

UNIVERZA V LJUBLJANI  
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

**TVEGANJA PRI UVELJAVLJANJU VIRTUALNIH VALUT:  
PRIMER BITCOIN**

Ljubljana, september 2016

RENATA ŠKOF

## IZJAVA O AVTORSTVU

Podpisana Renata Škof, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Tveganja pri uveljavljanju virtualnih valut: Primer Bitcoin, pripravljenega v sodelovanju s svetovalcem prof. dr. Alešem Berk Skokom

### IZJAVLJAM

1. da sem predloženo delo pripravila samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;
7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 30. 9. 2016

Podpis študentke: \_\_\_\_\_

# KAZALO

<b>UVOD .....</b>	<b>1</b>
<b>1 VIRTUALNE VALUTE.....</b>	<b>5</b>
1.1 Sistem virtualnih valut.....	5
1.1.1 Opredelitev virtualnih valut.....	5
1.1.2 Vrste virtualnih valut.....	6
1.1.3 Deležniki v sistemu virtualnih valut.....	8
1.2 Kriptovalute.....	9
1.3 Prednosti virtualnih valut.....	11
<b>2 VIRTUALNA VALUTA BITCOIN.....</b>	<b>13</b>
2.1 Opredelitev in zgodovinski razvoj bitcoina.....	13
2.2 Bitcoin kot plačilno sredstvo.....	15
2.3 Tehnične značilnosti.....	19
2.3.1 Delovanje Bitcoina.....	19
2.3.2 Rudarjenje oz. ustvarjanje novih bitcoinov.....	21
2.3.3 Nakup in prodaja bitcoinov.....	23
2.3.4 Bitcoin denarnica.....	23
2.3.5 Bitcoin avtomati.....	25
2.4 Kronologija pomembnejših dogodkov.....	26
2.5 Prednosti in pomanjkljivosti.....	28
2.5.1 Prednosti.....	28
2.5.2 Pomanjkljivosti.....	30
2.6 Spletne menjalnice za trgovanje z virtualnimi valutami.....	32
<b>3 ZAKONSKA UREDITEV VIRTUALNIH VALUT.....</b>	<b>32</b>
3.1 Zakonska ureditev virtualnih valut v svetu.....	32
3.2 Zakonska ureditev virtualnih valut v Sloveniji.....	36
<b>4 DEJAVNIKI, KI VPLIVAJO NA VREDNOST VALUTE BITCOIN.....</b>	<b>39</b>
4.1 Splošni dejavniki.....	39
4.2 Bančna kriza.....	39
4.3 Pravna regulacija.....	40
4.4 Količina bitcoinov v obtoku.....	40
4.5 Trgovanje z bitcoin valuto.....	40
4.6 Vpliv medijev.....	40
4.7 Špekulacije.....	41
<b>5 TVEGANJA POVEZANA Z VIRTUALNO VALUTO.....</b>	<b>41</b>
5.1 Področja tveganj.....	41
5.2 Tveganja povezana z obstoječimi plačilnimi sistemi.....	42
5.2.1 Vpliv virtualnih valut na cenovno stabilnost.....	42
5.2.2 Vpliv virtualnih valut na finančno stabilnost.....	43
5.2.3 Vpliv virtualnih valut na stabilnost plačilnih sistemov.....	44
5.2.3.1 Raba plačil v virtualnih valutah.....	44

5.2.3.2	Kreditna tveganja .....	45
5.2.3.3	Likvidnostna tveganja .....	45
5.2.3.4	Operativna tveganja .....	45
5.2.3.5	Pravna tveganja .....	46
5.2.3.6	Vloga Evropske centralne banke pri nadzoru virtualnih valut....	46
5.3	Tveganja povezana s kriminaliteto .....	46
5.3.1	Pregled izzivov za organe pregona.....	46
5.3.2	Pranje denarja .....	49
5.3.3	Davčne utaje .....	50
5.3.4	Kraje in prevare .....	51
5.3.5	Napadi na spletne menjalnice in vdori v denarnice.....	52
5.4	Tveganje pri uporabnikih virtualnih valut .....	54
5.5	Nihanje vrednosti valute bitcoin .....	55
<b>6</b>	<b>IZZIVI ZA PRIHODNOST .....</b>	<b>57</b>
	<b>SKLEP .....</b>	<b>67</b>
	<b>LITERATURA IN VIRI.....</b>	<b>72</b>

## KAZALO TABEL

Tabela 1: Razvrstitev virtualnih valut glede na opredelitev FATF .....	8
Tabela 2: Tržna kapitalizacija kriptografskih valut v USD na dan 17. 5. 2016 .....	10
Tabela 3: Enote bitcoina.....	21

## KAZALO SLIK

Slika 1: Prikaz virtualnih kriptovalut glede na tržno kapitalizacijo .....	10
Slika 2: Prikaz števila dnevnih nakazil .....	19
Slika 3: Velikost verige blokov .....	31
Slika 4: Zakonska regulativa Bitcoina po svetu .....	33
Slika 5: Gibanje vrednosti bitcoina v obdobju od 1. 1. 2009 do 31. 7. 2016.....	56

## UVOD

V zadnjem desetletju se je tehnologija močno razvila in uporaba interneta narašča, kar je vplivalo na kreiranje virtualnih valut, ki so se začele uporabljati za nakup dobrin in plačilo storitev. Razširjenost uporabe virtualnih denarnih valut se v zadnjem času naglo povečuje. Ob tem se poraja vprašanje, ali lahko virtualne valute, kot je bitcoin, ogrozijo obstoječi finančni sistem, ali gre zgolj za muho »nekaj letnico«?

Bitcoin je, verjetno ne po naključju, nastal v času največjega padca zaupanja v finančni sistem v njegovi zgodovini. Nadzor nad finančnimi tokovi, zamrznitev računov ali blokiranje transakcij, v bitcoin ekonomiji, ki jo tvorijo v omrežje povezani osebni računalniki, enostavno ni možno. Pričakovati je, da se finančna industrija in države z vodilnimi svetovnimi valutami ne bodo kar sprijaznile z oblikovanjem vzporedne ekonomije (Upelj, 2013).

Z vprašanjem, kam umestiti virtualno valuto bitcoin se ukvarjajo domala vse svetovne finančne institucije, saj se zavedajo, da po nekaj letih obstoja te valute, to ni le muha enodnevnica. V političnih, ekonomskih in pravnih krogih je nenaden porast virtualnih valut sprožil burne razprave glede možnosti regulacije in nadzora s strani državnih in mednarodnih finančnih institucij. Zaradi hitre, cenovno ugodne in transparentne plačilne storitve prinašajo te valute uporabnikom številne prednosti. Po drugi strani se zaradi anonimnosti uporabnikov in decentraliziranega značaja ter pomanjkanja nadzora in ustrezne zakonodaje, z njim okoriščajo kriminalne združbe, ki izkoriščajo virtualno valuto kot sredstvo, ki jim omogoča pranje denarja, davčne utaje in materialno okoriščanje na račun drugih uporabnikov virtualnih denarnih valut.

Trenutno obstaja na svetu zelo širok spekter virtualnih valut, vendar med vsemi po pomembnosti, vrednosti, dejanski uporabi in razširjenosti, prednjači **bitcoin**. Slednji tako po tržni kapitalizaciji, ki na dan 17. 5. 2016 znaša kar 7.078.401.870 ameriških dolarjev (v nadaljevanju USD) (Coinmarketcap, 2016), zaseda prvo mesto. Cena za enoto valute bitcoin je istega dne, dosegla 455,07 USD oz. 401,52 evrov (v nadaljevanju EUR). Število virtualnih kriptovalut je po podatkih spletne strani Coinmarketcap, na dan 17. 5. 2016 znašalo 618, s skupno tržno kapitalizacijo 8.809.289.805,00 USD.

Posebnost te valute je omejeno število enot v cirkulaciji. Trenutno je v obtoku 15.554.500 bitcoin kovancev (v nadaljevanju BTC). Vrednost bitcoina se oblikuje na podlagi ponudbe in povpraševanja, trgovanje pa poteka na borzah, namenjenim izključno trgovanju s kriptovalutami. Transakcijski stroški so v primerjavi z navadnimi valutami zelo majhni. Skupno število vseh ustvarjenih enot bitcoin kovancev je omejeno na 21 milijonov BTC, kar se predvideva, da bo doseženo v letu 2140 (Murphy, Murphy & Seitzinger, 2015, str. 3).

Bitcoin bi lahko opredelili kot prvo decentralizirano kriptovaluto, pri kateri nastajanje in prenos bitcoinov temelji na odprtokodnem protokolu, ki ni odvisen od centralne banke ali drugega regulatornega organa. Nastaja s pomočjo t.i. rudarjenja (angl. *mining*), po sistemu, ki ga je v članku iz leta 2008 objavil avtor, pod psevdonimom Satoshi Nakamoto, kjer je opisan protokol, po katerem sistem ustvarjanja novih bitcoinov deluje. V njem je opisal idejo elektronskega denarja, ki omogoča direktna plačila preko spleta brez posredovanja finančne ustanove. Sistem deluje na podlagi vrstniškega omrežja, po sistemu »vsak z vsakim« (angl. *Peer-to-peer*, v nadaljevanju P2P), preko katerega lahko uporabniki med seboj izvajajo plačila (Nakamoto, 2008). Računalniki na omrežju preverjajo pravilnost izvedenih transakcij in jih beležijo v javno dostopno podatkovno bazo, imenovano blockchain. Transakcije potekajo neposredno od uporabnika do uporabnika preko omrežja in ne preko posrednikov, kot so banke, hranilnice ipd. Pri transakcijah sistem uporablja valuto, imenovano bitcoin.

Nad njo nima nadzora nobena finančna institucija, vendar jo Evropska centralna banka in druge finančne institucije budno spremljajo, saj bi ob vse večji uporabi in zaupanju v to valuto, lahko ogrozila obstoječe valute in bančni sistem.

Evropski bančni organ (angl. *European Banking Authority*, v nadaljevanju *EBA*) je v zvezi z virtualnimi valutami prvič reagiral 13. 12. 2013, ko je izdal opozorilo uporabnikom v zvezi z navideznimi valutami, v katerem opozarja na nevarnosti pri vlaganju v virtualne valute in na tveganja, povezana z goljufijami, utajami davkov ter drugimi kaznivimi dejanji (EBA, 2013). Poleg navedenega dokumenta je EBA v juliju 2014 objavila mnenje o virtualnih valutah (EBA, 2014), pri čemer pomemben del tega mnenja predstavljajo tveganja, ki ga lahko predstavlja poslovanje z virtualnimi valutami. Svoje delo na področju virtualnih valut je opravila tudi Evropska centralna banka (angl. *European Central Bank*, v nadaljevanju *ECB*) z dvema dokumentoma, v katerih prav tako opozarja na pasti virtualnih valut. V letu 2012 je ECB izdala obširno poročilo, v katerem je ocenila potencial virtualnih valut na ekonomijo in posledice, ki jih le-te lahko povzročijo (ECB, 2012).

Tveganj, ki so povezani z bitcoin valuto, je veliko. Eden od dejavnikov tveganja, je njegova visoka nestanovitnost, ki omejuje uporabnost bitcoina kot zanesljivo sredstvo za hranjenje vrednosti in obračunsko enoto. Zaradi svoje nestanovitnosti in velikih razlik v vrednosti na različnih borzah je priljubljen tudi pri špekulantih, ki skušajo to izkoristiti za svoj zaslužek.

Z razširjenostjo uporabe virtualnih valut pa se ukvarjajo tudi organi pregona, saj zaradi anonimnosti daje neslutene možnosti zlorab v špekulativne namene. Anonimnost omogoča, da se virtualne valute uporabljajo za nezakonite dejavnosti na črnem trgu, kot so trgovanje z drogami ali orožjem. Ameriški zvezni preiskovalni urad (angl. *Federal Bureau of Investigation*, v nadaljevanju *FBI*) je zaradi visoke stopnje anonimnosti, ki jo omogočajo virtualne valute, v svojem poročilu zapisal, da ugotavljajo visoko stopnjo kibernetike

kriminalitete. Vedno več bo kriminalnih združb, ki bodo uporabljale virtualne valute za pranje denarja, financiranje kriminala, vedno več bo vdorov v računalnike posameznikov zaradi kraje virtualnih denarnih enot iz virtualnih denarnic (FBI, 2012). To uporabnikom omogoča programska oprema TOR, ki deluje preko omrežja »temnega spleta« (angl. *Dark Web*).

Lahko rečemo, da so virtualno valuto bitcoin njeni uporabniki ter finančne in vladne institucije spremenili v plačilno sredstvo, ki bi lahko pomenilo revolucijo v svetu bančništva. Ker za opravljanje finančne transakcije ni potreben vmesni člen finančne institucije, 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.

Strokovnjaki, ki se ukvarjajo s področjem raziskovanja vpliva virtualnih valut, si niso enotni. Zagovorniki menijo, da bodo ravno nizki stroški transakcij bitcoinov nekega dne spremenili trg globalnih denarnih transferjev in nakazil (Brito & Castillo, 2013, str. 10-11). Jon Matonis meni, da bitcoin kot prva neodvisna svetovna valuta vsekakor ima potencial, da revolucionarno spremeni sistem plačevanja, saj niti omrežje niti posamezna enota ne potrebuje nadzora, kar jo postavlja v edinstven položaj, ko lahko zaobide obstoječo bančno infrastrukturo (Upelj, 2013).

Bitcoin omogoča hitrejša in cenejša nakazila ter revnim ljudem v državah v razvoju ponuja dostop do finančnih storitev, ki jih drugače ne bi bili deležni. Praprotnik (2015) meni, da lahko pozitivni vpliv bitcoina in drugih medijev izmenjave banke prisili, da znižajo stroške za mednarodne transakcije, ker ponuja možnost zelo poceni prenosa denarja za revnejše ljudi, hkrati pa bi lahko klasične banke prisilil v posodabljanje svojih storitev, ki bodo tako postale hitrejše, morda tudi bolj varne in cenejše.

Glavni problem pri bitcoinu je torej, da precej niha v vrednosti in da ga še ne sprejema dovolj trgovcev. Zaradi te nestanovitnosti ni in ne more biti prava valuta (Praprotnik, 2015), hkrati pa je izpostavljena pranju denarja ter izogibanju davčnih obveznosti, zaradi česar kritiki dvomijo, da bi lahko bitcoin kdaj prevzel klasične denarne trge in nadomestil dolar ali evro.

Virtualne valute pa so še posebej privlačne kot sredstvo za izogibanje plačila davkov, predvsem zaradi anonimnosti in dejstva, da država nima pristojnosti nad njo in zatorej niso predmet obdavčitve. Omri Marian (2013, str. 39) meni, da imajo virtualne valute tradicionalne značilnosti davčnih oaz: dohodki niso obdavčeni, anonimnost davkoplačevalcev je zagotovljena. Njihovo delovanje ni odvisno od finančnih institucij, zaradi česar lahko ogrozijo dosedanja prizadevanja vlad na področju boja proti utaji davkov.

Virtualna valuta bitcoin je eksperimentalna valuta, ki se še vedno razvija. Njeno prihodnost je težko napovedovati, pa vendarle bom v nalogi skušala podati širši pregled nad področjem uporabe virtualnih valut kot alternativnim načinom plačevanja ter odgovoriti na vprašanje, ali se virtualne valute, kot je bitcoin, lahko uveljavijo kot prava valuta in sredstvo za izmenjavo.

Namen magistrskega dela je prikazati vse hitrejši razcvet virtualnih valut in opisati prednosti in izzive, ki jih ta decentraliziran sistem prinaša, hkrati pa opozoriti na nevarnosti oz. tveganja, tako za uporabnika, kot tudi vpliv bitcoina na stabilnost finančnega sistema oziroma uporabo virtualnih valut v špekulativne namene. Namen naloge je raziskati, ali lahko virtualne valute, kot so bitcoin, resno ogrozijo ali spremenijo tradicionalni bančni sistem, ali gre zgolj za poskus uvedbe le-tega, ki pa je zaradi špekulacij in svoje nestanovitnosti še vedno tvegana naložba.

Cilj magistrskega dela je predstaviti tveganja, ki se pojavljajo zaradi neregularnosti trga virtualnih valut in odsotnosti nadzora tako med izdajatelji virtualnih valut, kot nad posredniki, in sicer s stališča uporabnika, kot tudi vpliv virtualnih valut na stabilnost finančnega sistema ter tveganja, povezana s kriminaliteto. Cilj magistrskega dela je proučiti mehanizme na različnih nivojih za obvladovanje tveganj, tako z vidika posameznika, kot z vidika regulatorne ureditve proučevanega področja.

Glavne metode dela, ki sem jih uporabila pri pripravi magistrskega dela, slonijo na analizi relevantne literature sekundarnih virov podatkov, predvsem strokovne literature tujih avtorjev, člankov, prispevkov, internetnih virov in drugih strokovnih virov z najnovejšimi dognanji proučevanega področja. Metodološki okvir sta analiza in sinteza sekundarnih virov in lastna kritična presoja ter lastna analiza za napoved dinamike prihodnjih verjetnih dogodkov oz. sprememb do uveljavitve novega plačilnega standarda.

Magistrsko delo je sestavljeno iz šestih poglavij. V prvem poglavju bodo opisane sheme virtualnih valut, njihova opredelitev, vrste virtualnih valut in kriptovalute ter prednosti, ki jih virtualne valute ponujajo. V drugem poglavju podrobneje razčlenjujem virtualno valuto bitcoin, z vidika samega delovanja, zasnove sistema in trgovanja ter z vidika valute bitcoin kot plačilnega sredstva. V nadaljevanju opišem kronologijo pomembnejših dogodkov ter prednosti in slabosti sistema in valute. Tretje poglavje je namenjeno zakonodajno pravnemu vidiku ureditve področja Bitcoin sistema v svetu, kjer bo poudarek na dosednji ureditvi zakonodajnega področja v nekaterih izbranih državah ter dosedanja zakonska ureditev tega področja v Republiki Sloveniji. Četrto poglavje predstavlja nekatere dejavnike, ki vplivajo na vrednost valute bitcoin. Peto poglavje se osredotoča na tveganja, ki so povezana z virtualno valuto. V njem opisujem tveganja vpliva na monetarni sistem in ekonomijo, tveganja, povezana s kriminaliteto, pranjem denarja in z davčnimi utajami, tveganja, ki so mu izpostavljeni uporabniki sistema, ter tveganja, povezana z visoko nestanovitnostjo vrednosti valute. V šestem poglavju predstavljam izzive za prihodnost z



vidika valute bitcoin in njene umestitve v bodoči plačilni sistem ter možnosti regulatorne ureditve z namenom preprečevanja kriminalitete. Prav tako predstavljam blockchain tehnologijo, ki lahko revolucionarno spremeni sistem ne samo na področju plačil, pač pa se lahko širi tudi na druga področja. Magistrsko delo zaključujem s sklepnimi ugotovitvami.

## **1 VIRTUALNE VALUTE**

### **1.1 Sistem virtualnih valut**

#### **1.1.1 Opredelitev virtualnih valut**

Glede opredelitve pojma virtualne valute v literaturi ni zaslediti enotne definicije. Vsaka institucija jo opredeljuje drugače. EBA (2014, str. 11) opredeli virtualne valute kot »digitalni zapis vrednosti, ki niso izdane s strani centralne banke ali drugega javnega organa, niti niso nujno vezane na fiat valuto, vendar so sprejete s strani fizičnih ali pravnih oseb kot sredstvo menjave in se lahko prenašajo, hranijo in trgujejo v elektronski obliki«.

EBA (2014, str. 13) v svojem dokumentu poudarja, da virtualne valute niso zakonito plačilno sredstvo, kar pomeni, da njihovo sprejetje ne zavezuje upnikov, da sprejmejo te valute. Prav tako EBA navaja, da v času nastajanja dokumenta, virtualne valute niso bile zakonito plačilno sredstvo v nobeni državi, dopušča pa teoretično možnost, da bi v prihodnosti lahko bila razglašena za zakonito plačilno sredstvo v nekaterih državah, vendar je zelo malo verjetno, da bi se to zgodilo v državi članici EU.

ECB opredeli virtualne valute kot »vrsta nereguliranega, digitalnega denarja, nad katerim imajo nadzor njihovi razvijalci in je sprejet med člani posebne, virtualne skupnosti« (ECB, 2012, str. 13).

ECB je kasneje v dokumentu (2015, str. 4) »Virtual currency schemes – a further analysis«, opredelila virtualno valuto kot »digitalno zastopanje vrednosti, ki ni izdano s strani centralne banke, kreditne institucije ali institucije, ki izdaja elektronski denar in se lahko v nekaterih okoliščinah uporablja kot alternativa denarju«.

Projektna skupina za finančno ukrepanje (angl. *The Financial Action Task Force*, v nadaljevanju FATF) opredeli virtualno valuto kot »digitalno zastopanje vrednosti, s katero se lahko digitalno trguje in ima funkcije kot (1) sredstvo menjave, in/ali (2) obračunska enota, in/ali (3) hranilec vrednosti, vendar nima statusa zakonitega plačilnega sredstva. Ni izdana s strani javnega organa in izpolnjuje zgoraj navedene funkcije samo na podlagi dogovora članov skupnosti, ki virtualno valuto uporabljajo. Virtualna valuta se razlikuje od t.i. fiat valute (realni denar oz. nacionalna valuta), ki je v obliki bankovcev in kovancev in je s strani države določena kot zakonito plačilno sredstvo. Prav tako se loči od e-denarja, ki

je zgolj digitalno zastopanje fiat valute in se uporablja pri elektronskih plačilih ter ima status zakonitega plačilnega sredstva« (FATF, 2014, str. 4).

Digitalna valuta pomeni digitalno zastopanje vrednosti, bodisi virtualne valute, bodisi fiat valute v obliki e-denarja. Pogosto jo zamenjujejo s terminološkim izrazom virtualna valuta (FATF, 2014, str. 4).

### **1.1.2 Vrste virtualnih valut**

Obstaja veliko različnih shem virtualnih valut, ki jih ni enostavno razvrstiti. ECB je v svojem dokumentu razvrstila virtualne valute glede na njihovo povezanost s pravim denarjem, kar pomeni zamenljivost denarnega toka med virtualno in realno valuto ter povezanost z realnim gospodarstvom, z možnostjo nakupa dobrin in storitev. Po tej razvrstitvi lahko virtualne valute razvrstimo v tri vrste virtualnih valut (ECB, 2012, str. 13-14), in sicer zaprti sistem virtualne valute, sistem virtualne valute z enosmernim tokom in sistem virtualne valute z dvosmernim tokom.

#### **1. Zaprti sistemi virtualne valute**

Te sheme nimajo skoraj nobene povezave z realnim gospodarstvom. Imenujemo jih tudi z izrazom »in game only«, kar pomeni, da se uporabljajo le v svetu računalniških iger. Uporabniki običajno plačajo članarino in nato imajo možnost zaslužiti virtualni denar, ki temelji na njihovi spletni uspešnosti. Tovrstne virtualne valute se lahko porabijo le za nakup virtualnih dobrin in storitev znotraj te virtualne skupnosti. Z njimi ni mogoče trgovati izven virtualne skupnosti. Primer takšne virtualne valute je virtualno zlato v računalniški igri, poimenovani *World of Warcraft Gold* (v nadaljevanju WoW Gold). Kot sredstvo menjave v igri se uporablja WoW Gold za nakup različnih stvari znotraj igre, medtem ko sta prodaja in nakup v realnem svetu strogo prepovedana.

#### **2. Sistem virtualne valute z enosmernim tokom**

Ta sistem pomeni nakup virtualne valute s tradicionalno valuto po določenem menjalnem tečaju, vendar pa te valute ni mogoče zamenjati nazaj za pravi denar. Pogoje menjave določi lastnik sheme. Shema virtualnih valut z enosmernim tokom omogoča, da se valuta uporablja za nakup virtualnih dobrin in storitev, nekatere sheme pa tudi dovoljujejo, da so tovrstne virtualne valute uporabljene za nakup pravih dobrin in storitev. *Primer* takšne virtualne valute so Facebook krediti, ki omogočajo uporabnikom nakup virtualnih dobrin na Facebook platformi, ter t.i. Nintendo točke, ki jih je ustanovila družba Nintendo, s katerimi lahko potrošniki kupijo točke preko spleta z uporabo kreditne kartice ali v trgovinah z nakupom Nintendo Points Card. Točk ni mogoče pretvoriti nazaj v pravi denar.

### 3. Sistem virtualne valute z dvosmernim tokom

Ta shema omogoča uporabnikom nakup in prodajo virtualnega denarja po menjalnih tečajih njihove valute. Virtualna valuta je podobna katerikoli drugi valuti v obtoku. Sistem omogoča tako nakup virtualnih, kot tudi pravih dobrin in storitev. *Primer*a takšne virtualne valute sta Linden dolarji (angl. *Linden Dollars*), ki se uporabljajo v virtualnem svetu, imenovanem Second Life ter Bitcoin, najbolj razširjena virtualna valuta.

FATF (2014, str. 4) v svojem dokumentu predlaga razdelitev virtualnih valut glede na to, ali so konvertibilne oz. zamenljive za fiat valute, in glede na to, ali so centralizirane ali decentralizirane.

**Konvertibilna** (odprta oz. zamenljiva) virtualna valuta ima enako vrednost kot realna valuta in jo je mogoče zamenjati za realno valuto. Primeri takšne valute so Bitcoin, E-Gold, Liberty Reserve, Second Life Linden Dollars in Webmoney.

**Nekonvertibilna** (zaprta oz. nezamenljiva) virtualna valuta je ustvarjena za določeno okolje, za posamezno realno ali virtualno skupnost. Deluje pod določenimi pravili, v skladu s pogoji, ki veljajo za to valuto, in ne more biti zamenjana za pravi denar oz. fiat valuto. Primeri takšnih valut so Project Entropia Dollars, Q Coins in World of Warcraft Gold (FATF, 2014, str. 4).

Vse nekonvertibilne virtualne valute so centralizirane. Izdane so s strani centralne avtoritete, ki postavi pravila, ki veljajo v okolju uporabe ter jih ni mogoče zamenjati za drugo sredstvo. Konvertibilne valute pa so lahko bodisi centralizirane, bodisi decentralizirane.

**Centralizirana** virtualna valuta ima skrbnika oz. administratorja, npr. tretjo udeleženo stranko, ki nadzoruje sistem. Skrbnik izdaja valuto, določa pravila za njeno uporabo, vzdržuje centralno knjigo plačil ter jo lahko tudi umakne iz obtoka. Menjalna vrednost se lahko določa na trgu s ponudbo in povpraševanjem, ali je določena s strani skrbnika ter vezana na fiat valuto oz. drugo realno vrednost, kot je npr. zlato ali košarica dobrin. Primeri takšnih valut so E-gold, Liberty Reserve dollars, Linden dollars v sistemu Second Life, Webmoney, World of Warcraft gold.

**Decentralizirana** virtualna valuta, imenovana tudi kriptovaluta, je distribuirana, odprtokodna valuta, ki temelji na osnovi matematičnih algoritmov. Te valute so zasnovane na P2P omrežju. So brez nadzora neke centralne avtoritete oz. skrbnika, ki bi nadzirala sistem. Primeri takšnih valut so Bitcoin, Litecoin, Ripple (FATF, 2014, str. 5).

*Tabela 1: Razvrstitev virtualnih valut glede na opredelitev FATF*

	Centralizirane	Decentralizirane
Konvertibilne	Skrbniki, izmenjevalci, uporabniki, posredniki; so zamenljive za realno valuto. Primer: WebMoney	Izmenjevalci, uporabniki (brez skrbnika), brez posrednikov; so zamenljive za realno (fiat) valuto. Primer: Bitcoin
Nekonvertibilne	Skrbniki, izmenjevalci, uporabniki, posredniki; niso zamenljive za realno (fiat) valuto. Primer: World of Warcraft Gold	Ne obstaja

*Vir: FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014, str. 8.*

Po zgornji razvrstitvi sodi bitcoin med decentralizirane, konvertibilne oz. zamenljive valute.

### 1.1.3 Deležniki v sistemu virtualnih valut

Za lažje razumevanje tega gradiva, je potrebno razčleniti posamezne deležnike, ki sodelujejo pri izmenjavi virtualnih valut (FATF, 2014, str. 7-8).

**Menjalec** (angl. *an exchanger*) je fizična ali pravna oseba, ki omogoča menjavo med virtualno in pravo valuto, med sredstvi ali med drugimi vrstami virtualnih valut ter plemenitih kovin za določeno provizijo.

**Skrbnik** (angl. *an administrator*) je fizična ali pravna oseba, ki izdaja centralizirano virtualno valuto, določa pravila za njeno uporabo, vzdržuje centralni plačilni zapis ter ima možnost umakniti valuto iz prometa.

**Uporabnik** (angl. *a user*) je oseba, ki pridobi virtualno valuto in jo uporabi za nakup blaga in storitev, jo uporablja kot transfer do drugega uporabnika ali jo hrani v obliki investicije. Uporabniki lahko pridobijo virtualno valuto na več načinov: z nakupom, lahko jo prisluži z opravljanjem dejavnosti ali pri decentraliziranih virtualnih valutah (npr. bitcoin) ustvari z rudarjenjem.

**Rudar** (angl. *a miner*) je posameznik ali subjekt, ki sodeluje v decentraliziranem virtualnem omrežju, s posebno programsko opremo, z reševanjem kompleksnih matematičnih algoritmov, ki se uporabljajo za potrditev transakcije v sistemu virtualne valute ter ustvarja virtualno valuto za lastno uporabo ali za trgovanje z drugimi valutami.

**Denarnica** (angl. *virtual currency wallet*) je oblika programske opreme, kjer lastnik virtualne valute hrani svojo valuto z namenom shranjevanja ali nakazovanja teh sredstev drugim subjektom v mreži.

**Ponudnik denarnice** (angl. *a wallet provider*) je pravna oseba, ki ponuja programsko opremo v obliki denarnice. Denarnica vsebuje zasebni ključ uporabnika, ki mu omogoča uporabo virtualne valute za transakcije na druge naslove v verigi blokov. Ponudnik denarnice omogoča sodelovanje v sistemu virtualne valute uporabnikom, izmenjevalcem in trgovcem ter zagotavlja varnost za shranjevanje in transakcije. Uporabnikom lahko omogoči dodatno šifriranje, večkratni ključ, zaščito s podpisom, idr. Vse bitcoin denarnice so medsebojno združljive z drugimi bitcoin denarnicami. Denarnico je mogoče shraniti na spletu (angl. *hot storage*) ali pa jo namestimo na različne naprave, kot so pametni telefon, tablični računalniki (angl. *cold storage*).

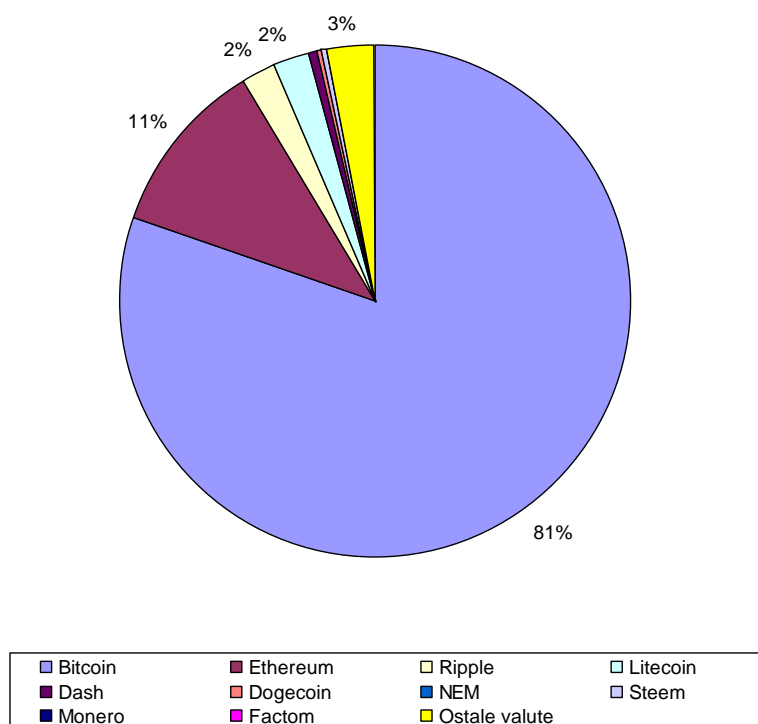
Poleg navedenih obstajajo na trgu še **ostali deležniki**, ki sodelujejo v sistemih virtualnih valut. Mednje uvrščamo spletne skrbnike, razvijalce programske opreme ter druge ponudnike aplikacij.

