Rizici korištenja kriptovaluta

Milić, Bruno-Marino

LIBERTAS MEĐUNARODNO SVEUČILIŠTE

Preddiplomski studij

„Menadžment poslovne sigurnosti“

ZAVRŠNI RAD

RIZICI KORIŠTENJA KRIPTOVALUTA

Mentor:dr.sc.Nikola Protrka

Student:Bruno-Marino Milić

Zagreb, rujan, 2018.

SADRŽAJ

1. UVOD

Razvojem računalnih tehnologija, kao i interneta pojavili su se i novi oblici vrijednosti vezani za navedene tehnologije, a ne spadaju u tradicionalna oblike vrijednosti s kojima se gotovo svakodnevno susrećemo. Takve oblike vrijednosti nazivamo virtualne valute. Protekom vremena sve više raste njihov obujam trgovanja, a samim time i njihov značaj u razmjeni i utjecaj na ekonomiju.

Niz je definicija virtualnih valuta, a najčešće se spominje definicija Europske centralne banke, koja je virtualne valute definirala kao „vrsta nereguliranog, digitalnog novca, koje izdaju i najčešće kontroliraju njezini osnivači i koristi se između članova posebnih virtualnih zajednica".

Najpoznatiji među virtualnim valutama je bitcoin, koji je stvoren 2009. godine te u samim počecima nije imao nešto zapaženu ulogu. Veću je ulogu dobila tek nekoliko godina kasnije kada se njegova vrijednost povećava do granice da je izazvao balon koji je 2013. godine pukao te je došlo do naglog pada cijene čiju najvišu razinu nije niti do danas ostvario.

Pojava koja se najčešće pojavljuje, a vezana je za virtualne valute, između ostalih i bitcoin, istaknula je Europska centralna banka je što imaju decentralizirani sustav kreiranja novih jedinica koji nije pod kontrolom nijedne institucije, u odnosu na centralizirane sustave kreiranja novih jedinica koji se danas koriste i koji su pod kontrolom centralnih banaka.

Ovaj završni rad se sastoji od 5 cjelina u kojima će se obrađivati tema „*Rizici virtualnih valuta"*, a to su:

1. Uvod
2. Trenutno stanje na tržištu
3. Rizici korištenja kriptovaluta
4. Primjeri u praksi te
5. Zaključna razmatranja.

U prvom, uvodnom dijelu rada predstaviti će se problem predmet i ciljevi istraživanja ovoga rada.

U drugom dijelu rada će se objasniti pojam, značaj i karakteristike virtualnih valuta, podijeliti će ih se na vrste, predstaviti će se najveća virtualna valuta bitcoin, objasniti pojmove koje vežemo za njih, razloge njihova korištenja, kako doći do njihovog posjedovanja, koje su

prednosti njihovog posjedovanja. Osim toga objasniti će se uloga i značaj blockchain tehnologije, kao i načina na kojise održava, odnosno garantira njezina sigurnost.

Treći dio će objasniti rizike virtualnih valuta, prvo rizike s kojima se susreću njezini korisnici, spomenuti rizike s kojima se susrećemo prilikom reguliranja samih virtualnih valute te objasniti povezanost virtualnih valuta i kriminalnih radnji.

U četvrtom će se dijelu prikazati primjeri iz prakse, navesti će se gdje su postavljeni bitcoin bankomati, objasnit će se pojam *wallet*, kao i detaljne upute za kupovinu bitcoina putem bankomata.

Na kraju će se izvesti zaključna razmatranja u odnosu na temu koja je obrađena.

2. TRENUTNO STANJE NA TRŽIŠTU KRIPTOVALUTA

Kriptovaluta je ime koje je dano nekom sustavu koji upotrebljava kriptografiju kako bi omogućio siguran transfer i razmjenu digitalnih tokena na distribuiran i decentraliziran način, pri čemu te tokene onda možemo mijenjati za standardne valute po njihovim uobičajenim tržišnim vrijednostima.[1]S druge strane, definicija koja je više tehničkog karaktera kaže da su kriptovalute fizičke te prethodno kalkulirani podaci koji koriste parove javnih te privatnih ključeva generiranih oko specifičnog enkripcijskog algoritma. Ključ dodjeljuje vlasništvo svakog para ključeva, ili kovanice, osobi koja je u posjedu privatnog ključa.

Ti parovi ključeva su pohranjeni u datoteci imena „wallet.dat“, koja egzistira u uobičajenom skrivenom direktoriju na tvrdom disku. Privatni se ključevi šalju korisnicima korištenjem adresa dinamične lisnice generiranih od strane korisnika uključenih u transakcije. Odredišna adresa plaćanja je javni ključ para ključeva kriptovalute. Postoji konačni iznos svake kriptokovanice dostupne na mreži, te vrijednosti svake jedinice se dodjeluje temeljeno na ponudi i potražnji, kao i prema fluktuirajućim razinama težine rudarenja svake kovanice.[2]

Može se vidjeti na koji način funkcioniraju kriptovalute već na provjeren način, koristeći pritom jednu od najpoznatijih kriptografskih shema u vidu duplih ključeva, jednog privatnog i jednog javnog. Na taj se način garantira mogućnost identifikacije iznutra, odnosno unutar same transakcije te njenih aktera, kao i zaštita od vanjskih utjecaja. Ktiptovalute imaju veliki broj karakteristika koje ih čine posebno korisnima kao sredstva razmjene, ako ne i kao obračunske jedinice. Brito i Duorado, između ostaloga navode da za razliku od papirnatog novca, mogu biti razmijenjene online kao i osobno, ukoliko postoji mrežna povezanost[3].

Bitno je izdvojiti i jedan od najčešće korištenih načina plaćanja, a to je putem kreditnih kartica. U odnosu prema kreditnim karticama, cijena jedne jednostavne transakcije je niska te se upotrebljava za poticanje brzog procesiranja transakcija od strane rudara. Neki trgovci upotrebljavaju trgovačke usluge kako bi zaprimili *bitcoin* uplate te imaju ekvivalentnu količinu stavljenu izravno na njihove bankovne račune. Pružatelji usluge najčešće naplaćuju tarifu od 1%

[1]Dourado, Eli i Brito, Jerry. 2014.: *The New Palgrave Dictionary of Economics,* Online Edition
[2]Heid, Alexander, 2013: *Analysis of the Crypotcurrency Marketplace*
[3]Dourado, Eli i Brito, Jerry. 2014.: *The New Palgrave Dictionary of Economics,* Online Edition

za tu pogodnost. Dodatna pogodnost koja najčešće privlači trgovce je činjenica dakupci ne mogu povući *bitcoin*transakciju kao što mogu transakciju koja ide preko kreditne kartice[4].

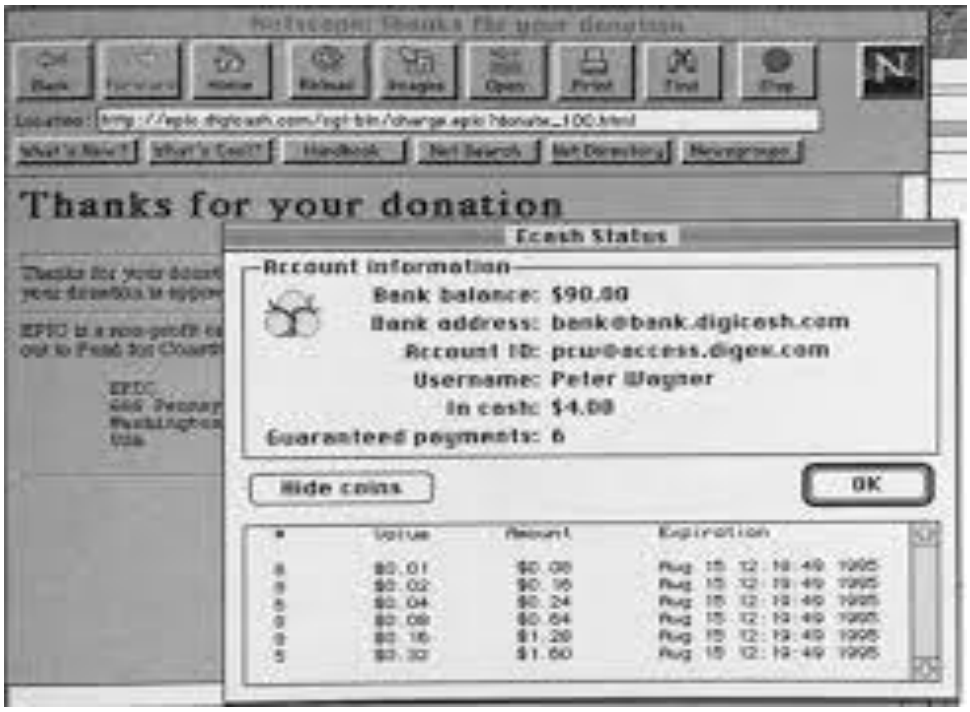
Decentralizirana priroda *open-source* protokola osigurava da kontrola mreže ostaje u rukama korisnika. Transakcije su ovisne o učesnicima u mreži, a korisnik je odgovoran za sigurnost vlastitih financija i podataka, bez potrebe da ovisi o trećoj strani poput bankarske institucije.[5]Kriptovalute predstavljaju svojevrsnu revoluciju u načinu na koji se upravlja novcem, što na fizičkoj, to na idejnoj razini. Trenutno i dalje, zbog neusuglašenosti oko definicija, postoji u metaprostoru između definicije novca, odnosno valute i predmeta razmjene.

2.1. Povijest kriptovaluta

Tehnički temelji kriptovaluta datiraju do 1980-ih, kada je američki kriptograf David Chaum izumio algoritam koji ostaje centralan modernoj mrežnoj enkripciji. Algoritam je dopuštao sigurnu, neizmjenjivu razmjenu informacija između stranaka. Chaum je ujedno osnovao i DigiChash kompaniju koja je proizvodila jedinice valute bazirane na tom algoritmu. DigiCashova kontrola nije bila decentralizirana, kao u slučaju s modernim kriptovalutama. DigiCash je držao monopol nad kontrolom ponude, slično kao što središnje banke drže monopol nad *fiat* valutama.[6]

[4]Ibid
[5]Heid, Alexander, 2013: *Analysis of the Crypotcurrency Marketplace*
[6]https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

Slika 1. DigiCash prikaz (informacije o korisničkom računu)



Izvor: Narayanan, Arvindetal., 2016: *BitcoinandCryptocurrency Technologies*

Slikom 2 prikazane su informacije o DigiCash korisničkom računu, gdje se jasno vidi trenutačni saldo, e-mail adrese, korisničkom ime kao i povijest transakcija. Drugi val mrežnog novca manifestirao se u vidu Paypala i e-Golda. Paypal je nudio neprekidan *peer-to-peer* transferni mehanizam kao i jednostavan način prihvaćanja uplata za trgovce. E-Gold je određeno vrijeme nudio alternativu Paypalu. Taj servis je prihvaćao depozite zlata od korisnika i izdavao je zlatne potvrde (ili e-Gold) na njihove račune. Na taj je način potaknut poveći volumen međunarodne trgovine i plaćanja. E-Gold je, doduše, ugađen nakon manifestacije Ponzi shema i generalnih prevara.[7]

Prvom modernom kriptovalutom smatra se *bitcoin.* To je prvi javno iskorišten način razmjene koji kombinira anonimnost korisnika kroz decentraliziranu kontrolu i omogućavanje pregleda povijesti transakcija kroz bockchain. Prvi je put spomenut 2008. godine u radu SatoshijaNakamotoa, čiji pravi identitet u stvarnosti nikada nije utvrđen. Godine 2009. Nakamoto je pustio *bitcoin* u javnost i grupa entuzijasta je započela sa razmjenom i rudarenjem

[7]https://medium.com/koinex-crunch/a-brief-history-of-cryptocurrency-889fed168555

valute. Krajem 2010. godine počele su se pojavljivati prve alternative *bitcoinu*, kao što je *ltecoin*, a ujedno se tada pojavila i prva javna *bitcoin*burza.[8]

