Professional paper / Stručni rad
Manuscript received: 2018-05-03
Revised: 2018-10-09
Accepted: 2018-10-15
Pages: 23 - 37

Kriptovalute - sofisticirani kodovi manipulacije

Ivana Cunjak Mataković
Centar-revizija d.o.o.
ivana.cunjak@gmail.com

Hrvoje Mataković
Hrvatska zaklada za znanost
hmatakovic@hrzz.hr

Sažetak: Predmet ovog rada je prikaz manipulativnih aktivnosti u segmentu informatičke tehnologije. Autori opisuju područja primjene kriptovaluta, te investicijskih aktivnosti povezanih s njima, pri čemu je naglasak stavljen na *Bitcoin*. Cilj rada je prepoznavanje upozoravajućih znakova (tzv. *red flags*) o postojanju ekonomskog mjehura i Ponzi sheme. U kontekstu ekonomskog mjehura, analizira se trend kretanja vrijednosti *Bitcoina* i pojedinih ekonomskih mjehura, kao što je bio *dot-com bubble*, s ciljem identifikacije potencijalnog financijskog rizika. Drugi dio rada usmjeren je na povezivanje *Bitcoina* s Ponzi shemom. Prikazane su prijevare u kojima je korišten Bitcoin, a posebno je dan osvrt na prijevare osmišljene poput Ponzi sheme, te se pokazalo da Ponzi shema može biti uspješno primijenjena i u okviru kompleksne informacijske tehnologije poput *blockchaina*.

Ključne riječi: kriptovalute, Bitcoin, blockchain tehnologija, ekonomski mjehur, Ponzi shema

UVOD

Dramatičan razvoj krize na financijskim tržištima u 2008. godini, uzrokovan kolapsom tržišta nekretnina u SAD-u, predstavljao je najveću depresiju nakon 1930. godine. Turbulencije u financijskom sustavu zahvatile su sve segmente gospodarstva. Tadašnja reakcija država i središnjih banaka zemalja ugroženih krizom bila je koordinirani odgovor na te negativne procese. Međutim, pozadina financijske krize mnogo je kompleksnija, ne samo zbog rasprostranjenosti i dubine, već i zbog međunarodnih ekonomskih i političkih odnosa. Ova kriza dovela je do porasta nepovjerenja u financijske institucije, monetarnu i fiskalnu politiku, što je za posljedicu, između ostalog, imalo ubrzan razvoj inovativnih tehnologija za financijsko poslovanje.

Povijesno gledajući, 2008. godina neće biti značajna samo zbog vrhunca financijske krize, već i zbog članka *Bitcoin – A Peer to Peer Electronic Cash System,* koji je objavljen pod pseudonimom Satoshi Nakamoto. Identitet autora i dalje nije poznat te se ne zna je li članak napisao pojedinac ili skupina autora [19]. Nakamoto je u tom članku predstavio elektronički sustav plaćanja, nazvan *Bitcoin*, koji otvara nove mogućnosti primjene digitalne tehnologije u financijskim sustavima. Pojam *Bitcoin* integrira organizaciju, softver i protokole inovativne tehnologije trgovanja. Međutim, trenutno tzv. inovativno trgovanje u većem svojem dijelu služi za financiranje ilegalnih aktivnosti i pranje novca, tako da promijenjen ambijent u financijskom sustavu zahtijeva istraživanje indikatora koji ukazuju na manipulativne aktivnosti u cilju pribavljanja koristi s temelja informacijske asimetrije.

Rad se sastoji od četiri dijela. U prvom dijelu rada pojašnjen je pojam virtualne valute s naglaskom na *Bitcoin* i pozadinsku tehnologiju. Prikazana su također temeljna obilježja informacijskog modela otvorenog sustava. U ovom dijelu rada ukazuje se i na mogućnosti koje donosi digitalna tehnologija implementirana u kriptovalutama. Drugi dio rada analizira područja primjene virtualnih valuta. Posebna pozornost usmjerena je na razvoj tržišta kriptovaluta, s naglaskom na *Bitcoin* kao financijski instrument. U trećem dijelu rada naglasak je na analizi trenda kretanja cijena kriptovaluta na tržištu, pri čemu se nastoji istražiti postojanje špekulativnog balona. Rezultati istraživanja koje su proveli Vasek i Moore [24] vezano uz prijevare s Ponzi shemom i *Bitcoinom* prezentirani su u četvrtom dijelu rada. Težište je na prepoznavanju vanjskih upozoravajućih znakova o primjeni Ponzijeve sheme u okviru digitalne tehnologije.

TEMELJNA OBILJEŽJA KRIPTOVALUTA

Vrhunac digitalne revolucije započinje u posljednjem desetljeću 20. stoljeća, a najvidljiviji je kroz pad cijena digitalnih komunikacijskih uređaja i smještanje Interneta u privatnu sferu [16]. Ubrzani razvoj informatičke tehnologije utjecao je i na komercijalni razvoj elektroničke mreže u segmentu financijskih transakcija. Naime, radi se o elektroničkom sustavu plaćanja koji je izgrađen na platformama poput Interneta ili mobilnih telefo-

na. Pojavio se velik broj komercijalnih rješenja poput *CyberCash*, *First Virtaul*, *DigiCash, Secure Pay*, *Web900* i drugih [8]. Navedeni sustavi elektroničkog plaćanja potaknuli su financijske aktivnosti na Internetu i na taj način doveli do pojave novog oblika imovine, odnosno tzv. elektroničkog novca. Ne postoji univerzalna definicija elektroničkog novca, međutim može se utvrditi „kako se odnosi na sustav plaćanja u realnom i virtualnom svijetu čiji je cilj unaprijediti efikasnost postojećih sustava plaćanja i zamijeniti novčanice i kovanice u maloprodajnim transakcijama" [13], p. 290.

