Modeliranje tehnologije distribuiranoga zapisa i njena primjena

Tomić, Bojan

SVEUČILIŠTE U RIJECI
EKONOMSKI FAKULTET U RIJECI

Bojan Tomić, univ.spec.oec.

MODELIRANJE TEHNOLOGIJE DISTRIBUIRANOGA ZAPISA I NJENA PRIMJENA

DOKTORSKI RAD

Rijeka, 2021.

SVEUČILIŠTE U RIJECI
EKONOMSKI FAKULTET U RIJECI

Bojan Tomić, univ.spec.oec.

MODELIRANJE TEHNOLOGIJE DISTRIBUIRANOGA ZAPISA I NJENA PRIMJENA

DOKTORSKI RAD

Mentor: prof.dr.sc. Saša Žiković

Rijeka, 2021.

UNIVERSITY OF RIJEKA
FACULTY OF ECONOMICS RIJEKA

Bojan Tomić, univ.spec.oec.

MODELING OF DISTRIBUTED LEDGER TECHNOLOGY AND ITS APPLICATION

DOCTORAL THESIS

Rijeka, 2021.

Mentor rada: prof.dr.sc. Saša Žiković

Doktorski rad je obranjen dana 04. ožujka 2021. godine na Ekonomskom fakultetu u Rijeci, Sveučilište u Rijeci, pred povjerenstvom u sastavu:

1. Dr. sc. Mario Pečarić, redoviti profesor Ekonomskog fakulteta u Rijeci, predsjednik povjerenstva,
2. Dr. sc. Mira Dimitrić, redovita profesorica Ekonomskog fakulteta u Rijeci, članica,
3. Dr. sc. Zdravka Aljinović, redovita profesorica Ekonomskog fakulteta u Splitu, članica.

SAŽETAK

Kontinuiranim razvojem informatičkih tehnologija i interneta intenzivirao se rad na postojećim idejama digitalnog novca. Kao rezultat toga, računalni program Bitcoin protokola je pušten u javnost 9. siječnja 2009. godine čime se kreira infrastruktura za prvu kriptovalutu s licencom otvorenog programskog koda koji je slobodan za javnost. To znači da svatko tko ima interes može replicirati postojeći protokol, kreirati novu kriptovalutu i pustiti u javnost. Ovo posljednje je omogućilo stvaranju niza novih kriptovaluta s različitim svojstvima i širenju njihove upotrebe prvo u platnom prometu, a zatim i u kontekstu njihovog trgovanja na novom sekundarnom tržištu.

Cilj ovog rada je formalno identificirati i opisati mogućnost konstrukcije portfelja kreiranih prema različitim optimizacijskim ciljevima, a čije sastavnice predstavljaju kriptovalute kao nova vrsta utržive imovine. Prva skupina portfelja je formirana i modelirana kroz vrijednost bitcoin kriptovalute, a druga skupina kroz dolarsku novčanu jedinicu. U tu svrhu je provedeno pet različitih optimizacijskih strategija, te su i prezentirani rezultati strategije s jednakim udjelima u portfelju. Inicijalne sastavnice portfelja su definirane prema razvoju programskog koda i veličini zajednice.

Rezultati portfelja izraženog kroz jedinice bitcoin kriptovalute sugeriraju da dinamika povijesnih prinosa kriptovaluta pruža mogućnost modeliranja portfelja u bitcoin valuti. Takvi rezultati su opravdani s obzirom da je dinamika prinosa optimizacijske strategije ostvarila kumulativni prinos viši od kumulativnog prinosa najuspješnije sastavnice portfelja. S druge strane, rezultati portfelja izraženog u dolarskoj vrijednosti nisu ostvarili kumulativni prinos viši od kumulativnog prinosa odabranog standarda usporedbe, pa se zaključuje da primijenjeni fundamentalni indikatori ne predstavljaju dobar pokazatelj za inicijalan odabir sastavnica portfelja.

Ključne riječi: *Bitcoin, kriptovalute, blockchain, optimizacija, prinos, rizik*

SUMMARY

The continuous development of information technologies and the Internet intensified work on existing ideas of digital money. As a result, the computer program of the Bitcoin protocol was released to the public on January 9th 2009, creating an infrastructure for the first cryptocurrency with an open source software license that is free to the public. This means that anyone with an interest can replicate an existing protocol, create a new cryptocurrency, and release it to the public. The latter enabled the creation of a series of new cryptocurrencies with different characteristics and the expansion of their use first in payment transactions and then in the context of their trading on a new secondary market.

The aim of this paper is to formally identify and describe the possibility of forming portfolios created according to different optimization goals, whose components represent cryptocurrencies as a new type of marketable assets. The first group of the portfolio was formed and modeled through the value of the bitcoin cryptocurrency, the second group through the dollar currency. For this purpose, five different optimization strategies were implemented, and the results of the strategy with equal shares in the portfolio were presented. The initial components of the portfolio are defined according to the development of the program code and the size of the community.

The results of the portfolio which are expressed through units of bitcoin cryptocurrency suggest that the dynamics of historical cryptocurrency returns provides the possibility of modeling a portfolio in bitcoin currency. Such results are justified given that the return dynamics of the optimization strategy achieved a cumulative return higher than the cumulative return of the most successful component of the portfolio. On the other hand, the results of the portfolio expressed in dollar value did not achieve a cumulative return higher than the cumulative return of the selected comparison standard, so it is concluded that the applied fundamental indicators are not a good indicator for the initial selection of portfolio components.

Keywords: *Bitcoin, cryptocurrencies, blockchain, optimisation, yield, risk*

SADRŽAJ

1. UVOD

1.1. Definiranje problema i predmeta istraživanja

Razvojem informatičkih tehnologija i interneta te porastom nepovjerenja u globalni financijski i platni sustav kao odgovor na proteklu globalnu financijsku krizu, intenzivira se rad na već postojećim idejama digitalnog novca. Kao rezultat tog rada, 2008. godine je prezentiran dokument pod nazivom „Bitcoin: *A Peer-to-Peer Electronic Cash System*“ u kojem se opisuje novi decentralizirani transakcijski sustav koji ne uključuje posrednika između entiteta od interesa. Prvi opis sadržaja članka navodi osoba koja se potpisuje kao Satoshi Nakamoto na internet stranicama http://www.metzdowd.com zajedno s linkom na cijeli članak istoimenog autora. Već na prvi pogled opisanih svojstava sustava koje naglašava autor, moglo se naslutiti koliko je revolucionarna, dalekosežna i obećavajuća ideja njegovog projekta. Računalni program, odnosno Bitcoin protokol je pušten u javnost 9. siječnja 2009. godine čime se kreira infrastruktura za prvu kriptovalutu – bitcoin. Bitcoin tehnologija je omogućila gotovo trenutno izvršenje transakcija, sa zanemarivim naknadama bez posrednika ili središnjeg tijela čime je privukla veliku pažnju, kao i velik broj samih korisnika. Važna karakteristika Bitcoin transakcijskog protokola je njegova licenca otvorenog programskog koda (engl. *open source*). Naime, svi algoritmi i korištena rješenja primijenjena u njegovoj izgradnji, slobodni su preko platforme za kolaboraciju razvojnih programera. Bilo tko s interesom je mogao pristupiti linijama koda, proučavati ih i raditi na sustavu. Ukoliko su prijedlozi u smjeru unapređenja, zajednica će prihvatiti promjene i unaprijediti protokol. Međutim, to isto znači da je postojeći protokol bilo jednostavno replicirati, u nekom segmentu promijeniti i prilagoditi svojim potrebama, kreirati novu kriptovalutu s novim svojstvima i pustiti u javnost. Upravo ovo posljednje je omogućilo stvaranju niza novih kriptovaluta s različitim svojstvima i širenju njihove upotrebe prvo u platnom prometu, a zatim i u kontekstu njihovog trgovanja na novom sekundarnom tržištu.

Bitcoin platforma je decentraliziran transakcijski sustav, odnosno distribuirana glavna javna knjiga (engl. *public ledger*), osigurana kriptografijom i upravljana konsenzusom, na koju su zapisane sve transakcije koje su se dogodile između sudionika u zajednici. Javnu glavnu knjigu sačinjavaju transakcije grupirane u tzv. blokove iz

čega proizlazi da je glavna knjiga zapravo lanac blokova (engl. *blockchain*). Na kraju svakog bloka se nalazi sažetak tog bloka, odnosno sažetak svih prethodnih transakcija zapisan kao sintaksa funkcije algoritma sažimanja (engl. *hash ili digest*) (Härdle, Harvey & Reule, 2019). Taj se zapis distribuira širom mreže i predstavlja prvi zapis za sljedeći blok transakcija. Osim sažetka svih transakcija, mrežom se distribuira i novi blok transakcija[1]. Kako je funkcija sažimanja jednosmjerni matematički algoritam koji iste ulazne podatke pretvara u izlazni zapis s jedinstvenom strukturom, ukoliko dođe do odstupanja u rezultatu funkcije sažimanja između čvorova u mreži (engl. *nodes*), to bi značilo da je došlo do promjene podataka, ili u prethodnim transakcijama, ili u kreiranom novom bloku transakcija. Drugim riječima, netko od sudionika mreže je promijenio bilancu stanja po nekom od računa u mreži i takav se blok transakcija odbacuje i klasificira kao netočan. Upravo je opisan proces rješenje problema koji je duže vrijeme bio kamen spoticanja u kontekstu razvoja digitalnih valuta, a to je dupla potrošnja.

Osim u smjeru digitalnih valuta, opisano je rješenje doprinijelo i razvoju niza mladih, tehnoloških firmi koji svoju poslovnu ideju razvijaju na javnoj, distribuiranoj glavnoj knjizi. Digitalni zapis i blockchain tehnologija omogućuje transparentnost zato što je zapis svake transakcije vidljiv i javno dostupan. Implementacijom takve tehnologije potrošnja svake jedinice novca bi bila javna čime u potpunosti nestaje mogućnost malverzacije, korupcije itd. Osim u kontekstu vrijednosti novčanih jedinica koje je moguće izraziti čak do 8 decimalnim mjesta (Symitsi i Chalvatzis, 2018), primjena takve tehnologije je jako široka. Tako se, na primjer, već razvijaju računovodstveni informacijski sustavi bazirani na distribuiranoj glavnoj knjizi jer se zapravo radi o elektronskom zapisu koji može imati različitu svrhu, npr. zapis salda na kontima kupaca i dobavljača, dokaz o vlasništvu financijskih instrumenata, glazbeni zapis itd.

Međutim, prednost distribuirane glavne knjige je u tome što, ukoliko se to omogući, svatko po potrebi može potvrditi/verificirati npr. stanje svog potraživanja na kontu dobavljača svog kupca, čime ovjera izvoda otvorenog stanja – IOS, postaje bespotrebna jer nitko neće imati potrebu da provjerava ono što već zna i što je sigurno točno. Pored toga, razvojem pametnih ugovora – ugovori koji se izvršavaju

[1] Nove transakcije se zapravo distribuiraju mrežom tek nakon što jedan od čvorova mreže riješi matematički problem metodom iteracije.

sami po ispunjavanju definiranih uvjeta (engl. *smart contract*), praktična primjena blockchaina se dodatno povećava. Na primjer, prijenos se vlasništva također može implementirati kroz pametne ugovore u blockchain. Drugim riječima, nije se moguće uknjižiti kao vlasnik nekog dobra, pokretnine, nekretnine itd., sve dok nisu zadovoljeni uvjeti iz ugovora. Iako se pretpostavlja da tako nešto niti danas nije moguće, uvijek postoje pojedinačni, izolirani slučajevi prodaje imovine koja nije za prodaju, krive uknjižbe iste, odnosno različitih prevara i malverzacija prilikom promjene vlasništva dobra/imovine. Primjenom blockchain tehnologije, takvi slučajevi više nisu mogući, te tako primjena instrumenata osiguranja, poput bankarskih garancija, zadužnica, akreditiva itd., u slučaju dužničko vjerovničkih odnosa, također više nije potrebna. Ovo su samo neki od osnovnih primjera praktične implementacije blockchain tehnologije na temelju kojih su nastale, i još uvijek nastaju, novi tehnološki startupovi širom svijeta. Sukladno navedenom, može se pretpostaviti kako bi u skoroj budućnosti – zajedno s razvojem tehnologije, trebalo doći do intenziviranja praktične primjene iste na široj globalnoj razini, ali i na razini pojedine države, odnosno društva. Takva pretpostavka otvara mogućnosti te daje prostora za izučavanje, odnosno poslovni razvoj korporacija, što čini dodatni poticaj za analizu kretanja tehnološkog razvoja blockchaina, kao i vrijednosti samog tržišta kriptovaluta. Pored tehnološkog dostignuća i praktične primjene istog, kriptovalute bazirane na blockchainu se mogu promatrati i kao nova vrsta digitalne imovine (Glaser, Zimmermann & Haferkorn, 2014). Postoje različite kategorizacije i definicije kriptovaluta, međutim za sada niti jedna od njih nije u potpunosti prihvaćena niti postoji konsenzus koju vrstu postojeće imovine predstavljaju kriptovalute.

Iako se dizajn tržišta kriptovaluta u svojoj inicijalnoj fazi bazirao isključivo na parametrizaciju postojećeg Bitcoin protokola (Elendner, Trimborn, Ong i Lee, 2016), upravo svojstvo otvorenog koda i praktična implementacija blockchain tehnologije – karakteristike koje su prepoznale mlade i inovativne tvrtke s ciljem prikupljanja kapitala potrebnog za svoj razvoj s jedne strane, te pozitivne reakcije javnosti na ideju decentralizacije s druge strane, doprinijelo je stvaranju uvjeta ponude i potražnje te je tako nastalo potpuno novo primarno tržišta kriptovaluta. Na jednoj su strani bile inovativne tvrtke koje su svoju ideju financirale emitiranjem kriptovaluta, a s druge strane investitori koji su htjeli investirati u tu ideju zasnovanu na blockchainu. Razvojem primarnog tržišta povećao se i broj mjenjačnica/burzi na kojima se aktivno

trgovalo čime je stvoren jedan novi, samostalno održivi, ekosustav primarnog i sekundarnog tržišta kriptovaluta.

Sekundarno tržište kriptovaluta je izrazito rizično tržište iz nekoliko razloga. Prvo, to je potpuno neregulirano tržište što znači da je podložno cjenovnim manipulacijama. Drugo, još nije izveden matematički izraz za izračun barem približne intrinzične vrijednosti kriptovaluta – kao u slučaju standardnih financijskih instrumenata. Prema tome, ako s jedne strane postoji imovina koja već deset godina postiže neku tržišnu vrijednost, a s druge strane ne postoji fundamentalno uporište koje opravdava tu vrijednost, nije niti čudno da pojedina kriptovaluta u jednom danu može ostvariti kumulativni prinos od čak nekoliko puta svoje početne vrijednosti, ali ga i izgubiti tako naglo. S ciljem procjene rizika i intrinzične vrijednosti, prvenstveno je potrebno definirati varijable koje bi mogle utjecati na tržišnu vrijednost kriptovaluta, pa tek onda izučavati njihove odnose. Bilo s poslovnog aspekta i investiranja ili sa znanstvene strane, takav pristup je više nužan nego poželjan kako bi se otklonio podređeni položaj interesnih sudionika i skupina.

Investiranje je rizičan proces koji podrazumijeva izlaganje tržišnim promjenama vrijednosti imovine u koju se investira. Svaka investicija podrazumijeva određeni stupanj rizika, a glavno svojstvo koje definira je li promatrana investicija pogodna za investitora ovisi o konkordanciji njegove preferencije rizika i očekivanog prinosa – kao osnovne mjere uspjeha investiranja na tržištu, s rizikom i očekivanim prinosom promatrane investicije. Prema tome, konačni cilj investitora je ostvariti prinos na uloženi kapital koji u domeni njegove tolerancije, odnosno averzije prema riziku, zadovoljava očekivanu premiju za preuzeti rizik. Neovisno o vrsti imovine, prilikom konstruiranja portfelja, investitori bi trebali razmotriti dinamiku odnosa prinosa odabrane imovine portfelja kako bi se identificirao i kvantificirao preuzeti rizik ulaganja. Kao naknadu za viši preuzeti rizik, investitor bi trebao ostvariti i viši očekivani prinos. Opisana relacija se može promatrati kao problem investiranja, a to je uvijek povezano s raznim oblicima i izvorima rizika iz čega se može zaključiti da se prilikom investiranja zapravo govori o problemu odlučivanja. Navedeni se problem može razmatrati kvalitativnim, ali i brojnim kvantitativnim pristupima u kojima se neizvjesnost i ostvareni prinos eksplicitno determiniraju i kvantificiraju kao rizik i očekivani prinos te tako uzimaju u daljnji proces odlučivanja. Svaki racionalni

investitor će težiti investiranju u onu imovinu koja maksimizira njegovu očekivanu korisnost. Iako samo kao koncepcijska formulacija ponašanja investitora, pretpostavka je da je preferencija korisnosti konačan rezultat brojnih ograničenja s kojima se može susresti investitor.

U ovom se radu provodi istraživanje u kojem se ispituju odnosi kriptovaluta s ciljem konstruiranja i modeliranja njihovog portfelja. Modeliranju portfelja se pristupilo primjenom moderne teorije portfelja koja predstavlja jedan od najviše korištenih modela za rješavanje problema alokacije imovine i definiranje optimalnog ulaganja. U svojoj osnovi, investitori primjenom različitih tehnika, modela i strategija pokušavaju konstruirati vlastiti portfelj čija bi dinamika performansi trebala pobijediti tržište, odnosno portfelj koji bi trebao ostvariti prinose više od prinosa tržišta u ravnoteži. Takva definicija podrazumijeva aktivnosti potrage za podcijenjenom imovinom što bi u konačnici rezultiralo tržištem koje je informacijski efikasno, tj. tržištem čija agregatna vrijednost odražava sve relevantne i dostupne informacije vezane za pojedinu imovinu. Ukoliko se standardne definicije investiranja stave u kontekst tržišta kriptovaluta, može se primijetiti njihova nepodudarnost. Prvo što se ne može staviti u kontekst tržišta kriptovaluta je sintagma *tržište u ravnoteži*. Da bi neko tržište bilo u svojoj ravnoteži, to bi značilo da postoji tržišni konsenzus očekivanih stopa prinosa imovine u koju se investira. Da bi postojao tržišni konsenzus, podrazumijeva se postojanje njegove fundamentalne vrijednosti, jer kako stvoriti konsenzus o očekivanom prinosu na neku imovinu ako dva neovisna investitora istu imovinu vrednuju potpuno različito (npr. investitor A vrednuje bitcoin tisuću kuna, a investitor B sto tisuća kuna, a trenutna cijena bitcoina je pet stotina kuna). Drugo, da bi tržište bilo informacijski efikasno, kao što je prethodno navedeno – prvo je potrebno definirati koje su to informacije koje mogu, trebaju, ali već i utječu na cijenu kriptovaluta, a tek onda ispitati postoji li pozitivna ili negativna cjenovna reakcija na njihovu objavu (npr. dolazi do razdvajanja/izdvajanja tzv. forkanja Bitcoin sustava što znači da se broj postojećih bitcoin jedinica duplicira, a vrijednost bitcoina ostane jednaka kao i prije objave te informacije). Prema tome, zbog odsutnosti barem približno jednakog vrednovanja podcijenjena, odnosno precijenjena imovina zapravo i ne postoji, pa stoga ne postoji niti tržišni konsenzus o očekivanim stopama prinosa, kao niti tržište u ravnoteži koje je informacijski efikasno. Međutim, bez obzira na sve navedeno, tržište kriptovaluta i cijela njegova infrastruktura kontinuirano bilježi rast iz

godine u godinu. Upravo zbog svoje dostupnosti sve je više institucionalnih i individualnih investitora različitih profila koji ulažu i trguju s kriptovalutama zbog čega se još više javlja potreba za analizom provedenom u ovom radu.

S aspekta portfolio menadžera, kritika tržišta kriptovaluta je, između ostalog, i problem njihove visoke korelacije. Da bi racionalan investitor kreirao dobro diverzificiran portfelj sukladno njegovoj averziji, odnosno toleranciji rizika, morao bi imati imovinu koja mu svojom dinamikom pruža takvu mogućnost, a kripto tržište to nije. Navedeno se može primijetiti iz konstrukcije CRIX indeksa. Osnovna zadaća CRIX indeksa je repliciranje kretanja ukupnog tržišta kriptovaluta koji broji skoro pet tisuća različitih kriptovaluta – sukladno bazi podataka korištenoj za indeks „CoinGecko“[2]. Prema tome, ako je broj ulaznih varijabli za konstrukciju indeksa pet tisuća, a trenutno je u sastavu indeksa samo pet vodećih kriptovaluta koje su dostatne da bi replicirale kretanje tržišta, očito je da se tržište kriptovaluta kreće u istom obrascu. Naravno, ovdje se treba uvažiti i metodologija CRIX-a koja uzima u obzir samo likvidne kriptovalute. Međutim, evidentno je da je mogućnost diverzifikacije zbog visoke pozitivne korelacije slaba, odnosno da se svodi na svega pet kriptovaluta[3]. Iako je u nekim od prethodnih radova korelacija kriptovaluta prezentirana i interpretirana, nigdje nije navedena ili opisana barem teorijska pretpostavka zašto je to tako. Neki su od razloga svakako veličina samog tržišta, kratko vrijeme njegovog postojanja, kao i nepostojanje regulatornih okvira. Međutim, po mišljenju autora ovog rada, jedan od glavnih razloga je aspekt promatranja pariteta prilikom analize, odnosno konstrukcije portfelja. Istraživanja koja su provedena do sada, kao i CRIX okvir, kriptovalute promatraju u protuvrijednosti fiat valuta, npr. BTC/USD. Jasno je da je takav aspekt poželjan ukoliko je cilj maksimalizacija bogatstva investitora izraženom u fiat valuti. Međutim, važno je naglasiti da je u tom slučaju vrijednost bilo koje druge kriptovalute određena vrijednošću bitcoina izraženom u protuvrijednosti fiat valute. Navedeno se može predočiti na primjeru domaćeg tržišta kapitala. Konstrukcija sekundarnih tržišta kriptovaluta je posložena kao da se npr. vrijednost dionica na Zagrebačkoj burzi prvo izražava u vrijednosti dolara, pa se tek onda preračunava u kunsku protuvrijednost.

[2] https://www.coingecko.com/

[3] Ovdje je važno naglastiti da su različita istraživanja dala oprečne rezultate o smjeru i jakosti korelacije između promatranih kriptovaluta. Navedeno se može pravdati odabirom različitog vremena promatranja.

Ukoliko je vrijednost dionica izraženo u dolarima ostala ista, ali je dolar aprecirao u odnosu na kunu, vrijednost dionica izražena u kunama je zapravo narasla. Drugim riječima, potrebno je više kuna da bi se kupila dionica čije je cijena u dolarima ostala nepromijenjena. Ista stvar se događa na kripto tržištu. Cijena svake kriptovalute se prvo preračunava u njenu protuvrijednost u BTC-u, pa se tek onda ta vrijednost BTC-a preračunava u fiat poput USD. Ukoliko dođe do rasta vrijednosti BTC/USD za npr. 5%, a vrijednost neke druge kriptovalute u BTC-u je ostala ista, onda je i ta promatrana kriptovaluta ostvarila prinos od 5% izražen u USD-u. Prema tome, ako se vremenske serije potrebne za analizu promatraju u vrijednosti fiat valute, logično je očekivati visoku pozitivnu korelaciju na kripto tržištu. Rijetke su one burze koje kotiraju direktan paritet kripto/fiat, odnosno burze koje pružaju mogućnost deponiranja i povlačenja fiat novca, kao i neposrednog trgovanja s njim. Daleko je puno više burzi koje posluju na gore opisan način te je to jedan od glavnih razloga visoke pozitivne korelacije na tržištu kriptovaluta[4]. Osim standardnog pristupa, u ovom se radu proširuje okvir do sada provedenih analiza i predlaže modeliranje vrijednosti portfelja izraženog kroz vrijednost BTC-a kao obračunske jedinice. Investitori ne moraju nužno zahtijevati povrat izražen u fiat valuti poput dolara. Zasigurno postoje investitori čiji je interes prinos u BTC-u upravo zbog optimističnih očekivanja njegove vrijednosti u budućnosti. Sukladno tome, modeliranje i interpretacija performansi portfelja izraženog u BTC-u, osim što pruža svrhu u kontekstu investicijske analize, kvantitativnim metodama neizvjesne situacije pretvara u mjerljiv rizik, što čini glavnu okosnicu znanstvenog doprinosa ovog rada.

Prethodno je navedeno da kriptovalute nemaju svoju intrinzičnu vrijednost, odnosno da još nemaju varijable za koje je dokazano da su pokretači njihove fundamentalne vrijednosti. Razlog tome je specifičnost njihovog ekosustava. Većina kriptovaluta je emitirana s ciljem prikupljanja kapitala mladih i inovativnih tvrtki koje svoju poslovnu ideju zasnivaju na blockchainu. Međutim, promatrajući ih s aspekta emitiranja standardnih financijskih instrumenata, moguće je doći do krivog zaključka. Naime,

[4] Osim korelacije, navedeno ima velike posljedice i na procjenu, odnosno tumačenje rizika kriptovaluta jer je tržište kriptovaluta opterećeno visokim sistematskim rizikom. Pored toga, ukoliko se analiziraju kriptovalute kreirane na postojećim protokolima (sekundarne kriptovalute), poput Ethereuma, sistematski se rizik u nekoj mjeri multiplicira. Na primjer, ukoliko cijena ETH-a izgubi 20% svoje vrijednosti zbog nekih tehnoloških problema, očekivano je da i tokeni kreirani na ethereum platformi izgube jedan dio svoje vrijednosti. Opisane odnose je tek potrebno ispitati jer ne postoje radovi koji se bave procjenom sistematskog rizika – iako postoji CRIX indeks koji bi mogao predstavljati cjelokupno tržište, kao niti radovi koji se bave procjenom sistematskog rizika sekundarnih kriptovaluta.

kriptovalute nisu i ne moraju biti isključivo vezane za poslovni uspjeh tvrtke koja ih je emitirala – kao što je to slučaj s dionicama. Kritptovalute se baziraju na otvorenom programskom kodu koji je slobodan za javnost i nalazi se na nekoj od platformi za kolaboraciju developera, poput GitHub-a[5]. Ukoliko se promatra javni i otvoreni blockchain, postoje različiti poticaji za održavanje jednog takvog ekosustava. Na primjeru Bitcoin platforme, za svaki novi spremljeni blok transakcija, čvorovi su u mreži, osim transakcijske naknade, nagrađeni i novim brojem bitcoina i to je jedini način stvaranja te kriptovalute. Drugim riječima, nakon prikupljanja kapitala potrebnog za inicijalne troškove kao što je najam prostora tvrtke, plaće razvojnih programera, marketinga itd., jednom kada blockchain postane aktivan i javan, zajednica je ta koja većim djelom utječe na njegov uspjeh razvojem i implementacijom programskog koda putem konsenzusa. Prema tome, ovdje se već definiraju dvije varijable koje bi potencijalno mogle utjecati na tržišnu vrijednost pojedine kriptovalute: razvoj programskog koda na GitHub-u i veličina i podrška zajednice.

Prethodno navedeno je utjecalo na daljnji teoretski razvoj ideje ovog rada. Naime, u dosadašnjim istraživanjima, inicijalni odabir sastavnica portfelja je uvjetovan nekim postojećim okvirom poput CRIX indeksa kriptovaluta, ili je prepušten odabiru koji proizlazi kao rezultat optimizacije portfelja više različitih kriptovaluta. Rezultat toga je optimalan portfelj kriptovaluta koje mogu, ali i ne moraju imati fundamentalno uporište. S druge strane, na stranicama CoinGecko aplikacije razvijena je metrika koja rangira kriptovalute prema njihovim fundamentalnim pokazateljima, kao što su: tržišna cijena, volumen trgovanja, tržišna kapitalizacija, razvoj otvorenog koda, veličina zajednice itd. U ovom se radu modelira portfelj sastavljen od kriptovaluta koje su imale najviše bodova prema CoinGecko metrici. Na taj će se način ispitati potencijalna mogućnost konstrukcije portfelja na tržištu kriptovaluta čiji su rezultati bolji od rezultata tržišta, odnosno CRIX indeksa, optimiziranog CRIX indeksa, ali i nasumično kreiranih portfelja u istom vremenskom periodu. Ukoliko se ispostavi da su rezultati portfelja pobijedili tržište, može se zaključiti da je na tržištu kriptovaluta, primjenom standardnih optimizacijskih tehnika u sklopu moderne teorije portfelja,

[5] https://github.com/

moguće konstruirati portfelj na temelju fundamentalnih pokazatelja – što do sada nije ispitano, a to čini drugi dio znanstvenog doprinosa ovog rada.

Sukladno navedenom, ovim istraživanjem se želi dati odgovore na dva važna pitanja. Prvo je pitanje potencijalne korisnosti modeliranja portfelja izraženom u vrijednosti bitcoin valute čiji je cilj multipliciranje količine bitcoina kao krajnje vrijednosti, a drugo je pitanje postojanja povezanosti između potencijalnih fundamentalnih varijabli pojedine kriptovalute i njene tržišne cijene, što se može tumačiti kao prvi korak u definiranju njihove intrinzične vrijednosti.

1.2. Svrha, ciljevi i hipoteze istraživanja

Rezultati dosadašnjih istraživanja impliciraju da se tržište kriptovaluta promatra isključivo u paritetu s fiat novcem, najčešće američki dolar. Međutim, s obzirom da bitcoin kao sredstvo razmjene postoji već deset godina, i s obzirom na postojeću ali i brzorastuću infrastrukturu koja mu pruža praktičnu upotrebu, može se pretpostaviti da će u budućnosti, nakon stabilizacije volatilnosti, doći do njegove sve veće svakodnevne upotrebe. S druge strane, investitori skloni riziku i optimističnim očekivanjima, projiciraju da će cijena jednog bitcoina doseći čak milijun dolara u razdoblju od nekih 7 do 10 godina. Sve ovo su razlozi zbog kojih postoji interes i potreba promatranja korisnosti ulaganja kroz količinu bitcoina kao konačne krajnje vrijednosti.

Na standardnom, redovnom sekundarnom tržištu kapitala, proces odabira dionica za portfelj, barem u teoriji, trebao bi biti popraćen fundamentalnom i tehničkom analizom dionice. Takav je pristup nužan kako bi se smanjio tržišni rizik, odnosno definirale potencijalno podcijenjene dionice. Prilikom odabira kriptovaluta za formiranje portfelja, pristup ne bi trebao biti drugačiji. Razumno je očekivati da će kriptovalute koje imaju širu zajednicu – to znači potencijalno više transakcija, više mrežnih čvorova – to znači da je glavna knjiga više distribuirana, brži i napredniji blockchain – veće mogućnosti, više transakcija s nižim naknadama itd., imati i veću potražnju te će postići i višu cijenu na sekundarnom tržištu. Iz tog se razloga navedene prednosti mogu uzeti kao pozitivni parametri prilikom odabira kriptovaluta za optimizaciju u portfelju.

Sukladno tome, svrha ovog rada ima dvije komponente. Prva komponenta je razmatranje investicijskih mogućnosti unutar primjene moderne teorije portfelja na tržištu kriptovaluta izučavajući varijable u kripto/BTC paritetu. Druga komponenta je ukazati na potencijalnu korisnost primjene fundamentalnih indikatora pojedinog blockchaina prilikom odabira inicijalnih kriptovaluta kod formiranja portfelja. S obzirom na svrhu, prvi cilj rada, povezan s prvom hipotezom rada, je ukazati na mogućnost modeliranja portfelja u kripto/BTC paritetu, te egzaktno izmjeriti, opisati i ocijeniti karakteristike jednog takvog portfelja, kako bi se ispitala mogućnost multipliciranja količine bitcoin kriptovalute, sukladno preferencijama investitora. Drugi cilj rada, povezan s drugom hipotezom u radu, je ispitati korisnost korištenja potencijalnih fundamentalnih indikatora pojedinih kriptovaluta prilikom odabira inicijalnih sastavnica za portfelj, kako bi se definirale investicijske mogućnosti, ali i rizici povezani s implementacijom investicijske strategije temeljene na potencijalnim fundamentalnim indikatorima. U svrhu ocjene uspješnosti alokacijske strategije, rezultati portfelja će se usporediti s rezultatima tržišta kojeg predstavljaju: CRIX indeks, optimizirani CRIX indeks i nasumično kreirani portfelji.

U radu se postavljaju dvije hipoteze:

H1.: Na sekundarnom tržištu kriptovaluta, primjenom aktivnih investicijskih strategija, moguće je formirati portfelj izražen kroz vrijednost bitcoin kriptovalute koji ostvaruje viši kumulativni prinos od prinosa pojedinačnih sastavnica portfelja.

H2.: Na sekundarnom tržištu kriptovaluta, uvažavajući fundamentalne pokazatelje, moguće je formirati portfelj kriptovaluta koji ostvaruje viši kumulativni prinos od kumulativnog prinosa CRIX indeksa.

1.3. Pregled dosadašnjih istraživanja

Prva relevantna istraživanja na ovu temu se provode na Sveučilištu Humboldt u Berlinu, na Odjelu za statistiku, znanstvenoj instituciji koja je razvila prvi formalni

indeks kriptovaluta – CRIX (engl. *CRyptocurrency IndeX* – CRIX)[6]. U sklopu analize performansi indeksa, Trimborn (2015) provodi optimizaciju portfelja kriptovaluta tadašnjih sastavnica CRIX-a i izvodi portfelj s minimalnom varijancom – MVCRIX (engl. *minimum variance* CRIX), te ga uspoređuje s dinamikom CRIX-a u istom razdoblju promatranja. Da bi usporedio njihovu dinamiku, autor se suočava s dva ograničenja – podaci koji nedostaju i nedovoljna duga vremenska serija podataka. Za prvo ograničenje u radu se provodi *bootstrapping* parametarska metoda gdje se istom procjenjuju vrijednosti koje nedostaju. S obzirom na ograničenje povijesne serije podataka kriptovaluta sastavnica indeksa, umjesto matrice kovarijanci, autor primjenjuje poopćeni autoregresijski model uvjetne heteroskedastičnosti (engl. *General Autoregressive Conditional Heteroskedasticity* – GARCH) model te procjenjuje volatilnost vremenskih serija. S aspekta volatilnosti, rezultati usporedbe portfelja s minimalnom varijancom i CRIX-a u prvom slučaju idu u korist MVCRIX portfelja gdje je volatilnost niža, ali je zato kumulativni prinos CRIX indeksa viši. S druge strane, ukoliko se iz analize izbace procijenjene vrijednosti koje su nedostajale, rezultati idu u korist CRIX ideksa gdje je volatilnost niža, a kumulativni prinos viši.

Tržište kriptovaluta se može promatrati i u kombinaciji s tradicionalnim financijskim instrumentima. Trimborn, Li i Härdle (2017) provode jedno takvo istraživanje gdje u postojeći portfelj kriptovaluta, koje imaju pojedinačnu tržišnu kapitalizaciju višu od milijun dolara, uvode tradicionalne instrumente – dionice, sastavnice S&P 100 i DAX30 indeksa, i dionice listane na burzi u Portugalu. U prvom se dijelu provodi analiza unutar uzorka (engl. *in the sample*) gdje se izvode i kompariraju dvije efikasne granice mogućih portfelja bez ograničenja na cijelom uzorku: efikasna granica portfelja kreiranog samo od dionica promatranih tržišta i efikasna granica portfelja kreiranog od dionica i kriptovaluta. Tržište kriptovaluta, u odnosu na tradicionalno tržište, ima daleko niži volumen trgovanja, odnosno puno manju agregatnu tržišnu kapitalizaciju, što može prouzročiti problem likvidnosti. Zbog toga, autori aproksimiraju mjeru likvidnosti kreirajući pokazatelj ukupne vrijednosti prometa (engl. *turnover value*) iz kojeg izvode ograničenje maksimalnog udjela kojeg pojedina kriptovaluta može postići prilikom optimizacije – LIBRO (engl. *LIquidity Bounded Risk-return Optimization*). U drugom se dijelu rada provodi analiza izvan uzorka

[6] https://thecrix.de

(engl. *out of sample*) s optimizacijskim ciljem minimalne varijance. Optimizacija je izvedena prvo samo na dionicama, zatim se u analizu uključuju i kriptovalute. Analiza se provodi sa i bez ograničenja na udjele te se kompariraju performanse portfelja. U oba slučaja, rezultati idu u korist kriptovaluta. Uključivanjem kriptovaluta u portfelj, poboljšava se omjer nagrade i rizika – za bilo koju razinu očekivanog prinosa s efikasne granice, manja je razina preuzetog rizika. Rezultati analize izvan uzorka također idu u korist kriptovaluta. Štoviše, portfelji izvedeni od dionica i kriptovaluta s ograničenjem na udjele, ostvaruju bolje kumulativne prinose od portfelja izvedenih bez ograničenja.

Trimborn et al. (2018) proširuje prethodno istraživanje i u istraživanje uvodi indeks tržišta obveznica (Barclays Capital US Aggregate Indeks) i indeks robnog tržišta (S&P GSCI). Pored toga, osim standardnog optimizacijskog modela srednje vrijednosti i varijance (engl. *meen-variance* – MV), u istraživanje se kao mjera rizika uvodi uvjetna rizičnost vrijednosti (engl. *Conditional Value at Risk* – CVaR). Kao i prethodno, portfelji se formiraju i testiraju na podacima unutar i izvan uzorka s optimizacijskim ciljem maksimalizacije Sharpe omjera, odnosno omjera pinos – CVaR. Za analizu unutar uzorka, formiraju se po četiri portfelja za svaki model, sa i bez ograničenja na udjele: a) portfelj kreiran samo od dionica, b) dionica i kriptovaluta, c) dionica i odabranih indeksa, i d) portfelj dionica, odabranih indeksa i kriptovaluta zajedno. Svi kreirani portfelji unutar uzorka koji u svom sastavu uključuju kriptovalute, bilo s ograničenjem na udjele ili bez njega, ostvarili su bolje rezultate od portfelja kreiranih samo od tradicionalne imovine. Za analizu izvan uzorka se promatra ista formacija portfelja, odnosno modela. Kao i prethodno, rezultati idu u korist kriptovaluta. Svaki portfelj koji uključuje u sastav kriptovalute ostvario je viši kumulativni prinos od portfelja sastavljenog samo od indeksa tradicionalne imovine. Pored toga, ispostavlja se da određeni portfelji koji za mjeru rizika uzimaju CVaR, za nijansu imaju viši kumulativni prinos od standardnog MV modela. Međutim, za razliku od rezultata iz prethodnog istraživanja, portfelji kreirani s ograničenjem ostvarili su niži kumulativni prinos od portfelja bez ograničenja na udjele[7].

[7] Istraživanje u prethodna dva rada se provelo s ograničenjima na tradicionalnu imovinu i kriptovalute što, po mišljenju autora nije najbolje rješenje. Zbog problema likvidnosti, gornje ograničenje udjela je trebalo postaviti samo na kriptovalute jer je odabrana imovina tradicionalnog tržišta kapitala dovoljno likvidna za inicijalne vrijednosti ulaganja prezentirane u radu.

Jedno od najobuhvatnijih istraživanja gdje se razmatraju performanse portfelja kreiranog od kriptovaluta i tradicionalne imovine također se provodi na Humboldtu u Berlinu (Petukhina, Trimborn, Härdle & Elendner, 2018). Postojeće standardne, ali i recentne modele optimizacije autori grupiraju u četiri skupine, odnosno strategije: strategije orijentirane prema riziku (engl. *risk-oriented strategies*), strategije orijentirane prema prinosu (engl. *return-oriented strategies*), strategije orijentirane prema riziku i prinosu (eng. risk-return-oriented strategies) i kombinirane strategije. Odabrane modele autori primjenjuju na portfelje sastavljene od 55 odabranih kriptovaluta i 16 varijabli koju predstavljaju 5 tipova tradicionalne imovine: vlasnički instrumenti, dužnički instrumenti, pariteti fiat valuta, roba i nekretnine. Portfelji se formiraju za razdoblje od tri godine te se analiza performansi portfelja provodi izvan uzorka s dnevnim, tjednim i mjesečnim rebalansom gdje se za treniranje modela koriste podaci od jedne godine[8]. Za usporedbu, promatrana su četiri portfelja tradicionalne imovine bez kriptovaluta: portfelj sastavljen samo od dionica za koji je korišten indeks S&P100 i tri portfelja kreirana različitom metodologijom koji uključuju svu odabranu tradicionalnu imovinu (portfelj s jednako zastupljenom imovinom, portfelj koji maksimizira Sharpe omjer i portfelj s minimalnom varijancom). Također, u analizu je uključena i LIBRO metodologija te su portfelji kreirani sa i bez ograničenja na udjele kako bi se kontrolirao rizik likvidnosti, odnosno ispitao utjecaj ograničenja na performanse portfelja. Performanse svih kreiranih portfelja ukazuju na korisnost uključivanja kriptovaluta u portfelj sačinjen od tradicionalne imovine. Efikasna granica portfelja s kriptovalutama bolje je pozicionirana u odnosu na portfelje bez njih – moguće je kreirati portfelje koji za danu razinu rizika ostvaruju puno viši očekivani prinos. Od svih promatranih portfelja i modela, najviši kumulativni prinos i Sharpe omjer je ostvario portfelj bez ograničenja kreiran modelom maksimalne diverzifikacije, a drugi je po redu model koji maksimizira očekivani prinos. Isti portfelji su ostvarili za nijansu niži kumulativni prinos ukoliko se podignu ograničenja na udjele.

Kriptovalute imaju svoju dinamiku tržišta. Zbog odsutnosti fundamentalne vrijednosti, tržišna se cijena kreće u širokim amplitudama. Lee Kuo Chuen, Guo i Wang (2017) modeliraju sentiment tržišta kao prosječni prinos povijesne serije prinosa i kreiraju portfolio strategiju na izvedenoj sentiment analizi. Performanse kreirane strategije

[8] Mjere uspješnosti diverzifikacije su provedene na ukupnom uzorku podataka.

uspoređuju s performansama CRIX indeksa i portfelja s jednako zastupljenim odabranim kriptovalutama u istom vremenskom periodu. Strategija kreirana na sentiment analizi ostvarila je daleko viši kumulativni prinos od komparativnih portfelja čime se potvrđuje postojanje sentiment dinamike na tržištu kriptovaluta. Također, u istraživanju se provodi optimizacija portfelja deset odabranih kriptovaluta zajedno s tradicionalnom imovinom koju čine dionički indeksi, indeks tržišta nekretnina i zlato. Zbog odsutnosti normalne distribucije prinosa, osim standardnog MV modela, izvodi se efikasna granica primjenom CVaR-a kao mjere rizika te se uspoređuju performanse i alokacija imovine portfelja. Kao i u prethodnim istraživanjima, uključivanje kriptovaluta u portfelj podiže efikasnu granicu mogućih portfelja čime se poboljšava omjer nagrade i rizika. Optimalni portfelj s kriptovalutama ostvario je viši Sharpe omjer u odnosu na portfelj bez kriptovaluta.

U sklopu svog istraživanja, Elendner et al. (2016) razmatra kriptovalute kao jedno zasebno tržište i modelira dva portfelja koristeći deset kriptovaluta s najvišom tržišnom kapitalizacijom. U prvom su portfelju kriptovalute jednako zastupljene, dok su u drugom udjeli definirani tržišnom kapitalizacijom pojedine kriptovalute. Također, u analizu uvodi i CRIX indeks te komparativno prezentira mjere deskriptivne statistike pojedinačno za kriptovalue i mjere rizika izražene kao standardna devijacija, VaR, CVaR i mjeru sistematskog rizika u odnosu na dionički indeks S&P500. Analiza rizika se provodi pojedinačno za promatrane kriptovalute, CRIX indeks i kreirana dva portfelja. Osim navedenog, autor u istraživanje uvodi i tradicionalnu imovinu: paritete fiat valuta, zlato, dioničke indekse, indeks tržišta nekretnina i dužničke instrumente novčanog tržišta, te ispituje pojedinačnu korelaciju kriptovaluta i tradicionalne imovine. Rezultati mjera rizika ukazuju da CRIX indeks nosi niži rizik i to u svim promatranim mjerama, osim u CAPM mjeri sistematskog rizika gdje neke kriptovalute, kao i kreirani portfelji, ostvaruju nižu betu. Korelacijska analiza ukazuje na slabu korelaciju između pojedinačno promatranih kriptovaluta, kao i kriptovaluta i tradicionalne imovine. S obzirom na rezultate, zaključuje se da tržište kriptovaluta doprinosi efikasnosti portfolio alokacije kroz učinkovitiju diverzifikaciju.

Ulogu bitcoina u dinamici portfelja kreiranim od tradicionalne imovine prema kontinentalnoj pripadnosti (EU, SAD i Kina), ispituju Kajtazi i Moro (2018). Tradicionalnu imovinu u ovom slučaju čine indeksi dužničkih instrumenata tržišta

novca i kapitala, indeksi vlasničkih instrumenata, pariteta valuta, zlata, robe, nekretnina i alternativne imovine koji su odabrani sukladno kontinentalnoj pripadnosti. Za razliku od prethodnih radova, autori postavljaju više fleksibilne inicijalne postavke i kreiraju četiri portfelja s različitim ograničenjima: portfelj s jednakim udjelima, portfelj u kojem nije dopuštena kratka prodaja, portfelj u kojem je dopuštena kratka prodaja s gornjom granicom na udjele (bez poluge) i portfelj bez ograničenja za svu imovinu osim za bitcoin (kratka prodaja nije dopuštena). Također, analiza se provodi izvan uzorka sa i bez periodičkog (polugodišnjeg) rebalansa udjela. Za mjeru rizika korišten je CVaR s optimizacijskim ciljem maksimalnog prinosa portfelja – osim za portfelj s jednakim udjelima, a za mjeru performansi Sharpe, Omega i Sortino omjeri. Optimizacija je provedena zasebno za svaku skupinu imovine, npr. portfelj je kreiran samo od EU imovine, a zatim je u analizu uključen i BTC. S obzirom na rezultate, zaključuje se da uključivanje bitcoin kriptovalute u dobro diverzificirani portfelj tradicionalne imovine doprinosi poboljšanju omjera rizika i nagrade. Također, uključivanje BTC-a kao imovine generira i viši kumulativni prinos.

U prethodnim novijim istraživanjima fokus razmatranja je bio portfelj koji uključuje više kriptovaluta. S obzirom da je bitcoin prva kriptovaluta koja je imala neki oblik formiranog sekundarnog tržišta (Mt. Gox je počeo s radom 2010. god.), te s obzirom na rast njegove cijene još 2013., odnosno 2014. godine, bitcoin je već tada privukao zanimanje i znanstvene zajednice te se uključuje u razmatranja kao pojedinačna alternativna imovina u području modeliranja portfelja. Prvi radovi gdje se ispituje njegov doprinos uključivanjem u dobro diverzificirani portfelj tradicionalne imovine provode Briere, Oosterlinck i Szafarz (2015) i Eisl, Gasser i Weinmayer (2015). U prvom se radu analiza provodi unutar uzorka, odnosno primjenom standardnog MV modela izvodi se efikasna granica mogućih portfelja na punom uzorku podataka i interpretira njegov doprinos performansama, odnosno diverzifikaciji portfelja. S obzirom na rezultate prvog rada – odsutnost normalne distribucije prinosa, u drugom se radu provodi analiza izvan uzorka gdje se za mjeru rizika prilikom optimizacije uzima CVaR. Rezultati istraživanja oba rada ukazuju da bi bitcoin trebao biti uključen u portfelj - viši preuzeti rizik kompenziran je višim očekivanim prinosom portfelja, što potvrđuje viši Sharpe omjer.

Carpenter (2016) također ispituje utjecaj uključivanja BTC-a u dobro diverzificirani portfelj tradicionalne imovine, međutim, za procjenu očekivanih prinosa pojedinačne imovine u portfelju koristi model za vrednovanje kapitalne imovine - CAPM (engl. C*apital Asset Pricing Model*). Budući da je za primjenu CAPM-a potrebna statistički signifikantna veza između dodatnih prinosa vrijednosnice i prinosa ukupnog tržišta aproksimiranog indeksom, a relacijom ne uspijeva dokazati vezu BTC-a i promatranog indeksa američkog tržišta kapitala, autor za očekivani prinos koristi srednju vrijednost povijesnih prinosa BTC-a. Također, u slučaju neuobičajeno visokih prinosa BTC-a u promatranom razdoblju, kao npr. u 2014. godini, magnituda prinosa se korigira i svodi na nižu vrijednost kako bi se otklonile ekstremne vrijednosti. Analiza se provodi izvan uzorka na dva seta podataka, sa i bez prinosa BTC-a iz 2014. godine. Rezultati istraživanja su podijeljeni. Performanse portfelja na ukupnom setu podataka idu u korist uključivanja BTC-a u portfelj. Međutim, ukoliko se iz razmatranja isključi razdoblje ekstremno visokih prinosa BTC-a, portfelj je ostvario niži omjer rizika i nagrade u odnosu na portfelj koji nije razmatrao bitcoin kao sastavnicu. S druge strane, ukoliko se ekstremno visoki prinosi korigiraju na niže vrijednosti, optimizacija uključuje BTC kao sastavnicu čime se doprinosi omjeru rizika i nagrade dobro diverzificiranog portfelja tradicionalne imovine.

Jedno od rijetkih istraživanja gdje se potencijalno opovrgavaju rezultati prethodnih istraživanja provode Klein, Hien i Walther (2018). Kako bi ispitali svojstvo tržišta kriptovaluta kao pozitivne komponente prilikom konstrukcije portfelja, autori odabiru indekse tradicionalne imovine: S&P500, MSCI World i MSCI EM50, te za svaki odabrani indeks kreiraju i optimiziraju po jedan zasebni portfelj koji uključuje bitcoin, odnosno zlato. Cilj optimizacije je portfelj s minimalnom varijancom. Usporedbom rezultata portfelja autori zaključuju da bitcoin nema investicijske karakteristike poput zlata. Portfelj koji uključuje bitcoin, npr. S&P 500/bitcoin, sadrži malu proporciju bitcoina, za razliku od portfelja S&P 500/zlato gdje je veći udio zlata u portfelju. Omjer rizika mjerenog standardnom devijacijom i CVaR-om i očekivanog prinosa portfelja, također više ide u korist zlata kao alternativne imovine za zaštitu portfelja. Osim bitcoina, autori u portfelje uključuju i CRIX indeks kao pojedinačnu varijablu te ističu da uključivanje indeksa može reducirati volatilnost i za nijansu popraviti očekivani prinos portfelja. Međutim, s obzirom da udio bitcoina prevladava u CRIX

ideksu, ostali rezultati značajno ne odstupaju od prethodnih, pa se zaključuje, da u komparaciji sa zlatom, CRIX indeks ne doprinosi diverzifikaciji rizika portfelja.

Osim istraživanja Elendner et al. (2016), svi prethodno prezentirani radovi ispituju reakcije uključivanja jedne ili više kriptovaluta u dobro diverzificirani portfelj sastavljen od nekog oblika tradicionalne, odnosno alternativne imovine. Međutim, s obzirom na njihov broj, sekundarno se tržište kriptovaluta može promatrati kao jedna zasebna cjelina te je iz tog razloga poželjno ispitati mogućnost konstrukcije efikasnog portfelja sačinjenog isključivo od kriptovaluta s različitim alokacijskim ciljevima, npr. portfelj s najvišim prinosom, minimalnom varijancom, maksimalnim Sharpe omjerom itd. Jedan od prvih radova gdje se analizira mogućnost optimizacije i diverzifikacije rizika tržišta kriptovaluta provodi Liu (2018). U radu se kreira šest portfelja i provode standardni optimizacijski ciljevi: minimizacija varijance, jednaka kontribucija rizika (engl. *risk parity*), maksimalizacija očekivanog prinosa, maksimalizacija Sharpe omjera i maksimalizacija funkcije korisnosti. Osim toga, za ocjenu uspješnosti optimizacije, u radu se izvodi i portfelj s jednako zastupljenim kriptovalutama, kao i Sharpe omjer za svaki pojedinačni portfelj. Analiza je provedena izvan uzorka s ograničenjem na kratku prodaju i rebalansom svakih 30 dana na temelju povijesnih podataka vremenske serije od godine dana (360 dnevnih promatranja). Promatrani uzorak sačinjava deset kriptovaluta čija je tržišna kapitalizacija veća od jedne milijarde dolara za razdoblje od četiri godine, kolovoz 2015. god. – travanj 2018. god. Rezultati su u suprotnosti s očekivanim. Osim portfelja s minimalnom varijancom, niti jedan od optimizacijskih modela nije zadovoljio svoj cilj. Najviši kumulativni prinos ostvario je portfelj s optimizacijskim ciljem maksimalizacije funkcije korisnosti, a najviši Sharpe omjer portfelj s jednako zastupljenim udjelima, pa autor zaključuje da na tržištu kriptovaluta sofisticirani modeli ne mogu pobijediti performanse portfelja s jednako zastupljenim udjelima – promatrajući ih s aspekta racionalnog investitora.

Slično istraživanje mogućnosti optimizacije i diverzifikacije rizika na tržištu kriptovaluta provode i Brauneis i Mestel (2018). Za razdoblje od tri godine, siječanj 2015. god. do prosinac 2017. god., autori inicijalno prikupljaju podatke od 500, a zatim od 20 najlikvidnijih kriptovaluta te kreiraju više različitih portfelja s pripadajućim optimizacijskim ciljevima: minimizacija varijance, maksimalizacije očekivanog prinosa i maksimalizacija Sharpe omjera. Autori razmatraju i nekoliko portfelja s kreirane

efikasne granice koji se nalaze u rasponu između portfelja s minimalnom varijancom i najvišim očekivanim prinosom. Za mjeru uspješnosti modela, također se kreira portfelj s jednako zastupljenim udjelima, Sharpe omjer, ali se koristi i CRIX indeks za usporedbu njihovih performansi. Analiza se provodi izvan uzorka s inicijalnim setom promatranja od 183 povijesna dnevna prinosa koja služe za procjenu parametara s dnevnim, tjednim i mjesečnim rebalansom. Osim inicijalnih postavki, u radu se provodi i alternativna parametrizacija. Drugim riječima, ispituju se i performanse portfelja s različitom duljinom uzorka inicijalnog seta podataka koji služi za treniranje modela, koristi se i više različitih vremenskih intervala za rebalans i mijenja broj sastavnica portfelja. Portfelji sekundarne parametrizacije ne odstupaju od rezultata portfelja s inicijalnim postavkama tako da oni nisu dalje razmatrani. Dobiveni rezultati potvrđuju prethodno istraživanje. Najviši očekivani prinos, kao i Sharpe omjer, je ostvario portfelj s jednako zastupljenim udjelima u portfelju, bez obzira na frekvenciju rebalansa. S obzirom na tabelarni prikaz deskriptivne statistike Sharpe omjera, autori ističu da je minimalna vrijednost Sharpe omjera portfelja s jednakim udjelima zapravo veća od 75% svih rezultata Sharpe omjera koji su dobiveni optimizacijskim modelima. Zaključuje se da je portfelj s jednakim udjelima najbolji izbor prilikom kreiranja i modeliranja portfelja na tržištu kriptovaluta.

Analizu uspješnost sofisticiranog modela optimizacije portfelja u odnosu na pasivni pristup jednakih udjela na tržištu kriptovaluta provodi i Platanakis, Sutcliffeb i Urquhartc (2018). Za razliku od prethodnih radova, analiza je provedena na tjednim opservacijama za samo četiri kriptovalute: bitcoin, litecoin, ripple i dash za razdoblje od veljače 2014. god. do siječnja 2018. god. Korišteni optimizacijski cilj je bio maksimalizacije funkcije korisnosti s ograničenjem na kratku prodaju, a za ocjenu uspješnosti su korišteni Sharpe i omega omjeri. Analiza je provedena izvan uzorka s dva vremenska perioda za treniranje modela: 26 i 52 tjedna. S obzirom na rezultate mjera performansi koji ne favoriziraju niti jedan od modela, autori zaključuju da je pasivna (naivna) diverzifikacija s jednakim udjelima bolji odabir za konstrukciju portfelja na tržištu kriptovaluta.

1.4. Korištene metode istraživanja

U radu se želi konstruirati, egzaktno izmjeriti, ocijeniti i opisati performanse dva portfelja sastavljena od kriptovaluta. Vrijednost prvog portfelja bit će modelirana i izražena u vrijednosti bitcoina kao vodeće varijable na tržištu kriptovaluta, a vrijednost drugog portfelja bit će modelirana i izražena u paritetu s dolarom. Sastavnice oba portfelja određene su prema ukupnim rezultatima metrike fundamentalnih pokazatelja dostupnim na stranicama CoinGecko. Metrika trenutno prati razvoj programskog koda na platformama: GitHub, GitLab i Bitbucket, te potporu zajednice preko socijalnih mreža: Facebook, Twitter, Reddit i Telegram. Prvih dvadeset kriptovaluta koje kumulativno ostvaruju najviše bodova, odabrane su kao sastavnice oba portfelja (izuzev prvog portfelja gdje je bitcoin isključen jer predstavlja mjernu jedinicu vrijednosti): bitcoin (BTC), ethereum (ETH), eos (EOS), xrp (XRP), bitcoin cash (BCH), litecoin (LTC), neo (NEO), monero (XMR), cardano (ADA), stellar (XLM), dash (DASH), zcash (ZEC), binance coin (BNB), iota (MIOTA), waves (WAVES), qtum (QTUM), dogecoin (DOGE), 0x (ZRX), nem (XEM) i ethereum classic (ETC). Performanse portfelja izraženom u dolarskoj vrijednosti usporedit će se s performansama CRIX indeksa u istom razdoblju promatranja. Trenutne sastavnice indeksa su: bitcoin (BTC), ethereum (ETH), xrp (XRP), bitcoin cash (BCH) i eos (EOS). Korišteno razdoblje promatranja koje pokriva sve odabrane kriptovalute je od 1. listopada 2017. god. do 1. kolovoza 2019. god., što čini uzorak od ukupno 669 dnevnih opservacija, odnosno 668 dnevnih prinosa.

Modeliranje portfelja se provodi primjenom koncepta moderne teorije portfelja (Markowitz, 1952). S obzirom na mogućnosti programskog rješenja, analiza je podijeljena u dva koraka. U prvom dijelu rada optimizacijski modeli se provode unutar uzorka (engl. *in the sample*), kreira se efikasna granica, analizira dinamika promjene udjela sukladno promjeni tolerancije prema riziku i interpretiraju performanse mogućih portfelja. U drugom dijelu rada isti modeli se provode izvan uzorka (engl. *out of sample*). Razdoblje promatranja dijeli se na dva seta podataka. Prvi set podataka služi za treniranje modela sukladno optimizacijskom cilju, a drugi dio za testiranje modela prema prethodno dobivenim parametrima na podacima koji su nepoznati modelu. U radu će se provesti tri optimizacijska cilja: portfelj s minimalnom varijancom, portfelj maksimalnim prinosom i portfelj s maksimalnim Sharpe omjerom.

Jednako tako, prezentirat će se i rezultati portfelja s jednakim udjelima da bi se usporedile i prezentirale moguće prednosti ili nedostaci takve strategije. Također, rezultati portfelja izraženom u dolarskoj vrijednosti usporedit će se s rezultatima portfelja koji predstavljaju standard usporedbe, čime će se ispitati mogućnost konstrukcije portfelja koji ostvaruje bolje rezultate od rezultata tržišta. S obzirom na rezultate prethodnih istraživanja Briere et al. (2015) i Lee Kuo Chuen et al. (2018) i odsutnost normalne distribucije prinosa, osim standardne devijacije, za mjeru rizika koristit će se i uvjetna rizičnost vrijednosti (engl. *Conditional Value at Risk* – CVaR), tako da je ukupno provedeno pet optimizacijskih strategija.

Prilikom izrade ovog rada, korištene su različite znanstvene metode. Tako će se metodom analize i metodom deskripcije raščlaniti, opisati i objasniti kompleksni proces transakcije na Bitcoin transakcijskom sustavu. Pored toga, metodom analize zajedno s metodom komparacije, definirat će se prednosti, odnosno nedostaci pojedinačno promatranih kriptovaluta i rezultata pojedinačno promatranih portfelja, a metodom sinteze tumačit će se njihovi zajednički rezultati. S obzirom na promatrane varijable, induktivnom metodom će se uopćiti ukupno stanje tržišta kriptovaluta u promatranom periodu. S druge strane, deduktivnom metodom izvest će se pojedinačni zaključci promatranih kriptovaluta na tržištu u kontekstu prinosa, rizika, svojstva lanca blokova itd. Za obradu podataka je korišten „R“ program, a najčešće korišteni paket je ROI (R *Optimization Infrastructure*). Glavne metode korištene u radu su matematičko-statistička metoda gdje se s obzirom na optimizacijski cilj koriste različiti rješavači (solveri): za portfelj s minimalnim rizikom i maksimalnim Sharpe omjerom koristi se metoda kvadratnog programiranja i paket „quadprog”. Za portfelj s maksimalnom očekivanim prinosom koristi se metoda linearnog programiranja i paket „glpk”. Osim spomenutih, u radu su korištene metode dokazivanja, odnosno opovrgavanja kojima će se potvrditi ili odbaciti predložene hipoteze u radu, te metode klasifikacije i kompilacije.

1.5. Struktura i znanstveni doprinos rada

Plan istraživanja ovog rada je formiran sukladno postavljenim ciljevima, te je strukturiran u devet dijelova. U prvom dijelu rada, UVODU, definiran je problem i predmet istraživanja, te su postavljene znanstvene hipoteze sukladno svrsi i ciljevima

koje se žele postići, odnosno na koje se želi dati odgovor. Jednako tako, dan je pregled rezultata dosadašnjih istraživanja, te se opisuje i korištena znanstvena metodologija, kao i struktura rada sa očekivanim znanstvenim doprinosom.

S obzirom da se u radu obrađuje nova vrsta digitalne imovine, u drugom dijelu rada, UVOD U KRIPTOVALUTE, dan je povijesni presjek prvih oblika alternativnih valuta, kako bi se utvrdila veza između recentnih istraživanja, ali i dostignuća na području alternativnih valuta i kriptovaluta koje su predmet istraživanja ovog rada. Također, s obzirom da Bitcoin transakcijski sustav predstavlja prvu kriptovalutu, u nastavku se opisuju karakteristike njegova programskog protokola, kao i specifičnost nastanka.

U trećem dijelu rada, KLASIFIKACIJA KRIPTOVALUTA, po prvi puta je dana sveobuhvatna podjela i klasifikacija kriptovaluta, kako bi se strogo definirale granice između različitih vrsta kriptovaluta. Jednako tako, u nastavku se obrađuje ekonomski okvir kriptovaluta, gdje se kroz kontekst funkcije novca interpretiraju njihove prednosti i nedostaci.

Kriptovalute su nova prenosiva digitalna imovina te kao takva ne ulazi u postojeće okvire definicije tradicionalnih financijskih instrumenata. Međutim, njihova struktura je omogućila transfer kapitala od štediša prema novim inovativnim tvrtkama kojima je kapital potreban, putem mehanizma grupnog financiranja, što predstavlja primarno tržište. Razvojem primarnog tržišta povećao se i broj platformi koje pružaju mogućnost njihove razmjene, čime je stvoren jedan novi ekosustav primarnog i sekundarnog tržišta kriptovaluta. Sukladno tome, u četvrtom dijelu rada, KLASIFIKACIJA TRŽIŠTA KRIPTOVALUTA, po prvi puta se opisuje sveobuhvatna podjela infrastrukture primarnog i sekundarnog tržišta kriptovaluta. Definiraju se prednosti i rizici ulaganja u kriptovalute, te se usporedbom ističu prednosti i nedostaci različitih modela financiranja.

U petom dijelu rada, REGULATIVNI OKVIR KRIPTOVALUTA, razmatra se dosadašnji napredak, odnosno trenutno korišteni regulatorni okvir tržišta kriptovaluta na području Europske unije, Sjedinjenih Američkih Država i Republike Hrvatske. Daje se tumačenje Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala i tumačenje Direktive elektroničkog novca i Direktive o platnim uslugama EU-a, o

klasifikaciji kriptovaluta kao financijskih instrumenata, odnosno digitalnog novca, čime se želi ukazati na dodatni rizik koji proizlazi iz nedostataka jednoznačne regulacije tržišta kriptovaluta.

Šesto poglavlje, POČELA BITCOIN TEHNOLOGIJE, obrađuje osnovne elemente infrastrukture Bitcoin transakcijskog sustava. Definira se važnost kriptografskih primitiva u funkciju konsenzus algoritma na kojemu je građena glavna distinkcija između drugih oblika digitalnih valuta i kriptovaluta. Jednako tako, prezentira se konstrukcija bloka transakcija svojstvena blockchain tehnologiji, čime se dodatno želi približiti nova tehnologija. Također, s obzirom na prednosti, odnosno nedostatke javnog blockchaina, uspoređuju se različite blockchain arhitekture koje su rezultat prilagodbe blockchain tehnologije potrebama korporativnog okruženja.

Sedmo poglavlje, PRAKTIČNE IMPLIKACIJE BLOCKCHAIN TEHNOLOGIJE, donosi prikaz dosadašnjih istraživanja, ali i praktičnih implikacija primjene blockchain tehnologije unutar područja računovodstvenih i financijskih poslova. Isto tako, u nastavku se kroz zasebno potpoglavlje po prvi puta obrađuje pojam decentraliziranih otvorenih financija, koje predstavljaju potpuno novu kategoriju financijskih usluga temeljenih na blockchain tehnologiji. Prezentiraju se prednosti, ali se i razmatraju prisutni rizici koji se dovode u vezu s novim financijskim uslugama.

Korištena metodologija je prikazana u osmom poglavlju METODOLOGIJA RADA. Kroz poglavlje se opisuju korištene formulacije optimizacijskih ciljeva temeljenih na modernoj teoriji portfelja koja predstavlja jedan od najviše korištenih modela za rješavanje problema alokacije imovine i definiranje optimalnog ulaganja. S obzirom na nedostatke optimizacije portfelja koji razmatra varijancu prinosa kao rizik, kroz poglavlje se prezentira metodologija uvjetne rizičnosti vrijednosti kao alternativna mjera rizika. Također, da bi se usporedili rezultati različitih alokacijskih modela, u nastavku su opisane korištene mjere za ocjenu uspješnosti pojedine optimizacijske strategije primijenjene na različitim alokacijskim modelima. Na kraju poglavlja, opisuje se odabir uzorka kriptovaluta kao inicijalnih sastavnica portfelja.

Rezultati provedenog istraživanja su prezentirani i interpretirani u devetom poglavlju REZULTATI. Sukladno postavljenim ciljevima i hipotezama rada, te s obzirom na

provedenu metodologiju, rezultati se prezentiraju kroz četiri potpoglavlja. Kroz prvo i drugo potpoglavlje prezentiraju se rezultati koji se odnose na prvu postavljenu hipotezu rada. U drugom i trećem potpoglavlju obrađuju se rezultati kojima se potvrđuje, odnosno odbacuje druga hipoteza rada. Također, osim interpretacije rezultata koji su neposredno vezani za postavljene hipoteze rada, kroz poglavlje se daju i sekundarna razmatranja rezultata, kojima se dodatno želi skrenuti pozornost na uočene obrasce, te kojima se dodatno doprinosi području ispitivanja investicijskih mogućnosti na tržištu kriptovaluta.

Na kraju, u ZAKLJUČKU, kao desetom dijelu ovog rada, istaknute su najvažnije primarne, ali i sekundarne spoznaje ovog istraživanja, te su sugerirani mogući smjerovi daljnjeg znanstvenog rada u području izučavanja investicijskih mogućnosti na tržištu kriptovaluta.

S obzirom na smjer razvoja tržišta kriptovaluta – kriptovalute se kotiraju u paritetu s bitcoinom zbog ograničenog pristupa fiat novca, bitcoin je postao daleko najrasprostranjenija kriptovaluta na njihovom primarnom, odnosno sekundarnom tržištu. Osim sekundarnih tržišta, bitcoin je i postao daleko najviše prihvaćena kriptovaluta u svakodnevnoj primjeni kao sredstvo razmjene. Navedeno je rezultiralo njegovom sve većom potražnjom i optimističnim cjenovnim projekcijama. Zbog toga se u ovom radu kvantificiraju odnosi kriptovaluta izraženi u vrijednosti bitcoin kriptovalute što do sada nije bilo predmet istraživanja u domaćoj i inozemnoj znanstvenoj i stručnoj literaturi, i čini prvi dio znanstvenog doprinosa ovog rada. Ukoliko se ispostavi da je moguće konstruirati jedan takav portfelj koji ostvaruje pozitivne rezultate u smislu agregatne količine bitcoina investitori, čiji je cilj multipliciranje bitcoina, bi mogli revidirati svoje postojeće strategije i prilagoditi modele rezultatima istraživanja.

Svojstvo otvorenog koda Bitcoin sustava rezultiralo je postojanju više od pet tisuća kritptovaluta s kojima se trguje na 348 različitih mjenjačnica, odnosno burzi. Da bi se kreirala jedna kriptovaluta i listala na nekoj od npr. decentraliziranih burzi, ponekad nije potrebno više od pet minuta – ovisno na kojoj se platformi kreira. Međutim, iako tako kreirana kriptovaluta postiže neku inicijalnu cijenu, to ne znači da ona ima svoju stvarnu fundamentalnu vrijednost. U svrhu procjene njene vrijednosti, potrebno je

razmotriti fundamentalne indikatore, poput razvoja i svojstva programskog koda, veličinu zajednice koja ju podržava, broj mrežnih čvorova itd. Zbog toga se u ovom radu konstruira portfelj sastavljen od dvadeset kriptovaluta koje su najviše rangirane sukladno dostupnoj metrici fundamentalnih indikatora. Rezultati takvog portfelja usporedit će se s rezultatima CRIX indeksa čiji je cilj repliciranje kretanja tržišta. Navedeni pristup do sada nije bio predmet istraživanja u domaćoj i inozemnoj znanstvenoj i stručnoj literaturi, a to čini drugi dio znanstvenog doprinosa ovog rada. Ukoliko se ispostavi da je moguće pobijediti tržište primjenom fundamentalnih indikatora, investitori bi mogli uvažiti i praktično implicirati rezultate istraživanja, odnosno ograničiti inicijalnu konstrukciju i daljnje modeliranje portfelja na kriptovalute koje imaju pozitivne vrijednosti fundamentalnih pokazatelja.

Osim prethodnih primarnih znanstvenih doprinosa koji proizlaze iz inicijalno postavljenih hipoteza rada, u radu su obrađene teme u kojima se po prvi puta daju stroge klasifikacije infrastrukture tržišta blockchain imovine. Tako je kroz shematski prikaz klasifikacije financijske imovine na blockchainu prezentirana, do sada, najobuhvatnija podjela kriptovaluta prema njihovoj svrsi, zakonskim ograničenjima i karakteristikama koje proizlaze iz različitih blockchain arhitektura. Jednako tako, kroz shematski prikaz tržišta kriptovaluta i tržišta token vrijednosnica, te njihov opis, daje se holistički pregled svih trenutnih primarnih i sekundarnih tržišta povezanih sa financijskom imovinom kreiranom na blockchain tehnologiji. Na kraju, s obzirom na provedenu metodologiju i širinu kreiranih alokacijskih modela, dodatnim razmatranjem rezultata se interpretiraju uočene prednosti i nedostaci optimizacijske strategije, s ciljem odabira mjere rizika adekvatne za tržište kriptovaluta. Provedeni metodološki pristup do sada nije bio razmatran na način na koji je proveden u ovom radu, što čini sekundarni znanstveni, ali i praktični, doprinos ovog rada unutar područja ispitivanja investicijskih mogućnosti na tržištu kriptovaluta.

2. UVOD U KRIPTOVALUTE

2.1. Povijest i klasifikacija alternativnih valuta

Povijesni razvoj digitalne tehnologije utjecao je i na razvoj inovativnih sustava plaćanja od kojih se mnogi baziraju na platformama poput mobilnih telefona, interneta i digitalnih kartica za pohranu podataka. Zajednička karakteristika svih trenutnih sustava digitalnih transakcija je njihova svrha u kontekstu infrastrukture za transakcije fiat novca, ali samo u digitalnom obliku. Međutim, osim digitalnog (elektroničkog) oblika fiat novca, postoje i drugi oblici alternativnog digitalnog, ali i materijalnog novca koji se klasificira prema različitim svojstvima poput svojstva pripadnosti – tko ga je kreirao, zatim svojstva postojanja njihove fundamentalne vrijednosti, svojstva zemljopisne pripadnosti itd. Iako se alternativni digitalni novac često opisuje kao virtualni kada se govori o valutama na temelju elektroničkog medija, pojam „virtualno“ ima negativnu konotaciju. „Virtualno“ ukazuje na nešto što je „naizgled stvarno“, ali nije baš „stvarno“, kada se odnosi na valutu koja se sprema u „digitalni“ ili elektronički registar. Međutim, valute koje se često opisuju kao „virtualne“ su vrlo „stvarne“ upravo zbog toga što one postoje u nekom digitalnom, odnosno elektroničkom registru (Pak Nian i Lee Kuo Chuen, 2015). Stoga se u nastavku rada prilikom opisivanja alternativnih oblika novca, neutralnijem pojmu *digitalne valute* daje prednost u odnosu na pojam *virtualne valute*.

Alternativne valute predstavljaju valute koje mogu služiti kao sredstvo razmjene, ali ne ulaze u kategoriju tradicionalnog fiat novca. Povijesno gledano postoje različiti oblici alternativnih valuta koje su prema Hileman (2014) klasificirane u dvije osnovne kategorije: valute koje su opipljive, odnosno imaju neki fizički oblik i digitalne valute. Vrijednost opipljivih valuta, usko povezanih s robnim novcem, prvenstveno proizlazi iz njihove oskudnosti i praktične, odnosno nemonetarne korisnosti i dijele se na:

a) Valute koje imaju fundamentalnu vrijednost;

   Ovaj oblik uključuje, na primjer, različite metale i cigarete u Berlinu nakon drugog svjetskog rata, dok su nešto suvremeniji primjeri telefonske i pametne kartice gotovinske vrijednosti. Nisu vezana za određeno zemljopisno područje, nisu rezultat niti predmet upravljanja monetarne politike, i ono najvažnije njihova vrijednost je stvarna, a ne apstraktna.

b) Tokeni;

Za razliku od prethodnog oblika, tokeni imaju manju intrinzičnu vrijednost jer je njihova upotreba više specifična i obično je ograničena nekim društvenim ugovorom ili sporazumom iz kojeg proizlazi njihova vrijednost prilikom razmjene robe. Povijesni primjeri tokena se mogu naći u Velikoj Britaniji u razdoblju od sedamnaestog do devetnaestog stoljeća, kao i tokeni koji su nastali kao zamjena za državnu valutu za vrijeme trajanja kriznog razdoblja Velike depresije. Nešto suvremeniji primjeri tokena su lokalne valute, odnosno valute zajednica nastale kao potpora lokalnoj ekonomiji, trgovini i proizvodnji. U tu skupinu ulaze tokeni poput Brixton i Bristol funte koji se koriste u Engleskoj, BerkShares valuta koja je u cirkulaciji u regiji Berkshire u državi Massachusetts u SAD-u i Salt Spring dolar u Kanadi.

S druge strane, alternativne digitalne valute se dijele na: centralizirane digitalne valute i distribuirane i/ili decentralizirane digitalne valute.

c) Centralizirane digitalne valute;

Praktični primjeri centraliziranih digitalnih valuta su bodovi vjernosti financijskih, telekomunikacijskih ili maloprodajnih kompanija, zračne milje od zrakoplovnih tvrtki, Linden dolar u virtualnom svijetu kompjuterske videoigre Second Life, zlato iz kompjuterske videoigre World of Warcraft – WOW itd. To su zatvoreni sustavi s transakcijama između entiteta unutar sustava. Drugim riječima, Linden dolar je jedino moguće koristiti unutar matične virtualne igre. S druge strane, digitalne valute poput Flooz-a i Beenz-a, koje su danas neaktivne, bile su otvoreni sustavi i pružale su mogućnost transakcija s drugim entitetima izvan sustava. S obzirom da su kreirane s namjerom da zauzmu poziciju internet valute, s njima je bilo moguće obavljati online kupovinu u različitim trgovinama koje su ih prihvaćale.

d) Distribuirane i/ili decentralizirane digitalne valute;

Ova skupina uključuje kriptovalute poput bitcoina, litecoina i ethereuma. Njihovo upravljanje je uglavnom decentralizirano i provodi se putem konsenzusa zajednice koja podržava valutu. Kako ne postoji formalno tijelo odgovorno za aktivnosti transakcijskog sustava, kriptovalute spadaju izvan okvira tradicionalnih propisa.

Bez obzira što kriptovalute ne ulaze u postojeće okvire tradicionalnih sustava, to nije utjecalo na njihovu egzistenciju, razvoj i svakodnevnu primjenu, pa tako najstarija kriptovaluta – bitcoin postoji već deset godina.

Zbog sve više upita od strane akademske zajednice, novinara, građana, poslovnih subjekata itd. što zapravo predstavljaju kriptovalute, Europska centralna banka (u nastavku teksta ECB), kao formalna institucija, definira digitalne alternativne valute kao vrstu nereguliranog, digitalnog novca, kojeg izdaju i kojeg najčešće kontroliraju njegovi programeri-osnivači, koristi se i prihvaćen je između članova određene virtualne zajednice (ECB, 2012). Osim definicije, ECB daje i klasifikaciju alternativnih digitalnih valuta u kontekstu interakcije sa stvarnim novcem, odnosno realnom ekonomijom, što rezultira interakcijom kroz dva osnovna kanala: a) interakcija sa realnom ekonomijom putem burzi alternativnih digitalnih valuta; b) interakcija u smislu mogućnosti direktne kupnje stvarne robe i usluga. Uzimajući navedeno u obzir, ECB promatra digitalne valute kroz tri osnovna tipa:

a) Zatvorene digitalne valute;

   Ovaj tip digitalnih valuta gotovo da i nije povezan s realnom ekonomijom, stvorene su za virtualni svijet kao što su kompjuterske videoigre. Mogu se potrošiti samo kupnjom virtualne robe i usluga ponuđenih unutar virtualne zajednice i teoretski se s njim ne može trgovati izvan virtualne zajednice. Primjer ovog tipa digitalnih valuta je već spomenuto zlato kompjuterske videoigre WOW.

b) Digitalne valute s jednosmjernim protokom;

   To su valute koje se mogu kupiti izravno fiat novcem po određenom tečaju, ali se ne mogu konvertirati natrag u izvornu fiat valutu. Nakon njihove kupnje, s njima je moguće kupovati virtualna dobra i usluge, ali i stvarnu robu i usluge ukoliko za to postoji infrastruktura. Primjeri ovog tipa valuta je danas neaktivna digitalna valuta Facebook Credits i Nintendo bodovi.

c) Digitalne valute s dvosmjernim protokom;

   Ovaj tip digitalnih valuta je u potpunosti povezan s realnom ekonomijom. Moguće ih je kupiti, ali i prodati za fiat novac prema važećem tečaju. Omogućuju kupnju virtualnih i stvarnih dobara i usluga. Primjer ovog tipa je digitalna kriptovaluta bitcoin.

Osim spomenute klasifikacije prema interakciji s realnom ekonomijom, ECB naglašava i razliku između opisanih digitalnih valuta i elektroničkog fiat novca. Prema definiciji, elektronički novac je novčana vrijednost koja čini novčano potraživanje prema izdavatelju, pohranjena u elektroničkom obliku i izdana nakon primitka novčanih sredstava u iznosu koji nije manji od izdane novčane vrijednosti te je prihvaćena kao sredstvo plaćanja od strane drugih subjekata osim izdavatelja (ECB, 2012). Iako se alternativni digitalni novac može dovesti u vezu s elektroničkim novcem, ECB naglašava jednu značajnu razliku. U shemi elektroničkog novca veza između monetarne vrijednosti tradicionalnog formata novca je očuvana i ima pravnu osnovu, jer su pohranjena sredstva izražena u istoj obračunskoj jedinici (npr. američki dolari, euro itd.). S druge strane, u shemi alternativne digitalne valute obračunska jedinica se mijenja u tu novu digitalnu valutu sukladno njihovom paritetu, pa se, u slučaju buduće obrnute konverzije, otvara pitanje valutnog rizika, jer se vrijednost digitalne valute obično temelji na vlastitoj potražnji i ponudi. Pored toga, ECB navodi i rizik konverzije, kao i pitanje stručnosti i profesionalnosti osnivača digitalne valute, što obično nisu financijske institucije.

Prethodne podjele ECB-a definiraju kriptovalute prema odnosu s realnom ekonomijom, odnosno stvarnim novcem. S druge strane, i same kriptovalute se mogu klasificirati kroz nekoliko različitih tipova. Izvorni i prvi transakcijski sustav koji je inkorporirao tehnologiju lanca blokova putem programskog koda je svakako Bitcoin, pa je u početku i klasifikacija kriptovaluta bila puno jednostavnija. Postojao je bitcoin kao vodeća kriptovaluta i alternativne kriptovalute (engl. *altcoins*) koje su nastale forkanjem - svojevrsnim kloniranjem izvornog programskog koda, ali bez prethodno zapisanih transakcija, i njihovim puštanjem u javnost s unaprijeđenom verzijom protokola. Takve alternativne kriptovalute su imale neku prednost u odnosu na inicijalni Bitcoin sustav, npr. više transakcija u sekundi, bolja sigurnost, anonimnost itd. U tu skupinu ulaze kriptovalute poput litecoina, dogecoina, primecoina i peercoina. S druge strane, 30. srpnja 2015. godine u javnost je puštena decentralizirana kompjuterska platforma Ethereum koja, za razliku od Bitcoin platforme, omogućava programerima da razvijaju i objave decentralizirane aplikacije. Ethereum kompjuterska platforma koristi ether (ETH) kriptovalutu za transakcijske naknade i usluge koje se koriste na platformi. S obzirom na mogućnosti nove blockchain infrastrukture, vrlo brzo nakon puštanja u javnost, mlade i inovativne

tvrtke financiraju svoje ideje putem inicijalne ponude tokena (engl. *initial coin offering*) i kreiraju prve decentralizirane aplikacije (engl. *decentralized applications* – DAPPS). Da bi decentralizirane aplikacije bile potpuno operativne, najčešće moraju koristiti drugu kriptovalutu tzv. token koji je također kreiran i koristi Ethereumu platformu za transakcije. Danas, pored Ethereuma, postoji niz drugih kompjuterskih platformi koje omogućuju stvaranje decentraliziranih aplikacija kao što su: Eos, Neo, Stellar, Nem, Tron itd. Može se reći da je glavna razlika između alternativnih kriptovaluta i tokena u njihovoj tehničkoj izvedbi. Prve su zasebne kriptovalute s vlastitim blockchainom, dok tokeni djeluju na nekom od već razvijenih blockchaina koji pruža mogućnost kreiranja decentraliziranih aplikacija.

2.2. Razvoj kriptovaluta

Povijest digitalnog oblika novca koji koristi kriptografske algoritme počiva na dva temelja: razvoj distribuiranih baza podataka i razvoj različitih sistema elektroničkog novca. U ranoj fazi istraživanja, navedena područja nisu bila previše povezana, nego se povezuju kroz istraživanja i napredak kriptografije, na što je posebno imao utjecaj razvoj asimetrične kriptografije. Bitcoin transakcijski protokol je zapravo osigurao vezu koja je nedostajala između ta dva polja istraživanja kako bi se kreirala decentralizirana kriptovaluta. Drugim riječima, Bitcoin protokol je implementirao najbolje dijelove iz oba područja u jedan transakcijski sustav kakav je poznat danas. Također, s porastom popularnosti bitcoin kriptovalute, sve je više istraživanja u području distribuiranih baza podataka i elektroničkih platnih sustava (Judmayer, Stifter, Krombholz i Weippl, 2017). Sukladno Franco (2015), u nastavku se prezentira sublimacija prvih radova koje se odnose na istraživanja u polju digitalnih valuta osiguranih kriptografijom, preteči današnjih kriptovaluta.

Povijest kriptovaluta započinje 1980-ih godina objavom istraživanja Davida Chauma kojeg obično nazivaju izumiteljem sigurnog digitalnog novca (Chaum, Fiat i Naor 1990), (Chaum, 1985) i (Chaum, 1983). David Chaum je kriptograf koji je objavio revolucionarne radove na polju anonimne komunikacije, sustava glasovanja i digitalnih valuta. U svom radu na sustavu anonimnih plaćanja Chaum predlaže novu kriptografsku shemu s ciljem sakrivanja sadržaj poruke prije digitalnog potpisa (engl. *blind signature*), pri čemu se takav slijepi potpis može se javno provjeriti kao i

uobičajeni digitalni potpis. Sustav plaćanja omogućava korisnicima da od banaka dobiju anonimne jedinice valute-tokene, a svaki token predstavlja fiksni iznos novca. Prilikom kreiranja tokena, korisnik bi banci prezentirao skriveni nasumični serijski broj kojeg bi banka digitalno potpisala i teretila korisnikov račun u banci za odgovarajući iznos. Tako potpisan token predstavlja iznos koji može otkupiti bilo tko u banci koja je potpisala isti. Drugim riječima, digitalno potpisani nasumično birani serijski broj koji prethodno nije bio poznat niti banci, niti korisniku, predstavlja određenu količinu novca s kojim korisnik može kupiti proizvode i usluge od trgovaca. Nakon toga, trgovci bi predali tokene banci koja bi provjerila je li serijski broj ispravno digitalno potpisan te bi, u svojoj bazi utrošenih serijskih brojeva, provjerila da serijski broj još nije potrošen. Ukoliko bi sve bilo u redu, banka bi doznačila sredstva trgovcu, ili bi izdala nove tokene na isti iznos. Povlačenje sredstava i trošenje istih se ne bi moglo povezati jer banka ne zna tko je izvorni vlasnik serijskog broja jer je broj slijepo potpisan. Chaumov digitalni novac omogućio je korisnicima potrošnju jedinca valute bez mogućnosti praćenja. U kasnijoj fazi poboljšava ideju dopuštajući transakcije koje se događaju izvan mreže (engl. *offline*) i uključujući mehanizam detekcije duple potrošnje. U tom slučaju korisnik mora banci poslati ne samo nasumični serijski broj, već i pažljivo generiran podatak koji uključuje nasumični serijski broj i neke skrivene, ali osobne podatke o korisniku. S druge strane, trgovac koji zaprima token ne može pristupiti podacima o identitetu korisnika, već samo ukoliko dva trgovca dobiju isti token u svojstvu plaćanja, njihovim kombiniranjem se mogu generirati podaci o korisniku. To znači da je anonimnost korisnika koji troši tokene samo jednom zagarantirana. Međutim, u slučaju duple potrošnje, identitet provjeren od strane banke je moguće otkriti. Iako sustav pruža mogućnost identificiranja potencijalnih varalica, svejedno veliki iznosi nisu bili sigurni jer bi prevaranti riskirali otkrivanje svog identiteta kako bi pronevjerili velike količine novca. Pored toga, nedostatak sustava je i u tome što su tokeni predstavljali fiksni iznos novca. Kako bi komercijalizirao svoju ideju o digitalnom novcu, Chaum 1990. godine osniva DigiCash korporaciju i pokreće eCash digitalnu valutu koja predstavlja prvu generaciju kriptovaluta. Međutim, da bi se sustav operativno provodio, morala bi postojati treća strana zadužena za izdavanje i odobravanje takvog elektroničkog novca, najčešće financijska institucija tj. banka. Unatoč naporima i pokušajima šire komercijalizacije, zbog centralizirane prirode, eCash nije naišao na odobravanje šire populacije gdje, nakon preuzimanja

od strane InfoSpace korporacije 1999. godine, prestaje postojati (Judmayer et al. 2017).

