Kriptovalute i njihov utjecaj na ekonomiju

Kozić, Krešimir

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Krešimir Kozić

Kriptovalute i njihov utjecaj na ekonomiju

ZAVRŠNI RAD

Varaždin, 2020.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Krešimir Kozić

Matični broj: 45096/16-R

Studij: Poslovni sustavi

Kriptovalute i njihov utjecaj na ekonomiju

ZAVRŠNI RAD

Mentor/Mentorica:

Prof. dr. sc. Neven Vrček

Varaždin, lipanj 2020.

Krešimir Kozić

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Područje istraživanja ovog rada obuhvaća pojam kriptovaluta i navodi vrste kriptovaluta prema tržišnom udjelu. Pojašnjava se povijest nastanka kriptovaluta te se objašnjava ideja iz koje proizlazi nastanak kriptovalute Bitcoin. Analizira se cijena kretanja kriptovaluta kroz prošlost i donose se zaključci o tome kako se cijena formirala. Ukratko, rad pojašnjava tehnologiju na kojoj se zasniva rad kriptovaluta, objašnjavajući metode kriptiranja, Blockchain mrežu i njezine mogućnosti te proces rudarenja kriptovaluta. Istražuje se tržište kriptovaluta te metode trgovanja kriptovalutama. Izvršena je analiza kriptovaluta kao mehanizma decentraliziranog sredstva plaćanja, ali i kao financijskog instrumenta. Ključan dio ove analize je usporedba kriptovaluta sa uobičajenim sredstvima plaćanja, kao i financijskim instrumentima, poput dionica. Posljednji dio rada proučava primjenu kriptovaluta u različitim državama svijeta uz različite primjere i utjecaj njihove upotrebe na današnju ekonomiju.

Ključne riječi: kriptovalute; blockchain; digitalne valute; Bitcoin; vrijednost kriptovaluta; trgovanje kriptovalutama

Sadržaj

1. Uvod

Zadnjih desetak godina došlo je do značajnog razvoja informacijske tehnologije kojom se stvara nova digitalna ekonomija. Digitalnu ekonomiju karakterizira digitalizacija različitih dijelova poslovanja. Brojni dokumenti više nisu arhivirani u papirnatom formatu nego se digitaliziraju radi praktičnosti, ali i uštede novca. U trenutku kada kupac izvrši internet kupnju, on primi digitalni račun u elektroničkom obliku koji je jednako važeći kao i papirnati. Isto tako se i financije digitaliziraju te se sve češće u literaturi spominje nova, brzorastuća znanost FinTech (eng. financial technology) koja se bavi tehnologijom i inovacijama koje unaprjeđuju tradicionalne financijske proizvode i usluge. FinTech uključuje aktivnost korištenja pametnih telefona za novčane transfere, prikupljanje kapitala za startupe, upravljanje vlastitim financijama i investicijama bez asistencije brokera. Uključuje i razvoj kriptovaluta kao novog digitalnog novca i sredstva plaćanja te razvoja pametnih ugovora za automatska izvršavanja dogovorenih uvjeta (Kagan, 2019).

U prošlost je upotreba kriptovaluta i njihove tehnologije bila rezervirana za pojedince, a danas postaje sve šire dostupna. U novije vrijeme se interes za kriptovalutama budi u sve više i više ljudi, a razlog tome zasigurno leži u velikom potencijalu kriptovaluta. Motivacija za izradu ovog rada bila je želja za izradom istraživanja o kriptovalutama i njihovoj zastupljenost u današnjoj ekonomiji te dublje razumijevanje smjera u kojem ide tehnologija kriptovaluta i koji je njezin utjecaj na današnju ekonomiju.

Rad se sastoji od sedam poglavlja od kojih je prvo poglavlje uvodno, drugo poglavlje pojašnjava metode i tehnike rada, a zadnje poglavlje je zaključak. Treće poglavlje započinje objašnjenjem što su kriptovalute i objašnjava kako su nastale kriptovalute, a zatim se prema tržišnom udjelu navode neke od poznatijih kriptovaluta. Dalje se nastavlja sa četvrtim poglavljem u kojem započinje s objašnjenjem zašto su nam za kriptovalute potrebni digitalni novčanici te kako oni funkcioniraju. Objašnjava se i pojam Blockchaina kao i proces rudarenja, gdje se pobliže objašnjavaju dva najkorištenija algoritma rudarenja. Peto poglavlje se bavi mjestima za trgovanjem kriptovalutama i kako ona funkcioniraju te povijesti trgovanjem Bitcoina i kretanjem njegove cijene. U šestom poglavlju istražujemo različite uloge kriptovaluta i primjere tih uloga u praksi, proučavamo po čemu se kriptovalute razlikuju od dionica i kako kriptovalute mijenjaju svijet prikupljanja kapitala. U završnom poglavlju donesen je sveobuhvatan zaključak ovoga rada.

2. Metode i tehnike rada

U izradi rada prilikom analize trenutnog tržišnog udjela kriptovaluta i trenutne cijene kriptovaluta korištena je CoinMarketCap web aplikacija koja preuzma podatke sa 400 dostupnih burzi.

Prilikom detaljnijeg analiziranja cijene gdje je u obzir je uzeta kronologija događaja i prikazana uzročno - posljedična veza, korištena je web aplikacija Bitcoin Historical Price & Events sa portala 99Bitcoins koja grafički prikazuje kretanje cijene Bitcoina, ali i bitne događaje koji su na tu cijenu i utjecali.

Za provjeru strukture provizija i izrađivanje snimke zaslona (eng. *Screenshoot*) koja prikazuje sučelje platforme za trgovanje kriptovalutama, a sadrži zid narudžbi, odnos cijene dviju kriptovaluta preko grafa te zadnje izvršene naloge, korištena je burza za trgovanje kriptovalutama Binance.

Prilikom utvrđivanja kretanje cijene S&P 500 indeksa korišten je web alat MarketWatch.

3. Kriptovalute

Izraz Kriptovaluta (eng. Cryptocurrency) nastao je kombinacijom riječi „kripto“ i „valuta. „Kripto“ dolazi od znanosti kriptografije, koja omogućava siguran proces izvršavanja transakcija u digitalnom obliku, dok pojam „valuta“ označava sredstvo plaćanja te daje digitalnom zapisu monetarnu vrijednost.

Kriptovalute su virtualne valute, odnosno valute koje nisu opipljive poput uobičajenih valuta. Kuna, Euro, Dolar i dr. valute je moguće fizički posjedovati u obliku kovanica i novčanica dok kriptovalute postoje samo digitalno, a ne i u fizičkom, opipljivom svijetu. Osoba koja posjeduje kriptovalutu zapravo posjeduje samo digitalni zapis, odnosno digitalni novčanik (eng. Wallet). Digitalni novčanik se sastoji od privatnog i javnog ključa. Privatni i javni ključevi su kriptografske metode koje se koriste za kreiranje digitalnih novčanika te će u nastavku ovog rada biti detaljnije pojašnjene.

Većina ljudi se sa digitalnom valutom po prvi puta susrela igrajući pojedine video igrice. Česta pojava su novčići s kojima je moguće u igrici kupovati predmete, a zarađuje ih se određenim radom i postignućima. Iste novčiće u igrici najčešće je moguće kupiti u stvarnoj valuti, tj u „stvarnom“ svijetu, i na taj način igrač si može olakšati uloženi rad. Novčići u igrici, kao i kriptovalute, imaju određenu vrijednost. Glavna razlika između kriptovaluta i nekog novčića u igrici je ta što iza kriptovaluta stoji tzv. Blockchain tehnologija koja kriptovalutama omogućuje decentralizaciju.

Naime, kada u nekoj igrici igrač sakupi ili kupi novčiće, onda je vlasnik tih novčića zapravo kompanija koja je napravila igricu. Kompanija u svakom trenutku može zamrznuti novčiće, dodati još novčića u digitalne novčanike ili provesti bilo kakvu promjenu bez znanja i pristanka igrača. Drugim riječima, svu zalihu novčića kontrolira jedna korporacija koja je vlasnik igre. Budući da su kriptovalute decentralizirane, nitko ne može zamrznuti neku transakciju ili pak generirati još kriptovaluta, kao što to može kompanija koja je napravila video igricu.

Sličnom analogijom mogu se promatrati državni regulatori i centralna banka koja kontrolira novac u opticaju. Državni regulator ima kontrolu da u svakom trenutku može odlučiti izdati obveznice i printati još novca te na taj način smanjiti vrijednost valute koja je već u optjecaju usljed inflacije.

Razlika između transakcije kripotovalutama i kreditnim/debitnim karticama je u tome što kriptovalute omogućuju nositelju da šalje točno ono što želi trgovcu ili primatelju bez ikakvih dodatnih informacija. Korištenje kriptovaluta ne zahtijeva imena, nego samo digitalnu oznaku novčanika, stoga nema trećih strana koje su uključene u transakciju (Europska komisija, 2020).

3.1. Povijest kriptovaluta

Američki inženjer računalstva i kriptograf David Chaum, tijekom svojeg doktorata 1982., izdao je rad o tehnologiji digitalnih potpisa. Tim tehnološkim izumom razvijen je novi koncept enkripcije javnim ključem koja će kasnije postati tehnička podloga za kriptovalute. Osam godina nakon izdavanja predhodno navedenog rada, Chaum otvara tvrtku „DigiCash Inc“ koja je bila fokusirana na korištenje novootkrivene tehnologije za pametne kartice, sve dok 1993. godine nisu napravili prvu kriptovalutu naziva „eCash“. Cilj eCash- a bio je omogućiti korisnicima ostavljanje što manjeg digitalnog traga, odnosno osigurati privatnost transakcija. Unatoč prvotnom zanosu, prva kriptovaluta nije doživjela komercijalni uspjeh te je tvrtka 5 godina kasnije doživjela bankrot (Mahler, 2018).

Prva uspješna kriptovaluta koja je zaživjela naziva se Bitcoin te je i danas poznata kao jedna od najpopularnijih kriptovaluta. 2008. godine objavljen je rad naziva „Bitcoin: A Peer-to-Peer Electronic Cash System" u kojem je pobliže opisan način funkcioniranja nove kriptovalute. Kreator tog rada potpisao se kao Satoshi Nakamoto, ali nije poznato je li to pravo osobno ime ili se samo radi o pseudonimu. Par mjeseci kasnije pokrenuta je Blockchain mreža te učinjena prva Bitcoin transakcija u kojoj je izrudaren prvi blok, a odvila se između Nakamota i računalnog programera Hal Finneya. Krajem godine objavljena je prva cijena Bitcoina, odnosno rata konverzije jednog američkog Dolara za 1,309.03 Bitcoina. Nakon ovoga bilo je samo pitanje vremena kada će se realizirati prva kupnja Bitcoinom. 2010. godine programer Laszlo Hanyecz poslao 10,000 Bitcoina za dvije pizze vrijednosti 25 američkih Dolara. Nedugo zatim vrijednost Bitcoina je porasla, nastala je nova burza za prodaju Bitcoina za Dolare naziva „Mt. Gox“ te su se rudari počeli udruživati kako bi zajedno rudarili Bitcoin (Fiorillo, 2018).