## 1.2 Kriptovalute

**Kriptovaluta** – je decentralizirana, konvertibilna virtualna valuta, ki temelji na zasnovi matematičnih algoritmov. Deluje na osnovi kriptografije, ki omogoča distribucijo varne informacijske ekonomije. Kriptovalute za svoje delovanje uporabljajo privatni in javni ključ, ki omogoča prenos vrednosti med dvema uporabnikoma (fizično ali pravno osebo), ki vsako transakcijo odobrita s kriptografskim podpisom. Varnost, integriteta in stanje zapisa so zagotovljeni z omrežjem povezanih udeležencev, ki potrjujejo transakcije in vzdržujejo verigo blokov v zameno za provizije. Pri sistemu Bitcoin se le-ti imenujejo rudarji (FATF, 2014, str. 5).

Trenutno na svetu obstaja zelo širok spekter virtualnih valut, ki so v uporabi, vendar med vsemi po pomembnosti, vrednosti, dejanski uporabi in razširjenosti, prednjači **bitcoin**. Število virtualnih kriptovalut je po podatkih spletne strani Coinmarketcap na dan 17. 5. 2016 znašalo 618, s skupno tržno kapitalizacijo 8.809.289.805,00 USD.

Slika 1: Prikaz virtualnih kriptovalut glede na tržno kapitalizacijo



Vir: Coinmarketcap, *Crypto-Currency Market Capitalizations*, 2016.

Bitcoin po tržni kapitalizaciji, ki na dan 17. 5. 2016 znaša kar 7.078.401.870 USD, zaseda prvo mesto. Trenutno je v obtoku 15.554.500 BTC (Coinmarketcap, 2016), cena pa je istega dne za enoto valute bitcoin dosegla vrednost 455,07 USD oz. 401,52 EUR. Največji zasledovalec je Ethereum, katerega vrednost ne dosega 15 % vrednosti bitcoina. Rangiranje virtualnih kriptovalut po tržni kapitalizaciji prikazuje tabela 2.

Tabela 2: Tržna kapitalizacija kriptografskih valut v USD na dan 17. 5. 2016

		Oznaka valute	Tržna kapitalizacija v USD
1	<b>Bitcoin</b>	BTC	7.078.401.870
2	<b>Ethereum</b>	ETH	962.104.198
3	<b>Ripple</b>	XRP	210.363.092
4	<b>Litecoin</b>	LTC	183.111.418
5	<b>Dash</b>	DASH	47.072.817
6	<b>Dogecoin</b>	DOGE	23.532.730
7	<b>NEM</b>	XEM	13.502.430
8	<b>Steem</b>	STEEM	11.238.443
9	<b>Monero</b>	XMR	10.107.508
10	<b>Factorom</b>	FCT	9.661.278

Vir: Coinmarketcap, *Crypto-Currency Market Capitalizations*, 2016.

Bitcoin ni vezan na nobeno nacionalno valuto, menjalni tečaj se določa na podlagi ponudbe in povpraševanja. Menjava nacionalnih valut v virtualne valute oz. trgovanje z virtualnimi valutami je mogoče preko posebnih menjalnih platform, imenovanih borze oz. spletne menjalnice.

### **1.3 Prednosti virtualnih valut**

Tehnologija interneta, ki neposredno povezuje uporabnika z drugimi uporabniki, odpira širok spekter možnosti. Prvič v zgodovini se s pomočjo tehnologije rušijo fizične in politične meje in celoten planet ima dostop do istih informacij, ki jo omogoča decentralizirana zasnova interneta (Caetano, 2015, str. 2).

Finančni trgi se srečujejo s številnimi težavami, kar je tudi eden izmed razlogov, da so se na tržišču pojavile nove oblike plačevanja, ki uporabnikom ponujajo hitrejša in cenejša plačevanja, brez birokratskih postopkov in brez čakalnih vrst. Virtualne valute ponujajo uporabnikom številne prednosti: nižji stroški transakcij omogočajo posameznikom in malim podjetjem alternativne oblike plačil, ki so bistveno cenejše v primerjavi z dragimi kreditnimi karticami, omogočajo hitrejša in cenejša mednarodna nakazila, plačevanje mikroplačil, ki do sedaj praktično niso bila mogoča, ščitijo posameznike pred zasegom sredstev na računih s strani vladnih organov, omogočajo večjo zasebnost ter spodbujajo inovacije na finančnem področju (Trautman & Harrell, 2016, str. 28-29).

Pojav virtualnih valut sovpada z bančno krizo, ki se je pojavila v letu 2008. Bančna kriza je povzročila izgubo zaupanja ljudi v tradicionalne bančne sisteme. Strah pred izgubo kapitala, nizke obrestne mere in negotovost nekaterih obstoječih valut je povzročilo, da so državljani začeli dvomiti v tradicionalno bančništvo (Richter, Kraus & Bouncken, 2015, str. 575). Na trgu so se pojavile nove oblike valut, ki so neodvisne od tradicionalnih finančnih sistemov.

Tehnologija virtualnih valut ponuja uporabnikom številne prednosti. Omogoča varen prenos velikih količin denarja na drugi konec sveta. Večji del svetovne populacije v državah v razvoju nima dostopa do bančnih storitev in ti ljudje so tako popolnoma odrezani od mednarodnih finančnih trgov in udeležbe v transakcijah v svetovni trgovini (Tsukerman, 2015, str. 1142). Mas navaja, da približno 2,5 milijarde ljudi na svetu nima dostopa do bančnega računa (Hernandez-Verme & Valdes-Benavides, 2013, str. 334).

Mednarodna nakazila za prenos denarja so še vedno izredno draga za uporabnike. Po podatkih Svetovne banke je ob koncu leta 2015 povprečni strošek za mednarodni prenos denarnih sredstev znašal 7,37 % na svetovni ravni, med državami članicami skupine G8 pa je bil le nekoliko nižji, v povprečju okoli 6,89 % (Raskin & Yermack, 2016, str. 14). Stroški prenosa mednarodnih nakazil se močno razlikujejo od države do države. Med državami članicami skupine G20, ki je v letu 2013 po podatkih Svetovne banke znašal v

povprečju 8,16 %, so bila najdražja nakazila v Južni Afriki, s kar 18,16 %. Sledi ji Japonska, s povprečnim stroškom nakazila 15,73 % (Trautman, 2014, str. 61). V letu 2014 sta Western Union in MoneyGram za svoje storitve pošiljanja nakazil zaračunavala nadomestilo približno v višini 8 odstotkov (Tsukerman, 2015, str. 1141). Mnogi trgovci pa celo zavračajo mednarodne plačilne transakcije preko kreditnih kartic. Glavni razlog za to je stopnja tveganja goljufij, ki je na zelo visoki ravni (Tsukerman, 2015, str. 1142).

Transakcijska nakazila z virtualnimi valutami so cenejša od transakcij s kreditnimi karticami. Medtem ko je za prenos sredstev preko kreditnih kartic trgovcem zaračunan znesek v razponu od 3 do 4 odstotke celotnega zneska transakcij, lahko transakcija v sistemu Bitcoin stane manj kot 1 odstotek (Allen, 2015, str. 36).

Za razliko od običajnih plačilnih sistemov, pri katerih prenosi denarnih sredstev iz enega konca sveta na drugega trajajo običajno nekaj dni, da gredo skozi proces preverjanja in verifikacije (Raskin & Yermack, 2016, str. 14), je za izvedbo transakcij nakazil v virtualnih valutah potreben bistveno krajši čas, običajno le okoli deset minut za transakcijo (Allen, 2015, str. 36). Obdelava plačil poteka po sistemu 24/7, kar pomeni, da je uporabnikom na voljo 24 ur na dan, vse dni v tednu (EBA, 2014, str. 17).

Virtualne valute preko spleta omogočajo nakazila zelo majhnih zneskov, imenovanih mikroplačila (angl. *micropayments*). Nakazovanje zneskov, kot npr. 30 centov, je bilo do sedaj praktično nemogoče, zaradi visokih transakcijskih stroškov plačilnih posrednikov. Zaradi nizkih provizij je sedaj mogoče nakazovati tudi zneske v višini do 1 USD (Grinberg, 2011, str. 170).

Mnogi posamezniki ne zaupajo svojega premoženja centralni banki oz. drugim finančnim institucijam in raje naložijo prihranke v druge oblike varčevanja, kot je npr. zlato. Za takšne posameznike bitcoin predstavlja alternativo, saj je brez bremen in tveganja, da bi se morali ukvarjati s fizično obliko vrednosti njihovega premoženja (Turpin, 2014, str. 352).

Plačilne transakcije z virtualnimi valutami ne zahtevajo posredovanja osebnih podatkov in uporabe gesel, za razliko od plačevanja s kreditnimi karticami v primeru običajnih načinov plačevanja. V tem smislu lahko virtualne valute obravnavamo kot poslovanje z gotovino (EBA, 2014, str. 19).

Virtualne valute so ustvarile nove vrste podjetij, ki prej niso obstajale. Decentralizirano omrežje virtualnih valut ponuja številne nove poslovne priložnosti ter s tem tudi priložnosti za gospodarsko rast. Razvijajo se podjetja za podporo tem tehnologijam, kot so spletne menjalnice za izmenjavo virtualnih valut, ponudniki specializirane rudarske opreme (EBA, 2014, str. 18), ponudniki avtomatov za izmenjavo virtualnih valut, posredniki, ki povezujejo trgovce in uporabnike in jim omogočajo lažje načine plačevanja.



## 2 VIRTUALNA VALUTA BITCOIN

### 2.1 Opredelitev in zgodovinski razvoj bitcoina

Oktober leta 2008 je avtor ali skupina avtorjev, pod imenom Satoshi Nakamoto objavil članek z naslovom »**Bitcoin: A Peer-to-Peer Electronic Cash System**«, v katerem je opisal idejo elektronskega denarja, ki bi »omogočala neposredna plačila preko spleta, brez posredovanja finančne institucije. Trgovanje preko spleta je bilo do tedaj odvisno od finančnih institucij, ki služijo kot zaupanja vredne tretje osebe, ki so potrebne za obdelavo elektronskih plačil. Medtem, ko sistem sicer deluje dobro, so še vedno prisotne pomanjkljivosti zaupanja v model. Popolnoma nepovratne transakcije v resnici niso vedno mogoče, saj se finančne institucije ne morejo izogniti posredovanju sporov. Stroški mediacije povečujejo transakcijske stroške, omejena je dejanska velikost transakcije in s tem večji strošek omeji možnost nepovratnih plačil za storitve. Z možnostjo povrnitve transakcije, se potreba po zaupanju povečuje. Potreben je elektronski plačilni sistem, ki temelji na kriptografskem dokazovanju namesto na zaupanju med strankami«. V prispevku avtor predlaga rešitev problema dvojne porabe z uporabo P2P tehnologije na podlagi matematičnih dokazil vrstnega reda zaporedij (Nakamoto, 2008, str. 1). Nekaj mesecev pozneje je bila objavljena prva verzija programskega plačilnega sistema Bitcoin.

Avtorja sistema Bitcoin je navdihnil članek, ki ga je leta 1998 napisal Wei Dai, po katerem si je zamislil sistem, v katerem bi psevdonimne osebe lahko sodelovale med seboj učinkoviteje, da bi se izognile posrednikom pri elektronskih transakcijah (Plassaras, 2013, str. 383).

Izraz Bitcoin je tvorjenka iz besede Bit, ki pomeni enoto informacije v digitalnem zapisu in besede Coin, kar označuje izraz za kovanec. Bitcoin<sup>1</sup> se nanaša tako na plačilni sistem in tehnologijo, kot tudi obračunsko enoto, ki ga plačilni sistem uporablja (Roux, 2015, str. 524).

Bitcoin je prva decentralizirana kriptovaluta na svetu (Brito & Castillo, 2013, str. 1), ki temelji na zasnovi matematičnih algoritmov. Temelji na odprtokodnem protokolu, po sistemu vrstniškega P2P omrežja, ki ni odvisen od centralne banke ali drugega regulatornega organa.

Antonopoulos (2014, str. 1) opredeli Bitcoin kot zbirko konceptov in tehnologij, ki tvorijo osnovo digitalnega denarnega ekosistema. Enota valute se imenuje bitcoin, ki se uporablja za shranjevanje in prenašanje vrednosti med udeleženci v Bitcoin omrežju. Bitcoin

---

<sup>1</sup> Bitcoin z veliko začetnico se uporablja za sistem (tehnologijo in skupnost), bitcoin z malo začetnico se uporablja za ime valute.

uporabniki komunicirajo med seboj s pomočjo Bitcoin protokola, predvsem preko interneta, čeprav se prenosi lahko opravijo tudi preko drugih prenosnih omrežij.

Ideja je temeljila na nekaj že predhodnih poizkusih uvedbe elektronskega denarja, kot sta b-denar ali HashCash, vendar pa je ustvarjena kot popolnoma decentraliziran elektronski denarni sistem, ki za emisijo ali potrjevanje transakcij ne potrebuje centralnega organa.

Ključna inovacija je uporaba sistema porazdeljenega računanja, imenovanega kot algoritem »Proof-Of-Work« (v nadaljevanju PoW), ki poteka po postopku globalne rešitve izračunov vsakih 10 minut, na podlagi dokazila o vložnem delu, da bi dosegli soglasje o stanju transakcij, s pomočjo decentraliziranega omrežja. To predstavlja rešitev pri problemu dvojne porabe, kjer se ena denarna enota lahko porabi dvakrat. Pred tem je bil problem dvojne porabe slabost dosedanjih poizkusov uvedbe digitalnih valut (Antonopoulos, 2014, str. 4).

Bitcoinovi so računalniške datoteke, podobno kot glasbene ali tekstovne datoteke, ki se lahko uničijo ali izgubijo, tako kot lahko izgubimo gotovino. Shranjeni so bodisi na osebнем računalniku ali jih uporabnik shrani pri ponudniku tovrstnih spletnih storitev. Pošiljanje nakazil drugim uporabnikom je podobno kot pošiljanje e-pošte preko interneta (Plassaras, 2013, str. 384).

Sistem deluje na podoben način kot BitTorrent protokol za izmenjavo datotek, kot so filmi, igre, glasba idr., preko omrežja. Deluje na globalni ravni in se lahko uporablja kot valuta za vse vrste transakcij, tako v virtualnem svetu kot tudi za plačilo pravih dobrin in storitev, pri čemer tekmuje s pravimi valutami, kot so denimo EUR ali USD (ECB, 2012, str. 21).

Tehnologija Bitcoin sistema je popolnoma nevtralna, ne pripada nikomur. Proces transakcij je popolnoma decentraliziran. Za razliko od tradicionalnega bančnega sistema ni mogoče zamrzniti sredstev na računu. Niti posameznik niti organizacija ne more manipulirati z algoritmom, saj gre za odprtokodni program, pri katerem je potrebno soglasje udeležencev.

Satoshi Nakamoto se je popolnoma umaknil iz javnosti aprila 2011, odgovornost za razvoj kode in omrežja pa prepustil skupini prostovoljcev. Kdo natanko se skriva pod psevdonimom Satoshi Nakamoto, kljub temu, da je avstralski podjetnik Craig Wright letos v začetku leta za BBC izjavil, da je on skrivnostni avtor (glej str. 28 za detajlnejše pojasnilo), še ni znano.

Vsekakor pa je izum Bitcoina prelomnica, ki je, lahko rečemo, ustvarila novo znanost na področju računalništva, ekonomije in ekonometrije (Antonopoulos, 2014, str. 4).

## 2.2 Bitcoin kot plačilno sredstvo

Mishkin (2004, str. 44) opredeljuje denar kot »vse, kar je splošno sprejeto kot plačilo za blago ali storitve ali poplačilo dolgov«. Ljudje trgujejo z različnimi oblikami denarja že tisoče let. Mnogo vrst dragocenih predmetov je v preteklosti že bilo uporabljenih kot menjalno sredstvo. V zgodnji eri so ljudje trgovali z žiti, živino, s školjkami in dragulji v zameno za ostale dobrine in storitve. Te oblike denarja so imele fizično, materialno obliko (Caetano, 2015, str. 2), značilno za tisto obdobje.

Decentralizirane oblike denarja, kot so plemenite kovine, zlato in srebro, obstajajo že več tisoč let. Njihova vrednost je priznana kot vrednost, zaradi njihove redkosti in fizičnih značilnosti (Pérez-Marco, 2016, str. 1). Skozi čas so blago zamenjale fiat valute. Fiat ali realna denarna valuta je vsako zakonito plačilno sredstvo, izdano in podprto s strani centralnih vladnih organov (Gup, 2014, str. 53).

Vrednost bitcoina ni podprta z nobenim blagom ali s plemenitimi kovinami, ki bi mu zagotavljale vrednost (Polasik, Piotrowska, Wisniewski, Kotkowski & Lightfoot, 2015, str. 16). Prav tako ni vezan na nobeno realno valuto na svetu. Menjalni tečaj se določi na podlagi ponudbe in povpraševanja na trgu (ECB, 2012, str. 21). Za razliko od drugih nacionalnih valut, ki jo podpirajo vlade in centralne banke, temelji njegova vrednost na zaupanju uporabnikov v matematične tehnološke rešitve. Nekaterim uporabnikom bitcoin predstavlja sredstvo nasprotovanja zaradi izgube zaupanja v tradicionalni finančni sektor, kar je tudi posledica nedavne finančne krize (Polasik et al., 2015, str. 16).

Teoretične zametke korenin bitcoina je mogoče najti že v Avstrijski ekonomski šoli in njihovi kritiki realnega denarja in intervencij vladnih organov in drugih finančnih institucij, kar po njihovem mnenju vodi do ponavljajočih se poslovnih ciklov in masivne inflacije. Friedrich A. Hayek je v svojem delu »Denacionalizacija denarja« iz leta 1976 menil, da vlade ne bi smele imeti monopola nad izdajo denarja. Predlagal je, da bi zasebnim bankam omogočili izdajo privatnega denarja, s katerimi bi se trgovalo po spremenljivih menjalnih tečajih. Večja konkurenca in maksimizacija dobička bi povečala učinkovitost monetarnega sistema (ECB, 2012, str. 22).

Vrsto let so že v uporabi virtualna sredstva, kot so kreditne in debetne kartice, namenjene plačilu transakcij in plačilu dobrin in storitev. Izdajatelji teh kartic so zasebna podjetja in ne vladni organi. Različne organizacije so že predstavile inovativne rešitve, kar je sčasoma pripeljalo do nastanka novih oblik denarja (Mikołajewicz-Woźniak & Scheibe, 2015, str. 369).

Navedba Miltona Friedmana iz leta 1999: »Ena stvar, ki še vedno manjka, vendar se bo hitro razvila, je zanesljiv e-denar, metoda, s pomočjo katere bo preko interneta mogoče prenesti sredstva od osebe A do osebe B, ne da bi oseba A vedela za osebo B, ali oseba B

za osebo A. Takšna stvar se bo razvila preko interneta in to bo lažje za ljudi, ki uporabljajo internet«, je pokazatelj zametkov za prihodnji gospodarski razvoj (Eikmanns & Sandner, 2015, str. 1).

Denar je, ne glede na obliko, tradicionalno povezan s tremi različnimi funkcijami (ECB, 2012, str. 10), in sicer kot:

- sredstvo menjave: uporablja se kot posrednik v trgovini,
- obračunska enota: deluje kot merilec vrednosti in stroškov blaga, storitev, sredstev in obveznosti,
- hranilec vrednosti: lahko ga shranimo in uporabimo v prihodnosti.

Kot sredstvo menjave se šteje sredstvo, ki se uporablja za trgovanje z blagom ali s storitvami. Število trgovcev, ki sprejemajo bitcoin v zameno za svoje izdelke ali storitve, narašča iz dneva v dan. Bitcoin sprejemajo tudi večja podjetja, kot so Lamborghini, Microsoft, Dell, idr. S tega vidika je mogoče bitcoin priznati kot sredstvo menjave.

Funkcija obračunske enote je tesno povezana s funkcijo sredstva menjave. Sredstvo izpolnjuje ta vidik, če ga posamezniki uporabljajo za ekonomske izračune. Dokler sredstvo ni splošno sprejeto kot sredstvo menjave, je tudi malo verjetno, da se bo na splošno uporabljalo za določitev cene ali za ekonomske izračune.

Funkcija hranilec vrednosti pomeni, da mora denar ohranjati svojo kupno moč. Bitcoin ni, tako kot druge valute, podprt z blagom in sam po sebi nima prave vrednosti. Vrednost lahko pridobi le z zaupanjem v delovanje sredstva kot sredstva menjave in kot hranilca vrednosti. Dolgoročno gledano, se funkcija hranilca vrednosti uporabi zaradi omejene ponudbe novih enot.

Lahko torej sklenemo, da bitcoin, do neke mere, že danes ustreza opredelitvi denarja. Tako menita tudi Eikmanns in Sandner (2015, str. 1-7) in Van Alstyne (2014, str. 30-31), ki meni, da ima bitcoin vse tri lastnosti denarja. Dokler ga namreč ljudje sprejemajo za plačilo svojih izdelkov in storitev ter ima vrednost, merjeno v cenah, opravlja funkcije denarja kot plačilnega sredstva. Sprejem denarja je tisto, kar mu daje vrednost.

Po drugi strani Yermack (2014, str. 2) meni, da bitcoin ne izpolnjuje vseh kriterijev valute v skladu z ekonomskimi merili, temveč bolj spominja na špekulativne naložbe. Zaradi svoje deflacijske lastnosti ima bitcoin nizko likvidnost na trgu. Uporabniki kopičijo bitcoine v upanju, da se bo njegova vrednost s časom povečala (Tasca, 2016, str. 71), saj je količina bitcoinov v obtoku omejena z matematičnim algoritmom na skupno 21 milijonov (Polasik et al., 2015, str. 17).

Avtorji Böhme, Christin, Edelman & Moore (2015, str. 233) trdijo, da Bitcoin sistem v širšem smislu izvaja varianto Milton Friedmanovega » $k$ -odstotnega pravila«. Ta teorija navaja, da je optimalen način za nadzorovano inflacijo na dolgi rok rast denarja s fiksno stopnjo rasti  $k$  % letno, in sicer po stopnji, ki je enaka rasti realnega bruto družbenega proizvoda, ne glede na ciklično stanje gospodarstva (Peters, Panayi & Chapelle, 2015, str. 13). Bitcoin protokol je zasnovan na način, da ima omejeno končno količino izdajanja kovancev in gre proti fazi, ko je  $k=0$ . V prihodnosti pa je  $k$  lahko celo negativna, saj se bitcoini lahko nepovratno uničijo zaradi izgubljenih privatnih ključev uporabnikov. To pa poraja klasično vprašanje v monetarni politiki: kaj se zgodi, ko obseg gospodarstva raste z drugačno stopnjo rasti kot količina denarja? Po mnenju Krugmana bi fiksna počasna stopnja rasti ustvarila možnost deflacije, če bi se bitcoin bolj množično uporabljal (Böhme et al., 2015, str. 233-234).

Kritiki opozarjajo, da ga nekateri investitorji uporabljajo zgolj kot hranilec vrednosti, kar zmanjšuje njegovo učinkovitost kot medij izmenjave. Raziskava iz maja leta 2012 je pokazala, da je 73 % naslovov uporabnikov bitcoine le prejemale. Ratcliff v letu 2014 potrjuje to tezo in pravi, da je bilo okoli 11 % bitcoinov v 4 letih neuporabljenih na naslovih uporabnikov in 39 % več kot leto ni bilo uporabljenih. Kopičenje (angl. *hoarding*) lahko vodi do povečanja kupne moči valute, kar pomeni tveganje za pojav deflacijske spirale (Polasik et al., 2015, str. 17). Tasca (2016, str. 72) navaja, da je v letu 2016 kar 85 % vseh dosedaj ustvarjenih bitcoinov, kopičenih na računih uporabnikov.

Deflacijska spirala se nanaša na gospodarski razvoj, kjer lahko hitro rastoča deflacija vodi v propad valute. Deflacijo obravnavamo kot padec splošne ravni cen. To se lahko zgodi, kadar cene blaga in storitev, merjene relativno glede specifično mero, začno padati, vendar ne nujno kot posledica dejstva, da je vrednost blaga in storitev sama po sebi znižana, namesto tega lahko preprosto pride zaradi dejstva, ko se vrednost valute poveča. Deflacijska spirala izhaja iz situacije, ko se vrednost valute, v primerjavi z blagom v gospodarstvu, nenehno povečuje zaradi kopičenja. Uporabniki pričakujejo, da bodo lahko kupili več izdelkov za manj denarja v prihodnosti, kar pa zaradi pomanjkanja razpoložljivih enot valute, povzroči znižanje cen proizvodov, kar vodi v nadaljnje kopičenje (Peters et al., 2015, str. 13).

Kovancev, ki so bili izgubljeni bodisi zaradi pozabljenih zasebnih ključev ali uničeni, ni mogoče nadomestiti, kar predstavlja še dodatni dejavnik krčenja denarja v obtoku (Barber, Boyen, Shi & Uzun, 2012, str. 6).

Yermack (2014, str. 11) meni, da se bitcoin sooča s številnimi ovirami, da bi lahko postal obračunska enota. Morda je najbolj resna ovira, da bitcoin postane razširjena obračunska enota po Yermacku (2014, str. 12-13), relativno visok strošek za 1 bitcoin v primerjavi z vrednostjo večine vsakdanjih izdelkov in storitev. Njegova visoka vrednost in deljivost na 8 decimalnih mest povzroči, da morajo trgovci cene za večino blaga prilagajati na več

decimalnih mest, računovodske programske opreme pa večinoma sprejmejo le dve decimalni mesti za ceno izdelka ali storitve.

Vendar pa so se nekateri ponudniki storitev bitcoina temu že prilagodili. Caetano (2015, str. 9) navaja, da nekateri ponudniki spletnih denarnic omogočajo uporabnikom, da v svojem računu spremenijo enoto bitcoin v manjše enote, kar lahko v nekaterih primerih, zlasti ko gre za več decimalnih mest, olajša izračune in računovodske prikaze.

Dodaten problem se pojavi, ko morajo trgovci potrošniku preračunati ceno v bitcoinih, saj se le-te pri različnih menjalnicah gibljejo zelo različno; razlike v cenah med menjalnicami so se v preteklosti gibale tudi do 7 %. Trgovci se sicer lahko poslužujejo portalov, ki prikazujejo povprečno vrednost bitcoina na več spletnih menjalnicah v zadnjih 24 urah, pri čemer ob tem niso zajeti tudi dejanski stroški, ki jih imajo trgovci in potrošniki v zvezi z nakupom oz. prodajo bitcoinov (Yermack, 2014, str. 12).

Nadaljnja slabost je nestabilnost valute, katere vrednost se dnevno spreminja, zato morajo trgovci, ki sprejemajo plačila v tej valuti, le-to pogosto preračunavati, kar povzroči dodatne stroške za trgovce in zmedo pri potrošnikih (Yermack, 2014, str. 11). Vendar pa se tudi na tem področju tehnologija nenehno razvija. Odpirajo se nova podjetja, ki trgovcem in kupcem olajšajo prodajo oz. nakup. Tako so trgovcem na voljo plačilni posredniki, ki jim olajšajo sprejem valute v bitcoinih. Tovrstni posredniki omogočajo trgovcem, da sprejmejo plačilo v bitcoinih, ne da jih dejansko prejeli. Protivrednost transakcije se zamenja v lokalno valuto, s čimer se trgovci izognejo tveganju izgube vrednosti zaradi menjave ali posedovanja bitcoinov. Najbolj znana ponudnika takšnih storitev sta Coinbase in BitPay (Luther & White, 2014, str. 5-6) v Združenih državah Amerike (v nadaljevanju ZDA) in Coinify v Evropi (Swan, 2015, str. 4). Provizije za tovrstne storitve se gibljejo okoli 1 %, kar je znatno manj od provizij, povezanih z drugimi elektronskimi plačili, kot so kreditne kartice (Brito, Shadab & Castillo, 2014, str. 157-158).

Trgovcem so na voljo tudi že pripomočki za avtomatsko menjavo valut, ki omogočajo prodajalcem, da določijo ceno v lokalni valuti, ki se ob nakupu pretvori v bitcoine po tržni menjalni vrednosti, kar je zlasti primerno za spletne trgovce. Januarja 2014 je na trg prišel izdelek BitTag, ki rešuje problem v tradicionalnih prodajalnah. BitTag je manjša naprava, ki prikazuje vrednost nekega artikla v obeh valutah, na majhnem OLED zaslonu. Cena posameznega artikla se posodablja preko Bluetooth tehnologije, z nizko porabo energije (Luther & White, 2014, str. 5).

Seznam trgovcev, ki svojim uporabnikom omogočajo plačevanje dobrin in storitev s to valuto, je raznolik. Bitcoin sprejemajo tako ponudniki internetnih storitev, spletnih trgovin, materialnih dobrin (npr. oblačil, dodatkov, elektronike, knjig, itd.), kot tudi poslovnih in strokovnih storitev ter turističnih potovanj (ECB, 2012, str. 21). V Sloveniji na dan 3. 7.

2016 valuto bitcoin sprejema 59 trgovcev oz. ponudnikov dobrin in storitev (Coinmap, 2016).

Statistični podatki kažejo, da se število transakcij skokovito povečuje. Od leta 2011, ko je bilo v omrežju opravljenih okoli 1.000 transakcij dnevno, se je število transakcij do leta 2016 povečalo skoraj na 300.000 dnevno. Nominalna vrednost dnevnega obsega transakcij se trenutno giblje v povprečju med 200 USD in 300 milijonov USD (Tasca, Liu & Hayes, 2016, str. 2).

*Slika 2: Prikaz števila dnevnih nakazil*



*Vir: Blockchain Charts, 2016.*

## **2.3 Tehnične značilnosti**

### **2.3.1 Delovanje Bitcoina**

Tehnologija sistema Bitcoin temelji na odprtokodnem protokolu P2P omrežja, brez centralnega nadzornega organa, ki bi potrjeval transakcije. Transakcije potrjujejo anonimni člani skupnosti, znani pod imenom rudarji (angl. *miners*) (Allen, 2015, str. 10). Znotraj omrežja je vsak udeleženec enakopravni član in je neposredno povezan z drugimi udeleženci preko omrežja, brez posrednikov (Eikmanns & Sandner, 2015, str. 4).

Sistem Bitcoin temelji na zapletenih matematičnih algoritmih kriptografskega sistema (Szczepeński, 2014, str. 2), ki skrbi za varno prenašanje podatkov med udeleženci sistema. Bitcoin za svoje delovanje uporablja kriptografsko zgoščevalno funkcijo (angl. *Hash*), imenovano SHA 256, sestavljeno iz niza črk in števil (Caetano, 2015, str. 131).

Vsak blok v verigi blokov predstavlja zgoščevalno funkcijo, ki se generira na podlagi SHA 256 kriptografskega zgoščevalnega algoritma v glavi bloka. Vsak blok se preveri na

podlagi prejšnjega bloka. Zaporedje zgoščenih vrednosti se navezuje na prejšnji blok v verigi blokov. Blok vsebuje podatkovno strukturo več transakcij. Povprečni blok vsebuje več kot 500 transakcij (Antonopoulos, 2014, str. 164).

Vsak blok v verigi blokov vsebuje sklop vseh transakcij v bloku, z uporabo Merklovega drevesa (angl. *Merkle Tree*). Merklovo drevo je podatkovna struktura, ki se uporablja za učinkovito združevanje in preverjanje celovitosti velikih sklopov podatkov oz. za združevanje transakcij v blok (Antonopoulos, 2014, str. 170).

