

# Rizik investiranja u Bitcoin na temelju Monte Carlo simulacije

---

**Jambrečec, Manuella**

**Master's thesis / Diplomski rad**

**2023**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Rijeka, Faculty of Tourism and Hospitality Management / Sveučilište u Rijeci, Fakultet za menadžment u turizmu i ugostiteljstvu**

*Permanent link / Trajna poveznica:* <https://urn.nsk.hr/urn:nbn:hr:191:076057>

*Rights / Prava:* [Attribution 4.0 International](#)/[Imenovanje 4.0 međunarodna](#)

*Download date / Datum preuzimanja:* **2024-11-26**



*Repository / Repozitorij:*

[Repository of Faculty of Tourism and Hospitality Management - Repository of students works of the Faculty of Tourism and Hospitality Management](#)



**SVEUČILIŠTE U RIJECI**  
**Fakultet za menadžment u turizmu i ugostiteljstvu**  
**Sveučilišni diplomski studij**

**MANUELLA JAMBREČEC**

**Rizik investiranja u Bitcoin na temelju Monte Carlo simulacije**

**Bitcoin investment risk based on Monte Carlo simulation**

Diplomski rad

Opatija, 2023.

**SVEUČILIŠTE U RIJECI**  
**Fakultet za menadžment u turizmu i ugostiteljstvu**  
**Sveučilišni diplomski studij**  
**Održivi razvoj turizma**

**Rizik investiranja u Bitcoin na temelju Monte Carlo simulacije**

**Bitcoin investment risk based on Monte Carlo simulation**

Diplomski rad

Kolegij: **Menadžment rizika**

Student: **Manuella JAMBREČEC**

Mentor: **Izv. prof. dr. sc. Goran  
KARANOVIĆ**

Matični broj: **ds3758/22**

Opatija, rujan 2023.



## IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

**Manuella Jambrečec**

(ime i prezime studenta)

**ds3758**

(matični broj studenta)

**Rizik investiranja u Bitcoin na temelju Monte Carlo simulacije**

(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor diplomskog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa diplomskim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog diplomskog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na <http://creativecommons.org/licenses/>.

U Opatiji, rujan 2023.

*Manuella Jambrečec*

Potpis studenta

## Sažetak

U današnje vrijeme tema kriptovaluta veoma je involvirana u sve aspekte društva te utječe na život cijele zajednice bilo direktno ili indirektno. Ovaj rad pruža dubinsko ispitivanje povijesti, tehnologije i konkurentskog okruženja Bitcoina, najpoznatije kriptovalute današnjice. Kroz rad se prikazuje razvoj Bitcoina kao digitalne valute, istražuje se temeljna blockchain tehnologija i raspravlja o tome kako je Bitcoin transformirao tradicionalno gospodarsko okruženje. Osim toga, ovaj rad istražuje konkurenciju s kojom se Bitcoin suočava u alternativnim kriptovalutama i izazove s kojima se susreće u održavanju svoje pozicije vodeće digitalne valute. Empirijskim dijelom rada, pomoću Monte Carlo metode, žele se simulirati budući scenariji kretanja cijene Bitcoina. Iako je područje kriptovaluta i dalje dovoljno neistraženo i zbog tehnološke kompleksnosti nepristupačno svima, nedvojbeno privlači zanimanje javnosti. Prikrivanje kriminalnih radnji, "laka zarada", istraživanje neistraženog, želja za znanjem ili potencijal za nešto više? Svijet kriptovaluta daleko je opsežniji i složeniji nego što se na prvu čini, a na svakom je da odluči hoće li pristupiti ovom rudniku punom tehnološkog napretka, znanja, mogućnosti stjecanja imovinske koristi, ali i nezaobilaznog rizika.

Ključne riječi: kriptovalute, Bitcoin, blockchain, Monte Carlo simulacija

## **Abstract**

Nowadays, the topic of cryptocurrency is very present in all aspects of society, affecting the lives of the entire community either directly or indirectly. This paper provides an in-depth examination of the history, technology, and competitive environment of Bitcoin, the most prominent cryptocurrency today. The paper traces the evolution of Bitcoin as a digital currency, examines the underlying blockchain technology, and discusses how Bitcoin has changed the traditional economic environment. It also examines how Bitcoin competes with alternative cryptocurrencies and the challenges it faces in maintaining its position as a leading digital currency. The empirical part of the paper, which uses the Monte Carlo method, aims to simulate future scenarios of Bitcoin price development. Although the field of cryptocurrencies is still sufficiently unexplored and inaccessible to everyone due to its technological complexity, it undoubtedly attracts public interest. Crime cover-up, "easy money," exploration of the unexplored, thirst for knowledge, or the potential for more? The world of cryptocurrencies is far more extensive and complex than it first appears, and everyone must decide for themselves whether they want to enter this mine of technological advances, knowledge, the possibility of acquiring wealth benefits, but also inevitable risks.

Key words: cryptocurrencies, Bitcoin, blockchain, Monte Carlo simulation

# Sadržaj

<b>Uvod</b>	<b>1</b>
<b>1. Kriptovalute</b>	<b>3</b>
1.1. Razvoj kriptovaluta	4
1.1.1. Rudarenje	6
1.1.2. Tržište kriptovaluta	7
1.2. Blockchain	10
1.3. Sigurnost kriptovaluta	11
<b>2. Bitcoin</b>	<b>13</b>
2.1. Povijest Bitcoina	14
2.2. Tehnologija Bitcoina	18
2.3. Konkurencija	22
2.4. SWOT analiza	24
<b>3. Rizik investiranja u kriptovalute s naglaskom na Bitcoin</b>	<b>28</b>
3.1. Pravna regulativa	29
3.2. Stajališta banaka	30
3.3. Upravljanje rizicima	33
<b>4. Monte Carlo simulacija</b>	<b>36</b>
4.1. Općenito o Monte Carlo simulaciji	37
4.2. Monte Carlo i VaR	38
4.3. Monte Carlo simulacija na primjeru Bitcoina	38
4.3.1. Implementacija	38
4.3.2. Analiza	39
<b>Zaključak</b>	<b>45</b>
<b>Bibliografija</b>	<b>47</b>

## Uvod

Kriptovaluta kao oblik valute koji postoji digitalno ili virtualno zadnjih godina uvelike intrigira javnost kao i akademsku zajednicu koja svakodnevno ulaže znatne napore u istraživanje trgovanja kriptovalutama. Za osiguranje privatnosti korisnika, ali i transakcija koristi se kriptografija, a ono što kriptovalute izdvaja je činjenica nepostojanja središnjeg tijelo za regulaciju i izdavanje kriptovaluta. Iste su na tržištu dosegle iznimnu prihvaćenost i brzi razvoj unatoč tek nedavnoj koncepciji, stoga se sve češće može vidjeti kako se uključuju u portfelje i strategije trgovanja. Danas na digitalnom tržištu postoji preko tisuću kriptovaluta, a najpoznatija je Bitcoin (BTC).

Predmet ovog rada čine teorijska saznanja o kriptovalutama s naglaskom na Bitcoin koja se nastoje ispitati kroz Monte Carlo simulaciju.

Problem rada prikazuje određene manjkavosti unutar same primijenjene simulacije. Ne postoji u potpunosti jedinstven model na temelju kojeg možemo predvidjeti budućnost kretanja cijena te je prilikom analize potrebno u vidu imati potencijalni rizik zbog nepredvidivosti i neizvjesnosti.

Hipotezu ovog rada predstavlja činjenica da se kroz empirijsko istraživanje nastoji potvrditi teorijska pretpostavka o rastu cijene Bitcoina kao i gubitak uloženog.

Svrhom rada želi se postići procjena kvalitete i preciznosti Monte Carlo simulacije, a cilj rada odnosi se na predviđanje potencijalnog gubitka u budućem razdoblju pomoću navedene simulacije.

Prilikom izrade diplomskog rada korišteni su primarni izvori podataka dobiveni na temelju izračuna vrijednosti unutar programskog jezika Python na temelju kojih se donijela procjena rezultata. Dodatno, kao sekundarni izvor podataka korištena je domaća i strana literatura, članci iz časopisa te javno dostupni podaci s internetskih stranica.

Metodama istraživanja nastojala se adekvatno analizirati problematika u radu. U teorijskom dijelu rada su se, pomoću metode kompilacije, kroz znanstvenoistraživačka mišljenja inkorporirale znanstvene konstatacije te se na temelju istih donio zaključak. Komparativnom metodom su se uspoređivali podaci, a pomoću metode analize raščlanjeni dijelovi cjeline



proučavani su pojedinačno. U empirijskom dijelu rada ponajviše je korištena povijesna metoda obzirom da je za provedbu istraživanja bilo neophodno aplicirati povijesno gledane vrijednosti. Osim toga, korištena je i statistička metoda gdje se pomoću odabranog uzorka donio zaključak o prosječnoj vrijednosti i prisutnim devijacijama.

Struktura diplomskog rada koncipirana je u sedam cjelina. U uvodnom dijelu predstavljena je tema, iznesen je predmet rada sa svrhom predstavljanja rizika ulaganja u Bitcoin, a zatim je naveden i problem rada koji karakterizira nedostatnost idealnog modela za procjenu rizika. Potom se postavlja hipoteza, cilj i svrha rada te navode korištene metode istraživanja. Nadalje, rad je strukturiran u četiri poglavlja. U prvom se poglavlju definira sam pojam kriptovaluta i povezanih sastavnica dok se drugo poglavlje u potpunosti odnosi na Bitcoin kroz analizu povijesti, tehnologije, konkurencije te SWOT analizu. U trećem poglavlju rada fokus je stavljen na pravnu regulativu dok se u četvrtom poglavlju prikazuje empirijski dio predočen Monte Carlo simulacijom. U zaključku se sumiraju se ranije navedene analize i rezultati provedenog istraživanja, a u posljednjem dijelu rada navedena je bibliografija korištena u svrhu pisanja diplomskog rada.

# 1. Kriptovalute

Perkušić (2020.) prema Douradu (2014.) kriptovalute definira kao: „sustav valuta koji se koristi kriptografijom, što omogućuje siguran prijenos i razmjenu digitalnih tokena na distributivan i decentraliziran način.“

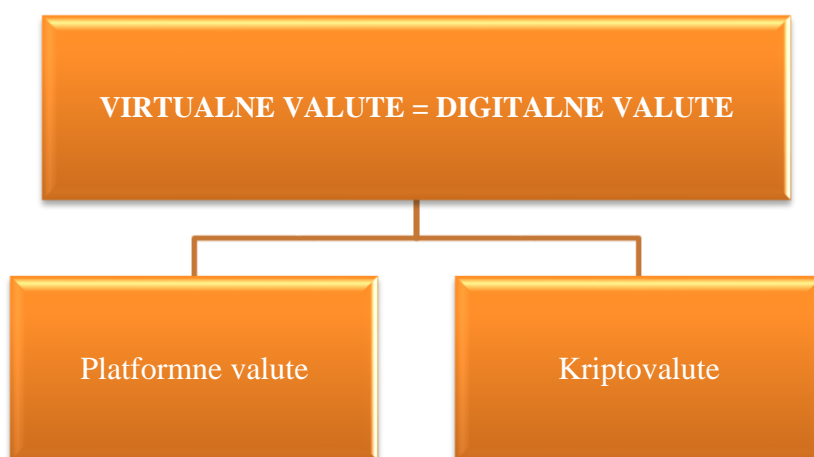
Kriptovalute iskorištavaju tehnologiju blockchaina za postizanje decentralizacije, transparentnosti i nepromjenjivosti. Pojednostavljeno, kriptovalute podrazumijevaju digitalni novac koji je i stvoren u digitalnom obliku, a njegova svrha je ista kao kod novca u fizičkom smislu te isti također predstavlja sredstvo razmjene. Kriptovalute su se pojavile kao oblik plaćanja u zadnjem desetljeću i zainteresirale cjelokupnu zajednicu.

Posjedovanje kriptovalute može se izjednačiti s posjedovanjem zlata obzirom da se njegova cijena mijenja sukladno zakonima tržišta. No unatoč tomu što kriptovalute imaju neke zajedničke značajke s tradicionalnom trgovinom, smjer njihova kretanja i ponašanje su još uvijek u procesu razumijevanja (Fang i sur. 2022).

Tržište kriptovaluta prikazuje se kao izrazito dinamično i nepredvidivo. Kriptovalute su poznate po visokoj volatilnosti, a navedeno predstavlja značajne oscilacije u kratkom vremenskom periodu. S jedne strane posjedovanje kriptovalute stvara mogućnost brzog dobitka, ali s druge strane navedeno nosi visok rizik od gubitka (Ječmínek 2020).

## 1.1. Razvoj kriptovaluta

Iako mnogi izjednačavaju pojmove virtualna valuta i kriptovaluta i zapravo se ne radi o sinonimima. Virtualnom odnosno digitalnom valutom smatraju se alternativni oblici plaćanja, isključivo elektroničkog oblika, koji nisu izdani od strane zakonom ovlaštenog tijela. Nadalje, kriptovaluta je najpoznatiji oblik virtualnih valuta, a osim istih postoje i platformne valute.



### Grafikon 1. Podjela virtualnih valuta

Izvor: izrada autora prema Perkušić M. (2020.) Pravo elektroničkog plaćanja

Perušić (2020.) prema Izvješću Europske središnje banke iz 2012. virtualne valute definira kao: „vrste neregulirana digitalnog novca koji izdaju i provjeravaju njegovi razvojni programeri te koji je prihvaćen među članovima specifične virtualne zajednice.“

U Republici Hrvatskoj Članak 4. Zakona o sprječavanju pranja novca i financiranja terorizma NN 108/17, 39/19, 151/22 tumači pojam virtualne valute kao „podvrstu virtualne imovine koja predstavlja digitalni prikaz vrijednosti koji nije izdala i za koji ne jamči središnja banka ni javno tijelo, koji nije nužno povezan sa zakonski uspostavljenom valutom te nema pravni status valute ili novca, ali ga fizičke i pravne osobe prihvaćaju kao sredstvo razmjene i može se prenositi, pohranjivati te se njime može trgovati elektroničkim putem.“

Platformne valute se odnose na centralizirane valute gdje platforme uvelike kontroliraju pravila po kojima se koriste njihove valute te također mogu postaviti značajke i svojstva valuta. Većina digitalnih valuta temeljenih na platformama ograničena je u barem nekim od svojih atributa pa čak i u samom prijenosu. Iste nisu osmišljene da u potpunosti zamijene zakonska sredstva plaćanja, već da privuku što veći broj korisnika platforme i olakšaju plaćanje proizvoda i/ili usluga (Haeringer G. i sur. 2021).

Za razliku od platformnih valuta, cilj kriptovaluta je postizanje konkurentnosti zakonskim sredstvima plaćanja i zamjena financijskih institucija. Teži se ostvariti kriptovalute kao univerzalno sredstvo plaćanja (Perušić 2020).

„Tržišta kriptovaluta novonastala su tržišta koja se razvijaju sukladno s razvojem informacijskih tehnologija te se pojavljuje mogućnost odljeva kapitala s tradicionalnih tržišta kapitala na tržišta kriptovaluta“ (Arnerić i Mateljan 2019).

„Tehnički temelji kriptovaluta datiraju do 1980-ih, kad je američki kriptograf David Chaum izumio algoritam koji ostaje centralan modernoj mrežnoj enkripciji. Algoritam je dopuštao sigurnu, neizmjenjivu razmjenu informacija između stranaka. Chaum je ujedno osnovao DigiCash kompaniju koja je proizvodila jedinice valute bazirane na tom algoritmu. DigiCashova kontrola nije bila decentralizirana, kao što je slučaj s modernim kriptovalutama“ (Turudić i sur. 2017).

„Drugi val mrežnog novca manifestirao se u vidu Paypala i e-Golda. Paypal je nudio neprekidan peer-to-peer transferni mehanizam i jednostavan način prihvaćanja uplata za trgovce. E-Gold je određeno vrijeme nudio alternativu Paypalu. Taj servis je prihvaćao depozite zlata od korisnika i izdavao je zlatne potvrde (ili e-Gold) na njihove račune. Time je potaknut povećani volumen međunarodne trgovine i plaćanja. E-Gold je, ugašen uslijed milijunskih prijevara i krađa“ (Turudić i sur. 2017).

Bitcoin se prvi put spominje 2008. godine u djelu Satoshija Nakamota te se smatra prvom modernom kriptovalutom. Još na samom početku 2009. godine, Nakamoto je ovu kriptovalutu plasirao u javnost, a manja grupa entuzijasta počela je trgovati i rudariti kriptovalute (više o rudarenju vidjeti u potpoglavlju 1.1.1). Sljedećih godina pojavile su se alternative i konkurenti, a zatim i prve Bitcoin mjenjačnice. Obzirom da i dalje druge

kriptovalute nisu toliko interesantne široj masi, a također nisu implementirane u sustav plaćanja, korisnicima je omogućeno da ih zamijene za Bitcoin na što sugeruraju Turudić i sur. (2017).

### 1.1.1. Rudarenje

Rudarenje (*engl. mining*) je proces izvođenja složenih matematičkih operacija pomoću snažnih računala na kriptografskoj mreži. Proces rudarenja zahtijeva snažna računala sposobna obraditi složene algoritme koji osiguravaju stabilnost cijelog sustava. Stoga današnja moćna računala, koja se oslanjaju na rad grafičkih kartica, iziskuju i iznimno efikasan sustav hlađenja koji troši neuobičajeno mnogo energije. Prethodno spomenuta složena struktura računalnog sustava sastavljena za potrebe rudarenja koja se naziva rudarskim rig-om (*engl. mining rig*) (Vondraček 2021).