Bitcoin je softver otvorenog koda (eng. open-source), što znači kako je programski kod Bitcoina ~~je~~ vidljiv svima i svatko tko ima tehničkog znanja ga može testirati i uvjeriti se radi li zbilja na način kako je opisano. Budući da je programski kod javno dostupan mnogi ga pokušavaju poboljšati i napraviti bolju kriptovalutu te su tako nastale brojne nove kriptovalute, koje su vrlo često samo poboljšana inačica programskog koda Bitcoina (eng. Fork).

3.2. Vrste kriptovaluta

Bitcoin je prva uspješna i globalno najkorištenija kriptovaluta pa se druge kriptovalute često nazivaju alternativnim digitalnim novcem ili novčićima (eng. Altcoins). Ovakvih alternativnih kriptovaluta danas je prisutno na tisuće. Iza njih stoje njihovi kreatori koji su najčešće privatne tvrtke koje imaju određenu viziju te su prikupili kapital investitora upravo preko izdavanja kriptovaluta.

Kriptovalute se najčešće sortiraju prema tržišnom udjelu, koji predstavlja iznos novca u Dolarima u određenoj kriptovaluti ili nekom drugom financijskom instrumentu. Ukoliko pojedinac koji je vlasnik Bitcoina odluči preprodati određenu količinu za vrijednosti X u Dolarima, tržišni udio Bitcoina će se smanjiti za vrijednost X. Bitcoin se smatra kriptovalutom koja dominira nad alternativnim kriptovalutama jer je njegov tržišni udio u trenutku pisanja ove rečenice 169,065,577,529 američkih Dolara, što je 66.1% tržišta kriptovaluta. Tržišni udio je moguće provjeriti koristeći se CoinMarketCap web stranicom (CoinMarketCap, 23.5.2020).

Slika 1: Prikaz kriptovaluta sortiran prema tržišnom udjelu (Izvor: CoinMarketCap, 23.5.2020)

Druga najpopularnija kriptovaluta prema tržišnom udjelu je Ether. Radi se o kriptovaluti koja nije poboljšana softverska inačica Bitcoina već ima svoj zaseban Blockchain naziva Ethereum te je on neka verzija programabilnog Blockchaina. Ideja Etherium mreže je da se na njoj programiraju i izvršavaju pametni ugovori. Pametni ugovor je programski kod upućen Etherium mreži (eng. *Deployed*), koji izvršava transakcije bez utjecaja treće stranke, gdje povjerenje izvršavanja garantira Blockchain. Primjerice, programski kod predstavlja neki ugovor između dvije osobe i ako se ispoštuju svi uvjeti ugovora kod će automatski izvršiti neku zadanu transakciju (Orešković, 18.2.2020). Ether je valuta kojom se plaća izvršavanje transakcija na Etherium Blockchainu. Vrlo česta podloga za novonastale kriptovalute je upravo Etherium Blockchain jer je na njemu jednostavno raditi nove tokene preko smart contracta.

Treća po tržišnom udjelu je kriptovaluta Ripple koja je zapravo protokol za internacionalna plaćanja između banaka. Konačna zamisao koja stoji iza valute Ripple je zamijeniti trenutno rješenje za transakcije koje se koristi u svijetu bankarstva poput SWIFT-a (Rogina, 2020). Četvrta po redu je Tether koji je tvz. stabilan novčić (eng. *Stable coin*), čija vrijednost je uvijek ista naspram Dolara. Tether je primjer kriptovalute koja tehnički to uopće nije jer ne koristi blockchain i centralizirana je, međutim vrlo je često korištena u trgovanju kriptovalutama. Koristi se u situacijama u kojima se želi zadržati stabilna vrijednost

kriptovalute, odnosno želi se izbjeći rizik volitabilnost cijene Bitcoina ili druge volitabilne kriptovalute.

Unatoč postojanju raznih iznimki, većina kriptovaluta ipak koristi Blockchain tehnologiju radi decentralizacije financija, odnosno kreiranja kriptovalute s idejom da ona bude sredstva plaćanja ili čuvanja novca koje nije kontrolirano od treće strane. Neke novije kriptovalute su samo bolja inačica već postojećih, primjerice Litecoin je verzija Bitcoina koja je povoljnija i brža za izvođenje transakcija.

4. Tehnologija na kojoj se baziraju kriptovalute

Kako su kriptovalute novac koji je virtualan, moguće im je pristupiti samo digitalno. Shodno tome nužno je imati softversku i hardversku tehnološku podlogu za korištenje kriptovaluta. Hardverska podloga je računalo koje ima pristup internetu. Za primanje i čuvanje kriptovaluta ili slanje istih potreban je i digitalni novčanik, odnosno softver. Kako bi transakcije između različitih digitalnih novčanika bile moguće koristi se distribuirani sustav Blockchain, a „proizvodnja“ kriptovaluta odvija se pomoću procesa naziva rudarenje. Svi ovi pojmovi biti će pobliže objašnjeni u nastavku.

4.1. Digitalni novčanici i tehnologija digitalnih novčanika

Slanje i primanje, odnosno korištenje kriptovaluta moguće je nakon posjedovanja digitalnog novčanika (eng. Wallet) instaliranog na računalu ili mobitelu. Budući da se cijeli proces primanja, slanja i čuvanja kriptovaluta izvodi na internetu (eng. Online), potrebno je osigurati da treća strana nema pristup mijenjanju transakcije ili iznosu sredstava na digitalnim novčanicima. Kako bi se to postiglo, kriptovalute koriste zaštitu informacija matematičkim pristupom koristeći kriptografiju.

4.1.1. Kriptiranje digitalnih novčanika

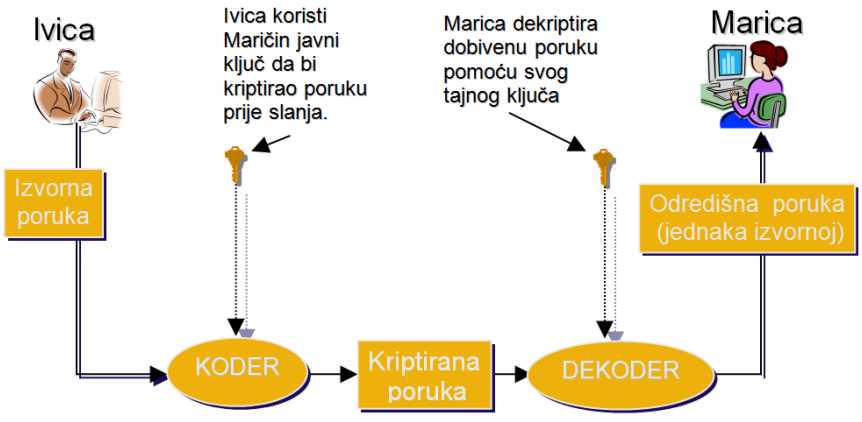
Osnovni zadatak kriptografije je omogućiti pošiljatelju i primatelju komuniciranje preko nesigurnog komunikacijskog kanala, poput računalna mreže, na način da treća osoba, koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke (Dujella, bez dat.). Dvije osobe koje žele na takav način razmjenjivati poruke mogu unaprijed dogovoriti pravila kriptiranja koja će pratiti, primjerice svako slovo poruke koja se šalje mogu zamijeniti s brojem, npr. slovo P zamjene brojem 1, slovo A brojem 2, slovo S brojem 3, itd. Ukoliko unaprijed dogovore ovo pravilo i jedna osoba pošalje drugoj poruku „123“, druga osoba će znati da 1 predstavlja P, 3 predstavlja A i 2 predstavlja S te će tako navedenu poruku moći dekriptirati. U slučaju kada je poruka poslana internetom, treća strana koja nadgleda mrežu će moći vidjeti samo kriptiranu poruku „123“ i neće je moći ispravno interpretirati, odnosno neće znati kako je poslana poruka zapravo „PAS“. Ovo je primjer simetričnog kriptiranja. Pravila dekriptiranja predstavljaju unaprijed dogovoreni tajni ključ. Simetrično kriptiranje poruka je najjednostavnija, ali vrlo sigurna metoda enkripcije.

Pravila dekriptiranja zapravo predstavljaju tajni ključ koji su osobe koje šalju poruku unaprijed dogovorile. Samo osobe koje imaju tajni ključ će kriptirane poruke moći dekriptirati i

saznati sadržaj poslane poruke koji je u gornjem primjeru bio „PAS“. Ovakvo kriptiranje poruka se naziva simetrično kriptiranje i to je najjednostavnija moguća metoda kriptiranja, a vrlo je sigurna.

Slanje ili primanje kriptovalute možemo poistovjetiti sa slanjem poruka koje predstavljaju transakcije, a potrebno ih je potpisati ili, pojednostavljeno rečeno, ovjeriti s tajnim ključem ili privatnim ključem. Javni ključ predstavlja adresu na koju se šalje poruka (transakcija). Dakle imamo isti zadatak koji je potrebno obaviti, ali metoda kriptiranja u ovakvoj situaciji će morati biti ponešto drugačija od prethodno opisanog primjera. Kako se transakcije slanja i primanja kriptovaluta događaju na internetu, a nerijetko između osoba koje se osobno ne poznaju, nemoguće je da osobe koje izvode transakciju unaprijed dogovore pravila kriptiranja, odnosno tajni ili privatni ključ. Iz tog razloga digitalni novčanici za kriptovalute koriste asimetrično kriptiranje.

Kod asimetričnog kriptiranja privatni ključ osobe koja šalje poruku ili transakciju služi samo za kriptiranje poruke, dok osoba koja prima transakciju ima svoj vlastiti privatni ključ kojim može samo dekriptirati transakciju. Poanta je da ne postoji jedan privatni ključ koji su osobe unaprijed dogovorile nego da svaka osoba ima svoj jedinstveni privatni ključ kojem može dekriptirati poruku, ili u ovom slučaju pristupiti sredstvima digitalnog novčanika. Kod takvog načina kriptiranja se dvije osobe koje izvode transkciju ne moraju predhodno naći kako bi dogovorili pravila kriptiranja , tj. podjelili zajednički privatni ključ.



Slika 2: Primjer asimetričnog kriptiranja (Izvor: Lončar, 2017)

Asimetrično kriptiranje se provodi algoritmom koji koristi jednosmjernu funkciju kako bi se postigla nemogućnost da se poruka dekriptira samo pomoću javnog ključa. Jednosmjerna

funkcija je svaka ona funkcija koja nema inverz, odnosno nemoguće ga je računski izračunati u razumnom vremenu (Škola koda, bez dat.). Postoji mogućnost kako će razvojem kvantnih računala jednog dana biti moguće probiti ovu enkripciju u nekom relativnom kratkom vremenu. Doduše tako nešto bi utjecalo na kompletan sustav enkripcije podataka i validacije koji se svakodnevno koristi, od podizanja gotovine na bankomatu do osiguravanja internetskih stranica.