Transakcije se med uporabniki potrjujejo na način, da oseba A, ki želi poslati osebi B bitcoine, pošlje sporočilo, imenovano transakcija v omrežje, ki vsebuje javni ključ osebe B in ga podpiše s svojim zasebnim ključem. Vsakdo v omrežju lahko preveri, da je oseba A s svojim digitalnim zasebnim ključem podpisala izmenjavo sredstev in tako oseba B postane novi lastnik bitcoinov. Transakcija se potrdi v naslednjem bloku v verigi blokov. Kriptografija zagotavlja, da se računalniki v omrežju posodablajo s preverjeno evidenco vseh transakcij v omrežju, kar preprečuje dvojno porabo in goljufije (Brito & Castillo, 2013, str. 5).

Vsaka transakcija se zabeleži v javno elektronsko knjigo nakazil, imenovano veriga blokov (angl. *Blockchain*). Vsaka nova transakcija se preveri na podlagi skupinske verige, s čimer se zagotovi, da enake transakcije niso bile že predhodno uporabljene. Preverjanje novih transakcij zagotavlja, da se bitcoini ne uporabijo dvakrat, s čimer se odpravi problem dvojne porabe. Kriptografski protokol zagotavlja, da udeleženci v omrežju Bitcoin delujejo s preverjenimi in posodobljenimi zapisi vseh transakcij znotraj omrežja, kar preprečuje dvojno porabo in goljufije. Uporabniki neposredno sklepajo posle med seboj, brez posredovanja tretje osebe. Globalno, P2P omrežje, sestavljeno iz več tisoč uporabnikov, prevzame mesto posrednika (Anning et al., 2015, str. 7-8). Vsak udeleženec lahko hrani podatke o vseh transakcijah v zgodovini valute na svetu. Zneski na posamičnem naslovu so javni. Vsakdo, ki pozna naslov, se lahko seznanj z zneskom v denarnici, vendar si lahko uporabnik zagotovi tajnost tako, da nihče ne more povezati naslova z njegovo identiteto. Zneske lahko prepošilja le, kdor ima ključ za kriptografsko podpisovanje nakazil (Završnik, 2015, str. 1). Ker ima vsak udeleženec vpogled v javno elektronsko knjigo nakazil, so transakcije popolnoma pregledne in transparentne, nihče pa ne more povezati transakcije z uporabnikom, v kolikor ne pozna gesla, saj je uporabnikova identiteta zakrita z alfanumerično kodo. Dejansko bi lahko rekli, da je bitcoin bolj »psevdonimen« kot anonimen, saj se uporabniki skrivajo za kodo, pod gesli, transakcije pa so javne (Brown, 2016, str. 5).

Bitcoin protokol je odprtokoden sistem, kar pomeni, da lahko vsak razvijalec sistema predlaga spremembe za izboljšanje jedra protokola. Komunikacija glede novih predlogov poteka preko omrežnih kanalov, kjer uporabniki o teh predlogih razpravljajo in jih



testirajo. Za uvedbo novih sprememb je potrebno večinsko soglasje, spremembe pa so vključene v naslednjo različico programske opreme (Anning et al., 2015, str. 10).

Bitcoini se delijo na osem decimalnih mest. Najmanjša obračunska enota se imenuje Satoshi (Anning et al., 2015, str. 9-10), poimenovana po avtorju sistema Bitcoin, Satoshiju Nakamotu. Izražena je v 0.00000001 BTC (Caetano, 2015, str. 9). Te enote sledijo standardnemu decimalnemu sistemu. Pri izražanju bitcoin zneskov se lahko uporabljajo sledeče predpone:

*Tabela 3: Enote bitcoina*

<b>Enota</b>	<b>Okrajšava</b>	<b>Decimalna mesta</b>
bitcoin	BTC	1.0
bitcent ali centi-bitcoin	cBTC	0.01
millibit ali milli-bitcoin	mBTC	0.001
bit ali micro-bitcoin	μBTC	0.000001
satoshi	-	0.00000001

*Vir: Caetano, R., Learning Bitcoin, 2015, str. 9.*

Če upoštevamo zgornjo tabelo, lahko vrednosti namesto več decimalk pišemo z uporabo predpone spredaj. Na primer: namesto 0.44234 BTC, lahko uporabimo 442.34 mBTC, kar je z vidika uporabnikov morda lažje. Nekateri ponudniki in spletne menjalnice so že sprejele to obliko zapisa za prikaz stanja na računih uporabnikov, ki je morda bolj sprejemljiva in prijaznejša do uporabnika. Caetano (2015, str. 9) navaja, da je bila skodelica kave v času pisanja publikacije, vredna 10 mBTC.

### **2.3.2 Rudarjenje oz. ustvarjanje novih bitcoinov**

Bitcoin omrežje je odvisno od uporabnikov, ki porabljajo računalniške moči in elektriko ter skrbijo za varno omrežje, za vzdrževanje, posodabljanje in potrjevanje transakcij v verigi blokov. Ti uporabniki so poznani pod imenom rudarji. Lahko bi se reklo, da so nekakšen bančni referent v omrežju, ki skrbijo za potrjevanje transakcij in beleženje v javno knjigo nakazil. Rudarji so za svoje delo in porabo stroškov, ki pri tem nastanejo, nagrajeni z novo ustvarjenimi bitcoini. Bitcoini se ustvarjajo oz. kopljejo s pomočjo zapletenih matematičnih algoritmov, ki preverjajo in potrjujejo transakcije v verigi blokov (Anning et al., 2015, str. 9-10). Rudarji med seboj tekmujejo v reševanju kompleksnih matematičnih izračunov. Prvi veljaven izračun je sprejet kot potrjen blok v členu verige blokov (Brown, 2016, str. 6). Bitcoini so ustvarjeni vsakič, ko uporabnik potrdi nov blok. Stopnja ustvarjanja blokov je približno šest na uro (Szczepeński, 2014, str. 4). Težavnost PoW je določena s spreminjajočim se povprečnim številom ustvarjenih blokov na uro. Hitreje kot se bloki ustvarjajo, bolj se težavnost povečuje (Nakamoto, 2008, str. 3). Stopnja težavnosti rudarjenja se izračuna na podlagi stopnje, po kateri so bili potrjeni zadnji bloki.

V kolikor je hitrost potrjevanja manjša kot 10 minut, se težavnost potrjevanja povečuje. V kolikor pa je stopnja izračuna zadnjega potrjenega bloka več kot 10 minut, se stopnja težavnosti zmanjša. Zahtevnost se posodablja vsakih 2.016 blokov (Caetano, 2015, str. 97). Število ustvarjenih bitcoinov za potrditev bloka je programirano tako, da se zmanjšuje s 50 % zmanjšanjem nagrade vsake štiri leta. Takšen algoritem je bil uporabljen zato, ker spominja na hitrost, s katero se lahko izkoplje pravo blago, kot je npr. zlato (Szczepeński, 2014, str. 4). Nagrada za novo ustvarjeni blok v verigi blokov je sprva znašala 50 bitcoinov. Novi blok se ustvari vsakih deset minut. Ko se v približno štirih letih ustvari 210.000 blokov, se nagrada razpolovi (Anning et al., 2015, str. 9-10).

Od 1. marca 2009 do 28. novembra 2012 je bilo na dan proizvedenih 7.200 bitcoinov. Od 28. novembra 2012 do 9. julija 2016 je nagrada za novo ustvarjeni blok znašala 25 bitcoinov, pri čemer je bilo proizvedenih v povprečju 3.600 bitcoinov dnevno. Od 9. julija 2016 se je nagrada za novo ustvarjeni blok razpolovila in sedaj znaša 12,5 bitcoinov oz. 1.800 bitcoinov, ki jih skupno v povprečju na dan proizvedejo rudarji. Skupinska nagrada rudarskih bazenov se zmanjšuje, hkrati pa rudarji predstavljajo pomemben segment v Bitcoin sistemu, saj skrbijo za sistem potrjevanja transakcij in oskrbo s kovanci (Tasca et al., 2016, str. 37).

Bitcoin sistem je zasnovan na način, da je najvišje možno število vseh ustvarjenih bitcoinov omejeno na 21 milijonov, kar bo po predvidevanjih doseženo leta 2140 (Anning et al., 2015, str. 9-10).

Proces rudarjenja sčasoma postaja vse bolj zapleten in zahteven, ker so procesirane baze podatkov večje. Na začetku je bil proces rudarjenja precej preprost. Da bi se transakcija uporabnika hitreje vključila v potrjevanje, lahko uporabniki nakažejo rudarjem tudi provizijo, kot nagrado za njihovo delo in porabljeno električno energijo (Szczepeński, 2014, str. 3). Tovrstne provizije so prostovoljne, odvisne od posameznega uporabnika. Lahko so zelo nizke, ali se uporabniki odločijo, da ne nakažejo provizije rudarjem, kot nagrado za njihovo delo. Vendar pa je večja verjetnost, da bo višja provizija rudarjem spodbuda le-tem, da transakcijo prednostno uvrstijo v nov blok. Tako višje provizije rudarjem s strani uporabnikov običajno zagotovijo, da se njihova transakcija prej potrdi (Pérez-Marco, 2016, str. 3).

Po nekaterih ocenah rudarji porabijo bistveno več denarja za elektriko in računalniško opremo, ki je potrebna za izračune, kot pa s tem pridobijo koristi. Zaradi tega uporabniki pogosto združijo več računalnikov skupaj in se povezujejo v nekakšne bazene, z namenom, da bi povečali svoje računalniške zmogljivosti, pri čemer si razdelijo tudi nagrade. Dosedaj še nikomur ni uspelo, da bi v takšen bazen privabil toliko računalniških zmogljivosti, da bi prevzel nadzor nad več kot 50 % celotnega omrežja. V kolikor bi se to zgodilo, bi obstajalo tveganje, da bi bila celovitost celotnega sistema ogrožena, saj bi to lahko omogočilo tudi

transakcije, ki bi jih bilo mogoče razveljaviti, v sistemu pa bi se lahko transakcije lažno potrdile (Szczepański, 2014, str. 4).

Izvorna koda Bitcoina je bila zasnovana na način, da proizvede določen znesek v določenem časovnem obdobju. Vendar pa je zaradi svoje priljubljenosti in zaradi vse večjega zanimanja med rudarji, ki so v tem videli priložnost za hiter zaslužek, prišla do stopnje rasti hitreje, kot je večina pričakovala. Razvijalci sistema se ukvarjajo z vprašanjem, kako odpraviti to težavo. Mnenja o tem so deljena. Ena skupina razvijalcev se zavzema za podvojitve velikosti blokov, kar bi učinkovalo le na kratek rok. Druga skupina razvijalcev se zavzema za ponovni zapis zasnove osnovnega protokola, ki bi imel veliko več blokov, ob tem, da bi stari, dosedaj že proizvedeni bitcoini bili združljivi z novimi (Thomas, 2016).

### **2.3.3 Nakup in prodaja bitcoinov**

Obstaja več načinov za pridobitev bitcoinov. Ena izmed možnosti je nakup preko spletnih menjalnic v zameno za tradicionalne valute, druga možnost je pridobitev bitcoinov v zameno za blago ali storitve v transakcijah, tretja možnost pa je preko rudarjenja (Eikmanns & Sandner, 2015, str. 6). Uporabnik pa lahko kupi bitcoine tudi preko avtomatov, ki so namenjeni tovrstnim menjavam denarnih sredstev.

Za povezavo z Bitcoin omrežjem mora uporabnik najprej na svoj računalnik prenesti programsko opremo (Murphy et al., 2015, str. 2).

### **2.3.4 Bitcoin denarnica**

Za plačevanje dobrin in storitev mora uporabnik imeti bitcoin denarnico. Denarnica je del programske opreme, ki uporabnikom omogoča dodeljevanje bitcoin naslovov za shranjevanje, pošiljanje in prejemanje bitcoinov (Virtual currency: Risks and Regulation, 2014, str. 10). Vsakdo, ki ima dostop do bitcoin denarnice, lahko ustvari neomejeno število naslovov. Bitcoin naslovi imajo običajno 26 - 35 znakov, ki vsebujejo velike in male črke ter številke. Primer naslova: 1MgErLiH1DuGMrd58fuL4CLQHc4VSboqKn (Caetano, 2015, str. 9-10). Denarnice sestojijo iz parov javnega in zasebnega ključa (Antonopoulos, 2014, str. 85). Naslov javnega ključa je kot nekakšen poštni nabiralnik, v katerega lahko vsakdo odda pismo, vendar pa le lastnik poseduje ključ za upravljanje s sredstvi v denarnici (Allen, 2015, str. 9). Naslovi se dejansko izračunajo na podlagi javnega ključa (Antonopoulos, 2014, str. 70). Antonopoulos (2014, str. 61) primerja javni ključ s številko bančnega računa, zasebni ključ pa je podoben analogiji tajne PIN številke ali podpisa na bančnem čeku, ki zagotavlja nadzor nad računom. Zasebni ključ se uporablja za podpisovanje transakcij (Pérez-Marco, 2016, str. 3). Preko zasebnega ključa, ki ga mora skrbno varovati, uporabnik dostopa do svojih sredstev. Zasebni ključi so dolgi nizi naključnih znakov, ki se generirajo s pomočjo programske opreme. Iz zasebnega ključa se

lahko ustvari le en naslov in tako je zasebni ključ nekakšno geslo za dostop do uporabnikovega bitcoin naslova. Zasebni ključi so običajno skriti v denarnici, uporabniki pa jih lahko običajno tudi natisnejo na papir (Caetano, 2015, str. 15).

Zasebni ključi največkrat vsebujejo 51 znakov, ki se začnejo s številko 5. Primer zasebnega ključa: 5Jd54v5mVLvyRsjDGTFbTZFGvwLosYKayRosbLYMxZFBLfEpCS7. Bitcoin denarnica je torej nekakšna zbirka naslovov in zasebnih ključev (Caetano, 2015, str. 16).

Vloga bitcoin denarnice je podobna klasični denarnici, v kateri hranimo nacionalno valuto, le da je ta zapis v elektronski obliki. Tehnično gledano se bitcoin valute dejansko ne shranjujejo. Gre za uporabo digitalnih varnostnih ključev, ki se uporabljajo za dostop do javnih naslovov in za izvedbo transakcije (Coindesk, 2016).

Glede na način shranjevanja, ločimo denarnice na t.i. vroče denarnice (angl. *hot wallet*), ki se nanašajo na spletno denarnico in se uporabljajo za vsakodnevne pologe in dvige, ter t.i. hladne denarnice (angl. *cold storage*), kjer so zasebni ključi shranjeni brez povezave do spleta (Caetano, 2015, str. 72).

Bitcoin denarnice obstajajo v različnih oblikah in vsaka deluje na svojstven način. Obstaja pet glavnih oblik digitalnih denarnic (Coindesk, 2016).

**Namizne bitcoin denarnice** (angl. *Desktop wallets*) – gre za programe oz. aplikacije, ki se jih namesti na osebne računalnike uporabnikov in so povezani z delujočo mrežo Bitcoin sistema. Uporabnikom omogoča popolni nadzor nad bitcoin denarnico in njihovih zasebnih ključev. Uporaba tovrstne denarnice vključuje tudi nekatera tveganja, kot so okvare strojne opreme, računalniške viruse ter nepooblaščen dostop. Pred namestitvijo denarnice je potrebno zagotoviti varnost pred zlonamernimi napadi (Caetano, 2015, str. 22-23).

**Spletne bitcoin denarnice** (angl. *Online wallets*) – omogočajo shranjevanje zasebnih digitalnih varnostnih ključev na spletu, na računalniku, ki ga nadzira nekdo drug, ne lastnik denarnice. Delujejo preko spletnega brskalnika ali mobilne aplikacije. Nekateri ponudniki omogočajo povezavo z namiznimi in mobilnimi bitcoin denarnicami. Prednost tovrstnih denarnic je v tem, da se do njih lahko dostopa od koderkoli, ne glede na napravo, ki se jo za to uporablja. Pomanjkljivost pa je, da če denarnica ni pravilno uporabljena, lahko organizacija, ki upravlja spletno stran, upravlja tudi z digitalnimi zasebnimi ključi takšne denarnice (Coindesk, 2016).

Izgubljenih zasebnih ključev ni mogoče obnoviti. Nekateri ugledni ponudniki spletnih denarnic so že sprejeli potrebne ukrepe za zaščito zasebnih ključev. Večina ponudnikov spletnih denarnic uporablja tehniko, imenovano »hladno shranjevanje«, kar pomeni, da so zasebni ključi fizično shranjeni v trezorju (Caetano, 2015, str. 16-17).

**Mobilne bitcoin denarnice** (angl. *Mobile wallets*) – gre za aplikacije, ki se jih namesti na mobilne naprave, kot so pametni telefoni. Uporabnikom omogočajo nakup dobrin ali storitev v realnem svetu, in sicer v trgovinah, ki omogočajo plačevanje s to virtualno valuto. Mobilno bitcoin denarnico je možno namestiti tudi na pametne ure, ki delujejo na osnovi operacijskega sistema Android (Coindesk, 2016).

**Mehanske bitcoin denarnice** (angl. *Hardware wallets*) – so namenske fizične naprave, na katere se shranijo digitalni zasebni ključi denarnice, pri čemer te naprave niso povezane z internetom. Na voljo so v zelo majhnem številu (Coindesk, 2016).

**Papirnate bitcoin denarnice** (angl. *Paper wallets*) – so dokumenti v papirni obliki, ki vsebujejo kopijo javnega naslova in zasebnega ključa, v obliki QR kode. Prednost teh denarnic je v tem, da zasebni ključi niso nikjer shranjeni v digitalni obliki in tako ne morejo biti podvrženi kibernetškemu napadu ali okvaram strojne opreme (Coindesk, 2016).

### 2.3.5 Bitcoin avtomati

Gre za avtomatsko napravo, ki se uporablja za izmenjavo fiat valute v valuto bitcoin. Obstajajo enosmerne naprave, kjer lahko uporabnik kupi bitcoine in dvosmerne naprave, kjer lahko uporabnik kupi in proda bitcoine (FATF, 2015, str. 44).

Po podatkih spletne strani History of Bitcoin (2016) je prvi bitcoin avtomat na svetu začel obratovati dne 2. maja 2013, v kraju San Diego, Kalifornija. Ostala literatura navaja postavitev prvega bitcoin avtomata oktobra 2013 v Kanadi.

Po podatkih spletne strani Coin ATM radar (2016) je bilo na dan 25. maja 2016 na svetu postavljenih 669 avtomatov, ki menjajo virtualne valute. V svetovnem merilu se Slovenija z devetimi postavljenimi avtomati uvršča na deseto mesto na svetu.

Provizije za menjavo realne valute v valuto bitcoin preko tovrstnih avtomatov so zelo visoke. Po podatkih spletne strani Coin ATM Radar (2016) je bila na dan 30. avgusta 2016 izračunana povprečna stopnja provizije 7,13 %, v svetovnem merilu. Povprečna stopnja provizije za nakup bitcoinov na tovrstnih avtomatih dosega okoli 7,79 %, povprečna stopnja provizije za prodajo za tiste avtomate, ki to omogočajo, je 5,57 %. Provizije se zelo razlikujejo od države do države ter so odvisne od ponudnika avtomata.

## 2.4 Kronologija pomembnejših dogodkov

Virtualna valuta bitcoin ima relativno kratko zgodovino, pa vendarle se je od njenega nastanka do danes zgodilo nekaj mejnikov, ki so vplivali na razvoj in njeno delovanje (History of Bitcoin, 2016).

Leto 2008:

- 18. avgusta 2008 je bila registrirana spletna domena z naslovom Bitcoin.org,
- 31. oktobra 2008 je bil objavljen dokument z naslovom A Peer-to-peer Electronic Cash System, v katerem avtor pod psevdonimom Satoshi Nakamoto, opiše protokol, po katerem deluje sistem Bitcoin.

Leto 2009:

- 3. januarja 2009 je bil ustvarjen izvorni blok (angl. *The Genesis Block*), ter ustvarjenih prvih 50 bitcoinov, s katerimi so zagnali plačilno omrežje,
- 9. januarja 2009 je bila objavljena prva verzija programske opreme 0.1, po kateri je določeno skupno število vseh novo ustvarjenih bitcoinov na 21 milijonov,
- 12. januarja 2009 je bila izvedena prva bitcoin transakcija, med Satoshi Nakamoto in Hal Finneyjem, kriptografskim programerjem,
- 5. oktobra 2009 je New Liberty Standard objavil prvi menjalni tečaj, po katerem je bila določena začetna vrednost valute bitcoin, in sicer po tečaju 1 USD = 1.309,03 BTC. Razmerje je bilo določeno na podlagi stroškov elektrike, ki ga računalnik porabi, da ustvari nove bitcoine.

Leto 2010:

- 6. februarja 2010 je bila ustanovljena prva spletna menjalnica za izmenjavo bitcoin valute,
- 22. maja 2010 je bila izvedena prva prava transakcija, v kateri je programer s Floride, Laszlo Hanyecz, na Bitcoin Forumu, ponudil za pizzo 10.000 BTC, kar je takrat znašalo približno 25 USD,
- 17. julija 2010 je bila ustanovljena borza Mt. Gox, ena izmed vidnejših spletnih borz za trgovanje z virtualnimi valutami,
- 15. avgusta 2010 je bila zaznana prva večja ranljivost bitcoin protokola, ko se je v transakciji generiralo preko 184 milijonov bitcoinov. To velja za edino večjo ranljivost protokola. Napaka je bila zaznana in v nekaj urah je bila transakcija izbrisana,
- oktobra 2010 FATF objavi prvo opozorilo glede uporabe novih plačilnih metod za pranje denarja oz. financiranje terorizma,

- 6. novembra 2010 tržna kapitalizacija preseže 1 milijon USD. Vrednost menjave na spletni borzi Mt. Gox je dosegla ceno 0,50 USD za BTC.

Leto 2011:

- Leta 2011 začne poslovati spletna tržnica, imenovana Silk Road, ki je postala največja spletna trgovina za nakup in prodajo drog in drugih nelegalnih storitev,
- 28. januarja 2011 se je z generiranjem bloka 105000 ustvarilo 5,25 milijonov bitcoinov, od skupno vseh možnih 21 milijonov, kar predstavlja več kot 25 % vseh možnih enot bitcoin valute,
- 9. februarja 2011 je bitcoin na spletni menjalnici Mt. Gox prvič dosegel valutno razmerje 1 USD/BTC,
- 23. aprila 2011 je bitcoin na spletni menjalnici Mt. Gox dosegel pariteto z evrom,
- 14. junija 2011 je WikiLeaks pričel s sprejemanjem donacij v valuti bitcoin.

Leto 2012:

- 28. novembra 2012 se je nagrada za novo ustvarjeni blok razpolovila. Iz takratnih 50 bitcoinov za blok je od takrat dalje nagrada znašala le še 25 bitcoinov.

Leto 2013:

- 18. marca 2013 je FinCEN podala svoje stališče glede virtualnih valut,
- 28. marca 2013 je tržna kapitalizacija dosegla 1 milijardo USD,
- 2. maja 2013 je bil predstavljen prvi bitcoin avtomat na svetu, v kraju San Diego, Kalifornija,
- 2. oktobra 2013 je FBI (angl. *Federal Bureau of Investigation*) zaprl Silk Road, razvpito tržnico, kjer se je trgovalo s prepovedanimi drogami in z drugimi nelegalnimi dobrinami in storitvami ter zasegel bitcoine v vrednosti 3,6 milijonov USD,
- 19. novembra 2013 je vrednost bitcoina preseгла 1.000 USD, po zasedanju ameriškega senata,
- 21. novembra 2013 je začela Univerza na Cipru, kot prva univerza, sprejemati bitcoin kot plačilno sredstvo,
- 5. decembra 2013 je Kitajska centralna banka finančnim institucijam prepovedala uporabo bitcoina.

Leto 2014:

- 28. februarja 2014 je največja spletna menjalnica Mt. Gox po izgubi večjega števila bitcoinov v vrednosti 450 milijonov USD, objavila bankrot (Bitcoin History, 2016),

- 17. julija 2014 The New York State Department of Financial Services izda predlog za Bitlicenco (angl. *BitLicense*).

Leto 2016:

- 2. maja 2016 je avstralski podjetnik Craig Wright za BBC podal izjavo, da je on idejni vodja Bitcoina, ki se je skrival za psevdonimom Satoshi Nakamoto. Pri razvoju naj bi sodelovala skupina programerjev, med njimi tudi znani kriptograf Hal Finney (BBC, 2016). Novica kasneje v medijih ni bila potrjena in tako še vedno obstajajo dvomi o pravem avtorju,
- 9. julija 2016 se je nagrada za novo ustvarjeni blok razpolovila. Iz prejšnjih 25 bitcoinov znaša nagrada rudarjem le še 12,5 bitcoinov (Huš, 2016).

## 2.5 Prednosti in pomanjkljivosti

### 2.5.1 Prednosti

Prednosti, ki jih prinaša revolucija v plačilnem sistemu virtualne valute bitcoin, so številne. Sistem je zasnovan na način, da uporabnikom omogoča zasebnost, preglednost nad transakcijami, omogoča hitrejša in cenejša nakazila, zagotavlja varnost pošiljanja nakazil, prav tako pa sredstev na računih uporabnikov ni mogoče zamrzniti s strani vladnih organov. Prav tako odpravlja možnost dvojne porabe sredstev, ki ga do sedaj ni bilo mogoče rešiti brez posredovanja tretje osebe. Posamezne prednosti so opisane v nadaljevanju.

**Anonimnost:** ena izmed prednosti valute bitcoin je njegova anonimnost. Uporabniki, ki imajo valuto bitcoin v elektronski denarnici, lahko opravijo storitve plačevanja brez identifikacije. Vendar pa je vidik anonimnosti privlačen tudi kot plačilno sredstvo za nakup nedovoljenih dobrin in storitev.

**Transparentnost:** ena izmed ključnih prednosti virtualne valute bitcoin je, da so vse transakcije javno dostopne in preverljive v elektronski knjigi, imenovani »blockchain«, kar omogoča neprimerljivo večjo preglednost in sledljivost (Guadamuz & Marsden, 2015, str. 9).

**Hitrost transakcij:** plačila preko sistema Bitcoin so običajno veliko hitrejša od drugih elektronskih plačil (Colley: *The Regulation of Virtual, Digital and Crypto-currencies*, 2015, str. 2). Medtem ko lahko transakcije mednarodnih nakazil trajajo tudi nekaj dni, da jih finančni posredniki odobrijo, transakcije v sistemu Bitcoin potrebujejo za potrditev približno 10 minut (Brito et al., 2014, str. 151).



**Nižji stroški transakcij:** čeprav bi po teoriji zasnove lahko bile transakcije med vsemi strankami brez plačil, ima sistem običajno provizijo, ki se razlikuje od izmenjave do izmenjave. Strošek transakcij gre običajno rudarjem, kot nagrada za spodbudo. Kljub tem provizijam oz. napitninam, pa se valuta bitcoin še vedno lahko postavlja z najnižjimi transakcijskimi stroški v primerjavi z drugimi plačilnimi metodami, pri katerih se ponekod zaračuna transakcija v povprečju okrog enega odstotka, medtem ko se pri nekaterih posredniških klirinških hišah, kot so Paypal in Western Union, zaračunavajo provizije tudi od dveh do štirih odstotkov. Vendar pa je na tem mestu potrebno opozoriti, da nekateri raziskovalci napovedujejo, da nizki stroški transakcij v prihodnosti ne bodo obstali (Guadamuz & Marsden, 2015, str. 9), saj se nagrada, ki jo pridobijo rudarji z ustvarjanjem novih kovancev, zmanjšuje, zaradi česar bi se lahko povečali stroški preverjanja transakcij (Murphy et al., 2015, str. 6).

Bitcoin **odpravlja problem dvojne porabe:** bitcoin predstavlja revolucijo v plačilnem sistemu tudi zato, ker odpravlja problem dvojne porabe, ki ga dosedaj ni bilo mogoče rešiti brez posrednika, kot so finančne institucije. Vsaka transakcija se zabeleži v javno verigo blokov, pri čemer se vsaka transakcija predhodno preveri znotraj omrežja, s čimer se zagotovi, da niso bili isti bitcoini že uporabljeni. P2P omrežje, sestavljeno iz več tisoč uporabnikov, prevzame mesto posrednika (Brito & Castillo, 2013, str. 4).

**Varnost:** virtualna valuta bitcoin za svoje delovanje uporablja 256-bitno verzijo varnega zgoščenega algoritma, ki je kriptični (kodirni) protokol, ustvarjen s strani ameriške agencije za nacionalno varnost (angl. *U.S. National Security Agency*). Protokol ohranja integriteto blockchain verige, prav tako se uporablja za podpisovanje transakcij in varnost bitcoin denarnic, saj temelji na matematičnih funkcijah, ki zagotavljajo, da so transakcije izvedene od lastnika denarnice. Prav tako podpis, od trenutka, ko je izveden, preprečuje ponarejanje transakcije s strani drugih udeležencev (Guadamuz & Marsden, 2015, str. 9).

**Varnost in nepovratnost transakcij z vidika trgovcev:** trgovci so zaščiteni pred izgubo plačila, saj ni avtomatskega povračila sredstev, v kolikor bi ga potrošnik želel izigrati, da ni prejel blaga ali da mu storitev ni bila opravljena (Colley: *The Regulation of Virtual, Digital and Crypto-currencies*, 2015, str. 2).

**Ni možnosti za cenzuro ali blokiranje računov:** bitcoin je decentralizirana valuta, ki nima centralne avtoritete ter ga ne izdaja noben finančni organ, kar pomeni, da je odporen na cenzuro (angl.  *censorship-resistant*) s strani vladnih avtoritet. Ker ni centralnega organa, ki bi nadzoroval omrežje, ni moč zamrzniti sredstev na računih uporabnika (Brito et al., 2014, str. 151). Ta vidik je še posebej zanimiv za območja s političnimi ali z gospodarskimi pretresi (Richter et al., 2015, str. 580).

**Spodbuda za finančne inovacije:** stvaritev bitcoin valute je vsekakor spodbudila inovacije na področju plačevanja, predvsem v smislu ustaljenih predstav o denarju, finančnih

institucijah in centralnosti bančnega sistema. Njegovi razvijalci celo trdijo, da naj bi virtualne valute nadomestile papirnati denar. Najbolj inovativen vidik Bitcoin sistema je razvoj »blockchain« tehnologije ali javne porazdeljene elektronske knjige nakazil, ki beleži vsako transakcijo v sistemu (Allen, 2015, str. 5). Tovrstni inovativni prispevek, ki so ga razvili razvijalci sistema Bitcoin, lahko služi kot platforma za finančne inovacije in druge inovativne rešitve, ki se lahko uporabi ne le za prenos valute, pač pa tudi za shranjevanje in obdelavo raznovrstnih evidenc in drugih storitev na področju plačil (Brito & Castillo, 2013, str. 18).

### 2.5.2 Pomanjkljivosti

Sistem Bitcoin pa ponuja tudi številne pasti z vidika uporabnika, ki se lahko sooča z veliko nestabilnostjo valute ter z izgubo sredstev, bodisi zaradi nepazljivosti, bodisi zaradi vdorov v sistem in spletne menjalnice. Anonimnost, ki po eni strani prinaša prednosti, pa se lahko zlorabi tudi v kriminalne namene. Pomanjkljivosti se kažejo tudi z ekonomskega in tehnološkega vidika, kot so energetska neučinkovitost stroškov rudarjenja in velikost verige blokov, ki se hitreje povečuje, kot je bilo sprva zasnovano. Posamezne slabosti so opisane v nadaljevanju.

**Nestabilnost valute:** vse od začetka trgovanja je vrednost bitcoina zelo nestabilna, kar je ena izmed večjih pomanjkljivosti sistema Bitcoin. Sistem zaradi narave decentraliziranosti nima nekega mehanizma, ki bi skrbel za urejeno ravnotežje. Kljub temu, da so se v zadnjem letu vrednosti vsaj na krajši rok umirile, pa še vedno med uporabniki, ki želijo trgovati s to valuto, vlada nelagodje.

