ki trenutno eksplicitno ne prepovedujejo Bitcoina in s tem posledično dopuščajo svojim državljanom, da ga uporabljajo. Seveda obstajajo tudi države, ki imajo pozitivno stališče do Bitcoina in je tam uporaba le-tega povsem legalna in njihovim uporabnikom ni potrebno trepetati pred regulatorji. V zgoraj označenih državah z zeleno barvo zaenkrat težav glede uporabe Bitcoina torej ni, vsaj s stališča uradne oblasti ne.

Po drugi strani imamo kar nekaj držav, kjer je uporaba Bitcoina pogojno dovoljena ali celo prepovedana. Stroga prepoved uporabe Bitcoina velja na Islandiji in na Tajskem, kjer centralni banki prepovedujeta kakršnokoli uporabo bitcoinov, tako sprejemanje kot pošiljanje bitcoinov. Status v državah, kjer pogojno dopuščajo uporabo, pa je dokaj zapleten, saj v osnovi to pomeni, da je uporaba Bitcoina prepovedana, status pa še ni povsem opredeljen. Med takšne države spadajo: Kitajska, Indija in Rusija (The Law Library of Congress, 2014, str. 1-24). Bitcoin skupnost je glede regulacije in reguliranja te virtualne decentralizirane valute razdeljena. Eni menijo, da bo regulacija na dolgi rok koristna za Bitcoin, saj bo pripomogla k večji legitimnosti in sprejetosti valute, drugi pa menijo, da bo uničila potencial nadaljnjih tehnoloških inovacij in postavila uporabnike v neugoden položaj.

Še nedavno davčna zakonodaja Slovenije ni vsebovala posebnih določb, ki bi urejale davčno ureditev poslovanja z virtualnimi valutami, v letu 2013 pa je Ministrstvo za finance opredelilo, da se Bitcoin kot virtualna valuta ne šteje za denarno sredstvo v smislu 7. točke 4. člena Zakona o plačilnih storitvah in sistemih (Ur.l. RS, št. 58/09, 34/10, 9/11 in 32/12). Prav tako se Bitcoin ne šteje za finančni instrument, to pomeni, da je davčna obravnava dohodka, doseženega pri takem poslovanju ali v taki obliki, odvisna od okoliščin posameznega primera. Tako je potrebno ugotoviti, kdo dosega določen dohodek in za kakšno vrsto dohodka v posameznem primeru gre. Zakonodaja različno obravnava dohodek iz kreiranja bitcoinov, iz kupovanja in prodajanja bitcoinov ter različno opredeljuje dohodek v primeru fizične osebe ali fizične osebe v okviru opravljanja dejavnosti (Ur.l. RS, št. 58/09, 34/10, 9/11 in 32/12).

3 PREDNOSTI IN SLABOSTI BITCOINA

Do sedaj je naša analiza ekonomske stabilnosti Bitcoina slonela na družbenem konsenzu, ki je dajal Bitcoinu vrednost. Mogoče je vredno premisliti, da notranja vrednost Bitcoina pravzaprav izvira iz kriptografije, kajti Bitcoin ni samo oblika denarja, ampak tudi sistem digitalnih plačil, ki sloni na matematičnih pravilih. Navsezadnje je Bitcoin tehnološka inovacija, ki ima mnoge uporabne lastnosti in zagotavlja platformo za nadaljnje finančne inovacije in bi lahko spremenila tudi družbeno dojemanje finančnih transakcij. Ti vidiki

dajejo Bitcoinu v prihodnosti možnost, da prekorači klasični okvir pridobivanja in ohranjanja vrednosti denarja ter spremeni tudi področje plačevanja.

Za boljše razumevanje, zakaj bi ljudje želeli uporabljati bitcoine, bi pomagalo, če o Bitcoinu ne bi razmišljali le kot o substitutu tradicionalnih valut, temveč kot o novem sistemu plačevanja. Sčasoma, ko bo vse več ljudi uporabljalo Bitcoin, se bo percepcija javnosti do Bitcoina spremenila iz nišne novotarije v legitimno valuto ali lastnino. Ko bo Bitcoin dosegel točko stabilnosti, se bodo mrežni učinki in koristi Bitcoina medsebojno okrepili. Do takrat pa bo Bitcoinovo gospodarstvo še nezrelo in v nevarnosti zaradi doživljanja šokov, ki lahko vodijo v škodljivo izgubo zaupanja. Kam se bo v prihodnosti prevesil razvoj Bitcoina, ne vemo, lahko pa preučimo prednosti in slabosti, ki pokažejo potencialne možnosti razvoja v prihodnosti.

3.1 Prednosti

Prednost Bitcoina v primerjavi s kreditnimi karticami je ta, da so transakcije pri plačevanju z Bitcoinom nepreklicne, enkrat ko so potrjene in dodane k verigi blokov. To ščiti prodajalce pred krajami, kar je pogost problem pri uporabi kreditnih kartic. Pri uporabi kreditnih kartic so nekateri kupci zlorabljali sistem, ker so izrabili možnost vračila denarja, kljub temu da ni bilo s prejetim izdelkom ali storitvijo nič narobe (Vagstad & Valstad, 2014, str. 12). Prav nepreklicnost transakcij daje Bitcoinu pozitivno lastnost varnosti in praktičnosti, saj izniči ranljivost trgovcev v razmerju do kupcev, ki imajo goljufive namene in so v preteklosti uporabljali kreditne kartice za povrnitev denarja. Trgovec prejme plačilo neposredno od kupca in mu zato ni potrebno uporabiti nobene zunanje storitve ali posrednika. Prav tako trgovcu ni potrebno skrbeti, da bi posrednik zavrnil plačilo, zadržal denar ali odrekel storitev.

Bitcoin je varen način plačevanja preko spleta, saj nima nobene baze ali uporabniških računov. V decentraliziranem vrstniškem omrežju nihče nima nadzora nad podatki uporabnikov in se jih zato tudi ne more zlorabiti (Štok, 2012, str. 32). Kljub varnemu sistemu pa je potrebno poudariti, da leži velika odgovornost glede zaščite predvsem v rokah uporabnikov, saj je pri uporabi bitcoinov potrebno biti pazljiv. Če poslujemo preko spletnih denarnic je potrebno biti previden, da nimamo računalnika okuženega z virusom ali s programi, ki nam lahko ukradejo vse potrebne informacije za zlorabo občutljivih podatkov. S tehničnega vidika je uporaba Bitcoina varna, kljub temu pa se moramo zavarovati, da pazljivo ravnamo z računalnikom, kjer imamo shranjene bitcoine.

Mnogi laični uporabniki verjamejo, da je Bitcoin popolnoma anonimni sistem. Kljub temu da ponuja številne načine prikrivanja identitete, Bitcoin vseeno razkriva veliko informacij, ki lahko vodijo do postopka pregona kaznivih dejanj in potencialno obdolžijo posameznika, če je le-ta povezan z določenim naslovom. Mnogim Bitcoin uporabnikom anonimnost veliko pomeni in zato lahko krizo zaupanja povzročijo že samo tehnične težave na mreži. Študije so pokazale, da je mogoče ugotoviti resnično identiteto za 40% vseh uporabnikov. Kljub temu pa Bitcoinov sistem nudi višjo mejo anonimnosti kot

katerokoli drugo plačilno sredstvo, ki poteka preko institucij ali posrednikov (Brito & Castillo, 2013, str. 7-9).