Kako bi se kreirao digitalni novčanik, odnosno generirao privatni i javni ključ, koristi se kriptografski algoritam koncipiran na asimetričnom kriptiranju naziva Elliptic Curve Digital Signature Algorithm (Sharma Kumar, 2018).

Javni ključ ili adresu moguće je poslati bilo kojem pošiljatelju ili javno objaviti. Ta adresa je potrebna pošiljatelju da pošalje sredstva na naš digitalni novčanik. Pošiljatelj može biti netko tko nešto kupuje kriptovalutom, mjenjačnica preko koje se kupuje kriptovaluta ili sl.

4.2. Blockchain

U situaciji u kojoj bi svaki klijent banke odlučio podići svoj saldo sa bankovnog računa, banke ne bi imale dovoljno novca kako bi svakom klijentu isplatiti njegov novac. Većina tog novca nije fizički novac u obliku novčanica već samo digitalni zapis o novcu. Danas je velik udio novca samo zapis o tome tko kome duguje koliko novca te su banke i slične institucije centralni entiteti koji vode brigu o ovim zapisima. Centralni entitet koji vodi zapise o transakcijama može promijeniti trenutno stanje salda bankovnih računa, promijeniti popis dužnika i njihove dugove, mijenjati povijest transakcija, birati tko može obaviti transakciju, a tko ne, odnosno ima moć neograničene kontrole nad bankovnim računima.

Blockchain je tehnologija koja rješava problematiku centralizacije i omogućuje vođenje transakcija bez centralnog entiteta, primjerice banke. Blockchain dolazi od riječi blok (eng. *Block*) i lanac (eng. *Chain*), koji predstavljaju lanac međusobno povezanih podataka gdje se jedan podatak nadovezuje na drugi. Svaki blok zapisa sastoji se od četiri podatka: reference o prethodnom bloku zapisa, sažetka o transakcijama koje se nalaze u tom bloku, vremenske oznake stvaranja tog bloka zapisa i dokaza o stvaranju dotičnog bloka zaštićenih zapisa (Pavić, 2020).

Blockchain je moguće jednostavnije objasniti kao javno dostupnu bazu podataka u kojoj su zapisane sve provedene transakcije te se kriptografijom osigurava da se iste ne mogu brisati ili mijenjati, već trajno ostaju elektronički zapisane i pohranjene. Ovakva baza podataka je ~~zapravo~~ distribuirani sustav, odnosno sustav koji se sastoji od više entiteta koji obrađuju transakcije. Entiteti ovog distribuiranog sustava su računala koja su zajedno umrežena te zajednički potvrđuju transakcije. Funkcija sažimanja se koristi kao metoda održavanja

dosljednosti podataka te se pomoću nje provjerava integritet i gotovo je nemoguće nešto promijeniti. Podaci u ovakvom distribuiranom sustavu postaju nepromjenjivi, dosljedni, transparentni i sigurni.

Kod klasičnih bankovnih transakcija u kojima primjerice osoba A prebacuje osobi B novac sa svojeg bankovnog računa na drugi bankovnog račun, banka je entitet koji će provjeriti ima li osoba A dovoljno novca na računu kako bi se transakcija uspješno provela. Kako su kriptovalute decentralizirane one ne koriste centralizirani entitet, koji bi u gore navedenom primjeru bila banka, već koriste Blockchain koji je skup decentraliziranih računala koja potvrđuju transakcije.

Postoji više vrsta Blockchaina pa tako osim javnog Blockchaina na kojem svi imaju uvid u transakcije, postoji i privatni Blockchain koji se može koristiti samo unutar, primjerice određene organizacije te on može imati određena ograničenja za sudionike. Također postoji još i konzorcijski Blockchain koji je kontroliran od strane više različitih organizacija od kojih svaka ima dozvoljen pristup te svaka može kreirati čvor u takvoj mreži (Živković, 2018).

Osim za transakcije Blockchain se može koristiti za pohranu podataka ili za druge svrhe gdje je potrebna decentralizacija. Primjerice Blockchain omogućuje sigurno provođenje elektroničkog glasanja za izbore ili referendum pri čemu su svi glasovi javno vidljivi te nema komisije koja broji pojedinačne glasove. Ranije spomenuti pametni ugovori ne bi bili mogući bez Blockchaina, a primjene su moguće i za upis vlasništva imovine, kao dokaz autentičnosti u upravljanju digitalnim identitetima i sl. Međutim i dalje su ovo vrlo osjetljiva područja za koje ćemo još morati čekati da se njihova sigurnost osloni isključivo na tehnologiju (Pavić, 2020).

4.3. Rudarenje

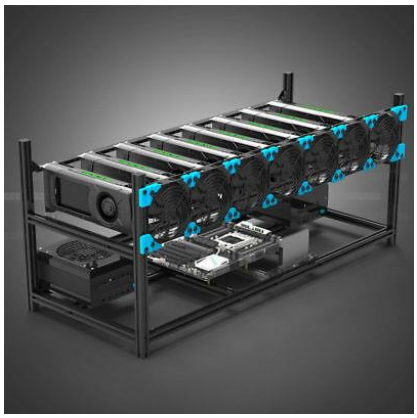
Ranije je spomenuto kako je Blockchain distribuirani sustav umreženih računala koja potvrđuju transakcije. Taj proces potvrđivanja transakcija naziva se rudarenje (eng. *Mining*), dok se čvorovi mreže, odnosno računala koja potvrđuju transakcije nazivaju rudari (eng. *Miners*). Rudarenje je rješavanje kriptografsko - matematičkih zagonetki snagom računala gdje se za riješenu zagonetku kao nagrada dodjeljuje određeni iznos kriptovalute koja se rudari.
Rješavanjem zagonetki se potvrđuju transakcije, a nagrada koje računalo koje potvrdi transakciju dobiva dolazi od onog računala koje je pokrenulo transakciju. Primjerice, kada osoba A šalje Bitcoine osobi B, osoba A za to plati određenu naknadu u Bitcoinima. Zatim rudari koji potvrde tu transakciju bivaju nagrađeni tom naknadom. Rudari tako rudarenjem dobivaju kriptovalute, međutim kriptovalute je moguće kupiti i od rudara ili neke osobe koja ih ima i želi prodati, ako se sami ne želimo baviti rudarenjem. Algoritam koji se koristi za rudarenje naziva se dokaz o radu (eng. *Proof of work)* i zaslužan je i za sigurnost Blockchaina.

4.3.1. „*Proof of work*“ algoritam

Sve je počelo 1993. godine kada su dva inženjera računalstva Cynthia Dwork i Moni Naor osmislili novu metodu za odvraćanje računalno poslane neželjene pošte (eng. *Spam*). Izdali su znanstveni rad naziva „Pricing via Processing or Combatting Junk Mail“ u kojem su objasnili kako je suviše lako i jeftino istu elektroničku neželjenu poruku poslati na više primatelja te zagovarali svoje rješenje ovoga problema. Njihovo rješenje je da ukoliko određeni nepoznati pošiljatelj po prvi put vama kao primatelju šalje poruku, onda se od njega zahtjeva da uloži neki rad, odnosno 10 sekundi procesorskog vremena računala prije slanja poruke. Na taj način slanje neželjene pošte postaje skuplje te se drastično povećava vrijeme potrebno za slanje neželjene pošte (Dwork i Naor, 1993). Kasnije je ova metoda nazvana „Proof of work“, međutim nije bila korištena sve do 2009. kada je Satoshi Nakamoto otkrio da se ovaj algoritam može koristiti kako bi se postigao konsenzus između računala u mreži te verificirale transakcije (Huskanović, bez. dat.).

Algoritam radi tako da sva računala u mreži, odnosno rudari, se natječu jedni protiv drugih u rješavanju funkcije sažimanja za čije rješavanje je potrebno puno računalne snage zbog kompleksnosti. Riječ je o SHA-256 kriptografskoj funkciji koja radi sa 512-bitnim blokovima poruke i 256-bitnim međurezultatima hash vrijednosti te je cilj računala da pogodi hash (Stipaničev, 2003.). Radi se o funkciji čije je rješavanje dosta zahtjevno i kompleksno, ali je zato potvrđivanje njenog rješenja vrlo jednostavan proces. Kada rudar jednom pogodi rješenje stvori se novi blok na Blockchain mreži gdje zatim drugi rudari potvrđuju točnost rješenja, a on tada prima nagradu za pogađanje u obliku kriptovalute. Visina nagrade je promjenjiva ~~je~~, a trenutno za jedan izrudaren blok Bitcoin Blockchaina iznosi 12,5 Bitcoina (Škvorc, 24.4.2018).

Ovakav koncept u kojem distribuirana računala rudare kriptovalute omogućava decentralizaciju i sigurnost Blockchaina, ali to ima i svoju cijenu. Budući da je za rješavanje funkcije sažimanja potrebna jaka procesorska snaga, prosječno računalo će rjeđe doći do rješenja pa se iz tog razloga za rudarenje obično koriste posebna računala sa naprednim grafičkim karticama, koja su vrlo skupa. Osim cijene računala, najskuplji faktor je svakako električna energija jer posebna računala namijenjena rudarenju troše znatne količine električne energije. S obzirom da sam postupak rudarenja nije jeftin, rudarenje je jedan od elemenata koji kriptovalutama daje određenu vrijednost.



Slika 3: Posebno računalo specijalizirano za rudarenje (Izvor: portal Nabava.net, bez. dat.)

4.3.2.„Proof of stake“ algoritam

Rudarenje putem predhodno navedenog „*Proof of work*“ algoritma, potvrđivanje transakcija je relativno sporo. Škvorc za rudarenje navodi „*radi se o jednom bloku svakih 10 minuta, i onoliko transakcija koliko stane u taj blok će se obraditi. Sve ostale čekaju, što dovodi do dugih perioda čekanja za potvrdu transakcije*“ (Škvorc, 2018). Osim ove mane, isti algoritam nije dobar za okoliš jer troši puno električne energije za potvrđivanje transakcija. Škvorc navodi „*Ovisnost kriptovalute o velikim količinama električne energije je neodrživa, i može opstati samo u ultra-stabilnom svijetu“* (Škvorc, 2018).

S obzirom na navedeno, danas sve više kriptovaluta počinje prihvaćati ~~i~~ novi način rudarenja, odnosno verificiranja transakcija. Riječ je o „*Proof of Stake*“ konceptu koji zapravo uopće nije klasično rudarenje i ne zahtjeva rješavanje kriptografsko-matematičkih zagonetki. Tako automatski nestaje zahtjev za velikom potrošnjom električne energije te korištenjem skupog hardvera. Ono što su kod „*Proof of work*“ algoritma bili rudari ovdje su validatori. Validatori potvrđuju (eng. *Validate*) transakcije te kao i kod predhodnog algoritma dobivaju nagradu za potvrđivanje transakcija, koja dolazi od onoga koji pokreće transakciju. Za svaku transakciju validatori su nasumično odabrani, a kako bi se validatore smatralo vjerodostojnima oni prethodno moraju zaključati određen dio sredstava, odnosno kriptovalute kao ulog (eng. *stake).* Ukoliko validator potvrdi neistinitu transakciju njegov ulog će biti oduzet. Uslijed rizika gubitka uloženog, validatorima se nikako ne isplati ponašati zlćudno pa se na taj način postiže vjerodostojnost. Budući da nema potrebe za rješavanjem kriptografsko-matematičkih zagonetki, potvrđivanje i procesuiranje transakcija je brže (Škvorc, 2018).