Intenzivan porast elektroničkog novaca i komercijalizacija plaćanja putem interneta dovela je do razvoja različitih oblika i sustava elektroničkog plaćanja. Jedan od sustava elektroničkog plaćanja je i *Peer-to-Peer* sustav ili skraćeno *P2P*. *Peer-to-Peer* je otvoren sustav i sastoji se od međusobno povezanih čvorova koji se mogu samostalno organizirati u mrežu sa svrhom dijeljenja raspoloživih resursa [18]. Komunikacija između čvorova je izravna te u njoj nema središnjeg autoriteta. *Peer-to-peer* sustav predstavlja mehanizam transakcijske platforme za primjenu digitalnih valuta odnosno njihove podvrste koja se naziva kriptovaluta.

Kriptovaluta predstavlja ekvivalent elektroničkog novca. Temeljna su karakteristika kriptovaluta kriptografski mehanizmi koji služe za stvaranje i bilježenje transakcija putem privatnih i javnih ključeva. Kao najveća prednost takvog sustava ističe se jednostavnost prijenosa putem interneta. Transakcijska platforma omogućuje izravno odvijanje transakcija između korisnika bez banke, kartične kuće ili neke druge financijske institucije. Za provođenje i bilježenje transakcija ne koristi se središnji poslužitelj, već u *peer-to-peer* sustavu postoje razni poslužitelji koji su smješteni između korisnika [18].

Navedene transakcije odvijaju se tako da se svaka transakcija generira iz adrese vezane za kriptografsku valutu, koja predstavlja matematičku relaciju privatnog i javnog ključa. Svaka transakcija sadrži digitalni potpis koji se generira iz kombinacije transakcijske poruke i privatnog ključa korisnika. Sigurnosni mehanizam ostvaruje se na način da se potpis u svakoj poruci razlikuje i na taj su način krivotvorenje i zloupotreba onemogućeni bez originalnog privatnog ključa [6].

Važno je napomenuti da, iako se iz sigurnosnih razloga koriste nove adrese, ovdje se ipak ne radi o transakcijama koje su potpuno anonimne, te za svaku transakciju u bilo kojem trenutku postoji mogućnost povezivanja s odgovarajućom adresom. „No, ono što stoji iza tih adresa samo po sebi jest anonimno drugim korisnicima mreže. Tako korisnik s druge strane ne zna tko stoji iza pojedine adrese. Ipak, postoje određene metode kako tajne službe i vladine agencije mogu utvrditi tko je koristio određenu adresu, pa možemo reći da svojstvo pseudonimnosti nije do kraja provedeno" [18], p. 3.

Kompleksnost kriptografskog mehanizma nadograđena je *blockchain* tehnologijom koja je primarno razvijena za potrebe digitalne valute *Bitcoin*. Potencijal *blockchain* tehnologije kasnije je prepoznat i u drugim industrijama, naročito u financijskom sektoru. Temeljna funkcija *blockchaina* u okviru *Bitcoin* sustava jest uloga glavne knjige u kojoj je zapisana svaka transakcija. Osnovna obilježja *blockchain* tehnologije su sljedeća: svaki sustav koji koristi *blockchain* tehnologiju izgrađen je prema sustavu ravnopravnih par-

tnera (*peer-to-peer*); radi se o decentraliziranom sustavu gdje nema potrebe za središnjim autoritetom (financijska institucija, kartična kuća ili druge institucije); svaki novi zapis u realnom je vremenu distribuiran između mnoštva čvorova unutar *peer-to-peer* sustava; u svrhu identifikacije sudionika u sustavu te mogućnosti korištenja prava čitanja/pisanja koristi se kriptografija; čvorovi sustava mogu dodavati podatke u sustav; čvorovi sustava mogu čitati podatke iz *blockchaina* te *blockchain sustav* ima mehanizam koji onemogućuje promjenu nad podacima [15]. *Blockchain* sadrži niz blokova koji sadrže određeni zapis, te su međusobno povezani u lanac. Blokovi se međusobno povezuju u lanac putem tzv. *hash* funkcije, koja u okviru *blockchaina* predstavlja mehanizam koji onemogućuje promjenu podataka upisanih u blokovima, odnosno otkriva promjene nad podacima.

Bitcoin, kao sustav koji se temelji na infrastrukturi *blockchain* tehnologije, pronalazi mogućnost upotrebe i u drugim područjima. Byström [7] smatra kako primjena *blockchain* tehnologije u području računovodstva investitorima osigurava pouzdane i pravovremene informacije. Mišljenja je da ukoliko se financijski podaci bilježe te čuvaju u *blockchainu* dramatično se smanjuje mogućnost za računovodstvene trikove. Byström također navodi kako *blochchain* infrastrukura koja se temelji na *peer-to-peer* sustavu osigurava transparentne informacije posebice između povezanih društava. Ovakva platforma omogućava dostupnost informacija ne samo unutarnjim korisnicima, već i vanjskim korisnicima poput investitora i regulatornih institucija.

Bitcoin, trenutačno najpoznatija digitalna odnosno virtualna valuta*,* integrira *peer-to-peer* sustav, *blockchain* tehnologiju i *hash* funkciju. Govoreći o *bitcoinu*, nužno je istaknuti razliku između virtualnog novca i tzv. *fiat* odnosno realnog novca koji se uobičajeno pojavljuje u formi kovanica ili papirnatog novca. *Fiat* novac prihvaćeno je sredstvo razmjene u zemlji koja ga je izdala. Elektronički novac značajno se razlikuje od virtualnog novca, budući da predstavlja reprezentaciju *fiat* valute koja služi elektroničkom prijenosu kovanica ili papirnog novca. „Međunarodna organizacija *Financial Action Task Force* u svojem izvješću definira virtualni novac kao digitalnu reprezentaciju određene vrijednosti kojom se može digitalno trgovati te koja zadovoljava sljedeće funkcije: 1.) sredstvo je razmjene (*medium of exchange*), 2.) jedinica je za mjeru vrijednosti (*unit of account*) te 3.) služi za pohranjivanje vrijednosti (*a store of value*), ali nije službeno sredstvo plaćanja ni u jednoj državi“ [10], p. 656.