Nakon toga se pojavila i svojevrsna konkurencija. *Litecoin*je počeo dobivati pažnju medija krajem 2013. godine kada je dosegnuo stopu na tržištu od 1 milijarde dolara. Ripplecoin je stvoren 2011. godine na jednakom protokolu kao i *bitcoin*, ali funkcionira kao sistem plaćanja, slično kao i Paypal za kriptovalute koji podržava *fiat* valute, kriptovalute te robu.[9] [6] Zatim, krajem 2012. godine WordPress je postala prva veća kompanija koja je prihvatila plaćanje *bitcoinom*. Ostali, kao što su Expedie i Microsoft su bili iza nje. Iako danas ostale kriptovalute nisu toliko raširene, kao niti prihvaćene kao načini plaćanja, aktivne razmjene pružaju mogućnost korisnicima da ih zamjene za *bitcoine* ili *fiat* valute, a to omogućuje potrebnu likvidnost te fleksibilnost.[10]

2.2. Najpoznatije kriptovalute

Prva kriptovaluta bazirana na SHA-256 algoritmu koja se pojavila je bila *bitcoin*. Visoka volatilnost cijene od *bitcoina* je napravila primamljivu ulagačku alternativu za trgovce koji traže profit putem tržišnih spekulacija, a u isto vrijeme volatilnost samog tržišta je i razlog zašto su dugoročni ulagači te svakodnevni korisnici počeli oklijevati kada je u pitanju sudjelovanje na duže periode.[11]

2.2.1. Bitcoin

Kao što je već ranije i navedeno, *bitcoin* je predstavljen 2008. godine i to sa člankom pod imenom „*Bitcoin: A Peer-to-Peer Electronic Cash System".*[12]Napisan je pod aliasom SatoshiNakamoto. Namjera je bila stvaranje potpune kontrole nad financijama stvaranjem stabilne, sigurne, svjetski prihvatljive i demokratske valute. Nakamoto je kombinirao nekoliko ranijih izuma kao što su b-money i HashCash kako bi kreirao u potpunosti decentralizirani elektronički platni sustav. Temeljna inovacija je bila korištenje distribuiranog sustava izračunavanja („proof-of-work" algoritam) kako bi se potvrdila transakcija. Vrijeme koje je potrebno kako bi se transakcija potvrdila iznosi otprilike desetak minuta. Ovaj način dopušta

[8]https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/
[9]Graydon, Carte, 2014: *What is Cryptocurrency?*
[10]https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/
[11]Heid, Alexander, 2013: *Analysis of the Crypotcurrency Marketplace*
[12]Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System, 2008*

decentraliziranoj mreži da stigne na konsenzus o stanju transakcije čime se spriječilo dvostruko trošenje koje je u prošlosti bilo velika mana digitalnih valuta.[13]

Bitcoin mreža započela je s radom 2009. godine. Bazirana je na implementacijskoj referenci objavljenoj od Nakamota. U samim počecima *Bitcoin* mreža je bila sklona pogreškama. U 2009. godini je pronađena pogreška u ranom *Bitcoin* klijentu, a to je dopustilo stvaranje velikog broja bitcoina. U ožujku 2013. godine. Tehnčki kvar je izazvao podjelu *Bitcoin* mreže na dva neovisna dijela. Šest sati dvije različite *Bitcoin* mreže su radile paralelno, svaka sa svojom verzijom povijesti transakcija. Programeri *Bitcoin* sustava pozvali su na privremenu obustavu prometa, a to je izazvalo oštar pad cijene. Normalni način rada ipak je obnovljen kroz nekoliko sati.

Veće web stranice su *bitcoin* počele prihvaćati otprilike 2013. godine. WordPress je započeo u studenom 2012. godine, a potom su uslijedili i OKCupid u travnju 2013., Atomic Mall u studenom 2013., TigerDirect i Overstock.com u siječnju 2014. te Ecpedia u lipnju 2014. Određene neprofitne ili interesne skupine kao što su Electronic FrontierFoundation dopuštaju *bitcoin* donacije. Vlasnik trgovine Overstock.com je u ožujku 2014. godine izjavio da ta trgovina ima dnevni promet od dvadeset do trideset tisuća dolara od kupaca koji plaćaju *bitcoinima*.

Kineski internetski gigant je u listopadu 2013. godine uveo plaćanje *bitcoinima*. U tijeku studenoga 2013. *Bitcoin* burza „BTC China“ osnovana u Kini pretekla je japansku burzu Mt. Gox i europsku burzu Bitstamp te je postala najveća *Bitcoin* burza po obujmu trgovine. Nakon što je u studenom 2013. godine na ročištu odbora Senata SAD-a bilo rečeno da su virtualne valute legitimna financijska usluga vrijednost *bitcoina* na burzi Mt. Gox je skočila na vrhunac od 900$. S druge strane, u Kini je zbog prevelike vrijednosti *bitcoina* Narodna banka Kine je zabranila kineskim financijskim institucijama korištenje *bitcoin* valutnog sustava. Nakon objave vrijednost *bitcoina* je pala i Baidu više ne prihvaća *bitcoine* za određene usluge.

Trenutni broj korisnika *Bitcoina* nije moguće utvrditi zbog činjenice što jedan korisnik može imati više adresa. SatoshiNakamoto se iz javnosti povukao u travnju 2011. ostavivši odgovornost razvijanja koda i mreže grupi nadobudnih volontera. Identitet osobe ili grupe koja stoji iza *Bitcoina* još uvijek je nepoznat. Unatoč tome, niti SatoshiNakamoto niti itko drugi ne zadržava kontrolu na *Bitcoin* sustavom koji djeluje po potpuno transparentnim matematičkim principima.

[13]Ibid

Sama ideja je revolucionarna te je već započela novu znanost u poljima distributivnih računalnih znanosti, ekonomije i ekonometrije.[14]

Jedan *bitcoin* se može potrošiti u razdjelnim inkrementima koji mogu iznositi do 000000001 BTC po transakciji. Najmanji inkrement *bitcoina* nazvanje Satoshi, prema autoru originalnog dokumenta u kojem se prvi puta spominje[15]. Bitne tehničke karakteristike *bitcoina*[16]*:*

- ✓ u odnosu na ostale valute, *bitcoin*nije potpomognut vladavinom prava, nego tehnologijom;
- ✓ u slučaju da svi pravni sustavi kolabiraju, *bitcoin* bi nastavio funkcionirati dokle god internet i dalje postoji te su ga ljudi spremni koristiti;
- ✓ *bitcoin*, naravno, i dalje podliježe zakonima kao takvima;
- ✓ njegova decentralizirana i robusna priroda ga čini teškim za reguliranje;
- ✓ snažnom kriptografijom osigurava vlasništvo,
- ✓ konačni broj *bitcoina* koji će ikada biti u cirkulaciji je 21 milijun;
- ✓ transakcije su anonimne, ali javne,
- ✓ pošiljatelj *bitcoina* mora biti *online,* za razliku od primatelja:
- ✓ *bitcoinu* ništa ne garantira vrijednost, izuzev mehanike ponude i potražnje.

2.2.2. Litecoin

Smatra se da je *Litecoin* pušten u opticaj putem *open-source* klijenta na GitHubu 7. listopada 2011. godine, te da je to napravio Charlie Lee, bivši djelatnik Googlea. Iako je stvoren 2011. godine sama povijest *Litecoin*dostiže u studeni 2013. godine. Razvojni je tim prvo objavio 0.8.5.1 inačicu, dok je ukupna vrijednost*Litecoin* doživjela golemo povećanje, a to uključuje i stopostotni skok unutar 24 sata. Početkom prosinca 2013. godine svjetlo dana je ugledala i nova inačica *Litecoina*. Nova, poboljšana inačica je nudila dvadesetostruko smanjenje transakcijske naknade, sigurnosno poboljšanje te poboljšanje učinkovitosti mreže[17].

[14]Frančišćković, I.: *Bitcoin*, Diplomski rad, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Matematički odsjek, Zagreb, studeni, 2015.
[15]Heid, Alexander, 2013: *AnalysisoftheCrypotcurrency Marketplace*
[16]Meisser, Luzius.: *Bitcoin – A PromiseofFreedom, NextGenerationFinance, 2013.*
[17]https://admiralmarkets.com.hr/education/articles/cryptocurrencies/sto-je-litecoin

Litecoin (LTC) se može smatrati „srebrnim standardom“ kriptovaluta, s obzirom na to da je druga najviše prihvaćena kriptovaluta i od strane rudara i burzi. *Litecoin* koristi Scrypt enkripcijski alogritam, za razliku od *bitcoina* koji koristi SHA-256. Kao jedan od ciljeva *litecoina*postavlja se postizanje veće brzine potvrde transakcija nego na *bitcoin* mreži, kao i iskorištavanje mogućnosti algoritma koji je otporan na ubrzane hardverske zahtjeve rudarskih tehnologija poput ASIC-a. Ukupan broj *litecoina* dostupnih za rudarenje i cirkulacije je 4 puta veći od broja *bitcoina*[18].

Litecoin je jedina internetska mreža koju korisnici mogu upotrebljavati za direktno plaćanje jedne osobe drugoj. To je decentralizirana *peer-to-peer* mreža, što znači da ga ne kontrolira bilo koji entitet kao niti vlada. Sustav plaćanja ne koristi nikakvu fizičku valutu, kakve su npr. dolar i euro. Umjesto fizičke valute on koristi vlastitu jedinicu računanja, koje se također naziva *Litecoin*. To je ujedno i razlog radio koje se učestalo viđa da je *litecoin* kategoriziran kao digitalna ili kriptovaluta[19].

Litecoin je na puno načina nalik *bitcoinu,* jer se smatra digitalnom valutom i digitalnim sustavom plaćanja. *Litecoin*koristi enkripcijske tehnike za dvije ključne aktivnosti:

- ✓ Za reguliranje generacije *litecoin* jedinica te
- ✓ Za verificiranje transfera fondova i osiguravanje transakcija.

Iako su *bitcoin* i *litecoin*na puno načina slični, ipak postoji nekoliko važnih razlika između te dvije kriptovalute. Kao neke od razlika mogu se navesti sljedeće[20]:

- ✓ *Litecoin* pruža bržu potvrdu: *Litecoin*mreža nastoji procesuirati blok svake 2.5 minute u odnosu prema *Bitcoin* koji to čini svakih 10 minuta. Njegovi programeri tvrde da upravo to pruža mogućnost brže potvrde transakcije.
- ✓ *Litecoin*koristi drugačiji *hashtag* algoritam: u svojem algoritmu za dokaz rada koristi skript, sekvencijalnu funkciju tvrde memorije, koja zahtijeva asimptotično više memorije od algoritma koji nije tvrda memorija.
- ✓ *Litecoin* mreža proizvest će višekriptovalute: *Litecoin* će proizvesti 84 milijuna *Litecoin,* odnosno četiri puta više jedinica valute od jedinica koje će u opticaj staviti *Bitcoin*mreža.

[18]Heid, Alexander, 2013: *AnalysisoftheCrypotcurrency Marketplace*
[19]https://admiralmarkets.com.hr/education/articles/cryptocurrencies/sto-je-litecoin
[20]Ibid

Sve u svemu, *Litecoin*može procesuirati i nositi se s većim brojem transakcija, a to umanjuje potencijalan problem uskog grla, koje se *Bitcoinu*ponekad događa.

2.2.3. Ethereum

Ethereum je decentralizirana platforma koja pokreće „pametne ugovore“ – aplikacije koje raede točno kako su isprogramirane bez mogućnosti deaktivacije, cenzure, prevare ili intervencije treće strane. Te su aplikacije pogonjene posebno napravljenim *blockchainom*, iznimno snažnom dijeljenom globalnom infrastrukturom koja može prenositi vrijednost i reprezentirati vlasništvo imovine[21].

Dodatna definicija o *Ethereumu*kao pozadinskoj tehnologiji govori sljedeće: *Ethereum*je globalna mreža međusobno povezanih računala koji osiguravaju, izvršavaju te validiraju programe u decentraliziranoj maniri bez potrebe korištenja servera, memorije, procesne snage, ili bilo koje druge računalne funkcije, jer je sve osigurano od strane tisuće ethereum točaka raspršenih diljem svijeta. Ukratko, *Ethereum*je globalno računalo. Ostale kriptovalute koje bi bilo potrebno posebno izdvojiti su *dash*, *ripple* te *monero*[22].