Isto tako, virtualna kripto mreža bilježi izvršenje mnogih transakcija, a rudari (*miners*) su potrebni kako bi mrežu očuvali stabilnom te pratili sve transakcije. Rudari stabiliziraju sustav koji služi u svrhu trgovanja kriptovalutama, na način kao što to rade središnje svjetske monetarne institucije. Iznimka je u tome što kod sustava kriptovaluta nema središnje institucije koja regulira transakcije koje se bilježe i prikupljaju. Iz istih se nadalje kreira lanac blokova (*engl. blockchain*). Sam proces rudarenja sastoji se od potvrđivanja ovih brojnih transakcija i njihovog knjiženja u glavnu knjigu (*engl. General ledger*). Rudari uzimaju transakcijske podatke koje pretvaraju u kraći oblik (hash) pomoću matematičkih operacija ili formula (numeričkih kodova). Upravo taj kraći oblik (hash – niz brojeva i slova) rudaru osigurava nagradu u kriptovaluti. Hash se koristi za ažuriranje lanca blokova odnosno blockchaina, a informacije su dostupne svima na mreži, odnosno svi su upoznati s tim da je kreirana nova kriptovaluta (RRIF 2018).

Hash se također smatra mjerom brzine rudarenja. Proces proizvodnje dobara ili pružanja usluga svoju profitabilnost dobiva iz pažljivog planiranja ulaznih troškova i određivanja cijene određenog proizvoda ili usluge. U procesu rudarenja postoji podosta nepoznanica, a nestabilno tržište koje određuje vrijednost kriptovaluta odjednom povećava rizik ulaganja te time može ugroziti profitabilnost poslovanja. Odgovarajući model sljedivosti ovisi o prirodi

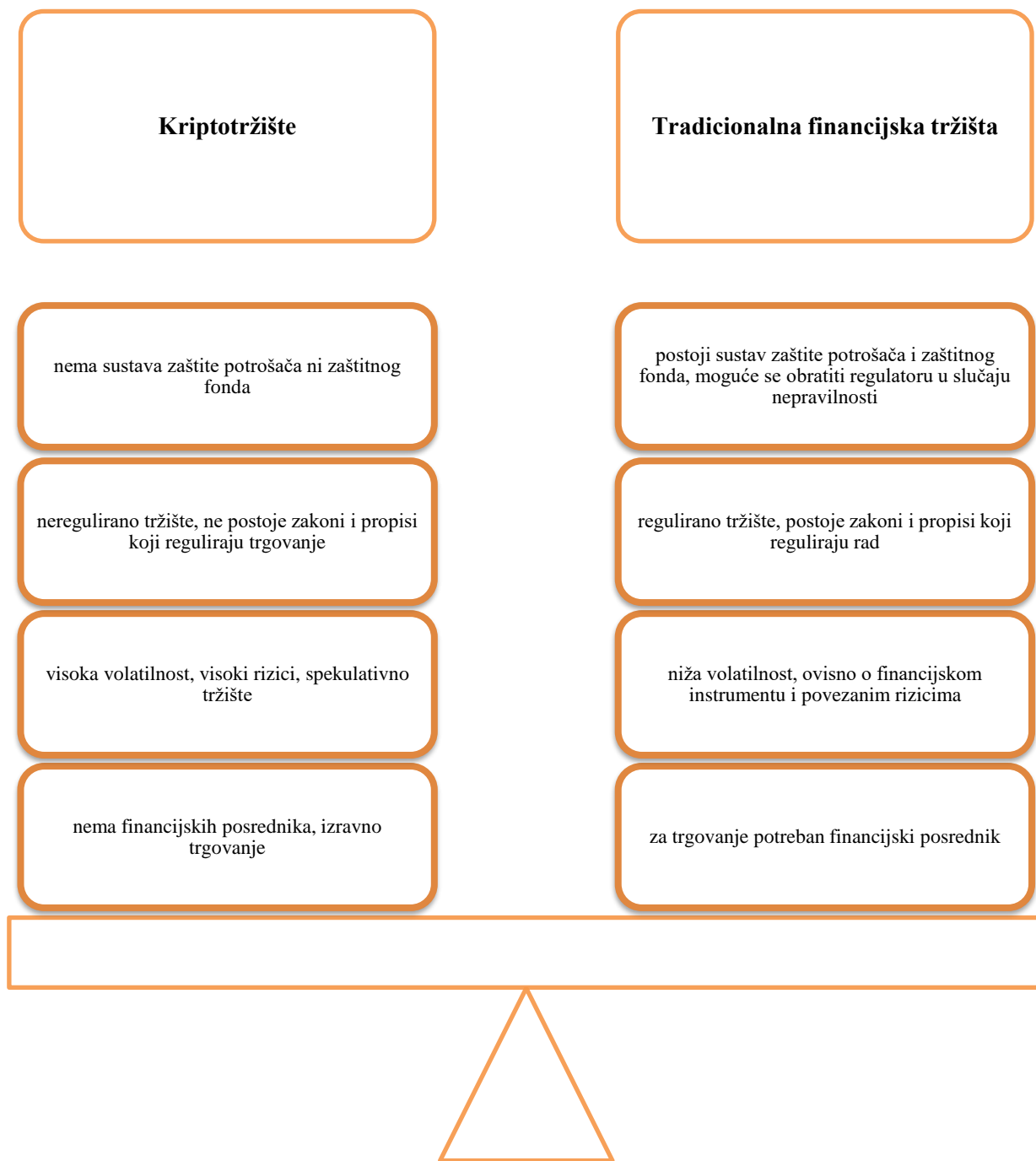
poslovanja s kriptovalutama, stoga ga treba objasniti u bilješkama uz financijska izvješća te prvenstveno na sadržaju transakcije ili događaja, a ne na pravnom obliku (RRIF 2018).

### 1.1.2. Tržište kriptovaluta

Sve izraženiji tehnološki napredak i sveopća digitalizacija suvremenog društva, kao i pojava COVID-19 pandemije koja je dovela do smanjenja fizičkih kontakata i traženja alternativnih načina poslovanja, rezultirali su očvršćivanjem tržišta virtualnog, odnosno digitalnog novca (Mijatović 2022).

Iako je primjena kriptovaluta kao sredstva plaćanja za isporučena dobra i dalje ograničena, mnogi investitori na ulaganje u kriptovalute gledaju kao na zanimljiv ulog koji dugoročno gledano može povećati njihovu imovinu. Takav progresivan razvitak tržišta i vrijednosti kriptovaluta otvara mogućnosti za industriju osiguranja koja pomno prati kretanja. U slučaju daljeg jačanja tržišta kriptovaluta, ako to procijeni potrebnim, industrija osiguranja može snažnije reagirati pružanjem svojih osigurateljskih proizvoda kao odgovora na izraženu nesigurnost tržišta kriptovaluta (Horvatić i Tafra 2022).

„Za razliku od tradicionalnih financijskih tržišta, sustav plaćanja na tržištu kriptovaluta potpuno je decentraliziran na osnovi kriptografskih protokola koji osiguravaju anonimnost, nisku cijenu i brzinu transakcija. Iako su tržišta kriptovaluta visokorizična, upravo su te osobine privukle velik interes javnosti, posebice zato što su prinosi na tim tržištima pozitivni i viši“ (Arnerić i Mateljan 2019).













**Grafikon 2.** Razlika između kriptotržišta i tradicionalnih financijskih tržišta

**Izvor:** izrada autora prema HANFA, preuzeto s <https://www.hanfa.hr/media/6631/kriptotr%C5%BEi%C5%A1te-12-2021.pdf>

Tržište kriptovaluta označava sinergiju ponude i potražnje. Arnerić i Mateljan (2019.) ukazuju kako se „trgovina kriptovalutama uglavnom odvija na javnim mrežnim

mjenjačnicama“. Dakle, te mjenjačnice djeluju poput reguliranih sekundarnih tržišta za vrijednosne papire kojima se trguje preko blagajni trgovca. Online mjenjačnice za trgovanje kriptovalutama značajno su se aktivirale posljednjih godina, a obzirom na popularnost kriptovaluta unazad nekoliko godina, bilježi se i porast kripto mjenjačnica. Na slici 1. prikazano je 10 mjenjačnica koje trenutno ostvaruju najveći promet.

#	Exchange	Score	Trading volume(24h)	Avg. Liquidity	Weekly Visits
1	 Binance	9.9	\$7,340,721,408	888	11,122,174
2	 Coinbase Exchange	8.6	\$1,141,396,239	775	23,615
3	 Kraken	8.1	\$501,430,329	741	967,635
4	 KuCoin	7.5	\$456,275,364	576	1,715,826
5	 Bybit	7.3	\$866,900,747	643	2,983,213
6	 OKX	7.3	\$1,026,386,774	609	2,749,077
7	 Bitfinex	7.2	\$133,416,981	605	500,638
8	 Bitstamp	7.0	\$131,195,701	584	238,513
9	 Gate.io	6.9	\$527,728,269	579	2,839,540
10	 Bitget	6.8	\$635,737,148	612	1,940,708

**Slika 1.** Najprometnije mjenjačnice na tržištu kriptovaluta

Izvor: <https://coinmarketcap.com/rankings/exchanges/>

Arnerić i Mateljan (2019) izdvajaju sljedeće „temeljne funkcije tržišta kriptovaluta:

- mobilizacija štednje,
- pružanje likvidnosti (omogućava brzu prodaju kriptovaluta),
- određivanje cijena (uravnoteženjem ponude i potražnje),



- alokacija resursa,
- omogućavanje dugoročnih investicija i
- kontinuirana dostupnost sredstava (kontinuirano trgovanje)“.

Nadovezujući se na navedeno, Orsag (2011.), sugerira kako je, kratak rok u kojem mogu unovčiti kriptovalutu, ulagačima veliki poticaj za ulaganje u iste.

## 1.2. Blockchain

Blockchain je digitalna knjiga ekonomskih transakcija koja se može koristiti za bilježenje ne samo financijskih transakcija, već bilo kojeg objekta s intrinzičnom vrijednošću (Fang i sur. 2022).

U svom najjednostavnijem obliku, blockchain je niz nepromjenjivih zapisa podataka s vremenskim oznakama, kojima upravlja klaster strojeva te koji ne pripadaju niti jednom entitetu. Svaki od ovih blokova podataka zaštićen je kriptografskim načelom i povezan je jedan s drugim u lancu (Fang i sur. 2022).

Blockchain tehnologija ima izuzetan potencijal u postizanju revolucije unutar financija, a posebno poduzetničkih financija. Kroz blockchain se rješava potreba rukovanja, pohranjivanja i prenošenja osjetljivih informacija između različitih entiteta kombinirajući jedinstveni zapis koji je stvorio centralizirani sustav, a istovremeno distribuirajući decentralizirani proces upravljanja podacima (Sharma 2022).

Transakcija je zapravo datoteka s informacijama, a korisnik koji vrši transakciju potpisuje istu koristeći svoj privatni ključ. Nakon potpisivanja, transakcija se emitira na mreži. Kad transakcija bude prepoznata, vrši se verifikacija valjanosti potpisa te, ukoliko je verifikacija valjana, blok se dodaje u lanac, a svi ostali blokovi dodani nakon njega potvrđuju tu transakciju. Sukladno navedenom, blockchain prati tijek transakcije, provodi istu bez posrednika te omogućuje stvaranje novih vrednosnih jedinica (Perkušić 2020).

Svaka transakcija koja uključuje kupnju, prodaju, ulaganje itd. uključuje blockchain izvorni token ili pod-token. Blockchain je platforma koja pokreće kriptovalutu i tehnologija koja djeluje kao distribuirana knjiga za mrežu. Mreža stvara sredstvo transakcije i omogućuje prijenos vrijednosti i informacija. Kriptovalute su tokeni koji se koriste u tim mrežama za slanje vrijednosti i plaćanje tih transakcija. Oni se mogu smatrati alatima na blockchainu, a u nekim slučajevima također mogu funkcionirati kao resursi ili uslužni programi. U drugim slučajevima, koriste se za digitalizaciju vrijednosti imovine.

### **1.3. Sigurnost kriptovaluta**

Sigurnost kriptovaluta izgrađena je na kriptografiji, dakle nisu je osmislili ljudi i ne počiva na povjerenju, navode Narayanan i sur. (2016). Kriptovalute reprezentiraju svojevrsni novitet po pitanju upravljanja novcem i to ne samo na fizičkoj, već i na idejnoj razini. Kriptografija eliptične krivulje je vrsta kriptografije s javnim ključem koja se oslanja na matematiku kako bi se osigurala sigurnost transakcija. Kada bi netko pokušao zaobići gore navedenu shemu šifriranja i "pogoditi brojeve", potrebna mu je jedna desetina starosti svemira da pronađe odgovarajuću vrijednost kada isproba 250 milijardi mogućnosti svake sekunde (Narayanan i sur. 2016).

Kao i svaki vid digitalne tehnologije i kriptovalute su podložne povredama kibernetičke sigurnosti ukoliko padnu u ruke hakera. U 2021. godini više od 600 milijuna dolara ethereuma i drugih kriptovaluta ukradeno u platformi Poly Network koja se temelji na blockchainu, prenio je Forbes (Ponciano 2021). Suprotstavljanje ovoj situaciji zahtijeva neprekidno nadgledanje sigurnosne infrastrukture i primjenu još naprednijih sustava i strategija kibernetičke sigurnosti u odnosu na one unutar tradicionalnih banaka (Narayanan i sur. 2016).

Zabrinutost oko autentifikacije, autorizacije i povjerljivosti transakcija kod kriptovaluta sprječava usvajanje istih od strane potencijalnih korisnika. Ukoliko bi se postigla standardizacija sigurnosnih tehnika i metodologija unutar sustava kriptovaluta na svjetskoj razini, krajnjim bi se korisnicima omogućilo lakše donošenje odluka oko usklađivanja (Psaila 2018).

Ono što je imperativ po pitanju sigurnosti unutar kripto svijeta je blockchain tehnologija koja zbog svoje kompleksnosti otežava kibernetičke napade. Dakako, pojedinci postavljanjem čvrstih lozinki, korištenjem dvostruke autentifikacije te zaštitom podatka uvelike doprinose zaštiti prvenstveno svoje kriptoimovine.

Pseudoanonimnost i nedostatak nadzora narušavaju sigurnost, stoga je neophodno koncipirati učinkovite okvire upravljanja sigurnošću na način da se osigura da sudionici na tržištu rade na transparentan i odgovoran način afirmirajući integritet financijskog sustava. (Bank for International Settlements 2023).

Za kriptovalute se može zaključiti da je sigurnost istih kontradiktorna. S jedne strane kriptografska rješenja su izuzetno adekvatno osmišljena provodeći najveću razinu zaštite prilikom upotrebe. S druge strane, zaštita nikada ne može biti potpuna obzirom na činjenicu da postoji i pa čak minimalna vjerojatnost da se sigurnost naruši.

## 2. Bitcoin

Bitcoin je kriptovaluta formulirana na konceptu "peer-to-peer"<sup>1</sup> mreže (Nakamoto, 2008).

Za ovaj 'izum' zaslužan je pseudonimni programer softvera ili možda haker po imenu "Satoshi Nakamoto". Ključna namjera bila je razviti sustav transakcija koji će se temeljiti na matematičkom algoritmu te neće zahtijevati intervenciju središnje ili monetarne vlasti. Nadalje, ono čemu se težilo je da se adekvatno osigura zaštita elektroničkih transakcija. Primjenjivost koncepcije Bitcoina podrazumijeva sustav plaćanja gdje se transakcije obavljaju izravnim putem između osobe koja vrši plaćanje (vlasnika Bitcoina) i osobe koja zaprima Bitcoine (primatelja) te se emitiraju putem P2P mreže. Ono što je također bitna stavka u cijelom procesu je da, usprkos činjenici da se rad o javnim informacijama, stvarni identitet korisnika ostaje anoniman (Smales 2019).

Bitcoin je označio je početak revolucije decentralizirane digitalne valute. Među klasama imovine, Bitcoin je imao jednu od najpromjenljivijih povijesti trgovanja. Povijesno gledano prvo značajnije povećanje cijene Bitcoina bilo je 2010. godine nakon što je vrijednost jednog Bitcoina skočila sa samo 0,0008 na 0,09 američkih dolara. Naime, kriptovaluta je postala popularna kao sredstvo razmjene. Ulagači su se okrenuli Bitcoinu kao načinu pohranjivanja vrijednosti, stvaranja bogatstva i zaštite od inflacije (Edwards 2023).

Kriptovalutu se smatra digitalnim ekvivalentom novca te kao takva objedinjuje određene specifičnosti. Ono što Bitcoin čini specifičnim je činjenica da čovječanstvo po prvi puta koristi proizvod čija je ponuda strogo ograničena. Neovisno o tome koliko ljudi koristi mrežu, koliko je napredna oprema korištena za proces proizvodnje te koliko vrijednost Bitcoina pada ili raste u konačnici može postojati samo 21 milijun Bitcoina. Shodno tome, zaključuje se kako ne postoji tehničko rješenje ni mogućnost povećanja broja Bitcoina kako bi se izbalansirala ponuda s potražnjom. Sukladno navedenom, jedini način da se potražnja zadovolji je kroz rast cijene postojeće ponude (Ammous, 2020).