Od 2008. godine kada je objavljen članak *Bitcoin – A Peer to Peer Electronic Cash*, pojavilo se mnoštvo valuta izgrađenih na sličnoj tehnologiji kriptografije. Podatci o kriptovalutama na [17] pokazuju da je dana 6. ožujka 2018. godine postojalo 1.541 kriptovaluta kojima se trguje na 9.123 tržišta te da tržišna kapitalizacija kriptovaluta iznosi 4,41 bilijuna USD, od čega se 41% odnosi na *Bitcoin*. U ovome trenutku tržišna kapitalizacija *Bitcoina* veća je od ekonomija pojedinih zemlja, što proizlazi iz određenih prednosti koje kriptovalute pružaju pojedincima. One omogućavaju niže troškove transakcija, osiguravaju veću privatnost ili čak mogu poslužiti kao zamjena za bankovne račune u zemljama s nerazvijenim financijskim sustavom. S druge strane, karakteristike poput nepostojanja središnjeg financijskog autoriteta i relativne anonimnosti transakcija vrlo je privlačna

kriminalnim strukturama u usvajanju kriptovaluta kao financijskog instrumenta za provedbu ilegalnih aktivnosti [5].

PODRUČJA PRIMJENE VIRTUALNIH VALUTA

Bitcon, koji se još naziva i kod povjerenja, svoju popularnost doživljava u prvoj polovini 2013. godine kada je zbog krize ciparskih banaka mnoštvo ljudi povuklo štednju iz tih banaka, te dio tog novca uložilo u kupnju *Bitcoina* [10]. Manje je poznata veza *Bitcoina* i Edwarda Snowdena, svjetski poznatog zviždača i informatičkog stručnjaka koji je prije nego je postao zviždač bio zaposlenik CIA-e. Naime, u svibnju 2013. godine, Snowden je sletio u Hong Kong s najmanje četiri računala na kojima se nalaze podaci klasificirani kao državna tajna. U lipnju iste godine, održao je konferenciju za novinare i objavio informaciju kako vlada SAD-a ima pristup podacima i dokumentima telekomunikacijskih subjekata poput *Verizon* ili mrežnih stranica poput *Google-a* i *Facebook-a.* Zanimljiv je podatak da su nakon što je Julian Assange, utemeljitelj WikiLeaksa, proglasio Snowdena herojom, *Bitcon* donacije WikiLeaksu porasle sa 20 na 700 USD dnevno [20].

U početnoj fazi primjene *Bitcoin* tehnologije ili, kako se u nekim slučajevima naziva, tehnologija povjerenja, značajan broj transakcija odnosio se na alternativan oblik poslovanja obilježen anonimnošću i odsustvom regulatornih pravila za predmet trgovanja. Istaknut primjer *online* prodaje izvan regulatornih pravila je prodaja narkotika poput marihuane, lijekova koji se mogu nabaviti samo na recept ili benzodiazepina. Kada je *Bitcoin* upotrijebljen kao alat anonimnosti mrežnog prometa, tržištu je omogućeno snažnije osiguranje povjerljivosti. Obujam transakcija snažno je porastao, te prema nekim procjenama promet na *Silk Road-u,* anonimnom *online* tržištu koje je prvo poduprlo transakcije *Bitcoinom*, dosegao razinu od 15 milijuna USD u prvoj godini primjene [4], p. 222.

Tablica 1: Deset najpopularnijih kategorija proizvoda na stranici *Silk Road* u razdoblju od siječnja do srpnja 2012. (preuzeto i prilagođeno iz [4], p. 223)

Kategorija	Broj predmeta	Postotak
Marihuana	**3.338**	**13,7%**
Lijekovi	**2.193**	**9,0%**
Recepti	**1.784**	**7,3%**
Benzodiazepini	**1.193**	**4,9%**
Knjige	**955**	**3,9%**
Kanabis	**877**	**3,6%**
Hašiš	**820**	**3,4%**
Kokain	**630**	**2,6%**
Tablete	**473**	**1,9%**

Mrežna stranica *Silk Road* pokrenuta je 2013. godine i djelovala je kao globalno crno *cyber* tržište posredujući u anonimnim, uglavnom kriminalnim transakcijama. *Silk Road* koristile su tisuće preprodavača droga i distributera različitih ilegalnih dobara i usluga, te se procjenjuje da je trećina vrijednosti prometa ostvarena unutar SAD-a. Prema nekim procjenama, ukupno ostvaren promet od prodaje iznosio je približno oko 1,2 bilijuna USD (više od 9,5 milijuna *Bitcoina*) od čega su naknade za ostvaren promet iznosile oko 80 milijuna USD (više od 600.000 *Bitcoina*) [11].

Financial Action Task Force u svojem izvješću navodi kako je sustav plaćanja *Silk Road-a* funkcionirao poput unutarnje *Bitcoin* banke, gdje je svaki korisnik imao račun kako bi mogao obavljati transakcije na *web* mjestu. Korisnici su imali barem jednu adresu *Silk Road Bitcoina* (i potencijalno tisuće) koje su bile povezane s korisničkim računom koje održava poslužitelj kontroliran od strane *Silk Road-a*. Kako bi se provela kupnja, korisnik je dobivao *Bitcoine* (obično putem *Bitcoin* mjenjačnice) i proslijedio ih na *Bitcoin* adresu povezanu s njegovim računom na *Silk Road-u*. Kada je kupnja izvršena, *Silk Road* prenio je *Bitcoine* korisnika na založni račun čekajući dovršetak transakcije. Nakon što je transakcija završena, sustav prenosi *Bitcoine* korisnika/kupaca na *Silk Road Bitcoin* adresu dobavljača. Sljedeći korak bio je tzv. „*tumble*r" za svaku kupovinu, pri čemu je gotovo nemoguće povezati uplate izvršene u *Bitcoinima*. U rujnu 2013. godine Ministarstvo pravosuđa SAD-a pokrenulo je istragu protiv vlasnika *Silk Roada.*