Adam Back 1997. godine predlaže implementaciju Hashcash metode za ograničavanje neželjene elektroničke pošte dodavanjem tokena zvanog hashcash u zaglavlje pošte (Back, 2002). Da bi se token kreirao, potrebno je potrošiti određenu količinu računalne snage, dok je za provjeru izvornosti poruke, trošak bio zanemariv. Dodavanje hashcash tokena u e-poštu promijenilo bi dinamiku stvaranja neželjenih pošiljaka prisiljavajući pošiljatelje da troše dodatnu količinu računalne energije ukoliko žele poslati elektroničku poštu. Iako Hashcash nije digitalni platni sustav, zbog opisanog rješenja, igra važnu ulogu u Bitcoin transakcijskom sustavu. Naime, da bi stvorio Hashcash, korisnik iterativnim postupkom mora riješiti kriptografsku zagonetku tako da rezultat funkcije sažimanja započinje sa zadanim brojem nula. Broj početnih nula u rezultatu funkcije sažimanja kontrolira težinu pronalaska uvjetovanog rješenja funkcije sažimanja. Njegovo izračunavanje nije uočljivo za korisnika, ali prisiljava pošiljatelja neželjene pošte na potrošnju dodatne energije i vremena – pola sekunde po jednoj e-pošti. Hashcash je decentraliziran jer su tokeni specifični za pošiljatelja, odnosno primatelj može provjeriti njegovu valjanost bez treće strane. Također je anoniman, ali i utrživ jer netko sa viškom računalne snage može generirati hashcash tokene na zahtjev i tako osloboditi korisnike potrebe da sami troše računalnu snagu. Sva prethodno navedena svojstva predstavljaju zapravo elemente konsenzus algoritma *dokaza o radu* (engl. *proof-of-work*), kao lako podesivu funkciju provjere rada koju je praktično implementirao Bitcoin transakcijski sustav.

Nick Szabo i Wei Dai predlažu sheme distribucije digitalnog novca pod nazivom bit gold (Szabo, 1998) i b-money (Dai, 1998). Niti jedan od predloženih sustava ne zahtjeva treću centralnu stranu između korisnika, već se baziraju na da ideju decentralizirane baze podataka. U b-money shemi novčane jedinice bi se stvarale primjenom funkcije sažimanja, odnosno kroz dokaz o radu čije je rješenje lako provjeriti, a količina novo stvorenih jedinica proporcionalna je težini pronalaska rješenja za kriptografski problem. Težina izračuna funkcije sažimanja bi se prilagođavala glasovanjem sudionika mreže. Nedostatak sustava je bio njegova ranjivost na entitet s velikim računalnim resursima koji bi sa svojom snagom

preplavio mrežu s novo kreiranim tokenima prije nego što mreža ima mogućnost adaptacije na novo stanje. U bit gold shemi nove jedinice valute bi također bile kreirane kroz rješenje dokaza o radu, uz razliku da je svako rješenje funkcije sažimanja povezano s prethodnim rješenjem. Drugim riječima, koristilo bi se rješenje kakvo je implementirano u Bitcoin protokol. To bi omogućilo mreži da prilagodi težinu izračuna funkcije sažimanja, odnosno dokaza o radu, u situaciji brzog kreiranja jedinice valute. Međutim, niti jedna od predloženih shema na opisuje u potpunosti kako se sudionici mogu složiti o rastu ponude jedinca valute. Korisnici oba sustava bi bili predstavljeni kroz pseudonime svojih javnih ključeva, a prijenos valute se vrši digitalnim potpisom poruke s javnim ključem koji najavljuje prijenos sredstava te emitiranjem poruke o transakciji na mrežu, što je također implementirano u Bitcoin transakcijski sustav. Pored toga, Dai (1998) i Szabo (1998) već tada raspravljaju i predlažu preteču verziju današnjih pametnih ugovora gdje strane u transakciji koriste uvjetni račun (engl. *escrow*) na mreži. Ukoliko su uvjeti iz ugovora uspješno ispunjeni ili su stranke postigle sporazum, sredstva sa uvjetnog računa bi bila oslobođena. S druge strane, ukoliko stranke ne postignu sporazum, obje strane bi poslale svoj prijedlog za korištenje sredstava, a čvorovi na mreži bi odlučili kako raspodijeliti sredstva sa uvjetnog računa. Također, u oba sustava se spominje problem istinite i točne komunikacije između čvorova u mreži, odnosno problem konsenzusa o stanju distribuirane baze podatak, kada u obje sheme poruka sa transakcijom može biti promijenjena. Za razliku b-money sustava koji nema rješenje, Szabo u narednom radu Szabo (1998) predlaže sustav kvoruma koji se oslanja na kvorum mrežnih bit gold adresa, a koje bi poslužile kao protokol za prihvaćanje promjena u distribuiranoj bazi podataka. Oba transakcijska sustava su bili samo teoretski prijedlozi i niti jedan se nije provodio u praksi. S druge strane, može se primijetiti da je Bitcoin transakcijski sustav zapravo praktično implementirao mnogih ideje prisutne u njihovom dizajnu, rješavajući nekoliko važnih pitanja koja u njihovim prijedlozima nisu bila predmet rasprave, niti je postojalo njihovo rješenje.

Sander i Ta-Shma (1999) predlažu anonimni elektronički novčani sustav u kojem ne postoji potreba za centralnim poslužiteljem koji bi izdavao slijepe potpise, već tokene predstavlja rezultat funkcije sažimanja njegovog serijskog broja, ali bi se popis ispravnih tokena koji predstavljaju sredstva čuvao kod banke. Popis ispravnih tokena

je predstavljen Merkelovim stablom[9] što čini sustav učinkovit u skladištenju i prijenosu, a njegov korijen, odnosno rezultat funkcije sažimanja, je objavljen javno te ga banka šalje svim sudionicima u sustavu. Da bi se dokazalo da token stvarno postoji i pripada jednoj strukturi stabla, provjerava se samo funkcija sažimanja od mjesta gdje je token zapisan do korijena stabla. Kako se novi tokeni dodaju na stablo, korijen se ažurira i ponovno šalje sudionicima. Prilikom plaćanja, trgovac korisniku šalje popis svih korijena koje trgovac čuva kod sebe, pri tom ne znajući koji token pripada kojem kupcu, odnosno korisniku. Korisnik kroz funkciju sažimanja dokazuje da se u tom stablu nalaze njegovi tokeni. Ovakav pristup osigurava anonimnost za kupca tako da trgovac ne zna pripadnost tokena, niti pripadnost tokena dijelu korijena stabla. Na kraju trgovac prezentira transakciju banci na provjeru moguće duple potrošnje. Po validaciji transakcije, banka sredstva doznačuje na račun trgovca, a serijski broj tokena se označavao kao potrošen. Sličnost sa Bitcoin transakcijskim sustavom je u propagaciji transakcija mrežom gdje se svako povećanje novo kreiranih tokena propagira mrežom putem Merkel stabla, tako da je svako povećanje tokena javno. S druge strane, nedostatak privatnog ključa korištenog za digitalni potpis, sustav čini manje ranjivim na potencijalne malverzacije nepoštene banke ili njegove krađe.

Hal Finney (2004) predlaže RPoW tj. višekratni dokaz o radu (engl. *reusable proof-of-work* kriptografsku metodu koja koristi prethodno navedeni Hashcash. Umjesto stvaranja hashcash tokena vezanog za određenu adresu e-pošte, PoW (engl.*proof-of-work*) tokeni nisu vezani za specifičnu aplikaciju i mogu se slobodno potrošiti. RPoW koristi Hashcash i njegov sistem dokaz o radu tako da se vrijednost PoW tokena može vezati za trošak računalne snage potrošene prilikom njegova stvaranja. Glavna inovacija koju je uveo Finney bila je omogućiti razmjenu PoW tokena bez potrebe za njihovim obnavljanjem. Drugim riječima, korisnik ne mora ponovno provoditi funkciju sažimanja kako bi ih obnovio i potrošio. PoW token prvo generira korisnik koji provodi Hashcash dokaz o radu. Kada korisnik odluči potrošiti token, šalje ga drugom korisniku koji ga zamjenjuje na RPoW poslužitelju (engl. *server*) za potpuno novi PoW token. Međutim, opisani proces pruža mogućnost duple potrošnje upravo zbog toga što izvorni vlasnik može poslati isti token drugom korisniku, prije

[9] Merkleovo stablo je kriptografski alat koji omogućuje sigurnu i brzu provjeru sadržaja velike količine podataka.

nego što ovaj prvi korisnik stigne na poslužitelju zamijeniti svoje tokene. RPoW poslužitelj omogućava uzastopno ponovno korištenje tokena, odnosno ponovno izdavanje novog PoW tokena kada mu se prethodni prezentira. RPoW sustav ovisi o središnjem poslužitelju na kojem se nalazi baza podataka sa svim potrošenim PoW tokenima. Poslužitelj ne stvara nove tokene, već ih samo objavljuje ukoliko nisu potrošeni prethodno. Finney je kreirao implementaciju RPoW poslužitelja i objavio je pod licencom otvorenog koda. Međutim, zbog mogućeg otkrivanja javnog ključa kod proizvođača potrebnih procesora, poslužitelj je na kraju ipak isključen sa mreže te je projekt ugašen.

Sve prethodno prikazane ideje utjecale su na razvoj i oblik kriptovaluta kakve postoje danas. Bitcoin protokol je sublimirao i praktično implementirao najbolje od prezentiranih ideja u svom transakcijskom sustavu. Iako je javno mnijenje da su kriptovalute nastale s objavom Bitcoin protokola, razvidno je da su i prije postojali pokušaji kreiranja i puštanja u javnost digitalnih valuta temeljenih na kriptografiji. Međutim, niti jedan od prethodnih pokušaja nije zaživio, odnosno ostao zapažen niti približno blizu koliko je u javnosti zapažen Bitcoin danas. Iako su tehnički elementi, koji su u osnovi kriptografska jednosmjerna funkcija sažimanja i asimetrična kriptografija, postojali već neko vrijeme, Bitcoin je bio prvi koncept koji je spojio ove tehničke elemente u poticajnom okruženju i tako stvorio prvu distribuiranu kriptovalutu u povijesti.

2.3. Bitcoin

Bitcoin je zbirka koncepata i tehnologija koja čine osnovu ekosustava digitalnog novca (Antonopoulos, 2017). Bitcoin je distribuirana glavna knjiga (engl. *public ledger*), upravljački decentraliziran transakcijski sustav i digitalna valuta, osigurana kriptografijom i upravljana konsenzusom, koja koristi *peer-to-peer* sustav za provjeru i obradu transakcija. Za razliku od centraliziranih sustava koji se oslanjaju na postojanje treće strane, poput financijskih institucija, Bitcoin koristi kriptografski dokaz u svom računalnom softveru za obradu transakcija i provjeru zakonitosti Bitcoina (Nakamoto, 2008). Ne ovisi o odlukama niti jedna vlade svijeta, drugih pravnih osoba ili bilo koje treće strane, kao niti o monetarnoj vrijednosti bilo kojih valuta ili realnoj vrijednosti zlata ili drugih roba. Glavna knjiga sadrži sve transakcije jedinca valute

koje su se dogodile između sudionika na mrežnom sustavu. Jedinice valute nazvane bitcoin[10] se koriste za pohranu i prijenos među sudionicima mreže i izražavaju se do 8 decimalnim mjesta. Najmanja jedinica bitcoina je 1 satoši (engl. *satoshi*), a jedan bitcoin sadrži 100 milijuna satošija. Programski kod Bitcoin protokola uvjetuje unaprijed planirano kreiranje i puštanje jedinica valuta u opticaj, a očekuje se da će bitcoin svoju maksimalnu količinu u opticaju (21 milijun) dostići u 2140. godini[11]. Bitcoin valuta se oslanja na ravnopravnu računalnu mrežu, a integritet održava pomoću kriptografije (Gervais, Karame, Capkun i Capkun, 2014). Korisnici Bitcoina transakcijskog sustava međusobno komuniciraju putem Bitcoin protokola prvenstveno putem interneta, mada se mogu koristiti i druge mreže. Bitcoin protokol, dostupan kroz licencu otvorenog koda, može se provoditi na širokom rasponu računalnih uređaja, uključujući prijenosna računala i pametne telefone, čineći tehnologiju lako dostupnom (Antonopoulos, 2017).

Bitcoin je prenosiva i utrživa digitalna valuta, prilagođena za internet jer je njegov transfer brz, siguran i bez ograničenja. Jednako kao i s tradicionalnim valutama, može se transferirati mrežom s ciljem kupnje i prodaje robe, slanja jedinica valute u svojstvu novca ili posuđivanja i kreditiranja. Bitcoin se može kupiti, prodati i zamijeniti za druge valute na specijaliziranim burzama kriptovaluta ili drugim prilagođenim platformama. Njegovom kupnjom zapravo se kupuju privatni ključevi kojim se dokazuje vlasništvo određenog broja jedinica valute koji se nalaze na distribuiranoj glavnoj knjizi i koji su povezani s javnim ključem. Potpisom transakcije privatnim ključem se dokazuje vlasništvo, odnosno otključava se prethodna transakcija koja je uključivala odgovarajući javni ključ. Također, u digitalni potpis se uključuje i javni ključ novog vlasnika te se bitcoin zaključava za taj novi javni ključ. Drugim riječima, samo vlasnik odgovarajućeg privatnog ključa iz kojeg je izveden taj novi javni ključ uključen u transakciju, može svojim digitalnim potpisom otključati sredstva na distribuiranoj glavnoj knjizi. Privatni ključevi se često pohranjuju u digitalnom novčaniku, na računalu ili pametnom telefonu korisnika. Prema tome, posjedovanje privatnog ključa kojim se potpisuje transakcija je jedini preduvjet trošenja bitcoina, čime je kontrola i vlasništvo u potpunosti u rukama svakog korisnika.

[10] Kada se koristi veliko početno slovo B u "Bitcoin" misli se na mrežu i tehnologiju, dok se “bitcoin”, s malim početnim slovom b, odnosi na jedinice valute
[11] Na datum 26.06.2020. god. u opticaju je 18.415.006 bitcoina.

Bitcoin se temelji na distribuiranom *peer-to-peer* načinu transmisije podataka u kojem ne postoji središnji poslužitelj ili kontrolna točka centralnog tijela. Jedinice valute se stvaraju kroz proces koji se naziva rudarenje (engl. *mining*). Proces rudarenja uključuje nadmetanje u što bržem pronalasku uvjetovanog rješenja za matematički problem funkcije sažimanja tijekom obrade preuzetih nepotvrđenih transakcija (engl. *transaction pool*). Sudionici Bitcoin mreže se nazivaju čvorovi (engl. *nodes*) i dijele se na pune čvorove (engl. *full nodes*) i lagane čvorove (*light nodes*). Za razliku od laganih čvorova koji samo verificiraju i propagiraju nepotvrđene transakcije te pružaju uvid u bazu istih, svaki puni čvor, osim verifikacija i propagiranja transakcija, može raditi kao rudar (engl. *miner*), koristeći računalnu snagu svog računala za provjeru i zapis transakcija na distribuiranu glavnu knjigu. Težina rudarenja se namješta svakih 2.016 blokova (dva tjedna) tako da se nove transakcije spreme u glavnu knjigu otprilike svakih 10 minuta. Glavnu knjigu sačinjavaju transakcije grupirane u tzv. blokove iz čega proizlazi da je glavna knjiga zapravo lanac blokova (engl. *blockchain*), a jedan blok može sadržavati od 500 do 2.500 transakcija, ovisno o težini rudarenja i veličini transakcija. Za svaki novi blok, rudar u mreži je nagrađen za potpuno novih 6,25 bitcoina, a svakih 210.000 blokova, otprilike 4 godine, nagrada se prepolovi. U osnovi, rudarenje bitcoina decentralizira funkcije izdavanja i obračuna valute središnje banke i zamjenjuje potrebu za bilo kojom središnjom bankom (Antonopoulos, 2017).

Prema Antonopoulosu (2017) Bitcoin predstavlja vrhunac više desetljeća istraživanja kriptografije i distribuiranih sustava i uključuje četiri ključna tehnička svojstva implementirana u jednu jedinstvenu i moćnu kombinaciju. Bitcoin se sastoji od:

a) Decentralizirane (*peer-to-peer*) mreže (Bitcoin protokol);
b) Glavne knjige transakcija (blockchain);
c) Skupa pravila za neovisnu provjeru transakcija i izdavanje valute (konsenzus pravila);
d) Mehanizma za postizanje globalnog decentraliziranog konsenzusa o valjanom blockchainu (proof-of-work algoritam).

2.4. Satoshi Nakamoto

Satoshi Nakamoto je ime ili pseudonim osobe ili osoba koje su stvorile Bitcoin transakcijski sustav. On (ona ili oni) su 31. listopada 2008. godine javnosti prezentirali dokument pod nazivom „*Bitcoin: A Peer-to-Peer Electronic Cash System*“ u kojem je opisan novi decentralizirani transakcijski sustav koji ne uključuje posrednika između entiteta od interesa. Računalni program, odnosno Bitcoin protokol je pušten u javnost 9. siječnja 2009. godine čime se kreirala *peer-to-peer* infrastruktura za prvu kriptovalutu. U početnim danima bitcoin je imao vrlo malo rudara tj. osoba koje su svoje kompjutorske resurse stavili na raspolaganje Bitcoin transakcijskom protokolu s ciljem osiguranja sigurnosti mreže, decentralizacije i postizanja konsenzusa o provedenim transakcijama. Kako je bilo jako malo rudara koji su predstavljali čvorove mreže, tako je i sama težina rudarenja bila značajno niža u odnosu na stanje kakvo je danas. Bitcoin se mogao rudariti i na prijenosnom računalu pa je nekoliko rudara uspjelo skupiti značajan broj jedinica bitcoin kriptovalute. Pretpostavlja se da je i sam kreator bitcoina skupio otprilike 1 milijun bitcoina, što trenutno čini oko 5,55% ukupne količine bitcoina u opticaju i postiže vrijednost višu od 9 milijardi dolara. Međutim, zanimljivo je istaknuti da tada kreirani bitcoin i dalje stoji na svojoj inicijalnoj adresi i da još nije transferiran niti najmanji dio bitcoina sa te adrese. Satoshi Nakamoto se povukao iz javnosti u travnju 2011. godine, ostavljajući odgovornost za razvoj mreže grupi volontera. Od 2009. godine pojavilo se desetak imena za koje se špekuliralo da su baš oni Satoshi Nakamoto, najozbiljnije kandidati su bili Nick Szabo, Hal Finney, Wei Dai, Craig Steven Wright, Shinichi Mochizuki, Gavin Andersen, Jed McCaleb i Dorian Nakamoto.

Nick Szabo je američki znanstvenik i kriptograf, koji je bio jedan od pionira kriptovaluta kakve postoje u današnjem svijetu. 2013. godine bloger pod imenom Skye Grey je iznio tvrdnju da je Szabo zapravo Satoshi Nakamoto. Szabo je kasnije izjavio da, iako su on, Finney i Wei Dai bili jedini ljudi koji su dovoljno vjerovali u ideju decentralizirane kriptovalute, on ipak nije Satoshi Nakamoto te je u svojim intervjuima jasno porekao povezanost s njegovim identitetom. Hal Finney je bio američki kriptograf i informatičar koji je prvi koristio Bitcoin protokol (osim samog Nakamota). Iako je Finney itekako bio umješan u same početke Bitcoina, kasnije su nađeni čak i dokazi o prvim transakcijama i elektroničkoj pošti koje su Finney i Nakamoto

međusobno slali jedan drugome. Tek nakon što je Finney više puta porekao da je on Nakamoto, otklonjena je sumnja da se radi baš o njemu. Wei Dai je zajedno sa Szabom i Finneyem bio jedan od prvih ljudi koji su kontaktirali sa Nakamotom oko ideje Bitcoina, pa je logično da se i njegovo ime provlačilo u kontekstu da je upravo on Satoshi Nakamoto. Međutim, za to također nikada nisu prezentirani nikakvi dokazi. S druge strane, Wei Dai je odigrao značajnu ulogu u kreiranju Ethereum kompjuterske platforme, pa je po njemu nazvana najmanja jedinica etherum kriptovalute - WEI. Craig Steven Wright je australski informatičar i poduzetnik koji je postao poznat po izjavama da je baš on izumitelj Bitcoina, odnosno Satoshi Nakamoto. Wrightovu priču su istraživali magazini Gizmodo i Wired a kasnije i australska federalna policija. Sve istrage su ukazivale na to da nema nikakvih dokaza da je upravo Wright Nakamoto, te da je cijela priča bila Wrightov način za samopromociju. Shinichi Mochizuki je japanski znanstvenik i matematičar. Mochizuki je postao poznat tako što je riješio poznati matematički problem ABC konjuktura, a zanimljivo je da je baš kao i Satoshi Nakamoto nakon rješavanja tog matematičkog problema nestao iz javnosti. Tvrdnje da je upravo Mochizuki Nakamoto je iznio američki poduzetnik i industrijalac Ted Nelson, koji je rekao da Mochizuki ima znanja, vještine i genijalnost da stvori Bitcoin. Kao i kod drugih kandidata konkretnih dokaza nema. Američki magazin Newsweek je 2014. godine objavio vijest da je Dorian Nakamoto, Japanac koji živi u SAD-u, zapravo Satoshi Nakamoto. Zanimljivo je da je Dorian Nakamoto rođen pod pravim imenom kao Satoshi Nakamoto, a tek je kasnije promijenio ime u Dorian. U slučaju Doriana Nakamoto postoje konkretni dokazi da je upravo on Satoshi Nakamoto. 2014. godine u intervjuu je na pitanje je li on osnivač Bitcoina dao izjavu: „Više nisam umješan u to i ne mogu raspravljati o tome, drugi ljudi se sada bave time“, ta izjava je kasnije potvrđena kao istinita i vjerodostojna i od strane američke policije koji su bili prisutni za vrijeme tog razgovora. Još jedna slučajnost je da je Doriana Nakamoto živio samo 2 ulice dalje od već spomenutog Hala Finneya koji je također bio jedan od kandidata za osnivača Bitcoina.

Premda se od osnivanja Bitcoina 2009. godine za brojne osobe tvrdilo da su baš oni Satoshi Nakamoto, konačnog odgovora, odnosno konačne istine još nema. Identitet tvorca Bitcoina i entiteta iza pseudonima Satoshi Nakamoto i dalje ostaje nepoznat. Brojni analitičari koji su analizirali programski kod kojim je napisan Bitcoin, su došli do zaključka da je malo vjerojatno da je Bitcoin stvoren od strane samo jedne osobe,

pošto je programski kod ekstremno kompleksan te bi ta osoba morala biti izrazit interdisciplinarni stručnjak u svakom području koji je implementirao Bitcoin. Puno su veće šanse da je Bitcoin stvorila skupina ljudi koja je kombinirajući uspjela iskoristiti elemente kriptografije, matematike, informatike i modernog koncepta novca kako bi u konačnici stvorili Bitcoin. Međutim, u trenutku kada Satoshi počne trošiti bitcoin sa svoje inicijalne adrese, otvorit će se trag koji bi na kraju mogao razotkriti tko stoji iza kreacije prvog decentraliziranog digitalnog novca u povijesti.

3. KLASIFIKACIJA KRIPTOVALUTA

Bitcoin programski kod je otvoren i slobodan za javnost. To znači da svatko tko želi može slobodno iskoristiti postojeći protokol, prilagoditi svojim potrebama te kreirati novu kriptovalutu. Upravo je licenca otvorenog programskog koda omogućila stvaranju niza novih kriptovaluta s različitim svojstvima. Prva alternativna kriptovaluta *namecoin* je nastala 2011. godine na temelju Bitcoin izvornog programskog koda, a do kraja godine je kreirano još 10 kriptovaluta, sve temeljene na Bitcoinu. Bitcoin repozitorij na GitHub - u trenutno pokazuje 25 tisuća izdvajanja tj. račvanja (engl. *fork*) programskog koda, što znači postoji mogućnost kreiranja isto tolikog broja i alternativnih kriptovaluta, bez da se ubrajaju nova račvanja od prethodnih račvanja[12]. Internet stranica Coinmarketcap[13] trenutno pokazuje kretanje vrijednosti za 5.520 prijavljenih kriptovaluta s kojima se trguje na 343 različite burze. Međutim, vrlo vjerojatno su neke od njih zapravo neki oblik prijevare tzv. *scamcoine* koji je osmišljen i listan kako bi koristio samo njihovim tvorcima. S druge strane, alternativne kriptovalute inicijalno niti ne moraju biti kreirane s ciljem isključivo prikupljanja sredstava za njihove kreatore. Postoje i legitimni projekti koji su naprosto nestali zbog loših poteza vodećih ljudi projekta ili nisu mogli prikupiti značajnu korisničku bazu kako bi kriptovaluta „zaživjela“.

Veliku ulogu u širenju korisničke baze za pojedinu kriptovalutu imaju i burze. Razvojem sekundarnog tržišta kriptovaluta, burze su preuzele značajnu ulogu u promociji i distribuciji kriptovaluta, iako je prethodno situacija bila obrnuta, odnosno kriptovaluta se listala na burzu tek nakon što je postigla određeni status i širu zajednicu. Danas su burze te koje svojim aktivnostima pružaju neki oblik garancije uspješnosti projekta. Štoviše, zbog statusa koje uživaju pojedine burze, listanje na njima, sa troškovima i do 5 milijuna dolara, ne predstavlja samo djelomično osiguranje uspješnosti, već uključuje pokazivanje prestiža i moći projekata iza njih. Sekundarno tržište alternativnih kriptovaluta je plitko, usko i imperfektno tržište. Zbog toga je suočeno s brojnim kritikama jer je često podložno različitim oblicima

[12] Pristupljeno: 28. svibnja 2020. godine.
[13] Internet stranica koja pruža uvid u povijesno kretanje vrijednosti prijavljenih kriptovaluta, pristupljeno: 28. svibnja 2020. godine.

dogovornog trgovanja, poput tzv. insajderskog trgovanja, *pump and dump*[14] cjenovnim manipulacijama, lažnim utjecajima kroz lažne korisničke račune i društvene medije kako bi se kreirao dodatni cjenovni momentum itd. Međutim, razvojem tržišta i uvođenjem regulacije, u budućnosti se može očekivati sve manje ovakvih aktivnost te stabilizacija sekundarnog tržišta kriptovaluta.

Zbog veličine tržišne kapitalizacije i svog robusnog programskog koda, Bitcoin protokol nije prikladan za testiranje novih blockchain ideja ili njegovih značajnijih izmjena. Zbog toga, nove ideje se razvijaju i implementiraju kroz nove alternativne kriptovalute. Tako je Litecoin promijenio algoritam funkcije sažimanja kako bi se rudarenje učinilo više decentraliziranim te ubrzao konfirmaciju bloka transakcija. Peercoin je prvi implementirao *dokaz o udjelu* (engl. *proof-of-stake*) PoS konsenzus algoritam kako bi se proces očuvanja integriteta mreže energetski učinkovitije provodio, Monero je uveo novu značajku anonimnih transakcija, Lisk je primijenio drugi programski jezik, kao i Nxt itd. Stvaranje alternativnih kriptovaluta doprinosi inovacijama u idejama programiranja. Nove ideje poput implementacije *Turing-complete*[15] programiranja na razini protokola i pametnih ugovora uvode pomak paradigme u načinu razmišljanja o decentralizaciji i digitalnom novcu. Međutim, primjena ovih naprednih rješenja na Bitcoin protokolu se može pokazati vrlo zahtjevnom jer ta rješenja nisu ono za što je stvoren Bitcoin. Iz tog razloga razvojnim programerima je lakše iskoristiti postojeći Bitcoin protokol kao bazu i nadograditi nova rješenja i ideje na njega. Tako stvorene kriptovalute imaju nove i bolje karakteristike i vjerojatno će ubrzati usvajanje digitalnih valuta i smanjiti troškove transakcija.

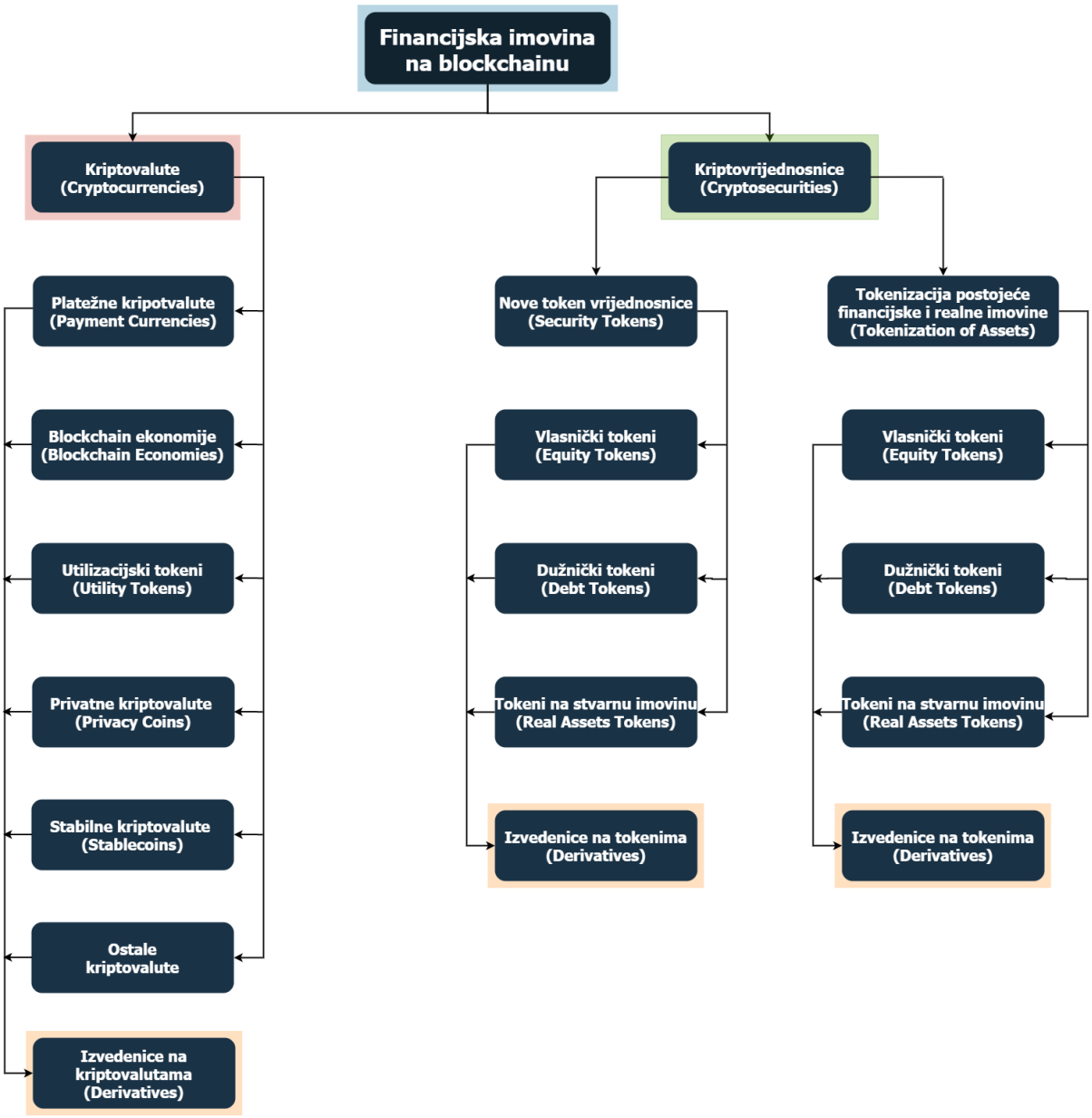
Ukoliko se Bitcoin promatra kao svojevrsni tehnološki benchmark mogućnosti blockchain tehnologije, kriptovalute se mogu grupirati u tri osnovne skupine:

a) Alternativne kriptovalute – kao inačice, odnosno poboljšane verzije Bitcoin protokola nastale kloniranjem otvorenog programskog koda;

[14] *Pump and dump* aktivnost uključuje agresivnu kupnju kriptovalute u kratkom period, čime se stvara likvidnost i privlači dodatne kupce, da bi se, nakon rasta vrijednosti, kriptovaluta prodala sa značajnim kapitalnim prinosom.
[15] *Turing-complete* (turing potpunost) je svojstvo što jamči da dani programski jezik može opisati i implementirati svaki računalni postupak (program/algoritam).

b) Kriptovalute kreirane za uspostavu decentraliziranih kompjuterskih platformi – pružaju mogućnost kreiranja decentraliziranih aplikacija;
c) Tokeni - kriptovalute kreirane s ciljem uspostave operativnog poslovanja decentraliziranih aplikacija.

Osim navedene osnovne podjele, kriptovalute se mogu klasificirati i prema drugim svojstvima, kao što je svojstvo praktične primjene. Međutim, iako se blockchain tehnologija može primijeniti u različitim industrijama, primarno je nastala kao transakcijska mreža na kojoj će se razmjenjivati bitcoin kao digitalna valuta. Tek s protekom vremena, sve više industrija je prepoznalo sigurnost i kvalitetu, što je rezultiralo razvoju blockchaina i njegovoj praktičnoj implementaciji. Kako su inicijalne alternativne kriptovalute zapravo dorađeni klonovi Bitcoin sustava, tako i njihove mogućnosti značajno ne odstupaju od transakcijskih mogućnosti bitcoina, što znači da je i njihova primarna svrha prijenos jedinica digitalne valute između krajnjih korisnika. Uzimajući navedeno u obzir, u nastavku se donosi podjela financijske imovine na blockchainu prema osnovnim karakteristikama i svojstvima praktične namjene, ilustrirana Shemom 1.:



Shema 1. Financijska imovina na blockchainu

Izvor: Izrada autora

a) Platežne kripotvalute (engl. *payment currencies*);

Kao što ime sugerira, ove se kriptovalute uglavnom koriste kao sredstvo razmjene za plaćanje robe ili usluga te se lako mogu unovčiti u lokalnu fiat valutu. Iako u teoriji svaka kriptovaluta može služiti kao platežno sredstvo, ova kategorija je više prihvaćena od strane trgovaca, dobavljača itd. U ovu skupinu ulaze kriptovalute poput bitcoina, litecoina, bitcoin casha, dasha, dogea i drugih popularnih i dobro poznatih platežnih kriptovaluta.

b) Kriptovalute kao blockchain ekonomije (engl. *blockchain economies*);

Blockchain ekonomije su zapravo decentralizirane kompjutorske platforme s matičnom kriptovalutom čija funkcionalnost i namjena pruža puno više od same platežne svrhe. Na njima se omogućuje kreiranje vlastite digitalne imovine – tokena, kao i decentraliziranih aplikacija. Iz tog razloga, blockchain platforme u ovom slučaju postaju vlastite blockchain ekonomije s različitom imovinom, decentraliziranim aplikacijama itd. Više poznate decentralizirane platforme uključuju kriptovalute kao što su ethereum, ethereum clasic, eos, neo, stellar, nem itd.

c) Utilizacijski tokeni (engl. *utility tokens*);

Utilizacijski tokeni su kriptovalute koje se većinom koriste za neku specifičnu svrhu i utilizaciju u proizvodu ili usluzi kreiranoj na decentraliziranoj kompjutorskoj platformi. Pokreću se i dio su blockchain ekonomije, te bez njih glavna funkcija decentralizirane aplikacije ne bi bila moguća. Većina utilizacijskih tokena su ERC20 tokeni koji se pokreću na Ethereum blockchainu. Na primjer, Golem je platforma na kojoj korisnici mogu iznajmiti računalnu snagu, a golem token (GNT) služi za plaćanje najma te snage. Osim golem tokena, neki od primjera utilizacijskih tokena su bat, civic, omisego, 0x itd. Međutim, uz kontinuirani razvoj drugih blockchain platformi, pojavile su se i druge vrste tokena, poput TRC10 i TRC20 tokena.

d) Privatne kriptovalute (engl. *privacy coins*);

Neke su kriptovalute stvorene s naglaskom na privatnost gdje količina tokena i korišteni privatni ključ u provedenoj transakciji ostaju nepoznati, odnosno poznati su samo pošiljatelju i primatelju u transakciji. Pored toga, saldo jedinica digitalne valute u digitalnom novčaniku je također nepoznat, što je u suprotnosti s npr. Bitcoin sustavom gdje je iznos transakcije i saldo digitalnog novčanika javan podatak. Poznatije privatne kriptovalute su zcash, monero, pivx, bytecoin, komodo, verge itd.

e) Stabilne kriptovalute (engl. *stablecoins*);

Stabilne kriptovalute predstavljaju značajnu ulogu na sekundarnom tržištu kriptovaluta jer je kao takvo iznimno volatilno, uključujući i bitcoin. Postojanjem stabilnih kriptovaluta čija je vrijednost vezana za vrijednost neke manje volatilne imovine ili imovine koja manje korelira s tržištem kriptovaluta, svakodnevnim trgovcima se pruža mogućnost da izađu iz svojih nepovoljnih

pozicija te zaštite ulaganje kupnjom stabilne kriptovalute. S obzirom na način na koji su stabilne kriptovalute kreirane, odnosno izvedene, postoji nekoliko podvrsta stabilnih kriptovaluta. Prvi i svakako najzastupljeniji tip stabilnih kriptovaluta predstavljaju kriptovalute vezane za neke fiat valute. Njihova vrijednost u ovom slučaju proizlazi iz vrijednosti fiat valuta iz koje su izvedene, a koja se nalazi kod treće strane, najčešće regulirane financijske institucije. Primjer ovog tipa kriptovaluta su trueUSD (TUSD), USD tether (USDT), binance USD (BUSD), USD Coin (USDC), paxos Standard (PAX) itd. Drugi tip predstavljaju kriptovalute čija je vrijednost vezana za vrijednost neke realne imovine poput plemenitih metala. Zbog temeljne imovine iz koje su izvedene, manje su zastupljene na tržište nego prethodni tip stabilnih kriptovaluta. Njihova tržišna kapitalizacija, odnosno vrijednost u opticaju mora odgovarati ukupnoj kapitalizaciji robe koja služi kao temeljna imovina i koju drži izdavatelj. Primjer ovog tipa su: digital gold (GOLD), digix Gold Token (DGX), PAX gold (PAXG), i dr. Treći tip stabilnih kriptovaluta se odnosi na kripotvalute koje su izvedene iz drugih kriptovaluta koje služe kao kolateral za njihovo kreiranje, ali njihova tržišna vrijednost ovisi o vrijednosti neke druge financijske, ali i realne imovine. Tako je, na primjer, kroz kolateriziranu dužničku poziciju (engl. *collateralized debt position*) moguće kreirati kriptovalutu dai (DAI) čija ja vrijednost vezana za vrijednost dolara, ali njena *intrinzična* vrijednost proizlazi iz kolaterala deponiranom u kriptovaluti ethereum (ETH). Proces kreiranja takve stabilne kriptovalute se provodi kroz pametne ugovore i najčešće uključuje i trošak kamata koje se plaćaju za vrijeme držanja DAI tokena, tzv. naknada za stabilnost (engl. *stability fee*). Primjer stabilne kriptovalute je već spomenuti dai (DAI) token.

f) Ostale kriptovalute i njihove izvedenice (engl. *derivatives*);

Osim spomenutih kategorija postoje i ostale kriptovalute koje ne ulaze niti u jednu skupinu. Točnije, to su transakcijski protokoli na kojima se vrši razmjena jedinica digitalne valute koja koristi kriptografske algoritme, ali njihova glavna knjiga nije potpunosti distribuirana, niti je njihovo upravljanje decentralizirano. Isto tako, većina kriptovaluta kotira na sekundarnom tržištu i kroz aktivnu trgovinu postižu neku tržišnu cijenu. Kao takve, burze kriptovaluta su ih prepoznale u svojstvu temeljne imovine (engl. *underlying asset*) te kreirale

izvedenice na njima. Trenutno najzastupljenije izvedenice na kriptovalutama su terminski ugovori (engl. *futures contracts*) i opcije (engl. *options*).

g) Kriptovrijednosnice (engl. *cryptosecurities*);

Drugu skupinu kriptovaluta predstavljaju nove kriptovrijednosnice, odnosno digitalna imovina koja koristi blockchain infrastrukturu za svoje postojanje. Jednako kao i utilizacijski tokeni i kriptovrijednosnice su kreirane na nekoj od decentraliziranoj kompjutorskoj platformi. Međutim, za razliku od većine kreiranih i izdanih utilizacijskih tokena, kriptovrijednosnice predstavljaju kriptovalute koje zadovoljavaju određeni zakonski okvir i regulativu države u kojoj se kreiraju, odnosno izdaju. Procjenjuje se da je okvirno oko 80% svih izdanih kriptovaluta do 2018. godine predstavljalo neki oblik prijevare investitora prilikom inicijalne ponude tj. ICO-a (engl. *initial coin offering*). Kako bi vratili izgubljeno povjerenje, sudionici tržišta kriptovaluta su kreirali nove decentralizirane platforme, poput Polymath, koje pružaju mogućnost izdavanja novih token vrijednosnica putem inicijalne ponude vrijednosnica tj. STO-a (engl. *security token offering*), ali koje i posluju pod zakonskim normama i uzancama države gdje se izdaje token. Kriptovrijednosnice su zapravo širok pojam i pokrivaju više kategorija digitalizirane imovine. Međutim, može ih se definirati kroz dvije osnovne skupine: a) nove token vrijednosnice (engl. *security tokens*) i b) tokenizirana postojeća financijska i realna imovina (engl. *tokenization of assets*). Nove token vrijednosnice su kriptovalute koje predstavljaju vlasničke tokene (engl. *equity tokens*), dužničke tokene (engl. *debt tokens*) i tokeni na stvarnu i realnu imovinu (engl. *real asset tokens*). Primjer je financiranje novog startupa izdavanjem vlasničkog tokena. S druge strane, tokenizirana postojeća imovina predstavlja kriptovalute koje su kreirane na već postojećoj financijskoj ili realnoj imovini kao temeljnoj imovini. Na primjer, postojeće dionice ili obveznice se prebacuju u digitalni oblik koji koristi blockchain infrastrukturu decentralizirane kompjutorske platforme. Jedina poveznica između novog koncepta kriptovarijednosnica i postojećih kriptovaluta je ta što obje koriste blockchain tehnologiju (Houben i Snyers, 2018).

Prethodna podjela pokriva širok spektar mogućih primjena kriptovaluta u svakodnevnom poslovanju. Također, njihova podjela nije konačna niti međusobno

isključiva. Drugim riječima, pojedine kriptovalute zapravo pripadaju u nekoliko kategorija. Tako se, na primjer, sa ethereum kriptovalutom koja je decentralizirana kompjuterska platforma mogu i vršiti plaćanja za robu ili usluge. Međutim, potrebno je naglasiti da je svaka od njih bazirana na ideji Bitcoin blockchain tehnologije, odnosno tehnologije čije je upravljanje decentralizirano, glavna knjiga tj. digitalni zapis je distribuiran i osiguran kriptografijom. Jednom po uspostavi sigurne i distribuirane baze podataka, ograničenja prilikom njihove praktične implementacije zapravo i ne postoje, odnosno postoje samo onoliko koliko su kreativni neposredni razvojni programeri. Drugim riječima, gdje god postoji nužnost za istinito i/ili transparentno iskazivanje podataka na siguran način, moguće je implementirati blockchain tehnologiju, sa ili bez kriptovaluta, ukoliko se dionici projekta dogovore tako.

3.1. Ekonomski okvir kriptovaluta

Da bi se jedinca neke valute smatrala legitimnim novcem, praktičnim za širu upotrebu, potrebno je da zadovolji tri osnovne karakteristike (funkcije) novca: obračunska jedinica (vrijednost roba i usluga se izražava u jedinici valute), sredstvo očuvanja vrijednosti (jedinica valute se može iskoristiti za prijenos kupovne moći iz sadašnjosti u budućnost) i sredstvo razmjene (jedinica valute se može zamijeniti za robu i usluge). Prema Franco (2015) Bitcoin bi mogao poslužiti kao novac jer zadovoljava tehnička svojstva novca: trajnost, djeljivost, zamjenjivost, prenosivost i nemogućnost krivotvorenja. Yermack (2015) smatra da bitcoin donekle zadovoljava funkciju sredstva razmjene jer je sve veći broj trgovaca, posebno trgovaca koji nude svoje proizvode i usluge putem interneta, spremno prihvatiti bitcoin kao oblik plaćanja. Međutim, kao nedostatak za njegovu širu upotrebu, autor ističe vremenski period potreban za provjeru provedene transakcije, što se poslije pokazalo kao jedan od glavnih nedostataka Bitcoin transakcijskog protokola, koji se danas pokušava otkloniti implementacijom *lightning network*-a[16].

[16] Lightning Network je protokol plaćanja druge razine koji djeluje na postojećem blockchain protokolu od promatrane kriptovalute. Primjenom *lightning network*-a otvorili bi se novi kanali između kupca i prodavatelja bez potrebe za verifikacijom transakcija na blockchainu. Tek nakon zatvaranja tih transakcijskih kanala, novo stanje bi se verificiralo i zapisalo na blockchain. Opisano rješenje bi smanjilo vremenski period potreban provjeru transakcija na blockchainu jer bi se verificiralo samo početno i zadnje, izmijenjeno stanje.

Kritičari navode da bitcoin ne zadovoljava funkciju obračunske jedince i funkciju sredstva očuvanja vrijednosti i da se zbog toga ne uklapa u definiciju novca. Da bi se cijena robe i usluga iskazala u bitcoin valuti, trgovci bi za uobičajenu maloprodajnu robu cijenu morali iskazati na šest ili sedam decimalnih mjesta i to sa pet ili šest vodećih nula ispred, što je praksa koja se rijetko viđa u marketingu potrošača i koja može zbuniti prodavače i kupce na tržištu. Također, u paritetu sa fiat valutama, bitcoin pokazuje izrazito visoku volatilnost. Trgovci bi morali imati digitalne cijene, iskazane i preračunate u bitcoin valutu u realnom vremenu, što zahtijeva kontinuirano ažuriranje i povezanost sa burzama kriptovaluta. S druge strane, cijene roba i usluga se mogu iskazati u fiat valuti, što je puno češći i praktičniji slučaj. Tada je cijenu robe ili usluga potrebno preračunati jednom, prilikom plaćanja. Međutim, i to zahtijeva povezanost sa burzama ili mjenjačnicama kriptovaluta i kontinuirano ažuriranje tečaja BTC/fiat. Navedeni nedostaci ruše korisnost bitcoina kao obračunske jedinice.

Zbog svoje volatilnosti, ali i hakerskih napada, gubitka i krađa privatnih ključeva, i ostalih problema vezanih za sigurnost, upitna je i funkcija bitcoina kao sredstva očuvanja vrijednosti. Budući da bitcoin nema intrinzičnu vrijednost, njegova ekonomska vrijednost u konačnici ovisi o korisnosti kao valuti u potrošačkoj ekonomiji (Yermack, 2015). Iako sve više trgovaca različitih profila prihvaća bitcoin kao sredstvo plaćanja, primjeri njegove primjene u svakodnevnom poslovanju trgovaca uglavnom dominiraju među tvrtkama koje pružaju usluge i proizvode na području informacijskih tehnologija. Prema tome, ukoliko s jedne strane relativno malo trgovaca neposredno prihvaća bitcoin u zamjenu za svoju robu i usluge, a njegov kumulativni prinos u zadnjih pet godina iznosi 4.000%, dolazi do disproporcije korisne vrijednosti BTC-a i tržišne vrijednosti. Drugim riječima, postavlja se pitanje ima li bitcoin neku drugu ulogu, osim uloge imovine dostupne svima u špekulativne svrhe, odnosno postavlja se pitanje može li bitcoin ispuniti svoju svrhu u funkciji sredstva očuvanja vrijednosti. S druge strane, trgovci neposredno niti ne moraju prihvaćati bitcoin kao valutu u zamjenu za isporučena dobra i usluge. Sve je više FinTech[17] aplikativnih rješenja koje pružaju mogućnost konverzije bitcoin valute u fiat valutu u trenutku kupnje proizvoda ili usluga. Takva rješenja su najčešće po uzoru na

[17] FinTech (engl. *financial technology*) je termin kojim se opisuju nova tehnološka rješenja na području financijskih usluga čiji je cilj transformirati tradicionalni oblik pružanja bankarskih i financijskih usluga.

tradicionalno poslovanje s debitnim karticama, što znatno otežava adekvatnu procjenu stvarnih transakcija kojima je obavljena kupnja roba ili usluga kod trgovaca.

3.1.1. Kriptovalute kao sredstvo razmjene

U nastavku se navode prednosti i nedostaci bitcoin kriptovalute kao sredstva razmjene u funkciji novca, pri čemu se sve navedene karakteristike odnose na sve blockchain kriptovalute[18]. Kao prva prednost se naglašava sigurnost decentralizirane glavne knjige koju uživaju njeni korisnici. Naime, prilikom kupnje robe ili usluga, svi privatni ključevi su u vlasništvu kupca i sigurnosni propust kod trgovca ne kompromitira privatne ključeve kupca, odnosno njegova sredstva nisu ugrožena. Ugrožena su samo sredstva povezana s novim javnim ključem trgovca. S druge strane, da bi se transakcija provela, kupac mora pokrenuti aplikaciju, povezanu s njegovim novčanikom, da bi privatnim ključem digitalno potpisao transakciju. U tom slučaju postoji rizik sigurnosnog propusta digitalnog novčanika. Sljedeća prednost koja je često predmet rasprave su transakcijski troškovi. Pristalice bitcoina naglašavaju da su transakcijski troškovi niži od naknada za debitne i kreditne kartice. S druge strane, kritičari ističu da nakon što se dodaju svi troškovi, poput zaštite od krađe, bitcoin nema značajnu troškovnu prednost. S aspekta trgovca, prednost Bitcoin protokola je i nepovratnost, odnosno njegova karakteristika jednosmjerne transakcije. Jednom kada se transakcija zapiše na bitcoin blockchain, pod uvjetom postignutog konsenzusa najdužeg lanca blokova, transakcija je nepovratna. Takvo svojstvo odgovara trgovcima jer ih osigurava od rizika prijevare koji uključuje povrat sredstava prema kupcu nakon isporučene robe ili usluga trgovaca. S druge strane, trgovci su u tom slučaju u prednosti jer su kupci ti koji su izloženi riziku. Međutim, navedeni se problem može riješiti implementacijom već spomenutog tehničkog rješenja *lightning network*, gdje bi reverzibilna transakcija bila moguća. Kao jedna od značajnijih prednosti Bitcoin transakcijskog sustava navodi se brzina realizacije transfera bitcoina u odnosu na tradicionalni bankarski sustav gdje transakcija može potrajati i do nekoliko dana. Međutim, drugi oblici plaćanja, kao što su debitne kartice, imaju čak i kraće vrijeme provedbe transakcije, ali se također implementacijom

[18] Ovdje je potrebno izuzeti nedostatke brzine transakcijskog sustava za kriptovalute koje su implementirale *dokaz o udjelu* konsenzus algoritam. Dokaz o udjelu konsenzus algoritam je zapravo jedno od rješenja čiji je cilj ubrzanje konfirmacija transakcija na blockchain distribuiranu bazu.

lightning network-a, njihova prednost gubi u odnosu na Bitcoin transakcijski sustav. Također, u bitcoin transakciji kupac je taj koji inicira i generira transakciju sredstava svojim digitalnim potpisom. Suprotno, kod drugih platnih sustava, poput sustava plaćanja kreditnim karticama, kupac autorizira trgovca te otkriva svoje osjetljive podatke, kao što je broj kartice, a trgovac zatim povlači sredstva terećenjem korisnikovog računa. U tom slučaju Bitcoin transakcijski sustav ima prednost jer su korisnici ti koji kontroliraju postupak kupnje. Prednost blockchain transakcijskog sustava je i u kontroli prezentiranja podataka prema javnosti. Bitcoin transakcije mogu biti manje ili više anonimne od tradicionalnih sustava plaćanja. Nitko ne mora znati ime osobe ili institucije iza javnog ključa na koji su doznačena sredstva, osim ukoliko se vlasnik ključeva samoinicijativno ne otkrije javnosti. Jednom kada se javni ključ poveže s entitetom iza njega, moguće je pratiti sve transakcije povezane s tim javnim ključem, odnosno pristup kompletnim financijskim podacima korisnika, što se smatra nedostatkom.

Jedan od nedostataka kriptovaluta u svojstvu sredstva razmjene predstavlja kompleksnost blockchain tehnologije, odnosno infrastrukture koja stoji iza kriptvaluta. Pretpostavlja se da bi većina korisnika kriptovaluta na kraju koristila posrednike, što zbog praktičnosti, što zbog zahtjevne tehnologije. U tom smislu, tehnologiju bi u prvenstveno koristile tvrtke, što znači da ne bi došlo do značajnijih smanjenja troškova krajnjih svakodnevnih korisnika. Kao jedan od nedostataka smatra se i značajnost postojećih mreža fiat valuta koje svojom veličinom onemogućavaju konkurenciju alternativnim sredstvima razmjene. Ovaj nedostatak je i usko povezan s nedostatkom vezanim za regulativni okvir kojim se uopće definira mogućnost postojanja paralelnog sustava plaćanja alternativnim valutama. U državama gdje je njihova uporaba zabranjena, kriptovalute niti ne mogu služiti kao sredstvo razmjene. Za razliku od tradicionalnih transakcijskih sustava kreditnim karticama koje u sebi imaju integrirane oblike kreditiranja, nedostatak transakcijskog sustava kriptovaluta je taj što, za sada, ne nudi mogućnost sličnog oblika kreditiranja kao što to nude kreditne kartične kuće. S druge strane, razvojem uvjetovanih transakcija kroz pametne ugovore na *lightning network*-u, osim što bi se ovaj nedostatak otklonio, razvili bi se i puno napredniji oblici plaćanja, odnosno mogućnosti plaćanja s odgodom i/ili naknadom. Kao jedan od glavnih, trenutnih, nedostataka bitcoin transakcijskog sustava, odnosno svih sustava koji se baziraju na *dokaz o radu*

konsenzus algoritmu, je vrijeme trajanja konfirmacije transakcije. Bez obzira na unapređenje transakcijskog sustava kroz *lightning network*, većina trgovaca još uvijek nije implementirala isti. To znači da transakcije prema njima u prosjeku traju oko 10 minuta (ovisno o veličini uključene naknade i težini rudarenja). U trenutku kada je kriptovaluta poslana prema trgovcu, ona ulazu u bazu nepotvrđenih transakcija te se zaključava. Drugim riječima, niti kupac, niti trgovac ne mogu raspolagati sa sredstvima na njihovim javnim ključevima sve dok se transakcija ne potvrdi. Pored toga, sa aspekta bitcoin sustava, tu je i problem skalabilnosti. Ukoliko se u prosjeku svakih 10 minuta potvrdi jedan blok transakcija, a jedan blok transakcija sadrži do 2.500 transakcija, to znači da bitcoin transakcijski sustav u prosjeku obradi oko 4 transakcije po sekundi, a maksimalno do 7 transakcija, što je, u komparaciji sa tradicionalnim sustavom kartičnog plaćanja poput viza-e koja obradi do 1.700 transakcija po sekundi, izrazito malo i bitcoin sustav čini nepraktičnim za širu implementaciju.

3.1.2. Kriptovalute kao sredstvo očuvanja vrijednosti

Glavna kritika kriptovaluta u svojstvu sredstva očuvanja vrijednosti proizlazi iz njihove cjenovne volatilnosti u paritetu s drugim valutama ili robom. Da bi neka valuta obnašala funkciju novca, kao takva bi morala osigurati donekle stabilan tečaj zbog prijenosa vrijednosti kupovne moći iz sadašnjosti u budućnost. Zbog toga se kriptovalute, barem za sada, više smatraju kao nova, rizična digitalna imovina koja pruža mogućnost ulaganja, nego stabilno sredstvo očuvanja vrijednosti. S druge strane, u komparaciji s fiat valutama, bitcoin ima nizak promet koji se djelomično može objasniti njegovim skladištenjem. Drugim riječima, više korisnika ulaže u bitcoin s ciljem ostvarenja kapitalnog prinosa, nego što ga koristi u transakcijske svrhe. Prema tome, iz svega proizlazi da, zbog svoje volatilnosti, bitcoin ne predstavlja adekvatno sredstvo za očuvanje vrijednosti u nekom kratkoročnom razdoblju, ali da dugoročno pruža investicijsku priliku zbog optimističnih cjenovnih očekivanja.

U nastavku se navode prednosti i nedostaci bitcoin kriptovalute kao sredstva očuvanja vrijednosti u funkciji novca, pri čemu se sve navedene karakteristike odnose na sve blockchain kriptovalute, s obzirom da počivaju na tehnologiji s istim karakteristikama. Franco (2015) navodi da se bitcoin ne može konfiscirati, kontrolirati

ili nerazmjerno oporezivati za razliku od fiat valuta ili plemenitih metala koji se mogu fizički oduzeti ili oduzeti putem financijskih posrednika gdje su sredstva deponirana. Suprotno tome, korisniku koji posjeduje bitcoin se ne može uskratiti pristup sredstvima sve dok on raspolaže sa svojim privatnim ključevima. Jedini je uvjet pristup internetu. Prednost kriptovaluta je i u tome što se za njihovo držanje ne naplaćuju dodatni troškovi, poput troškova vođenja računa u tradicionalnom bankarskom sustavu. Kao prednost se ističe i njihova prenosivost. Privatni ključ, potreban za autorizaciju transakcije, se može prenositi na različitim medijima poput memorijski disk, pohrana u oblak (engl. *cloud storage*), ispis na papir u fizičkom obliku (engl. *cold storage*) ili na posebno izrađene uređaje za pohranu privatnih ključeva koji nalikuju memorijskom disku.

Kada se razmatra bitcoin, broj jedinica valuta u opticaju je definiran programskim kodom. Da bi se provela promjena na programskom kodu i promijenio njihov konačni broj, potreban je konsenzus svih korisnika u zajednici, točnije razvojnih programera i rudara. Prema tome, niti jedno središnje tijelo ili centralna banka ne odlučuje o količini jedinica valute u opticaju, što znači da deprecijaciju, odnosno devalvaciju nije moguće provesti. Navedeno svojstvo se tumači na različite načine i pruža oprečna razmišljanja. Pristalice ideje decentralizacije smatraju da je uzimanje moći upravljanja količinom valute u opticaju od centralnih banaka zapravo pozitivno stanje, te da centralne banke ne ispunjavaju svoju osnovnu funkciju u smislu povećanja konjunkture gospodarstva provedbom monetarne politike. S druge strane, izuzimanje centralnog tijela u funkciji stabilizacije vrijednosti valute i prevaljivanje takve aktivnosti na nestručno osoblje kritičari smatraju nedostatkom, te smatraju da bi takve aktivnosti ipak trebalo prepustiti stručnim osobama iz tog područja. Drugim riječima, ukoliko bitcoin kao valuta zaživi u još širem formalnom omjeru, u budućnosti se možda može očekivati suradnja između razvojnih programera i monetarnih stručnjaka, koji bi kroz savjetodavnu ulogu posredno mogli doprinijeti gospodarskim aktivnostima neke države. S druge strane, u slučaju nekih drugih kriptovaluta, poput ripplea (XRP), sve jedinice valute su već puštene u opticaj, tako da one niti nisu predmet rasprave takvih mogućnosti. Prednost kritovaluta u svojstvu sredstva očuvanja vrijednosti je njihova sigurnost koja se zasniva na kriptografiji. Da bi zlato ili fiat valute, zapravo bilo koja pokretnina značajnije vrijednosti, bila sigurna od potencijalne krađe, potreban je fizički sef ili financijska institucija koja će pružati

uslugu njenog čuvanja. Također, prilikom promjene vlasništva, odnosno prijenosa jedinca valute, blockchain osigurava automatsko provođenje i vođenje zapisa o njihovom vlasništvu.

Nedostaci kriptovaluta u funkciji sredstva očuvanja vrijednosti su prvenstveno vezani za već spomenutu volatilnost, odnosno nemogućnost intervencija središnje institucije na stabilnost njihovog tečajnog pariteta kroz ponudu. S druge strane, količina jedinca valute u opticaju bi se mogla mijenjati preko konsenzusa oko otvorenog programskog koda, što se uzima kao negativna konotacija zbog nestručnih ljudi koji bi bili uključeni u takav proces. Također, u mnogim državama kriptovalute nemaju status legalnog sredstva plaćanja i njihova upotreba, kao trgovina s njima, je strogo zabranjena i kažnjiva. Zabrana proizlazi iz prevencije nelegalnih aktivnosti s kriptovalutama kao što je pranje novca ili naprosto postizanja veće kontrole nad njima. Međutim, transakcijski sustav kriptovaluta počiva na distribuiranim bazama pa se nameće pitanje je li takva zabrana uopće moguća. Ekosustav kriptovaluta poznaje samo granicu transfera vrijednosti od fiat valuta prema kriptovalutama. Jednom kada se sredstva deponiraju u ekosustav kriptovaluta, ograničenja ne postoje, odnosno postoje samo ukoliko potencijalni korisnici nemaju pristup internetu. To su zapravo i jedini načini kako se kriptovalute donekle mogu kontrolirati. Ili korisnicima ograničiti pristup internetu ili ograničiti transfere fiat valuta prema institucijama koje pružaju takvu uslugu (engl. *gateway*).

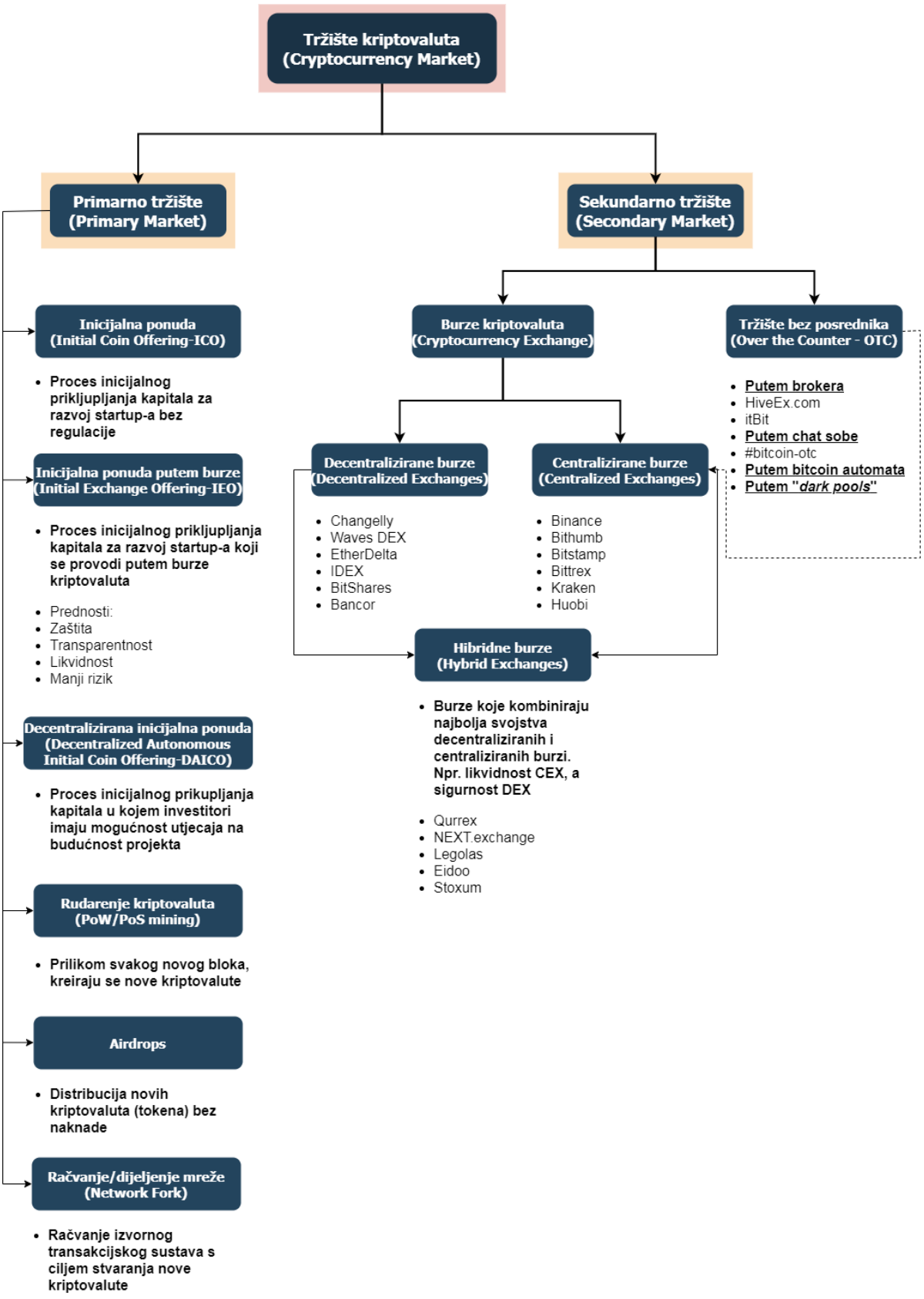
Kao nedostatak kriptovaluta se navodi i odsutnost njihove intrinzične vrijednosti. Kriptovalute u pozadini nisu podržane s nekom fizičkom imovinom poput plemenitih metala. Kriptovalute predstavljaju zapis nepotrošenih izlaza u distribuiranoj tablici (engl. *unspent transaction output*-UTXO) povezan s javnim ključem korisnika i kao takve nemaju fundamentalnu vrijednost. S druge strane, kriptovalute koje počivaju na konsenzusu *dokaz o radu*, mogu se povezati troškovima potrebnim za njihovo rudarenje, iz čega proizlazi da je njihova fundamentalna vrijednost jednaka vrijednosti utrošene energije i vrijednosti kupljene opreme potrebne za rudarenje. Za razliku od bankovnih depozita, korisnici bitcoin mreže nemaju mogućnost osiguranja sredstava. U slučaju gubitka privatnih ključeva, jedinice valute povezane s njima su bespovratno izgubljene, što predstavlja dodatni nedostatak.

3.1.3. Kriptovalute kao obračunska jedinica

Bitcoin se, za sada, ne može smatrati adekvatnom obračunskom jedinicom. Iako se bitcoin može zamijeniti za različite proizvode i usluge, rijetko koji trgovci kotiraju cijene izražene u bitcoin valuti. Iskazivanje maloprodajne cijene u bitcoin valuti zahtijeva implementaciju digitalnih zaslona s mogućnosti prikazivanja cijene do osam decimalnih mjesta. Pored toga, cijene se moraju iskazati i preračunati u bitcoin valutu u realnom vremenu, što zahtijeva kontinuirano ažuriranje i povezanost sa burzama kriptovaluta, a trenutno se jako malo proizvoda inicijalno iskazuje u protuvrijednosti bitcoina. Primjer toga je oprema za rudarenje kriptovaluta ili digitalni novčanici koji se isključivo proizvode u tu svrhu. Također, prisutan je i problem velikog raspona cijena kriptovaluta na različitim tržištima. Trgovci se ne bi mogli oslanjati na samo jedan izvor za iskazivanje referentne vrijednosti bitcoina, već bi morali koristiti prosječene vagane indekse cijena prema, na primjer, volumenu trgovanja sa pripadajuće burze. S druge strane, cijene robe i usluga se mogu iskazivati u fiat valuti, a da trgovac prihvaća kriptovalutu kao jedan od oblika plaćanja. U tom slučaju cijenu je potrebno preračunati jednom kod plaćanja. Međutim, i to zahtijeva povezanost sa institucijama koje pružaju vjerodostojan paritet tečaja BTC/fiat. Postoji nekoliko rješenja, ali i razmišljanja u smjeru otklanjanja ovog problema. Prvo potencijalno rješenje koje se nameće je očekivanje stabilizacije tečaja bitcoin kriptovalute u odnosu na fiat valute u budućnosti. Drugo je stvaranje bitcoin ekosustava, odnosno ekonomskog okvira gdje se sva povezana dobra potrebna za proizvodnju robe i usluga izražavaju u cijeni bitcoina, pa tako problem volatilnosti tečaja nije niti prisutan. Međutim, za sada takvo rješenje nije moguće.

4. KLASIFIKACIJA TRŽIŠTA KRIPTOVALUTA

Kriptovalute predstavljaju novu vrstu digitalne imovine koja, kao što je već navedeno, ne ulazi u postojeće okvire definicija tradicionalnih financijskih instrumenata. Bitcoin transakcijski sustav je program koji je pušten u javnost, te iza njega ne stoji institucija ili pojedinac odgovoran za buduće aktivnosti na programskom kodu koje definiraju njegove mogućnosti. S druge strane, zbog prirode otvorenog programskog koda i praktične implementacije blockchain tehnologije, mlade i inovativne tvrtke su prepoznale mogućnost prikupljanja početnog kapitala potrebnog za svoj inicijalni razvoj kreiranjem i emitiranjem kriptovaluta. Pored toga, pozitivna reakcija javnosti na ideju decentralizacije doprinijela je stvaranju uvjeta ponude i potražnje te je tako nastalo potpuno novo primarno tržišta kriptovaluta. Razvojem primarnog tržišta povećao se i broj mjenjačnica/burzi na kojima se aktivno trgovalo čime je stvoren jedan novi, samostalno održivi, ekosustav primarnog i sekundarnog tržišta kriptovaluta.



Shema 2. Tržište kriptovaluta

Izvor: Izrada autora

Shema 2. Ilustrira podjelu tržišta kriptovaluta. Tržište kriptovaluta predstavlja tržište nove prenosive digitalne imovine, što znači da je njihovom razmjenom omogućen prijenos njihovog vlasništva između trgovaca i investitora. Sukladno tome, jednako kao i na tradicionalnom tržištu financijskih instrumenata, tržište kriptovaluta se može definirati kroz primarno tržište, tržište na kojem kroz određene aktivnosti i procese kriptovalute nastaju po prvi puta, i sekundarno tržište koje omogućuje njihovu naknadnu razmjenu između interesnih strana.

4.1. Primarno tržište

Sa aspekta tradicionalnog tržišta kapitala, primarno tržište se definira kao tržište novoizdanih financijskih instrumenata putem kojeg se omogućava transfer sredstava od štediša/investitora (osoba i/ili institucija) s viškom kapitala prema pravnim osobama s manjkom kapitala potrebnim za svoj razvoj. Koncept financiranja emitiranjem kriptovaluta ne odstupa previše od prethodne definicije. Naime, s jedne strane postoje investitori s viškom kapitala koji vjeruju u prezentiranu ideju startupa zasnovanu na blockchainu, a s druge strane inovativne tvrtke kojima su sredstva potrebna za razvoj i koje svoju ideju financiraju emitiranjem kriptovaluta, čime se zadovoljava mobilizacijska funkcija tradicionalne definicije financijskih tržišta. Međutim, za razliku od primarnog tržišta tradicionalnih financijskih instrumenata, kriptovalute se temelje na programskom kodu preko kojeg je njihova emisija strogo pred definirana, ali koji dopušta veću fleksibilnost u dinamici njihovog inicijalnog stvaranja prilikom financiranja startupova. Također, u usporedbi sa tradicionalnim i uhodanim načinom transfera sredstava, financiranje kriptovalutama koristi koncept grupnog financiranja (engl. *crowdfunding*).

Grupno financiranje predstavlja revolucionarni koncept pokrenut još 2006. godine tijekom Web 2.0 ere i od tada je postigao veliku popularnost. Opisuje se kao alternativni izvor financiranja gdje veliki broj investitora transferira sredstva u manjim apoenima prema vlasniku projekta, najčešće putem interneta, odnosno putem platformi namijenjenim za grupno financiranje. Grupno financiranje se provodi kroz javni poziv za financijsko ulaganje distribuiran među velikom skupinom korisnika koji procjenjuju i podržavaju poslovni koncept vlasnika projekta. Prednost ovakvog oblika

financiranja se očituje kroz sposobnosti okrupnjavanja novca od pojedinaca koji imaju zajednički interes i koji su spremni dati mali doprinos projektu (Lynn i Sabbagh 2012). Za razliku od drugih oblika financiranja preko kojih se posredno uključuju odabrani investitori za projekte visokih očekivanja, grupno financiranje je postalo popularno za financiranje manjih projekata koji su najčešće tek u svojoj početnoj idejnoj fazi. Grupno financiranje podrazumijeva komponentu tradicionalnog oblika programa financiranja učinkovito olakšavajući interakciju između vlasnika projekta i pojedinca koji su spremni financirati odabrani projekt. Drugim riječima, za provedbu financiranja jednog projekta potrebno je uključiti barem još jednu treću stranu, najčešće banka, koja će pružati uslugu platnog prometa i olakšati potrebne financijske transakcije. Prema tome, bilo koji projekt grupnog financiranja uključuje najmanje tri aktera: investitori koji ulažu novac, posrednik koji prenosi novac i vlasnici projekta koji traže novac. Svi oni preuzimaju različite rizike potrebne za uspješno grupno financiranje. Za razliku od tradicionalnog financiranja listanjem vlasničkih financijskih instrumenata, grupno financiranje pruža prednost poduzetnicima zbog toga što im, ovisno o prethodno dogovorenim uvjetima, pruža mogućnost zadržavanja prava na donošenje strateških poslovnih odluka, dostupnost nisko rizičnog kapitala, dostupnost relativno brzog izvora financiranja u smislu ne postojanja nužnosti procjene kreditne sposobnosti poduzetnika itd. S druge strane, unatoč mnogim prednostima, grupno financiranje uključuje i neke nedostatke kao što je veliko oslanjanje na posrednika i slaba zaštita potencijalnih investitora. Navedeni nedostaci se uspješno otklanjaju uključivanjem blockchain tehnologije u proces grupnog financiranja, što su prepoznali mladi i inovativni startupovi i jednim komplementarnim pristupom iskoristili najbolje od oba koncepta i kreirali novi koncept financiranja izdavanjem različitih vrsta kriptovaluta kroz njihovu inicijalnu ponudu (engl. *initial token offering* - ICO).

Iako je inicijalna ponuda kriptovaluta funkcijski vrlo slična inicijalnoj javnoj ponudi dionica (engl. *initial public offering* - IPO), njihove se strukture i procesi značajno razlikuju. Tako, na primjer, proces IPO-a najčešće za treću stranu provodi investicijska banka, dok se kod ICO-a najčešće provodi od strane samog predlagatelja i vlasnika projekta. Za IPO je potrebno više različite dokumentacije odobrene od strane regulatora, dok je za ICO potreban dokument koji opisuje tehnološko rješenje projekta (engl. *whitepaper*) i internet stranica. Uspješnost emisije

značajno ovisi i o marketinškim kanalima koji su kod IPO-a puno „ozbiljniji“, dok se kod ICO-a koriste različiti medijski i komunikacijski kanali. Proces prodaje, odnosno zamjene sredstava za emitiranu imovinu je također različit. Za ICO se najčešće koristi automatiziran proces kroz pametne ugovore gdje se u zamjenu za tu novu kriptovalutu prema platformi šalju najčešće bitcoin ili ethereum, dok se za IPO novoizdani instrumenti alociraju vlasniku preko financijskog posrednika. Nakon izdavanja, dionice se listaju na uređenim tržištima, dok se kriptovalute listaju na burzama kriptovaluta (trgovinske platforme/mjenjačnice). Jedna od značajnijih razlika se odnosi na sama prava koja proizlaze iz držanja kriptovaluta, odnosno dionica. Držanje kriptovaluta ne pruža dodatno formalno pravo utjecaja na razvoj projekta ili proizvoda, dok vlasnici dionica, preko skupštine dioničara, imaju mogućnost utjecaja na strateške odluke društva. Također, značajna je razlika i u tome što se financiranje kriptovalutama najčešće provodi tek za projekte u nastajanju, dok se kod IPO-a dionice emitiraju za već postojeće poslovne subjekte, s uhodanim i profitabilnim poslovanjem. Za razliku od IPO-a dionica koji je više lokalan u smislu države u kojoj se provodi, ICO-i se provode na globalnoj razini, što predstavlja jednu do značajnijih prednosti ICO-a u odnosu na tradicionalne IPO-e.

Quest (2018) definira inicijalnu ponudu tokena kao mehanizam koji se koristi za prikupljanje sredstava, odnosno za financiranje projekata vezanih uz kriptovalute, a najčešće ga koriste startupovi kao način izbjegavanja reguliranih mehanizama za prikupljanje kapitala preko banaka ili drugih financijskih institucija, kao što su fondovi poduzetničkog kapitala (engl. *venture capital* - VC). Iako su od drugog kvartala 2017. godine do drugog kvartala 2018. godine ICO-i dominirali u području financiranja blockchain startupova, od trećeg kvartala 2018. godine VC fondovi preuzimaju vodeću poziciju u tom segmentu. Razlog tome je već prethodno spomenuti nedostatak regulatornog okvira kod ICO-a, što je rezultiralo da je oko 80% svih ICO-a provedenih u tom razdoblju predstavljalo neki oblik prijevare investitora.

ICO projekti se obično odnose na tehnološki bazirane eksperimente povezane s unapređenjem područja blockchain tehnologije, kriptovaluta i općenito povezane s implementacijom tehnologije kojom se provodi decentralizacija nekih poslovnih procesa, usluga itd. Također, to su projekti usmjereni prema već postojećim investitorima u području kriptovaluta. Vlasnici i voditelji takvih projekata su najčešće

razvojni programeri koji vide prostor za praktičnom implementacijom blockchain tehnologije u određeni segment poslovanja. S druge strane, tokom 2017. i 2018. godine sve više je špekulanata bez tehničkog znanja pokazalo interes za ulaganje u blockchain startupove, pri čemu je njihov glavni motiv bio ostvarivanje profita kroz rast vrijednosti kriptovalute. Prilikom provedbe ICO-a, svaki startup putem *whitepapera* pruža informaciju edukativne i promotivne prirode s ciljem predstavljanja određenog rješenja tehnologije distribuiranog zapisa kroz svoj proizvod ili uslugu potencijalnom investitoru. W*hitepaper* služi da se investitori informiraju o odredbama i uvjetima tokena koji kupuju, pri čemu taj dokument nije zakonski obvezujući već je samo jedan od marketinških alata kojeg koriste vlasnici projekta. U predstavljenoj dokumentaciji trebao bi biti razrađen plan s objašnjenjem projekta, problemima koji će se riješiti kroz implementaciju projekta, količini sredstava potrebnih za financiranje projekta i postotak sredstava koji vlasnici zadržavaju za sebe ukoliko projekt zaživi. Postoji više tipova ICO-a sa različitim karakteristikama, dinamici otpuštanja novih kriptovaluta, vremenu trajanja, strukturi traženog iznosa itd. Najzastupljeniji tip je prodaja fiksnog broja nove kriptovalute po fiksnoj cijeni i principu sukcesivne prijave, dok se ne prodaju sve kriptovalute planirane za prodaju[19]. S druge strane, ukoliko se ne skupe planirana sredstva, do tada prikupljena sredstva se vraćaju investitorima, a ICO se klasificira kao neuspješan. Ukoliko su prikupljena dostatna sredstva, projekt se pokreće i sredstva se mogu upotrijebiti za nastavak projekta. Investitori mogu aplicirati u ICO proces samostalno putem internet stranice projekta, ili putem platformi za zajednička ulaganja kroz tzv. ICO *pools*. U tom slučaju, investitorima se osigurava barem minimalna provjera ljudi koji predstavljaju tim projekta, njihove stručnosti i legitimiteta[20].

Bez obzira na manji tržišni udio u komparaciji s fondovima za rizična ulaganja, odnosno na povezane rizike, ICO-i se provode i dalje. Sukladno Lee Kuo Chuen i Low (2018), sa aspekta startupa prednosti financiranja putem ICO-a u odnosu na fondove se mogu sažeti u nekoliko sljedećih točaka. Kao prvi razlog se navodi niži trošak financiranja. ICO-i smanjuju troškove prikupljanja sredstava u značajnoj mjeri, što za tvrtke koje su u fazi nastajanja može biti izrazito važno. U usporedbi s tradicionalnim VC metodama prikupljanja kapitala, gdje je uži krug potencijalnih

[19] Više o drugim tipovima ICO-a vidjeti Lee Kuo Chuen i Low (2018).
[20] https://crypthena.com/ico-pools/

investitora, ICO-i su otvoreni za javnost omogućavajući startupovima prikupljanje većeg iznosa novca. Također, kao prednost se navodi i odsutnost obveze ispunjavanja zahtijeva revizije, pripreme dokumentacije ili pravnog odobrenja. Drugim riječima, financiranje putem ICO-a i izdavanje digitalne imovine koja se klasificira kao kriptovaluta, ne podliježe zakonskim i regulativnim normama. U tom slučaju, prednost ICO-a u odnosu na VC metodu financiranja je također i u pravima koji ne(proizlaze) iz tako provedenog oblika financiranja. Primjenom ICO metode financiranja razvojni programeri, koji su u najčešćem slučaju nositelji i vlasnici projekta, se ne moraju odreći kontrole u svom startupu. Osim što dobivaju sredstva bez odricanja udjela u vlasničkoj strukturi, ICO-i mogu doprinijeti povećanju interesa šire zajednice za projektom, a prikupljena sredstva mogu pomoći timu da bolje razvije projekt kako bi se osigurao njegov dugoročno održivi rast.

Sukladno Shemi 2. proces prikupljanja kapitala putem grupnog financiranja emitirajući kriptovalutu se može provesti i putem burzi kriptovaluta (engl. *initial exchange offering* – IEO). U tom slučaju burze preuzimaju značajnu ulogu u funkciji jamstva uspješnog financiranja i svojim aktivnostima pružaju određene prednosti projektu za koji se prikupljaju sredstva, kao što su: zaštita ulaganja, transparentnost, likvidnost novih kriptovaluta i u konačnici manji rizik. Sa aspekta investitora, nedostatak ICO procesa je nepovratnost sredstava, odnosno nemogućnost utjecaja investitora na tijek razvoja projekta. Investitor koji se ne slaže sa smjerom razvoja startupa, iz svoje pozicije može izaći jedino prodajom kriptovaluta na sekundarnom tržištu. Kako bi se otklonio ovaj nedostatak i eventualno privuklo više zanimanja za ulaganje u projekte putom ICO-a, razvojni programeri su doradili postojeći proces ICO-a dajući veću mogućnost utjecaja investitora na tijek razvoja projekta kroz pametne ugovore, odnosno koncept decentralizirane autonomne inicijalne ponude (engl. *decentralized autonomous initial coin offering* – DAICO). DAICO koncept pruža vlasnicima tokena mogućnost glasovanja za budućnost projekta te povrat sredstava ukoliko nisu zadovoljni napretkom koji su postigli razvojni programeri. S druge strane, za projekte koji implementiraju DAICO koncept, programerima će se pružiti određena odgovornost, a vlasnici tokena zauzvrat dobivaju dodatnu sigurnost koja jamči da će vidjeti barem minimalno održivi proizvod.

Pred definirana dinamika otpuštanja jedinica vrijednosti valute za kriptovalute koje nisu prethodno puštene u opticaj u potpunosti se također može smatrati primarnim tržištem kriptovaluta. U tom slučaju, prilikom svakog potvrđenog novog bloka transakcija, kreiraju se nove kriptovalute koje povećavaju broj jedinica valute u opticaju. Pored toga, blockchain ekonomije su decentralizirane kompjutorske platforme koje pružaju mogućnost kreiranja novih kriptovaluta kao utilizacijskih tokena na matičnom blockchainu. Tako kreirani novi utilizacijski tokeni mogu biti rezultat grupnog financiranja putem inicijalne ponude, ali mogu biti kreirani i distribuirani kao *airdrops*, što također predstavlja primarno tržište. *Airdrops* predstavlja distribuciju novih tokena vlasnicima postojeće kriptovalute blockchain ekonomije na kojoj se utilizacijski token kreira bez potražnje za sredstvima ili naknadom u bilo kojem obliku. Uvjet zaprimanja *airdrops* tokena je držanje matične kriptovalute u novčanicima ili na burzama kriptovaluta koje takvu akciju podržavaju. U nekim situacijama, *airdrops* se provode samo uz registraciju korisnika na internet stranicama projekta koji provodi aktivnost distribucije novih tokena.

Račvanje svojevrsno kloniranje izvornog programskog koda (engl. *network fork*), ali u ovom slučaju sa svim prethodno zapisanim transakcijama, se isto može tretirati kao oblik primarnog tržišta kriptovaluta. Naime, blockchain transakcijskim protokolom se upravlja usuglašavanjem između razvojnih programera koji održavaju i razvijaju sustav putem platformi za kolaboraciju. Da bi se određena promjena prihvatila i implementirala u transakcijski sustav u punom omjeru, potreban je konsenzus svih punih čvorova (engl. *full nodes*) u mreži koji vrše funkciju propagacije i potvrđivanja transakcija. U situaciji kada dođe do razilaženja u razmišljanjima, neki čvorovi ne moraju prihvatiti implementaciju promjena, što znači da se zadržavaju na izvornom transakcijskom protokolu. S druge strane, čvorovi koji podržavaju izmjenu sustava, nadograđuju transakcijski protokol i usmjeravaju svoju opremu za rudarenje na taj novi sustav koji uključuje i nove karakteristike poput naziva kriptovalute, brzinu transakcija, veličinu memorije za transakcije i neka druga, nova svojstva. U tom se slučaju zapravo postojeći broj kriptovaluta izvornog blockchaina duplicira i doznačava na javne ključeve vlasnicima izvorne kriptovalute, ali kao potpuno nova kriptovaluta sa svim implementiranim promjenama i unapređenjima. Najpoznatiji primjeri takvog unapređenja protokola su se dogodili na Ethereum mreži gdje je od izvornog protokola nastavo novi Ethereum s implementiranim promjenama (u ovom slučaju je

novi protokol zadržao izvorni naziv), a stari je promijenio naziv u Ethereum classic, također i na Bitcoin protokolu, gdje je iz izvornog Bitcoin protokola kreiran novi Bitcoin cash transakcijski protokol. Sve ovo su različiti oblici kreiranja i emitiranja novih kriptovaluta pa se iz tog razloga smatraju primarnim tržištem.

4.2. Sekundarno tržište

Promatrano u kontekstu primarne svrhe, a to je funkcija pružanja ponude i potražnje listane imovine, sekundarno tržište kriptovaluta ne odstupa previše sekundarnog tržišta tradicionalnih financijskih instrumenata i dijeli se na burze koje predstavljaju uređeno tržište, i tržište bez posrednika ili preko šaltera (engl. *over the counter* - OTC). Međutim, osim sličnosti po primarnoj funkcijskoj svrsi, između njih postoji niz operativnih razlika koje prvenstveno proizlaze zbog prirode kriptovaluta. Jedna od značajnijih razlika sekundarnog tržišta kriptovaluta, u odnosno na tradicionalno tržište financijskih instrumenata, je postojanje decentraliziranih burzi kriptovaluta. U tom slučaju vlasnici kriptovaluta ne šalju svoje kriptovalute na burzu ili prema brokeru preko kojeg žele trgovati – što je slučaj kod centraliziranih burzi kriptovaluta, nego su kriptovalute cijelo vrijeme vezane za javne ključeve izvedene iz privatnih ključeva koji se nalazi kod vlasnika. Niža likvidnost decentraliziranih burzi i nemogućnost implementacije naprednijih programskih rješenja od strane kreatora tržišta (engl. *market maker*), potaknulo je razvoj najnovijih hibridnih rješenja u vidu burzi kriptovaluta koje kombiniraju najbolje od oba prethodna slučaja.