---

<sup>1</sup> Peer-to-peer (P2P) decentralizirani je komunikacijski model u kojem svaka strana ima iste mogućnosti i bilo koja strana može pokrenuti komunikacijsku sesiju (Nakamoto, 2008).

## 2.1. Povijest Bitcoina

Godine 2009. Bitcoin je prvi put korišten nakon što je objavljen kao softver otvorenog koda, kada je Nakamoto rudario početni blok blockchaina. Ovo se naziva *Genesis Block*, a isti je blok sadržavao prvih 50 Bitcoina ikada stvorenih. Od tada pa nadalje, Bitcoinom su nastavile rudariti druge grupe ljudi sve do 2010. godine. Tada je programer Laszlo Hanyecz napravio prvu poznatu komercijalnu transakciju koristeći kriptovalutu kupnjom dviju Papa John's pizza za 10.000 Bitcoina. Ukoliko bi gledali 2021. godinu kada je Bitcoin postigao svoju najveću vrijednost, to bi značilo da je spomenuti programer dvije pizze platio preko 687 milijuna američkih dolara. Od tada se Bitcoinom trgovalo stotine milijuna puta, a najranije velike transakcije dogodile su se na crnim tržištima. Najveći od njih bio je Silk Road, koji je trgoval s gotovo 10 milijuna Bitcoina tijekom svog postojanja. Silk Road je bio prvo online mjesto za anonimnu kupnju i prodaju ilegalnih proizvoda i usluga pomoću Bitcoina (Edwards 2023).

U periodu od 1998. do 2009. godine postojalo je nekoliko prethodnih pokušaja stvaranja online valuta s prateći osiguranim enkripcijama. Dva primjera toga bili su Bit Gold i B-Money, koji su formulirani, ali uopće nisu u potpunosti razvijeni. Godine 2008. rad pod nazivom "Bitcoin: Peer-to-Peer sustav elektroničke gotovine" objavljen je na raspravi o kriptografiji na mailing listi. Objavio ju je netko tko se zove Satoshi Nakamoto, čiji je pravi identitet do danas ostao misterij. Tijekom 2009. godine softver za Bitcoin je prvi put dostupan javnosti i počinje proces zvan 'rudarenje' kroz koji se stvaraju novi Bitcoin, a transakcije bilježe i provjeravaju na blockchainu (Marr 2017).

U 2010. godini Bitcoin kao kriptovaluta je prvi put valorizirana. Budući da se njome nikada nije trgovalo, već samo rudarilo, bilo je nemoguće dodijeliti novčanu vrijednost jedinicama kriptovalute u nastajanju. Kao što je ranije rečeno, godine 2010. programer Laszlo Hanyecz je prvi put odlučio prodati svoju digitalnu valutu za dvije pizze i tada napravio prvu komercijalnu transakciju kriptovalutom Bitcoin. U 2011. godini pojavljuju se prve konkurentske kriptovalute. Kako je Bitcoinu rasla popularnost tako je rasla i ideja o decentraliziranim i šifriranim valutama pri čemu se pojavljuju prve alternativne kriptovalute. Prve alternativne digitalne valute koje su se pojavile bile su Namecoin i Litecoin. Trenutno

je u opticaju više od 1.000 vrsta kriptovaluta, a nove se često pojavljuju na kriptovalutnom tržištu (Marr 2017).

U 2013. godini zabilježen je pad cijene Bitcoina. Ubrzo nakon što cijena jednog Bitcoina prvi put dosegla 1.000 dolara, cijena je nakon toga brzo počela padati. Brojni ulagači su u ovom trenutku pretrpjeli gubitke jer je cijena Bitcoina pala za čak 70%. Tijekom 2014. godine su zabilježene prve značajnije prijevare i krađe. Bitcoin se pokazao kao atraktivna i unosna meta za kriminalne radnje što zapravo i ne iznenađuje za valutu dizajniranu s anonimnošću i nedostatkom monetarne kontrole. U siječnju 2014. godine tada jedna od najvećih svjetskih Bitcoin mjenjačnica Mt.Gox ukinula je svoju stranicu te onemogućila trgovanje, a vlasnici 850.000 Bitcoina nikada više nisu vidjeli svoj digitalni novac. Istrage su još uvijek u tijeku, no u konačnici netko je prijevarom stekao korist koja je procijenjena u to vrijeme na više od 450 milijuna dolara. (Marr 2017).

U 2016. godini javlja se nova digitalna platforma Ethereum koja ujedno predstavlja i prvog pravog konkurenta Bitcoinu. Ova platforma koristi kriptovalutu poznatu kao Ether za olakšavanje sklapanja ugovora i aplikacija temeljenih na blockchainu. Njegova najzbudljivija značajka je njegova sposobnost stvaranja obvezujućih financijskih sporazuma koji se mogu provesti u potpunosti pomoću softvera, što znači da nije potrebno sudjelovanje sudova ili drugih ljudskih posrednika. U SAD-u SEC<sup>2</sup> je upozorio ulagače da bi zbog nedostatka nadzora, takvi financijski sporazumi mogli značiti prijevare prerusene u legitimna ulaganja. Kineska vlada otišla je korak dalje te ih u potpunosti zabranila (Edwards 2023).

---

<sup>2</sup> SEC (Securities and Exchange Commission) je komisija za vrijednosnice i burzu Sjedinjenih Američkih Država. Radi se o glavnom nadzornom i regulatornom tijelu financijske industrije u SAD-u. (SEC)



**Slika 2.** Povijest promijene cijene Bitcoina od 2016. do 2023. godine

Izvor: <https://coinmarketcap.com/currencies/bitcoin/>

Kao što se može vidjeti na slici 2., pred kraj 2017. godini započinje nagli rast Bitcoina. U prosincu iste godine, Bitcoin prvi puta doseže vrijednost od 10.000 USD.

Nakon toga u 2018. i u prvoj polovici 2019. cijena uglavnom pada ili neznatno raste, a od druge polovice 2019. godine započinje ponovni rast cijene. Interes tržišta oko Bitcoina raste, a time se proširuje i ponuda mjesta na kojima se može trgovati ovom kriptovalutom. Kroz 2020. godinu i dalje je prisutan trend rasta cijene, a u 2021. Bitcoin doseže najveću vrijednost svih vremena - 68.798,63 USD. Nakon toga, zbog neizvjesne situacije vezane uz inflaciju i pandemiju virusa COVID-19 daljnja ulaganja stagniraju, a u 2022. godini cijena Bitcoina pada do ispod 20.000 USD. U 2023. cijena ponovno raste, no zasad bez značajnijih oscilacija bilo u negativnom ili pozitivnom smislu.

Zbog korištenja kriptovaluta na crnom tržištu, pravne regulative su se pojavila u nekoliko zemalja. Narodna banka Kine pokrenula je najutjecajnije propise s tri odvojene akcije:

- U prosincu 2013. godine banka je naložila financijskim institucijama da više ne koriste Bitcoin;
- U rujnu 2017. godine izdana je potpuna zabrana korištenja Bitcoina;
- U lipnju 2021. godine banka je organizirala posebne grupe koje će nadzirati kriptovalutne transakcije vodećih kriptovalutnih platformi u Kini.

Nakon svakog od ovih slučajeva, cijena Bitcoina se prepolovila. Međutim, unatoč ovim regulativnim propisima, cijena Bitcoina i dalje je podržana i raste zahvaljujući institucijama i zemljama koje dopuštaju korištenje kriptovalute. Tako se javlja partnerstvo Tala, Circle i Stellar Development Foundation s Visom sa svrhom implementiranja blockchain rješenja na tržišta u razvoju kao i nastojanje za proširenje pristupa financijskim uslugama. (Chan i sur. 2022).

Osim prethodno navedenog, potrebno je izdvojiti i primjer države El Salvador koju se naziva globalnim pionirima kriptovalute. Iako je službena valuta države američki dolar, El Salvador je prva država u svijetu koja je 2021. godine Bitcoin učinila zakonskim sredstvom plaćanja. Vlada je razvila digitalni novčanik pod nazivom *Chivo* te je svakom građaninu za registraciju dala ekvivalent od 30 USD u Bitcoinu. Cijeli eksperiment zamišljen je na način da se Bitcoin integrira u sustav plaćanja zemlje u razvoju jer se stanovništvo uglavnom oslanja na gotovinu, a velika većina nema bankovni račun ni usluge korištenja mobilnog bankarstva. Korištenje Bitcoina uključuje niže troškove financijskih transakcija (osobito kod prekograničnih plaćanja), ali i veću financijsku uključenost zahvaljujući njihovoj lakšoj dostupnosti. Vlada El Salvadora promiče usvajanje Bitcoina kroz inicijative kao što su popusti na gorivo koje se plaća u Bitcoinu. Također, od svih poduzeća se zahtijeva da prihvate Bitcoin obzirom, da kao pružatelji usluga, moraju prihvatiti plaćanja u kriptovaluti. (PWC, 2021).

Iako se teži da El Salvador bude neovisniji o američkoj monetarnoj politici, uporaba Bitcoina i dalje nije dovoljno raširena u svakidašnjem životu stanovnika ove države, no rezultati budućih istraživanja donijet će konačnu ocjenu uspješnosti ovog eksperimenta.



## 2.2. Tehnologija Bitcoina

Bitcoin se može steći na originalan način, točnije ranije opisanim procesom rudarenja te derivativnim načinom koji se temelji na kupnji Bitcoina u mjenjačnici ili primanjem Bitcoina kao sredstva plaćanja. Navedeni načini stjecanja Bitcoina ilustrativno su predočeni nižim prikazom (Perkušić 2020).



**Grafikon 3.** Načini stjecanja Bitcoina

Izvor: izrada autora prema Perkušić M. (2020.) Pravo elektroničkog plaćanja

Kako bi se Bitcoin mogao slati, primiti i pohranjivati, neophodno je posjedovati elektronički novčanik (*engl. wallet*). Radi se o računalnom programu gdje se nalaze sve adrese korisnika, privatni ključevi, zalihe Bitcoina te informacije o obrađenim transakcijama. Osim mjesta za pohranu, neophodno je da korisnik posjeduje Bitcoin adresu koja je sačinjena od niza brojeva i slova. Također, za uspješno obavljanje transakcije, potreban je javni ključ (*engl. public key*) koji služi za slanje i prihvaćanje Bitcoina te je isti vezan uz privatni ključ (*engl. private key*) koji se koristi kao lozinka za otključavanje transakcija. Za pristupanje Bitcoin novčaniku, korisnik treba postaviti lozinku prema zadanim parametrima. Tehnologija blockchain čini svaku transakciju Bitcoin sigurnom, provjerenom i gotovo anonimnom. Bitcoin je nereguliran, a ponuda je predvidljiva zbog primjene matematičkog algoritma. Svaki financijski instrument može imati dvije temeljne namjene: pohranu vrijednosti i sredstvo razmjene (Perkušić 2020).

Korisnici mogu kupiti Bitcoine i prodati ih kada tečaj poraste i na taj način ostvariti visoke povrate od ulaganja. O sposobnosti Bitcoina da izbjegne smetnje pravne regulacije koje donose banke, centralizirani sustavi plaćanja i vlade raspravljali su Maurer i sur. (2013.) jer se pozivaju na dvije glavne značajke "privatizaciju" identiteta i njegov "digitalni metalizam". Prema njima Bitcoin je čvrsta digitalna valuta, osigurava sigurnu razmjenu, stabilan je, osigurava anonimnost te pruža kriptovalutnu provjerenu zajednicu. Načelo "dokaza funkcionalnosti rada" pomno su proučili Becker i dr. (2012) te ističu da je Bitcoin sustav plaćanja prilično siguran kada niti jedna strana ne kontrolira više od 50% računalne snage mreže. Međutim, kritiziraju to da potrošnja električne energije potrebna za izvođenje velikih računalnih problema ostavlja iza sebe posljedice štetne za okoliš.

Ögel (2021.) prema Baur i sur. (2018.) navodi kako kriptovalute funkcioniraju unutar digitalnog svijeta pa se i njihovo formiranje, pohrana i trgovina odvija se u potpunosti u digitalnom okruženju. Svaki vlasnik Bitcoina mora imati dva digitalna novčanika. Prvi novčanik je otvoren za javnost i koristi se za primanje Bitcoina dok je drugi novčanik privatniji te se koristi za pohranu i nošenje valuta.

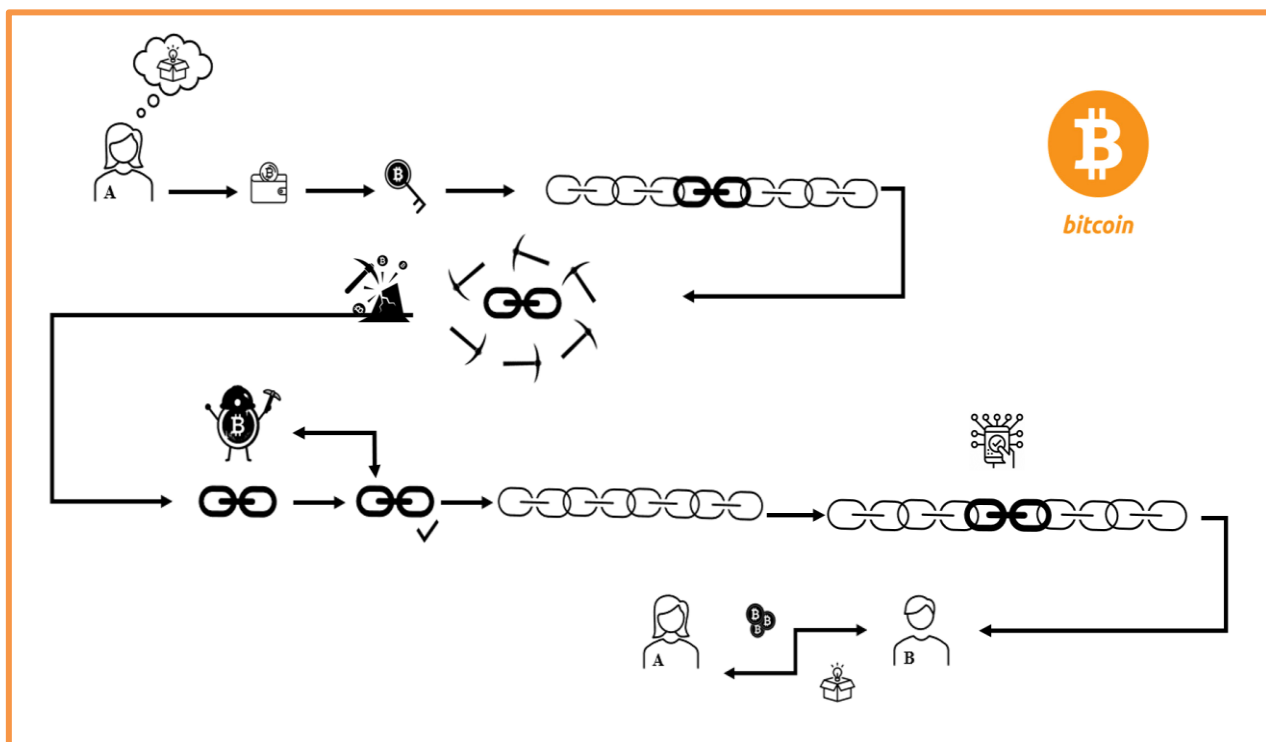
Carrick (2016.) smatra Bitcoin vrlo učinkovitim kriptovalutom za transakcije i može se koristiti u kombinaciji s fiat valutama (tradicionalne valute kao američki dolar i euro) tj. nije zamjena, već suplement. Nadalje, Bitcoin može balansirati između toga da bude sredstvo razmjene, ali i spekulativni instrument, ovisno o sposobnosti korisnika za preuzimanje rizika (Luther i White, 2014). Literatura predlaže da je Bitcoin atraktivan izbor ulaganja, posebno u diverzifikaciji i zaštiti od rizika, a naročito zbog svoje tehnologije koju koristi sugeriraju Wang i sur. (2019). Cijeli mehanizam Bitcoin transakcija temelji se na blockchain tehnologiji i više manje svaki oblik tehnologije se s vremenom razvija kako bi postao bolji.

Prije Bitcoina, postojala je potreba za trećom stranom od povjerenja koja bi vodila glavnu knjigu, odnosno sustav za vođenje evidencije financijskih podataka tvrtke ili osobe kako bi se zabilježilo tko koliku vrijednost posjeduje. Sada svatko ima kopiju ove "knjige" s Bitcoin mrežom, tako da nema potrebe za trećim stranama. Svaka Bitcoin transakcija događa se u Bitcoin blockchain mreži koja je digitalni prostor u kojem se odvija rudarenje Bitcoinima. Blockchain je vrsta baze podataka koja je skup informacija pohranjenih u elektroničkom obliku u računalnom sustavu, čije je funkcioniranje objašnjeno u ranijim poglavljima. Ono što se čuva u bazama podataka, informacije ili podaci obično je strukturirano u obliku tablice

koja olakšava pretraživanje i filtriranje informacija. Baze podataka dizajnirane su za pohranjivanje velikih količina informacija kojima mnogi korisnici u bilo kojem trenutku mogu lako i brzo pristupiti, filtrirati ih i uređivati (Conlon i McGee 2020).