Nakon zatvaranja *Silk Roada* nastala su nova anonimna *online* tržišta. Međutim, isto tako dolazi i do promjene percepcije *Bitcoina* kao valute povjerenja. U studiji koju je provela *Recorded Future,* kompanija za prikupljanje *cyber* informacija, utvrđeno je kako *Bitcoin* gubi poziciju broj jedan valute na *Darknet-u*, tajnoj web platformi koja štiti privatnost i anonimnost [22] . U cilju postizanja veće anonimnosti razvijaju se nove tehnologije, kao što je „*zero-proof technology*" integrirana u okviru kriptovalute *altcoin*. *Zero-proof* tehnologija uklanja iz *blockchain* infrastrukture sve informacije pomoću koji se može napraviti identifikacija pošiljatelja, primatelja ili iznosa transakcije [3]. Prvi *altcoin* pojavljuje se 2011. godine pod nazivom *Namecoin*.

Bitcoin se isto tako može koristiti i kao sredstvo za izbjegavanje kontrole međunarodnog kretanja kapitala. U prosincu 2013. godine, Narodna banka Kine, kao središnja regulatorna financijska institucija, zabranila je kineskim bankama transakcije povezane s *Bitcoinom*. Radi se o odluci koju je magazin *Economist* pripisao težnji koja želi spriječiti prebacivanja yuana u inozemstvo putem *Bitcoina*. Slično se dogodilo i u Argentini, gdje je porastao interes za *Bitcoin,* s obzirom da državna politika ograničava transfere u druge valute [4], p. 224.

Složena infrastruktura kriptovaluta omogućuje provedbu transakcija izvan regulatornog okvira, osiguravajući pritom visok stupanj anonimnosti. Kao što je prethodno navedeno, anonimnost osiguravaju *peer-to-peer* sustavi, kao decentralizirani sustavi bez središnjeg autoriteta. Primjerice, dizajn *Bitcoin* adrese funkcionira kao račun, pri čemu se ne pojavljuje ime ili druga identifikacijska oznaka, a sam sustav nema središnjeg poslužitelja ili davatelja usluge. *Bitcoin* protokol ne zahtijeva identifikaciju ili neki oblik provjere sudionika te nema središnjeg nadzornog tijela. Budući da se radi o decentraliziranim

sustavima, u slučaju provedbe istražnih radnji ne može se utvrditi središnja lokacija ili administrator. Na ovaj način postignuta je anonimnost koja kod tradicionalnih kreditnih kartica ili starijih sustava plaćanja poput *PayPala* nije moguća.

KRIPTOVALUTE KAO SREDSTVO INVESTIRANJA

Pojava *Bitcoina* nagovijestila je dolazak fenomena digitalnih odnosno virtualnih valuta. Njegova pojava na tržištima obilježena je snažnim rastom odnosno padom vrijednosti, što može dovesti do sumnje kako se radi o špekulativnom mjehuru. Međutim, promatranje *Bitcoina* u kontekstu investiranja zahtijeva razumijevanje prirode ulaganja i mogućnost pojave financijskog mjehura.

Prepoznavanje tržišnog rizika koji se pojavljuje kao financijski mjehur implicira analiziranje trenda vrijednosti *Bitcoina* kroz duže razdoblje. Financijski mjehur ovisi o obilježjima predmeta investiranja. Za sada ne postoji jasan i jednoznačan stav na koji način definirati pojam financijskog mjehura. Jedan od načina detekcije financijskog mjehura je pristup određivanja cijene imovine. Smatra se da se financijski mjehur, u kontekstu tržišne cijene, pojavljuje kad cijena značajno nadmašuje ili potkopava temeljnu vrijednost imovine. U kontekstu temeljne vrijednosti imovine podrazumijeva se sadašnja vrijednost isplata u okviru svih dostupnih relevantnih informacija. Međutim, kod *Bitcoina* to je teško utvrditi, budući da nema određenih novčanih priljeva [9], p. 2350.

Kao što je ranije navedeno, *Bitcoin* je digitalna valuta sa sjedećim obilježjima: sredstvo je razmjene, a istodobno je i jedinica za mjeru vrijednosti te služi za pohranjivanje vrijednosti, ali nije službeno sredstvo plaćanja niti u jednoj državi. *Bitcoin* nema nikakvu intrinzičnu vrijednost te njegova vrijednost najviše ovisi o njegovoj spekulativnoj vrijednosti. Spekulativna vrijednost temelji se na *spinovima o* tehnološkom misteriju povezanim s *rudarenjem* kriptovalute. Slučaj tvrtke Mt. Gox zasigurno je najbolji primjer financijskog rizika prisutnog na tržištu, kao špekulativnog mjehura spremnog za pucanje u bilo kojem trenutku.

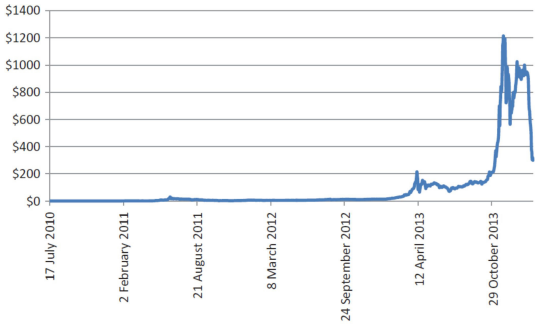
Mt. Gox pokrenut je u srpnju 2010. godine sa sjedištem u mjestu Shibuya u Japanu, kao forum za trgovanje karticama za igru „Magic", pod nazivom *Mt. Gox: Magic the Gathering Online Exchange*. Bez obzira što je inicijalno zamišljen kao forum za trgovanje karticama, Mt. Gox je do 2013. godine preuzeo preko 90% svih transakcija *Bitcoinom* širom svijeta kao najveći *Bitcoin* posrednik. Imao je gotovo 1,1 milijun aktivnih računa iz 239 zemalja. Mt. Gox je u 88% vlasništvu japanske tvrtke Tibbane koja se pak nalazi u 100% vlasništvu Marka Karpelesa, izvršnog direktora Mt. Gox-a [14].