2.3. Blockchain tehnologija

Blockchain tehnologija u smislu temelja sustava virtualnih valutnih shema je predstavljena svijetu 2009. godine. Pod pseudonimom SatoshiNakamoto objavio ju je nepoznati autor ili organizacija u vidu software-a otvorenog koda (eng. *Open source*), na web stranici *https://bitcoin.org.*[23]Iako postoje brojne špekulacije, do današnjega dana nije sa sigurnošću utvrđen identitet autora. Kako osnovna verzija software-a – koji se od 2009. godine stalno unaprjeđuje i razvija od zajednice, sadrži preko 31 000 linija koda, a to bi uz neke prosječne standarde značilo minimalno 2-3 godine rada uz puno radno vrijeme za jednog programera, jasno je zašto mnogi sumnjaju da je cijeli projekt djelo jednog čovjeka, neovisno od toga što je i ta mogućnost realna.

[21]https://crobitcoin.com/altcoin/ethereum/
22Quentson, A.: WhatisEthereum?, 2017.
23SatoshiNakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

Blockchain je baza podataka u digitalnom obliku, koja sadrži dnevnik svih transakcija učinjenih u sustavu. Decentralizirana je u smislu da svaki sudionik sustava ima mogućnost pohraniti kod sebe vlastitu kopiju. Sudionici ili čvorovi u sustavu (eng. *nodes*)[24] su ravnopravni svjedoci i kontrolori autentičnosti svake pojedinačne transakcije. Transakcije su grupirane kronološki, u tzv. Blokove transakcija. Svaki blok transakcija digitalno je „potpisan" odnosno pridružena mu je određena digitalna šifra (eng. *hash*) koja je garancija da je blok autentičan, tj. svaki pokušaj promjene sadržaja bloka je vrlo lako otkriti.

Uz navedeno, osim određenog broja transakcija, svaki blok sadrži i hash prethodnog bloka, što znači da ako netko želi promijeniti sadržaj određenog bloka (npr. dodajući ili mijenjajući transakcije), mora izmijeniti sve blokove u nizu nakon izmijenjenog bloka. Blokovi su na taj način povezani ili ulančani, odakle i potječe naziv Blockchain.[25] Ovo je pojednostavljen prikaz funkcioniranja Blockchain tehnologije i tu nisu opisani svi detalji sustava kao ni njegove varijante. Cilj je istaknuti funkcionalnost cijelog sustava baziranog na ravnopravnoj mreži sudionika i tehničkom rješenju, a bez određenog centraliziranog sustava autorizacije, kao što je slučaj kod Internet bankarstva, gdje banka autorizira i kontrolira transakcije.[26]

Blockchain tehnologija može biti privatna i javna, a ajvniblockchain može biti „javan" na dva načina:

- ✓ Da svi mogu zapisivati i čitati podatke,
- ✓ Da svi mogu čitati podatke, a samo validirane osobe zapisivati.

Privatni blockcahin je onaj kojem ne može svatko pristupiti nego osoba mora biti verificirana, i recimo imati određeni token s kojim može zapisivati transakcije. To može biti korisno u velikim organizacijama koje će iskoristiti prednosti blockchaina, ali tim podacima javnost neće moći pristupiti. U današnje vrijeme kompanije imaju jedan centralni server na kojem su svi podaci – i to je jedna točka na kojoj se može dogoditi greška i podaci mogu postati nedostupni.

[24]Rogojanu, A., Badea, L., Others: Theissueofcompetingcurrencies. Casestudy-Bitcoin, Theor.Appl.Econ., sv.21, izd. 1, 2014.
[25]Abramowicz, M.: Cryptocurrency – BasedLay, ArizRev, sv. 58, 2016.
[26]Turpin, J. B., Bitcoin: Theeconomiccase for a global, virtualcurrencyoperating ina n unexploredleaglframework, Indiana J. Global Leg. Stud., sv. 21., izd. 1, 2014.

Blockchain zapisi se mogu zamisliti kao obične datoteke, koje su strukturirane. Podaci su logični posloženi i spremljeni. Baza podataka inače može biti skup tablica koje imaju kolone i redove, može biti tekstualna datoteka, mogu biti podaci koji su odvojeni zarezom ili nekim drugim znakom i slično. Blockchain ima sadržaj (npr. podaci o Bitcoin transakcijama), a u zaglavlju se nalaze meta – podaci (broj stranice, naslov i sl.) o bloku u koji se podaci spremaju, referencu na prijašnji blok, jer je blockchain skup vezanih podataka koji se „vežu“ u blok i tako nastaje lanac informacija, *hashirani* otisak i mnoge druge podatke.

U svaki se blok podatka može zapisati određeni broj podataka, odnosno transakcija. Kada se blok popuni, kreira se novi i tako dalje. Samim time se stvara neprekinuti blok informacija, a svi su međusobno povezani i nemoguće ih je prekinuti. Oni su konzistentni te se u blockchainu nalazi datoteka po datoteka koje su povezane međusobno. Samim time što se podaci *hashiraju*, nije moguće retroaktivno izmijeniti podatke. Čak i da se nekim čudom to uspije, trebalo bi se istovremeno podatke izmijeniti na svim lokacijama gdje se ti podaci čuvaju, što je tehnički i praktički nemoguće za napraviti.

Jednako tako, validatori bi te iste radnje odbili i ne bi se to moglo napraviti niti na jednom serveru. Upravo je u tome velika prednost ove tehnologije, jer kada se podatak jednom zapiše, on više nije izmjenjiv. Primjerice ako klijent napravi transakciju koju ustvari nije htio, samo će napraviti novu s kojom će prethodnu poništiti, ali će obje radnje ostati zapisane u blockchain. Svaka blockchain mreža funkcionira na način da ima određena pravila koja se moraju zadovoljiti.

Kada se sva pravila zadovolje, podatak se može zapisati. Ukoliko se transakcija krši za pravilima ona će biti odbijena. *Nodovi* koji su zaduženi za validaciju transakcija se mogu ažurirati i nadograditi novim pravilima te će se onda budući zapisi validirati po tim pravilima. Blockhain tehnologija je dosta fleksibilna i sigurna. Svaki *node* ili čvor zna pravila, dobiva podatkeu realnom vremenu, te svi znaju sve. Nema skrivanja podataka, mijenjanja istih, brisanja, ili pak neke druge radnje.

Sve ostaje zapisano u jednom od blokova podataka koje čini blockhain. Svaki blockchain može imati razne varijacije, ali u srži su jednak, tj. funkcioniraju na jednaki način.[27]

[27]https://pcchip.hr/ostalo/tech/uvod-u-blockchain-tehnologiju/

Postavlja se pitanje na koji se način održava, odnosno garantira sigurnost blockchaina. Naime, 3 su temeljna faktora koja pripomažu u tome:

- ✓ Kriptografija,
- ✓ Proofofwork (dokaz rada)
- ✓ Distribuirani sustav

2.3.1. Kriptografija

Blockchain, u prijevodu lanac blokova, sastoji se od niza podatkovnih paketa, odnosno blokova, od kojih svaki sadržava skup transakcija ostvarenih u određenom vremenskom periodu. Svaki podatkovni paket u lancu, logički je povezan s prethodnim paketom jednom vrstom kriptografskog potpisa pod koji još zovemo i – *hash*. Hash je broj ispisan u posebnom formatu i izgleda kao niz nasumično odabranih znakova:

7c96cf30947914ab1d9844d93707baf2435f9d9b290c8258622ab635054c8041

Hash je rezultat *hash*funkcije koja s jedne strane prima bilo koji digitalni sadržaj kao što je tekst, fotografija, video, pdf ili bilo koji drugi tip datoteke te nad njima izvršava niz matematičkih operacija, a kao rezultat vraća unikatanpotpis u obliku niza znakova točno određene duljine.Kroz *hash* funkciju možemo provući jedno slovo ili riječ, ali i kompletnu knjigu. *Hash* će u oba slučaja biti jednake duljine. Osim toga, ako sadržaj iste knjige provučemo više puta kroz *hash* funkciju, rezultat će biti uvijek isti.

Međutim, ako bilo gdje u knjizi zamijenimo samo jedno slovo, zarez ili razmak, *hash* knjige će biti potpuno drugačiji. Različitim *hashevima* ne možemo ukazati gdje je u knjizi nastala promjena, ali ono što možemo dokazati bez trunke sumnje je da sadržaj knjige nije identičan zbog toga što se *hashevi* razlikuju.U Bitcoinblockchainu svaki blok transakcija u lancu je potpisan na ovaj način, a svaki generirani potpis postaje dio sadržaja idućeg bloka u lancu. Ako netko zamijeni bilo koji podatak u nekom od blokova, to će automatski uzrokovati neispravnost potpisa tog bloka. Ponovno generiranje ispravnog potpisa poništit će ispravnost idućeg bloka jer idući blok sadrži stari potpis. Ukratko, ako bilo gdje u blockchainu napadač pokuša promijeniti bilo koji detalj, uzrokovat će lančanureakciju koja ne može proći neprimijećeno.

2.3.2. Proofofwork

Generiranje *hasha* je za računalo trivijalan zadatak. Onaj tko želi izmijeniti podatak u blockchainu bi mogao preračunati sve *hasheve* kompletnog lanca u vrlo kratko vrijeme, da nema jednog sitnog pravila u Bitcoin protokolu koji definira uvjet ispravnog *hasha*, a on kaže da *hash* mora započeti s određenim brojem nula.

0000000000000000d9844d93707baf2435f9d9b290c8258622ab635054c8041

Spomenuli smo da će svaki sadržaj koji ulazi u *hash* funkciju, ako je nepromijenjen, svaki puta vratiti isti *hash*. To znači da će isti skup transakcija svaki put vratiti isti *hash*, a ako taj *hash* ne počinje za određenim brojem nula, *hash* se smatra neispravnim. Kako bi dobili drugačiji *hash*, moramo nešto izmijeniti u sadržaju koji ulazi u *hash* funkciju. Same transakcije su također zaštićene malo drugačijom kriptografskom metodom pa nam ne preostaje ništa drugo nego da dodamo još jednu varijablu x koju proizvoljno možemo mijenjati.

Rotacijom vrijednosti varijable, svaki put ćemo dobiti drugačiji ulaz u *hash* funkciju i samim time drugačiji *hash* kao izlaz. *Hash*je potpuno nepredvidiv pa zato računalu ne preostaje ništa drugo nego metodom pokušaja i pogodaka izračunavati *hasheve* sve dok ne pronađe pravi, odnosno onaj koji počinje sa zadanim brojem nula. Ovaj proces pogađanja nazivamo *proofofwork* jer svaki ispravan *hash* je ujedno i dokaz da se računalo 'naradilo' dok ga nije pronašlo.Jednom *hashiran* set transakcija na ovaj način postaje trajno zaključan jer bi svaka promjena zahtijevala ponavljanje procesa traženja ispravnog *hasha* za svaki blok u lancu kreiran od tog trenutka nadalje.

2.3.3. Distribuirani blockchain

U Bitcoin mreži, onoga tko pronađe ispravan *hash*, protokol nagrađuje – novim bitcoinima. Ljude koji traže *hasheve* nazivamo mineri (rudari) jer u opticaj unose nove bitcoine, jednako kao što rudari iskapaju novo zlato. Za pogađanje *hasha*potrebna je procesorska snaga računala i vrijeme. Što je brži procesor, brže će se pronaći ispravan *hash*. Brži procesor za rad zahtijeva i više električne energije pa rudari neprestano ulažu znatna financijska sredstva u procesorsku i električnu infrastrukturu jer su u konstantnoj utrci protiv drugih rudara koji također traže ispravan *hash*.Jednom pronađeni *hash* znači da je blok podataka uspješno zatvoren i rudar

objavljuje svoj pronalazak ostatku Bitcoin mreže. Svako računalo u mreži provjerava ispravnost *hasha* ponovnim potpisivanjem bloka s uključenom varijablom koju je rudar prezentirao kao rješenje. Ako dobiveni *hash* počinje s predefiniranim brojem nula, računalo dodaje novi blok na svoju kopiju blockchaina.

Ostali sudionici u mreži će također provjeriti i dodati novonastali blok na svoju kopiju blockchaina pa se tako ujedno ostvaruje i sinkronizacija blockchaina između računala.