Da bi se to postiglo, opsežne baze podataka čuvaju podatke na poslužiteljima koji se sastoje od vrlo jakih računala. Ti se poslužitelji mogu izgraditi pomoću stotina i stotina računala. Potrebno je imati računalnu pohranu i snagu potrebnu za više korisnika za pristup bazi podataka istovremeno, što je razlika i od baze podataka, primjerice diskova nalik oblaku za pohranu. Blockchain se razlikuje od baze podataka, a glavna razlika je u načinu strukturiranja podataka. Baza podataka strukturira podatke u tablice, dok blockchain prikuplja informacije u grupe, točnije blokove, koji sadrže skupove podataka. Svaki blok ima određeni kapacitet pohrane koji je ulančan na prethodni ispunjeni blok kada se napuni, tvoreći lanac podataka. Zbog toga se i zove blockchain (lanac blokova), a milijuni blokova ispunjenih podacima lančano su povezani (Wang i sur. 2019).

Dakle, blockchain omogućava snimanje i pohranu digitalnih informacija, ali ne i uređivanje istih. Zato se može konstatirati da se u slučaju blockchaina ne radi o bazi podataka obzirom da ga nitko ne može promijeniti kad je jednom ispunjen i zatvoren. Pojavom Bitcoin tehnologije blockchain je dobio svoju prvu stvarnu primjenu.



**Slika 3.** Proces plaćanja Bitcoinom

Izvor: izrada autora prema Perkušić M. (2020.) Pravo elektroničkog plaćanja

Na slici 3. prikazan je proces plaćanja Bitcoinom za određeni proizvod. Iako naizgled kompleksno, plaćanje Bitcoinom uvelike je konkurentnije od tradicionalnog načina plaćanja posebice zbog brzine obrade transakcije i jeftinijeg pristupa u vidu plaćanja naknada (Pekušić 2020).

Osoba **A** želi od osobe **B** kupiti određeni proizvod na način da kao sredstvo plaćanja koristi Bitcoin. Osoba **A** pristupa svom privatnom elektroničkom novčaniku te odabire količinu Bitcoina koji želi preusmjeriti osobi **B**. Također, za nastavak procesa bitno je da osoba **A** unese adresu (javni ključ osobe **B**), a potom pomoću svog privatnog ključa vrši autorizaciju i pokreće transakciju koja se stavlja u transakcijski blok. Nadalje, rudari se natječu koji će prvi potvrditi zadanu transakciju na način da rješavaju matematički zadatak. Onaj koji bude najbrži među rudarima transakcijski blok stavlja u lanac blokova te ga pohranjuje u glavnu knjigu. Kao nagradu za izvršeni zadatak, rudar dobiva nagradu u vidu Bitcoina. Nakon

provedene transakcije, osoba **B** u novčanik sprema Bitcoine zaprimljene od osobe **A** (Pekušić 2020).

### **2.3. Konkurencija**

Bitcoin je samo jedna od brojnih kriptovaluta. Iako postoji preko tisuće kriptovaluta, prvih pet u smislu tržišne kapitalizacije od kolovoza 2022. godine bili su Bitcoin, Ethereum, Tether, US Dollar Coin i Binance Coin (Tretina 2022; Kerr i sur. 2023).

Bitcoin je najstarija i najpopularnija kriptovaluta koja se danas koristi, ali nije bila prva kriptovaluta. Ta ideja zapravo pripada eCash-u, koju je osmislio David Chaum u radu objavljenom 1983. godine koju je kasnije razvio 1990. godine kroz svoju tvrtku DigiCash (Chaum 1983). DigiCash je proglasio bankrot 1998. godine, ali Chaumove ideje ostale su ključne u razvoju kasnijih kriptovaluta.

Poput Bitcoina, Ethereum je kriptovalutna platforma decentralizirane digitalne valute čija valuta, poznata kao Ether, nema intrinzičnu vrijednost, nema centraliziranog izdavatelja i koristi blockchain tehnologiju za bilježenje povijesti transakcija. Međutim, za razliku od Bitcoina, Ethereum ide dalje dopuštajući transakcije ne samo putem kriptovalute već i putem "pametnih ugovora" koji korisnicima omogućuju razmjenu bilo čega vrijednog bez potrebe za uslugama odvjetnika ili javnog bilježnika ili neke druge treće strane (Zapotochnyi 2022).

Osnovan 2015. godine od strane Vitalika Buterina, Ethereum je od tada izrastao u drugu najveću platformu za kriptovalute na svijetu. Međutim, Ethereum je doživio neke značajne rastuće probleme, uključujući krađu Ethern 2016. godine vrijednu 50 milijuna USD od strane anonimnog hakera, što je rezultiralo zabrinutošću za sigurnost platforme (Leising, 2017). Poput Bitcoina, cijena Ethern pokazala je ekstremnu nestabilnost. Na primjer, početkom 2021. godine cijene etera bile su oko 750 USD, da bi do studenog 2021. godine cijena porasla na najvišu vrijednost svih vremena od 4.867 USD, što je povećanje od preko 500% u manje od godinu dana.

Tether, koji se izvorno zvao "Realcoin", osnovan je 2014. godine u Santa Monici i trenutno je u vlasništvu tvrtke iFinex, Inc sa sjedištem u Hong Kongu. Kriptovaluta Tether privlači

mnoge ulagače jer je jedna od prvih kriptovaluta koja se označava kao "stabilna valuta". Izdavatelji stabilnih valuta nastoje povezati svoju tržišnu cijenu s valutom koju je izdala vlada ili drugom neovisnom referentnom točkom, smanjujući tako volatilitet cijena svojstvenu drugim vrstama kriptovaluta. U slučaju Tethera, njegova je cijena prvenstveno vezana uz vrijednost američkog dolara (Casey 2014).

Niti razvoj Tethera kroz povijest nije prošao bez kontroverzi. Godine 2017. godine haker je ukrao Tether tokene u vrijednosti od 31 milijun USD iz Tetherova digitalnog trezora te iste prenio ih na neovlaštenu Bitcoin adresu, što je izazvalo zabrinutost za sigurnost platforme. Godine 2021. godine, Američko povjerenstvo za trgovinu robnim ročnicama (CFTC) kaznilo je Tether s 41 milijun USD zbog tvrdnji da je Tether u potpunosti podržan američkim dolarima. (Schroeder 2017) .

Slično Tetheru, USD Coin je stabilna kriptovaluta. Njegova vrijednost je vezana i podržana američkim dolarom, a vlasnici USD Coina mogu otkupiti 1 USD Coin za 1 američki dolar. Kao stabilna kriptovaluta, jedna od njezinih primarnih svrha je pružiti ulagačima stabilnost vrijednosti, a ne povećanje vrijednosti. Za razliku od Tethera, koji je poznat po tome što njegove rezerve nisu revidirane od strane profesionalnih neovisnih revizora, rezerve USD Coina mjesečno pregledava računovodstvena tvrtka Grant Thornton LLP (Bhattacharya 2021).

Najveća svjetska burza kriptovaluta u smislu dnevnog volumena trgovanja je Binance. Binance izdaje dvije kriptovalute, Binance Coin (BNB) i Binance USD (BUSD). Binanceove relativno niske naknade za transakcije i mogućnost zarađivanja Binance Coina kao nagrade za preporuku Binancea drugim ljudima pomogle su u povećanju njegove popularnosti. S negativne strane, neki ljudi smatraju da je Binance težak za korištenje, a ljudi u Sjedinjenim Američkim Državama ne mogu koristiti platformu Binance, jer je zakonski zabranjena od 2019. godine. Američki građani, međutim, mogu pristupiti Binance US, koja je drugačija i ograničenija burza od Binancea. Businessweek izvještava da su američki regulatori, uključujući Komisiju za vrijednosne papire, Ministarstvo pravosuđa i Poreznu upravu, istraživali Binance US i Binance zbog pranja novca i prijevare u lipnju 2022. godine (Davidson 2022).

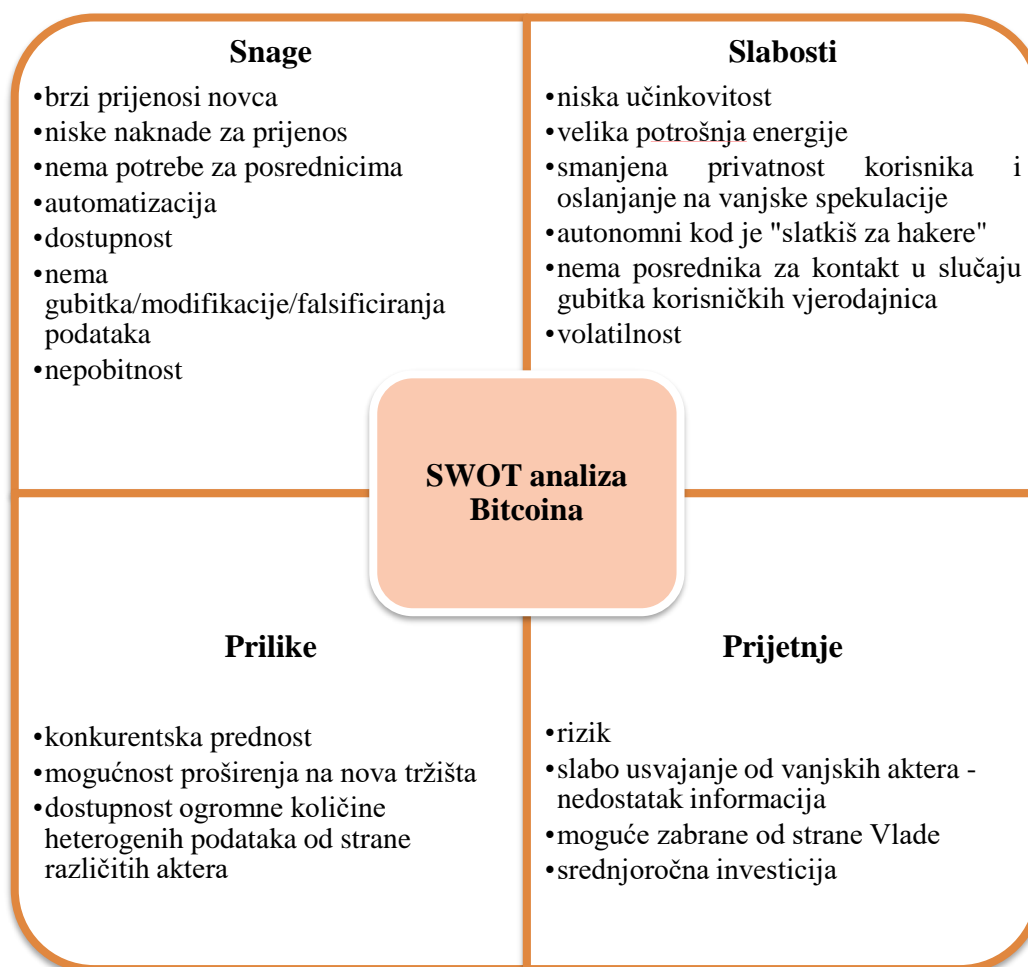
## 2.4. SWOT analiza

Kako bi se što bolje mogao donijeti zaključak o budućnosti Bitcoina, SWOT analizom razmotrit će se sadašnje i buduće snage, prilike koje kriptovaluta može stvoriti, a s druge strane prikazat će se slabosti i prijetnje koje će, primjenom odgovarajuće strategije, biti reducirane.

Dok je Bitcoin možda izvorna digitalna valuta, od tada su stvorene mnoge druge kriptovalute. Ipak, Bitcoin je uspio ostati jedinstven na više načina, a druge kriptovalute se čak nazivaju Altcoins (alternativne kriptovalute za Bitcoin). Druge kriptovalute razvijane su od 2009. godine pa nadalje s potencijalom za upravljanje digitalnim ekonomijama poput Ethereum (Cocco i sur. 2017).

Bitcoin je ostao oblik valute na više platformi. Bez ograničenja za korištenje na određenim platformama samo za Bitcoin, ova se kriptovaluta može koristiti za kupnju bilo gdje u svijetu gdje je prihvaćena. Nadalje, glavni cilj iza Bitcoina je povećanje brzine transakcija bez brojnih državnih ograničenja. Godine 2020. Bitcoin je dospio na naslovnice kada je Paypal (PYPL) objavio da će ova popularna valuta biti priznata kao plaćanje na njihovoj platformi.

Na sljedećem shematskom prikazu predstavljene su snage, slabosti, prilike i prijetnje Bitcoin valute.



**Grafikon 4.** SWOT analiza kriptovalute Bitcoin

Izvor: izrada autora prema Stilgherrian, B. (2017.) Let's quit the blockchain magic talk

Prednosti blockchain tehnologije uglavnom se odnose na predstavljene tehnološke aspekte, a upravo taj segment čini glavnu snagu Bitcoina. Uklanjanjem posrednika mogu se smanjiti troškovi prijenosa novca, a ubrzati procesi transakcije jer se kriptovalute izravno premještaju s adrese novčanika jednog korisnika na drugu bez međukoraka (kao što se obično događa, npr. u inozemstvu kod bankovnih transfera). Pametni ugovori pružaju visok stupanj automatizacije. Transparentnost je zajamčena jer se blockchainu može pristupiti diljem svijeta. Osim toga, budući da bi potencijalno svatko mogao pisati u glavnu knjigu, blockchain bi mogao postati spremište ogromne količine informacija, koji bi se mogli koristiti za analizu podataka u različitim sektorima (ne nužno povezanima s osiguranjem i financijama, već sektorima poput medicine, obrazovanja itd.). Temeljni kriptografski



mehanizam jamči to da podaci nisu modificirani i da se transakcije ne mogu odbiti (Bitinfocharts 2017).

Najrelevantnije slabosti odnose se na nisku učinkovitost, veliku potrošnju energije i performanse. Zapravo, trenutačno je broj komercijalnih transakcija kojima se može upravljati u sekundi izuzetno nizak u usporedbi s tradicionalnim sustavima i to uglavnom zbog računalne snage potrebne za potvrdu blokova (Stilgherrian, 2017).

Osim vremena, prostor je također problem, jer se podaci repliciraju na svakom mrežnom čvoru. Primjerice, Bitcoin blockchain zahtijeva više od 170 GB prostora za pohranu na svakom mrežnom čvoru. Osim toga, iznos energije koju troše mrežni čvorovi i trošak hardvera potrebnog za provjeru valjanosti novih blokova je iznimno visok, procjenjuje se na oko 6 američkih dolara po transakciji (Cocco i sur. 2017).

Činjenica da su informacije, jednom kodirane u blockchainu, nepromjenjive i dostupne još je jedna slabost i navedeno može naštetiti privatnosti korisnika. Primjerice, svatko bi mogao provjeriti iznos novca koji posjeduje neka osoba, analizirajući dolazne transakcije te osobe. Nepromjenjivost i samoizvršavanje koda mogli bi biti još jedna slabost blockchaina, jer pametni ugovori mogli bi postati tzv "slatkiš za hakere". Zapravo, hakeri bi mogli iskoristiti greške u pametnim ugovorima kao što se dogodilo na mreži Ethereum, gdje je, u lipnju 2016. godine ukradeno više od 60 milijuna američkih dolara (Wang i sur. 2019).

Najslabija točka bi u ovom slučaju bile bi spekulacije oko rasta ili pada cijene Bitcoina jer se spekulacije mogu temeljiti na pogrešnim informacijama iz različitih izvora koje ostaju stalno u blockchainu (Stilgherrian, 2017).

Još jedan aspekt slabosti je volatilnost kriptovaluta. Obzirom na činjenicu da su kriptovalute predmet spekulacija i na to da tehnologija još nije u potpunosti zrela (i greške se često pojavljuju), vrijednost kriptovaluta izložena je ogromnim fluktuacijama. Još jedna slabost povezana je s činjenicom da su razvojni alati još uvijek u ranoj fazi te standardi za razvoj aplikacija temeljenih na blockchainu još nisu definirani (Peck 2017).

Prilike se uglavnom odnose na to hoće li tržište prihvatiti tehnologiju Bitcoina ili ne. U ovom trenutku, interakcija s blockchainom zahtijeva neke tehničke vještine (npr. svladavanje pojma blokova, instaliranje novčanika i sl.) (Stilgherrian 2017).

Druga prilika je vezana uz mogućnost ulaska na nove vrste tržišta i kreiranja novih vrsta usluga, uglavnom iskorištavanjem toga što nema trećih osoba koje bi isto nadzirale i niskih naknada za transakcije. Konačno, ako velik broj aktera upisuje velike količine podataka na blockchain vremensku traku, bezbroj novih aplikacija bi se moglo pojaviti. Primjerice, blockchain bi mogao postati spremište medicinskih podataka koje bi mogli koristiti znanstvenici istraživači, opskrbeni lanci temeljeni na blockchainu mogli bi biti učinkovitiji budući da se podaci mogu dijeliti gotovo trenutačno među heterogenim uključenim akterima, a u slučaju osiguranja, podaci bi se mogli koristiti za sprječavanje prijevara, personalizaciju policaj i sl. Unatoč tome, vrsta i učinak tih aplikacija ovisit će o količini i kvaliteti zabilježenih informacija i podataka (Liu i sur. 2017; Peck 2017).