**Izguba sredstev:** bitcoini dejansko obstajajo le kot datoteke v računalniku ali mobilni napravi, ki so dostopne z zasebnim, šifrirnim ključem. V kolikor uporabnik ustrezno ne zaščiti svojih sredstev, ključev ali naprave, na katerih hrani svoje imetje, so bitcoini za vedno izgubljeni (Guadamuz & Marsden, 2015, str. 13).

**Ni kreditiranja:** za kupovanje dobrin in storitev z bitcoini je potrebno imeti le-te na računu oz. v elektronski denarnici. Sistem ne dovoljuje kreditiranja, kar je lahko pomanjkljivost bitcoina, saj so potrošniki dandanes pogosto navajeni kupovati preko kreditnih kartic (Yermack, 2014, str. 11).

**Kraje in goljufije:** uporabniki niso zaščiteni pred vdori v računalnike, kjer hranijo svoje bitcoine. Če sredstva zaupajo spletnemu ponudniku denarnice ali spletni menjalnici, so le-te prav tako lahko žrtve vdorov v njihov sistem.

**Uporaba v nezakonite dejavnosti:** zaradi narave anonimnosti, ki jo sistem omogoča, se bitcoin zlorablja v nezakonitih dejavnostih, kot so trgovanje s prepovedanim blagom,

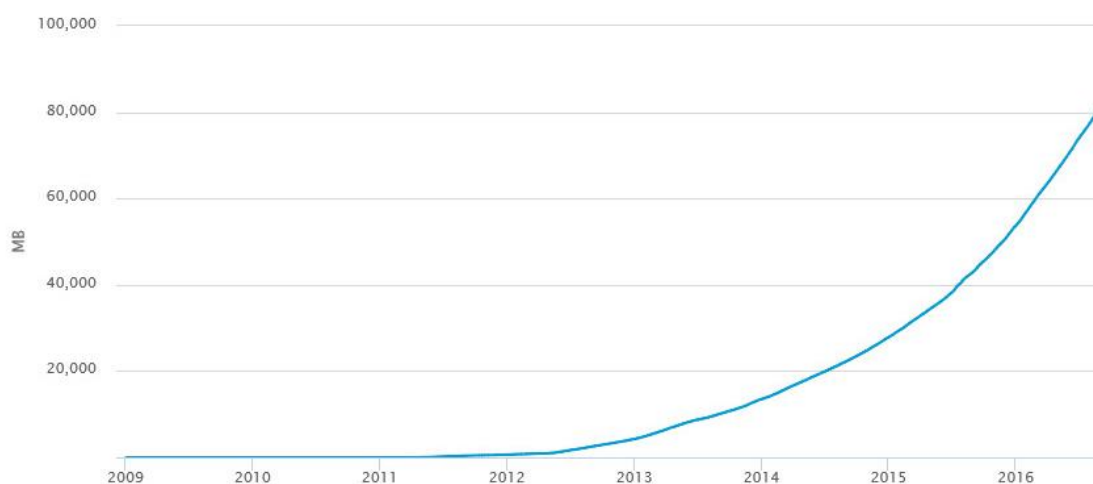
spodbuja igre na srečo, davčne utaje, pranje denarja, uporaba v terorističnih dejavnostih (Rogojanu & Badea, 2014, str. 112).

**Povečanje centraliziranosti sistema:** ena od temeljnih načel bitcoina je njegova decentralizirana narava. Rudarji, ki skrbijo za potrjevanje transakcij in emisijo novih kovancev, so razpršeni po vsem svetu. Ker pa proces rudarjenja postaja vse kompleksnejši, se rudarji povezujejo v nekakšne bazene, ki s skupnimi računalniškimi močmi skrbijo za omrežje. Obstaja bojazen, da če bi se združilo več kot 51 odstotkov rudarjev v konglomerat, sistem ne bi bil več decentraliziran in bi skupina obvladovala celoten sistem (Guadamuz & Marsden, 2015, str. 16). Obstaja nevarnost, da bi skupina, ki bi se združila v 51 % konglomerat, skušala uničiti sistem Bitcoina. Temu pravimo **Goldfinger napad**. Po mnenju avtorjev Kroll, Davey in Felten (2013, str. 13) obstajajo vsaj trije možni motivi za Goldfinger napad, in sicer bi lahko vladne ali druge institucije želele blokirati bitcoin transakcije z namenom uničiti sistem, da bi preprečile pranje denarja in uporabo bitcoina v nelegalne namene, drugi vidik bi lahko bil povezan s političnim ali z družbenim ciljem, v obliki socialnega protesta, s katerim bi napadalci zasedli omrežje bitcoina, tretji motiv pa je investicijski dobiček.

**Energetska neučinkovitost:** sistem Bitcoina zaradi čedalje težjega procesa rudarjenja in preverjanja transakcij zahteva ogromno računalniške moči in s tem porabo električne energije, pri čemer se poraja vprašanje upravičenosti takšne porabe z ekonomskega vidika (Guadamuz & Marsden, 2015, str. 16).

**Velikost verige blokov:** z naraščanjem transakcij se povečuje velikost verige blokov (angl. *Blockchain*), kar predstavlja oviro, saj se transakcije z naraščanjem verige blokov in s tem celotnega omrežja, potrjujejo počasneje (Guadamuz & Marsden, 2015, str. 17).

*Slika 3: Velikost verige blokov*



*Vir: Blockchain Charts, 2016.*

## 2.6 Spletne menjalnice za trgovanje z virtualnimi valutami

Platforme za menjavo virtualnih valut lahko obravnavamo kot »elektronske« menjalnice, ki trgujejo z virtualnimi valutami za tradicionalne valute (Evropska komisija, 2016). Spletne menjalnice omogočajo uporabnikom trgovanje z bitcoini z izmenjavo v tradicionalne valute ali ostale virtualne valute. Menjalni tečaj se oblikuje na podlagi ponudbe in povpraševanja, podobno kot na tradicionalnih finančnih trgih, provizija za izmenjavo pa se običajno giblje v razponu med 0,2 in 2 %. Nekatere spletne menjalnice ponujajo več naprednih orodij za trgovanje, kot sta limit ali preklic naročila (Böhme et al., 2015, str. 220). Do februarja leta 2014 je bila prevladujoča spletna menjalnica za nakup in prodajo bitcoinov japonska menjalnica Mt. Gox, ki je obvladovala kar 70 % tržni delež, nato je zaradi številnih vdorov v menjalnico in izgube sredstev razglasila stečaj.

Po propadu menjalnice Mt. Gox je tedaj vodilno mesto med spletnimi menjalnicami virtualnih valut zasedla menjalnica Bitstamp<sup>2</sup> (Yermack, 2014, str. 2). V marcu 2015 je trg obvladovalo sedem največjih menjalnic, kot so BTC China, OKCoin, Huobi, Bitfinex, LakeBTC, Bitstamp in BTC-e, ki so od oktobra 2014 do marca 2015 obvladovale 95 % tržišča (Böhme et al., 2015, str. 220).

Nekatere države so zakonsko uredile področje spletnih menjalnic. V ZDA spletne menjalnice delujejo kot menjalni posrednik, zato se morajo registrirati pri FinCEN<sup>3</sup>, kot ponudniki denarnih storitev ter plačati pristojbine in zavarovanja. Podobna pravila so uvedli tudi v nekaterih drugih državah. V Nemčiji se spletne menjalnice, ki upravljajo z depoziti v imenu strank, obravnavajo na podoben način kot poslovne banke, ki sprejemajo depozite, z minimalno kapitalsko zahtevo 5 milijonov EUR (Böhme et al., 2015, str. 220).

## 3 ZAKONSKA UREDITEV VIRTUALNIH VALUT

### 3.1 Zakonska ureditev virtualnih valut v svetu

V večini držav po svetu status virtualnih valut še ni definiran. Razvoj novih tehnologij poteka veliko hitreje, kakor se spreminja oz. prilagaja zakonodaja novim okoliščinam. V svetu se krog uporabnikov in ponudnikov storitev, ki omogočajo plačilo v virtualnih valutah, še posebno v bitcoinih, nezadržno veča, zato se vladne organizacije in bančni organi poskušajo opredeliti oz. zavzeti stališče do pojava tega fenomena, ki pridobiva

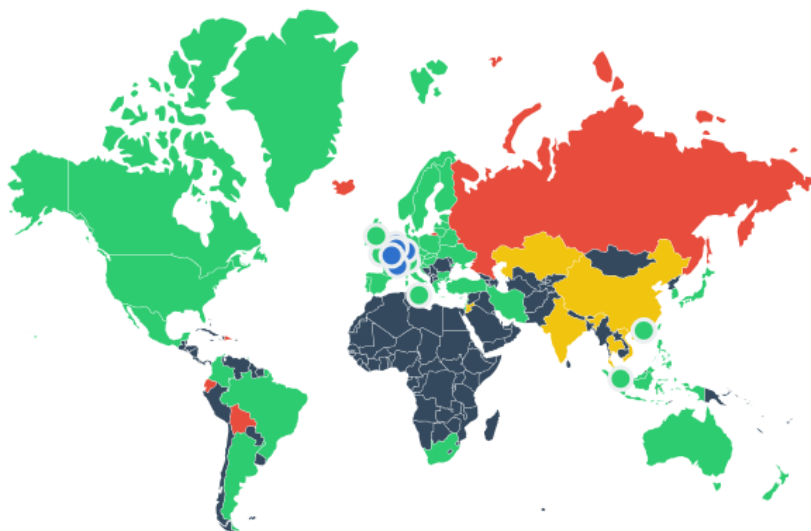
---

<sup>2</sup> Menjalnico Bitstamp sta v letu 2011 ustanovila Slovenca, v okviru družbe Bitstamp d.o.o. Sprva je delovala iz Slovenije, v letu 2013 sta sedež podjetja preselila v Veliko Britanijo, pod imenom Bitstamp Ltd. Svoje poslovalnice imajo tudi v Luxembourgu in New Yorku, ZDA.

<sup>3</sup> FinCEN (angl. *Financial Crimes Enforcement Network*) je Urad ameriškega Ministrstva za finance, ki zbira in analizira podatke o finančnih transakcijah v boju proti preprečevanju pranja denarja, financiranju terorizma in drugih finančnih kaznivih dejanj.

čedalje večje razsežnosti. Regulacija tega področja je bolj ali manj, še vedno prepuščena posameznim državam. Po podatkih spletne strani Bitlegal (2016) je v nekaterih državah uporaba bitcoina dovoljena, ponekod pogojno dovoljena, ponekod pa tudi prepovedana, kot je to razvidno s spodnje slike:

*Slika 4: Zakonska regulativa Bitcoina po svetu*



*Vir: Bitlegal, 2016.*

**Legenda:**

- Zeleno območje – uporaba bitcoina dovoljena
- Rumeno območje – uporaba bitcoina pogojno dovoljena
- Rdeče območje – uporaba bitcoina prepovedana
- Modro območje – neznan področje

**Prepovedane jurisdikcije:** od oktobra 2013 je nekaj držav popolnoma prepovedalo uporabo bitcoina: Bangladeš, Bolivija, Ekvador, Islandija, Kirgizistan (Swan, 2015, str. 6-7), Rusija in Dominikanska republika (Bitlegal, 2016).

Islandija ima glede uporabe virtualnih valut eno izmed najbolj restriktivnih politik na svetu. Centralna banka Islandije je v pisnem sporočilu pojasnila, da je trgovanje z valuto bitcoin prepovedano, na podlagi zakona države o deviznem poslovanju, ki opredeljuje splošne omejitve trgovanja s tujo valuto in pretok kapitala med Islandijo in drugimi državami. Določbe zakona se nanašajo tudi na trgovanje v valuti bitcoin za blago in storitve (Regulation of Bitcoin in Selected Jurisdictions, 2014, str. 11). Medtem ko je nakupovanje bitcoinov prepovedano, je prodaja še vedno dovoljena (Tasca, 2015, str. 47) .

V Rusiji je Urad generalnega tožilstva objavil, da so sistemi anonimnih plačilnih sredstev, vključno z bitcoinom, »nadomestek denarja« in so zato v Rusiji prepovedani (ECB, 2015, str. 31–32). Centralna banka Rusije je v januarju 2014 objavila informacije o virtualnih valutah, v katerih opozarja posameznike, pravne osebe in finančne institucije pred uporabo virtualnih valut v zameno za dobrine ali storitve ali menjavo v nacionalno ali druge valute in bo tako izmenjava teh valut nadzorovana s strani Ruske centralne banke zaradi potencialne vpletenosti uporabnikov v sumljive transakcije, na podlagi zakonodaje o preprečevanju pranja denarja in financiranja terorizma (FATF, 2015, str. 19). V pripravi je zakonodaja, ki predvideva globe za izdajatelje virtualnih valut (Bitlegal: Russia, 2016).

Med **pogojno dovoljene jurisdikcije** sodijo Kitajska, Tajska, Indonezija, Indija, Jordanija, Libanon, Tajvan, Vietnam (Tasca, 2015, str. 47-48) in Kazahstán (Bitlegal, 2016).

Na Kitajskem je vlada v decembru 2013 prepovedala bankam in finančnim institucijam trgovanje z bitcoini (Swan, 2015, str. 7). Hkrati je izdala opozorilo, da bitcoin ni valuta in se ne more uporabljati kot zakonito plačilno sredstvo. Prav tako predstavlja bitcoin tveganje za pranje denarja, zato so Kitajske oblasti utrdile nadzor nad spletnimi stranmi, ki se ukvarjajo s trgovanjem z bitcoini (Turpin, 2014, str. 363-364).

**Dovoljene jurisdikcije:** države, ki dopuščajo uporabo bitcoina, so ZDA, večina držav Južne Amerike, Evropske države, Kanada, Japonska in Avstralija (Tasca, 2015, str. 48).

Države povečini še razpravljajo o tem, ali uvrstiti bitcoin kot valuto ali kot premoženje ter kako ga obdavčiti. Nekatero državo, kot je na primer Velika Britanija, razvršča bitcoin kot valuto, zato ta ni predmet DDV, medtem ko v drugih državah, kot je na primer Avstralija, bitcoina niso mogli opredeliti kot valuto, zaradi obstoječe zakonodaje in je tako predmet obdavčitve, kot so blago in storitve (Swan, 2015, str. 7).

V ZDA Ameriški davčni urad (angl. *Internal Revenue Service*) obravnava bitcoin kot premoženje in ne kot valuto, kar pomeni, da so uporabniki bitcoina odgovorni za plačevanje davkov na kapitalske dobičke. Drugi ameriški vladni organi, vključno s FinCEN, SEC in drugimi bančnimi regulatorji, obravnavajo bitcoin kot valuto (Swan, 2015, str. 7).

Največji korak pri regulaciji ureditve virtualnih valut je v ZDA dosedaj uspelo organizaciji FinCEN in New York Department of Financial Services (v nadaljevanju NYDFS). FinCEN je v marcu leta 2013 izdala smernice za uporabo virtualnih valut, v katerih je opredelila, da menjalnice in administratorji oz. skrbniki virtualnih valut opravljajo denarne storitve podjetja in se zato morajo registrirati v skladu s pravili preprečevanja pranja denarja. Uporabniki in rudarji, ki vzdržujejo sistem virtualnih valut, v to niso vključeni (FinCEN, 2013).

NYDFS je 4. junija 2015 objavila pravila za trgovanje z virtualnimi valutami, pod imenom BitLicens. Gre za licenco za trgovanje z virtualnimi valutami, ki jo mora pridobiti podjetje, ki se ukvarja z dejavnostjo poslovanja z virtualnimi valutami. Na tej stopnji še ni posebej jasno, katera podjetja sodijo v ta okvir. Odvetniška družba Davis Polk je predlagala, da bi morali registracijo pridobiti spletne menjalnice, ponudniki denarnic ter podjetja, ki se ukvarjajo s trgovanjem, posredništvom in tudi vzajemni skladi, ki vlagajo v virtualne valute. Večina uporabnikov in trgovci, ki zgolj sprejemajo plačila v teh valutah, v to ne bodo vključeni. Pravne osebe, ki bodo zaprosile za licenco, bodo morale izpolnjevati merila za zaščito varstva potrošnikov, izpolniti zahteve za zaščito sredstev na računih strank in razviti celovit sistem kibernetične varnosti ter zadostiti pogojem boja proti pranju denarja (Allen, 2015, str. 38-39).

Evropske države, ki so članice Evropske unije (v nadaljevanju EU), povečini povzemajo stališče ECB in EBA.

EBA je v zvezi z virtualnimi valutami prvič reagirala 13. 12. 2013, ko je izdala Opozorilo uporabnikom v zvezi z navideznimi valutami, v katerem opozarja na tveganja, ki bi se jih morali uporabniki zavedati, če kupujejo, posedujejo ali trgujejo z virtualnimi valutami. Ob tem EBA opozarja na nevarnosti pri investiranju v virtualne valute, vključno z izgubo denarja na menjalni platformi, s krajo denarja iz digitalne denarnice, z nestanovitnostjo virtualnih valut, uporabo virtualnih valut v kriminalne dejavnosti ter davčnimi obveznostmi (EBA, 2013).

Poleg navedenega dokumenta je EBA v juliju 2014 objavila mnenje o virtualnih valutah, pri čemer pretežni del mnenja predstavljajo tveganja v zvezi s poslovanjem z virtualnimi valutami. EBA je v navedenem dokumentu objavila več kot 70 različnih vrst tveganj, ki jih je razvrstila v pet različnih kategorij: a) tveganja za uporabnike, b) tveganja za ostale udeležence na trgu, c) tveganja za finančno integriteto, d) tveganja za ponudnike plačilnih sistemov in e) tveganja za regulatorne organe. Nekatera med njimi veljajo tudi za obstoječe plačilne sisteme, nekatera pa so specifična za virtualne valute. Prav tako pa je pozvala pristojne nadzorne organe, da odvrčajo finančne institucije od nakupa, prodaje ali hrambe virtualnih valut (EBA, 2014).

ECB je glede virtualnih valut podala svoje mnenje z dvema dokumentoma, in sicer je v oktobru 2012 objavila poročilo o shemah virtualnih valut, v katerem je razvrstila virtualne valute v povezavi z realnim gospodarstvom ter ocenila vpliv virtualnih valut na stabilnost cen, finančno stabilnost in stabilnost plačilnih sistemov (ECB, 2012). V letu 2015 je ECB objavila dodatno poročilo, ki temelji na nadaljnji analizi z vidika centralnih bank Evro sistema, pri čemer je na novo opredelila virtualne valute ter opozorila tudi na tveganja, povezana z visoko nestanovitnostjo vrednosti virtualnih valut, s tečajnim tveganjem, tveganjem nasprotne stranke v zvezi z anonimnostjo uporabnikov, s pomanjkanjem preglednosti in tveganja, povezana z goljufijami (ECB, 2015).

Stanje na področju virtualnih valut je ocenil tudi Evropski parlament; 26. maja 2016 je namreč sprejel Resolucijo Evropskega parlamenta o virtualnih valutah. V njej pripoznava tako priložnosti, kot tudi tveganja virtualnih valut in poudarja pomen tehnologije distribuirane knjige transakcij – blockchain tehnologije, v hitro se razvijajočem tehnološkem okolju plačil. Hkrati je podal priporočila za celovito analizo virtualnih valut, po kateri bi se po potrebi spremenila veljavna zakonodaja EU o plačilih glede na nove možnosti, ki jih ponuja tehnološki razvoj, vključno z virtualnimi valutami in s tehnologijo distribuirane knjige transakcij, s čimer bi dodatno okrepili konkurenčnost in znižali stroške transakcij (Evropski parlament, 2016).

Obstaja tveganje, da lahko teroristične organizacije prek transferjev v virtualnih valutah prikrijejo transferje, saj ni mehanizma za poročanje, ki bi bil enakovreden mehanizmu v tradicionalnem bančnem sistemu in bi se uporabljal za odkrivanje sumljivih dejavnosti. Komisija EU v Sporočilu Komisije Evropskemu parlamentu in Svetu o akcijskem načrtu za okrepitev boja proti financiranju terorizma predlaga, da bi bila anonimna menjava valut pod nadzorom pristojnih organov, in sicer z razširitvijo področja uporabe Direktive o preprečevanju pranja denarja<sup>4</sup>, ki bi vključevala tudi menjalne platforme za menjavo virtualnih valut. Tovrstne menjave bi se nadzorovale v okviru nacionalne zakonodaje o preprečevanju pranja denarja in boja proti financiranju terorizma (Evropska komisija, 2016, str. 5).

Nemčija je bila ena prvih evropskih držav, ki je opredelila področje virtualnih valut. Nemški zvezni urad za finančni nadzor (*BaFin*) je opredelil bitcoin kot obračunsko enoto, ki za razliko od denarnih valut nimajo statusa zakonitega plačilnega sredstva. Uporabniki so zavezani davku na kapitalski dobiček, v kolikor posedujejo virtualne valute manj kot leto dni. BaFin je zavzel stališče, da je potrebno za določene aktivnosti, povezane s trgovanjem z bitcoini, pridobiti njihovo licenco. Gre za aktivnosti, povezane z organiziranim trgovanjem, z investicijskim posredništvom ter posredništvom pri transakcijah (Tasca, 2015, str. 53).

### **3.2 Zakonska ureditev virtualnih valut v Sloveniji**

Področje virtualnih valut v Republiki Sloveniji (v nadaljevanju RS) ni posebej urejeno z nobenim pravnim aktom. Svoje stališče do opredelitve virtualnih valut so do sedaj podale Ministrstvo za finance RS (v nadaljevanju MF RS), Finančna uprava Republike Slovenije (v nadaljevanju FURS), Urad za preprečevanja pranja denarja (UPPD) in Banka Slovenije.

MF je dne 23. 12. 2013 podal zgolj pojasnilo v zvezi z davčno obravnavo poslovanja z bitcoini. Po mnenju MF se »bitcoin virtualna valuta ne šteje za denarno sredstvo v smislu

---

<sup>4</sup> Direktiva (EU) 2015/849 Evropskega parlamenta in Sveta z dne 20. maja 2015 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma.



7. točke 4. člena Zakona o plačilnih storitvah in sistemih (Uradni list RS, št. 58/09, 34/10, 9/11 in 32/12), prav tako se bitcoin ne šteje za finančni instrument. Davčna obravnava dohodka, doseženega pri takem trgovanju/poslovanju ali v taki obliki, je odvisna od okoliščin posameznega primera. Treba je ugotoviti, kdo dosega dohodek in za kakšne vrste dohodek v posameznem primeru gre (dohodek iz kreiranja bitcoinov, iz kupovanja in prodajanja bitcoinov, izplačilo drugega dohodka v bitcoinih)« (FURS, 2013). Pri obdavčitvi pravnih in drugih oseb veljajo določila Zakona o davku od dohodkov pravnih oseb (v nadaljevanju ZDDPO-2), po katerem zavezanci ugotavljajo davčno osnovo na podlagi prihodkov in odhodkov, kot so jih ugotovili na podlagi računovodskih predpisov. Med prihodke upoštevajo prihodke iz rudarjenja in finančne prihodke za dobičke iz poslovanja oz. trgovanja z bitcoini ter finančne odhodke za izgube pri trgovanju z njimi ali zaradi tečajnih razlik. V primeru, da je podjetje obdavčeno po sistemu normiranih odhodkov, izguba iz trgovanja ne vpliva na davčno osnovo (Vukovič, 2015, str. 9).

Prav tako FURS različno opredeljuje dohodek fizične osebe ali če ga fizična oseba doseže v okviru opravljanja dejavnosti (FURS, 2013). Pri obdavčitvi dohodkov fizičnih oseb je treba upoštevati določila Zakona o dohodnini (v nadaljevanju ZDoh-2), pri čemer je treba razlikovati dohodke, ki ga dosežajo fizične osebe, ki opravljajo dejavnost (samostojni podjetniki in zasebniki) in dohodke, ki ga dosežajo fizične osebe, ki ne dosežajo dohodkov iz opravljanja dejavnosti. Za fizične osebe, ki opravljajo dejavnost (samostojni podjetniki in zasebniki), veljajo enaka določila kot pri pravnih osebah, katere so obdavčene po ZDDPO-2. Fizična oseba, ki ne dosega dohodkov iz opravljanja dejavnosti, se lahko pojavi v različnih vlogah. Če fizična oseba trguje z bitcoini, tako ustvarjeni dobički kot ustvarjene izgube ne vplivajo na njeno obdavčitev, saj gre pri tem za oproščene dohodke po 32. členu ZDoh-2. Če fizična oseba rudari, se njeni dohodki obravnavajo kot drugi dohodki po 105. členu ZDoh-2, ki so obdavčeni po 25 % stopnji. Enako velja, če fizična oseba dosega druge dohodke (npr. avtorske), ki so bili plačani v bitcoinih, se bitcoini upoštevajo kot način plačila teh dohodkov, dohodek pa se obdavči na način, kot bi bil sicer obdavčen, če bi bil plačan v EUR. Vrednost dohodka se določi tako, da se upošteva vrednost bitcoina v EUR v času, ko je bil dohodek prejet (Vukovič, 2015, str. 9).

FURS je dne 7. 12. 2015 na svoji spletni strani objavila, da se na podlagi sodbe Sodišča Evropske unije, v zadevi C-264/14, spremeni stališče glede obravnave provizij pri prodaji bitcoinov, kot z DDV obdavčenih transakcij. »Virtualna valuta bitcoin na podlagi zadevne sodbe predstavlja neposredno plačilno sredstvo med subjekti, ki jo sprejmejo, zato je transakcija menjave v zvezi z njo, ki se šteje za opravljanje storitev za plačilo, oproščena plačila DDV s skladu 4. d) točko 44. člena ZDDV-1 (člen 135(1)(e) Direktive o DDV). Izhajajoč iz zadevne sodbe je zato treba provizijo, ki je zaračunana za nakup bitcoinov v zameno za evre, oprostiti plačila davka na dodano vrednost, v skladu s 4. d) točko 44. člena ZDDV-1« (FURS, 2015).

Banka Slovenije je na svoji spletni strani objavila Opozorilo uporabnikom z dne 12. 12. 2013 (EBA, 2013), v katerem povzema stališče in opozorilo, ki ga je izdala EBA v zvezi z virtualnimi valutami. V njem EBA opozarja uporabnike na tveganja, s katerimi se lahko srečujejo, če kupujejo, hranijo ali trgujejo z virtualnimi valutami (npr. bitcoin). Povzema stališče EBA, da so virtualne valute oblika nereguliranega digitalnega denarja, ki ga ne izda centralna banka in zato zanj ne jamči. EBA v svojem gradivu opozarja uporabnike, »da ne obstajajo nobeni regulativni zaščitni ukrepi, ki bi uporabnikom povrnili izgube, če platforma, na kateri se menja ali hrani virtualne valute, propade ali preneha poslovati«. EBA proučuje tudi vsa pomembna vprašanja, povezana z virtualnimi valutami, da bi ugotovila, ali jih je mogoče nadzorovati ter ali je to potrebno storiti. Kot je zapisala EBA v svojem opozorilu, lahko »uporabniki izgubijo denar na menjalni platformi, če le-ta propade ali preneha poslovati, denar lahko uporabnikom ukradejo iz digitalne denarnice, uporabniki pri uporabi virtualne valute kot plačilnega sredstva za plačilo blaga in storitev niso zaščiteni, saj jih v skladu z zakonodajo ne ščiti nobena pravica do povračila, kot je to pri prenosih z bančnega ali plačilnega računa. Prav tako se lahko vrednost virtualne valute hitro spremeni ali pade na nič, transakcije v virtualni valuti se lahko zlorabijo za kriminalne dejavnosti, vključno s pranjem denarja, prav tako pa EBA opozarja uporabnike, da lahko zanje veljajo davčne obveznosti« (Banka Slovenije, 2014).

Urad RS za preprečevanje pranja denarja (v nadaljevanju UPPD) glede virtualne valute bitcoin v svojem obvestilu za zavezance povzema stališče Banke Slovenije, po katerem »virtualna valuta bitcoin ni elektronski denar, kot to določa Zakon o plačilnih storitvah in sistemih (Uradni list RS št. 58/09, 34/10, 9/11 in 32/12) (v nadaljevanju ZPlaSS), niti ni tuja valuta oz. deviza, kot to določa Zakon o deviznem poslovanju (Uradni list RS št. 16/08, 85/09 in 109/12), (v nadaljevanju ZDP). UPPD navaja, da lahko virtualno valuto bitcoin z vidika pranja denarja umestimo v kontekst 16. c točke 4. člena Zakona o preprečevanju pranja denarja in financiranja terorizma (Uradni list RS, št. 60/07, 19710, 77/11 in 108/12) (v nadaljevanju ZPPDFT), ki kot »zavezance po ZPPDFT določa tudi pravne in fizične osebe, ki v RS opravljajo posle v zvezi z dejavnostjo izdajanja in upravljanja drugih plačilnih sredstev, pri čemer ne gre za plačilno storitev v skladu z zakonom, ki ureja plačilne storitve in sisteme. Zavezanci morajo zaradi odkrivanja ter preprečevanja pranja denarja pri opravljanju svojih dejavnosti izvajati naloge, določene v ZPPDFT in na njegovi podlagi sprejetih predpisih. Po določilih ZPPDFT je tako zavezanec vsak, ki se ukvarja s trgovanjem oziroma z izdajanjem virtualne valute bitcoin«. Stališče UPPD opozarja, da obstajata vsaj dve potencialni nevarnosti pri poslovanju z virtualno valuto bitcoin, in sicer: »virtualna valuta v večini držav ni regulirana in nadzorovana, prav tako pa omogoča tudi veliko stopnjo anonimnosti pri poslovanju, predvsem zaradi proste prenosljivosti elektronske denarnice (angl. *E-wallet*), v kateri se hranijo bitcoini. Navedeni potencialni nevarnosti poslovanja z virtualno valuto bitcoin predstavljata razlog za obstoj povečanega tveganja zlorabe virtualne valute bitcoin tudi za namene pranja denarja ali financiranja terorizma« (UPPD, 2014).

## **4 DEJAVNIKI, KI VPLIVAJO NA VREDNOST VALUTE BITCOIN**

### **4.1 Splošni dejavniki**

Na vrednost bitcoin valute vplivajo med drugim mediji, zakonske regulative, špekulacije na borzah, vdori v spletne menjalnice in zaprtje le-teh. Prav tako dogodki, ki so povezani z delovanjem bank, kot je denimo bilo zaprtje bank na Cipru, s čimer se je izgubilo zaupanje uporabnikov v tradicionalna plačilna sredstva (Szczepański, 2014, str. 5).

Cena virtualne valute in njena nestanovitnost je po mnenju ECB odvisna od petih glavnih dejavnikov (ECB, 2012, str. 38):

- oskrbe z denarjem in drugimi ukrepi izdajatelja, kot je posredovanje na trgu, z namenom, da bi vplivali na menjalni tečaj;
- razsežnosti omrežja: vrednost virtualnih valut je odvisna od tega, v kolikšni meri so sprejete med uporabniki in trgovci. Pričakovati je, da se bo z rastjo omrežja, tj. s povečanim sprejetjem valute med potrošniki in trgovci, povečala tudi vrednost valute. Nizek obseg trgovanja ima običajno večje nihanje menjalnih tečajev;
- institucionalnih pogojev: virtualne skupnosti, ki imajo bolj jasno in transparentno politiko in vgrajene mehanizme varnostnih ukrepov, bodo ustvarile zaupanje med uporabniki ter s tem zagotovile močnejšo valuto;
- ugleda in zaupanja pri uporabnikih, ki ga je deležen izdajatelj valute. Ključni element, ki vpliva na menjalni tečaj, je odvisen od uresničitve izpolnjevanja svojih obveznosti;
- špekulacij glede prihodnje vrednosti valute in preteklih vdorov v sistem ter kraj, ki so jih utrpeli ponudniki storitev virtualnih valut.