U svibnju 2013. godine u Marylandu zaplijenjen je Dwolla[1] račun povezan s Mt. Gox. Naime, Mt. Gox prekršio je američke zakone jer su otvorili račune u novčanoj *fiat* valuti, razmijenili te račune u kriptovalute, odnosno *Bitcoin*, i nakon provedenih transakcija korisnicima omogućili povlačenje u novčanoj, *fiat* valuti. Mt. Gox tada je najavio strateško partnerstvo s tvrtkom CoinLab za poslovanje u Kanadi i SAD-u. CoinLab kao ne-fi-

1 Dwolla je *on-line* sustav za plaćanje sa sjedištem u Iowi.

nancijska institucija namjeravao je provesti registraciju za pružanje financijskih usluga u skladu s pravilima o sprječavanju pranja novca [20], p. 163.

Međutim, 25. veljače 2014. godine trgovanje na Mt. Gox iznenada je zaustavljeno, te je zatvorena mrežna stranica. Mark Karpeles, izvršni direktor Mt. Gox, pismom se obratio korisnicima kako bi ih uvjerio da je u Japanu i da poduzima sve mjere u cilju pronalaska rješenja za tadašnju situaciju [23], p. 100. Više od 24.000 korisnika diljem svijeta ostalo je bez uloženih sredstava. Naime, 7. veljače 2014. godine Mt. Gox utvrdio je, kako je rekao Karpeles, „neobične aktivnosti" nakon čega je cijena *Bitcoina* naglo pala. Mt. Gox kontinuirano je pljačkan u razdoblju od 2011. do 2014. godine te je ukradeno oko 650.000 *Bitcoina*, sadašnje vrijednosti oko 4 bilijuna USD. Mt. Gox podnio je zahtjev za stečajnu zaštitu na Okružnom sudu u Tokiju. U početku postupka Mt. Gox navodi kako im nedostaje 850.000 *Bitcoina*, međutim naknadno su izjavili da su pronašli 202.185 *Bitcoina* uskladištenih u njihovom sustavu [14]. U nastavku je grafički prikaz kretanja vrijednosti *Bitcoina* na Mt. Gox.



Slika 1: Trend vrijednosti *Bitcoina* na Mt. Gox (preuzeto iz [9], p. 2349)

U kontekstu prepoznavanja financijskog rizika povezanog s ulaganjem u *Bitcoin*, zanimljiv je grafički prikaz kretanja vrijednosti *Bitcoina* u dužem vremenskom razdoblju. Na sljedećem grafu prikazano je kretanje vrijednosti *Bitcoina* u razdoblju od 2013. do 2018. godine.

Slika 2: Trend vrijednosti *Bitcoina* u razdoblju od srpnja 2013. do siječnja 2018. (preuzeto iz [17])

S aspekta dugoročnog promatranja kretanja vrijednosti, značajna promjena vrijednosti *Bitcoina* odvija se unazad godinu dana, odnosno od siječnja 2017. godine, kada dolazi do snažnog rasta vrijednosti, koji je u relativno kratkom vremenu popraćen snažnim padom vrijednosti.

Isto tako, zanimljiv je usporedni prikaz cijena koji je na svom blogu objavio Max Galka [12]. Galka je usporedio kretanje cijene *Bitcoina* s kretanjem cijene NASDAQ indeksa.

Slika 3: Usporedba trend vrijednosti *Bitcoina* i NASDAQ (preuzeto iz [12])

Kao što je vidljivo iz prikaza, vremenska skala za *Bitcoin* i NASDAQ nije ista. Naime, indeks NASDAQ trebao je više od 5 godina kako bi dostigao rekordne vrijednosti. Promatrajući trend kretanja vrijednosti *Bitcoina*, rekordne vrijednosti ostvarene su za svega godinu dana. Početkom 2018. godine dolazi do naglog pada vrijednosti *Bitcoina*, a neki kritičari smatraju kako je to povezano sa slučajem Mt. Goxa. Nobuaki Kobayashi, stečajni upravitelj Mt. Goxa, podnio je 7. ožujka 2018. godine izvještaj Okružnom sudu u Tokiju u kojem je naveo kako je u posljednja tri mjeseca prodao *Bitcoina* u vrijednosti od 300 milijuna USD te da planira prodati još 166.344 *Bitcoina* i 168.177 *Bitcon Cash.* Analitičari koji su promatrali povezanosti Kobayashijeve akcije i kretanja cijene *Bitcoina* u kratkom roku, utvrdili su kako postoji negativna korelacija. Međutim, upozorili su na učinke informacija koje je u izvještaju Kobayashi podnio Okružnom sudu i koje će utjecati na ponašanje i odluke investitora vezano za buduće prodaje [21].