Druga najpopularnija kriptovaluta po tržišnom udjelu, „Ether“, u postupku je uvođenja „*Proof of Stake“* koncepta koji se trenutno razvija, a neke popularne kriptovalute danas su u potpunosti koncipirane na ovom algoritmu. Osim ova dva navedena algoritma, postoje i drugi

algoritmi, međutim njihova uporaba značajno je rjeđa, primjerice „*Delegated Proof of Stake*“, gdje se validatori biraju glasanjem.

5. Trgovanje kriptovalutama

Trgovanje kriptovalutama ima mnoge sličnosti trgovanju dionicama. Primjerice, kupnja i prodaja kriptovaluta nalikuje na kupnju i prodaju dionica, a nerjetko se događa da se tržište kriptovaluta kreće u istom smjeru kretanja dionca u vremenima krize. Za razliku od dionica banke ne favoriziraju klijente koji trguju kriptovalutama jer su kriptovalute konkurencija bankarskom sektoru budući da naknade za slanje ne idu bankama već rudarima te je tržište manje regulirano. Osim toga, cijena dionica značajno ovisi o poslovanju tvrtke koja je izdala tu dionicu, dok kod kriptovaluta toga nema. Kriptovalute se razlikuju i po iznimno velikoj volatibilnosti cijene te upravo radi tog faktora trgovanjem kriptovaluta moguće je ostvarivanje velikih dobitaka ili velikih gubitaka.

5.1. Mjesta za trgovanje kriptovalutama

Tek napravljen novčanik za kriptovalute će uvijek biti prazan, a ako ćemo htjeti posjedovati određenu kriptovalutu to je moguće li rudarenjem ili kupnjom. Ako se ne želimo baviti rudarenjem i odlučimo se za kupnju ona je moguća na više načina. Najidealnija i najjednostavnija metoda je pronaći osobu koja je spremna prodati kriptovalutu, naći se s njom te obaviti kupnju tako da joj damo novac, a ona nama pošalje kriptovalutu na naš digitalni novčanik. Ono što uvelike pojednostavljuje traženje onoga tko je kriptovalutu spreman prodati su mjesta za trgovanje kriptovalutama, najčešće u obliku web platforme, odnosno na internetu (eng. *Online*). Takva mjesta dijele se na:

- Mjenjačnice kriptovaluta
- Burze kriptovaluta

5.1.1. Mjenjačnice kriptovaluta

Mjenjačnice kriptovaluta su privatne tvrtke koje omogućuju klijentima kupnju ili prodaju kriptovaluta za novac. Primjer jedne takve mjenjačnice u Hrvatskoj je „*Bitcoin store*“, koja ima web stranicu na kojoj je moguće uplatom na njihov račun ili kartičnim plaćanjem, kupiti 68 različitih kriptovaluta. Nude i mogućnost prodaje, koja prvo zahtijeva slanje kriptovalute na njihov digitalni novčanik nakon čega mjenjačnica na bankovni račun klijenta uplaćuje sredstva od prodaje. Ovakve tvrtke imaju kupovni i prodajni tečaj, odnosno od svake transakcije uzimaju proviziju od 1% do 5% (Bitcoin store, 20.6.2020.).

Osim mjenjačnica na internetu postoje i fizičke mjenjačnice poput poslovnica ili bankomata za kupnju i prodaju kriptovaluta. Primjerice, u Zagrebu postoji i „*Bitcoin store*“ poslovnica gdje je moguće kupiti i prodati kriptovalute za gotovinu. Budući da su transakcije gotovinom skuplje

obično su i provizije na mjestima gdje se fizički kupuju kriptovalute veće. Primjerice, prosječni Bitcoin bankomat naplaćuje prosječnu proviziju od čak 8,93%, a budući da u Hrvatskoj postoji samo nekoliko Bitcoin bankomata moguće da je provizija ponegdje i veća (Orešković, 18.2.2020). Stoga se većina ljudi ipak odlučuje za kupnju ili prodaju kriptovaluta preko interneta gdje je moguće kupiti kriptovalute virmanskim i kartičnim plaćanjem uz manje provizije ili se odlučuje na kupnju preko burzi kriptovaluta.

Slika 4: Bitcoin bankomat u Ljubljani (Izvor: Wikiwand, bez. dat.)

5.1.2. Burze kriptovaluta

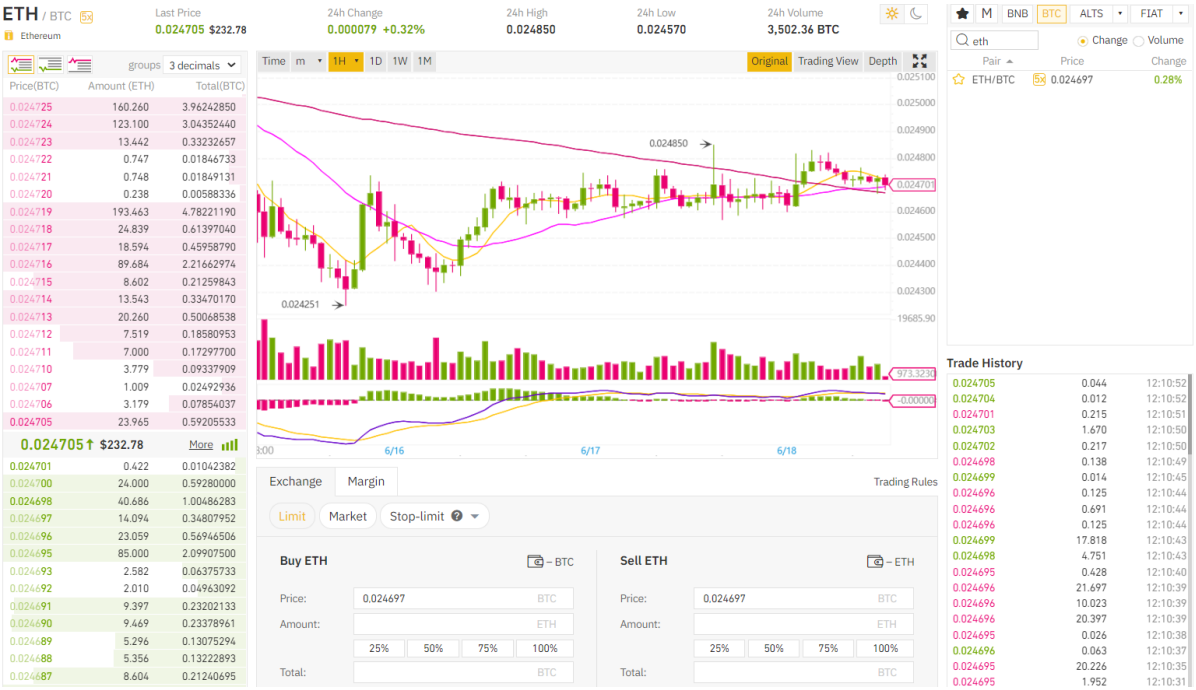
Burze kriptovaluta se razlikuju od mjenjačnica kriptovaluta po tome što se kriptovalute kupuju i prodaju od drugih korisnika, a ne od same burze. Burza je samo posrednik koji omogućuje rad web platforme za trgovanje, a od same kupnje i prodaje uzima malu proviziju koja je znatno manja od mjenjačnica kriptovaluta. Primjerice, na jednoj od najpopularnijih burzi, „*Binance*“, provizija za kupnju ili prodaju iznosi 0.1000%, što je svakako manje od 1% do 5% koliko obično uzimaju mjenjačnice kriptovaluta (Binance, bez. dat.). Prodaja ili kupnja se izvršava postavljanjem naloga za prodaju ili kupnju gdje sami birate po kojoj cijeni želite prodati ili kupiti kriptovalutu te onda čekate da je netko izvrši odnosno od vas kupi kriptovalutu ili kriptovalutu vama proda.

Osim mogućnosti kupnje ili prodaje kriptovaluta, burze daju i mogućnosti špekulacije cijena kriptovaluta te klađenja na njihov rast ili pad. Primjerice, ako osoba smatra kako će određena kriptovaluta pasti 5% u određenom razdoblju moguće je kladiti se na to te

zapravo zaraditi i kada neka kriptovaluta pada. Takvo klađenje omogućuju i različite burze dionica, nafte, zlata i drugih financijskih instrumenata, a zbog velike volatibilnosti kriptovaluta ni klađenje na kriptovalute nije rijetkost. Mjenjačnice uz mogućnost klađenja vrlo često nude i mogućnost trgovanja s polugom (eng. *Leverage trading*), gdje je moguće s manjim iznosom novca zauzeti puno veću poziciju. S druge strane, trgovanje sa polugom je izrazito rizično i u pravilu, što je poluga veća, oklada je rizičnija. Iz tog razloga često ljudi koji nemaju iskustva s trgovanjem na burzama općenito, precijene rizik i izgube svoj novac. Većina ljudi se ipak ne bavi ozbiljnijim trgovanjem već isključivo želi kupiti kriptovalutu kao dugoročnu investiciju ili sredstvo plaćanja.

5.2. Formiranje cijena kriptovaluta

Cijenu definiramo kao omjer ponude i potražnje pa tako i cijena svake kriptovalute ovisi o tome koliko je netko neku kriptovalutu spreman platiti, odnosno za koju cijenu ju je netko spreman prodati. Mjesta na kojima je moguće pronaći ponudu i potražnju za kriptovalutama su burze za kriptovalute. Burze kriptovaluta imaju više korisnika koji postavljaju naloge koji su kao narudžbe za kupnju ili prodaju kriptovaluta (eng. *Orders*).



Slika 5: Odnos ponude i potražnje kriptovaluta Ether i Bitcoin (Izvor: Binance, 2020)

Graf pokazuje mijenjanje odnosa cijene Ethera i Bitcoina kroz određeno vrijeme pa se prema njemu može zaključiti kako u određenom periodu primjerice Ether vrijedi više od Bitcoina.

Na slici na skroz lijevoj strani možemo vidljivi su crveni i zeleni brojevi. Ti brojevi predstavljaju zid narudžbi (eng. *Order wall*) ili knjigu narudžbi (eng. *Order book*) na temelju koje se i kreira graf. Crveni brojevi predstavljaju korisnike koji određenu kriptovalutu prodaju, dok oni zeleni određenu kriptovalutu kupuju. Na slici je riječ o mijenjanju kriptovalute Ether za kriptovalutu Bitcoin, kratice za Ether su ETH, dok za Bitcoin BTC. Iz knjige narudžbi sa slike vidljivo je da netko upravo prodaje 23.965 Ethera po tečaju 0.024705 Bitcoina po Etheru, dok s druge strane netko kupuje 0.422 Ethera za cijenu 0.024701 Bitcoina po Etheru. Navedene informacije mogu se interpretirati kao kupovni i prodajni tečaj u datom trenutku. Kada bi se netko odlučio kupiti, primjerice 50 Ethera, cijena bi narasla jer bi narudžba bila popunjena i prelazilo bi se na sljedeće narudžbe. Isto vrijedi i obrnuto, cijena bi padala kada bi netko odlučio prodati veću količinu Ethera. Osim odnosa kriptovaluta Ether i Bitcoin, moguće je pratiti i odnose drugih kriptovaluta kao i odnosa Dolar-Bitcoin ili Euro-Bticoin.