Prijetnje su povezane s različitim vanjskim uzrocima. Prije svega, još uvijek postoji rizik da tržište ne vjeruje ovoj vrsti tehnologije, doživljava je kao nesigurnu ili nepouzdanu, zbog grešaka, volatilnosti, rizika i neizvjesnosti. Drugi bi akteri mogli misliti da je usvajanje znanja o kriptovalutnoj tehnologiji prekomplicirano, a stopa usvajanja znanja na svjetskoj razini može biti vrlo niska (Peck 2017; Wang i sur. 2019).

Posebnu pozornost treba obratiti na zakonske propise vlada, banaka i drugih regulatornih organa koji bi mogli ugroziti poslovanje na kriptovalutnim tržištima. Što se tiče praktičnih aspekata, trgovanje i ulaganje u kriptovalute je srednjoročno. Konačno, ako blockchain tehnologija postane praksa, to bi moglo utjecati na odnos tvrtke sa svojim kupcima. Prije svega, neki bi kupci mogli odbiti prihvatiti ga, jer smatraju osobnu interakciju boljom (Cocco i sur. 2017).

### **3. Rizik investiranja u kriptovalute s naglaskom na Bitcoin**

Od pojave vjerojatnosne procjene rizika, rizik se definira kao matematički umnožak vjerojatnosti događaja i neke mjere njegovih negativnih posljedica. U financijskim analizama rizik se često mjeri pomoću varijance, odnosno što je veća varijanca, to je veći rizik. Međutim, povijesno gledano, varijanca se također smatrala mjerom disperzije, nesigurnosti i sredstvom za procjenu prilagodbe modela (Dionísio i sur. 2006).

Rizik se često poistovjećuje s pojmom neizvjesnosti, a Knight (1921.) u svom djelu razlikuje ta dva pojma na temelju kvantifikacije.

„Rizik je pojava koja se da kvantitativno iskazati (izmjeriti); sadrži vjerojatnost koja se može identificirati, odnosno procijeniti. Ako nešto ne možemo ni identificirati, ni definirati, ni mjeriti onda time ne možemo ni upravljati i tada govorimo o neizvjesnosti“ (Sajter 2017).

Zapravo neizvjesnost postoji kada je distribucija vjerojatnosti rezultata nepoznata. Uz pojmove rizika i neizvjesnosti povezuju se i sama ulaganja u kriptovalute obzirom da se ista često percipiraju kao neizvjesna i rizična.

### 3.1. Pravna regulativa

Bitcoin radi na decentraliziranom mehanizmu koji mu omogućuje da bude izoliran od bilo kakve intervencije regulatornog tijela. Nadalje, Bitcoin je odobren kao anonimna u smislu identiteta korisnika i svaka transakcija je nepovratna, naznačuje Bradbury, (2013).

Zebeć (2018) sugerira da na razini Europske unije svaka država utemelji svoje propise koji reguliraju trgovinu Bitcoinom obzirom da se ova razina jurisdikcije virtualne valute još uvijek smatra dostatnom. Do sada niti jedna institucija Europske Unije nije izdala posebne propise za trgovanje virtualnim valutama. No, 2012. godine Europska središnja banka je u svom izvješću navela da se tradicionalni financijski propisi možda neće primjenjivati na Bitcoin, koji je također opisala kao decentraliziranu konvertibilnu virtualnu valutu (Europska središnja banka 2012). Naime, oni upozoravaju da sustavi okruženi pravnom nesigurnošću virtualnih valuta mogu predstavljati izazov za vlasti, uglavnom zato što se ti sustavi mogu koristiti za nezakonite kriminalne aktivnosti, prijevare i pranje novca.

Jedna od najvećih rasprava u regulatornim razgovorima je treba li kriptovalutu klasificirati kao vrijednosni papir, robu, valutu ili nešto treće. Od sada, ovo je uglavnom pitanje bez odgovora. Ako se kriptovaluta smatra robom poput sirove nafte, kave ili prirodnog plina, njezin primarni američki regulator bio bi Commodity Futures Trading Commission (CFTC). Ova agencija regulira trgovanje valutama, a pokrivala bi i trgovanje kriptovalutama ako bi se iste smatrale valutama. No, ukoliko zakonodavci i regulatori dođu do ideje da se kripto treba smatrati vrijednosnim papirom, poput dionica, obveznica i fondova kojima se trguje, to bi potpalo pod nadležnost SEC-a (Duggan 2023). Predsjednik SEC-a, Gary Gensler, jasno je dao do znanja kako vjeruje da su velika većina kriptovaluta vrijednosni papiri, na temelju Howey testa, koji proizlazi iz presude Vrhovnog suda iz 1946. godine u predmetu SEC protiv WJ Howey Co. Međutim, Gensler je također posebno spomenuo Bitcoin kao iznimku, klasificirajući ga kao robu. Prema Howeyevom testu, transakcija se smatra vrijednosnim papirom ako ispunjava sljedeća četiri kriterija:

- Novac je uložen.
- Postoji očekivanje da će investitor zaraditi.

- Ulaganje je u zajedničko poduzeće.
- Profiti se generiraju trudom drugih (Duggan 2023).

SEC i druga regulatorna tijela godinama pokušavaju zavladata nezakonitim aktivnostima u kripto sektoru, ali njihovo slamanje je uzelo maha nakon kolapsa kripto burze FTX u studenom 2022. godine. Kada je FTX propao u studenom 2022. godine, SEC je podigao razne optužbe protiv osnivača FTX-a Sama Bankman-Frieda, kao i nekoliko drugih rukovoditelja povezanih s FTX-om, zbog njihove navodne uloge u prijevari investitora. Troje rukovoditelja povezanih s FTX-om od tada su se izjasnili krivima za optužbe i surađuju s tužiteljima, uključujući suosnivača FTX-a Garyja Wanga, izvršnu direktoricu Alameda Research Caroline Ellison i FTX-ovog direktora inženjerstva Nishada Singha (Duggan 2023).

Bitcoin je stoga još uvijek u embrionalnoj fazi i mora se razvijati s vremenom, posebno držeći korak s tehnološkim napretkom. Trebao bi biti robustan tj. postojan kako bi bio prihvaćen kao alternativna valuta i kako bi mogao ukloniti bilo kakvo lažno iskorištavanje kao što je to bilo u prethodno navedenom slučaju.

### **3.2. Stajališta banaka**

Za Bitcoin se kaže da je prvi primjer digitalne gotovine: spoj fizičke gotovine i digitalnog plaćanja. Bitcoin kao kripto valuta je primarno tehničko rješenje koje korisnicima omogućava digitalno plaćanje bez dodatnog posredovanja trećeg korisnika (Ammous 2020). Iako se svijet kripto valuta neprestano širi i dobiva na popularnosti, tradicionalne banke oklijevaju prihvatiti upotrebu ove digitalne imovine vjerujući da su njihovi inherentni rizici veći od njihovih potencijalnih koristi. Međutim, regulatorne agencije poput Ureda za kontrolu valuta<sup>3</sup> (OCC) rade na promjeni percepcije banaka o digitalnim valutama, vjerujući

---

<sup>3</sup> Office of the Comptroller of the Currency (OCC) - ured Ministarstva financija Sjedinjenih Američkih Država koji je neovisan, a bavi se osnivanjem, reguliranjem i nadziranjem nacionalnih banaka, saveznih štednih udruženja i saveznih podružnica i agencija stranih banaka. (OCC)

da bi ta imovina mogla pozitivno potaknuti financijske institucije u novu eru inovacija i učinkovitosti (Scicchitano 2023).

Naime, OCC je izdao nekoliko pisama s tumačenjem u kojima se detaljno opisuje kako tradicionalne financijske institucije mogu ulaziti u transakcije (ili razvijati usluge) koje uključuju digitalne valute. Ovaj napor podudara se s nadom OCC-a da će dodatne regulatorne smjernice pomoći bankama da se lakše snađu u trgovanju digitalnim valutama. Banke su oprezne s kriptovalutama, jer smatraju da transakcije koje uključuju tu imovinu predstavljaju povećani rizik i zahtijevaju dugotrajnu i pojačanu dubinsku analizu. Nadalje, kripto imovina stvorena je kao alternativa tradicionalnoj bankarskoj infrastrukturi koja ne treba posrednika i nije povezana s kapacitetom centralizirane vlade, banke ili agencije. Umjesto oslanjanja na centralizirane posrednike u ovim transakcijama, povjerenje se polaže u blockchain kod i distribuiranu prirodu blockchainea što izravno ugrožava funkciju postojanja banaka (Scicchitano 2023).

Kriptovaluta kojom upravlja središnja banka prije svega umanjuje privlačnost imovine, pa neke banke ne vjeruju da će moći uspješno ući u taj prostor. Smatra se da decentralizirana priroda valute potkopava autoritet središnjih banaka, ostavljajući neke da vjeruju da im više neće biti potrebne ili da neće moći kontrolirati ponudu novca. Kriptovalute omogućuju peer-to-peer transakcije bez reguliranog posrednika, dajući korisniku mogućnost jednostavnog brzog prijenosa sredstava bez plaćanja transakcijskih naknada (Bhattacharya 2021).

Umjesto identificiranja transakcije pojedinačnim bankovnim računom putem financijske institucije, transakcije se jednostavno povezuju s ID-om transakcije na blockchainu. Ova vrsta pseudonimnosti zabrinjava mnoge banke zbog nepoznatosti identiteta korisnika digitalne valute. Banke često imaju dojam da se transakcije kriptovalute ne mogu pratiti, što bi moglo dovesti do nezakonitih aktivnosti i prijevara na mreži koje su se već dogodile. Cijene kriptovaluta (konkretno Bitcoina) općenito su bile promjenjive tijekom svog kratkog vijeka. Mnogo je razloga za to, uključujući veličinu tržišta, likvidnost i broj sudionika na tržištu. Banke to vide kao rizik jer povijesno gledano, cijena nije bila stabilna pa vjeruju da valuta možda neće ostati stabilno sredstvo ulaganja tijekom vremena (Scicchitano 2023; Wang i sur. 2019).

Financial Action Task Force (FATF)<sup>4</sup> bavi se problematikom vezanom uz kriptovalute duže vrijeme. U listopadu 2018. FATF je unutar međunarodno priznatih Preporuka za borbu protiv sprječavanja pranja novca, financiranja terorizma te financiranja proliferacije oružja za masovno uništenje implementirala standarde koji se odnose na virtualnu imovinu i pružatelje usluga virtualne imovine. Od tada, neke jurisdikcije su uvele propise, no globalna integracija relativno je loša, a usklađenost unutar većine financijskih sektora je zaostala (FATF 2023).

Prema podacima sa službene stranice HANFA<sup>5</sup> od 2020. godine provodi nadzorne aktivnosti provjere provođenje mjera i postupaka koji su propisani Zakonom o sprječavanju pranja novca i financiranja terorizma tim zakonom u „odnosu na osobe koje se bave djelatnošću pružanja usluga razmjene virtualnih i fiducijarnih valuta i/ili pružanja skrbničke usluge novčanika” (HANFA 2021).

Obzirom na pojačanu uporabu kryptoimovine u nezakonite i kriminalne svrhe, pojmovi vezani uz virtualne valute se djelomično reguliraju pravnim propisima RH i EU u dijelu vezanom uz sprječavanje pranja novca i financiranja terorizma. Da bi izbjegle zaostajanje, banke moraju pronaći način da prihvate ovu tehnologiju i tretiraju je kao mogućnost za napredak, a ne kao prijetnju. Usvajanje kriptovalute moglo bi pojednostaviti, poboljšati i nadograditi financijske usluge, a postoji mnogo nedavnih napredaka u industriji koji mogu ublažiti zabrinutost banaka oko rizika i umjesto toga im omogućiti da prepoznaju potencijalne koristi. S druge strane, prihvaćanjem virtualnih valuta i unaprjeđenjem tehnologije, banke bi mogle razviti sustav monitoriranja posebice u pogledu sprječavanja pranja novca i financiranja terorizma. Smjernice i propisi vezani uz digitalnu imovinu su rijetki, zbog čega mnoge financijske institucije zaziru od usvajanja istih. Zabrinutost oko sigurnosti i stabilnosti kriptovalute također sprječava banke da uđu na ova tržišta, ali umjesto da se boje rizika ove tehnologije, banke bi trebale unaprijed gledati na njezine potencijalne koristi.

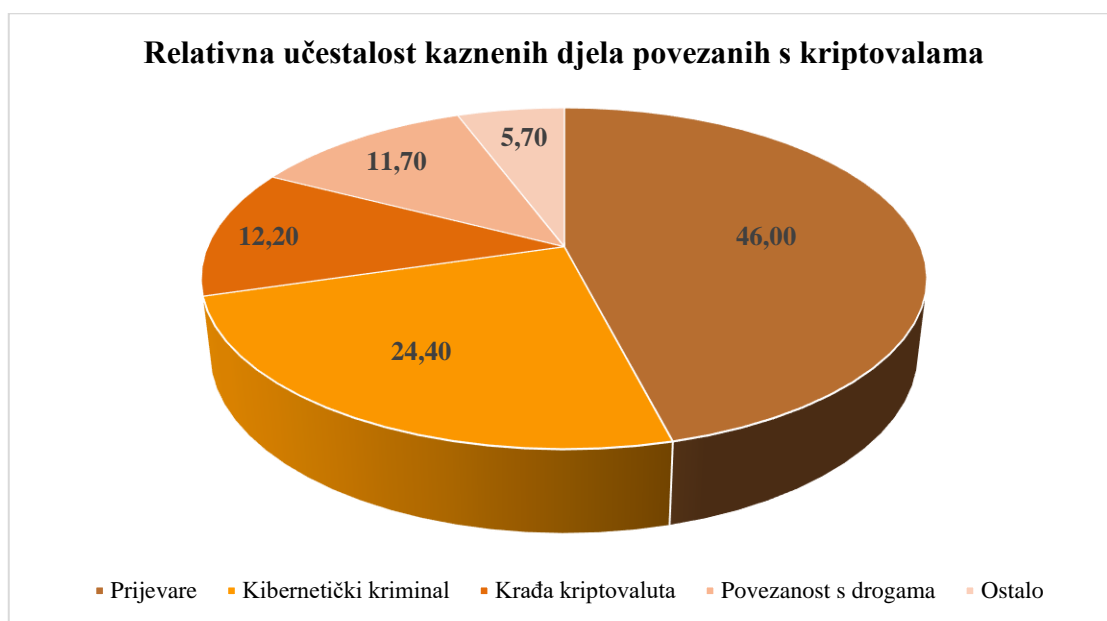
---

<sup>4</sup> FATF je „međunarodno tijelo osnovano 1989. s ciljem postavljanja standarda i promicanja učinkovite implementacije zakonskih, regulatornih i operativnih mjera za borbu protiv pranja novca, financiranja terorizma i drugih srodnih prijetnji integritetu međunarodnog financijskog sustava” (HANFA).

<sup>5</sup> Hrvatska agencija za nadzor financijskih usluga - nadzorno tijelo u čiji djelokrug i nadležnost spada nadzor financijskih tržišta, financijskih usluga te pravnih i fizičkih osoba koje te usluge pružaju (HANFA).

### 3.3. Upravljanje rizicima

Korištenje kriptovalute značajno je poraslo posljednjih godina, a očekuje se nastavak rekordnog rasta. Najčešće promatrane vrste kriminala koje uključuju kriptovalute su prijevare (46%), zatim kibernetički kriminal (24,4%), krađa kriptovaluta (12,2%) i povezanost s drogama (11,7%) (Kerr i sur. 2023).



**Grafikon 5.** Relativna učestalost kaznenih djela povezanih s kriptovalutama

Izvor: izrada autora prema Kerr i sur. 2023. Cryptocurrency Risks, Fraud Cases, and Financial Performance

Ilegalne aktivnosti u vezi s kriptovalutama javljaju se češće nego ikad, posebice prijevare i krađe u vezi s kriptovalutama, pri čemu njihovi počinitelji koriste sve inovativnije metode u svrhu prikrivanja svojih aktivnosti. Prijevare s visokim prinosima (Ponzi sheme) još su jedna tehnika koju kibernetički kriminalci koriste za krađu sredstava koja uključuju kriptovalute. Žrtvama ovih shema plaćeni su povrati na njihova ulaganja, s malim ili nikakvim povratima od stvarnih ulaganja. Primjerice, 2021. godine majka i sin iz Las Vegasa ukrali su više od 12 milijuna američkih od 277 investitora nakon što su im obećali izvanredne povrate od 20 do 30 posto godišnje od ulaganja u kriptovalute i vrijednosne papire. Međutim, vrlo malo novca došlo je od ulaganja u kriptovalute ili vrijednosne papire, umjesto toga, gotovo sva



sredstva došla su od samih ulagača što je predstavljalo klasičnu Ponzijevu shemu (Woolley i Wells 2021).

Kriminalci putem kriptovaluta pokušavaju izbjegavati načela sprječavanja pranja nova i financiranja terorizma obzirom na decentraliziranost kriptovaluta, anonimnost korisnika kao i otežano praćenje transakcija. Upravo zbog toga nastoji se integrirati regulativa kojim bi se osiguralo da se kriptovalute ne koriste za kriminalne radnje.

Sukladno posljednjim izmjenama od svibnja 2023., a u cilju prevencije od pranja novca i financiranja terorizma, pružatelji usluga kripto imovine obligatorni su sakupiti informacije o pošiljatelju i primatelju kripto imovine neovisno o samom iznosu. Na taj se način osigurava monitoriranje, identificiranje te blokiranje potencijalnih sumnjivih transakcija (Europsko vijeće i Vijeće EU-a 2023).