Analizirajući navedena kretanja, postavlja se pitanje predstavlja li *Bitcoin* financijski mjehur? Prilikom pronalaženja odgovora na ovo pitanje, potrebno je uzeti u obzir njegovu volatilnost koja u odnosu na drugu financijsku imovinu može biti visoka. Njegova dnevna volatilnost iznosi oko 4,8% dok ona kod, primjerice, NASDAQ indeksa iznosi 0,89%. Ako ga usporedimo s *dot-com bubble*, gdje je NASDAQ indeks izgubio oko 78% svoje vrijednosti ili sa S&P500 indeksom koji je tijekom 1930.-tih pao za 85% vrijednosti, možemo zaključiti da zaista sadrži određene indikatore koji ukazuju na postajanje financijskog mjehura [12]. Neki analitičari išli su još dalje pa je tako Goldman Sachs u siječnju 2018. godine naveo kako *Bitcoin* predstavlja financijski mjehur veći i od *dot-com bubblea.*

POVEZANOST BITCOINA I PONZI SHEME

Na temelju svega navedenog teško je s potpunom sigurnošću potvrditi da *Bitcon* predstavlja financijski mjehur. Međutim, postoje određeni indikatori koji ukazuju na prisutnost financijskog rizika, odnosno na postojanje špekulativnog mjehura. *Bitcoin* nema intrinzičnu vrijednost te nije jasno zauzet stav radi li se o valuti ili robi, prisutna je visoka volatilnost te se njime trguje na tržištima koja nisu regulirana. Radi se o predmetu ulaganja koji zasigurno predstavlja inovaciju na financijskom tržištu, međutim njegova temeljna obilježja i trend kretanja vrijednosti ukazuju na potencijalnu prisutnost Ponzijeve sheme. U nastavku ćemo se osvrnuti na osnovna obilježja Ponzijeve sheme.

Ponzijeva shema predstavlja jednu od najvećih prijevara svih vremena, a izveo ju je Charles Ponzi. Razumijevanje ove prijevare važno je stoga što je njezina osnovna shema, nakon što ju je izmislio Charles Ponzi, kasnije primijenjena u nevjerojatno velikom broju slučajeva. Charles Ponzi poduzetničku aktivnost započeo je 1919. godine s posuđenih 200 dolara [2], p. 10. Financijski program koji je ponudio investitorima odnosio se na ulaganje u kupone pri čemu je obećavao ulagačima da će ostvariti 50% povrata uloženih sredstava već nakon 90 dana, uz vrlo mali ili nikakav rizik. Interesantno je da su prvi investitori ostvarili povrat uloženih sredstva već nakon 45 dana. Koliko je primamljiva Ponzijeva shema, govori podatak da je prikupio 9,8 milijuna USD od 10.550 investitora među kojima su, između ostalog, bili i bostonski policajci. Novcem novih ulagača Ponzi je isplaćivao „stare“ ulagače, te je u samo osam mjeseci isplatio 7,8 milijuna USD ulagačima. Međutim, nakon tih početnih isplata u jednom trenutku prekinuo je isplate i ostatak novca je zadržao za sebe. Ulagači koji su investirali u ovu shemu prije urušavanja piramide ostali su prevareni i bez ičega [2], p. 11.

Koliko je Ponzijeva shema i danas aktualna govori i podatak da se u današnje vrijeme od 500 tužbi koje se svake godine podnose Komisiji za vrijednosne papire u SAD-u, njih 25% odnosi na Ponzijevu shemu. Najveću Ponzijevu shemu izveo je Bernie Madoff koja je 2009. godine, kada je otkrivena, vrijedila približno 65 milijardi USD [1], p. 313.

Tijekom vremena osim klasične Ponzijeve sheme, pojavile su se slične strukture kao što je „piramidalna shema“ i „ekonomski prijevarni mjehur“. Piramidalna shema temelji se na pogrešnom vjerovanju u ulaganja koja osiguravaju visoke stope povrata. Za sudjelovanje članovi se najčešće kontaktiraju seminarima, e-poštom ili kućnim sastancima. U tipičnoj shemi piramide članovi uglavnom plaćaju kako bi se pridružili. Kako bi svatko mogao ostvariti dobit, broj ulagača trebao bi biti beskonačan. U literaturi se navodi i matematički dokazuje kako se piramidalna shema puno brže raspada od klasične Ponzijeve sheme jer zahtijeva eksponencijalno povećanje sudionika. Ponzijeva shema može preživjeti samo uvjeravanjem, tako da većina postojećih ulagača ne povlači svoj novac, već da i dalje investira. To je najbolje dokazao Bernie Madoff koji je pomoću klasične Ponzijeve sheme djelovao skoro 40 godina [1], p. 319.

Ekonomski prijevarni mjehur djeluje slično Ponzijevoj shemi na način da se prethodni sudionici isplaćuju doprinosima novih sudionika. Za ovu vrstu prijevarne sheme karakteristično je postojanje mjehura ili balona. Mjehur se javlja u situaciji kada se postiže rast,

napuhavanje cijena na tržištu (primjerice cijena dionica, nekretnina i slično). Rast cijena posljedica je povećane potražnje na tržištu što dovodi do nerealnog rasta, a kupovina se čini isplativom budući da dolazi do značajnih povrata. Rast mjehura temelji se na „teoriji veće budale" ili „teoriji veće gluposti". Kao i s Ponzijevom shemom, cijena na tržištu prelazi stvarnu vrijednost predmeta trgovine [1], p. 319.

Prvo empirijsko istraživanje prijevara temeljenih na *Bitcoinu* proveli su 2014. godine Marie Vasek i Tyler Moore [24]. Rezultati istraživanja objavljeni su u članku pod nazivom *There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams*. U istraživanju koje se sastojalo u povezivanju izvještaja različitih osviještenih pojedinaca i praćenja *online* foruma, identificirali su 192 prijevare, te su utvrdili da osim Ponzijeve sheme postoje također i tzv. *mining* prijevare, *wallets* prijevare i prijevarne razmjene.