Srednji tečaj, odnosno trenutna cijena je cijena po kojoj se izvršila zadnja narudžba i po toj cijeni prati se vrijednost kriptovalute. Jedna od najpreciznijih metoda praćenja vrijednosti kriptovaluta je web aplikacija „*CoinMarketCap“* pomoću koje je predhodno određen tržišni udio Bitcoina. Ta aplikacija funkcionira tako da za svaku kriptovalutu uzima srednji tečaj sa svih dostupnih burzi kriptovaluta na kojima se trguje tom kriptovalutom te onda izračunava srednji tečaj. Budući da stalno netko kupuje i prodaje kriptovalute tečaj se stalno mijenja pa se ova web aplikacija osvježava više puta u minuti i tečaj se često mijenja više puta u minuti. Vrijedi napomenuti da se ista pravila primjenjuju i za određivanje cijene drugih financijskih instrumenata.

Budući da je tržište kriptovaluta generalno takvo da većina alternativnih kriptovaluta prati cijenu Bitcoina, koja je najpopularnija i najprihvaćenija kriptovaluta fokus prilikom proučavanja trgovanja i kretanja cijene kriptovaluta u ovom radu biti će na Bitcoinu. Kad kažemo da alternativne kriptovalute prate Bitcoin misli se na to da kad cijena Bitcoina raste uglavnom cijena većine alternativnih kriptovaluta raste i obrnuto. Razlog tomu je vrlo slična ili gotovo ista tehnička izvedba kriptovaluta kao i mehanika tržišta.

5.3. Kretanje cijene Bitcoina

U početnom razdoblju nakon nastanka Bitcoina, Bitcoin je bio veoma nepoznat i imao je poprilično malu vrijednost koju je bilo vrlo teško procijeniti jer se nije moglo lako ga zamijeniti za novac. Također, nije bilo platformi na kojima je bilo moguće trgovanje kriptovalutama kao danas. U to vrijeme je s njime gotovo nemoguće bilo nešto kupiti jer rijetko tko bi bio spreman

nešto fizički prodati za Bitcoin, a neko vrijeme su čak i postojale stranice na kojima je bilo moguće besplatno preuzimanje Bitcoina jednostavnim pritiskom na gumb. Tada su ga isključivo entuzijasti koristili za transakcije jer im je to bilo zanimljivo i novo, a tek rijetki su mislili da ima potencijal daljnjeg napretka ili rasta cijene. Rudarenjem se koristeći jako malo procesorske snage moglo stvoriti velike količine Bitcoina te su ljudi uglavnom mislili da ga je lako izrudariti i da će tako biti uvijek pa će shodno tome i cijena biti uvijek ista.

Prvi tečaj Bitcoina objavljen je od strane forumaša pod korisničkim imenom „*New Liberty Standard*“, a bazirao se na cijeni rudarenja Bitcoina. Tečaj se računao tako da je jedan američki Dolar bio podijeljen sa prosječnom količinom struje koja je potrebna da napaja računalo tokom cijele godine te pomnožen sa prosječnom cijenom struje u Americi. Taj iznos se zatim podijelio sa 12 mjeseci te sa brojem generiranih Bitcoina u 30 dana. Kako bi se izvršila kupnja ili prodaja Bitcoina bilo je potrebno kontaktirati dotičnog forumaša putem email-a, a novčana transakcija se odvijala putem PayPal računa (Sedgwick, 2019).

$1.00 USD	=	1,578.77 BTC	12/28/2009
$1.00 USD	=	1,578.77 BTC	12/27/2009
$1.00 USD	=	1,578.77 BTC	12/26/2009
$1.00 USD	=	1,578.77 BTC	12/25/2009
$1.00 USD	=	1,578.77 BTC	12/24/2009
$1.00 USD	=	1,578.77 BTC	12/23/2009
$1.00 USD	=	1,578.77 BTC	12/22/2009
$1.00 USD	=	1,594.63 BTC	12/21/2009

Slika 6: Prva tečajna lista Bitcoina (Izvor: portal Web Archive, bez. dat.)

Nedugo zatim, tijekom 2010. godine, obavljena je prva fizička Bitcoin transakcija za dvije pizze te je iste godine otvorena i prva web platforma za kupnju i prodaju Bitcoina, odnosno mjenjačnica naziva „*Mt. Gox*“. Prvobitno, to je bila platforma za razmjenu „*Magic: The Gathering Online*“ igraćih karata koju je izradio programer Jed McCaleb. Budući da mu taj

projekt nije uspio i shvativši da bi trebala postojati mjenjačnica za Bitcoine, prenamijenio je svoj neuspjeli projekt u mjenjačnicu Bitcoina. Njemu je bilo teško pratiti potrebe poslovanje te je početkom 2011. godine, McCaleb je prodao mjenjačnicu Marku Karpelèsu koji će ju onda postepeno razviti u mjenjačnicu koja je više od tri godine dominirala tržištem za kupnju i prodaju Bitcoina (99Bitcoins, bez. dat.).

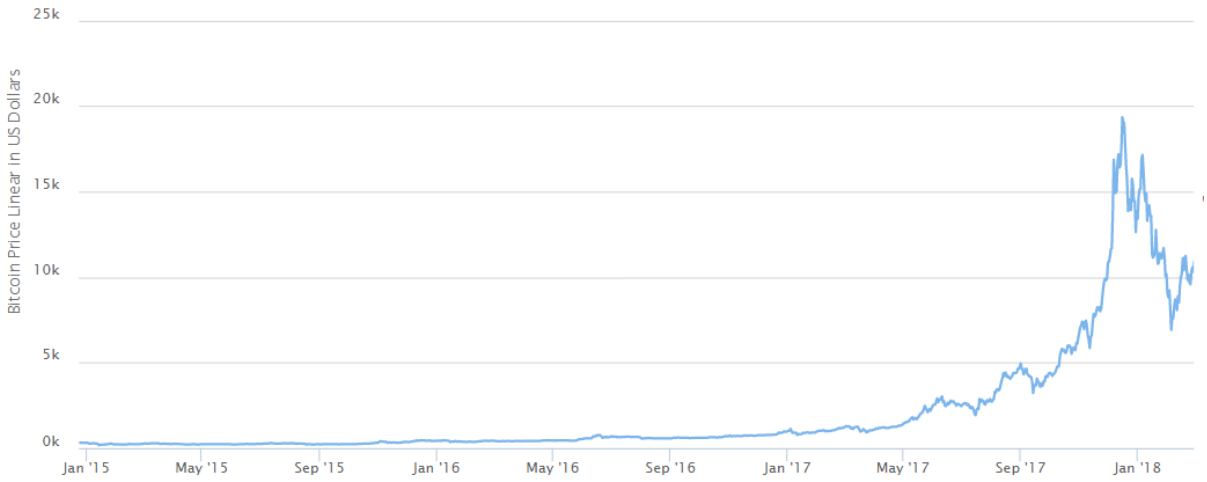
Mnoge neprofitne organizacije su 2011. godine počele prihvaćati Bitcoin donacije, jedna od njih je bila primjerice „WikiLeaks“, stranica koja objavljuje povjerljive, diskreditirajuće informacije i vijesti garantirajući izvorima, najčešće zviždačima, anonimnost. Budući da je stranice izgrađena na ideji anonimnosti, bilo je važno da se i donacije ne mogu pratiti (Greenberg, 2011). Valja napomenuti, kako je u počecima Bitcoin često bivao prihvaćen kao sredstvo plaćanja upravo radi njegove karakteristike pseudoanonimnosti, radi koje je teško indentificirati sudionike u Bitcoin transakcijama. Javno su vidljive sve transakcije na Blockchainu pa nije potpuno anoniman, ali je vrlo teško povezati kome pripada koji digitalni novčanik.

Bitcoin se počeo sve više prihvaćati kao sredstvo plaćanja te je 2012. godine „BitPay“ objavio kako preko 1000 trgovaca prihvaća Bitcoin (Browdie, 2012.). Budući da se sve više ljudi počelo susretati s Bitcoinom, mnogi počinju prepoznavati njegov potencijal kao investiciju. S obzirom na to da je algoritam Bitcoina napravljen tako da se svake četiri godine nagrada rudarima prepolavlja (eng. *Halving*), odnosno smanjuje za pola, Bitcoin svake četiri godine postaje dvostruko skuplji za rudarenje. S istom računalnom snagom odjednom se rudari dvostruko manje Bitcoina pa mnogi smatraju kako sukladno tome i cijena treba rasti.

Tako je 28.11.2012. prvi put u povijesti bio „*Halving day*“ kada je Bitcoin doista postao skuplji za rudarenje, a cijena mu je postepeno počela rasti. Na dan prepolavljanja cijena Bitcoina je bila 12.25 američkih Dolara, a oko 10 mjeseci kasnije, dana 4.9.2013. godine, je dostigla čak 230 američkih Dolara prije nego li je krenuo nagli pad te zatim stabilizacija cijene (vidljivo na slici ispod). Nagli pad je bio uzrokovan rušenjem servera „*Mt Gox*“ burze koja je tad dominirala tržištem, a do rušenja servera je došlo uslijed povećanog obujma trgovanja Bitcoinom (99Bitcoins, bez. dat.). Dakle u manje od 10 mjeseci je cijena narasla za preko 1750% te je to bio najveći rast Bitcoina do tad.

Slika 7: Graf kretanja cijene Bitcoina u periodu između ožujka 2012. i svibnja 2013. godine (Izvor: *Buy Bitcoin Worldwide*, 21.6.2020.)

Nakon spomenute stabilizacije cijena je polako rasla, ali ne naglo. Sve dok nije došao novi „Halving day“,ovog puta 9.7.2016., nakon kojeg je cijena porasla za preko 2950% sve dok nije opet došlo do naglog pada, a zatim i stabilizacije. Ovaj put rast je bio znatno viši, ali je zato i trajao 17 mjeseci. Maksimalna dosegnuta cijena tada bila je oko 20 000 američkih Dolara i to je i dan danas maksimalna cijena koju je Bitcoin dosegnuo, dok je trenutna cijena Bitcoina 9450 američkih Dolara, što je dvostruko manje od najviše cijene koju je Bitcoin postigao (CoinMarketCap, 21.6.2020).



Slika 8: Graf kretanja cijene Bitcoina u periodu između siječnja 2015. i siječnja 2018. godine (Izvor: *Buy Bitcoin Worldwide*, 21.6.2020.)