Osim ilegalnih radnji vezanih uz kriptovalute, za tehnologiju kriptovaluta neophodne su značajne količine električne energije. Isto pak kulminira destruktivnim učinkom na prirodu i okoliš. Smatra se da je potrošnja energije Bitcoina ekvivalentna potrošnji energije manje države (Europski parlament 2023).

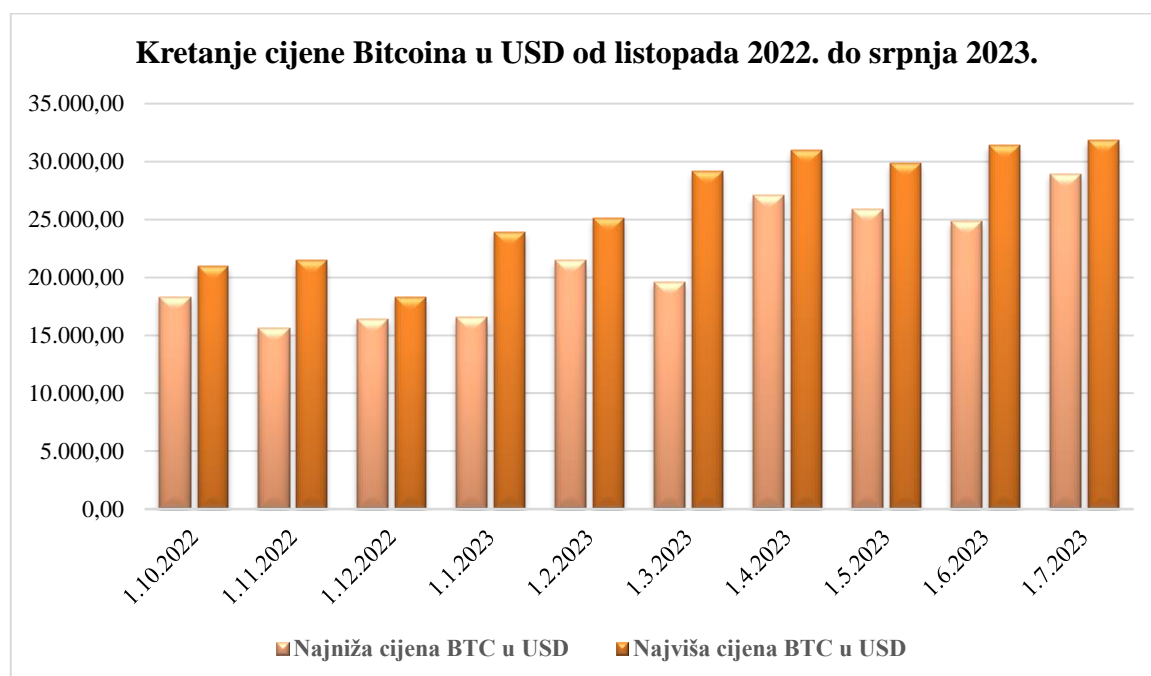
Ono što uvelike otežava proces upravljanja rizikom je neznanje. Ako postoji želja pojedinca da se bavi ulaganjem u kriptovalute, a s druge strane isti ne raspolaže adekvatnim informacijama i terminologijom, to predstavlja iznimno velik rizik u vidu gubitka kapitala ili davanja osobnih podataka putem neprovjerenih stranica koje mogu biti dalje zlouporabljene. Ono što je olakotna okolnost kod takve vrste rizika je činjenica da se isti može otkloniti edukacijom od strane stručnjaka, učenjem i usavršavanjem u ovom i dalje u potpunosti nejasnom i neistraženom svijetu.

Tržište kriptovaluta je notorno promjenjivo i nepredvidivo, a bez učinkovitih strategija upravljanja rizikom trgovci kriptovalutama mogu se brzo naći suočeni sa značajnim gubicima (Sun 2023).

U konačnici još nije razvijena sveobuhvatna strategija upravljanja rizicima ulaganja u kriptovalute, nego se većina istih svodi na preporuke središnjih banaka i stručnjaka koji ulažu u kriptovalute, a ono što je potrebno da bi se najoptimalnije upravljalo rizicima je definiranje cilja, educiranje, analiziranje, planiranje neplaniranog, procjenjivanje

potencijalnog gubitka te praćenje tržišta i konkurencije. Dakako da se rizik ulaganja ne može bazirati samo na teorijskim pretpostavkama, stoga je neophodno koristiti određene metode pomoću kojih se može procijeniti rizik ulaganja u Bitcoin.

Grafikon 6. prikazuje kako su se kretale cijene Bitcoin na prvi dan u mjesecu od listopada 2022. do srpnja 2023. Izvršena je usporedba najniže i najviše cijene iz koje se mogu utvrditi određene oscilacije. Iz niže navedenog grafikona zaključuje se kako u posljednjih 9 mjeseci cijena Bitcoina u prosjeku raste, no isto nije garancija da će se navedeni trend i dalje kretati istom uzlaznom putanjom.



**Grafikon 6.** Kretanje cijene Bitcoina od listopada 2022. do srpnja 2023.

Izvor: izrada autora prema podacima preuzetih s Yahoo Finance <https://finance.yahoo.com/quote/BTC-USD?p=BTC-USD&.tsrc=fin-srch>

Upravo zbog toga potrebno je teorijsko znanje implementirati unutar neke od metoda za procjenu rizika, a u tu svrhu u sljedećem poglavlju prikazat će se Monte Carlo simulacija.

## 4. Monte Carlo simulacija

Ljudi su uvijek težili što bolje shvatiti prošlost kako bi mogli biti što spremniji za budućnost. Uvijek se može desiti da nešto krene po zlu i da procjena ne bude valjana, no svakako se rizik koji budućnost nosi treba prihvatiti. Jasno je kako se budućnost ne može predvidjeti u potpunosti, no postoji način da se pod određenim uvjetima budućnost simulira. Naime, Monte Carlo simulacija je metoda koja na temelju povijesnih podataka uz korištenje nasumičnog odabira može dati zadovoljavajuću procjenu budućih vrijednosti. Pomoću simulacije se odgovara na pitanja koja počinju sa “što ako“, a na konkretnom primjenu Bitcoina simulirat će se gubici do kojih može doći u ekstremnim slučajevima.

## 4.1. Općenito o Monte Carlo simulaciji

Kockarske igre baziraju se na rizičnim i neizvjesnim ulaganjima te nasumičnim ishodima koji se, zbog velikog broja izvođenja, u određenim intervalima i ponavljaju. Simulacija neizvjesnosti koja se temelji na nasumičnim ishodima dobila je ime po Monte Carlu, četvrti Monaca koja je poznata po brojim kockarnicama (Sajter 2017).

Prema McLeishu (2004.) simulacija predstavlja jedan od najvažnijih alata današnjice za analiziranje stohastičkog sustava. Ista djeluje na način da imitira proces ili određeni sustav iz stvarnog svijeta. Simulacija je matematički model imitacije procesa ili sustava iz stvarnog svijeta.

Ovaj rad bazira se na kriptovaluti Bitcoin i pretpostavkama oko kretanja cijene istoga u budućnosti. Navedeno se u radu ispituje pomoću simulacije pod nazivom Monte Carlo.

„Monte Carlo simulacija skupni je naziv za metode koje nastoje aproksimirati određeni ishod nizom nasumičnih pokušaja. Kod te metode hipotetske promjene tržišnih faktora nasumično se uzimaju iz odabrane statističke distribucije“ (Sajter 2017).

Prema Sajteru (2017.), Monte Carlo simulacijom zapravo se simulira „virtualna budućnost“ na način da se generira stotine i stotine tisuća mogućih ishoda određenog procesa u vremenskom periodu.

Ova metoda predviđanja budućih vrijednosti ne predstavlja točan matematički izračun kojim se pokrivaju ulazni i izlazni parametri određenog sistema, već se unutar iste primjenjuje nasumičan odabir i statistička obrada podataka (Uroić 2011).

Monte Carlo simulacijom nastoje se utvrditi rizici, neizvjesnost kao i sam utjecaj distribucije vjerojatnosti na rezultate koji su predmet analize. Prednost koju pruža Monte Carlo simulacija odnosi se na kvalitetniju procjenu budućih vrijednosti na temelju dobivenih rezultata kojom se, primjerice investitoru, daje veća sigurnost. Također, analizirani rezultati doprinose jednostavnijoj usporedbi i klasifikaciji predviđenih ishoda te odabiru onog najoptimalnijeg (Karanović 2012).

## 4.2. Monte Carlo i VaR

Jedna od metoda za izračun rizične vrijednosti (VaR) je upravo Monte Carlo. VaR (*engl. Value-at-Risk*) mjera je kojom se na temelju povijesnih podataka iskazuje potencijalni gubitak u odabranom periodu razdoblju koji nastaje uslijed modifikacija cijena sastavnica portfelja (Šverko 2002).

Sajter (2017.) VaR iskazuje kao „iznos gubitka ako stvari krenu po zlu odnosno gubitak koji se može očekivati u određenom razdoblju uz specifičnu razinu statističke ignifikantnosti.“

Mikulčić (2001.) ističe kako je rizična vrijednost „jedinstvena, sažeta, statistička mjera mogućih portfeljnih gubitaka. Rizičnost vrijednosti izražava očekivani maksimalni gubitak (ili najgori gubitak) tijekom određenog razdoblja unutar statistički definiranog područja prihvaćanja.“

## 4.3. Monte Carlo simulacija na primjeru Bitcoina

Monte Carlo simulacijom nastoji se predvidjeti buduće ponašanje vrijednosti dionica na temelju povijesnih podataka uz korištenje nasumične i hipotetske promjene tržišnih faktora. Za potrebe izvođenja simulacije u svrhu empirijskog istraživanja unutar diplomskog rada korišteni su podaci o Bitcoinu sa stranice burzovnog indeksa S&P 500 Yahoo Finance, a analizom je obuhvaćen od rujna 2014. do rujna 2022. godine. Za adekvatnije praćenje rezultata korištene su povijesne cijene Bitcoina na tjednoj bazi.

### 4.3.1. Implementacija

Unutar Monte Carlo simulacije pretpostavljeno je da su log-povrati normalno distribuirano Matematički, pretpostavlja se da vrijedi

$$\ln \frac{S_{t+\Delta t}}{S_t} \sim N(\mu, \sigma),$$

gdje  $S_t$  predstavlja cijenu Bitcoina u trenutku  $t$ . Također  $\mu$  predstavlja prosječan povijesni prinos, a  $\sigma$  standardnu devijaciju.

Sajter (2017) navodi da su log-normalne distribucije vrijednosti su isključivo pozitivne.

Monte Carlo simulacija koristi se za promatranje vremenskog perioda, točnije više vremenskih trenutaka, no u najosnovnijem obliku dovoljno je promatrati samo jedan period unaprijed.

Radi jednostavnosti provedbe simulacije u ovom radu analiziran je portfelj koji se sastoji od 1 Bitcoina, a za promatrani period uzeti su povijesni podaci na tjednoj frekvenciji u razdoblju od rujna 2014. do rujna 2022. Na temelju istih dobiveni su parametri distribucije: prosječan povijesni prinos u promatranom periodu kojeg nazivamo drift i standardna devijacija, najčešće korištena mjera volatilnosti. Izračunati prosječni povijesni prinos u promatranom periodu iznosi 0,009 dok standardna devijacija iznosi 0,104.

Prethodno spomenuta volatilnost predstavlja sklonost promjenama cijena, a upravo su kriptovalute poznate po svojoj visokoj volatilnosti.

Inače je kod kriptovaluta uobičajeno kratkoročno trgovanje, no u sklopu ovog diplomskog rada uzet je relativno dug period od 100 tjedana u svrhu analize rizika dugoročnih investicija u Bitcoin. Jednostavnije rečeno, postavlja se pitanje “što ako“ bi netko dugoročno posjedovao Bitcoin te koji su rizici istoga.

#### 4.3.2. Analiza

Nakon postavljanja modela i određivanja pretpostavke da je prinos log normalno distribuiran, u svrhu izračuna VaR vrijednosti, odnosno potencijalnog gubitka, na razini 95% i 99% pouzdanosti, koristeći se Monte Carlo metodom, simulirana je cijena Bitcoina u vremenskom periodu od 100 tjedana.

Iz prethodno navedenog zaključuje se da VaR ima sljedeće komponente:

- a) Vremensko razdoblje (t): 100 tjedana
- b) Razina signifikantnosti ( $\alpha$ -kvantil): 95% i 99%
- c) Mogući iznos gubitka od uloženog 1 Bitcoina

- d) Povijesno razdoblje: četvrta, tehnička komponenta koja utječe na rezultate analize i na temelju koje izračunava VaR, tj. razdoblje od rujna 2014. do rujna 2022.

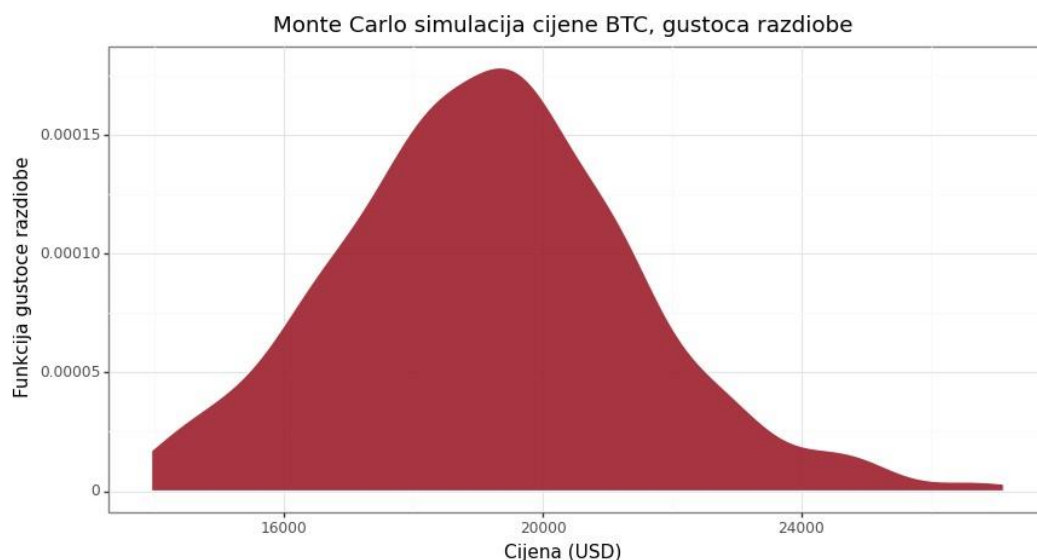
Za svaku iteraciju i svaki vremenski trenutak simulira se jedna normalna slučajna varijabla s procijenjenim parametrima, a na temelju slučajne varijable i prethodne cijene može se izračunati cijena u sljedećem trenutku. To je realizirano u programskom jeziku Python sljedećim linijama koda.

```
h = rd.normalvariate(drift1,sd1)
nova_cijena = predv_cijene[k-1]*np.exp(h)
predv_cijene.append(nova_cijena)
```

**Slika 4.** Linije koda

Izvor: izrada autora u programu Python

Iteracije predstavljaju scenarije odnosno moguće ishode, a pomoću Monte Carlo metode simuliraju se budući potencijalni scenariji tržišta te se na temelju istih radi analiza. Početna vremenska točka simulacije je cijena postignuta u zadnjoj vremenskoj točki povijesnih podataka, odnosno zadnja povijesna cijena koja iznosi 19.431,79 USD.

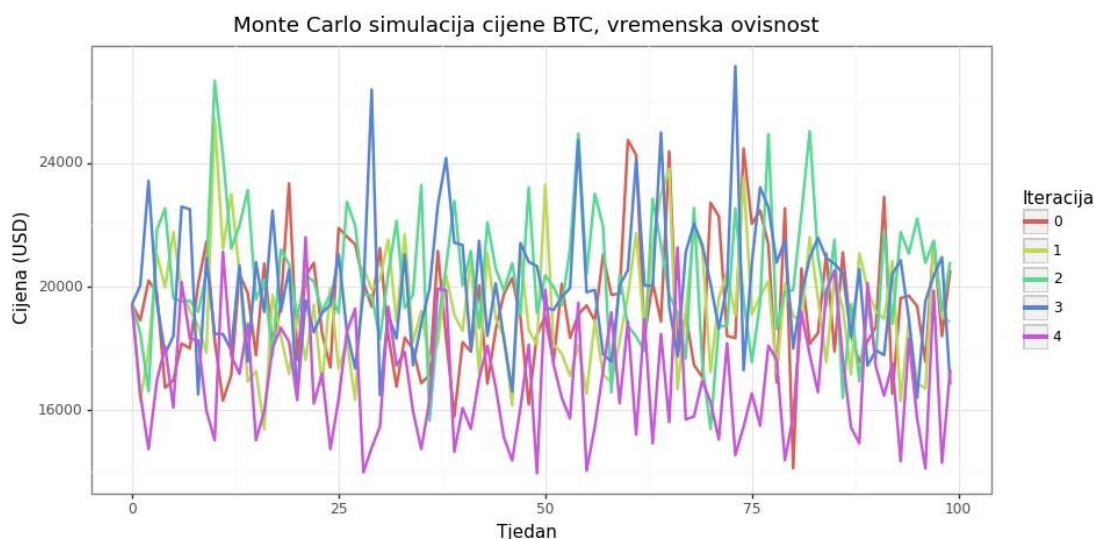


**Slika 5.** Gustoća razdiobe simuliranih cijena Bitcoina za 5 iteracija

Izvor: izrada autora u programu Python

Na slici 5. prikazana je gustoća razdiobe. Na x-osi prikazano je kretanje cijena, a na y-osi proporcija cijena u nekom intervalu, točnije gustoća vjerojatnosti. Kako bi simulacija prikazala što bolje rezultate, neophodno je da se gledaju izrazito mali intervali u neprekidnom slučaju.