Kriptovalute rešujejo problem varnega prenosa lastništva brez posrednika. Potencial te tehnologije je zmanjšanje stroškov pri prenosu denarja. Poslovanje preko kreditnih kartic prinese strošek v višini 2-3%, pri spletnem trgovanju ta strošek znaša v povprečju 2,9%, medtem ko pri mednarodnem prenosu denarja tovrstni stroški znašajo kar 8,9% zneska transakcije. Bitcoin nudi daleč najnižje stroške pošiljanja denarja, saj za opravljeno transakcijo odštejemo le 1% poslanega zneska (Blundell-Wignall, 2014, str. 15). Nizke provizije pri transakcijah so tista prednost, ki nudi velik potencial za razvoj in razširitev Bitcoina, saj je prejemanje bitcoinov brezplačno, pošiljanje pa stane manj kot 1%. Glede na to, da Bitcoin pospešuje direktne transakcije brez vmesnega člena, s tem odstrani drage stroške, ki spremljajo transakcije kreditnih kartic. To je še posebej privlačno za ljudi, ki trgujejo preko državnih meja. Če pošiljamo denar v druge države, to prinese ogromne transakcijske stroške in tudi precejšnji časovni zamik, kadar uporabljamo storitve centraliziranih sistemov. V primeru Bitcoina smo že ugotovili, da so stroški nizki tako za velike kot za male zneske, hkrati pa je plačilo potrjeno v roku desetih minut, ne glede na to, kateri dan v tednu je in kje se nahajamo.

Danes v dobi virtualnih svetov vse pogosteje prihaja do plačevanja storitev v manjših zneskih, kjer gre za t.i. mikroplačila. Splošna definicija o mikroplačilih ne obstaja, šlo naj bi za zneske denarja, ki se pošiljajo digitalno in so premajhni, da bi se procesirali skozi kreditno kartico. Običajno gre pri mikroplačilih za transakcije, ki so nižje od 5€. Povpraševanje po mikroplačilih se je razmahnilo zaradi vse večje ponudbe novih vsebin s strani spletnih distributerjev: od audio vsebin, različnih vrst aplikacij do računalniških iger. Ocenjuje se, da je bil evropski trg mikroplačil leta 2011 vreden okoli 6 milijard evrov, in naj bi po projekcijah zrasel na več kot 15 milijard v letu 2015 (Value Partners, 2011, str. 8). Bitcoin bi lahko razpršil industrijo mikroplačil, ki predstavlja sektor znotraj širšega spletnega prostora, kateri je pred kratkim doživel eksponentno rast.

Kljub atraktivni rasti mikroplačil v spletnem prostoru še vedno ni podana prava rešitev za optimalno izrabo potenciala tovrstnih storitev. Optimalna rešitev plačevanja bi morala imeti nizke stroške, biti zelo hitro opravljena in nuditi uporabnikom dodano vrednost. Bitcoin ima potencial za zapolnitev te potrebe, saj nima vmesnika, kar pomeni, da je cenejši in hitrejši kot tradicionalne mreže plačil. Medtem ko plačila s kreditno kartico lahko trajajo nekaj dni, da se odobrijo, vsaka Bitcoin transakcija potrebuje za potrditev le okoli deset minut. Zagovorniki menijo, da bodo ravno nizki stroški transakcij bitcoinov nekega dne spremenili trg globalnih denarnih transferjev in nakazil (Brito & Castillo, 2013, str. 10-11).

Bitcoin bi lahko postal medij plačevanja za majhna podjetja, ki želijo priti do veliko nižjih transakcijskih stroškov. Majhna podjetja so že začela sprejemati bitcoine in se posledično začela izogibati stroškom poslovanja v primerjavi s podjetji, ki poslujejo s kreditnimi karticami. Bitcoin ponuja nižje transakcijske stroške podjetjem zato, ker vse več ljudi

sprejema valuto Bitcoina. Drugi uporabniki so sprejeli valuto zaradi hitrosti in učinkovitosti transakcij (Brito & Castillo, 2013, str. 10-11). Ena najbolj obetajočih uporab Bitcoina služi kot platforma za finančne inovacije, ki v današnjem svetu lahko nudijo nov nivo funkcionalnosti in razvoja plačevanja.

3.2 Slabosti

Kljub prednostim, ki jih Bitcoin prinaša, ima sam sistem tudi nekaj potencialnih slabosti in pomankljivosti, ki pretijo uporabnikom.

Slika 5: Gibanje vrednosti Bitcoina

Vir: Blockchain, 2015.

Iz zgornje slike lahko razberemo veliko volatilnost Bitcoina, saj se je skozi čas pokazalo precejšnje nihanje, ki je izraženo v USD. Največja nihanja so bila naslednja:

- 8. junija 2011 je vrednost Bitcoina znašala 31,91 USD, kar je pomenilo najvišjo točko do takrat, hkrati pa je tržna kapitalizacija znašala že okoli 206 milijonov USD. Nato se je vrednost v naslednjih 3 dneh prepolovila na 14,65 USD, kar je postalo znano kot veliki balonček 2011. Z vse večjim omenjanjem v medijih je Bitcoin postal zanimiv tudi za kriminalne združbe, ki so vse bolj napadale uporabnike in njihove spletne denarnice, še pogosteje pa menjalnice, kot je bila MtGox, ki je bila v tistem času največja in najpomembnejša menjalnica Bitcoina. Tako je vrednost bitcoinov zaradi številnih prevar vse bolj padala. V primeru MtGoxa so varnostne luknje v sistemu povzročile zaprtje menjalnice in izgubo vseh bitcoinov, ki jih je imela. Kmalu za tem je MtGox bankrotirala. Posledično so določena podjetja in organizacije prenehali sprejemati bitcoine, saj je v naslednjih mesecih prišlo do kraje bitcoinov še na tretji največji svetovni menjalnici Bitomat, ki je izgubila kar 17.000 bitcoinov. Kasneje so

vdrli še v menjalnico Bitcoinica, kjer so ukradli več kot 61.000 bitcoinov (Piasecki, 2012, str. 53).

- V aprilu 2013 je vrednost presegla 100 USD in 20. aprila dosegla novo najvišjo točko 266 USD, kar je pomenilo kar 2000 % rast v primerjavi z letom poprej. Temu je spet sledil velik padec, kar je bila posledica kraj večjih količin bitcoinov. Vrednost je nato padla pod 70 USD (History of Bitcoin, 2015).

- Zadnji izmed večjih balončkov se je zgodil v novembru 2013, ko je vrednost iz 200 USD naraščala, predvsem zaradi pozitivnih informacij, da je bitcoine začel sprejemati Baidu, največji kitajski spletni iskalnik, kateremu je sledila tudi veriga restavracij Subway in nekatera manjša podjetja, kar je dne, 17. novembra 2013 posledično pripeljalo do podvojitve vrednosti bitcoina na 503 USD (History of Bitcoin, 2015).