Najpopularniji način prve, inicijalne kupovine kriptovaluta na sekundarnom tržištu je preko OTC tržišta, odnosno izravno putem različitih internetskih platformi poput Bitcoin mjenjačnice[21], Uphold platforme[22] itd., ili putem uređenih platformi za njihovu razmjenu (burzi) koje pružaju mogućnost depozita fiat novca putem bankovnog transfera, PayPal-a i/ili kreditnih ili debitnih kartica, poput Bitstamp, Binance, Kraken burze itd[23]. Trenutno u HR je moguće kupiti kriptovalute kroz 12 internet platformi koje podržavaju kupnju preko jedinstvenog područja plaćanja u eurima (engl. s*ingle*

[21] https://bitcoin-mjenjacnica.hr/#exchange
[22] https://uphold.com/
[23] Na internet stranici https://www.buybitcoinworldwide.com/ se mogu pronaći informacije gdje i na koji način kupiti kriptovalute iz HR.

euro payments area – SEPA), a 8 platformi podržava kreditne i debitne kartice[24]. Ovisno o ciljevima ulaganja, potrebno je odabrati najbolju metodu. Na primjer, dnevni trgovci s kriptovalutama najčešće koriste tradicionalne burze kriptovaluta ili brokerske platforme za njihovu razmjenu zbog kvalitete usluge koju platforme pružaju, poput likvidnosti, većeg izbora mogućih parova za trgovinu, potencijalnog pasivnog prihoda koji proizlazi iz držanja kriptovaluta vezanih za adrese vlasnika itd. Međutim, ukoliko je konačni cilj kupnja kriptovaluta i držanje zbog stjecanja dugoročnog kapitalnog prinosa, dovoljne su platforme koju pružaju OTC trgovinu, s adekvatnim odabirom novčanika za njihovo čuvanje.

4.2.1. Centralizirane burze

Centralizirane burze kriptovaluta (engl. *centralized cryptocurrency exchange* - CEX) posluju po principu tradicionalnih burzi financijskih instrumenata. Njihova primarna svrha je spajanje kupaca i prodavatelja kriptovaluta, pri čemu burza ima ulogu posrednika između prodavatelja i kupca te za to naplaćuje proviziju. Nedostatak centraliziranih burzi je upravo njihova centralizacija, odnosno način kojim raspolažu sa sredstvima svojih korisnika. Naime, transakcijski sustavi kriptovaluta počivaju na ideji decentralizacije, što znači da se prilikom njihove razmjene izbjegava alokacija sredstava centralnom entitetu kao posredniku u transakciji. S druge strane, trgovanje na CEX burzama upravo zahtijeva odricanje kontrole nad svojim sredstvima jer, da bi se aktivno trgovalo na njima, sredstva se moraju prvo deponirati[25] na adresu (javni ključ) koja je, preko odgovarajućeg privatnog ključa, isključivo i u kontroli samo CEX burze. Drugim riječima, centralizirane burze pružaju prividnu kontrolu nad sredstvima svojim korisnicima, iz čega proizlazi njihov glavni nedostatak, a to je sigurnost, odnosno ranjivost na hakerske napade. Postoji više primjera uspješnih hakerskih napada na centralizirane burze širom svijeta, a najpoznatiji među njima je napad koji se dogodio na japanskoj burzi Mt Gox 2014. godine, iz koje je „pokradeno“ 850 tisuća bitcoina, što je u to vrijeme u protuvrijednosti u dolarima iznosilo 450 milijuna dolara, a danas po cijeni bitcoina od 9.092 dolara, više od 7 milijardi dolara. Iako je 200 tisuća bitcoina spašeno, preostalih 650 tisuća nikada nije pronađeno. S druge strane,

[24] Osim navedenih metoda, kriptovalute je moguće kupiti i preko bankomata. Na datum 28.06.2020. u Hrvatskoj trenutno posluje 5 bankomata, s lokacijama u Rijeci, Puli i Zagrebu.
[25] Točan termin za ovu aktivnost bi bio vezanje sredstava, a ne doznačavanje jer se sredstva vežu za javni ključ (adresu) korisnika.

iako to nigdje nije formalno navedeno, burze kriptovaluta znaju jamčiti za sredstva svojih korisnika, pa su tako u nekim prošlim uspješnim hakerskim napadima, centralizirane burze zbog svoje reputacije odlučile refundirati ukradena sredstva svojim korisnicima. Isto tako, trgovina na centralnim burzama se provodi izvan zapisa na blockchain (engl. *off-chain*). Tek u trenutku kada korisnik napravi zahtjev za povlačenjem sredstava sa burze, platforma doznačuje kriptovalute na javni ključ korisnika koji je, preko privatnog ključa, u kontroli korisnika i ta transakcija se bilježi na blockchain (engl. *on-chain*).

Prema interakciji s fiat novcem, centralizirane burze kriptovaluta se mogu podijeliti u dvije skupine: burze koje pružaju trgovinu u paritetu s fiat novcem kripto/fiat i koje omogućavaju neki oblik deponiranja fiat novca na njihovu platformu, i burze koje pružaju trgovinu samo u kripto/kripto paritetu, odnosno pružaju mogućnost samo depozita u kriptovalutama. Iako je u početku bilo puno više burzi koje su pružale samo uslugu trgovine u kripto/kripto paritetu, sve je više centraliziranih burzi koje su omogućile transfere fiat valuta prema njima. Neke od najpoznatijih su: Coinbase, Bitstamp, Bittrex, Binance, Bitfinex, Gemini, Kraken, Robinhood itd. Druge popularne burze koje nude trgovinu samo u kripto/kripto paritetu su: Huobi, KuCoin, OKEx, HitBTC, BKEX itd.

4.2.2. Decentralizirane burze

Decentralizirane burze kriptovaluta (engl. *decentralized cryptocurrency exchange* - DEX) su decentralizirane platforme koje pružaju trgovinu s kriptovalutama, ali bez svojstva posrednika između kupaca i prodavatelja. To su platforme koje omogućavaju izravnu trgovinu s kriptovalutama između interesnih strana na decentralizirani *peer-to-peer* način bez otkrivanja svojih privatnih ili javnih ključeva, odnosno odricanja kontrole nad sredstvima. Osim izravne trgovine, decentralizirane burze pružaju različite mogućnosti kao što je kreiranje novih kriptovaluta putem pametnih ugovora, kreiranje derivativnih stabilnih ili drugih kriptovaluta putem kolaterala, uzimanje zajmova itd. Svi ovi procesi se provode na siguran i decentralizirani način, što se često prezentira kao prednost u odnosu na centralizirane burze. Međutim, i decentralizirane burze imaju svoje nedostatke. Po gubitku lozinke za prijavu na burzu, sredstva deponirana na decentraliziranu burzu

su izgubljena zauvijek jer ne postoji formalan ured u pozadini koji bi mogao provesti oporavak lozinke (engl. *password recovery*). Pored toga, poznato je da su DEX burze manje popularne od CEX burzi, pa zbog toga imaju manje korisnika, odnosno nizak volumen trgovanja i nisku likvidnost, što predstavlja problem kod brze prodaje, odnosno kupnje kriptovaluta. Jednako tako, zbog problema likvidnosti, DEX burze su više podložne cjenovnim manipulacijama gdje se, kroz značajniju kupnju pojedine kriptovalute, utječe na njenu likvidnost i volumen, što privlači trgovce i programe specifične za pružanje likvidnosti, a to u konačnici može imati pozitivan učinak na njenu cijenu. Pored navedenog, većina DEX burzi nema mogućnost neposrednog deponiranja i povlačenja fiat valuta, već se transakcije provode preko treće strane koje pruža takvu uslugu (engl. *gateway*). Jednako tako, depozit i povlačenje drugih kriptovaluta zahtijeva plaćanje naknade i potvrdu bloka transakcija, što DEX burze čini tromim i ponekad skupim. Neke od popularnijih DEX burzi su: Bitshares, IDEX, Waves DEX, Stellar DEX i Bisq DEX.

4.2.3. Hibridne burze

Hibridne burze kriptovaluta (engl. *hybrid cryptocurrency exchange* - HEX) predstavljaju najnovije platforme za trgovinu kriptovaluta koje su prepoznale i u svoje poslovanje implementirale najbolja svojstva od CEX i DEX burzi. Namjera HEX burzi je osigurati funkcionalnost i likvidnost CEX burzi, a privatnost i sigurnost DEX burzi. Unapređenjem svoje funkcionalnosti, HEX burze teže privlačenju institucionalnih korisnika koji su navikli na više profesionalnu uslugu, nego što to trenutno pružaju CEX i DEX burze. HEX burza na decentralizirani način povezuje elemente centralizirane burze, osiguravajući tako svojim korisnicima pristup trgovačkoj platformi i iskustvo CEX burzi, dok se trgovinske konfirmacije provode kroz *peer-to-peer* mrežu, kao što je to slučaj kod DEX burzi.

Prednosti hibridnih burzi je moguće sažeti kroz nekoliko sljedećih točaka. Korisnici HEX burzi imaju veću kontrolu nad svojim sredstvima, iako je njeno operativno poslovanje djelomično centralizirano i ovisi o trećoj strani. Hibridne burze štite anonimnost svojih korisnika te su više regulirane od nekih CEX i DEX burzi. Sredstva deponirana na HEX burzu se ne vežu za privatni ključ korisnika otvoren na burzi i samo za potrebe burze, nego su vezana za privatne ključeve pod kontrolom

korisnika. Transparentnost poslovanja, brzina transakcija i skalabilnost koja proizlazi iz njihove arhitekture su također pozitivna svojstva HEX burzi, što ih čini atraktivnom opcijom u odnosu na CEX burze, gdje se sve događa bez znanja korisnika, osim onog što je prezentirano preko medija. Iako su još uvijek relativno nepoznat pojam, HEX burze se prezentiraju javnosti kao budućnost trgovine s kriptovalutama, a to namjeravaju postići preko platformi koje pružaju odgovorniju i više formalnu trgovinu s njima.

4.3. Prednosti i rizici ulaganja u kriptovalute

Kriptovalute predstavljaju novu vrstu digitalne imovine preko koje se investitorima pruža mogućnost ulaganja u startup projekte na primarnom tržištu, te mogućnost njihove naknadne trgovine na sekundarnom tržištu. Kao takvo, tržište kriptovaluta pruža neke prednosti u odnosu na tradicionalno tržište financijskih instrumenata, ali i nedostatke u obliku rizika analognim rizicima ulaganja na tradicionalnom tržištu kapitala. Osim poznatih rizika, tržište kriptovaluta uključuje i neke nove rizike specifične samo za okruženje kriptovaluta. U nastavku se sumiraju i tumače prednosti, rizici i nedostaci povezani s ulaganjem u kriptovalute na njihovom primarnom i sekundarnom tržištu.

Kao prvi razlog investiranja u ICO se navodi potencijal kapitalnog prinosa novokreirane kriptovalute na sekundarnom tržištu. Pozitivan momentum rasta vrijednosti kriptovalute može trajati i do nekoliko mjeseci. Tokom 2017. godine najzapaženiji primjeri jednog takvog cjenovnog rasta se odnose na kriptovalute neo (NEO) i pivx (PIVX) koje su ostvarile kumulativni pronos od 1.549 puta, odnosno 1.796 puta u odnosu na cijenu s početka 2017. godine.

Prednost neposrednog investiranja u blockchain projekte u odnosu na fondove poduzetničkog kapitala predstavlja i relativno jednostavan izlazak iz vlasničke pozicije. ICO projekti se mogu uspješno pokrenuti unutar mjesec ili čak tjedan dana nakon inicijalnog ulaganja što, uz uvjet da je kriptovaluta uvrštena na neku od burzi kriptovaluta, a to je najčešće tako, omogućava brz izlazak iz pozicije. Ukoliko je cijena te nove kriptovalute na sekundarnom tržištu povoljna za investitora, kriptovaluta se putem interneta transferira prema nekoj od platformi koja može, ali i

ne mora pružati mogućnost konverzije u fiat valutu (engl. *getaway*). U slučaju da takva mogućnost postoji, vrši se konverzija u fiat valutu po tržišnom tečaju i investitor može transferirati sredstva na svoj bankovni račun. U slučaju da takva mogućnost ne postoji, kriptovaluta se može konvertirati u neku stabilnu kriptovalutu ili bitcoin, i onda transferirati prema trgovinskoj platformi koja pruža izlaz prema fiat valutama, pri čemu bilo koji transfer u ova dva slučaja ne poznaje formalne granice neke države. Pored toga, neke platforme za trgovinu pružaju mogućnost trgovine s kriptovalutama koje još nisu niti zaživjele u smislu svog transakcijskog sustava, odnosno blockchaina, pri čemu se u tom slučaju izdaje dužnički digitalni instrument tzv. IOU (*I owe you*). Po emitiranju te nove kriptovalute, bilo da se radi o primarnim kriptovalutama sa svojim blockchain protokolom, ili sekundarnim kriptovalutama izvedenim na blockchain ekonomijama, IOU se zamjenjuje u omjeru 1:1 sa IOU instrumentima. Sekundarno tržište kriptovaluta pruža širok dijapazon mogućih ulaganja u projekte koji imaju različitu praktičnu implikaciju pri čemu se otvara mogućnost diverzifikacije ulaganja. Iako su promjene vrijednosti kriptovaluta povezane sa značajnom volatilnošću, recentna istraživanja poput Trimborn et al. (2018) i Petukhina et al. (2018), svejedno ukazuju na korisnost uključivanja kriptovaluta u dobro diversificirani portfelj sastavljen od tradicionalne imovine.

Kriptovalute novije generacije predstavljaju projekte startupova koji stoje iza njih. U kontekstu tradicionalnog tržišta kapitala, uspješnost projekta bi se trebala odraziti i na tržišnu vrijednost kriptovalute koja predstavlja startup. Međutim, startupovi nemaju ustrojstvo i pravni oblik dioničkih društava, u smislu da ne ostvaruju kontinuirane prihode i dobit iz poslovanja te zbog toga nemaju niti mogućnost distribucije dividendi vlasnicima kriptovaluta. S druge strane, kako bi privukli investitore, pojedini startupovi isplaćuju pasivne prihode svojim investitorima za vrijeme držanja predmetne kriptovalute što se može protumačiti kao oblik dividendi ili kamata. U tom slučaju držanjem kriptovalute u odgovarajućem novčaniku (engl. *staking*), ostvaruje se pasivni dohodak u toj valuti, što kroz protokol blockchain sustava osigurava dodatnu participaciju procesu verifikacija i potporu sigurnosti mreže, te se smatra dodatnim motivom za ulaganje u kriptovalute.

Blockchain projekte koji uključuju kriptovalute potrebno je razmatrati kroz više različitih segmenata kako bi se prepoznali i definirali potencijalni rizici. Kriptovalute

uključuju rizike povezane s tradicionalnim financijskim instrumentima i investiranjem, rizike povezane s tehnologijom na kojoj počivaju i rizike povezane sa sigurnošću poslovanja putem interneta. Jedan od glavnih rizika ulaganja u kriptovalute je tržišni rizik promjene vrijednosti koji nastaje zbog odsutnosti fundamentalnih indikatora povezanih s projektima startupova. Naime, kao nova digitalna imovina, kriptovalute se ne mogu dovesti u vezu s okvirom fundamentalnih i sistematskih faktora postojećih financijskih instrumenata tradicionalnog tržišta kapitala. Zbog nedostatka strogo definiranih fundamentalnih indikatora, pa tako i matematičkog izraza za izračun barem teorijske vrijednosti, podržane rezultatima istraživanja akademske zajednice, a koja bi služila kao stabilizator cjenovnog momentuma pojedine kriptovalute, razmatranje kriptovaluta kao investicijskih prilika može dovesti investitore u podređeni položaj, odnosno u situaciju potpune neizvjesnosti. Kriptovalute i cijela njihova tehnička infrastruktura još uvijek predstavljaju svojevrsnu nepoznanicu široj javnost. Zbog toga, ali i nedostatka regulatornog okvira, investitori se moraju oslanjati na ponekad neobjektivne informacije prikupljene kroz razne medijske platforme. Sve to je u konačnici dovelo do loše prosudbe investitora te kupnjom kriptovaluta na njihovim najvišim razinama tokom 2017. godine, što je rezultiralo time da su investitori na sekundarnom tržištu ostvarili najviše gubitke (engl. *drawdown*) čak i do 98% svog inicijalnog ulaganja.

Tržišni rizik se očituje i kroz rizik volatilnosit. Većina modela koji se koriste prilikom razmatranja investicijskog odabira, poput modela za vrednovanje imovine na tržištu kapitala (engl. *Capital Assets Pricing Model* – CAPM), podrazumijeva pretpostavku da niti jedan investitor nije dovoljno velik da bi svojom kupnjom ili prodajom mogao utjecati na promjenu tržišne vrijednosti imovine. Tržište kriptovaluta ne zadovoljava navedenu pretpostavku jer bilo koji malo veći investitor može umjetno stvoriti likvidnost i privući dodatne investitore, što znači da je, osim rizika volatilnosti, tržište kriptovaluta podložno i riziku manipulacije. Rizik manipulacije se ogleda kroz dogovorno trgovanje, poput tzv. insajderskog trgovanja, *pump and dump* cjenovne manipulacije, lažnih utjecaja kroz lažne korisničke račune i društvene medije kako bi se kreirala dodatna potražnja i dodatni cjenovni momentum. Rizik manipulacije posebno je izražen na derivativnom tržištu kriptovaluta, točnije tržištu terminskih ugovora (engl. *futures*). Tržište terminskih ugovora izvedeno na kriptovalutama kao temeljnoj imovini pruža mogućnost trgovine uz polugu čak i do 125 puta. S obzirom

da investitori svojom kupnjom ili prodajom mogu potaknuti smjer kretanja vrijednosti pojedine kriptovalute, zadavanje suprotne pozicije u terminskim ugovorima bi im moglo osigurati značajne profite, ovisno o veličini pozicije i poluge koju koriste. Opisani primjer je samo jedan od načina kako je moguće manipulirati s cijenama na tržištu kriptovaluta kroz terminske ugovore, zbog čega potencijalni investitori moraju biti oprezni.

Također, postavlja se pitanje i informacijske efikasnosti tržišta, odnosno općenitog tumačenja pojava na tržištu kriptovaluta. Na primjer, dolazi do razdvajanja/izdvajanja tzv. forkanja Bitcoin transakcijskog sustava što znači da se broj postojećih bitcoin jedinica duplicira, a vrijednost bitcoina, kao i agregatnog tržišta kriptovaluta izraženog u protuvrijednosti fiat valute, ostane jednaka kao i prije objave te informacije. Štoviše, ne samo da ostane ista, nego tržišna vrijednost prije dijeljenja transakcijskog sustava dodatno raste, jer dupliciranje jedinica bitcoina zapravo predstavlja *besplatan novac*, a to dodatno privlači investitore. Međutim, paradoks je u tome što nova količina fiat novca koja bi fundamentalno pravdala agregatno povećanje vrijednosti tržišta nije uopće ušla u ekosustav kriptovaluta. Drugim riječima, iz ničega se kreira novi sintetički novac, a isti taj novac se vrlo brzo i jednostavno može pretvoriti u bilo koju fiat valutu, pa čak i kunu. Opisana situacija zapravo i povlači pitanje vjerodostojnosti fundamentalne vrijednosti agregatnog tržišta kriptovaluta. Naime, stabilna kriptovaluta tether (USDT)[26], prema Međunarodnoj udruzi za standardizaciju tokena (engl. *International Token Standardization Association* - ITSA)[27], predstavlja čak do 87% tržišnog udjela svih stabilnih kriptovaluta kolateraliziranih i vezanih za vrijednost dolara. Tržišna kapitalizacija USDT-a je trenutno viša od 9 milijardi dolara i nalazi se na trećem mjestu po kapitalizaciji svih kriptovaluta, s tendencijom kontinuiranom rasta. Drugim riječima, sve više fiat novca, u ovom slučaju dolara, ulazi u ekosustav kriptovaluta. Druga po redu stabilna kripotvaluta je USD coin sa kapitalizacijom od nešto malo više od 1 milijarde dolara, ali također s tendencijom rasta kapitalizacije. Međutim, pred kraj 2017. godine, organizacija koja stoji iza tethera je privremeno zatvorila mogućnost prijava novih investitora koji žele transferirati dolare u USDT, a USDT se nastavio kreirati, što je povuklo neke sumnje u vjerodostojno stanje omjera 1:1 između deponiranih dolara na račun u banci tvrtke koja stoji iza tethera i broja

[26] https://tether.to/
[27] https://itsa.global/

novih kreiranih USDT-a. Drugim riječima, špekuliralo se umjetnom povećanju agregatne kapitalizacije tržišta kriptovaluta. Iako su posljednja istraživanja pokazala da nema opravdanja takvim sumnjama i da je USDT u potpunosti pokriven dolarima u omjeru 1:1, ostaje i dalje pitanje može li se to transparentno dokazati[28]. S druge strane, takve sumnje su otvorile vrata drugim organizacijama koje su vidjele mogućnost pružanja profitabilne usluge kreirajući nove stabilne kriptovalute, što je dovelo do stvaranja niza novih stabilnih kriptovaluta. Sva negativna razmatranja i špekulacije, tržište kriptovaluta i cijelu ideju oko njih čine izrazito neizvjesnim, a u domeni modeliranja portfelja, jako volatilnim i rizičnim.

Iako broj platformi gdje se može trgovati s kriptovalutama raste na mjesečnoj, možda i tjednoj bazi i daleko nadmašuje broj burzi tradicionalnih financijskih instrumenata, tržište kriptovaluta je i dalje plitko, usko i imperfektno što utječe na rizik likvidnosti. Rizik likvidnosti vezan je za utrživost kriptovalute i ogleda se u teškoćama kupnje i naknadne prodaje imovine na sekundarnom tržištu po očekivanoj ili željenoj tržišnoj cijeni u bilo kojem trenutku. Prilikom aktivne trgovine u 2017. godini, znalo se dogoditi da se određene burze nisu bile spremne nositi s rastućom potražnjom za kriptovalutama, što je rezultiralo njihovom privremenom obustavom s radom. S druge strane, tokom 2017. godine pojedine banke su bile zabranile transfere sredstava koji su se odvijali prema i od platformi koje su pružali uslugu trgovine kriptovalutama, a imale su mogućnost deponiranja i povlačenje fiat valuta, što je zabrinulo mnoge investitore jer nisu imali mogućnost transfera fiat novca na svoje račune u banci.

Tržišna vrijednost kriptovaluta ovisi i o prihvaćanju blockchain tehnologije od strane šire populacije. Veća popularnost pojedinog blockchain rješenja neizbježno će utjecati i na vrijednost kriptovalute koja je izvedena na njemu. Blockchain tehnologija se kontinuirano razvija, a rješenja koja ne budu pratila inovacije, postat će zastarjela što će utjecati na vrijednost kriptovalute. Prema tome, ovdje se uvodi novi rizik koji proizlazi iz zastarjele tehnologije povezane sa hardverom i softverom. Gubitak kriptografskih privatnih ključeva također predstavlja jedan od rizika. U slučaju njihovog gubitka, jedinice valute povezane s javnim ključem su zauvijek izgubljene, jer ne postoji mogućnost obnove privatnih ključeva iz pripadajućih javnih ključeva.

[28] https://www.coindesk.com/tether-review-claims-crypto-asset-fully-backed-theres-catch

Pretpostavlja se da je u rasponu od 17% do 23% ukupnih bitcoina zauvijek izgubljeno, djelomično zbog gubitka privatnih ključeva kada je bitcoin bio još puno niže vrijednosti i nepoznat, a djelomično zbog problema sa odabirom adekvatnog načina čuvanja privatnih ključeva, problema sa hardverima itd. Stoga korisnici blockchain infrastrukture moraju dodatnu pažnju posvetiti pravilnom i sigurnom čuvanju privatnih ključeva kako bi umanjili rizik gubitka. Kriptovalute su podložne i riziku transfera, odnosno regulatornom riziku zabrane korištenja, trgovanja ili bilo kojih radnji povezanih s njima od strane pojedine države. Jedna od zapaženijih zabrana se dogodila 2017. godine kad je Narodna Republika Kina uvela zabranu na ICO-e i trgovinu s kriptovalutama, što je prouzročilo nesigurnost kod investitora i značajnu volatilnost u narednim danima.

Osim navedenih, postoji još niz rizika vezanih za proces ICO-a. Lee Kuo Chuen i Low (2018) sumiraju nedostatke ICO-a kroz rizike povezane sa nedostatkom zakonskog okvira, rizikom transparentnosti, rizikom kapitala, rizikom gubitka koji proizlazi iz neuspješnog projekta i rizikom prijevare. Zakonski okvir u kojem se provode ICO-u su uglavnom nedefinirani i nejasni. Dosadašnja interpretacija kriptovaluta se uglavnom ogleda kroz postojeće zakonske okvire tradicionalnih financijskih instrumenata. Kriptovaluta može predstavljati ili standardni financijski instrument, odnosno vrijednosnicu, ili utilizacijski token, a u tom slučaju je nejasno kako s kriptovalutom postupati prema postojećim zakonom i propisima koji nemaju definiciju utilizacijskog tokena. U izostanku regulative i propisanog standarda, način kako se ICO-i provode su uglavnom definirani od strane razvojnih programera i voditelja startup projekta, što otežava budući nadzor za regulatore. Rizik nedostatka zakonskog okvira se ogleda i kroz poslovanje burzi kriptovaluta. Prema trenutnom stanju, burze kriptovaluta nemaju definiran okvir internih pravila kojim bi spriječile manipulaciju tržištem ili neke druge prijevarne aktivnosti. Također, burze ne podliježu obvezi transparentnog i periodičnog objavljivanja financijskog rezultata i rizika poslovanja. Lee Kuo Chuen i Low (2018) navode da bi, u slučaju potpune regulacije koja uključuje dodatne napore i troškove, ICO-i zapravo izgubili na svojoj prednosti u odnosu na tradicionalni metode prikupljanja kapitala.

Rizik transparentnosti također proizlazi iz odsustva regulatornog okvira ICO-a i očituje se u nedostatku strogo definiranog plana startupa koji prikuplja sredstva kroz

ICO proces. Jedini dokument, za kojeg startup niti nema obvezu prezentacije investitorima, predstavlja idejno tehnološko rješenje (engl. *whitepaper*), kojeg startup objavljuje na svojim internet stranicama prilikom početka ICO-a. Međutim, takav dokument nema strogo definiranu strukturu u smislu propisanih stavki, kao što je to slučaj prilikom IPO-a i prezentiranja prospekta. *Whitepaper* može biti iznimno opširan dokument, s detaljno razrađenom tehnološkom idejom, poslovnim planom i planom gospodarenja s prikupljenim kapitalom, kao i obvezama koje proizlaze iz projekta. Ali može i biti iznimno sažet i bezidejan, samo sa natuknicama ideje projekta, bez ikakvog plana o gospodarenju sredstava, ili mogućeg programa za povrat istih investitorima u slučaju neuspjeha projekta, što uključuje i rizik kapitala. Rizik kapitala se ogleda u nedostatku internog menadžmenta projekta koji bi adekvatno gospodario s prikupljenim sredstvima.

Jedan on najvećih ICO projekata provedenih do sada, koji je trajao godinu dana, pripada startupu Block One[29]. Block One je razvio Eos blockchain transakcijski sustav kao decentraliziranu kompjutersku platformu na *dokaz o ulogu* konsenzus algoritmu. Ukupno prikupljena sredstva kroz ICO proces su iznosila više od 4,1 milijardi dolara što, po veličini prikupljenih sredstava, ulazi u kategoriju institucionalnog i državnog financiranja, te za jedan startup predstavlja značajan iznos novca, ali i obvezu. Ukoliko menadžment startupa nema strogo definiran poslovni plan, strategiju razvoja, strategiju upravljanja s rizicima, plan gospodarenja sredstvima te adekvatne ljude na vodećim pozicijama, investitori na sebe preuzimaju dodatan rizik neuspjeha projekta.

Izostanak regulacije u ICO procesu i općenito izostanak sekundarnog naknadnog nadzora u projektima koji su privlačili velik broj investitora, privukao je i veliki broj voditelja projekata s upitnim moralnim načelima. Procjenjuje se da je u 2017. god. okvirno oko 80% svih projekata na primarnom tržištu bilo neki oblik prijevare investitora. S jedne strane velika sloboda startupa, a s druge strane slabo poznavanje, ili potpuno nepoznavanje blockchain tehnologije i mogućnosti koje ona

[29] Block One je nastao na ideji glavnog programera Daniela Larimera. Osim Eos blockchaina, Daniel Larimer je prethodno razvio i Bitshares i Steem blockchain. Prilikom Bitshares ICO-a, sredstva su prikupljena u bitcoin kriptovaluti na najvišim cjenovnim razinama što je, nakon pada vrijednosti bitcoina, uzrokovalo probleme s likvidnosti projekta i njegov razvoj dovelo u pitanje. Poučeni iskustvom, vodeći ljudi iza Block One startupa su odlučili produljiti vrijeme trajanja Eos ICO-a na godinu dana, upravo kako bi izbjegli rizik volatilnosti, odnosno likvidnosti projekta.

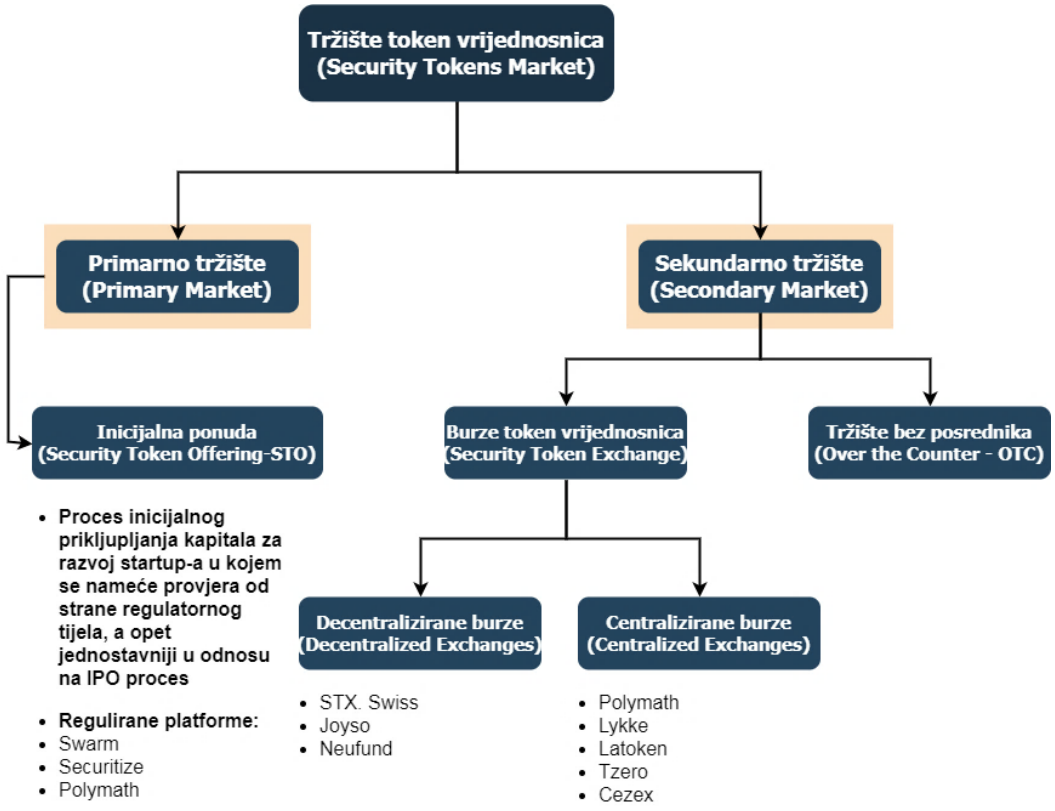
pruža, ali i velikih financijskih očekivanja od strane investitora, rezultiralo je velikim brojem lažnih projekata, čiji je cilj bio isključivo samo prijevarom prikupiti značajniji iznosa kapitala, bez stvarnog pokretanja projekta. Postoji niz ovakvih primjera koji su se dogodili na tržištu kriptovaluta, a značajniji su projekti poput Ifan i Pincoin gdje je 2018. god. na temelju lažnog ICO-a od investitora izvučeno više od 600 milijuna dolara. Zatim najpoznatija ponzijeva shema koja je trajala od 2016. god do 2018. god. gdje se pretpostavlja da su investitori izgubili sredstva u vrijednosti od 700 milijuna dolara[30]. Prema pisanju MIT Technology Review[31], kripto ponzi sheme su se u 2019. godini utrostručile, u odnosno na godinu prije. Doslovno su milijuni ljudi bili prevareni za više od 4,3 milijarde dolara zbog činjenice da je široj populaciji pojam kriptovaluta i korištenih modela financiranja njihovog razvoja, i općenito načina funkcioniranja, tehnološkog okruženja i njihovih mogućnosti, još uvijek nepoznat.

4.4. Tržište token vrijednosnica

Kao odgovor na velik broj javno potvrđenih skandala i prijevara na primarnom, ali i sekundarnom tržištu kriptovaluta, s ciljem vraćanja povjerenja investitora, ali i daljnjeg razvijanja tržišta, nastalo je novo primarno i sekundarno tržište token vrijednosnica koje koristi blockchain infrastrukturu za svoje operativno poslovanje/postojanje. Međutim, najznačajnija razlika između postojećeg tržišta kriptovaluta i novog tržišta token vrijednosnica se očituje u tome što tržište token vrijednosnica podrazumijeva kriptoimovinu za koju se prilikom njenog kreiranja nameće regulacija od strane nadzornog tijela.

Aktivno tržište token vrijednosnica podrazumijeva i postojanje platformi za njihovo kreiranje i trgovanje koje su regulirane od strane države u kojoj platforme posluju. U komparaciji sa ostalom financijskom imovinom na blockchainu, token vrijednosnice bi zapravo predstavljale utilizacijske tokene kreirane na nekoj od decentraliziranih kompjutorskih platformi, trenutno je to najčešće Ethereum platforma. Token vrijednosnice predstavljaju digitalnu imovinu koja koristi kriptografiju i blockchain za svoju operativnu infrastrukturu ali koja, za razliku od većine utilizacijskih kriptovaluta, zadovoljava određeni zakonski okvir i regulativu države u kojoj je kreirana.

[30] https://medium.com/@tozex/the-five-biggest-ico-scams-54967ec92b87
[31] https://www.technologyreview.com/2020/01/30/275964/cryptocurrency-ponzi-scams-chainalysis/



Shema 3. Tržište kriptovrijednosnica

Izvor: Izrada autora

Token vrijednosnice ili kriptovrijednosnice (engl. *cryptosecurities*) kreiraju se na primarnom tržištu putem njihove inicijalne ponude kroz STO proces *(engl. security token offering* - STO*).* U svojoj osnovi, STO proces je jako sličan ICO procesu i predstavlja aktivnosti prikupljanja kapitala za razvoj startup projekta. Iako se najčešće kreiraju s ciljem financiranja startupa koji pružaju financijske usluge, neki STO procesi su uspješno provedeni i s ciljem financiranja npr. izgradnje studentskog smještaja gdje je prikupljeno više od 14 milijuna dolara, ili financiranja razvoja tvornice vozila s niskom potrošnjom gdje je skupljeno blizu 17 milijuna dolara itd. Kriptovrijednosnice ovog tipa mogu biti vlasničkog karaktera (engl. *equity tokens*) ili dužničkog karaktera (engl. *debt tokens*). Nakon što se kreiraju, uvrštavaju se na sekundarno tržište, odnosno platforme koje predstavljaju burze token vrijednosnica, specifično namijenjene njihovoj trgovini, sukladno Shemi 3.

Iako je tržište token vrijednosnica najavljivano kao sljedeći veliki uspjeh tržišta financijske imovine na blockchainu, ono nije zaživjelo niti blizu očekivanjima. Mogući razlozi neuspjeha su različiti, ali jedan je zasigurno postojanje zakonskog i regulatornog okvira koji je smanjio financiranje velikog broja projekata bez fundamentalne osnove, što je bio slučaj sa ICO projektima. Prema internet stranici za praćenje STO projekata „stoscope“[32], trenutno je 86 startup projekata koji se financiraju putem STO-a, 6 ih provodi glavnu prodaju token vrijednosnica, a 10 projekata je uspješno financirano.

4.5. Usporedba karakteristika inicijalne ponude

Tablica 1. usporedno prikazuje osnovne karakteristike najčešće korištenih procesa prikupljanja kapitala startupova putem inicijalne ponude kriptovaluta. Sve tri metode se oslanjaju na koncept grupnog financiranja emitiranjem nove digitalne financijske imovine na blockchain infrastrukturi. Kao što je prikazano u tablici, najmanje angažmana i sredstava zahtijeva ICO proces. U pravilu, za njegovu provedbu bila je dovoljna web stranica, *whitepaper* i komunikacijski kanal poput Telegram aplikacije za poruke i druge medije. Druga po redu je inicijalna ponuda putem burze, a najzahtjevnija je svakako regulirana inicijalna ponuda token vrijednosnica iz razloga što takav koncept podrazumijeva dodatne korake u komunikaciji s regulatorom i troškove povezane s regulacijom projekta.

S druge strane, viša regulacija potencijalnim investitorima može ograničiti pristup inicijalnoj ponudi. STO proces može biti zatvoren za širu javnost, odnosno otvoren samo užem krugu investitora, ili investitorima u domeni države gdje se STO provodi. Također i IEO proces je ograničen djelovanjem burze koja ponudu provodi. Ukoliko se zabrani pristup burzi kriptovaluta, potencijalni investitori nemaju mogućnost alokacije sredstava u IEO proces. Dakako, zbog svoje pristupačnosti, ICO koncept financiranja ima najveću bazu potencijalnih investitora.

Da bi se apliciralo u neki od ICO-a, ponekad je potrebna samo adresa elektroničke pošte i adresa kriptovalute (javni ključ) kao dokaz izvora sredstava s koje će se

[32] https://stoscope.com/

sredstva doznačiti od investitora prema ICO projektu. Sva daljnja komunikacija i postupanja s novim izdanim kriptovalutama se mogu dogovoriti naknadno.

Tablica 1. Usporedni prikaz procesa inicijalne ponude blockchain imovine

	Inicijalna ponuda (Initial Coin Offering - ICO)	**Inicijalna ponuda pute burze (Initial Exchange Offering-IEO)**	**Inicijalna ponuda token vrijednosnica Security Token Offering-STO)**
Definicija/opis	Grupno financiranje (crowdfunding) izdavanjem utilizacijskog tokena/kriptovalute	Grupno financiranje (crowdfunding) izdavanjem utilizacijskog tokena/kriptovalute putem burze kriptovaluta	Grupno financiranje (crowdfunding) izdavanjem token vrijednosnice putem reguliranih platformi
Razina regulacije	**Niska** - većim dijelom potpuno neregulirano (zbog toga su 80%-90% ICO-a lažni projekti)	**Srednje visoka** – burza jamči za tim i proizvod	**Visoka** – platforma provodi ponudu u skladu s regulacijskim okvirom države u kojoj se provodi
Težina provođenja	**Niska** – potreban je „whitepaper", web stranica i komunikacijski kanal	**Srednje visoka** – burze zahtijevaju zadovoljavanje određenih uvjeta	**Visoka –** regulirane platforme zahtijevaju zadovoljavanje uvjeta postavljenih od strane regulatora države u kojoj se provodi
Troškovi provođenja	**Niski** – trošak stranice, marketinga itd.	**Srednje visoki** – burza naplaćuje određenu naknadu	**Visoki** – veći troškovi regulacije (naknade zakonskim i financijskim savjetnicima)
Pristupačnost široj javnosti	**Visoka** – svatko može pristupiti (osim u slučaju privatne ponude npr. Telegram - GRAM – 1,7 milijardi $)	**Srednje visoka** – pristup je ograničen pristupom burzi koja provodi ponudu (u nekim državama je zabranjeno trgovati), burza provodi provjere „poznavanja klijenata" (Know Your Customer – KYC)	**Niska** – ovisno o regulaciji, može biti zatvorena za širu javnost
Razina upravljanja (model)	**Širok** – svatko može utjecati na odluke	**Srednje visok** – tim zajedno s burzom donosi i provodi važne odluke	**Uzak** – upravljanje startupom je formalno regulirano zakonskim okvirima
Likvidnost	**Srednje visoka** – nakon izdavanja, imovina se uvrštava na burze	**Visoka** – odmah po završetku procesa IEO-a, trgovina može početi	**Niska** – burze token vrijednosnica nemaju visoku likvidnost kao burze kriptovaluta (za sada)

Izvor: Izrada autora

Model upravljanja javnom ponudom je također determiniran konceptom javne ponude koja se provodi. Najveću fleksibilnost dakako ima ICO projekt gdje svatko, ukoliko se takav model prihvati, može utjecati na donošenje odluka vezanih za provedbu financiranja, ali i daljnjeg razvoja projekta. Općenito, upravljanje blockchain projektima najčešće jeste centralizirano u smislu da važne odluke projekta donosi tim razvojnih programera koji je nositelj projekta. S obzirom na taj nedostatak te razvojem primarnog tržišta i prethodno navedenog DAICO koncepta, vlasnicima tokena je pružena veća mogućnost utjecaja kako na proces financiranja, pa tako i na daljnji razvoj projekta kroz primjenu ustrojstva decentralizirane autonomne organizacije (engl. *decentralized autonomous organization*)[33]. U slučaju IEO koncepta financiranja burza je ta koja, zajedno sa timom iza projekta, donosi i provodi važnije odluke o samom procesu financiranja i projektu, dok je kod STO procesa upravljanje startupom definirano ustrojstvom i pravnim oblikom startupa sukladno formalnim zakonskim okvirima gdje se STO provodi.

U kontekstu naknadne utrživosti kriptovaluta, projekti koji se financiraju putem burzi imaju prednost u odnosu na financiranje kroz ICO, odnosno STO proces. Po završetku financiranja, kriptovalute se neposredno uvrštavaju na tržište što omogućava bržu trgovinu s njima. S druge strane, zbog manje razvijenosti, burze token vrijednosnica za sada ne pružaju dovoljnu razinu likvidnosti, bez obzira koliko se uspješno financirao projekt.

5. REGULATIVNI OKVIR KRIPTOVALUTA

Kriptovalute su nova vrsta digitalne imovine koja koristi blockchain tehnologiju kao svoju primarnu transakcijsku infrastrukturu. Prva kriptovaluta bitcoin je prezentirana putem otvorenog, javnog i samoodrživog transakcijskog protokola za čije kreiranje nije korišten tradicionalni mehanizam financiranja koji bi ga svrstao u postojeći okvir vlasničkih ili dužničkih financijskih instrumenata. Štoviše, transakcijski sustav Bitcoin, barem koliko je poznato široj javnosti, nije financiran niti na jedan uobičajen način

[33] Decentralizirana autonomna organizacija – DAO je nova ideja poslovnog modela upravljanja tvrtkom (organizacijom) koji se provodi na decentraliziran način putem softvera. Tvrtkom upravljaju svi vlasnici razmjerno ulogu u digitalnoj imovini (kriptovalutama), što znači da ljudi na vodećim pozicijama u tvrtci (menadžeri, uprava i nadzorni odbor) u tom slučaju više nisu potrebni.

privatnom ili javnom ponudom, grupnim financiranjem ili nekim drugim oblicima prikupljanja sredstava. Isto tako, po standardnim definicijama, bitcoin ne zadovoljava sve karakteristike novca niti karakteristike vrijednosnica. S druge strane, tokom cijelog razdoblja od njegova nastanka, siječanj 2009. god., bitcoin se samo i za tu svrhu koristi, jedinica digitalne valute za platežne transakcije i financijski instrument koji pruža investicijske mogućnosti, iz čega proizlazi da je bitcoin zapravo hibridni oblik ove dvije imovine. Zbog neobične i specifične geneze, regulatorna tijela nisu imala, a nemaju još niti sada, unaprijed definirane zakonske okvire nove specifične digitalne imovine. Međutim, upravo zbog funkcijske svrhe, regulacija se, barem za sada, razmatra kroz dva smjera, kriptovalute kao novac i kriptovalute kao financijski instrumenti. Formalnoj regulaciji velik problem predstavlja i brz razvoj blockchain tehnologije koji zasigurno utječe na smjer razvoja kriptovaluta. Među prvim uspješnim račvanjima Bitcoin transakcijskog protokola je bilo kreiranje Litecoin transakcijskog sustava koji nema integrirane mogućnosti pametnih ugovora, kakve danas ima više različitih blockchain ekonomija. S obzirom da takva kripotovaluta nema strukturu formalnih institucija, upravu, menadžment, zaposlenike, i ne predstavlja udio u vlasništvu nekog društva koji bi mogao donijeti njenim vlasnicima budući profit, nego ima razvojne programere širom svijeta koji održavaju sustav kroz čvorove mreže, takva kriptovaluta bi se mogla klasificirati kao novac. S druge strane, kriptovalute izdane u svrhu upravljanja decentralizirane autonomne organizacije, u neku ruku predstavljaju instrument s kojim se može utjecati na smjer razvoja DAO projekta i koji im može osigurati budući profit, te se one mogu klasificirati kao vrijednosnice.

5.1. Regulacija unutar Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala

Trenutno prema zakonima o financijskim vrijednosnim papirima unutar Europske unije ne postoji zakonska definicija kriptovaluta (ESMA, 2019). S ciljem boljeg razumijevanja okolnosti pod kojima se kriptovalute mogu smatrati financijskim instrumentima u Europskoj uniji, Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala (engl. *European Securities and Markets Authority* - ESMA) je u 2019. god provelo istraživanje preko nacionalnih nadležnih tijela (engl. *National Competent*

Authorities – NCAs[34]) država članica. Istraživanje je provedeno na način u kojem je određena država članica morala utvrditi razinu primjene Direktive o tržištu financijskih instrumenata (engl. *Markets in Financial Instruments Directive* – MiFID II[35]) u svoje nacionalno pravo, gdje se na temelju primjene Direktive dalo mišljenje da li se šest kriptovaluta iz uzorka klasificiraju kao financijski instrumenti prema nacionalnim zakonima. Istraživanje je uključivalo pitanja koja se odnose na vrste financijskih instrumenata uzimajući u obzir svaki element definicije financijskih instrumenata u skladu sa MiFID II. Od svih uključenih, 29 nacionalnih nadležnih tijela je pružilo odgovore na anketu, uključujući 27 država članica EU (sve osim Poljske), Lihtenštajna i Norveške. Neki NCA-i nisu dali odgovore na sva pitanja. Konkretno, neki NCA-i su smatrali da dostupni podaci nisu dovoljni za kvalificiranje šest kriptovaluta, pa se navodi da određene članice još nisu formirale pogled i stav na određena pitanja vezana za kriptovalute zbog njihovog brzog nastajanja i razvoja. Uzorak od 6 kriptovaluta odražavao je različite karakteristike koje su predstavljale imovinu s investicijskim karakteristikama (uzorak 1. i 2.), utlizacijska imovina (uzorak 5.) i hibridne oblike kombinacija investicijske imovine, utilizacijske imovine i platežne imovine (uzorak 3., 4. i 6.), sukladno Shemi 4. Također, navodi se da kriptovalute koje predstavljaju isključivo sredstvo plaćanja nisu bile uključene u uzorak ankete te da se rezultati ankete ne bi trebali ekstrapolirati na ukupni ekosustav kriptovaluta, odnosno da platežne kriptovalute poput bitcoina nisu prikazane u anketi. Kriptovalute razmatrane u anketi su sljedeće:

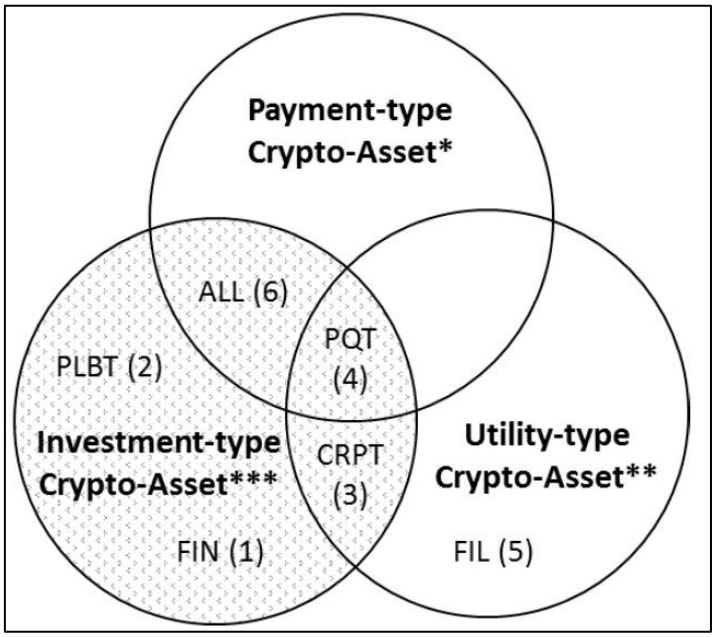
a) Potencijalni investicijski tip kriptovaluta:

   Uzorak 1. Kriptovaluta FINOM (FIN) koristi Blockchain tehnologiju za pružanje potpuno integriranih financijskih usluga. Cilj ekosustava FINOM je omogućiti pristup kriptovalutama širokom krugu korisnika. Ostale očekivane koristi uključuju potpunu transparentnost i sljedivost transakcija. Izdana kriptovaluta (FIN) ima sljedeća priložena prava: 1) pravo na dobivanje dijela dobiti tvrtke u obliku dividendi, 2) pravo sudjelovanja u upravljanju zajednicom i 3) pravo na dio imovine društva. Projekt je prikupio 42 milijuna dolara.

   Uzorak 2. Drugi primjer kriptovaluta koji bi potencijalno predstavljao investicijski tip je kriptovaluta Polybius Bank (PLBT). Polybius Bank je projekt

[34] https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf
[35] https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014L0065&qid=1595031226028&from=EN

je Zaklade Polybius čiji je cilj ponuditi sve tradicionalne usluge bankarskog sustava, bez postojanja ikakvih podružnica ili ureda, primjenom tehnologije distribuiranog digitalnog zapisa. Prema *whitepaper*-u projekta, kriptovaluta Polybius (PLBT) uključuje pravo na primanje 20% raspodjeljive dobiti u financijskoj godini poslovanja Polybius banke. Međutim, kriptovalute svojim vlasnicima ne daju mogućnost sudjelovanja u upravljanju i odlučivanju. Kroz ICO proces, prikupljeno je 30 milijuna dolara za projekt.



Shema 4. Potencijalno mapiranje primjera kriptovaluta
Izvor: ESMA (2019)

b) Potencijalni hibridni tip između investicijskog tipa i utilizacijskog tipa kriptovaluta:

Uzorak 3. Crypterium (CRPT) je kriptovaluta iza tvrtke čiji je cilj izgradnja "kripto banke" s vertikalno integriranim uslugama na međunarodnoj razini koje bi bile brže i jeftinije od postojećih tradicionalnih bankarskih rješenja. Kriptovaluta CRPT bi se koristila za plaćanje naknada prilikom obavljanja transakcije pri korištenju usluga kripto banke. Pored toga, vlasnici kriptovalute imaju pravo na dobivanje mjesečnog udjela u prihodima od transakcija, ali i besplatne, ili po nižoj cijeni, buduće usluge banke. Projekt je putem ICO-a prikupio 51 milijun dolara.

c) Potencijalni hibridni tip između investicijskog tipa, utilizacijskog tipa i platežnog tipa kriptovaluta:

Uzorak 4. PAquarium (PQT) tvrtka radi na izgradnji najvećeg svjetskog akvarija. PAquarium obećava da će godišnje vlasnicima kriptovaluta isplaćivati 20% operativne dobiti akvarija. U *whitepaper*-u se također spominje mogućnost prodaje i razmjene PQT tokena. Kriptovalute dolaze s pravom glasa prilikom upravljanja akvarija, a u budućnosti će biti dostupne dodatne odredbe za glasovanje. Pored toga, mogu se koristiti kao sredstvo plaćanja za robu u akvariju. Kupnja određene količine kriptovaluta omogućava besplatan doživotni ulazak u akvarij. Projekt je još uvijek u vrlo ranoj fazi, a glasovanje o mjestu akvarija još uvijek je u tijeku. Projekt je financiran kroz ICO gdje je prikupljeno 120 milijuna dolara.

d) Utilizacijske kriptovalute distribuirane uz memorandum o ponudi kroz Jednostavni ugovor za buduće kriptovalute (engl. *Simple Agreement for Future Crypto-assets* – SAFT) akreditiranim investitorima i u skladu sa zakonima o vrijednosnim papirima Komisije za vrijednosnice i burzu u SAD-u (engl. *Securities and Exchange Commission* – SEC) i zakonima Agencije za nadzor financijskih usluga (engl. *Financial Conduct Authority* – FCA):

Uzorak 5: Filecoin (FIL) je decentralizirana mreža koja pohranu u oblak (engl. *cloud storage*) pretvara u algoritamsko tržište. Filecoins se može potrošiti za pristup neiskorištenom kapacitetu za pohranu na računalima širom svijeta. Davatelji neiskorištenog prostora za pohranu zauzvrat zarađuju filecoine koji se tada mogu prodati za druge kriptovalute ili fiat novac[36].

e) Potencijalni hibridni tip između investicijskog tipa i platežnog tipa kriptovaluta:

Uzorak 6. AlchemyBite (SVE) je oblik kriptovalute koja pruža mogućnost kreiranja derivativnog oblika kriptovalute. Vrijednost kriptovalute se određuje vrijednošću imovine iz koje je izvedena. Između 70% i 75% udjela kriptovalute se odnosu na druge kriptovalute, dok se preostali dio udjela odnosi na imovinu povezanu sa kriptovalutama, kao što su dionice u kompanijama koje razvijaju tehnologiju distribuiranog zapisa.

[36] Prikazani primjer je sličan prethodnom primjeru utizilacijskog tokena golem platforme na kojoj korisnici mogu iznajmiti računalnu snagu, a golem token (GNT) služi za plaćanje najma te snage.

U rezultatima istraživanja se ističe kako većina nacionalnih nadležnih tijela procjenjuje da se uzorci kriptovaluta 1., 2., 4. i 6. mogu smatrati prenosivim vrijednosnim papirima i/ili drugim vrstama financijskih instrumenata kako je definirano u MiFID II. Također, deset nacionalnih nadležnih tijela je istaknulo u svom odgovoru barem jedan primjer kriptovalute iz svoje nadležnosti (izvan šest predstavljenih slučajeva kriptovaluta) koja bi se mogla smatrati prenosivim vrijednosnim papirima ili drugom vrstom financijskog instrumenta u skladu sa MiFID II. Također, ističe se da postojanje prava na dobit koja proizlaze iz poslovanja tvrtke ili startupa, bez da su nužno uključena vlasnička ili upravljačka prava (uzorak 1. i 2. kriptovaluta), dovoljno da većina nacionalnih nadležnih tijela kriptovalute kvalificiraju kao prenosive vrijednosne papire, gdje takve kriptovalute također zadovoljavaju i ostale uvjete za kvalificiranje kriptovaluta kao prenosivih vrijednosnih papira. S obzirom da niti jedno nacionalno nadležno tijelo nije označilo uzorak 5. kao prenosivi vrijednosni papir i/ili financijski instrument, takav situacija sugerira postojanje kriptovaluta koje ne ulaze u trenutni okvir financijske regulative u državama članicama. Između svih nacionalnih nadležnih agencija postignut je dogovor da se kriptovalute, koje ispunjavaju potrebne uvjete, reguliraju kao financijski instrumenti. Jednako tako, određeni broj nacionalnih državnih tijela predložio je da će trebati promjene postojećeg zakonodavstva ili dodatnih odredaba kako bi se odgovorilo na specifične karakteristike tehnologije distribuiranog zapisa, npr. decentralizirana priroda tehnologije, rizik od račvanja mreže i skrbništvo imovine. Nacionalna nadležna tijela su također istaknula da će možda biti potrebna revizija i postojećih odredbi koje se odnose na poravnanje, namirenje, skrbništvo i evidenciju vlasništva povezanog s prijenosom kriptovaluta. Isto tako, u izvješću se napominje da je velika većina ispitanika država članica smatrala da bi kvalificiranje svih kriptovaluta kao financijskih instrumenata imalo neželjene kolateralne efekte, što znači da možda postoji potreba za razlikovanjem različitih vrsta kriptovaluta. Takvi komentari su razumljivi s obzirom na raznolikost kriptovaluta koje se svakodnevno kreiraju i izdaju. Razlozi kojima su potkrijepljeni takvi komentari su: 1) postojeća regulativa nije sastavljena imajući na umu kriptovalute; 2) priznavanje kriptovaluta kao financijskih instrumenata omogućilo bi im potencijalno neželjeni legitimitet; 3) potrebni nadzorni alati i resursi možda nisu adekvatni za ovu specifičnu imovinu. Na kraju, velika većina nacionalnih nadležnih tijela se složila da bi sve kriptovalute trebale podlijegati nekom obliku regulacije. Malo je konsenzusa oko toga treba li dizajnirati regulatorni režim za kriptovalute koje nisu

kvalificirane kao financijski instrumenti unutar okvira MiFID-a ili izvan njega. Postoje i različita stajališta u vezi s opsegom tog regulatornog režima, iako bi barem sve kriptovalute trebale biti podložne zakonima o pranju novca.

Europska komisija u svojoj inicijativi „*Directive/regulation establishing a European framework for markets in crypto assets*[37]„ definira kriptovalute kao vrstu digitalne imovine koja prvenstveno ovisi o kriptografiji i tehnologiji distribuiranog zapisa (engl. *distributed ledger technology* - DLT). U dokumentu se navodi da postoji širok spektar kriptovaluta koje obuhvaćaju različite značajke i funkcije, stoga predstavljaju različite izazove i rizike. Također, ističe se da trenutno ne postoji klasifikacija od strane Europske unije za kriptovalute, ali se regulatorne institucije uglavnom slažu oko tri vrste kriptovaluta:

a) tokeni za plaćanje/razmjenu (digitalne valute poput bitcoina);
b) investicijski tokeni (koji daju pravo na vlasnička prava i/ili prava slična dividendi, kao što su kriptovrijednosnice koji se prema Direktivi o tržištu financijskih instrumenata - MiFID II) mogu se ili ne moraju smatrati financijskim instrumentima;
c) utilizacijski tokeni koji omogućavaju pristup određenom proizvodu ili usluzi.

5.2. Regulacija unutar Direktive elektroničkog novca i Direktive o platnim uslugama EU-a

Kriptovalute se ne priznaju niti u nijednoj državi članici ili od strane Europske središnje banke kao fiat novac tj. vrijednost označena kao legalno sredstvo plaćanja, obično u obliku novčanica ili kovanica, depozita ili drugih instrumenata plaćanja (EBA Report, 2019). Međutim, s obzirom na razvoj različitih vrsta kriptovaluta za različite svrhe, Europska bankovna uprava (engl. *European Banking Authority* - EBA) je provela procjenu da li kriptovalute mogu biti klasificirane kao „elektronički novac“ unutar Direktive elektroničkog novca (engl. *EU E-Money Directive* - EMD2[38]) ili sredstvo plaćanja unutar Direktive o platnim uslugama Europske unije, (engl.

[37] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595027276299&uri=PI_COM:Ares(2019)7834655
[38] https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:02009L0110-20180113&from=EN

Payment Services Directive - PSD2[39]). Procjena je provedena s ciljem nadopune prethodnog razmatranja ESMA-e o pitanju trebaju li se kriptovalute klasificirati kao financijski instrumenti.

Imajući u vidu da različite kriptovalute imaju različite karakteristike koje se tokom razvoja kriptovalute u njenog ekosustava mogu mijenjati, procjena je provedena od slučaja do slučaja. Na primjer, startup provodi ICO na Etherum kompjuterskoj platformi kako bi prikupio inicijalna sredstva za razvoj svog projekta pri čemu izdaje token koji će, po razvoju matičnog blockchaina, naknadno biti zamijenjen za primarnu kiptovalutu. Dakle, ta digitalna imovina prolazi kroz dva stanja, odnosno tokom svog procesa stvaranja, ulazi u dvije kategorije prethodno opisanih kriptovaluta: utilizacijski token (ili samo token jer nema nikakvu svrhu u proizvodu ili uslugama startupa) i vrstu kriptovalute koja ima matični blockchain, poput blockchain ekonomija.

Rezultati procjene ukazuju da kriptovalute mogu biti klasificirane kao elektronički novac samo ako zadovoljavaju sljedeću definiciju: „elektronički novac znači elektronički, uključujući magnetski, pohranjena novčana vrijednost kako je predstavljena na zahtjev upućen izdavatelju i koja je izdana po primitku sredstava u svrhu izvršenja platnih transakcija u smislu članka 4. točke 5. Direktive 2007/64/EZ, te koju prihvaća fizička ili pravna osoba koja nije izdavatelj elektroničkog novca“[40]. U tom smislu, primjer kriptovaluta kao elektroničkog novca bi bila situacija u kojoj tvrtka želi stvoriti otvorenu blockchain platežnu mrežu, u kojoj mogu sudjelovati trgovci i potrošači, izdavanjem tokena koji bi služio kao sredstvo plaćanja u mreži. Token bi se izdavao po primitku fiat valute i bio bi fiksno vezan za tu valutu po paritetu 1:1. Također, token bi se morao moći otkupiti po tom istom paritetu u bilo kojem trenutku u budućnosti. Prema procjeni Europske bankovne uprave, takav token bi zadovoljavao definiciju elektroničkog novca sukladno Direktivi elektroničkog novca – EMD2, odnosno zadovoljio bi sljedeće karakteristike:

a) pohranjuje se elektroničkim putem;
b) ima novčanu vrijednost;
c) predstavlja potraživanje od izdavatelja;
d) izdaje se po primanju sredstava;

[39] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[40] https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:02009L0110-20180113&from=EN

e) izdaje se u svrhu izvršenja platnih transakcija;
f) prihvaćaju ga osobe koje nisu izdavatelj.

Slijedom toga, izdavanje predloženog tokena zahtijevalo bi, prema procjeni Europske bankovne uprave, autorizaciju tvrtke izdavatelja kao institucije za elektronički novac (osim ako nije dostupno relevantno izuzeće) (EBA Report, 2019).

Također, primjer kriptovaluta kao elektroničkog novca je situacija u kojoj tvrtka stvara platežnu mrežu koju osigurava kroz pametne ugovore kako bi transferirala donacije u dobrotvorne svrhe. Nakon primitka novčanih donacija na zasebnom bankovnom računu u financijskoj instituciji, tvrtka kreira i izdaje token koji predstavlja upravo primljeni iznos. Token se potom pohranjuje u novčaniku donatora i može se deponirati prema određenoj dobrotvornoj organizaciji ili otkupiti po nominalnoj vrijednosti. Umjesto direktnog transfera fiat novca od donatora prema dobrotvornoj organizaciji, tokeni se transferiraju upotrebom pametnih ugovora, ali tek nakon što dobrotvorna organizacija ispuni unaprijed dogovorene uvjete i potvrdi ih neovisna treća strana. Dobrotvorna organizacija tada bi dobila tokene koji bi mogli biti otkupljeni kod kreatora i izdavatelja tokena, po nominalnoj vrijednosti na zahtjev, što rezultira efektivnim prijenosom sredstava u fiat valuti prema dobrotvornoj organizaciji putem tradicionalnih platnih mreža. Mreži bi mogli pristupiti samo provjereni korisnici, a tokenima se ne bi smjelo trgovati na sekundarnim tržištima. Kao i u prethodnom primjeru, ovaj token zadovoljava kriterije elektroničkog novca kako je utvrđeno u Direktivi elektroničkog novca – EMD2. Sukladno rezultatima procjene, mogu postojati slučajevi u kojima će se na temelju specifičnih karakteristika predmetne kriptovalute kvalificirati kao elektronički novac i stoga će biti obuhvaćene Direktivom elektroničkog novca – EMD2. U takvim slučajevima je nužna autorizacija institucija povezanih s aktivnostima koje se odnose na elektronički novac.

Prema regulaciji unutar Direktive o platnim uslugama – PSD2 kriptovalute nisu novčanice, kovanice ili multiplicirani novac unutar financijskog sistema. Iz tog razloga, kriptovalute ne spadaju u definiciju novčanih sredstava prema članku 4. PSD2, osim ako se u svrhe EMD2 ne kvalificiraju kao „elektronički novac“, navodi Europska bankovna uprava u svojoj procjeni (EBA Report, 2019). Europska bankovna uprava u svojoj procjeni ističe ukoliko tvrtka predloži da se primjenom

tehnologije distribuiranog zapisa kreira transakcijski sustav koji bi imao mogućnost izvršenja platnih transakcija, izdavanje platnih instrumenata i/ili pribavljanje platnih transakcija i doznaka novca, s kriptovalutama koje su kvalificirane kao elektronički novac, takva bi aktivnost spadala u opseg PSD2 iz razloga što bi takva aktivnost uključivala platežna sredstva.

S obzirom na razmatranje kriptovaluta unutar Direktive elektroničkog novca i Direktive o platnim uslugama, kao nadopuna istraživanju koje je provedeno od strane ESMA nadzornog tijela prema MiFID-u, a u smislu primjene postojećeg zakona o financijskim uslugama EU-a na kriptovalute, trenutni stav regulatornih tijela je takav da se kriptovalute mogu, ovisno o njihovim karakteristikama, kvalificirati kao financijski instrumenti, elektronički novac ili ništa od prethodnog. Također, kao rezultat razmatranja, izgledno je da značajan dio aktivnosti koje uključuju kriptovalute na spada u područje primjene postojećeg zakona o financijskim uslugama EU-a, ali može spadati u opseg nacionalnih zakona. U izvještaju Europske bankovne uprave se ističe da aktivnosti koje uključuju kriptovalute ne podliježu zajedničkoj shemi reguliranja EU-a, čime se otvaraju potencijalna pitanja o zaštiti potrošača npr. subjektivna objava u vezi s rizicima koji su povezani s aktivnostima kriptovalute. Štoviše, činjenica da kriptovalute mogu spadati u područje primjene postojećeg zakona o financijskim uslugama EU-a, ne znači nužno da se svi rizici povezani sa odnosnom kriptovalutom aktivno i učinkovito kontroliraju, što zahtijeva daljnju razradu i analizu (EBA Report, 2019).

5.3. Regulacija kriptovaluta unutar SAD-a

Regulativni okvir vrijednosnih papira u SAD-u predstavlja vrlo široko područje tako da pokriva većinu transakcija i načina na koji se novac prikuplja od investitora (Jabotinsky, H. Y. 2018). Prema dosadašnjoj analizi sudske prakse u SAD-u, bitcoin kriptovaluta se ne kvalificira kao vrijednosni papir, niti pod kategoriju „Ugovora o investiranju“ (engl. *Investment Contract*[41]), zbog činjenice da ne spada u definiciju uobičajene vrste vrijednosnih papira. Prema Komisiji za vrijednosnice i burzu Ugovor o investiranju postoji kada s radi o ulaganju novca u zajedničko poduzeće s

[41] https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

razumnim očekivanjem da će se ostvariti dobit od napora drugih. U skladu s navedenim, Jabotinsky, H. Y. (2018) navodi da bitcoin doista sliči drugim vrstama fiat valuta. Njegova cijena je određena ponudom i potražnjom, a ne temelji se na naporima drugih, što je jedan od uvjeta tretiranja kriptovaluta kao vrijednosnica prema definiciji Ugovora o investiranju. Međutim, postavlja se pitanje što je s ostalim kriptovalutama poput ethereum blockchain ekonomije, litecoina, EOS-a itd. Definicije „vrijednosnica“ na temelju Zakona o vrijednosnim papirima iz 1933. godine (engl. *Securities Act*[42]) i Zakona o burzi vrijednosnih papira iz 1934. godine (engl. *the Exchange Act*[43]) su gotovo identične i svaka je dovoljno široka da uključuje različite vrste financijskih instrumenata kojima se trguje na komercijalnim tržištima, a za koje se može posumnjati da spadaju u uobičajene koncepte vrijednosnih papira (Lee Kuo Chuen i Low, 2018). Definicije uključuju dionice, obveznice i instrumente novčanog tržišta, kao i razne investicijske fondove i zajednička poduzeća koja su osmislili osobe koje žele ostvariti profit od napora i ulaganja drugih. Kada se ostale kriptovalute, poput DAO-a i ethereuma, stave u kontekst prethodno navedenih zakonskih okvira, može se uvidjeti njihova sličnost s vrijednosnim papirima, što znači da su u tom slučaju, prema regulativi SAD-a, izdani bez poštivanja zakona i propisa. U nastavku se daje pregled osnovnih definicija vrijednosnih papira i okruženja koje se odnosi na trgovanje vrijednosnim papirima prema zakonskoj regulativi SAD-a, s ciljem interpretiranja i utvrđivanja potencijalnog okvira koji bi regulirao kriptovalute.

Osnovni je cilj Zakona o vrijednosnim papirima iz 1933. god. osigurati objavu svih relevantnih informacija javnosti kako bi potencijalni investitori mogli procijeniti vrijednost financijskih instrumenata na tržištu i donijeti odgovarajuće odluke o investiranju (Hu, 2012). Kako bi se to postiglo, Zakon o vrijednosnim papirima zahtijeva registraciju izdavatelja prije izdavanja vrijednosnih papira, koja podrazumijeva podnošenje prijave o registraciji prema SEC-u koja uključuje prospekt koji pruža sve relevantne informacije investitorima u vezi s tvrtkom čije će se dionice uskoro ponuditi (Jabotinsky, 2018). Bitcoin transakcijski sustav je kreiran od strane nepoznate ili nepoznatih osoba, stoga nije jasno tko bi bio obvezan registrirati izdavanje bitcoin kriptovalute. S druge strane, u slučaju projektno orijentiranih kriptovaluta, financiranih putem ICO-a, moguće je definirati tim koji je bio začetnik

[42] https://venturebeat.com/wp-content/uploads/2010/05/sa33.pdf
[43] https://www.nyse.com/publicdocs/nyse/regulation/nyse/sea34.pdf

projekta, što znači da bi se, sukladno Zakonu o vrijednosnim papirima, kriptovalute prije njihova izdavanja morale registrirati. Ovdje se već može uočiti nedostatak adekvatne prilagodbe regulativnog okvira SAD-a prema kriptovalutama. Naime, nije jasno što u tom slučaju predstavlja račvanje postojećeg programskog koda bez prethodno zapisanih transakcija. Drugim riječima, ukoliko se Bitcoin transakcijski sustav klasificira kao platežna kirptovaluta, račvanjem transakcijskog sustava i sinkroniziranim podizanjem čvorova mreže npr. u Japanu, Kini, Njemačkoj i SAD-u, uz uvjet širenja mreže privlačenjem novih korisnika, a to se može postići kroz nekoliko linija programskog koda implementirajući naknadni otkup, kreira se transakcijski sustav bez pozadinskog tima, organizacije ili startupa koji bi bio predmet regulacije.

Prema Zakonu o burzi vrijednosnih papira iz 1934. godine, svaka osoba čije poslovanje uključuje izvršavanje transakcija vrijednosnim papirima (bilo da je riječ o vlastitim vrijednosnim papirima ili vrijednosnim papirima drugih ljudi), smatra se brokerom ili trgovcem (Jabotinsky, 2018). Takva definicija utječe na burze koje pružaju mogućnost trgovine kriptovalutama. Ukoliko se kriptovalute kao takve tretiraju kao vrijednosnice, svaka institucija koja pruža mogućnost trgovine kriptovalutama, mora registrirati svoju djelatnost kod Komisije za vrijednosnice i burzu, osim ako nije izuzeta od takve regulacije. Također, djelatnost investicijskih fondova u SAD-u je regulirana Zakonom o investicijskim društvima (engl. *Investment Company Act*) iz 1940. godine. Prema Zakonu o investicijskim društvima, „investicijsko društvo“ se, između ostalog, definira kao svaki izdavatelj koji se bavi ili predlaže da se bavi poslom ulaganja, naknadnog ulaganja, posjedovanja, držanja ili trgovanja vrijednosnim papirima (Jabotinsky, 2018). Ukoliko se kriptovalute tretiraju kao vrijednosni papiri, svaka institucija osnovana s ciljem pružanja prethodnih djelatnosti, podložna je zakonskim normama Zakona o investicijskim društvima. Drugim riječima, takva djelatnost uključuje registraciju djelatnosti kod SEC-a, osim ako je izuzeta od regulacije, što je obično slučaj kod privatnih plasmana, ograničenog broja investitora ili poslovanja s kvalificiranim kupcima koji su više sofisticirani.

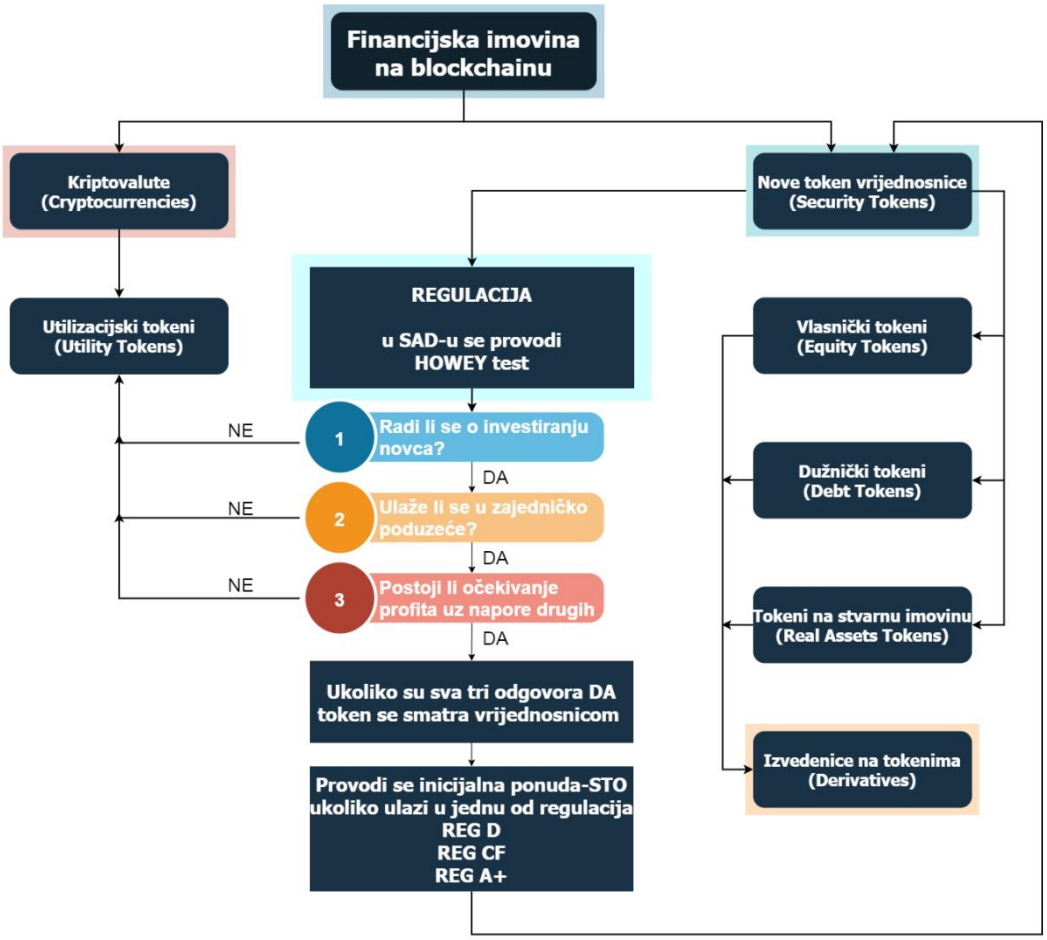
S obzirom na prethodni presjek aktualne zakonske regulative SAD-a kojom se definiraju buduća postupanja s vrijednosnim papirima ili potencijalnim vrijednosnim papirima, razvidno je kako postojeći okvir nije dostatan za klasificiranje trenutnog

ekosustava kriptovaluta i njihovog okruženja. Drugim riječima, sve kriptovalute, osim bitcoina, bi se prema gore navedenim zakonskim normama, klasificirale kao vrijednosni papiri, što značajno odstupa od razmatranja regulative kriptovaluta od strane EU-a, koji uvažava institut utilizacije, odnosno svrhe tokena u proizvodu i usluzi. Međutim, s obzirom na kontinuirani razvoj kriptovaluta i tehnologije povezane s njima, te zbog sve veće potrebe za formalnom regulacijom s ciljem razvoja tržišta kriptovaluta, regulacija digitalne imovine u SAD-u se značajno oslanja na regulaciju kroz Ugovor o investiranju. Komisija za vrijednosnice i burzu i savezni sudovi često koriste metodologiju Ugovora o investiranju kako bi utvrdili je li nova financijska imovina, poput digitalne imovine, ulazi u kategoriju vrijednosnih papira čime bi bila podložna njihovim zakonima o vrijednosnim papirima.

Regulatorni okvir unutar Ugovora o investiranju zahtijeva da se sve ponude i prodaje vrijednosnih papira, uključujući i one koje uključuju digitalnu imovinu, ili registriraju u skladu s njezinim odredbama, ili se mogu kvalificirati za izuzeće od registracije. Odredbe o registraciji su strogo definirane i zahtijevaju potpune i istinite informacije koje se pružaju prema potencijalnim investitorima. Važnu stavku predstavljaju informacije koje se odnose na suštinske upravljačke napore koji utječu na uspjeh poduzeća za korporativno okruženje, ali i za ostale vrste poduzeća bez obzira na njihovu organizacijsku strukturu ili oblik, kao što je DAO organizacija. Ukoliko se relevantne informacije o naporima, napretku i izgledu poduzeća ne objavljuju, dolazi do značajnih informacijskih asimetrija između uprave i promotora poduzeća s jedne strane, i investitora i potencijalnih investitora s druge strane. Smanjenje asimetrije informacija putem potrebnih objavljivanja štiti investitore i jedna je od glavnih svrha saveznih zakona o vrijednosnim papirima SAD-a.

Regulacija kroz Ugovor o investiranju se provodi primjenom tzv. „Howey testa“. Howey test se primjenjuje na bilo koji ugovor, plan ili transakciju, neovisno o tome ima li predmet ispitivanja neke karakteristike tipičnih vrijednosnih papira. Osim forme i uvjeta digitalne imovine, Howey test analizira i okolnosti digitalnog sredstva i način na koji se plasira javnosti, prodaje ili preprodaje, što uključuje prodaju na sekundarnom tržištu. Iz tog razloga, svi dionici projekta koje provode marketing, inicijalnu ponudu, preprodaju ili distribuciju digitalne imovine, moraju analizirati

relevantne transakcije kako bi utvrdili primjenjuje li se zakonska regulativa na njih, odnosno na digitalnu imovinu.



Shema 5. Regulacija kriptovaluta kroz Ugovor o investiranju u SAD-u
Izvor: Izrada autora

Metodologija Howey testa se provodi razmatrajući okruženje pod kojim se digitalna imovina kreira putem interpretacije odgovora na tri pitanja, ilustrirana Shemom 5. :

a) Radi li se o investiranju novca;
b) Ulaže li se u zajedničko poduzeće;
c) Postoji li očekivanje profita uz napore drugih.

Ukoliko su odgovori na sva tri pitanja pozitivna, nova digitalna imovina (kriptovaluta) se smatra token vrijednosnicom i ulazi u jednu od kategorija regulacije vrijednosnica prema Komisija za vrijednosnice i burzu. Regulacija D prema Zakonu o vrijednosnim

papirima iz 1933. godine pruža brojna izuzeća od zahtjeva za registraciju, omogućavajući nekim tvrtkama da nude i prodaju svoje vrijednosne papire, a da pri tome ne moraju registrirati ponudu kod Komisije za vrijednosnice i burzu[44]. Postoji samo obveza elektroničke predaje "Obrasca D" SEC-u nakon što izdavatelj prvi puta prodaje svoje vrijednosne papire i uključuje samo akreditirane investitore. Regulacija CrowdFund (CF) također ne zahtijeva registraciju ponude kod SEC-a i omogućuje širi i pristupačniji pristup šireg raspona demografske skupine investitora. U prvog krugu prodaje je moguće prikupiti 1.07 milijuna američkih dolara. Ograničenje koliko se može investirati ovisi o neto vrijednosti individualnog investitora i godišnjem prihodu[45]. Regulacija A + zahtijeva pružanje baznih informacija prema SEC-u i može uključivati i neakreditirane ulagače. Postoje određena ograničenja oko razine prihoda investitora i njihovog državljanstva. Iznos sredstava koji se prikuplja mora biti minimalno u visini od 2 milijuna američkih dolara, a maksimalno u visini od 50 milijuna dolara i glavno mjesto poslovanja moraju biti Sjedinjene Države ili Kanada[46]. S druge strane, ukoliko je samo jedan od odgovora Howey testa negativan, kriptovaluta se smatra utilizacijskim tokenom, što znači da ne podliježe postojećoj regulaciji vrijednosnih papira u SAD-u.

5.4. Regulacija kriptovaluta unutar HR

Pitanje regulacije kriptovaluta u Hrvatskoj započelo je razmatranjem upita o mogućim poreznim obvezama investitora i trgovaca s kriptovalutama. Porezna uprava Republike Hrvatske (Porezna uprava) izdala je mišljenje 7. svibnja 2015. godine na pitanje jesu li transakcije, uključujući posredovanje, u vezi s virtualnim valutama, kao što je bitcoin, oslobođene plaćanja PDV-a (Čičin-Šain, 2017). Mišljenje Porezne uprave se temeljilo na upitu poslanom prema Hrvatskoj narodnoj banci (HNB). U svom očitovanju, zajedno s očitovanjem HNB-a, Porezna uprava navodi da bitcoin ne potpada niti pod jednu zakonom reguliranu kategoriju sredstava plaćanja te da ne predstavlja novac, niti sredstvo plaćanja u Republici Hrvatskoj niti stranu valutu odnosno strano sredstvo plaćanja. Također, HNB navodi da bitcoin ne predstavlja zamjenu za ekvivalentnu vrijednost fiat valute te da iz tog razloga ne može biti

[44] https://www.sec.gov/fast-answers/answers-regdhtm.html
[45] https://www.investor.gov/introduction-investing/investing-basics/glossary/regulation-crowdfunding
[46] https://www.securexfilings.com/regulation-a/

elektronički novac. Sukladno očitovanju HNB-a, Porezna uprava navodi mišljenje prema kojem se za potrebe oporezivanja PDV-om bitcoin može smatrati prenosivim instrumentom (koji omogućuje ispunjenje novčane obveze) te da su njegove transakcije oslobođene od plaćanja PDV-a. Čičin-Šain (2017) daje mišljenje kako kategorija dohodak od kapitala, odnosno kapitalni dobici najbolje odgovaraju „pravnoj prirodi" bitcoina, s obzirom na dano stajalište Porezne uprave u kojem se navodi da se radi o prenosivim financijskim instrumentima. Isto tako, sukladno upitu o načinu oporezivanja dobitaka proizašlih iz trgovanja i poslovima povezanim s kriptovalutama, i RRiF[47] je dao mišljenje prema kojem se ostvareni dohodak iz trgovanja s kriptovalutama smatra dohotkom od kapitala, odnosno oporezuje se po osnovi kapitalnih dobitaka. Budući se radi o dobitku po osnovi kupoprodaje kriptovaluta, takva aktivnost je ekvivalentna aktivnostima s instrumentima tržišta novca. S druge strane, Čičak (2019) navodi kako sa aspekta računovodstvenog procesuiranja kriptovaluta, njihova klasifikacija prema MRS-u 7[48] ne odgovara novčanim ekvivalentima (instrumentima tržišta novca) jer su kriptovalute podložne značajnoj volatilnost cijena, što je u suprotnosti s osnovnim karakteristikama instrumenata tržišta novca. Autor navodi da se kriptovalute računovodstveno evidentiraju kao Nematerijalna imovina (MRS 38), i u određenim okolnostima Zalihe (MRS 2), pa je razvidno razilaženje poreznog i računovodstvenog tretmana kriptovaluta u HR.

S obzirom na navedeno, primjetno je da su određene formalne institucije u Republici Hrvatskoj zauzele jednoznačni stav o klasifikaciji kriptovaluta kao financijski instrumenata tržišta novca. Drugim riječima, trenutno regulatorno okruženje u HR ne priznaje razlike između vrsta kriptovaluta, niti bilo koji drugi oblik njihove klasifikacije, kojim bi se možda izuzela porezna obveza, kao što je to slučaj u istraživanju provedenom od strane ESMA-e. Takvo postupanje, zajedno s izostankom proaktivne formalne regulacije, ne ide u prilog stvaranju pozitivne poduzetničke klime koja bi privukla potencijalne investitore čime bi se potaknuo razvoj FinTech područja u Republici Hrvatskoj.

[47] https://www.rrif.hr/Porezni_tretman_kapitalnih_dobitaka_po_osnovi_trgo-3543-misljenje.html
[48] Međunarodni računovodstveni standard (MRS)

6. POČELA BITCOIN TEHNOLOGIJE

Bitcoin je digitalna valuta koja počiva na kriptografiji. Kriptografija je znanost koja se bavi proučavanjem područja matematičkih i računalnih tehnika s ciljem efikasnije informacijske sigurnosti, odnosno sigurnijeg prijenosa podataka. Dva su osnovna kriptografska primitiva[49] korištena u Bitcoin transakcijskom protokolu: funkcija sažimanja (engl. *hash ili digest*) i asimetrična kriptografija (engl. *asymmetric cryptography*). Oba primitiva su nužna za siguran i vjerodostojan transfer vrijednosti, odnosno konsenzusno distribuirani zapis te zbog toga bitcoin ulazi u kategoriju kriptovaluta.

6.1. Funkcija sažimanja

Važan primitiv u kontekstu kriptovaluta utemeljenih na *dokaz o radu* konsenzus algoritmu je kriptografska funkcija sažimanja jer se koristi prilikom rudarenja novih blokova u mreži, sažimanja javnog ključa i konstrukcije bitcoin adrese, te digitalnog potpisa. Funkcija sažimanja H je jednosmjerni matematički algoritam koji ulazne podatke x različite, ali definirane veličine, pretvara u izlazni zapis s jedinstvenom strukturom i fiksnom veličinom h. Da bi se funkcija sažimanja smatrala kvalificiranim kriptografskim algoritmom, postoje četiri dodatna svojstva koja moraju biti ispunjena (Judmayer et al., 2017):

a) Lakoća izračuna – računalno je lako izračunati sažimanje bilo koje određene konačne poruke:

$$h = H(x), gdje\ je\ h\ fiksne\ veličine$$

b) Jednosmjerna operacija – nije moguće generirati poruku koja ima zadani rezultat funkcije sažimanja:

$$Za\ dani\ rezult\ h\ nemoguće\ je\ pronaći\ podatak\ x\ gdje\ je\ h = H(x)$$

[49] Kriptografski primitivi su kriptografski algoritmi niže razine koji se koriste za izradu cjelovitih kriptografskih protokola.

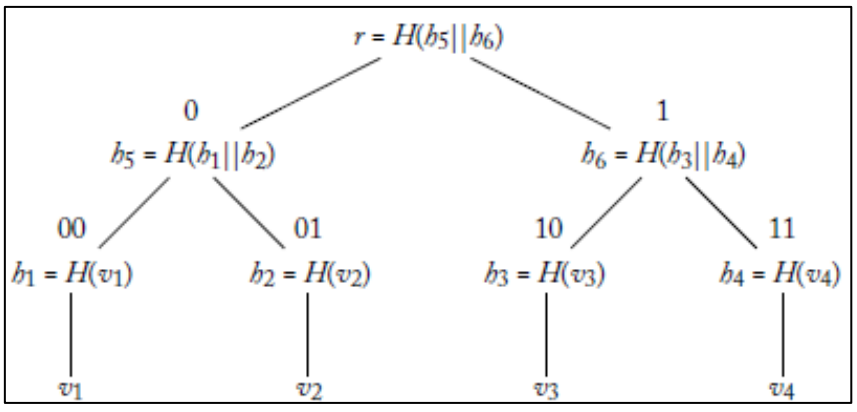
c) Otpornost na podudarnost rezultata funkcije ulaznog podatka – primjenom funkcije sažimanja na dva moguća različita podatka, nije moguće pronaći identičan izlazni rezultat:

$$Za\ dani\ podatk\ x\ nemoguće\ je\ pronaći\ drugi\ podatak\ x'tako\ da\ je$$
$$x \neq x'\ i\ \ H(x) = H(x')$$

d) Otpornost na podudarnost rezultata funkcije bilo koja dva različita podatka – primjenom funkcije sažimanja na bilo koja dva različita podatka, nije moguće pronaći identičan izlazni rezultat:

$$Nemoguće\ je\ pronaći\ bilo\ koja\ dva\ podatka\ x, x'\ gdje\ je$$
$$x \neq x'\ i\ \ H(x) = H(x')$$

Osim kriptografske funkcije sažimanja, tehnologija kriptovaluta se značajno oslanja i na kriptografski alat poznat kao Merkle stablo koji omogućuje brzu i sigurnu provjeru sadržaja velike količine podataka. Merkle stabla su binarna stabla u kojima su čvorovi (listovi) označeni vrijednostima koje treba provjeriti, a svaki čvor koji ne predstavlja list Merkle stabla je označen kao rezultat funkcije sažimanja prethodne vrijednosti podređenog čvora (Judmayer et al., 2017).