### **4.2 Bančna kriza**

Večina uporabnikov sistema Bitcoin sestoji bodisi iz tehnoloških navdušencev, bodisi iz privržencev, ki vidijo prednost bitcoina v tem, da ni povezan z nobeno vlado. Nekateri izmed teh privržencev javno izražajo nezaupanje v svetovni finančni sistem, saj je bil bitcoin vpeljan ravno v času, ki je sovpadel z dnom globalne finančne krize v letih 2008 – 2009, kar je pripomoglo k njegovemu razcvetu (Yermack, 2014, str. 7-8).

Finančni trg je 15. septembra 2008 zaznamoval prelomni trenutek, ko je Lehman Brothers, takrat četrta največja ameriška investicijska banka, po množičnem padcu cen delnic na borznem trgu, doživela bankrot. Kolaps trga je pomenil začetek globalne finančne krize leta 2008 (Caetano, 2015, str. 77).

Finančna kriza na Cipru je povzročila drastično zvišanje cene za enoto bitcoin, ki je takrat zrasel kar na 1.216,73 USD na enoto (Raskin & Yermack, 2016, str. 12).

### **4.3 Pravna regulacija**

Na ceno bitcoina vplivajo ukrepi vladnih organov in uradne izjave glede regulacije virtualnih valut. Vsakokrat, ko vladni organi objavijo omejitve oz. opozorila glede uporabe bitcoina, se njegova vrednost na menjalnih tečajih bistveno spremeni. Čeprav odločitve vladnih organov niso neposredno vezane na regulacijo bitcoina, lahko dogodki, povezani z bančnim sektorjem, občutno vplivajo na spremembo cene, kot je bilo to ob primeru ciprske bančne krize, kjer so vladne oblasti zasegle sredstva na bančnih računih uporabnikov (Some Factors That Influence The Bitcoin Price, 2015).

### **4.4 Količina bitcoinov v obtoku**

Ker je ponudba na dolgi rok omejena, bi razširjena uporaba bitcoina pomenila, da bo povpraševanje po bitcoinih verjetno raslo hitreje kot ponudba denarja, zaradi česar bi se cena bitcoina povečevala. Posledica tega bi bila, da bi cene blaga in storitev v bitcoinih padle, kar bi povzročilo deflacijo (Murphy et al., 2015, str. 8).

### **4.5 Trgovanje z bitcoin valuto**

Vrednost bitcoina se oblikuje na podlagi ponudbe in povpraševanja na trgu. Odvisna je predvsem od tega, po kakšni vrednosti je prodajalec pripravljen prodati valuto in po kakšni vrednosti je kupec pripravljen plačati za to valuto. Vrednost menjalnih tečajev se določa na spletnih menjalnicah za izmenjavo virtualnih valut (Lemos, 2013). Do leta 2014 je bila prevladujoča spletna menjalnica Mt. Gox, ki je imela več kot 70 % tržni delež.

### **4.6 Vpliv medijev**

Mediji lahko bistveno vplivajo na ceno bitcoina. Medijske pozitivne predstavitve sprožijo porast vrednosti, medtem ko lahko negativna poročanja medijev povzročijo padec vrednosti bitcoina. Poročanja medijev o bankrotih spletnih menjalnic ali vdorih v sistem, kot tudi poročanja o vladnih regulativah ter novice o uporabi bitcoinov v nelegalnih dejavnostih, lahko povzročijo paniko med uporabniki, ki začno prodajati bitcoine, kar povzroči padec cene valute (Some Factors That Influence The Bitcoin Price, 2015). Objave v medijih, da večji trgovci sprejemajo bitcoin za plačilo svojih izdelkov in storitev, lahko povzročijo drastičen porast zanimanja med potencialnimi uporabniki, kar lahko privede do povišanja cen. Večja medijska pokritost bo zagotovila večjo prepoznavnost v širši javnosti in tako širila mrežo uporabnikov, kar bo dvignilo povpraševanje po valuti (Brito et al., 2014, str. 156).

V prvih dveh in pol letih obstoja je bila vrednost bitcoina manj kot 1 USD. Rudarjenje te valute je bilo takrat dokaj enostavno. Zaradi majhne konkurence so rudarji za svoje delo

zaslužili 50 bitcoinov na dan. Ko je bila v začetku leta 2011 določena pariteta z ameriškim dolarjem, so začeli mediji množično objavljati novice o bitcoinu. Zanimanje za bitcoin je naraslo, kar je vodilo tudi do večjega zanimanja za rudarjenje bitcoinov in s tem do večje konkurence med rudarji. Vrednost bitcoina je narasla (Caetano, 2015, str. 29).

## **4.7 Špekulacije**

Bitcoin se v literaturi pogosto omenja v zvezi s špekulacijami, ki so povzročile, da njegov menjalni tečaj nepredvidljivo niha v daljšem časovnem obdobju (Valdes-Benavides & Hernandez-Verme, 2014, str. 5). Nestanovitnost cen vodi do špekulativnega obnašanja posameznikov, ko lahko uporabniki kupijo valuto po nižji ceni ter jo nato prodajo po višji ceni, da ustvarijo dobiček. Špekulacije povečujejo povpraševanje, s čimer se povečuje tudi vrednost bitcoina. Z naraščanjem vrednosti valute se lahko zgodi, da bodo vlagatelji kopicili valuto, z namenom ustvarjanja dobička v prihodnosti. Umetno povzročena rast vrednosti lahko sčasoma ustvari cenovni mehurček, kar lahko hitro privede do padca vrednosti valute (Papp, 2014, str. 44). Avtorji Murphy et al. (2015, str. 7) menijo, da nestanovitnost cene kaže na to, da povečano povpraševanje po bitcoinih ne izhaja zaradi povečanih transakcij med trgovci in potrošniki, temveč da tržišče še vedno obvladujejo špekulativni investitorji, ki spodbujajo uporabnike da kopičijo valuto, namesto da jo porabijo.

## **5 TVEGANJA POVEZANA Z VIRTUALNO VALUTO**

### **5.1 Področja tveganj**

Z naraščanjem števila virtualnih valut in vse bolj razširjeno uporabo pa se je v strokovnih krogih pojavila zaskrbljenost, saj poleg prednosti, ki jih prinašajo virtualne valute, predstavljajo tudi velika tveganja, tako za uporabnike, plačilne sisteme, finančne institucije, ostale posrednike tovrstnih storitev na trgu, kot tudi zlorabo virtualnih valut v kriminalne dejavnosti.

Nad virtualnimi valutami nima nadzora nobena finančna institucija, vendar jih centralne banke in druge finančne institucije širom sveta budno spremljajo in proučujejo vidike možnosti prevelike razširjenosti uporabe virtualnih valut, ki niso pod njihovim nadzorom ter analizirajo, ali bi lahko razširjena uporaba virtualnih valut imela znaten vpliv na stabilnost plačilnih sistemov in monetarno ekonomijo. Povečanje uporabe virtualnih valut bi lahko povzročilo zmanjšanje uporabe fiat valut in vplivalo na makroekonomsko stabilnost in stabilnost plačilnih sistemov, s čimer bi bilo težje zagotavljati stabilno monetarno politiko in gospodarski razvoj. Bančni organi proučujejo tveganja, ki so povezana z obstoječimi plačilnimi sistemi ter vpliv virtualnih valut na cenovno stabilnost, stabilnost finančnega sistema ter stabilnost plačilnih sistemov.

Prav tako so zaskrbljeni organi pregona, saj se je uporaba virtualnih valut, predvsem zaradi svoje narave anonimnosti in decentraliziranega značaja, razširila tudi med kriminalnimi združbami, ki izkoriščajo virtualno valuto kot sredstvo, ki jim preko nevidnega omrežja TOR, olajša zakriti dejavnosti nelegalne trgovine s prepovedanim blagom in storitvami. Prav tako uporabnikom, ki se ukvarjajo z nezakonitimi dejavnostmi, virtualne valute omogočajo pranje denarja, katerega so na nezakonit način pridobili s kaznivimi dejanji ter davčne utaje. Prav tako pa je prisotno tudi materialno okoriščenje na račun drugih uporabnikov virtualnih valut, z vdori v elektronske naprave uporabnikov, kot tudi napadi na spletne menjalnice, pri katerih nekateri uporabniki hranijo svoje virtualne valute.

Eden izmed pomembnih dejavnikov tveganja pa je nenazadnje, tudi njegova visoka nestanovitnost vrednosti oz. volatilitnost, ki omejuje uporabnost bitcoina kot zanesljivo obračunsko enoto in zanesljivo sredstvo za hranjenje vrednosti. Prav zaradi svoje visoke nestanovitnosti in velikih razlik v vrednostih na različnih spletnih menjalnicah pa je priljubljen tudi pri špekulantih, ki skušajo to izkoristiti za svoj zaslužek ter kopičijo sredstva, z namenom, da bo vrednost valute sčasoma narasla.

## **5.2 Tveganja povezana z obstoječimi plačilnimi sistemi**

### **5.2.1 Vpliv virtualnih valut na cenovno stabilnost**

ECB (2012, str. 33–37) je v svojem dokumentu proučevala vpliv virtualnih valut na cenovno stabilnost. Sheme virtualnih valut bi lahko imele vpliv na stabilnost cen in monetarno politiko, če bi bistveno spremenile količino denarja v obtoku, če bi imele vpliv na hitrost in kroženje denarja v obtoku, na uporabo gotovine ali bi vplivale na merjenje denarnih agregatov, ali če bi obstajala interakcija med virtualnimi valutami in realnim gospodarstvom. Kar zadeva prvi vidik se domneva, da bo ponudba denarja ostala stabilna skozi čas, vendar za to ni zagotovila. Čeprav se predvideva, da bo ponudba denarja ostala stabilna, je potrebno oceniti tudi posledice, ki nastanejo zaradi nihanja menjalnega tečaja, ob pretvorbi virtualnih valut v realne valute. Kar zadeva drugi vidik, je vpliv odvisen od števila aktivnih uporabnikov sheme virtualne valute, tj. koliko bodo potrošniki pripravljene plačevati s temi virtualnimi valutami in koliko bo trgovcev, ki bodo pripravljene sprejemati plačila v tej valuti. V skrajnem primeru bi virtualne valute lahko imele substitucijski učinek na prave valute, ki jih izdajajo centralne banke, v primeru, da bi se začele uporabljati bolj množično. Povečanje uporabnikov virtualnega denarja bi lahko privedlo do zmanjšanja uporabe pravega denarja, s čimer bi se zmanjšal tudi denar, potreben za izvedbo transakcij nominalnega dohodka. Razširjena uporaba virtualnih valut pa bi lahko pomenila tudi zmanjšanje velikosti bilanc centralnih bank in s tem sposobnost vplivanja na kratkoročne obrestne mere. Centralne banke bi morale proučiti orodja za reševanje tega tveganja, s tem da bi npr. poskušale uveljaviti zahteve glede obveznih rezerv shem virtualnih valut. Učinek substitucije bi lahko povzročil tudi težje merjenje denarnih agregatov in posledica bi se kazala v odnosu denarnih agregatov do inflacije, ki se

uporablja za merjenje tveganja stabilnosti cen v srednjeročnem in dolgoročnem obdobju. Virtualne valute se ustvarjajo izven dosega centralne banke in lahko se zgodi, da se virtualna posojila razširijo do te mere, da bi to vplivalo na odločitev centralnih bank v zvezi z obrestnimi merami, zaradi česar bi nadzor centralnih bank nad denarjem in kreditnimi gibanji lahko postal manj učinkovit. Kar zadeva interakcijo med virtualnimi valutami in realnim gospodarstvom, ekonomska teorija do sedaj še ni prišla do zaključkov. Avtorja Peng Hui in Sun Yanli sta v svojem članku razpravljala o tem, da sheme virtualnih valut delujejo kot sredstvo menjave pri trgovanju za prave dobrine in storitve ter zato lahko vplivajo na realni BDP. Virtualne valute bi lahko imele učinek na ponudbo pravega denarja. Vpliv virtualnih valut na oskrbo z realnim denarjem, bi se lahko kazal z dveh vidikov (ECB, 2012, str. 36): a) kot substitucijski učinek virtualnega gospodarstva na realno gospodarstvo. Na podlagi raziskave se je na Kitajskem skupni dohodek realnega gospodarstva zmanjšal zaradi vključenosti prebivalstva v virtualne sheme (ljudje so preživeli veliko časa z igranjem igrice ter posledično manj časa porabili za delo v realnem svetu), kar je vplivalo tudi na zmanjšanje denarnih sredstev, b) virtualne valute bi lahko do neke mere vplivale na pravi denar. Z uporabo večje količine virtualnih valut ljudje porabljajo manj denarja v realnem življenju, kar povzroči zmanjšanje deleža gotovine. To lahko povzroči zmanjšanje denarnih depozitov, kar lahko posledično vodi do povečanje denarnih multiplikatorjev. Avtorji trdijo, da bi Centralne banke morale spremljati obseg ponudbe virtualnega denarja. Poročilo ECB za zaključek navaja, da zaenkrat virtualne sheme na tem nivoju ne predstavljajo tveganja za stabilnost cen. V kratkoročnem in srednjeročnem obdobju se tudi ne pričakuje bistven vpliv na hitrost in kroženje denarja v obtoku. Vsekakor pa bo potrebno spremljati interakcijo med virtualnimi valutami in realnim gospodarstvom (ECB, 2012, str. 37).

## **5.2.2 Vpliv virtualnih valut na finančno stabilnost**

ECB opredeljuje finančno stabilnost kot stanje, v katerem je finančni sistem, ki ga sestavljajo finančni posredniki, trgi in tržna infrastruktura, sposoben prenašati finančne šoke, da bi se tako zagotovila varnost investiranja za donosne naložbene priložnosti. Zagotavljanje finančne stabilnosti zahteva opredelitev glavnih virov tveganj in ranljivosti, kot so neučinkovitost pri dodeljevanju finančnih sredstev od varčevalcev do investorjev, neučinkovito oblikovanje cen ali slabega upravljanja finančnih tveganj (ECB, 2012, str. 37).

V okviru shem virtualnih valut, ki delujejo izven bančnega sistema, bi glavni vir potencialne finančne nestabilnosti predstavljala interakcija med virtualnimi valutami in realnim gospodarstvom, tj. med menjalnimi tečaji in izmenjavo na trgu. Na sheme virtualnih valut tipa 1 in 2, kot jih razvrsti v svojem dokumentu ECB, to nima vpliva. Pri shemah virtualnih valut tipa 3, med katere sodi tudi virtualna valuta bitcoin, pa je vrednost valute odvisna od ponudbe in povpraševanja denarja na deviznem trgu. Razlika med realnimi valutami in virtualnimi valutami je v tem, da za slednjimi ne stoji nobena država

ali valutno območje, zato gospodarstvo s svojimi neravnovesji ali produktivnostjo, na menjalni tečaj nima tolikšnega vpliva.

ECB ocenjuje, da virtualne valute zaenkrat ne ogrožajo finančne stabilnosti, saj imajo omejeno povezavo z realnim gospodarstvom, nizki obseg trgovanja in nezadostno število sprejemanja teh valut s strani uporabnikov.

Tveganje bi se lahko povečalo, v kolikor bi virtualne valute postale alternativa tradicionalnim valutam. Pravi učinek sistemov virtualnih valut bo v veliki meri odvisen od števila aktivnih uporabnikov teh valut, kakor tudi od trgovcev, ki bodo pripravljene sprejeti virtualne valute za dobrine in storitve.

Sistem virtualnih valut zaenkrat ne omogoča najema ali odobritve posojila, kar pa ne izključuje možnosti, da se v prihodnosti razmere ne bi spremenile. V kolikor bi banke odigrale vlogo posrednika, s čimer bi delovale kot depozitorji za spletne denarnice, bi lahko uporabniki začeli bolj množično uporabljati virtualne valute, saj bi se zanašali na varnost in tehnična znanja bank. Banke bi lahko ponudile obresti za uporabnike, ki bi pri njih hranili svoje virtualne valute. Obstaja pa tudi teoretična možnost, da bi sistem Bitcoin spremenili do te mere, da bi deloval kot obstoječi multiplikacijski sistem odobravanja posojil, ki temelji na delnih rezervah. To pa bi bilo v nasprotju s samo zasnovo Bitcoina. ECB ocenjuje, da bi takšen razvoj v prihodnosti lahko imel znaten vpliv na stabilnost finančnega sistema (ECB, 2012, str. 37-39).

Svoje stališče do tega vprašanja je podala tudi Centralna banka Združenega kraljestva (*Bank of England*) (Ali, Barrdear, Clews & Southgate, 2014, str. 11), ki meni, da virtualne valute trenutno ne predstavljajo pomembnejšega tveganja za finančno stabilnost v Združenem kraljestvu. Skupna zaloga virtualnih valut je trenutno premajhna, da bi ogrožala finančno stabilnost. Kljub temu pa ni izključeno, da bi tveganja skozi čas narasla. Potencialno tveganje na monetarno stabilnost bi se lahko pojavilo, v kolikor bi virtualne valute dosegle velik delež porabe v gospodarstvu.

### **5.2.3 Vpliv virtualnih valut na stabilnost plačilnih sistemov**

#### **5.2.3.1 Raba plačil v virtualnih valutah**

Plačila v virtualnih valutah se uporabljajo za nakup realnih dobrin in storitev, zato se tudi uporabniki virtualnih valut soočajo z običajnimi tveganji plačilnih sistemov. Poleg tega virtualne valute niso pod nadzorom centralnih bank, ki bi lahko zagotavljale določeno varnost plačil.

Uporabniki se pri tem soočajo s številnimi tveganji, kot so npr. kreditno tveganje, likvidnostno tveganje, operativno tveganje in pravna tveganja.



### 5.2.3.2 Kreditna tveganja

Kreditnemu tveganju so uporabniki izpostavljeni v povezavi z imetništvom sredstev na svojih virtualnih računih, saj ni zagotovila, da bo izdajatelj sposoben v celoti poravnati svoje finančne obveznosti do uporabnikov (ECB, 2012, str. 40). Primer je bankrot spletne menjalnice Mt. Gox, ki je bila znana kot platforma z maksimalno konverzijo bitcoinov na svetu do leta 2014, s 70 % tržnim deležem. Februarja 2014 je spletna menjalnica zamrznila račune svojih uporabnikov ter zaprla svojo spletno stran in vse storitve menjalnice, pri čemer je bilo izgubljenih 850.000 BTC, kar je v takratni vrednosti pomenilo vsoto 450 milijonov USD. Ustanovitelja platforme Mt. Gox so avgusta leta 2015 aretirali (EUROPOL, 2015a, str. 40).

### 5.2.3.3 Likvidnostna tveganja

Sheme virtualnih valut imajo nizko likvidnost zaradi omejenega števila enot, s katerimi se trguje. Uporabniki so izpostavljeni likvidnostnemu tveganju, kadar institucija ne izpolni svojih obveznosti do uporabnikov za zagotavljanje likvidnosti. V primeru vdora v shemo, bi masovna pretvorba sredstev virtualne valute za pravi denar s strani uporabnikov, lahko povzročila velike izgube vrednosti njihovih sredstev (ECB, 2012, str. 40). Cena enote virtualne valute se v primerjavi s tradicionalnimi valutami oblikuje izključno na podlagi ponudbe in povpraševanja na posameznih menjalnih platformah virtualnih valut (Rijavec, 2013, str. 21), kar lahko pomeni visoko nestanovitnost vrednosti (EUROPOL, 2015a, str. 40).

### 5.2.3.4 Operativna tveganja

Operativno tveganje pri virtualnih valutah nastane v povezavi z virtualnimi denarnicami, ki jo mora, za izvedbo plačila, imeti tako plačnik, kot tudi prejemnik plačila. Virtualne denarnice običajno zagotavljajo izdajatelji posameznih virtualnih valut oz. z delovanjem sheme povezane osebe (npr. virtualne denarnice za valuto bitcoin lahko uporabnik pridobi tudi na platformah za menjavo iz virtualnih v tradicionalne valute) in so zaradi zagotavljanja primernih tehnoloških rešitev za varno hrambo virtualnih denarnic in posledično enot virtualnih valut odvisne od stabilnega in varnega poslovanja izdajateljev oz. z delovanjem sheme povezanih oseb (Rijavec, 2013, str. 21). Čeprav so mnogi sistemi virtualnih valut dobro zaščiteni, obstaja verjetnost hekerskega vdora v platformo menjalnice. Primer je slovenska menjalna platforma Bitstamp, ko je 1. maja 2015 začasno prenehala poslovati, sklicujoč se na nepooblaščen vdor v t.i. operacijsko denarnico. Ukradenih je bilo 19.000 bitcoinovih enot, njihova vrednost pa je dosegla 4,4 milijona EUR (EUROPOL, 2015a, str. 41).

### 5.2.3.5 Pravna tveganja

Pravna tveganja za uporabnike virtualnih valut nastajajo zaradi pravne negotovosti glede sistemov delovanja shem virtualnih valut. Pomanjkanje ustreznega pravnega okvirja bistveno povečuje tudi druga tveganja (ECB, 2012, str. 40). Primer je Liberty Reserve ali Silk Road (EUROPOL, 2015a, str. 41).

### 5.2.3.6 Vloga Evropske centralne banke pri nadzoru virtualnih valut

Ena od nalog ECB je zagotavljanje nemotenega delovanja plačilnih sistemov. Uporabniki virtualnih valut lahko sodelujejo neposredno v tem sistemu in s tem vplivajo na plačilni sistem. ECB je v svojem dokumentu (2015, str. 27) ocenila, da virtualne valute zaradi majhnega obsega trgovanja, ne ogrožajo stabilnosti plačilnega sistema. Vendar pa bi se stanje lahko spremenilo, v kolikor bi prišlo do inovacij na tem področju in bi večji ponudniki finančnega sektorja začeli ponujati storitve, povezane s podporo tem virtualnim valutam oz. bi se bistveno povečalo število uporabnikov in bi narasla velikost transakcij plačil v virtualnih valutah. V kolikor bi virtualne valute postale del rednega finančnega sistema in bile uporabljene v velikem obsegu, bi teoretično bilo možno, da bi virtualne valute lahko vplivale na tradicionalni plačilni sistem preko finančnih institucij, ki bi bile udeležene v ponudbi storitev, povezanih z virtualnimi valutami in v tradicionalnih sistemih. To pa bi lahko privedlo do tega, da bi uporabniki izgubili zaupanje v virtualne valute, prav tako pa bi to lahko spodkopalo zaupanje uporabnikov v že obstoječe elektronske plačilne instrumente.

Upravičeno se lahko pričakuje, da se bo rast uporabnikov virtualnih valut v prihodnje širila. Možnost njihove širitve pa je odvisna od tega, ali bodo sistemi virtualnih valut uspeli izboljšati svoje pomanjkljivosti, zlasti glede tehničnih pomanjkljivosti in nestabilnosti valute ter na področju zagotavljanja varnosti uporabnikov.

ECB (2015, str. 27) budno spremlja razvoj dogodkov v zvezi z uporabo virtualnih valut ter njihovo vlogo v procesu plačil kot alternativo tradicionalnim bančnim sistemom.

## 5.3 Tveganja povezana s kriminaliteto

### 5.3.1 Pregled izzivov za organe pregona

Uporaba virtualnih valut pa se, predvsem zaradi anonimnosti, ki jo omogoča sistem Bitcoin, zlorablja tudi v kriminalne dejavnosti. Virtualne valute predstavljajo velik izziv organom pregona zaradi svoje sposobnosti, da presegajo državne meje v delčku sekunde, posebnosti pravnih sistemov posameznih držav in anonimnosti. Predvsem zaradi slednjega, so virtualne valute povezane s številnimi vrstami kaznivih dejanj, vključno s ponudbo tržnic, preko katerih je mogoče naročiti napade na podjetja, izkoriščanje otrok (vključno s

pornografijo), korporativno vohunstvo, ponarejanje valut, trgovanje z drogami, ponarejene osebne izkaznice in potne liste, sheme z visoko donosnostjo naložbe, kot so Ponzijeve sheme in druge finančne prevare, spolno izkoriščanje, kraje kreditnih kartic in številke kreditnih kartic. Prav tako pa je mogoče preko takih tržnic naročiti tudi orožje ali umor (Trautman, 2014, str. 2).

Razlogi, zakaj so virtualne valute tako zelo privlačne za kriminalce, so različni. Virtualne valute ponujajo največjo stopnjo anonimnosti, tako za uporabnike kot tudi za transakcije. Omogočajo hiter in zanesljiv prenos sredstev, pridobljenih s protipravno pridobljeno premoženjsko koristjo, iz ene države v drugo, imajo nizko nestanovitnost, kar ima za posledico nižje valutno tveganje ter tako povečujejo zmožnost za prenašanje in shranjevanje pridobljenega bogastva. Prav tako so širše sprejete v kriminalnem podzemlju ter vredne zaupanja (Trautman, 2014, str. 7).

Virtualne valute se pogostokrat omenjajo s pojmom temni splet (angl. *Dark Web*) in globoki splet (angl. *Deep Web*). Temni splet je del širšega t.i. globokega spleta, ki deluje na P2P omrežju. Primer temnega spleta predstavlja programska oprema TOR, Freenet ali Invisible Internet Project (I2P). Temni splet za svoje delovanje zahteva visoko specializirana orodja in opremo za dostop, uporabnikom pa omogoča zakrivanje identitete (Ciancaglini, Balduzzi, McArdle & Rösler, 2015, str. 6). Temni splet uporabnikom zagotavlja določeno stopnjo anonimnosti, kar s pridom izkoriščajo kriminalci za nelegalne dejavnosti. Trenutno najbolj razširjena šifrirna programska oprema je TOR (EUROPOL, 2015a, str. 21). Do TOR-a lahko dostopa praktično vsak. Potrebno si ga je le namestiti na svoj računalnik. TOR (angl. *[T]he [O]nion [R]outing*) je bil prvotno razvit kot projekt U.S. Naval Research Laboratory v ZDA za zaščito vladne komunikacije. Sistem deluje na način, da prenaša transakcije preko več točk omrežja, da se zakrije identiteta uporabnikov (Trautman, 2014, str. 16). TOR pogosto opisujejo kot e-bay za nakup drog, ker je zaradi šifrirnega sistema praktično skoraj nemogoče izslediti IP (angl. *Internet Protocol*) naslov uporabnika. Največja spletna tržnica, ki je delovala preko anonimnega omrežja TOR, je bila tržnica Silk Road.

Silk Road je pričela delovati januarja 2011 (FATF, 2014, str. 11) in je bila dostopna le osebam, ki so uporabljale programsko opremo TOR. Ker so druge oblike plačilnih sistemov, kot je npr. PayPal, enostavno sledljive, je bilo edino plačilno sredstvo, ki se je uporabljalo za plačevanje blaga in storitev na spletni strani Silk Road, z namenom neizsledljivega plačevanja, virtualna valuta bitcoin (Ogunbadewa, 2014, str. 36).

Skrita spletna stran Silk Road, ki je bila namenjena le njihovim uporabnikom, je omogočala nakup in prodajo prepovedanih drog, orožja, podatke o ukradenih identitetah in druge nezakonite dobrine in storitve. Spletna stran se je uporabljala za trgovino z mamili, za vdore v računalniške sisteme in pranje denarja. Preko nezakonitih transakcij je bilo opranih za nekaj sto milijonov USD (ocenjena vrednost na podlagi bitcoin tečaja na datum

zasega sredstev). Provizije so se gibale v razponu od 8 do 15 odstotkov celotne prodajne cene.

Uporaba bitcoinov kot ekskluzivne valute v teh transakcijah je omogočala kupcem in prodajalcem, da prikrijejo svojo identiteto, saj lahko uporabniki P2P omrežja uporabijo anonimni bitcoin naslov. Prav tako ima lahko uporabnik neomejeno število naslovov in lahko uporablja za vsako transakcijo drugi naslov, z namenom, da se zabrišejo sledi nezakonito pridobljene premoženjske koristi (FATF, 2014, str. 11).

Nicolas Christin, raziskovalec na univerzi Carnegie Mellon, ocenjuje, da je bila ocenjena vrednost bitcoin transakcij na Silk Road-u vredna okoli 1,2 milijona USD mesečno (Christin, 2012, str. 3) in je tako postala prva izbira za preprodajalce drog, ki si ne želijo tvegati izpostavljenosti in aretaciji na ulicah (Ogunbadewa, 2014, str. 36). Po raziskavi, ki jo je opravil Christin v času delovanja spletne strani Silk Road, izhaja, da je bilo od 4,5 % do 9 % vseh bitcoin transakcij izvedenih na Silk Roadu (Christin, 2012, str. 20).

Po dve leti trajajoči preiskavi je FBI 2. oktobra 2013 zaprl spletno stran Silk Road in aretiral njenega ustanovitelja Rossa Ulbrichta, poznanega pod vzdevkom »Dread Pirate Roberts« (Brito & Castillo, 2013, str. 24). Ameriški organi pregona so ob zaprtju spletne podzemne tržnice Silk Road sprva zasegli 29.655 bitcoinov, kasneje pa objavili, da je bilo zaseženih skupno 173.991 bitcoinov v zvezi z delovanjem Silk Road, ki so bili takrat vredni več kot 33,6 milijonov USD (Trautman, 2014, str. 96). Obtoženih je bilo tudi nekaj največjih trgovcev (Brito & Castillo, 2013, str. 25). FBI v svojem dokumentu (Nigh & Pelker, 2015, str. 2) navaja podatek, da je bilo v operaciji organov pregona na Silk Roadu zaseženih več kot 179.000 enot bitcoinov. V juniju 2014 je ameriški U.S. Marshals Service organiziral dražbo, na kateri so prodali 29.656 bitcoinov, ki so bili zaseženi ob zaprtju spletne strani Silk Road. To je bil prvi primer tovrstne dražbe, ocenjena vrednost v času dražbe je bila 18 milijonov USD. Po štirih tednih trajajočem sojenju je bil Ross Ulbricht 5. februarja 2015 spoznan za krivega po vseh točkah obtožnice na Zveznem sodišču na Manhattnu, 29. maja 2015 je bil obsojen na dosmrtno ječo (Trautman & Harrell, 2016, str. 55).

Zaprtje podzemne spletne tržnice Silk Road pa ni odpravilo problema trgovanja s prepovedanim blagom. Pojavile so se njene naslednice, ki so prav tako delovale na črnem trgu preko globokega spleta, kot so Black Market Reloaded, Sheep Marketplace in naslednica Silk Road 2.0, ki so predstavljale nove izzive za organe pregona. Vendar so slednje delovale krajši čas: Sheep Marketplace se je zaprla konec novembra 2013, zaradi ranljivosti sistema, kar je povzročilo uporabnikom 6 milijonov USD izgube, Black Market Reloaded pa so kmalu zatem prostovoljno zaprli zaradi varnostnih razlogov (Brito & Castillo, 2013, str. 25).

EUROPOL (2015 a, str. 52) navaja, da so organi pregona v novembru 2014 izvedli operacijo, imenovano Onymous, pri kateri je sodelovalo 21 držav, pri čemer so zasegli 619 naslovov uporabnikov, v vrednosti 900.000 EUR v bitcoinih ter 180.000 EUR v gotovini, drogah, zlatu ali srebru. Operacija organov pregona je zajela 33 spletnih podzemnih tržnic, 17 posameznikov je bilo aretiranih. Ocenjujejo, da zasežene strani predstavljajo približno 37 % tržnega deleža na temnem spletu.

FBI je zaradi visoke stopnje anonimnosti, ki jo omogočajo virtualne valute, v svojem poročilu zapisal, da ugotavljajo visoko stopnjo kibernetске kriminalitete. Vedno več bo kriminalnih združb, ki bodo uporabljale virtualne valute za pranje denarja, financiranje kriminala, vedno več bo vdorov v računalnike posameznikov zaradi kraje denarnih virtualnih enot iz virtualnih denarnic (FBI, 2012).

### **5.3.2 Pranje denarja**

FATF, mednarodni organ, ki razglša standarde za preprečevanja pranja denarja in financiranje terorizma, je sprožila številne pomisleke glede uporabe virtualnih valut za namene uporabe pranja denarja in financiranje terorizma, saj protokol ne zahteva identifikacije uporabnikov in je zaradi narave anonimnosti bolj privlačna za storilce kaznivih dejanj. Decentraliziranost virtualnih valut, ki nimajo centralnega skrbnika, otežuje preiskavo kaznivih dejanj (Allen, 2015, str. 37).