- Naslednji dan je ameriški senat obravnaval Bitcoin kot virtualno valuto z vidika potencialnih tveganj, groženj in potencialov. Posledica pozitivnih odzivov se je poznala že dan kasneje, 19. novembra 2013, ko je vrednost 1 bitcoina preskočila tisočico in je znašala kar 1.242 USD. V tistem trenutku je Bitcoin z vidika velikosti transakcij prehitel ameriškega ponudnika finančnih in komunikacijskih storitev Western Union ter postal z 245 milijoni USD 8. največji tovrstni ponudnik. To je posledično spodbudilo nov pozitivni val sprejemanja te valute, kajti v naslednjih dneh so bitcoine začeli sprejemati še mnogi drugi: npr. ciprska univerza, ki je kot prva omogočila plačevanje šolnin preko bitcoinov, podjetje za potovanje v vesolje Virgin Galactic in spletna trgovina Shopify (History of Bitcoin, 2015).

Če bo ekonomija Bitcoina zopet rasla, se bo valuta Bitcoina počasi stabilizirala in bodo imeli cenovni šoki manjši vpliv. Volatilnost je produkt slabih trgov, medtem ko bi bolj masovna uporaba bitcoinov doprinesla k večji likvidnosti trga. 90% uporabnikov Bitcoina je investitorjev, saj ima kar 97% naslovov manj kot 10 opravljenih transakcij, zato je Bitcoin trenutno bolj špekulativna investicija kot pa medij izmenjave. Dokler Bitcoin ne dozori in doseže uravnotežene ekonomije, bo ostal občutljiv na špekulativne balončke (Peng, 2013, str. 20-21). Iz grafa se da razbrati, da Bitcoin še ni dosegel faze zrelosti. Glede na gibanje vrednosti lahko razberemo, da je bila tržna vrednost Bitcoina precenjena, saj ni odražala realnega stanja na trgu. Vrednost je 29. novembra 2014 dosegla najvišjo točko, ko je 1 bitcoin znašal 1.242 USD, medtem ko je na začetku leta znašal nekaj več kot 10 USD. Trg se bo sam uravnaval toliko časa, dokler ne bo dosegel optimalne vrednosti. Najpomembnejši element, ki podpira trenutno vrednost, je ravno upanje investitorjev, da bo ta zopet zrasla.

Te cenovne uravnave so podobne tradicionalnim špekulativnim mehurčkom, kjer posledica višje vrednosti bitcoinov ni število transakcij trgovcev ali uporabnikov Bitcoina, temveč na trg vplivajo špekulativni investitorji, ki kopičijo bitcoine in tako vplivajo na trg. Težava pri kopičenju bitcoinov je ta, da je ponudba bitcoinov omejena in bi torej večje povpraševanje

vodilo v povišano ceno bitcoinov, kar bi pripeljalo do deflacije oz padca cen dobrin in storitev v bitcoinih (Elwell, Murphy & Seitzinger, 2015, str. 6-7). Velika nihanja ne napovedujejo nujno konca Bitcoina, saj gre lahko le za testiranje sistema. Če bi bili bitcoini uporabljeni le za ohranjanje vrednosti, potem bi lahko ta volatilnost ogrozila prihodnost Bitcoin valute, vendar pa to ni edina uporaba Bitcoina. Če se trg obnaša divje in nepredvidljivo, potem v takem okolju ni optimalno opravljati poslovnih financ ali varčevati v bitcoinih.

Bitcoin pa se lahko uporablja tudi kot medij izmenjave, kjer njegova volatilnost predstavlja manjši problem. Trgovci lahko ocenijo vrednost blaga v tradicionalni valuti in sprejmejo temu primerno število bitcoinov (Blundell-Wignall, 2014, str. 9-10). Strankam, ki kupijo bitcoine za izvršitev enkratnega nakupa, je vseeno, kakšen bo menjalni tečaj jutri, temveč jim je pomembno le to, da Bitcoin zniža transakcijske stroške v sedanjosti. Verjetno je, da bo vrednost Bitcoina postala manj volatilna, ko ga bo začelo uporabljati vse več ljudi, kajti večja seznanjenost z Bitcoinom in njegovo tehnologijo bo pripomogla k vzpostavitvi bolj realnih pričakovanj glede vrednosti Bitcoina v prihodnosti.

Velika potencialna slabost je tudi deflacionirana spirala, saj je ponudba bitcoinov fiksna. S širitvijo Bitcoinove ekonomije bo edini možni način ekonomske rasti skozi apreciacijo vrednosti valute. Glede na to, da bo ponudba bitcoinov fiksna, povpraševanje pa se bo povečevalo, to pomeni, da bo valuta pridobivala na vrednosti. Dobrine, ki so izražene v bitcoinih, pa bodo stale manj, kar bo posledično vodilo v deflacijo. Tradicionalne ekonomije se zanašajo na centralno banko, da skozi uravnavanje obrestnih mer in kontroliranega tiskanja denarja izvaja monetarno politiko za dosego cilja nizke stabilne stopnje inflacije. Ti vzvodi niso mogoči v sistemu Bitcoina, saj centralna avtoriteta, ki bi bdela nad gospodarstvom Bitcoina, ne obstaja. Prav tako tudi niso možni klasični vzvodi uravnavanja preko obrestne mere in obsega denarja (Peng, 2013, str. 22).

Z hitrejšim naraščanjem ponudbe ostalih fiat valut v primerjavi s ponudbo bitcoinov bodo bitcoini skozi čas v vrednosti apreciirali. To bi lahko vodilo v deflacionarno spiralo, ko bi denominirane cene v bitcoinih dramatično padle. Proizvajalci bi se odzvali z znižanjem proizvodnje, kar bi vodilo v nižje plače, nižje povpraševanje in nižje cene. Apreciacija vrednosti bitcoinov bi spodbudila ljudi, da Bitcoin kovance hranijo in za isti denar raje kupijo več dobrin v prihodnosti (Antonopoulos, 2014, str. 180-181). Kot rezultat zmanjšanega obsega transakcij bi postalo tudi za rudarje ustvarjanje blokov in rudarjenje manj profitabilno, kar bi vodilo v zmanjšanje zaupanja v Bitcoinov sistem kot celoto. Tako bi posledice deflacionarne spirale ogrozile sam sistem Bitcoina zaradi nenadne izgube zaupanja in padca vrednosti Bitcoina (Peng, 2013, str. 22).

Sistemu predstavlja veliko nevarnost tudi t.i. 51% oz. Goldfinger napad, ko napadalec pridobi nadzor nad vsaj 51% mrežne računalniške moči in tako teoretično kontrolira sistem, na novo napiše pravila in zavrača transakcije, ki so ustvarjene s strani drugih uporabnikov. Goldfinger napad stremi k uničenju sistema Bitcoin, glavni namen takega dejanja pa bi koristil gospodarstvu izven Bitcoina (Piasecki, 2012, str. 41-42). Dve največji

združenji rudarjev AntPool in F2Pool skupaj kontrolirata približno tretjino mrežne računalniške moči. V juniju 2014 pa je v določenem 12-urnem obdobju več kot 50% rudarske moči nadzorovalo združenje rudarjev GHash, kar pomeni, da bi teoretično že lahko manipuliralo s transakcijami v sistemu (Böhme, Christin, Edelman, & Moore, 2015, str. 222). Za Bitcoin to predstavlja resno grožnjo in nevarnost - kljub temu da smo danes zaenkrat še daleč od te možnosti, se to v prihodnosti lahko zgodi. Če bi do tega prišlo, bi bilo pridobivanje bitcoinov vse dražje, poleg tega bi za pridobivanje novih bitcoinov in potrjevanje transakcij skrbele specializirane družbe. Po takem scenariju bi Bitcoin izgubil mnogo prednosti, ki jih kot decentralizirana virtualna valuta ima, saj v tem primeru ne bi več mogli govoriti o decentraliziranem sistemu.