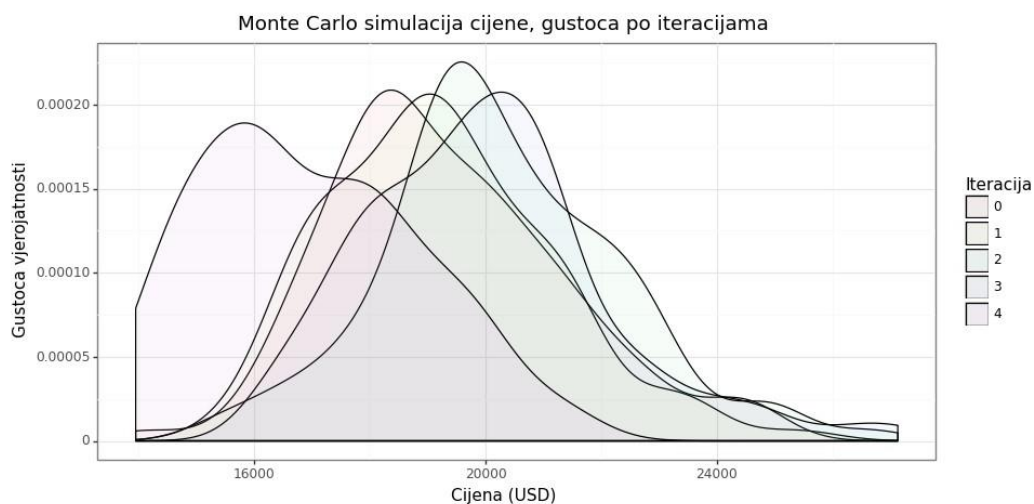
Iz oblika funkcije zaključuje se da je bilo relativno najviša cijena Bitcoina u simuliranim podacima predočena oko područja na krivulji gdje je najviša točka. Grafički prikaz nalaže da bi cijena mogla biti oko 19.000 USD, no obzirom na raspršenost, mogući su i drugi ishodi. Isto tako, raspršenost na x-osi poistovjećuje se s volatilnošću jer je masa vjerojatnosti raspoređena šire po mogućim vrijednostima cijene Bitcoina pa se u tom pogledu zaključuje da je cijena Bitcoina volatilnija.



**Slika 6.** Kretanje simuliranih cijena Bitcoina za 5 iteracija  
Izvor: izrada autora u programu Python

U svrhu inicijalne vizualizacije, na slici 6. prikazano je 5 iteracija simulacije cijene Bitcoina koje su predočene kroz vremenski period od 100 tjedana. Na x-osi je vrijeme, a na y-osi cijena u USD, a svaka linija iteracije određena je sa 100 podataka. Promatrajući prikaz može se utvrditi kako cijena Bitcoina nema dugoročni trend da drastično raste ili pada, već titra oko istih vrijednosti, a volatilnost se poistovjećuje s cijenama na y-osi obzirom da ista oscilira kroz vrijeme.

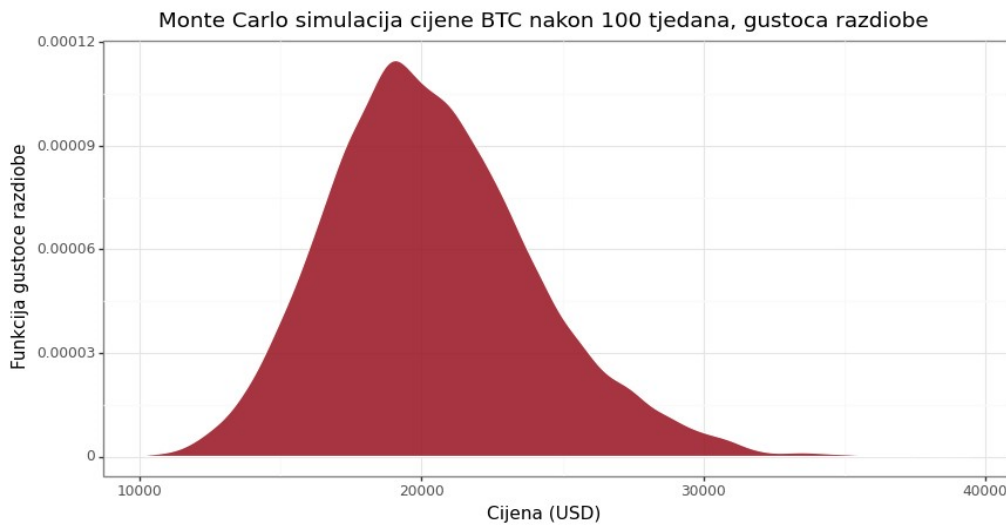




**Slika 7.** Gustoća po iteracijama  
Izvor: izrada autora u programu Python

U odnosu na sliku 5. na kojoj su prikazani svi podaci zajedno kroz 100 tjedana u 5 iteracija koje smo simulirali, slika 7. prikazuje svaku simulaciju odvojeno. Na ovaj način, kroz razgraničenje svake iteracije, može se optimalnije prikazati stabilnost iteracija. Idealno bi bilo da su sve iteracije slične gustoće, no na temelju prikaza se zaključuje kako 4 iteracije definiraju sličnu razdiobu gustoće što je poželjno dok lijeva linija prikazuje odstupanje. Navedeno odstupanje je za očekivati obzirom da je i sama Monte Carlo simulacija bazirana na slučajnosti te je normalno da se ponekad dogode i određena odstupanja. Opisano odstupanje može se poistovjetiti s pojmom crnih labudova – nezamislivi događaji će se dogoditi, ali uzimajući prosjek i zanemarivu učestalost u odnosu na ostale scenarije, neće puno mijenjati krajnji rezultat. Iako je na repovima<sup>6</sup> distribucije mala vjerojatnost od pojave crnih labudova, na financijskim tržištima vjerojatnost ekstremnih događaja ipak nije tako zanemariva koliko implicira pretpostavka distribucije pa je neophodno simulirati što veći broj scenarija kako bi se pokazala učestalost pojave anomalija. Nakon prikazanih gustoća razdioba, simulacija je pokrenuta 10.000 puta na istom modelu kako bi se procijenio interval pouzdanosti modela te kako bi se suzbio utjecaj nasumične varijacije na dobivene cijene.

<sup>6</sup> Repovi distribucije su krajevi distribucije s lijeve i desne strane te su prilično udaljeni od aritmetičke sredine. Isti su veoma važni kod upravljanja rizicima jer su upravo u repovima smješteni rizici koji imaju malu vjerojatnost nastanka (Sajter, 2017).



**Slika 8.** Kretanje simuliranih cijena Bitcoina za 10.000 iteracija  
Izvor: izrada autora u programu Python

Uspoređujući sliku 8. sa slikom 5. može se uvidjeti kako su konceptualno veoma slične. Slika 5. dobivena je simuliranjem 5 iteracija u periodu 100 tjedana (ukupno 500 podataka), a na slici 7. prikazana je simulacija s 10.000 iteracija na 100 tjedana (ukupno 1.000.000 podataka) kako bi se određene anomalije imale što manji utjecaj na krajnji rezultat. Za bolju procjenu stvarnosti i eventualnih ekstremnih događaja, bolji će se zaključak generirati na temelju simuliranja više scenarija. Iz tog razloga slika 8. donosi adekvatniji prikaz obzirom da je korišteno više iteracija.

Nakon simuliranja 10.000 scenarija u vremenskom okviru promatranja 100 tjedana unaprijed, za izračun vrijednosti prikazanih u tablici 1., promatran je 100. tjedan simulacije, a računata srednja zadnja cijena, 95%-tni i 99%-tni interval pouzdanosti u zadnjem trenutku simulacije i VaR na razini pouzdanosti 95% i 99%.

**Tablica 1.** Izračunate vrijednosti za 10.000 iteracija simulacije nakon 100 tjedana

Izračunate vrijednosti	
Srednja zadnja cijena nakon 100 tjedana	20.395,09
95% CI za simuliranu zadnju cijenu	[13.123,15, 27.667,03]
99% CI za simuliranu zadnju cijenu	[10.822,84, 29.967,33]
VaR na razini pouzdanosti od 95%	-32,47%
VaR na razini pouzdanosti od 99%	-44,30%

Izvor: izrada autora pomoću izračuna u programu Python prema podacima preuzetih s Yahoo Finance  
<https://finance.yahoo.com/quote/BTC-USD?p=BTC-USD&.tsrc=fin-srch>

Zaključuje se da srednja zadnja cijena nakon 100 tjedana iznosi 20.395,09 USD što je u odnosu na zadnju povijesnu cijenu povećanje od 4,96%. Nadalje, konstatira se da će, s vjerojatnošću od 95%, cijena Bitcoina za 100 tjedana od promatranog perioda, biti između 13.123,15 USD i 27.667,03 USD. Također, uzimajući vjerojatnost od 99%, predviđena cijena Bitcoina za 100 tjedana od promatranog perioda biti će između 10.822,84 USD i 29.967,33 USD.

Promatrajući cijene u zadnjem trenutku, može se izračunati i VaR na način da u izračun ulazi samo zadnji trenutak simulacije, odnosno samo 100. tjedan. Uz razinu pouzdanosti od 95% dobiven je VaR od -32,47%. Kako VaR predstavlja potencijalni gubitak, sukladno dobivenom izračunu, zaključilo se da gubitak u portfelju koji sadrži 1 Bitcoin nakon 100 tjedana uz razinu pouzdanosti 95% neće biti veći od 32,47%, odnosno postoji 5%-tna vjerojatnost da se ulaganjem u Bitcoin nakon 100 tjedana može izgubiti više od 32,47% uloženog. Istodobno, uz razinu pouzdanosti od 99% može se utvrditi da gubitak u portfelju koji sadrži 1 Bitcoin neće biti veći od 44,30% nakon 100 tjedana, odnosno postoji 1% vjerojatnosti da se ulaganjem u Bitcoin nakon 100 tjedana može izgubiti više od 44,30% uloženog.

Na temelju simulacije zaključeno je kako se povećanjem simuliranih iteracija povećava i preciznost rezultata, no navedeno se nikada ne može u potpunosti potvrditi obzirom na prisutnost neizvjesnosti i rizika od potencijalnog gubitka.

U konačnici bilo da se radi o investitoru kojeg zanima procjena rizika ulaganja u određenu dionicu ili menadžeru koji nastoji riješiti određene poslovne odluke na način da adekvatno utvrdi mogućnost negativnog ishoda, Monte Carlo se ističe kao jedna od najtemeljitijih metoda za procjenu utjecaja rizika i neizvjesnosti na kapitalna ulaganja (Karanović 2012).

## Zaključak

Bitcoin, prvu i najpoznatiju kriptovalutu, 2008. godine stvorila je anonimna osoba ili grupa pod pseudonimom Satoshi Nakamoto. Princip Bitcoina opisan je u dokumentu pod nazivom "Bitcoin: Peer-to-Peer sustav elektroničke gotovine". U siječnju 2009. godine, Nakamoto je rudario prvi blok Bitcoin mreže, poznat kao *Genesis Block*. Nakon toga Bitcoin je uveden kao alternativa tradicionalnim centraliziranim financijskim sustavima i imao je za cilj omogućiti sigurne, decentralizirane peer-to-peer transakcije. Jedna od njegovih primarnih inovacija bila je upotreba blockchain tehnologije, transparentne i nepromjenjive javne knjige koja bilježi sve Bitcoin transakcije.

U ranim godinama Bitcoin se suočavao sa skepticizmom, ali je postupno stekao popularnost među korisnicima. Tijekom vremena, Bitcoin je doživio nekoliko značajnih fluktuacija cijena na kriptovalutnom tržištu i tržišnih ciklusa. Njegova cijena je zabilježila dramatična povećanja i oštre padove. Iako se u početku povezivao s nedopuštenim aktivnostima i spekulacijama, Bitcoin je stekao kredibilitet i usvajanje od šire mase obzirom da su uglednije financijske institucije i investitori krenule ulagati u kriptovalutno tržište. Temeljna tehnologija Bitcoina, blockchain, također je utjecala na razvoj drugih kriptovaluta i prepoznata je po svojim potencijalnim primjenama izvan financija, kao što su upravljanje opskrbnim lancem i sustavi glasovanja. Danas je Bitcoin i dalje najpriznatija i najvrjednija kriptovaluta, a sve veći broj pojedinaca i tvrtki koristi je u različite svrhe, uključujući ulaganja, e-trgovinu, pohranu vrijednosti i slično. Njegova decentralizirana i transparentna priroda nastavlja privlačiti i entuzijaste i kritičare, čineći ga stalnim predmetom interesa i rasprava.

Iako ga mnogi i dalje kriptovalute smatraju jedim od načina za pranje novca i financiranja kriminalnih radnji, potrebno je osvrnuti se i na prednosti koje kriptovalute nude. Dakako za što transparentnije poslovanje s ciljem prevencije od pranja novca i financiranja terorizma, prvenstveno je potrebno kriptovalute pravno utvrditi, regulirati i uskladiti s poslovanjem financijskih institucija.

Ono što najviše zanima potencijalne investitore u Bitcoin je rizičnost ulaganja. Nedvojbeno je da je povrat ulaganja nepredvidljiv, stoga je nužno generirati što više mogućih scenarija kako bi se utvrdila isplativost ulaganja i barem djelomično predvidjeli nepoželjni ishodi. Monte Carlo simulacijom ne može se sa 100%-tnom sigurnošću predvidjeti cijena Bitcoina u budućnosti, no pomoću iste može se procijeniti potencijalni gubitak ukoliko nešto krene po zlu. Simuliranjem budućih scenarija pada ili rasta cijene Bitcoina nastoji se procijeniti rizičnost odnosno sigurnost ulaganja u samu kriptovalutu što će zasigurno pomoći olakšati odluku investitorima o eventualnom ulaganju.

## Bibliografija

Knjige:

- Ammous S. (2020). Bitcoin standard – Decentralizirana alternativa središnjem bankarstvu. Zagreb, Mate
- Knight, F. (1921). Risk, Uncertainty and Profit. Boston and New York: The Riverside Press Cambridge.
- Haeringer G., Halaburda, H. i Sarvary, M., (2021). Beyond Bitcoin: The Economics of Digital Currencies and Blockchain Technologies Guillaume. Palgrave Macmillan
- McLeish, D.L. (2004). Monte Carlo simulation and finance. Wiley Finance
- Narayanan A., Bonneau J., Felten E., Miller A. i Goldfeder S. (2016). Bitcoin i tehnologije kriptovaluta: sveobuhvatan uvod. Princeton University Press, Princeton.
- Orsag, S. (2011). Vrijednosni papiri, investicije i instrumenti financiranja. Sarajevo: Revicon.
- Perkušić M. (2020). Pravo elektroničkog plaćanja. Školska knjiga 275-341
- Sajter, D. (2017). Osnove upravljanja rizicima u financijskim institucijama. Ekonomski fakultet u Osijeku

Ostala građa:

- Arnerić, J. i Mateljan, M. (2019). Analiza međuovisnosti tržišta kapitala i tržišta kriptovaluta. Ekonomska misao i praksa, 28 (2), 449-465. Preuzeto s <https://hrcak.srce.hr/230521> (pristupljeno 04. kolovoza 2023.)
- Arslanian, H., Robert Donovan, R., Blumenfeld, M., i Zamore, A. (2021). El Salvador's law: a meaningful test for Bitcoin. PWC (pristupljeno 07. rujna 2023.)

- Bank for International Settlements (2023). The crypto ecosystem: key elements and risks. ISBN 978-92-9259-670-5. Preuzeto s <https://www.bis.org/publ/othp72.htm> (pristupljeno 02. kolovoza 2023.)
- Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H.P. i Böhme, R. (2012). Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. Workshop on the Economics of Information Security, Berlin, Germany. Preuzeto s <https://ssrn.com/abstract=2041492> (pristupljeno 21. srpnja 2023.)
- Bhattacharya, S. (2021). USD Coin: Everything You Should Know about the Second-Largest Stablecoin. Analytics Insight. Preuzeto s <https://www.analyticsinsight.net/usd-coin-everything-you-should-know-about-the-second-largest-stablecoin/> (pristupljeno 21. srpnja 2023.)
- Bitinfocharts. Cryptocurrency statistics. Preuzeto s <https://bitinfocharts.com/> (pristupljeno 21. srpnja 2023.)
- Bradbury D. (2013). The problem with Bitcoin. Computer Fraud & Security, Journal of Financial Risk Management. 2013(11), 5-8. Preuzeto s [https://doi.org/10.1016/S1361-3723\(13\)70101-5](https://doi.org/10.1016/S1361-3723(13)70101-5) (pristupljeno 19. srpnja 2023.)
- Carrick, J. (2016). Bitcoin as a Complement to Emerging Market Currencies. Emerging Markets Finance and Trade, 52(10), 2321-2334. Preuzeto s <https://doi.org/10.1080/1540496X.2016.1193002> (pristupljeno 19. srpnja 2023.)
- Casey, M. J. (2014). Dollar-Backed Digital Currency Aim's to Fix Bitcoin's Volatility Dilemma. The Wall Street Journal. Preuzeto s <https://www.wsj.com/articles/BL-MBB-23780> (pristupljeno 18. srpnja 2023.)
- Chan, S., Chu, J., Zhang, Y. i Nadarajah, S. (2022). An extreme value analysis of the tail relationships between returns and volumes for high frequency cryptocurrencies. Research in International Business and Finance, 59. Preuzeto s <https://doi.org/10.1016/j.ribaf.2021.101541> (pristupljeno 30. lipnja 2023.)
- Chaum, D. (1983). Blind Signatures for Untraceable Payments. Zbornik: Advances in Cryptology. Springer. Preuzeto s [https://doi.org/10.1007/978-1-4757-0602-4\\_18](https://doi.org/10.1007/978-1-4757-0602-4_18) (pristupljeno 29. lipnja 2023.)