Nadalje, Bitcoin mreža je potpuno otvorena i slobodna za korištenje. Svatko može postati dio mreže i imati svoju kopiju blockchaina, čitati njegov sadržaj bez ograničenja, provjeravati točnost zapisa ili preuzeti ulogu rudara. Ovako decentraliziran sustav smatra se sigurnim jer ne postoji jedan centralni server koji se može napasti.[28]

[28]https://www.netokracija.com/sto-je-blockchain-132284

3. RIZICI KORIŠTENJA KRIPTOVALUTA

Virtualne se valute još uvijek nalaze u svojoj početnoj fazi postojanja, s obzirom da se koriste manje od 10 godina još uvijek nisu riješile probleme s kojima se suočavaju. Problemi se uobičajeno javljaju kao rizici s kojima se njihovi korisnici susreću te ih je nužno navesti i obraditi. S obzirom na rizike koji postoje niz godina te se ni na koji način ne dolazi do njihovog rješenja, može sve pretpostaviti kako će se kriptovalute još dugo susretati s njima.

Europsko nadzorno tijelo za bankarstvo (EBA) je 2013. godine navela više razloga zbog kojih se stvaraju rizici koji su vezani za korištenje virtualnih valuta. Prema njima su neki izvori valuta sljedeći[29]:

- Virtualne valute mogu biti kreirane od bilo koga anonimno (nprSatoshiNakamoto);
- Sudionici u transakciji su anonimni
- S obzirom da se koriste na globalnoj razini ne poštuju državne zakone;
- Nema prvanih osoba (sudionici se ne vode kao entiteti);
- Nedostatak definicije i standarda;
- Neadekvatna sigurnost (u kontekstu informatičkih tehnologija);
- Ne mogu se prijaviti prijevare,
- Nepostojanje stabilizirajućeg autoriteta i sl.

Oko same vrste rizika postoje različita mišljenja. Prema mišljenju Europske centralne banke postoje četiri vrste rizika koje se vežu uz kriptovalute, a to su: pravni rizik, kreditni rizik, rizik likvidnosti i operativni rizik. Osim toga Europska centralna banka dodaje rizik od prevare, nedostatka regulacije i slično. S druge strane ostali autori razdvajaju rizike u centraliziranim i decentraliziranim sustavima. Za centralizirane sustavi koji su pod kontrolom centralne banke su Ali etal. Prema Finanetal. Istaknuli da postoje tri rizika: operativni, likvidni i kreditni, a uz njih su još dodali i rizik od prijevare.

U decentraliziranim sustavima kao što su virtualne valute zbog same njihove prirode postoje samo operativi rizici (koji su poprilično veći) dok likvidni i kreditni ne mogu postojati. Jednako tako ističe se da i kod decentraliziranih sustava postoji mogućnost prevare, samo u nešto

[29]Europsko nadzorno tijelo za bankarstvo: Upozorenje za korisnike virtualnih valuta, EBA/WRG/2013/01, 2013.

drugačijem obliku (primjerice kod centraliziranih sustava to može biti gubitak kartice, a u decentraliziranim sustavima je to npr. gubitak ključeva za pristup računu).[30]

3.1. Rizici za korisnike virtualnih valuta

TheClearingHouse(TCH) je objavila pet osnovnih rizika sa kojima se korisnici virtualnih valuta[31]:

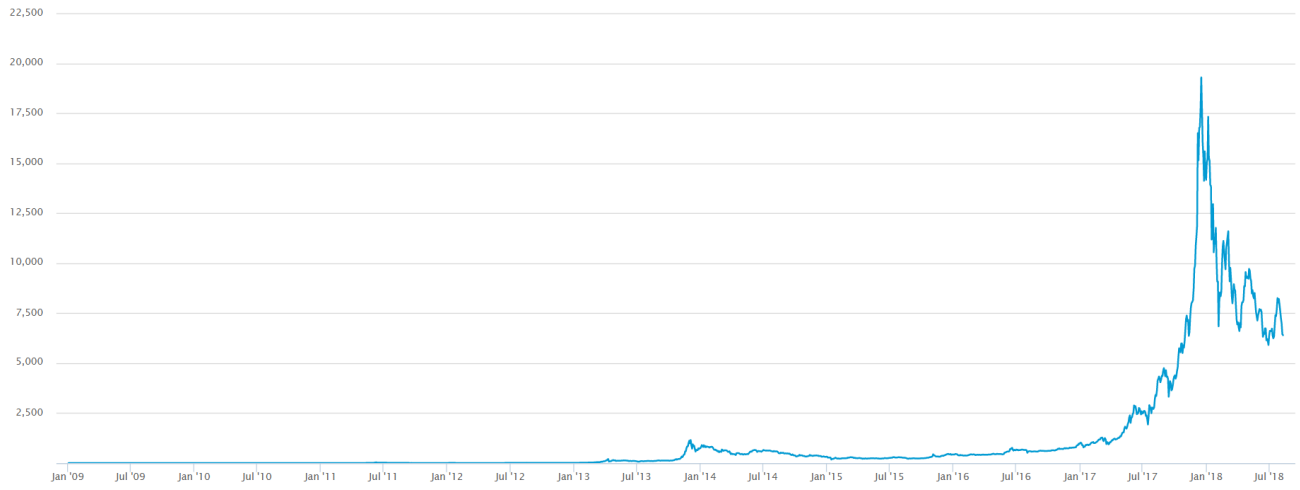
- Krađa virtualnih valuta koje mogu nastati zbog nepažnje, propusta u sustavu, itd.;
- Neautorizirano korištenje od ostalih koji su dobili priliku upravljati s virtualnim valutama te ih mogu zloupotrijebiti, npr. trošiti bez posljedica, jer nema mogućnosti povratka transakcije (kao ni odgovornosti za zloupotrebu);
- Greška prilikom transakcije – vrijednost u obliku virtualnih valuta je poslana na krivu adresu bila nepažnjom pošiljatelja ili greškom u sustavu, kako nema mogućnosti povratka ili poništenja transakcije, pošiljatelj ostaje bez vrijednosti koju je posjedovao;
- Greška novčanika (wallet), odnosno, kada primjerice radi zaboravljanja šifre za pristup računu ili greške u sustavu ne možemo pristupiti korištenju virtualnih valuta koje posjedujemo;
- Nepostojanje obveze regulatora da objavi troškove transakcije određene virtualne valute.

Najčešći rizik koji je povezan s virtualnim valutama s kojima se njen korisnik može susreti su velike varijacije u vrijednostima virtualnih valuta. Promijene vrijednosti dvije valute s najvećom tržišnom kapitalizacijom su prikazane na slici 2. za bitcoin, na slici 3. za ethereum, na slici 4. za terracoin (ne spada u virtualne valute s najvećom tržišnom kapitalizacijom već je odličan primjer naglog pada vrijednosti određene virtualne valute), a objašnjeno je i kretanje cijena od njihovog puštanja u promet do kraja razdoblja koje je prikazano na slikama.

[30]Ali, R., Barrdear, J., Clews, R., Southgate J.: Innovationsinpaymenttechnologiesandtheemergenceofdigitalcurrencies, Bank ofEnglandQuarterlyBulletin, Vol.54, No.3, str. 262-275

[31]TheClearingHouse: Virtualcurrency: risksandregulation, June 23, 2014

Slika 2. Ukupna povijest kretanja cijene jedinica Bitcoina u američkim dolarima (od početka do 18.7.2018)

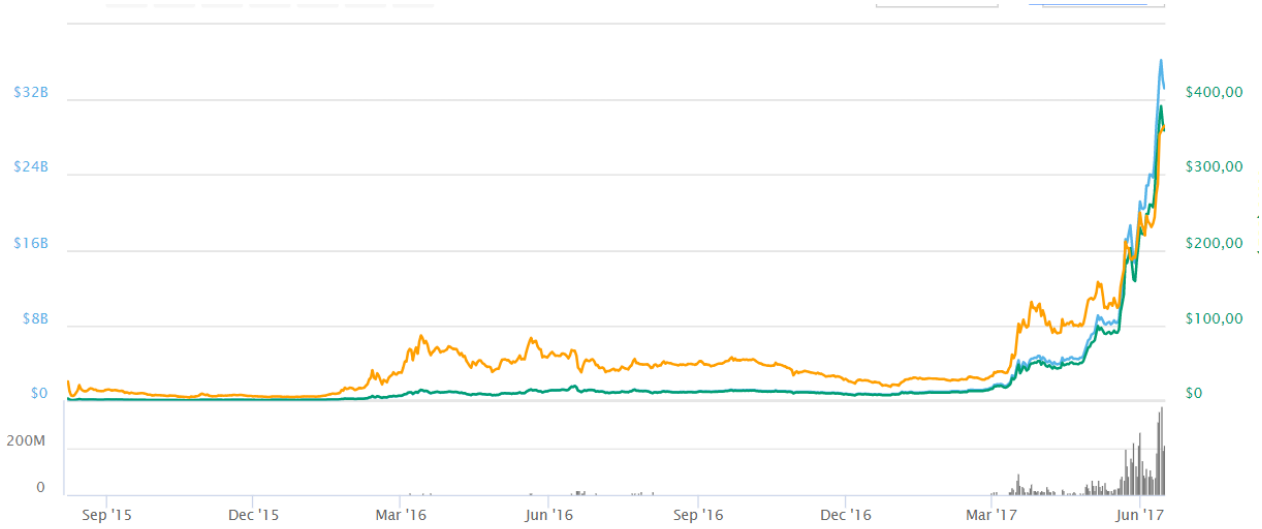


Izvor: https://www.blockchain.com/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

Od prvog dana postojanja bitcoina pa svedo početka 2013. godine nije bilo nikakvih značajnijih promjena u cijeni. Čitavo vrijeme od puštanja u promet početkom 2009. pa sve do početka 2013. godine cijena je iznosila manje od 0,01 američkih dolara. Jedina iznimka u tom razdoblju je bila sredinom 2011. godine kada je cijena iznosila oko 30 američkih dolara, ali kratko poslije toga je iznova došlo do pada na razinu manju od 0,01 američkih dolara za jednu jedinicu. Prvi značajniji rast se dogodio u prvoj polovici 2013. godine kada je bitcoin narastao na više od 200 američkih dolara, ubrzo je njegova cijena i pala, ali se o tada do danas više nikada nije vratio na razinu manju od 0,01 američkih dolara koju je imao u prvih nekoliko godina.[32]

[32] https://www.blockchain.com/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

Slika 3. Kretanje cijene ethereuma od 7.9.2016. do 15.6.2017 (cijena po jedinici američkog dolara, ukupna kapitalizacija u američkim dolarima i volumen trgovine u 24 h)

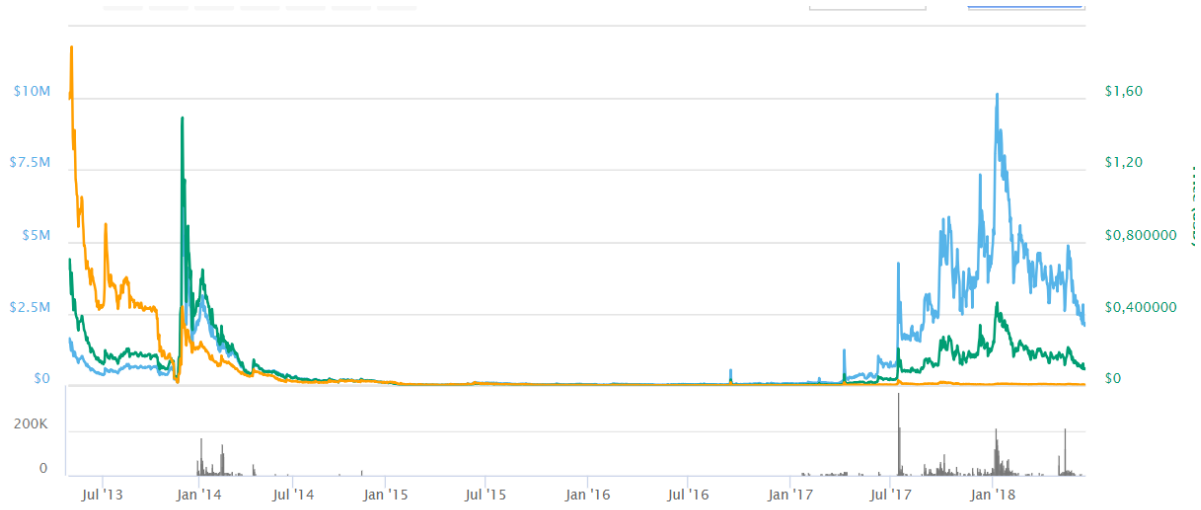


Izvor: https://coinmarketcap.com/currencies/ethereum/#charts

U odnosu na bitcoin, u početku cijena nije bila preniska, manja od 0,01 američkih dolara, već je odmah varirala. Razlog tome je jednostavan jer su u razdoblju njegova osnivanja virtualne valute (kriptovalute) bile u širokoj upotrebi. Cijena je 7.8. 2016. godine iznosila 1,33 američka dolara. Do siječnja 2018. godine, iznosila je 2,83 američkih dolara za jednu jedinicu. Ona se ubrzo smanjila te je samo jedan dan nakon iznosila 1,33 američka dolara. Do siječnja 2016. godine, cijena je bila manja od 2 američka dolara, a tada po drugi put prelazi vrijednost od 2 američka dolara. Tijekom sljedeća četiri mjeseca, vrijednost je više rasla nego padala, svoj vrhunac je doegnula 13.3.2018. godine kada je iznosila 14,89 američkih dolara, što do kraja razdoblja prikazanim grafom više puta dosegnuto, a povijesno najveća cijena jedinica je iznosila 18,82 američkih dolara na dan 14.6.2018., dakle jedan dan prije kraja prikaza na slici.