Nepreklicnost transakcij Bitcoina smo že obravnavali kot prednost, to značilnost pa lahko obravnavamo tudi kot slabost. Značilnost, ki ščiti prodajalce pred zlorabami zahtevanih plačil, po drugi strani pušča uporabnike ranljive za prevare. Čeprav so bile v preteklosti žrtve zlorab različni uporabniki v Bitcoinovem ekosistemu, je vsem zlorabam skupno, da je uporabnik izkoristil prednost nepreklicnosti in pomanjkanje transparentnosti transakcij (Vagstad & Valstad, 2014, str. 12). Z večjo stopnjo širšega družbenega sprejemanja kriptovalut bi Bitcoin imel bolj pomembno vlogo in s tem pritegnil pozornost držav zaradi potrebe po regulaciji. Takrat bi bila pomanjkljivost zaščite potrošnikov zmanjšana, saj je v interesu držav, da za svoje državljane čimbolj poskrbijo in jih zaščitijo. Anonimnost predstavlja težavo tudi z vidika transparentnosti, saj je za katerikoli javni naslov Bitcoina možno preveriti, kakšno je njegovo stanje in videti vse transakcije, ki jih je ta naslov izvedel do sedaj. Kljub temu pa ne moremo vedeti, čigav je javni ključ, dokler določen posameznik ne potrdi, da gre za njegov javni ključ.

Čeprav je bil Bitcoin ustvarjen za reševanje pomanjkljivosti pri trenutno veljavnih plačilnih sredstvih, pa je nekatere prednosti Bitcoina moč uporabiti tudi za transakcije kaznivih dejanj. Zakonodaja ima zaradi anonimnih transakcij večje težave pri zaznavanju nezakonitih aktivnosti in ugotavljanju resničnih identitet uporabnikov. Bitcoin je res psevdoanonimen, vendar ne popolnoma anonimen. Vse transakcije so javno objavljene v javni knjigi, kajti mreža sama ne skriva IP naslovov, s katerih so bile transakcije opravljene (Vico & Arago, 2014, str. 35-36).

Po zaprtju spletne strani Silk Road je FBI 1. oktobra 2013 aretiral ustanovitelja in upravljalca zloglasne strani Ross William Ulbrichta. Na prenosnem računalniku obdolženca je FBI odkril 144.336 bitcoinov, ki so bili takrat vredni približno 28 milijonov USD in jih v 446 transakcijah prenesel na nov račun. (Dorit & Shamir, 2013, str. 5). To je dokaz, da je zasledovanje nezakonitih transakcij težje, ne pa nemogoče. Mediji radi izpostavljajo anonimnost Bitcoina kot zelo negativno značilnost, ker se Bitcoin lahko bolj enostavno uporablja za nezakonite posle. Vendar pa je anonimnost značilna tudi za današnji denar - gotovino. Vsaka valuta se lahko uporablja tako za legalne kot za nelegalne posle, torej to ni samo Bitcoinova specifična lastnost.

Bitcoin ima iz varnostnega vidika enake značilnosti kot gotovina. Če nekje pozabite kup bankovcev in jih nekdo vzame, jih verjetno nikoli več ne boste dobili nazaj. Enako je pri Bitcoinu, vendar s to razliko, da ste preko interneta kraji še dodatno izpostavljeni. Ko svoj zasebni ključ pustite na namizju in imate vaš računalnik okužen z virusom, vam bitcoine lahko ukradejo (Brito & Castillo, 2013, str. 7-8). To je tudi področje, ki predstavlja največji izziv za razvijalce varnostnih sistemov Bitcoin denarnic, saj mora biti sistem varen tudi za vsakdanje uporabnike, ki so pri upravljanju z računalniki manj vešči.

Bitcoin je kot nova digitalna valuta relativno nelikvidna, saj ga zaenkrat uporablja še razmeroma malo ljudi. Novi investitorji so zaradi medijske pozornosti in fenomena nagle rasti vrednosti te digitalne kriptovalute sledili potencialnim dobičkom in pričakovali rast vrednosti kriptovalut tudi v prihodnosti, kar je pripeljalo do vse širše sprejetosti Bitcoina. To vodi v vprašanje, kdo uporablja in sprejema bitcoine. Glede na to, da je Bitcoin psevdoanonimen in decentraliziran, je bila originalna baza uporabnikov majhna in zelo nišno usmerjena, uporabljali so ga predvsem kriptografski navdušenci, ki ne zaupajo vladam in centralnim bankam, ter monetarni idealisti in špekulativni investitorji (Coinmonk, 2013, str. 5). Z vse večjim razumevanjem Bitcoina in njegove uporabne vrednosti ga bo začelo sprejemati tudi vse več trgovcev, s tem pa se bo likvidnost valute povečevala. Bitcoin bi z večjo likvidnostjo pridobil stabilnost in večjo verodostojnost v očeh javnosti, kar bi zopet vodilo v večjo razširjenost uporabe Bitcoina.

4 BITCOIN DANES IN V PRIHODNOSTI

Priljubljenost virtualnih svetov je povzročila veliko povpraševanje po virtualnih dobrinah in valutah, kar se kaže v naraščajočih prihodkih podjetij, ki delujejo v okoljih, povezanih z virtualnimi dobrinami in storitvami. Bitcoin je bil ustvarjen kot alternativa bančnemu sistemu. Ideja, ki je botrovala nastanku te digitalne kriptovalute, je bila želja, da bi se ustvaril denar, katerega vrednost ne bi mogla biti zmanipulirana s strani centralne oblasti.

Tako kot vsaka valuta do zdaj tudi vrednost Bitcoina izvira iz zaupanja ljudi, da ima Bitcoin vrednost. Vendar to zaupanje za razliko od običajnih valut ne temelji na zaupanju v oblast ali v centralne banke, temveč sloni na matematiki. Bitcoinu dajejo vrednost matematični zakoni, saj je količina bitcoinov omejena, način njihovega nastajanja pa vnaprej predviden. Torej za razliko od današnjih valut, pri katerih centralne banke denar ustvarjajo brez kakih strogih omejitev, to pri Bitcoinu ni možno (Seaman, 2013, str. 13). Bitcoin ima kljub že predstavljenim omejitvam velik potencial, da bi ogrozil tradicionalne valute na določenih področjih, predvsem zaradi zanesljivega decentraliziranega sistema, hitrih transakcij in nižjih transakcijskih stroškov.

Ravno nerazumevanje osnovnih značilnosti Bitcoina regulatorjem povzroča težave pri odločanju o načinu regulacije Bitcoina. Glede na zadnje odločitve različnih državnih in finančnih institucij se zdi, da Bitcoina nimajo namena prepovedati, večinoma pa ga želijo regulirati. Pomembno pri regulaciji je predvsem to, da morebitne obdavčitve in omejitve ne

uničijo pozitivnih učinkov, ki jih Bitcoin prinaša, predvsem v smislu potenciala pri razvoju nišnih podjetij, ki so s pomočjo plačilnega sistema Bitcoin bolj konkurenčna, kot bi bila sicer. Regulacija bi sicer prinesla tudi strožji nadzor, kar pa ni nujno dobro. S pretirano obdavčitvijo Bitcoina bi se javnost zaradi nekonkurenčnosti usmerila k drugim plačilnim sistemom, kar bi lahko pripeljalo do konca Bitcoina. Tudi v tem primeru bi najbrž katera druga alternativna valuta zapolnila ta izpraznjen prostor.

Če bi se države odločile za večjo stopnjo regulacije, bi Bitcoin lahko postal bolj centraliziran. Tudi tak hibridni sistem bi še vedno predstavljal veliko bolj decentraliziran sistem v primerjavi s trenutnim finančnim sistemom. Problem prevelike obdavčitve uporabnikov Bitcoina bi se lahko pokazal v obliki dvojne obdavčitve: npr. v primeru podjetij, ki bitcoine proizvajajo in jih hkrati tudi uporabljajo pri svojem poslovanju. Glede na to, da so države trenutno monopolisti na področju monetarne politike, kar se tiče izdajanja denarja in nadzora nad njim, ne gre pričakovati, da bi se bile pripravljene temu odreči. Prav zato gre v prihodnosti pričakovati, da bodo tako države kot večje finančne institucije natančno opredelile status Bitcoina in drugih kriptovalut ter ga želele v določeni meri tudi nadzorovati ali regulirati.

Decentralizacija ščiti sistem Bitcoina pred vladno intervencijo, saj so ravno posredniki pogosto tisti, na katere vlada lahko pritiska. Pri vprašanju omejitve in regulacije kriptografije je prisoten povsem legitimen pomislek, da bi tehnologija lahko bila izkoriščena s strani kriminalnih skupin ali posameznikov, kljub temu pa uporabnost, praktičnost in potenciali, ki jih ponuja tehnologija digitalnih plačil, pretehtajo ta tveganja. Medtem ko so skrbi glede zlorabe tehnologije Bitcoina upravičene, je prav tako potrebno razumeti, da se Bitcoin uporablja predvsem kot valuta in kot globalni plačilni sistem, tako na področju spletnega poslovanja, pošiljanja denarja, kot tudi na področju finančne pomoči ljudem tretjega sveta. Prav zato bi bilo nepravično obsoditi valuto in njegove uporabnike zaradi neprimerne uporabe s strani kriminalnih manjšin. Podobno so bili v zgodnjih dneh interneta mnogi zaskrbljeni zaradi njegovih nezakonitih uporab. Problem kriminalitete pri Bitcoinu bi se lahko rešil tako, da se Bitcoin v določeni meri zakonsko regulira, saj bi se s tem definirale tudi pravne meje nadzora in bi se tako zaščitilo uporabnike.

Vse več držav se zaveda, da bi s pretiranim omejevanjem uničili tudi pozitivne učinke Bitcoina, ki jih je veliko več, kot je nevarnosti. Zato menim in pričakujem, da se bo v prihodnosti veliko naredilo na področju varnosti uporabnikov, kar bo omogočilo lažjo uporabo in zaščito pri uporabi te kriptovalute.

V prihodnosti bo Bitcoin verjetno vplival predvsem na področje pošiljanja denarja. Najbolj verjetno bo šlo za primere, ko bodo posamezniki npr. pošiljali denar svojim družinam in sorodnikom iz bolj razvitih v manj razvite države. V trenutnih transakcijah jih tovrstna transakcija stane do 9,05% zneska, ki ga pošljejo, medtem ko je z Bitcoinom celotno transakcijo mogoče opraviti le za desetino dosedanjih stroškov. Govorimo o celotnem procesu transakcije - od spreminjanja denarja iz tuje valute v bitcoine, nato pošiljanje bitcoinov iz enega na drug naslov ter nazadnje spreminjanje bitcoinov v lokalno valuto.

Celoten strošek tovrstne transakcije bi skupaj znašal manj kot 0,0005 bitcoina oz 1% celotnega prenesenega zneska (Brito & Castillo, 2013, str. 13-14).

Če vzamemo za primer pošiljanje 1.000 USD enega uporabnika drugemu preko Paypala, Western Uniona, običajne banke ali Bitcoina jasno vidimo, katera možnost pošiljanja je najbolj ugodna. Če bi poslali 1.000 USD preko Paypala, bi nas tovrstna transakcija stala 25 USD. Prek Western Uniona so stroški pošiljanja denarja različni glede na višino zneska - pri uspešno poslanih 1.000 USD bi prejemnik prejel le okoli 950 USD. Bančni transferji so ponavadi še dražji od zgoraj omenjenih opcij in bi za tovrstno transakcijo odšteli najmanj 60 USD. Pri pošiljanju preko Bitcoina bi za uspešno poslanih 1.000 USD naslovnik prejel kar 999,75 USD, kar pomeni, da je slednja transakcija daleč najbolj ugodna (Forrester & Solomon, 2013, str. 23). Glede na drastično razliko v stroškovnem vidiku je moč pričakovati, da bo Bitcoin v prihodnosti predstavljal resnega konkurenta tistim podjetjem, ki opravljajo tovrstne transakcije že danes. Večja sprejetost Bitcoina v naši družbi bo posledično vodila k zmanjšanju stroškov, saj se bodo današnji ponudniki plačilnih storitev morali prilagoditi trgu, če bodo želeli ohraniti svoj tržni delež.

Kreditne kartice niso narejene za internetno obdobje, saj so stroški proizvodnje same fizične kartice kot tudi stroški procesiranja transakcij z njo previsoki. Bitcoin ni sistem, ki bi izboljšal plačilne kartice, kot je Visa ali Mastercard, temveč je sistem, ki deluje na drugačen način in bi lahko spremenil dojemanje in proces plačil na globalni ravni. Tako bi lahko posameznik iz Slovenije poslal plačilo v bitcoinih v protivrednosti nekaj evrov drugemu posamezniku, transakcija bi bila opravljena v trenutku, potrditev pa bi sledila v roku desetih minut. Vse skupaj bi bilo veliko hitreje kot tudi ceneje, predvsem pa v dobi spletnih plačil veliko enostavnejše.

Danes smo priča rojstvu nove industrije - od razvoja, izdajanja do upravljanja s privatnimi valutami. Prav ta aspekt resnično digitalnega denarja predstavlja monetarno svobodo: svobodo ustanoviti, širiti in trgovati z monetarnimi instrumenti. Internet danes nudi možnost izdajanja in širjenja nove svetovne valute z dostopno tehnologijo, če ne Bitcoina, pa v prihodnosti katere druge kriptovalute. Skupnost, ki podpira Bitcoin, ima vizijo demokratične svobode. Skupnost bo nadaljevala z inovacijami in izboljšavami na tehničnem področju Bitcoina, dokler ne bo ustvarjena boljša digitalna valuta. Glede na to, da je Bitcoin v razmeroma zgodnji fazi razvoja, saj obstaja šele 7 let, še ne moremo z gotovostjo trditi, v katero smer bo potekal njegov razvoj. Brito in Castillo (2013, str. 10) menita, da Bitcoin omogoča boljši dostop do kapitala in posledično lahko lajša globalno revščino, zaščiti posameznike pred nadzorom kapitala ter zagotovi finančno zasebnost za zatirane skupine. Na globalni ravni bi Bitcoin z nižjimi stroški transakcij lahko spremenil globalna denarna nakazila. Menim, da je prav tehnologija Bitcoina najbolj pomemben element sistema, ki bo doprinesel tudi k nadaljnjemu razvoju, saj gre namreč za koncept, ki praktično deluje in ima ogromen potencial za razvoj na mnogih področjih.

Današnje svetovne oblasti ne morejo več uničiti Bitcoina, lahko le onemogočijo njegovo uporabo skozi regulacijo. Glede Bitcoina je veliko nejasnosti glede zakonske klasifikacije

in primernosti za regulacijo. Če bi se Bitcoin začel uporabljati namesto denarja, kakršnega poznamo danes, bi bile posledice za naš družbeno politični sistem nepredstavljive. Teža moči bi se preselila iz centralnih bank in vlad na ljudstvo, kar bi najverjetneje prineslo veliko pozitivnih sprememb. Če primerjamo Bitcoin z razvojem interneta, lahko potegnemo veliko vzporednic. Zametki interneta so nudili veliko potenciala, vendar se internet zaradi uporabnikom neprijaznih programov in slabih internetnih povezav ni uspel takoj uveljaviti. Z razvojem praktičnih aplikacij in s pojavom hitrih internetnih povezav je internet uspel izkoristiti potencial, ki ga je imel, in je s svojo razširjenostjo vplival na razvoj globalnega gospodarstva. Podobno je tudi z Bitcoinom, kjer je trenutni protokol verjetno samo prva upodobitev Bitcoinove tehnologije, ki se bo z razvojem razširila tudi na druga področja.

Bitcoin kljub vsem predstavljenim pozitivnim vidikom verjetno ne predstavlja "superiorne" valute, je pa ena od zametkov kriptovalut, ki bodo vplivale na nov način dojemanja valut. Danes imamo veliko različnih valut, ki so vezane predvsem na geografsko področje delovanja: od evra, jena do ameriškega dolarja, v prihodnosti pa bomo verjetno imeli več kriptovalut, ki bodo namenjene za različno uporabo. Ena kriptovaluta bi lahko bila primernejša za večje nakupe, kot je recimo hiša, druga primernejša za nakup vrednostnih papirjev in tretja za osebno zavarovanje ljudi ipd. Valuta Bitcoin je samo prva aplikacija tehnologije Bitcoina, v prihodnosti pa bi lahko bili priča vpeljevanju tovrstne tehnologije na mnoga druga področja, kjer bi matematično podprta pravila zagotavljala varnost in verodostojnost najrazličnejših sistemov, kot so bančni, finančni ali upravni registri. Glede na to, da je decentralizirani sistem neodvisen, za njim torej ne stoji nikakršna organizacija, podjetje ali država, lahko rečemo, da gre za standard, ki si ga nihče ne lasti in nihče ne more vplivati nanj, kar bi tem sistemom dajalo tudi večjo veljavnost.

Še vedno ni jasno, kakšno obliko bo Bitcoin prevzel v prihodnosti. Lahko bi postal tarča mednarodnih zakonodaj, ki bi prepovedale njegovo uporabo, po drugi strani pa se odpira možnost, da bi postal svetovni standard menjave med valutami. Medtem ko je na začetku kazalo, da gre le za projekt zanesenjakov, se skozi čas vse bolj potrjuje, da ima Bitcoin močne temelje, na katerih je moč graditi tudi naprej. Terminologija Bitcoina je precej nejasna, zato je na tem področju potrebno storiti še veliko, da bo lahko vsak povprečen človek razumel in tudi uporabljal tehnologijo Bitcoina. Če primerjamo Bitcoin z internetom, je bilo 20 let nazaj podobno, kot je sedaj z Bitcoinom, saj si moral biti za uporabo interneta strokovnjak. Danes pa je razvitih že toliko orodij, ki lajšajo delo z internetom, da ga lahko uporablja praktično vsak. Tu je potencial, ki se ponuja predvsem skozi Bitcoin kot tehnologijo in nudi priložnost za mnoge, ki bodo z razvojem različnih aplikacij prišli do velikih poslovnih uspehov, hkrati pa bodo znatno pripomogli tudi k evoluciji celotnega sistema, kar bo dolgoročno koristilo vsem.

SKLEP

Kot smo lahko videli, je bil denar skozi zgodovino razumljen kot družbeni in kulturni pojav. Denar se je nenehno razvijal in lahko trdimo, da razvoj z dobo virtualnega sveta še ni zaključen. Trenutno se nahajamo na prelomni točki in lahko le ugibamo, kakšne oblike bo denar prevzel v prihodnosti. Popularnost virtualnih svetov je povzročila veliko povpraševanje po virtualnih dobrinah in valutah, kar pa zahteva tudi varno digitalno valuto in menjalnice, ki bodo olajšale menjavo med realnimi in virtualnimi valutami, kot tudi zaščitile uporabnike pred goljufijami. Če bo izpolnjena zahteva po učinkovitih ukrepih proti prevaram in goljufijam, bi Bitcoin lahko postal naslednji standard virtualnih valut.

Od samih zametkov v letu 2008 do danes Bitcoin postopoma v svetu pridobiva na veljavi. Medtem ko so bili prvi uporabniki predvsem tehnološki navdušenci in kriptografski strokovnjaki, je Bitcoin počasi postal širše sprejet v družbi. Za te ljudi je Bitcoin predstavljal dolgo pričakovan odgovor na njihove težave. Interes zgoraj navedenih skupin ljudi je bil motiviran preko odpora do vladnega nadzora, zato so bili toliko bolj zadovoljni nad potencialom, ki ga Bitcoin ponuja: je decentralizirana digitalna valuta, ki s pomočjo vrstniške mreže zagotavlja zasebnost in varnost spletnih transakcij.

Denar ima vrednost zato, ker ljudje priznavajo, da ima vrednost. Večina valut je namreč izdanih s strani centralne oblasti, ki nadzoruje tudi ponudbo denarja. Danes Bitcoin ponuja alternativo danim sistemom, tako da ponuja ljudem svobodo, nižje stroške in hitrejše procesiranje prenosa denarja. Valute, s katerimi rokujemo danes, so nam "vsiljene", saj smo jih v naših poslovnih odnosih prisiljeni uporabljati. Bitcoin pa nam ponuja možnost izbire nove neodvisne valute, s katero izražamo tudi svoj odnos do denarja in državnih oblasti. Tako se lahko odločimo za tisti denar, ki nam nudi boljše možnosti za uporabo in nižje transakcijske stroške, kar je vsekakor prednost Bitcoina.

Pravi digitalni denar združuje področji ekonomije in kriptografije. Bitcoin zagotovo uteleša to značilnost in poseduje mnoge bistvene elemente, ki so zaželjeni za idealno digitalno valuto - je varen, psevdoanonimen, prenosen in deljiv. Najbolj revolucionarni aspekt kriptovalute je zagotovo njegova decentralizirana narava, kjer so vse transakcije objavljene v javni knjigi. Bitcoin tehnologija skozi razpršeno mrežo uporabnikov dosega soglasje, ki ga je bilo do sedaj moč doseči le skozi centralizirani sistem. Najbolj edinstvena značilnost Bitcoina je uspešno razrešen problem dvojne porabe brez posrednika. Pri Bitcoinu gre torej za sistem, ki ne potrebuje nadzornika, saj je zasnovan na zbirki pravil, ki jih mora spoštovati vsak člen sistema, če želi delovati v tem sistemu.

Perspektiva, iz katere ocenjujemo sistem Bitcoina, je izjemno pomembna, kajti bitcoine lahko jemljemo bodisi kot naložbo, kot samostojno valuto, plačilno sredstvo ali pa zgolj kot tehnologijo. Bitcoin kot sistem ima tako svoje prednosti kot tudi slabosti. Največje prednosti Bitcoina so nepreklicnost transakcij, varen način plačevanja, psevdoanonimnost in nizki transakcijski stroški. Uporabniki lahko torej opravljajo transakcije na varen in hiter način, pri čemer sistem nudi višjo mejo anonimnosti kot marsikatero drugo plačilno

sredstvo. Vseeno pa ima relativno mlad sistem Bitcoina tudi pomanjkljivosti, ki se kažejo predvsem v obliki volatilnosti Bitcoina kot valute, kar je predvsem posledica negativnih odzivov ob večjih krajah in večjemu medijskemu poročanju o tem. Sam sistem Bitcoina je sicer zelo varen in preverjen, vendar pa zaščita pred krajami bitcoinov še ni dovolj razvita. Trenutno je velik del uporabnikov Bitcoina špekulativnih investitorjev, saj danes predstavlja ta kriptovaluta bolj špekulativno investicijo kot pa resnično valuto za poslovanje, vendar pa se to z večjo razširjenostjo uporabe bitcoinov in stabilizacijo trga lahko spremeni. Pomembno vlogo pri uravnavanju Bitcoina bodo imele tudi države, ki imajo v tem trenutku različen odnos do statusa in regulacije Bitcoina.

Razvoj kriptovalut v prihodnosti bo v veliki meri odvisen od regulatorjev, saj bodo le-ti s svojo politiko določili meje, znotraj katerih bodo ljudje lahko uporabljali novodobni digitalni denar. Kljub verjetnosti za vse večjo regulacijo in obstoja nevarnosti zlorab, pa bo Bitcoin zaradi svojih prednosti spodbudil razvoj na mnogih področjih in prinesel veliko tehnoloških inovacij. Definitivno se bo Bitcoin ali njegov morebitni naslednik uveljavil kot ena izmed valut, ki bodo na posameznih področjih nadomestili danes znane valute. Vendar po mojem mnenju v celoti ne bo mogel nadomestiti tradicionalnih valut zaradi njihove prevelike vpetosti v nadzor, regulacijo in uravnavanje gospodarstev. Po mojem mnenju bo Bitcoin največji pečat pustil na področju spletnega plačevanja in tehnologije, saj to področje danes predstavlja velik potencial nadaljnjega razvoja.

LITERATURA IN VIRI

1. Antonopoulos, M. A. (2014). *Mastering Bitcoin: Unlocking digital crypto-currencies* (1st ed.). Beijing: O'Reilly Media.
2. Banka Slovenije. (2015). Nadzor družb za izdajo elektronskega denarja. Najdeno 13. decembra 2014 na spletnem naslovu https://www.bsi.si/placilni-sistemi.asp?MapaId=1436
3. Barber, S., Boyen, W., Shi, E., & Uzun, E. (2012). Bitter to Better - How to Make Bitcoin a Better Currency. V A. D. Keromytis (ur.), *Financial Cryptography and Data Security* (str. 399-414). Berlin: Springer.
4. *Blockchain*. (2015). Najdeno 13. marca 2015 na spletni strani https://blockchain.info/sl/
5. Blundell-Wignall, A. (2014). The Bitcoin Question: Currency versus trust-less transfer technology. *OECD Working Papers on Finance, Insurance and Private Pensions, No. 37*. Paris: OECD Publishing.
6. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives, 29*(2), 213-238.
7. Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security, 2013*(11), 5-8.
8. Brito, J., & Castillo, A. (2013). *Bitcoin: A Primer for Policymakers*. Arlington: George Mason University.
9. Clark, C. (2013). *Bitcoin Internals*. Najdeno 15. decembra 2014 na spletnem naslovu https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=clark+bitcoin+internals
10. Coinmonk. (2013, 8. avgust). What is bitcoin and bitcoin mining? Najdeno 3. januarja 2014 na spletnem naslovu http://www.coinmonk.com/What%20is%20Bitcoin%20-%20CoinMonk.pdf
11. Davies, G. (2002). *A History of Money: From Ancient Times to the Present Day* (3rd ed.). Cardiff: University of Wales Press.
12. De Feis, N. M., & Patterson P. C. (2014, 30. januar). Bitcoins: 'Illegal Tender' or Currency of the Future? *New York Law Journal, 251*(20), 1-3.
13. Deloitte Center for Financial Services. (2014). *Bitcoin The new gold rush?* London: Deloitte Center for Financial Services.
14. Dorit, R., & Shamir, A. (2013). How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth? V R. Böhme, M. Brenner, T. Moore & M. Smith (ur.), *Financial Cryptography and Data Security* (str. 3-15). Berlin: Springer Heidelberg.
15. Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2015). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Washington D.C.: Library of Congress. Congressional Research Service.
16. European Central Bank. (2012, oktober). *Virtual Currency Schemes*. Frankfurt: European Central Bank.
17. Federal Bureau of Investigation. (2012, 24. april). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Washington: Federal Bureau of Investigation.

18. Forrester, D., & Solomon, M. (2013). Bitcoin Exposed: Today's Complete Guide to Tomorrow's Currency. Najdeno 19. decembra 2014 na spletnem naslovu http://www.amazon.com/gp/product/B00COYR4XQ?keywords=Bitcoin%20Exposed%3A%20Today%27s%20Complete%20Guide%20to%20Tomorrow%27s%20Currency&qid=1444830501&ref_=sr_1_1&sr=8-1
19. Friedman, M. (1994). *Money Mischief: Episodes in monetary history*. Orlando: Harcourt Brace & Company.
20. Gervais, A., Karame, G. O., Capkun, V. & Capkun, S. (2014). Is Bitcoin a Decentralized Currency? Najdeno 14. februarja 2015 na spletnem naslovu http://www.infoq.com/articles/is-bitcoin-a-decentralized-currency
21. Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal,4*, 160-207.
22. Gup, B. E. (2014). What is Money? From Commodities to Virtual Currencies. *Alternative Investment Analyst Review,3*(3), 52-59.
23. *History of Bitcoin*. Najdeno 24. junija 2014 na spletnem naslovu http://historyofbitcoin.org/
24. *IRS*. Najdeno 22. decembra 2014 na spletnem naslovu https://www.irs.gov/irb/2014-16_IRB/ar12.html
25. Kroll, A. J., Davey, C. I., & Felten, W. E. (2014). The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries. Najdeno 15. januarja 2015 na spletnem naslovu https://www.cs.princeton.edu/~kroll/papers/weis13_bitcoin.pdf B. k.: Princeton University.
26. The Law Library of Congress. (2014, januar). *Regulation of Bitcoin in Selected Jurisdictions*. Washington, D.C.: The Law Library of Congress.
27. Matonis, J. W. (1995). Digital Cash and Monetary Freedom. Najdeno 3. avgusta 2014 na spletnem naslovu https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAA&url=http%3A%2F%2Flibertarian.co.uk%2Flapubs%2Feconn%2Feconn063.pdf&ei=youIVeyDCsOE7gak6YOgBw&usg=AFQjCNGG8kqrEQTv0ajmvqHbou99K66aEQ&bvm=bv.96339352,d.ZGU&cad=rja
28. *Merkletree*. Najdeno 9. januarja 2015 na spletnem naslovu http://merkletree.io/
29. Mishkin, F. S. (2004). *The Economics of Money, Banking, and Financial Markets* (7th ed.). Boston: Pearson.
30. Nakamoto, S. (2008). Bitcoin: A Peer-to-peer Electronic Cash System. Najdeno 15. julija 2014 na spletnem naslovu https://bitcoin.org/bitcoin.pdf
31. *Paypal Case Study*. (b.l.) Najdeno 29. januarja 2015 na spletnem naslovu http://www.ecommerce-digest.com/paypal-case-study.html
32. Peng, S. (2013). *BITCOIN: Cryptography, Economics, and the Future* (diplomsko delo). Philadelphia: School of Engineering and Applied Science.
33. Piasecki, P. (2012). *Design and security analysis of Bitcoin infrastructure using application deployed on Google Apps Engine* (magistrsko delo). Łódź: Fakulteta za fiziko, računalništvo in uporabno matematiko.
34. Plassaras, N. A. (2013). Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF. *Chicago Journal of International Law,14*,1-26.
35. Ribnikar, I. (1999). *Monetarna ekonomija I.* Ljubljana: Ekonomska fakulteta.

36. Rice, D. T. (2013). The Past and Future of Bitcoins in Worldwide Commerce. Najdeno 16. aprila 2015 na spletnem naslovu http://www.americanbar.org/publications/blt/2013/11/05_rice.html
37. Salmon, F. (2013). The Bitcoin Bubble and the Future of Currency. Najdeno 16. maja 2015 na spletnem naslovu https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb
38. Samuelson, A. P., & Nordhaus D. W. (2002). *Ekonomija* (XXXIII. izd.). Ljubljana: GV Založba.
39. Seaman, D. (2013). The Bitcoin Primer: Risks, Opportunities, And Possibilities. Najdeno 14. novembra 2014 na spletnem naslovu http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=The+Bitcoin+Primer%3A+Risks%2C+Opportunities%2C+And+Possibilities.
40. Segendorf, B. (2014).What is Bitcoin? *Sveriges Riksbank Economic Review, 2014*(2), 71-87.
41. Simmel, G. (2005). *The Philosophy of Money* (3rd enlarged ed.). London: Taylor & Francis e-Library.
42. Sterry, R. D. (2012). You Can Learn Bitcoin. Najdeno 27. decembra 2014 na spletnem naslovu http://www.lulu.com/shop/http://www.lulu.com/shop/david-r-sterry/you-can-learn-bitcoin/ebook/product-20423608.html.
43. Štok, A. (2012). *Varnost spletnih plačil* (diplomsko delo). Maribor: Fakulteta za elektrotehniko, računalništvo in informatiko.
44. Takemoto, Y., & Knight, S. (2014). Mt. Gox files for bankruptcy, hit with lawsuit. Najdeno 13. januarja 2015 na spletnem naslovu http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228
45. Value Partners. (2011, januar). Capturing the Micropayments Opportunity. Najdeno 11. marca 2015 na spletnem naslovu http://www.valuepartners.com/downloads/PDF_Comunicati/Perspective/estrattomicropayments(1).pdf.
46. Vagstad, K., & Valstad, O. C. A. (2014). *A bit risky? A comparison between Bitcoin and other assets using an intraday value at Risk* (magistrsko delo). Trondheim: Norwegian University of Science and Technology.
47. Vico, D. J., & Arago, S. A. (2014). Bitcoin: A Cryptographic Currency. Najdeno 14. februarja 2015 na spletnem naslovu https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin_en.pdf
48. Zakon o plačilnih storitvah in sistemih. *Uradni list RS* št. 58/09, 34/10, 9/11 in 32/12.

PRILOGA

Priloga 1: Slovarček osnovnih terminov, povezanih z Bitcoinom

Bitcoin - je ime projekta, ki ga je začel posameznik ali skupina ljudi pod psevdonimom Satoshi Nakamoto. Cilj Satoshi Nakamota je bil ustvariti prvo decentralizirano kriptovaluto.

Bitcoin - ime valute same.

bitcoin - je številni samostalnik, oznaka posamezne enote Bitcoin valute, ki ima kratico BTC. Vsak BTC je deljiv, in sicer je mera sledeča: 1 Satoshi = 0,000000001 bitcoina (100.000.000 Satoshijev = 1 Bitcoin).

Naslov - je par ključev, ki so uporabljeni s strani uporabnika za dostop do svojih bitcoinov.

Transakcija - je posamezna operacija prenosa bitcoinov iz enega naslova na drug naslov (ali več naslovov); transakcija je podobna bančnemu transferju.

Izvorni blok (Genesis Block) - gre za prvi ustvarjeni blok in je uporabljen kot začetna točka blokovne verige.

Blok (block) - je paket informacij, ki vsebujejo vse transakcije, ustvarjene od prejšnjega bloka, gre torej za povezavo s predhodnim blokom, vse nazaj do izvornega bloka.

Veriga blokov (Blockchain) - je zbirka povezanih blokov od najnovejšega do izvornega (genesis) bloka.

Odjemalec (Client) - je aplikacija, uporabljena s strani uporabnikov, da izvedejo postopke na Bitcoin mreži.

Standardni odjemalec (Standard Client) - je odjemalec, razvit s strani razvijalcev, ki so delali na Bitcoin projektu. Določa standarde, kako bi morali odjemalci delati in komunicirati med seboj.

Protokol (Protocol) - definira pravila, kako klienti komunicirajo med seboj in kako so transakcije in bloki zakodirani.

Mreža (Network) - Bitcoin mreža je združeno ime za vse aplikacije povezane skupaj, za izmenjavo informacij o Bitcoin blokih, transakcijah in povezanih klientih.

Denarnica (Wallet) - je skupek naslovov, ustvarjenih s strani klienta in shranjenih lokalno v registru.

Rudar (Miner) - je računalniški stroj in spremljevalna aplikacija, namenjena proizvajanju novih blokov.

Menjalnica - je internetna stran, ki dovoljuje menjavo med bitcoini in tradicionalnimi valutami.

Vrstniško omrežje (Peer-to-peer) - je omrežje, kjer si izmenjujejo podatke po vnaprej dogovorjenem protokolu. Omrežje izpolnjuje svoje funkcije, dokler je večina vključenih vrstnikov poštena in se drži protokola.

Proof of work (PoW) - Je posrednik protokola, preko katerega lahko nekdo dokaže, da je bil v procesu pridobivanja vložen velik računalniški napor za odkrivanje zahtevane rešitve.

Zgoščevalna funkcija (Hash) - je algoritem, ki dobi kot vhod poljubno dolgo sporočilo, kot izhod pa vrne fiksno dolgo binarno vrednost (hash value). Uporabljamo jo za preoblikovanje poljubno dolgih vhodnih sporočil v izhodne vrednosti dolžine 128 bitov.

Pomembnost te funkcije je, da je nepovratna ali enosmerna, to pomeni, da je nemogoče najti vhodno sporočilo, če poznamo izhodno vrednost. Prav tako je nemogoče najti dve vhodni sporočili, ki bi ob izhodu tvorili enaka rezultata.

Programska odprta koda (Open source) - je razvojna metodologija, ki ponuja praktično kodo produkta v obliki ugodnosti in znanja in je dostopna vsakomur. Nima patenta in si jo lahko kdorkoli ogleda ter uporablja brez plačila.