- Cocco, L., Pinna, A. i Marchesi, M. (2017). Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. *Future Internet*, 9(3), 1-20. Preuzeto s <https://doi.org/10.3390/fi9030025> (pristupljeno 19. srpnja 2023.)
- CoinMarketCap. Preuzeto s <https://coinmarketcap.com/rankings/exchanges/> (pristupljeno 09. rujna 2023.)
- Conlon, T. i McGee, R. (2020). Safe haven or risky hazard? Bitcoin during the COVID-19 bear market. *Finance Research Letters*, 35. Preuzeto s <https://doi.org/10.1016/j.frl.2020.101607> (pristupljeno 22. srpnja 2023.)
- Davidson, J. (2022). Using Binance in the United States (Complete 2022 Guide). *Wallet Whys*. Preuzeto s <https://www.walletwhys.com/using-binance-in-the-united-states/> (pristupljeno 20. srpnja 2023.)
- Dionísio, A., Menezes, R. i Mendes, D. (2006). An econophysics approach to analyse uncertainty in financial markets: An application to the Portuguese stock market. *European Physical Journal B*, 50, 161–64. Preuzeto s <https://doi.org/10.1140/epjb/e2006-00113-2> (pristupljeno 22. srpnja 2023.)
- Duggan, W. (2023). How Does The SEC Regulate Crypto? *Forbes Advisor*. Preuzeto s <https://www.forbes.com/advisor/investing/cryptocurrency/sec-crypto-regulation/#:~:text=If%20crypto%20is%20deemed%20a,if%20cryptocurrencies%20are%20deemed%20currencies> (pristupljeno 22. srpnja 2023.)
- Edwards, J. (2023). Bitcoin's Price History. Preuzeto s <https://www.investopedia.com/articles/forex/121815/Bitcoins-price-history.asp> (pristupljeno 19. srpnja 2023.)
- European Central Bank. 2012. Virtual currency schemes. ISBN: 978-92-899-0862-7. Preuzeto s <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> (pristupljeno 21. srpnja 2023.)
- Europski parlament. (2023). Kriptovalute: koji su rizici i kako EU zakonodavstvo može pomoći? preuzeto s <https://www.europarl.europa.eu/news/hr/headlines/economy/20220324STO26154/kriptovalute-koji-su-rizici-i-kako-eu-zakonodavstvo-moze-pomoci> (pristupljeno 27. lipnja 2023.)



- Europsko vijeće i Vijeće EU-a (2023). Sprečavanje pranja novca: Vijeće donijelo pravila kojima će se omogućiti sljedivost prijenosa kriptoinovine. Preuzeto s <https://www.consilium.europa.eu/hr/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/> (pristupljeno 15. srpnja 2023.)
- Fang, F., Ventre, C., Basios, M. i sur. (2022). Cryptocurrency trading: a comprehensive survey. *Financial Innovation* 8, 13. Preuzeto s <https://doi.org/10.1186/s40854-021-00321-6> (pristupljeno 05. srpnja 2023.)
- Horvatić, H. i Tafra, V. (2022). Identifikacija komercijalne blockchain tehnologije te izazovi i opasnosti primjene kroz konkretne primjere. *Obrazovanje za poduzetništvo - E4E*, 12 (2), 105-120. Preuzeto s <https://doi.org/10.38190/ope.12.2.7> (pristupljeno 12. srpnja 2023.)
- Hrvatska agencija za nadzor financijskih usluga - HANFA (2021). Kriptotržište. Preuzeto s <https://www.hanfa.hr/media/6631/kriptotr%C5%BEi%C5%A1te-12-2021.pdf> (pristupljeno 08. kolovoza 2023.)
- Hrvatska agencija za nadzor financijskih usluga – HANFA (2021). Kriptotržišta: kakva je zaštita potrošača? Preuzeto s <https://www.hanfa.hr/vijesti/kriptotr%C5%BEi%C5%A1ta-kakva-je-za%C5%A1tita-potro%C5%A1a%C4%8Da/> (pristupljeno 19. srpnja 2023.)
- Ječmínek, J.,Kukalová, G. & Moravec. L. (2020). Volatility Modelling and VaR: The Case of Bitcoin, Ether and Ripple. *DANUBE*, 11(3), 253-269. Preuzeto s <https://doi.org/10.2478/danb-2020-0015> (pristupljeno 08. kolovoza 2023.)
- Karanović G. i Gjosevska B. (2012). Analysis of Risk and Uncertainty Using Monte Carlo Simulation and its Influence on Project Realization. *Annals - Economic and Administrative Series, Faculty of Business and Administration, University of Bucharest*, 6(1), 145-162. Preuzeto s [https://www.researchgate.net/publication/233844760\\_Analysis\\_of\\_Risk\\_and\\_Uncertainty\\_Using\\_Monte\\_Carlo\\_Simulation\\_and\\_its\\_Influence\\_on\\_Project\\_Realization](https://www.researchgate.net/publication/233844760_Analysis_of_Risk_and_Uncertainty_Using_Monte_Carlo_Simulation_and_its_Influence_on_Project_Realization) (pristupljeno 10. kolovoza 2023.)
- Kerr, D.S., Loveland, K.A., Smith, K.T. i Smith, L.M. (2023). Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks*. 11(3), 51. Preuzeto s

[https://www.researchgate.net/publication/368803393\\_Cryptocurrency\\_Risks\\_Fraud\\_Cases\\_and\\_Financial\\_Performance](https://www.researchgate.net/publication/368803393_Cryptocurrency_Risks_Fraud_Cases_and_Financial_Performance) (pristupljeno 19. srpnja 2023.)

- Leising, M. (2017). The Ether Thief. Bloomberg, Preuzeto s <https://www.bloomberg.com/features/2017-the-ether-thief/> (pristupljeno 18. srpnja 2023.)
- Liu, X., Zhao, M., Li, S., Zhang, F. i Trappe, W. (2017). A Security Framework for the Internet of Things in the Future Internet Architecture. Future Internet, 9(3), 27. Preuzeto s <https://doi.org/10.3390/fi9030027> (pristupljeno 15. srpnja 2023.)
- Luther, W.J. i White, L.H. (2014). Can Bitcoin become a major currency? SSRN Electronic Journal 36, 78-79. Preuzeto s <https://doi.org/10.2139/ssrn.2446604> (pristupljeno 22. srpnja 2023.)
- Marr, B. (2017). A Short History Of Bitcoin And Crypto Currency Everyone Should Read. Preuzeto s <https://bernardmarr.com/a-short-history-of-Bitcoin-and-crypto-currency-everyone-should-read/> (pristupljeno 22. srpnja 2023.)
- Maurer, B., Nelms, T.C. i Swartz, L. (2013). When perhaps the real problem is money itself! the practical materiality of Bitcoin. Social Semiotics, 23(2), 261–277. Preuzeto s <http://dx.doi.org/10.1080/10350330.2013.777594> (pristupljeno 19. srpnja 2023.)
- Mijatović, N. (2022). Pravna (ne)uređenost kriptovaluta i njihov utjecaj na industriju osiguranja. Hrvatski časopis za OSIGURANJE, (6), 93-106. Preuzeto s <https://hrcak.srce.hr/280262> (pristupljeno 10. srpnja 2023.)
- Mikulčić, D. (2001). Hrvatska narodna banka. Value at Risk (Rizičnost vrijednosti) Teorija i primjena na međunarodni portfelj instrumenata s fiksnim prihodom. ISSN 1332-2168. Preuzeto s <https://www.hnb.hr/documents/20182/121891/p-007.pdf/b51d2a34-82ad-4fcb-a7c1-1a480f980f4a> (pristupljeno 19. srpnja 2023.)
- Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Preuzeto s <https://bitcoin.org/bitcoin.pdf> (pristupljeno 19. srpnja 2023.)
- Office of the Comptroller of the Currency (OCC). Preuzeto s <https://www.occ.gov/about/who-we-are/index-who-we-are.html> (pristupljeno 19. srpnja 2023.)

- Ögel, S. i Ögel, İ.Y. (2021). The Interaction Between Perceived Risk, Attitude, and Intention to Use: An Empirical Study on Bitcoin as a Crypto Currency. Özen, E., Grima, S. i Gonzi, R.D. (Ed.) New Challenges for Future Sustainability and Wellbeing (Emerald Studies in Finance, Insurance, and Risk Management), Emerald Publishing Limited, 211-241. Preuzeto s <https://doi.org/10.1108/978-1-80043-968-920211012> (pristupljeno 19. srpnja 2023.)
- Peck, M.E. (2017). Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectrum 54(10), 38–60. Preuzeto s <https://ieeexplore.ieee.org/document/8048838> (pristupljeno 13. lipnja 2023.)
- Ponciano, J. (2021). More Than \$600 Million Stolen In Ethereum And Other Cryptocurrencies-Marking One Of Crypto’s Biggest Hacks Ever. Forbes. Preuzeto s <https://www.forbes.com/sites/jonathanponciano/2021/08/10/more-than-600-million-stolen-in-ethereum-and-other-cryptocurrencies-marking-one-of-cryptos-biggest-hacks-ever/?sh=3ed172447f62> (pristupljeno 27. srpnja 2023.)
- Psaila, S. (2018). Cryptocurrency Security Standard (CCSS). Deloitte Malta article. Preuzeto s [https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/technology/dt\\_mt\\_article\\_Cryptocurrency\\_Security\\_Standard-sandro-psaila.pdf](https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/technology/dt_mt_article_Cryptocurrency_Security_Standard-sandro-psaila.pdf) (pristupljeno 10. kolovoza 2023.)
- RRIF. (2018). Porezni tretman kapitalnih dobitaka po osnovi trgovanja kriptovalutama. Preuzeto s [https://www.rrif.hr/porezni\\_tretman\\_kapitalnih\\_dobitaka\\_po\\_osnovi\\_trgo-3543-misljenje/](https://www.rrif.hr/porezni_tretman_kapitalnih_dobitaka_po_osnovi_trgo-3543-misljenje/) (pristupljeno 21. srpnja 2023.).
- Ryan, J. i Stein Smith, S. (2021). History of Blockchain. Baker, H.K., Nikbakht, E. i Smith, S.S. (Ed.). The Emerald Handbook of Blockchain for Business, Emerald Publishing Limited, Bingley, 15-29. Preuzeto s <https://doi.org/10.1108/978-1-83982-198-120211004> (pristupljeno 21. srpnja 2023.)
- Schroeder, S. (2017). \$31 Million Worth of Tether Stolen in Latest Crypto Heist. Mashable. Preuzeto s <https://mashable.com/article/tether-crypto-heist> (pristupljeno 19. srpnja 2023.)

- Scicchitano, M. (2020). How Cryptocurrencies May Impact the Banking Industry. Wolf & Company, P.C. Preuzeto s <https://www.wolfandco.com/resources/insights/how-cryptocurrencies-may-impact-the-banking-industry/> (pristupljeno 21. srpnja 2023.)
- Sharma, Rashmi, (2022). The new digital era: Emerging risks and opportunities. Grima, S., Özen, E. and Boz, H. (Ed.) The New Digital Era: Digitalisation, Emerging Risks and Opportunities (Contemporary Studies in Economic and Financial Analysis, 109A), Emerald Publishing Limited, Bingley, 151-167. Preuzeto s <https://doi.org/10.1108/S1569-37592022000109A010> (pristupljeno 19. srpnja 2023.)
- Smales, L.A. (2019). Bitcoin as a safe haven: Is it even worth considering? Finance Research Letters, 30, 385–393. Preuzeto s <https://doi.org/10.1016/j.frl.2018.11.002> (pristupljeno 13. lipnja 2023.)
- Stilgherrian, B. (2016). Let's quit the blockchain magic talk. Preuzeto s <https://www.zdnet.com/article/lets-quit-the-blockchain-magic-talk/> (pristupljeno 21. srpnja 2023.)
- Sun, M. (2023). Risk Management at Crypto Firms Is in Focus Following FTX Collapse. Preuzeto s <https://www.wsj.com/articles/risk-management-at-crypto-firms-is-in-focus-following-ftx-collapse-11672966099> (pristupljeno 19. srpnja 2023.)
- Šverko, I. (2002). Rizična vrijednost (Value at risk) kao metoda upravljanja rizicima u financijskim institucijama. Ekonomski pregled, 53 (7-8), 640-657. Preuzeto s <https://hrcak.srce.hr/28367> (pristupljeno 21. srpnja 2023.)
- The Financial Action Task Force - FATF (2023). Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF. Preuzeto s <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf> (pristupljeno 10. kolovoza 2023.)
- Tretina, K. (2022). 10 Best Cryptocurrencies of August 2022. Forbes Advisor. Preuzeto s <https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/> (pristupljeno 21. srpnja 2023.)

- Turudić, D. A., Milić, J. i Štulina, K. (2017). Korištenje kriptovaluta u međunarodnom poslovanju. Zbornik sveučilišta Libertas, 1-2 (1-2), 191-210. Preuzeto s <https://hrcak.srce.hr/191294> (pristupljeno 01. kolovoza 2023.)
- U.S. Securities and Exchange Commission (SEC). Preuzeto s <https://www.sec.gov/> (pristupljeno 13. srpnja 2023.)
- Uroić, M. (2011). Uvod u Monte Carlo metodu. Matematičko fizički list, 62 (246), 87-92. Preuzeto s <https://hrcak.srce.hr/243941> (pristupljeno 01. kolovoza 2023.)
- Vondraček, D. (2021). Kriptovalute – kako iz neopipljivog poslovanja utvrditi poreznu obvezu? Preuzeto s <http://www.ekonost.hr/naslovnica/kriptovalute-kako-iz-neopipljivog-poslovanja-utvrditi-poreznu-obvezu/> (pristupljeno 21. srpnja 2023.)
- Wang, G.J., Xie, C., Wen, D. i Zhao, L. (2019). When Bitcoin meets economic policy uncertainty (EPU): Measuring risk spillover effect from EPU to Bitcoin. Finance Research Letters, 31. Preuzeto s <https://doi.org/10.1016/j.frl.2018.12.028> (pristupljeno 20. srpnja 2023.)
- Woolley, S. i Charlie, W. (2021). Vegas Mother-Son Duo Swindled Investors in Crypto Scam. SEC Says. Financial Advisor. Preuzeto s <https://www.famag.com/news/vegas-mother-son-duo-swindled-investors-in-crypto-scam--sec-says-63200.html> (pristupljeno 20. srpnja 2023.)
- Yahoo Finance. Preuzeto s <https://finance.yahoo.com/quote/BTC-USD?p=BTC-USD&.tsrc=fin-srch> (pristupljeno 04.08.2023.)
- Zapotochnyi, A. (2022). What are Smart Contracts? Blockgeeks. Preuzeto s <https://blockgeeks.com/guides/smart-contracts/> (pristupljeno 18. srpnja 2023.)
- Zebec, S. (2018). Bitcoin - pravna regulacija u Europskoj uniji i domaćem zakonodavstvu. Zbornik radova Međimurskog veleučilišta u Čakovcu, 9 (1), 93-97. Preuzeto s <https://hrcak.srce.hr/202082> (pristupljeno 22. srpnja 2023.)

## Popis ilustracija

### Tablice

Tablica 1. Izračunate vrijednosti za 10.000 iteracija simulacije nakon 100 tjedana .....	43
--	----

### Grafikoni

Grafikon 1. Podjela virtualnih valuta .....	4
Grafikon 2. Razlika između kriptotržišta i tradicionalnih financijskih tržišta .....	8
Grafikon 3. Načini stjecanja Bitcoina .....	18
Grafikon 4. SWOT analiza kriptovalute Bitcoin .....	25
Grafikon 5. Relativna učestalost kaznenih djela povezanih s kriptovalutama .....	33
Grafikon 6. Kretanje cijene Bitcoina od listopada 2022. do srpnja 2023. ....	35

### Slike

Slika 1. Najprometnije mjenjačnice na tržištu kriptovaluta .....	9
Slika 2. Povijest promijene cijene Bitcoina od 2016. do 2023. godine .....	16
Slika 3. Proces plaćanja Bitcoinom .....	21
Slika 4. Linije koda .....	40
Slika 5. Gustoća razdiobe simuliranih cijena Bitcoina za 5 iteracija .....	40
Slika 6. Kretanje simuliranih cijena Bitcoina za 5 iteracija .....	41
Slika 7. Gustoća po iteracijama .....	42
Slika 8. Kretanje simuliranih cijena Bitcoina za 10.000 iteracija .....	43