Iz navedenih porasta i padova cijene Bitcoina možemo zaključiti da je Bitcoin vrlo volitabilan. Cijena se kreće ovisno o različitim špekulacijama na tržištu. Dok nešto ima negativan utjecaj na rast kriptovaluta investitori se plaše i prodaju svoje kriptovalute, a kada vladaju pozitivne vijesti vlada intenzivna kupovina i optimizam (eng. *hype)*.

Osim „*Halving day*“ događaja koji se ponavlja svake četiri godine, na porast cijene Bitcoina utječe i to da je Bitcoin opskrba (eng. *Supply)* ograničena, odnosno može nastati i u cirkulaciji biti samo 21 milijun Bitcoina. Upravo iz ovog razloga se često može čuti kako se za Bitcoin kaže da je digitalno zlato jer je ograničen i za njegovo rudarenje je potrebno sve više vremena i novca (Hayes, 2020). Trenutno je izrudareno i u cirkulaciji 18,409,837 Bitcoina, što je više od 80% Bitcoina (CoinMarketCap, 21.6.2020).

Valja napomenuti da iako Bitcoin dugoročno raste zadnjih 10 godina, imao je i znatne padove kroz taj period što je značilo velike gubitke za pojedince. Mnoge pojave u ekonomiji kriptovaluta imaju značajan negativan utjecaj na cijenu Bitcoina. Primjerice, jedan od negativnih utjecaja na cijenu dogodio se kada je u prosincu 2013. godine kineska vlada zabranila financijskim institucijama u Kini da koriste Bitcoin. Cijena Bitcoina tada je pala sa 1022 američka Dolara na 654 američka Dolara u samo jednom danu (99Bitcoins, bez.dat.).

6. Utjecaj kriptovaluta na ekonomiju

Budući da cijena kriptovaluta jako varira iz godine u godinu, tako se i tržišni udio globalnog novca u kriptovalutama stalno mijenja pa je tako početkom 2018. godine tržište kriptovaluta bilo veće od tržišta popularnih kompanija Amazona i Facebooka, dok su krajem iste godine navedene dionice imale veće tržište od kriptovaluta (CoinMarketCap, 2020). Također je, primjerice 2016. godine, tržište kriptovaluta vrijedilo 11.3 milijardi američkih Dolara, a samo godinu kasnije naraslo za čak 15 puta što je i prikazano na slici ispod (Desjardins, 2017). Iz naverdenih podataka mogu se izvući dva zaključka - tržište kriptovaluta je jako volatibilno te gotovo svake godine postaje sve veće i veće.

Slika 9: Prikaz povećanja tržišta kriptovaluta kroz godine u milijardama američkih Dolara (Izvor: *Desjardins*, 2017)

Kako se tržište povećava tako se povećava i interes vlada, banaka i drugih organizacija za kriptovalute. Primjerice, kineska vlada je pokrenula pilot program u kojem testira digitalnu verziju svoje službene valute. Ta digitalna valuta jednaka je novčanicama i kovanicama kineskog juana, a jedina razlika je što se nalazi na mobitelu u obliku digitalnog novčanika. Takva digitalna valuta bi bila centralizirana i upravljana od strane Kineske vlade, a njome bi Kina mogla kontrolirati novčane tokove koje nije moguće kontrolirati kada se izvode fizičkim novcem, odnosno gotovinom. Budući da joj je cilj uspostaviti veću kontrolu kineska vlada jedna je od rijetkih koja je zabranila Bitcoin i druge kriptovalute pretežito uslijed činjenice da ih državne vlasti ne mogu kontrolirati (Bloomberg, 1.6.2020.)

Za razliku od Kine većina država ipak ne zabranjuje trgovanje kriptovalutama, već naplaćuje porez na dobit zarađenu trgujući kriptovalutama. Primjerice, u Hrvatskoj se na dobit zarađenu od kriptovaluta plaća 12% poreza te prirez ovisno o prebivalištu. Ukoliko građanin posjeduje kriptovalutu dulje od dvije godine na digitalnom novčaniku, unatoč tome što njoj poraste vrijednost, porez nije dužan platiti (RRIF, 2018).

Američka kompanija Facebook planira uvesti svoju kriptovalutu imena Libra koja bi bila digitalna valuta stabilne cijene vezane uz američki Dolar. Primarni cilj je olakšati digitalna

plaćanja svima u svijetu, primarno korisnicima nekih od njihovih aplikacija poput Messengera ili WhatsAppa, koji ne posluju s bankama i nemaju kreditnu ili debitnu karticu. Kriptovalutu Libra bit će moguće kupiti za novac bilo gdje u svijetu, a plaćanja njome će se obavljati brzo i sigurno putem mobilnih telefona. Libra će biti zasnovana na blockchainu koji će jamčiti sigurnost i brzinu transakcija, dok će ulagački kapital u rezervi jamčiti njezinu stabilnost. Neki od investitora u ovome projektu su Uber, Visa, Mastercard, PayPal, Andreessen Horowitz, Coinbase, Booking, eBay i drugi (Vrbanus, 18.6.2019).

Veliki interes za kriptovalute prisutan je među stanovništvom u državama Južne Amerike gdje vlada visoka razina inflacije. Primjerice, u Venezueli koja je ozbiljno pogođena krizom, prosječna stopa inflacije mjeri se u tisućama posto na godišnjoj razini, dok za usporedbu, u Europskoj Uniji je prosječna stopa inflacije 2.39% (Trading Economics, 2020). Budući da se za kriptovalute poput Bitcoina kaže da defliraju jer svakih četiri godine Bitcoin postaje skuplji za rudarenje, kriptovalute postaju sve češći oblik očuvanja vrijednosti i sredstva plaćanja u takvim zemljama hiperinflacije (Carigrad, 2019). I u ostalim zemljama južne hemisfere se kriptovalute sve češće koriste kao alternativna metoda financijskog sustava, primjerice u Brazilu gdje 30% stanovništva i dalje nema bankovni račun zbog nepovjerenja u bankovni sustav i nepraktičnosti, poput dugih redova čekanja, limita podizanja novca i visokih naknada (Ríos, 2020). U praksi kriptovalute ipak ne osiguravaju nužno dobru alternativu čuvanja vrijednosti jer je volatibilnost cijena kriptovaluta iznimno velika.

6.1. Kriptovalute kao sredstvo plaćanja

Ideja Bitcoina, a i mnogih drugih kriptovaluta, je da postane decentralizirani digitalni novac koji omogućuje direktna plaćanja preko interneta od pošiljatelja do primatelja bez uplitanja treće strane, odnosno financijskih institucija (Nakamoto, 2009). Ova ideja realizirana je Blockchain tehnologijom i djelomično je uspjela. Međutim, ono što koči ovaj način plaćanja su tehnička ograničenja Blockchaina. Rašireno je vjerovanje kako će kriptovalute jednog dana postati široko prihvatljivo sredstvo plaćanja te da ćemo kriptovalutama plaćati u svakodevnom životu. Iz istog razloga mnogi ih kupuju i čuvaju jer smatraju da će im iz istog razloga jednog dana porasti cijena.

S jedne strane, istina je da kriptovalute postaju sve češće birane kao način plaćanja, ali to najčešće ne biva radi praktičnost nego jer ljudi vole isprobavati nove stvari pa tako i nove tehnologije. Teorija da će se većina transakcija obrađivati preko Blockchaina naprosto ne drži vodu, a razlog tome je što Blockchain ima visoku skalibilnost, odnosno ovisnost potrebnih resursa u odnosu na količinu podataka (eng. *Scalability).* Naime, prosječan broj transakcija koji stane u jedan Bitcoin blok je trenutno 2759 transakcija, a vrijeme potrebno za rudarenje jednog bloka 10 minuta. Drugim riječima, kada to jednostavno preračunamo vidimo da Bitcoin

Blockchain garantira provođenje samo 4.6 transakcija u jednoj sekundi dok druge transakcije, ako ih ima, čekaju u redu. Usporedbom Bitcoin Blockchaina sa globalnom kompanijom koja procesuira kartična plaćanja, „*Visa",* jasno je da je Visa puno brža jer oni dnevno obrađuju 150 milijuna transakcija, dakle u prosjeku 1700 transakciju u sekundi (Li, 2019).

Moderniji Blockchaini djelomično rješavaju problem skalibilnosti i uvelike povećavaju brzinu obrade transakcija pa zato i mnoge kriptovalute postaju popularne radi puno bržih transakcija od Bitcoina. Primjerice, kriptovaluta EOS koja koristi „Delegated Proof of Stake" algoritam postiže i do 3,996 transakcija u sekundi, međutim i dalje govorimo o manjem broju transakcija po sekundi od kompanije „*Visa"*. U situacijama velikog opterećena brojem transakcija poput američkog „*Black Friday*" dana bitna je sposobnost obrade velikog broja transakcija u sekundi (Le, 2019).

Činjenica je da su transakcije na Blockchainu sporije jer zahtjevaju visoke računalne resurse za potvrđivanje transakcija, a samim time i znatno veću potrošnju energije. Godišnje se potroši čak 60.24 TWh električne energije na rudarenje Bitcoina, što je približno godišnjem utrošku električne energije cijelog Alžira (Digiconomist, 2020). Iz tog razloga vrlo je bitno da se što više kriptovaluta prebaci s „*Proof of work"* koncepta na „*Proof of stake"* koncept, u suprotnom bi češća upotreba kriptovaluta dovela do znatnog negativnog ekološkog utjecaja.

Daljnjim razvojem Blockchain tehnologije mogući je pronalazak rješenja problema skaliranja kao i problema potrošnje velike količine električne energije, međutim, bitno je naglasiti da za sad u ovome trenutku, kriptovalute još uvijek nisu tehnički sposobne zamijeniti većinu kartičnih transakcija. Također valja naglasiti i veliku volitabilnost cijene kriptovaluta koja znatno otežava prihvaćanje kriptovaluta kao sredstvo plaćanja, premda bi se problem volitabilnosti cijene mogao riješiti u onom trenutku kada kriptovalute budu prihvaćene od strane većeg broja korisnika.

6.2. Kriptovalute kao oblik investicije

Prosječni korisnik kriptovaluta rjeđe ih koristi kao sredstvo plaćanja, ali puno češće kao sredstvo za investiranje novca. Osim fizičkih osoba, sve češći investitori u kriptovalute su i institucionalni investitori. Prisutni su i fondovi koji trguju kriptovalutama u koje mogu ulagati pojedinci koji nemaju dovoljno znanja sami trgovati kriptovalutama. Hrvatska agencija za nadzor financijskih usluga (Hanfa) je društvu Griffon Asset Management d.o.o. iz Osijeka izdala odobrenje upravljanja otvorenim alternativnim investicijskim fondom za ulaganje u kripto imovinu, koji je specijaliziran za ulaganje u Bitcoin (Vrbanus, 11.6.2020.).