Shema 6. Primjer Merkle stabla sa $v = 4$ vrijednosti.
Izvor: Judmayer et al. (2017)

Shema 6. ilustrira Merkle stablo, odnosno korijen stabla kao rezultat funkcije sažimanja sa $v = 4$ vrijednosti. U Bitcoin transakcijskom sustavu vrijednosti od $v1$ do $v4$ predstavljaju transakcije koje je potrebno pohraniti na distribuiranu mrežu. Provjera pripadnosti transakcije $v1$ Merkle korijenu stabla r se provodi naknadnim pokretanjem funkcije sažimanja na parovima vrijednosti Merkle stabla, što značajno ubrzava naknadnu provjeru vjerodostojnosti zapisa. Na primjer, da bi se potvrdila pripadnost vrijednosti v_1 korijenu Merkle stabla r, potrebne su samo vrijednosti h_2 i h_6. Ukoliko naknadni rezultat korijena Merkle stabla odstupa od prethodnog rezultata korijena stabla, došlo je do izmjene u vrijednostima podataka. Opisani proces verifikacije zapisa predstavlja važnu komponentu blockchain tehnologije i čini suštinski dio konsenzus algoritma.

6.2. Asimetrična kriptografija

Druga važna komponenta kriptografije koju koristi Bitcoin transakcijski sustav je asimetrična kriptografija, odnosno kriptografija javnog ključa. Vlasništvo nad bitcoinom se uspostavlja putem digitalnih ključeva, bitcoin adresa i digitalnog potpisa, gdje digitalni ključevi zapravo nisu pohranjeni u mreži, već ih korisnici stvaraju i pohranjuju u datoteku ili jednostavnu bazu podataka koja se naziva novčanik (Antonopoulos, 2017). Digitalni ključevi asimetrične kriptografije su rezultat algoritma kojim su kreirani i potpuno su neovisni o bitcoin protokolu. Bitcoin transakcijski protokol ne koristi enkripciju javnog ključa u svom izvornom obliku. Razlog tome je izostanak potrebe za skrivanjem podataka. Štoviše, sve transakcije na bitcoin transakcijskoj mreži su javne i moguće ih je pratiti. Bitcoin protokol za verifikaciju transakcija koristi digitalni potpis koji uključuje kriptografiju javnog ključa, ali u obrnutoj primjeni. Cilj digitalnog potpisa sličan je onom rukom pisanog potpisa. Njime se osigurava da je poruku generirao potpisnik, da poruka nije promijenjena i krivotvorena i da se potpis ne može poreći (Franco, 2015).

Kao odgovor na nedostatke simetrične kriptografije, kriptografiju javnog ključa razvili su tijekom 1970-ih Diffie, Hellman i Merkles i predstavlja temelj za računalnu i informacijsku sigurnost (Franco, 2015). Simetrična kriptografija se oslanja na enkripciju i dekripciju podataka upotrebom jednog ključa, što uključuje slanje istog komunikacijskim kanalima, odnosno predstavlja rizik presretanja šifrirane poruke i

ključa te otkrivanja njenog sadržaja. S druge strane, Bitcoin protokol koristi asimetričnu kriptografiju za kreiranje para ključeva. Par ključeva se sastoji od javnog ključa iz kojeg je izvedena bitcoin adresa i za koji se vežu jedinice valute i privatnog ključa koji služi za dokazivanje porijekla sredstava i njihovo trošenje digitalnim potpisom.

Prema Judmayer et al. (2017) shema kriptografije javnog ključa se definira kao trostruko učinkoviti algoritam $\mathcal{E} = (A, E, D)$ gdje je:

e) A – algoritam za generiranja ključeva koji ne koristi vrijednosni input, a kreira output u obliku ključeva (pk, sk), gdje je pk javni ključ koji se može javno dijeliti i sk privatni ključ koji bi trebao ostati tajan:

$$(pk, sk) \leftarrow A()$$

f) E – enkripcijski algoritam koji uzima javni ključ pk, kao i poruku $m \in \mathcal{M}$ kao input te kreira šifrirani output $c \in \mathcal{C}$ kriptiran javnim ključem pk povezanim s parom javni/privatni ključ (pk, sk) namjeravanog primatelja:

$$c = E(pk, m)$$

g) D – (deterministički) dekripcijski algoritam koji uzima privatni ključ sk, kao i šifriranu poruku $c \in \mathcal{C}$ te kreira izvornu poruku $m \in \mathcal{M}$ koja je kriptirana javnim ključem pk povezanim sa privatnim ključem sk, ili $\perp$ (*false*) ukoliko je korišten neodgovarajući privatni ključ:

$$m = D(sk, c)$$

Iz čega slijedi da ukoliko su prethodne operacije reverzibilne $\forall(pk, sk)$ od A stoji da je:

$$\forall m \in \mathcal{M} : D\big(sk, E(pk, m)\big) = m$$

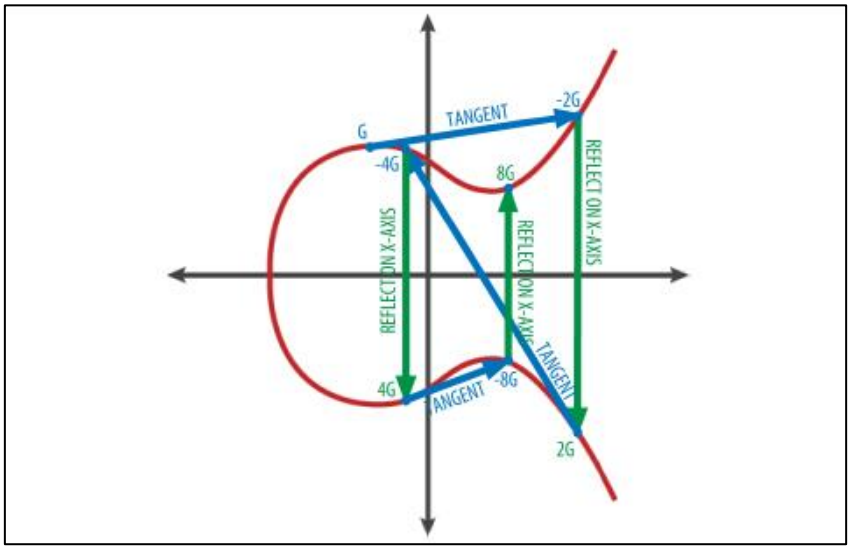
Privatni ključ je nasumično odabirani broj između 1 i $1-n$ pri čemu je n konstanta ($n = 1{,}158 \times 10^{77}$, nešto manje od 2^{256}) definirana kao redoslijed eliptičke krivulje koju koristi bitcoin (Antonopoulos, 2017). S obzirom da se privatnim ključem kroz digitalni potpis dokazuje porijeklo sredstava i pruža mogućnost potrošnje jedinica valute, vlasništvo i kontrola nad privatnim ključem temelj je korisnikove kontrole nad svim sredstvima povezanim s odgovarajućom bitcoin adresom. Sukladno tome, otkrivanje privatnog ključa javnosti, pruža mogućnost neželjene potrošnje jedinica valute jer njegovo otkrivanje daje nadzor na bitcoinom osiguranim tim ključem. Privatni ključ također mora biti sigurnosno kopiran i zaštićen od slučajnih gubitaka, jer ako se izgubi, ne može se vratiti, a sredstva kojim je osiguran su izgubljena zauvijek (Antonopoulos, 2017).

Javni ključ je izveden iz privatnog ključa provedbom množenja eliptičke krivulje, odnosno matematičkim procesom provedenim na eliptičkoj krivulji uvjetovanim veličinom privatnog ključa. Matematički izračun javnog ključa je nepovratan proces, što znači da je moguće izvesti javni ključ iz privatnog, ali je nemoguće izvesti privatni ključ iz javnog i u tome leži sva značajnost asimetrične kriptografije javnog ključa. Sve što je kodirano javim ili privatnim ključem može dešifrirati samo odgovarajući ključ tog para. Javni ključ je javni podatak koji služi za enkripciju podataka, ili u slučaju kriptovaluta, služi da bi korisnici transakcijskog sistema mogli slati, odnosno vezati jedinice valute za njega transakcijskim protokolom. S druge strane, samo digitalnim potpisom transakcije s odgovarajućim privatnim ključem se otključavaju i autoriziraju prethodno vezana sredstva za javni ključ, i bitcoin „prelazi“ od jednog korisnika prema drugom. Javni ključevi se mogu tumačiti kao brojevi bankovnih računa, a privatni ključevi se tada mogu protumačiti kao potpisi ili lozinke potrebne za otključavanje tih bankovnih računa.

Antonopoulos (2017) navodi da se javni ključ koji koristi Bitcoin transakcijski sustav izvodi pomoću eliptičke krivulje izvođenjem matematičke operacije na eliptičkoj krivulji: $pk = sk * G$, gdje je G konstantna točka koja se naziva točka generatora. Bitcoin transakcijski sustav koristi vrstu (oblik) eliptičke krivulje „secp256k1“[50] definiranu od strane Nacionalnog instituta za standarde i tehnologiju (engl. *National*

[50] Oblik eliptičke krivulje „secp256k1“ je definiran funkcijom $y^2 = (x^3 + 7)$ na ograničenom polju koordinatnog sustava. Izvor: https://www.johndcook.com/blog/2018/08/14/bitcoin-elliptic-curves/

Institute of Standards and Technology – NIST), gdje je točka generatora poznata i jednaka za sve korisnike koji kreiraju (pk, sk) par ključeva. Obrnuta operacija, izračunavanje privatnog ključa sk, ukoliko je poznat javni ključ pk, provodi se metodom iteracije i jednako je zahtjevna koliko i pokušaj svih mogućih vrijednosti. Ukoliko bi netko i pokušao izvesti privatni ključ iz dostupnog javnog ključa kojeg koristi Bitcoin blockchain, bilo bi mu potrebno $2^{116,45}$ sekundi koristeći samo jedno računalo s centralnim procesorom (engl. *central processing unit* – CPU) snage 3 GHz ili oko $2^{91,54}$ godina, otprilike 3.599.861.590.422.752.583.114.293.248 godina, ugrubo 260.859.535.537 puta starosti svemira (Franco, 2015).



Shema 7. Kriptografija eliptičke krivulje: vizualizacija množenja točke G s cijelim brojem (privatni ključ) sk na eliptičkoj krivulji
Izvor: Antonopoulos (2017)

Shema 7. ilustrira proces izvedbe javnog ključa pk iz danog privatnog ključa sk. Pojednostavljeno, kriptografija eliptičke krivulje može se promatrati kao vrlo velika sukcesija točaka (Franco, 2015). Proces pronalaska javnog ključa na eliptičkoj krivulji počinje od određene poznate točke G i njenim množenjem sa proizvoljno odabranim brojem, odnosno privatnim ključem: $pk = sk * G$, što je zapravo isto kao i dodavanje G broja samom sebi sk puta zaredom. U kriptografiji eliptičke krivulje, dodavanje točke samoj sebi stvara tangentnu liniju koja će presijecati krivulju u novoj točki (Furneaux, 2018). Definiranjem nove točke $-2G$ i njenim preslikavanjem preko osi x,

kreira se nova točka $2G$. Točka u kojoj tangentna linija te nove točke sječe eliptičku krivulju predstavlja točku $-4G$ koja će se ponovno reflektirati preko osi x. Proces se ponavlja sk puta sve dok se ne izvede javni ključ $pk = (x, y)$, (Antonopoulos, 2017). Prema tome, konačni javni ključ je točka na eliptičkoj krivulji i sastoji se od para koordinata uobičajeno s prefiksom 04, a privatni ključ je broj koraka od generatora koje se moraju proći da bi se stiglo do točke javnog ključa.

6.3. Digitalni potpis

Digitalni potpis (engl. *digital signature*) je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i autentičnost potpisanog elektronskog dokumenta[51]. Algoritam digitalnog potpisa koji se koristi u Bitcoin transakcijskom mreži je algoritam digitalnog potpisa eliptičke krivulje (engl. e*lliptic curve digital signature algorithm* – ECDSA). Antonopoulos (2017) ističe da digitalni potpis služi tri svrhe u kontekstu bitcoin transakcije. Prva je da se potpisnom dokazuje da je vlasnik privatnog ključa, koji je implicitno vlasnik sredstava, odobrio trošenje tih sredstava, druga svrha je neporecivost autorizacije transakcije i treća je da se potpisom dokazuje da transakciju (ili određene dijelove transakcije) nitko nije i ne može mijenjati nakon što je potpisana. Bitcoin transakcijski protokol digitalni potpis provodi kroz dva dijela. Prvi dio je algoritam za stvaranje digitalnog potpisa na transfer jedinica valute inicirajući bitcoin transakciju. Drugi dio je algoritam koji omogućava verifikaciju digitalnog potpisa javnom provjerom koja uključuje transakciju i javni ključ, potvrđujući bitcoin transakciju. Međutim, iako je digitalni potpis verificiran kao ispravan, odnosno transakcija potvrđena, to ne znači da je ona provedena. Tak nakon provedbe *dokaza o radu* od strane neovisnog čvora u mreži, transakcija će biti zabilježena na Bitcoin distribuiranu blockchain mrežu i može se smatrati izvršenom. Važno je istaknuti da iako je transakcija verificirana i proveden je *dokaz o radu* algoritam te je ista propagirana mrežom dalje u obliku bloka transakcija, može se dogoditi da se sve transakcije u zadnjem bloku transakcija odbace. To je situacija u kojoj su dva neovisna čvora proveli *dokaz o radu* na odabranim transakcijama otprilike u isto

[51] Izvor: https://sh.wikipedia.org/wiki/Elektronski_potpis

vrijeme[52]. S obzirom da mreža može uvažiti samo jedan *dokaz u radu* koji će se dalje propagirati, drugi blok transakcija se odbacuje i transakcije se vraćaju u bazu nepotvrđenih transakcija (engl. *transaction pool*). Stoga, da bi se transakcija smatrala potpuno izvršenom, poželjno je sačekati kreiranje dodatnih blokova transakcija nakon bloka u koji je uključena transakcija koja se prati kako bi se izbjegla mogućnost odbacivanja provedene transakcije, odnosno duple potrošnje.

Prema Judmayer et al. (2017) shema digitalnog potpisa se definira kao trostruko učinkoviti algoritam $\mathcal{S} = (A, S, V)$ gdje je:

a) A – jednako kao i prethodno (algoritam za generiranja para ključeva):

$$(pk, sk) \leftarrow A()$$

b) S – algoritam za potpis koji uzima privatni ključ sk, kao i poruku (transakciju[53]) $m \in \mathcal{M}$ kao input te kreira potpis $\sigma \in \Sigma$ koji može biti propagiran javno zajedno s porukom (transakcijom) u izvornom obliku. Poziva se kao:

$$S: \sigma \leftarrow E(sk, m)$$

c) V – (deterministički) algoritam koji uzima javni ključ pk, poruku (transakciju) $m \in \mathcal{M}$ u izvornom obliku kao i potpis $\sigma \in \Sigma$ kao input i kreira prihvaćanje ili odbijanje (engl. *accept or reject*) kao output, u ovisnosti o valjanosti potpisa σ na poruci (transakciji) m:

$$\{prihvaćanje, odbijanje\} \leftarrow V(pk, m, \sigma)$$

Iz čega slijedi da je potpis σ generiran preko algoritma S prihvaćen od strane algoritma V ukoliko su (pk, sk) validni javni i privatni par ključeva. Prema tome, $\forall(pk, sk)$ od A stoji da je:

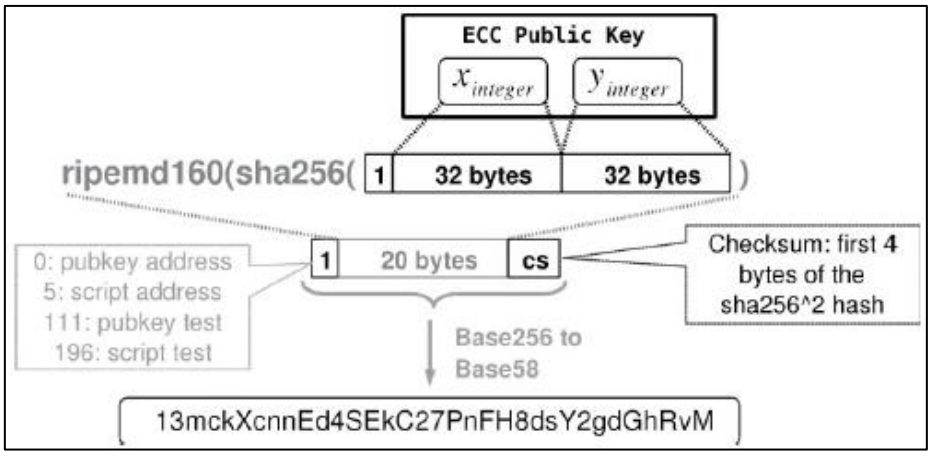
[52] Provedba *dokaz o radu* konsenzus algoritma u istom vremenu od strane dva neovisna čvora rezultira račvanjem sustava (engl. *fork*). Moguće je da u tom trenutku pola mreže, odnosno čvorova rudara slijedi prvi izvorni blockchain, a da druga polovica rudara slijedi novu liniju blokova tj. novi blockchain. U tom slučaju, Bitcoin protokol određuje da je ispravni blockchain onaj koji je najduži, što usmjerava čvorove rudare kako bi radili na blockchainu koji je prihvaćen od zajednice.

[53] Prije potpisivanja privatnim ključem, transakcije se provode kroz funkciju sažimanja tako da se potpisuje rezultat funkcije sažimanja, a ne transakcija u svom izvornom obliku.

$$\forall m \in \mathcal{M} : V(pk, m, S(sk, m)) = prihvaćanje$$

6.4. Bitcoin adrese

Bitcoin adrese koje služe za zaprimanje (vezanje) jedinica valute su u osnovi javni ključevi na kojima je provedena funkcija sažimanja i aktivnosti transformacije u zapis kakav je poznat kao bitcoin adresa. Da bi se potrošila jedinica bitcoina, transakcija koja autorizira potrošnju mora biti potpisana odgovarajućim privatnim ključem. Softver za novčanik stvara bitcoin adresu pokretanjem algoritma za generiranje ključeva i na taj način bilo koji korisnik može stvoriti onoliko bitcoin adresa koliko želi (Franco, 2015).



Shema 8. Generiranje bitcoin adrese
Izvor: Franco (2015)

Algoritmi koji se koriste za izradu bitcoin adrese iz javnog ključa ja *Secure Hashing Algorithm* – SHA256 i algoritam *Integrity Primitives Evaluation Message Digest* – RIPEMD160 (Antonopoulos, 2017). Shema 8. ilustrira proces generiranja bitcoin adrese od javnog ključa kao inputa. Prvi korak je provedba funkcija sažimanja SHA256 na javnom ključu čime se kreira broj veličine 256 bita (32 bajta)[54]. Drugi korak je provedba funkcije sažimanja RIPEMD160 na rezultatu prethodne funkcije

[54] Bit i bajt predstavljaju mjerne jedinice za količinu podataka u računarstvu.

čime se kreira broj veličine160 bita (20 bajta)[55]. Kao treći korak provodi se *checksum na* samo 4 bajta, odnosno provjera ispravnosti adrese kako bi se izbjeglo slanje sredstava na neispravno kreirane adrese. Softver bitcoin novčanika provjerava je li adresa ispravna prije slanja sredstava na tu adresu. Ukoliko je znamenka s bitcoin adrese pogrešno upisana ili kopirana, novčanik će prepoznati pogrešku i izbjeći slanje sredstava na ovu adresu. Čak i ako novčanik ne uspije prepoznati pogrešku, a transakcija se nekako uspije propagirati mrežom, čvorovi u mreži bi otkrili nevažeću adresu i odustali od transakcije (Franco, 2015). Na kraju, kako bi se dugi binarni brojevi na kompaktni način pretvorili i prezentirali kao bitcoin adresa, provode se dva algoritma „Base256“ i „Base58“ koji dugi binarni format prevode u tekstualni format, odnosno bitcoin adresu u obliku kakva se koristi danas.

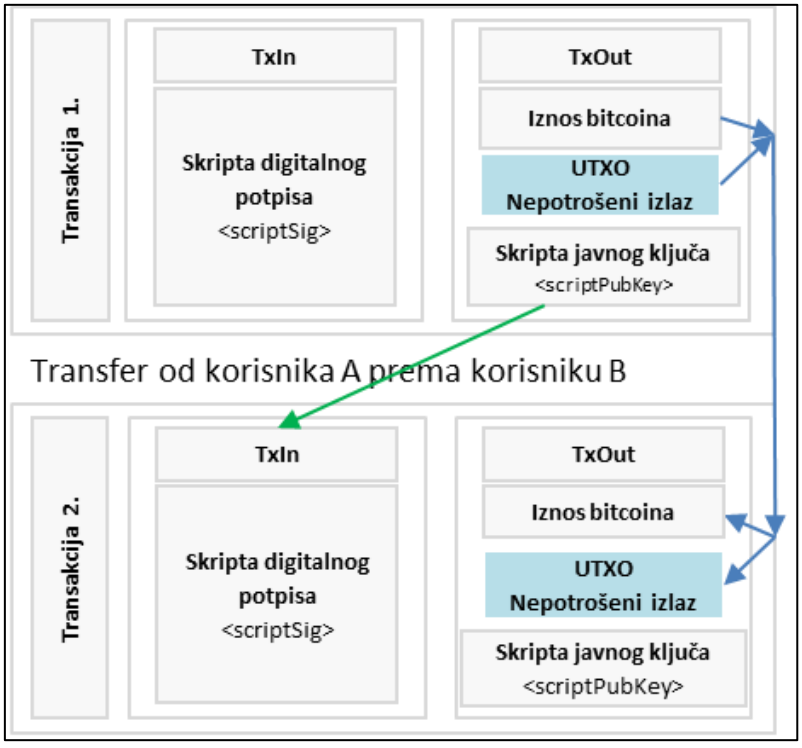
6.5. Transakcije

Transakcije su najvažniji dio bitcoin sustava. Sve ostalo u Bitcoinu protokolu je dizajnirano tako da osigura da se transakcije mogu kreirati, propagirati mrežom, verificirati i na kraju zapisati u globalnu distribuiranu javnu knjigu transakcija (Antonopoulos, 2017). Jedinice valute bitcoin se ne nalaze na računalima korisnika, nego predstavljaju unose u distribuiranu bazu podataka koja se naziva blockchain (Franco, 2015). Za razliku od centraliziranih digitalnih valuta, Bitcoin transakcijski protokol na pohranjuje brojeve računa i salda tih računa, kao što je to slučaj kod tradicionalnih bankovnih transakcija. Bitcoin blockchain pohranjuje transakcije, odnosno vrijednosti vezane za određene javne ključeve. Furneaux (2018) navodi da adresa može, ali i ne mora, imati dodijeljenu vrijednost jedinica valute, te da se zapravo bilo koja vrijednost može dodijeliti gotovo bilo kojoj adresi, uključujući i blok teksta. Drugim riječima, osim jedinice valute, protokol može prenositi bilo koji drugi digitalni zapis pri čemu bi svojstvo sigurnosti i distribucije javne glavne knjige i dalje bilo prisutno. Pored toga, implementacijom pametnih ugovora u blockchain, otvara se mogućnost uvjetovanih transakcija, odnosno transakcija koje se izvršavaju po ispunjavanju unaprijed postavljenih uvjeta. Mogućnost takvih transakcija pružaju decentralizirane kompjutorske platforme, poput Ethereuma i Eosa. Praktična

[55] Pretpostavlja se da je tvorac Bitcoin protokola odabrao drugu funkciju sažimanja kako bi smanjio veličinu adrese čineći transakcije manjima, ali opet zadržavajući dostatnu veličinu bita kako bi vjerojatnost kreiranja iste adrese od dva različita javna ključa bila što manja.

implikacija takvog svojstva prepoznata je od strane inovativnih startupova koji rješenje, za različite svakodnevne poslovne izazove, vide kroz implementaciju blockchain tehnologije u širok spektar djelatnosti.

Bitcoin transakcije se sastoje od popisa ulaznih podataka transakcije (engl. *transaction inputs* – TxIn) i popisa izlaznih podataka transakcije (engl. *transaction outputs* – TxOut). Svaki izlazni podatak transakcije sadrži dva podatka: iznos i adresu sljedećeg primatelja za koju se vežu jedinice valute. S obzirom da je adresa kreirana iz javnog ključa koji je izveden od odgovarajućeg privatnog ključa primatelja, samo vlasnik privatnog ključa može otključati sredstva pohranjena u popisu izlaznih transakcija. Kako bi se sredstva otključala, vlasnik privatnog ključa mora digitalno potpisati transakciju koja sredstva šalje na novu bitcoin adresu.



Shema 9. Pojednostavljeni prikaz bitcoin transakcije
Izvor: Izrada autora

Shema 9. prikazuje pojednostavljeni prikaz bitcoin transakcije. Transakcija se provodi u tri koraka:

a) Prvi korak – korisnik A digitalno potpisuje transakciju 2. kao ulaz (TxIn) i tako otključava izlaz (TxOut) transakcije 1. Drugim riječima, skripta digitalnog potpisa (engl. *scriptSig*) transakcije 2. je programski kod neophodan za skriptu javnog ključa (engl. *scriptPubKey*) transakcije 1. Potpis se provodi s privatnim ključem povezanim s javnim ključem na bitcoin adresi. Ukoliko je potpis neispravan, transakcija se smatra nevažećom.
b) Drugi korak – korisnik A uključuje iznos bitcoina prezentiran u izlazu (TxOut) transakcije 1. u izlaz (TxOut) transakcije 2. i „zaključava" sa skriptom javnog ključa korisnika B. Drugim riječima, samo korisnik B digitalnim potpisom (privatnim ključem) može otključati izlaz (TxOut) transakcije 2.
d) Treći korak – transakcija se objavljuje na bitcoin mreži i ulazi u skupinu nepotvrđenih transakcija. Po preuzimanju transakcije, rudari (čvorovi) utvrđuju ispravnost skripte digitalnog potpisa transakcije 2. kojom je otključana skripta javnog ključa transakcije 1.

Prvi čvor u mreži koji prima transakciju potvrđuje valjanost transakcije. Ukoliko je transakcija ispravna, čvor je prosljeđuje prema ostalim čvorovima u mreži. Za provjeru ispravnosti transakcije, čvorovi slijede sljedeće korake (Franco, 2015):

a) Provjera postoje li prethodni izlazni podaci o transakciji na koje se transakcija odnosi i da isti već nisu potrošeni. Čvor u mreži provodi ovu provjeru kontrolom nepotrošenih izlaza transakcija (engl. *unspent transaction output* – UTXO). UTXO je baza podataka koja sadrži samo nepotrošene izlaze transakcija. Svaka nova transakcija zapravo troši prethodno zabilježene neiskorištene izlaze transakcija i stvara nove koje može samo iskoristiti buduća transakcija. Na ovaj način, najmanje jedince bitcoina se kreću od vlasnika do vlasnika u lancu transakcija koje troše i stvaraju UTXO-a (Antonopoulos, 2017). Osim transakcija zabilježenih u UTXO-u, svaki novi blok sadrži i *coinbase* transakciju koja se odnosi na nove jedinice valute koje će dobiti čvor koji uspješno provede *dokaz o radu* konsenzus algoritam. Prednost UTXO-a je u tome što se može koristiti za brzu verifikaciju transakcija pretraživanjem UTXO baze. Ukoliko se transakcija nalazi u bazi, transakcija je valjana i proces verifikacije se nastavlja. Suprotno, ukoliko nije pronađena, transakcija nije važeća i može se odbaciti.

b) Provjera da je zbroj vrijednosti izlaznih transakcija (TxOut) jednak ili veći od zbroja vrijednosti prethodnih ulaznih transakcija (TxIn). Naime, nepotrošeni izlazi (TxOut) u Bitcoin protokolu se mogu potrošiti samo jednom i moraju se potrošiti u potpunosti tako da jedna transakcija može uključivati više prethodnih transakcija. Ukoliko korisnik šalje broj jedinica valute veći nego što je zaprimio po jednoj prethodnoj transakciji, softver korištenog novčanika će uključiti dodatnu prethodnu transakciju kako bi transferirao željeni broj jedinica valute. Razlika između zbroja vrijednosti izlaza i zbroja vrijednosti ulaza čini naknadu za čvor koji uspješno provode konsenzus algoritam. Naknada je uključena u *coinbase* transakciju.
c) Verifikacija digitalnog potpisa, odnosno provjera je li transakcija potpisana privatnim ključem koji odgovara javnom ključu bitcoin adrese.

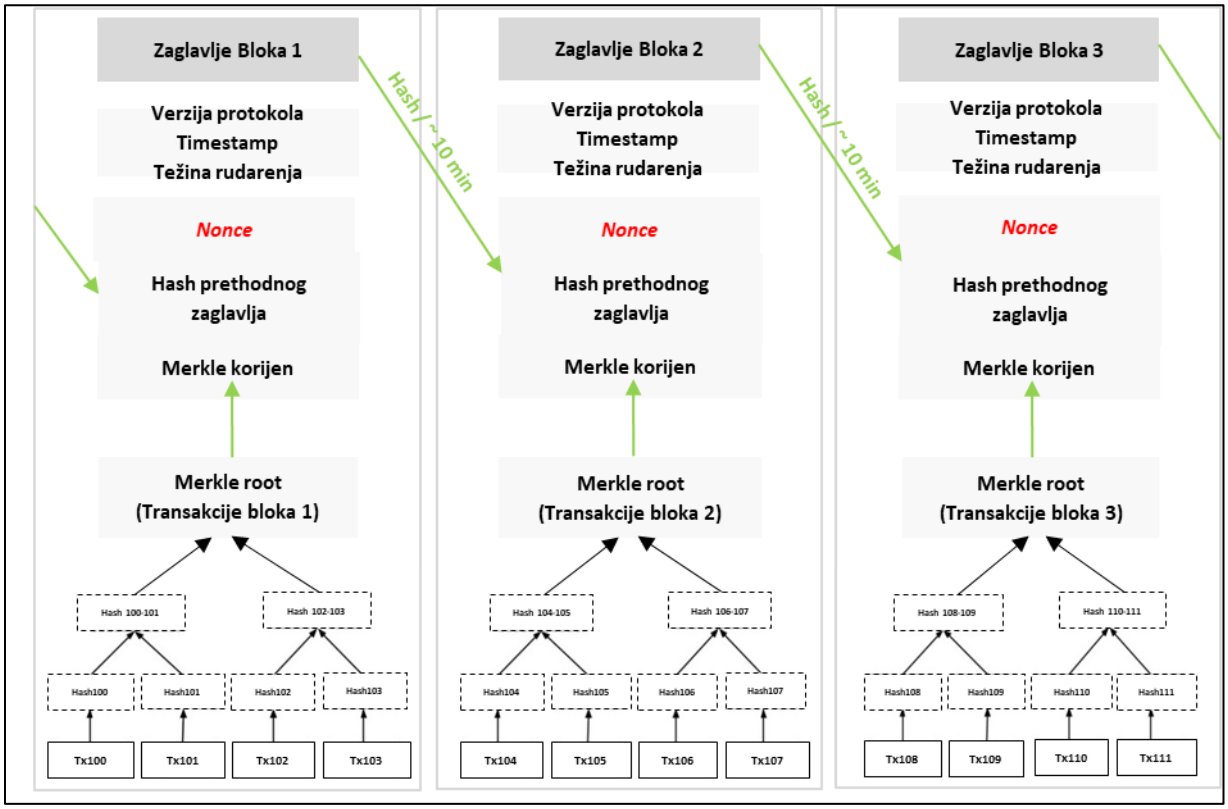
Bitcoin se zapravo prenosi od nepotrošenih izlaza (TxOut) od korisnika A prema nepotrošenim izlazima (TxOut) korisnika B. Kriptovalute predstavljaju zapis nepotrošenih izlaza (TxOut) u distribuiranoj predmemoriji (engl. *unspent transaction output* – UTXO), a svaki izlaz je povezan s javnim ključem korisnika.

6.6. Lanca blokova – blockchain

Blockchain je decentralizirani transakcijski sustav, odnosno distribuirana javna knjiga (engl. *public ledger*) osigurana kriptografijom i upravljana konsenzusom, na kojoj su zapisane sve transakcije koje su se dogodile između sudionika u mreži. To je rastuća lista distribuiranih zapisa aktivnosti na mreži međusobno povezana kriptografijom i nalazi se u svakom čvoru mreže. Javnu glavnu knjigu sačinjavaju transakcije grupirane u tzv. blokove iz čega proizlazi da je glavna knjiga zapravo lanac blokova (engl. *blockchain*). Svaki blok sadrži sažetak tog bloka, odnosno sažetak svih prethodnih transakcija zapisan kao sintaksa funkcije algoritma sažimanja SHA256 (Härdle et al., 2019), koji mu služi za identificiranje unutar blockchaina. Zbog toga što sažetak zadnjeg bloka uključuje i rezultat funkcije sažimanja prethodnog bloka, sve su transakcije na blockchain mreži zapravo povezane. Rezultat funkcije sažimanja zadnjeg bloka uključuje svaku transakciju nastalu na blockchain mreži sve od početnog bloka koji se naziva *genesis.* Promjena bilo kojeg podatka u prethodnim blokovima bi utjecala na rezultat funkcije sažimanja svih blokova koji su nastali nakon

trenutka promjene. S obzirom da se rezultat funkcije sažimanja distribuira širom mreže i predstavlja jedan od zapisa za sljedeći blok transakcija, ispravnost i vjerodostojnost rezultata funkcije, odnosno transakcija koje su se dogodile na mreži, se mora moći provjeriti na jednostavan način. Provjera se provodi naknadnim pokretanjem funkcije na parovima vrijednosti Merkle stabla. Ukoliko dođe do odstupanja u rezultatu funkcije sažimanja između čvorova u mreži, to bi značilo da je došlo do promjene podataka, ili u prethodnim transakcijama, ili u kreiranom novom bloku transakcija. Drugim riječima, netko od sudionika mreže je promijenio zapis po nekoj od adresa u mreži i takav se blok transakcija odbacuje i klasificira kao netočan.

Blockchain je vjerojatno najvažnija inovacija koju je uveo Bitcoin transakcijski sustav, omogućavajući *peer-to-peer* digitalne valute. U osnovi, Bitcoin blockchain je distribuirana baza podataka koja sadrži sve bitcoin transakcije od početka (03. siječanj 2009. god.), kao i metoda zaštite tih transakcija (Franco, 2015).



Shema 10. Pojednostavljeni prikaz konstrukcije niza blokova transakcija
Izvor: Izrada autora

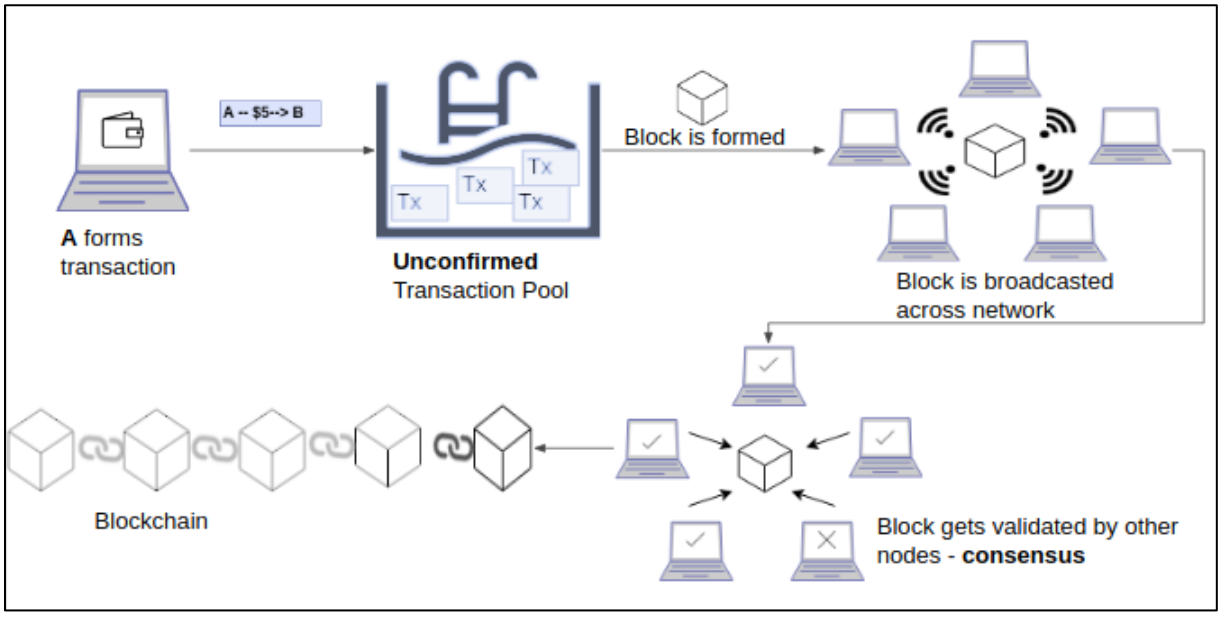
Blockchain se često vizualizira kao vertikalni snop s blokovima naslaganim jedan na drugi, a prvi blok služi kao temelj snopa. Vizualizacija blokova postavljenih jedan na drugi rezultira uporabom izraza kao što su „visina“ za udaljenost od prvog bloka i „vrh“ za identifikaciju zadnje dodanog bloka (Antonopoulos, 2017).

Shema 10. prikazuje pojednostavljeni prikaz tri bloka podataka i način na koji su oni povezani. Prilikom provedbe *dokaz o radu* konsenzus algoritma, čvor prvotno preuzima podatke o transakcijama u svom izvornom obliku, te na njima provodi funkciju sažimanja SHA256 da bi dobio Merkle stablo, odnosno korijen kao konačni rezultat provedenih funkcija. Podaci o transakcijama se početno pojedinačno sažimaju, da bi se poslije sažimali parovi rezultata funkcije. Nakon kreiranja Merkle korijena, kreira se zaglavlje bloka (engl. *block header*). Zaglavlje bloka sadrži tri osnovna podatka: Merkle korijen transakcija uključenih u blok, rezultat funkcije sažimanja prethodnog bloka i *nonce* nasumični broj koji se mijenja prilikom rudarenja da bi se postigao i osigurao konsenzus. Osim nasumičnog broja, zaglavlje bloka uključuje u druge metapodatke[56], kao što je verzija protokola, težinu rudarenja i vremensku oznaku (engl. *timestamp*). Težina rudarenja se kalibrira na deset minuta i to svakih 2.016 blokova, što je otprilike oko dva tjedna. Drugim riječima, uvijek će biti potrebno deset minuta da se započeta transakcija zapiše na distribuiranu bazu podataka. Težina rudarenja se prilagođava kako bi se proveo *dokaz o radu* konsenzus algoritam. U tehničkom smislu Bitcoin blockchaina, *dokaz o radu* konsenzus algoritam predstavlja mijenjanje nasumičnog broja (*nonce*) metodom iteracije kako bi zaglavlje bloka imalo rezultat funkcije sažimanja koji počinje s određenim brojem nula[57]. Također, pruža dodatnu sigurnost mreži čineći naknadnu izmjenu podataka na mreži računalno teško izvedivu. Naime, maliciozni čvor koji ima namjeru promijeniti stanje na mreži, morao bi naknadno ponovno provesti *dokaz o radu* za sve transakcije od trenutka promjene stanja po adresi pa sve do kraja blockchaina, i pri tome bi morao zadržati prednost ispred ostalih čvorova u mreži kreirajući najdulji blockchain. Pored toga, *dokaz o radu* prevenira kreiranje velikog broja transakcijskih blokova zahtijevajući potrošnju električne energije i ostalih

[56] Metapodatci su podatci o podatcima – podatci koji opisuju karakteristike nekog izvora u digitalnom obliku. Korisni su kod pregledavanja, prijenosa i dokumentiranja informacijskog sadržaja. Izvor: https://hr.wikipedia.org/wiki/Metapodatci

[57] Na datum 11.08.2020. god. rezultat funkcije sažimanja mora početi sa 19 nula. Izvor: https://www.blockchain.com/btc/block/000000000000000000007f9b5d85f191a25923182c1f1945328e11eac591dd5ab

resursa koji bi pravdali fundamentalnu vrijednost bitcoina kroz proces rudarenja. Prvi čvor koji pronađe rješenje s takvim izlaznim rezultatom funkcije sažimanja, kreirao je novi blok i nagrađen je sa novih 6,25 BTC-a. Svakih 210.000 blokova, otprilike 4 godine, nagrada se prepolovi, a ukupan broj bitcoina koji se može kreirati (rudariti) je 21 milijun. Nakon što je proveden *dokaz o radu* od strane jednog neovisnog čvora, blok podataka se propagira ostalim čvorovima u mreži koji svojom verifikacijom potvrđuju ili odbacuju konsenzus. Verifikacija čvorova u mreži se provodi slično kao i verifikacija transakcija, odnosno digitalnog potpisa. Naime, jednom kada su poznati svi ulazni podaci za funkciju sažimanja (svi elementi bloka zajedno s nasumičnim brojem), vrlo je jednostavno i brzo ponovno pokrenuti funkciju s ciljem usporedbe propagiranog rezultata i dobivenog rezultata naknadne funkcije sažimanja. Ukoliko se rezultati podudaraju, blok se smatra kao validan i propagira se dalje mrežom. Suprotno, ukoliko se rezultati ne podudaraju konsenzus nije postignut, blok se odbacuje i smatra se nevažećim.



Shema 11. Transakcijski model Bitcoin blockchaina
Izvor: https://labs.imaginea.com/utxo/#utxo-transaction-model

Shema 11. sublimira sve prethodno navedeno u transakcijski model kakav koristi Bitcoin protokol. U trenutku kada korisnik A želi poslati bitcoin korisniku B, korisnik A formira transakciju preko softvera korištenog novčanika. Softver novčanika digitalno

potpisuje zahtjev za slanjem bitcoina čime se kreira transakcija koja se prosljeđuje do prvog povezanog čvora mreže. Čvor verificira transakciju i distribuira ju dalje u mrežu kako bi se provela provjera njene valjanosti, nakon čega transakcija ulazi u bazu nepotvrđenih transakcija.

Puni čvorovi rudari dobivaju obavijest o kreiranoj transakciji, preuzimaju istu, verificiraju i provode *dokaz o radu*, odnosno sažimaju više transakcija u jedan blok podataka. Nakon uspješnog sažimanja, novi blok se emitira dalje mrežom gdje svi ostali čvorovi provjeravaju njegovu ispravnost i identificiraju ga kao posljednji važeći blok (nadogradnja blockchaina). Ukoliko je blok uspješno verificiran, isti se propagira dalje mrežom što znači da je konsenzus postignut i korisnik B može raspolagati s jedinicama bitcoin kriptovalute.

6.7. Konsenzus algoritmi

Konsenzus mehanizam predstavlja proces donošenja odluke koji osigurava da su svi čvorovi u mreži (nodovi) međusobno sinkronizirani i složni u tome koje su transakcije legitimne za dodavanje u blok. To je proces verifikacije transakcija koje će se dodati u blok, odnosno distribuirani dogovor oko jedne verzije istine s ciljem sprječavanja duple potrošnje. Prvi konsenzus algoritam *dokaz o radu* (engl. *proof-of-work* - PoW) je predstavljan kroz Bitcoin blockchain. Međutim, s obzirom na nedostatak iznimno velike potrošnje električne energije pri izvođenju funkcija sažimanja, zajednica iza blockchain ekosustava predložila je druge više učinkovite oblike verifikacije transakcija i transakcijskih blokova te postizanja konsenzusa.

Prvi sljedeći predloženi konsenzus algoritam je bio *dokaz o udjelu* (engl. *proof-of-stake* - PoS). PoW čvorovi provode rudarenje kriptovaluta (engl. *mining*), a PoS čvorovi provode kovanje kriptovaluta (engl. *minting*). U PoW konsenzus algoritmu vjerojatnost o pronalaska rješenja funkcija sažimanja ovisi o korištenoj računalnoj snazi koje posjeduje čvor rudar, dok u PoS algoritmu vjerojatnost o pronalasku novog bloka ovisi o udjelu u broju kriptovaluta koji posjeduje čvor kovač u odnosu na druge čvorove kovače u mreži. Kako bi se izbjegla nepoželjna centralizacija prema kovaču s najvećim udjelom kriptovaluta u mreži, osmišljeno je nekoliko različitih algoritama koji odabiru sljedećeg čvora kovača (engl. *forger*) koji će nadograditi blockchain

(engl. *forge*) s novim blokom verificiranih transakcija, kao što su: nasumični odabir bloka (engl. *randomized block selection*) i odabir prema duljini držanja kriptovalute (engl. *coin age-based selection*)[58]. U smislu potrošnje resursa kako bi se mreža održala sigurnom, PoS algoritam svakako ima prednosti, ali i nedostatke poput lakšeg napada 51% kupnjom kriptovaluta u udjelu u mreži većem od 50%.

Da bi se otklonili nedostaci, PoS algoritam je nadograđen ulogom odabranih delegata odgovornih za proces kovanja blokova te prelazi u *delegirani dokaz o ulogu* (engl. *delegated proof of stake* – DPoS). Delegirani PoS algoritam predstavlja konsenzus algoritam u kojemu korisnici na transakcijskoj mreži odabiru svog predstavnika (delegata) koji će u njihovo ime provoditi verifikaciju transakcija i kovanje novih blokova transakcija. Nastanak DPoS-ima veliku ulogu i u okruženju decentraliziranih financija jer omogućava ostvarivanje pasivnog dohotka korisnicima mreže (engl. *staking*) koji na taj način participiraju u sigurnosti mreže preko svog udjela, neovisno o njegovoj veličini. Prema (Dhillon, Metcalf i Hooper, 2017), dva su osnovna sudionika u DPoS konsenzus procesu: korisnici mreže (engl. *stakeholders*) koji imaju otvorene račune na mreži i mogućnost odabira delegata mreže i delegati (engl. *block producers*) entiteti koji upravljaju DPoS konsenzus protokolom. Čvorovi delegati DPoS protokola su ekvivalentni čvorovima rudarima PoW protokola. U kontekstu sigurnosti PoS i DPoS konsenzus algoritma, poticaj čvorova kovača je u tome što su uvjetovani svojim udjelom u mreži. Drugim riječima, niti jedan racionalan delegat mreže svojim nečasnim aktivnostima ne želi dovesti u pitanje integritet i sigurnost mreže, jer bi na taj način i njegov udio izgubio na tržišnoj vrijednosti.

Tablica 2. usporedno prikazuje osnovne karakteristike, prednosti i nedostatke tri vodeća konsenzus mehanizma. Kao što je već prethodno navedeno, u PoW algoritmu, odabir rudara je određen količinom računalne snage za izvođenje uvjetovane funkcije sažimanja. Kao glavni nedostatak se ističe potrošnja velike količine električne energije i općenito resursa za kupnju potrebne opreme za rudarenje. Zbog toga dolazi do centralizacije, odnosno udruživanja rudara u državama s nižom cijenom električne energije. Pored toga, u svom izvornom obliku PoW mehanizmi ne pružaju dostatnu brzinu u procesu verifikacije i pohranjivanja

[58] Izvor: https://en.wikipedia.org/wiki/Proof_of_stake

transakcija na blockchain mrežu u usporedbi s tradicionalnim transakcijskim sistemima.

Tablica 2. Usporedba karakteristika tri osnovna konsenzus mehanizma

Konsenzus mehanizmi	Opis	Prednosti	Nedostaci	Primjena
Dokaz o radu „Proof of Work" (PoW)	Odabir rudara je određen količinom računalne snage	Visoka sigurnost mreže	- Visoka potrošnja el. energije; - Zahtijeva skupu opremu; - Udruživanje rudara (mining pools); - Centralizacija rudarske snage; - Bogati postaju bogatiji; - Problem skalabilnosti.	- Bitcoin; - Bitcoin Cash; - Litecoin; - Ethereum (u planu je prelazak na hibridni PoS); - Monero.
Dokaz o ulogu „Proof of Stake" (PoS)	Odabir kovača je određen veličinom uloga u sistemu	- Ne zahtijeva visoku potrošnju el. energije i skupu opremu ; - Veća decentralizacija (nema udruživanja kovača); - Veća skalabilnost i učinkovitost.	- Bogati postaju bogatiji; - Lakše moguć *51% napad* (kupnja udjela od 51%).	- Dash; - Neo; - Pivx; - Decred.
Delegirani dokaz o ulogu „Delegated Proof of Stake" (DPoS)	Izabrana grupa delegata je odgovorna za proces kovanja bloka	- Visoka učinkovitost - Visoka skalabilnost - Bolja distribucija nagrade	- Djelomično centraliziran - Delegati s *lošom* namjerom lakše mogu naštetiti sistemu	- Eos; - Lisk; - Bitshares.

Izvor: Izrada autora

Odabir kovača u PoS protokolu je određen veličinom njihovog uloga na mreži. Prednost PoS u odnosnu na PoW su niži potrebni resursi u procesu verifikacije transakcija i kovanja blokova, čime se postiže veća decentralizacija, ali i brža obrada konsenzus protokola. Nedostaci PoS protokola je lakša centralizacija kupnjom udjela većem od 50%. Međutim, ovaj nedostatak se otklanja uz pretpostavku racionalnosti entiteta iza PoS protokola. Franko (2017) navodi da je jedan od glavnih nedostataka PoS zapravo račvanje mreže. U slučaju račvanja mreže na PoW protokolu, čvorovi rudari moraju odabrati jedan od mogućih lanaca blokova i na njega alocirati svoje resurse. S druge strane, u PoS protokolu, račvanje mreže s prethodno zapisanim

transakcijama znači i doznačavanje istog broja jedinica valute već postojećim kovačima koji neometano mogu nastaviti izvoditi konsenzus protokol i na tom novom blockchain, jer su dobili isti broj jedinca te nove kriptovalute. Drugim riječima, veća je mogućnost umnožavanja transakcijskih protokola. Za verifikaciju transakcija i kovanje novih blokova transakcija u DPoS konsenzus protokolu odgovorni su kovači delegati, odnosno pojedinci odabrani od strane korisnika mreže. Jednako kao i u PoS protokolu, DPoS je više učinkovit i brži u provedbi konsenzusa. Međutim, nedostaci se očituju u centralizaciji moći delegatima koji su potencijalno neadekvatni.

Osim navedenih, postoje i druga konceptualna rješenja koja nude mogućnost postizanja konsenzusa na blockchain mrežama. Blockchain je fleksibilan protokol u ovisnosti prema potrebi i krajnjoj ideji, pa se tako i konsenzus algoritmi prilagođavaju njihovom konceptu. Bashir (2017) navodi primjer razvoja konsenzusa *dokaz o proteklom vremenu* (engl. *proof of elapsed time* – PoET) od strane korporacije Intel za potrebe hibridnog blockchaina, odnosno korporativne primjene. Čest je slučaj da pojedini blockchain projekti kreiraju jedinstveno rješenje samo za njihove specifične potrebe. Tako je Namecoin blockchain kreirao *dokaz važnosti* (engl. *proof of importance* – PoI) konsenzus algoritam u kojem se odabir čvora koji provodi protokol konsenzusa ne oslanja samo na veličinu udjela korisnika u sustavu, nego se također nadzire i upotreba i kretanje tokena od strane korisnika radi uspostavljanja razine povjerenja i važnosti. Stellar blockchain koristi *federativni konsenzus* (engl. *federated consensus* ili *federated byzantine agreement* – FBA) gdje čvorovi rudari koriste samo druge odabrane čvorove od strane zajednice i njima propagiraju odobrene nove transakcije i blokove. Eigelshoven, Ullrich i Bender (2020) ističu da trenutno postoje čak 33 konsenzus protokola za javni blockchain. Neki od njih se provode u praktičnoj primjeni, a neki su još uvijek u akademsko istraživačkoj i razvojnoj fazi.

6.8. Prednosti i nedostaci blockchain tehnologije

Svojstvo decentraliziranog upravljanja i svojstvo distribuiranog zapisa, blockchain tehnologiji pruža određene prednosti, ali i nedostatke u odnosu na postojeću tehnologiju digitalnog, ali i fizičkog zapisa. Koristi se mogu sažeti kroz osam sljedećih točaka (Gates, 2017):

a) Transparentnost – blockcahin tehnologija povećava transparentnost u odnosno na postojeću tehnologiju. Promjene na javnoj knjizi su vidljive svim korisnicima na mreži, a transakcije ne mogu biti promijenjene ili izbrisane jednom kada su zapisane na blockchain. Na postojećim, tradicionalnim bazama, nedostatak transparentnosti omogućava korisnicima da izmijene stanje zapisa ili manipuliraju s podacima bez znanja drugih o nastalim promjenama. Blockchain tehnologija pruža transparentnost korisnicima na mreži preko transakcija koje su osigurane kriptografijom i upravljane konsenzusom između čvorova u mreži. Sve promjene su zabilježene skoro u realnom vremenu tako da bilo kakva manipulacija s podacima nije moguća. Uključivanjem blockchain tehnologije u svoju djelatnost, različite industrije povećavaju svoju transparentnost, bilo da se radi o aktivnostima transfera vrijednosti ili bilo kojim drugim djelatnostima koje uključuju spremanje digitalnog zapisa.
b) Izuzimanje centralnog entiteta – većina postojećih tradicionalnih sistema se oslanja na posrednika prilikom izvršavanja transakcija između korisnika, kao što su banke koje pružaju sigurnost i povjerenje u transfer valuta. Prednost blockchain tehnologije u odnosu na njih je u tome što pruža mogućnost transfera sredstava bez uključivanja treće strane. Zapravo, gdje god postoji nepovjerenje između dvije strane u poslu, može se implementirati tehnologija distribuiranog zapisa, s ciljem izuzimanja potrebe za trećom stranom kao kontrolnim tijelom. Navedeno značajno koristi milijunima ljudi širom svijeta koji žive u zemljama gdje nije moguće imati potpuno povjerenje prema trećoj strani zbog prisutnosti korupcije, visoke stope kriminala, slabe regulacije kompanija, fizičke evidencije zapisa itd. Blockchain je posebno koristan u ovim situacijama gdje ne postoji povjerenje u treću stranu i gdje su neposredne transakcije između ljudi nemoguće i riskantne.
c) Decentralizacija – decentralizacija upravljanja, odnosno distribucija digitalnog zapisa je ključna komponenta koja omogućava komunikaciju bez centralnog tijela na transparentan i siguran način. Blockchain predstavlja jednu glavnu knjigu distribuiranu širom javne mreže, umjesto više baza podataka upravljanih od strane privatnih organizacija. Blockchain omogućava disperziju moći, pojedinačni korisnici i kompanije ne moraju predati kontrolu samo jednoj instituciji, što olakšava kolaboraciju između interesnih strana i brže i

jednostavnije upravljanje. Na primjer, ukoliko financijske institucije transferiraju sredstva između sebe, svaka interesna strana mora održavati svoju bilancu sredstava koja može, ali i ne mora, odgovarati bilanci stanja suprotne strane. Primjenom blockchain glavne knjige, interesne strane samo moraju imati uvid u stanje transakcije na blockchainu koji bi im bio dostupan, kako bi se složili oko transakcije. Isto tako, decentralizacija doprinosi i kompanijama koje su jedna drugoj konkurencija, ali koje čine jednu industriju ili konzorciji. Pružanje kontrole nad podacima kompanije konkurenciji, svakako nije u interesu kompaniji. Međutim, blockchain tehnologija pruža fleksibilnost na način da kompanije mogu odabrati, dozirati i kanalizirati odabrane podatke koji se pružaju konkurenciji sve s ciljem njihovog komplementarnog odnosa usmjerenog prema širenju svoje djelatnosti. Također, centralizirane baze podataka su sklone sigurnosnim propustima i gubicima podataka. Blockchain ne počiva na jednoj bazi podataka te tako eliminira mogućnost jedinstvene točke kvara (engl. *single point of failure*), manipulacije, odnosno bilo kakve nečasne radnje koje bi dovela u pitanje integritet podataka. Svi čvorovi u mreži imaju kopiju istih podataka smanjujući tako mogućnost izmjene i gubitka podataka. Manipulacija s podacima na Bitcoin blockchainu zahtijeva kontrolu nad više od 50% čvorova koji čine transakcijsku mrežu, i to u isto vrijeme, što je praktički skoro neizvedivo.

d) Povjerenje – trenutne transakcijske metode plaćanja zahtijevaju povjerenje od korisnika u treću stranu kako bi provele transakciju. Blockchain dopušta izuzimanje centralnog entiteta, ali i dalje osigurava sigurnost i povjerenje između interesnih strana u provedbu transakcije. Nositelj povjerenja u ovom slučaju je blockchain mreža, a ne treća strana.
e) Sigurnost – podaci jednom pohranjeni na blockchain su nepromjenljivi čime se preveniraju naknadne izmjene podataka i malverzacije transakcijama. Svojstvo nepromjenljivosti, kombinirano s podacima povezanim u blokovima, osigurava jednostavnu i brzu provjeru transakcija sve od početka, odnosno trenutka nastanka blockchaina. Također, svojstvo nepromjenljivosti nedvojbeno ukazuje na trenutak nastanka transakcije, odnosno njenog zapisa na mrežu.
f) Širok spektar potencijalnih primjena – bilo kakav digitalni zapis koji ima neku ili nekome značajnost se može zapisati na blockchain kako bi se iskoristile i

osigurale sve prednosti koje blockchain pruža. Vrijednost ne mora biti isključivo monetarna, odnosno financijska. Neki od primjera su knjige, dokaz o vlasništvu, glazbeni zapis, digitalni identitet, licence itd. Razvojem Ethereum decentralizirane kompjutorske platforme i pametnih ugovora kojima se uvjetno izvršavaju transakcije i aktivnosti na mreži, dijapazon mogućih praktičnih implikacija blockchain tehnologije je sve širi. Blockchain ima potencijal promijeni skoro svaku industriju na svijetu.

g) Smanjenje troškova – blockchain tehnologija može osigurati značajno smanjenje troškova u različitim industrijama izuzimajući posrednika u procesu bilježenja i transfera imovine. Na tradicionalnim transakcijskim sustavima svaki transfer imovine, ili njena pohrana, zahtijeva uključivanje treće strane kao kontrolnog tijela u tom procesu kojemu se zauzvrat plaća naknada. Distribuirani transakcijski sustavi dopuštaju stranama transfer sredstava na jednoj dijeljenoj glavnoj knjizi, smanjujući tako troškove koji bi nastali održavanjem zasebnih baza podataka interesnih strana. Recentni primjer značajnijeg transfera sredstava za nisku naknadu se proveo na Bitcoin transakcijskom sustavu, gdje se jednom transakcijom transferirala vrijednost viša od milijarde dolara za naknadu od pet dolara[59].
h) Brzina transakcije – blockchain transakcijski sustavi ne samo da smanjuju troškove transakcija, nego i značajno ubrzavaju njihov proces. Isključujući posrednika, transakcije se mogu provoditi trenutno, u ovisnosti o odabranom konsenzus algoritmu decentralizirane mreže. Primjer je Bitshares DEX platforma gdje se sve transakcije sa matičnom valutom bitshares, neovisno o njihovoj veličini ili zemljopisnoj lokaciji, provode za manje od pet sekundi. S druge strane, za tradicionalni bankovni transfer, ponekad je potrebno više sati, pa čak i dana. Blockchain nije isključivo ograničen na transfer financijske vrijednosti. Bilo koji tip transakcije ili transfera vrijednosti potencijalno može uključivati blockchain tehnologiju čime se značajno povećava brzina prijenosa zapisa.

S druge strane, nedostaci blockchain tehnologije se očituju kroz više različitih aspekata. Prvi i osnovni nedostatak je propagiranje i obećanje praktične

[59] Izvor: https://cointelegraph.com/news/someone-transferred-a-billion-dollars-in-bitcoin-for-less-than-5

implementacije blockchain tehnologije kao rješenja za širok spektar problema i nedostataka u svakodnevnom poslovanju različitih industrija. Svakog dana kontinuirano nastaju startupovi temeljeni na blockchainu i kriptovalutama, prezentirajući projekte s poslovnom idejom za svaku industriju i djelatnost. Gates (2017) ističe kako trenutna situacija s tržištem kriptovaluta i blockchain tehnologijom dosta nalikuje razdoblju nastanka i razvoja interneta. Iako je internet promijenio svijet, većina obećavajućih projekata tog vremena danas niti ne postoji. U nastavku se navode ostali osnovni nedostaci povezani s blockchain tehnologijom i njenom praktičnom primjenom:

a) Nedostatak privatnosti – decentralizirani javni blockcahin, poput Bitcoin mreže, ne pruža privatnost, što otežava potpuno prihvaćanje tehnologije od šire javnosti, odnosno njenu širu primjenu. Iako se vlasnik sredstava predstavlja preko javne adrese, svaku transakciju koja je bilo kada nastala na blockchainu, moguće je pratiti još od *coinbase* transakcije. Na primjer, svaki trgovac koji zaprimi sredstva u zamjenu za isporučenu robu ili usluge, može pratiti stanje svojih kupaca preko adrese s koje su sredstva poslana, odnosno povezati adresu s osobom vlasnikom te adrese. Isto tako, činjenica da se svaka nastala i potvrđena transakcija objavljuje na mreži, ne ide u korist korisnicima koji bi htjeli da transakcija i njihov saldo novčanika ostanu skriveni. Ovo posebno uključuje osobe, odnosno općenito korisnike iz država različitih društvenih i političkih uređenja koje dopuštaju mogućnost nadziranja svojih građana. Pitanje privatnosti riješeno je preko privatnih kriptovaluta. Međutim, značajniji iznosi se za sada ne mogu transferirati, s obzirom da je ukupna tržišna kapitalizacija najveće kriptovalute koja pruža privatnost transakcija tek 1,5 milijardi dolara, što usporedbe radi s bitcoinom, iznosi 0,7% tržišne kapitalizacije bitcoina.
b) Sigurnosna pitanja – blockchain koristi naprednu kriptografiju i enkripciju kako bi pružio sigurnost svojim korisnicima. Međutim, raspolaganje sa sredstvima vezanim za adresu korisnika, uvjetovano je raspolaganjem privatnih ključeva iz kojih je izveden javni ključ, odnosno njegova adresa. U slučaju njihovog gubitka, jedinice valute povezane s parom javnih i privatnih ključeva su zauvijek izgubljene, jer ne postoji mogućnost obnove privatnih ključeva iz pripadajućih javnih ključeva. Postoji niz primjera u kojima korisnici zbog gubitka privatnih ključeva ne mogu pristupiti svojim sredstvima. Jedan od

primjera je slučaj iz Velike Britanije u kojoj je korisnik preko svog prijenosnog računala pružao podršku Bitcoin mreži i rudario bitcoin. Nažalost, prijenosno računalo na kojemu se nalazilo 7.500 bitcoina je bačeno, što danas iznosi u protuvrijednosti više od 85 milijuna dolara, a sigurnosna kopija privatnih ključeva ne postoji[60]. Isto tako, moguć je i sigurnosni propust različitih internet stranica i platformi koje pružaju usluge s kriptovalutama. Naime, oporavak, odnosno stopiranje transfera sredstava kreditnih kartica ili bankovnih računa se može provesti, dok se neželjenim dijeljenjem privatnih ključeva daje kontrola trećoj strani, bez mogućnosti oporavka jer su transakcije nepovratne. Sa aspekta šire uporabe, metode veće sigurnosti ne idu u korist blockchain tehnologije i čine ju teže prihvatljivom za širu svakodnevnu uporabu u svom izvornom obliku. Međutim, s obzirom na kontinuirani razvoj različitih programskih rješenja i mogućnosti u transakcijskom smislu, za očekivati je da će tehničko rješenje, poput *Lightning Network* protokola plaćanja druge razine, otkloniti navedene nedostatke i približiti blockchain tehnologiju široj populaciji.

c) Izostanak centralnog kontrolnog tijela – blockchain sustavi su dizajnirani tako da zamijene posrednike vraćajući kontrolu i odgovornost pojedincima uključenim u transakciju. S druge strane, bilo kakva promjena na programskom kodu, u smislu unapređenja mreže, zahtijeva konsenzus svih korisnika u zajednici, odnosno razvojnih programera i rudara putem platformi za kolaboraciju. Svojstvo decentralizacije nije korisno u usporedbi s tradicionalnim, centraliziranim transakcijskim sustavima, gdje se sve promjene provode brzo nakon odobrenja odgovornih osoba u korporaciji. Da bi se provelo unaprjeđenje Bitcoin blockchaina potreban je dogovor zajednice što utječe na sposobnost brze prilagodbe zahtjevima korisnika mreže. U slučaju da se dogovor ne postigne, dolazi do račvanja mreže (engl. *network fork*). Jedan dio čvorova rudara i razvojnih programera podržava matični blockchain, a drugi dio podržava novi blockchain, sa svim implementiranim promjenama i svojstvima. Učestalo račvanje mreže dovodi u pitanje i njenu sigurnost. Manji broj čvorova rudara znači i manju podršku sustava, odnosno veću mogućnost lakšeg preuzimanja kontrole nad mrežom i manipulacije. Sve navedeno budućnost javnog blockchaina čini i dalje neizvjesnim i riskantnim za širu

[60] Izvor: https://www.tportal.hr/tehno/clanak/bacio-milijune-u-bitkoinima-u-smece-20131128

implementaciju i razvoj decentraliziranih programskih rješenja od strane organizacija.

d) Rizik od napada 51% – napad 51% predstavlja situaciju u kojoj pojedini čvor rudar, ili grupa rudara čvorova, posjeduje kontrolu nad više od 50% čvorova koji čine transakcijsku mrežu, odnosno posjeduje dovoljnu količinu računalne snage koja mu pruža mogućnost da uvijek prvi provede funkciju sažimanja nad preuzetim transakcijama. Takva mogućnost kreira dualni transakcijski sustav tj. račvanje mreže, gdje maliciozni čvor na jednom transakcijskom kanalu koji je unaprijed predodređen kao blockchain koji će biti odbačen, vrši potrošnju veće količine jedinica valute i ta se transakcija validira i pohranjuje na odabrani blockchain od strane drugih čvorova rudara. Međutim, na drugom blockchainu, maliciozni čvor svoju transakciju ne povlači i ne zapisuje u novi blok, nego provodi funkciju sažimanja nad drugim preuzetim transakcijama. S obzirom da je brži u kreiranju blokova od ostalih čvorova, njegov blockchain je najduži, što znači da ga prate i drugi čvorovi u mreži, čime se prethodno potrošena sredstva oslobađaju jer transakcija pohranjena na blockchain, i mogu se ponovno potrošiti. Napad 51% dogodio se više puta na Ethereum classic blockchainu, a u zadnjem uspješnom pokušaju napadač je uspio duplo potrošiti više od 5,6 milijuna dolara, a trošak opreme koja mu je pružila takvu mogućnost je iznosio 0,2 milijuna dolara[61].

e) Nedokazana nova tehnologija – blockchain tehnologija se primarno koristi u domeni kriptovaluta i usluga povezanim s njihovim trgovanjem i njima kao temeljnom imovinom na području decentraliziranih financija. Ukoliko se promatra omjer izdanih kriptovaluta, financiranih projekata koji stoje iza njih i projekata koji stvaraju svakodnevnu primjenu, postoji veliki jaz između obećanog i realiziranog. Nedostatak stvarne svakodnevne primjene koja bi dala uporište fundamentalnoj vrijednosti kriptovalutama, ali projektima koji stoje iza njih i njihovim tehnološkim dostignućima, svrstava blockchain još uvijek u kategoriju nove i nedovoljno istražene tehnologije s nedokazanom praktičnom primjenom. Gates (2017) ističe da su upravo superiornosti blockchain tehnologije spram pandanu u tradicionalnog tehnologiji zapravo nedostaci. Na primjer, blockchain je više siguran jer ne dopušta naknadne

[61] Izvor: https://www.coindesk.com/ethereum-classic-suffers-second-51-attack-in-a-week

izmjene na mreži, međutim gubitkom privatnih ključeva, gubi se vlasništvo i kontrola nad digitalnim zapisom. Korisnici su primorani zapisivati privatne ključeve na komadu papira kako bi vjerojatnost gubitka kontrole sveli na minimalnu razinu. Također, nameće se pitanje stvarne koristi izuzimanja treće strane prilikom transakcija. Većina blockchain korisnika je mlađe populacije kojima otvaranje korisničkih računa i slanje transakcija ne predstavlja zahtjevne aktivnosti. S druge strane, korisnici koji nemaju iskustva s novom tehnologijom, vjerojatno bi htjeli uključiti treću stranu i dati im pristup privatnim ključevima kako bi si olakšali svakodnevnu uporabu nove tehnologije, čime se gubi ostvarena prednost izuzimanjem posrednika u transakciji.

f) Troškovi – *dokaz o radu* konsenzus algoritam koristi metodu iteracije koja zahtijeva potrošnju električne energije i drugih resursa prije nego što se blok podataka može zapisati na mrežu. Da bi se mreža nastavila održavati, trenutno je potrebno više energije nego što se potroši na razini manje države u godini dana, poput Švicarske[62]. Velika potrošnja energije ističe komparativne prednosti država gdje je električna energija povoljnija. Upravo zbog toga, decentralizirana mreža bi mogla u budućnosti postati sve više centralizirana, neovisno o vrsti korištenog konsenzus algoritma, tako da i ovdje postoji potencijalni problem centralizacije moći.

g) Nedostatak skalabilnosti – Bitcoin blockchain je opterećen problemom skalabilnosti. Protokol transakcija je konfiguriran tako da može podnijeti prosječno tri do četiri, a maksimalno do sedam transakcija po sekundi. Usporedbom sa tradicionalnim sustavom kartičnog plaćanja kojim se obradi više tisuća transakcija po sekundi, Bitcoin transakcijski sustav nije praktičan za širu implementaciju u svom izvornom obliku. Međutim, problem skalabilnosti, kao i drugih komparacijskih nedostataka za Bitcoin transakcijski sustav, pokušava se riješiti implementacijom protokola druge razine *lightning network-a*. Pored toga, postoje i druge kriptovalute koje pružaju mogućnost izvršenja puno većeg broja transakcija, čak i od komercijalnih sustava. Međutim, gledajući bitcoin kao svojevrsni tehnološki benchmark i mrežu koja je daleko najsigurnija u pogledu decentralizacije, blockchain još uvijek zaostaje za komercijalnim rješenjima.

---

[62] Izvor: https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison

h) Povjerenje, reputacija i razumijevanje blockchain tehnologije – blockchain je nova tehnologija čije se koristi tek trebaju dokazati. Blockchain isključuje treću stranu koja pruža povjerenje u transakciji. Međutim, korisnici moraju imati povjerenje u tehnološku infrastrukturu i anonimne osobe iza čvorova mreže koja im to omogućava. Postoje brojni primjeri gdje se bitcoin i općenito kriptovalute, dovode u vezu s različitim ilegalnim aktivnostima, najčešće za uklanjanje traga porijekla novca tzv. pranje novca, što je negativno utjecalo na njihovu reputaciju. Također, za potpuno shvaćanje i razumijevanje komparativnih prednosti, ali i nedostataka blockchain tehnologije, potrebna je svjesnost tržišnih potreba i tehnoloških mogućnosti blockchaina, ali i trenutne tradicionalne tehnologije. Tek onda bi se njihovom usporedbom mogli razlučiti nedostaci, prednosti i rizici koji proizlaze iz obje tehnologije. Zbog nerazumijevanja osnovnih karakteristika, koristi blockchain tehnologije su još uvijek nepoznanica široj javnosti. Zbog toga, većina korisnika kriptovaluta koristi usluge treće strane, kao i standardne lozinke da se prijave na platforme koje im pružaju usluge s kriptovalutama, gubeći prednost decentralizacije.

i) Regulacija i implementacija – tržište kriptovaluta je suočeno s problemom nedostatka pravne sigurnosti koji trenutno postoji oko postupanja s kriptovalutama u financijskoj regulaciji širom svijeta. Kriptovalute nisu nastale kao proizvod financijskih institucija, gdje bi se postepenim prijenosom znanja kroz vrijeme, preuzele i implementirale u izvornom obliku, ili u obliku inačice, u financijske institucije koje bi od njih imale koristi. Naprotiv, kriptovalute i cijeli njihov ekosustav su nastale i nastaju neovisno o okvirima postojećeg prototipa financijskog sistema kontinuirano pomičući granice svojim brzim razvojem. Upravo zbog toga, trenutno ne postoji definicija što predstavljaju kriptovalute, niti je jasno kako se i na koji način postojeći regulatorni okviri financijskih usluga odnosi na njih, što predstavlja veliku prepreku razvoju održivog ekosustava kriptovaluta. Navedeno vrijedi kako za kriptovalute koje imaju karakteristike financijskih instrumenata, tako i za kriptovalute koje ulaze u područje elektroničkog novca, ali i za kriptovalute koje zbog svojih značajki trenutno nisu obuhvaćene postojećim zakonodavstvom EU-a. S obzirom da kriptovalute koje ne spadaju u područje primjene EU zakonodavstva o financijskim uslugama, neke države razmatraju uspostaviti nacionalni zakonodavni okvir za uređivanje kriptovaluta. Međutim, takav pristup može

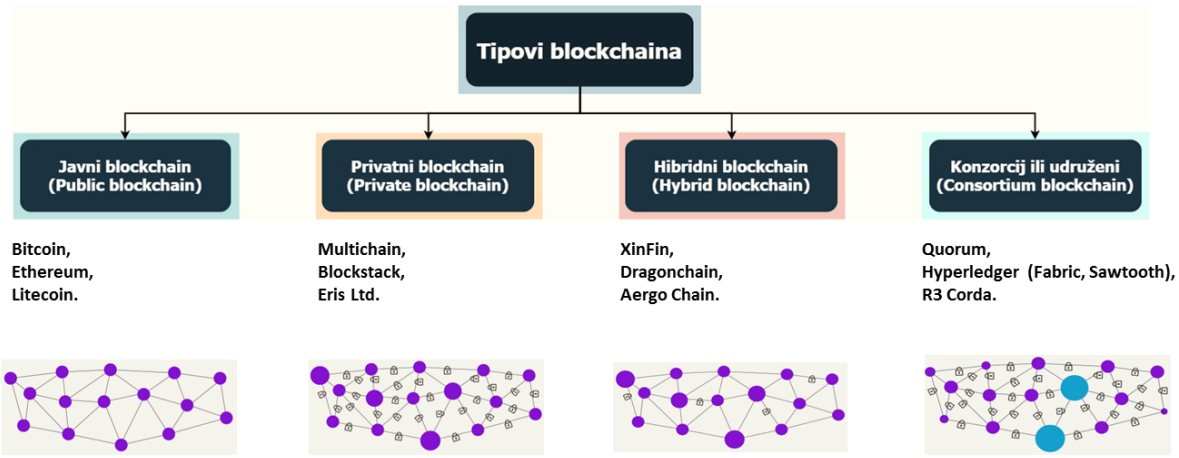
ograničiti pružanje prekograničnih usluga povezanih s transferima kriptovaluta, što se ističe kao jedna od značajnijih prednosti takvih transakcijskih sustava. Također, primjena regulative na nacionalnoj razini predstavlja rizik u smislu zaštite investitora/potrošača, integriteta tržišta i konkurencije, jer se provodi na lokalnoj (nacionalnoj) razini, odnosno predstavlja različite uvjete na jedinstvenom tržištu. Drugim riječima, regulacija tržišta kriptovaluta u državama članicama na nacionalnoj razini, ne otklanja rizik s kojim su suočeni potrošači, investitori i sudionici na tržištu u drugim državama članicama te oni ostaju nezaštićeni od nekih najznačajnijih rizika koji proizlaze iz kriptovaluta. S druge strane, blockchain i tržište blockchain imovine se kontinuirano razvija i privlači sve više korisnika zbog čega se još više javlja potreba za jednoznačnom regulacijom na području EU-a s ciljem definiranja rizika i izbjegavanja podređenog položaja korisnika, te široj korporativnoj primjeni tehnologije distribuiranog zapisa.

j) Prevelika ushićenost oko nove tehnologije (engl. *hype*) – digitalizacija i decentralizacija (tokenizacija) bilo koje realne i financijske imovine ili vlasništva, i osiguranje tokenizirane imovine preko kriptografskih primitiva, zasigurno zvuči revolucionarno. Nova tehnologija privlači i utječe na svakodnevni razvoj različitih startupova preko kojih se obećava praktična implementacija tehnologije distribuiranog zapisa isključujući niz tehnoloških nedostataka i rizika postojeće tehnologije, odnosno unapređujući istu. Međutim, kao što je prethodno navedeno, realna interpretacija stvarnih i objektivnih mogućnosti obećavanih projekata, proizlazi iz adekvatnog razumijevanja nove tehnologije, što u slučaju blockchaina i kriptovaluta najčešće nije slučaj. Upravo zbog odsutnosti razumijevanja i objektivnog vrednovanja mogućnosti blockchain tehnologije, često dolazi do iracionalnih očekivanja i pretjerivanja, kao što je to bio slučaj i devedesetih i „DotCom“ balona, odnosno precjenjivanja vrijednosti dionica starupova povezanih s razvojem interneta. Iako je ineternet je nedvojbeno utjecao na svakodnevno poslovanje, većina startupova tog vremena danas niti ne postoji. Gates (2017) navodi kako vremensko razdoblje od razvoja do implementacije tehnologije značajno varira ali i da je značajno podcijenjeno. Drugim riječima, potrebno je puno više vremena od ideje do implementacije u širu svakodnevnu primjenu, nego što je to prezentirano javnosti. Dokaz tome su već prethodni pokušaji

digitalnih valuta baziranih na kriptografiji, poput DigiCash, HashCash itd. Blockchain je samo novi način pohranjivanja i upravljanja s podacima i ne predstavlja odgovor na sve svjetske probleme (Gates, 2017). Međutim, imajući u vidu tendenciju digitalizacije svakodnevnog poslovanja različitih djelatnosti, važnost upravljanja podacima na decentraliziran način sve više dolazi do izražaja, i vjerojatno će tek budućnost pokazati veličinu blockchaina kao nove tehnologije.

6.9. Vrste blockchain arhitekture

Osnovna karakteristika Bitcoin blockchain transakcijske mreže je decentralizacija upravljanja, odnosno distribucija pohranjenog zapisa na siguran i samoodrživ način što se ističe kao prednost u odnosu na tradicionalne transakcijske sustave. Međutim, takva prednost proizlazi iz transparentnog, javno dostupnog protokola što se, u određenom korporativnom okruženju ili okruženju specifičnom prema potrebama korisnika, može smatrati nedostatkom. Na primjer, korporacija ne želi podatak o narudžbi ili prodaji učiniti javnim podatkom. Jednako tako, korisnici moraju imati povjerenje u tehnološku infrastrukturu i anonimne entitete iza čvorova mreže. Zbog reputacijskog rizika, korporativno okruženje zasigurno ne želi koristiti javni blockchain, ukoliko se dovodi u vezu s različitim ilegalnim aktivnostima. Upravo ovo posljednje je potaknulo razvoj novih blockchain oblika koji koriste tehnologiju distribuiranog zapisa (engl. *distributed ledger technology* - DLT) i sve prednosti blockchain tehnologije. U tom slučaju, privatne kompanije, organizacije ili udruženja razvojnih programera razvijaju prilagođeni blockchain na sustavima otvorenog programskog koda i ne žele u potpunosti koristiti usluge i mogućnosti javnog blockchaina.



Shema 12. Vrste blockchain arhitekture

Izvor: Izrada autora

Zbog komercijalne potrebe krajnjih korisnika, nastale su različite blockchain arhitekture prilagođene njihovim specifičnim potrebama, pa se blockchain sustavi mogu podijeliti u četiri osnovna tipa arhitekture, sukladno Shemi 12.:

a) Javni blockchain;
b) Privatni blockchain;
c) Hibridni blockchain;
d) Konzorciji blockchain.

Tablica 3. usporedno prikazuje osnovne karakteristike različitih tipova blockchain arhitekture. Javni blockchain je nastao s pojavom Bitcoin transakcijske mreže i predstavlja arhitekturu gdje su sve aktivnosti na matičnom blockchainu transparentne i javno vidljive. U usporedbi s drugim tipovima, javni blockchain je potpuno decentraliziran i bilo tko bez dozvole može pristupiti mreži u svojstvu čvora i doprinijeti postizanju konsenzusa. Takve karakteristike doprinose decentralizaciji čineći javni blockchain više robusnim i sigurnim, ali manje učinkovitim u usporedbi s drugom arhitekturom. S druge strane, privatni blockchain predstavlja arhitekturu tehnologije distribuiranog zapisa kreiranu samo za potrebe jedne organizacije. Glavna razlika između javnog i privatnog blockchaina je u tome što se u javnom isključuje centralno tijelo kao kontrolni entitet, dok privatni organizira i upravlja tvrtka za čije se potrebe koristi. Zbog toga, samo poznatim entitetima se dozvoljava pristup u funkciji čvora mreže. U kontekstu sigurnosti, privatni blockchain je ograničen na

čvorove unutar organizacije pa je zbog toga daleko manje siguran, a samim tim se i konsenzus donosi na razini organizacije čime se doprinosi njihovoj brzini obrade podataka. Internacionalne kompanije svakako mogu imati koristi od tehnologije distribuiranog zapisa poput, banaka, drugih financijskih institucija ili nekih drugih tipova organizacija, poput trgovačkih lanaca. U tom slučaju svaka podružnica bi mogla predstavljati jedan čvor u mreži, neovisno o zemljopisnoj lokaciji, veličini itd. Hibridni oblik blockchaina predstavlja kombinirani oblik javnog i privatnog blockchaina. Kao odgovor na izazov korporativne primjene, razvojni programeri sve više prilagođavaju javni blockchain kako bi njegove mogućnosti zadovoljile specifične korporativne potrebe i zahtjeve. Primjeri prilagodbe javnog blockchaina korporativnim potrebama su XinFin[63], Enterprise Ethereum Alliance[64] itd., hibridni oblici blockchaina koji su više fleksibilni u kontekstu krajnjih potreba. Zbog svojih mogućnosti, više različitih organizacija mogu koristiti prednosti javnog blockchaina, ali na prilagođen način, odnosno samo za one podatke koji se žele podijeliti, decentralizirati i distribuirati mrežom. Zbog toga, hibridni oblici blockchaina su više decentralizirani i sigurni u odnosni na privatni blockchain, jer uključuju više selektivnih, ali nevezanih čvorova različitih organizacija koji pružaju potporu sigurnosti mreže. Zadnji oblik, konzorcij blockchain predstavlja arhitekturu tehnologije distribuiranog zapisa kreiranu samo za potrebe više organizacija. Za razliku od hibridnog oblika, koji uključuje javni blockchain na prilagođen način, konzorcij arhitektura ne koristi prednosti javnog blockchaina, nego se oslanja na samostalan razvoj tehnologije, koja čak niti ne uključuje kriptovalute. U javnom i hibridnom obliku blockchaina kriptovalute su neophodne da bi pružale poticaj u obliku naknada čvorovima mreže u funkciji sigurnosti sustava.

Konzorciji izuzimaju kriptovalute iz sistema jer smatraju da nisu potrebne za osiguranje sustava između korporacija s istim interesom. Zbog svoje primarne reputacije, niti jednoj korporaciji nije u interesu da svojim aktivnostima prouzroče neki oblik nepovjerenja u implementiranu tehnologiju, čime zapravo takvi sustavi postaju neovisni i samoodrživi. Svatko u funkciji čvora u mreži, imat će ulogu u konsenzusu u najboljoj namjeri. Linux fondacija 2015. godine je kreirala je Hyperledger Project[65] za

[63] https://xinfin.org/
[64] https://entethalliance.org/
[65] https://www.hyperledger.org/use/distributed-ledgers

razvoj tehnologije distribuiranog zapisa u obliku konzorcij blockchain ekosustava otvorenog programskog koda. Linux fondacija je željela stvoriti okruženje u kojem se zajednice proizvođača softvera i kompanija sastaju i koordiniraju kako bi izgradili blockchain okvire.

Tablica 3. Usporedba karakteristika blockchain arhitekture

Karakteristike	Javni blockchain	Privatni blockchain	Hibridni blockchain	Konzorcij blockchain
Tip mreže	Decentraliziran	Centraliziran	Djelomično decentraliziran	Djelomično decentraliziran
Pristup mreži	Bilo tko	Jedna organizacija	Više odabranih organizacija	Više odabranih organizacija
Sudionici mreže čvorova (nodovi)	Bez dozvole (*permissionless*) Identitet nepoznat	S dozvolom (*permissioned*) Identitet poznat	Bez dozvole/ s dozvolom (*permissioned/permissionless*) Identitet poznat/nepoznat	S dozvolom (*permissioned*) Identitet poznat
Sigurnost mreže	Visoka/konsenzus mehanizam PoW/PoS	Niska/mreža ograničena na čvorove (nodove) unutar organizacije	Visoka/više čvorova (nodova) različitih organizacija	Visoka/više čvorova (nodova) različitih organizacija
Postizanje konsenzusa	Svi rudari (nodovi) u mreži	Unutar organizacije	Odabrani skup čvorova (nodova) u mreži	Odabrani skup čvorova (nodova) u mreži
Učinkovitost/ brzina transakcija	Niska	Visoka	Visoka	Visoka

Izvor: Izrada autora

Sam Hyperledger Project ne predstavlja infrastrukturu za druge kriptovalute, već otvoreni centar za blockchain projekte poduzetničkih razreda kako bi se inkubirali i sazrijevali kroz sve faze razvoja i komercijalizacije (Dhillon et al., 2017). Bashir (2017) navodi da Hyperledger zapravo niti nije blockchain, te ističe da je napor njegovih članova u smjeru izgradnje okvira otvorenog programskog koda tehnologije

distribuiranog zapisa, koji se može koristiti za razvoj i primjenu blockchain aplikacija i sustava između različitih industrija, pri čemu je ključni fokus izgradnja i pokretanje platformi koje podržavaju globalne poslovne transakcije. U odnosu na javni blockchain, konzorciji arhitektura pruža djelomičnu decentralizaciju transakcijskog sustava kroz kontroliran pristup više čvorova različitih organizacija u funkciji pružanja sigurnosti mreže. Više čvorova različitih organizacija pruža i veću decentralizaciju, odnosno sigurnost mreže u odnosu na privatni blockchain. S obzirom da se konzorcij arhitektura više fokusira na poboljšanje, pouzdanosti i performanse blockchain sustava, manji broj čvorova s dopuštenjem doprinosi performansama sustava čineći ga više učinkovitim u odnosu na javni blockchain, gdje se broj čvorova izražava u tisućama.

7. PRAKTIČNE IMPLIKACIJE BLOCKCHAIN TEHNOLOGIJE

Blockchain pruža svojstvo decentralizirane pohrane digitalnih podataka preko javne glavne knjige distribuirane kroz više umreženih baza podataka, odnosno čvorova u mreži. Prvi blockchain je predstavljen preko Bitcoin transakcijskog protokola koji je implementirao PoW konsenzus algoritam, odnosno proceduru koja osigurava jednu verziju istine među distribuiranim podacima. Iako je prvotna namjera bila konstrukcija transakcijskog sustava jedinica bitcoin valute isključivanjem posrednika u transakciji, vrlo brzo je prepoznato da vrijednost vezana za javni, odnosno privatni ključ, ne mora biti isključivo samo jedinica valute, te da implementirana tehnologija pruža i druge mogućnosti preuzimanjem svih prednosti inicijalnog Bitcoin blockchaina. Međutim, takva primjena zahtijevala je i određene preinake u mogućnostima prvog oblika blockchaina, što je razlog nastanka decentraliziranih kompjuterskih platformi poput Ethereuma, više fleksibilnih i učinkovitih konsenzus algoritama i novih blockchain arhitektura. Postoje različiti pristupi kojim se utvrđuje postoji li uopće potreba za implementacijom blockchain tehnologije. Međutim, razmatrajući osnovni pristup efikasnosti i sigurnosti, gdje god je prisutno nepovjerenje između dvije strane u poslu, odnosno nužnost za istinito i/ili transparentno iskazivanje podataka na siguran način, može se implementirati tehnologija distribuiranog zapisa, s ciljem izuzimanja potrebe za trećom stranom kao kontrolnim tijelom, što dovodi do povećanja sigurnosti, učinkovitosti i smanjenja troškova. Navedena definicija pokriva širok spektar djelatnosti moguće primjene blockchain tehnologije, a u nastavku se razmatra njena osnovna primjena u okviru poslova računovodstva i financija.

7.1. Primjena blockchain tehnologije u računovodstvu

Digitalizacija računovodstvenih sustava, promatrajući s makro aspekta, još uvijek je u povojima u usporedi s drugim industrijama. Razlozi tome se mogu naći u izuzetno visokim regulatornim zahtjevima u pogledu valjanosti i cjelovitosti računovodstvenih procesa, odnosno računovodstvene evidencije. Računovodstveni sustavi moraju biti kreirani tako da je krivotvorenje nemoguće, ili barem vrlo skupo. Da bi se to postiglo, sustav se oslanja na mehanizme uzajamne kontrole, provjere i ravnoteže, što neizbježno utječe na svakodnevne aktivnosti. Pored toga, nužnost objektivnosti i istinitosti računovodstvenih zapisa uključuje dodatne napore, opsežnu dokumentaciju

i periodične kontrole od strane trećih tijela. Većina tih aktivnosti su radno intenzivni zadaci i daleko od toga da su potpuno digitalizirani, odnosno automatizirani (Deloitte, 2016).

Suvremeno financijsko računovodstvo se temelji na sustavu dvojnog unosa i revolucioniralo je dotadašnji oblik evidencije poslovnih promjena. Međutim, da bi se postiglo istinito i objektivno evidentiranje poslovnih promjena, te steklo povjerenje treće strane (države) u objektivnost financijskih izvještaja, neovisni javni revizori također provode provjeru financijskih podataka nastalih poslovnih događaja. Javna revizija, osim što za zaposlenike tvrtke nad kojom se provodi predstavlja dodatne aktivnosti u smislu prikupljanja tražene dokumentacije i izvještaja, dodatnih sastanaka itd., predstavlja i dodatni trošak u smislu utrošenog vremena, ali i u kontekstu komercijalne obveze prema revizorskoj kući koja istu provodi. Jednako kao što je koncept dvojnog knjigovodstva revolucionarno promijenio način na koji se evidentiraju poslovne promjene, tako i tehnologija distribuiranog zapisa ima potencijala da zauvijek promjeni procese financijskog knjigovodstva. S obzirom na svoje osnovne počelo izuzimanja potrebe za trećom stranom u funkciji kontrole, te u kontekstu računovodstvenih i financijskih poslova i aktivnosti koje se svakodnevno provode, tehnologija distribuiranog zapisa ima široku potencijalnu primjenu pojednostavljujući regulatorne zahtjeve i unapređujući dvostruko knjigovodstvo. Umjesto vođenja zasebnih knjigovodstvenih evidencija, tvrtke mogu svoje poslovne promjene evidentirati izravno u zajedničku distribuiranu javnu knjigu, stvarajući međusobni sustav trajnih, sigurnih i objektivnih računovodstvenih evidencija. Budući da bi sve knjigovodstvene evidencije bile osigurane kriptografijom u smislu decentralizirane naravi, njihovo krivotvorenje ili uništavanje kako bi se prikrile određene aktivnosti bi bile praktički neizvedive. Implementacija blockchain tehnologije u korporativno okruženje u okviru financijskog računovodstva, tvrtkama bi doprinijelo na više načina. Blockchain bi pružio višu standardizaciju koja bi revizorima omogućila bržu i efikasniju provjeru analitičkih podataka iz kojih se generiraju sublimirani financijski izvještaji. Jednako tako, troškovi i vrijeme potrebni za provođenje vanjske revizije bi se također znatno smanjili, a revizija bi se mogla usmjeriti na područja kojima mogu više doprinijeti svojom savjetodavnom ulogom, kao što su složenije transakcije, mehanizmi unutarnje kontrole, itd (Deloitte, 2016).

Blockchain tehnologija se može implementirati postupno, odnosno nije nužno da se u početku sve poslovne transakcije evidentiraju na javnu knjigu, što pruža svojstvo selektivnosti, ali i fleksibilnosti. Blockchain kao izvor povjerenja također može biti od velike pomoći u današnjem računovodstvu. Postupnom implementacijom se može integrirati u aktivnosti povezane s računovodstvenim postupcima, počevši od osiguranja integriteta evidencija do sljedivih revizijskih aktivnosti što bi dovelo do potpune automatizirane revizije. Za račune u fizičkom obliku, rizik od naknadne preinake podataka se smatra relativno niskim. S druge strane, elektroničke datoteke su podložne naknadnim izmjenama, te su stoga više ranjive, što za posljedicu ima uvođenje novih preventivnih mjera u slučaju digitalizacije papirnatih zapisa. Rezultat je širok raspon organizacijskih, tehnoloških i procesnih odredbi. Sve preventivne mjere moraju biti dokumentirane na definiran način za treće strane, zbog toga ne iznenađuje što mnoge tvrtke zaziru od uvođenja holističkog elektroničkog sustava arhiviranja, iako su svjesne njegove prednosti (Deloitte, 2016).

Primjena blockchaina u računovodstvu omogućavala bi laku provjeru i dokazivanje cjelovitosti elektroničkih datoteka provjerom pripadnosti datoteka Merkle korijenu stabla, kako je to opisano na Shemi 6. u poglavlju 6.1. Funkcija sažimanja. Svaka datoteka, u računovodstvenom smislu poslovna promjena, bila bi zapisana kao rezultat funkcije sažimanja, i kao takva pridružena svom paru drugog elektroničkog zapisa rezultata funkcije sažimanja u daljnjem procesu sažimanja, čime bi naknadna verifikacija poslovnih promjena bila lako provediva. Važno istaknuti da bi javna knjiga digitalnih zapisa bila distribuirana širom javne, ili neke druge, mreže, ovisno o odabiru blockchain infrastrukture. Podaci o poslovnim promjenama zapisani u obliku bloka podataka, odnosno kao rezultat funkcije sažimanja, u bilo kojem sljedećem trenutku se mogu po zahtjevu verificirati čime bi se dokazao njihov digitalni integritet. U slučaju da se naknadnom provjerom ne dobije rezultat funkcije sažimanja jednak onom zapisanom na blockchainu, došli je do promjene podataka, odnosno zapisa o poslovnim promjenama na npr. kontu obveze za PDV. Jednako tako, provjera vremenske oznake (engl. *timestamp*) na blockchainu pruža vremensku komponentu kreiranja dokumenta, što dodatno isključuje rizik naknadne promjene dokumenta tijekom vremena potrebnog za njegovo digitalno čuvanje. Osim osnovnih podataka o poslovnim promjenama, implementacija blockchain tehnologije može doprinijeti i poslovnim procesima prije evidencije poslovne promjene, kao konačne

računovodstvene aktivnosti. Svi interni poslovni procesi u velikim kompanijama, koji obuhvaćaju više odjela ili tvrtki kćeri, postaju lako sljedivi. Također, implementacijom blockchain tehnologije koja podržava pametne ugovore, procesi financija i platnog prometa se također mogu automatizirati, pa samim time i procesi knjiženja poslovnih promjena. Na primjer, automatizirano plaćanje fakture po isporuci robe ili usluga i zadovoljavanju specifikacija iz ugovora, uz uvjet pozitivnog salda na bankovnom računu. Iako i danas postoji tehnologija koja kroz konzorcije omogućava slične aktivnosti, tehnologija distribuiranog zapisa to čini na način koji isključuje potrebu za povjerenjem (engl. *trustless*) u drugu ili treću stranu.

Neposredan utjecaj blockchain tehnologije na računovodstvene procese se može razmotriti kroz nekoliko sljedećih točki:

a) Izuzimanje revizije. Budući da su svi unosi u blockchainu distribuirani i osigurani preko kriptografskih primitiva, gotovo je nemoguće uništiti ili manipulirati informacijama, sprječavajući bilo koji oblik financijskih prijevara, izmjena podataka i slično. U takvom poslovnom okruženju, godišnja revizija gotovo da i nema svoju svrhu u obliku kakvom je imala do sada, jer su sve poslovne promjene digitalno zapisane u lanac blokova koji je distribuiran širom transakcijske mreže. Blockchain infrastruktura može pružiti uvid u računovodstvenu evidenciju poslovnih događaja u bilo kojem trenutku, ne samo tijekom godišnje redovne ili izvanredne revizije. S druge strane, to implicira da će revizori, osim većeg fokusa na sustave upravljanja i kontrola, morati biti više educirani u području sustava tehnologije distribuiranog zapisa nad kojima će provoditi provjeru sigurnosti i integriteta podataka, te provjeru ispravnosti aplikacija.
b) Pametni ugovori. Implementacijom pametnih ugovora preko decentraliziranih kompjutorskih platformi, postavljaju se ugovorni uvjeti koje je potrebno ispuniti kako bi se transakcije iz sporazuma uopće provele. Pametni ugovori imaju mogućnost zadržavanja sredstava te automatiziranog otpuštanja istih po ispunjavanju ugovornih uvjeta. S obzirom na takve mogućnosti, blockchain tehnologija ima potencijala zauvijek promijeniti način funkcioniranja uobičajenih računovodstvenih aktivnosti implementacijom uvjetovanih transakcija, pa tako i knjiženja, te ukidanjem trenutno nužnih trećih strana, poput pravnika.

c) Uključivanje treće strane. Bitcoin blockchain je inicijalno zamišljen s ciljem izuzimanja nužnosti treće strane prilikom transakcija. Međutim, u kontekstu transfera računovodstvenih aktivnosti na blockchain tehnologiju, implementacija blockchaina zapravo uvjetuje uključivanje treće strane koja prije nije bila potrebna, u ovom slučaju blockchain transakcijskog sustava. Slijedom toga, može se reći da dvostruko knjigovodstvo zapravo prelazi u trostruko decentralizirano knjigovodstvo.

Najbolji primjer smjera i dinamike praktične implementacije blockchain tehnologije se može uočiti na primjeru SAP[66] inovacijskog centra koji trenutno broji 41 projekt vezan za računovodstvo, financije i općenito razmatranje korisnosti primjene blockchain tehnologije u poslovnim procesima korporativnog, ali i drugog okruženja[67]. Od ukupno 41 projekt, 11 projekata je već pušteno u produkciju, za 16 projekata je dokazan koncept praktičnosti (engl. *proof of concept* – POC), a 14 projekata se nalazi u idejnoj fazi razrade. Osam produkcijskih projekata predstavljaju neki oblik implementacije blockchaina u domenu upravljanja opskrbnim lancem (engl. *supply chain management*). S obzirom da opskrbni lanci, između ostalog, uključuju razmjenu faktura između kupaca i dobavljača, očekivani slijed razvoja je integracija računovodstvenih aktivnosti sa aktivnostima opskrbnih lanaca, preko implementacije blockchaina. Unutar koncepata za koje dokazana praktičnost, posebno se ističe projekt koji ima za cilj povećanje efikasnosti procesa operacija zajedničkog ulaganja u naftu i plin[68]. Naime, kapitalno zahtjevna istraživanja naftne i plinske industrije često zahtijeva zajednički napor više kompanija za bušenje i proizvodnju nafte, što uključuje obradu i praćenje zajedničkih knjigovodstvenih knjiga. Takav pristup povećava opće troškove projekta, što dodatno povećava cijenu neiskorištenosti potrebnu za profitabilno poslovanje zajedničkog ulaganja. Trenutno, partneri iz zajedničkih ulaganja se oslanjaju na pojedinačne, odnosno zasebne knjigovodstvene sustave kako bi bilježili poslovne događaje i povezane troškove zajedničkog ulaganja koji se moraju alocirati prema organizacijskom nositelju troškova između partnera. Takvo poslovanje dovodi do situacije u kojoj mogu nastati značajne razlike evidencije troškova između kompanija, a to opet zahtijeva dodatnu reviziju s ciljem njihovog

[66] SAP je korporacija koja predstavlja jedan od vodećih svjetskih proizvođača softvera za upravljanje poslovnim procesima.
[67] https://innovation-guide.sap.com/?technologies=Blockchain
[68] https://innovation-guide.sap.com/joint-venture-accounting

usklađenja. Kako bi unaprijedili svoje operativno poslovanje i sigurnu razmjenu istinitih knjigovodstvenih podataka, razvili su računovodstveno rješenje temeljeno na blockchainu za zajednička ulaganja (engl. *joint venture accounting* - JVA) koje pruža jedinstven izvor istinitih podataka svim dionicima projekta, ali i financijskim institucijama koje financiraju projekt. Njihovo rješenje je osmišljeno kako bi pomoglo u praćenju računa, plaćanja, upita, odobrenja proračuna i odluka. Blockchain služi kao zajednička i transparentna javna glavna knjiga i pojednostavljuje proces zajedničke revizije poslovnih događaja vezanih za projekt. Njihova blockchain infrastruktura je osmišljena na način da sudionicima pruža distribuiranu bazu podataka koja se može koristiti za učinkovitu razmjenu informacija bez potrebe da središnja druga strana bilježi transakcije u njihovo ime. Aplikativno rješenje zasnovano na SAP oblak platformi (engl. SAP *cloud*) podrazumijeva uslugu računovodstva te uključuje tri osnovna opsega poslovnih procesa:

a) generiranje, distribucija i prihvaćanje zajedničkog obračuna kamata;
b) praćenje plaćanja;
c) digitalno odobrenje za praćenje suglasnosti za troškove.

Rješenje računovodstvenog sustava temeljenog na blockchain infrastrukturi podrazumijeva kreiranje mreže korisnika koja omogućava svim korisnicima i uključenim kompanijama da postanu članovi na blockchain platformi, što predstavlja prethodno opisanu konzorcij blockchain arhitekturu. Na kraju, u konačnoj verziji, financijske institucije bi bile uključene u proces namirivanja transakcija te bi pružale sudionicima mreže transparentan status obrade plaćanja.

7.2. Primjena blockchain tehnologije u financijama

Razmatranje praktične primjena blockchain tehnologije u okviru aktivnosti koji uključuju poslove financija, potrebno je razmatrati kroz dva vremenska okvira: vrijeme prije pojave FinTech-a i blockchaina i vrijeme nakon njihovog razvoja. Prije puštanja u javnost prvog Bitcoin transakcijskog sustava, transfer sredstava putem tradicionalnog financijskog sustava je bio opterećen dužim vremenskim periodom kada je u pitanju provjera valjanosti transakcije. Pored toga, za svaku transakciju, financijske institucije obračunavaju i naplaćuju naknadu za transfer sredstava između korisnika, jer djeluju kao posrednici. Međutim, predstavljanjem novih konkurentnih

tehnoloških rješenja na FinTech području, a pogotovo s razvojem blockchain transakcijskih sustava, nastala je nova era digitalizacije koja, na neki način, prisiljava dotadašnji tromi financijski sustav na nužne promjene, a sve s ciljem očuvanja broja korisnika svojih usluga. Upravo zbog relativno novih *peer-to-peer* aplikativnih rješenja koja nude kreiranje dužničko vjerovničkog odnosa između interesnih strana bez centralnog entiteta kao posrednika u usluzi, grupnog financiranja (engl. *crowdfunding*), ali i rješenja za brz transfer sredstava i plaćanja putem mobilnih aplikacija, razvojni programeri Fintech područja prisiljavaju financijske institucije da evoluiraju u smjeru koji više odgovara potrebama korisnika, nego što je to bilo ranije.

Promatrajući s aspekta slobodnog kapitala za velike kapitalne projekte, FinTech sektor još uvijek ne može ispuniti njihove potrebe za kapitalom. Tradicionalne financijske institucije će zasigurno još neko vrijeme dominirati u sektoru financijskih usluga. Jednako tako, niti startupi zasnovani na blockchain infrastrukturi čija je djelatnost pružanje usluga prijenosa kapitala u funkciji kreditiranja, nemaju za sada toliko duboku bazu korisnika koji bi posrednim putem kreditirali velike projekte. S druge strane, kroz određeno vrijeme i edukacijom, svakodnevni korisnici tradicionalnih financijskih usluga, bi mogli uvidjeti praktične prednosti različitih FinTech rješenja u području financiranja, odnosno transfera sredstava. Zbog toga, određene tradicionalne financijske institucije su prepoznale koristi koje pruža nova tehnologija, te spajaju tradicionalno s modernim, a tome svjedoče nova aplikativna rješenja kao što je George aplikacija za mobilno i internetsko bankarstvo[69], kojom se pruža usluga otvaranja računa ili aplikacije za kredit bez potrebe za dolaskom u poslovnicu, personalizirani pregled osobnih financija i potrošnje, kao i naprednu tražilicu. Jednako tako, prema pisanju Hrvatske narodne banke (HNB)[70], odnosno Financijske agencije (FINA)[71], FINA je razvila je novi instant platni sustav NKSInst koji omogućava prijenos novčanih sredstava s jednog računa za plaćanje na drugi u roku od svega nekoliko sekundi s trenutnom dostupnošću sredstava primatelju plaćanja 24/7, 365 dana u godini.

[69] https://www.poslovni.hr/trzista/george-mijenja-postojece-aplikacije-erstea-4253123
[70] https://www.hnb.hr/-/obavijest-o-pocetku-rada-nksinst-platnog-sustava
[71] https://www.fina.hr/-/financijska-agencija-dobila-odobrenje-za-rad-novog-platnog-sustava-nksinst

Upravo zbog prilagodbe sve naprednijim tehnološkim rješenjima, ali i svojevrsnom pritisku koji dolazi od strane blockchain infrastrukture koja je pruža daleko više kao transakcijski sustav, Nacionalni klirinški sustav je morao provesti brzu prilagodbu kako bi pružio infrastrukturu mogućnostima novih aplikacija. S druge strane, prema pisanju HNB-a, sudionici u NKSInst platnom sustavu i dalje mogu biti samo banke, i to na načelu dobrovoljnosti. Također se navodi da banke u skladu sa svojom poslovnom odlukom samostalno definiraju dinamiku kojom će pojedinim kategorijama klijenata (potrošači, poslovni subjekti) omogućiti izvršenje instant plaćanja kao i kanale plaćanja (internet, mobilno bankarstvo, mobilne aplikacije) kojima se klijenti mogu koristiti u svrhu izvršenja instant plaćanja. Drugim riječima, sva plaćanja će se i dalje provoditi preko banaka za određenu naknadu, i to samo onih koju prihvate NKSInst platni sustav i njihovim odobrenim klijentima unutar HR, što još uvijek nije na razini transfera od jedne milijarde dolara za naknadu u visini od pet dolara na Bitcoin transakcijskom sustavu, koja je isto tako mogla biti i međunarodna, ali svakako predstavlja tehnološki pomak naprijed i prilagodbu FinTech rješenjima poslovnih modela.

7.2.1. Decentralizirane financije - DeFi

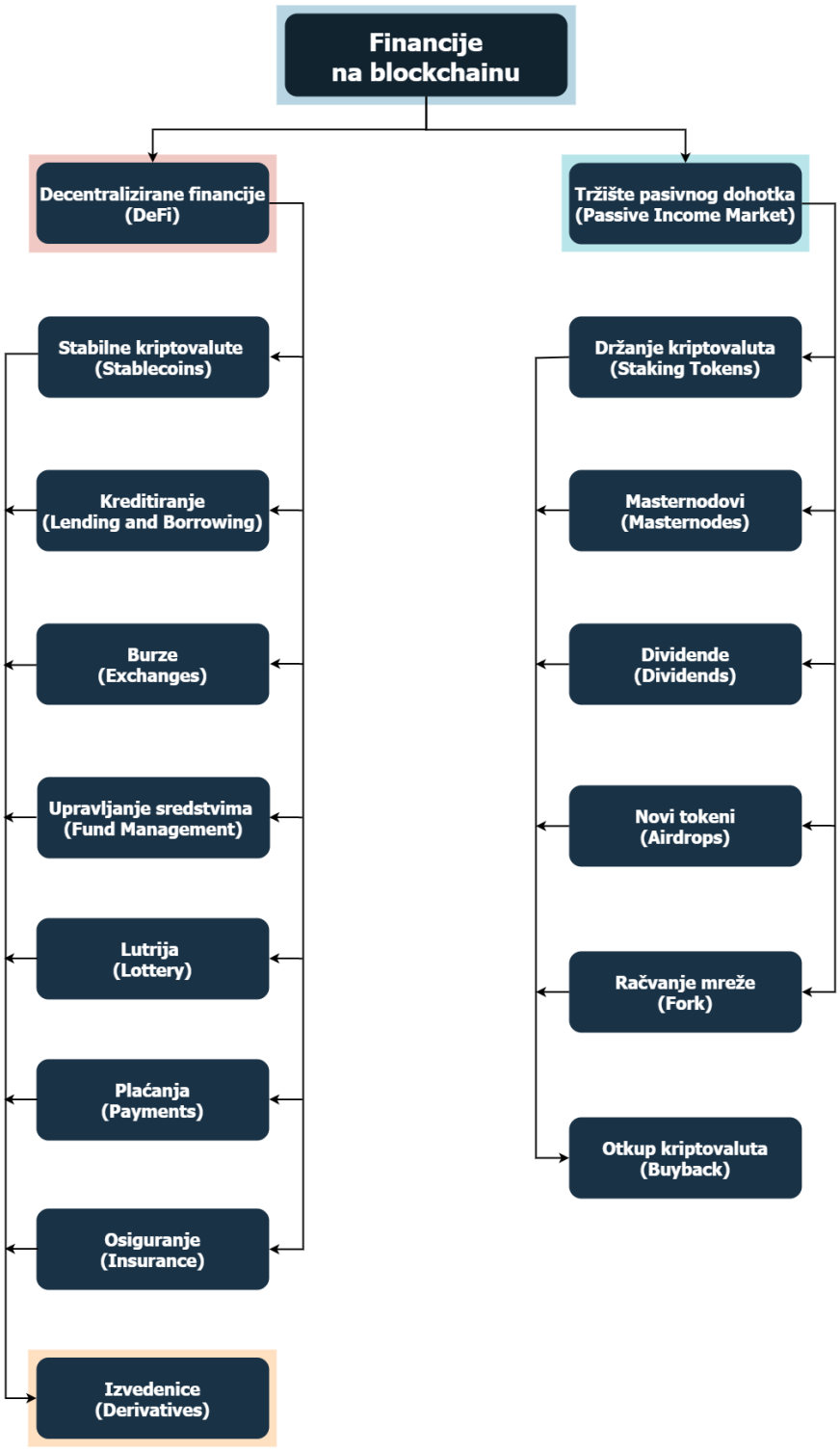
Decentralizirane financije (engl. *decentralized finance* – DeFi) predstavljaju ekosustav decentraliziranih aplikacija (engl. *decentralized applications* – DAPPS) koje pružaju različite financijske usluge i mogućnosti kroz primjenu blockchain tehnologije kao temeljne infrastrukture za njihovo operativno poslovanje. U svojoj osnovi, decentralizirane financije pružaju tri mogućnosti svojim korisnicima: pozajmljivanje, kreditiranje i trgovinu s financijskom imovinom kreiranom na blockchainu. S obzirom da se temelje na blockchain tehnologiji, usluge koje DAPPS pružaju se provode kroz *peer-to-peer* način obrade i transmisije podataka, bez centralnog entiteta kao kontrolnog tijela. Decentralizirane financije ne počivaju samo ne jednom proizvodu ili kompaniji, već predstavljaju skup proizvoda i usluga koje se tretiraju kao zamjena za institucije u rasponu djelatnosti od bankarstva, osiguranja, dužničkog i novčanog tržišta (Lau, Lau, Jin Teh, Kho, Azmi, Lee i Ong, 2020).

Prema Lau et al. (2020) DeFi čini osam osnovnih kategorija usluga ilustriranih kroz Shemu 13. Međutim, pokraj navedenih kategorija, decentralizirane financije

predstavlja i tržište pasivnog dohotka[72]. U prvu kategoriju pasivnog dohotka ulazi prinos od držanja kriptovaluta (engl. *staking*) što je ustvari pasivni prinos od njihovog rudarenja. Međutim, da bi se ostvario, blockchain mreža mora biti izgrađena na *dokaz o ulogu* konsenzus algoritmu, odnosno imatelj kriptovalute svoj ulog mora držati (zaključati) u odgovarajućem novčaniku koji podržava nagrade koje se distribuiraju u obliku novih jedinica te kriptovalute. Na taj se način osigurava dodatna participacija procesu verifikacije blockchain mreže. Pojedinačni ulog se najčešće pridružuje većim bazenima uloga (engl. *staking pools*) koji predstavljaju čvorove u mreži, gdje se onda zajedno participira u sigurnosti mreže[73].

Masternodovi (engl. *masternodes*) predstavljaju specifičan oblik čvorova u blockchain mreži zaduženi za verifikaciju transakcija. Međutim, osim same verifikacije transakcija, masternodovi pružaju i druge usluge poput instant transakcija, privatnih transakcija, upravljanja mrežom itd. Kako bi bili operativni, masternodovi zahtijevaju minimalan broj jedinica kriptovalute. Na primjer, transakcijski sustav Dash zahtijeva 1.000 jedinica dash kriptovalute, što po trenutnoj cijeni od 71,90 dolara po jedinici, rezultira iznosom od 71.900 dolara potrebnim da bi se pokrenuo Dash masternode. S druge strane, vlasnici kriptovalute mogu svojim udjelom participirati u mreži preko masternoda, a zauzvrat dobivaju dio novokreiranih jedinica valute, što se može smatrati pasivnim dohotkom. Blockchain transakcijski sustavi koji koriste masternodove su Dash, Stratis, Zcoin, PIVX itd[74].

[72] *yield farming* je postao uobičajeni termin u ekosustavu kriptovaluta koji okrupnjava različite aktivnosti s ciljem ostvarivanja pasivnih prihoda.
[73] Visinu nagrade za participaciju u sigurnosti blockchain mreže pojedine kriptovalute se može pratiti na stranici https://www.stakingrewards.com/
[74] Kriptovalute koje koriste masternodove se mogu pratiti na stranici https://masternodes.online/



Shema 13. DeFi tržište i tržište pasivnog dohotka

Izvor: Izrada autora

Pasivni dohodak također predstavljaju i svojevrsne dividende koje najčešće isplaćuju burze kriptovaluta vlasnicima kriptovaluta koje su one kreirale i izdale. Jednako kao i

prethodno, da bi se dividenda ostvarila, kriptovalutu je potrebno držati u odgovarajućem novčaniku i određenim uvjetima. Burze kriptovaluta koje isplaćuju dividende su KuCoin, Bibox, BitMax itd.

Nove kriptovalute kreirane kao utilizacijski tokeni na matičnim blockchain ekonomijama i distribuirane bez naknade u obliku *airdrops* se također smatraju pasivnim dohotkom. Novi utilizacijski tokeni mogu biti rezultat grupnog financiranja putem inicijalne ponude, ali mogu biti kreirani i distribuirani postojećim vlasnicima blockchain ekonomija kao što je Ethereum. Jedna od značajnijih takvih distribucija je bila 2017. godine kada se pojedinačno po registraciji distribuiralo tisuću jedinica ontology kriptovalute. Ontology kriptovaluta je poslije postigla cijenu čak od 10,66 dolara, što je vlasnicima koji su participirali u *airdrops*, donijelo pasivni prihod veći od 10 tisuća dolara u nešto malo više od mjesec dana. Trenutna tržišna vrijednost ontology kriptovalute je 0,65 centi[75].

Račvanje transakcijske mreže sa svim prethodno zapisanim transakcijama, drugim riječima dupliciranje mreže i njenih jedinica kriptovalute, također se karakterizira kao pasivni dohodak. U tom slučaju, vlasnik kriptovalute koja prolazi kroz proces račvanja, dobit će broj novih jedinica kriptovalute jednak broju kriptovaluta koje su povezane s javnim ključem inicijalne kriptovalute u trenutku račvanja blockchaina. Naknadni okup kriptovalute (engl. *buyback*) od strane nositelja projekta, ili automatiziranim procesom putem pametnih ugovora, isto se može tretirati kao pasivni dohodak. Kupnja kriptovaluta na točno određeni datum i po strogo definiranim pravilima, te njihovo kasnije uništavanje (engl. *coin burning*) često podiže vrijednost kriptovalute zbog manje količine jedinica u opticaju smanjujući tako ponudu koja utječe na povećanje tržišne cijene. Poznatiji primjer naknadnog otkupa i uništenja provodi Binance burza kriptovaluta koja ima u planu otkupiti i uništiti 50% od ukupnog broja kriptovaluta u opticaju (100 milijuna jedinica). Otkup i uništenje se provodi prema unaprijed definiranom kvartalnom rasporedu. Zadnji je proveden u travnju 2020. godine gdje je otkupljeno i uništeno više od 3 milijuna jedinica BNB kriptovalute, što je u tom trenutku iznosilo 52,5 milijuna u protuvrijednost američkih dolara.

[75] Listu budućih besplatnih distribucija (*airdrops)* je moguće pratiti na stranici https://airdrops.io/

Važnu komponentu u ekosustavu decentraliziranih financija imaju stabilne kriptovalute čija je vrijednost vezana za vrijednost fiat valuta. Prethodno je navedeno da postoji nekoliko vrsta stabilnih kriptovaluta, svaka sa svojim prednostima i nedostacima. Podtip stabilnih kriptovaluta koje su uključene u aktivnosti DeFi područja su kripotvalute izvedene iz drugih kriptovaluta koje služe kao kolateral za njihovo kreiranje. Najpoznatija kolaterizirana stabilna kriptovaluta vezana za vrijednost američkog dolara u omjeru 1:1 je DAI kreirana od strane Maker DAO-a[76] kao kolaterizirana dužnička pozicija (engl. *collateralized debt position* - CDP). Da bi se kreirao 1$ DAI, kroz pametne ugovore je potrebno zaključati protuvrijednost ethereum (ETH), basic attention token (BAT) ili USD Coin (USDC) kriptovalute u minimalnom omjeru od 150%. Drugim riječima, za kreiranje DAI tokena u vrijednosti 1$, potrebno je izdvojiti minimalno 1,5$ ETH ili BAT kriptovalute. Nakon što se kreira DAI, pametni ugovori prate omjer kreiranog i posuđenog DAI tokena i vrijednost zaključanog kolaterala. U situaciji kada vrijednost kolaterala padne ispod 150%, događa se tzv. likvidacija pozicije (engl. *liquidation*) ili na Bitshares DEX platformi koja je preteča današnjeg DeFi ekosustava[77], provodi se maržni poziv (engl *margin call*), sve dok se omjer kolaterala i posuđene pozicije na vrati na visinu od 150%. Za provedenu likvidaciju pozicije na Maker platformi zaračunava se naknada u visini od 13% od kollaterala. Druga po značajnosti DeFi platforma koja pruža mogućnost kreiranja kolaterizirane dužničke pozicije je Compound[78]. U osnovi, Compound pruža istu uslugu kao i Maker platforma i trenutno podržava devet kriptovaluta koje je moguće koristiti kao kolateral za dužničku poziciju, ali i koristiti kao depozit te ostvariti kamate po depozitu, što je puno više od Maker platforme gdje se za kolateral koriste samo tri kriptovalute i kreira samo DAI token.

[76] Maker je decentralizirana autonomna organizacija upravljana DAO modelom, financirana putem javne ponude MKR utilizacijskog tokena na Ethereum blockchainu: https://makerdao.com/en/

[77] Široj popularnosti decentraliziranih financija svakako je doprinijela Maker platforma i njen DAI token. Međutim, manje je poznato, pa čak i na cijelom tržištu i ekosustavu kriptovaluta, da je inicijalni začetnik DeFi okruženja kakvo je prisutno danas upravo Bitshares DEX platforma (tim programera koji stoji iza nje), na kojoj se i danas mogu kreirati kolaterizirani instrumenti čija je vrijednost vezana za fiat valute, plemenite metale ili bilo koju drugu financijsku ili realnu imovinu. Međutim, za razliku od svih današnjih platformi, Bitshares DEX ne zaračunava trošak prilikom kreiranja kolaterizirane imovine. Drugim riječima, korisnik može posuditi sredstva bez troška kamata. Najveća trenutna kolaterizirana pozicija na Bitshares DEX platformi na kreirani i beskamatno posuđeni američki dolar (bitUSD) iznosi 193 tisuće dolara: https://wallet.bitshares.org/#/asset/USD, a 2017. god. je iznosila preko 17 milijuna $.

[78] Compound je protokol novčanog tržišta na Ethereum blockchainu koji pruža mogućnost pozajmljivanja i kreditiranja DeFi korisnika: https://compound.finance/

U kontekstu tradicionalne financijske industrije, decentralizirane financije omogućavaju kreiranje dužničko vjerovničkog odnosa, samo što je druga strana u odnosu ustvari pametni ugovor, odnosno kompjuterski program. Pored toga, tradicionalni financijski sustav većim djelom zahtijeva posrednika koji će realizirati dužničko vjerovnički odnos. U DeFi praksi, posrednik je DeFi platforma sa implementiranim pametnim ugovorima koji na automatizirani način provode proces pozajmljivanja i kreditiranja korisnika. Proces kreiranja DAI tokena zapravo predstavlja pozajmljivanje sredstava na principu zalagaonice, jer se za vrijeme držanja DAI tokena plaća trošak kamata tzv. naknada za stabilnost (engl. *stability fee*) na godišnjoj razini od 8,50%[79]. S druge strane, deponiranjem, odnosno oročavanjem DAI tokena kroz pametne ugovore, može se ostvariti godišnja kamatna stopa DSR (engl. *dai savings rate* - DRS) u visini od 4.11%[80].

Za razliku od Maker platforme, Compound pruža veći izbor kriptovaluta po kojima se može izvoditi dužničko vjerovnički odnos. Compound koristi tzv. bazen likvidnosti u koji s jedne strane korisnici pružaju likvidnost DeFi sustavu oročavanjem svojih kriptovaluta (trenutno devet mogućih), a drugi korisnici te kriptovalute posuđuju preko kolaterizirane dužničke pozicije uz određenu kamatu. Korisnici koji oročavaju kriptovalute zauzvrat dobivaju cTokene čija je vrijednost u početku ekvivalentna vrijednosti oročenih kriptovaluta 1:1. Međutim, prilikom zatvaranja pozicije (otkupa oročenih kriptovaluta), cTokeni imaju višu vrijednost od oročenih kriptovaluta, i to za kamate nakupljene tokom razdoblja držanja cTokena koje se obračunavaju svakih 13 sekundi, što je vrijeme kreiranja jednog bloka transakcija na Ethereum transakcijskoj mreži. S druge strane, korisnici koji žele posuditi kriptovalute, moraju pružiti kolateral u minimalnoj vrijednosti od 150% od željenog iznosa posuđenih sredstava[81]. Prilikom zatvaranja kreditnog odnosa, vraćaju posuđene kriptovalute, otključavaju svoj kolateral te plaćaju kamate za razdoblje u kojem su koristili sredstva[82].

[79] https://mkr.tools/governance/stabilityfee
[80] https://defiprime.com/defi-rates
[81] Kriptovalute koje se posuđuju i koje se drže kao kolateral ne mogu biti jednake.
[82] Lista kriptovaluta koje trenutno podržava Compound platforma se može naći na internet stranici https://compound.finance/markets

Pored primarne svrhe pružanja mogućnosti kreditiranja i oročavanja kriptovaluta, decentralizirane financije čine sustav povezanih decentraliziranih aplikacija, odnosno sustav DEX burzi. Unutar DeFi ekosustava se mogu pronaći dva osnovna tipa DEX burzi: DEX burze sa tradicionalnim oblikom zadavanja naloga za kupnju i prodaju, gdje se nalozi izvršavaju na burzi sukladno ponuđenom i traženom cijenom imovine (engl. *bid – ask price*), ali i hibridni oblik DEX burzi koji eliminira *bid-ask* cijene i temelji se na algoritmu za izračun cijene. U drugom slučaju, kada se želi kupiti kriptovaluta, platforma kreira tu kriptovalutu prema cijeni koja se određuje sukladno zadanoj formuli, odnosno količini koja se želi kupiti. Algoritam za kreiranje je namješten tako da kupnja utječe na rast cijene, a prodaja na pad cijene kriptvalute. Međutim, za razliku od prvog oblika burzi, njihovom kupnjom kriptovalute se kreiraju i puštaju u sustav, a njihovom prodajom platforma otkupljuje jedinice valuta prema cijeni koju je odredio algoritam i uništava ih. Cijeli proces se provodi kroz pametne ugovore čime se pokušava eliminirati problem likvidnosti na DEX tržištima.

Osim same trgovine s kriptovalutama, sustav DEX burzi i DAPPS platformi pruža i druge mogućnosti svojim korisnicima. Jedna od tih mogućnosti je upravljanje sredstvima (engl. *fund management*) automatiziranom trgovinom unaprijed definiranom strategijom, ali i mogućnost repliciranja strategije uspješnih korisnika DEX platformi[83]. Tržište kriptovaluta se još uvijek ne može povezati sa fundamentalnim indikatorima pripadne djelatnosti. Rijetko koji startupi praktično provode svoje projekte u kojima kriptovalute ispunjavaju svoju fundamentalnu svrhu jer je velika većina još uvijek u razvojnoj fazi. Međutim, u okviru decentraliziranih financija, posuđivanje i kreditiranje korisnika se praktično provodi na dnevnoj bazi, čime se, barem za sada, ispunjava DeFi svrha. S obzirom na specifičnu dinamiku tržišta kriptovaluta, koja se očituje naglim i brzim kreiranjem trenda određenog sektora, potencijalni investitori bi trebali imati instrument preko kojeg bi se brzo i efikasno mogli izložiti promjena vrijednosti kriptovaluta iz rastućeg sektora. DeFi platforme su to prepoznale i pružile mogućnost kreiranja indeksa sektora kriptovaluta, kao što je DeFi indeks[84]. Izlaganje promjenama vrijednosti indeksa investitori postižu kupnjom utilizacijskog tokena koji prezentira indeks. U komparaciji sa tradicionalnim tržištem kapitala token je zamjena za dionicu ETF fonda (engl. *exchange traded fund*

[83] https://www.tokensets.com/
[84] https://synthetix.exchange/#/synths/sDEFI

- ETF). Međutim, razlika između standardnog ETF-a i tokena koji predstavlja DeFi sektor je u tome što je rebalans indeksa automatiziran proces dok se ne postignu udjeli prema tržišnoj kapitalizaciji (ukoliko je tako definirano). Razlika je i u fleksibilnosti i pristupačnosti DeFi platformi koje uopće pružaju takve investicijske mogućnosti. Primjer fleksibilnosti je Tokensets platforma koja pruža mogućnost algoritamske trgovine sa cTokenima koji, za vrijeme držanja svoje pozicije u njima, ostvaruju kamate preko Compound platforme. Drugim riječima, DeFi trenutno omogućava oročavanje sredstava po pozitivnim kamatnim stopama te prijenos i trgovinu sa oročenim sredstvima na decentralizirani način putem algoritamskih strategija, zbog često se DeFi ekosustav često naziva novčane lego kockice (engl. *money lego*).

Da bi se privukla likvidnost DeFi okruženja oročavanjem depozita, izuzev visokih kamatnih stopa po depozitu, platforme i alternativnim načinima pokušavaju privući dodatne korisnike. Jedan primjer zanimljivog rješenja su igre na sreću, odnosno PoolTogether[85] lutrija u kojoj se korisnici natječu za nakupljene kamate oročenog DAI tokena. Korisnici na platformi oročavaju svoje DAI token, a obračunate kamatne se transferiraju pobjedniku tog kruga izvlačenja. U okviru decentraliziranih financija, kreiraju se i različita inovativna rješenja za plaćanje po obveznim odnosima, ali u kriptovalutama. Primjeri takvih aplikacija su TrustSwap[86] i Sablier[87]. Preko TrustSwap platforme, moguće je automatizirati pretplatu korisnika, dogovoriti transfer sredstava u budućnosti na točno određeni datum, ugovoriti plaćanje ili korištenje sredstava s odgodom itd. Sablier omogućuje plaćanje i podizanje sredstava u stvarnom vremenu u malim dijelovima između interesnih strana, ukoliko je tako dogovoreno. Na primjer, zaposlenik od poslodavca može zatražiti isplatu plaće u realnom vremenu, odnosno po sekundi kao vremenskoj jedinici, umjesto mjesečne isplate što je današnji standard. U oba slučaja plaćanja se provode na Ethereum transakcijskoj mreži putem pametnih ugovora, čime se izuzima nužnost povjerenja između sudionika u plaćanju po obveznom odnosu (engl. *trustless*). Sredstva koja se nalaze u novčaniku u DeFi okruženju mogu se i osigurati od rizika potencijalne krađe, rizika greške u programskom kodu pametnog ugovora, sigurnosnog propusta koji bi rezultirao

[85] https://www.pooltogether.com/
[86] https://trustswap.org/
[87] https://sablier.finance/

financijskim gubicima itd. Međutim, osiguranje ne pokriva gubitke proizašle gubitkom privatnih ključeva ili sigurnosne propuste CEX burzi. Platforme koje pružaju mogućnost osiguranja kriptovaluta su Nexus Mutual i Opyn[88].

Kolaterizirana dužnička pozicija predstavlja izgradnju imovine kolateralom i čija tržišna vrijednost ovisi o tržišnoj vrijednosti imovine za koju je kreirana imovina vezana. Osnovna definicija, sada već tradicionalnih financijskih izvedenica, poput opcija, terminskih ugovora i zamjena, opisuje izvedenice kao financijske instrumente izvedene iz neke druge temeljne imovine i čija vrijednost, kao i buduća činidba po njima, ovisi o vrijednosti te temeljne imovine. Usporedbom definicija, može se uočiti njihova sličnost. Naime, jedina značajna razlika u strukturi između tradicionalnih financijskih izvedenica i izvedenica kreiranih kao CDP, je u tome što CDP imaju novu građevnu komponentu, a to je kolateral. Vrijednost standardnih izvedenica i izvedenih instrumenata kreiranih kao CDP, kao i buduća činidba s njima, ovisi o vrijednosti neke druge imovine, bilo da se radi o temeljnoj imovini iz koje su izvedene (vezane), ili njihovom kolateralu. Sudionici tržišta kriptovaluta su prepoznali potencijal kreiranja decentraliziranih derivativnih financijskih proizvoda preko CDP-a kako bi investitorima pravovremeno pružili financijske proizvode po njihovoj želji i potrebama. Primjer platforme koja pruža takve mogućnost je Synthetix Exchange[89]. DeFi platforma Synthetix Exchange je burza decentraliziranih derivativnih proizvoda kreiranih kao CDP pri čemu je osnovna komponenta za njihovo kreiranje utlizacijski token platforme synthetix network token (SNX). Osim derivativnih proizvoda čija je vrijednost vezana za kriptovalute kao temeljnu imovinu, platforma pruža i druge proizvode vezane za fiat valute, indekse tradicionalnog tržišta kapitala i realnu imovinu poput zlata, srebra itd., ali i tradicionalnih izvedenica poput opcija.

7.2.2. Prednosti i rizici decentraliziranih financija

Prednost decentraliziranih financija u odnosu na tradicionalni financijski sustav se očituje kroz dostupnost DeFi usluga, posebno prema onima koji trenutno nemaju pristup uslugama tradicionalne financijske industrije. Decentralizirane financije predstavljaju niz povezanih internet platformi koje na decentralizirani način pružaju

[88] Nexus Mutual: https://nexusmutual.io/ Opyn: https://opyn.co/#/
[89] https://synthetix.exchange/#/

mogućnost korištenja financijskih usluga, ali u najboljem interesu korisnika. Prema tome, prednost DeFi-a je i u većoj fleksibilnosti, odnosno bržoj transmisiji podataka, poput visine kamatnih stopa putem decentraliziranih aplikacija, u odnosu na tradicionalni financijski sustav. Na primjer, DeFi platforme omogućavaju korisnicima da putem pametnih ugovora optimiziraju svoju štednju. Drugim riječima, korisnik može odabrati automatiziranu uslugu oročavanja gdje računalni program na dnevnoj bazi prebacuje sredstva korisnika prema platformi koja nudi najbolje kamate. Isto tako, korisnik može odabrati automatizirani proces rebalansa svoje kolaterizirane dužničke pozicije, gdje platforma drži omjer kolaterala i pozajmljenog DAI tokena na željenoj razini, npr. 250%[90]. Povezanost DAPPS i DEX platformi također doprinosi optimizaciji DeFi aktivnosti. Ukoliko neka druga kriptovaluta na alternativnoj platformi pruža bolje kamatne stope na štednju, promjenu valute štednje i kamatnih stopa korisnik može izvršiti preko jedne decentralizirane aplikacije koja služi kao generator protokola, poput 1inch[91]. Također, s obzirom da ne postoji centralni entitet između dvije interesne strane, kao npr. u tradicionalnom dužničko vjerovničkom odnosu, troškovi realizacije takvog odnosa su puno niži. Isto tako, DeFi počiva na blockchain tehnologiji koja kroz distribuiranu bazu eliminira jedinstvenu točku kvara (engl. *single point of failure*). Podaci zabilježeni na blockchain glavnu knjigu se distribuiraju na tisuće čvorova u mreži čime se smanjuje rizik cenzure i ograničenja dostupnosti usluge.

Lau, D. et al. (2020) navodi da u komparaciji s tradicionalnim dužničko vjerovničkim odnosom kojeg provode banke, DeFi praksa također ima određene prednosti. Kao prva prednost se ističe decentralizacija kreditnog odnosa kroz izuzimanje potrebe centralnog entiteta koji će provesti transakciju. Decentralizacija kreditnog odnosa povlači i druge prednosti, kao što su izuzimanje restriktivnog kriterija financiranja, zemljopisnog ili zakonskog ograničenja pristupa financijskim institucijama, neadekvatno visoke kriterije za prihvaćanje zajma i ekskluzivan pristup pojedinaca industriji koja pruža visoke stope prinosa s preuzetim niskom rizikom kroz kreditne odnose dužničko vjerovničke pozicije. DeFi ekosustav isključuje navedena ograničenja primjenom kolaterizirane dužničke pozicije. Drugim riječima, svatko tko

[90] https://defisaver.com/
[91] https://1inch.exchange/#/

ima dio kapitala kojim eliminira kreditni rizik, može aplicirati u kreditni odnos i realizirati zajam za svoje potrebe.

Postoj više kategorija nedostataka, odnosno rizika povezanim s DeFi ekosustavom. Prvi i glavni rizik koji se povezuje sa DeFi ekosustavom je motiv korisnika za korištenjem DeFi platformi. U vrijeme niskih, pa čak i negativnih kamatnih stopa po dužničkim instrumentima tradicionalnog tržišta kapitala, visoke inflacije, odnosno deprecijacije domicilnih valuta pojedinih država na svijetu i općenito turbulentne situacije na tradicionalnom tržištu kapitala, neosporno je da decentralizirane financije investitorima pružaju mogućnost transferiranja rizika živičenjem svoje pozicije (engl. *hedging*) kroz usluge DeFi platformi. Međutim, s obzirom da se cijeli ekosustav decentraliziranih financija temelji na kolateriziranoj dužničkoj poziciji, velik broj investitora špekulanata koriste mogućnost kreiranja sintetičkog DAI dolara da bi povećali svoje pozicije u željenoj kriptovaluti multiplikativnim deponiranjem i zaduživanjem, i tu se zapravo očituje najveći rizik DeFi sistema. Na primjer, korisnik koji se želi zadužiti i kreirati DAI token u visini od 100$ preko Maker platforme deponira 200$ protuvrijednosti ethereum kriptovalute. Sa novo kreiranim sredstvima korisnik može ponovno kupiti ethereum kriptovalutu i ponovno deponirati 100$ vrijednosti ethereum kriptovalute, odnosno sada kreirati DAI token u visini od 50$. Proces se ponavlja sve dok se ciklusno ne iscrpe sva sredstva i ne kreira X sintetičkih dolara čime zapravo investitori, vođeni motivom špekulativne zarade jer su njihove pozicije sada uvećane, umjetno povećavaju vrijednost decentraliziranih financija multipliciranjem inicijalne vrijednosti ethereum kriptovalute preko DAI tokena. Ovdje je potrebno postaviti nekoliko pitanja. Prvo je pitanje što se događa sa sintetičkim DAI dolarima koju su pušteni u opticaj te kako oni mogu utjecati na općeniti monetarni sustav, u ovom slučaju monetarni sustav SAD-a. Drugo pitanje je opstojnost ciklusa multipliciranja. Naime, opisani proces kreiranja CDP-a ispunjava svrhu samo dok imovina koja služi kao kolateral ima stabilnu tržišnu vrijednost ili vrijednost u porastu. U turbulentnim situacijama, svojstvenim tržištu kriptovaluta, kada tržišna vrijednost kolaterala počne naglo gubiti svoju vrijednost, pametni ugovori će pokrenuti proces likvidacije kolaterala, što će dodatno potaknuti pad vrijednosti kolaterala. U tom se trenutku može dogoditi da ukupna kolaterizirana pozicija bude rasprodana daleko ispod tržišne vrijednosti zbog negativnog momentuma pada vrijednosti kolaterala, što se već dogodilo u ožujku 2020. godine, te da korisnici

izgube 100% svoje kolaterizirane pozicije[92]. Zbog svega navedenog, nastala je potreba za novom kategorijom upravljanja rizicima (engl. *risk management*) unutar DeFi ekosustava, pogotovo u CDP okruženju, s ciljem kvantifikacije rizika pozicija korisnika različitim simulacijama cjenovne dinamike kolaterala i/ili sintetičke imovine.

DeFi nije u potpunosti decentraliziran. Naime, DeFi može predstavljati jedna ili više aplikacija, odnosno platformi koje pružaju DeFi usluge. Te usluge zahtijevaju informacije poput kretanja trenutnih kamatnih stopa u DeFi ekosustavu, kretanja cijene imovine koja služi kao kolateral itd. Ukoliko platforma (projektni tim) sama određuje uvjete oročavanja, posuđivanja sredstava ili cijenu imovine, usluga se ne može smatrati decentraliziranom. Na primjer, korištenje Nexo platforme[93] za oročavanje DAI tokena vezanog za američki dolar je zapravo pružanje centralizirane usluge na decentraliziranoj imovini. Jednako tako, ukoliko je cijena imovine prilikom trgovanja derivirana samo iz jednog izvora, to se isto ne može smatrati decentralizirana usluga. S druge strane, ukoliko platforma koristi automatiziran proces deriviranja cijene imovine (engl *price feed*) iz različitih izvora (engl. *oracle*) koji određuje uvjete kamata za posuđivanje, oročavanje ili trgovinu, usluga se može smatrati decentraliziranom. Postoji više razina decentralizacije DeFi usluga u ovisnosti koji procesi su u potpunosti decentralizirani, a koji nisu. Međutim, većina projekata ima tendenciju razvoja na decentraliziranim segmentima, odnosno teže prema potpunoj decentralizaciji svojih usluga.

Zbog velikih mogućnosti razvojnih programera i slobode kreiranja usluga prema tržišnim zahtjevima, ali i izostanka regulativnog okvira, cijeli DeFi ekosustav je eksperimentalne prirode i značajno je opterećen različitim tehnološkim i tržišnim rizicima. Upravo zbog toga, možda se može dogoditi da kroz određeno vrijeme niti jedan od opisanih procesa više ne bude aktivan i da DeFi tržište potpuno izgubi svoju vrijednost, trenutno skoro 2,5 milijardi dolara[94]. S druge strane, mogućnost digitalizacije i monetizacije različitih vrsta imovine za koje postoji aktivno DeFi tržište, potiče razvoj i ukazuje da granice zapravo i ne postoje. Drugim riječima, bilo koja blockchainom digitalizirana imovina se može monetizirati i predstavljati temeljnu

[92] https://medium.com/defi-saver/black-thursday-at-defi-saver-3c35ea6cd0d0
[93] https://nexo.io/earn-interest
[94] https://defipulse.com/

imovinu preko koje se izvodi proces kreditiranja DeFi korisnika, pa čak i predstavljati kolateral u CDP-u. Jednako tako, dostupnost visokih kamatama na štednju i ostalih proizvoda DeFi platformi, također može privući dodatne korisnike, što će potaknuti daljnji razvoj tehnologije i rast vrijednosti ukupnog DeFi ekosustava.

7.3. Dodatni praktični primjeri blockchain tehnologije

U nastavku se navode dodatni praktični primjeri primjene tehnologije distribuiranog zapisa kroz nekoliko osnovnih kategorija:

a) Kibernetička sigurnost. Tvrtka Guardtime[95] stvara digitalne sustave pomoću blockchaina koji se trenutno koristi za osiguranje zdravstvenih kartona za milijun državljana Estonije. Također, tvrtka REMME[96] je decentralizirani sustav provjere autentičnosti čiji je cilj zamijeniti sigurnosne sustave, prijave i lozinke SSL (engl. *secure socket layer*) certifikatima pohranjenim na blockchainu.

b) Zdravstvo. Gem[97] startup surađuje sa zdravstvenim institucijama kako bi podatke o epidemijama različitih bolesti stavio na blockchain te povećao učinkovitost i prevenirao širenju istih. Također, cilj je osigurati decentraliziranu evidenciju o pacijentima koja bi bila pohranjena na blockchain. Tvrtka MedRec[98] je projekt Instituta za tehnologiju u Massachusettsu MIT (engl. *Massachusetts Institute of Technology*) koji uključuje blockchain elektroničku medicinsku dokumentaciju namijenjenu upravljanju autentifikacijom, povjerljivošću i razmjenom podataka.

c) Financijske usluge. Barclays korporacija[99] je pokrenula niz blockchain inicijativa koje uključuju praćenje financijskih transakcija, poštivanje zakona i borbu protiv prijevara. Maersk[100] konzorcij za prijevoz je otkrio planove koji se temelje na blockchain rješenjima za pojednostavljenje morskog osiguranja. Doprinos blockchaina u transakcijskim uslugama se očituje najviše kroz smanjenje troškova i ubrzanjem provedbe transakcije, pogotovo na području globalnog plaćanja. DeFi okruženje pruža mogućnost provedbe dužničko vjerovničkih odnosa, te alokaciju imovine po višim kamatnim stopama nego

[95] https://guardtime.com/
[96] https://remme.io/
[97] https://enterprise.gem.co/health/
[98] https://www.media.mit.edu/research/groups/1454/medrec
[99] https://www.barclayscorporate.com/insights/innovation/what-does-blockchain-do/
[100] https://fortune.com/2017/09/05/maersk-blockchain-insurance/

što je to trenutno moguće ostvariti kroz usluge tradicionalne financijske industrije. Primjenom pametnih ugovora mogu se i unaprijediti procesi poravnanja i namire prilikom trgovanja financijskim instrumentima izbacujući posrednika dijeljenom javnom knjigom, te ubrzavajući sam proces prijenosa vlasništva kroz jednu evidenciju[101].

d) Proizvodnja i industrija. Blockchain može pomoći potrošačima da prate proizvod s aspekta kontrole kvalitete za vrijeme prijevoza od svog mjesta podrijetla do prodavača. Tvrtkama može pomoći da utvrde moguću neučinkovitost u svojim dobavljačkim lancima (engl. *supply chain*) prateći stavke u realnom vremenu. Provenance[102] provodi projekt u kojem je cilj implementirati blockchain za evidenciju podrijetla robe u dobavljačkim lancima. Također, najave su da i Reliance Industries[103], najveći indijski konglomerat, razvija logističku platformu dobavljačkog lanca koja se temelji na blockchainu, zajedno s vlastitom kriptovalutom. S druge strane, na primjeru električne energije, korisnicima koji imaju instalirane solarne panele, blockchain može pomoći kroz bolju vidljivost transakcije i pomoći im da razumiju model ostvarivanja prihoda, što bi potaknulo sudjelovanje većeg broja korisnika, omogućavajući visoko distribuirani energetski scenarij na više kontroliran i siguran način[104].

e) Implementacija blockchaina na razini države. Dubai je postavio cilj da postane prva država na svijetu koja implementira blockchain. U 2016. god. predstavnici 30 vladinih odjela osnovali su odbor posvećen istraživanju mogućnosti zdravstvene zaštite, brodarstva, registracije poduzeća i sprečavanju širenja malverzacija s trgovinom dijamantima[105]. Sjeverna Koreja je već razvila „MyID“ savez koji uključuje 39 partnera državnih i privatni tvrtki iz sektora financija, osiguranja, internet prodaje i proizvodnje kako bi implementirali pouzdan decentralizirani ekosustav digitalne identifikacije[106].

---

101 https://aeternity.com/
102 https://www.provenance.org/whitepaper
103 https://www.ccn.com/jiocoin-indias-biggest-conglomerate-launch-cryptocurrency/
104 https://www.renewableenergyworld.com/2018/02/16/blockchain-could-change-everything-for-energy/#gref
105 https://www.zdnet.com/article/could-blockchain-run-a-city-state-inside-dubais-blockchain-powered-future/
106 https://theicon.ist/2019/11/05/a-comprehensive-look-at-iconloops-myid-alliance-its-partners-advisors-and-upcoming-roadmap/

f) Maloprodaja. OpenBazaar[107]. je kreirao decentralizirano tržište na kojem se trguje s robom i uslugama bez posrednika i naknade

g) Zabava. Portal Ujomusic[108] je osnovan s ciljem praćenja autorske naknade za glazbenike koji omogućava da se stvori zapis o vlasništvu nad njihovim radom.

h) Glasovanje. Startup Follow My Vote[109] koristi blockchain tehnologiju kako bi osigurao jednostavan i transparentan izborni proces. Svaki potencijalni birač se može sigurno prijaviti putem svoje web kamere i formalne osobne iskaznice. Nakon završetka glasovanja, svatko može koristiti svoju iskaznicu kako bi pratio svoje glasove i provjerio je li glasovanje dodijeljeno ispravno. Također, birači čak mogu mijenjati svoju odluku više puta sve do isteka roka glasovanja.

i) Internat stvari (engl. *internet of things* - IoT). Prema Shrivastava, Le, i Sharma (2020), 50 milijardi uređaja bi trebalo biti umreženo u 2020. godini. Internet stvari predstavlja zajednički naziv za sve digitalne uređaje koji su u stanju se povezati s većom komunikacijskom mrežom. Tehnologija distribuiranog zapisa se može koristiti za praćenje milijardi povezanih uređaja, omogućiti njihovu obradu transakcija i koordinaciju, čineći značajne uštede za proizvođače IoT industrije. Decentralizirani pristup eliminira jedinstvenu točku kvara, stvorivši otporniji ekosustav za uređaje na kojima će se pokrenuti (Shrivastava et al., 2020) .

[107] https://www.openbazaar.org/
[108] https://ujomusic.com/
[109] https://followmyvote.com/

8. METODOLOGIJA RADA

Kriptovalute su nova vrsta digitalne imovine čija struktura omogućava prijenos njihovog vlasništva na primarnom i sekundarnom tržištu kriptovaluta. Prijenos vlasništva podrazumijeva kupnju, odnosno naknadnu prodaju imovine po različitoj tržišnoj cijeni, što predstavlja proces investiranja. Proces investiranja je rizičan proces koji uključuje izloženost tržišnim promjenama vrijednosti imovine koja je predmet trgovine. Ukoliko se investira u više rizičnu imovinu, investitori očekuju kompenzaciju u obliku višeg očekivanog prinosa. S obzirom da je proces investiranja povezan s raznim oblicima i izvorima rizika, investiranje zapravo predstavlja problem odlučivanja investitora prilikom alokacije sredstava. Racionalan investitor alocira sredstva s ciljem ostvarivanja prinosa na uloženi kapital koji u domeni njegove tolerancije, odnosno averzije prema riziku, adekvatno kompenzira očekivanu/ostvarenu premiju za preuzeti rizik. Svojstvo koje određuje je li promatrana investicija pogodna za investitora, ovisi o podudarnosti preferencije rizika i očekivanog prinosa investitora, s rizikom i očekivanim prinosom promatrane investicije. Prema tome, problem odlučivanja se razmatra kvalitativnim, ali i brojnim kvantitativnom pristupima, gdje se neizvjesnost i ostvareni prinos eksplicitno determiniraju i kvantificiraju kao rizik i očekivani prinos te tako uzimaju u daljnji proces odlučivanja. Bez obzira na vrstu imovine koja se razmatra kao sastavnica portfelja, investitori bi trebali razmotriti dinamiku odnosa prinosa odabrane imovine portfelja kako bi se identificirao i kvantificirao preuzeti rizik ulaganja. U ovom se radu formalno identificiraju i opisuju odnosi rizika i prinosa različitih portfelja kreiranih od nove vrste digitalne imovine – kriptovaluta, s ciljem ocjene uspješnosti potencijalnog ulaganja. U tu svrhu, modeliranju portfelja se pristupilo primjenom koncepta moderne teorije portfelja koji predstavlja jedan od najviše korištenih baznih modela za rješavanje problema alokacije imovine i definiranje optimalnog ulaganja.

Ispitivanje uspješnosti modeliranja portfelja se provodi u dva dijela. U prvom će se dijelu istraživanja ispitati mogućnost kreiranja portfelja unutar uzorka (engl. *in the sample*), kreirat će se efikasne granice, opisati dinamika promjene udjela sukladno promjeni tolerancije prema riziku te će se interpretirati odnosi prinosa i rizika mogućih portfelja. U drugom se dijelu rada isti modeli provode izvan uzorka (engl. *out of sample*), čime se više želi približiti i interpretirati mogućnost praktične implikacije

optimizacijskih ciljeva. U tom slučaju, razdoblje promatranja se dijeli na dva seta podataka. Prvi dio seta podataka služi za treniranje modela, odnosno definiranje udjela portfelja sukladno optimizacijskom cilju, a drugi dio za testiranje modela prema prethodno dobivenim udjelima na novim podacima koji ne ulaze u set podataka za treniranje optimizacijskih ciljeva. U radu će se formirati više portfelja s različitim optimizacijskim ciljevima minimizacije rizika, maksimalizacije prinosa i maksimalizacije omjera prinosa i rizika. S obzirom na rezultate prethodnih istraživanja Briere et al. (2015) i Lee Kuo Chuen et al. (2018) i odsutnost normalne distribucije prinosa, osim standardne devijacije, za mjeru rizika će se koristiti i uvjetna rizičnost vrijednosti (engl*. Conditional Value at Risk* – CVaR).

S obzirom na optimistična očekivanja buduće vrijednosti bitcoina, investitori ne moraju nužno zahtijevati povrat izražen u fiat valuti poput dolara. Naime, postoji interes i potreba promatranja bitcoina kao obračunske jedinice korisnosti ulaganja portfelja, s ciljem akumuliranja veće količine bitcoina kao krajnje vrijednosti. Sukladno postavljenim hipotezama istraživanja, vrijednost prvog seta portfelja bit će modelirana i izražena u vrijednosti bitcoina kao vodeće varijable na tržištu kriptovaluta, a vrijednost drugog seta portfelja bit će modelirana i izražena u paritetu s dolarom. Razdoblje u kojem će se razmotriti bitcoin kao obračunska jedinica korisnosti ulaganja predstavlja period od 18. listopada 2018. god. do 24. rujna 2020. god., što čini ukupno 1.071 dnevnu opservaciju, odnosno 1.070 dnevnih prinosa. Notacija optimizacijskih ciljeva portfelja izraženih u vrijednosti bitcoin kriptovalute je sljedeća: minimizacija varijance – bitcoin (MinVar-B), minimizacija CVaR-a – bitcoin (MinCVaR-B), maksimalizacija Sharpe omjera – bitcoin (MaxSR-B), maksimalizacija STARR omjera – bitcoin (MaxSTARR-B) i maksimalizacija očekivanog prinosa – bitcoin (MaxMean-B). S druge strane, notacija optimizacijskih ciljeva portfelja izraženih u dolarskoj protuvrijednosti je sljedeća: minimizacija varijance (MinVar), minimizacija CVaR-a (MinCVaR), maksimalizacija Sharpe omjera (MaxSR), maksimalizacija STARR omjera (MaxSTARR) i maksimalizacija očekivanog prinosa (MaxMean).

Osim navedenih optimizacijskih ciljeva, kreirat će se i portfelj s jednakim udjelima $(1/N)$ gdje je N broj sastavnica u portfelju, za oba seta portfelja da bi se usporedile i prezentirale moguće prednosti ili nedostaci takve strategije. Rezultati portfelja

izraženom u dolarskoj vrijednosti usporedit će se s dinamikom kretanja CRIX indeksa koji služi kao indikator kretanja tržišta kriptovaluta (engl. *benchmark*) čime se želi ispitati mogućnost konstrukcije portfelja koji ostvaruje bolje rezultate od rezultata tržišta u istom razdoblju promatranja. Sastavnice indeksa koji odgovara periodu promatranja su: bitcoin (BTC), ethereum (ETH), eos (EOS), ripple (XRP) i litecoin (LTC). Pored toga, s obzirom na metodologiju CRIX indeksa koja ne uključuje optimizacijske modele, prethodno navedeni optimizacijski ciljevi bit će provedeni i na sastavnicama CRIX indeksa, kako bi se ispitao značaj korištenja fundamentalnih indikatora prilikom konstrukcije portfelja kriptovaluta. Također, s ciljem utvrđivanja prednosti uključivanja fundamentalnih indikatora, u radu će se predstaviti dodatnih deset portfelja čije su sastavnice uzorak od dvadeset nasumično odabranih kriptovaluta[110] od ukupno mogućih prvih sedamdeset kriptovaluta po tržišnoj kapitalizaciji, te će na njima također biti provedeni isti optimizacijski ciljevi. Teorijska opravdanost ovakvog pristupa proizlazi upravo iz odsutnosti veze između fundamentalnih pokazatelja i tržišne vrijednosti kriptovaluta. Drugim riječima, prilikom odabira sastavnica portfelja, investitori su često prepušteni nasumičnom odabiru zbog nepoznavanja pozadinske tehnologije kriptovaluta i realnih mogućnosti koje pruža projekt. Također, investitori se često oslanjaju i na uljepšano stanje prezentirano u medijima i/ili na stranicama projekta, što je gotovo uvijek subjektivne naravi. Korišteno razdoblje za procjenu značaja fundamentalnih indikatora koje pokriva sve uključene kriptovalute je od 25. siječnja 2018. god. do 1. kolovoza 2019. god., što čini uzorak od ukupno 554 dnevnih opservacija, odnosno 553 dnevnih prinosa.

8.1. Moderna teorija portfelja

Bazni model optimizacije korišten u ovom radu se temelji na modernoj teoriji portfelja (eng. *Modern Portfolio Theory* – MPT), koja je predstavljena 1952. godine objavom članka „*Portfolio Selection*“ od strane autora Harry M. Markowitz, a koji je nastao kao rezultat njegove doktorske disertacije (Žiković, 2005). U svom izvornom obliku model se fokusira na minimizaciju varijance portfelja imovine za neku danu razinu očekivanog prinosa unutar određenih teorijskih pretpostavki, zbog čega se često

[110] Za nasumični odabir kriptovaluta kao sastavnica alternativnih portfelja je korišten online algoritam sa internet stranice: https://www.dcode.fr/random-sampling

naziva i model srednje vrijednosti i varijance (engl. *Mean-Variance* M-V). Doprinos Markowitzevog rada se očituje uključivanjem dodatne ulazne varijable prilikom konstrukcije portfelja. Naime, Žiković (2005) navodi kako su i prije objave rada postojali teorijski modeli koji su razmatrali očekivani prinos imovine portfelja, kao i njezin rizik, prilikom odabira investicije i konstrukcije portfelja. Međutim, razlika između prijašnjih modela i objavljenog Markowitzevog rada je u tome što je on prvi razmotrio međuovisnosti između sastavnica portfelja kao input u procesu odlučivanja, čime je prezentirani pojam diverzifikacije postao standard u procesu donošenje odluke o investiranju. Prema tome, osim dvije osnovne varijable: prinos (r) i rizik (σ), koje su do tada utjecale na odluku o formiranju pojedinačnog portfelja, Markowitz u svom radu uključuje međuovisnost kretanja pojedinačnih vrijednosnica koje se nalaze unutar portfelja, kao novu varijablu, prezentiranu njihovim koeficijentom korelacije (ρ). Opisani pristup pružio je investitorima mogućnost da kreiraju nove portfelje koji im za danu razinu rizika, pružaju viši očekivani prinos, odnosno za dani očekivani prinos, pružaju niži rizik, pri čemu inicijalne varijable imovine u portfelju $(r \text{ i } \sigma)$ ostaju nepromijenjene (Žiković, 2005).

Prije objave Markowitzevog rada, težište investicijske industrije je bilo na identificiranju dionica „pobjednika“, dionica koje su po svojim fundamentima podcijenjene ili obećavaju održivi rast, odnosno dionica s visokim očekivanim prinosom. Markowitz je zaključio da ulagači trebaju odlučiti na temelju očekivanog povrata od ulaganja, kao i rizika od ulaganja. Međutim, u tom slučaju je rizik definiran kao varijanca portfelja koja uključuje korelaciju sastavnica. Ideja o uključivanju rizika u odluke o ulaganju i primjeni discipliniranog kvantitativnog okvira za upravljanje investicijama, bila je nova u to vrijeme. Izvorno je ova investicijska filozofija generirala malo interesa, no na kraju ju je financijska zajednica prihvatila. Tijekom godina, teorija odabira portfelja koju je formulirao Markowitz se proširivala i iznova utemeljila na modifikaciji pretpostavki izvornog modela koji je djelomično ograničavao njegovu primjenu. Markowitz je uveo potpuno novu terminologiju koja je sada norma u zajednici za upravljanje investicijama, a 1990. godine je dobio Nobelovu memorijalnu nagradu za ekonomske znanosti kao priznanje za svoj temeljni rad.

Markowitz je u svom radu u osnovi kvantificirao konvencionalnu mudrosti „sva jaja ne smiju ići u jednu košaru“. Matematički, varijanca portfelja je zbroj pojmova koji

uključuju i varijance povrata pojedine imovine i kovarijance (što je jednako korelacijama) između tih prinosa. Ulaganje ukupnih sredstava u imovinu koja je u snažnoj korelaciji se ne smatra razboritom strategijom, čak i ako se čini da je svaka od imovine na temelju preliminarne fundamentalne analize "pobjednik". Ukoliko bilo koja pojedinačna imovina portfelja ne ostvari očekivana predviđanja, vjerojatno će, zbog svoje visoke korelacije s drugom imovinom, i ta druga imovina ostvariti negativan ili manji prinos, značajno smanjujući vrijednost cijelog portfelja.

Neka se razmotri ulaganje u sljedeće dvije dionice, dionicu 1. i dionicu 2. Očekivani prinos dionice 1. je $E(\tilde{r}_1) = \mu_1 = 10\%$, a dionice 2. je $E(\tilde{r}_2) = \mu_2 = 12\%$, a njihova standardna devijacija je $\sigma_1 = 16\%$ i $\sigma_2 = 15\%$. Da bi se izračunao očekivani prinos dionice, potrebni su podaci o njihovim povijesnim prinosima. Dnevni diskretni prinos pojedine dionice, a koji je ujedno korišten i kao vremenski interval za izračun prinosa kriptovaluta u ovom radu, računa se na sljedeći način (Žiković, 2005):

$$r_i = \left(\frac{P_t - P_{t-1}}{P_{t-1}}\right) \times 100 \qquad (1)$$

Gdje je r_i dnevni diskretni prinos dionice i, P_t predstavlja cijenu dionice i na dan t, a P_{t-1} cijenu dionice i na dan $t-1$.Očekivani prinos pojedinačne dionice je dan kao srednja vrijednost (aritmetička sredina) slučajne varijable[111] (prinosa) u promatranom razdoblju, označena (~). Očekivani prinos je ponderirani prosjek svih mogućih ishoda u distribuciji prinosa dionice, gdje su ponderi prinosa jednake vjerojatnosti (Pachamanova i Fabozzi, 2016):

$$E(\tilde{r}_i) = \sum \tilde{r}_i \times P(\tilde{r}_i = r_i) \qquad (2)$$

Gdje $P(\tilde{r}_i = r_i)$ vjerojatnost ishoda slučajne varijable (prinosa dionice). Mjera standardne devijacije, odnosno varijance slučajne varijable se može uzeti kao adekvatna mjera rizika. Rizi predstavlja mogućnost da se ne ostvari planirani povrat na sredstva alocirana u određeni portfelj vrijednosnica (Žiković, 2005). Rizik

[111] Slučajna varijabla je varijabla kojoj su vrijednosti slučajne, tj. ne mogu se predvidjeti sa sigurnošću, nego samo s određenom vjerojatnošću.

predstavlja stanje u kojem postoji mogućnost negativnog odstupanja od poželjnog ishoda koji se očekuje (Vaughan i Vaughan, 1998). Prema tome, rizik je šansa da se dogodi nešto što će imati utjecaj na naše ciljeve, ali čije su posljedice i vjerojatnost događaja kvantitativno mjerljive veličine. Stoga se disperzija raspodjele vrijednosti od očekivanih ciljeva prezentirana varijancom i standardnom devijacijom nameće kao adekvatna mjera rizika. Varijanca predstavlja sumu ponderiranih kvadrata odstupanja mogućih prinosa oko očekivane srednje vrijednosti, a što su veća odstupanja oko očekivane srednje vrijednosti i što je veća vjerojatnost njihova nastajanja, varijanca će biti veća (Žiković, 2005). Matematički, varijanca slučajne varijable (prinosa dionice) u promatranom razdoblju se računa primjenom izraza (3) (Pachamanova i Fabozzi, 2016):

$$\sigma_i^2 = Var(\tilde{r}_i) = \sum (r_i - \mu)^2 \times P(\tilde{r}_i = r_i) \tag{3}$$

Gdje μ predstavlja srednju vrijednost distribucije. Zbog toga što je vrijednost varijance teže interpretirati u odnosi na veličinu jedince slučajne varijable koju predstavlja, varijancu je potrebno izraziti kao drugi korijen, čime se dobije mjera standardne devijacije (4):

$$\sigma_i = \sqrt{Var(\tilde{r}_i)} \tag{4}$$

Ukoliko bi se razmatrali samo ponuđeni parametri iz prethodnih mogućnosti, dionica 2. predstavlja bolji investicijski odabir sa višim očekivanom prinosom i nižom standardnom devijacijom. Prema tome, alocirajući 100% sredstava u dionicu 2., potencijalni investitor bi mogao ostvariti bolji rezultat uz niži rizik, ukoliko je rizik definiran samo kao pripadna standardna devijacija mogućih ishoda. Neka se u proces odlučivanja uključe novi parametri: međuovisnosti između dionica prezentirana kao koeficijent korelacije[112] koji iznosi $\rho_{12} = -0{,}30$, te udjeli dionice 1. w_1 i dionice 2. w_2 u portfelju. S obzirom da ukupna veličina ulaganja mora iznositi 100%, udio u dionici 2. je $w_2 = 1 - w_1$. Prinos portfelja $\tilde{r}_p$ je slučajna varijabla i za dvije dionice (ili bilo koja druga dva financijska instrumenta u portfelju) se može izraziti kao (5):

[112] Izraz za izračun koeficijenta korelacije dan je u nastavku rada kao izraz (10).

$$\tilde{r}_p = w_1\tilde{r}_1 + w_2\tilde{r}_2 \quad (5)$$

Ili u vektorskoj notaciji:

$$\tilde{r}_p = [w_1 \quad w_2] \times \begin{bmatrix}\tilde{r}_1 \\ \tilde{r}_2\end{bmatrix} = \mathrm{w}'\tilde{\mathrm{r}}$$

Gdje apostrof (') predstavlja oznaku za transponiranje matrice. Očekivani prinos portfelja dan je izrazom (6):

$$E\left[\tilde{r}_p\right] = E[w_1\tilde{r}_1 + w_2\tilde{r}_2] = E[w_1\tilde{r}_1] + E[w_2\tilde{r}_2] = w_1E[\tilde{r}_1] + w_2E[\tilde{r}_2] = w_1\mu_1 + w_2\mu_2 \quad (6)$$

Odnosno u vektorskoj notaciji:

$$E\left[\tilde{r}_p\right] = E[\mathrm{w}'\tilde{\mathrm{r}}] = \mathrm{w}'E[\tilde{\mathrm{r}}] = [w_1 \quad w_2] \times \begin{bmatrix}E[\tilde{r}_1] \\ E[\tilde{r}_2]\end{bmatrix} = \mathrm{w}'\mu$$

Varijanca portfelja za dvije dionice je dana izrazom (7):

$$\begin{aligned}\sigma_p^2 = Var(w_1\tilde{r}_1 + w_2\tilde{r}_2) &= Var(w_1\tilde{r}_1) + Var(w_2\tilde{r}_2) + 2 \times Covar(w_1\tilde{r}_1 + w_2\tilde{r}_2) \\ &= w_1^2\sigma_1^2 + w_2^2\sigma_2^2 + 2w_1w_2\sigma_{12} \quad (7)\end{aligned}$$

Dok je varijanca portfelja u vektorskoj notaciji dana kao:

$$\begin{aligned}\sigma_p^2 = \mathrm{w}'\Sigma w &= [w_1 \quad w_2] \times \begin{bmatrix}\sigma_1^2 & \sigma_{12} \\ \sigma_{21} & \sigma_2^2\end{bmatrix} \times \begin{bmatrix}w_1 \\ w_2\end{bmatrix} \\ &= [w_1\sigma_1^2 + w_2\sigma_{21} \times w_1\sigma_{12} + w_2\sigma_2^2] \times \begin{bmatrix}w_1 \\ w_2\end{bmatrix} \\ &= w_1^2\sigma_1^2 + w_2^2\sigma_2^2 + 2w_1w_2\sigma_{12}\end{aligned}$$

Odnosno, u slučaju procjene koeficijenta korelacije, varijanca portfelja s dvije dionice se može izraziti kao (8):

$$\sigma_p^2 = w_1^2\sigma_1^2 + w_2^2\sigma_2^2 + 2w_1w_2\sigma_1\sigma_2\rho_{12} \quad (8)$$

Ukoliko se koristi matrica koeficijenata korelacije, varijanca portfelja u vektorskoj notaciji se može zapisati kao:

$$\sigma_p^2 = [w_1\sigma_1 \quad w_2\sigma_2] \times \begin{bmatrix} 1 & \rho_{12} \\ \rho_{21} & 1 \end{bmatrix} \times \begin{bmatrix} w_1\sigma_1 \\ w_2\sigma_2 \end{bmatrix}$$

$$= [w_1\sigma_1 + w_2\sigma_2\rho_{21} \times w_1\sigma_1\rho_{12} + w_2\sigma_2] \times \begin{bmatrix} w_1\sigma_1 \\ w_2\sigma_2 \end{bmatrix}$$

$$= w_1^2\sigma_1^2 + w_2^2\sigma_2^2 + 2w_1w_2\sigma_1\sigma_2\rho_{12}$$

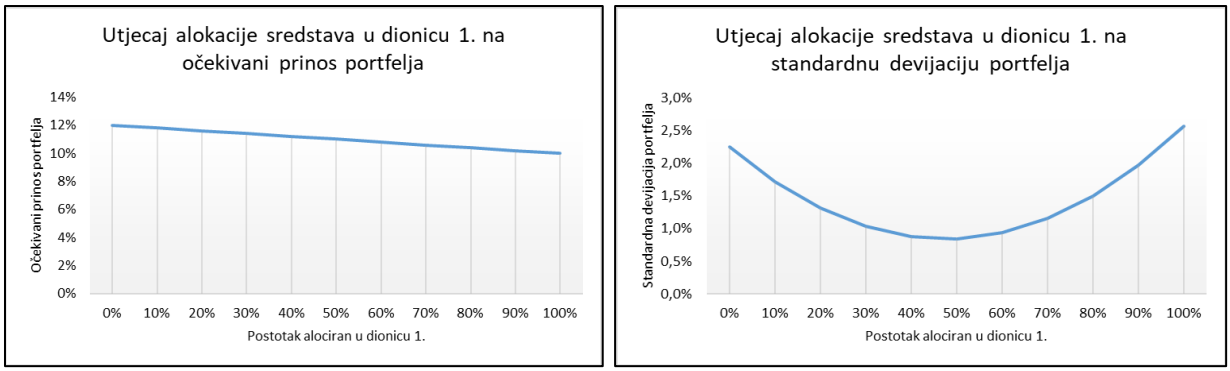
Da bi se izveo koeficijent korelacije ρ, potrebna je kovarijanca dionica koja se matematički može izraziti kao (9). Kovarijanca mjeri simultana odstupanja od srednje vrijednosti μ_1 i μ_2, za dvije slučajne varijable, u ovom slučaju prinose dionica $\tilde{r}_1$ i $\tilde{r}_2$.

$$Cov(\tilde{r}_1\tilde{r}_2) = E[\tilde{r}_1 - \mu_1)(\tilde{r}_2 - \mu_2)] \tag{9}$$

Gdje E predstavlja očekivanja, odnosno prosjek. Prema tome, kovarijanca ukazuje kreću li se dvije slučajne varijable u prosjeku zajedno. Konačno, koeficijent korelacije za dvije slučajne varijable (prinose dionica) je dan kao izraz (10):

$$\rho = Corr(\tilde{r}_1\tilde{r}_2) = \frac{Cov(\tilde{r}_1\tilde{r}_2)}{\sigma_1\sigma_2} \tag{10}$$

Grafikon 1. ilustrira dinamiku promjene očekivanog prinosa i standardne devijacije portfelja sačinjenom od dvije dionice, s obzirom na promjenu alokacije sredstava u dionicu 1. Iako je očekivani prinos portfelja najveći kada je 0% sredstava alocirano u dionicu 1., ukoliko se sredstva ravnomjerno alociraju između dionice 1. i dionice 2., moguće je ostvariti daleko bolji omjer prinosa i rizika, što je ilustrirano krivuljom konveksnog oblika na desnoj strani Grafikona 1.



Grafikon 1. Promjene očekivanog prinosa i standardne devijacije portfelja sukladno povećanju udjela dionice 1. u portfelju
Izvor: Izrada autora

Sukladno tome, uvažavajući negativnu međuovisnost između imovine portfelja, moguće je postići rizik portfelja koji je značajno niži od razine standardne devijacije pojedinačne imovine u portfelju, čime se potvrđuje korisnost razmatranja međuovisnosti kao treće varijable prilikom donošenja odluke o investiranju.

8.2. Portfelj srednje vrijednosti i varijance

Neka se pretpostavi da investitor želi alocirati svoja sredstva u N broj rizične imovine. Izbor investitora se može prezentirati kao $N \times 1$ vektorski niz $\mathrm{w} = (w_1, \dots, w_N)'$ udjela u portfelju. Svaki udio portfelja w_i predstavlja proporciju imovine i držanu u portfelju, a zbroj ukupnih udjela portfelja mora iznositi 100%, odnosno:

$$\sum_{i=1}^{N} w_i = 1 \tag{11}$$

U vektorskoj notaciji, gornji izraz se može zapisati kao izraz (12) (Pachamanova i Fabozzi, 2016):

$$w'\iota = 1 \tag{12}$$

Gdje ι predstavlja $N \times 1$ vektorski niz jedinica. Ukoliko je posudba instrumenata portfelja dozvoljena s namjerom njihove kratke prodaje, odnosno prodaje pa naknadne kupnje kako bi se instrumenti vratili brokeru od koga su posuđeni, udjeli u portfelju mogu biti negativni. Međutim, s obzirom da tržište kriptovaluta za sada nema dovoljno likvidnu infrastrukturu za kratku prodaju imovine, te su zbog toga naknade za posuđene kriptovalute iznimno visoke, u radu se mogućnost kratke prodaje kriptovaluta kao varijable u optimizaciju neće razmatrati. Tijekom perioda razmatranja, prinosi N imovine u portfelju se mogu prezentirati kao vektorski niz slučajnih varijabli: $\tilde{r} = (\tilde{r}_1, \dots, \tilde{r}_N)'$, gdje je očekivani prinos N imovine notiran kao $\mu = (\mu_1, \dots, \mu_N)'$, a matrica kovarijanci prinosa je prikazana sukladno matričnom zapisu (13):

$$\Sigma = \begin{bmatrix} \sigma_{11} & \cdots & \sigma_{1N} \\ \vdots & \ddots & \vdots \\ \sigma_{N1} & \cdots & \sigma_{NN} \end{bmatrix} \tag{13}$$

Gdje σ_{ij} predstavljaju kovarijancu između prinosa imovine i i j, dok je dijagonalni element σ_{11}varijanca imovine i, odnosno $\sigma_{11} = \sigma_i^2$. S obzirom na simetričnost matrice kovarijance, kovarijanca između imovine i i j jednaka je kovarijanci imovine j i i. Sukladno notacijama, očekivani prinos μ_p i varijanca portfelja σ_p^2, sa sredstvima alociranim prema $\mathrm{w} = (w_1, \dots, w_N)'$, su dani kao (14) i (15):

$$\mu_p = \sum_{i=1}^{N} \mu_i \times w_i = \mu' \mathrm{w} \tag{14}$$

Odnosno:

$$\sigma_p^2 = \mathrm{w}' \Sigma \mathrm{w} \tag{15}$$

Ukoliko se umjesto matrice kovarijance, koristi matrica koeficijenata korelacije (16):

$$\mathrm{C} = \begin{bmatrix} 1 & \dots & \rho_{1N} \\ \vdots & \ddots & \vdots \\ \rho_{1N} & \dots & 1 \end{bmatrix} \tag{16}$$

U tom je slučaju prvo potrebno kreirati vektor umnoška udjela imovine u portfelju i njihove standardne devijacije $\mathrm{w}^s = (w_1\sigma_1, \dots, w_N\sigma_N)'$. Nakon toga, varijanca portfelja je dana izrazom (17):

$$\sigma_p^2 = (\mathrm{w}^s)'\mathrm{C}\mathrm{w}^s \tag{17}$$

Osnovni oblik Markowitz formulacije izražen u formi linearne algebre se može zapisati na sljedeći način (Pachamanova i Fabozzi, 2016):

$$\begin{aligned} \min_{w} \quad & \sigma_p^2\,(w) = \mathrm{w}'\Sigma\mathrm{w} \\ podložno\ ograničenjima \quad & w'\mu \geq r_{target} \\ & w'\iota = 1 \\ & w_i \geq 0, \;\; i = 1, \dots, N \end{aligned} \tag{18}$$

Gdje je σ_p^2 varijanca portfelja, $\mathrm{w} = (\mathrm{w}_1, \dots, \mathrm{w}_\mathrm{N})'$ vektorski niz udjela pojedinačne imovine u portfelju i Σ procijenjena matrica kovarijanci imovine N, odnosno njenih prinosa. Rezultat gornje relacije je podložan prema tri dodatna ograničenja: $w'\mu$ je $(N \times 1)$ vektor očekivanih prinosa imovine portfelja čiji zbroj, s obzirom na pojedinačne udjele imovine u portfelju, mora biti viši ili jednak željenom ukupnom prinosu portfelja, $w'\iota$ predstavlja $(N \times 1)$ vektor gdje svi elementi vektora predstavljaju udjele portfelja i njihov zbroj mora biti 1 (*full investment constraint*) i zadnje ograničenje definira zabranu kratke prodaje imovine, odnosno svi udjeli u portfelju moraju biti pozitivne veličine. Navedena relacija minimizira varijancu portfelja σ_p^2 preko mogućih vrijednosti udjela imovine u portfelju w. Daljnjom formulacijom, model se više prilagođava stvarnim potrebama gdje se razvijaju njegove inačice korištene u ovom radu i opisane u nastavku.

8.3. Portfelj s minimalnom varijancom

Ukoliko se iz izraza (18) izostavi ograničenje zahtijevane stope prinosa, optimizacijom portfelja s ciljem minimizacije rizika, dobit će se portfelj s najmanjim

rizikom (engl. *Global Minimum Variance Portolio* – GMV). Korištena formulacija za GMV u ovom radu je dana izrazom (19).

$$\begin{aligned} \min_{w} \quad & \sigma_p^2\,(w) = \mathrm{w}'\Sigma\mathrm{w} \\ podložno\ ograničenjima \quad & w'\iota = 1 \\ & w_i \geq 0, \;\; i = 1, \dots, N \end{aligned} \tag{19}$$

Navedena strategija u izračun uzima samo matricu kovarijanci prinosa i temelji se na pronalasku udjela pojedinačne imovine koji minimiziraju ukupnu varijancu portfelja.

8.4. Portfelj s minimalnom uvjetnom rizičnošću vrijednosti

Kao što je prethodno prikazano, varijanca je mjera raspona ili disperzije raspodjele vjerojatnosti slučajne varijable. U kontekstu optimizacije portfelja, slučajna varijabla u ovom radu predstavlja diskretnu varijablu, odnosno dnevne prinose promatrane kriptovalute, odnosno portfelja. Međutim, prinosi mogu poprimiti negativnu, ali i pozitivnu vrijednost, iz čega proizlazi da korištenje varijance kao mjere rizika u kontekstu optimizacije portfelja znači da se ishodi iznad očekivanog povrata portfelja smatraju jednako rizičnim kao i ishodi ispod očekivanog povrata portfelja. Takav pristup je kontraintuitivan, jer je vjerojatnije da potencijalne investitore zabrinjavaju ishodi koji ne ispunjavaju očekivanja, a ne ishodi koji premašuju očekivanja. Sukladno tome, u radu se razmatra i alternativna mjera rizika koja uzima u obzir samo negativne ishode slučajne varijable, kako bi se otklonio nedostatak inicijalnog Markowitz modela srednje vrijednosti i varijance, što podrazumijeva model uvjetne rizičnosti vrijednosti – CVaR.

8.4.1. Rizičnost vrijednosti (VaR)

Događaji s početka devedesetih godina su motivirali financijsku industriju da razvije metode za mjerenje potencijalnih gubitaka vrijednosti portfelja uslijed nepovoljnih kretanja na tržištu. Mjerenje rizika je nužan uvjet za upravljanje rizikom, pri čemu je prvo potrebno kvantificirati količinu rizika prema kojemu je investitor izložen, a zatim razraditi strategiju za kontrolu učinka potencijalnih gubitaka. U nastavku se

prezentiraju osnovne karakteristike VaR metode, a koja služi za mjerenje financijskog rizika, posebno tržišnog rizika koji predstavlja gubitke proizašle iz nepovoljnih kretanja financijskih instrumenata, odnosno u ovom slučaju kriptovaluta.

Rizičnost vrijednosti (engl. *Value at Risk* - VaR) je sredinom 1990-ih predložila investicijska banka J. P. Morgan kao pristup za mjerenje potencijalnog gubitka portfelja s kojim bi se financijska institucija mogla suočiti ukoliko se dogodi nepovoljan događaj u određenom vremenskom horizontu. Prema Žiković (2005) VaR je mjera koja daje najveći gubitak koji se može ostvariti od određene investicije, u promatranom periodu, uz određenu vjerojatnost uslijed „normalnog" kretanja tržišta. Navedena definicija podrazumijeva nekoliko opažanja koje je potrebno naglasiti (Alexander i Sheedy, 2005):

a) VaR je procjena, a ne jedinstveno definirana vrijednost.
   Vrijednost bilo koje VaR procjene ovisit će o stohastičkom procesu za koji se pretpostavlja da predstavlja slučajnu varijablu tržišnih podataka. Struktura slučajnog procesa mora biti identificirana i specifični parametri tog procesa se moraju kalibrirati. To zahtijeva korištenje povijesnih podataka i postavlja čitav niz pitanja kao što su duljina povijesnog uzorka koji se koristi i trebaju li nedavna događanja imati veću težinu u uzorku od onih u daljnjoj prošlosti. U suštini, cilj je doći do najbolje moguće procjene stohastičkog procesa koji predstavlja podatke o tržištu tijekom određenog kalendarskog razdoblja na koje se primjenjuje VaR procjena. Štoviše, jasno je da tržišni podaci ne generiraju stabilni slučajni proces. Različite metode rješavanja nesigurnosti oko promjena u tim slučajnim procesima predstavlja glavni razlog zašto VaR procjene nisu jedinstvene.
b) Slučajna varijabla koja se razmatra je fiksna za predmetno razdoblje.
   Navedeno predstavlja problem kada je razdoblje procjene dovoljno dugo da bi takva pretpostavka bila nerealna. Čest primjer toga je zahtjev za procjenom VaR-a tijekom vremenskog perioda od deset dana za potrebe regulatornog kapitala za tržišni rizik u skladu s Bazelskim sporazumom o kapitalu. U tom slučaju najčešće je potrebno skaliranje VaR procjene za kraće razdoblje pod pretpostavkom da se tržišni podaci kreću neovisno iz dana u dan.
c) VaR mjera ne nudi distribuciju mogućih gubitaka u onim rijetkim slučajevima kada je gubitak veći od procjene VaR-a.

Nikad nije ispravno tretirati veličinu VaR mjere kao nagori mogući scenarij gubitka. Prilikom analiza veličine rijetkih, ali ekstremnih gubitaka moraju se koristiti alternativni alati koji ulaze u teoriju ekstremnih vrijednosti (engl. *Extreme Value Theory* – EVT), poput uvjetne rizičnosti vrijednosti (CVaR-a) korištene u ovom radu ili simulacije vođene povijesnom dinamikom tržišta u najgorem slučaju.

Rizična vrijednost – VaR je povezana s percentilom[113] statističke mjere. VaR mjeri predviđeni maksimalni gubitak portfelja u jedinicama valute, uz određenu razinu pouzdanosti, odnosno statistički definirano područje vjerojatnosti, tijekom određenog vremenskog razdoblja. Uobičajene razine vjerojatnosti uključuju 0,95 i 0,99, a pripadajući VaR se naziva 95% VaR i 99% VaR (drugim riječima, vjerojatnost se navodi u postocima). Standard vremenskog horizonta izražavanja veličine VaR-a uključuje 1 dan i 10 dana. Matematički, pri razini vjerojatnosti $100(1-\epsilon)\%$ VaR se definira kao vrijednost γ tako da je vjerojatnost da negativni prinos portfelja premaši γ nije veća od nekog malog broja ϵ (Pachamanova i Fabozzi, 2016):

$$VaR_{(1-\epsilon)}(\tilde{r}) = min\{\gamma | P(-\tilde{r} > \gamma) \leq \epsilon\} \tag{20}$$

U navedenom izrazu $\tilde{r}$ označava slučajnu varijablu koja predstavlja prinos portfelja, dok $-\tilde{r}$ predstavlja gubitke portfelja (negativne prinose). Na primjer, kada je $\epsilon = 0{,}05$, onda je $(1-\epsilon) = 0{,}95,\ 100(1-\epsilon)\% = 95\%$, odnosno 95% VaR, što je razina gubitaka portfelja koji neće biti premašeni s vjerojatnošću većom od 5%. VaR se temelji na pretpostavci da prinosi portfelja (pojedinačne imovine) slijede normalnu distribuciju podataka. U tom slučaju, vrijednost VaR-a je umnožak broja standardnih devijacija moguće distribucije prinosa portfelja, što predstavlja jednostavan izračun jer se percentili normalne distribucije prinosa mogu predstaviti izrazom koji uključuje srednju vrijednost i standardnu devijaciju distribucije (Pachamanova i Fabozzi, 2016):

$$VaR_{(1-\epsilon)} = \left(-\mu_r + q_{(1-\epsilon)} \times \sigma_r\right) \times V_t \tag{21}$$

[113] Percentil predstavlja raspon podijeljen na sto dijelova − centil (percentil).

Gdje μ_r predstavlja očekivani prinos, σ_r standardnu devijacija prinosa, V_t trenutnu vrijednost portfelja i $(1-\epsilon)$ je $100(1-\epsilon)$ percentil standardne normalne distribucije. Rizična vrijednost ima nekoliko ekvivalentnih interpretacija (Kisiala, 2015):

a) VaR je minimalni gubitak koji s određenom vjerojatnošću $(1-\epsilon)$ neće biti premašen;
b) VaR je $\epsilon - kvantil$[114] normalne distribucije slučajne varijable;
c) VaR je najmanji gubitak u $100(1-\epsilon)\%$ najgorem slučaju;
d) VaR je najveći gubitak u $\epsilon \times 100\%$ najboljem slučaju.

Pfaff (2016) navodi da VaR mjera rizika nije koherentna mjera rizika, odnosno da ne zadovoljava osnovne postulate koherentne mjere rizika, dok CVaR zadovoljava. Kisiala (2015), a prema Artzner, Delbaen, Jean-Marc i Heath (1999), navodi da koherentna mjera rizika zadovoljava četiri osnovna svojstva/aksioma:

a) Monotonost (engl. *monotonicity*) – veći gubici znače i veći rizik. Mjera rizika ρ je monotona ukoliko je za sve slučajne varijable X, Y:

$$X \leq Y \Rightarrow \rho(X) \leq \rho(Y)$$

b) Translacijska nepromjenjivost (engl. *translation equivariance*) – povećanje (smanjenje) gubitka povećava (smanjuje) rizik za istu veličinu. Mjera rizika ρ je translacijski nepromjenjiva ukoliko za svaku slučajnu varijablu X i konstantu c vrijedi:

$$\rho(X + c) = \rho(X) + c$$

c) Subaditivnost (engl. *subadditivity*) – diverzifikacija smanjuje rizik. Mjera rizika ρ je subaditivna ukoliko za sve slučajne varijable X, Y vrijedi:

$$\rho(X + Y) \leq \rho(X) + \rho(Y)$$

[114] Kvantil je zajednički naziv za percentile, decile i kvartile. To je mjera koja dijeli distribuciju na jednaka percentilna rastojanja.

d) Pozitivna homogenost (engl. *positive homogeneity*) – povećanje udjela imovine u portfelju povećava i rizik za istu veličinu. Mjera rizika ρ je pozitivno homogena ukoliko je za sve X, λ:

$$\rho(\lambda X) = \lambda \rho(X)$$

VaR kao mjera rizika, temeljen na pretpostavci normalne distribucije slučajne varijable, je suočen s brojnim problemima. Međutim, bez obzira na nedostatke, brojne ga financijske institucije i dalje koriste, ne razumijući ili zanemarujući njegove nedostatke. Naime, mjera rizika bi trebala omogućiti procjenu financijskog rizika u neobičnim situacijama koje se ne mogu prikazati uobičajenom distribucijom prinosa. Sukladno tome, mjeriti rizik koji se temelji na repovima distribucije vjerojatnosti preko vrijednosti standardne devijacije slučajne varijable, što predstavlja uobičajenu aproksimaciju VaR-a, nije zadovoljavajuća mjera rizika. Pored toga, VaR ne ukazuje na veličinu gubitka koja bi se mogla dogoditi ukoliko se dogodi negativni prinos male vjerojatnosti. Stoga, upotreba VaR-a kao granične veličine za odobravanje investicijske strategije, potencijalne investitore može izložiti ekstremnim gubicima. Također, s obzirom da VaR mjera ukazuje na gubitak pri određenom percentilu distribucije, ne razmatrajući veličinu gubitka u repu distribucije, potencijalni investitori mogu ući u pozicije s malom vjerojatnosti događanja, ali velikim utjecajima, odnosno posljedicama. Takvi se rizici ne prikazuju u procjenama VaR-a, ali mogu imati iznimno negativan učinak na portfelj te mogu zapravo destabilizirati cjelokupni financijski sustav, što je pokazao kolaps financijskog sustava u jesen 2008. godine (Pachamanova i Fabozzi, 2016). Isto tako, i Žiković (2005) ističe da je VaR suočen s tvrdnjama da su izračuni VaR-a previše neprecizni, te da nisu od posebne koristi, budući da različiti modeli daju značajno različite procjene veličine rizika, uz iste promatrane podatke. Trgo (2015) kao nedostatak navodi da VaR metode slabije funkcioniraju na nelikvidnim tržištima, što bi podrazumijevalo kontekst tržišta kriptovaluta, te da se temelje na povijesnim podacima, koji se ne moraju nužno ponavljati u budućnosti. Isti autor navodi da je nedostatak i to što VaR procjenjuje mogući gubitak na kraju razdoblja, a ne prikazuje rizik tijekom razdoblja držanja pozicije. Međutim, kao najveći nedostatak koji se pripisuje VaR-u predstavlja odsutnost subaditivnosti, što znači da nije sigurno da iznos VaR-a ukupnih pozicija

portfelja neće biti veći od sume VaR-a pojedinačnih pozicija koje čine portfelj (Žiković, 2005).

8.4.2. Uvjetna rizičnost vrijednosti (CVaR)

Mjera tržišnog rizika CVaR se definira kao očekivani gubitak koji premašuje mjeru rizične vrijednosti VaR za određeni interval pouzdanosti. Rockafellar i Uryasev (1999, 2000 i 2002) u nizu svojih radova predstavljaju model optimizacije portfelja s obzirom na uvjetnu rizičnost vrijednosti. Sinonimi za CVaR su srednja vrijednost gubitka (engl. *mean excess loss*), srednji gubitak (engl. *mean shortfall*) i rep VaR (engl. *tail VaR*). Za kontinuiranu distribuciju slučajne varijable koja predstavlja gubitak, CVaR je identičan očekivanom gubitku u repu distribucije (engl. *expected shortfall* - ES ili *expected tail loss* - ETL) (Pfaff, 2016). Kao što je navedeno prethodno, VaR nije koherentna mjera rizika, ali ES i CVaR predstavljaju koherentne mjere. S aspekta optimizacije, Rockafellar i Uryasev (2002) pokazuju da je CVaR konveksna funkcija, ali isto tako ukazuju da VaR nije konveksan, što može rezultirati portfeljem čiji se rezultat odnosi na lokalno, a ne globalno optimizacijsko rješenje. Za razliku od globalnog optimalnog rješenja koje predstavlja najbolje rješenje za bilo koju vrijednost vektora varijabli odluke u skupu svih izvedivih rješenja, lokalno optimalno rješenje je najbolje rješenje u „susjedstvu“ izvedivih rješenja. Drugim riječima, optimizacijom portfelja se ne postižu najbolje performanse preko varijabli odluke, odnosno udjela imovine u portfelju, nego se izvodi drugo ili treće najbolje rješenje. Zbog toga je jako važno poznavanje mogućnosti rješavača prilikom optimizacije, a koji odgovaraju prethodno postavljenoj ciljnoj funkciji, ograničenjima, kao i vrsti varijable odluke. Prema Pachamanova i Fabozzi (2016) neki opći optimizacijski problemi imaju "lijepu" strukturu u smislu da je lokalno optimalno rješenje zajamčeno globalno optimalno rješenje. To svojstvo imaju konveksni optimizacijski problemi u koje ulaze optimizacijski ciljevi korišteni u ovom radu. Autori također navode da problemi konveksnog programiranja obuhvaćaju nekoliko klasa problema s posebnom strukturom, uključujući linearno programiranje (engl. *linear programming* – LP) i kvadratno programiranje (engl. *quadratic programming* – QP). Linearno i kvadratno programiranje su metode implementirane u algoritme kojima se pokušava postići najbolji ishod (npr. maksimalni profit ili minimalni gubitak) u nekom matematičkom modelu uz određena ograničenja. Linearno programiranje se odnosi

na probleme optimizacije u kojima su i ciljna funkcija i ograničenja linearni izrazi u varijablama odluke, dok problemi kvadratnog programiranja imaju ciljnu funkciju koja je kvadratni izraz, a ograničenja su linearni izrazi u varijablama odluke (Pachamanova i Fabozzi, 2016).

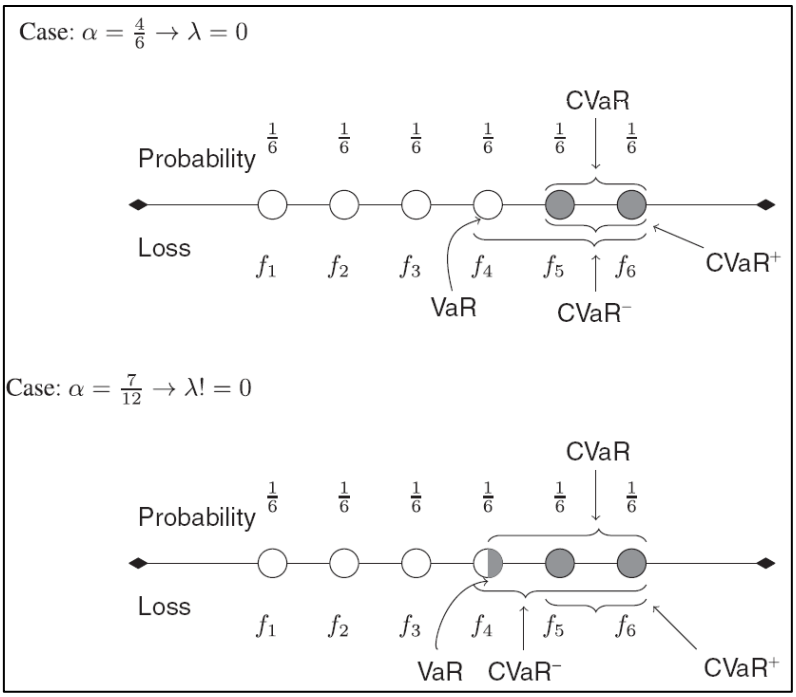
Izravna optimizacija s obzirom na CVaR je zahtjevna s numeričkog strane zbog ovisnosti CVaR-a o VaR-u (Pfaff, 2016). Da bi riješili ovu problematiku, Rockafellar i Uryasev (2002) su uveli raspon gubitaka u repu distribucije kao mjeru rizika, a zatim definirali CVaR kao njihov ponderirani prosjek, što je omogućilo izvođenje konveksne funkcije s obzirom na težine portfelja, kao varijable odluke. Uz to, ciljna funkcija se može optimizirati upotrebom tehnika linearnog programiranja, a također je primjenjiva za slučajne varijable koje ne prate normalnu distribuciju prinosa, što je važno svojstvo za ovaj rad, s obzirom da je u prethodnim radovima dokazano odsustvo normalne distribucije prinosa. U nastavku se navode mjere rizika potrebne kako bi se definirao CVaR (Pfaff, 2016):

a) $VaR_{(1-\epsilon)}$, $\epsilon - kvantil$ distribucije gubitaka;
b) $CVaR^{+}$, očekivani gubici koji striktno prelaze VaR (srednja vrijednost gubitaka u repu distribucije - ES);
c) $CVaR^{-}$, očekivani gubici koji slabo premašuju VaR (gubici koji su ili jednaki VaR-u, ili ga slabo premašuju). Ova je mjera poznata kao rep VaR.

Tada se CVaR definira kao ponderirani prosjek između $VaR_{(1-\epsilon)}$ i $CVaR^{+}$ (22):

$$CVaR = \lambda VaR + (1 + \lambda)CVaR^{+} \tag{22}$$

Gdje λ predstavlja udio/težinu $0 \leq \lambda \leq 1$ VaR-a u CVaR-u i dan je kao $\lambda = (\Psi(VaR) - \epsilon)/(1 - \epsilon)$, a $\Psi(\mathrm{VaR})$ predstavlja vjerojatnost da gubici ne premašuju, ili su jednaki VaR-u za dani interval pouzdanosti.



Shema 14. Diskretna distribucija gubitaka: VaR, CVaR, CVaR$^+$ i CVaR$^-$
Izvor: Pfaff (2016):

Shema 14. Ilustrira relaciju između mjera rizika za diskretnu distribuciju gubitaka (Pfaff, 2016). Na shemi je prikazano šest hipotetskih gubitaka s jednakom vjerojatnošću nastanka $f_1, \ldots, f_6$. Prvi slučaj se odnosi na razinu pouzdanosti $\epsilon = 4/6$ koja se podudara s VaR kvantilom, pa težina λ VaR-a u CVaR-u iznosi nula. Mjere rizika CVaR i CVaR$^+$ su u tom slučaju identične i jednake prosjeku gubitaka $f_5, \ldots, f_6$. Mjera VaR-a je dana kao gubitak f_4, a mjera rizika CVaR$^-$ kao prosjek ponderiran vjerojatnošću gubitaka f_4, f_5, f_6. U ovom odnosu, relacija između mjera rizika je dana kao VaR < CVaR$^-$ < CVaR = CVaR$^+$. Kada se razmatra drugi slučaj sa Sheme 14. prema kojem je razina pouzdanosti $\epsilon = 7/12$, vrijednost CVaR$^+$ je jednaka prethodnoj veličini. Međutim, u tom slučaju težina VaR-a iznosi $\lambda = 1/5$, tako da je uvjetna rizičnost vrijednosti jednaka:

$$CVaR = \frac{1}{5f_4} + \frac{2}{5f_5} + \frac{2}{5f_6}$$

U drugom slučaju, relacija između mjera rizika je dana kao VaR < CVaR$^-$ < CVaR < CVaR$^+$. Sukladno dobivenoj mjeri CVaR-a, moguće izvesti ciljnu funkciju. Pfaff (2016)

navodi da, iako postojanje (kontinuirane) funkcije multivarijatne distribucije prinosa portfelja, kao i postojanje gubitaka povezanima s distribucijom, ne predstavlja ključnu stvar, njihovo postojanje se pretpostavlja zbog notacijske pogodnosti. Neka se pretpostavi da prinos portfelja $\tilde{r}_p$ prati distribuciju vjerojatnosti s funkcijom gustoće f. U tom slučaju, $100(1-\epsilon)\%$ CVaR se može izraziti kao (23) (Pachamanova i Fabozzi, 2016):

$$CVaR_{(1-\epsilon)} = \frac{1}{\epsilon} \times \int_{-r \geq VaR_{(1-\epsilon)}} (-r) \times f(r)\ dr \tag{23}$$

Gdje pojam unutar integrala predstavlja očekivanu vrijednost gubitka portfelja (kao postotak uloženog iznosa) u repu distribucije. S obzirom na ograničenje mogućnosti optimizacije VaR-a kao ciljne funkcije, a prethodna jednakost to podrazumijeva jer je potrebno prvotno izračunati optimalnu veličinu VaR-a da bi se dobila veličina CVaR-a, Rockafellar i Uryasev (2000) predlažu upotrebu pomoćne ciljne funkcije umjesto CVaR-a koja ima bolja svojstva za izračun (24):

$$F_{1-\epsilon}(\mathrm{w}, \xi) = \xi + \frac{1}{\epsilon} \times \int_{-r \geq \xi} (-r - \xi) \times f(r)\ dr \tag{24}$$

Gdje ξ predstavlja očekivanu vrijednost gubitka. Minimizacijom prethodne funkcije mijenjanjem veličina w i ξ, minimalna vrijednost funkcije je zapravo jednaka $100(1-\epsilon)\%$ CVaR-u, bez prethodnog poznavanja VaR veličine (Pfaff, 2016). Drugim riječima, vrijednost ξ u optimalnom rješenju će zapravo biti jednaka VaR-u portfelja, s optimalnim ponderima utvrđenim optimizacijom ciljne funkcije CVaR-a, ali ponderi portfelja koji rezultiraju minimalnim CVaR-om ne moraju nužno biti ponderi portfelja koji rezultiraju minimalnim VaR-om. Optimizacija u praksi uključuje scenarije vjerojatnosti određenog ishoda slučajne varijable, odnosno prinosa pojedinog financijskog instrumenta. Međutim, s obzirom da se optimizacija najčešće provodi na povijesnim podacima, svakom povjesnom prinosu se pridružuje jednaka vjerojatnost nastanka. Uvođenjem dodatnih varijabli odluke $y_i = y_1, \ldots, y_N$ po jednu za svaki mogući ishod (očekivani prinos portfelja), problem minimizacije CVaR-a koji je

korišten u ovom radu, te izražen diskretnim izrazima, može se zapisati kao (25) (Pachamanova i Fabozzi, 2016):

$$\begin{aligned} & \min_{w,\xi,y} \quad \xi + \frac{1}{[\epsilon \times N]} \times \sum_{i=1}^{N} y_i \\ podložno\ ograničenjima \quad & y_i \geq -\left(r^{(i)}\right)' w - \xi, \quad i = 1, \dots, N \\ & w'\iota = 1 \\ & w_i \geq 0, \ \ i = 1, \dots, N \end{aligned} \tag{25}$$

Nedostatak relacije (18), odnosno M-V modela je pretpostavka normalne distribucije prinosa imovine portfelja za kojeg se procjenjuju parametri. S obzirom na rezultate istraživanja Briere et al. (2015) i Lee Kuo Chuen et al. (2018) gdje su prezentirani dokazi o prisutnosti distribucije s teškim repovima (engl. *heavy-tailed*) prinosa kriptovaluta, prethodne postavke optimizacije (25) odgovaraju optimizaciji korištenoj u radu Petukhina et al. (2018) i Eisl (2015), odnosno metodologiji koja prati rad Rockafellar i Uryasev (2000), sa razinom pouzdanosti od 95%. U tom slučaju za mjeru rizika se koristi više pouzdana mjera uvjetna rizičnost vrijednosti (engl. *Conditional Value at Risk* – CVaR), tako da model srednje vrijednosti i varijance, konceptualno prelazi u model srednje vrijednosti i uvjetne rizičnosti vrijednosti (engl. *Mean-Conditional Value at Risk* M-CVaR).

8.5. Portfelj s maksimalnim Sharpe i STARR omjerom

Osnovna Markowitz relacija (18) minimizira varijancu prinosa portfelja s obzirom na zadani očekivani prinos. S druge strane, stavljajući u odnos očekivani prinos portfelja (korigiran za nerizičnu kamatnu stopu u istom periodu promatranja) i standardnu devijaciju portfelja, dobit će se Sharpe ratio, odnosno omjer koji ukazuje koliko se dodatnog prinosa dobije po preuzetoj jedinici rizika. Uz uvjet racionalnog investiranja, promjenom tolerancije investitora prema riziku, investitori će očekivati viši očekivani prinos za preuzetu dodatnu jedinicu rizika. U tom se slučaju provodi optimizacijski cilj maksimalizacije prinosa za danu razinu rizika. Portfelji koji za danu razinu rizika imaju najviši očekivani prinos kreiraju efikasnu granicu mogućih portfelja, a portfelj koji ima

najviši Sharpe omjer predstavlja optimalan portfelj, odnosno tangentni portfelj korišten u ovom radu (26).

$$\begin{aligned} \max_{w} \quad & \left\{\frac{w'\mu}{\sqrt{\mathrm{w}'\Sigma\mathrm{w}}}\right\} \\ podložno\ ograničenjima \quad & w'\iota = 1 \\ & w_i \geq 0, \;\; i = 1, \dots, N \end{aligned} \tag{26}$$

Za potrebe ovog istraživanja nerizična kamatna stopa je izostavljena što je vidljivo iz jednakosti (26) i (27). Ukoliko se u nazivniku izraza (26) umjesto standardne devijacije kao mjera rizika koristi CVaR, Sharpe omjer prelazi u stabilni omjer prilagođen repovima distribucije (engl. *Stable Tail-Adjusted Return Ratio* – STARR) i dan je izrazom (27). Optimizacijski cilj je maksimalizacija STARR omjera s razinom pouzdanosti od 95%.

$$\begin{aligned} \max_{w} \quad & \left\{\frac{w'\mu}{\mathrm{CVaR}_{\epsilon}(w)}\right\} \\ podložno\ ograničenjima \quad & w'\iota = 1 \\ & w_i \geq 0, \;\; i = 1, \dots, N \end{aligned} \tag{27}$$

8.6. Portfelj s maksimalnim prinosom

U suprotnosti sa strategijom koja minimizira rizik, u radu se provodi i optimizacijska strategija koja maksimizira očekivani prinos portfelja, odnosno ne uključuje unaprijed definiranu razinu rizika. U tom slučaju optimizacijski algoritam ne uzima u obzir matricu varijanci i kovarijanci, nego koristi prosječne prinose prethodnog perioda za procjenu najvišeg očekivanog prinosa portfelja u sljedećem periodu. Imovina portfelja s najvišim prosječnim prinosom prethodnog perioda ostvarit će najviši udio u portfelju u budućem periodu. Zbog toga što strategija ne razmatra rizik kao input u optimizaciji, smatra se visokorizičnom. Korištena formulacija u ovom radu za maksimalizaciju očekivanog prinosa je dana izrazom (28).

$$\begin{aligned} \max_{w} \quad & \mu_p\,(w) = w'\mu \\ podložno\ ograničenjima \quad & w'\iota = 1 \end{aligned} \tag{28}$$

$$w_i \geq 0, \;\; i = 1, \ldots, N$$

Gdje je μ_p očekivani prinos portfelja.

8.7. Mjere uspješnosti kreiranih portfelja

Za ocjenu uspješnosti pojedine optimizacijske strategije u radu su prezentirani rezultati više različitih apsolutnih i relativnih mjera uspješnosti: Sharpeov omjer (Sharpe, 1963), MSquared omjer (Modigliani & Modigliani, 1997), regresijska alfa, Jensenova alfa (Jensen, 1968), Treynorov omjer (Treynor, 1965) i informacijski omjer (Bacon, 2008), pri čemu su vrijednosti za izračun iskazane na godišnjoj razini i odnose se na ukupnu vremensku seriju prinosa portfelja dobivenih optimizacijom. Za izračun ostvarenog prinosa portfelja je korišten godišnji prosječni geometrijski prinos: $R_{Gi} = prod(1 + R_{di})^{\frac{scale}{n}} - 1$, gdje je R_{di} dnevni ostvareni prinos promatranog portfelja i u vremenu t, n ukupan broj postojećih opservacija i $scale$ broj opservacija u godini 252. Standardna devijacija, VaR and CVaR su iskazane godišnje izrazom $risk_{a,i} = risk_{d,i} \times \sqrt{252}$, gdje je $risk_{d,i}$ mjera rizika dnevnih prinosa. Ukoliko se iz izračuna izostavi nerizična kamatna stopa u svojstvu indikatora oportunitetne profitabilnosti, Sharpe ratio SR korišten u ovom radu je dan izrazom (29).

$$SR = \frac{R_{Gi}}{\sigma_{ai}} \tag{29}$$

Osim rangiranja investicijskih mogućnosti, Sharpe omjer ne pruža dodatne informacije. Samo za investicije s jednakom razinom rizika, Sharpe omjer točno ukazuje koliko je jedna investicija bolja u odnosu na drugu. Mjera koja ispravlja taj nedostatak je MSquared M^2 (30) koja ukazuje na razliku omjera prinosa i rizika između investicija, bez obzira na razinu rizika. Nerizična kamatna stopa je izostavljena.

$$M^2 = R_{Gi} \times \frac{\sigma_{aM}}{\sigma_{ai}} \tag{30}$$

Gdje je σ_{aM} godišnja standardna devijacija tržišta, u ovom slučaju CRIX indeksa ili neke druge kriptovalute kao indikatora profitabilnosti. Komparacijom vrijednosti gornjih mjera se mogu dobiti informacije o superiornosti jedne strategije u odnosu na drugu na tržištu kriptovaluta. Međutim, gornje mjere su izračunate unutar uzorka (engl. *in the sample*), odnosno na ukupnom uzorku podataka. U tom smislu rezultati ukazuju na prosječne vrijednosti mjera izračunate na prinosima portfelja pojedine optimizacijske strategije. U funkciji razmatranja investicijskih mogućnosti, poželjno je razmotriti i rezultate modela linearne regresije (31) između vremenskih serija prinosa portfelja kao zavisnih varijabli i prinosa CRIX indeksa, ili neke druge kriptovalute, kao nezavisne varijable koja predstavlja tržišni indikator (engl. *benchmark*), s obzirom da je procijenjena vrijednost nagiba pravca ulazni parametar za Treynorov omjer (32) i Jensenovu alfu (33).

$$R_{di} = a_i + \beta_i \times R_{dM} + \epsilon_i \tag{31}$$

Gdje je a_i regresijski odsječak – alfa, β_i nagib pravca regresije - beta, R_{dM} dnevni ostvareni prinos tržišta (CRIX indeksa ili drugog indikatora profitabilnosti) i ϵ_i rezidualna odstupanja od pravca. Zamjenom standardne devijacije u izrazu (29) za procijenjenu vrijednost nagiba pravca regresijske jednadžbe $\bar{\beta}_i$ kao mjere rizika volatilnosti, dobit će se Treynorov omjer TR, mjera korištena u ovom radu (32).

$$TR = \frac{R_{Gi}}{\bar{\beta}_i} \tag{32}$$

U sklopu Modela za određivanje cijene kapitalne imovine (engl. *capital asset pricing model* – CAPM), vrijednost nagiba pravca iz (31) je procijenjena veličina regresijske jednadžbe s kojim se povezuje rizik potencijalne investicije s ravnotežnim očekivanim prinosom rizičnog ulaganja. Ukoliko je potencijalna investicija više varijabilna u odnosu na tržište, racionalni investitori će očekivati premiju na svoje ulaganje kao kompenzaciju za viši preuzeti rizik, pa će procijenjeni nagib pravca $\bar{\beta}_i$ biti iznad jedan. Osnovna relacija CAPM modela ukazuje da je očekivana stopa prinosa na investiciju jednaka nerizičnoj kamatnoj stopi uvećanoj za premiju rizika tržišnog portfelja (standard usporedbe) koja je korigirana s njenim sistematskim rizikom, odnosno $\bar{\beta}_i$. Pored toga, CAPM model zanemaruje postojanje specifičnog rizika investicije ϵ_i,

odnosno uvažava samo njen sistematski rizik koji proizlazi iz kretanja cijelog tržišta. Preuređenjem osnovne jednadžbe CAPM modela, može se izvesti izraz (33) koji predstavlja Jensenovu alfu, mjeru korištenu u ovom radu. Jensenova alfa predstavlja mjeru čija vrijednost ukazuje je li investicija ostvarila viši ili niži prinos od očekivanog, odnosno zahtijevanog prinosa po CAPM relaciji. Uz pretpostavku adekvatne aproksimacije kretanja tržišta kriptovaluta CRIX indeksom ili nekom drugom varijablom, ukoliko su Jensenove alfe portfelja pozitivne veličine, može se reći da je optimizacijska strategija pobijedila tržište jer je ostvarila viši prinos nego što to zahtijeva CAPM model. U izrazu (33) nerizična kamatna stopa je izostavljena.

$$\alpha_i = R_{Gi} - \beta_i \times R_{GM} \tag{33}$$

Gdje je R_{GM} ostvareni godišnji prosječni geometrijski prinos CRIX indeksa. Zadnja mjera performansi korištena u ovom radu je informacijski omjer IR (34). Informacijski omjer je relativna mjera koja stavlja u omjer razliku između godišnjeg prosječnog geometrijskog prinosa portfelja i CRIX indeksa (ili drugog indikatora profitabilnosti) kao aktivne premije (engl. *active premium*) i godišnju standardnu devijaciju aktivne premije između prinosa portfelja i CRIX indeksa (engl. *trackin error*). Ukoliko je IR pozitivna vrijednost, to bi značilo da je optimizacijska strategija ostvarila bolje rezultate od CRIX indeksa (ili drugog indikatora profitabilnosti) koji aproksimira kretanje tržišta kriptovaluta.

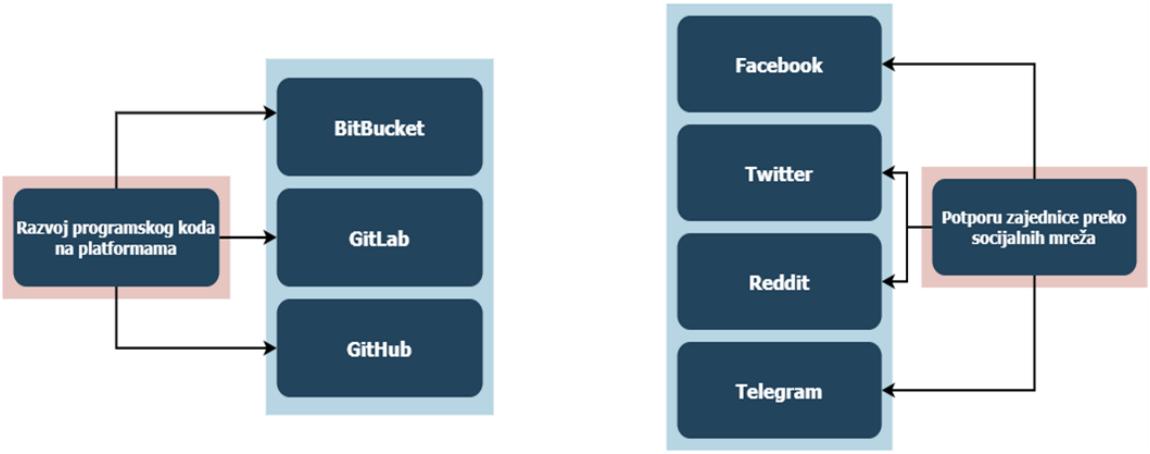
$$IR = \frac{R_{Gi} - R_{GM}}{\sigma_{iM}} \tag{34}$$

Gdje je σ_{iM} standardna devijacija aktivne premije između prinosa portfelja i CRIX indeksa. Osim gore navedenih, u radu je i prezentiran kumulativni prinos portfelja pojedinačnih optimizacijskih strategija i CRIX indeksa uz pretpostavku inicijalnog ulaganja od 1 jedinice valute, kao i njihov najveći gubitak (engl. *worst drawdown*) u odnosu na najvišu vrijednost kumulativnog prinosa u promatranom razdoblju.

8.8. Odabir uzorka kriptovaluta

Kriptovalute najčešće predstavljaju različite startupove, odnosno njihove projekte. Zbog toga bi se moglo zaključiti da i njihova fundamentalna vrijednost mora biti povezana s prihodovnom stranom startupa. Međutim, odnos fundamentalne vrijednosti kriptovalute i uspješnosti projekta, ne mora niti postojati. Naime, rijetko koji startupi praktično provode svoje projekte u kojima kriptovalute ispunjavaju svoju fundamentalnu svrhu jer je velika većina još uvijek u razvojnoj fazi. Isto tako, jedan dio startupova zapravo niti nema za krajnji cilj kontinuirano ostvarivanje prihoda, čime se otežava njihova procjena fundamentalne vrijednosti. Njihova namjera je kroz tržišno povećanje vrijednosti kriptovalute ostvariti sredstva dostatna za njihovo operativno poslovanje. Također, kriptovalute nisu i ne moraju biti isključivo vezane za poslovni uspjeh startupa. Kriptovalute se baziraju na otvorenom programskom kodu koji je slobodan za javnost i nalazi se na nekoj od platformi za kolaboraciju razvojnih programera. Nakon što blockchain postane aktivan i javan, korisnici i razvojni programeri većim djelom utječu na njegov uspjeh, razvojem i implementacijom programskog koda. U tom su slučaju transakcijske naknade i novo kreirane kriptovalute osnovni i dostatni poticaji za održavanje jedne takve decentralizirane mreže, čineći javni blockchain samoodrživim transakcijskim sustavom.

Sa aspekta investitora, navedene karakteristike infrastrukture blockchaina predstavljaju problem procjene fundamentalne vrijednosti. Zbog toga što se kriptovalute ne mogu povezati s okvirom fundamentalnih indikatora pripadne djelatnosti, niti s okvirom postojećih sistematskih faktora financijskih instrumenata tradicionalnog tržišta kapitala, te zbog odsutnosti matematičkog izraza za izračun barem teorijske vrijednosti koja bi služila kao stabilizator cjenovnog momentuma pojedine kriptovalute, potrebno je definirati nove okvire indikatora koji bi potencijalno mogli utjecati na selekciju kriptovaluta kao sastavnica portfelja investitora. Indikatori koji utječu na odabir kriptovaluta kao sastavnica korišteni u ovom radu predstavljaju metriku vrednovanja fundamentalnih pokazatelja dostupnim na stranicama CoinGecko. Metrika trenutno prati razvoj programskog koda na platformama: GitHub, GitLab i Bitbucket, te potporu zajednice preko socijalnih mreža: Facebook, Twitter, Reddit i Telegram.



Shema 15. CoinGecko metrika
Izvor: Izrada autora

Prvih dvadeset kriptovaluta koje kumulativno ostvaruju najviši broj bodova su odabrane kao sastavnice oba seta portfelja, osim prilikom ispitivanja prve hipoteze gdje je bitcoin (BTC) isključen jer predstavlja mjernu jedinicu vrijednosti. Ostale varijable od interesa predstavljaju kriptovalute koje se mogu klasificirati kao platežne kriptovalute, tj. kao poboljšane verzije bitcoina i kriptovalute koje predstavljaju decentralizirane kompjuterske platforme. U kategoriju platežnih kriptovaluta ulaze: bitcoin cash (BCH – kriptovaluta nastala 2017. god. račvanjem bitcoin transakcijskog protokola, te se prvenstveno koristi u platežne svrhe), ripple (XRP – kriptovaluta koja se koristi u platežne svrhe na digitalnoj platežnoj platformi RippleNet), litecoin (LTC – platežna kriptovaluta nastala 2011. god. kao poboljšanje bitcoin protokola), monero (XMR – predstavlja prvu kriptovalutu koja pruža privatnost prilikom transakcija, kreirana je 2014. godine), dash (DASH – kriptovaluta nastala 2014. god. kao poboljšana verzija bitcoina i koristi se samo u platežne svrhe), zcash (ZEC – druga kriptovaluta čiji je fokus na privatnost transakcija, nastala 2016. godine), binance coin (BNB – kriptovaluta kreirana prvo kao utilizacijski token ERC-20 Binance burze, a onda prebačena u omjeru 1:1 na svoj matični blockchain), iota (MIOTA – kriptovaluta kreirana na platformi za izvršavanje transakcija između IoT uređaja), dogecoin (DOGE – platežna kriptovaluta, nastala račvanjem litecoin kriptovalute 2013. godine) i 0x (ZRX - infrastrukturni protokol koji omogućava korisnicima da lako trguju ERC-20 tokenima i drugom imovinom na Ethereum transakcijskoj mreži).

Kriptovalute koje predstavljaju decentralizirane kompjuterske platforme čine: ethereum (ETH – kriptovaluta nastala 2015. god. s pokretanjem najpoznatije decentralizirane platforme Ethereum), eos (EOS – kriptovaluta nastala kao projekt startupa Block One koji je implementirao dokaz o ulogu konsenzus algoritam i imao najdulji proces financiranja u povijesti u trajanju od jedne godine, čime je prikupljeno više od 4 milijarde dolara), neo (NEO – kriptovaluta inicijalno poznata kao antshares, pokrenuta 2014. god. kao prvi kineski javni blockchain), cardano (ADA – kriptovaluta osnovana 2017. godine, također na dokaz o ulogu konsenzus algoritmu kao i EOS, s ciljem postizanja veće učinkovitosti i nižih troškova decentralizirane mreže), stellar (XLM – je kiptovaluta nastala kao račvanje platežne kriptovalute ripple 2014 godine zbog razilaženja u smjeru razvoja Ripple protokola vodećih ljudi projekta), waves (WAVES – je razvijen 2016. godine od strane ukrajinskih znanstvenika kao višenamjenska blockchain platforma koja podržava decentralizirane aplikacije i pametne ugovore), qtum (QTUM – kriptovaluta kreirana na platformi koja koristi dokaz o ulogu konsenzus algoritam, sa poboljšanom verzijom Bitcoin transakcijskog sustava, u smislu funkcionalnošću izvršenja pametnih ugovora), nem (XEM – predstavlja kriptovalutu izgrađenu na ekosustavu platformi koje koriste blockchain i kriptografiju za pružanje rješenja za tvrtke i pojedince) i ethereum classic (ETC – kriptovaluta nastala 2016. god. kao račvanje Ethereum transakcijskog sustava, s glavnom funkcijom izvršavanja pametnih ugovora i podrškom decentraliziranim aplikacijama).

9. REZULTATI

9.1. Deskriptivna statistika prinosa kriptovaluta

Razdoblje u kojem će se razmotriti bitcoin kao obračunska jedinica korisnosti ulaganja predstavlja period od 18. listopada 2018. god. do 24. rujna 2020. god., što čini ukupno 1.071 dnevnu opservaciju, odnosno 1.070 dnevnih prinosa. U razmatranju mjera centralne tendencije, srednja vrijednost dnevnih prinosa kriptovaluta izraženih u bitcoin jedinicama vrijednosti, sugerira da su samo kriptovalute LTC, DASH, ZEC, QTUM i ETC ostvarile negativnu aritmetičku sredinu, sve druge kriptovalute su ostvarile pozitivnu srednju vrijednost u promatranom razdoblju. Najvišu srednju vrijednost je ostvarila kriptovaluta BNB u visini od 0,0281 što je očekivano s obzirom na njenu cjenovnu dinamiku. S druge stane, sve kriptovalute su ostvarile negativne medijane, odnosno centralne vrijednosti. Najniži medijan je ostvarila kriptovaluta ZRX, a drugi najniži kriptovaluta ZEC. Iako je većina kriptovaluta ostvarila pozitivne srednje vrijednosti prinosa, promatrano razdoblje karakteriziraju ipak negativni prinosi, što sugerira najčešće ponavljana vrijednost mod, gdje je od ukupno devetnaest kriptovaluta, čak njih petnaest ostvarilo negativan najčešće dobiveni prinos.

Tablica 4. Vrijednosti deskriptivne statistike (DS) dnevnih prinosa – valuta BTC
(I. dio)

Mjere DS	ETH	EOS	XRP	BCH	LTC	NEO	XMR	ADA	XLM	DASH	ZEC	BNB
Min	-0,2437	-0,3217	-0,2892	-0,3025	-0,2091	-0,2195	-0,1929	-0,3390	-0,3576	-0,2812	-0,3110	-0,6397
Medijan	-0,0021	-0,0014	-0,0032	-0,0041	-0,0032	-0,0034	-0,0017	-0,0034	-0,0038	-0,0040	-0,0050	-0,0011
Aritmet. Sredina	0,00	0,0022	0,0008	0,0004	-0,0001	0,0001	0,0001	0,0023	0,0014	-0,0009	-0,0010	0,0281
Mod	-0,0368	-0,0185	-0,0424	-0,0402	-0,0341	-0,0573	-0,0278	-0,0187	-0,1242	-0,0220	-0,0155	-0,6396
Max	0,2895	0,4261	0,7730	0,6461	0,4564	0,4259	0,3480	1,2943	0,5544	0,6859	0,2948	25,392
Varijanca	0,0012	0,0030	0,0032	0,0031	0,0016	0,0023	0,0015	0,0047	0,0030	0,0023	0,0020	0,6091
St. Dev.	0,0343	0,0547	0,0570	0,0560	0,0404	0,0480	0,0391	0,0688	0,0548	0,0480	0,0449	0,7804
Simetričnost	0,7956	1,9822	5,2366	3,1032	3,4521	2,0138	1,8003	8,2589	2,6842	4,4141	1,0835	32,13
Kurtozis	9,8730	14,15	56,23	27,85	32,66	14,79	15,73	103,37	24,01	55,76	8,6686	1041,6

Izvor: Izrada autora

Tablica 4. Vrijednosti deskriptivne statistike (DS) dnevnih prinosa – valuta BTC (II. dio)

Mjere DS	MIOTA	WAVES	QTUM	DOGE	ZRX	XEM	ETC
Min	-0,2567	-0,1734	-0,3024	-0,2094	-0,2686	-0,3623	-0,3118
Medijan	-0,0039	-0,0045	-0,0046	-0,0028	-0,0053	-0,0043	-0,0035
Aritmet. sredina	0,00	0,0002	-0,0007	0,0015	0,0016	0,0008	-0,0002
Mod	-0,0736	-0,0514	-0,0221	-0,0187	0,0057	-0,0103	-0,036
Max	0,4479	0,5039	0,7537	0,5249	0,5289	1,8411	0,3769
Varijanca	0,0026	0,0029	0,0033	0,0028	0,0037	0,0058	0,0023
St. Dev.	0,0512	0,0541	0,057	0,0526	0,0607	0,0762	0,0480
Simetričnost	2,1157	2,2784	4,4017	3,4514	1,7957	13,66	0,8296
Kurtozis	15,12	15,85	48,82	27,27	10,17	319,5	10,32

Izvor: Izrada autora

Razmatranje mjere disperzije, u kontekstu minimalnih i maksimalnih vrijednosti, kao i varijance, odnosno standardne devijacije dnevnih prinosa kriptovaluta, sugerira da se radi o izrazito varijabilnoj, odnosno rizičnoj imovini. Najviši raspon između min i max vrijednosti ostvarila je kriptovaluta BNB, kao i standardnu devijaciju dnevnih prinosa u visini od 0,7804. Najmanji raspon je ostvario WAVES, a najnižu standardnu devijaciju ETH u visini od 0,0343. Ukoliko se razmotri vrijednost koeficijenta zaobljenosti distribucije prinosa kao mjere normalnosti, vrijednosti ukazuju na izrazito visoku leptokurtičnost, sve vrijednosti koeficijenta zaobljenosti su više od 3, što sugerira veću frekvenciju ekstremnih vrijednosti nego što se pretpostavlja po dinamici normalne distribucije. Jednako tako, i mjera simetrije distribucije ukazuje na odstupanje dnevnih prinosa od normalne distribucije. Sve vrijednosti su pozitivne veličine u rasponu od 0,80 do čak 32 za kriptovalutu BNB, što ukazuje na pozitivnu nakrivljenost, odnosno krivulja distribucije je dulja u svom desnom repu distribucije, što sugerira više pozitivne prinose za pojedine kriptovalute, nego što se pretpostavlja po normalnoj distribuciji. Upravo dobiveni rezultati koji značajno odstupaju od pretpostavljene normalne distribucije prinosa, utjecali su dodatnu primjenu uvjetne rizičnosti vrijednosti CVaR-a kao mjere rizika, čime se želi premostiti opisane nedostatke distribucije prinosa kriptovaluta.

Razdoblje za procjenu značaja fundamentalnih indikatora u kontekstu ispitivanja druge hipoteze rada, odnosno koje pokriva svih dvadeset kriptovaluta je od 25. siječnja 2018. god. do 1. kolovoza 2019. god., što čini uzorak od ukupno 554 dnevnih

opservacija, odnosno 553 dnevnih prinosa. S ciljem potvrđivanja, odnosno opovrgavanja druge hipoteze rada, u istraživanje se uključuje CRIX indeks, kao indikator profitabilnosti. Mjera centralne tendencije, srednja vrijednost dnevnih prinosa kriptovaluta izraženih u paritetu s američkim dolarom, ukazuje da je čak sedamnaest kriptovaluta ostvarilo negativnu aritmetičku sredinu, a samo su tri kriptovalute ostvarile pozitivne vrijednosti.

Tablica 5. Vrijednosti deskriptivne statistike (DS) dnevnih prinosa – valuta USD (I. dio)

Mjere DS	BTC	ETH	EOS	XRP	BCH	LTC	NEO	XRM	ADA	XLM	DASH	ZEC
Min	-0,1597	-0,1869	-0,1944	-0,1714	-0,3361	-0,1533	-0,2335	-0,1891	-0,1880	-0,1691	-0,1945	-0,1707
Medijan	0,0017	-0,0008	0,00	-0,0033	-0,0040	-0,0028	-0,0022	-0,0006	-0,0050	-0,0038	-0,0023	-0,0058
Aritmet. Sredina	0,0006	-0,0015	0,00	-0,0011	-0,0006	0,0004	-0,0025	-0,0009	-0,0025	-0,0021	-0,0022	-0,0021
Mod	-0,0078	0,0008	0,00	-0,0687	-0,0232	-0,0196	0,00	0,0207	-0,0221	0,0421	0,00	-0,338
Max	0,1736	0,1807	0,4150	0,3799	0,5121	0,3373	0,2863	0,1927	0,2783	0,2125	0,3334	0,2302
Varijanca	0,0016	0,0026	0,0045	0,0030	0,0048	0,0030	0,0038	0,0030	0,0036	0,0030	0,0029	0,0029
St. Dev.	0,0398	0,0508	0,0674	0,0550	0,0695	0,0549	0,0617	0,0549	0,0601	0,0543	0,0537	0,0540
Simetričnost	0,0257	-0,0800	1,0458	1,2273	1,3055	1,0177	0,3862	0,0402	0,4873	0,2472	0,6497	0,3786
Kurtozis	2,5042	1,6526	5,6271	6,7480	9,6575	5,1638	2,3916	1,6071	2,0579	1,3274	5,2499	1,6998

Tablica 5. Vrijednosti deskriptivne statistike (DS) dnevnih prinosa – valuta USD (II. dio)

Mjere DS	BNB	MIOTA	WAVES	QTUM	DOGE	ZRX	XEM	ETC	CRIX
Min	-0,2069	-0,2169	-0,2243	-0,2157	-0,2037	-0,2895	-0,2072	-0,2144	-0,1856
Medijan	0,00	-0,0041	-0,0038	-0,0028	-0,0020	-0,0052	-0,0015	0,00	0,0018
Aritmet. sredina	0,0029	-0,0019	-0,0014	-0,0026	-0,0001	-0,0012	-0,0030	-0,0012	-0,0002
Mod	0,00	0,00	0,00	0,00	0,00	0,00	-0,1149	0,00	0,00
Max	0,2587	0,2523	0,4662	0,5052	0,4953	0,3084	0,2992	0,2783	0,1727
Varijanca	0,0029	0,0038	0,0041	0,0042	0,0034	0,0048	0,0037	0,0032	0,0018
St. Dev.	0,0543	0,0617	0,0644	0,0651	0,0582	0,0691	0,0607	0,0568	0,0424
Simetričnost	0,4224	0,1746	1,2348	1,1142	1,8350	0,4368	0,6018	0,2095	-0,2066
Kurtozis	2,6061	1,6365	8,2035	7,9890	12,3944	2,2354	3,5165	2,8984	2,4115

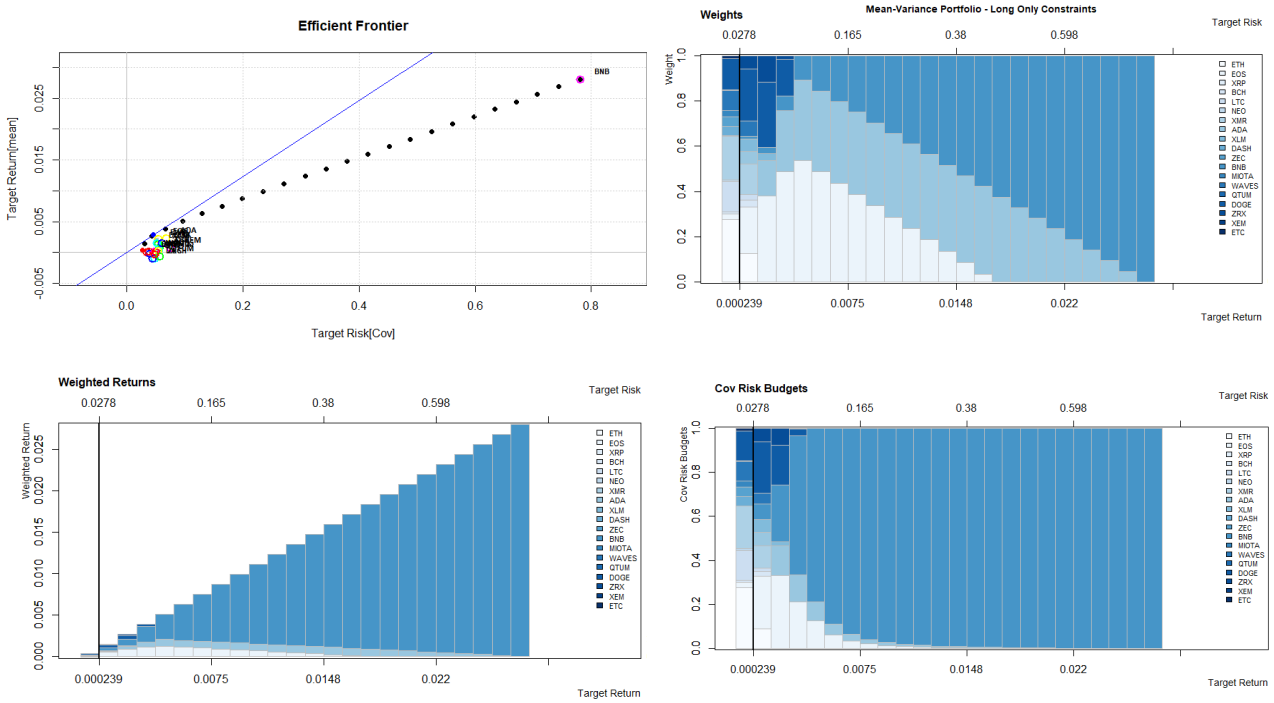
Izvor: Izrada autora

Najnižu dnevnu srednju vrijednost je ostvarila kriptovaluta XEM u visini od -0,0030, a najvišu kriptovaluta BNB u visini od 0,0029. Sukladno tome, samo je pet kriptovaluta ostvarilo pozitivne medijane. Najniži dnevni medijan je ostvarila kriptovaluta ZEC koji

iznosi -0,0058, dok je najviši medijan ostvario CRIX indeks čija je visina 0,0018, što je indikativno za očekivane rezultate rada. Razmatranje disperzije dnevnih prinosa u kontekstu minimalnih i maksimalnih vrijednosti, kao i varijance, odnosno standardne devijacije dnevnih prinosa kriptovaluta, također sugerira izrazito rizičnu dinamiku prinosa. Najviši raspon između min i max vrijednosti, kao i standardnu devijaciju dnevnih prinosa je ostvarila kriptovaluta BCH, u rasponu od od -0,3361 do 0,5121, a standardnu devijaciju u visini od 0,0695. S druge strane, najmanji raspon min i max vrijednosti, a posljedično i najmanju standardnu devijaciju u visini od 0,0398 je ostvario BTC. Razmatrajući vrijednost zaobljenosti distribucije prinosa kao mjere normalnosti distribucije, devet kriptovaluta je ostvarilo vrijednost višu od 3, što ukazuje veću frekvenciju ekstremnih vrijednosti nego što se pretpostavlja po dinamici normalne distribucije. Suprotno, jedanaest kriptovaluta, uključujući i CRIX, je ostvarilo vrijednost zaobljenosti nižu od 3, što sugerira spljoštenu, mezokurtičnu distribuciju, tj. njeno odstupanje od normalne distribucije. Jednako tako, sve kriptovalute, osim ETH, su ostvarile pozitivnu mjeru simetrije, što ukazuje na pozitivnu nakrivljenost i ekstremne prinose. S druge strane, kriptovaluta ETH je ostvarila negativnu nakrivljenost, što ukazuje na ekstremno visoke negativne prinose. Jedino je kriptovaluta BTC ostvarila mjeru simetrije u visini od 0,0257, što je najbliže normalnoj distribuciji podataka. S obzirom na takve rezultate, uključena je mjera uvjetne rizičnosti vrijednosti, s ciljem ispitivanja drugih mogućnosti prilikom optimizacije.

9.2. Rezultati optimizacije portfelja unutar uzorka – valuta BTC

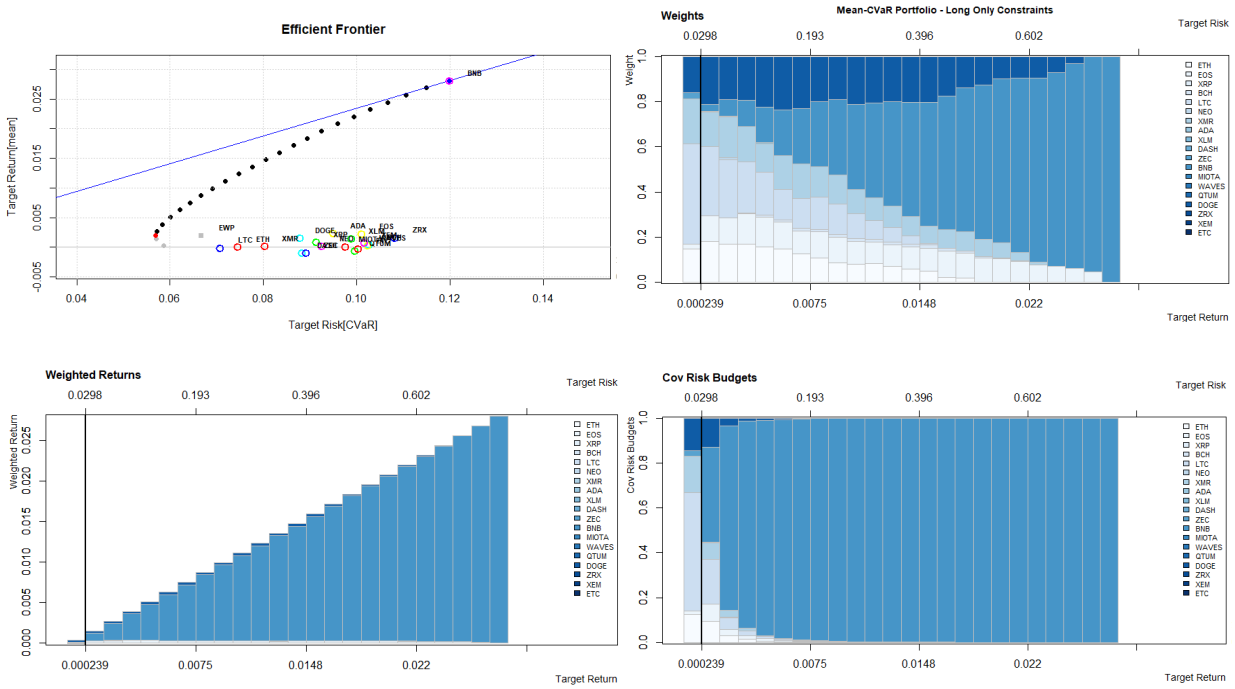
Ilustracija rezultata konstrukcije efikasne granice kreirane od kriptovaluta denominiranih u bitcoin kriptovaluti kao obračunskoj jedinici korisnosti ulaganja prezentirana je Grafikonom 2. U promatranom periodu daleko najviši očekivani prinos, ali i rizik izražen kao standardna devijacija, unutar ukupnog razdoblja promatranja je ostvarila kriptovaluta BNB. Zbog prinosa, ali i rizika BNB kriptovalute, efikasna granica pokriva šire područje, odnosno u koordinatnom sustavu grupira očekivane rezultate odnosa prinosa i rizika pojedinačnih kriptovaluta, što je prikazano na gornjem lijevom dijelu Grafikona 2. Promjenom tolerancije prema riziku, efikasna granica je izvedena kroz 25 mogućih kombinacija kriptovaluta, odnosno portfelja unutar uzorka koje predstavljaju moguće optimizacijsko rješenje adekvatno maksimiziranom odnosu prinosa i rizika.



Grafikon 2. Ilustracija efikasne granice – mjera rizika varijanca – valuta BTC

Izvor: Izrada autora

Efikasna granica je izvedena između portfelja s minimalnim rizikom MinVar-B i portfelja s maksimalnim očekivanim prinosom MaxMean-B, odnosno u rasponu standardne devijacije u visini od 0,44 za MinVar-B portfelj do čak 12,39 na godišnjoj razini koju je ostvarila BNB kriptovaluta, odnosno MaxMean-B portfelj. Povećanjem tolerancije prema riziku s ciljem povećanja očekivanog prinosa, udjeli portfelja se odmiču od MinVar-B portfelja prema MaxMean-B portfelju s najvišim očekivanim prinosom, što predstavlja 100% udjela u BNB kriptovaluti i prikazano je na gornjem desnom dijelu Grafikona 2. Donji dio Grafikona 2. predstavlja doprinos kriptovaluta ukupnom očekivanom prinosu, odnosno riziku portfelja što odgovara dinamici udjela portfelja sa efikasne granice. Drugim riječima, doprinos ukupnom očekivanom prinosu i riziku portfelja sa efikasne granice pripada kriptovalutama koje čine portfelje u rasponu od MinVar-B do MaxMean-B optimizacijske strategije.



Grafikon 3. Ilustracija efikasne granice – mjera rizika CVaR – valuta BTC
Izvor: Izrada autora

Grafikon 3. ilustrira efikasnu granicu mogućih portfelja u kojima mjeru rizika predstavlja uvjetna rizičnost vrijednosti – CVaR. Slično kao i prethodno, najviši očekivani prinos, ali i rizik, ostvario je portfelj koji u svom sastavu uključuje BNB kriptovalutu u visini udjela od 100%. Međutim, usporedbom veličine rizika pojedinačnih kriptovaluta na x osi, primjetno je da CVaR mjera bolje aproksimira rizik od standardne devijacije, pa se ističe da standardna devijacija, kao mjera rizika portfelja, podcjenjuje preuzeti rizik portfelja kreiranog od kriptovaluta. Slično kao i prethodno, dinamika udjela sa efikasne granice se kreće od portfelja sa minimalnim rizikom prema portfelju s najvišim očekivanim prinosom koji u svom sastavu sadrži kriptovalutu BNB u 100% udjelu. S druge strane, razmatrajući površinu efikasne granice kao moguća optimalna rješenja, značajno prevladava utjecaj BNB kriptovalute, što se može primijetiti iz donjeg dijela Grafikona 3. Takav rezultat, u kontekstu prinosa i rizika, sugerira veću ovisnost optimalnih portfelja prema BNB kriptovaluti. Štoviše, u slučaju uvjetne rizičnosti vrijednosti kao mjere rizika, doprinos preostalih kriptovaluta ukupnom očekivanom prinosu i riziku optimalnih portfelja sa efikasne granice je niži u odnosu na portfelj srednje vrijednosti i varijance.

Tablica 6. usporedno prikazuje rezultate mjera uspješnosti za pet optimizacijskih strategija (MaxMean-B, MinVar-B, MaxSR-B, MinCVaR-B i MaxSTARR-B), i rezultate portfelja s jednakim udjelima (EQ-W-B), izražene u BTC jedinici valute. Svi rezultati su izračunati na ukupnom uzorku podataka i prezentirani su na godišnjoj razini.

Tablica 6. Usporedba rezultata mjera uspješnosti optimizacijskih strategija unutar uzorka – valuta BTC

			Varijanca-B		CVaR-B	
Mjere uspješnosti	EQ-W-B	MaxMean-B	MinVar-B	MaxSR-B	MinCVaR-B	MaxSTARR-B
God. očekivani prinos $\mu_{a,i}$	0,63	1.068,56	0,09	1,05	0,64	1.068,57
God. stdev. $\sigma_{a,i}$	0,81	12,39	0,44	0,73	0,76	12,39
Godišnji $VaR_{a,i}$	0,67	0,90	0,60	0,78	0,60	0,90
Godišnji $CVaR_{a,i}$	1,06	1,90	0,97	1,12	0,90	1,90

Izvor: Izrada autora

Prva kolona u Tablici 6. opisuje korištene mjere uspješnosti prezentirane u četiri reda tablice (godišnji očekivani prinos $\mu_{a,i}$, godišnja standardna devijacija $\sigma_{a,i}$, godišnji $VaR_{a,i}$ i godišnji $CVaR_{a,i}$). U drugoj koloni su prezentirane vrijednosti portfelja s jednakim udjelima, a u trećoj koloni vrijednosti portfelja s optimizacijskom strategijom maksimalizacije očekivanog prinosa. U četvrtoj i petoj koloni tablice prezentirane su vrijednosti optimizacijskih strategija minimizacije rizika, u ovom slučaju standardne devijacije, i maksimalizacije omjera prinosa i standardne devijacije. Šesta i sedma kolona prikazuju rezultate iste optimizacijske strategije, samo što je u ovom slučaju korištena CVaR mjera rizika. U kontekstu standardne devijacije kao mjere rizika portfelja, najniži očekivani rizik ostvario je MinVar-B portfelj, što odgovara cilju optimizacijske strategije. Od mogućih 19 kriptovaluta (BTC nije uključen jer predstavlja jedinicu valute), 14 kriptovaluta su ostvarile pozitivne udjele u MinVar-B portfelju, što je prikazano na gornjem lijevom dijelu Grafikona 10. u Prilogu rada. Najviši udio u MinVar-B portfelju je ostvarila ETH kriptovaluta kojoj pripada čak 27,4% udjela, a najniži udio BNB kriptovaluta sa udjelom od 0,1% u portfelju. S druge strane, značajniji doprinos očekivanom prinosu portfelja proizlazi samo iz dvije kriptovalute DOGE i EOS, što je prikazano u gornjem desnom dijelu Grafikona 10.

Doprinos pojedinačne kriptovalute ukupnom riziku portfelja je jednak pojedinačnim udjelima kriptovaluta u MinVar-B portfelju. Ukoliko se razmatraju rezultati rizičnosti vrijednosti (VaR) i uvjetne rizičnosti vrijednosti (CVaR), MinVar-B optimizacijska strategija je ostvarila drugi po redu najbolji rezultat. Očekivano, od svih preostalih strategija, najniži VaR i CVaR je ostvarila upravo strategija s ciljem njihove minimizacije. U usporedbi rezultata sa portfeljem s jednakim udjelima (EQ-W-B), MinVar-B portfelj je ostvario daleko niži očekivani godišnji prinos, ali isto tako i niži rizik.

Strategija koja maksimizira omjer prinosa i standardne devijacije MaxSR-B je ostvarila drugi po redu najbolji rezultat po visini standardne devijacije. Takav rezultat odgovara optimizacijskom cilju, s obzirom da uzima standardnu devijaciju kao mjeru rizika. S druge strane, povećanje očekivanog prinosa skoro 12 puta u odnosu na MinVar-B portfelj, dostatno kompenzira višu preuzetu standardnu devijaciju. Od 19 mogućih, 5 kriptovaluta je ostvarilo pozitivne udjele u rasponu od najvišeg udjela od čak 40,20% koji se odnosi na kriptovalutu EOS, pa do najnižeg koji uključuje kriptovalutu BNB u omjeru od 3,4%, što je prikazano na gornjem lijevom dijelu Grafikona 11. u Prilogu rada. Doprinos očekivanom prinosu i riziku portfelja uključuje 5 kriptovaluta, pri čemu jednake omjere ostvaruju kriptovalute EOS i BNB, te kriptovalute ADA i DOGE. Navedeno je dodatno ilustrirano kroz Grafikon 11. u Prilogu. Očekivano, veličine VaR-a i CVaR-a su nešto više u odnosu na MinVar-B strategiju sukladno višem preuzetom riziku.

Optimizacijska strategija koja minimizira uvjetnu rizičnost vrijednosti (CVaR) je ostvarila najniži očekivani rizik u CVaR mjeri rizika. Takav rezultat je konzistentan s optimizacijskim ciljem. Međutim, ukoliko se razmotri omjer očekivanog prinosa i rizika, MinCVaR-B strategija pruža bolji omjer u odnosu na MinVar-B portfelj, pa se može pretpostaviti da bi dinamičkim testiranjem unatrag izvan uzorka (engl. *backtesting*), navedena optimizacijska strategija također trebala postići bolji rezultat. Sukladno tome, potencijalnim se investitorima sugerira davanje prednosti CVaR mjeri rizika naspram standardne devijacije prilikom modeliranja portfelja na tržištu kriptovaluta, ukoliko se vrijednost portfelja izražava u bitcoinu kao jedinici vrijednosti. Dinamika optimizacijskog rješenja MinCVaR-B strategije je dodatno prezentirana Grafikon 13. Najviši udio u portfelju je ostvarila kriptovaluta LTC od 30,10%, a najniži

kriptovaluta XLM od 0,4%. Od svih kriptovaluta uključenih u portfelj, samo je kriptovaluta BNB ostvarila značajniji doprinos ukupnom prinosu i riziku portfelja u odnosu na ostale uključene sastavnice, ilustrirano kroz Grafikon 13. u Prilogu rada.

Primjenom strategije maksimalizacije omjera prinosa i CVaR-a, optimizacijski algoritam je alocirao 100% udjela u BNB kriptovalutu, s obzirom da kriptovaluta BNB ima najviši očekivani omjer prinosa i CVaR-a od svih pojedinačnih, ali i mogućih kombinacija kriptovaluta. Naime, u periodu razmatranja BNB kriptovaluta je ostvarila iznimno velike prinose izražene u vrijednosti BTC-a, pa se iz tog razloga svrstava i u optimizacijsko rješenje maksimalizacije očekivanog prinosa portfelja. Drugim riječima, strategije MaxMean-B i MaxSTARR-B su ostvarile jednake očekivane vrijednosti prinosa i rizika portfelja. Ilustracija optimizacijskih rješenja je prikazana na Grafikonu 12 i 14. u Prilogu. Od svih promatranih modela alokacije imovine, najviši očekivani prinos unutar uzorka su ostvarile prethodno spomenute strategije. S druge strane, očekivano, najniži rizik izražen kao standardna devijacija je ostvario MinVar-B portfelj, a najnižu uvjetnu rizičnost vrijednosti MinCVaR-B portfelj. Ukoliko se kao potencijalna alokacijska strategija razmatra portfelj s jednakim udjelima, samo MinVar-B portfelj je ostvario lošiji očekivani rezultat od EQ-W-B pasivne strategije. Ovako dobiveni rezultati sugeriraju da investitori imaju mogućnost donositi suvisle investicijske odluke u području modeliranja portfelja čija je vrijednost izražena u jedinicama bitcoin valute. Međutim, ovdje je važno naglasiti da prethodno prezentirani rezultati predstavljaju optimizacijska rješenja dobivena na ukupnom uzorku podataka. Drugim riječima, rezultati predstavljaju očekivane vrijednosti kao ulazni podatak za realokaciju i rebalans portfelja za naredni period sukladno povijesnoj dinamici prinosa kriptovaluta, a ne realizirane, odnosno ostvarene veličine.

9.3. Rezultati optimizacije portfelja izvan uzorka – valuta BTC

Prethodno navedena konstatacija nameće sljedeći korak istraživanja proveden u ovom radu s ciljem ispitivanja mogućnosti modeliranja vrijednosti portfelja izraženom u jedinicama bitcoin kriptovalute. Sukladno postavljanoj prvoj hipotezi rada „H1.: *Na sekundarnom tržištu kriptovaluta, primjenom aktivnih investicijskih strategija, moguće je formirati portfelj izražen kroz vrijednost bitcoin kriptovalute koji ostvaruje viši kumulativni prinos od prinosa pojedinačnih sastavnica portfelja*“, u nastavku se

prezentiraju rezultati testiranja unatrag izvan uzorka (engl. *backtesting*), kako bi se potvrdila ili odbacila postavljena hipoteza rada.

Prije interpretacije rezultata, potrebno je navesti i parametre koji su se koristili prilikom testiranja izvan uzorka te koji su ostvarili najbolji i prezentirani rezultat. Sukladno postavljenoj hipotezi, cilj je bio utvrditi mogućnost ostvarenja kumulativnog prinosa strategije višeg od kumulativnog prinosa potencijalnih sastavnica portfelja. U tu svrhu uvedeno je dodatno ograničenje gornje moguće granice udjela sastavnice u portfelju od 33%. Za inicijalnu optimizaciju je korišten set od 20 povijesnih prinosa, a za svaku sljedeću je korišten pomični set podataka (engl. *rolling window*) koji je uključivao 19 povijesnih prinosa kriptovaluta. Kako bi optimizacijska strategija što bolje opisala i prilagodila izrazito dinamičnim tržištu kriptovaluta, korišten je dnevni rebalans portfelja sukladno prethodno dobivenim rezultatima optimizacijskog cilja.

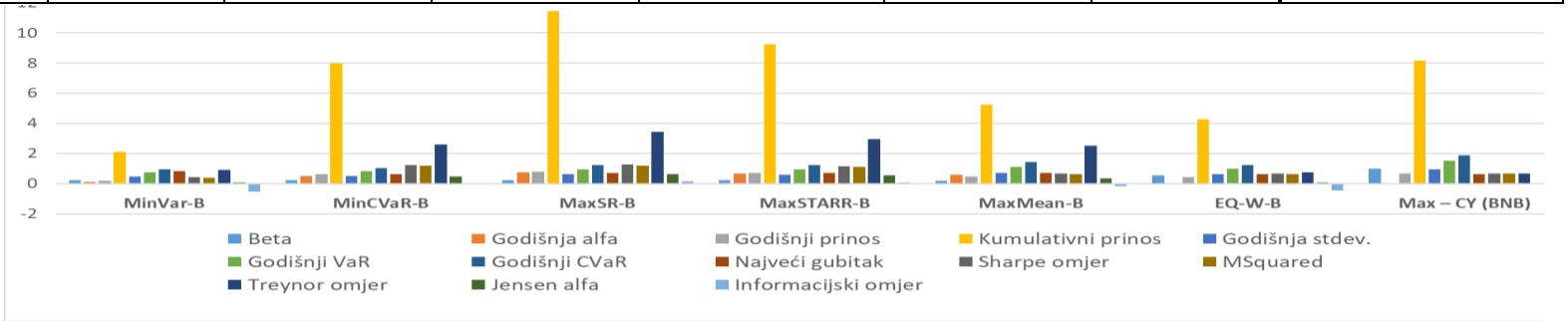
Tablica 7. usporedno prikazuje rezultate svih provedenih mjera uspješnosti optimizacijskih strategija gdje se kao indikator uspješnosti (engl. *benchmark*) koristi upravo kriptovaluta BNB koja je unutar ukupnog promatranog razdoblja ostvarila najviši kumulativni prinos. U 1. koloni Tablice 7. se nalazi opis korištenih mjera uspješnosti i rizika. U kolonama od 2. do 6. su prikazani rezultati mjera uspješnosti za pet provedenih optimizacijskih strategija, te portfelj s jednakim udjelima čiji su rezultati prikazani u koloni 7. Posljednja kolona 8. prikazuje rezultate za kriptovalutu BNB koja služi kao indikator profitabilnosti. Grafikon 4. ilustrira vrijednosti rezultata iz Tablice 7. Sve optimizacijske strategije su ostvarile niži nagib pravca regresije β_i od veličine 1, čime se sugerira niži rizik optimizacijskih strategija u odnosu na pojedinačnu BNB kiptovalutu. Također, sve optimizacijske strategije su ostvarile pozitivnu regresijsku alfu $a_{a,i}$ koja predstavlja ostvareni prosječni godišnji prinos portfelja u slučaju stagnacije BNB kriptovalute. Najvišu prosječnu alfu, kao i najviši godišnji geometrijski prinos $R_{G,i}$ je ostvarila MaxSR-B optimizacijska strategija. Osim spomenute, samo je i MaxSTARR-B strategija ostvarila viši geometrijski prinos od geometrijskog prinosa BNB kriptovalute. Sve preostale strategije, pa i portfelj s jednakim udjelima, su ostvarile niži ukupni geometrijski prinos. Rezultati kumulativnog prinosa su konzistentni s prethodno navedenim.

Tablica 7. Usporedni prikaz rezultata mjera uspješnosti optimizacijskih strategija i kriptovalute s najvišim kum. prinosom (BNB)

		Optimizacijski modeli alokacije imovine						
Mjere uspješnosti		MinVar-B	MinCVaR-B	MaxSR-B	MaxSTARR-B	MaxMean-B	EQ-W-B	Max – CY (BNB)
Beta	β_i	0,21	0,25	0,23	0,24	0,20	0,56	1,00
Godišnja alfa	$a_{a,i}$	0,10	0,51	0,76	0,66	0,60	0,03	/
Godišnji prinos	$R_{G,i}$	0,19	0,65	0,80	0,71	0,49	0,42	0,66
Kumulativ. prinos	CY	2,10	7,98	11,47	9,24	5,23	4,27	8,17
Godišnja stdev.	$\sigma_{a,i}$	0,46	0,53	0,62	0,61	0,71	0,62	0,94
Godišnji VaR	$VaR_{a,i}$	0,74	0,82	0,97	0,97	1,13	0,98	1,50
Godišnji CVaR	$CVaR_{a,i}$	0,94	1,04	1,22	1,22	1,43	1,24	1,89
Najveći gubitak	WD	0,82	0,62	0,73	0,71	0,73	0,64	0,65
Sharpe omjer	SR	0,42	1,23	1,29	1,15	0,68	0,68	0,69
MSquared	M^2	0,40	1,20	1,20	1,10	0,64	0,64	0,66
Treynor omjer	TR	0,91	2,60	3,44	2,94	2,50	0,75	0,66
Jensen alfa	α_i	0,05	0,48	0,64	0,55	0,36	0,05	/
Info. omjer	IR	-0,54	-0,01	0,15	0,05	-0,16	-0,46	/

Izvor: Izrada autora

Grafikon 4. Ilustracija vrijednosti Tablice 7.

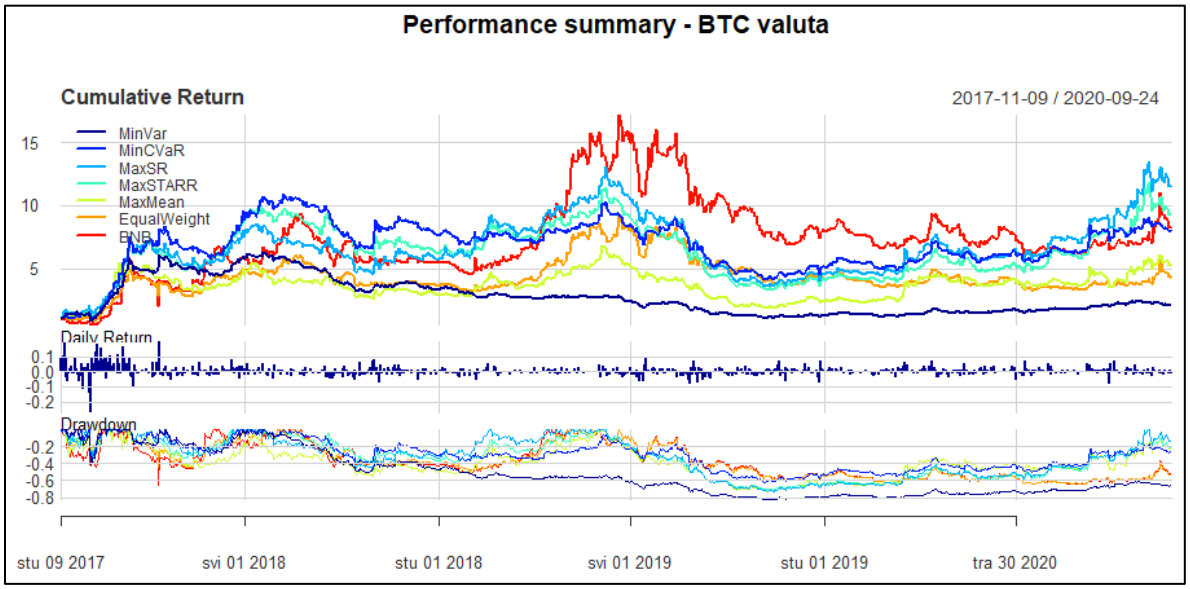


Izvor: Izrada autora

Obje strategije su ostvarile viši kumulativni prinos od BNB kriptovalute. Međutim, svakako je potrebno i usporediti rezultate strategija koje minimiziraju rizik u kontekstu ostvarenog prinosa. Naime, prilikom prethodne interpretacije rezultata optimizacije unutar uzorka, navedeno je da se očekuje da strategija koja minimizira CVaR ostvari bolje rezultate izvan uzorka od strategije koja minimizira standardnu devijaciju, što se ovdje potvrdilo. Iako je ukupno promatrani rizik nešto viši, MinCVaR-B strategija je ostvarila tri puta viši prinos od MinVar-B strategije, što dostatno kompenzira povećanje rizika. Od svih kreiranih alokacijskih modela najnižu standardnu devijaciju portfelja $\sigma_{a,i}$ je ostvarila MinVar-B, zatim MinCVaR-B strategija, što odgovara optimizacijskim ciljevima. S druge strane, najvišu standardnu devijaciju je postigla strategija koja maksimizira očekivani prinos. Međutim, sve strategije su ostvarile nižu standardnu devijaciju od BNB kriptovalute, čime se potvrđuje korisnost primjene optimizacijskih strategija u ovom kontekstu. Iako je strategija MinVar-B ostvarila nešto niži rizik u kontekstu rizičnosti vrijednosti od MinCVaR-B strategije, ostvareni rezultati VaR-a i CVaR-a potvrđuju prethodno navedene omjere, odnosno sve strategije su ostvarile niži VaR i CVaR od pojedinačne BNB kriptovalute. Ukoliko se razmotri mjera rizika najvećeg gubitka WD, samo je portfelj s jednakim udjelima i portfelj koji minimizira uvjetnu rizičnost vrijednosti ostvario manji najviši gubitak od BNB kriptovalute.

Donji dio Tablice 7. prikazuje relativne mjere uspješnosti optimizacijskih strategija u odnosu na BNB kriptovalutu kao svojevrsni indikator profitabilnosti tržišta kriptovaluta izraženom u vrijednosti BTC jedinici valute. Tri optimizacijske strategije: MinCVaR-B, MaxSR-B i MaxSTARR-B su ostvarile viši Sharpe omjer od BNB kriptovalute. Mjera MSquared koja ukazuje na razliku omjera prinosa i rizika u odnosu na BNB kriptovalutu također potvrđuje prethodne odnose. Omjer ostvarenog geometrijskog prinosa i regresijskog koeficijenta između vremenskih serija prinosa strategije i BNB kriptovalute prezentiranog kroz Treynor omjer također ide u korist svih optimizacijskih strategija. Sve vrijednosti su više od veličine Treynor omjera BNB kriptovalute. Isto tako, u kontekstu CAPM modela, sve vrijednosti Jensen alfe su pozitivne veličine. Drugim riječima, sve strategije su ostvarile viši prinos nego što to zahtijeva osnovna CAPM relacija. Takav rezultat ne iznenađuje s obzirom na veličinu beta koeficijenta optimizacijskih strategija β_i koji ukazuje da su strategije ispod prosječno rizične u

odnosno na BNB kriptovalutu, odnosno njihov rizik negativno korigira očekivani prinos strategije po CAPM relaciji.



Grafikon 5. Ilustracija kumulativnog prinosa različitih optimizacijskih strategija i BNB kriptovalute

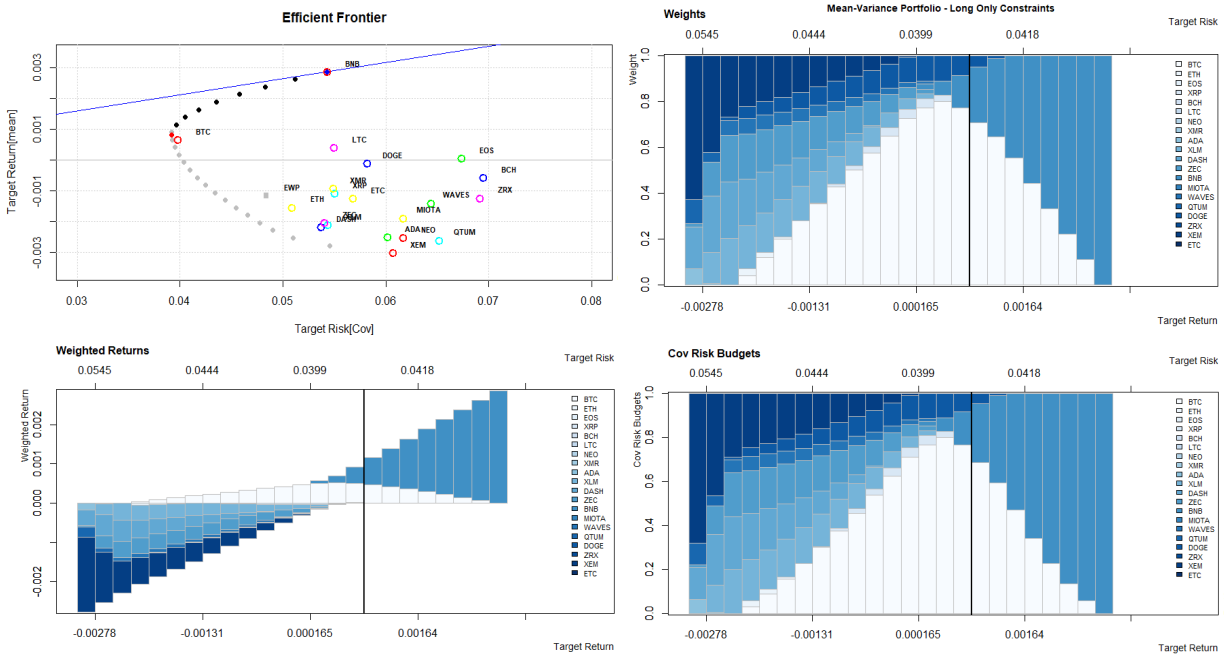
Izvor: Izrada autora

Na kraju, pozitivan omjer prinosa i standardne devijacije aktivne premije, prezentiran kao informacijski omjer IR, su ostvarile MaxSR-B i MaxSTARR-B strategije, čim se potvrđuju prethodno prezentirani rezultati. Navedene strategije su jedine ostvarile viši kumulativni prinos od kriptovalute koja je imala najviši kumulativni prinos u istom vremenskom periodu. Na Grafikonu 5. je prikazana dinamika dnevnih kumulativnih prinosa pojedinačnih strategija i BNB kriptovalute, ukupni dnevni prinosi svih strategija i najveći gubitak, s kojom se dodatno ilustriraju performanse optimizacijskih ciljeva portfelja. S obzirom na prezentirane rezultate, a sukladno prvoj postavljenoj hipotezi rada, zaključuje se da je aktivnim strategijama moguće konstruirati portfelj izražen u vrijednosti BTC kripotvalute koji ostvaruje viši kumulativni prinos od pojedinačnih sastavnica portfelja, čime se prihvaća H1 hipoteza rada.

9.4. Rezultati optimizacije portfelja unutar uzorka – valuta USD

U nastavku rada se prezentiraju rezultati optimizacije portfelja unutar ukupnog uzorka na istim potencijalnim sastavnicama portfelja, uključujući i bitcoin kriptovalutu.

Ilustracija rezultata konstrukcije efikasne granice kreirane od kriptovaluta denominiranih u američkom dolaru kao obračunskoj jedinici vrijednosti ulaganja, te standardnoj devijaciji u funkciji mjere rizika, prezentirana je Grafikonom 6. Gornji lijevi dio grafikona prikazuje područje mogućih portfelja, odnosno efikasnu granicu u koordinatnom sustavu prinosa i rizika. Slično kao i prethodno, od svih pojedinačno promatranih sastavnica, ali i njihovih kombinacija u portfelju, BNB kriptovaluta ostvaruje najbolji omjer očekivanog prinosa i rizika, što rezultira tangentnim portfeljem na efikasnoj granici. Međutim, u ovom slučaju očekivani prinos i rizik BNB kriptovalute nisu značajno više izraženi u odnosu na druge sastavnice portfelja i njihove kombinacije, pa je područje efikasne granice bolje raspoređeno u koordinatnom sustavu. Efikasna granica je izvedena promjenom tolerancije prema riziku kroz 25 mogućih kombinacija kriptovaluta. Za razliku od prethodnog razmatranja, može se uočiti da je skoro pola područja mogućih kombinacija portfelja zapravo ostvarilo negativan očekivani prinos, što ne iznenađuje, s obzirom da je i većina potencijalnih sastavnica ostvarilo negativan očekivani prinos. Efikasna granica optimalnih portfelja je izvedena između portfelja s minimalnim rizikom MinVar i portfelja s maksimalnim očekivanim prinosom MaxMean.



Grafikon 6. Ilustracija efikasne granice – mjera rizika varijanca – valuta USD

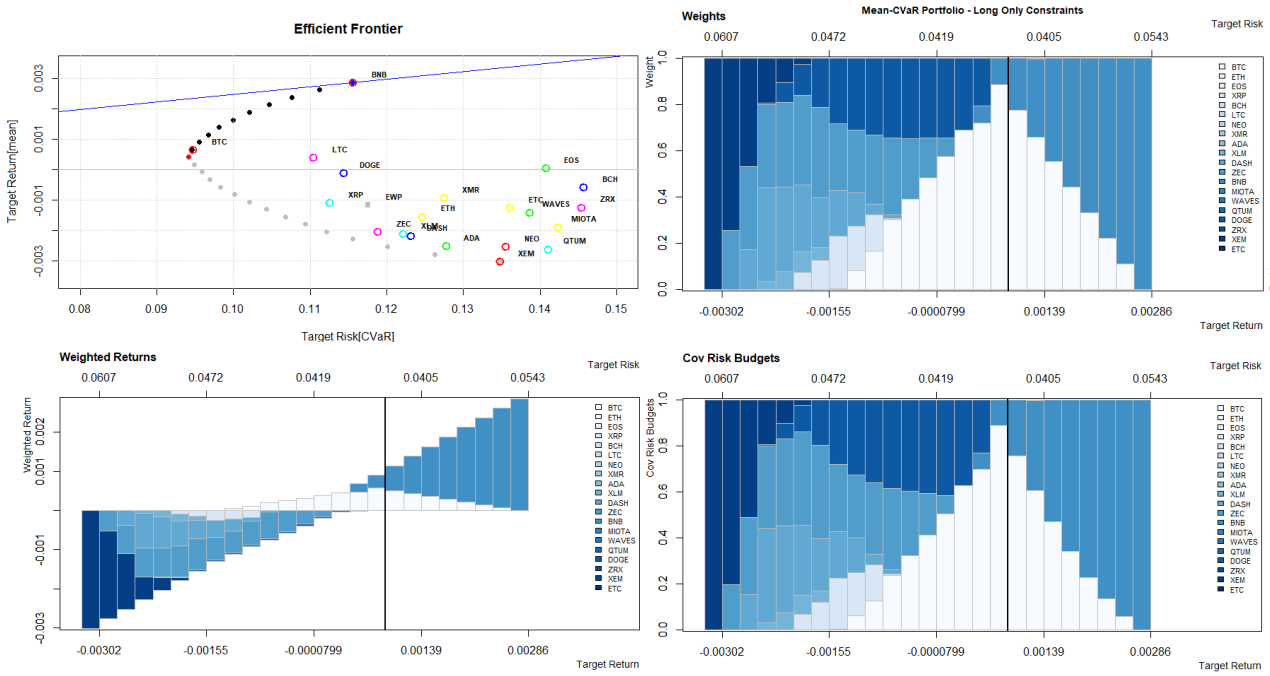
Izvor: Izrada autora

Promjenom tolerancije prema riziku, očekivani prinos portfelja se povećava uključujući više rizičnu BNB kriptovalutu. Štoviše, udjeli prikazani na gornjem desnom dijelu Grafikona 6. sugeriraju da su se za izvedbu efikasne granice optimalnih portfelja s pozitivnim očekivanim prinosom koristile samo tri kriptovalute: BTC, BNB i DOGE. Donji dio Grafikona 6. predstavlja doprinos kriptovaluta ukupnom očekivanom prinosu, odnosno riziku portfelja što odgovara dinamici udjela portfelja sa efikasne granice. Doprinos očekivanom prinosu ostvaruju samo BTC i BNB kriptovaluta, a doprinos riziku uključuje i kriptovalutu DOGE.

Sa aspekta razmatranja mogućih portfelja kao potencijalnog investicijskog odabira, prethodno opisani odnosi sa efikasne granice, ne idu u prilog konstrukciji profitabilnog i dobro diverzificiranog portfelja. Naime, ukoliko se od mogućih 20 kriptovaluta, samo tri kriptovalute koriste za konstrukciju efikasne granice, a to je posljedica općenito negativnih stvarnih povijesnih, ali i očekivanih prinosa pojedinačnih kriptovaluta, takvo zapažanje već sada sugerira zapravo loše rezultate optimizacije izvan uzorka. Drugim riječima, u kontekstu postavljene H2 hipoteze rada, gdje se primjenom potencijalnih fundamentalnih indikatora pokušava determinirati uzorak kriptovauta koji će u obliku portfelja ostvariti bolji rezultat od kretanja indikatora profitabilnosti, poput CRIX-a, rezultati upućuju na potencijalno loš odabir sastavnica, odnosno sugeriraju krivu strategiju njihovog inicijalnog odabira.

Grafikon 7. prikazuje efikasnu granicu mogućih portfelja u kojima mjeru rizika predstavlja uvjetna rizičnost vrijednosti – CVaR. Moguće kombinacije udjela u kriptovalutama, kreiraju portfelje čija se efikasna granica značajno ne razlikuje od prethodno opisane efikasne granice, tako da i u ovom slučaju tangentni portfelj predstavlja BNB kriptovaluta sa 100% udjelom na efikasnoj granici. Međutim, za razliku od prethodne, CVaR efikasna granica ne uključuje BNB kriptovalutu u portfelj sa minimalnim rizikom, nego je portfelj kreiran samo od kriptovaluta BTC i DOGE. Promjenom očekivanog prinosa portfelja, pozitivni dio efikasne granice se proteže od MinCVaR portfelja prema MaxMean portfelju, koji ne razmatra rizik kao input u optimizaciji. S druge strane, CVaR efikasna granica ukazuje na jednu prednosti u odnosu na standardnu devijaciju. Naime, gornji dio pozitivne efikasne granice optimalnih portfelja kreiran je samo od dvije kriptovalute BTC i BNB, odnosno sastavnica koje su ostvarile pozitivan očekivani prinos, što bi značilo da prethodno

uključena DOGE kriptovaluta, sada ne predstavlja sastavnicu portfelja. Drugim riječima, CVaR optimizacija uzima u obzir prosječne negativne prinose u repovima distribucije te iz tog razloga izuzima kriptovalutu DOGE kao moguću sastavnicu, ukoliko se ciljano optimizira očekivani prinos. Doprinos očekivanom prinosu i riziku kreiranim portfeljima sa efikasne granice, prikazan na donjem dijelu Grafikona 7., također prati prethodnu dinamiku pojedinačnih udjela kriptovaluta. Povećanjem udjela više rizične kriptovalute u optimalnom portfelju sa efikasne granice, povećava se i ponder te kriptovalute u agregatnoj vrijednosti koji determinira očekivani prinos i rizik portfelja.



Grafikon 7. Ilustracija efikasne granice – mjera CVaR varijanca – valuta USD

Izvor: Izrada autora

Tablica 8. usporedno prikazuje rezultate mjera uspješnosti za pet optimizacijskih strategija provedenih unutar uzorka (MaxMean, MinVar, MaxSR, MinCVaR i MaxSTARR) i rezultate portfelja s jednakim udjelima (EQ-W), izražene u USD jedinici valute. Svi rezultati su izračunati na ukupnom uzorku podataka i prezentirani su na godišnjoj razini. Interpretacija Tablice 8. je jednaka prethodnoj. U prvoj koloni tablice su opisane korištene mjere, a u preostalim kolonama se nalaze vrijednosti korištenih mjera po pripadnosti optimizacijskoj strategiji navedenoj u zaglavlju tablice.

Tablica 8. Usporedba rezultata mjera uspješnosti optimizacijskih strategija unutar uzorka – valuta USD

			Varijanca		CVaR	
Mjere uspješnosti	EQ-W	MaxMean	MinVar	MaxSR	MinCVaR	MaxSTARR
God. očekivani prinos $\mu_{a,i}$	-0,25	1,05	0,23	1,05	0,11	1,05
God. stdev. $\sigma_{a,i}$	0,77	0,86	0,62	0,86	0,64	0,86
Godišnji $VaR_{a,i}$	1,31	1,31	1,02	1,31	1,04	1,31
Godišnji $CVaR_{a,i}$	1,87	1,83	1,51	1,83	1,49	1,83

Izvor: Izrada autora

Sukladno optimizacijskom cilju, najnižu očekivanu standardnu devijaciju portfelja je ostvarila MinVar strategija. Od mogućih 20 kriptovaluta, samo tri kriptovalute su uključene u MinVar portfelj, što je prikazano na gornjem lijevom dijelu Grafikona 16. u Prilogu rada. Najviši udio je ostvario BTC u postotku od čak 79,30%, BNB je ostvario 10,70%, a najniži udio kriptovaluta DOGE u visini od 9,90%. Značajniji doprinos očekivanom prinosu MinVar portfelja je raspoređen između BTC i BNB kriptovalute, što je prikazano u gornjem desnom dijelu Grafikona 16., dok je kontribucija riziku jednaka udjelima kriptovaluta u portfelju, prikazano na donjem dijelu Grafikona 16. u Prilogu. Za razliku od optimizacije u BTC jedinici valute, osim standardne devijacije, MinVar strategija je ostvarila i najniži očekivani VaR od svih promatranih optimizacijskih strategija, dok je CVaR ipak nešto viši od MinCVaR strategije.

Drugi po redu najlošiji očekivani prinos je ostvarila MinCVaR optimizacijska strategija čiji su rezultati dodatno ilustrirani Grafikonom 19. u Prilogu. Sastav portfelja uključuje samo BTC i DOGE kriptovalute, a samo BTC kriptovaluta ima očekivani prinos koji je relevantan kao doprinos ukupnom očekivanom prinosu portfelja, ilustrirano na desnom gornjem dijelu grafikona. Jednako tako, kontribucija riziku portfelja je slična postignutim udjelima portfelja. Ukoliko se usporede ukupni rezultati MinVar i MinCVaR strategija, bolje rezultate omjera prinosa i rizika je ostvarila MinVar strategija, što je u suprotnosti s rezultatima optimizacije provedene u bitcoinu kao jedinici valute, gdje su rezultati optimizacije sugerirali prednost CVaR mjeri rizika.

Optimizacija portfelja unutar uzorka se provela na 20 kriptovaluta koje su po svojim fundamentalnim indikatorima predstavljale najbolji mogući odabir u funkciji sastavnica portfelja. Međutim, loš povijesni rezultat većine odabranih kriptovaluta ograničio je izvedbu optimizacijskih strategija na nekolicinu kriptovaluta koje su ostvarile pozitivne veličine prinosa. U tom su smislu indikativni i rezultati portfelja s jednakim udjelima. Naime, sa aspekta prinosa portfelja, najlošiji rezultat je ostvarila strategija u kojoj su udjeli jednako raspoređeni u visini od 5%, te u kojoj je očekivani pronos portfelja ispao negativan, Grafikon 21. u Prilogu. Zbog navedenog ograničenja, čak tri optimizacijske strategije: MaxSR, MaxMean i MaxSTARR su ostvarile jednake rezultate optimizacije portfelja unutar ukupnog uzorka podataka, što je prikazano u Tablici 8. i dodatno ilustrirano na Grafikonu 17., 18. i 20. u Prilogu rada. Za sva tri portfelja 100% udjela predstavlja kriptovaluta BNB s očekivanim godišnjim prinosom od 105% i godišnjoj standardnoj devijaciji u visini od 86%. Prethodno prezentirani rezultati optimizacije predstavljaju ulazne omjere udjela portfelja za naredni vremenski period držanja kriptovalute, koji su dobiveni na ukupnom uzorku podataka. Kako bi se jedna takva optimizacijska strategija što više približila praktičnoj primjeni, u nastavku se rada prezentiraju rezultati testiranja unatrag izvan uzorka (engl. *backtesting*) gdje se prethodno dobivena optimizacijska rješenja uzimaju dalje kao ulazni podatak za realokaciju i rebalans portfelja za naredni period sukladno povijesnoj dinamici prinosa kriptovaluta.

9.5. Rezultati optimizacije portfelj izvan uzorka – valuta USD

Ispitivanje kvalitete odabranih indikatora koji bi mogli reprezentativno predstavljati fundamentalne varijable ne temelju koji se konstruira portfelj kriptovaluta se nastavlja provedbom testiranja unatrag. S obzirom da metodologija CRIX indeksa ne uključuje optimizacijske strategije, osim standardnog kretanja indeksa u svom nominalnom obliku, prezentirani su i rezultat optimizacije CRIX-a za sve odabrane strategije. Pored toga, s ciljem utvrđivanja prednosti uključivanja fundamentalnih indikatora, u nastavku se prezentiraju i rezultati deset portfelja čije su sastavnice uzorak od dvadeset nasumično odabranih kriptovaluta od populacije koja čini sedamdeset mogućih kriptovaluta po tržišnoj kapitalizaciji, te su na njima također provedene iste optimizacijske strategije. Za provedbu optimizacije izvan uzorka je korišten pomični set podataka (engl. *rolling window*) koji je uključivao 30 povijesnih prinosa

kriptovaluta uz mjesečni rebalans, pri čemu je 30 povijesnih prinosa predstavljao i inicijalni set podataka za treniranje modela.

Sukladno postavljanoj drugoj hipotezi rada „H2.: *Na sekundarnom tržištu kriptovaluta, uvažavajući fundamentalne pokazatelje, moguće je formirati portfelj kriptovaluta koji ostvaruje viši kumulativni prinos od kumulativnog prinosa CRIX indeksa*“, u nastavku se prezentiraju rezultati testiranja unatrag izvan uzorka (engl. *backtesting*), kako bi se potvrdila ili odbacila postavljena hipoteza rada. U Tablici 9. usporedno su prezentirani rezultati za MaxSR optimizacijsku strategiju između različitih alokacijskih modela koja je odabrana kao reprezentativna strategija za interpretaciju sublimiranih rezultata mjera uspješnosti. Grafikon 8. ilustrira vrijednosti rezultata iz Tablice 9. U prvoj koloni tablice su opisane korištene mjere uspješnosti prezentirane u trinaest redova tablice. Notacije u zaglavlju kolone tablice opisuju sljedeće alokacijske modele: 20-F predstavlja portfelj kreiran prema fundamentalnim indikatorima, CRIX-O označava optimiziran indeks, CRIX predstavlja indeks u svom izvornom obliku i EQ-W označava portfelj s jednakim udjelima. Notacije od N-1 do N-10 označavaju deset portfelja po 20 nasumično odabranih kriptovaluta na kojima su provedene iste optimizacijske strategije. U Prilogu rada Tablice od 10. do 22. prikazuju matricu rezultata pojedinačno provedenih mjera uspješnosti. Prva kolona u tablici opisuje provedene optimizacijske strategije, a u zaglavlju svake sljedeće kolone su navedeni alokacijski modeli. U zadnjem redu tablice nalaze se rezultati za portfelj s jednakim udjelima. U naslovu svake tablice je navedena vrijednost pojedinačno provedene mjere za izvorni CRIX indeks, koji je služio kao indikator za usporedbu. Kako bi se bolje prezentirale razlike, Grafikoni od 22. do 34. ispod tablica usporedno ilustriraju veličinu provedene mjere između svake strategije optimizacije. Također, u nastavku Priloga, od Grafikona 35. do Grafikona 46. ilustrira se kretanje kumulativnog prinosa za svaki alokacijski model, odnosno za svaku optimizacijsku strategiju provedenu na alokacijskom modelu.

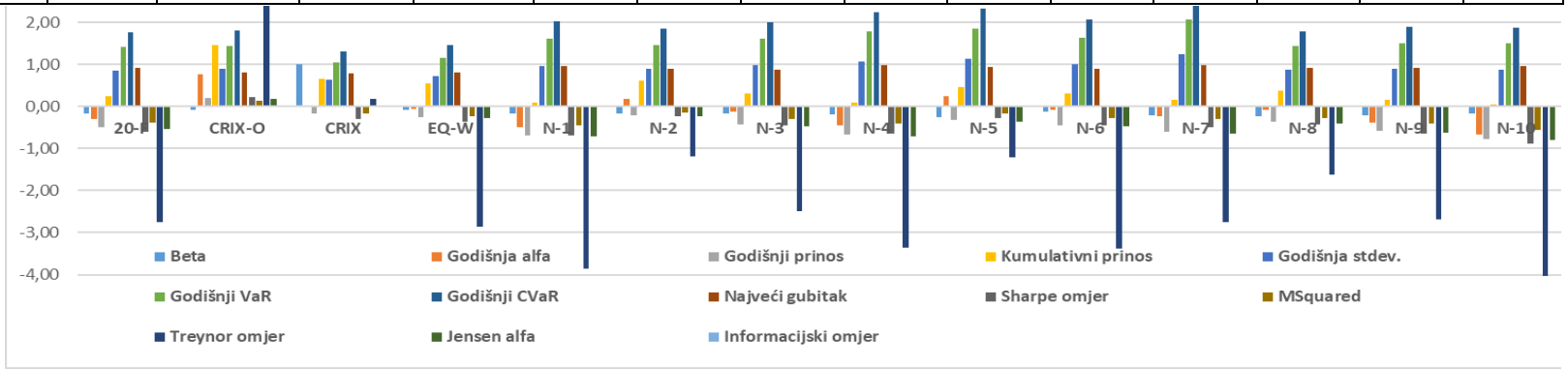
Negativna vrijednost nagiba regresijskog pravca β_i između prinosa portfelja kao rezultata MaxSR optimizacijske strategije za svaki alokacijski model i prinosa CRIX indeksa ukazuje na suprotno kretanje prinosa portfelja u odnosu na tržište. Veličine su prezentirane u prvom redu Tablice 9.

Tablica 9. Usporedni prikaz rezultata mjera uspješnosti za MaxSR optimizacijsku strategiju između različitih alokacijskih modela

Mjere uspješnosti		Alokacija imovine													
		20-F	CRIX-O	CRIX	EQ-W	10 portfelja po 20 nasumično odabranih kriptovaluta									
						N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
Beta	β_i	-0.18	-0.08	1,00	-0.09	-0.18	-0.18	-0.18	-0.20	-0.26	-0.13	-0.22	-0.23	-0.22	-0.18
Godišnja alfa	$a_{a,i}$	-0.29	0.76	0.00	-0.05	-0.49	0.18	-0.12	-0.45	0.25	-0.09	-0.24	-0.09	-0.38	-0.66
Godišnji prinos	$R_{G,i}$	-0.50	0.20	-0.18	-0.26	-0.68	-0.21	-0.44	-0.67	-0.32	-0.45	-0.60	-0.37	-0.59	-0.77
Kumulativ. prinos	CY	0.24	1.45	0.66	0.54	0.10	0.61	0.30	0.10	0.45	0.30	0.15	0.38	0.16	0.05
Godišnja stdev.	$\sigma_{a,i}$	0.84	0.89	0.63	0.71	0.96	0.90	0.97	1.06	1.14	1.00	1.24	0.87	0.90	0.88
Godišnji VaR	$VaR_{a,i}$	1.41	1.44	1.04	1.16	1.62	1.46	1.60	1.78	1.85	1.64	2.06	1.43	1.51	1.51
Godišnji CVaR	$CVaR_{a,i}$	1.76	1.81	1.31	1.46	2.03	1.84	2.01	2.23	2.33	2.06	2.58	1.79	1.89	1.98
Najveći gubitak	WD	0.92	0.81	0.78	0.81	0.96	0.90	0.88	0.97	0.94	0.90	0.98	0.92	0.92	0.96
Sharpe omjer	SR	-0.60	0.22	-0.29	-0.36	-0.70	-0.24	-0.46	-0.64	-0.28	-0.45	-0.49	-0.43	-0.65	-0.88
MSquared	M^2	-0.38	0.14	-0.18	-0.23	-0.45	-0.15	-0.29	-0.40	-0.18	-0.28	-0.31	-0.27	-0.41	-0.56
Treynor omjer	TR	-2.74	2.57	-0.18	-2.86	-3.86	-1.18	-2.49	-3.35	-1.21	-3.38	-2.76	-1.63	-2.68	-4.26
Jensen alfa	α_i	-0.53	0.18	0,00	-0.27	-0.71	-0.24	-0.48	-0.71	-0.37	-0.47	-0.64	-0.41	-0.63	-0.80
Info. omjer	IR	-0.28	0.34	/	-0.08	-0.41	-0.03	-0.22	-0.38	-0.10	-0.22	-0.29	-0.16	-0.34	-0.51

Izvor: Izrada autora

Grafikon 8. Ilustracija vrijednosti Tablice 9.



Izvor: Izrada autora

Ukoliko CRIX indeks predstavlja jedini sistematski faktor tržišta kriptovaluta, rezultati sugeriraju obrnutu povezanost između svih alokacijskih modela i CRIX indeksa. U kontekstu CAPM modela, to bi zapravo značilo odsutnost sistematskog rizika, drugim riječima, osnovna relacija CAPM modela ne zahtijeva premiju za preuzeti rizik, iz razloga što je beta negativna. Međutim, ovakva interpretacija može imati i pogrešne implikacije. Naime, u ovisnosti o strategiji koja se provodi, odnosno u ovisnosti o razini povezanosti s faktorom koja se želi postići, negativna izloženost sistematskom faktoru za vrijeme pozitivnog kretanja ukupnog tržišta kriptovaluta, nije poželjna. Štoviše, rastavljajući izloženost fakturu na pozitivno i negativno stanje, za vrijeme rasta vrijednosti tržišta, investitori bi trebali težiti statistički signifikantnoj pozitivnoj beti, jer bi u tom razdoblju i alokacijski modeli ostvarili pozitivne prinose. S druge strane, za vrijeme pada vrijednosti agregatnog tržišta kriptovaluta, poželjna je negativna povezanost s tržištem. Upravo prethodno opisano se dogodilo u razdoblju koje se razmatra u ovom radu. Naime, svi alokacijski modeli, pa čak i optimizirani CRIX, su ostvarili negativnu povezanost sa CRIX indeksom za vrijeme pozitivnog kretanja tržišta. Ukoliko se razmotre i vrijednosti beta koeficijenta drugih optimizacijskih strategija prezentiranih u Tablici 10. u Prilogu rada, niti jedna strategija nije ostvarila pozitivu betu. Očekivano, CRIX-O alokacijski model je za sve optimizacijske strategije ostvario najmanje negativnu betu.

Regresijski odsječak prezentiran kao godišnja alfa $a_{a,i}$ potvrđuje prethodne rezultate, ali i sugerira jedini alokacijski model koji je ostvario viši prosječni prinos za vrijeme stagnacije ukupnog tržišta kriptovaluta prezentiranog CRIX indeksom, a to je optimizirani CRIX indeks. Prema tome, osim negativnog nagiba pravca koji sugerira negativnu povezanost, svi alokacijski modeli optimizirani MaxSR strategijom, izuzev optimiziranog CRIX indeksa, su ostvarili i negativne prosječne prinose za vrijeme stagnacije tržišta kriptovaluta. Također, i druge optimizacijske strategije provedene za sve alokacijske modele, prezentirane u Tablici 11. u Prilogu rada, osim za optimizirani CRIX, su ostvarile negativne regresijske odsječke, a samo MinVar strategija za alokaciju CRIX-O je ostvarila negativan regresijski odsječak.

Veličina ostvarenog godišnjeg geometrijskog prinosa $R_{G,i}$ također ide u prilog samo optimiziranom CRIX indeksu. Svi drugi alokacijski modeli, pa čak i izvorni CRIX, su ostvarili negativni godišnji geometrijski prinos. MaxSR portfelj kreiran prema

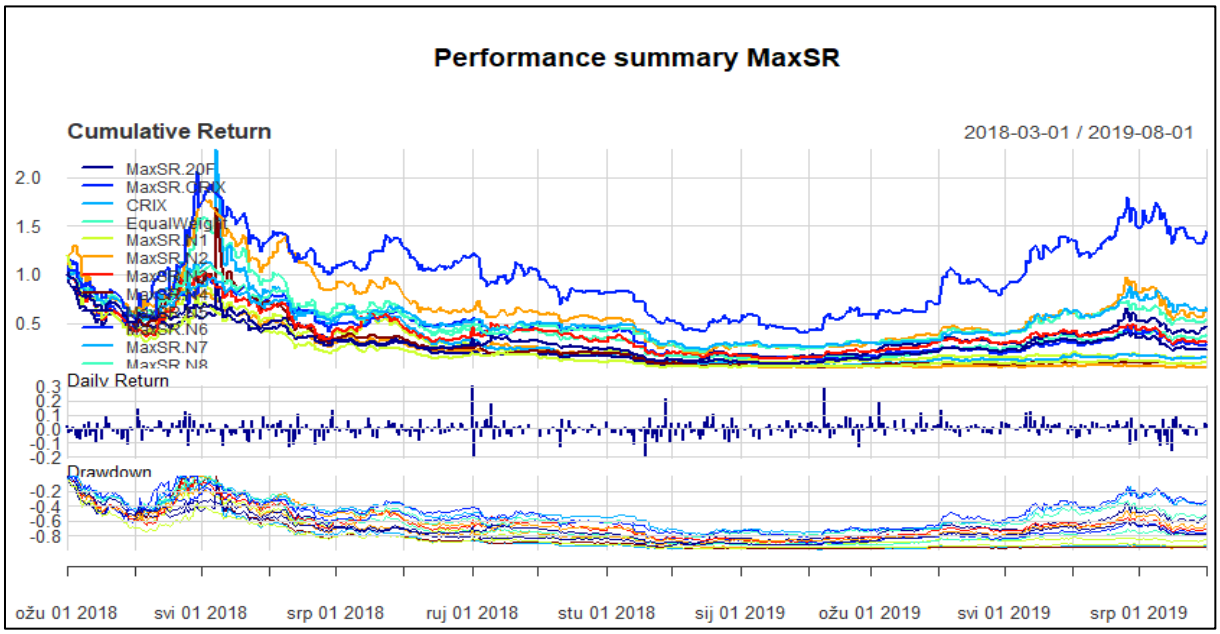
fundamentalnim indikatorima je ostvario čak niži prinos od portfelja s istim sastavnicama koje su jednako zastupljene. S druge strane, najviši geometrijski prinos, prezentiran u Tablici 12., od svih optimizacijskih strategija primijenjenih na sastavnicama CRIX-a, je ostvarila MaxSTARR optimizacijska strategija, što zapravo potvrđuje očekivanja, jer su optimizacijom unutar uzorka, MaxSR i MaxSTARR ostvarili najbolje očekivane rezultate.

Kumulativni prinos CY koji bi se ostvario ukoliko bi se MaxSR strategija primijenila u praksi, prezentiran je u sljedećem redu Tablice 9., odnosno za sve optimizacijske strategije u Tablici 13. Od svih alokacijskih modela, jedini pozitivni i najviši kumulativni prinos je ostvario optimizirani CRIX indeks. Svi drugi alokacijski modeli bi ostvarili gubitak. Portfelj kreiran prema fundamentalnim indikatorima je ostvario gubitak od čak 76%, što je više i od izvornog CRIX indeksa i portfelja s jednako zastupljenim udjelima. Također, niti drugi nasumično kreirani portfelji nisu ostvarili pozitivne kumulativne prinose i njihov gubitak je po visini sličan gubitku 20-F portfelja. Druge optimizacijske strategije, prezentirane u Tablici 13., također su ostvarile slične rezultate prema pripadajućim modelima alokacije. Međutim, za razliku od MaxSR i MaxSTARR strategija, i ostale optimizacijske strategije provedene na sastavnicama CRIX indeksa su ostvarile negativan kumulativni prinos, odnosno gubitak u promatranom vremenu. Unutar 20-F portfelja, najveći gubitak je ostvarila MaxMean optimizacijska strategija, a najmanji gubitak je ostvarila strategija koja minimizira standardnu devijaciju. Ukoliko se promatra omjer MinVar i MinCVaR na sastavnicama CRIX indeksa, MinCVaR portfelj je ostvario gubitak od samo 6%, dok je MinVar strategija izgubila čak 33%.

Od svih alokacijskih modela, najnižu godišnju standardnu devijaciju $\sigma_{a,i}$ je ostvario CRIX indeks u svom izvornom obliku, dok je druga po redu standardna devijacija portfelja s jednakim udjelima. Najnižu rizičnost vrijednosti $VaR_{a,i}$ i uvjetnu rizičnost vrijednosti $CVaR_{a,i}$, te sukladno tome i najniži gubitak u razdoblju promatranja WD je također ostvario CRIX indeks, dok je portfelj s jednako zastupljenim udjelima ostvario ipak malo više vrijednosti mjera rizika. Promatrajući samo mjere rizika, optimizirani CRIX u komparaciji s izvornim CRIX indeksom je ostvario ipak lošije rezultate. Međutim, viši rizik je kompenziran daleko boljim očekivanim, odnosno realiziranim

prinosom. Vrijednosti godišnje standardne devijacije za sve optimizacijske strategije prikazane su u Tablici 14. iz koje je vidljivo da je MinVar optimizacijska strategija ipak ostvarila najniže vrijednosti standardne devijacije za alokacijski model N-3, kao i mjere rizika VaR i CVaR, u odnosnu na CRIX indeks. Međutim, takvi rezultati su očekivani s obzirom na optimizacijski cilj minimiziranja rizika. S druge strane, jednako kao i prethodno, viši rizik MinCVaR portfelja u odnosu na MinVar portfelj za sve provedene mjere rizika, kompenziran je većim ostvarenim prinosom, što je prikazano kroz Sharpe omjer opisan u nastavku.

Visina Sharpe omjera SR također potvrđuje prethodno interpretirane rezultate. S obzirom da je CRIX-O jedini alokacijski model koji je ostvario pozitivan geometrijski prinos, tako je i njegov odnos prinosa i rizika jedini pozitivan. Uspoređujući rezultate Sharpe omjera drugih optimizacijskih strategija prezentiranih kroz Tablicu 18. u Prilogu, uz MaxSR samo je i MaxSTARR strategija ostvarila pozitivan Sharpe omjer koji je čak i viši od prethodne strategije. Isto tako, mjera MSquared koja uzima u obzir apsolutnu veličinu rizika, kao i Treynor omjer, također sugeriraju da je najbolji alokacijski model CRIX-O, odnosno MaxSR i MaxSTARR optimizacijske strategije. Zbog negativnog ostvarenog prinosa, sve druge optimizacijske strategije su ostvarile negativne veličine Sharpe omjera za sve alokacijske modele.



Grafikon 9. Ilustracija kumulativnog prinosa MaxSR optimizacijske strategije

Izvor: Izrada autora

Razmatrajući CRIX indeks u kontekstu sistematskog faktora, odnosno CAPM modela, samo optimizirani CRIX je ostvario prinos portfelja viši od zahtijevanog prinosa po osnovnoj CAPM relaciji, prezentiran kao Jensen alfa a_i. Svi drugi alokacijski modeli nisu ostvarili dostatne prinose za preuzeti rizik. Uvid u Tablicu 21. gdje su prezentirane Jensen alfe za sve optimizacijske strategije također sugerira da su jedini adekvatno kompenzirani rizik ostvarile MaxSR i MaxSTARR strategije za alokacijski model CRIX-O. Na kraju, Informacijski omjer IR koji stavlja u omjer aktivnu premiju sa standardnom devijacijom aktivne premije, isto tako favorizira MaxSR i MaxCVaR optimizacijske strategije provedene na CRIX-O alokacijskom modelu. Na Grafikonu 9. su prikazani dnevni kumulativni prinosi MaxSR optimizacijske strategije za sve alokacijske modele, ukupni dnevni prinosi svih strategija i najveći gubitak, s kojom se dodatno ilustrira razlika između prinosa portfelja. Plava linija označava kretanje MaxSR optimizacijske strategije za CRIX-O alokacijski model koji je jedini ostario pozitivan kumulativni prinos. Svi drugi alokacijski modeli, pa tako i portfelj kreiran prema fundamentalnim indikatorima 20-F, ostvarili su gubitak u promatranom razdoblju. Sukladno prezentiranim rezultatima, a kontekstu postavljene druge hipoteze rada, zaključuje se da na sekundarnom tržištu kriptovaluta, uvažavajući fundamentalne pokazatelje, nije moguće formirati portfelj kriptovaluta koji ostvaruje viši kumulativni prinos od kumulativnog prinosa CRIX indeksa, čime se odbacuje H2 postavljena hipoteza rada.

S druge strane, razmatranje rezultata izvan okvira konteksta hipoteze rada ipak sugerira neka zapažanja koje je potrebno istaknuti i izvesti određene zaključke. Prvo zapažanje koje se ističe su rezultati primjene uvjetne rizičnosti vrijednosti (CVaR) kao mjere rizika prilikom konstrukcije portfelja kriptovaluta. Naime, uspoređujući kumulativni prinos, MaxSTARR optimizacijska strategija je ostvarila viši kumulativni prinos od MaxSR optimizacijske strategije, koja za mjeru rizika uzima standardnu devijaciju, u osam od dvanaest alokacijskih modela (CRIX-O, N-1, N-3, N-4, N-7, N-8, N-9 i N-10). Dva alokacijska modela (20-F i N-5) imaju jednak kumulativni prinos između MaxSTARR i MaxSR strategija, a samo su dva alokacijska modela (N-6 i N-2) ostvarila niži kumulativni prinos. Jednako tako, usporedbom rezultata Sharpe omjera, devet od dvanaest alokacijskih modela (20-F, CRIX-O, N-1, N-3, N-4, N-7, N-8, N-9 i N-10) je ostvarilo viši omjer prinosa i standardne devijacije ukoliko je

korištena mjera rizika CVaR. Samo za alokacijske modele N-2 i N-5 Sharpe omjer MaxSTARR strategije je lošiji od MaxSR strategije. Sukladno tome, može se zaključiti da MaxSTARR optimizacijska strategija koja za mjeru rizika uzima uvjetnu rizičnost vrijednosti (CVaR), na istom uzorku podataka pruža bolje mogućnosti modeliranja portfelja od MaxSR optimizacijske strategije jer ostvaruje viši omjer prinosa i rizika, odnosno viši kumulativni prinos kao ultimativni cilj svakog investitora. Navedeno opažanje predstavlja sekundarni znanstveni, ali i praktični doprinos ovog rada unutar područja ispitivanja investicijskih mogućnosti na tržištu kriptovaluta koje do sada nije bilo ispitano tj. čiji rezultati nisu bili prezentirani na ovaj način.

Drugo zapažanje koje se navodi je važnost postojanja fundamentalnih indikatora tehnologije distribuiranog zapisa. Naime, odbacivanje druge hipoteze rada u smislu razmatranja fundamentalnih indikatora za odabir kriptovaluta kao sastavnica portfelja, nikako ne bi trebalo biti od presudne važnosti prilikom donošenja investicijskih odluka na tržištu kriptovaluta. Iako kreirani fundamentalni portfelj nije ostvario viši kumulativni prinos od CRIX indeksa, razmotreni indikatori zasigurno i dalje imaju svoju težinu u razumijevanju infrastrukture transakcijskih sustava blockchain tehnologije. Kao što je navedeno u uvodu rada, i dalje se može očekivati da će kriptovalute sa širom zajednicom imati veći broj transakcija, odnosno veći broj čvorova u mreži. Veći broj čvorova u mreži znači više distribuiran i siguran transakcijski sustav. Također, šira zajednica znači uključivanje više razvojnih programera u razvoj i implementaciju programskog koda što se očituje kroz aktivnosti na platformama za kolaboraciju razvojnih programera. Tretirati kriptovalutu kao potencijalnu investiciju bez prethodne analize fundamentalnih indikatora blockchain infrastrukture na kojoj je kriptovaluta izvedena, ima smisla jednako kao kupnja dionica bez razmatranja osnovnih financijskih pokazatelja korporacije koja je emitirala dionicu. Određeni fundamentalni indikatori kriptovaluta na kraju ipak moraju imati svoju intrinzičnu vrijednost koja će se, vjerojatno u dugom roku, reflektirati na tržišnu vrijednost kriptovalute. Zadnje navedeno otvara prostor za daljnje znanstveno istraživanje potencijalnih sistematskih faktora koji su pokretači promjene vrijednosti kriptovaluta. Trenutna kretanja promjene vrijednosti tržišta kriptovaluta se mogu pravdati kroz više teoretskih pretpostavki. Prva je da na nju utječu neki drugi fundamentalni, odnosno tehnički sistematski faktori koji još nisu definirani i ispitani stoga ostaju nepoznati. Druga je da tržište kriptovaluta ovisi isključivo o stanju

raspoloženja investitora koji svoje pozicije temelje samo na tehničkoj analizi, i treća je da vrijednost tržišta kriptovaluta definira agregatno raspoloženje investitora tradicionalnog tržišta kapitala, što se moglo uočiti tokom cijele 2020. godine. Međutim, bez obzira na razlog, činjenica je da tržište kriptovaluta i cijela njegova infrastruktura kontinuirano bilježi rast. Zbog svoje dostupnosti sve više investitora ulaže i trguje s kriptovalutama zbog čega se još više javlja potreba za istraživanjem provedenim u ovom radu kako bi se definirale investicijske mogućnosti, ali i rizici povezani s implementacijom investicijske strategije temeljene na potencijalnim fundamentalnim indikatorima.

10. ZAKLJUČAK

Primjena različitih optimizacijskih strategija na sekundarnom tržištu kriptovaluta je primarna tema ovog rada, pri čemu rezultati provedenog metodološkog pristupa višestruko doprinose razmatranju investicijskih mogućnosti. Primijenjene optimizacijske strategije su provedene unutar okvira moderne teorije portfelja i predstavljale su osnovni metodološki pristup za rješavanje problema alokacije imovine i definiranje optimalnog ulaganja. Razmatranje investicijskih mogućnosti se provelo uvažavajući određene pretpostavke koje su sudjelovale u kreiranju i oblikovanju znanstvenih hipoteza ovog rada.

Prva hipoteza rada se postavila uz pretpostavku budućeg značajnog razvoja blockchain infrastrukture, te posljedično budućeg razvoja i stabilizacije tržišta kriptovaluta kojim bi se smanjila volatilnosti i povećala tržišna vrijednost bitcoin kriptovalute u svojstvu vodećeg sistematskog faktora agregatnog tržišta kriptovaluta. Zbog toga, investitori skloni riziku i optimističnim očekivanjima, projiciraju da bi cijena jednog bitcoina u periodu od sedam do deset godina mogla doseći tržišnu vrijednost od čak milijun dolara. U tom smislu, razmatranje korisnosti modeliranja portfelja kriptovaluta kroz količinu bitcoina kao konačne vrijednosti, privlači sve više pažnje, što otvara prostora znanstvenim istraživanjima, ali i razmatranju praktičnih implikacija modeliranja portfelja u bitcoin jedinicama vrijednosti, što je predstavljalo osnovu za prvu hipotezu ovog rada. U svrhu ispitivanja prve hipoteze rada, provedeno je pet različitih optimizacijskih strategija sa pripadajućim notacijama: minimizacija varijance (MinVar-B), minimizacija uvjetne rizičnosti vrijednosti (MinCVaR-B), maksimalizacija Sharpe omjera (MaxSR-B), maksimalizacija STARR omjera (MaxSTARR-B) i maksimalizacija očekivanog prinosa (MaxMean-B), kao i naivna strategija s jednakim udjelima portfelja (EQ-W-B). Navedene strategije su odabrane kako bi se razmotrili rezultati različitih optimizacijskih ciljeva u funkciji donošenja investicijskih odluka. Sukladno prvoj hipotezi rada, cilj optimizacije portfelja je bio ostvariti kumulativni prinos viši od kriptovalute koja je ostvarila najviši kumulativni prinos od svih promatranih potencijalnih sastavnica, u istom vremenu promatranja. Potencijalne sastavnice portfelja su determinirane prema razvoju programskog koda na platformama za kolaboraciju programera i veličini potpore blockchain zajednice preko socijalnih mreža. Sukladno dobivenim i prezentiranim rezultatima, dvije

optimizacijske strategije MaxSR-B i MaxSTARR-B su ostvarile viši kumulativni prinos od kriptovalute BNB koja je imala najviši pojedinačni kumulativni prinos od svih sastavnica portfelja, te je poslužila u svojstvu indikatora ciljane profitabilnosti. Također, osim kumulativnog prinosa, tri strategije: MaxSR-B, MaxSTARR-B i MinCVaR-B su ostvarile i viši Sharpe omjer od BNB kriptovalute. S obzirom na takve rezultate, prihvaćena je prva hipoteza rada, pa se zaključuje da dinamika vrijednosti kriptovaluta izražena u bitcoinu kao jedinici valute pruža mogućnost modeliranja portfelja, odnosno primjene različitih strategija optimizacije s ciljem prikupljanja veće količine bitcoina. Osim razmatranja rezultata u domeni strogo definirane prve hipoteze rada, rezultati sugeriraju i dodatnu prednost primjene optimizacijskih strategija u ovom kontekstu koju je potrebno istaknuti. Naime, promatrajući ostvareni rizik portfelja, svih pet optimizacijskih strategija, pa i portfelj s jednakim udjelima, su ostvarili niži rizik od rizika BNB kriptovalute, izraženog kao standardna devijacija, VaR i CVaR. Sukladno tome, primjena aktivnih strategija na kriptovalutama izraženim u BTC paritetu, ne samo da pruža mogućnost ostvarenja višeg kumulativnog prinosa portfelja, već pruža i mogućnost modeliranja rizika. Ovo posljednje je posebno važno za investitore koji se odluče na ovakav investicijski pristup, ali koji nisu toliko skloni riziku, što čini dodatni znanstveni doprinos ovog rada.

Druga hipoteza rada se postavila uz pretpostavku povezanosti između fundamentalnih indikatora blockchain infrastrukture i tržišne vrijednosti kriptovaluta. Razmatranje tržišta kriptovaluta prema fundamentalnim indikatorima opravdano je teoretskom pretpostavkom o postojanju njihovog značajnog utjecaja na tržišnu vrijednosti koji bi dao prostora modeliranju očekivane vrijednosti portfelja kriptovaluta na temelju indikatora aktivnosti blockchaina. Koristi postojanja takve pozitivne veze se očituju najmanje kroz dva smjera. Prvi je svakako da bi takva pozitivna veza pružala investitorima fundamentalno uporište prilikom razmatranja potencijalnih sastavnica portfelja, čime bi se smanjio inicijalni rizik koji proizlazi iz velikog broja prijevara na tržištu kriptovaluta. Drugi je u kontekstu razmatranja sekundarnih investicijskih mogućnosti kroz modeliranje portfelja gdje bi se primjenom fundamentalnih indikatora definirale potencijalno podcijenjene kriptovalute. Sukladno navedenom, drugom hipotezom ovog istraživanja se želi dati odgovor na važno pitanje postojanja povezanosti između fundamentalnih varijabli pojedine kriptovalute i njene tržišne cijene, što se može tumačiti kao prvi korak u definiranju njihove

intrinzične vrijednosti. U svrhu ispitivanja druge hipoteze rada, provedeni su isti optimizacijski ciljevi, pri čemu su njihove notacije sljedeće: minimizacija varijance (MinVar), minimizacija uvjetne rizičnosti vrijednosti (MinCVaR), maksimalizacija Sharpe omjera (MaxSR), maksimalizacija STARR omjera (MaxSTARR) i maksimalizacija očekivanog prinosa (MaxMean), kao i naivna strategija s jednakim udjelima portfelja (EQ-W). Potencijalne sastavnice portfelja su odabrane prema razvoju programskog koda na platformama za kolaboraciju programera i veličini potpore blockchain zajednice preko socijalnih mreža, kao fundamentalnim indikatorima tržišta kriptovaluta. Sukladno drugoj hipotezi rada, primarni cilj provedbe optimizacije portfelja je bio ukazati na korisnost primjene fundamentalnih pokazatelja prilikom formiranja portfelja kriptovaluta koji bi trebao ostvariti kumulativni prinos viši od kumulativnog prinosa CRIX indeksa. Jednako tako, s obzirom da metodologija CRIX indeksa ne uključuje optimizacijske strategije, osim standardnog kretanja indeksa u svom nominalnom obliku, prezentirani su i rezultati optimizacije CRIX-a, ali i rezultati od deset portfelja čije su sastavnice uzorak od dvadeset nasumično odabranih kriptovaluta od populacije koja čini sedamdeset mogućih kriptovaluta po tržišnoj kapitalizaciji. Sukladno dobivenim i prezentiranim rezultatima, zaključuje se da na sekundarnom tržištu kriptovaluta, uvažavajući fundamentalne pokazatelje, nije moguće formirati portfelj kriptovaluta koji ostvaruje viši kumulativni prinos od kumulativnog prinosa CRIX indeksa, čime se odbacuje druga postavljena hipoteza rada.

S druge strane, razmatrajući rezultate izvan okvira druge postavljene hipoteze, te s obzirom na provedenu metodologiju koja je uključivala optimizaciju dodatnih alokacijskih modela: 20-F portfelj kreiran prema fundamentalnim indikatorima, optimiziran CRIX i deset portfelja s uzorkom od dvadeset nasumično odabranih kriptovaluta, dobiveni rezultati ipak sugeriraju prednost određenih optimizacijskih strategija koje je potrebno naglasiti, odnosno donijeti pojedine zaključke. Uspoređujući rezultate MaxSR i MaxSTARR optimizacijske strategije na istim sastavnicama portfelja, MaxSTARR optimizacijska strategija je ostvarila viši kumulativni prinos u osam od mogućih dvanaest alokacijskih modela. Dva alokacijska modela su ostvarila jednak kumulativni prinos, a samo u dva slučaja bolji rezultat je ostvarila MaxSR optimizacijska strategija. Isto tako, komparacijom rezultata Sharpe omjera na rezultatima provedenih optimizacijskih strategija, devet od dvanaest

alokacijskih modela je ostvarilo viši omjer prinosa i rizika, ukoliko se portfelj optimizirao primjenom MaxSTARR optimizacijske strategije, a samo u dva slučaja MaxSR je ostvarila viši Sharpe omjer od MaxSTARR strategije. S obzirom da MaxSTARR optimizacijska strategija kao rizik razmatra uvjetnu rizičnost vrijednosti, investitorima se sugerira davanje prednosti CVaR mjeri rizika spram standardne devijacije prilikom modeliranja portfelja na sekundarnom tržištu kriptovaluta. Provedena metodologija ispitivanja praktične implikacije različitih mjera rizika do sada nije bila razmatrana i ispitana te predstavlja sekundarni znanstveni, ali i praktični, doprinos ovog rada u području ispitivanja investicijskih mogućnosti na tržištu kriptovaluta. Jednako tako, iako se interpretacijom rezultata odbacila druga postavljena hipoteza, prilikom procesa investicijskog odlučivanja, investitorima se sugerira prethodno ispitivanje kvalitete matične blockchain infrastrukture kriptovalute uvidom u veličinu zajednice koja ju podržava i aktivnostima na platformama za razvoj programskog koda, kako bi se preuzeti rizik investiranja sveo na što nižu razinu. Kao prijedlog daljnjeg istraživanja, sugerira se ispitivanje reakcije portfelja na odabir kriptovaluta kao sastavnica kroz druge sistematske varijable i fundamentalne indikatore koji bi potencijalno mogli biti pokretači intrinzične vrijednosti pojedinačne kriptovalute, ali i agregatnog tržišta kriptovaluta. S obzirom na kontinuirani razvoj i aktivnosti tržišta kriptovaluta, postojanje takvih indikatora nije upitno, ali je još uvijek nepoznato. Njihova identifikacija bi doprinijela akademskoj zajednici kao poticaj za daljnja istraživanja, ali i u procesu investiranja kroz praktičnu implikaciju dobivenih rezultata, što bi posredno pozitivno utjecalo na stabilan i fundamentalan rast tržišta kriptovaluta te manji rizik, ali i sigurniji daljnji razvoj cjelokupne financijske industrije na blockchain infrastrukturi.

LITERATURA

Knjige

1. Antonopoulos, A. M. (2017) „Mastering Bitcoin: Programming the Open Blockchain“. O'Reilly Media, Inc., Boston, MA

2. Bacon, C. (2008) „Practical Risk-adjusted Performance Measurement“. John Wiley & Sons, Ltd. United Kingdom

3. Bashir, I. (2017) „Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition“. Packt Publishing. Birmingham, ISBN: 9781788839044

4. Dhillon, V., Metcalf, D. & Hooper, M. (2017) „Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You“. Apress, Berkeley, DOI: https://doi.org/10.1007/978-1-4842-3081-7

5. Franco, P. (2015) „Understanding Bitcoin Cryptography, engineering, and economics“. John Wiley & Sons Ltd, Chichester

6. Furneaux, N. (2018) „Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence“. John Wiley & Sons Ltd, Chichester

7. Gates. M. (2017) „Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money“. CreateSpace Independent Publishing Platform, North Charleston, ISBN 1547090685, 9781547090686

8. Judmayer, A., Stifter, N., Krombholz, K., & Weippl, E. (2017) „Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms“. Morgan and Claypool, San Rafael, California

9. Kuo Chuen, D. L & Low, L. (2018) „Inclusive FinTech:Blockchain, Cryptocurrency and ICO“. World Scientific Books, World Scientific Publishing Co. Pte. Ltd., Singapore, https://doi.org/10.1142/10949

10. Lau, D., Lau, D., Jin Teh, S., Kho, K., Azmi, E., Lee, TM. i Ong, B. (2020) „How to DeFi, 1st Edition“. Kindle Edition ed. [E-book]

11. Pachamanova, D. & Fabozzi, F. (2016) „Portfolio Construction and Analytics“. John Wiley & Sons, Inc., Hoboken, New Jersey

12. Pfaff, B. (2016) „Financial Risk Modelling and Portfolio Optimization with R“. John Wiley & Sons, Ltd. DOI:10.1002/9781118477144. United Kingdom

13. Quest, M. (2018) „Cryptocurrency Master: Everything You Need To Know About Cryptocurrency and Bitcoin Trading, Mining, Investing, Ethereum, ICOs, and the Blockchain“. CreateSpace Independent Publishing Platform, North Charleston, SC, USA. ISBN:978-1-7219-6163-4

Poglavlja u knjizi

1. Pak Nian, L., & Kuo Chuen, D. L. (2015) „Introduction to Bitcoin". Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Elsevier, pp. 5-30. Collection Lee Kong Chian School Of Business. (DOI): 10.3386/w19747Research

2. Yermack, D. (2015) „Is Bitcoin a Real Currency?” Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Elsevier, pp. 31-44. Collection Lee Kong Chian School Of Business. (DOI): 10.3386/w19747Research

Članci

1. Artzner, P., Delbaen, F., Eber, J.M. & Heath, D. (1999) „Coherent Measures of Risk“. Mathematical Finance. no 9. pp. 203 - 228. DOI: https://doi.org/10.1111/1467-9965.00068

2. Brauneis, A., & Mestelb, R. (2018) „Cryptocurrency-portfolios in a mean-variance framework“, Finance Research Letters, vol. 28, pp. 259–264

3. Briere, M., Oosterlinck, K. & Szafarz, A. (2013) „Virtual currency, tangible return: Portfolio diversication with bitcoins“, Journal of Asset Management, vol.16, no. 6, pp. 365–373

4. Carpenter, A. (2016) „Portfolio diversification with Bitcoin“, Journal of Undergraduate Research in France, vol. 6, no. 1, pp. 1-27

5. Chaum, D. (1983) „Blind signatures for untraceable payments“, In Advances in Cryptology, pp. 199–203. Springer, DOI: 10.1007/978-1-4757-0602-4_18

6. Chaum, D. (1985) „Security without identification: Transaction systems to make big brother obsolete“. vol 28, pp. 1030–1044. DOI: 10.1145/4372.4373

7. Chaum, D., Fiat, A. and Naor, M. (1990) „Untraceable electronic cash“, In Proc. on Advances in Cryptology, pp. 319–327. Springer-Verlag, New York, 1990. DOI: 10.1007/0-387-34799-2_25

8. Chuen, D. L. K., Guo, L. & Wang, Y. (2017) „Cryptocurrency: A New Investment Opportunity?“, The Journal of Alternative Investments, vol. 20, no. 3, pp. 16–40

9. Čičak, J. (2019) „Računovodstveno procesiranje kriptovaluta“, Računovodstvo, revizija i financije, vol 29, no. 1, pp. 57-62

10. Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. & Siering, M. (2014) „Bitcoin - Asset or currency? Revealing users' hidden intentions. ECIS 2014 Proceedings - 22nd European Conference on Information Systems. vol. 3, pp. 1-14

11. Hu, H. T. C. (2012) „Too Complex to Depict? Innovation, 'Pure Information,' and the SEC Disclosure Paradigm“. Texas Law Review, vol. 90, no. 7, Available at SSRN: https://ssrn.com/abstract=2083708

12. Jensen, M.C. (1968) „The Performance of Mutual Funds in the Period 1945-1964“. Journal of Finance vol. 23, no. 2, pp. 389-416, https://doi.org/10.1111/j.1540-6261.1968.tb00815.x

13. Kajtazi, A., & Moro, A. (2019) „The role of bitcoin in well diversified portfolios: A comparative global study“, International Review of Financial Analysis, vol. 61, pp. 143–157

14. Klein, T., Hien, P. & Walther, T. (2018) „Bitcoin Is Not the New Gold: A Comparison of Volatility, Correlation, and Portfolio Performance“. International Review of Financial Analysis, vol. 59, pp. 105-116

15. Liu, W. (2018) „Portfolio Diversification across Cryptocurrencies“, Finance Research Letters, vol. 29, pp. 200-205

16. Markowitz, H. (1952) „Portfolio selection“, The journal of finance, vol. 7, no. 1, pp. 77-91

17. Modigliani, F. & Modigliani, L. (1997) „Risk-Adjusted Performance“. Journal of Portfolio Management, vol. 23, no. 2, pp. 45–54. DOI: https://doi.org/10.3905/jpm.23.2.45

18. Platanakis, E., Sutcliffeb, C. & Urquhartc, A. (2018) „Optimal vs naïve diversification in cryptocurrencies“, Economics Letters, vol. 171, pp. 93-96

19. Rockafellar, R. & Uryasev, S. (2000) „Optimization of conditional value-at-risk“. The Journal of Risk, vol 2, no. 3, pp. 21–41. DOI: 10.21314/JOR.2000.038

20. Rockafellar, R. & Uryasev, S. (2002) „Conditional value-at-risk for general loss distributions“. Journal of Banking & Finance, vol. 26, no 7, pp. 1443-1471. DOI: https://doi.org/10.1016/S0378-4266(02)00271-6

21. Sharpe, W. (1963) „A Simplified Model for Portfolio Analysis“. Management Science, vol. 9, no. 2. pp. 277-293. http://www.jstor.org/stable/2627407

22. Symitsi, E. & Chalvatzis, K.J. (2018) „The Economic Value of Bitcoin: A Portfolio Analysis of Currencies, Gold, Oil and Stocks“, Research in International Business and Finance, vol. 48. pp. 97-110

23. Treynor, J.L. (1965) „How to Rate Management of Investment Funds“. Harvard Business Review, vol. 43, no. 1, pp. 63-75. ISSN 0017-8012, ZDB-ID 2382-6.

24. Vaughan, E. & Vaughan T (1998) „Rizici i upravljanje rizicima” (prijevod), Poslovni savjetnik, br. 11-12/98., Zagreb

Doktorski, magistarski i specijalistički završni radovi

1. Kisiala, J. (2015) „Conditional Value-at-Risk: Theory and Applications“, Dissertation Presented for the Degree of MSc in Operational Research, University of Edinburgh. Available at https://www.researchgate.net/publication/283471536_Conditional_Value-at-Risk_Theory_and_Applications

2. Trgo, A. (2015) „Uvjetna rizičnost vrijednosti (CVaR) u procjeni rizika na hrvatskom tržištu kapitala“, Završni rad, Ekonomski fakultet u Splitu. Available athttps://repozitorij.efst.unist.hr/islandora/object/efst%3A970/datastream/PDF/view

3. Trimborn, S. (2015) „Towards Cryptocurrency Index – Analysis of the market“, Master’s Thesis, Humboldt-Universität zu Berlin. Available at https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.870.4305&rep=rep1&type=pdf

4. Žiković, S. (2005) „Formiranje optimalnog portfelja hrvatskih dionica i mjerenje tržišnog rizika primjenom VaR metode“, magistarski rad, Sveučilište u Ljubljani. Available at http://www.cek.ef.uni-lj.si/magister/zikovic513.pdf

Ostali izvori

1. Alexander, C. & Sheedy, E. (2005) „The professional risk managers' handbook: a comprehensive guide to current theory and best practices“. PRMIA Publications, New York & London. ISBN 9780976609704

2. Andersen, N. (2016) „Blockchain Technology A game-changer in accounting?“ https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

3. Back, A. (2002) „Hashcash—a Denial of Service Counter-measure“. www.hashcash.org/papers/hashcash.Pdf

4. Čičin-Šain, N. (2017) „Oporezivanje bitcoina“. Zbornik Pravnog fakulteta u Zagrebu, 67 (3-4), pp. 655-693. Preuzeto s https://hrcak.srce.hr/186941
5. Dai, W. (1998) „b-money“. www.weidai.com/bmoney.txt

6. EBA Report (2019) „Report on crypto-assets - Report with advice for the European Commission“. https://eba.europa.eu/eba-reports-on-crypto-assets

7. Eigelshoven, F., Ullrich, A. & Bender, B. (2020) „Public blockchain – a systematic literature review on the sustainability of consensus algorithm“. Twenty-Eighth European Conference on Information Systems (ECIS2020) – A

Virtual AIS Conference, Marrakech, Morocco. pp. 1-19, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1201&context=ecis2020_rp

8. Eisl, A., Gasser, S. & Weinmayer, K. (2015) „Caveat emptor: Does bitcoin improve portfolio diversication?“ Working Paper, WU. Available at SSRN: https://ssrn.com/abstract=2408997 or http://dx.doi.org/10.2139/ssrn.2408997

9. Elendner, H., Trimborn, S., Ong, B. & Lee, T. M., (2016) „The Cross-Section of Crypto-Currencies as Financial Assets: An Overview“. SFB 649 Discussion paper 2016-038. Berlin: Humboldt-Universit¨at zu Berlin. Available at http://hdl.handle.net/10419/148874

10. ESMA (2019) „Annex 1 Legal qualification of crypto-assets – survey to NCAs. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf

11. European Central Bank (2012) „Virtual currency schemes“. Frankfurt am Main: European Central Bank. Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

12. Finney, H. (2004) „RPOW—Reusable Proofs of Work“. www.finney.org/~hal/rpow/

13. Gervais, A., Karame, G., Capkun, V. & Capkun, S. (2014) „Is Bitcoin a decentralized currency?“. https://eprint.iacr.org/2013/829.pdf

14. Härdle, Wolfgang, K., Harvey, C. R., & Reule, R. C. G., (2019) „Understanding Cryptocurrencies“. Available at SSRN: https://ssrn.com/abstract=3360304 or http://dx.doi.org/10.2139/ssrn.3360304

15. Hileman, Garrick. (2014) „From Bitcoin to the Brixton Pound: History and Prospects for Alternative Currencies“ (Poster Abstract). 8438. 163-165. 10.1007/978-3-662-44774-1_13

16. Houben, R. & Snyers, A. (2018) „Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion“. publication office of the european union. DOI 10.2861/263175. https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

17. Jabotinsky, H. Y., (2018) „The Regulation of Cryptocurrencies - Between a Currency and a Financial Product“. Hebrew University of Jerusalem Legal Research Paper No. 18-10, Available at SSRN: https://ssrn.com/abstract=3119591 or http://dx.doi.org/10.2139/ssrn.3119591

18. Lynn, D. & Sabbagh, H. (2012) „The jobs act opens door for crowdfunding offerings“. https://www.sociallyawareblog.com/2012/04/05/the-jobs-act-opensdoor-for-crowdfunding-offerings/

19. Nakamoto, S. (2008) „Bitcoin: A Peer-to-Peer Electronic Cash System“ https://bitcoin.org/bitcoin.pdf

20. Petukhina, A., Trimborn, S., Härdle, Wolfgang, K. & Elendner, H. (2018) „Investing with Cryptocurrencies – evaluating the potential of portfolio allocation strategies“, IRTG 1792 Discussion Paper 2018-058. Berlin: Humboldt-Universität zu Berlin

21. Rockafellar, R. & Uryasev, S. (1999) „Optimization of conditional value-at-risk“. Research Report 99-4, Department of Industrial and Systems Engineering, University of Florida, http://janroman.dhis.org/finance/VaR/cvar2.pdf

22. Sander, T., Ta-Shma, A. (1999) „Auditable, Anonymous Electronic Cash“. www.cs.tau.ac.il/~amnon/Papers/ST.crypto99.pdf

23. Shrivastava, G. & Le, D.N. & Sharma, K. (2020) „Call for Edited Book Chapters: Cryptocurrencies and Blockchain Technologies and Applications:

Decentralization and Smart Contracts“ Wiley & Sons, Ltd., Due date 15 May 2019

24. Szabo, N. (1998) „Bit Gold“. http://unenumerated.blogspot.com/2005/12/bit-gold.html

25. Szabo, N. (1998) „Secure Property Titles with Owner Authority“. https://nakamotoinstitute.org/secure-property-titles/

26. Trimborn, S., Li, M. & Härdle, Wolfgang, K. (2017) „Investing with Cryptocurrencies - A Liquidity Constrained Investment Approach“, SFB 649 Discussion paper 2017-014. Berlin: Humboldt-Universität zu Berlin

27. Trimborn, S., Li, M. & Härdle, Wolfgang, K. (2018) „Investing with Cryptocurrencies - A Liquidity Constrained Investment Approach“, SFB 649 Discussion paper 2017-014. Berlin: Humboldt-Universität zu Berlin. http://hdl.handle.net/10419/169204

Internetski izvori

1. https://1inch.exchange/#/
2. https://aeternity.com/
3. https://airdrops.io/
4. https://bitcoin-mjenjacnica.hr/#exchange
5. https://cointelegraph.com/news/someone-transferred-a-billion-dollars-in-bitcoin-for-less-than-5
6. https://compound.finance/
7. https://compound.finance/markets
8. https://crypthena.com/ico-pools/
9. https://defiprime.com/defi-rates
10. https://defipulse.com/
11. https://defisaver.com/

12. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
13. https://en.wikipedia.org/wiki/Proof_of_stake
14. https://enterprise.gem.co/health/
15. https://entethalliance.org/
16. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595027276299&uri=PI_COM:Ares(2019)7834655
17. https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:02009L0110-20180113&from=EN
18. https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:02009L0110-20180113&from=EN
19. https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014L0065&qid=1595031226028&from=EN
20. https://followmyvote.com/
21. https://fortune.com/2017/09/05/maersk-blockchain-insurance/
22. https://github.com/
23. https://guardtime.com/
24. https://hr.wikipedia.org/wiki/Metapodatci
25. https://innovation-guide.sap.com/?technologies=Blockchain
26. https://innovation-guide.sap.com/joint-venture-accounting
27. https://itsa.global/
28. https://labs.imaginea.com/utxo/#utxo-transaction-model
29. https://makerdao.com/en/
30. https://masternodes.online/
31. https://medium.com/@tozex/the-five-biggest-ico-scams-54967ec92b87
32. https://medium.com/defi-saver/black-thursday-at-defi-saver-3c35ea6cd0d0
33. https://mkr.tools/governance/stabilityfee
34. https://nexo.io/earn-interest
35. https://nexusmutual.io/
36. https://opyn.co/#/
37. https://remme.io/
38. https://sablier.finance/
39. https://sh.wikipedia.org/wiki/Elektronski_potpis

40. https://stoscope.com/
41. https://synthetix.exchange/#/
42. https://synthetix.exchange/#/synths/sDEFI
43. https://tether.to/
44. https://thecrix.de
45. https://theicon.ist/2019/11/05/a-comprehensive-look-at-iconloops-myid-alliance-its-partners-advisors-and-upcoming-roadmap/
46. https://trustswap.org/
47. https://ujomusic.com/
48. https://uphold.com/
49. https://venturebeat.com/wp-content/uploads/2010/05/sa33.pdf
50. https://wallet.bitshares.org/#/asset/USD
51. https://www.barclayscorporate.com/insights/innovation/what-does-blockchain-do/
52. https://www.blockchain.com/btc/block/000000000000000000007f9b5d85f191a25923182c1f1945328e11eac591dd5ab
53. https://www.buybitcoinworldwide.com/
54. https://www.ccn.com/jiocoin-indias-biggest-conglomerate-launch-cryptocurrency/
55. https://www.coindesk.com/ethereum-classic-suffers-second-51-attack-in-a-week
56. https://www.coindesk.com/tether-review-claims-crypto-asset-fully-backed-theres-catch
57. https://www.coingecko.com/
58. https://www.dcode.fr/random-sampling
59. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf
60. https://www.fina.hr/-/financijska-agencija-dobila-odobrenje-za-rad-novog-platnog-sustava-nksinst
61. https://www.hnb.hr/-/obavijest-o-pocetku-rada-nksinst-platnog-sustava
62. https://www.hyperledger.org/use/distributed-ledgers
63. https://www.investor.gov/introduction-investing/investing-basics/glossary/regulation-crowdfunding
64. https://www.johndcook.com/blog/2018/08/14/bitcoin-elliptic-curves/

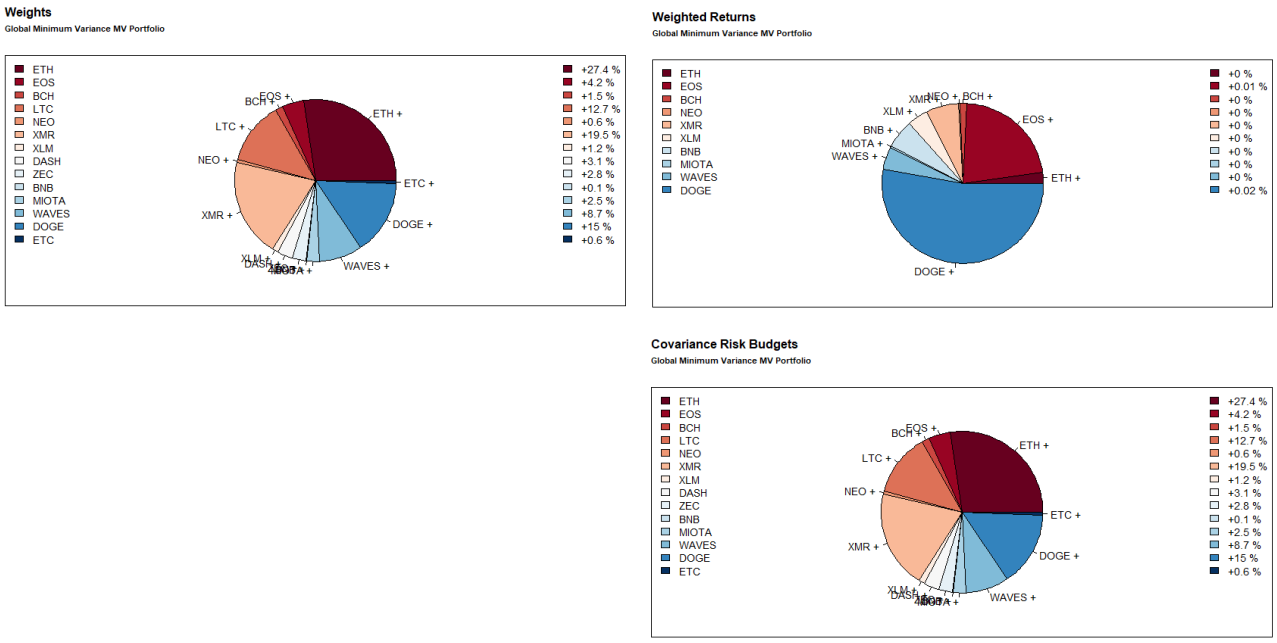
65. https://www.media.mit.edu/research/groups/1454/medrec
66. https://www.nyse.com/publicdocs/nyse/regulation/nyse/sea34.pdf
67. https://www.openbazaar.org/
68. https://www.pooltogether.com/
69. https://www.poslovni.hr/trzista/george-mijenja-postojece-aplikacije-erstea-4253123
70. https://www.provenance.org/whitepaper
71. https://www.renewableenergyworld.com/2018/02/16/blockchain-could-change-everything-for-energy/#gref
72. https://www.rrif.hr/Porezni_tretman_kapitalnih_dobitaka_po_osnovi_trgo-3543-misljenje.html
73. https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets
74. https://www.sec.gov/fast-answers/answers-regdhtm.html
75. https://www.securexfilings.com/regulation-a/
76. https://www.stakingrewards.com/
77. https://www.technologyreview.com/2020/01/30/275964/cryptocurrency-ponzi-scams-chainalysis/
78. https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison
79. https://www.tokensets.com/
80. https://www.tportal.hr/tehno/clanak/bacio-milijune-u-bitkoinima-u-smece-20131128
81. https://www.zdnet.com/article/could-blockchain-run-a-city-state-inside-dubais-blockchain-powered-future/
82. https://xinfin.org/

POPIS TABLICA

POPIS SHEMA

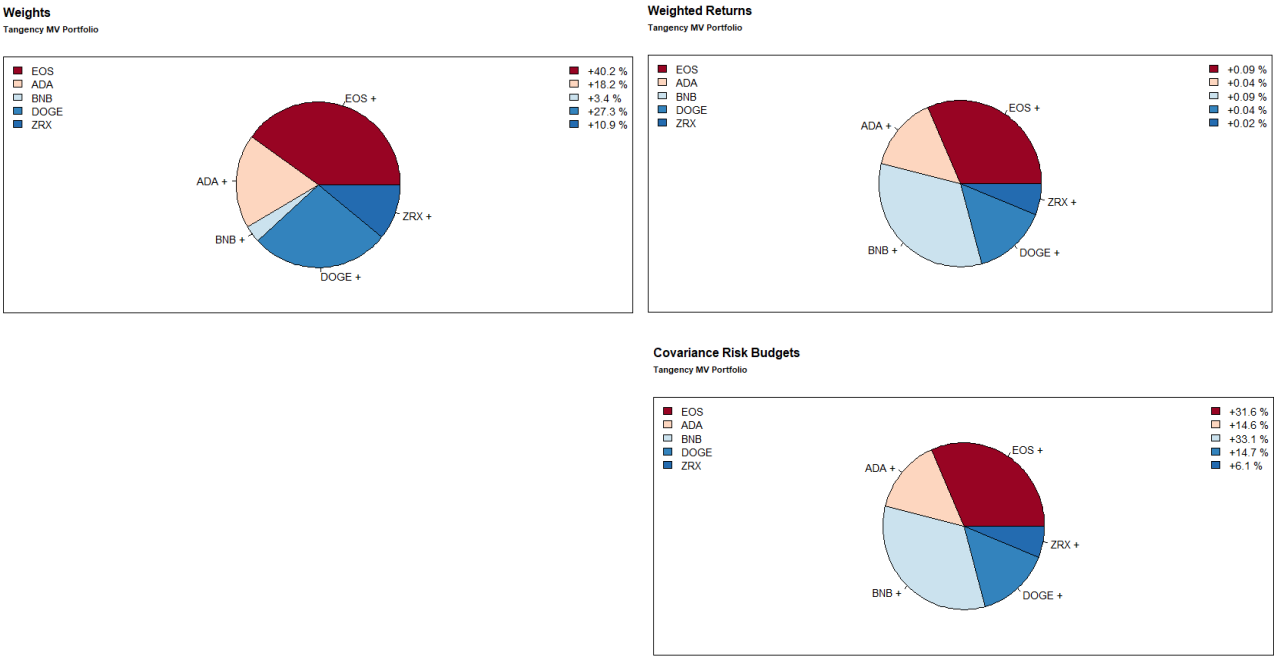
POPIS GRAFIKONA

PRILOG



Grafikon 10. Ilustracija rezultata optimizacije – MinVar-B portfelj

Izvor: Izrada autora

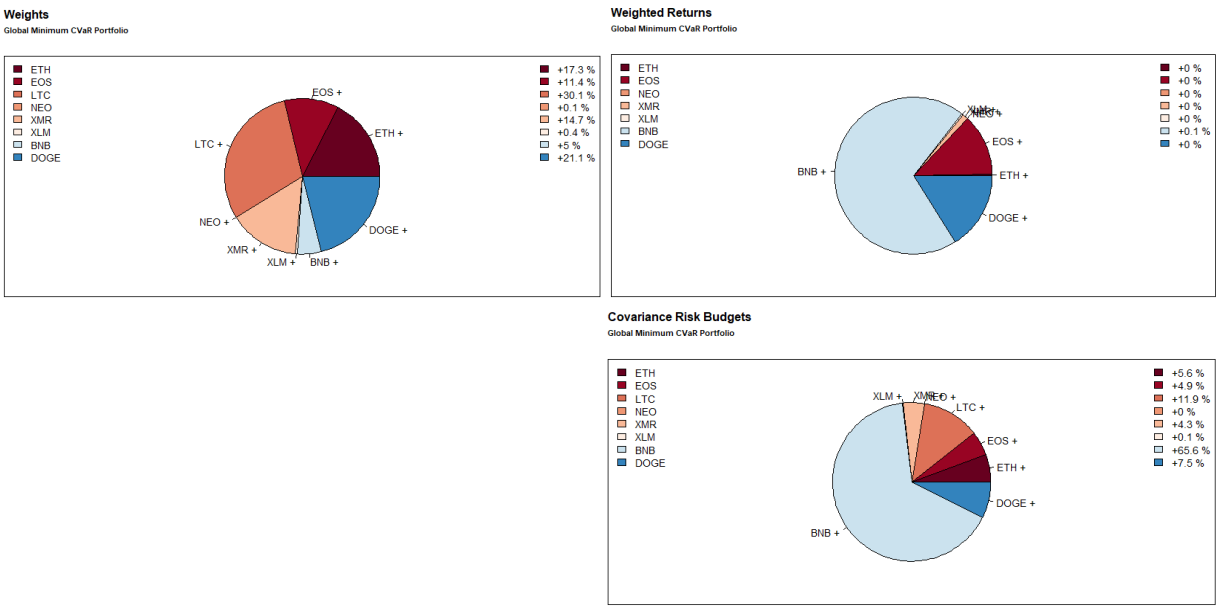


Grafikon 11. Ilustracija rezultata optimizacije – MaxSR-B portfelj

Izvor: Izrada autora

Grafikon 12. Ilustracija rezultata optimizacije – MaxMean-B portfelj

Izvor: Izrada autora

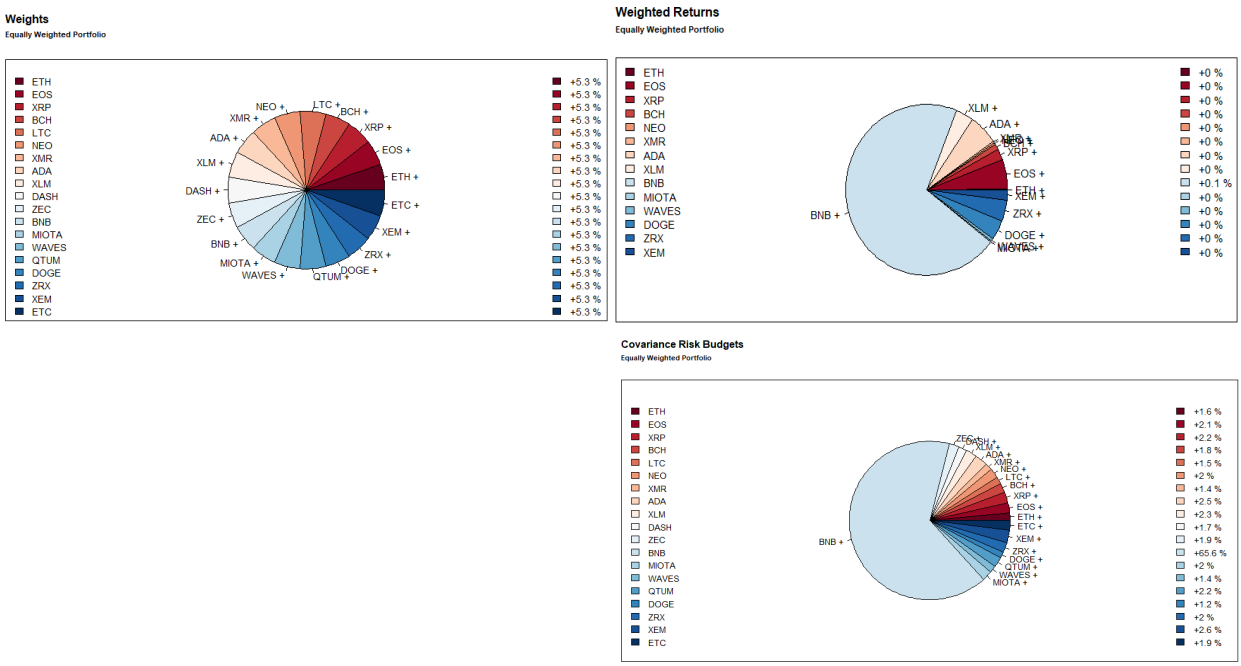


Grafikon 13. Ilustracija rezultata optimizacije – MinCVaR-B portfelj

Izvor: Izrada autora

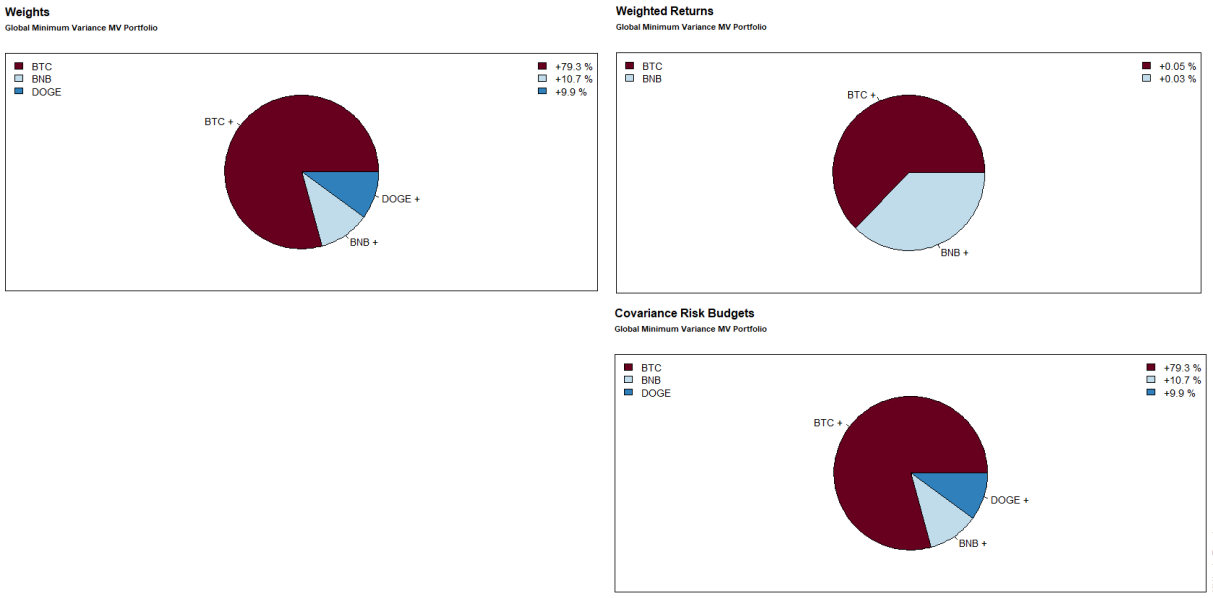
Grafikon 14. Ilustracija rezultata optimizacije – MaxSTARR-B portfelj

Izvor: Izrada autora



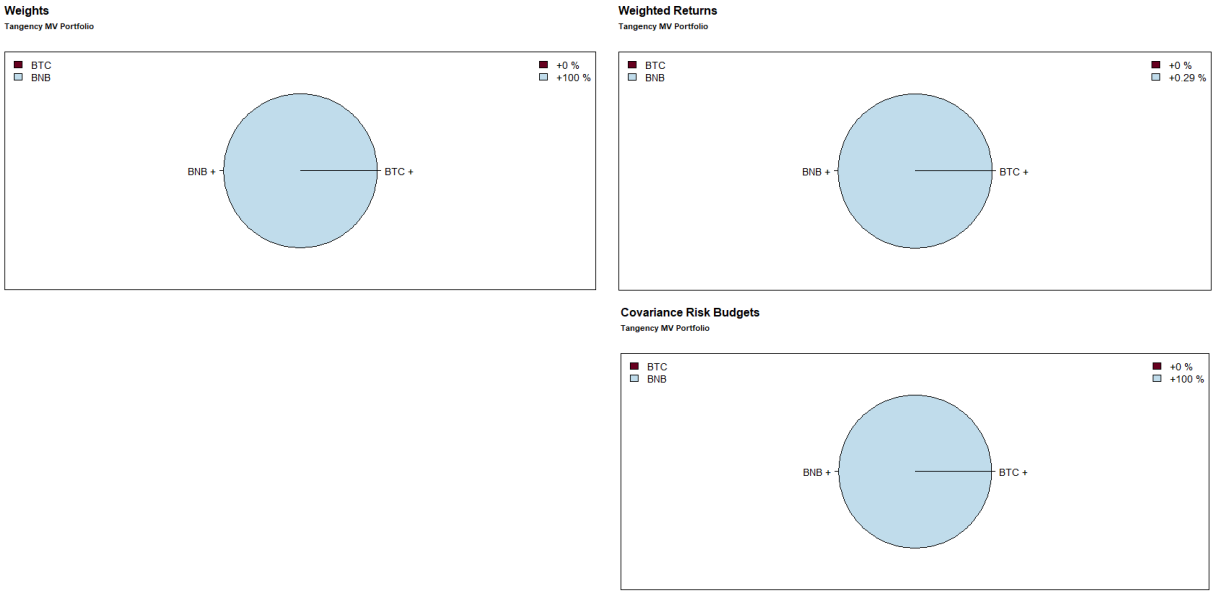
Grafikon 15. Ilustracija rezultata optimizacije – EQ-W-B portfelj

Izvor: Izrada autora



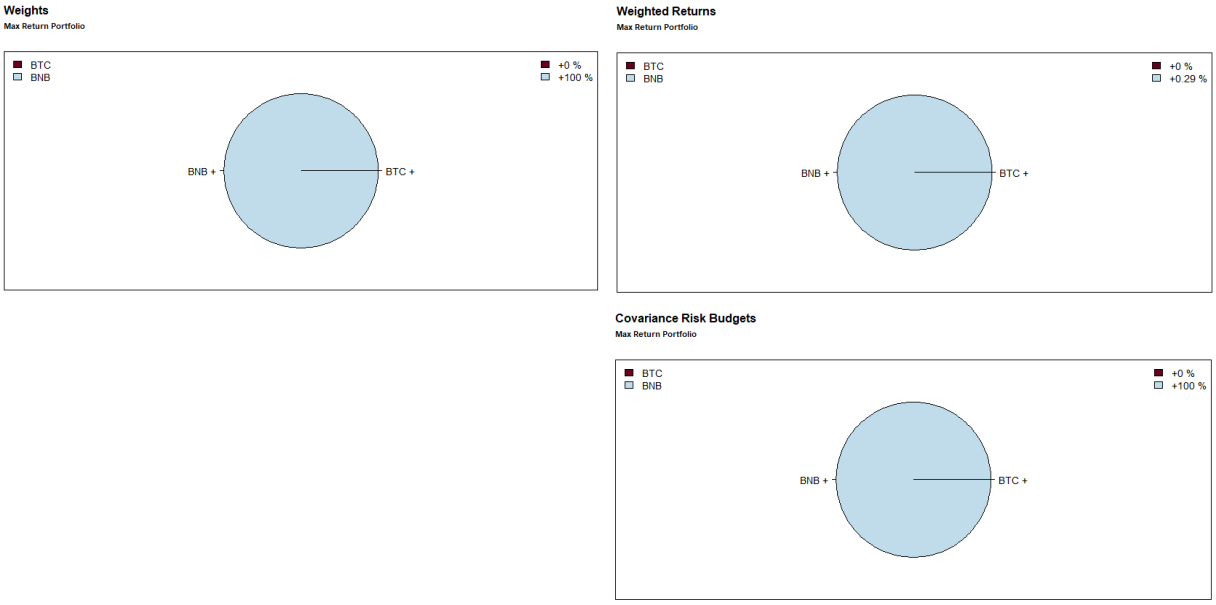
Grafikon 16. Ilustracija rezultata optimizacije – MinVar portfelj

Izvor: Izrada autora



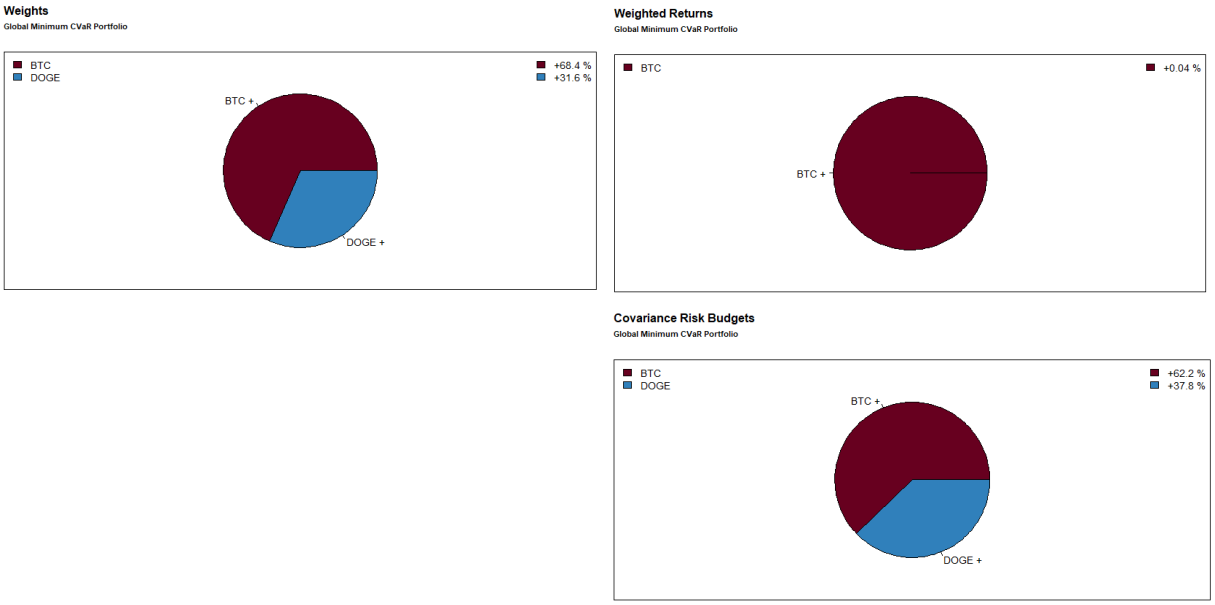
Grafikon 17. Ilustracija rezultata optimizacije – MaxSR portfelj

Izvor: Izrada autora



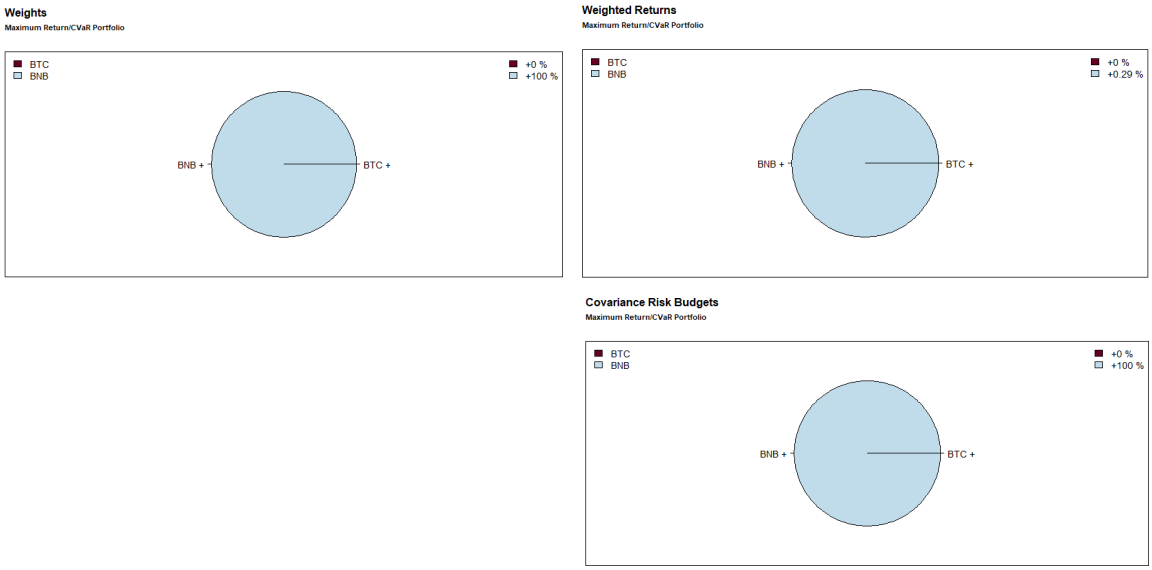
Grafikon 18. Ilustracija rezultata optimizacije – MaxMean portfelj

Izvor: Izrada autora



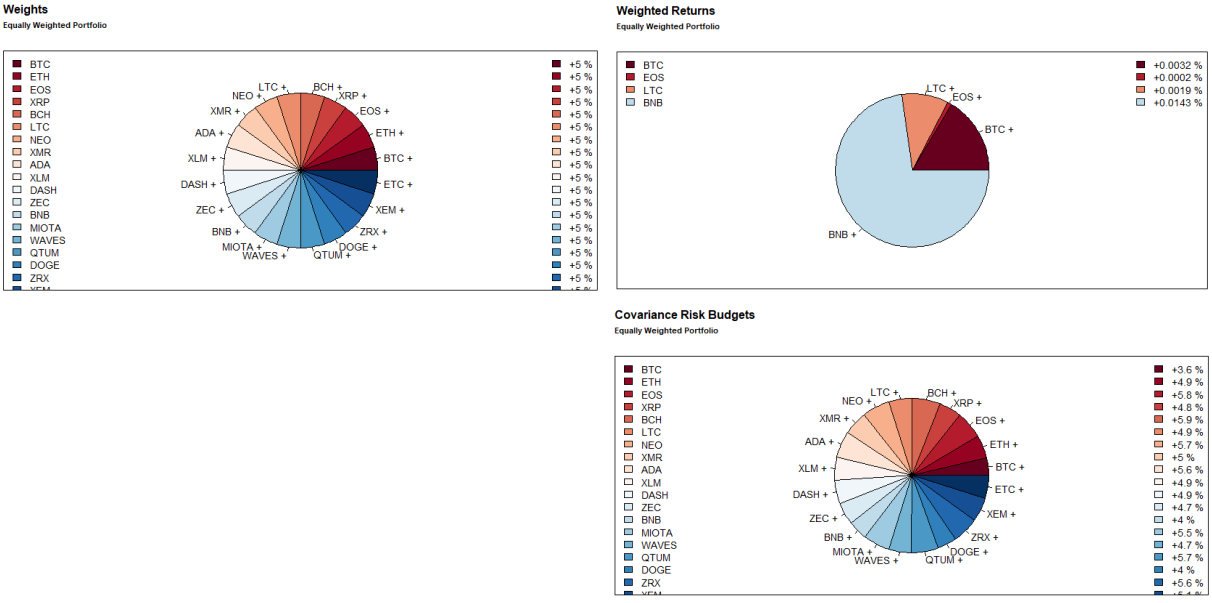
Grafikon 19. Ilustracija rezultata optimizacije – MinCVaR portfelj

Izvor: Izrada autora



Grafikon 20. Ilustracija rezultata optimizacije – MaxSTARR portfelj

Izvor: Izrada autora



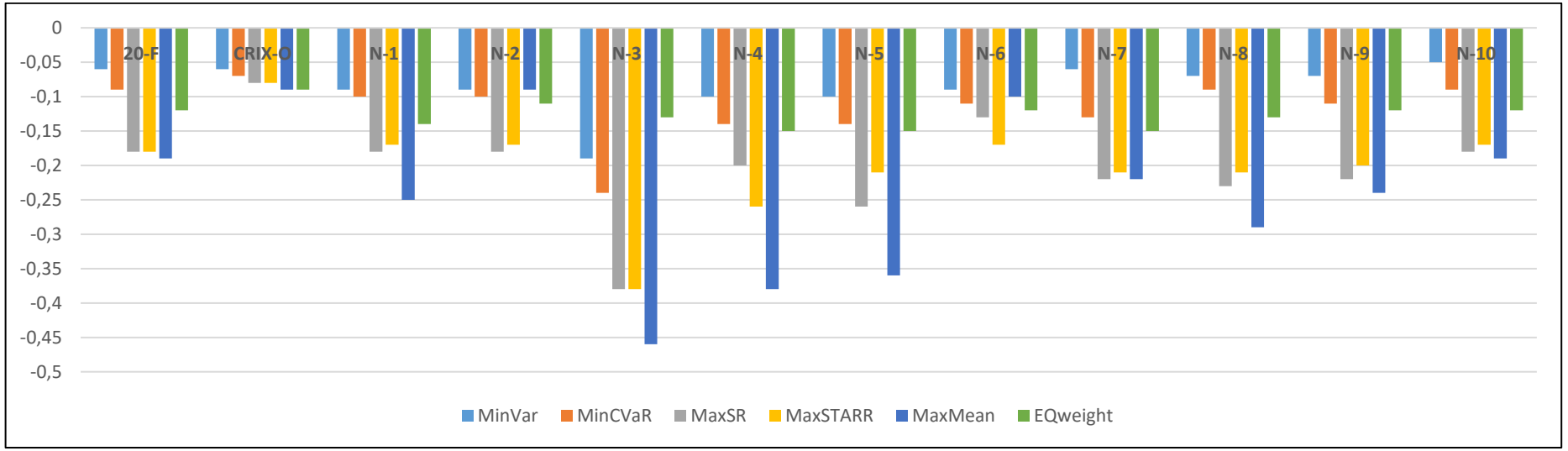
Grafikon 21. Ilustracija rezultata optimizacije – EQ-W portfelj

Izvor: Izrada autora

Tablica 10. Usporedni prikaz rezultata regresijskog pravca β_i između prinosa modela alokacije i CRIX-a. Vrijednost CRIX: 1

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,06	-0,06	-0,09	-0,09	-0,19	-0,10	-0,10	-0,09	-0,06	-0,07	-0,07	-0,05
MinCVaR	-0,09	-0,07	-0,10	-0,10	-0,24	-0,14	-0,14	-0,11	-0,13	-0,09	-0,11	-0,09
MaxSR	-0,18	-0,08	-0,18	-0,18	-0,18	-0,20	-0,26	-0,13	-0,22	-0,23	-0,22	-0,18
MaxSTARR	-0,18	-0,08	-0,17	-0,17	-0,38	-0,26	-0,21	-0,17	-0,21	-0,21	-0,20	-0,17
MaxMean	-0,19	-0,09	-0,25	-0,09	-0,46	-0,38	-0,36	-0,10	-0,22	-0,29	-0,24	-0,19
EQweight	-0,12	-0,09	-0,14	-0,11	-0,13	-0,15	-0,15	-0,12	-0,15	-0,13	-0,12	-0,12

Grafikon 22. Ilustracija rezultata regresijskog pravca β_i između prinosa modela alokacije i CRIX-a

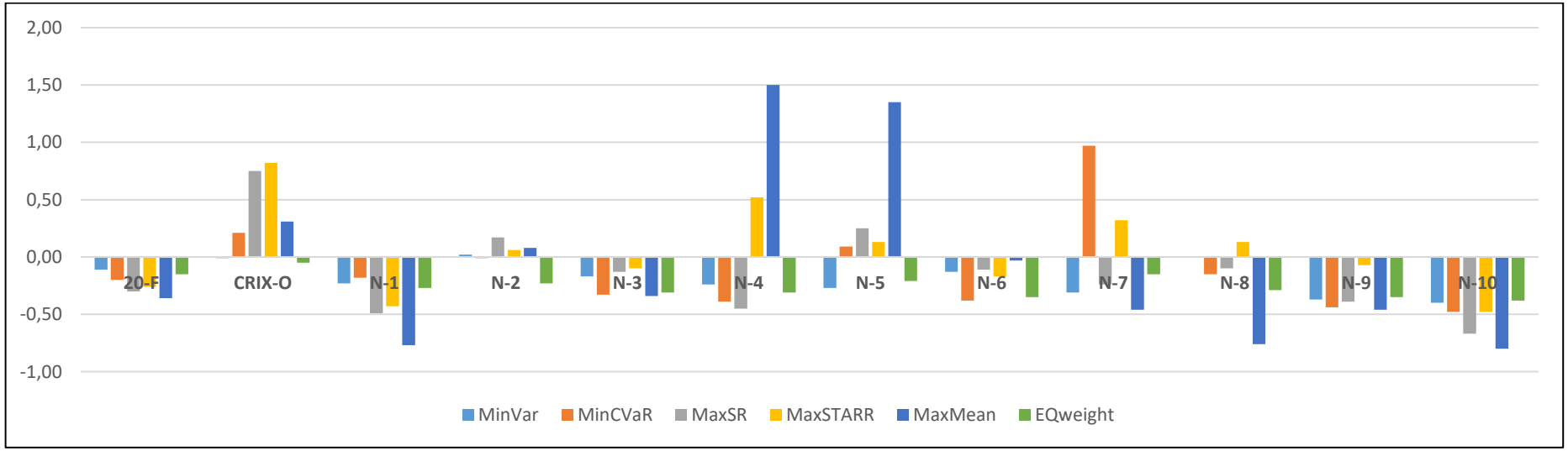


Izvor: Izrada autora

Tablica 11. Usporedni prikaz rezultata godišnjeg regresijskog odsječka $a_{a,i}$ između modela alokacije i CRIX-a. Vrijednost CRIX: 0

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,11	-0,01	-0,23	0,02	-0,17	-0,24	-0,27	-0,13	-0,31	0,00	-0,37	-0,40
MinCVaR	-0,20	0,21	-0,18	-0,01	-0,33	-0,39	0,09	-0,38	0,97	-0,15	-0,44	-0,48
MaxSR	-0,30	0,75	-0,49	0,17	-0,13	-0,45	0,25	-0,11	-0,24	-0,10	-0,39	-0,67
MaxSTARR	-0,26	0,82	-0,43	0,06	-0,10	0,52	0,13	-0,17	0,32	0,13	-0,07	-0,48
MaxMean	-0,36	0,31	-0,77	0,08	-0,34	1,50	1,35	-0,03	-0,46	-0,76	-0,46	-0,80
EQweight	-0,15	-0,05	-0,27	-0,23	-0,31	-0,31	-0,21	-0,35	-0,15	-0,29	-0,35	-0,38

Grafikon 23. Ilustracija rezultata godišnjeg regresijskog odsječka a_{ai} između modela alokacije i CRIX-a

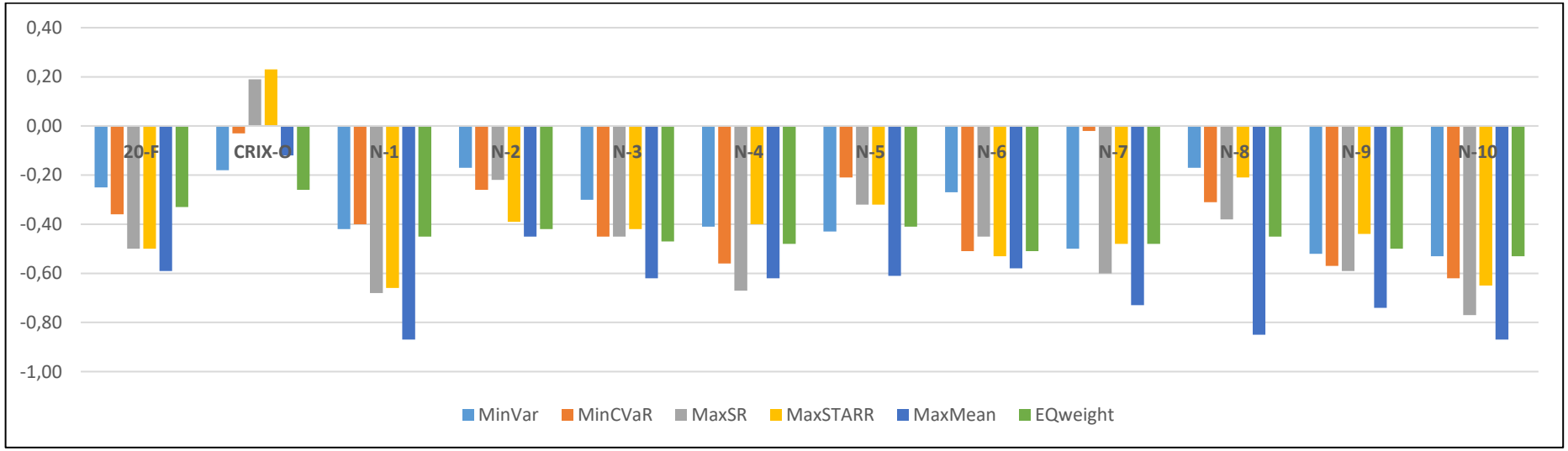


Izvor: Izrada autora

Tablica 12. Usporedni prikaz rezultata godišnjeg geometrijskog prinosa $R_{G,i}$. Vrijednost CRIX: -0,18

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,25	-0,18	-0,42	-0,17	-0,30	-0,41	-0,43	-0,27	-0,50	-0,17	-0,52	-0,53
MinCVaR	-0,36	-0,03	-0,40	-0,26	-0,45	-0,56	-0,21	-0,51	-0,02	-0,31	-0,57	-0,62
MaxSR	-0,50	0,19	-0,68	-0,22	-0,45	-0,67	-0,32	-0,45	-0,60	-0,38	-0,59	-0,77
MaxSTARR	-0,50	0,23	-0,66	-0,39	-0,42	-0,40	-0,32	-0,53	-0,48	-0,21	-0,44	-0,65
MaxMean	-0,59	-0,12	-0,87	-0,45	-0,62	-0,62	-0,61	-0,58	-0,73	-0,85	-0,74	-0,87
EQweight	-0,33	-0,26	-0,45	-0,42	-0,47	-0,48	-0,41	-0,51	-0,48	-0,45	-0,50	-0,53

Grafikon 24. Ilustracija rezultata godišnjeg geometrijskog prinosa R_{Gi}

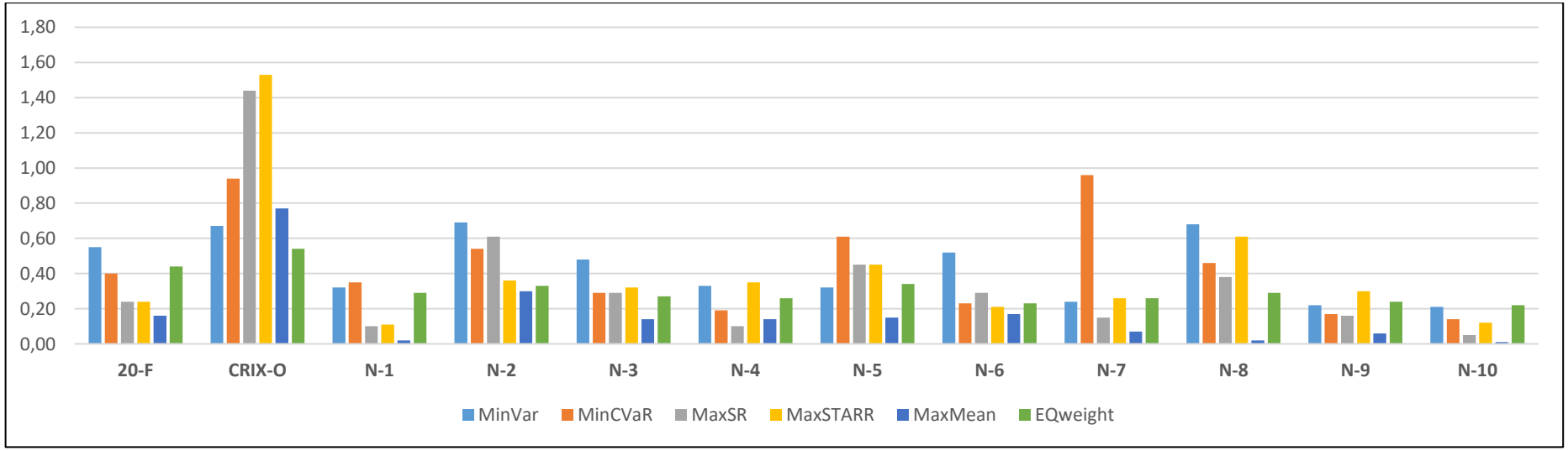


Izvor: Izrada autora

Tablica 13. Usporedni prikaz rezultata kumulativnog prinosa CY. Vrijednost CRIX: 0,66

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	0,55	0,67	0,32	0,69	0,48	0,33	0,32	0,52	0,24	0,68	0,22	0,21
MinCVaR	0,40	0,94	0,35	0,54	0,29	0,19	0,61	0,23	0,96	0,46	0,17	0,14
MaxSR	0,24	1,44	0,10	0,61	0,29	0,10	0,45	0,29	0,15	0,38	0,16	0,05
MaxSTARR	0,24	1,53	0,11	0,36	0,32	0,35	0,45	0,21	0,26	0,61	0,30	0,12
MaxMean	0,16	0,77	0,02	0,30	0,14	0,14	0,15	0,17	0,07	0,02	0,06	0,01
EQweight	0,44	0,54	0,29	0,33	0,27	0,26	0,34	0,23	0,26	0,29	0,24	0,22

Grafikon 25. Ilustracija rezultata kumulativnog prinosa CY

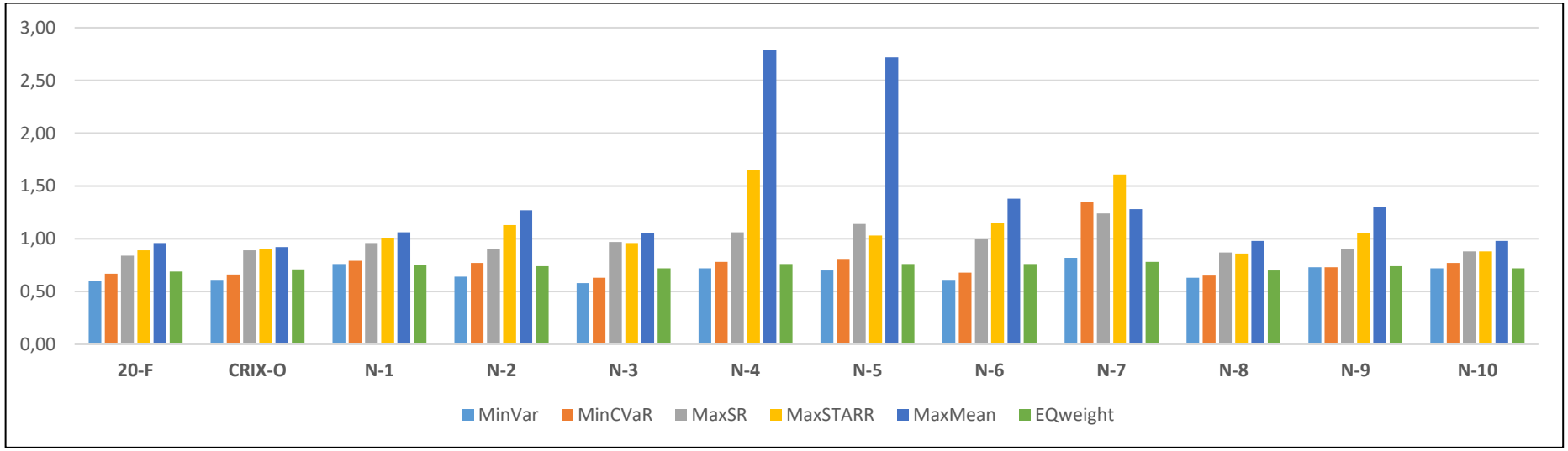


Izvor: Izrada autora

Tablica 14. Usporedni prikaz rezultata godišnje standardne devijacije $\sigma_{a,i}$. Vrijednost CRIX: 0,63

Optimizacijske strategije	Alokacija imovine										
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	0,60	0,61	0,76	0,64	0,58	0,72	0,70	0,61	0,82	0,63	0,73	0,72
MinCVaR	0,67	0,66	0,79	0,77	0,63	0,78	0,81	0,68	1,35	0,65	0,73	0,77
MaxSR	0,84	0,89	0,96	0,90	0,97	1,06	1,14	1,00	1,24	0,87	0,90	0,88
MaxSTARR	0,89	0,90	1,01	1,13	0,96	1,65	1,03	1,15	1,61	0,86	1,05	0,88
MaxMean	0,96	0,92	1,06	1,27	1,05	2,79	2,72	1,38	1,28	0,98	1,30	0,98
EQweight	0,69	0,71	0,75	0,74	0,72	0,76	0,76	0,76	0,78	0,70	0,74	0,72

Grafikon 26. Ilustracija rezultata godišnje standardne devijacije σ_{ai}

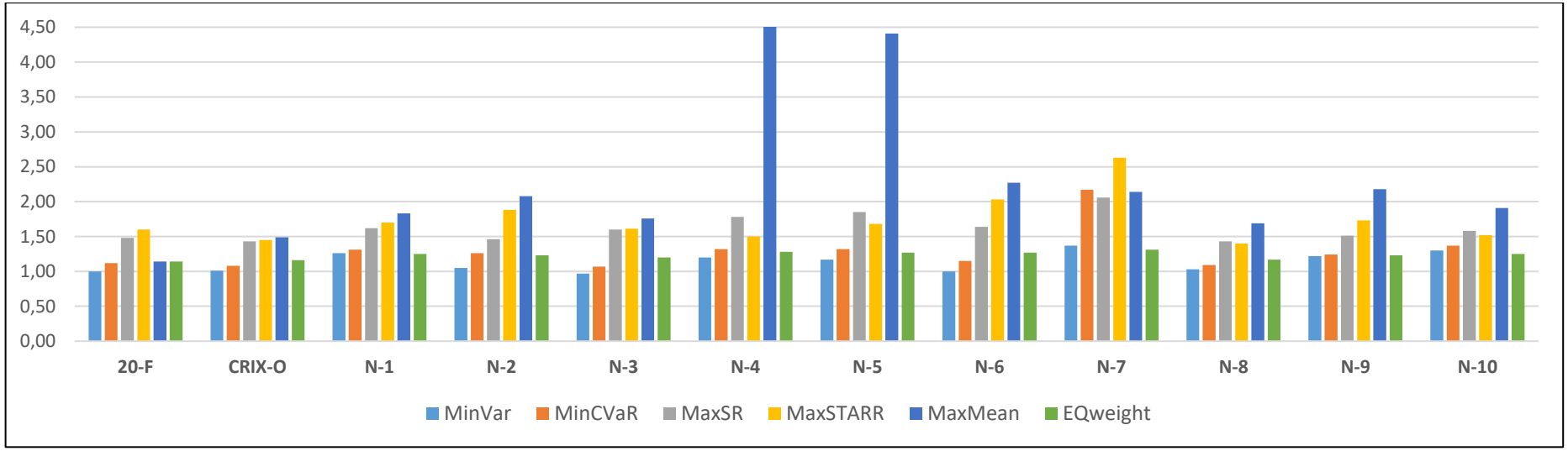


Izvor: Izrada autora

Tablica 15. Usporedni prikaz rezultata godišnje rizičnosti vrijednosti $VaR_{a,i}$. Vrijednost CRIX: 1,04

Optimizacijske strategije	Alokacija imovine										
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	1,00	1,01	1,26	1,05	0,97	1,20	1,17	1,00	1,37	1,03	1,22	1,30
MinCVaR	1,12	1,08	1,31	1,26	1,07	1,32	1,32	1,15	2,17	1,09	1,24	1,37
MaxSR	1,48	1,43	1,62	1,46	1,60	1,78	1,85	1,64	2,06	1,43	1,51	1,58
MaxSTARR	1,60	1,45	1,70	1,88	1,61	1,50	1,68	2,03	2,63	1,40	1,73	1,52
MaxMean	1,14	1,49	1,83	2,08	1,76	4,53	4,41	2,27	2,14	1,69	2,18	1,91
EQweight	1,14	1,16	1,25	1,23	1,20	1,28	1,27	1,27	1,31	1,17	1,23	1,25

Grafikon 27. Ilustracija rezultata godišnje rizičnosti vrijednosti $VaR_{a,i}$

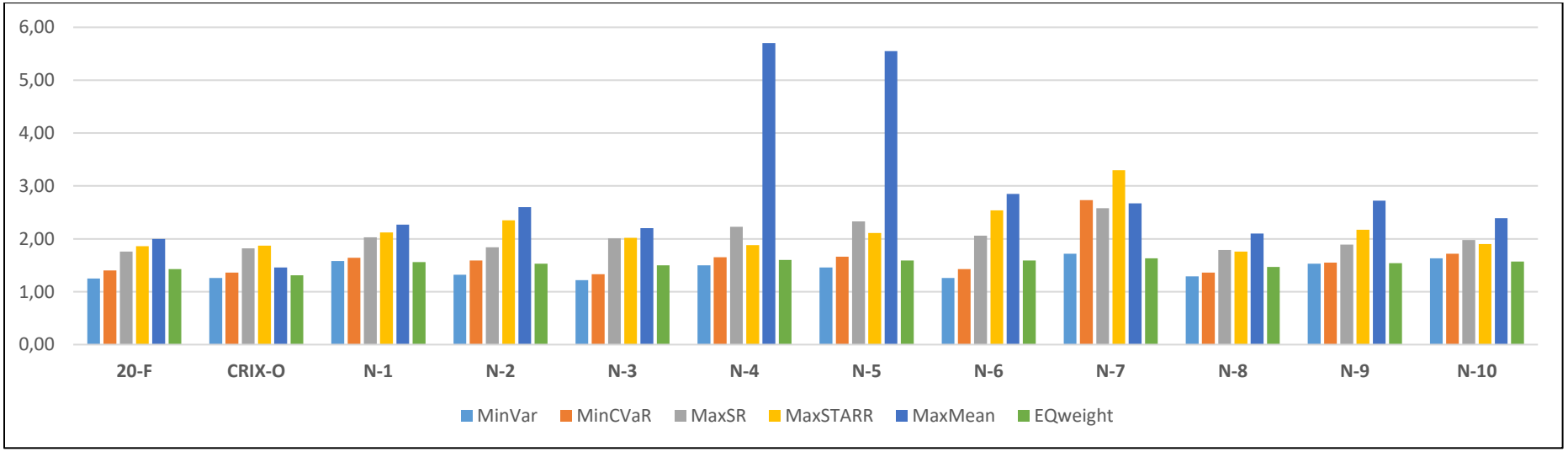


Izvor: Izrada autora

Tablica 16. Usporedni prikaz rezultata godišnje uvjetne rizičnosti vrijednosti $CVaR_{a,i}$. Vrijednost CRIX: 1,31

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	1,25	1,26	1,58	1,32	1,22	1,50	1,46	1,26	1,72	1,29	1,53	1,63
MinCVaR	1,40	1,36	1,64	1,59	1,33	1,65	1,66	1,43	2,73	1,36	1,55	1,72
MaxSR	1,76	1,82	2,03	1,84	2,01	2,23	2,33	2,06	2,58	1,79	1,89	1,98
MaxSTARR	1,86	1,87	2,12	2,35	2,02	1,88	2,11	2,54	3,30	1,76	2,17	1,90
MaxMean	2,00	1,46	2,27	2,60	2,20	5,70	5,55	2,85	2,67	2,10	2,72	2,39
EQweight	1,43	1,31	1,56	1,53	1,50	1,60	1,59	1,59	1,63	1,47	1,54	1,57

Grafikon 28. Ilustracija rezultata godišnje uvjetne rizičnosti vrijednosti $CVaR_{a,i}$

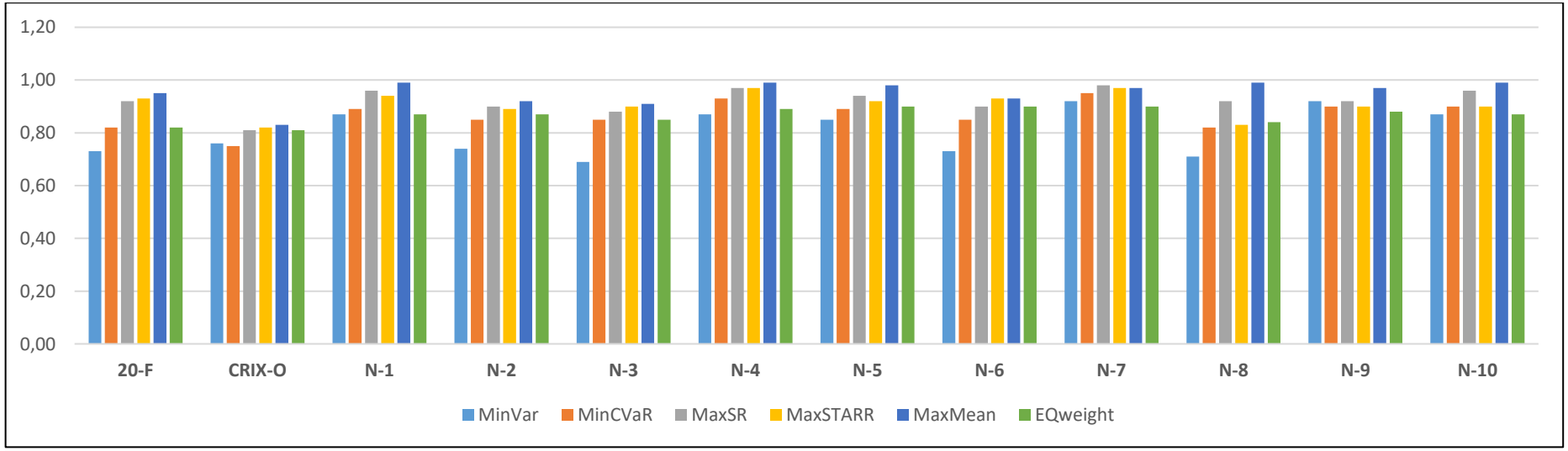


Izvor: Izrada autora

Tablica 17. Usporedni prikaz rezultata najvećeg gubitka WD. Vrijednost CRIX: 0,78

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	0,73	0,76	0,87	0,74	0,69	0,87	0,85	0,73	0,92	0,71	0,92	0,87
MinCVaR	0,82	0,75	0,89	0,85	0,85	0,93	0,89	0,85	0,95	0,82	0,90	0,90
MaxSR	0,92	0,81	0,96	0,90	0,88	0,97	0,94	0,90	0,98	0,92	0,92	0,96
MaxSTARR	0,93	0,82	0,94	0,89	0,90	0,97	0,92	0,93	0,97	0,83	0,90	0,90
MaxMean	0,95	0,83	0,99	0,92	0,91	0,99	0,98	0,93	0,97	0,99	0,97	0,99
EQweight	0,82	0,81	0,87	0,87	0,85	0,89	0,90	0,90	0,90	0,84	0,88	0,87

Grafikon 29. Ilustracija rezultata najvećeg gubitka WD

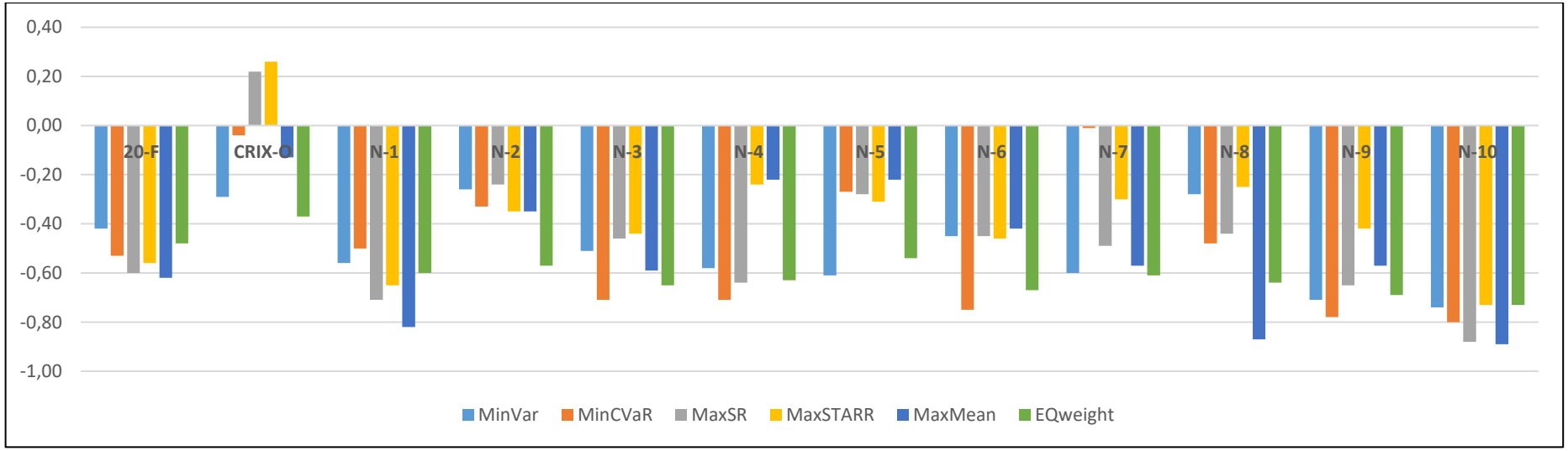


Izvor: Izrada autora

Tablica 18. Usporedni prikaz rezultata Sharpe omjera SR. Vrijednost CRIX: -0,29

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,42	-0,29	-0,56	-0,26	-0,51	-0,58	-0,61	-0,45	-0,60	-0,28	-0,71	-0,74
MinCVaR	-0,53	-0,04	-0,50	-0,33	-0,71	-0,71	-0,27	-0,75	-0,01	-0,48	-0,78	-0,80
MaxSR	-0,60	0,22	-0,71	-0,24	-0,46	-0,64	-0,28	-0,45	-0,49	-0,44	-0,65	-0,88
MaxSTARR	-0,56	0,26	-0,65	-0,35	-0,44	-0,24	-0,31	-0,46	-0,30	-0,25	-0,42	-0,73
MaxMean	-0,62	-0,13	-0,82	-0,35	-0,59	-0,22	-0,22	-0,42	-0,57	-0,87	-0,57	-0,89
EQweight	-0,48	-0,37	-0,60	-0,57	-0,65	-0,63	-0,54	-0,67	-0,61	-0,64	-0,69	-0,73

Grafikon 30. Ilustracija rezultata Sharpe omjera SR

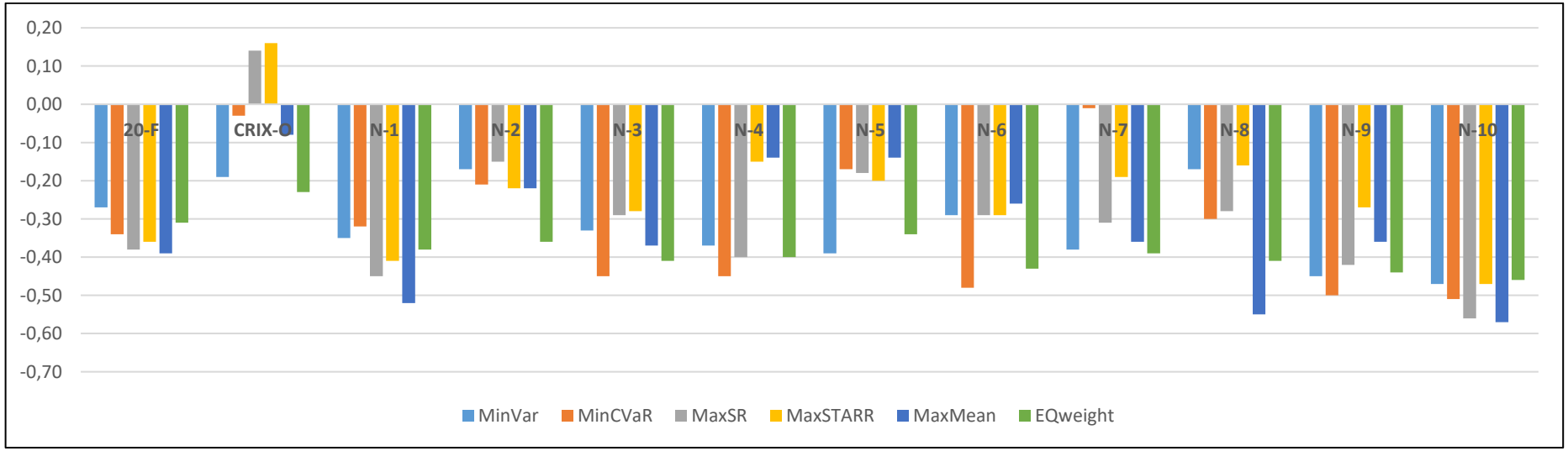


Izvor: Izrada autora

Tablica 19. Usporedni prikaz rezultata MSquared M^2. Vrijednost CRIX: -0,18

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,27	-0,19	-0,35	-0,17	-0,33	-0,37	-0,39	-0,29	-0,38	-0,17	-0,45	-0,47
MinCVaR	-0,34	-0,03	-0,32	-0,21	-0,45	-0,45	-0,17	-0,48	-0,01	-0,30	-0,5	-0,51
MaxSR	-0,38	0,14	-0,45	-0,15	-0,29	-0,40	-0,18	-0,29	-0,31	-0,28	-0,42	-0,56
MaxSTARR	-0,36	0,16	-0,41	-0,22	-0,28	-0,15	-0,20	-0,29	-0,19	-0,16	-0,27	-0,47
MaxMean	-0,39	-0,08	-0,52	-0,22	-0,37	-0,14	-0,14	-0,26	-0,36	-0,55	-0,36	-0,57
EQweight	-0,31	-0,23	-0,38	-0,36	-0,41	-0,4	-0,34	-0,43	-0,39	-0,41	-0,44	-0,46

Grafikon 31. Ilustracija rezultata MSquared M^2

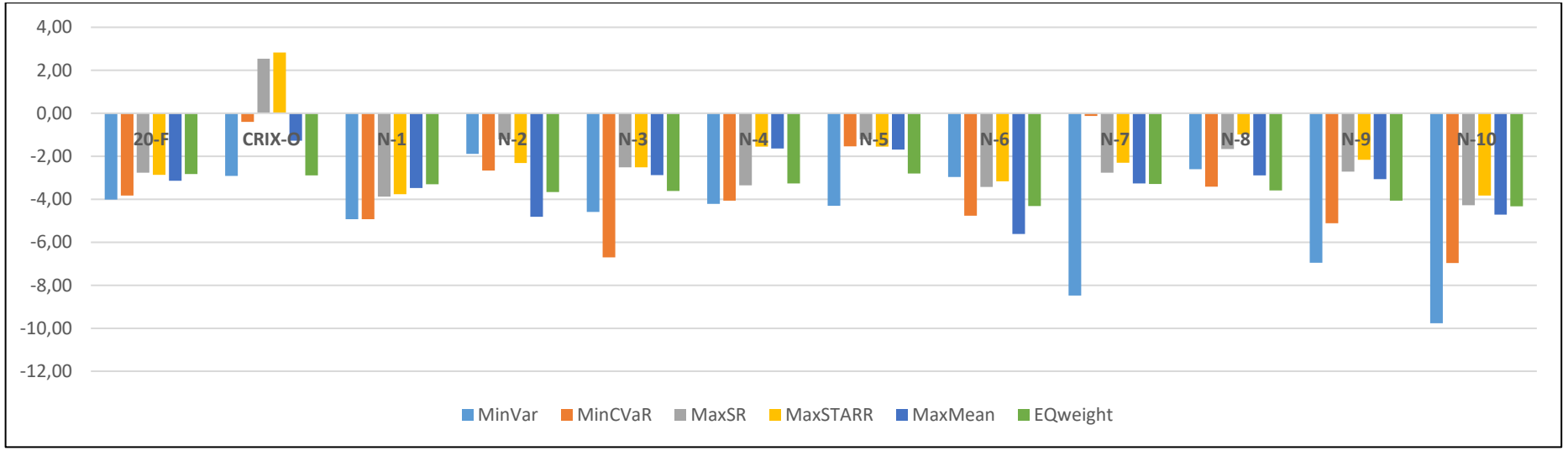


Izvor: Izrada autora

Tablica 20. Usporedni prikaz rezultata Treynor omjera TR. Vrijednost CRIX: -0.18

Optimizacijske strategije	Alokacija imovine										
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-4,02	-2,92	-4,93	-1,89	-4,59	-4,22	-4,30	-2,97	-8,48	-2,60	-6,96	-9,77
MinCVaR	-3,83	-0,40	-4,93	-2,66	-6,71	-4,07	-1,54	-4,77	-0,13	-3,41	-5,12	-6,97
MaxSR	-2,76	2,54	-3,88	-1,21	-2,52	-3,35	-1,21	-3,43	-2,76	-1,66	-2,72	-4,28
MaxSTARR	-2,86	2,82	-3,76	-2,32	-2,52	-1,55	-1,55	-3,17	-2,30	-0,99	-2,17	-3,83
MaxMean	-3,14	-1,28	-3,48	-4,81	-2,88	-1,64	-1,69	-5,61	-3,26	-2,89	-3,06	-4,72
EQweight	-2,83	-2,89	-3,30	-3,66	-3,61	-3,26	-2,80	-4,32	-3,29	-3,59	-4,06	-4,33

Grafikon 32. Ilustracija rezultata Treynor omjera TR

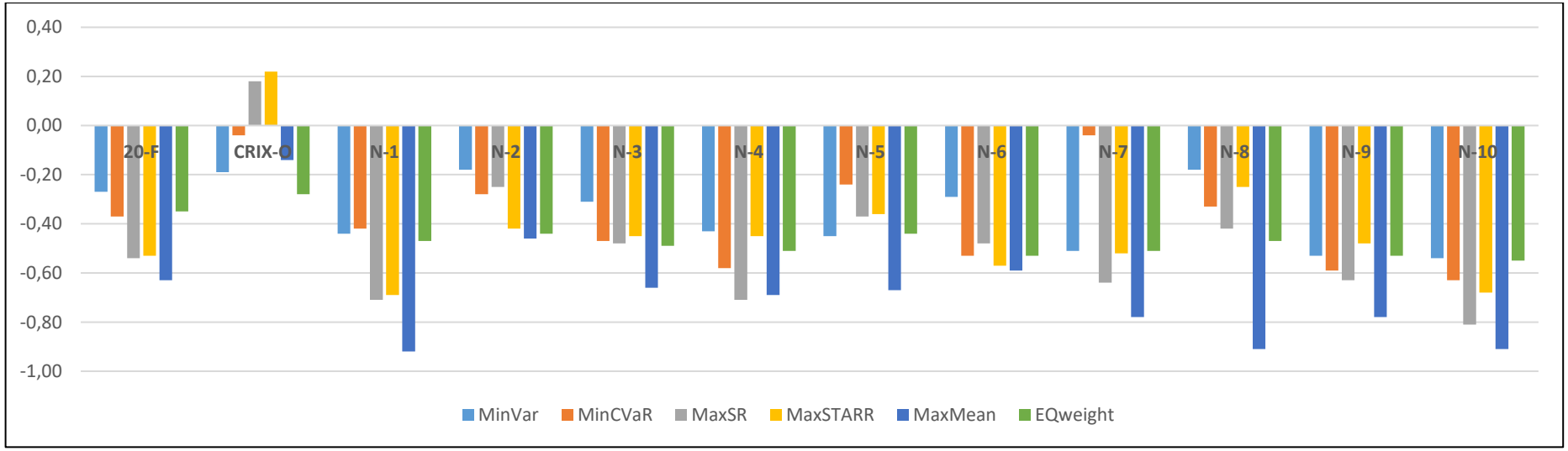


Izvor: Izrada autora. Veličine iz tablice su pomnožene sa vrijednosti -1.

Tablica 21. Usporedni prikaz rezultata Jensen alfe $a_{,i}$. Vrijednost CRIX: 0,00

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,27	-0,19	-0,44	-0,18	-0,31	-0,43	-0,45	-0,29	-0,51	-0,18	-0,53	-0,54
MinCVaR	-0,37	-0,04	-0,42	-0,28	-0,47	-0,58	-0,24	-0,53	-0,04	-0,33	-0,59	-0,63
MaxSR	-0,54	0,18	-0,71	-0,25	-0,48	-0,71	-0,37	-0,48	-0,64	-0,42	-0,63	-0,81
MaxSTARR	-0,53	0,22	-0,69	-0,42	-0,45	-0,45	-0,36	-0,57	-0,52	-0,25	-0,48	-0,68
MaxMean	-0,63	-0,14	-0,92	-0,46	-0,66	-0,69	-0,67	-0,59	-0,78	-0,91	-0,78	-0,91
EQweight	-0,35	-0,28	-0,47	-0,44	-0,49	-0,51	-0,44	-0,53	-0,51	-0,47	-0,53	-0,55

Grafikon 33. Ilustracija rezultata Jensen omjera a_i

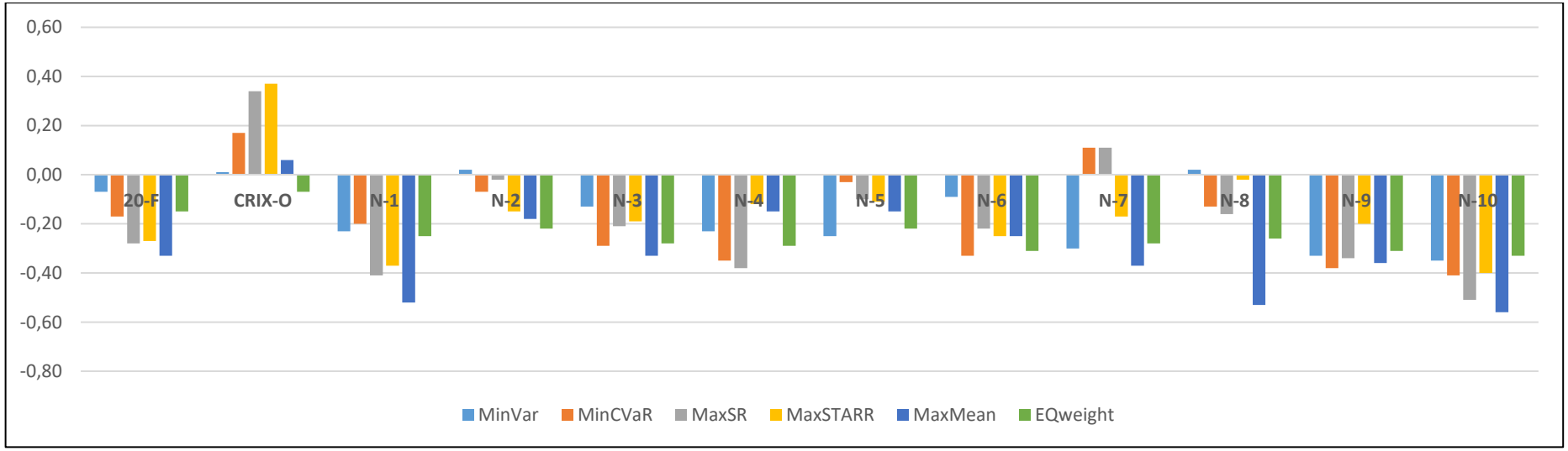


Izvor: Izrada autora

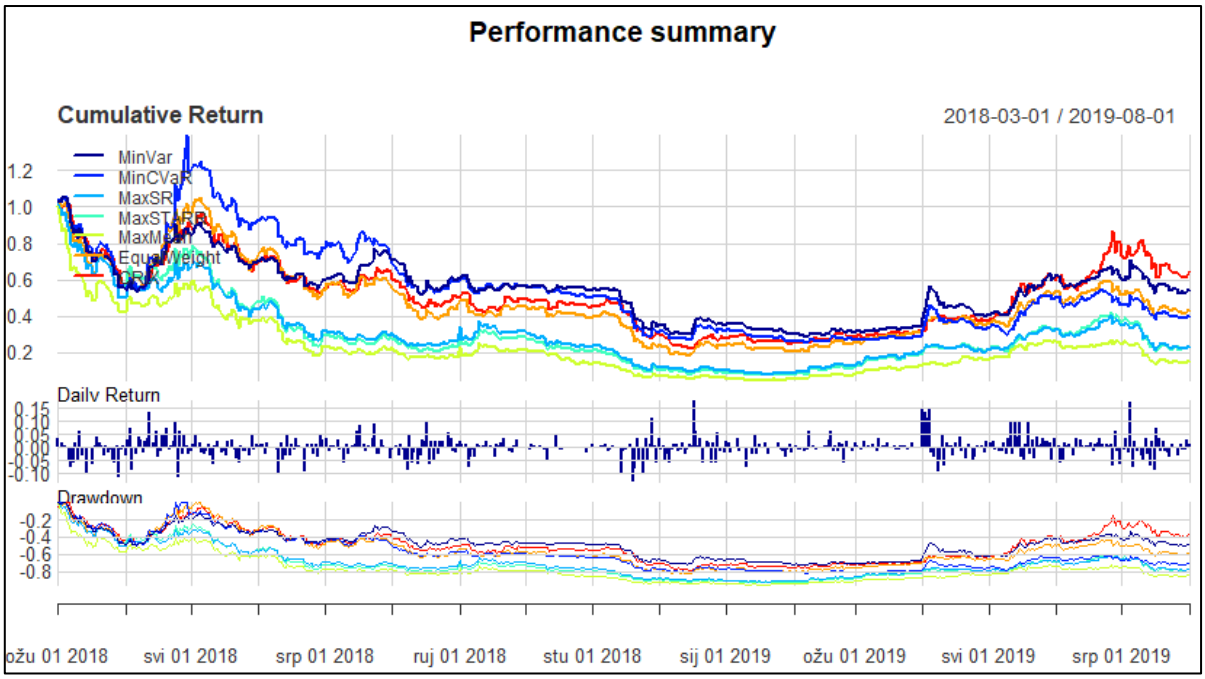
Tablica 22. Usporedni prikaz rezultata informacijskog omjera IR.

Optimizacijske strategije	Alokacija imovine											
	20-F	CRIX-O	10 portfelja po 20 nasumično odabranih kriptovaluta									
			N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	N-9	N-10
MinVar	-0,07	0,01	-0,23	0,02	-0,13	-0,23	-0,25	-0,09	-0,30	0,02	-0,33	-0,35
MinCVaR	-0,17	0,17	-0,20	-0,07	-0,29	-0,35	-0,03	-0,33	0,11	-0,13	-0,38	-0,41
MaxSR	-0,28	0,34	-0,41	-0,02	-0,21	-0,38	-0,10	-0,22	-0,29	-0,16	-0,34	-0,51
MaxSTARR	-0,27	0,37	-0,37	-0,15	-0,19	-0,12	-0,11	-0,25	-0,17	-0,02	-0,20	-0,40
MaxMean	-0,33	0,06	-0,52	-0,18	-0,33	-0,15	-0,15	-0,25	-0,37	-0,53	-0,36	-0,56
EQweight	-0,15	-0,07	-0,25	-0,22	-0,28	-0,29	-0,22	-0,31	-0,28	-0,26	-0,31	-0,33

Grafikon 34. Ilustracija rezultata informacijskog omjera IR

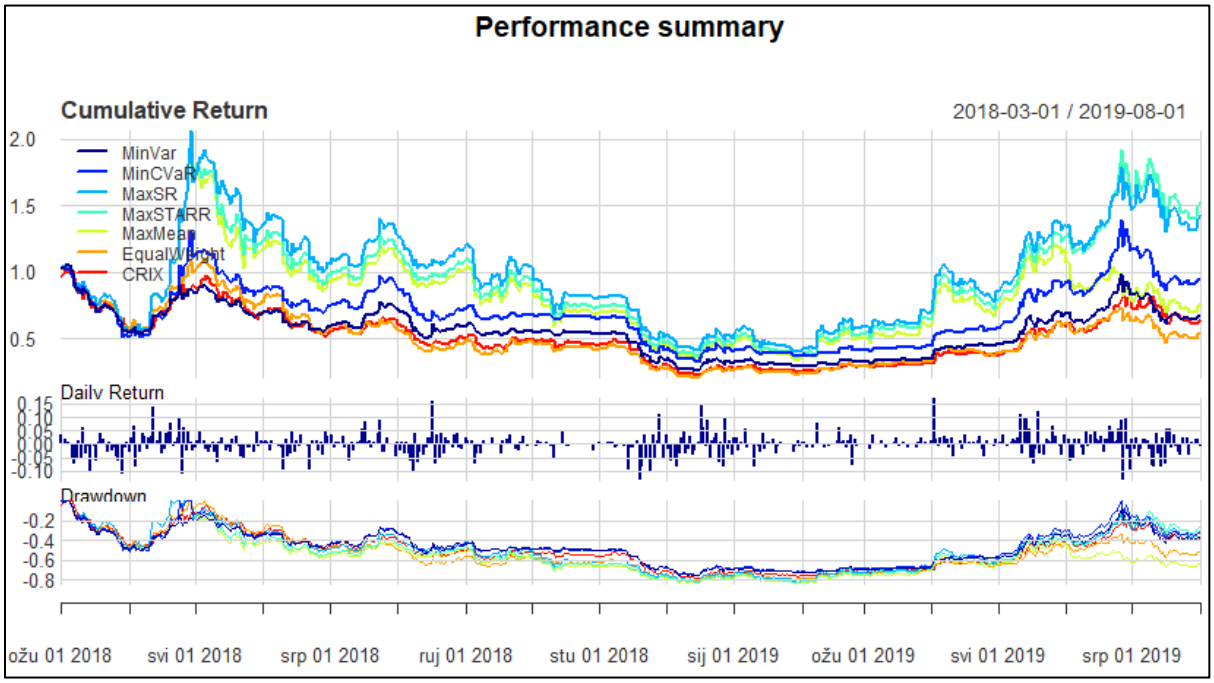


Izvor: Izrada autora



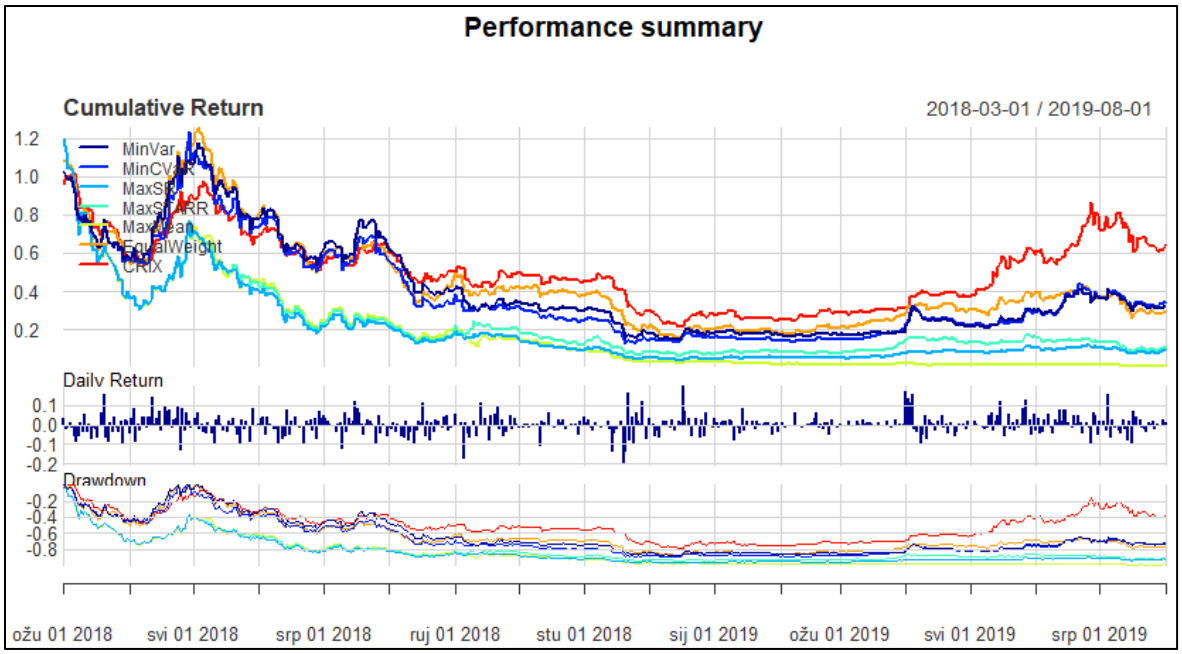
Grafikon 35. Ilustracija kumulativnog prinosa 20-F alokacijskog modela

Izvor: Izrada autora



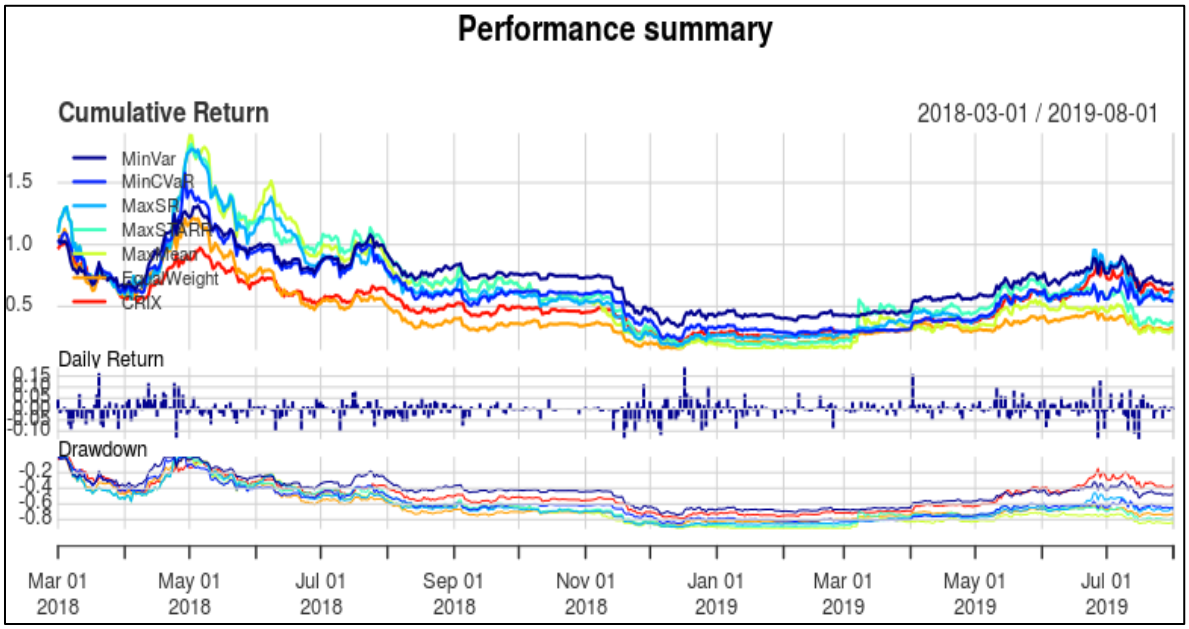
Grafikon 36. Ilustracija kumulativnog prinosa CRIX-O alokacijskog modela

Izvor: Izrada autora



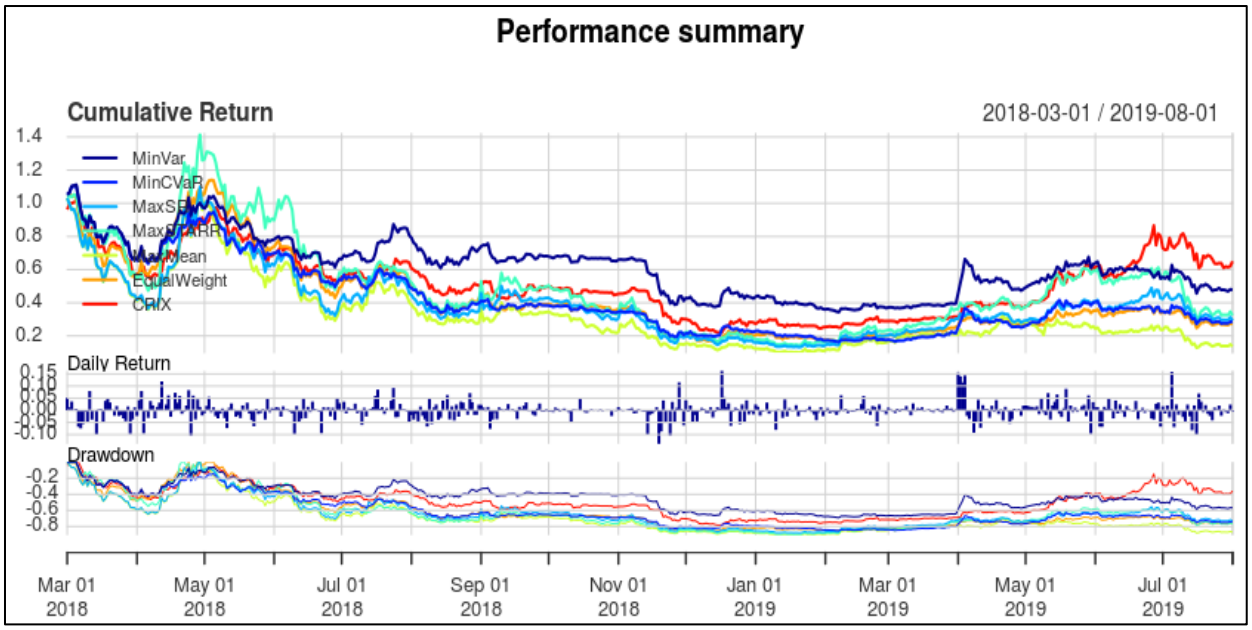
Grafikon 37. Ilustracija kumulativnog prinosa N-1 alokacijskog modela

Izvor: Izrada autora



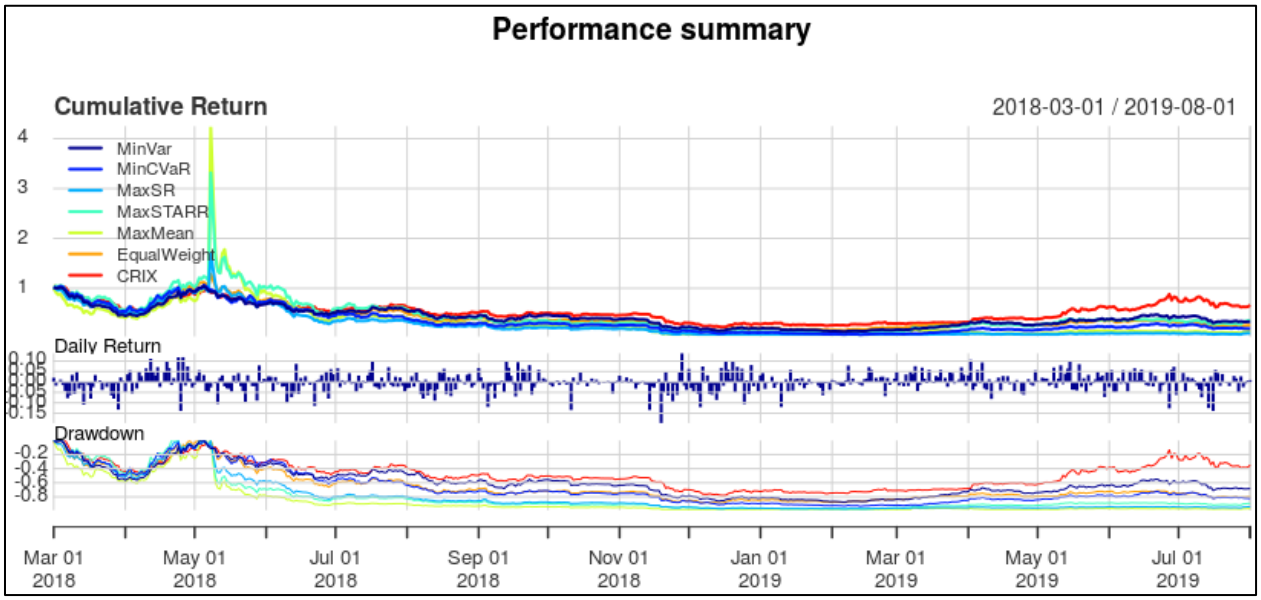
Grafikon 38. Ilustracija kumulativnog prinosa N-2 alokacijskog modela

Izvor: Izrada autora



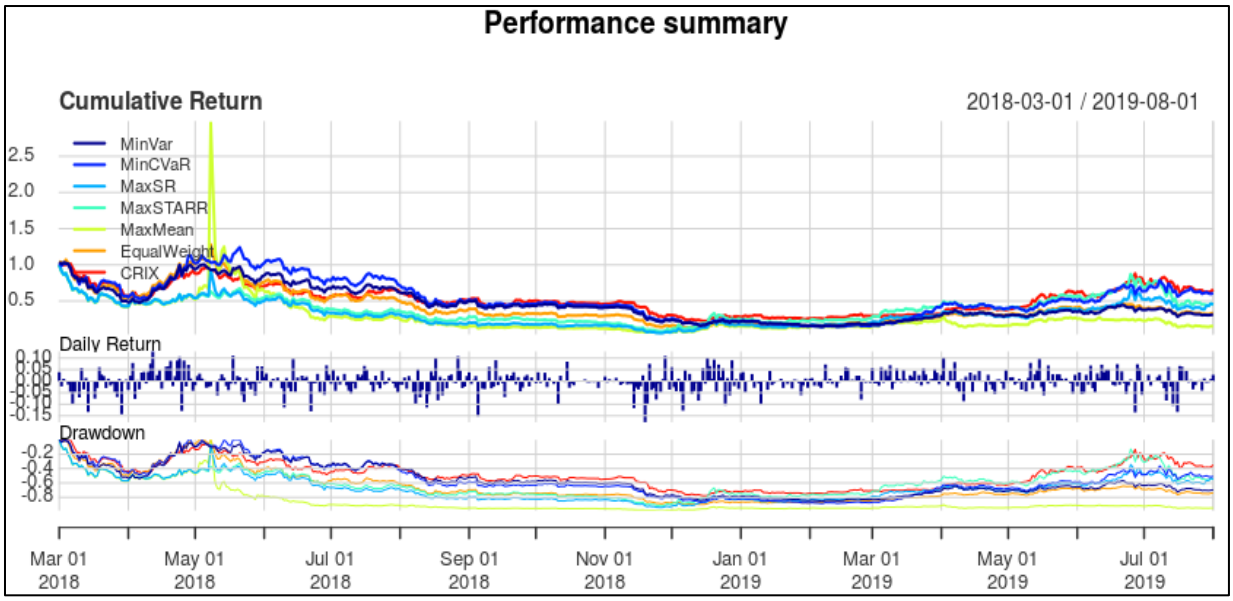
Grafikon 39. Ilustracija kumulativnog prinosa N-3 alokacijskog modela

Izvor: Izrada autora



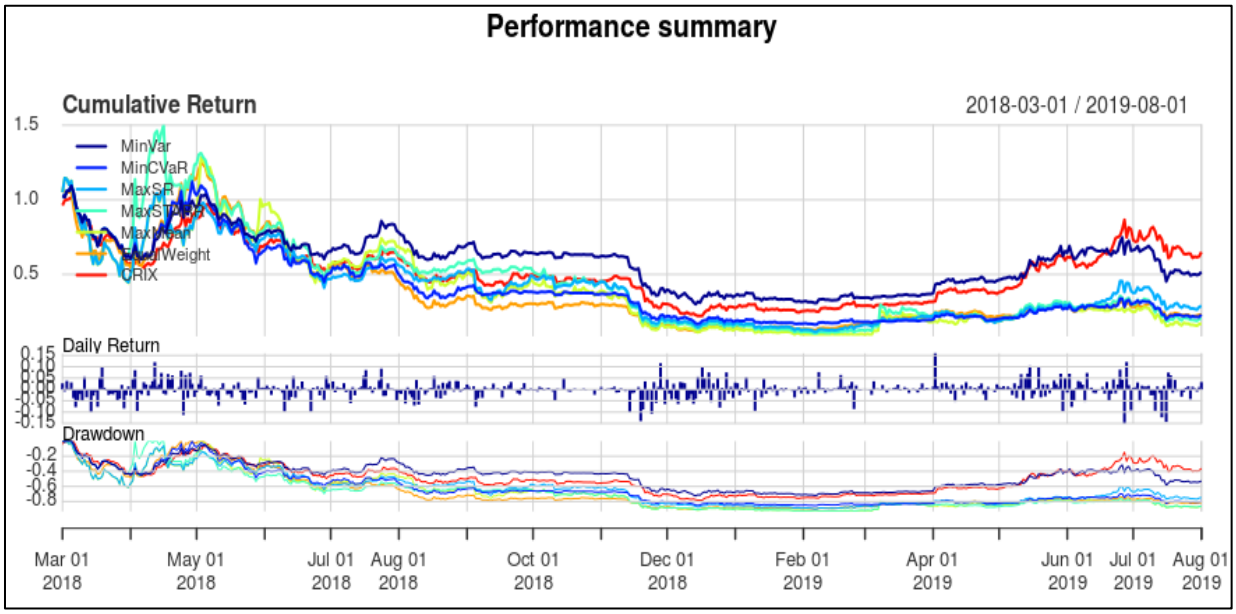
Grafikon 40. Ilustracija kumulativnog prinosa N-4 alokacijskog modela

Izvor: Izrada autora



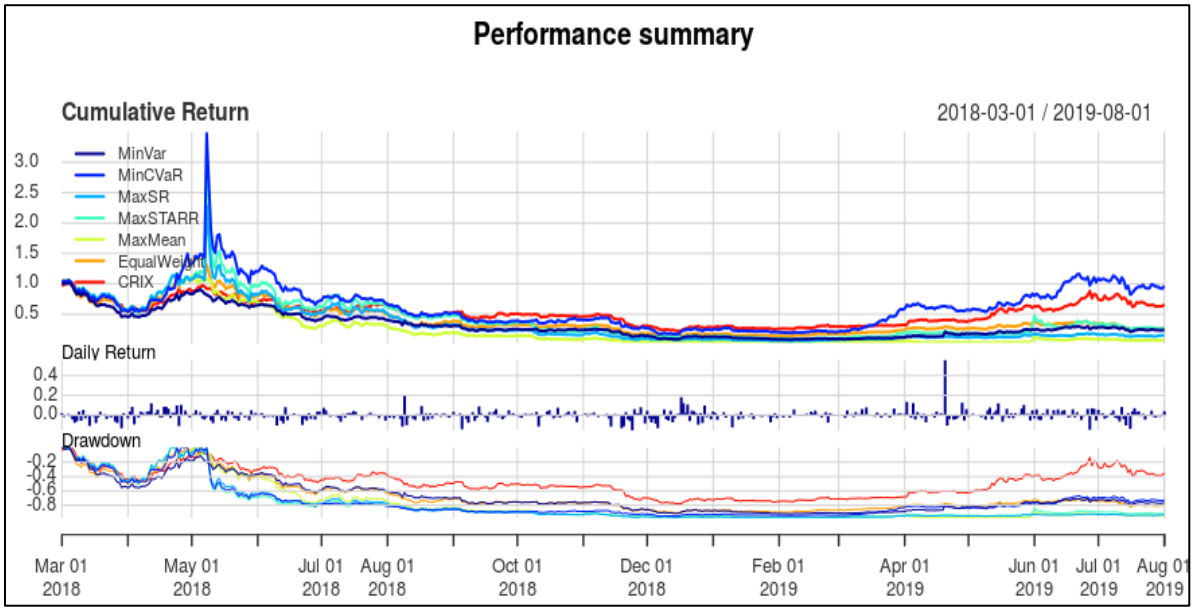
Grafikon 41. Ilustracija kumulativnog prinosa N-5 alokacijskog modela

Izvor: Izrada autora



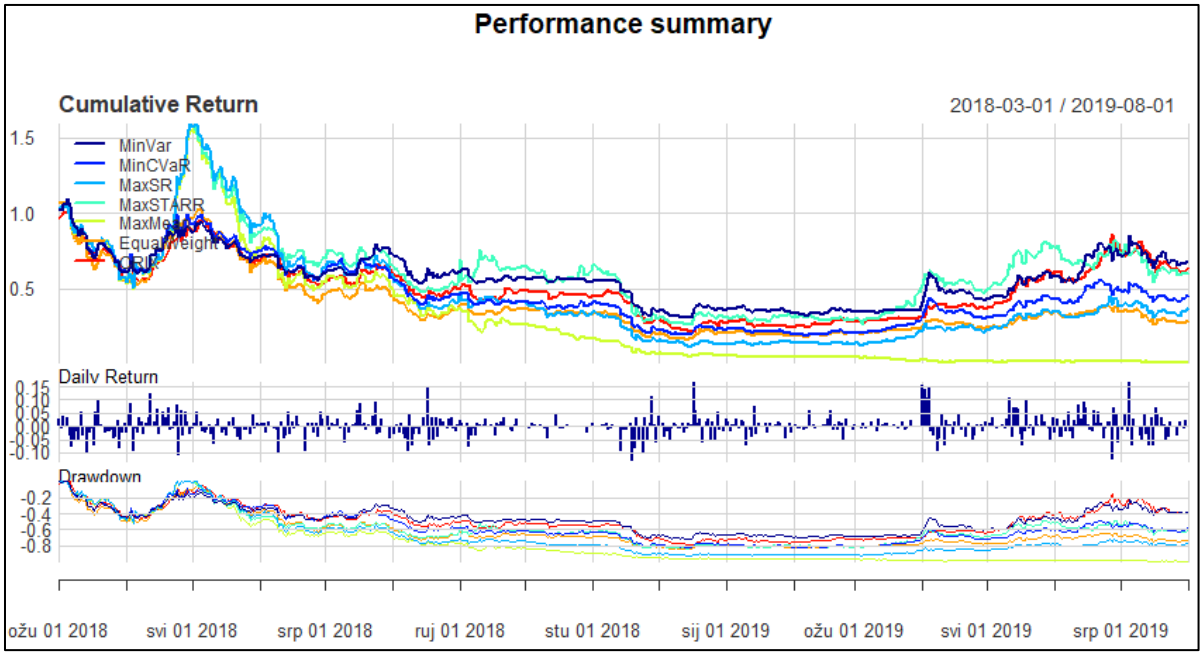
Grafikon 42. Ilustracija kumulativnog prinosa N-6 alokacijskog modela

Izvor: Izrada autora



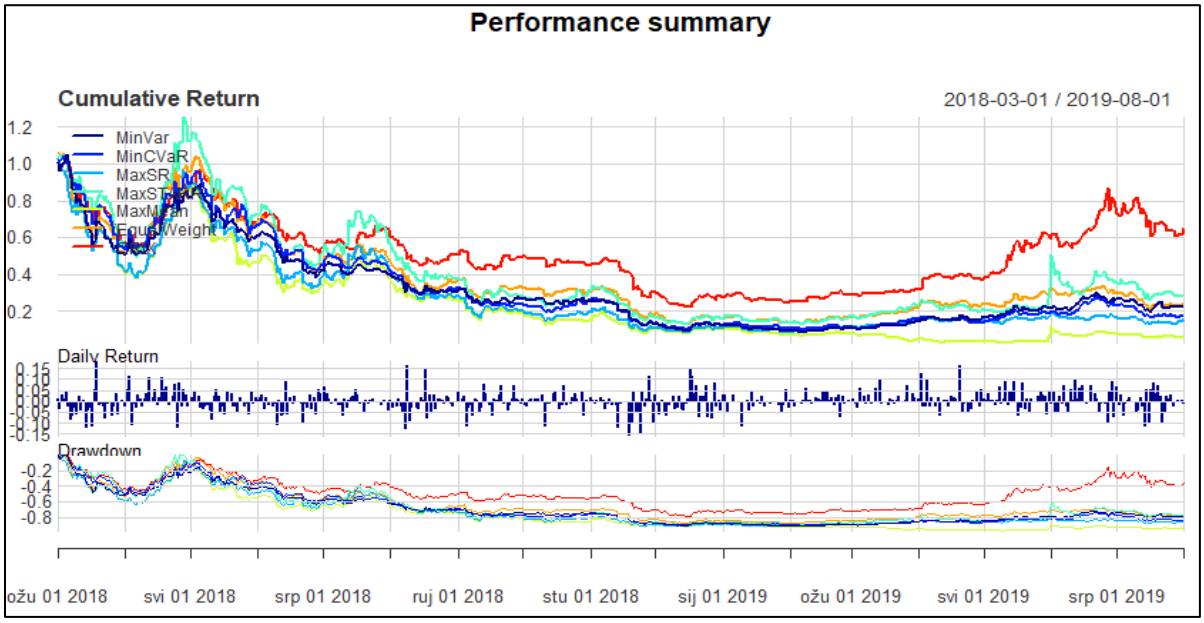
Grafikon 43. Ilustracija kumulativnog prinosa N-7 alokacijskog modela

Izvor: Izrada autora



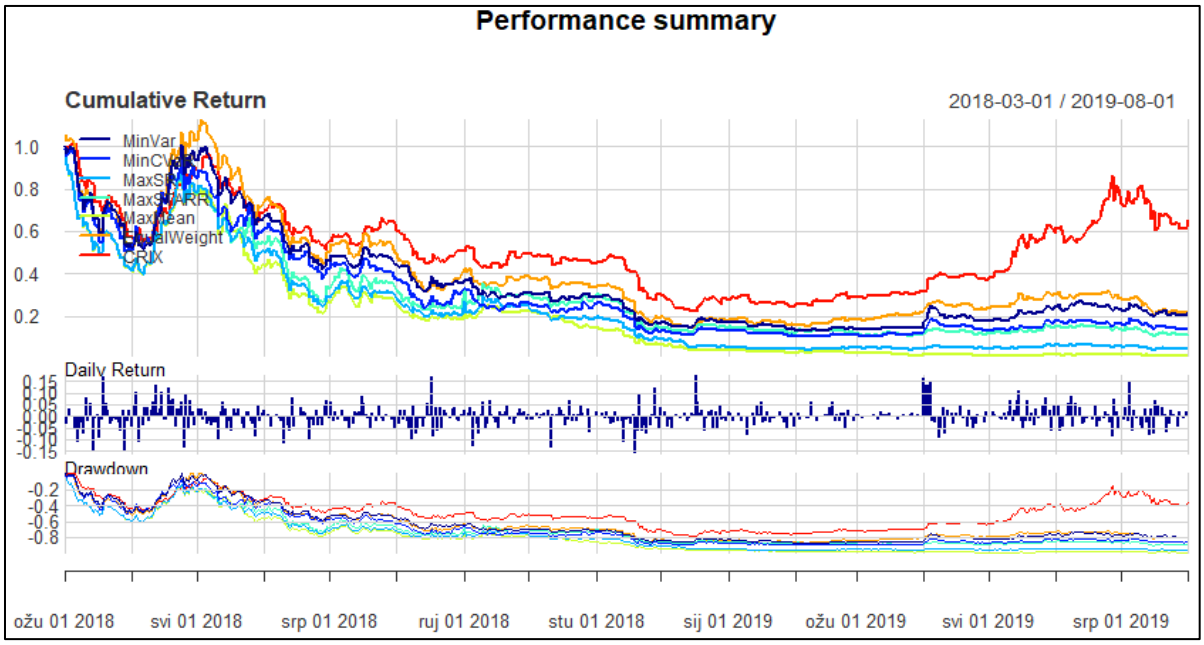
Grafikon 44. Ilustracija kumulativnog prinosa N-8 alokacijskog modela

Izvor: Izrada autora



Grafikon 45. Ilustracija kumulativnog prinosa N-9 alokacijskog modela

Izvor: Izrada autora



Grafikon 46. Ilustracija kumulativnog prinosa N-10 alokacijskog modela

Izvor: Izrada autora

ŽIVOTOPIS

Rođen 29.06.1982. godine u Banja Luci. Svoj dodiplomski studij završava 2008. godine na Ekonomskom fakultetu Sveučilišta u Splitu. Nakon završenog dodiplomskog studija, upisuje diplomski studij, smjer Bankarstva, financija i osiguranja na Visokoj poslovnoj školi u Zagrebu, gdje 2011. godine brani diplomski rad na temu „Izdavanje i trgovanje obveznicama u RH“. Formalno obrazovanje nastavlja na poslijediplomskom specijalističkom studiju Ekonomskog fakulteta Sveučilišta u Osijeku. Uz pohvalu te preporuku za upis na doktorski studij, 2014. godine brani završni rad „Utjecaj makroekonomskih pokazatelja na promjenu vrijednosti CROBEX-a“.

Posjeduje certifikate ovlaštenog internog revizora te ovlaštenog računovođe. Član je udruge Hrvatski računovođa, kao i Hrvatske zajednice računovođa i financijskih djelatnika. Svoje radno iskustvo stekao je tokom višegodišnjeg rada kroz više organizacijskih jedinica unutar HEP ODS-a, a od 2018. godine radi na mjestu voditelja Odjela za financije u Sektoru za ekonomske poslove.

Svoj je znanstveni i istraživački interes usmjerio na izučavanje poslovnih financija, financijskih tržišta, financijskih instrumenata i njihovih izvedenica, suvremenih financijskih tehnologija, kriptovaluta, kao i izučavanje i ispitivanje dinamike pojava na financijskim tržištima.

Popis objavljenih knjiga:

1. Tomić, B. (2016). „Financijski instrumenti i izvedenice“, Effectus, Zagreb.

Popis objavljenih radova:

1. Žiković, S., Čuljak, M. & Tomić, B. (2020) „Value of picking sectors in cryptocurrency optimization“. Conference Proceedings – EDT Digitomics Rijeka. Available at https://www.edt-conference.com/conference-proceedings.php

2. Šestanović, A, Horvat, Đ. & Tomić, B. (2018) „Ispitivanje teorije hijerarhije financijskih izbora na hrvatskom tržištu kapitala“, Ekonomski pregled, vol. 69, no. 1, pp. 58-72.

3. Tomić, B. & Sesar, A. (2015) „Interdependence of Industrial Production Index and capital market in Croatia: VAR model“. Journal of Accounting and Management, vol. 5, no. 1, pp. 17-32.

4. Tomić, B. & Strancarić, S. (2014) „Organizacijski aspekti računovodstvenih informacijskih sustava i njihova važnost“. RiF, vol. 60, no. 7, pp. 39-40.

5. Tomić, B. (2013) „The application of the capital asset pricing model on the croatian capital market“. Financije i pravo, vol. 1, no. 1, pp. 105-123.

6. Tomić, B. (2015) „Impact Of Macroeconomic Indicators On The Movement Of Crobex“. Financije i pravo, vol. 2, no. 1, pp. 45-60.

7. Tomić, B. (2016) „Basic Characteristics of Bonds and their Dynamics on the Croatian Secondary Market“. Financije i pravo, vol. 4, no. 1, pp. 115-132.

8. Tomić, B. (2016) „Ispitivanje kalendarskih sezonaliteta na hrvatskom tržištu kapitala“. 17. International Scientific and Professional Conference. Zbornik radova, svezak I. – scientific papers. Primošten Hrvatska. 09-10.06.2016. Zagreb. pp. 175-192.

9. Tomić, B. (2020) „BITCOIN: Systematic Force of Cryptocurrency Portfolio“. Conference Proceedings - FEB Zagreb International Odyssey Conference on Economics & Business , vol. 2, no. 1. Zagreb. pp. 384-398.

10. Tomić, B., Sesar, A. i Džaja, T., (2014) „Comparative analysis of european capital market and Dow Jones Industrial Average Index“. 15. International Scientific and Professional Conference. Zbornik radova, svezak I. – scientific papers. Rovinj Hrvatska. 05-07.06.2014. Zagreb. pp. 265-283.

IZJAVA

kojom ja, Bojan Tomić, univ.spec.oec., broj indeksa: 000555 doktorand Ekonomskog fakulteta Sveučilišta u Rijeci, kao autor doktorske disertacije s naslovom: Modeliranje tehnologije distribuiranoga zapisa i njena primjena:

1. Izjavljujem da sam doktorsku disertaciju izradio samostalno pod mentorstvom prof. dr. sc. Saša Žiković. U radu sam primijenio metodologiju znanstvenoistraživačkog rada i koristio literaturu koja je navedena na kraju rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u radu citirao sam i povezao s korištenim bibliografskim jedinicama sukladno odredbama Pravilnika o izradi i opremanju doktorskih radova Sveučilišta u Rijeci, Ekonomskog fakulteta u Rijeci. Rad je pisan u duhu hrvatskog jezika.

2. Dajem odobrenje da se, bez naknade, trajno pohrani moj rad u javno dostupnom digitalnom repozitoriju ustanove i Sveučilišta te u javnoj internetskoj bazi radova Nacionalne i sveučilišne knjižnice u Zagrebu, sukladno obvezi iz odredbe članka 83. stavka 11. Zakona o znanstvenoj djelatnosti i visokom obrazovanju (NN 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14, 60/15).

Potvrđujem da je za pohranu dostavljena završna verzija obranjene i dovršene doktorske disertacije. Ovom izjavom, kao autor dajem odobrenje i da se moj rad, bez naknade, trajno javno objavi i besplatno učini dostupnim studentima i djelatnicima ustanove.

_____

Bojan Tomić, univ.spec.oec.