Najveća tržišna kapitalizacija je, logično, bila na isti dan kad je iznosila najveća vrijednost jedinice ethereuma, 14.06.2016., a tada je tržišna kapitalizacija iznosila više od 1,5 milijardu američkih dolara. Najveći promet u 24h ethereum je imao također 14.06.2016. kada je iznosio više od 63,1 milijuna američkih dolara.

Slika 4. Kretanje vrijednosti terracoina (od 28.4.2015. do 15.6.2018. godine)



Izvor: https://coinmarketcap.com/currencies/terracoin/

Slučaj kao ethereumov u kojem u kratkom vremenu brzo naraste vrijednost virtualne valute nije jedini, a kao primjeri nekih od ranijih slučajeva izdvaja se terracoin koji je na vrhuncu u ožujku 2017. imao tržišnu kapitalizaciju 6,1 milijun američkih dolara, a vrijednost jedne jedinice je iznosila 1,38 američkih dolara. 15.6.2018. godine je imao tržišnu kapitalizaciju nešto višu od 43 tisuće američkih dolara, a jedinica je iznosila 0,01 američka dolara. Slikom 4 prikazano je kretanje cijene terracoina gdje je zelena linija vrijednost jedne jedinice terracoina, a plava linija vrijednost ukupne tržišne kapitalizacije[33].

Pojave balona u cijenama virtualnih valuta nisu rijetka pojava, a kao jedan od najvećih balona spominje se auroracoin. Niti sam bitcoin nije bio imun na balon u svojoj početnoj fazi (sam vrhunac balona bio je krajem 2013. godine, ali bitcoin ga je preživio te do danas nije dolazio do toliko naglih rasta vrijednosti, a potom naglih padova) ali za razliku od terracoina i auroracoina je izdržao te je zadržao status najvrijednije virtualne valute.

[33]White, L., H., Themarket for cryptocurrencies, CatoJorunal, Vol. 35., No. 2. (Spring/Summer 2015), str. 383-402.

Banque de France je 2013. godine navela četiri rizika koji su povezani za investicijsku svrhu bitcoina, no isto se može primijeniti i na većinu ostalih virtualnih valuta koje dijele s bitcoinom slične karakteristike, to su[34]:

- Vrijednost bitcoina nije povezana s nekom djelatnošću u stvarnosti ili s vrijednošću neke imovine;
- Velika varijacija vrijednosti bitcoina;
- Sporije realiziranje transakcija;
- Nepostojanje investicija u stvarnosti koje su vezane za bitcoin i potencijalni rizici vezani za zakone.

Usprkos činjenici što se smatra da virtualne valute u najvećem broju slučajeva upotrebljavaju osobe s dobrim poznavanjem računala i interneta, ali i općenito informatičkih tehnologija, neki autori napominju kako između korisnika postoje i oni koji ipak nisu toliko dobro upoznati s time. Rizik koji oni s time povezuju je da osobe koje slabije poznaju rad na računalu mogu napraviti neku pogrešku prilikom rada s virtualnim valutama, konkretno mogu ostati bez sredstava na svojim računima prilikom nenamjernog odvajanja informacija o ključevima kod korištenja bitcoina i slično.[35]

Problem koji je navela TCH, a koji se ujedno može povezati i s navedenim je mogućnost da se transakcija preusmjeri na krivi račun svojom nepažnjom ili tehničkom greškom, u oba slučaja pošto ne postoji središnje tijelo koje sustav virtualnih valuta ima pod kontrolom do poništavanja ili povratka transakcije neće doći čime se stvara rizik za korisnike.[36]

Prilično je teško pronaći i navesti primjer gdje su korisnici zbog nepažnje ili, pak neznanja ostali bez virtualnih valuta iako ih sigurno ima. Usprkos tome što nije konkretan primjer za navedeno, ipak je na tom tragu slučaj Mt Gox iz veljače 2014. godine, kada se dogodilo da u na jednom od najvećih tržnica za razmjenu bitcoina u Japanu pod imenom Mt Gox odjednom bez traga nestali bitcoini. Mt Gox je tada bio jedan od najvećih tržnica preko kojih su se obavljale transakcije, a jedno vrijeme oko 80% obavljenih transakcija se obavljalo preko njega. Nestalo je gotovo 750,000 jedinica bitcoina.[37]

[34]Banque de France (2013), Thedangerslinked to theemergenceofvirtualcurrencies: theexampleofbitcoins, Focus, No 10., 5 December 2013.
[35]Buterin, D., Ribarić, E., Savić, S., (2015), Bitcoin - Nova globalna valuta, investicijska prilika ili nešto treće?, Zbornik Veleučilišta u Rijeci, Vol. 3 (2015), No. 1, str. 145-158.
[36]TheClearingHouse: Virtualcurrency: risksandregulation, June 23, 2014,
[37]Sidel, R., Casey, M. J., Warnock, E.: Shutdownof Mt. GoxRattlesBitcoin, 2014.

Skandal koji je vezan za MtGox je doveo u pitanje sigurnost te sami smisao upotrebe bitcoina, ali i ostalih kriptovaluta, međutim s obzirom na daljnje kretanje cijena bitcoina, kao i sve veći broj virtualnih valuta može se reći da se s obzirom na predviđanja prešlo preko tog problema. MtGox nje jedini slučaj nestajanja bitcoina, te su se takvi slučajevi događali i na tržnicama MyCoina[38] (prijave su se odnosile na Ponzijeve sheme (vrsta prijevare gdje se uključivanjem novih članova vrši isplata starih članova ili investitora.[39]) te je procijenjena šteta bila 387 milijuna američkih dolara), Bistamps (hakiranjem se ukralo oko 19,000 jedinica bitcoina, procijenjena šteta oko 5 milijuna američkih dolara)[40] i slično.

Svaki od navedenih slučajeva samo ukazuje na činjenicu da virtualne valute nisu imune na krađu, neovisno o tome radi li se o hakiranju ili nekom drugom načinu. Učestalost nestanaka samo ukazuje na to da su virtualne valute što se sigurnosti tiče podosta nesigurniji sustavi ond onih kojima upravljaju same centralne banke.

3.2. Regulatorni rizici virtualnih valuta

Kriptovalute još uvijek nisu priznate kao službeno sredstvo za plaćanje od niti jedne države ili područja na svijetu, međutim događanja, kao i promjene u Japanu ipak ukazuju da bi i u tome uskoro moglo doći do nekih promjena. Usprkos činjenici što nisu priznate u velikoj većini država one važnije kriptovalute kao što je bitcoin nisu ilegalne za samu upotrebu. Posljednjih nekoliko godina koliko su virtualne valute aktivna tema dovoljno govori da su razne međunarodne institucije te centralne banke davale svoja mišljenja o njima, uglavnom se odnosilo na rizike kriptovaluta.

Kao jedna od rijetkih država u kojoj je bitcoin uistinu i zabranjen (ako bi išli po strogoj definiciji odnosi se na kriptovalute) je Rusija. U toj je zemlji zabranjeno korištenje kriptovaluta, dok se kao neki razlozi zabrane od strane ruske centralne banke spominju visoki rizici gubitka uloženoga, financiranje terorizma i slično tome.[41]Osim Rusije i neke druge države zabranjuju upotrebu bitcoina, a to su Island, Kina, Bolivija, Ekvador itd.[42]

Međutim postoje i države koje zakonom određuju da je upotreba virtualnih valuta pod kontrolom države. Jedna od njih je i Japan. Zapravo, razmjena virtualnih valuta će biti regulirana

[38]Osborne, C.: MyCoinclosesitsdoors, $387 millionininvestorfundsvanishes, 2015.
[39]http://dario-dolic.from.hr/ponzijeva-sema-charles-ponzi/
[40]Whittaker, Z.: Bitstampexchangehacked, $5M worthofbitcoinstolen, 2015.
[41]Baczynska, G., i Pomeroy, R.: RussianauthoritiessayBitcoinillegal, 2014
[42]https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp

od strane države, njeni korisnici moraju biti registrirani, a virtualne valute će se smatrati imovina koja se može koristiti u razmjeni za robu i usluge. Razlog za uvođenje je službeno objašnjen kao odgovor na pranje novca te pokušaj veće zaštite korisnika. Razlog zašto baš Japan je prilično jasan jer se radi o državi u kojoj se dogodio prethodno spomenuti MtGox skandal vezan za bitcoin.[43]

Veliki broj ostalih drž-ava i u današnje vrijeme ostavljaju bitcoin, ali i ostale kriptovalute nereguliranima, ali ih niti ne zabranjuju, a neke su, pak, njihovu kontrolu obuhvatile nekim drugim zakonima. Kao najbolji primjer može poslužiti Kanada u kojoj je regulacija virtualnih valuta obuhvaćena zakonom protiv pranja novca i terorizma.[44]

U Republici Hrvatskoj status bitcoin do danas nije precizno određen, kao ni činjenica treba li se za samo njegovo korištenje platiti porez. Kao jedino dostupno priopćenje za bitcoin od strane Hrvatske Narodne banke izdano je u lipnju 2014. godine te kaže sljedeće: „bitcoin" ne potpada niti pod jednu zakonom reguliranu kategoriju sredstava plaćanja te prema Zakonu o Hrvatskoj Narodnoj banci, kao i prema Zakonu o deviznom poslovanju „bitcoin" ne predstavlja novac, ali ni sredstvo plaćanja u Republici Hrvatskoj niti stranu valutu odnosno strano sredstvo plaćanja."[45]

Zatim u odgovoru Porezne uprave o mišljenju HNB-a stoji: „obzirom da vrijednost „bitcoina" ne odražava vrijednost novca koji je za njega primljen, „bitcoin" ne može niti biti elektronički novac u smislu Zakona o elektroničkom novcu."[46] Još ranije Hrvatska Narodna banka se oglasila o tome gdje su također napisali da bitcoin nije elektronički novac i da samo njegovo korištenje nije ilegalno te da će dalje slijediti regulative Europske Unije.[47]

Kao jedan od temeljnih rizika sa kojim se korisnici kriptovaluta mogu susretati je porez. Na transakcije virtualnih valuta nema jedinstvenog pravila u svijetu što se tiče oporezivanja. Sukladno logici, u zemljama u kojima je bitcoin, kao i ostale kriptovalute zabranjen nema niti oporezivanja, dok je u ostalima, u kojima je dozvoljena njihova razmjena, njihova se razmjena se smatra trampom i prema tome se porez naplaćuje ovisno od svrhe njihove upotrebe, a u

[43]AFP: Japan regulatesvirtualcurrencyafterBitcoinscandal, 2016.
[44]Rubenfeld, S.: Canada EnactsBitcoinRegulations, 2014.
[45]http://www.porezna-uprava.hr/HR_publikacije/Lists/mislenje33/Display.aspx?id=19252
[46]Ibid
[47]Ivezić, B.: HNB: Bitcoin je poput zlata u World ofWarcraftu, 2013.

Sjedinjenim Američkim Državama bitcoin se smatra imovinom i sukladno toj odluci se i oporezuje.[48]

Regulatorni rizik upotrebe virtualnih valuta javlja se u državama u kojima je on zabranjen, ali realan riki postoji i u onim državama gdje se dopušta njegovo korištenje jer država u bilo koje vrijeme može odrediti da će započeti s kontrolom prometa virtualnih valuta ili ih jednostavno proglasiti ilegalnima. Kao još jedan rizik može se navesti oporezivanje virtualnih valuta, odnosno zaobilaženje plaćanje poreza prilikom korištenja virtualnih valuta.

3.3. Povezanost kriptovaluta sa kriminalnim radnjama

Postoje razni načini na koje se virtualne valute mogu zloupotrebljavati, a kao neki od njih javljaju se plaćanje za obavljanje kriminalnih radnji, zatim kupovanje ilegalnih sredstava, financiranje terorizma i slično. Razlozi radio kojih se baš virtualne valute upotrebljavaju za kriminalne radnje su vrlo jednostavni: radi anonimnosti upotrebe, nepostojanja kontrole nad njima itd. Kao najpoznatiji primjer iz kojeg se može uočiti povezanost kriptovaluta sa plaćanjem djelatnosti koje su povezane s kriminalnom radnjom je slučaj SilkRoad.

SilkRoad je web stranica na kojoj su se bitcoinima mogle kupiti droge, ali i ostala ilegalna dobra.Prilikom posjećivanja dotične web stranice morao se koristiti software uz pomoć kojega bi samikorisnici ostali anonimni, odnosno izbrisao bi se trag da se toj web stranici pristupalo s nekogodređenog računala. Stranica SilkRoad je postojala od veljače 2011. pa sve do listopada 2013. godine. U tom je razdoblju na njoj zabilježen promet od oko 1,2 milijarde američkih dolara.

U listopadu 2013. godine FBI je zatvorio dotičnu stranicu, međutim to nije označilo kraj povezanosti kriminalnih radnji i bitcoina jer su se ubrzo osnovale nove, mnogo naprednije stranice koje su imale slične ciljeve.[49] Ovo je rizik na koji utjecaja ima isključivo ljudski faktor s obzirom da o njenim korisnicima ovise u kakve svrhe će se koristiti kriptovalute.

[48]https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp
[49]Global Drug Police Observatory: SilkRoadandBitcoin. Swansea: Swansea University PrifysgolAbertawe, 2013.

4. PRIMJERI U PRAKSI

Temeljna ideja koncepta bitcoina bila je stvoriti sustav P2P (person to person). Koncept se temelji na stvaranju sustava decentralizirane valute koji će omogućiti izravni dodir dviju osoba u transakciji bez posredovanja institucija kao što su centralne državne banke. Centralne banke nadgledaju stanje na svom, ograničenom financijskom tržištu i određuju količinu novca u optjecaju čime utječu na odnos ponude i potražnje, odnosno utječu na tržišnu vrijednost valute i za to ubiru provizije ili spekulativnim radnjama na tržištu ostvaruju dobit. Koncept bitcoina temelji se na ideji da se s tržišta uklone institucije koje mogu utjecati na stanje ponude i potražnje, odnosno da se stvori svijet bez banaka utemeljen na otvorenemopen-source softwareu koji će nadgledati razmjenu valute i algoritmima osiguravati odgovarajući broj bitcoina na računima vlasnika.

Ovaj koncept naišao je na plodno tlo, osobito u vrijeme velike financijske krize kada su banke doživljavane kao veliko zlo i glavni krivac za krizu. Bitcoin je zamišljen tako da se stvori svjetska transakcijska valuta gdje nitko ne može doznati podatke o uplatitelju i vlasniku računa. Ubrzo su se u priču oko bitcoina umiješali spekulanti koji su u toj valuti pronašli novu mogućnost za trgovanje na Forex tržištu. Najveće svjetske burze bitcoina su MtGox i BitStamp.

Vlasnik na zaslonu svog računala ima jedan ili više online računa (novčanika) na kojima može držati bitcoine ili ih iz novčanika prebaciti na privatni račun. Bitcoini se mogu steći kupnjom kroz postupak zamjene realnih valuta američkog dolara ili eurovalute i njihovim pretvaranjem u bitcoine prema važećem tržišnom tečaju u trenutku kupnje, te uplatama koje dolaze u novčanik na temelju prodaje roba ili usluga.

Uplatitelj na svome računalu unosi samo ID transakcije i količinu bitcoina koje kupuje u svoj novčanik. Ostali podaci o imenu i prezimenu, broju kreditne kartice, PIN i drugi osobni podaci koji su obvezni i služe kao kontrola pri plaćanju drugim kreditnim karticama ovdje nisu nužni. Uplatitelj može uplatu izvršiti izravno u drugi novčanik korištenjem bitcoins softwarea koji vrši provjeru ID transakcije da ne dođe do prijevare. Pri tome računalo ne ostavlja podatke o IP adresi uplatitelja na temelju kojih bi se kasnije moglo utvrditi tko šalje novac[50].

[50]http://www.glas-slavonije.hr/220167/7/Bitcoin---umjetni-virtualni-novac-ili-valuta-snova

4.1. Bankomati za virtualne valute

Primjena virtualnih valuta je sve učestalija u različitim segmentima poslovanja te novčanih transakcija. Diljem svijeta je postavljeno niz bankomata za virtualne valute, koji svojim korisnicima pružaju mogućnost jednostavnog baratanja virtualnim valutama. Prvi bitcoin bankomat postavljen je u listopadu 2013. godine u Kanadi. U Hrvatskoj su do sada postavljena četiribitcoin bankomata – u Zagrebu, Rijeci i Splitu. Onaj u Zagrebu postavljen je 2014. godine u kafiću History u Tkalčićevoj ulici, a postavili su ga Vedran Kajić i Ivan Šimurina. Radi se, ustvari o dvosmjernom bitcoin bankomatu kanadske kompanije Bitaccess. Dvosmjerni bankomat znači da osim što je moguće kupovati bitcoine za kune, moguće je i prodavati bitcoine za kune.[51]

U Zagrebu je najveća pojedinačna kupnja bitcoina do sada išla u iznosu od 60 tisuća kuna, a najveća zamjena bitcoina za kune u iznosu od 19 tisuća kuna. Drugi bitcoin bankomat u Zagrebu nalazi se na križanju Gagarinovog puta i Zelenog trga u Caffe bar Agram. Pritom je Hrvatska, prije tri godine postala prva država jugoistočne Europe u kojoj se bitcoin mogao koristiti za plaćanje roba i usluga.

Dvije godine kasnije Ivan Šimurina je u suradnji sa Dunjom Despot, predstavio bitcoin bankomat u Rijeci.[52] U Rijeci je bankomat smješten u Botelu Marina, koji je istovremeno hotel, restoran i noćni klub s raznovrsnim sadržajima, otvoren od 0 do 24.[53]Iste godine, nešto ranije nego u Rijeci, postavljen je i prvi bitcoin bankomat u Splitu. Postavio ga je Vedran Kajić u centru grada u frizerskom studiju Models na adresi Vukovarska 5.[54]

Jedan bitcoin bankomat postavljen je i u noćnom klubu u Las Vegasu, a omogućuje posjetiteljima kluba da striptiz ples plaćaju upravo putem virtualnih valuta, odnosno putem Bitcoina. Cijela stvar funkcionira vrlo jednostavno, a posjetiteljima striptiz kluba jamči anonimnost prilikom plaćanja. Naime, pri ulasku u striptiz klub nalazi se bankomat za Bitcoin koji korisnicima omogućuje Bitcoin transakcije. S druge strane, striptizete na sebi imaju otisnut privremeni QR kod koji zapravo sadržava podatke o njihovom virtualnom novčaniku.

Jednostavnim skeniranjem QR koda posjetitelj dobiva potrebne podatke i može uplatiti novac za usluge koje može vidjeti. Na taj način osigurava se anonimnost samih posjetitelja koji plaćaju,

[51]http://www.investicije.biz/bitcoin_virtualna_valuta.html
[52]http://www.poslovni.hr/tehnologija/razisli-se-pioniri-bitcoin-poduzetnistva-u-hrvatskoj-samostalni-jos-ambiciozniji-313373
[53]https://www.netokracija.com/bitcoin-bankomat-hrvatska-rijeka-118988
[54]http://www.poslovni.hr/startup-i-vase-price/i-u-splitu-bitcoin-bankomat-s-hrvatskim-potpisom-312481

ali se osigurava i sam transfer novca. Sve zajedno čini jednu zanimljivu cjelinu koja bi vrlo lako mogla postati standard na drugim sličnim mjestima.Uz plaćanje striptiza, u istom je klubu moguće platiti i piće putem Bitcoina. No, omogućeno i standardno plaćanje gotovinom, koje trenutno bira još jako veliki broj korisnika. Prema dostupnim podacima, sve je više onih koji za plaćanje biraju upravo Bitcoin i ostale virtualne valute.[55]

4.2. Primjer iz prakse

Prva pekarnica koja koristi plaćanje bitcoinima je pekarnica Kroštula koja se nalazi u centru Zagreba. Naime, njezin vlasnik smatra kako je to vrlo zanimljiv i praktičan oblik plaćanja koji stranci sve više koriste te kako će vrlo brzo i u Hrvatskoj kriptovalute biti sve prisutnije.[56] U Splitu je otvoren i dućan za kriptovalute. Naime, u Splitu se otvorila fizička trgovina u kojoj se mogu kupiti kriptovalute za gotovinu. Trgovina za direktnu kupnju kriptovaluta za gotovinu je smještena na adresi Ulica Hrvatske Mornarice 1C.

U trgovini Bitcoin Store se mogu kupiti altcoinovi, ethereum i najpopularnija kriptovalutabitcoin, a samo plaćanje se odvija gotovinom ili karticom. Na kraju svoje kupnje kupci dobiju fiskalizirani račun kao i prilikom svake druge kupnje. Provizija trgovine je 5%, a to znači da kupci plaćaju 5% višu cijenu kriptovaluta nego što je njezina trenutna vrijednost na tržištu.[57]

Najpoznatija hrvatska Internet stranica na kojoj se može kupiti bitcoine zove se bitocin – mjenjacnica.hr. Dovoljno je samo da se klikne na logo bitcoina te da se odabere opcija „Kupi“. Potom kupac upisuje vrijednost bitcoina koju želi kupiti te mora kopirati javni ključ iz svoj bitcoin novčanika i to onaj uz koji piše „SHARE“. Korisnik dobije podatke za uplatu i potom putem svog Internet bankarstva prebacuje tražene kune na račun te mjenjačnice.[58]

U nastojanju da se prihvati bitcoin, kao i ostale kriptovalute, putnička agencija iz Malte, otoka Gozo odlučila je ponuditi svojim klijentima paket aranžmana koji se plaćaju isključivo bitcoinom. To je početkom listopada 2017. godine urodilo plodom te su dva turista rezervirali odmor. Odmor su rezervirali Japanski inženjer Koideu i njegova supruga, koji navode da su se odlučili na bitcoin kao oblik plaćanja jer je takav način plaćanja u Japanu sve prihvaćeniji od

[55]https://pcchip.hr/kriptovalute/bankomat-za-bitcoin-postavljen-u-striptiz-klub/
[56]http://studentski.hr/vijesti/hrvatska/krostula-postala-prva-pekarnica-koja-prima-bitcoine
[57]https://crobitcoin.com/ducan-za-kriptovalute-otvoren-u-splitu/
[58]http://www.poslovni.hr/poduzetnik/isprobali-smo-kupnju-i-prodaju-popularne-kriptovalute-335517

strane maloprodajnih trgovina. Malta već duže vrijeme podržava kriptovalute što je čini jednom od zemalja koje prihvaćaju Bitcoin u Europi.[59]

4.3. Wallet (novčanik)

Wallet ili novčanik je posebna adresa koja može primati kriptovalute. Može se usporediti s običnom *e-mail* adresom. Svaki blockchain ima svoju vrstu walleta te ih u ovom trenu većina nije međusobno kompatibilna, primjerice nije moguće poslati Bitcoin na Ethereum adresu. Ustvari, svatko može imati koliko god adresa poželi te ne postoji način da se adresa poveže s pravim identitetom korisnika, osim u slučaju kada korisnik sam ne učini neke propuste ili to javno objavi. Na većini blockchainova stanje svačije adrese je javno te svatko vidi koliko koja adresa ima sredstva. Ukoliko na to gledamo kao na *e-mail*, wallet u kripto svijetu je kao *e-mail*inbox kojeg svatko može pročitati, ali samo vlasnik može pisati odgovore.

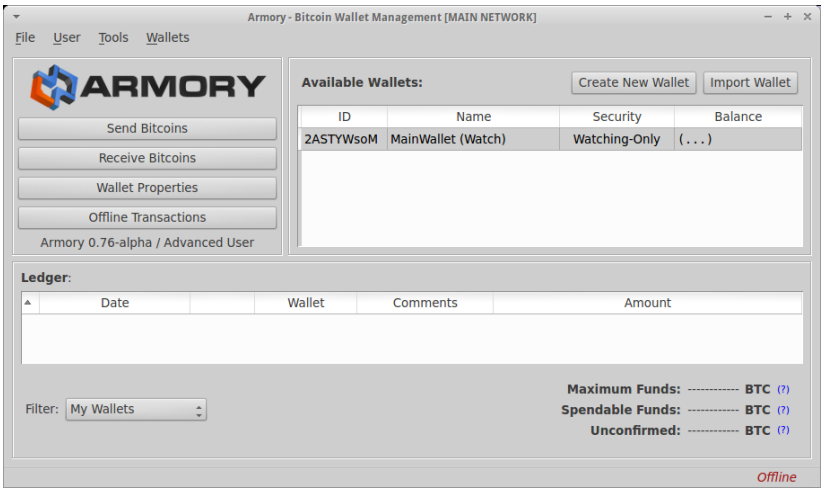
Način na koji se sredstva na nekoj adresi koriste je da se uz pomoć privatnog ključa (kombinacije brojki i slova koju je nemoguće matematički pogoditi) potpiše izjava (tzv. transakcija) da se vrši prijenos sredstava s adrese A na adresu B, i to se onda šalje u blockchain na potvrdu od strane svih ostalih korisnika.[60]

Nekoliko je različitih vrsta novčanika:

Desktop novčanici(slika 5)–korisnik kada instalira originalan bitcoin klijent (Bitcoin-QT) atda već ima novčanik, iako možda toga nije niti svjestan. U svrhu prenošenja transakcija preko mreže, taj software jednako tako omogućuje stvaranje bitcoin adrese za slanje, primanje virtualne valute te pohranu njenog privatnog ključa. Postoje i ostali desktop novčanici, svaki sa drugačijim karakteristikama. Multibit je dostupan za Windows, Mac OSX i Linux. Hive je OSX novčanik s nekim jedinstvenim karakteristikama, uključujući aplikaciju koja se povezuje direktno na bitcoin servise. Neki novčanici su sigurnosno orijentirani, primjerice Armory. Nekima je cilj omogućiti dodatnu anonimnost, primjerice DarkWallet.[61]

[59]https://cointelegraph.com/news/malta-based-travel-agency-decides-to-exclusively-accept-bitcoin-payments
[60]https://bitfalls.com/hr/2017/08/31/what-cryptocurrency-wallet/
[61]https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/

Slika 5. Primjer desktop novčanika



Izvor: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/

Mobilni novčanici(slika 6) – desktop novčanici nisu od neke koristi ako se korisnik nalazi na ulici pokušavajući nešto platiti. U takvoj situaciji se mobilni novčanici pokazuju poprilično korisnima. Pokrenuti kao aplikacije na pametnim telefonima, novčanici spremaju korisnikove privatne ključeve od bitcoin adresa te omogućuju direktno plaćanje putem uređaja. U nekim će slučajevima novčanik iskoristiti prednosti NFC opcije na pametnim telefonima te će korisnicima omogućiti plaćanje dodirom uređaja s čitačem bez unosa bilo kakvih informacija. Zajednička karakteristika mobilnih novčanika jest što nisu potpuni bitcoin klijenti. Potpuni bitcoin klijent mora skinuti cijeli bitcoinblockchain koji uvijek raste i veličine je nekoliko gigabajta.

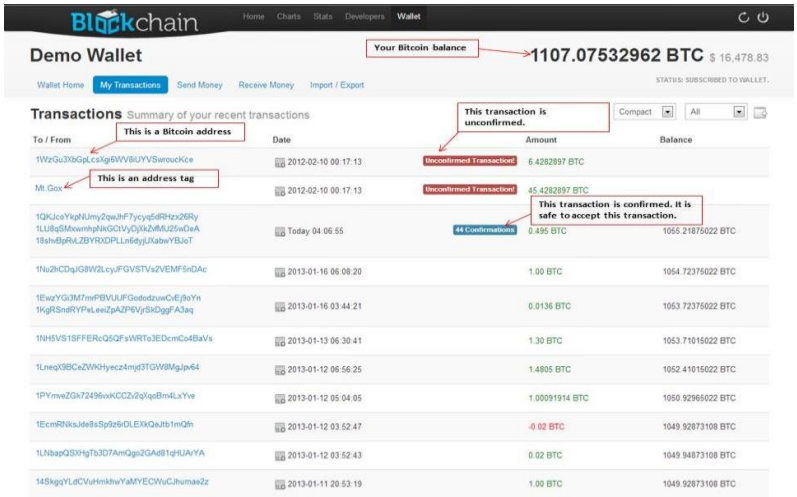
Slika 6. Primjer mobilnog novčanika

Izvor: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/

Umjesto toga, mobilni novčanici su dizajnirani pomoću SPV-a (*Simplifiedpaymentverification*). Oni skidaju mali dio blockchaina i oslanjaju se na druge *nodove* u bitcoin mreži kako bi potvrdili da imaju prave informacije.Primjeri mobilnih novčanika: Bitcoinwallet, Mycelium, Blockchain (on čuva bitcoinoveenkriptirane na uređaju korisnika i pohranjene na web serveru kao dodatnu zaštitu). Neki imaju posebne karakteristike, kao primjerice Kipochi, koji kao bitcoin adresu nudi korištenje korisnikovog broja mobitela. Apple je posebno paranoičan što se tiče bitcoin novčanika te se intenzivno bori protiv njih tako da korisnici iPhonea ne mogu pronaći takve aplikacije na App storeu, ali mogu koristiti one na webu.[62]

Web/online novčanici(slika 7) - Web orijentirani novčanici pohranjuju korisničke ključeve online – na računalo koje kontrolira netko drugi i koje je povezano na internet. Postoji nekoliko takvih servisa od kojih neki nude mogućnost povezivanja mobitelom ili desktop novčanikom korisnika sinkronizirajući sve adrese koje korisnik posjeduje.Velika prednost web novčanika jest što im se može pristupiti bilo gdje ukoliko uređaj ima pristup internetu. Međutim, imaju jednu veliku manu: ako nisu korektno implementirani, mogu omogućiti organizaciji koja je u vlasništvu novčanika da vidi i upravlja ključevima korisnika, što znači da mogu upravljati njihovim novcem bez njihova znanja i dozvole.

Slika 7. Primjer web/online novčanika



[62]Ibid

Izvor: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/

To je poprilično zastrašujuće ako korisnik ima izdašnu svotu bitcoinova. Coinbase, integrirani novčanik/burza omogućen je svima u svijetu, ali je kupovina dopuštena samo unutar SAD-a. Blockchain također ima web orijentiran novčanik, a Strongcoin nudi hibridni novčanik koji korisnicima omogućava enkripciju privatnih ključeva prije nego ih šalju na njihov server – enkripcija se obavlja u browseru.[63]

Hardware novčanici su za sada vrlo rijetki. To su uređaji koji mogu pohraniti privatne ključeve elektronički i obavljati plaćanja. Trezor i Mycelium trenutno imaju takve novčanike u izradi, ali još nema rezultata. Zanimljivo rješenje je Nymisportswristband koje djeluje kao novčanik i otključava se pomoću srčanog ritma vlasnika.[64]

4.4. Upute za kupovinu bitcoina

Kupovina Bitcoina odvija se u nekoliko koraka koji su objašnjeni u nastavku[65]:

Kod 1. koraka (slika 8) se na početnom ekranu može vidjeti trenutačna cijena bitcoina. Može se birati između četiri jezika: hrvatskog, engleskog, francuskog i njemačkog. Potom treba pritisnuti „Započni“ te slijediti upute.

Slika 8. Korak 1. – početni ekran

[63]Ibid
[64]ibid
[65]https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

Izvor: https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

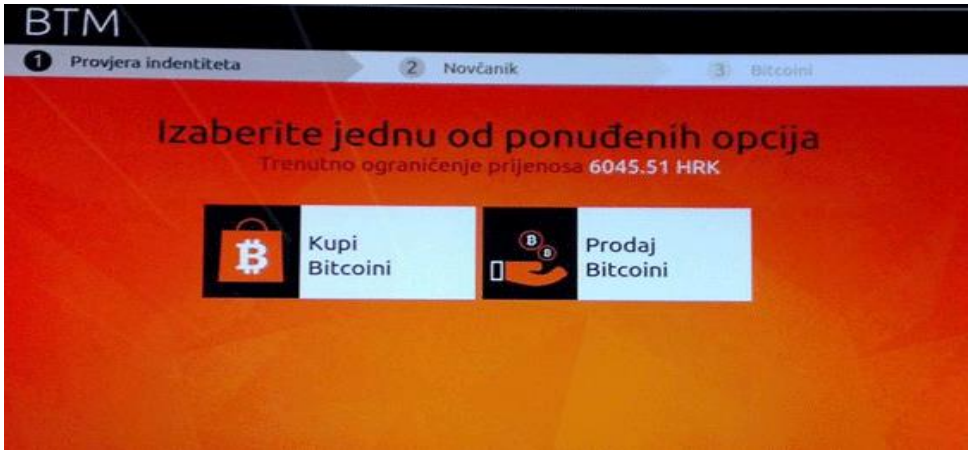
Potom korisnik mora unijeti broj mobitela (slika 9), na koji će mu stići SMS poruka s verifikacijskom porukom.

Slika 9. Korak 2. – broj mobitela

Izvor: https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

U sljedećem koraku (slika 10) korisnik mora odabrati želi li prodati ili kupiti bitcoine (u primjeru je opisana kupovina bitcoina).

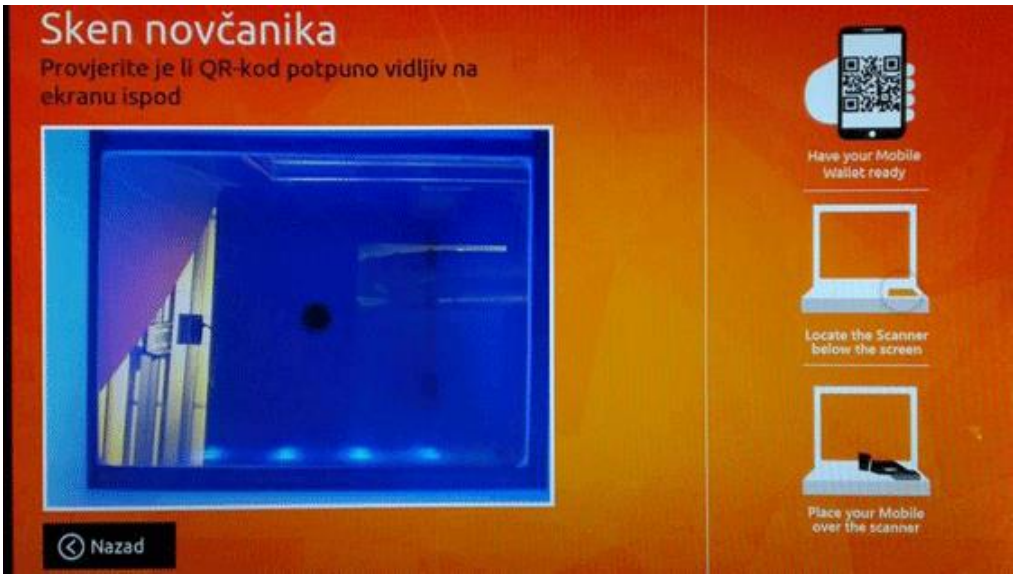
Slika 10. Korak 3. – kupnja ili prodaja



Izvor: https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

Ako korisnik nema bitcoin novčanik, npr. *MyceliumBitcoinWallet*, onda će se adresa i ključ ispisati na papiriću. Ako ima novčanik onda je potrebno skenirati QR kod novčanika na način da se prisloni mobitel na skener (slika 11).

Slika 11. Korak 4 – skeniranje novčanika



Slika 11. Korak 4 – skeniranje novčanika
Izvor: https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

Sljedeći je korak unos gotovine (slika 12), a sam tečaj se očitava sa Bitstampa, a kao minimalni iznos gotovine postavljeno je 100 kuna. Korisnik u bilo kojem trenutku može odustati od kupnje.

Slika 12. Korak 5 – unos gotovine

Izvor: https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

Nakon što je korisnik ubacio novčanice, bankomat mu prikazuje koliko je ubacio. Ako je to iznos koji želi, mora odabrati „Završi“. Tada će mu bitcoini biti poslani na njegovu Bitcoin adresu (slika 13). **Slika 13.** Korak 6. – završetak kupnje

Izvor: https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/

5. ZAKLJUČAK

Virtualne su valute s razvojem informatičkih tehnologija postale sve važniji faktor u ekonomiji. Toliko su napredovale da postoje uži i širi pojmovi vezani uz njih, dijele se na više vrsta, neka su ih poduzeća počela prihvaćati kao sredstva plaćanja itd. Kroz rad je najzastupljeniji bitcoin, s obzirom da za njega postoji najviše primjera te ga je najjednostavnije obrađivati, uspoređivati itd.

Bitcoin je, ustvari relativno zanimljiv po svom principu rada koji se naziva blockchain i za čiji rad nije potrebna središnja institucija koja bi kontrolirala čitavi sustavi. Sustav blockchain se već testira te se razmatra da se uvede u puno širu upotrebu od samog sustava virtualnih valuta. Neovisno od razvoja i dalje postoje određeni rizici s kojima se susreću kriptovalute u svom djelovanju i koje bi se protekom vremena i razvojem trebale riješiti.

Kao najčešći rizici se spominju ogromne varijacije u vrijednostima, mogućnost krađe, špekulacije s njima, pitanje legalnosti virtualnih valuta, ali i niz drugih. Jedan od problema koji se vrlo često veže uz virtualne valute je njihovo korištenje u kriminalne svrhe, jedan od glavnih pohoda njihovoj zloupotrebi je anonimnost korištenja.

Temeljna ideja koncepta bitcoina bila je stvoriti sustav P2P (person to person). Koncept se temelji na stvaranju sustava decentralizirane valute koji će omogućiti izravni dodir dviju osoba u transakciji bez posredovanja institucija kao što su centralne državne banke.

Diljem svijeta je postavljeno niz bankomata za virtualne valute, koji svojim korisnicima pružaju mogućnost jednostavnog baratanja virtualnim valutama. U Republici Hrvatskoj su do sada postavljena takva 4 bankomata, dva u Zagrebu, jedan u Splitu i jedan u Rijeci. U Splitu se otvorila i fizička trgovina u kojoj se mogu kupiti kriptovalute za gotovinu.

Svaki blockhain ima svoju vrstu walleta, a trenutno ih većina nije međusobno kompatibilna. Način na koji se sredstva na nekoj adresi koriste je da se uz pomoć privatnog ključa (kombinacije brojki i slova koje je nemoguće matematički pogoditi) potpiše izjava da se vrši prijenos sredstava s adrese A na adresu B, i to se onda šalje u blockchain na potvrdu od strane svih ostalih korisnika.

LITERATURA

Knjige:

[1] Abramowicz, M.: Cryptocurrency – BasedLay, ArizRev, sv. 58, 2016.

[2] Meisser, Luzius.: *Bitcoin – A PromiseofFreedom, NextGenerationFinance, 2013*

[3] Narayanan, Arvindetal., 2016: *BitcoinandCryptocurrency Technologies*

[4] Rogojanu, A., Badea, L., Others: Theissueofcompetingcurrencies. Casestudy-Bitcoin, Theor.Appl.Econ., sv.21, izd. 1, 2014.

[5] Turpin, J. B., Bitcoin: Theeconomiccase for a global, virtualcurrencyoperating ina n unexploredleaglframework, Indiana J. Global Leg. Stud., sv. 21., izd. 1, 2014.

Časopisi i stručni članci:

[1] AFP: Japan regulatesvirtualcurrencyafterBitcoinscandal, 2016. Dostupno na: https://www.yahoo.com/tech/japan-regulates-virtual-currency-bitcoin-scandal-083419986- -finance.html [13.08.2018.]

[2] Ali, R., Barrdear, J., Clews, R., Southgate J., (2014a), Innovationsinpaymenttechnologiesandtheemergenceofdigitalcurrencies, Bank ofEnglandQuarterlyBulletin, Vol. 54, No. 3, str. 262-275. Dostupno na: http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digit alcurrenciesbitcoin1.pdf, pristup 12.8. 2018.

[3] Banque de France (2013), Thedangerslinked to theemergenceofvirtualcurrencies: theexampleofbitcoins, Focus, No 10., 5 December 2013. Dostupno na: https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus10-the_dangers_linked_to_the_emergence_of_virtual_currencies_the_example_of_bitcoinsGB.pdf [13.8.2018.]

[4] Baczynska, G., i Pomeroy, R.: RussianauthoritiessayBitcoinillegal, 2014. Dostupno na: http://www.reuters.com/article/us-russia-bitcoin-idUSBREA1806620140209 [13.8.2018.]

[5] Buterin, D., Ribarić, E., Savić, S., (2015), Bitcoin - Nova globalna valuta, investicijska prilika ili nešto treće?, Zbornik Veleučilišta u Rijeci, Vol. 3 (2015), No. 1, str. 145-158.

[6] Dourado, Eli i Brito, Jerry. 2014.: *The New PalgraveDictionaryofEconomics,* Online Edition; http://jerrybrito.com/pdf/cryptocurrency-newpalgrave.pdf, 3. 8. 2018.

[7] Europsko nadzorno tijelo za bankarstvo: Upozorenje za korisnike virtualnih valuta, EBA/WRG/2013/01, 2013., Dostupno na: https://www.eba.europa.eu/documents/10180/598420/EBA_2013_01030000_HR_TRA 1-HR-19+12+13.pdf, pristup: 12.8.2018.

[8] Frančišćković, I.: *Bitcoin*, Diplomski rad, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Matematički odsjek, Zagreb, studeni, 2015.

[9] Global Drug Police Observatory: SilkRoadandBitcoin. Swansea: Swansea University PrifysgolAbertawe, 2013. Dostupno na: https://www.swansea.ac.uk/media/GDPO%20Situation%20Analysis%20silk%20rd%20and% 20bitcoin.pdf, pristup: 15.8.2018.

[10] Graydon, Carte, 2014: *WhatisCryptocurrency?,* https://www.ccn.com/cryptocurrency/, 4. srpnja 2018.

[11] Heid, Alexander, 2013: *AnalysisoftheCrypotcurrency Marketplace;* https://bravenewcoin.com/assets/Whitepapers/HackMiami-Analysis-of-the-Cryptocurrency-Marketplace.pdf, 3. srpnja 2018.

[12] Ivezić, B.: HNB: Bitcoin je poput zlata u World ofWarcraftu, 2013. Dostupno na: http://www.poslovni.hr/trzista/hnb-bitcoin-je-poput-zlata-u-world-ofwarcraftu-i-linden-dolara-u-second-lifeu-258543 [15.08.2018.]

[13] Osborne, C.: MyCoinclosesitsdoors, $387 millionininvestorfundsvanishes, 2015.; Dostupno na: http://www.zdnet.com/article/mycoin-closes-its-doors-387-millionin-investor-funds-vanishes/ [13.8.2018.]

[14] Quentson, A.: WhatisEthereum?, 2017., dostupno na: https://www.ccn.com/what-is-ethereum/, 22.7.2018.

[15] Rubenfeld, S.: Canada EnactsBitcoinRegulations, 2014. Dostupno na: http://blogs.wsj.com/riskandcompliance/2014/06/23/canada-enacts-bitcoin-regulations/ [13.8.2018]

[16] SatoshiNakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.*; https://bitcoin.org/bitcoin.pdf, 4. srpnja 2018.

[17] Sidel, R., Casey, M. J., Warnock, E.: Shutdownof Mt. GoxRattlesBitcoinMarket; Dostupno na:

http://www.wsj.com/articles/SB10001424052702304834704579404101502619422 [30.06.2016.]

[18] TheClearingHouse: Virtualcurrency: risksandregulation, June 23, 2014, dostupno na: https://www.theclearinghouse.org/~/media/Files/Research/20140623%20Virtual%20Currency%20White%20Paper.pdf, pristup: 12.8.2018.

[19] White, L., H., Themarket for cryptocurrencies, CatoJorunal, Vol. 35., No. 2. (Spring/Summer 2015), str. 383-402. Dostupno na: http://object.cato.org/sites/cato.org/files/serials/files/cato-journal/2015/5/cj-v35n2-13.pdf [12.8.2018.]

[20] Whittaker, Z.: Bitstampexchangehacked, $5M worthofbitcoinstolen, 2015. Dostupno na: http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amidhack-concerns-heres-what-we-know/ [13.8.2018.]

Internet izvori:

[1] https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/, 3. srpnja 2017.

[2] https://medium.com/koinex-crunch/a-brief-history-of-cryptocurrency-889fed168555, 4. srpnja 2018.

[3] https://admiralmarkets.com.hr/education/articles/cryptocurrencies/sto-je-litecoin, pristup, 21.7.2018.

[4] https://crobitcoin.com/altcoin/ethereum/, pristup, 22.7.2018.

[5] https://www.blockchain.com/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=, pristup: 12.8.2018.

[6] https://coinmarketcap.com/currencies/ethereum/#charts, pristup: 12.8.2018.

[7] http://dario-dolic.from.hr/ponzijeva-sema-charles-ponzi/, pristup: 13.8.2018.

[8] https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp, pristup: 13.8.2018.

[9] http://www.porezna-uprava.hr/HR_publikacije/Lists/mislenje33/Display.aspx?id=19252, pristup: 13.8.2018.

[10] https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp, pristup: 15.8.2018

[11] https://pcchip.hr/ostalo/tech/uvod-u-blockchain-tehnologiju/, pristup: 17.8.2018.
[12] https://www.netokracija.com/sto-je-blockchain-132284, pristup: 17.8.2018.
[13] http://www.glas-slavonije.hr/220167/7/Bitcoin---umjetni-virtualni-novac-ili-valuta-snova, pristup: 20.8.2018.
[14] http://www.investicije.biz/bitcoin_virtualna_valuta.html, pristup: 20.8.2018.
[15] http://www.poslovni.hr/tehnologija/razisli-se-pioniri-bitcoin-poduzetnistva-u-hrvatskoj-samostalni-jos-ambiciozniji-313373, pristup: 20.8.2018.
[16] https://www.netokracija.com/bitcoin-bankomat-hrvatska-rijeka-118988, pristup: 20.8.2018.
[17] http://www.poslovni.hr/startup-i-vase-price/i-u-splitu-bitcoin-bankomat-s-hrvatskim-potpisom-312481, pristup. 20.8.2018.
[18] https://pcchip.hr/kriptovalute/bankomat-za-bitcoin-postavljen-u-striptiz-klub/, pristup: 22.8.2018.
[19] http://studentski.hr/vijesti/hrvatska/krostula-postala-prva-pekarnica-koja-prima-bitcoine, pristup: 22.8.2018.
[20] https://crobitcoin.com/ducan-za-kriptovalute-otvoren-u-splitu/, pristup: 22.8.2018.
[21] https://www.regnata.com/bitcoin-bankomat-atm-hrvatska-zagreb-history-i-village/kriptovalute-335517, pristup: 22.8.2018.
[22] https://bitfalls.com/hr/2017/08/31/what-cryptocurrency-wallet/, pristup: 24.8.2017.
[23] https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/, pristup: 24.8.2018.
[24] http://www.poslovni.hr/poduzetnik/isprobali-smo-kupnju-i-prodaju-popularne-kriptovalute-335517, pristup: 24.8.2018.
[25] https://cointelegraph.com/news/malta-based-travel-agency-decides-to-exclusively-accept-bitcoin-payments, pristup: 25.8.2018.

POPIS SLIKA