Obstaja tveganje, da se lahko bitcoin uporabi za pranje denarja, financiranje terorizma in tihotapljenje prepovedanega blaga. Čeprav so te skrbi osnovane na teoriji in nimajo dokaznih temeljev, bi lahko bitcoin uporabljali tisti, ki želijo diskretno oprati nelegalno pridobljeni denar. Zaskrbljenost, da bi se bitcoin uporabljal za namene pranja denarja, se je pojavila po dogodkih v Liberty Reserve, ki je bila zasebna, centralizirana digitalna valuta, zasnovana v Costa Rici, katero so organi pregona zaprli na podlagi obtožb pranja denarja (Brito & Castillo, 2013, str. 25-26). Liberty Reserve je omogočala široko izbiro spletnih kriminalnih dejavnosti, vključno z goljufijami s kreditnimi karticami, kraji identitete, investicijskimi prevarami, z vdori v računalniške sisteme, z otroško pornografijo in s trgovino z mamili. Po navedbah preiskovalcev je bilo v teh poslih, domnevno v 55 milijonov ločenih finančnih transakcijah nelegalno opranih preko 6 milijard USD. Organi pregona so 28. maja 2013 vložili kazenske ovadbe zoper pet glavnih akterjev, ki so delovali v Liberty Reserve, preiskovalno delo organov pregona pa je potekalo v 18 državah (Barnett, 2014, str. 4).

Medtem ko se Liberty Reserve in Bitcoin zdita podobni valuti, ker sta obe virtualni valuti, obstajajo med njima pomembne razlike. Liberty Reserve je bila centralizirana valuta v lasti zasebnega podjetja, ki je bila ustvarjena domnevno z namenom omogočanja pranja denarja, medtem ko je bil sistem Bitcoin ustvarjen iz drugih razlogov. Transakcije znotraj skupnosti Liberty Reserve niso bile pregledne. Dejansko je Liberty Reserve obljubljal

uporabnikom anonimnost. Bitcoin je po drugi strani decentralizirana odprta valuta, ki zagotavlja javno evidenco vseh transakcij. Tisti, ki perejo umazan denar, lahko sicer poskušajo zaščititi svoje bitcoin naslove in identiteto, vendar bodo njihove transakcije vedno javne in kadarkoli dostopne za organe pregona. Pranje denarja preko Bitcoin sistema se tako zdi mnogo bolj tvegano početje, kot preko centraliziranega sistema, npr. pri Liberty Reserve. Poleg tega, je nekaj spletnih menjalnic virtualnih valut sprejelo ukrepe za izpolnjevanje zahtev politike preprečevanja pranja denarja, kot je vodenje evidenc in poročanje. Kombinacija sistema javne knjige in sodelovanje spletnih menjalnic pri zbiranju podatkov o njihovih strankah, bo verjetno za uporabnike Bitcoin sistema manj privlačno za pranje denarja, v primerjavi z zasebnimi anonimnimi ostalimi virtualnimi valutami (Brito & Castillo, 2013, str. 26).

Medtem ko je EBA v svojem dokumentu (2014, str. 22) ocenila tveganje za pranje denarja in financiranja terorizma z visoko stopnjo tveganja, Brown (2016, str. 6) navaja, da po podatkih, ki jih je v letu 2015 predstavila HM Treasury za Združeno kraljestvo, virtualne valute zaenkrat predstavljajo nizko stopnjo tveganja za pranje denarja. Kljub temu pa ne izključujejo možnosti, da v kolikor bi se uporaba virtualnih valut povečala, bi se tudi stopnja tveganja lahko povečala. HM Treasury ugotavlja, da je uporaba virtualnih valut v kriminalne namene, zaenkrat še vedno osredotočena na podzemne spletne nelegalne tržnice, kjer se trguje s prepovedanim blagom in storitvami (Brown, 2016, str. 6).

Potrebno je omeniti, da so pasti, s katerimi se srečuje Bitcoin sistem, enako mogoče tudi pri poslovanju z gotovino, ki je bila od nekdaj priljubljena izbira preprodajalcev drog in drugih, ki na ta način operejo denarna sredstva. Pa vendarle se bo gotovinsko poslovanje uporabljalo še naprej in oblasti ne razmišljajo o tem, da bi ukinili gotovinsko poslovanje. Ko bodo poskušale oblasti regulirati bitcoin, bo potrebno razmisliti o nevarnosti prestroge ureditve. V najslabšem primeru bi lahko prestroga regulativa preprečila legitimno poslovanje podjetij, problema pranja denarja pa s tem ne bi rešili. Izziv za oblikovalce politik in regulatorjev je, kako razviti sistem nadzora, ki bo omejil pranje denarja in uporabo bitcoinov v nezakonite dejavnosti, ne da bi pri tem zatrli prednosti, ki jih ponuja bitcoin za zakonite uporabnike v njihovem vsakdanjem življenju (Brito & Castillo, 2013, str. 26-27).

### **5.3.3 Davčne utaje**

Problem, ki se pojavlja v zvezi z virtualno valuto bitcoin, so davčne utaje. Obstajata dva glavna načina za ustvarjanje dohodka. Prvič, ker vrednost bitcoina niha, se lahko bitcoini prodajo po višji vrednosti od prvotne nabavne cene, kar pomeni dobiček za prodajalca. Drugič, bitcoine lahko prejmejo trgovci kot plačilo za blago in storitve in je tako obdavčljiv, kot če trgovci prejmejo sredstva v nacionalni valuti. Potencialno lahko posameznik, zaradi anonimnosti, ki jo zagotavlja bitcoin, ne prijavi dohodka, ki ga je prejel v bitcoinih in se s tem izogne plačilu davkov (Ly, 2014, str. 595-596).

Omri Marian (2013, str. 39) meni, da bodo virtualne valute postale ključni instrumenti za davčne utajevalce, ki ne morejo več najti zatočišča v davčnih oazah. Marian meni, da imajo virtualne valute tradicionalne značilnosti davčnih oaz: dohodki niso obdavčeni, anonimnost davkoplačevalcev je zagotovljena. Virtualne valute imajo eno dodano vrednost: njihovo delovanje ni odvisno od finančnih institucij. Zaradi te prednosti imajo virtualne valute potencial, da ogrozijo dosedanja prizadevanja vlad na področju boja proti utaji davkov.

#### 5.3.4 Kraje in prevare

Čeprav je sistem Bitcoin sam po sebi precej varen, saj ni tveganja ponarejanja denarne valute in vdori v sistem niso zelo pogosti, se uporabniki spletnih denarnic soočajo s podobnimi tveganji (Turpin, 2014, str. 345), kot uporabniki nacionalnih denarnih valut in kreditnih kartic.

Uporabniki, ki hranijo svoje spletne denarnice na osebnih računalnikih, se lahko soočijo z vdorom v računalniški sistem, v kolikor ustrezno ne poskrbijo za antivirusne programe za zaščito svojih osebnih računalnikov in zaščito svojih podatkov. V letu 2011 so zaznali zlonamerno programsko opremo, ki je povzročila kraje bitcoinov iz osebnih računalnikov uporabnikov. Po drugi strani pa uporabniki, ki shranjujejo svoje bitcoine preko spletnih ponudnikov denarnic, zaupajo ponudnikom spletnih storitev, da le-ti ustrezno zaščitijo sredstva svojih imetnikov pred nepooblaščenimi vdori in kraji sredstev iz njihovih spletnih denarnic (Turpin, 2014, str. 345).

Bitcoin omrežje je potencialno dovzetno tudi za t.i. **DDoS napade** (angl. *Distributed Denial of Service*) ali napade porazdeljene zavrnitve storitve, pri čemer lahko napadalci začasno onespobijo strežnike, kar lahko povzroči neodzivnost omrežja v času trajanja napada. Omrežje v času napada ni dostopno za obdelavo novih transakcij. DDOS napadi neposredno ne ogrožajo samega sistema, vendar pa bi ponavljajoči se napadi načeli zaupanje uporabnikov v vrednost valute, kar lahko privede tudi do množične prodaje (Lloyd's, 2015, str. 12-13). EUROPOL navaja, da se je v začetku leta 2015 pojavila skupina pod imenom DD4BC (DDoS za Bitcoin). Gre za kriminalno združbo, ki izvaja DDoS napade ter od žrtev zahteva odkupnino v bitcoinih. Njihove zahteve za odkupnino se gibljejo med 1 in 100 bitcoini, odvisno od ocene finančnega položaja žrtve in njene pripravljenosti, da sledi navodilom napadalca. DD4BC se je osredotočila predvsem na spletne igralnice, v zadnjem času pa opažajo, da je skupina razširila svojo dejavnost tudi na finančni sektor (EUROPOL 2015b, str. 42).

**Finney-ev napad** je poimenovan po razvijalcu sistema Bitcoin, Halu Finneyju, ki je poznan kot prva oseba, ki je prejela bitcoine. V tem napadu mora rudar najprej izračunati nov blok, ki ga ne pošlje naprej v omrežje, temveč poskuša kovance najprej porabiti pri trgovcu, predno jih doda v nov blok. V kolikor je plačilo še nepotrjeno, bo novi blok

vključeval transakcije dvojne porabe. Rešitev bi bila, da se počaka vsaj 6 potrditev (Caetano, 2015, str. 101).

Dodatna skrb glede bitcoina je možnost investicijskih prevar. Lastnik Savings and Trust, Trendon T. Shavers, je preko investicijskih prevar deloval po sistemu Ponzijeve sheme (Ly, 2013, str. 596). Vlagateljem je obljubljal 7 % tedenske donose za naložbe, vredne 25.000 bitcoinov. Sklad je 17. avgusta 2012 nenadoma prenehal delovati, na njegovem računu pa naj bi se zbralo za 500.000 BTC sredstev uporabnikov. SEC (the Securities and Exchange Commission) je 23. julija 2013 vložila tožbo zoper lastnika, vrednost odtujenih bitcoinov pa je takrat preseгла 60 milijonov USD (Turpin, 2014, str. 347). V obrambi je Shaver trdil, da pri bitcoinih ne gre za vrednostne papirje, ker bitcoin ni denar in ni zakonsko reguliran v ZDA, zato s tem ni kršil nobenega zakona (Ly, 2013, str. 596).

### **5.3.5 Napadi na spletne menjalnice in vdori v denarnice**

Znatno tveganje za imetnike bitcoin valute predstavljajo tudi spletne menjalnice. Uporabniki, ki imajo shranjena sredstva pri spletnih menjalnicah, tvegajo izgubo sredstev ob zaprtju menjalnice. V raziskavi, ki sta jo v letu 2013 izvedla Moore in Christin, je bilo ugotovljeno, da je bilo od leta 2010 odprtih 40 spletnih menjalnic, od tega jih je 45 % propadlo, pri čemer je veliko uporabnikov izgubilo svoja sredstva. Podatki raziskave so pokazali, da 45 % menjalnic, ki so propadle, uporabnikom ni povrnilo sredstev (Moore & Christin, 2013, str. 15).

Mt. Gox, nekoč prevladujoča spletna menjalnica za nakup in prodajo bitcoinov, je 25. februarja 2014, propadla. Veliko vlagateljev v bitcoine je izgubilo svoje prihranke. Spletna menjalnica Mt. Gox je v letu 2009 pričela delovati kot menjalnica za zamenjavo zbirateljskih kart, vezanih na priljubljeno spletno igro imenovano Magic: The Gathering. Kmalu je preusmerila svojo pozornost na bitcoin (Trautman, 2014, str. 100-101). Prvi dan trgovanja je 20 bitcoinov zamenjalo lastnika, po vrednosti 4.951 centov za BTC, skupna vrednost trgovanja je znašala nekoliko manj kot 1 USD (Yermack, 2014, str. 6). V letu 2010 je Mt. Gox postala vodilna spletna menjalnica za trgovanje z virtualnimi valutami. Leta 2011 je prišlo do vdora v menjalnico, pri čemer je bilo ukradenih preko 60.000 uporabniških imen in gesel. Trgovanje je bilo za sedem dni ustavljeno, kar je povzročilo padec v vrednosti enote bitcoin iz 17,51 USD na 0,01 USD na tej menjalnici. Ponovni vdor v sistem je menjalnica doživela februarja 2014, pri čemer je bilo izgubljenih kar za 500 milijonov USD vrednosti bitcoinov. Družba je na Japonskem februarja 2014 vložila predlog za stečaj (Szczepański, 2014, str. 5). Po nekaterih ocenah je bilo izgubljenih kar 7 % vseh bitcoinov v obtoku, ocenjena tržna vrednost izgubljenih bitcoinov pa naj bi bila med 450 milijoni USD in 500 milijoni USD, na dan vložitve stečaja (Virtual currency: Risks and Regulation, 2014, str. 15). Ob propadu menjalnice Mt. Gox je presenetljiv podatek, da je vrednost bitcoina na drugih spletnih menjalnicah ostala presenetljivo visoka.



Na dan 24. februarja 2014 je bil bitcoin vreden okoli 525,00 USD, le dan za tem, ko je novica prišla v javnost (Trautman, 2014, str. 101).

Omrežje Bitcoina je podvrženo tudi **Sybil napadom** (angl. *Sybil attacks*), pri katerih skuša napadalec določiti eno ciljno vozlišče v omrežju, denimo podjetje, ki se ukvarja z bitcoini. Napadalec kreira zadostno število bitcoin vozlišč, ki mejijo na ciljno vozlišče, da postane žrtvino edino sredstvo za priklop na omrežje. Napadalec obda žrtev z zlonamernimi odjemalci, ki so pod nadzorom napadalca. Tako se zdi, da žrtev dostopa do omrežja prek številnih poštenih posameznikov, v resnici pa je dostop omejen na peščico posameznikov, ki so pod nadzorom napadalca. Druga možnost tovrstnega napada je, da napadalec pošilja žrtvi napačne informacije o stanju omrežja. Napadalec pod pretvezo domnevnega kupca, da bo prenesel bitcoine na ciljno menjalnico in jih pretvoril v realno valuto, lahko pošlje žrtvi goljufive različice zapisa veljavnih transakcij. Omrežje Bitcoin je samo po sebi sicer elastično pred temi napadi. Da bi napadalec uspel s tovrstnimi prevarami, bi moral nenehno pošiljati žrtvi goljufive bloke, ki bi delovali kot pravi. Novih blokov pa ni tako enostavno ustvariti, saj je zato potrebna velika računalniška moč. Napadalec z le 10 % računalniške moči celotnega omrežja, bi lahko ustvaril lažne bloke z 10 % normalne hitrosti, kar pomeni še vedno veliko količino energije za posameznega udeleženca. Žrtev lahko postane blok trenutnega vozlišča, na katerega se povezujejo drugi, pošteni posamezniki uporabniki znotraj P2P omrežja. Razvijalec Gavin Andresen je označil tak napad sicer teoretično možen, vendar v praksi težko izvedljiv. Spletne menjalnice in druga podjetja, ki se ukvarjajo z bitcoinom, bi morala sprejeti ustrezne ukrepe proti tovrstnim napadom z razvitimi avtomatiziranimi procesi (Lloyd's, 2015, str. 12).

V preteklih letih se je zgodilo kar nekaj vdorov v spletne menjalnice oz. kraje iz spletnih denarnic uporabnikov. Nekaj pomembnejših kršitev varnosti je opisanih v nadaljevanju:

- iz spletne menjalnice Bitcoinica je bilo v letu 2011 ukradenih več kot 60.000 bitcoinov v dveh ločenih napadih (Turpin, 2014, str. 346);
- septembra 2012 je spletna menjalnica Bitfloor iz New Yorka, doživela varnostni vdor, ki je povzročil izgubo 24.000 bitcoinov, v protivrednosti 250.000 USD (Murphy et al., 2015, str. 9);
- 3. aprila 2013 je ponudnik spletne denarnice Instawallet, doživel varnostni vdor v sistem, ki je povzročil izgubo preko 35.000 bitcoinov, v skupni vrednosti skoraj 4,6 milijona USD (Murphy et al., 2015, str. 9);
- 11. avgusta 2013 je Bitcoin Foundation objavila, da so opazili pomanjkljivost v programski opremi operacijskega sistema Android, pri čemer je prišlo do kraje bitcoinov iz spletnih denarnic uporabnikov (Murphy et.al., 2015, str. 9);
- oktobra 2013 sta bila zaznana dva glavna napada: iz avstralske Bitcoin banke Inputs.io je bilo v več zaporednih napadih odtujenih za 4.100 bitcoinov, v takratni vrednosti približno 1,2 milijona USD; na Kitajskem pa je spletna menjalnica GBL kar naenkrat prenehala obstajati in z računov uporabnikov je izginilo 4,1 milijona USD. GBL, ki je

delovala le 6 mesecev, je hitro zrasla v četrto največjo kitajsko spletno menjalnico. Podrobnosti, ki so prišle na plan ob njenem zaprtju, so nakazovale na to, da je bila spletna menjalnica že od vsega začetka prevara (Virtual currencies: Out of the deep web, into the light, 2014, str. 4);

- novembra 2013 je bila žrtev napada češka spletna menjalnica Bitcash.cz, iz katere je bilo ukradenih za okoli 100.000 USD iz približno 4.000 spletnih denarnic uporabnikov (Santos, 2013);
- Danska Bitcoin Internet Payment System (BIPS) je prav tako v novembru 2013 doživela napad, ki se je odražal v izgubi 1,5 milijonov USD (Virtual currencies: Out of the deep web, into the light, 2014, str. 4);
- v letu 2013 je bila takrat največja spletna menjalnica Mt. Gox žrtev DDOS napadov, iz katere je bilo ukradenih 850.000 bitcoinov, takrat vrednih več kot 400 milijonov USD (Murphy et al., 2015, str. 8);
- v januarju 2015 je evropska spletna menjalnica Bitstamp za nekaj časa prenehala delovati, ko je doživela vdor v menjalnico, od koder je bilo ukradenih za 19.000 bitcoinov, v takratni vrednosti približno 5 milijonov USD (Murphy et al., 2015, str. 8).

## 5.4 Tveganje pri uporabnikih virtualnih valut

Velik poudarek javnih razprav o ureditvi virtualnih valut je namenjen ravno varstvu potrošnikov. Za razliko od tradicionalnih plačilnih sistemov, ki nudijo zaščito potrošnikov pred različnimi tveganji, je področje ureditve virtualnih valut z vidika zaščite potrošnikov še dokaj neurejeno. Zaradi vse večjega razvoja novih tehnologij in naložb se uporaba virtualnih valut med uporabniki povečuje, področje zaščite potrošnikov pa še vedno ni ustrezno urejeno.

Pomembna tveganja, ki so jim izpostavljeni potrošniki in so povezana predvsem z uporabo in lastništvom virtualnih valut, so predvsem sledeča (Virtual currency: Risks and Regulation, 2014, str. 4–5):

**Izgube ali kraje:** virtualna valuta se lahko izgubi zaradi kršitve s področja varnosti, napake uporabnika ali tehnoloških pomanjkljivosti na virtualni denarnici ali spletni menjalnici. Izgubljenih sredstev na računu ni moč povrniti.

**Goljufije ali nepooblaščen uporaba:** virtualne valute lahko porabi vsakdo, ki poseduje lastniška gesla oz. privatni ključ. Transakcij se ne da povrniti, čeprav gre za prevaro ali nepooblaščen uporabo.

**Napaka pri obdelavi transakcij:** v primeru, da se plačilo naslovi na drugega uporabnika, pri nakazilu napačnega zneska transakcije ali če transakcija ni pravilno zaključena zaradi napake v virtualni denarnici, spletni menjalnici ali na računalniškem procesorju, v večini primerov virtualnih valut sredstev na računu ni možno povrniti. Napake se ne da popraviti

in potrošnik nima podlage, da bi lahko povrnil sredstva. Colley (2015, str. 2) navaja, da je 28. oktobra 2011, uporabnik izgubil več kot 2.600 bitcoinov, ker plačnik ni uporabil pravega naslova prejemnika plačila.

**Napaka v denarnici ali spletni menjalnici:** v primeru napake v denarnici ali spletni menjalnici pri ponudnikih teh storitev, oz. če le-te propadejo in računi postanejo nedostopni, ne obstaja varovalni mehanizem, ki bi zaščitil imetnika oz. njegovih sredstev na računu.

**Nepripravljena razkritja podatkov:** ponudniki denarnic in spletnih menjalnic nimajo obveznosti, da zagotovijo razkritje podatkov za potrošnike v zvezi s pristojbinami za storitve ali stroške, povezane s transakcijami virtualnih valut, niti da objavijo podatke v zvezi z nestanovitnostjo cene oz. druga opozorila.

## 5.5 Nihanje vrednosti valute bitcoin

Največje tveganje, s katerimi se soočajo uporabniki bitcoina, izhaja iz precejšnje nestanovitnosti njegove vrednosti. Do aprila 2011 je vrednost bitcoina ostala pod 1 USD za 1 BTC (Turpin, 2014, str. 344), 1. aprila 2011 je bil 1 bitcoin vreden 0,785 USD. Vrednost je 8. junija 2011 narasla na 30,99 USD (ECB, 2012, str. 38). Po več odmevnih krajah in vdorih v sistem, je njegova vrednost 20. junija 2011 strmoglavila na 0,10 USD za 1 BTC (Turpin, 2014, str. 344).

V letu 2013 se je vrednost bitcoina močno spreminjala, razlike v vrednosti so narasle do 142 %, kar je občutno višje, kot se je spreminjala vrednost ostalih valut na menjalnih trgih, ki je znašala med 7 % in 12 %. Za primerjavo, imajo celo tvegane oblike naložb stopnjo nestanovitnosti med 20 % do 30 %, najbolj tvegane oblike naložb pa redko presežejo stopnjo 100 %. Zlato, kot hranilec vrednosti, ki se pogosto omenja kot alternativa virtualnim valutam, je imelo v letu 2013 stopnjo nestanovitnosti 22 %, v primerjavi z menjalnim tečajem USD. Po mnenju Yermacka je zaradi nestanovitnosti bitcoin tvegana naložba (Yermack, 2014, str. 14-15).

Caetano (2015, str. 30) navaja, da so se v obdobju od leta 2011 do leta 2015 zgodili trije večji cenovni mehurčki, za katere je značilna hitra rast cene, čemur sledi nenaden padec vrednosti posamezne valute.

Prvi mehurček je nastopil v juliju 2011, ko so mediji prvič obširneje poročali o bitcoinu. Do takrat se je menjalni tečaj na spletnih menjalnicah virtualnih valut gibal okrog 2 do 3 USD za 1 BTC. Kmalu zatem so cene na menjalnih tečajih presegle 30 USD v le nekaj tednih. Pred koncem leta 2011 je vrednost menjalnega tečaja padla na 2 USD za 1 BTC.

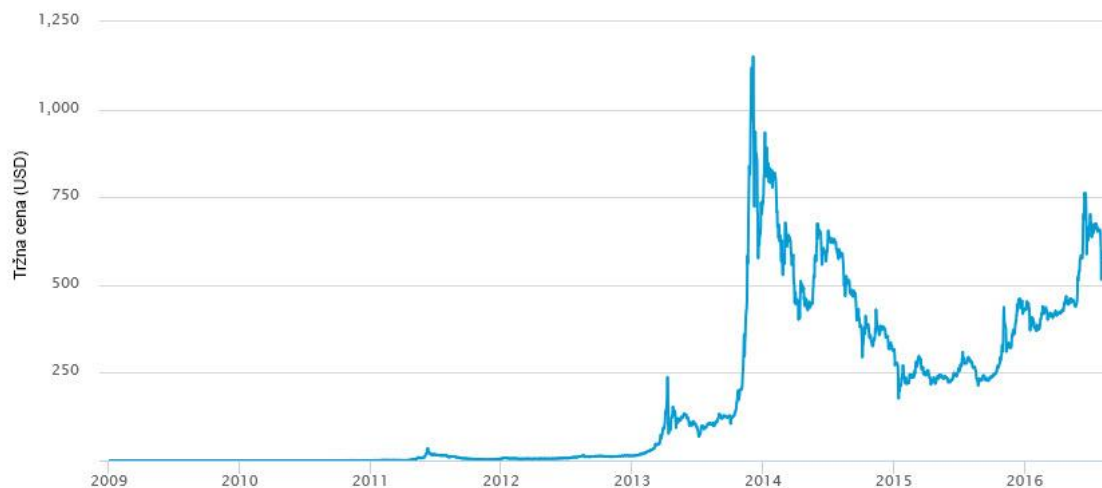
Naslednji večji mehurček se je zgodil v aprilu 2013. Vrednost bitcoina je naraščala in več uporabnikov se je začelo zanimati zanj. Istočasno je ciprska vlada napovedala ukrepe v bančnem sektorju. Vse to je povzročilo, da je vrednost bitcoinu narasla na 260 USD. Po tem se je cena ustalila na približno 140 USD za 1 BTC.

Največji mehurček se je zgodil proti koncu leta 2013, zaradi nepričakovanega povečanega obsega trgovanja z valuto bitcoin na kitajskem trgu. Povečano povpraševanje po bitcoinu s strani kitajskih investitorjev je povzročilo, da je vrednost bitcoinu v kratkem času narasla na preko 1.100 USD za 1 BTC. Kitajska vlada se je nato odzvala in prepovedala svojim bankam transakcije v bitcoinih. Ta prepoved sicer ni veljala za nakup in prodajo bitcoinov, vendar je na trgu vseeno povzročila preplah. V manj kot 12 urah, ko je bila novica o tem objavljena, je menjalniški tečaj padel pod 600 USD za 1 BTC. Negotovost glede nadaljnje vladne regulative in omejenega dostopa do sredstev je povzročila padec v ceni.

V letu 2014 je vrednost bitcoina še vedno precej nihala. 7. februarja 2014 je bitcoin dosegel menjalni tečaj po vrednosti 697,93 USD (Turpin, 2014, str. 344). Sredi januarja 2015 se je vrednost bitcoina gibala okrog 200 USD za 1 BTC (Murphy et al., 2015, str. 7).

Spodnji graf prikazuje gibanje vrednosti bitcoina v obdobju od januarja 2009, ko je bil ustvarjen izvorni blok, do julija 2016.

*Slika 5: Gibanje vrednosti bitcoina v obdobju od 1. 1. 2009 do 31. 7. 2016*



*Vir: Blockchain Charts, 2016.*

ECB (2012, str. 38) navaja, da se nestanovitnost vrednosti virtualnih valut lahko pojavi iz več razlogov, kot so pomanjkanje zrelosti nove valute, pomanjkanje zaupanja s strani

uporabnikov sistema, ki je še neuveljavljen, zaradi nizkega obsega trgovanja, pomanjkanja pravne varnosti, špekulacij, vdorov v sistem ipd.

Eden od pomembnejših dejavnikov gibanja vrednosti bitcoina je nestabilnost nekaterih centralnih valut. Investitorji iščejo alternativni trg za svoje naložbe, izven omejitev, ki jih določa finančni trg. Ker je negotovost glede sprejemanja regulatornih ukrepov s strani vladnih organov ponekod še vedno precej nejasna, je tudi trgovanje s to valuto še vedno precej tvegano (Caetano, 2015, str. 30). Vladni organi, bančne institucije in gospodarski sektor nočejo izgubiti nadzora nad monetarnim sistemom in gospodarskim razvojem (Richter et al., 2015, str. 580).

Yermack (2014, str. 16) meni, da bi morala dnevna vrednost bitcoina postati bolj stabilna, da bi lahko služila kot hranilec vrednosti in kot obračunska enota za trgovanje. Po drugi strani Jon Matonis verjame, da je nestanovitnost oz. volatilitnost nekaj povsem običajnega za valuto, ki je stara komaj nekaj let (Upelj, 2013).

Nestanovitnost cene sama po sebi ne more biti vzrok, da blago ne bi moglo biti sprejeto kot valuta. Pravo vprašanje, ki se postavi je, ali se lahko tržišče zavaruje pred nestanovitnostjo. Nihanje vrednosti valute se lahko zniža, ko je tehnologija širše sprejeta s strani uporabnikov. Večja kot je baza uporabnikov, manjša je verjetnost vplivanja na cene (Van Alstyne, 2014, str. 32). Na dolgi rok se lahko nestanovitnost cene bitcoina zmanjša. Bolj ko ga bodo ljudje uporabljali kot valuto, višja bo tržna kapitalizacija, kar bo vodilo v znižanje nestabilnosti cene menjalnih tečajev. Ravno visoka nestanovitnost cene pa povzroči, da jo ljudje še ne sprejemajo v večjem številu, je manj priljubljena in uporabljena kot plačilno sredstvo (Eikmanns & Sandner, 2015, str. 8).

Bolj kot bo baza uporabnikov naraščala, je pričakovati, da se bo tudi nestanovitnost umirila. Pripravljenost potrošnikov, da sprejmejo novo valuto, je v precejšnji meri odvisna od zaupanja vanjo. Potrošniki ne želijo tvegati in imeti svojega premoženja naloženega v valuti, ki je ne bodo mogli prodati. Vendar pa je zaradi razvoja interneta in rasti elektronskega poslovanja pričakovati, da se bo zaupanje potrošnikov v virtualne valute povečalo, kar bo vplivalo tudi na stabilnost cene valute. Kljub temu pa na zaupanje potrošnikov vpliva tudi pravna negotovost (Turpin, 2014, str. 344-345), česar ne moremo prezreti.

## **6 IZZIVI ZA PRIHODNOST**

Bitcoin prinaša številne gospodarske koristi. Z bistvenim zmanjšanjem transakcijskih stroškov se lahko poveča hitrost kroženja denarja v obtoku, omogočena so mikroplačila, hkrati pa ta valuta posameznikom v državah v razvoju omogoča dostop do bančnih

storitev, kjer je bančna infrastruktura slabo razvita in mnogi nimajo dostopa do storitev tradicionalnega bančništva (Turpin, 2014, str. 350-351).

V mnogih državah v razvoju je dostop do bančnih storitev še vedno zelo omejen. Za te države predstavlja bitcoin in podobni sistemi velik potencial kot način plačevanja dobrin ali storitev, saj lahko z nizkimi stroški shranjujejo svoje prihranke, izvajajo plačila in pošiljajo denar preko spleta z enega konca sveta na drugega. Poleg tega je bitcoin razdeljen na osem decimalnih mest, zaradi česar omogoča plačevanje mikroplačil, ki se lahko prenašajo v majhnih količinah, ki prej, zaradi transakcijskih stroškov, niso bila mogoča (Turpin, 2014, str. 366-367).

Bitcoin omogoča hitrejša in cenejša nakazila ter revnim ljudem v državah v razvoju ponuja dostop do finančnih storitev, ki jih drugače ne bi bili deležni (Praprotnik, 2015). V državah v razvoju lahko stroškovno učinkovita čezmorska mednarodna nakazila olajšajo ekonomsko preživetje lokalnih prebivalcev podeželskih gospodinjstev, saj lahko nižje provizije mednarodnih nakazil omogočijo, da delavci, ki delajo v tujini, ohranijo več zaslužka (Folkinshteyn, Lennon & Reilly, 2015, str. 121) s pošiljanjem nakazil svojim družinam. Svetovna banka ocenjuje, da je bilo v letu 2014 takšnih nakazil v skupni vrednosti 582 milijard USD, od tega so predstavljala nakazila v države v razvoju v skupni vrednosti 35 milijard USD, ki vključuje približno 232 milijonov migrantov. Do leta 2016 so svetovna nakazila narasla preko 601 milijard USD, pri čemer nakazila v države v razvoju predstavljajo znesek v višini 440 milijard USD (Trautman & Harrell, 2016, str. 29).

Simonite (2012) meni, da je v ZDA in Evropi meteorski vzpon bitcoina predvsem posledica špekulantov, ki so valuto zgolj hranili in je niso uporabljali za dejansko plačevanje dobrin in storitev. Po mnenju Rüdigerja Kocha, nemškega razvijalca programske opreme, pa bi se uporaba bitcoina lahko razlikovala v Afriki, kjer bi univerzalna, virtualna valuta lahko vplivala na reševanje realnih problemov. Hitro rastoča afriška gospodarstva, kot sta npr. Kenija in Nigerija, so močno odvisna od gotovinskih transakcij, zlasti na podeželju, kjer ni bankomatov, dostop do bančnega računa pa ima le malo ljudi.

V Keniji je bila leta 2007 razvita posebna oblika elektronskega denarja, imenovanega M-Pesa, za plačilo dobrin in storitev. Plačilo se lahko izvede preko prenosnih telefonov, uporablja pa ga že okoli tretjina tamkajšnjega prebivalstva. Nedavno so bili izvedeni poizkusi, da bi integrirali bitcoin z M-Peso, kar bi približalo bitcoin uporabnikom M-Pese, plačila pa bi se izvajala preko običajnih mobilnih telefonov (Pérez-Marco, 2016, str. 8). V Nairobiju se je že pojavilo inovativno podjetje, Bitpesa, ki je menjalnica za izmenjavo virtualnih valut, kjer sprejemajo bitcoine in jih menjajo v kenijsko nacionalno valuto. Prejemnik prejme sredstva preko mobilne elektronske denarnice, kot so npr. *M-Pesa*, *Orange*, *Airtel*, *ali Yu* (Folkinshteyn et al., 2015, str. 122).

Bitcoin so prav tako zelo privlačni za državljane in vlade narodov, za katere veljajo prisilni zakonski ukrepi. Za državljane držav, kjer je valuta relativno stabilna, je bitcoin zaradi svoje nestanovitnosti še vedno dokaj nepriljubljen. V državah, kjer je uradna valuta enako tvegana in nestabilna, pa je bitcoin vse bolj privlačna opcija. Na primer v Iranu so državljani, ki so želeli zaščititi svoje premoženje pred hiperinflacijo, pretvorili svoja sredstva v druge valute, npr. USD, kar je zaradi mednarodnih bančnih sankcij postalo težje izvedljivo. Zaradi tega se veliko število Irancev odloča pretvoriti svoje prihranke v bitcoine, saj je to mogoče storiti anonimno in elektronsko. Ta pojav pa ni omejen zgolj na državljane, za katere veljajo prisilni zakonski ukrepi. Marca 2013, ko je ciprski predsednik naznanil, da bodo zasegli del prihrankov na računih, shranjenih v ciprskih bankah, je varčevalce na Cipru in v drugih evropskih nestabilnih državah zajel preplah. Po dveh dneh je pričela cena bitcoinu močno naraščati, internetni brskalniki pa so pokazali bistven porast zanimanja za virtualno valuto (Turpin, 2014, str. 359).

Državljan držav z nepredvidljivimi in nestanovitnimi menjalnimi tečaji, kot je npr. Brazilija, bi lahko investirali svoje prihranke v bitcoin, ki jih nato bodisi lahko spremenijo v druge, bolj stabilne valute, bodisi uporabljajo kot plačilno sredstvo. Zanimanje za bitcoin je že naraslo v državah, ki se soočajo z nestabilnostjo njihove valute, kot so Argentina, Nikaragva in Venezuela (Darlington, 2014, str. 11). V Argentini se je povpraševanje uporabnikov po bitcoinih povečalo, kot odziv na visoko inflacijo nacionalne valute in strogih kapitalskih zahtev (Brito & Castillo, 2013, str. 17).

Upelj (2013) meni, da je projekt Bitcoin zanimiv ekonomski eksperiment. V nasprotju s prevladujočo ekonomsko doktrino, ki trdi, da je za poganjanje gospodarstva nujna inflacija, je bitcoin zasnovan kot deflatorna valuta – njena vrednost s časom raste. Po mnenju Yermacka (2014, str. 2) bitcoin nima dodatnih značilnosti, ki so običajno povezane z valutami moderne ekonomije. Namesto, da je naložen v banki, je potrebno imeti digitalno denarnico, ki so pogostokrat tudi tarče napadov.

Glede kritike, da bitcoin spodbuja nezakonite dejavnosti, avtorji Tasca, Liu in Hayes (2016, str. 40) menijo, da so pomisleki nekaterih regulatornih organov glede uporabe bitcoina za nezakonite dejavnosti, v tem trenutku morda pretirane. Van Alstyne (2014, str. 32) meni, da je to problem družbe, kot celote. Kriminalci prav tako uporabljajo gotovino, da operejo denar, pridobljen na nezakonit način. Jeremy Millar meni, da bitcoin ni več »skupnost hekerjev«, temveč se zdaj s tem ukvarjajo velika podjetja, ki svoje poslovanje prilagajajo veljavnim predpisom (Virtual currencies What are the risks and benefits, 2016).

Valdes-Benavides in Hernandez-Verme (2014, str. 6) menita, da si večina pomanjkljivosti virtualnih valut deli podobno usodo kot tradicionalne, fiat valute. Fiat valute so se skozi zgodovino prav tako uporabljale za financiranje nezakonitih dejavnosti in pranje denarja. Prav tako so fiat valute nagnjene k špekulacijam, h krajam in vdorom v sisteme, ki so povzročile nihanje vrednosti brez opazne spremembe v gospodarstvu.

Za odkrivanje kaznivih dejanj, je po mnenju nekaterih, lažje izslediti bitcoin transakcije, kot transakcije z gotovino. Van Alstyne (2014, str. 30) meni, da je sistem Bitcoin boljši v smislu odkrivanja goljufij, kot je to pri kreditnih karticah, saj vsaka transakcija zahteva javno preverjanje pristnosti kupcev in prodajalcev. Javne transakcije ne pomenijo kršitve zasebnosti kupcev in prodajalcev. Kljub temu, da so transakcije javne in zabeležene, ne razkrivajo, kdo je lastnik tega računa. Največji izziv za organe pregona bo povezati bitcoin naslove uporabnikov kaznivih dejanj s pravo identiteto uporabnika (Nigh & Pelker, 2015, str. 7). Sčasoma se bodo tudi organi pregona poslužili javne evidence bitcoin transakcij za izsleditev storilcev kaznivih dejanj, na način, ki jih morda nikoli ne bi izsledili z uporabo bankovcev (Van Alstyne, 2014, str. 32).

Ker se virtualne valute zlorabljujejo v kriminalne namene tudi na globalni ravni, bi bilo potrebno zakonske regulatorne ukrepe uskladiti z drugimi državami, enotno, da ne bi prihajalo med državami do nasprotujočih si vrzeli. Zaradi anonimnosti transakcij, ki jo omogočajo kriptovalute, je organom pregona težje izslediti posameznike, ki uporabljajo te valute zgolj v kriminalne namene in za pranje denarja ter presegajo meje posameznih držav. Barnett (2014, str. 7-8) navaja, da bi zmerne regulatorne reforme, ki bi morale biti meddržavno usklajene in bi posegale predvsem na področje delovanja spletnih menjalnic, preko katerih se sredstva, uporabljena v kriminalne namene, pretvorijo nazaj v fiat valute, ter ustrezen nadzor nad njimi, morda okrepile ugled virtualnih valut, da bi se lahko uveljavile kot plačilno sredstvo in jih obranila pred izkoriščanjem kriminalnih organizacij.

Ustrezna regulacija in nadzor nad spletnimi menjalnicami, bi lahko bilo učinkovito sredstvo v boju proti zatiranju kriminala in odkrivanju storilcev kaznivih dejanj. Nekatere države so na tem področju že naredile korak naprej in prilagodile zakonodajo, po kateri morajo spletne menjalnice pridobiti licenco in se registrirati v skladu s pravili preprečevanja pranja denarja. V ZDA se morajo spletne menjalnice za izmenjavo virtualnih valut registrirati pri FinCEN, ki določa pravila, po katerih so tovrstni zavezanci dolžni izdelati celovito oceno tveganja izpostavljenosti pranju denarja, izvajati ukrepe v skladu z zakonodajo AML (Anti-Money Laundering Program), voditi evidence ter spremljati in poročati o sumljivih transakcijah (FinCEN, 2014, str. 5).

Virtualne valute predstavljajo vladam resno tveganje za makroekonomsko stabilnost in dejavnik, ki omejuje njihovo sposobnost, da vplivajo na gospodarstvo. Povečanje uporabe virtualnih valut lahko vodi do zmanjšanja uporabe realnega denarja, s čimer je težje izvajati monetarno politiko (Mikołajewicz-Woźniak & Scheibe, 2015, str. 374).

Vprašanje, ki se postavlja je, kako naj vlade, centralne banke in drugi regulatorni organi, sprejmejo ukrepe, s katerimi bi uredili trg virtualnih valut. Bitcoin predstavlja svojevrsten izziv za regulatorne organe. Na eni strani zato, ker gre za odprt protokol in decentralizirano omrežje, kjer ni osrednjega organa, ki bi ga lahko nadzorovali. Po drugi strani pa nastaja več novih posrednikov, ki delujejo v omrežju Bitcoin, ki jih je vsekakor moč nadzirati in



jim določiti standarde. Ti vključujejo spletne menjalnice, trgovske posrednike in ostale ponudnike, ki zagotavljajo storitve za uporabo valute bitcoin za uporabnike (Brito et al., 2014, str. 146).

Turpin (2014, str. 367) meni, da je najverjetnejši in morda tudi najbolj učinkovit pristop regulatornih organov, da poskušajo urediti le transakcije, ki potekajo v bitcoinih, namesto da posegajo v sam sistem. Jasno je, da se bodo morale spletne menjalnice za izmenjavo virtualnih valut prilagoditi predpisom, tako kot to velja za ostale menjalnice. Glede na koristi, ki bi ga prineslo regulirano omrežje Bitcoin, bi bilo s strani regulatornih organov nesmotrno zavzeti bolj sovražen pristop do samega sistema.

Van Alstyne (2014, str. 32) meni, da je glavna grožnja, s katero se sooča bitcoin, usklajeno nasprotovanje centralnih bank po svetu. Tajska je v juliju 2013, kot prva država na svetu, prepovedala uporabo bitcoina. Sledila ji je Kitajska, ki je bankam prepovedala trgovanje z bitcoini (Eikmanns & Sandner, 2015, str. 8). Centralna banka Kitajske je 5. decembra 2013 prepovedala trgovanje z bitcoin valuto ali menjavo v nacionalno valuto yuan, kar je močno zmanjšalo povpraševanje, cena bitcoina pa je v enem tednu padla za 25 %. Ruska centralna banka je 7. februarja 2014 prepovedala uporabo bitcoina, kar je znižalo njegovo vrednost za 10 % (Van Alstyne, 2014, str. 32).

Manj restriktivna regulatorna politika bi lahko povečala zaupanje potrošnikov v bitcoin. To bi tudi zmanjšalo negotovost glede pravnih in davčnih vprašanj. S povečanjem regulatorne ureditve posameznih držav pa bi se zmanjšala neodvisnost sistema Bitcoin in anonimnost uporabnikov (Eikmanns & Sandner, 2015, str. 8).

Novo tehnologije odpirajo nekatera vprašanja v zvezi z bančnimi strategijami. Pojav bitcoina je vsekakor povzročil nelagodje bančnemu sektorju, saj z nižjimi stroški in hitrejšimi transakcijami konkurira tradicionalnim valutam, ki so pod nadzorom nacionalnih bank in bančnim storitvam (Rogojanu & Badea, 2014, str. 112).

Tehnološka infrastruktura finančnih transakcij se hitro spreminja, deloma tudi zaradi novosti, ki so jih uvedle kriptovalute, ki delujejo po sistemu P2P omrežja (Boel, 2016, str. 147). Prednost takšnih sprememb, nastalih s širitvijo uporabe internetnih storitev, je z vidika uporabnikov storitev v povečanju konkurenčnosti ponudnikov finančnih storitev. Avtor Michel Roux v svojem članku (2015, str. 529) kritično razmišlja o inovacijah, ki jih je prinesla uporaba interneta v finančnem sektorju. Intervali sprememb so takšni, da od bank in finančnih institucij zahtevajo prilagoditev novim tehnologijam, ali pa da preprosto nadaljujejo z načinom svojega poslovanja. Te inovacije bi lahko korenito spremenile tradicionalno poslovanje modela poslovnih bank in centralnih bank pri oblikovanju monetarne politike. Avtorica Paola Boel (2016, str. 147) v članku analizira, kako bi lahko tovrstne inovacije vplivale na poslovanje centralnih in poslovnih bank. Vloga tradicionalnih poslovnih bank bi se lahko spremenila in tako bi lahko količina rezerv

neposredno vplivala na višino posojil v gospodarstvu. V kolikor bi plačila preko virtualnih valut začela pridobivati na razsežnosti, bi centralne banke težje vplivale na ponudbo denarja in likvidnost z določitvijo obrestne mere, nadzor plačilnih sistemov bi bil otežen. Centralne banke in nadzorni organi bodo morali spremljati razvoj novih tehnologij in analizirati možne posledice.

Praprotnik (2015) meni, da lahko pozitivni vpliv bitcoina in drugih medijev izmenjave, prisili banke, da znižajo stroške mednarodnih transakcij, ker ponuja možnost zelo poceni prenosa denarja za revnejše ljudi (in njihove sorodnike, ki delajo v tujini, ki so do sedaj morali uporabljati storitve, kot je npr. Western Union money transfer). Hkrati pa bi lahko bitcoin klasične banke prisilil v posodabljanje svojih storitev, ki bi tako postale hitrejše, morda tudi bolj varne in cenejše.

Finančni trgi in bančne institucije ne morejo prepričati ljudem, da izberejo druge metode plačevanja (Rogojanu & Badea, 2014, str. 105), lahko pa se novemu načinu prilagodijo. Tovrstno poslovno priložnost je že prepoznala nemška banka Fidor AG, ki je julija 2013 najavila sodelovanje z nemško bitcoin spletno menjalnico Bitcoin.de. Tovrstno sodelovanje naj bi uporabnikom te virtualne valute olajšalo uporabo plačil z bitcoini, saj bodo le-ti lahko transakcije opravljali neposredno preko plačilnega računa pri banki, nadzor bančnega poslovanja pa naj bi zagotovil varnejše poslovanje. Nemška spletna menjalnica Bitcoin Deutschland GmbH bo tako z namenom, da zagotovi varnost svojih uporabnikov, izpolnjevala vse zakonodajne zahteve, ki veljajo za finančne posrednike, vključno z zahtevami pravil glede preprečevanja pranja denarja. Bitcoin Deutschland GmbH je od 7. avgusta 2013 registriran pri nemškem finančnem nadzorniku BaFin kot finančni posrednik Fidor Bank AG (Rijavec, 2013, str. 20).

Čeprav so bili bitcoin in ostale virtualne valute ustvarjene ravno z namenom, da se izognejo nadzoru centralnih bank, pa je ideja o tem, da bi centralne banke morda ustvarile svoje digitalne valute, med ekonomisti postala privlačna tema razprave. Gledano z makroekonomskega stališča, bi izdaja digitalne valute, ki bi jo izdale centralne banke, vladam in finančnim institucijam omogočila, da bi imele nadzor nad digitalnimi valutami. Takšen nadzor bi omogočil centralnim bankam učinkovitejši nadzor nad porabo sredstev svojih vlagateljev, prav tako bi omogočil posredovanje centralnih bank, ko bi bilo to potrebno, hkrati pa bi zagotavljal pregled nad pobiranjem davkov in izvajanjem pravil v boju proti preprečevanju pranja denarja (Raskin & Yermack, 2016, str. 10-16). Blockchain tehnologija, na kateri temeljijo virtualne valute, ima vsekakor potencial za izboljšanje poslovanja centralnih in poslovnih bank in bo morda služila kot platforma, iz katere bi lahko centralne banke celo začele izdajati svoje digitalne valute. Suverena digitalna valuta bi lahko imela pomembne posledice za bančni sistem (Raskin & Yermack, 2016, str. 15).

ECB ocenjuje, da bi lahko nekateri elementi tehnološke inovacije, kot so jo zasnovale virtualne valute, morda služile kot navdih ali celo podlaga za inovativne plačilne rešitve pri

tradicionalnih ponudnikov plačilnih storitev (ECB, 2015, str. 27). Virtualne valute, ki temeljijo na blockchain tehnologiji, predstavljajo velik izziv in priložnost za centralne banke. V nekaterih gospodarstvih se je bitcoin izkazal za učinkovitega tekmeča proti fiat valutam, ko so se banke soočale z izzivi nezaupanja uporabnikov v bančni sistem (Raskin & Yermack, 2016, str. 10-16).

Vprašanje, ki se postavi je, ali je učinkovitost kriptovalut, kot je bitcoin, mogoče združiti z resničnostjo centralnih bank. Van Alstyne (2014, str. 32) verjame v to, da bodo države stopile korak naprej in morda ponudile svojo kriptovaluto. Bo morda bitdollar, biteuro, bityen ali bitminbi postala nova svetovna rezervna valuta? Prva država, ki se bo približala temu, kar nudi bitcoin, bo naredila tako svojemu gospodarstvu, kot tudi svetu, uslugo.

Guverner Centralne banke Kitajske *Zhou Xiaochuan* meni, da bodo t.i. digitalne valute neizogibno zamenjale gotovino, vendar bo vlada tista, ki bo regulirala in nadzirala kakršnokoli digitalno valuto, ki se bo uporabljala kot zakonito plačilno sredstvo. Digitalna valuta bi morala biti izdana in nadzorovana s strani centralnih bank po enakih načelih, kot je to pri tradicionalnih valutah. Ocenjuje, da bo Kitajska izdala svojo digitalno valuto, ki pa se bo razlikovala od virtualne valute bitcoin. Morda nova valuta ne bo vsebovala blockchain tehnologije, vsekakor pa bo temeljila na naprednih kriptografskih algoritmih, ki se bodo sproti nadgrajevali (BTCC, 2016).

Vlada Velike Britanije se je avgusta 2014 resno lotila proučevanja virtualnih valut ter raziskav koristi, ki jih le-te prinašajo ter tveganj, z namenom zakonske ureditve področja virtualnih valut. V novembru 2014 je objavila razpis, z namenom zbrati čim več mnenj in dokazov o teh vprašanjih, na katerega je bilo prejetih več kot 120 odzivov, s strani uporabnikov, ki uporabljajo virtualne valute, razvijalcev virtualnih valut, družb, ki zagotavljajo storitve, povezane z virtualnimi valutami, odzvale pa so se tudi banke, finančne institucije, akademiki, svetovalne ter druge vladne službe in agencije. Marca 2015 pa je objavila dokument, v katerem povzema številna različna stališča posameznikov in organizacij o prednostih, ki jih virtualna valuta prinaša ter tveganjih, ki jih le-ta predstavljajo. Prav tako je zavzela svoje stališče do posameznega vprašanja (Digital currencies: response to the call for information, 2015).

Ključni koraki, za katere se bo vlada Velike Britanije zavzela, kot izhaja iz objavljenega dokumenta (Digital currencies: response to the call for information, 2015), je spodbujanje konkurence na področju bančništva ter večje inovativnosti pri plačilih. Želijo ustvariti nekakšno vodilno svetovno okolje za razvoj inovativnih plačil in finančne tehnologije. Prav tako bo posebna pozornost namenjena varstvu potrošnikov ter regulativnim ukrepom za boj proti uporabi virtualnih valut v kriminalne namene ter preprečevanju pranja denarja.

Po mnenju Velike Britanije ponujajo virtualne valute, če se uporabljajo zakonito, inovativne, alternativne možnosti plačil, ki lahko konkurirajo obstoječim plačilnim

modelom ter prinašajo številne prednosti, kot so npr. mikroplačila, nakazila v druge države ter čezmorska nakazila. Poleg tega pa je Centralna Banka Anglije že napovedala, da bo sprožila začetek raziskav o možnosti razvoja svoje valute (Digital currencies: response to the call for information, 2015).

Valute se razvijajo skupaj s tehnološkim in gospodarskim razvojem. Premik od blagovnega denarja do kreditnega denarja je naravna posledica razvoja trgovine. Skoraj neizogibno je, da bodo gotovinsko poslovanje zamenjali novi proizvodi in nove tehnologije, ki imajo večjo varnost in nižje stroške. Hiter razvoj sistema interneta in globalnih plačil kaže na to, da bo potrebno izdati digitalno valuto, ki bo izboljšala finančno infrastrukturo in povečala gospodarsko kakovost in učinkovitost (BTCC, 2016).

V zadnjih letih se je v strokovnih krogih pojavila razprava glede potrebe po gotovinskem denarju v sodobnih družbah. Rogoff je predlagal odpravo papirne valute v korist elektronskih transakcij predvsem iz dveh razlogov: brezgotovinsko poslovanje bi lahko omogočilo centralnim bankam, da bi določile negativne obrestne mere, ki bi lahko spodbudile gospodarski razvoj, po drugi strani pa gotovinske transakcije zaradi anonimnosti olajšujejo izogibanje zakonom in plačevanju davkov. S tem bi se ustvarile ovire za sivo ekonomijo, kar bi privedlo do povečanja davčne osnove in prihodkov nacionalnih gospodarstev. Nekaj evropskih držav, kot so npr. Belgija, Grčija, Italija, Španija in Slovaška so že uvedle omejitve za gotovinske transakcije, prav tako Evropska komisija pripravlja strožje ukrepe glede uporabe gotovine (Boel, 2016, str. 148).

Avtorji v članku, ki ga je izdala *Bank of England* (Ali et al., 2014, str. 1), navajajo, da bi lahko ključna inovacija Bitcoin tehnologije, ki temelji na javni elektronski knjigi nakazil oz. blockchain tehnologiji, ki omogoča, da plačilni sistem deluje povsem decentralizirano, brez posrednikov, povzročila širše spremembe v finančnem sistemu transakcij, ki se vse bolj digitalizira. To odpira možnosti za splošno preoblikovanje finančnega sistema. Uporaba blockchain tehnologije v plačilnih sistemih bi lahko spremenila način obračunov in transakcij v bančnem sektorju. Sistem bi lahko postal še bolj revolucionaren, če bi banke sprejele blockchain tehnologijo kot skupinsko verigo transakcij, kar bi lahko olajšalo nadzor nad predpisi, s čimer bi se lahko zagotovila tudi varnost in trdnost plačilnih sistemov (Boel, 2016, str. 153). Decentralizirani pristop pa ni omejen zgolj na izvajanje plačil. Večina finančnih sredstev, kot so posojila, delnice in obveznice, niso več zabeležene v papirni obliki, temveč obstajajo le kot digitalni zapisi. Porazdeljena elektronska knjiga se lahko uporabi v katerikoli vrstah finančnih sredstev, za razliko od sedanje strukture vodenja evidenc, ki potekajo v stopenjski strukturi (evidence računov posameznikov in sredstva rezerv centralnih bank). Teoretično bi bilo mogoče v prihodnosti finančni sistem preoblikovati na način, da se postopoma nadomesti z različnimi porazdeljenimi sistemi (Ali et al., 2014, str. 10).

Blockchain tehnologija bi se lahko sčasoma razširila tudi na druga področja. Zasnova blockchain tehnologije bi lahko pomenila nov pristop k temu, kako si uporabniki med seboj izmenjujejo pravice tudi za druge vrste sredstev, kot so hiše ali delnice, kako se posodablja evidence in plačevanje med uporabniki brez zanašanja na tretjo osebo, ki je zdaj potrebna za to, da se preveri transakcija. Da bi to postalo realnost, pa bi se moralo tehnologiji pridružiti več uporabnikov (Thomas, 2016).

Lahko rečemo, da je bitcoin prvo denarno sredstvo, ki resno izziva sistem tradicionalnih fiat valut. Vsa negotovinska plačila so pred pojavom bitcoina tekla izključno preko finančnih institucij, ki z namenom pravilnosti in poštenosti poslovanja skrbno beležijo vse transakcije ter v skladu z njimi posodablja stanja na osebnih računih uporabnikov, v primeru sporov pa se postavijo v vlogo razsodnika (Upelj, 2013).

Vsekakor pa je odločilnega pomena za uspešen nadaljnji razvoj bitcoina, še vedno v rokah potrošnikov in trgovcev. Glavna prednost z vidika potrošnikov je visoka stopnja zasebnosti. Javna elektronska knjiga nakazil ne vsebuje imen ali osebnih podatkov. Bitcoin naslovi se uporabljajo na način, da je izvedba dejanskega plačila anonimna in tako se potrošnikom ni treba bati kraje informacij. Poleg tega imajo potrošniki popoln nadzor nad svojim denarjem, kar lahko poveča zaupanje potrošnikov v spletna plačila (Eikmanns & Sandner, 2015, str. 7).

V primeru nakupa blaga in storitev preko spleta, bitcoin znižuje negotovost goljufivih transakcij. Transakcije v sistemu Bitcoin zagotavljajo, da se plačila ne morejo ponovno obračunati, ko je enkrat plačilo vključeno v blok in dodano k verigi blokov. Posledično lahko trgovci prihranijo administrativne stroške, povečajo marže ali znižajo cene njihovim izdelkom ali storitvam. Prednost Bitcoin tehnologije se kaže tudi v tem, da se posamezna enota bitcoin lahko razdeli na skorajda neskončne frakcije, kar omogoča plačevanje mikroplačil.

Bitcoin je še posebej privlačen za mala podjetja, ki iščejo načine za zniževanje stroškov transakcij. Čeprav je uporaba kreditnih kartic mnogo lažja za uporabnike, pa morajo trgovci plačevati različne avtorizacijske stroške, transakcijske stroške, provizije ter druge stroške, povezane s kartičnim poslovanjem. Provizije znašajo običajno 2 do 3 odstotke za transakcijo. Nepovratnost transakcij omogoča trgovcem, da se izognejo tudi goljufijam, pri katerih potrošniki trdijo, da niso prejeli izdelka ali da storitev ni bila opravljena (Tsukerman, 2015, str. 1141).

Eden izmed pomembnejših izzivov, s katerimi se sooča bitcoin, je pomanjkanje sprejetja valute med uporabniki. Dokler obstaja le malo potrošnikov, ki uporabljajo bitcoin, pri trgovcih ni potrebe, da bi sprejemali to valuto. Hkrati pa velja tudi obratno. Dokler je le nekaj trgovcev, ki sprejemajo bitcoin kot plačilno sredstvo, potrošniki nimajo razloga, da bi pridobili bitcoine (Eikmanns & Sandner, 2015, str. 8).

Mnogi kritiki menijo, da je ravno nestanovitnost valute bitcoin glavni razlog, zakaj le-ta ni širše sprejet med trgovci in uporabniki. Eden izmed razlogov, zakaj ni bitcoin bolj množično sprejet med uporabniki, je tudi nezaupanje potrošnikov. Ker bitcoin ne podpira nobena centralna avtoriteta, prav tako ga še vedno ne sprejema dovolj trgovcev, je morda težko prepričati posameznike, naj zaupajo svoje premoženje virtualnim valutam (Turpin, 2014, str. 348). Trgovci zaradi nestabilnosti menjalnega tečaja tvegajo izgube vrednosti prejetih sredstev, ko le-te pretvorijo v fiat valute.

Na tržišču pa že delujejo podjetja, ki omogočajo uporabnikom, da imajo sredstva shranjena v fiat valutah pri ponudniku takšne storitve, uporabnik pa lahko plačuje v bitcoinih. Primer takšnega ponudnika je podjetje Bitreserve (Swan, 2015, str. 6). Prav tako so trgovcem že na voljo plačilni posredniki, ki jim omogočajo sprejemanje plačil v bitcoinih, ne da bi jih dejansko prejeli, s čimer se izognejo tveganju izgube sredstev zaradi nestanovitnosti menjalnega tečaja.

Avtorji Tasca, Liu in Hayes (2016, str. 40) so naredili raziskavo omrežja plačil z bitcoin, po kateri je bilo ugotovljeno, da se mreža uporabnikov širi in je glede na pretekla leta, bolj dozorela.

Eden od pomislekov zoper kriptovalute je, da je to le »lastništvo številke z zanimivimi matematičnimi lastnostmi«. Vendar pa lahko tudi na lastništvo konvencionalnega denarja gledamo kot le na »lastništvo papirja« - valutam vrednosti ne daje nosilec, temveč zaupanje vanje. Nihanje cene in špekulativnost virtualnih valut se nič ne razlikuje od že videnege v sodobni ekonomiji. Tveganje izgube denarja prav tako obstaja pri vseh valutah. Završnik (2015, str. 1-2) meni, da se večja težava zdi dejstvo, da naj bi bilo na manj kot tisoč največjih bitcoin računih več kot 50 odstotkov vseh bitcoinov ter dejstvo, da so lastniki ob padanju vrednosti »zaklenjeni« v lastništvo nad vse manj vredno številko. Shema spominja na že videno pri udeležencih denarnih verig.

Glavni problem pri bitcoinu je torej, da precej niha v vrednosti in da ga še ne sprejema dovolj trgovcev. Zaradi te nestanovitnosti ni in ne more biti prava valuta (Praprotnik, 2015), hkrati pa je izpostavljen pranju denarja ter izogibanju davčnim obveznostim, zaradi česar kritiki dvomijo, da bi lahko bitcoin kdaj prevzel klasične denarne trge in nadomestil dolar ali evro.

Morda bo bitcoin nadomestila druga virtualna valuta. Vsekakor pa dejstva, da je bitcoin revolucionarno posegel na področje denarnih plačil na globalni ravni, ni mogoče zanikati. Svet se nenehno spreminja, vladni organi in podjetja pa bodo morala, če bodo želela ohranjati svoje pozicije moči, slediti tem spremembam (Turpin, 2014, str. 368).

Nobenega zagotovila ni, da bo bitcoin valuta prihodnosti, ki bo uspešno konkurirala obstoječim plačilnim sistemom. V tej fazi se bitcoin še vedno razvija in si utira svoj prostor

pod soncem. Še vedno predstavlja uganko tako mnogim potencialnim uporabnikom po vsem svetu, ki se s tovrstno valuto šele spoznavajo, trgovcem, ki so morda skeptični do sprejema te valute v zameno za nakup dobrin ali storitev ter regulatornim organom in organom pregona, ki poskušajo v zakonske okvire umestiti delovanje novitete, ki pa se med uporabniki nezadržno širi.

Na razvoj prihodnjih dogodkov ne moremo vplivati. V tej fazi še vedno ni jasno, kaj se bo v prihodnosti dogajalo z bitcoinom. Ne glede na to, kaj prinašajo prihodnji izzivi na področju plačilnih sistemov, pa si vsekakor moramo priznati, da je njegov vpliv revolucionarno spremenil naš pogled na to, kako razmišljamo o denarju in plačilih. Tudi če bitcoin ne bo preživel kot valuta, si moramo priznati, da bodo tehnologije, ki jih je načrtal sistem Bitcoina, preživele.

## **SKLEP**

Pojav virtualnih valut sovпада z vse hitrejšim tehnološkim razvojem in nezaupanjem ljudi v obstoječe plačilne sisteme. Izguba zaupanja v tradicionalne bančne sisteme, visoki stroški transakcij, regulative posameznih držav, nizke obrestne mere in negotovost nekaterih obstoječih valut so povzročili, da uporabniki iščejo nove, alternativne oblike plačevanja dobrin in storitev, kar je prispevalo k iskanju cenejših in hitrejših načinov plačevanja, ki so neodvisni od tradicionalnih bank in dosedanjih plačilnih sistemov.

Bitcoin, kot prva decentralizirana kriptografska virtualna valuta se je pojavila s sovpadom bančne krize v letu 2008. Ideja o nastanku je temeljila na nekaj že predhodnih poizkusih uvedbe elektronskega denarja, pa vendar lahko rečemo, da bitcoin predstavlja revolucijo na področju plačilnih sistemov. Virtualne valute bitcoin ne izdaja noben osrednji centralni organ, njena emisija poteka po sistemu vrstniškega P2P omrežja na podlagi zahtevnih matematičnih algoritmov, kjer prenos transakcij poteka od uporabnika do uporabnika, po protokolu, ki ga je zasnoval avtor pod imenom Satoshi Nakamoto v letu 2008. Ključni inovativni vidik Bitcoin tehnologije je javna veriga vseh zabeleženih transakcij, imenovana blockchain tehnologija. Vsaka transakcija se zabeleži v javno verigo blokov, s čimer je moč preveriti vsako transakcijo v omrežju. Sistem odpravlja problem dvojne porabe, ki ga do sedaj, brez posrednikov ni bilo mogoče rešiti. V nekaj letih je njegova uporaba doživela razcvet in povzročila zanimanje širše javnosti.