Vasek i Moore prvi su opisali *high-yield investment programs*[2]. HYIP su *online* Ponzi sheme koje sudionicima obećavaju neobično visoke prinose na uloge, s obzirom da kamata iznosi od 1-2% dnevno. Ove sheme raspadaju se brzo i zamjenjuju se novim prijevarnim programima. U ovom istraživanju Vasek i Mooore [24] navode kako se neke prijevare prvo pojavljuju u tradicionalnom HYIP, međutim, kasnije sheme uključuju i transakcije s *Bitcoinom*. Tako su, primjerice, na *bitcointalk.org* forumu tvrdili da su primili depozit u ukupnoj vrijednosti većoj od 5 milijuna USD-a s osnove različitih valuta. Promatrajući uplate povezane s *Bitcoin* adresama, Vasek i Moore procijenili su da se od tih 5 milijuna USD oko 1.674.270 USD odnosi na depozite u *Bitcoinu* [24], p. 5.

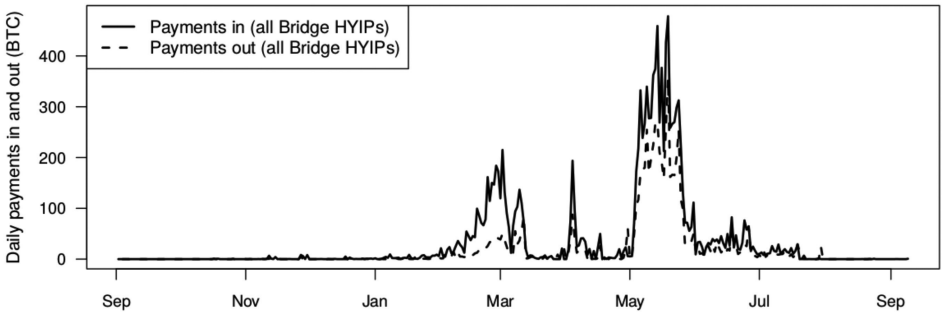
U okviru devet promatranih prijevara u razdoblju od 2. listopada 2013. do 9. listopada 2014. godine, prijevare su obuhvatile oko 12.622 *Bitcoina* (približno 6,5 milijuna USD). U nastavku je tablični prikaz koji uspoređuje tzv. *Bridge HYIPs* (programi koji obuhvaćaju depozite u *Bitcoinu* i ostalim valutama) i HYIPs temeljen samo na *Bitcoinu*:

Tablica 2: Sažetak statistike za HYIPs (preuzeto i prilagođeno iz [24], p. 5)

	Bridge HYIPs	**Bitcoin HYIPs**
Broj prijevara	9	23
Trajanje u danima (medijan)	125	37
Ukupne uplate sudionika (žrtve prijevare)	6.456.593 $	842.909 $
Ukupne isplate sudionicima (žrtve prijevare)	3.464.476 $	802.655 $
Isplate prevarantima	2.992.117 $	40.254 $

U svojem istraživanju su pratili su i dinamiku dnevnih uplata odnosno isplata sredstva. U nastavku je prikaz kretanja dinamike u okviru *Bridge HYIPs*:

2 Dalje u tekstu: HYIP.



Slika 4: Dnevne uplate i isplate u Bridge HYIPs (preuzeto iz [24])

Iz ovog grafičkog prikaza vidljivo je da priljevi u okviru prijevarne sheme održavaju korak s isplatama. Prostor između trenda priljeva i trenda odljeva predstavlja zadržavanje prikupljenih sredstava. Zadržavanje sredstava pokazuje kako prevaranti uspješno održavaju prijevarnu shemu budući da su zahtjevi za isplatu manji u odnosu na nove priljeve. Održivost Ponzi sheme osigurana je kroz ponovno uvjeravanje sudionika da ulažu svoj novac. Na ovaj način održava se privid legitimnosti i poštivanja zahtjeva ulagača. U trenutku kada prestanu pritjecati nova ulaganja, prijevarna shema se raspada, a prevaranti zadržavaju akumulirana sredstva. Prijevarna shema funkcionira na identičan način kao i prije jednog stoljeća kada je prvi puta primijenjena, što potvrđuje njezinu bezvremenost.

ZAKLJUČAK

Temeljni cilj rada bio je istražiti manipulativne operacije kriptovalutama s naglaskom na *Bitcoin*. Digitalne valute, dizajnirane pomoću sofisticirane pozadinske tehnologije, predstavljaju izazov za istraživanje. Koliko su kompleksne najbolje svjedoči činjenica da središnji regulatorni mehanizmi još nisu postigli konsenzus oko definiranja prirode *Bitcoina.* Javljaju se različiti koncepti unutar kojih je *Bitcoin* promatran kao novac odnosno kao dobro. Dok god *Bitcoin,* kao financijski instrument, nije reguliran, on predstavlja mogućnost za različite prijevarne operacije. Osim izravne financijske štete kojima su pogođeni investitori, neizravno se također stvara šteta s obzirom da nastaje negativna percepcija virtualnih valuta, koja nije točna.

Povezanost *Bitcoina* i ekonomskog mjehura predstavlja predmet rasprava. Dio sudionika tih rasprava zauzima stav kako *Bitcoin* ne predstavlja ekonomski mjehur, budući da je značajna potražnja zapravo posljedica njegove ograničene količine. Suprotnog stajališta su kritičari, koji analizirajući trend kretanja vrijednosti *Bitcoina*, prepoznaju sljedeće rizike: sama priroda *Bitcoina* nije u potpunosti definirana; radi se o ulaganju u financijski instrument koji nema intrinzičnu vrijednost; tržišta na kojima se trguje nisu regulirana pravnim okvirom što otežava zaštitu vjerovnika; prisutna je visoka volatilnost njegove vrijednosti te iza *Bitcoina* stoji kompleksna pozadinska tehnologija.