6.2.1. Usporedba Bitcoina s dionicama

Ono što se može izdvojiti kao krucijalna razlika između kriptovaluta i drugih financijskih instrumenata je puno veća volatibilnost kriptovaluta. 2015. godine cijena burzovnog indeksa „*S&P 500*“, najpopularnijeg indeksa koji trguje dionicama 500 najvrijednijih kompanija, bila je oko 2000 američkih Dolara (MarketWatch, 2020). Ovaj indeks je jedan od indeksa koji se vrlo često koristi za usporedbu s drugim financijskim instrumentima jer njegova cijena prati velik dio tržišta dionica, a čak i ako nekoj od dionica naglo padne cijena, ovaj indeks i dalje tu promjenu gotovo da i ne osjeti te dugoročno i dalje nosi prinose.

U isto vrijeme, 2015. godine, Bitcoinu cijena oscilira između 200 i 300 američkih Dolara, dok 2017. godine indeksu „*S&P 500*“ cijena raste postepeno do 2300 američkih Dolara. Bitcoinu cijena iste godine skače na preko 20 000 američkih Dolara (MarketWatch, 2020). Dakle dok su indeksi i dionice donekle predvidivi te imaju stabilni rast i prinose, Bitcoin s druge strane ima iznimno velike skokove i padove cijene. U samo zadnjih pola godine cijena Bitcoina je oscilirala između 3858 i 10369 američkih Dolara po Bitcoinu (Marquit, 2020).

Razlog takvim velikim oscilacijama Bitcoina je što Bitcoin slabo prati intrinzičnu vrijednost koja se vrlo često smatra „stvarnom“ ili „poštenom“ vrijednošću nekog financijskog instrumenta. Intrinzična vrijednost (eng. *intrinsic value*) je stvarna vrijednost ili realna vrijednost poduzeća, odnosno dijelova njegova kapitala ili imovine, odnosno vrijednost koju poduzeće, kapital ili imovina imaju sami po sebi (WMD, bez.dat.). Intrinzičnu vrijednost neke dionice moguće je odrediti proučavajući financijske izvještaje kompanije. Kompanije svojim poslovanjem stvaraju novu vrijednost te na kraju godine investitori dobivaju dividende na temelju uspješnog poslovanja s dobiti.

Međutim, Bitcoin nije kao dionice jer iza njega ne stoji poslovanje i uspješnost toga poslovanja koje se potkrjepljuje financijskim izvještajima. Jedino što donekle daje Bitcoinu intrinzičnu vrijednost je rudarenje koje zahtjeva resurse poput opreme i električne energije. Unatoč tome omjer težine rudarenja Bitcoina i cijene Bitcoina i dalje često odstupa. U povijesti Bitcoina događali su se nagli porasti i padovi cijene na koje su utjecala zbivanja u industriji kriptovaluta te mediji, dok se cijena rudarenja nije promijenila. Primjerice, vijest da je društvena mreža „*Twitter*“ integrirala Bitcoin emotikon (eng. *emoji*) uzrokovala je rast cijene sa 9333 američka Dolara na 10347 Dolara u roku 10 dana u veljači 2020. godine bez da je cijena rudarenja narasla (99bitcoins, bez. dat.).

Svakako valja naglasiti da i kod dionica zbog vijesti u medijima o toj dionici cijena ponekad padne ili naraste, ali je to zato jer se vijest odnosi na neku informaciju koja direktno ili indirektno utječe na poslovanje kompanije koja je izdala dionicu. Nasuprot tome, vijest o implementaciji novog emotikona na društvenoj mreži „*Twitter*“ tehnički nikako ne može utjecati na rast cijene rudarenja koja bi dovela do veće intrinzične vrijednosti. Ovakve i slične pojave

vrlo često uzrokuju pojavu razdoblja intenzivne kupovine i optimizma o porastu cijene Bitcoina (eng. *hype*). Takav porast cijene privlači mnoge nove investitore, a temelji se najčešće na špekulaciji o daljnjem porastu cijene.

Dokle god Bitcoin ne bude striktnije pratio svoju intrinzičnu vrijednost javljat će se vremena intenzivne kupovine zbog porasta cijene koji uzrokuje tvz. financijski balon kojeg karakterizira nagli rast cijene Bitcoina i drugih kriptovaluta, a potom i nagli pad. Ovakve financijske balone smo moguće je uočiti kod grafova o kretanju cijene Bitcoina na slici 7 i slici 8 iz poglavlja 4.3., gdje je primjerice, na grafu cijena od one najviše postignute cijene pala za gotovo upola. Česta je pojava da investitori koji su ulaganje proveli tijekom razdoblja intenzivne kupovine i optimizma ostvare veliki gubitak zbog čega se kriptovalute smatraju visoko rizičnom investicijom.

Još jedna znatna razlika između dionica i kriptovaluta leži u državnoj regulaciji. U pravilu svatko tko ima tehnička znanja za to može napraviti vlastitu kriptovalutu te je tržište kriptovaluta teže regulirati, dok s druge strane, dionice se strogo provjeravaju od strane vladinih agencija. Isto tako jasno je da je puno rizičnije investirati u nešto neregulirano jer postoji veća šansa prevare. Tako je u 2017. godini bilo puno nereguliranih inicijalnih ponuda kriptovaluta, tvz. ICO-a (eng. *Initial coin offer*), gdje su investitori mogli investirati u razvoj novonastalih kriptovaluta. Međutim, nitko nije garantirao da investitori neće izgubiti novac ako projekt propadne, odnosno inicijalne ponude kriptovaluta nisu bile regulirane od strane države u kojoj se izdaju.

6.2.2. Tokenizacija crowdfunding kampanja

Danas nereguliranih inicijalnih ponuda kriptovaluta gotovo da i nema te su ih zamijenile regulirane inicijalne ponude kriptovaluta, tvz. ETO (eng. *Equity token offering).* Ovakve inicijalne ponude kriptovaluta su odobrene od financijskih agencija te predstavljaju udjele u kompaniji koja ih izdaje, dakle imaju određenu vrijednost koja stoji iza njih. Kao što postoje tvrtke koje prvi put izdaju dionice, odnosno inicijalne javne ponude tvz. IPO (eng. „*Initial Public Offering*“), tako sve popularnije postaju i inicijalne ponude kriptovaluta.

Inicijalne ponude kriptovaluta omogućuju tvrtkama pribavljanje kapitala za pokretanje ili proširivanje svojeg poslovanja. Primjerice, tvrtka koja ima ideju za izradu aplikacije može napraviti kampanju skupljanja kapitala (eng. „*crowdfunding*“) na način da investitorima izda tokene na Blockchainu koji predstavljaju udjele u toj kompaniji. Ti tokeni su kriptovalute koje nemaju vlastiti Blockchain već su napravljenje na Etheriumovom ili nekom drugom Blockchainu radi jednostavnosti i jer nema potrebe za posebnim svojstvima. Cijena tokena se kreće u smjeru kretanja vrijednosti kompanije, a tokeni, koji su poput dionica, se mogu prodati na određenim burzama. Ovakav način skupljanja kapitala omogućuje da i osobe koje nisu investitori i nemaju brokera investiraju novac iz udobnosti vlastitog doma u kompanije u koje

vjeruju. Velika je prednost što se kod ovakvih inicijalnih ponuda može investirati i manji iznos novca, što kod dionica često ne biva tako pa investiranje postaje šire dostupna pojava.

Primjer regulirane inicijalne ponude u Hrvatskoj su „*Greyp"* tokeni koje je izdala tvrtka Greyp Bikes d.o.o. Osnivač i većinski vlasnik ove tvrtke je Mate Rimac koji je odlučio prikupljati kapital izdajući tokene koji predstavljaju udjele u njegovoj kompaniji pa tako svatko tko vjeruje u rast njegove kompanije je lako mogao, ulažući eure ili Etherium, kupiti udio u njegovoj tvrtki. Kapital je prikupljan na njemačkoj platformi Neufund te je prikupljeno 1,44 milijuna eura u eurima i etherima što je čak i premašilo njihova očekivanja (Oršulić, 16.1.2020).

6.2.3. Rizici kriptovaluta

Osim prethodno spomenutih ekonomski rizika kriptovaluta, koji podrazumijevaju zabranu upotrebe kriptovaulta od strane državnih regulatora ili primjerice volatibilnost cijene, postoje i tehnički rizici koje je bitno znati prije nego li se trguje ili investira sa kriptovalutama. Ranije je objašnjeno kako je Blockchain protokol siguran, kao i digitalni novčanici koji su osigurani kriptografijom. S druge strane, web mjesta za trgovanja kriptovaluta se nalaze na internetu te ne ovise o sigurnosti kriptografije, već o sigurnosti interneta. Digitalni novčanici koji se nalaze na web mjestima za trgovanje kriptovaluta se nazivaju „vrućim" novčanicima (eng. *Hot wallets*). Pridjev „vrući" proizlazi iz toga što se njihovi privatni ključevi nalaze na internetu te su zato česta meta hakera. Nove ranjivosti web stranica i internetskih platformi se otkrivaju gotovo svakodnevno, a ponekad otkriće ranjivosti bude iskorišteno za hakerski napad. Najveći hakerski napad na burzu kriptovaluta dogodio se 2018. godine kada je sa japanske burze Coincheck ukradeno čak 534 milijuna američkih Dolara (FortKnoxster, 2019). Najčešće vrste hakerskih napada koji su doveli do krađe kriptovaluta su tvz. *phishing* napadi, XSS napadi na temelju ranjivosti JavaScripta u web aplikacijama (eng. *Cross Site Scripting*), napadi NoSQL ubrizgavanja zlućudnog koda i iskorištavanje logičkih ranjivosti (Novikov, 2018). Osim burzi kriptovaluta, navedenim vrstama napada podložne su i druge web platforme te aplikacije na internetu.

Shodno navedenom, bitno je kriptovalute čuvati što je moguće kraće vrijeme pohranjene na web mjestima za trgovanje kriptovalutama te ih dugoročno pohranjivati na sigurnim digitalnim novčanicima. Sigurni digitalni novčanici su oni čiji su privatni ključevi enkriptirani i pohranjeni lokalno, a ne na internetu. Daleko najsigurniji način pohrane kriptovaluta je na hardverskom novčaniku, elektroničkom uređaju koji čuva privatni ključ izvan interneta (eng. *Offline*). Prilikom svake transakcije potrebno je uređaj fizički spojiti na računalo te na uređaju upisati unaprijed kreiran pin kako bi se autentificirao vlasnik hardverskog novčanika.

Slika 10: Hardverski novčanik za kriptovalute (Izvor: *Singh*, 2018)

Prijetnja korisnicima kriptovaluta mogu biti i mnoge prevare koje postoje na internetu. Kod bankovnih i kartičnih transakcija banka može vratiti transakciju ili ju zamrznuti ukoliko dođe do zloupotrebe od strane neovlaštene osobe. Kod kriptovaluta ne postoji centralni entitet kojem se pojedinac može obratiti ako izgubi kriptovalute, budući da su transakcije na Blockchainu inverzibilne.

Iz činjenice da su kriptovalute isključivo digitalnog karaktera te nisu regulirane kao druga sredstva plaćanja proizlaze dodatni rizici kojima tradicionalni financijski instrumenti nisu podložni. Zato je, prije ikakvog eventualnog ulaganja, važno biti upućen u rizike trgovanja i pohrane kriptovaluta.

7. Zaključak

Kako se razvijala FinTech industrija, nastale su i virtualne valute koje se koncipiraju na Blockchain tehnologiji koja omogućava izvršavanje transakcija bez centralnog entiteta. Kriptovalute su inovacija koja počinje sve značajnije utjecati na ekonomiju i zaprimati sve veći interes javnosti. Centralne banke i drugi državni regulatori sve više reagiraju na njihov utjecaj regulacijom novonastalog tržišta, a stručnjaci u navedenom području sve češće pronalaze mjesto u financijskim organizacijama. Karakteristike kriptovaluta, poput decentralizacije i pseudoanonimnosti imaju veliki potencijal za širu upotrebu kao alternativnog sredstva plaćanja, a veliki potencijal kriptovaluta stvorio je iz njih novi financijski instrument. S druge strane, ova nova vrsta imovine nosi rizik velikih gubitaka.

Povijest kriptovaluta nije duga te je fundamentalnom analizom teško utvrditi kako će se tržište kriptovaluta kretati i kakvu budućnost ono nosi. S druge strane tehnička analiza otkriva kako Bitcoin postaje sve teže rudariti te investitori postaju sve više zainteresirani za ulaganje. Pojavljivanjem sve većeg broja različitih burzi i mjenjačnica kriptovaluta trgovanje kriptovalutama postaje dostupnije široj javnosti, a provizije sve manje.

Daljnjim razvojem Blockchain tehnologije trebalo bi se postići smanjenje trošenja električne energije na rudarenje te povećanje brzine obrađivanja transakcija na Blockchainu. S druge strane, korištenje sredstava plaćanja koja nisu regulirana od strane države snosi i visoke rizike, a u krajnjoj liniji i zabranu trgovanja, što može kompletno preokrenuti daljnji razvoj ove industrije. Hoće li kriptovalute postati dio povijesti kao još jedan financijski balon i biti zaboravljene ili će se svaka druga osoba koristiti kriptovalutama kao sredstvom plaćanja možemo samo nagađati. Na svakom pojedincu preostaje da samostalno promisli i odluči je li potencijalan uspjeh vrijedan rizika.

Popis literature

99Bitcoins (bez. dat.). *Bitcoin Historical Price & Events* [Webstranica s webalatom za analiziranje cijene Bitcoina preko grafa]. Pristupano 17.6.2020. i 21.6.2020 preko https://99bitcoins.com/bitcoin/historical-price/

Binance (bez. dat.). *Struktura provizija*. Preuzeto 20.6.2020. s https://www.binance.com/en/fee/schedule

Bitcoin store (bez. dat.) *Česta pitanja?* [izbornik na stranici]. Preuzeto 20.6.2020. s https://www.bitcoin-store.hr/en/faq

Bloomberg (1.6.2020). *China's Digital Currency Could Challenge Bitcoin and Even the Dollar.* Pristupano 27.6.2020. preko https://www.bloomberg.com/news/articles/2020-06-01/china-is-making-cryptocurrency-to-challenge-bitcoin-and-dollar

Browdie Brian (2012). *BitPay Signs 1,000 Merchants to Accept Bitcoin Payments.* Preuzeto 17.6.2020. s https://www.americanbanker.com/news/bitpay-signs-1-000-merchants-to-accept-bitcoin-payments

Carigrad (2019). *The Crypto Space is Booming in Latin America*. Pristupano 24.6.2020. preko https://carigrad.org/news/article/1

CoinMarketCap (2020). Web aplikacija koju koristim kao alat za provjeru tržišnog udjela i cijene kriptovaluta. Pristupano 23.5.2020., 21.6.2020 i 27.7.2020. preko https://coinmarketcap.com/

Desjardins Jeff (2017). *The Unparalleled Explosion in Cryptocurrencies*. Pristupano 26.6.2020. preko https://www.visualcapitalist.com/unparalleled-explosion-cryptocurrencies/

Digiconomist (2020). *Bitcoin Energy Consumption Index*. Pristupano 24.6.2020. preko https://digiconomist.net/bitcoin-energy-consumption

Dujella Andrej. Bez. dat. *Klasična kriptografija*. Preuzeto 24.04.2020. s https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html

Dwork Cynthia and Naor Moni (1993). *Pricing via Processing or Combatting Junk Mail.*

Preuzeto 14.6.2020. s https://link.springer.com/content/pdf/10.1007%2F3-540-48071-4_10.pdf

Europska komisija – predstavništvo u Hrvatskoj (2020). *Kriptovalute i blockchain – sve što Trebate znati.* Preuzeto 24.4.2020. s https://ec.europa.eu/croatia/cryptocurrencies_and_blockchain_all_you_need_to_know_hr

Fiorillo Steve (2018). *Bitcoin History: Timeline, Origins and Founder.* Preuzeto 19.5.2020. s https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578

Fortknoxster (2019). The top 10 crypto exchange biggest hacks ever. Preuzeto 7.7.2020. s https://fortknoxster.com/blog/the-top-10-crypto-exchange-biggest-hacks-ever/

Greenberg Andy (2011). *WikiLeaks Asks For Anonymous Bitcoin Donations*. Preuzeto 21.6.2020. s https://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/#1cb52c974f73

Hayes Adam (2020) *What Happens to Bitcoin After All 21 Million Are Mined.* Pristupano 21.6.2020. s https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/

Huskanović Alen (bez. dat.). *Proof of work: what it is and how does it work*. Preuzeto 14.6.2020. s https://www.asynclabs.co/blog/proof-of-work-what-it-is-and-how-does-it-work/

Kagan Julia (2019). *Financial Technology – Fintech*. Preuzeto 23.4.2020. s https://www.investopedia.com/terms/f/fintech.asp

Le Kenny (2019) *The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed*. Pristupano 24.6.2020. s https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44

Mahler Till Antonio (2018). *'82 | The Birth Of Digital Cash*. Preuzeto 19.5.2020. s https://medium.com/blockwhat/82-the-birth-of-digital-cash-ea08b53379d8

MarketWatch (2020). *S&P 500 Index* [Web alat za praćenje cijene indeksa]. Pristupano 25.6.2020. preko https://www.marketwatch.com/investing/index/spx

Marquit Miranda (2020). *Should You Invest in Stocks or Bitcoin?* Pristupano 25.6.2020. preko https://www.marketwatch.com/investing/index/spx

Nakamoto Satoshi (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Pristupano 23.6.2020. s https://bitcoin.org/bitcoin.pdf

Novikov Ivan (2018). *Why Are Crypto Exchanges Hacked So Often?* Preuzeto 7.7.2020. s https://www.forbes.com/sites/forbestechcouncil/2018/09/17/why-are-crypto-exchanges-are-hacked-so-often/#733499933421

Orešković David (18.2.2020). *Tehnologija pametnih ugovora objašnjena kroz infografiku.* Preuzeto 23.5.2020. s https://crobitcoin.com/tehnologija-pametnih-ugovora/

Orešković David (18.2.2020). *Koje su lokacije Bitcoin bankomata u Hrvatskoj?* Preuzeto 18.6.2020. s https://crobitcoin.com/koje-su-lokacije-bitocin-bankomata-u-hrvatskoj/

Oršulić Nikolina (16.1.2020). *Iz prve ruke: Greyp Bikes otkriva kako uspješno provesti ETO digitalno prikupljanje kapitala*. Pristupano 26.6.2020. preko https://www.lider.media/sto-i-kako/iz-prve-ruke-greyp-bikes-otkriva-kako-uspjesni-provesti-eto-129709

Pavić Zvonko (2020). *Što je Blockchain?* Preuzeto 11.6.2020. s https://tockanai.hr/tehnologija/sto-je-blockchain-32409/

Rios Ana Maria (2020). *Share of adult population with a bank or mobile money service account in Brazil between 2011 and 2017*. Pristupano 24.6.2020. preko https://www.statista.com/statistics/898974/population-bank-account-type-brazil/

Rogina Nikola (2020). *Što je Ripple (XRP) te isplati li se ulagati?* Preuzeto 23.5.2020. s https://www.kriptovaluta.hr/altcoin/sto-je-ripple-xrp-te-isplati-li-se-ulagati/

RRIF Visoka škola za financijski menadžment (2018). *Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama.* Pristupano 27.6.2020. preko https://www.rrif.hr/Porezni_tretman_kapitalnih_dobitaka_po_osnovi_trgo-3543-misljenje.html

Sedgwick Kai (2019). *Bitcoin History Part 8: When 1,500 BTC Cost Less Than $1.* Preuzeto 17.6.2020. s https://news.bitcoin.com/bitcoin-history-part-8-when-1500-btc-cost-less-than-1/

Stipaničev Zoran (2003). *SHA-256*. Preuzeto 15.6.2020. s http://sigurnost.zemris.fer.hr/algoritmi/hash/2004_stipanicev/index.htm

Škola koda. Bez dat. *Učimo blockchain.* Preuzeto 25.04.2020. s https://skolakoda.org/hash-funkcija

Škvorc Bruno (2018). *Po čemu se razlikuju Proof of Work, Proof of Stake, i Delegated PoS metoda?* Preuzeto 15.6.2020. s https://bitfalls.com/hr/2018/04/24/whats-the-difference-between-proof-of-work-pow-proof-of-stake-pos-and-delegated-pos/

Toshendra Kumar Sharma (2018). *How does blockchain use public key cryptography.* Preuzeto 24.04.2020. s https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

Trading Economics (2020) *Venezuela Inflation Rate and European Union Inflation Rate.* Pristupano 24.6.2020. preko https://tradingeconomics.com/venezuela/inflation-cpi

Vrbanus Sandro (11.6.2020). *Hrvatska dobiva investicijski fond koji će ulagati u bitcoin.* Pristupano 26.6.2020. preko https://www.bug.hr/kriptovalute/hrvatska-dobiva-investicijski-fond-koji-ce-ulagati-u-bitcoin-15059

Vrbanus Sandro (18.6.2019). *Službeno najavljena Facebookova kriprovaluta Libra.* Pristupano 27.6.2020. preko https://www.bug.hr/kriptovalute/sluzbeno-najavljena-facebookova-kriptovaluta-libra-10035

WebHosting-WMD (bez.dat.). *Intrinzična vrijednost.* Pristupano 25.6.2020. preko https://webhosting-wmd.hr/rjecnik-pojmovi-i/web/intrinzicna-vrijednost

Živković Sven (2018). *Blockchain tehnologija* [Diplomski rad]. Preuzeto 11.6.2020. s https://zir.nsk.hr/islandora/object/infri:289/preview

Popis slika

Izvor: Jeff Desjardins (2017). Preuzeto 26.6.2020. preko https://www.visualcapitalist.com/unparalleled-explosion-cryptocurrencies/

Slika 10: Hardverski novčanik za kriptovalute

Izvor: Singh Surajdeep (2018) Preuzeto 7.7.2020. preko https://cryptocurrencynews.com/best-hardware-wallets/