Zasnova sistema Bitcoin je kasneje spodbudila razvijalce kriptografskih valut, da so se v nekaj letih na trgu pojavile številne kriptografske virtualne valute, med katerimi ima bitcoin, z več kot 80 % tržnega deleža med virtualnimi valutami, prevladujočo vlogo.

Tehnologija virtualnih valut, ki poteka preko decentraliziranega omrežja, ponuja uporabnikom številne prednosti, ki jih dosednji načini plačil niso omogočili. Omogoča

varen prenos denarnih sredstev direktno od uporabnika, do uporabnika, brez posredovanja osrednjega centralnega organa, kot so plačilni posredniki in finančne institucije, s čimer se bistveno zmanjšajo stroški pošiljanja nakazil. Transakcije se potrjujejo hitreje od dosedanjih plačilnih sistemov. Medtem ko transakcije preko finančnih institucij potrebujejo tudi nekaj dni, da se odobrijo in potrdijo, je zasnova protokola Bitcoin zasnovana na način, da je potreben čas za odobritev posamezne transakcije le okoli 10 minut. Virtualne valute omogočajo cenejša in hitrejša mednarodna nakazila ter dostop do bančnih storitev za uporabnike v državah v razvoju, kjer je dostop do bančnih storitev še vedno zelo omejen. Deljivost enote bitcoin omogoča plačevanje mikroplačil, ki do sedaj niso bila mogoča, zaradi visokih stroškov finančnih nakazil.

Po drugi strani virtualne valute predstavljajo številna tveganja, tako za uporabnike, obstoječe plačilne sisteme, kot tudi njihova široka uporaba v kriminalne dejavnosti, pranje denarja in davčne utaje. Številne pasti, ki jih ponuja virtualna valuta in nepričakovan razmah njene uporabe med uporabniki, so pritegnili pozornost tako vladnih organov, centralnih bank, organov pregona in drugih strokovnih institucij, ki spremljajo razvoj dogodkov in poskušajo umestiti to noviteto v zakonske okvire.

Nad virtualnimi valutami nima nadzora nobena centralna banka, vendar jih centralne banke in druge finančne institucije širom sveta budno spremljajo in ocenjujejo njihov vpliv na obstoječe plačilne sisteme, saj bi lahko povečana uporaba virtualnih valut, kot je bitcoin, ogrozila obstoječe plačilne sisteme. Po dosedanjih analizah ECB ocenjuje, da trenutno virtualne valute ne predstavljajo grožnje obstoječemu finančnemu sistemu, saj je obseg trgovanja v tej fazi še nezadosten, da bi lahko znatno vplival na obstoj obstoječih finančnih trgov. Kljub temu, pa centralne banke podajajo svoje mnenje in opozarjajo na številne pasti, ki jih ponujajo virtualne valute, tako z vidika uporabnikov, ki so lahko izpostavljeni številnim tveganjem, kot tudi z vidika opozoril finančnim institucijam.

Zaradi razširjene uporabe virtualnih valut pa so zaskrbljeni tudi organi pregona, saj se virtualne valute zaradi narave svoje anonimnosti in decentraliziranosti, zlorabljujejo tudi v kriminalne dejavnosti, za nezakonite dejavnosti na črnem trgu, kot so trgovanje z drogami ali orožjem. Njihovo delovanje poteka preko podzemnih spletnih tržnic, ki delujejo preko nevidnega omrežja s pomočjo programske opreme TOR, ki pomaga zakriti IP naslov uporabnika. Najbolj znana t.i. podzemna tržnica je bila spletna stran, pod imenom Silk Road, ki je delovala od januarja 2011 do oktobra 2013, ko je FBI po dve leti trajajoči preiskavi, uspešno zaprl spletno stran in aretiral njenega ustanovitelja. Vendar pa zaprtje Silk Rooda ni odpravilo problema trgovanja na črnem trgu, saj so se pojavile nove podzemne spletne strani, ki se uporabljajo za nezakonite dejavnosti, edino plačilno sredstvo na teh tržnicah pa je valuta bitcoin. Virtualne valute se zaradi hitrosti transakcij, globalnega omrežja ter pomanjkanja regulative in nadzora na tem področju uporabljajo tudi za pranje denarja, ki je bil pridobljen s kaznivimi dejanji in za davčne utaje.



Eden izmed dejavnikov tveganja je visoka nestanovitnost vrednosti virtualne valute bitcoin, katere cena se določa na podlagi ponudbe in povpraševanja na spletnih menjalnicah. Vrednost je v zadnjih letih močno nihala in povzročila nekaj cenovnih mehurčkov, kar je povzročilo, da na trgu še vedno prevladujejo špekulativni uporabniki, ki kopičijo valuto, z namenom, da bo vrednost valute sčasoma narasla.

Uporabniki so še vedno previdni pri pretvorbi svojih fiat valut v valuto bitcoin, saj s tem tvegajo izgubo svojih sredstev, bodisi zaradi svoje nepazljivosti oz. neustrezne zaščite svojih digitalnih ključev, bodisi zaradi odmevnih medijskih poročanj o vdorih v spletne menjalnice in v spletne strani ponudnikov spletnih denarnic.

Eden izmed pomembnejših izzivov, s katerimi se sooča bitcoin, je pomanjkanje sprejetja valute med uporabniki. Visoka nestanovitnost vrednosti valute bitcoin je eden izmed razlogov, da ni širše sprejeta med uporabniki. Po mnenju nekaterih pa se bitcoin še vedno razvija ter še ni dosegel faze zrelosti. Nihanje vrednosti se lahko sčasoma umiri, ko bo tehnologija širše sprejeta med uporabniki. Ravno visoka nestanovitnost vrednosti valute bitcoin pa je po mnenju nekaterih kritikov pglavitni razlog, zakaj ni valuta širše sprejeta med uporabniki. Zaradi razvoja elektronskega poslovanja lahko pričakujemo, da se bo zaupanje potrošnikov v virtualne valute povečalo, s čimer bi se zmanjšala tudi nestanovitnost vrednosti same valute.

Širša sprejetost s strani uporabnikov in trgovcev bi lahko povzročila tudi večjo stabilnost njene vrednosti, s čimer bi se povečalo zaupanje uporabnikov v to valuto. Na trgu so se že pojavila številna inovativna podjetja, ki delujejo kot posredniki, preko katerih lahko uporabniki in trgovci uporabljajo bitcoin brez tveganja izgube sredstev zaradi visoke nestanovitnosti pri menjavi sredstev v fiat valute.

Področje ob vsej svoji razsežnosti zbuja interes zakonodajalcev. Nekatere države so že uredile področje zakonodaje, ki zadeva predvsem zakonsko ureditev poslovanja spletnih menjalnic in drugih ponudnikov storitev virtualnih valut. Tako je v številnih državah potrebno pridobiti licenco za trgovanje z virtualnimi valutami ter zadostiti kriterijem, v skladu z zakonodajo boja proti preprečevanju pranja denarja in financiranja terorizma. Z namenom preprečitve zlorabe virtualnih valut v kriminalne namene, ki se zaradi svojih značilnosti izvajajo tudi na globalni ravni, bi bilo smotrno proučiti možnost enotne uskladitve regulatornih ukrepov z drugimi državami, da ne bi prihajalo do nasprotujočih si ukrepov med državami.

Izziv za regulatorne organe je, kako urediti področje delovanja virtualnih valut, ne da bi s tem ogrozili njihov obstoj. Prestroga regulacija in poseg regulatornih organov bi lahko odvrnila uporabnike od širše uporabe virtualnih valut. Tako bi po vsej verjetnosti uporabniki začeli iskati nove načine in poti plačevanja. Virtualne valute so bile ustvarjene ravno z namenom, da se izognejo strogim birokratskim omejitvam in pretogim bančnim

strategijam, ki niso sledile koraku s časom. Posebno pozornost bi bilo potrebno nameniti ravno varstvu potrošnikov ter področju ureditve spletnih menjalnic ter ponudnikov avtomatov, preko katerih se sredstva, pridobljena s kaznivimi dejanji operejo na način, da se pretvorijo v fiat valute, s čimer se zabrišejo sledi denarnih transakcij.

Po mnenju nekaterih pa je transparentnost nakazil, preko katerih se lahko izsledi uporabnika, še vedno bolj učinkovita pri odkrivanju in preprečevanju uporabe virtualnih valut v nezakonite namene, kot sledenje gotovinskih transakcij. Sčasoma bodo tudi organi pregona pričeli uporabljati javne evidence verige nakazil, preko katerih bodo sledili denarnemu toku in tako preprečili zlorabo virtualnih valut v nezakonite dejavnosti. Dosedanje izkušnje kažejo, da tudi organi pregona žanjejo uspehe v boju proti zatiranju kriminala.

Čeprav so sprva na trgu prevladovali tehnološki navdušenci, kriptografski strokovnjaki ter špekulativni uporabniki, se po mnenju nekaterih zdaj s tem ukvarjajo velika podjetja, ki svoje poslovanje prilagajajo zahtevanim predpisom. To velja tudi za spletne menjalnice, ki morajo po nekaterih zakonodajah pridobiti licenco za trgovanje in zadostiti vsem kriterijem, v skladu z zakonodajo. Zaradi konkurence se spletne menjalnice in drugi posredniki tovrstnih storitev trudijo pridobiti zaupanje uporabnikov z varnejšimi načini shranjevanja sredstev na računih svojih uporabnikov ter z zaščito pred vdori v sistem menjalnice.

Nova tehnologija, na kateri temelji zasnova bitcoina, pa je sprožila tudi pozitiven odziv v bančnem sektorju. Tehnološki razvoj od bank in finančnih institucij zahteva prilagoditev novim tehnologijam, ki zahtevajo hitrejše, cenejše in dostopnejše poti do uporabnikov. Banke in finančne institucije pa že razmišljajo o uvedbi blockchain tehnologije tudi na druga področja vodenja javnih evidenc in ostalih storitev.

Strokovni krogi večinoma priznavajo prednosti nove tehnologije, saj se zavedajo, da morajo znižati stroške na področju plačil in pri vodenju evidenc, če hočejo uspešno konkurirati na trgu, pa vendar se zdi, da centralne banke ne bodo izpustile nadzora nad nacionalnimi valutami. Tako mnoge centralne banke razmišljajo, da bi uvedle svoje virtualne valute, ki bi bile pod njihovim nadzorom, in tako bi lahko obdržale vpliv in nadzor nad finančnimi sistemi. Nekaterе države že vlagajo sredstva v raziskave in razvoj, da bi ustvarile svoje valute, ki bi jim zagotavljale prednosti nove tehnologije v boju za zniževanje stroškov in večjo konkurenčnost. Še vedno pa bi bile to nacionalne valute, le da bi se spremenil način plačil v skladu z novimi tehnologijami.

Nove tehnologije vsekakor silijo vladne organe in finančne institucije, da izberejo poti, ali bodo te novosti prepovedale, dopustile ali na podlagi novih tehnologij razvile svoje virtualne valute. V večini razvitih gospodarstev centralne banke proučujejo možnosti vključitve virtualnih valut v svoje poslovanje. Kljub vsemu pa je blockchain tehnologija še

vedno v povojih. Tako radikalen predlog uvedbe virtualne valute v finančni sistem, se zdi še vedno precejšnje tveganje za preostali del finančnega sistema.

Bitcoin, kot prva decentralizirana virtualna valuta, je vsekakor povzročila revolucijo ne samo na področju plačil in načinu razmišljanja, pač pa je njena inovativna tehnologija, na kateri sloni, pritegnila zanimanje širše strokovne javnosti in možnosti vključitve uporabe tudi na druga področja. Tehnologija se nenehno spreminja in pričakovati je, da se bo uporaba virtualnih valut sčasoma povečala in uveljavila kot plačilno sredstvo. Morda bo bitcoin nadomestila druga virtualna valuta, vendar pa dejstva, da je bitcoin revolucionarno posegel na področje plačilnih sistemov, ni mogoče zanikati.

## LITERATURA IN VIRI

1. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, Q3.
2. Allen, H. J. (2015). *\$=€=Bitcoin?* Boston: Suffolk University Law School. Legal Studies Research Paper Series, Research Paper 15-33.
3. Anning, P., Brazell, L., Brailsford, M., Brito, J., Cleary, M. J., Friedman, J., Hoegner, S., Taylor, M., Straus, R. J., & Von Unruh C. N. (2015). *The Law of Bitcoin*. Bloomington: iUniverse.
4. Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital crypto-currencies*. Sebastopol: O'Reilly Media.
5. Banka Slovenije. (2014, 8. januar). *Opozorilo uporabnikom z dne 12. 12. 2013*. Najdeno 29. maja 2016 na spletnem naslovu <https://www.bsi.si/informacije-za-potrosnike.asp?MapaId=1562>
6. Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. *International Conference on Financial Cryptography and Data Security* (str. 399-414). Springer Berlin Heidelberg.
7. Barnett, E. R. (2014). Virtual Currencies: Safe for Business and Consumers or just for Criminals? Haag: *13th European Security Conference & Exhibition*. April 2, 2014.
8. BBC. (2016, 2. maj). *Australian Craig Wright claims to be Bitcoin creator*. Najdeno 6. maja 2016 na spletnem naslovu <http://www.bbc.com/news/technology-36168863>
9. *Bitcoin History*. Najdeno 25. maja 2016 na spletnem naslovu <https://coin.co/bitcoin-guide/history>
10. *Bitlegal*. Najdeno 28. maja 2016 na spletnem naslovu <http://bitlegal.io/>
11. *Bitlegal: Russia*. Najdeno 16. julija 2016 na spletnem naslovu <http://map.bitlegal.io/nation/RU.php>
12. *Blockchain Charts*. Najdeno 23. marca 2016 na spletnem naslovu <https://blockchain.info/sl/charts>
13. Boel, P. (2016). Thinking about the future of money and potential implications for central banks. *Sveriges Riksbank Economic Review*, 1 (str. 147-158). Stockholm: Claes Berg.
14. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29(2), 213-238.
15. Brito, J., & Castillo, A. (2013). *Bitcoin: A primer for policymakers*. Arlington: George Mason University.
16. Brito, J., Shadab, H., & Castillo, A. (2014). Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling. *Columbia: Science & Technology Law Review*, 16, 144-221.
17. Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. SAGE Publications. *The Police Journal: Theory, Practice and Principles*, 1–13.

18. BTCC. (2016, 16. februar). *China's Central Bank Governor Says Digital Currencies Will Inevitably Replace Cash*. Najdeno 4. junija 2016 na spletnem naslovu <https://www.btcc.com/news/article/chinas-central-bank-governor-says-digital-currencies-will-inevitably-replace-cash>
19. Caetano, R. (2015). *Learning Bitcoin*. Birmingham: Packt Publishing Ltd.
20. Christin, N. (2012). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. Pittsburgh: Carnegie Mellon University.
21. Ciancaglini, V., Balduzzi, M., McArdle, R., & Rösler, M. (2015). *Below the Surface: Exploring the Deep Web*. *Trend Micro*. Najdeno 21. marca 2016 na spletnem naslovu [http://www.cybersecurityconference.co.uk/system/files/protected/whitepaper/Trend%20Micro%20-%20wp\\_below\\_the\\_surface.pdf](http://www.cybersecurityconference.co.uk/system/files/protected/whitepaper/Trend%20Micro%20-%20wp_below_the_surface.pdf)
22. *Coin ATM Radar*. Bitcoin ATM map. Najdeno 25. maja 2016 na spletnem naslovu <https://coinatmradar.com/>
23. Coindesk. (2015, 19. oktober). *How to Store Your Bitcoins*. Najdeno 19. maja 2016 na spletnem naslovu <http://www.coindesk.com/information/how-to-store-your-bitcoins/>
24. *Coinmap*. Najdeno 3. julija 2016 na spletnem naslovu <https://coinmap.org/#/world/46.05045290/14.50826210/8>
25. Coinmarketcap. (2016). *Crypto-Currency Market Capitalizations*. Najdeno 2. marca 2016 na spletnem naslovu <http://coinmarketcap.com/currencies/>
26. Colley LLP. (2016). *The Regulation of Virtual, Digital and Crypto-currencies*. Najdeno 9. marca 2016 na spletnem naslovu <https://www.cooley.com/70734>
27. Darlington III, J. K. (2014). *The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis*. Knoxville: University of Tennessee.
28. Digital currencies: response to the call for information. (2015). *London: HM Treasury*. Najdeno 21. marca 2016 na spletnem naslovu [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/414040/digital\\_currencies\\_response\\_to\\_call\\_for\\_information\\_final\\_changes.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf)
29. European Banking Authority. (2014, 4. julij). *EBA Opinion on 'virtual currencies'*. *EBA/Op/2014/08*. Najdeno 7. marca 2016 na spletnem naslovu <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
30. European Central Bank. (2012, oktober). *Virtual Currency Schemes*. Frankfurt: European Central Bank. Najdeno 9. februarja 2016 na spletnem naslovu <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
31. European Central Bank. (2015, februar). *Virtual currency schemes – a further analysis*. Najdeno 20. maja 2016 na spletnem naslovu <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
32. Evropski bančni organ. (2013, 12. december). *Opozorilo uporabnikom v zvezi z navideznimi valutami*. Najdeno 7. marca 2016 na spletnem naslovu [https://www.eba.europa.eu/documents/10180/598420/EBA\\_2013\\_01030000\\_SL\\_TRA.pdf](https://www.eba.europa.eu/documents/10180/598420/EBA_2013_01030000_SL_TRA.pdf)

33. Eikmanns, B. C., & Sandner, P. G. (2015). *Bitcoin: The Next Revolution in International Payment Processing? An Empirical Analysis of Potential Use Cases*. Najdeno 21. maja 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2619759](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2619759)
34. EUROPOL. (2015a). *Alternativne bančne platforme*. Najdeno 23. maja 2016 na spletnem naslovu [https://issuu.com/martinksinan/docs/brozurka\\_slo](https://issuu.com/martinksinan/docs/brozurka_slo)
35. EUROPOL. (2015b). *The Internet Organised Crime Threat Assessment (iOCTA)*. Najdeno 28. marca 2016 na spletnem naslovu <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>
36. Evropska komisija. (2016, 2. februar). *Sporočilo Komisije Evropskemu parlamentu in Svetu o akcijskem načrtu za okrepitev boja proti financiranju terorizma*. Strasbourg: COM(2016) 50 final. Najdeno 20. avgusta 2016 na spletnem naslovu <http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52016DC0050>
37. Evropski parlament. (2016, 26. maja). *Virtualne valute. Resolucija Evropskega parlamenta z dne 26. maja 2016 o virtualnih valutah (2016/2007(INI))*. Bruselj. Najdeno 28. avgusta 2016 na spletnem naslovu <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0228+0+DOC+PDF+V0//SL>
38. The Financial Action Task Force Report. (2014, junij). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Najdeno 12. marca 2016 na spletnem naslovu <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
39. The Financial Action Task Force. (2015, junij). *Guidance for a risk-based approach. Virtual Currencies*. Najdeno 20. junija 2016 na spletnem naslovu <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
40. Federal Bureau of Investigation. (2012, 24. april). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Washington: Federal Bureau of Investigation. Najdeno 26. marca 2016 na spletnem naslovu <http://cryptome.org/2012/05/fbi-bitcoin.pdf>
41. FinCEN. (2013) *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. Najdeno 9. marca 2016 na spletnem naslovu [http://www.fincen.gov/statutes\\_regs/guidance/pdf/FIN-2013-G001.pdf](http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf)
42. FinCEN. (2014). *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*. Najdeno 16. julija 2016 na spletnem naslovu <https://www.fincen.gov/sites/default/files/shared/FIN-2014-R012.pdf>
43. Folkinshteyn, D., Lennon, M., & Reilly, T. (2015). The Bitcoin Mirage: An Oasis of Financial Remittance. *Journal of Strategic and International Studies*, 10(2), 118-124.
44. Finančna uprava Republike Slovenije. (2013, 23. december). *Davčna obravnava poslovanja z virtualno valuto po ZDoh-2 in ZDDPO-2*, Pojasnilo DURS, št. 4210-11634/2013, 23. 12. 2013. Najdeno 6. maja 2016 na spletnem naslovu [74](http://www.racunovodstvo.net/pojasnila/4835/davcna-obravnavaposlovanjaz-</a></li>
</ol>
</div>
<div data-bbox=)

virtualno-valuto-po-zdoh-2-in-zddpo-2-pojasnilo-durs-st-4210-11634-2013-23-12-2013

45. Finančna uprava Republike Slovenije. (2015, 7. december). *Obravnava provizije pri prodaji "bitcoinov" po ZDDV-1*. Najdeno 27. maja 2016 na spletnem naslovu [http://www.fu.gov.si/fileadmin/Internet/Davki\\_in\\_druge\\_dajatve/Podrocja/Davek\\_na\\_dodano\\_vrednost/Novice/2015/Obravnava\\_provizije\\_pri\\_prodaji\\_bitcoinov\\_po\\_ZDDV-1.pdf](http://www.fu.gov.si/fileadmin/Internet/Davki_in_druge_dajatve/Podrocja/Davek_na_dodano_vrednost/Novice/2015/Obravnava_provizije_pri_prodaji_bitcoinov_po_ZDDV-1.pdf)
46. Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, 4, 159-208.
47. Guadamuz, A., & Marsden, C. (2015). Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, 20(12).
48. Gup, B. E. (2014). *What Is Money? From Commodities to Virtual Currencies/ Bitcoin*. Najdeno 20. julija 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2409172](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172)
49. Hernandez-Verme, P. L., & Valdes-Benavides, R. A. (2013). Virtual currencies, Micropayments and the payments systems: a challenge to fiat money and monetary policy? *European Scientific Journal*, 9(19), 325-343.
50. Huš, M. (2016, 10. julij). *Za rudarje odslej dvakrat manj bitcoinov*. Najdeno 20. julija 2016 na spletnem naslovu <https://slo-tech.com/novice/t677523#crt>
51. *History of Bitcoin*. Najdeno 23. marca 2016 na spletnem naslovu <http://historyofbitcoin.org/>
52. Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*. Najdeno 20. julija 2016 na spletnem naslovu <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.5595&rep=rep1&type=pdf>
53. Lemos, M. (2013). *What factors influence the value of Bitcoin?* Najdeno 28. marca 2016 na spletnem naslovu <http://www.quora.com/Bitcoin/What-factors-influence-the-value-of-Bitcoin>
54. Lloyd's. (2015). *Bitcoin. Risk factors for insurance. Emerging Risk Report*. Najdeno 20. maja 2016 na spletnem naslovu <https://www.lloyds.com/~~/media/files/news%20and%20insight/risk%20insight/2015/bitcoin%20%20final.pdf>
55. Luther, W. J., & White, L. H. (2014). *Can Bitcoin Become a Major Currency?* Najdeno 22. maja 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/Papers.cfm?abstract\\_id=2446604](https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2446604)
56. Ly, M. K. M. (2014). Coining Bitcoin's Legal-Bits: Examining the Regulatory Framework for Bitcoin and Virtual Currencies. *Harvard Journal of Law & Technology*, 27(2), 587-608.
57. Marian, O. (2013). Are Cryptocurrencies Super Tax Havens? *Michigan Law Review First Impressions*, 112(1), 38-48.
58. Mikołajewicz-Woźniak, A., & Scheibe, A. (2015). Virtual currency schemes—the future of financial services. *Foresight*, 17(4), 365-377.

59. Mishkin, F. S. (2004). *The Economics of Money, Banking, and Financial Markets* (7<sup>th</sup> ed.). Boston: Pearson.
60. Moore, T., & Christin, N. (2013). *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*. Najdeno 19. julija 2016 na spletnem naslovu <http://tylermoore.ens.utulsa.edu/fc13pres.pdf>
61. Murphy, E. V., Murphy, M. M., & Seitzinger, M. V. (2015). *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. Washington D.C.: Library of Congress. Congressional Research Service, 7-5700.
62. Nakamoto, S. (2008). *Bitcoin: A Peer-to-peer Electronic Cash System*. Najdeno 8. februarja 2016 na spletnem naslovu <https://bitcoin.org/bitcoin.pdf>
63. Nigh, B., & Pelker, A. (2015). FBI - Virtual Currency: Investigative Challenges and Opportunities. *FBI Law Enforcement Bulletin*. Najdeno 16. julija 2016 na spletnem naslovu <https://leb.fbi.gov/2015/september/virtual-currency-investigative-challenges-and-opportunities>
64. Ogunbadewa, A. (2014). *The Virtues and Risks Inherent in the 'Bitcoin' Virtual Currency*. Cardiff University.
65. Papp, J. (2014). A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for the Growth of E-Commerce. *Pittsburgh: Journal of Technology Law and Policy*, 15(1), 33-56.
66. Pérez-Marco, R. (2016). *Bitcoin and Decentralized Trust Protocols*. Najdeno 2. avgusta 2016 na spletnem naslovu <https://arxiv.org/pdf/1601.05254.pdf>
67. Peters, G. W., Panayi, E., & Chapelle, A. (2015, 19. avgust). *Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective*. Najdeno 19. maja 2016 na spletnem naslovu <https://arxiv.org/pdf/1508.04364.pdf>
68. Plassaras, N. A. (2013). Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. *Chicago Journal of International Law*, 14(1), 377-407.
69. Polasik, M., Piotrowska, A., Wisniewski, T. P., Kotkowski, R., & Lightfoot, G. (2015). *Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry*. Najdeno 26. maja 2016 na spletnem naslovu [https://www.researchgate.net/profile/Michal\\_Polasik/publication/280570108\\_Price\\_Fluctuations\\_and\\_the\\_Use\\_of\\_Bitcoin\\_An\\_Empirical\\_Inquiry/links/55ba961308aed621de0ad360.pdf](https://www.researchgate.net/profile/Michal_Polasik/publication/280570108_Price_Fluctuations_and_the_Use_of_Bitcoin_An_Empirical_Inquiry/links/55ba961308aed621de0ad360.pdf)
70. Praprotnik, A. (2015, 6. marec). *Bitcoin – ali lahko (pre)živimo brez bank?* Najdeno 27. marca 2016 na spletnem naslovu <http://damijan.org/2015/03/06/bitcoin-ali-lahko-prezivimo-brez-bank/>
71. Raskin, M., & Yermack, D. (2016). *Digital Currencies, Decentralized Ledgers, and the Future of Central Banking*. Najdeno 9. avgusta 2016 na spletnem naslovu <http://www.nber.org/papers/w22238.pdf>
72. Regulation of Bitcoin in Selected Jurisdictions. (2014, januar). *The Law Library of Congress, Global Legal Research Center*. Najdeno 21. marca 2016 na spletnem naslovu <https://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>



73. Richter, C., Kraus, S., & Bouncken, R. B. (2015). Virtual Currencies Like Bitcoin As A Paradigm Shift In The Field Of Transactions. *The International Business & Economics Research Journal*, 14(4), 575-586.
74. Rijavec, A. (2013). Razvoj virtualnih valut in izzivi, ki jih ta prinaša. *Bančni vestnik*, 62(10), 17-23.
75. Rogošanu, A., & Badea, L. (2014). The issue of competing currencies. Case study - Bitcoin. *Theoretical and Applied Economics*, 21(1), 103-114.
76. Roux, M. (2015). Finance Otherwise: The End of Banks? *Monetary Policy in the Context of the Financial Crisis: New Challenges and Lessons. International Symposia in Economic Theory and Econometrics*, 24, 517-536. Emerald Group Publishing Limited.
77. Santos, M. (2013, 13. november). *Hacker steals Bitcoins from 4.000 wallets hosted by the exchange Bitcash.cz*. Najdeno 7. avgusta 2016 na spletnem naslovu <https://99bitcoins.com/hacker-steals-bitcoins-from-4000-wallets-hosted-exchange-bitcash-cz>
78. Simonite, T. (2012, 21. marec). Bitcoin seeks new life in Africa. *Technology Review*. Najdeno 29. julija 2016 na spletnem naslovu [https://www.technologyreview.es/printer\\_friendly\\_article.aspx?id=39829](https://www.technologyreview.es/printer_friendly_article.aspx?id=39829)
79. *Some Factors That Influence The Bitcoin Price*. Najdeno 15. junija 2016 na spletnem naslovu <http://totalbitcoin.org/some-factors-that-influence-the-bitcoin-price/>
80. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol: O'Reilly Media.
81. Szczepański, M. (2014). Bitcoin: Market, economics and regulation. *European Parliamentary Research Service, Briefing*.
82. Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities, and Risks*. Najdeno 16. junija 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/Papers.cfm?abstract\\_id=2657598](https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2657598)
83. Tasca, P. (2016, 29. februar). *The Dual Nature of Bitcoin as Payment Network and Money. VI Chapter SUERF Conference Proceedings 2016/1 "Cash on Trial" by Christian Beer, Ernest Gnan and Urs W. Birchler*, 68-73. Najdeno 16. junija 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2805003](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2805003)
84. Tasca, P., Liu, S., & Hayes, A. (2016). *The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships*. Najdeno 29. avgusta 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2808762](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762)
85. Thomas, Z. (2016, 6. maj). Does Bitcoin still matter? *BBC News*. Najdeno 23. maja 2016 na spletnem naslovu <http://www.bbc.com/news/technology-36197703>
86. Trautman, L. J. (2014). Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law and Technology*, 20(4).
87. Trautman, L. J., & Harrell, A. C. (2016, 18. julij). Bitcoin versus Regulated Payment Systems: What Gives? Najdeno 20. avgusta 2016 na spletnem naslovu [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2730983](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2730983)

88. Tsukerman, M. (2015). The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future. *Berkeley Technology Law Journal*, 30(4), 1127-1170.
89. Turpin, J. B. (2014). Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework. *Indiana Journal of Global Legal Studies*, 21(1), 335-368.
90. Upelj, B. (2013, 2. marec). Virtualna valuta spreminja pravila igre. *Objektiv; priloga časnika Dnevnik*. Najdeno 27. marca 2016 na spletnem naslovu <https://www.dnevnik.si/1042578914/posel/novice/virtualna-valuta-spreminja-pravila-igre>
91. Urad Republike Slovenije za preprečevanje pranja denarja. (2014). *Virtualna valuta bitcoin – obvestilo za zavezanca*. Najdeno 7. februarja 2016 na spletnem naslovu [http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Bitcoin\\_obvestilo.pdf](http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Bitcoin_obvestilo.pdf)
92. Valdes-Benavides, R. A., & Hernandez-Verme, P. L. (2014). Virtual currencies, Micropayments and Monetary Policy: Where Are We Coming from and Where Does the Industry Stand? *Journal of Virtual Worlds Research*: 7(3).
93. Van Alstyne, M. (2014). Why Bitcoin has value. *Communications of the ACM*, 57(5), 30-32.
94. *Virtual currencies: What are the risks and benefits*. (2016, 26. januar). Najdeno 7. februarja 2016 na spletnem naslovu <http://www.europarl.europa.eu/news/en/newsroom/20160126STO11514/Virtual-currencies-what-are-the-risks-and-benefits>
95. *Virtual currencies: Out of the deep web, into the light. Issues, risks, and opportunities around the digitization of money*. (2014, marec). Najdeno 9. marca 2016 na spletnem naslovu [https://www.pwc.com/im/en/publications/assets/banking/pwc\\_virtual\\_currencies\\_risk\\_opportunities.pdf](https://www.pwc.com/im/en/publications/assets/banking/pwc_virtual_currencies_risk_opportunities.pdf)
96. *Virtual currency: Risks and Regulation*. (2014, 23. junij). *The Clearing House*. The Independent Community Bankers of America.
97. Vukovič, K. (2015, september). Bitcoin vztrajajo. *Unikum*, str. 8-9. Najdeno 20. junija 2016 na spletnem naslovu <https://issuu.com/matijag/docs/unikum9-2015>
98. Yermack, D. (2014). Is Bitcoin a real currency? *An economic appraisal*. New York University Stern School of Business and National Bureau of Economic Research.
99. Završnik, A. (2015). Digitalne valute. *Pravna praksa*, 34(16/17), GV Založba.