Na temelju svega navedenog možemo zaključiti kako *Bitcoin* predstavlja inovativnu tehnologiju te da ovisno o percepciji i interesima pojedinaca proizlazi i njegova upotreba. Neovisno od tehnološkog napretka, uvijek postoji prostor za primjenu Ponzijeve sheme, a znakovi koji mogu ukazati na Ponzijevu shemu ili neki drugi sličan oblik prijevare su sljedeći:

- Visoka ulaganja vraćaju se s malo ili nimalo rizika,
- Neregistrirana ulaganja
- Neovlašteni prodavači
- Složene strategije ulaganja
- Poteškoće pri primanju povrata na ulaganje“ [1], p. 392.

Ovaj rad zaključit ćemo zanimljivim razmišljanjem Belaka o prijevarama, koje ukazuje na razloge uspjeha Ponzijeve sheme i ostalih prijevarnih radnji: „Glavna osnovica prijevare je lakomost ljudi da na brzinu zarade veliki novac bez truda. Ta je ljudska mana tisućama godina uzrokom bezbrojnih prijevara. Prema tome, ako čovjek nije lakom, teže ga je prevariti“ [1], p. 394.

LITERATURA

[1] Belak, V. (2017). Lažiranje financijskih izvještaja, prijevare i računovodstvena forenzika. Zagreb: Belak Excellens d.o.o.

[2] Belak, V. (2011). Poslovna forenzika i forenzično računovodstvo. Zagreb: Belak Excellens d.o.o.

[3] Bloomberg, J. (2017). Using Bitcoin Or Other Cryptocurrency To Commit Crimes? Law Enforcement Is Onto You. Dostupno na http://forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcon-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you

[4] Böhme, R., Christin, N., Edelman, B., Moore., T, (2015). Bitcoin: Economics, technology, and Governance. Journal of Economic Perspectives, no. 2, vol. 29, pp. 213-238

[5] Breing, C., Accorsi, R., Müller, G, (2015). Economic analysis of cryptocurrency backed money laundering. Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany.

[6] Buterin, D., Ribarić, E., Savić, S. (2015). Bitcoin - nova globalna valuta, investicijska prilika ili nešto treće? Zbornik Veleučilišta u Rijeci, no. 1, vol. 3, pp. 145-158.

[7] Byström, H. (2016). Blochchains, Real-Time Accounting and the Future of Credit Risk Modeling. Working paper 2016: 4, Lund University, Department of Economics. Dostupno na http://project.nek.lu.se/publications/workpap/papers/wp16_4.pdf

[8] CARNET i CERT (2010). Elektronički novac. Dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-09-311.pdf

[9] Cheung, A., Roca, E., Su, J. J. (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. Applied Economics. no. 23, vol. 47, pp. 2348-2358.

[10] Čičin-Šain, N. (2017). Oporezivanje Bitcoina. Zbornik PFZ, no. 3-4, vol. 67, pp. 655-693.

[11] Financial Action Task Force, Virtual Currencies – Key Definitions and Potentional AML/CFT Risks. (2014). Dostupno na www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[12] Galka, M. (2018). You can‘t compare Bitcoin to other assets - but when you do, it looks like a bubble. Dostupno na https://elementus.io/blog/bitcoin-bubble/

[13] Hamdi, H. (2007). Problemi razvoja elektroničkog novca. Financijska teorija i praksa, no. 3, vol. 31, pp. 289-303.

[14] Harney, A., Stecklow, S. (2017). Special Report: Twice burned - How Mt. Gox‘s bitcoin customers could lose again. Dostupno na https://www.reuters.com/article/us-bitcoin-gox-specialreport/special-report-twice-burned-how-mt-goxs-bitcoin-customers-could-lose-again-idUSKBN1DG1UC

[15] Hozjan, D (2017). Blockchain. Diplomski rad. Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Matematički odsjek. Dostupno na https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A779/datastream/PDF/view

[16] https://hr.wikipedia.org/wiki/Informacijsko_doba

[17] https://coinmarketcap.com/currencies/bitcoin/

[18] Kaselj, M. (2015). Bitcoin. Diplomski rad. Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku. Dostupno na https://repozitorij.mathos.hr/islandora/object/mathos%3A24/datastream/PDF/view

[19] Marr, B. (2017). A Short History Of Bitcoin And Crypto Currency Everyone Should Read. Dostupno na https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#1fec92f23f27

[20] Simers, J (2015). Bitcoin and moderan alchemy: in code we trust. Journal od Financial Crime, no. 2, vol. 22, pp. 156-169.

[21] Thompson, P. (2018). Effects of Mt. Gox Trustee‘s $400 Mln Sale on Bitcoin Market. Dostupno na https://cointelegraph.com/news/effects-of-mt-gox-trustees-400-mln-sale-on-bitcoin-market

[22] Thompson, P (2018). Is Darknet Done With Bitcoin? Dostupno na https://cointelegraph.com/news/is-darknet-done-with-bitcoin

[23] Trautman, L. (2014). Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? Richmond Journal of Law and Technology, no. 4, vol. 20, pp. 1-108.

[24] Vasek, M., Moore, T. (2015). There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. 19th International Conference on Financial Cryptography and Dana Security (FC), San Juan, PR, January 26-30, 2015. Dostupno na http://fc15.ifca.ai/preproceedings/paper_75.pdf

Cryptocurrency – sophisticated manipulation codes

Abstract: The subject of this paper is an overview of manipulative activities in the IT field. The authors describe the application areas of cryptocurrency, and investment activities connected with them, with emphasis on Bitcoin. The goal of the paper is to identify red flags which indicate economic bubble and the Ponzi scheme. Value trends of bitcoin and various economic bubbles are analysed in the context of an economic bubble, such as a dot-com bubble to identify potential financial risks. The second part of the paper is focused on linking Bitcoin to the Ponzi scheme. Bitcoin based frauds are presented, particularly frauds designed as the Ponzi scheme, and it has been shown that the Ponzi scheme can be successfully applied in the framework of complex information technology such as blockchain.

Keywords: cryptocurrency, Bitcoin, blockchain technology, economic bubble, Ponzi scheme

List of figures:

List of tables: