Značaj mobilnog poslovanja u svrhu trgovanja kriptovalutama

Grgić, Ivan

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:068588

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ivan Grgić

ZNAČAJ MOBILNOG POSLOVANJA U SVRHU TRGOVANJA KRIPTOVALUTAMA

DIPLOMSKI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 6. srpnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sustavi elektroničkog poslovanja**

DIPLOMSKI ZADATAK br. 6566

Pristupnik: **Ivan Grgić (0135238159)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Značaj mobilnog poslovanja u svrhu trgovanja kriptovalutama**

Opis zadatka:

U diplomskom radu potrebno je prikazati arhitekturu i tehnologije mobilnog poslovanja te pružiti pregled razvoja i principe rada kriptovaluta. Uz navedeno potrebno je analizirati sigurnosne aspekte mobilnog poslovanja prilikom trgovanja kriptovalutama. Ove aktivnosti predstavljaju podlogu za ostvarenje cilja diplomskog rada u okviru kojega je potrebno analizirati upotrebu mobilnih uređaja i mobilnog poslovanja prilikom rudarenja i trgovanja kriptovalutama.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

ZNAČAJ MOBILNOG POSLOVANJA U SVRHU TRGOVANJA KRIPTOVALUTAMA

THE IMPORTANCE OF MOBILE BUSINESS FOR THE PURPOSE OF CRYPTOCURRENCY TRADING

Mentor : dr.sc. Ivan Cvitić

Student: Ivan Grgić

JMBAG: 0135238159

Zagreb, veljača 2022.

ZNAČAJ MOBILNOG POSLOVANJA U SVRHU TRGOVANJA KRIPTOVALUTAMA

SAŽETAK

Tema ovog rada je „Značaj mobilnog poslovanja u svrhu trgovanja kriptovaluta“. U prvom djelu rada govorimo o arhitekturi i tehnologiji mobilnog poslovanja, zatim se u nastavku baziramo na kriptovalutama, njihovoj ulozi te mogućnostima koje nude mobilni uređaji u svrhu rada s kriptovalutama. U većinskom dijelu rada fokusiramo se na Bitcoinu, jer je najveća i ujedno najlakša kriptovaluta. U radu su obrađene kriptovalute od nastanka te se spominje vrijednost kriptovaluta. Na kraju je obrađen način prikupljanja, čuvanja te trgovanja kriptovalutama putem mobilnog uređaja na temelju čega je i donesen zaključak.

Ključne riječi: bitcoin, kriptovalute, mobilno poslovanje, rudarenje, blockchain

SUMMARY

The topic of this paper is "The importance of mobile business for the purpose of cryptocurrency trading". In the first part of the paper we talk about the architecture and technology of mobile business, then we are based on cryptocurrencies, their role and the opportunities offered by mobile devices for the purpose of working with cryptocurrencies. For the most part, we are based on Bitcoin, because it is the largest and easiest cryptocurrency. The paper deals with cryptocurrencies from the beginning, the value of cryptocurrencies is mentioned. Finally, the method of collecting, storing and trading cryptocurrencies via a mobile device is discussed, on the basis of which I draw my conclusion.

Keywords: bitcoin, cryptocurrencies, mobile business, mining, blockchain

SADRŽAJ

1. UVOD

Svijet u kojem tehnologija preuzima sve veću ulogu i gdje se područje bez interneta ne može zamisliti, dobar dio ljudi je izgubilo povjerenje u financijske sustave pa se javila potreba za drugačijim pristupom rješavanju problema cijelokupnog financijskog sustava. Kriptovalute su stoga donijele potpuno drugačiji financijski sustav koji je u mnogočemu drugačiji od tradicionalnog oblika. Prethodnih godina digitalni novac sve više postaje predmet zanimanja javnosti, posebice zbog velike praktičnosti i brzine obavljanja transakcija za razliku od klasičnih oblika, a to su čimbenici koji nedvojbeno utječu na porast popularnosti različitih oblika internetskog plaćanja. Digitalne valute i njihova primjena na globalnom tržištu je raznovrsna, dok u Hrvatskoj još uvijek postoji određena dvojba korisnika o njihovom korištenju pa je samim time manja mogućnost njihove primjene.

Rudarenje i trgovanje kriptovalutama već dugi niz godina privlači veliki broj korisnika, čime se povećava korištenje informacijske tehnologije, računala, mobilnih uređaja i slično. Porastom trenda trgovanja i rudarenja kriptovalutama dolazi do porasta marketinga za kriptovalute, promocije kriptovaluta na raznim društvenim mrežama, web stranicama i drugim digitalnim komunikacijskim kanalima, što omogućuje korisnicima lakše upoznavanje s kriptovalutama i trgovanje na kripto burzama.

Svrha i cilj istraživanja ovog diplomskog rada je prikazati razvoj i načine korištenja kriptovalute, zatim upoznati značaj mobilne tehnologije i samog mobilnog poslovanja u svrhu trgovanja kriptovalutama. Trgovanje kriptovalutama i mobilno poslovanje svakako zahtjeva znanje o mnogim tehnologijama. Mobilno poslovanje uključuje korištenje mobilnih uređaja i to u cilju komunikacije, mobilnih financija, trgovine i drugo. Također, cilj istraživanja ovog diplomskog rada je analiza informiranosti korisnika s rudarenjem i trgovanjem, te načinima i vrstama pristupa rudarenju i trgovanju kriptovalutama.

Za pisanje ovog diplomskog rada koristit će se podaci dobiveni primarnim i sekundarnim istraživanjem. Sekundarnim istraživanjem prikupit će se informacije iz knjiga, znanstvenih članaka te internet izvora kako bi se što bolje objasnili pojmovi iz teorijskog dijela rada. Primarnim istraživanjem koristiti će se kvantitativne i kvalitativne metode, te metoda anketiranja. U radu je prikazana provedena anketa korisnika u dobi od 18 do 45 godina. Anketa je izvršena putem Google docs obrasca, a na temelju dobivenih informacija rezultati su interpretirani te prikazani grafički i tablično.

Diplomski rad podijeljen je u 7 cjelina:

1. Uvod
2. Arhitektura i tehnologija mobilnog poslovanja
3. Pregled razvoja i princip rada kriptovaluta
4. Sigurnost mobilnog poslovanja u svrhu trgovanja kriptovalutama
5. Značajke i utjecaji marketinških procesa u trgovanju kriptovalutama
6. Analiza korištenja mobilnih uređaja u svrhu rudarenja i trgovanja kriptovalutama
7. Zaključak

U prvom poglavlju rada je uvod u sam rad. Dugo poglavlje odnosi se na teorijski dio mobilnog poslovanja, gdje se objašnjava što je to mobilno poslovanje te koje su mu karakteristike i razlike u odnosu na klasično poslovanje. Trećim poglavljem obuhvaćena je teorija kriptovaluta, gdje se spominje povijest i pojam kriptovaluta, zatim prednosti i nedostaci, te vrste kriptovaluta. Četvrtim poglavljem prikazana je sigurnost mobilnog poslovanja u svrhu trgovanja kriptovalutama, gdje je detaljno obrazložen pojam kriptonovčanika odnosno „*Walleta*“ kao način pohranjivanja kriptovaluta. Zatim su prikazane i ranije spomenute transakcije, pojam rudarenja, te na koje se sve načine pojavljuje kriminal u trgovanju kriptovaluta. Petim poglavljem ističu se marketinški procesi odnosno utjecaj kriptovaluta na međunarodno poslovanje i međunarodnu trgovinu. U šestom poglavlju naglasak je na empirijskim dijelu rada, gdje je kroz anketu prikazan stav i mišljenje ispitanika na mobilno poslovanje ali i na trgovanje i rudarenje kriptovaluta. Sedmim poglavljem izneseni su zaključci provedenog istraživanja diplomskog rada.

2. ARHITEKTURA I TEHNOLOGIJA MOBILNOG POSLOVANJA

Prije definiranja mobilnog poslovanja, važno je istaknuti što predstavlja pojam poslovanja. Poslovanje je skup aktivnosti u poduzeću koja se bave raznim pružanjem usluga ili prodajom dobara kako bi ostvarili profit [1]. U ovom radu naglasak je na mobilnom poslovanju i tehnologiji mobilnog poslovanja.

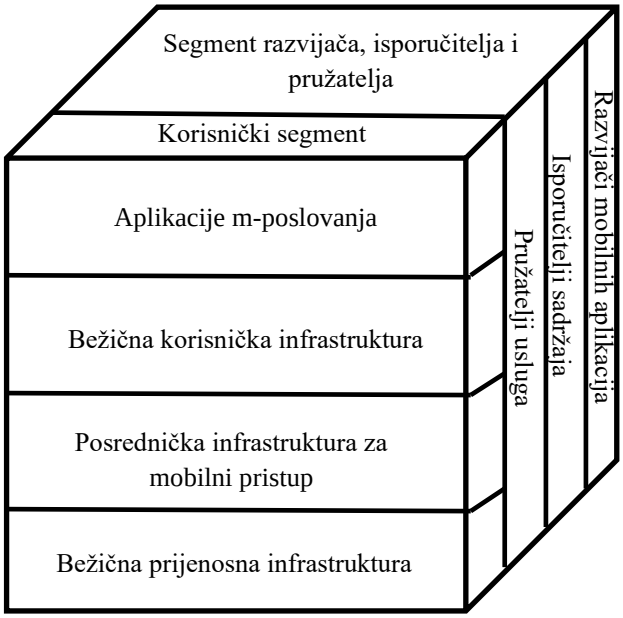
2.1. Pojam i karakteristike mobilnog poslovanja

Pojam mobilnog poslovanja se kroz različite izvore i literaturu opisuje različito, a ono što uzrokuje nedosljednost definicija je dvojba je li mobilno poslovanje ograničeno samo na telekomunikacijsku bežičnu mrežu ili se ono odnosi i na poslovanje kroz bežični pristup bilo kojoj računalno posredovanoj mreži. Jedna od definicija je da mobilno poslovanje podrazumijeva korištenje mobilnih uređaja u cilju komunikacije i informiranja [2]. Također, mobilno poslovanje označava pristup raznim poslovnim procesima bilo kada i bilo gdje. Procesi se odvijaju pomoću mobilnih komunikacijskih mreža, koje procese čine dostupni neovisno gdje se korisnik nalazi [1]. Mobilno poslovanje usko je vezano uz elektroničko poslovanje, budući da se usluge i kod jednog i kod drugog obrađuju elektroničkim putem, bilo putem računalom posredovanih mreža ili putem telekomunikacijskih mreža. Jedina razlika u odnosu na elektroničko poslovanje je da se u mobilnom poslovanju telekomunikacijskim mrežama pristupa putem mobilnih uređaja.

Osim toga, mobilno poslovanje predstavljaju jedinstvene značajke koje imaju određene prednosti u odnosu na klasične oblike poslovnih transakcija, uključujući elektroničko poslovanje. Mobilno poslovanje korisnicima pruža mogućnost pristupa internetu s bilo kojeg mjesta u bilo koje vrijeme, zatim mogućnost određivanja lokacije korisnika, funkcionalnosti pristupa informacijama u trenutku potrebe i ažuriranja potrebnih podataka odnosno informacija [3]. Kod mobilnog poslovanja korisnici su uključeni u sve aktivnosti, primjerice i za vrijeme obavljanja transakcija ali i kod poslovnih sastanaka i sl. Mobilno poslovanje stoga je sveprisutno, obavlja se u bilo kojem trenutku i na bilo kojem mjestu.

Struktura mobilnog poslovnog sustava sastoji se od četiri glavne komponente: poslovne aplikacije, posredničke infrastrukture za mobilni pristup, bežičnog korisnika i prijenosne infrastrukture. Ako organizacija ima uspostavljen okvir za različite odnosno

spomenute komponente sustava, tada može implementirati vlastite usluge bez da mora sama uspostaviti sve komponente. Slikom 1 prikazan spomenuti organizacijski okvir poslovanja.



Slika 1. Okvir organizacije poslovanja u pokretu [4]

Znano je kako poduzće odnosno organizacije uz takav okvir ne moraju raditi na stvaranju svih komponenti, već se koristiti funkcionalnostima i uslugama koje pruža netko drugi. Oni mogu biti isporučitelji sadržaja, pružati mobilne usluge ili kreirati neku mobilnu aplikaciju. Isporučitelj sadržaja stvara svoje usluge pomoću raznih aplikacija koriteći više kreatora tih aplikacija, a vlastiti sadržaj sistematizira iz sadržaja drugih isporučitelja sadržaja. Spomenuti sadržaj dostavi se operatoru mreže ili pružatelju mobilnih usluga. Dalje, operatori imaju aktivnu ulogu u radu mobilnog poslovanja jer djeluju kao posrednici koji krajnjim korisnicima pružaju različite usluge. Korisnik od operatora očekuje kvalitetnu uslugu [4].

Kako bi se razumijelo kako funkcionira sustav poslovanja, važno je navesti različite faze ciklusa sustava poslovanja u pokretu, a to su: faza inicijalizacije, faza proširenja, faza konsolidacije i faza zrelosti. Kao prva navedena faza, faza inicijalizacije, započinje razvojem aplikacije. U toj fazi proučava se literatura, istražuje se tržište i internet, te se konzultira sa suradnicima i krajnjim korisnicima. Svaka ideja se obično detaljno razrađuje, s detaljnom analizom funkcionalnosti buduće aplikacije ili usluge, kao i mogućom isplativošću projekta.

Druga faza ubrzava rast sustava. Uključuje programiranje mobilne aplikacije koja se može pokrenuti na različitim platformama. Programiranje aplikacije odnosi najviše vremena.

Ova faza uključuje ispravljanje ili prekid aplikacije koja je naišla na pogreške ili ima nedostatak. Faza konsolidacije odnosi se na testiranje i verifikaciju aplikacije. U ovoj fazi ispravljaju se određene pogreške nastale razvijanjem aplikacija. Jasno je kako se svi nedostaci i pogreške moraju ispraviti i otkloniti kako ne bi kasnije došlo do problema i ugleda od strane korisnika [4].

Faza rada mobilne mreže obično se naziva fazom eksploatacije ili zrelosti. Ovo je vrijeme kada se sustav koristi za obavljanje svojih osnovnih funkcija. Prije početka faze rada sustava isporučuje se sva potrebna oprema za njegov nesmetan rad. Tijekom faze rada oprema se može mijenjati, nadograđivati ili poboljšavati. Kreatori koji su razvili aplikaciju šalju istu isporučitelju sadržaja koji će je napuniti sadržajem, a on će je dalje proslijediti operatoru. Takav sadržaj isporučitelj sadržaja može isporučiti pružatelju mrežnih usluga. Operater bežične mreže mora isporučiti sadržaj aplikacije korisniku u obliku sučelja koje će omogućiti korisniku da izvrši svoje zadatke. Ciklus završava s isporukom mrežnog operatora aplikacije korisniku s cijelim sadržajem sa svim dodatnim uslugama [4].

Svakako kako bi se sve navedeno omogućilo potrebni su uređaji odnosno infrastruktura. U temeljnu infrastrukturu mobilnog poslovanja svrstavaju se: mobilni uređaji, mobilni operativni sustavi, bežične mreže i sustav. Najčešće korišteni uređaji su pametni telefon (mobitel), tablet, prijenosno računalo, stolno računalo i sl. U nastavku navedene su skupine mobilnih usluga, odnosno servisa koje je moguće uspostaviti sa najznačajnijim uređajima mobilnog poslovanja.

2.2. Mobilne usluge

Karakteristika mobilnih usluga je globalni domet, visoki stupanj sigurnosti i privatnosti. Mobilne usluge većini su jednostavne za korištenje, neovisne su o vremenu i mjestu. Pod uvjetom da korisnici poštuju preporuke ponuđača usluga i operatera one su poprilično sigurne [5]. Mobilni uređaji kao najčešće korišteni uređaj mobilnog poslovanja, pored glavne usluge telefoniranja koristi se i za neke dodatne usluge poput: mobilne pošte, mobilnog bankarstva, mobilnog plaćanja i sl. Autor May [6] navodi tri skupine mobilnih usluga a to su [6]:

- komunikacijske usluge kao što su: prijenos podataka, SMS, MMS,
- usluge za korisnike (novosti, sport, putovanja, ulaznice, mobilno bankarstvo, kupovina, plaćanje, igrice) i

- poslovne usluge (oglašavanje, odlučivanje, upravljanje, izvršavanje naloga i sl).

Komunikacijske usluge poput prijenosa podataka, SMS-a, MMS-a usluge su koje se mogu koristiti i dostupne su bilo gdje u cijelom svijetu. Spomenute usluge lako se koriste i neovisne su o vremenu. Isto tako i usluge za korisnike. Koriste se uvijek kada ima dostupnog interneta. Također, razna istraživanja upućuju na to, da iako su mobilni telefoni nekada bili prvenstveno za obavljanje poziva, u današnje vrijeme to je jedna od njihovih najmanje popularnih funkcija [25].

U današnje vrijeme vrlo popularna usluga je mobilno bankarstvo. Mobilno bankarstvo usluga je koju banka omogućuje svojim korisnicima da obavljaju različite bankarske aktivnosti izravno sa svojih pametnih telefona. Prije korištenja mobilnog bankarstva banka, odnosno korisnik mora instalirati aplikaciju te unijeti razne kodove da bi aplikacija bila valjanja i spremna na korištenje. Od strane banke, prilikom provjere valjanosti i autorizacije transakcija poslužitelj generira brojčanu vrijednost koja se sastoji od šest znamenki. Isto tako su se spominju poslovne usluge, gdje se najviše koriste nalozi.

Kod mobilnih usluga važno je spomenuti kako ponuđači odabiru osnovnu bazu komunikacijskih tehnologija preko koje će nuditi određene usluge privatnim i poslovnim korisnicima. Istaknute tehnologije mobilnih servisa odnosno usluga su SMS, USSD, MMS, WAP i SIM [5]. SMS je svima poznata usluga, a predstavlja uslugu slanja i primanja kratkih poruka teksta, dok je MMS usluga slanja multimedijskog sadržaja. USSD je vrlo sličan SMS-u, ali za razliku od njega on omogućava povezanost u realnom vremenu. USSD je usluga za posredovanje kratkih tekstualnih poruka među korisnicima GSM mreže [5]. Primjer popularnog USSD servisa (usluge) je *mPay*, horoskop, vremenska prognoza i sl.

WAP servis je osmišljen za rad unutar ograničenja koja imaju telefoni i računala. WAP povezuje mobilno okruženje s internetom i njegovim okruženjem pa na taj način omogućava korisnicima mobilnih telefona pristup sadržajima na webu. SIM odnosno SIM *Application Toolkit* je kartica gdje se nalaze sve informacije o GSM pretplatniku. Također, SIM predstavlja vezu mobilnog telefona s GSM mrežom. Pojmom SIM *Application Toolkit* označuje se poseban oblik upotrebe i primjene SIM kartica koje omogućavaju izvršavanje određenih mobilnih usluga na telefonu odnosno na pametnoj SIM kartici [5].

3. PREGLED RAZVOJA I PRINCIP RADA KRIPTOVALUTA

Glavni čimbenici razvoja digitalne valute su razvoj tehnologije i znanosti, kvalitativni i kvantitativni razvoj interneta, razvoj kriptografije kao posebne znanstvene discipline te razvoj specifičnih tehničkih rješenja poput softvera blockchain. Razvoj velike uporabe internetske infrastrukture ogleda se u svim aspektima života, ali samo je pitanje kada će to početi kao medij ekonomskih transakcija. Osim povećanja broja korisnika, internet je također tehnološki razvijen, a brzina je sve brža, a širenjem telekomunikacijskih mreža i razvojem tehnologije pristupačnost interneta također je postala veća.

Razvojem interneta mnogi su pokušali razvijati digitalni novac odnosno digitalnu valutu. Zamišljeno je da korisnici kriptovaluta međusobno izmjenjuju transakcije, a sve to da funkcionira pomoću kriptografije. Kriptografija je znanost o obradi matematike i računala za kodiranje i dekodiranje podataka. Razvojem mikroprocesora stvoreni su uvjeti za pojavu kriptografskih funkcija u računalnim funkcijama. Jedno od polja kriptografije su hash funkcije. Ove funkcije mogu primiti niz podataka proizvoljne duljine za unos i proizvesti određeni "potpis" ili niz unaprijed određenih znakova duljine. Važno je da će svaka mala promjena ulaznog niza uzrokovati značajnu promjenu izlaznog niza, a brzina cijelog procesa izravno utječe na upotrebljivost funkcije. Sama funkcija je "jednosmjerna", odnosno izračunavanje raspršivanja ulaznih podataka jednostavno je i brzo, ali nemoguće je dobiti izvorni skup podataka iz raspršivača. Ova se tehnologija koristi za osiguravanje autentičnosti i kontrole podataka, a autentičnost podataka osigurava se raspršivanjem.

3.1. Povijest i pojam kriptovaluta

Kroz povijest novac je uvijek postojao u nekom obliku. Svako doba imalo je svoj način na koji je određen oblik i značenje novca. Kod razmjene dobara postojala je potreba za zadovoljanja svih strana, čime je nekad davno umjesto novca postojalo dobro primjerice davale su se životinje, oružje u zamjenu za drugo dobro. Nakon toga, počeo se razvijati novac, najprije su to bile kovanice a zatim i novčanice. Što se tiće samog novca, javljaju se transakcije, pa se u današnje vrijeme umjesto samog novca pojavljuju kriptovalute kao sredstvo plaćanja.

Isto tako, kroz povijest bili su razni pokušaji za stvaranje digitalnog novca. Tako je 1982. godine David Chaum objavio rad gdje predlaže zamjenu elektroničkih transakcija. Rad Davida Chauma smatra se prvim prijedlogom za postojanje digitalnog novca [7]. Zatim, 1998. godine pojavljuje se „BitGold“ koji je ideja Nicka Szabo-a, koja je morala predstaviti decentraliziranu digitalnu valutu koja je upućivala na sve nedostatke postojećeg financijskog sustava [7]. BitGold sustav nije implementiran, ali se smatrao prethodnikom danas najpoznatije kriptovalute Bitcoina. Bitcoin je prva prava kriptovaluta koja je teorijski razrađena u 2008. godini od strane organizacije pod „umetničkim imenom“ Satoshi Nakamoto, a pušten je u svijet 2009. godine [8]. Bitcoin predstavlja jednu od kriptovaluta pomoću koje se može vršiti internetsko plaćanje, on još nije izdan od središnje banke, ali također se još ne veže uz poslovne banke. Kroz Bitcoin tehnologiju pomoću blockchain radi se jedinstvena baza skupa podataka sa svim postojećim i provedenim transakcijama koje su pohranjene u knjigu. Financijska ni vladina institucija nije u položaju pomoću kojega bi mogli mijenjati postavke blockchaina kroz sustav, a ne možemo ni utjecati na samo plaćanje [9].

Riječ „kripto“ dolazi iz pojma „kriptiranje“ koje predstavlja pretvaranje jasnog teksta u šifrirani. Kriptovaluta jest virtualna valuta, odnosno digitalni novac koji ne postoji u fizičkom obliku, već se nalazi samo u računalima, a pristup takvom novcu najčešće se ostvaruje putem interneta [10]. Kriptovaluta je vrsta digitalnog novca kojeg nije moguće kopirati ni proizvesti. Funkcionira putem elektronskog zapisa određenih vrijednosti koji su pohranjeni u novčanicima te internetskim stranicama zaduženih za takvu vrstu usluge. Kriptovalute proizvode ljudi diljem svijeta tako što koriste softver koji rješava matematičke zadatke. Vrijednost im se utvrđuje svake sekunde na temelju ponude i potražnje. Ovo je potpuno novi koncept koji mijenja način plaćanja i način kako novac doživljavamo. *„Kriptovaluta predstavlja ekvivalent elektroničkog novca. Temeljna su karakteristika kriptovaluta kriptografski mehanizmi koji služe za stvaranje i bilježenje transakcija putem privatnih i javnih ključeva.“* [11]

Status kriptovalute kao novca nije utvrđen, a legalnost još nije definirana i različita je u odnosu na države. U nekim zemljama je potpuno zabranjeno, dok je u većini potpuno legalno. Nad kriptovalutama ne postoji središnja institucija koja ih kontrolira, već je to sustav koji se zasniva na šifriranju. Kriptografija nije novina, tisućljećima se primjenjuje kod osiguravanja tajnosti vojne komunikacije. Kako proces šifriranja i dešifriranja nije jednostavan, tako ni kriptovalute nisu jednostavne.

3.2. Princip rada kriptovaluta

Kriptovalute je vrlo teško shvatiti, objasniti, većina se ne razumije u njihovo funkcioniranje. Kako bi netko shvatio kriptovalute mora imati barem nekakvo predznanje i riječnik iz područja informatike. Specifičnost kriptopvalute leži u tome da se ona ne može kopirati, iako je dostupna svima putem interneta. Kriptovaluta je decentralizirana te nije regulirana od strane središnje banke, niti kontrolirana od države. Pa se u tom slučaju spominje sustav P2P odnosno *Peer-to-peer*. *Peer-to-peer* mreža koncept je povezivanja računala bez središnje točke, bez centralnog servera. Svako računalo izravno komunicira sa drugima, nema središnjeg, najpoznatiji primjer ovakve mreže su *torrenti*[1]. Skraćeno, koncept P2P uključuje izravna plaćanja bez uključivanja financijskih institucija.

Vrlo važnu ulogu kod funkcioniranja kriptovaluta ima *Open-source* pristup razvoju softvera, odnosno računalni program čiji je programski kod objavljen na internetu i svatko ga može i vidjeti i mijenjati. *Open-source* se temelji na dobrovoljnoj suradnji ljudi, bez naknade, koji zajedno unapređuju softver za dobrobit svih korisnika. Cijela zajednica nadgleda prijedloge promjena i odobrava samo one koje smatra kvalitetnima.

Peer-to-peer i *open-source* temeljni su građevni elementi dizajna kriptovaluta. Kriptovaluta se po mnogo čemu se razlikuje od digitalnog novca u banci. Kriptovalute su posebne jer su odvojene od monetarnog sustava, u ovome svijetu nitko nikome ne duguje, ako imate kriptovalutu to je kao da imate zlato, vrijednost mu varira, ali nikome niste dužni. Tako se svugdje spominje najpoznatija kriptovaluta pod imenom Bitcoin. Bitcoin je osim što je jedinica kriptovalute, i specifična pod-mreža na internetu. Također, to je sustav elektroničkoga plaćanja koji se zasniva na kriptografiji. Kriptografija se tisućljećima primjenjuje za osiguravanje tajnosti diplomatske, vojne i preljubničke komunikacije. Povjerenje je temelj svakog financijskog sustava, kod kriptovaluta je potrebno imati povjerenja u sustav na kojem se nalaze ove valute.

Kao što je spomenuto transakcije kriptovaluta temelje se na kriptografiji, koja je izumljena kako bi komuniciranje putem interneta ostalo sigurno, a zasniva se na temelju dva ključa, isto kao i elektroničko potpisivanje dokumenata u Hrvatskoj. Za transakciju je potrebno da primatelj i pošiljatelj imaju svoj novčanik koji se mogu besplatno intalirati na

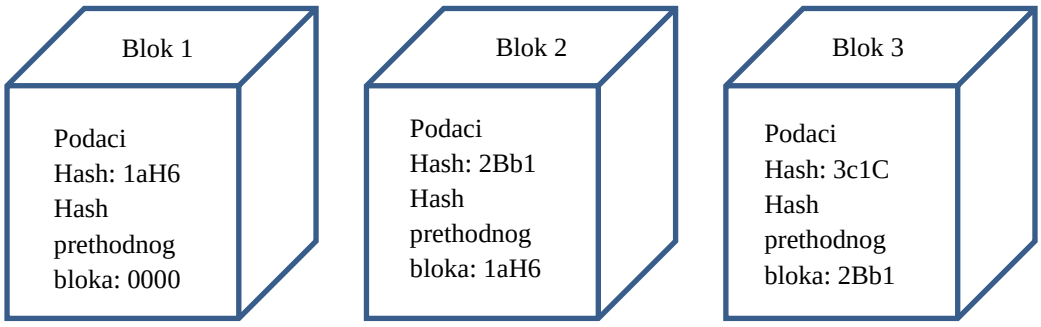
[1] format dokumenta koji služi kako bi korisnika uputio na internet stranicu gdje se nalazi datoteka i lokacija za preuzimanje željenih podataka

računalo ili mobitel, ili pak na internet pregledniku. Svaki novčanik ima svoj privatni ključ koji služi za raspolaganje sredstvima u novčaniku. Privatni ključevi nisu isto što i lozinke koje se uobičajeno koriste na internetu jer su mnogo dulji i složeniji. Pošiljatelj bitcoina šalje transakciju u mrežu i čeka potvrdu transakcije. Bitcoin mrežu čine računala koja potvrđuju transakcije, a kao nagradu za verifikaciju plaćeni su u bitcoinima, što se naziva rudarenje. Osoba može steći bitcoin tako da ga kupi, stekne u transakciji ili ga zaradi rudareći. Za stjecanje zlata potrebno je rudariti, a nagrada za računalno rudarenje su novi bitcoini u sustavu. Sve transakcije zapisane su u blockchainu, transakcije se udruže u blokove i zatim potvrđuju blok, tu knjigu posjeduju svi i ona se sinkronizira među računalima na mreži. Identitet osoba u transakciji je šifriran te se preporuča mijenjanje adrese kako bi anonimnost ostala zajamčena.

Sustav kriptovaluta usmjeren je da kriptovaluta s vremenom dobiva na vrijednosti i da nikada ne bude inflacije jer nema središnje institucije koja bi ubacila valutu u sustav. U početku je bilo tko mogao na kućnom računalu rudariti bitcoine, ali širenjem mreže rudara i smanjenja nagrada, kako bi korisnik zaradio mora imati sve jače računalo. Danas je u praksi manja zarada na rudarenju nego što je trošak cijene električne energije za pogon računala, tako da se rudarenjem bave samo oni koji imaju pristup iznimno jeftinoj električnoj energiji.

Isto tako, većina bankara i ekonomista ne razumije se u kriptovalute, i to s pravom, jer njih ne stvaraju ekonomisti, nego računalni programeri, stoga će teško širi krug ljudi prihvatiti kriptovalute ako ne mogu razumjeti osnove funkcioniranja digitalnoga novca [7]. Poznato je kako je kod uvođenja prvih bankomata postojao problem dvostruke potrošnje, gdje je bilo moguće dva puta podići sav iznos novca s računa na različitim bankomatima u kratkom vremenu jer informacije nisu bile usklađene. Decentralizacija novčanog sustava zahtijevala je rješavanje problema dvostruke potrošnje i krivotvorenja novca. Kriptovalute sklanjaju posrednike, pa se svaka transakcija obavlja veoma brzo i direktno između dva subjekta bez obzira na kojem su dijelu svijeta. Transakcije su sigurnije od standardnih bankarskih i mogu se obaviti bez obzira gdje se korisnik nalazi. Decentralizirana priroda *open-source* protokola osigurava da kontrola mreže ostaje u rukama korisnika. Transakcije su ovisne o sudionicima u mreži, a korisnik je odgovoran za sigurnost vlastitih financija i podataka, bez potrebe da ovisi o trećoj strani poput bankarske institucije. Iz svega navedenoga proizlazi da je razvoj kriptografije preduvjet za razvoj elektroničkih platnih sustava i poboljšanje njihove sigurnosti, čime se formiraju različiti oblici digitalne valute. Blok lanac je digitalna baza podataka koja

sadrži zapisnik svih transakcija u sustavu. U određenom je smislu decentraliziran, a svaki sudionik u sustavu ima priliku zadržati svoju kopiju. Transakcije su grupirane kronološkim redom, tzv. blok transakcija. Svaka blok transakcija digitalno je „potpisan“ odnosno pridružena mu je određena digitalna šifra koja je garancija da je blok autentičan, tj. svaki pokušaj promjene sadržaja bloka je vrlo lako otkriti [12]. Blok se sastoji od primarno tri glavna dijela, a vizualno kako to izgleda prikazano je slikom u nastavku.



Slika 2. Jednostavniji prikaz bloka [28]

Osim određenog broja transakcija svaki blok sadrži *hash* prethodnog bloka, što bi značilo da ukoliko netko želi promijeniti sadržaj bloka mora izmijeniti sve prethodne blokove. Na taj način su blokovi povezani i odatle i potječe naziv blockchain. Njega treba vizualizirati kao niz kockica koji su u vertikalnoj strukturi, a najnoviji blok uvijek je na vrhu lanca. Prvi blok svih vremena nastao je 2009. godine i zove se *Genesis Block* [12].

3.2.1. Prednosti kriptovaluta

Nakon osnovog prikaza o teoriji, povijesti i kriptovaluta, važno je spomenuti kako postoje određeni čimbenici koji pozitivno utječu na ulaganje u kriptovalute. Hakiranje određenog sustava zvanog blockchain je teško i zahtjeva hakiranje više tisuća osobnih računala, što je zapravo nemoguće. Kriptovalute su veliki napredak i imaju veliki potencijal te bi u budućnosti mogle zamijeniti trenutni novčani sustav zbog rasta korisnika kriptovaluta. Ni jedna osoba nema mogućnost promijeniti količinu novca te ubrzati rast i vrijednost. Količina novca je ograničena te je otporana na inflaciju. Osoba koja želi kreirati novi novčić mora ulagati novac u hardvere i električnu energiju. Ne mora se trošiti novac za samo održavanje računala. Pomoću transakcija dolazi do verifikacije i trajne registracije u glavnoj knjizi. Kada šaljemo novac, slanje je slično običnom slanju e-maila. Svaki korisnik svoje transakcije može

provjeravati kada god poželi. Sustav nije kontroliran te ni jedna osoba nije zadužena za kontroliranje samog sustava, sustav ima svoju mrežu koja radi po principu od korisnika do korisnika [8].

Isto tako Martucci [13] navodi sljedeće prednosti kriptovaluta:

- sigurnost,
- transparentnost,
- rudarstvo kriptovaluta dostpuno je svakome,
- fluktuacija cijena može donijeti zaradu,
- zaštićenost od inflacije,
- decentraliziranost i
- niski transakcijski troškovi.

Kako su kriptovalute u 99% slučajeva bazirane na blockchain tehnologiji koja je temeljena na kriptografiji, vrlo ih je teško ili skoro nemoguće dekodirati. Što znači, ne postoji mogućnost krivotvorenja ili falsificiranja za razliku od korištenja papirnatog novca ili kartica.

Kada govorimo o transparentnosti, tu mislimo na to da banka (primjerice ESB) široj javnosti daje sve važne informacije o svojim postupcima i financijskoj strategiji. Što se tiče rudarenja i dostupnosti autor Martucci spominje kako se samo uz nekoliko internetskih pretraživanja računalo može postaviti da počne rudariti novčiće umjesto korisnika. Također, kod Bitcoina je mala vjerojatnost da će se novac zaraditi rudarenjem bez velike i dobre opreme, ali primjerice na nekim manje poznatim kovanicama računalo bi svakako moglo generirati dodatni novac za korisnika bez učinjenog pokreta samog korisnika [13].

Poznato je kako se u toku samo jednog mjeseca cijena virtualne valute može se promijeniti za više od 20%. Dalje, budući da kriptovalute općenito imaju ograničenu ponudu ugrađenu u svoj izvorni kod, one su prirodna zaštita od inflacije. Što se tiče decentralizacije kriptovalute nisu kontrolirane od strane ni jedne organizacije.

S obzirom da nema uključenih trećih strana pri kupoprodaji kriptovaluta automatski ne postoje uvijek i transakcijski troškovi ili su oni jako niski, dakle u ovom slučaju nije potrebno koristiti posrednike kao što je npr. *PayPal* ili *Visa* kako bi proveli neku transakciju i stoga troškovi ostaju 0 kuna ili su relativno niske visine [13].

3.2.2. Nedostaci kriptovaluta

Svaka stvar uz prednosti ima i nekoliko nedostataka također kriptovalute imaju svoje nedostatke i izazove. Kriptovalute žele preuzeti funkciju novca, ali ne ispunjavaju funkcije novca. Novac je opće prihvaćeno sredstvo razmjene, a kriptovalute nisu mjerilo vrijednosti te se ne proučavaju da postanu sredstvo razmjene.

Nedostaci kriptovaluta prikazani su kroz daljnji tekst. Kriptovalute su nepovratne transakcije koje se ne mogu povratiti nazad te također nisu napravljene poput kreditnih kartica da štite korisnike od prijevara. Banke također mogu odbiti potpunu uslugu osobama koja se bavi kriptovalutama, mogu odbiti suradnju s digitalno valutnom kampanjom. Kriptovalute moraju zadovoljiti sve potrebne uvijete kako bi došle u sustav korištenja na svim globalnim nivoima. Kod tehnoloških napredaka mogu se javiti potrebe koje zahtijevaju sve jaču računalnu tehnologiju te specijalne hardvere i softvere. Svi financijski proizvodi imaju vrlo velik i dobro razvijen sustav koji štiti zasititi samih potrošača za razliku od kriptovaluta. Još jedan nedostatak kriptovaluta je taj što nisu stalne, mogu biti zauvijek izgubljene ili uništene zbog greške na softveru ili gubitka interneta. Kriptovalute zasnivamo na kompliciranim i teškim matematičkim algoritmima tako da neke države imaju oprezan pristup ili ga izbjegavaju. U nekim državama kriptovalute su potpuno zabranjene i osobe koje ih koriste dobivaju velike novčane kazne [9].

Isto tako kao nedostaci navode se [13]:

- volatilnost
- regulatorno okruženje je stalno u promjeni
- rudarenje zahtjeva ozbiljne resurse
- nedostatkom regulative pokreće crno tržište.

Volatilnost predstavlja određeni raspon i brzinu kretanja cijena na nekom tržištu, odnosno to je mjera rizika, gdje se točno vidi koliko jako ili slabo se mijenjaju cijene. Kriptovalute su dobar primjer jer su upravo one vrlo nestabilne. Što se tiče regulatornih okruženja tu se spominju zakoni koji su u tom području vrlo promjenjivi. Jasno je kako samo jedna promjena na tržištu može slomiti bogatstvo u samo par sekundi [13].

Poznato je kako da bi se zarađivao novac rudarenjem potrebno je imati mnogo vremena, novaca ali i kvalitetnih resursa. Korisnici koji se žele posvetiti takvom zadatku morat će pripremiti ozbiljan skup hardvera. Osim toga, najveća regulatorna briga oko kriptovalute je njezina sposobnost olakšavanja nezakonitih aktivnosti. Mnoge online transakcije na sivom i crnom tržištu denominirane su u Bitcoinima i drugim kriptovalutama [13].

3.3. Vrste kriptovaluta

Na trenutnom tržištu postoji više od 5000 kriptovaluta. Kriptovalute se mogu podijeliti na razne načine ali najpoznatiji način odnosno pokazatelj važnosti kriptovalute je tržišna kapitalizacija. Tržišna kapitalizacija kriptovaluta je ukupna tržišna vrijednost dolarskih tržišnih vrijednosti dionica tvrtke. Izračunava se množenjem ukupnog broja izdanih dionica tvrtke s trenutnom tržišnom cijelom jedne dionice [14]. Tablicom u nastavku prikazane su trenutne top 10 kriptovalute prema tržišnoj kapitalizaciji.

Tablica 1: TOP 10 kriptovaluta prema tržišnoj kapitalizaciji

Redni br.	Naziv kriptovalute	Vrijednost
1.	Bitcoin (BTC)	1 179 944 996 640 $
2.	Ethereum (ETH)	539 836 564 907 $
3.	Binance Coin (BNB)	93 397 831 196 $
4.	Solana (SOL)	72 623 954 461 $
5.	Tether (USDT)	71 447 633 858 $
6.	Cardano (ADA)	67 994 519 197 $
7.	XRP	58 535 278 804 $
8.	Polkadot	52 430 311 077 $
9.	HEX	37 823 705 293 $
10.	Dogecoin (DOGE)	35 518 406 180 $

Izvor: rad autora prema [15]

U nastavku prva objašnjena je najbolje pozicionirana kriptovaluta, Bitcoin.

3.3.1. Bitcoin

Bitcoin (skraćeno BTC) predstavlja najpoznatiju i najrasprostranjeniju kriptovalutu, predstvljenu u znanstvenom radu pod nazivom „Bitcoin: *A Peer-to-peer Electronic Cash System*“. *„Bitcoin je digitalni novac, stvoren i čuvan elektronički. Bitcoin nije tiskan i nije kontroliran od strane bilo koga. Proizvode ga brojni ljudi pomoću računala u cijelom svijetu koristeći software koji rješava matematičke probleme“* [9]. Bitcoin je kao valuta za razliku od ostalih valuta, primjerice kune ili eura, stvoren i čuvan elektronički, što bi značilo da se niti može printati ili kovati niti ga je moguće posjedovati u fizičkom obliku.

Bitcoin se može steći na dva načina, prvi način predstavlja kupnju novca ili pak zamjenu za druge proizvode s drugim korisnicima, a drugi način predstavlja samo rudarenje. Svaki korisnik na svom računalu ili mobilnom uređaju također na webu može slati, ali i primati bitcoine. Kad osoba trguje Bitcoinom ne postoji sama zaštita potrošača, naknadu za sve transakcije plaća kupac, a ne trgovac, transakcije su nepovratne i nije ih moguće poništiti.

Najčešće upotrebe Bitcoina su:

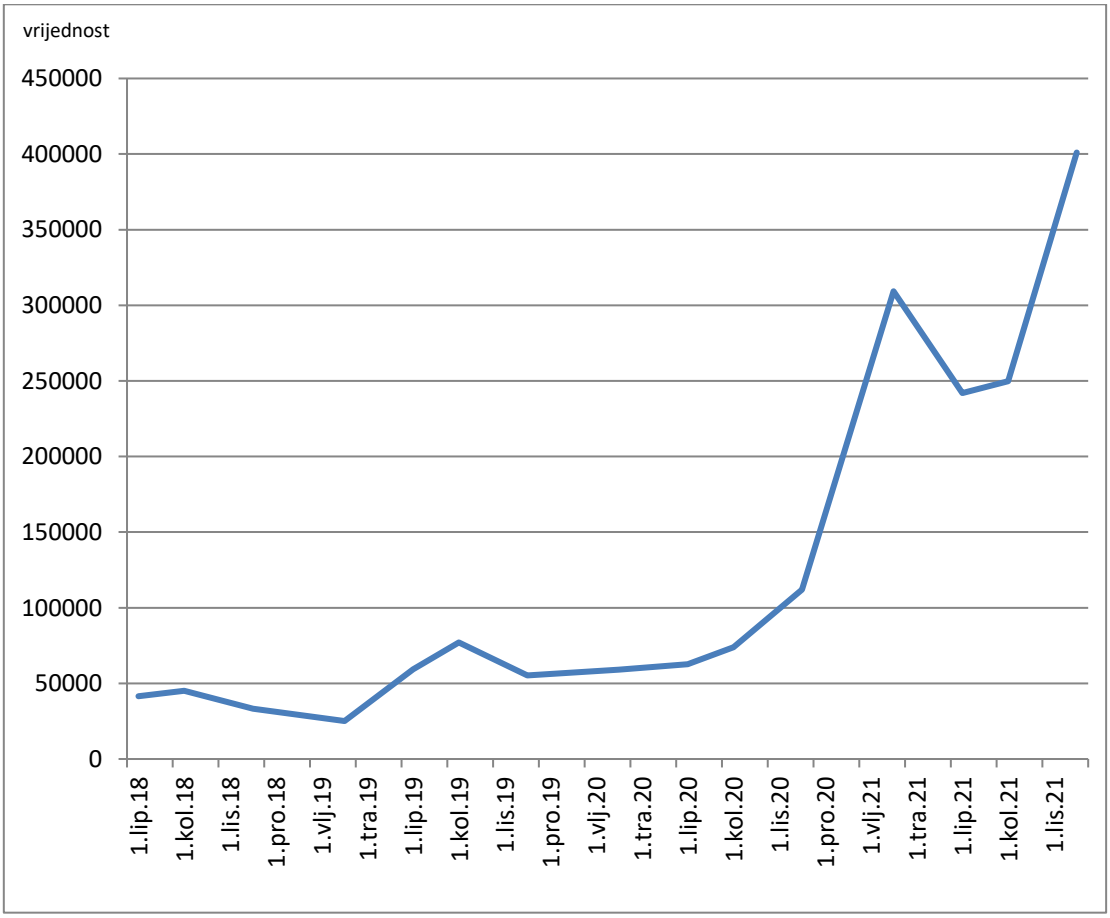
- kupnja – danas se s Bitcoinom može plaćati svašta, od umjetničkih djela pa do kuće i automobila
- slanje novca – kod slanja novca Bitcoin ima mnoštvo prednosti jer je brže, nema posrednika, samim time i jeftinije, nisu potrebni dokumenti za otvaranje računa, jedina je mala kada pretvaramo Bitcoin u pravi novac
- investicija – u Bitcoin možemo ulagati, jedina razlika je što Bitcoin brzo mijenja cijenu pa je ulaganje rizičnije, ali i moguće profitabilnije
- trgovanje kriptovalutama - Bitcoin nije centraliziran, stoga ovisi o ponudi i potražnji, cijena se ponekad mijenja i do 20% u jednome danu, mnogi zbog brze zarade i ulaze u ovu vrstu ulaganja.

Korištenje Bitcoina raste svake godine, mnogi potrošači žele iskoristiti prednosti kako bi povećali svoju prodaju i plaće radnika. Njegova vrijednost se određuje na temelju ponude i potražnje, stoga dolazi do visoke stope oscilacija cijene.

Bitcoin je decentralizirana digitalna imovina koja ljudima omogućuje besprijekoran prijenos bogatstva. Njegova stopa usvajanja trenutno je prilično spora zbog složenosti transakcija povezanih s blockchainom. Kriptovaluta je distribuirana knjiga koja se vodi na

zajedničkoj mreži. Njegova decentralizirana priroda čini ga sigurnim i otpornim na miješanje. Zbog sve veće popularnosti kriptovalute kao načina plaćanja, mnogi su trgovci počeli prihvaćati kriptovalute kao svoj glavni način plaćanja.

Na slici ispod može se vidjeti rast vrijednosti Bitcoina, gdje je vidljivo da je svakog mjeseca vrijednost rasla, a ako se usporede vrijednost na početku i na kraju, zabilježiti će se porast od 13 puta. Bitcoin je programiran na način da novi blok nastaje otprilike svakih deset minuta, a svaki je blok na početku imao nagradu od 50 novčića u prvih četiri godine postojanja Bitcoina, koja se nakon toga prepolovila na 25 nakon sljedećih četiri godine i tako na sve manje dijelove svakih četiri godina. Stoga, dokle god će rasti potražnja za Bitcoinom rast će i količina procesorske snage potrebne za rudarenje, a to znači da će Bitcoin kontinuirano povećavati težinu zadataka potrebnih da se otključaju nagrade za rudare, a sve s ciljem da osigura da proces kreiranja Bitcoina ostane na desetak minuta [16].



Slika 3. Kretanje cijene Bitcoina [9].

Bitcoin sustav osmišljen je imajući na umu zlato kao novac. Zlato je vrlo rijetko, i među ostalim zato se smatra vrijednim. I bitcoin je osmišljen tako da bude oskudan: zahtjevno ga je "rudariti", i jednako kao što s vremenom zlatni rudnik postaje sve više iscrpljen, sve je manje zlata u njemu i sve je više truda potrebno da se do zlata dođe, i "rudarenje" bitcoina s vremenom donosi sve manje nagrade. Svake četiri godine nagrada za "rudarenje" postaje dvostruko manja, te će 2140. godine (doduše, ako sustav do tada opstane) svi bitcoini (njih ukupno 21 milijun) biti izrudareni i više neće biti novih jedinica. Predviđa se da će do tada biti osmišljeni procesori koji će biti toliko snažni i energetski učinkoviti da će se troškovi mreže pokrivati iz naknada za transakcije.

Trenutno je nemoguće utvrditi broj korisnika Bitcoina jer jedan korisnik može imati više adresa. Japan je svakako vodeća zemlja kada se govori o usvajanju Bitcoina. Također, poznato je kako su neke od avio kompanija, trgovačkih lanaca i najpoznatijih kompanija počele prihvaćati Bitcoin kao valutu.

3.3.1.1. Ranjivost Bitcoina

Decentralizirano vlasništvo Bitcoin mreže štiti je od napada. Decentralizirani sustav može se bolje zaštititi od napada, ali nije potpuno neranjiv, što znači da su još uvijek mogući napadi na Bitcoin [18]. Istraživanja su pokazala da su rudari Bitcoina potrošili mnogo više na troškove električne energije i specijaliziranu opremu od ukupne vrijednosti Bitcoina koje su iskopali. Ovo istraživanje pokazalo je da su ljudi potrošili 17 milijuna dolara na rudarstvo, dok su nagrade iznosile 4,4 milijuna dolara. Kako bi se spriječio taj problem, rudari su se pokušali boriti protiv toga udružujući svoje resurse, stvarajući sinergiju za povećanje računske snage i dijeljenje većih nagrada [17].

Teoretski, udruživanjem ovakvih resursa entitet s dovoljnom računalnom snagom mogao bi kontrolirati većinu rudarstva (više od 50% iskorištavanja hash stope od strane jednog entiteta) i pritom preuzeti kontrolu nad mreže, a zatim imaju mogućnost manipuliranja blokovskim lancem, to se zove napad od 51%. To bi omogućilo poništavanje transakcija i trošenje istih Bitcoina više puta (inače poznato kao problem dvostruke potrošnje). Ovaj su problem međutim ublažili programeri protokola Bitcoin. Rudarstvo je već dizajnirano za stalno prebacivanje bazena, što sprječava bilo koju osobu da dobije 51% energije.

Mreža također zahtijeva šest potvrda svake transakcije u zasebnom bloku, što otežava vraćanje transakcija i njihovo potvrđivanje. To je, međutim, i dalje legitimna briga za Bitcoin. Računalna se tehnologija neprestano poboljšava, a problemi poput ovoga povećavaju motivaciju rudara Bitcoina da smisle načine napada na sustav i od njega profitiraju. Drugi problem s bitcoinima su transakcije prašine [18]. Transakcije prašine, poznate i kao napadi uskraćivanja usluge (DOS), napadi su koji prekidaju uslugu. U prošlosti je bilo moguće poslati više transakcija od minimalno 0,00000112 USD jednom korisniku, što bi ispunilo i napunilo blok lanac, učinilo ga prevelikom i srušilo mrežu. Programeri su ovaj problem riješili postavljanjem fiksnog ograničenja na količinu transakcija koje se mogu poslati jednom klijentu, ali još uvijek postoji rizik da talentirani hakeri koda sruše mrežu. Usprkos tome što su bitcoini i kriptovalute valute temeljene na kodu, uvijek postoji opasnost od napada temeljenih na kodu [19].

Bitcoin je bio u središtu kontroverzi za mnoge masovne digitalno povezane krađe. Primjer za to je Ovčja tržnica - tržnica koja je otvorena nakon gašenja crnog trga Puta svile. Web stranica je najavila narušavanje sigurnosti i na kraju nestalo s izgubljenim bitcoinima u vrijednosti od preko 40 milijuna dolara. Ljudi su nagađali da je web stranica od početka postavljena s lažnim namjerama kako bi korisnicima opljačkala njihove bitcoine. S obzirom na anonimnu prirodu sustava kriptovaluta, možda će biti nemoguće ući u trag tim lopovima. U Danskoj, procesoru plaćanja za Bitcoin, došlo je do sigurnosnih grešaka zbog kojih je tvrtka u to vrijeme izgubila 1 milion dolara vrijednih bitcoina [18].

Najveća međunarodna razmjena bitcoina na svijetu, Mt. Gox, također se odvila u rukama hakera. Budući da je Bitcoin *open source,* programeri neprestano dodaju nove značajke. Tijekom ovog procesa na površinu mogu izaći nove greške koje hakeri mogu iskoristiti za napad na mrežu. Iako mnogi ljudi pažljivo ispituju izvorni kôd prije izdanja, radi težeg uočavanja, još uvijek postoji mogućnost prolaska velikih sigurnosnih propusta [19]. Pad Mt. Gox, koja se u jednom trenutku smatrala vrhuncem trgovanja Bitcoinima, procjenjuje se da broji 70% globalnih transakcija kriptovaluta, primjer je opasnosti od napada na Bitcoin temeljenih na kodu i kriptovalute. Padom planine Gox „izgubilo“ se preko 800.000 bitcoina, a sve to zahvaljujući stručnjacima koji su napali Bitcoin pooću kodova. Prilikom pada planine Gox nije bilo entiteta ili financijskog regulatora koji bi došao u pomoć, čime je sav novac nestao bez načina da se vrati ili dobije bilo kakva podrška. Stoga, možemo zaključiti, da nema jamstva nakon gubitka što ukazuje na ozbiljan problem s bitcoinom i kriptovalutama. Ovaj napad najveća je krađa digitalne valute u povijesti. Stečajem najveće međunarodne burze

nestalo je bitcoina vrijednih stotine milijuna dolara. Učinak ovoga dovodi do problema koji dolazi s decentralizacijom [20]. Budući da je valuta dizajnirana da bude decentralizirana kako bi se spriječila bilo kakva smetnja, ona također nema jamstvo sigurnosti koje ima fiat valuta[2].

3.3.2. Ethereum

Sljedeća kriptovaluta je Enthereum (skraćeno ETH). Ruski programer Vitalik Buterin kreirao je Ethereum krajem 2013-te godine. Ethereum je blockchain platforma koja svakome omogućava izgradnju i korištenje pametnih ugovora. Aplikacije rade bez mogućnosti kašnjenja, prevare ili ulaska treće strane [21]. Spomenuta kriptovaluta ima puno istih značajki kao i Bitcoin, a to je da je digitalna valuta koja se može instantno poslati bilo kome u svijetu neovisno o mjestu gdje se nalaze.

U Ethereum je ugrađen poseban token *Ether* kojeg dobivaju rudari za nagradu što su vršili interakciju s blockchainom. Pametni ugovor se koristi kao naziv za program koji olakšava razmjenu novca, sadržaja, nekretnina itd. Kada se izvrši pametni ugovor na blockchain mreži on postaje program koji izvršava kada se zadovolje određeni preduvjeti.

Ethereum se definira kao stroj stanja. To znači da u bilo kojem trenutku postoji snimka svih stanja na računu i svih pametnih ugovora kako trenutno izgledaju. No, umjesto da prati samo stanje vlasništva valute, Ethereum prati prijelaze stanja skladišta podataka opće namjene, tj. spremište koje može sadržavati bilo koji podatak koji se može izraziti kao skup ključeva i vrijednosti [22]. Ethereum često nazivaju svjetskim računalom, jer se izvršavaju operacije koje su decentralizirane i ugrađene u blockchain te su samim time nezaustavljive. Takve aplikacije su napravljene od koda koji se pokreće i izvršava na blockchain mreži. Najveća prednost Ethereuma je njegova razvojna zajednica te široka primjena. Vjeruje se da je Ethereum pred širokom budućnosti te da će stvoriti mnoštvo korisnih informacija koje ćemo svi zajedno moći koristiti u budućnosti. Smatra se da će omogućavati kompliciranije aplikacije i veći broj transakcija te da će postajati sve sigurniji i brži. Ethereum zbog naglog rasta ima povećani broj skeptika i kritičara, ali privlači dosta ljudi jer napreduje brže od drugih kriptovaluta. Mnogi investitori vide potencijal i moć Ethereuma upravo u mogućnostima koje pruža pametni ugovor.

Bitcoin su zamislili kao digitalnu valutu, a kako bi se to realiziralo morali su izumiti blockchain tehnologiju. Kod Bitcoina se ona koristi samo za bilježenje transakcija, na tom se

[2] Sve poznate valute: kuna, euro, američki dolar, dinar i sl.

lancu upisuju samo transakcije, dok je Ethereum dizajniran da bude prilagodljiv pa se na njegovom lancu upisuju ne samo transakcije nego bilo kakav kod koji je moguće izvršiti.

3.3.3. Tether

Tether nije ni približno vrijedan kao Bitcoin i Ethereum, ali je ipak od svojeg osnutka pa sve do danas postao popularan kao kriptovaluta kojom se puno zamjenjuju druge kriptovalute. Tether ili skraćeno USDT je kriptovaluta stabilne vrijednosti, te samim time zbog svoje stabilnosti pruža sigurnost u vremenu kada je tržište nestabilno, što se veoma često zna dogoditi, te prema tome korisnici na tržištu zamjenjuju popularne valute za Tether, najviše se to odnosi na Tether vezan za američki dolar. Kada se pogledaju podaci o zamjeni Bitcoin-a i Ethereum-a s drugim kriptovalutama u mjenjačnicama kao primjerice Binance ili OKEx, na prvim mjestima je uvijek par BTC/USDT i ETH/USDT. Količina sredstava koja se zamjenjuje je daleko iznad bilo kojeg drugog para kriptovaluta [23]. Tether je kriptovaluta koja je stvorena da bude dovoljno stabilna u svojoj kupovnoj moći, a isto tako lako ju je objasniti običnim korisnicima. Tether je kriptovaluta s fiksnom cijenom koja se mjeri fiat valutom, odnosno valutom koju izdaje država.

3.3.4. IOTA

IOTA je kriptovaluta nove tehnologije jer ne koristi blockchain. Na tržištu je od 1. lipnja 2017. godine, koristi DAG tehnologiju koja omogućava transakcije bez troškova te offline transakcije. Kod ove tehnologije svaka pojedinačna transakcije stvori novi blok.

Karakteristike IOTE su:

- Nema provizije po transakciji – planirana je za IoT tržište gdje se transakcije provode između 2 uređaja, kako bi privukli korisnike ukinuli su proviziju jer je provizija jedan od najvećih problema u kripto svijetu.
- Neograničena skalabilnost – zbog dizajna Bitcoin mreže transakcije su spore, brzina transakcija raste s brojem korisnika u mreži. DAG tehnologija se ponaša suprotno od blockchain tehnologije, kod koje se skalabilnost smanjuje s brojem korisnika na mreži.
- Trenutačne transakcije – u teoriji brzina transakcije je trenutačna no zbog trenutnog broja korisnika to i nije tako, ako broj korisnika poraste, transakcije će se obavljati trenutačno.

3.4. Vrijednost kritpovaluta

Najveći izazov s digitalnom valutom je to što ju je vrlo lako stvoriti i reproducirati. Da bi imala vrijednost, valuta mora imati određene karakteristike. Stvaranje digitalne valute lakše je od ispisivanja. Središnje tijelo koje obrađuje transakcije i potvrđuje ih najbolji je način za izbjegavanje prijevara.

Peer-to-peer mreže su vrsta mreže koja omogućuje dvoje ljudi da komuniciraju i obavljaju transakcije bez potrebe za povezivanjem na zasebni poslužitelj. Bitcoin je također izgrađen na softveru otvorenog koda. *Peer-to-peer* mreže slične su mrežama otvorenog koda po tome što ih razvijaju pojedinci umjesto središnje figure. Bitcoin je uspio autentificirati transakcije putem svog decentraliziranog lanca blokova. Mnoge web stranice čuvaju kopiju lanca blokova koji se koristi za praćenje transakcija. Njegovo postojanje provjeravaju rudari. Budući da je prijenos novca digitalnim putem brži i sigurniji od korištenja fizičkog novca, također je teško spriječiti ljude da nose svoje bitcoin novčanike u druge zemlje. Potražnja za digitalnom valutom identificirana je kao razlog postojanja crnih tržišta. To je zato što se, za razliku od fiat novca, Bitcoin može koristiti za transakcije na tim tržištima. Put svile bio je internetsko tržište na kojem su korisnici mogli kupovati i prodavati kontrolirane tvari i ilegalne droge. Korisnici su mogli anonimno međusobno obavljati transakcije. Prema Christinovoj studiji, broj transakcija provedenih na platformi Puta svile povećan je nakon što ju je FBI isključio. Nagli skok cijene Bitcoina odmah je uslijedio nakon primjene zakona. Iako Bitcoin nije anoniman, njegovi vlasnici i dalje mogu sakriti svoje transakcije na razne načine, primjerice putem međunarodnih Bitcoin razmjena. Priroda mjenjačnica bitcoina zasnovanih na narudžbama omogućuje trgovanje kovanicama putem tržišnih naloga.

Prvu transakciju s bitcoinom izvršio je 19. veljače 2015. gospodin Gox u iznosu od 0,04951 USD. Tijekom siječnja dana 27.01. u 21:30sati, 2022. godine, cijena jednog bit coina je iznosila 245 169 kuna, ali ista je promjenjiva te u svakom trenutko može doći do porasta ili pada. U studenom 2013. Bitcoin je bio na vrhuncu, a u ožujku 2014. počeo je padati. Porast cijena bitcoina povezan je s nedostatkom ponude na tržištu. To je zato što Bitcoin ima potencijal riješiti probleme jednostavne reprodukcije i autentificirati transakcije.

4. SIGURNOST MOBILNOG POSLOVANJA U SVRHU TRGOVANJA KRIPTOVALUTAMA

Sigurnost je svakako vržo važan faktor mobilnog poslovanja, jer bez pouzdanosti i sigurnosti korisnik nema povjerenje u navedeno. Sigurnost je moguće sagledati kroz više aspekata, a najvažnije je svakako da su svi podaci na telefonu zaštićeni kako ne bi bili zlonamjerno upotrebljeni. Tako je poznato, kako blockchain može zaštititi sve aktivnosti vezane uz mobilno poslovanje i trgovanje kriptovalutama. Samim time, sigurnost blockchaina može se potvrditi pomoću 3 faktora:

Prvi faktor predstavlja kriptografija, sastoji s od određenog niza blokova, svaki blok sadržava skup transakcija koje su ostvarene u određenom vremenu. Svi paketi u lancima su logički povezani i imaju prethodni paket, kriptografski potpis koji se naziva *hash. Hash* prikazuje broj koji je ispisan u posebno određenom formatu te izgleda kao niz nasumično odabranih znakova. Primjer jednog *hash* broja: 7914ab1d9844d935f9d9b290c8258622. *Hash* prikazuje rezultat funkcija koje se primaju s jedne strane sav digitalni sadržaj poput teksta, fotografija, videozapisa, pdf-a ili bilo koje druge datoteke. Nad njima se izvršavaju razni nizovi matematičkih operacija te se kao rezultat vidi unikatni potpis koji je u obliku znakova točno određene duljine. *Hashevima* se ne može ukazati gdje je nastala promjena, ali se može dokazati da sadržaj knjige nije identičan, zbog razlike u *hashevima*.

Drugi faktor naziva se *Proof of work* ili dokaz rada, njime osoba koja želi može izmijeniti podatke u blockchainu i može preračunati sve *hashove* u jako kratkom vremenu, a on govori da *hash* mora započinjati s određenim brojem nula. Primjer jednog takvog je: 00000000000000000d9844d93707baf2435f9d9b290c8258622ab635054c8041. Svakom transakcijom *hash* se vrati isti, a kada on ne bi započinjao određenim brojem nula smatrao bi se neispravnim. U slučaju da se želi dobiti drugačiji *hash* mora se promijeniti sadržaj koji ulazi u njega. Svaki *hash* je nepredvidiv i zato ga računalo mora metodom pokušaja i pogađanja pronaći. Proces samog pogađanja naziva se *Proof of work.*

Treći faktor naziva se Distributivni sustav, konkretno u Bitcoin mreži svakog tko pronađe ispravan *hash* sustav nagradi bitcoinima. Osobe koje su u potrazi za *hashevima* nazivaju se rudari ili mineri, a svaki od njih u opticaj unosi nove bitcoine. Velika procesorska snaga računala i vrijeme uvjet su za pogađanje *hasha*. Svaki pronađeni *hash* govori da je blok podataka uspješno zatvoren te da rudari ili mineri objavljuju svoj pronalazak ostatku mreže,

dok će ostali sudionici, rudari ili mineri provjeriti i dodati novonastali blok na svoju kopiju blockchaina i tako ostvariti i sinkronizirati blockchain među računalima.

4.1. Novčanici za kriptovalute

Wallet ili novčanik prikazuje posebnu adresu koja ima mogućnost slanja i primanja raznih kriptovaluta. Svaki novčanik sprema privatni ključ, a privatni ključ potreban je kako bi se imao pristup adresi i svim novčanim sredstvima. Novčanik se sastoji od dva dijela:

1) Javni ključ – može se dijeliti s bilo kim bez ikakve brige

2) Privatni ključ – ne smije se dijeliti s nikim. Privatnim ključem vrši se prijenos vrijednosti i nju posjeduje samo vlasnik adrese.

Kako bi osoba došla do vlastitog novčanika postoji nekoliko načina:

- Generiranjem privatnog ključa i adrese uz pomoć programa blockchaina te željene valute,
- Korištenjem hardverskih rješenja, uređaja koja nalikuju na USB stiku (on sprema privatni ključ te može sadržavati više različitih adresa za različite valute),
- Otvaranjem računa u kripto mjenjačnici. Najjednostavniji oblik otvaranja je u mjenjačnici, jer mjenjačnice čuvaju svaki privatni ključ svakog korisnika, ali svakako je opasno duže držanje sredstava na takvom servisu.

Tri su vrste novčanika za kriptovalute i to: softverski, hardverski i papirnati.

Softverske novčanike možemo pronaći na desktopu, mobilnom ili pak web. Desktop novčanike možemo preuzeti na internetu ili ih instalirati na vlastito računalo. Kod novih novčanika treba obratili veliku pažnju i oprez, ne instalirati na bilo kojem računalu, ako dođe do backupa i zaboravi se privatni ključ sredstva postanu izgubljena. Ako dođe do kvara tvrdog diska također sredstva mogu biti potpuno izgubljena. Mobilni novčanici poput mnogobrojnih aplikacija na pametnim telefonima zapamte privatne ključeve i omogućuju direktno plaćanje putem uređaja.

Web ili *online* novčanici prikazuju specijalne internet stranice na kojima svako od nas može kreirati nalog koji šalje ili prima kriptovalutu. Takve novčanike kontrolira treća osoba i taj se oblik smatra najsigurnijim te je njihova prednost pristup na bilo kojem mjestu. Ako

implementacija nije dobra može se omogućiti organizaciji koja je u vlasništvu novčanika i upravlja ključevima, može upravljati novcem korisnika bez znanja i dozvole [24].

Hardverski novčanici prikazuju uređaje koji su nalik USB-u i na njima se čuvaju privatni ključevi, ako korisnik ima želju obavljanja transakcija na uređaju potrebno je samo unjeti zaštitni pin. Transakciju potpisujemo privatnim ključem koji se čuva na određenom uređaju. Ti uređaji imaju zaštitnu šifru od najčešće 12 ili pak 24 riječi, to nam služi u slučajevima kada dođe do gubitka uređaja kako bi povratili sredstva [24].

Papirnati novčanici imaju jako veliki nivo sigurnosti i na njima se izbjegava digitalno čuvanje valuta, ključ možemo prepisati na papir, a papir spremiti na tajno mjesto. Papir možemo spremiti gdje god poželimo da nije u doticaju s kamerama, tehnologijom, samo jedan pogled može dovesti do gubitka [24].

4.2. Transakcije

Transfer vrijednosti između dva digitalna novčanika naziva se transakcija, transakcija je registrirana u blockchainu, sustavu ulančanih blokova. Radi jedinstvenog sustava, Bitcoin transakcije izvršavaju se na jedinstven način. Svaka od transakcija sadrži ulaz i izlaz. Najčešće postoji jedan ulaz iz prethodne transakcije i više ulaza u kombinaciji manjih iznosa, a najviše dva ulaza kada je jedan zadužen za plaćanje a jedan za vraćanje promjene natrag pošiljatelju. [29] Sama transakcija ima uputu i naredbu javljati mreži da je njen korisnik dao ovlasti za prijenos kriptovalute drugom vlasniku, a novi vlasnik može na isti način kriptovalutu proslijediti trećem vlasniku, ili zadržati kriptovalutu u svojem vlasništvu. Kada se izlazi iz jedne u drugu transakciju tu transakciju može se koristiti kao prolaz kroz novu transakciju i time stvoriti lanac vlasništva. Lanac se stvara prijenosom kriptovalute s jedne na drugu adresu. Svaka transakcija kriptovaluta sadrži određene dokaze, dokaz o vlasništvu za sve količine kriptovaluta koja se vrijednost prenosi u obliku digitalnog vlastoručnog potpisa vlasnika.

Transakcije koje se prenose preko mreže nisu potvrđene sve dok ne postanu dio globalne mreže blockchaina, a ako se želi potvrditi vjerodostojnost transakcije potreban je proces verifikacije. Za svako rudarenje i verifikaciju potrebno je 10- ak minuta. Kako bi se izvršila transakcija, odnosno prebacivanje s jednog računa na drugi, potrebne su tri stvari: adresa ili javni ključ, privatni ključ te kriptografski potpis.

Adresa ili javni ključ (engl. *Public Key*) izmišljena je sedamdesetih godina i ona predstavlja matematičku osnovu koja je zaslužna za računalnu i informacijsku sigurnost. Glavna bit korištenja adrese ili javnog ključa je stvaranje ključnog para pomoću kojeg se kontrolira pristup kriptovalutama. Adresa je određena i generirana postupcima. Postupci izgledaju kao nasumična kombinacija slova i brojeva koji su jedinstveni te se također taj račun može povezati s više adresa ili javnih ključeva.

Privatni ključ (engl. *Private Key*) prikazuje broj koji je odabran slučajnim odabirom. U svako doba dana i noći korisnik može nadzirati svoje vlasništvo i kontrolirati privatni ključ. Privatni ključ korisnici upotrebljavaju kako bi stvorili potpis kojim se dokazuje vlasništvo nad sredstvima koji se koriste u transakcijama. Privatni ključ je tajni dio podataka pomoću kojeg se može dokazati pravo podnošenja kriptovaluta i vađenje iz određenog novčanika pomoću kriptografskog potpisa. U slučaju otkrivanja privatnog ključa drugim osobama dolazi do davanja kontrole nad kriptovalutama. Privatni ključ potrebno je što bolje zaštititi kao ne bi došlo do gubitka, jer u slučaju da dođe do gubitka, sredstva su zauvijek izgubljena.

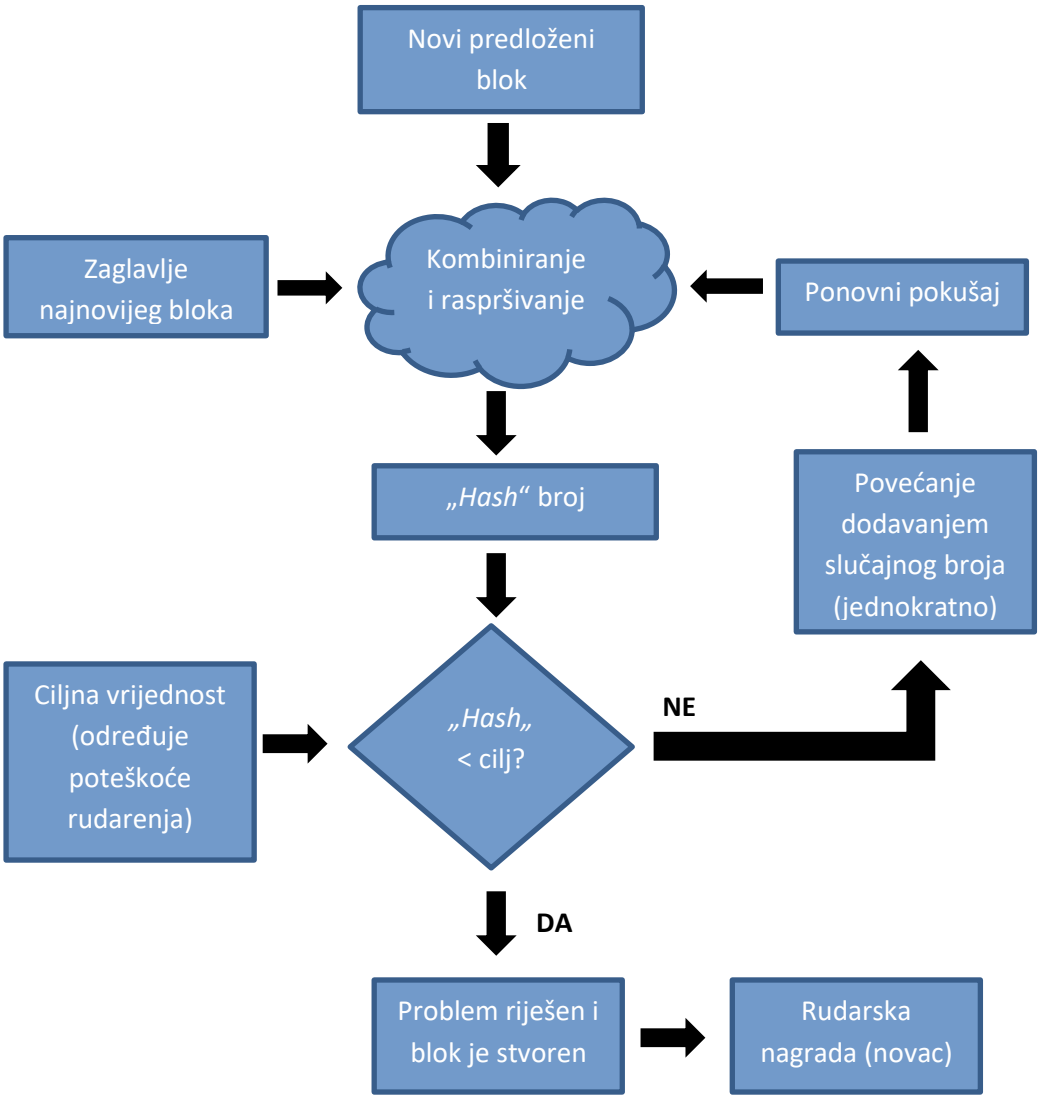
Kriptografski potpis predstavlja matematički mehanizam pomoću kojeg osoba može dokazati da su kriptovalute u njihovom vlasništvu te da je vlasnik adrese, odnosno novčanika. Kada dođe do transakcije pomoću odgovarajućeg privatnog ključa, mreža može vidjeti potpis vlasnika, ali ne i privatni ključ koji štiti cijeli račun.

4.3. Analiza procesa rudarenja kriptovaluta

Proces pomoću kojeg dolazi do stvaranja novih bitcoina i novčanih sredstava naziva se rudarenjem. Rudarenjem se osigurava cijeli sustav Bitcoina, kako bi se spriječile prijevare ili velike potrošnje. U zadnjih nekoliko godina, rudarenje je postala vrlo popularna opcija za zaradu. Rudarenje je način na koji se blok-lanac održava, odnosno način kojim se stvaraju novi blokovi iz novih transakcija koje se šalju iz čvorova diljem svijeta [30].

Kod procesa rudarenja, rudari imaju pred sobom teške matematičke zadatke koje moraju riješiti i predstaviti kao svoj dokaz. Onaj koji prvi riješi i predstavi svoj dokaz, taj ima pravo dodati novi blok i sve pripadne transakcije u lanac blokova, a za to je nagrađen određenim novčanim tj. Bitcoin iznosom. Proces rudarenja i stvaranja novog bloka prikazan je u nastavku slikom 4. U procesu se prvenstveno traži broj transakcija i predlaže se stvaranje novog bloka. Kao što je vidljivo slikom u nastavku novi predloženi blok povezan je sa zaglavljem nanovijeg bloka. U blockchainu, svaki blok mora uključivati hash broj prethodnog

bloka prije njega kako bi se osiguralo da su sve informacije dobro strukturirane u svim čvorovima mreže. Kada se generira hash broj, on se zatim uspoređuje sa hash ciljem. Cilj je generirati hash broj koji je manji ili jednak ciljanom hash. Ako je hash broj manji ili jednak hash cilju, zagonetka je riješena i blok se kreira, istovremeno nagrađujući rudara kroz novoizdani bitcoin. Ako je hash broj veći od ciljanog hashiranja, raspršena transakcija se povećava dodavanjem slučajnog broja (engl. *nonce*) i izračun se ponavlja. Ovaj proces se može nastaviti sve dok se ne pronađe hash broj manji od cilja [37].



Slika 4. Proces rudarenja [37].

Mehanizam rudarenja se zapravo temelji na dužini lanca tj. „duži lanac pobjeđuje“, a kako svi rudari nastoje rudariti na istom lancu tu se može pojaviti i lažni rudar koji želi dodati

lažni blok, kako bi on ostvario zaradu. [36] Proces rudarenja bitcoina može služiti u dvije svrhe. Prva svrha predstavlja stvaranje novih bitcoina pomoću rudarenja, količina bitcoina koja se stvara u bloku može biti fiksna, ali može se i smanjiti s vremenom. Druga svrha predstavlja stvaranje povjerenja kod rudarstva kroz osiguravanje transakcije, kako bi transakcije bile potvrđene snagom računala Ako računalo ima više blokova dolazi do većeg broja računanja, a i samog povjerenja.

Kada transakcija postane dio globalne distribucije knjige blockchain tek tada ona zapravo postaje potvrđena i njome se može rudariti svakih 10 minuta. Kada se primaju nove transakcije one se konstantno nakupljaju u mrežu korisničkog novčanika u tzv. bazen nepotvrđenih transakcija. Svi rudari bave se izgradnjom novih blokova te dodaju nepotvrđene transakcije iz bazena u blok prema određenima kriterijima transakcija.

Rudari uzimaju informacije koje su pohranjene u bloku i te informacije primjenjuju na matematičku formulu, a zatim informacije pretvaraju u nasumičan niz brojeva i slova (*hash*). Proces miniranja tj. stvaranja novih blokova izrađuju i pokreću rudari i ispunjavaju ga transakcijom te započinje izračunavanje dokaza za novi blok. Kako bi rudari osvojili „nagradu“ moraju pronači rješenje da blok bude valjan, te je nakraju svaki valjani blok dodan globalnom blockchainu. Svaki rudar može dobiti nagradu na dva načina: novi novčići stvoreni novim blokom ili transakcijske naknade od svih transakcija koje su uključene u blok. Kako bi rudari zaradili nove nagrade međusobno se natječu rješavajući teške matematičke probleme koji se temelje na kriptografi *hash* algoritmima. Usporedbe radi, Bitcoin novac prolazi kroz rudarstvo slično kao što banka tiskanjem novca izdaje novac.

Isto tako, svaki rudar može ostvariti zaradu kroz naknadu od svih transakcija i to predstavlja 0.5% ili manje prihode. Rudarenje je novi izum koji kriptovalute čini posebnim, ali i sigurnim mehanizmom. Rudari koji rade sami nemaju šanse za uspjehom, a vjerojatnost da će pronaći ispravan blok koji će nadoknaditi troškove električne energije i hardvera jednaka je gotovo nuli. Svi rudari sudjeluju zajedno kako bi formirali rudarske bazene te također zajedno dijelili nagrade, ali rudari tada dobivaju manji dio ukupne nagrade, a svakodnevno budu nagrađivani. Kada netko od rudara u bazenu minira blok tada nagrada bude podijeljena na sve rudare, ali svi rudari moraju pridonijeti tome. Tvrtka ili pojedinačni voditelj upravljaju rudarskim bazenom. Svaki rudar morao je uložiti određenu količinu novca u opremu, a povrat novca očekivan je kroz 6 do 10 mjeseci. Jedna od popularnih kriptovaluta

je Ethereum, popularna je iz razloga sto svaka osoba koja ima bolju grafičku karticu u svom kućnom računalu može rudariti i tako zarađivati [25].

Spominjujući blok lanac sustave, važno je spomenuti kako je blok-lanac tehnologija omogućila stvaranje financijskih sustava, gdje se transparentne i pouzdane financijske transakcije mogu izvršavati bez potrebe za posrednicima.

Kao i većina distribuiranih računalnih sustava, sudionici kriptovalutne mreže moraju se redovito dogovarati o trenutnom stanju blok-lanca, a to je ono što se naziva postizanjem konsenzusa. Postizanje konsenzusa na distribuiranim mrežama, na siguran i učinkovit način, nije lak zadatak. Najčešće primjenjeni algoritmi konsenzusa su *Proof of Work* i *Proof of Stake* koji su objašnjeni u nastavku.

4.3.1. Pregled *Proof of work* koncepta

Proof of work (PoW) ili „dokaz o radu“ opisuje sustav koji zahtijeva ne beznačajan, ali izvediv napor kako bi se spriječilo neozbiljno ili zlonamjerno korištenje računalne moći. *Proof of work* osigurava da korisnici ne troše novac koji nemaju pravo potrošiti. Većina glavnih kriptovaluta koristi PoW kao svoj algoritam konsenzusa. [29]. PoW čini osnovu i mnogim drugim kriptovalutama, dopuštajući siguran, decentraliziran konsenzus. Ovo objašnjenje će se usredotočiti na dokaz rada koji funkcionira u bitcoin mreži. Bitcoin je digitalna valuta koju podupire vrsta distribuirane knjige poznate kao "blockchain". Ova knjiga sadrži evidenciju svih transakcija bitcoina, poredanih u uzastopne "blokove", tako da nijedan korisnik ne smije dvaput potrošiti bilo koje svoje vlasništvo. Kako bi se spriječilo neovlašteno miješanje, knjiga je javna ili "distribuirana"; izmijenjenu bi verziju drugi korisnici brzo odbili.

Način na koji korisnici u praksi otkrivaju neovlašteno miješanje je raspršivanje (dugi nizovi brojeva koji služe kao dokaz rada). Stavlja se zadani skup podataka putem *hash* funkcije (bitcoin koristi SHA-256) i on će generirati samo jedan hash. Zbog "učinka lavine", čak i mala promjena bilo kojeg dijela izvornih podataka rezultirat će potpuno neprepoznatljivim raspršivanjem. Bez obzira na veličinu izvornog skupa podataka, raspršivanje generirano danom funkcijom bit će iste duljine. Raspršivanje je jednosmjerna funkcija što ne znači da se ne može koristiti za dobivanje izvornih podataka, već samo za provjeru mogu li se podaci podaci koju su generirali raspršivanje podudaraju s izvornim podacima. Budući da zadani skup podataka može generirati samo jedan raspršivač, rudari se brinu da generiraju raspršivanje ispod cilja na način da mijenjaju ulaz dodavanjem cijelog

broja, koji se naziva *nonce* ("broj koji se koristi jednom"). Nakon što se pronađe valjani *hash*, emitira se na mrežu, a blok se dodaje u blockchain.

Rudarstvo je natjecateljski proces, ali više je lutrija nego utrka. U prosjeku će svakih deset minuta netko generirati prihvatljiv dokaz rada, ali tko će to biti, može se samo pretpostaviti. Rudari se udružuju kako bi povećali svoje šanse za rudarske blokove, što generira transakcijske naknade i, ograničeno vrijeme, nagradu za novostvorene bitcoine.

Ono što se predstavlja kao mana proof-of-work algoritma je količina resursa koja se mora potrošiti za rudarenje. Za glavne kriptovalute uvjeti su izrazito izazovni, a sve to da se blokovi ne pronađu prebrzo [31]. Isto tako korisniku ili skupu korisnika također otežava monopoliziranje računalne snage mreže, budući da su strojevi i snaga potrebni za dovršavanje funkcija raspršivanja preskupi. Dokaz rada zahtijeva da se računalo nasumično uključi u funkcije raspršivanja dok ne dođe do izlaza s ispravnom minimalnom količinom vodećih nula. Na primjer, hash za blok #660000, miniran 4. prosinca 2020. je 000000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6. Nagrada bloka za taj uspješni raspršivač bila je 6,25 BTC.

4.3.2. Pregled *Proof of stake* koncepta

Proof of stake (PoS) kaže da osoba može rudarati ili potvrđivati blok transakcije prema broju novčića koje ima. To znači da što više kovanica posjeduje rudar, to ima više rudarske moći. *Proof of stake* koristi pseudo slučajni postupak za odabir čvora koji će biti verifikator sljedećeg bloka, na temelju kombinacije čimbenika koji mogu uključivati starost udjela, slučajnost i vrijednost čvora [32]. Kriptovalute koje koriste *proof of stake* često započinju prodajom prethodno rudarenih kovanica ili se pokreću s algoritmom *proof of work*, a kasnije prebacuju na *proof of stake.* Trenutačno samo *altcoini* koriste koncept dokaza udjela odnosno *proof of work.*

Svaka kriptovaluta koja koristi *proof of stake* algoritam ima svoj skup pravila i metoda kombinacija za rudarenje. Kada se transakcija pokrene, podaci o transakciji ugrađuju se u blok s maksimalnim kapacitetom od 1 megabajta, a zatim se dupliciraju na više računala ili čvorova u mreži. Čvorovi su administrativno tijelo blockchaina i provjeravaju legitimnost transakcija u svakom bloku. Da bi izveli korak provjere, čvorovi ili rudari trebali bi riješiti računalnu zagonetku, poznatu kao dokaz problema rada. Prvi rudar koji dešifrira svaki

problem transakcije bloka nagrađuje se novčićem. Nakon što je blok transakcija verificiran, dodaje se u blockchain, javnu transparentnu knjigu. Rudarstvo zahtijeva veliku računalnu snagu za izvođenje različitih kriptografskih izračuna za otključavanje računalnih izazova. Računska snaga pretvara se u veliku količinu električne energije i snage potrebne za dokaz rada. *Proof of stake* (PoS) nastoji riješiti ovo pitanje pripisujući rudarsku moć udjelu kovanica koje drži rudar. Na ovaj način, umjesto da koristi energiju za rješavanje PoW zagonetki, PoS rudar je ograničen na rudarstvo postotka transakcija koje odražavaju njihov vlasnički udio. Na primjer, rudar koji posjeduje 3% dostupnih kovanica teoretski može minirati samo 3% blokova. Bitcoin koristi PoW sustav i kao takav je osjetljiv na potencijalnu tragediju zajedničkog dobra. Tragedija zajedničkog dobra odnosi se na buduće razdoblje u kojem će biti dostupno manje rudara bitcoina zbog male ili nikakve blok nagrade od rudarenja. Jedine naknade koje će se zaraditi dolazit će od transakcijskih naknada koje će se s vremenom također smanjivati jer se korisnici odlučuju plaćati niže naknade za svoje transakcije.

S manje rudara nego što je potrebno za kovanice, mreža postaje ranjivija na napad od 51%. Napad od 51% je kada rudar ili rudarski bazen kontrolira 51% računalne snage mreže i stvara lažne blokove transakcija za sebe, poništavajući transakcije drugih u mreži. S PoS -om, napadač bi trebao pribaviti 51% kriptovalute za izvođenje napada od 51%. Dokaz udjela izbjegava ovu „tragediju“ čineći je nepovoljnom za rudara s 51% udjela u kriptovaluti za napad na mrežu. Iako bi bilo teško i skupo prikupiti 51% uglednog digitalnog novčića, rudaru s 51% udjela u novčiću nije u najboljem interesu napasti mrežu u kojoj drže većinski udio. Ako vrijednost kriptovalute padne, to znači da bi pala i vrijednost njihovih udjela, pa bi vlasnik većinskog udjela bio više potaknut na održavanje sigurne mreže. Osim Bitcoina, Litecoin (LTC) također koristi PoW metodu. Nxt (NXT) je primjer kriptokoina koji koristi PoS metodu. Neki novčići poput Peercoina (PPC) koriste mješoviti sustav u koji su uključene obje metode. Trenutno je Ethereum (ETH) u procesu prelaska na PoS sustav [23].

4.4. Krađe, prevare i nezakonito postupanje s kriptovalutama

Krađe kod kriptovaluta uključuju neke od najčešćih vrsta kibernetičkog kriminala i to: krađa identiteta, napadi na lanac opskrbe i hakiranje računala. Postoji mnogo vrsta opcija novčanika za kriptovalute, od kojih svaka ima svoje jedinstvene sigurnosne značajke. To uključuje slojeve hardvera i softvera. Novi podvizi koji ciljaju na određene transakcije događaju se prilično često. Jedan od njih je problem savitljivosti transakcija s Bitcoinom.

Jedna od osoba koju se povezuje uz prevaru vrijednosnih papira je Joshua Garza, bivši izvršni direktor ZenMinera i GaW Minersa, osuđen na zatvorsku kaznu 2015. godine nakon što se izjasnio krivim za prijevaru putem žice. Godine 2018. pokrenuta je grupna tužba protiv BitConnecta, koji je optužen za rad na lažnoj shemi. Platforma je bila poznata po svojim mjesečnim isplatama. Promotori BitConnecta preusmjerili su više od 2 milijarde dolara ulagačkih sredstava u svoje osobne digitalne novčanike, prema američkom SEC -u. Tvrdili su da koriste bot za trgovanje kriptovalutama kako bi obećali zajamčeni povrat ulaganja. OneCoin je bila višerazinska marketinška Ponzi shema koja je prevarila ulagače diljem svijeta. Izvelo ga je nekoliko ljudi.

4.4.1. Napadi zločudnim softverom

Vrsta Mac zlonamjernog softvera poznata kao Bitvanity otkrivena je 2013. godine, a ukrala je privatne ključeve i adrese od drugih klijenata za bitcoin. Druga varijanta poznata kao *CoinThief* također je bila odgovorna za više krađa Bitcoina. U veljači 2014. objavljeno je da je virus koji potječe iz Pony botneta ukrao kriptovalute u vrijednosti od preko 220.000 dolara, uključujući Bitcoin. Iznos je bio ekvivalentan oko 26.000 dolara po novčaniku. U ovom slučaju zlonamjerni softver krade privatne ključeve iz bitcoin novčanika.

CryptoLocker je vrsta *ransomwarea* koji se širi putem krađe identiteta putem elektroničke pošte. Traži plaćanje otkupnine u Bitcoinu kako bi se otključalo zaraženo računalo. U studenom 2013. policija u Massachusettsu platila je otkupninu od 2 Bitcoina kako bi riješila slučaj koji uključuje hakera koji je upotrijebio valutu za krađu novca od policije. Od lipnja 2018. većina napada *ransomwarea* izvedena je putem Monera, kriptovalute koja je vrlo privatna i teško joj ući u trag.

4.4.2. Neovlašteno rudarenje

U lipnju 2011. Symantec je upozorio na mogućnost da bi botneti mogli tajno rudariti za bitcoine. Zlonamjerni softver koristio je mogućnosti paralelne obrade grafičkih procesora ugrađenih u mnoge moderne video kartice. Iako je prosječno računalo s integriranim grafičkim procesorom gotovo beskorisno za rudarenje bitcoina, deseci tisuća računala opterećenih rudarskim zlonamjernim softverom mogli bi dati tražene rezultate. Sredinom kolovoza 2011. otkriveni su botneti za rudarenje bitcoina, a manje od tri mjeseca kasnije trojanski rudari za bitcoin zarazili su Mac OS X. U travnju 2013., elektronička sportska

organizacija E-Sports Entertainment optužena je za otmicu 14.000 računala za miniranje bitcoina.

Njemačka policija uhitila je dvije osobe u prosincu 2013. koje su prilagodile postojeći softver botneta za izvođenje bitcoina, za koje je policija rekla da su korištene za miniranje bitcoina u vrijednosti od najmanje 950.000 dolara. Četiri dana u prosincu 2013. i siječnju 2014. Yahoo! Europa je bila domaćin oglasa koji sadrži zlonamjerni softver za rudarenje bitcoina koji je zarazio oko dva milijuna računala. Softver, nazvan Sefnit, prvi je put otkriven sredinom 2013. godine i isporučen s više različitih programskih paketa. Microsoft je uklanjao zlonamjerni softver kroz Microsoft Security Essentials.

Dana 20. veljače 2014. članu Harvardske zajednice oduzet je pristup univerzitetskim istraživačkim računalnim objektima nakon što je uspostavio rudarsku operaciju Dogecoin pomoću istraživačke mreže Harvard, prema internoj elektronskoj pošti koju je poslao Fakultet znanosti i umjetnosti Službenici za istraživanje računalstva. Ars Technica izvijestila je u siječnju 2018. da oglasi na YouTubeu sadrže JavaScript kôd koji je iskopao kriptovalutu Monero.

4.4.3. Phishing

Web stranica koja je uspijela generirati privatne pristupne fraze IOTA novčanika i prikupila ključeve otkrivena je u siječnju 2018. Procjenjuje se da je ukradeno do 4 milijuna dolara žetona. Michael Terpin, izvršni direktor blockchain tvrtke Transform Group, tužio je Ellis Pinsky 2020. godine zbog vođenja sofisticirane kampanje kibernetičkog kriminala koja je ukrala više od 24 milijuna USD u kriptovaluti. Također je dobio sličnu tužbu protiv Nicholasa Truglie 2019. 15. srpnja 2020. hakirani su računi istaknutih pojedinaca i tvrtki, uključujući Elona Muska, Joea Bidena i Baracka Obamu. Napadači su pomoću računa slali poruku za slanje bitcoina u bitcoin novčanik.

Bitcoin je postao sastavni dio svjetskog financijskog krajolika. Njegova decentralizirana priroda i brojne prednosti privukle su pozornost lovaca i ulagača. Bitcoin prevare postale su sve prisutnije kako je cijena kriptovalute rasla. Koristili su ga za transakcije i postali neprivlačan izbor za ulaganje. Priroda Bitcoin-ovih prijevara također je paralelna s evolucijom njegove infrastrukture. Rast cijena Bitcoina u 2017. promijenio je prirodu mnogih prijevara koje su se dogodile unutar mreže. Većina su to bili od strane *Initial coing offering-a*

(ICO) koje je američka Komisija za vrijednosne papire i burze uglavnom nije regulirala. Zbog porasta Bitcoina i njegove decentralizirane prirode, hakeri su svoju strategiju preusmjerili na novčanike kriptovaluta. Jedna od njihovih najpopularnijih metoda je krađa identiteta. Prevare su neophodne za evoluciju Bitcoina jer mogu identificirati različite slabosti u njegovoj mreži. Oni će postati sve sofisticiraniji kako se bitcoin ekosistem povećava.

U nastavku je kratak pregled pet važnih bitcoin prijevara koje su se posljednjih godina infiltrirale u njegov ekosustav [16]:

- **Prevara pri razmjeni i krađa novčanika** - Burze kriptovaluta nekada su bile glavni izvori bogatstva za hakere. Međutim, u posljednjih nekoliko godina preusmjerili su svoju pozornost na druga područja, poput internetskih novčanika.
- **Prevara putem društvenih mreža** - Zbog porasta društvenih medija, hakeri su ciljali vlasnike Bitcoina. Oni su stvorili lažne račune kako bi im ukrali Bitcoin. U srpnju 2020. hakirano je nekoliko računa na Twitteru, uključujući one istaknutih pojedinaca poput Elona Muska, Warrena Buffetta i Floyda Mayweathera. Nakon što su dobili pristup tim računima, hakeri su tvitali o doniranju novca na određenu adresu blockchaina. Nekoliko minuta nakon što su poruke objavljene, transakcije su pokrenute. Osim toga, YouTube je također patio od Bitcoin prijevara. U srpnju 2020. godine, Steve Wozniak, suosnivač Applea, podnio je tužbu protiv Googlea nakon što su njegovi razgovori o Bitcoinu predstavljeni u videu o darivanju kriptovaluta.
- **Prevare društvenog inžinjeringa** - Prevare društvenog inženjeringa koriste hakeri za krađu informacija od svojih žrtava. Na primjer, phishing je uobičajena tehnika koju hakeri koriste za krađu osjetljivih podataka od svojih žrtava. Phishing prijevare kripto novčanika postaju sve prisutnije. Uglavnom su usredotočeni na informacije o privatnim ključevima internetskih novčanika. Bitcoin ucjena tehnika je društvenog inženjeringa koju koriste hakeri za krađu privatnih podataka od korisnika. Šalju elektronsku poštu s prijetnjama za otkrivanje njihovih privatnih podataka. Kako ne bi bili žrtve phishing prijevara, korisnici bi trebali izbjegavati klikanje na veze u elektorniskim poštama koje sadrže veze na lažne web stranice.
- **Prevare temeljene na ponudi** - ICO prevare su se pojavile tijekom naglog rasta i potražnje kriptovaluta. Učestalost ovih lažnih aktivnosti smanjila se nakon provedbenih radnji DIP -a. Prevare su se odvijale izradaom lažnih web stranica i slanjem elektronskih poruka koje izgledaju kao da su s ICO -a. Kada takve radnje DIP

regulatori uhvate, obično kažnjavaju promicatelje i osnivače takvih pothvata. To uključuje uhićenje, pa čak i zatvorsku kaznu.

- **DeFi prevare** - Decentralizirano financiranje ili DeFi prijevara je koja pogađa tržišta kriptovaluta. Razvoj DeFi platformi ima svoj niz problema. Hakeri su se uspjeli infiltrirati u te mreže i ukrasti sredstva investitora. Hakeri obično koriste pametne ugovore za krađu sredstava od Bitcoina. Kad ugovor ima postavljeni prag, obično koriste programske funkcije kako bi to iskoristili. U prosincu 2020. hakeri su ukrali milijune dolara s mjenjačnice kriptovaluta poznate kao Compounder Finance. Projekt je obećao investitorima veći povrat nego što bi oni dobili od tradicionalnih ulaganja. Međutim, nisu mogli zadržati svoja sredstva do isteka pametnog ugovora [16].

5. ZNAČAJKE I UTJECAJI MARKETINŠKIH PROCESA U TRGOVANJU KRIPTOVALUTA

Na razvoj platnog prometa uvelike je utjecao porast digitalnih valuta i blockchaina. Budućnost tehnologije plaćanja leži u rukama ljudi koji koriste mobilne uređaje i računala. Glavna knjiga (blockchain) ili lanac svih blokova pokazuje podatkovni blok koji je povezan u jednosmjerni lanac u kojem se nalazio svaki blok ovisno od vrijednosti najstarijeg bloka. Blokovi se povezuju na temelju kriptografije, a ona je bitna zbog sigurnosti i privatnosti. Blockchain se može proučavati kao knjiga koju nije moguće uređivati nakon što se podaci jednom upišu u nju.

Dalje, e-trgovina je bila odgovorna za više od 3,53 bilijuna prodaje u 2019. S ovim snažnim rastom očekuje se da će doseći 5,69 bilijuna dolara do 2022. godine, što predstavlja očekivani rast prodaje od 61%. 2021. godine više od 72% prodaje e-trgovine ostvarivat će se s mobilnih uređaja. Ovaj rezultat svakako je posljedica sve veće popularnosti mobilnih platformi poput Facebooka i Googlea. Iako je brzi razvoj trgovine promijenio način na koji ljudi trguju, većina prodaje i dalje se odvija tradicionalnim metodama. Osim toga, što se tiče načina plaćanja a usko je vezano uz transakcije, većina ustanova i dalje koristi kombinaciju kreditnih i debitnih kartica.

U zemlji poput Koreje za obavljanje bilo kakve transakcije najviše se koriste novčanici s više kriptovaluta, te se kao takve smatraju potpuno sigurnim i brzim među korisnicima. O njegovoj pouzdanosti i praktičnosti svjedoči broj lokacija koje ga trenutno provode. S vremenom se očekuje da će upravo plaćanja kriptovalutama stvoriti gospodarstvo bez granica i globalizaciju. Također, transakcije kriptovalutama pomažu u borbi protiv financijske nejednakosti pružajući ljudima brži i siguran pristup financijskim uslugama.

5.1. Kriptovalute u međunarodnoj trgovini

. Iako je razvoj digitalne tehnologije pojedincima omogućio plaćanje robe i usluga, još uvijek nije jasno hoće li kriptovalute postati glavni način plaćanja za pravne osobe. O tome svjedoči interes mnogih pojedinaca za aktivno sudjelovanje u transformaciji međunarodnog poslovanja.

5.1.1. Primjena kriptovaluta u međunarodnoj trgovini

Najizravnija prilika u međunarodnoj trgovini predstavljena je u obliku internetskih plaćanja. Glavni izazov internetskih plaćanja leži u tome što su te transakcije podložne prijevari. Poznato je kako se većinu vremena transakcije s pojedincima obavljaju putem banke ili trgovca. Međutim, nema razloga zašto shema plaćanja ne bi uključivala upotrebu kriptovaluta. I *Mastercard* i *Visa* otvaraju svoje novčanike kako bi korisnicima omogućili obavljanje transakcija. Ugovorne strane dogovaraju se o tome koja će usluga internetskog plaćanja prihvatiti kriptovalutu, a transakcija se obavlja baš kao i standardna bankovna transakcija.

Kriptovaluta koju podržava država imala bi dobre temelje za korištenje u međunarodnom poslovanju. Umjesto korištenja Bitcoina, ljudi bi mogli slati novac jedni drugima putem mobilnog novčanika. Sustav bi koristio blockchain tehnologiju za upravljanje varijacijom glavne knjige, koja bi se razlikovala od trenutne metode prijenosa novca.

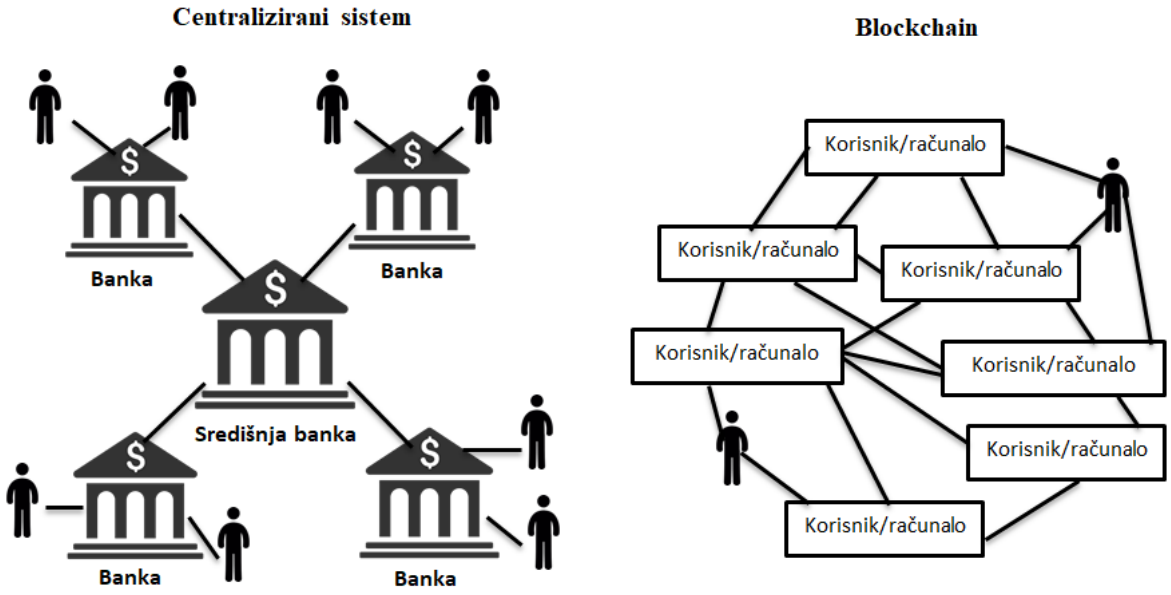
Izvješće koje je objavio Kuvajtski financijski centar govori o mogućnosti korištenja Bitcoina za prodaju nafte. U izvješću se napominje da bi ova metoda mogla biti korisna za zaljevsko gospodarstvo jer bi potrošačima omogućila transakcije bez korištenja američkog dolara.

Poznato je kako postoji transportni sustav koji koristi kriptovalute. Stručnjaci navode da se spomenuti sustav riješiti jedan od najvećih izazova u industriji, misleći na nedostatak povjerenja korisnika. Australijska Commonwealth banka i Wells Fargo 2016. godine postale su prve banke koje su uspješno prekogranične trgovine pamukom koristile blockchain tehnologiju. To nije puki izum koji može promijeniti način na koji se odvija međunarodna trgovina. Ima sposobnost pružiti platformu za primjenu različitih tehnoloških smjerova. To će omogućiti stranim ulagateljima da kupuju nekretnine koristeći Etherium. Bitcoin je za sada još uvijek udaljen od korištenja u *business to business* (B2B) tržištu. U nekim zemljama se već sada kriptovalute koriste umjesto *Western Uniona* i *Paypala* za primanje manjih plaćanja [18].

5.1.2. Sigurnost transakcija u međunarodnom poslovanju

Tehnologija transakcija kriptovalutama detaljnije se razmatra u ovom dijelu rada. Blockchain je okvir koji omogućuje nesmetano izvršavanje transakcija, a njegovu sigurnost i pouzdanost priznaju mnoge velike korporacije.

Postoje i slučajevi u kojima se sigurnosni spektar može promatrati s pozitivne strane. Na primjer, Falcon Private Bank, koja je bila prva banka u Švicarskoj koja je svojim klijentima omogućila kupnju i prodaju Bitcoina, dobila je potrebno regulatorno odobrenje od Švicarske uprave za financijsko tržište (FINMA) [33]. Također, jedna od najvećih ruskih banaka odlučila je koristiti blockchain temeljen na Ethereumu i sve to radi poboljšanja sigurnosti i ubrzanja transakcija [34]. Blokchain tehonologija nastaje na način da se više zapisa o transakcijama zajedno povežu u zasebne blokove zapisa. Na slici u nastavku prikazana je razlika između tradicionalnih banaka i blockchaina radi lakšeg razumijevanja.



Slika 5. **Razlika između tradicionalnih banaka i blockchain tehnologije [38]**

Kako bi se nova transakcija dodala u određeni blok zapisa, ona treba imati veći broj neovisnih potvrda o valjanosti zapisa. To bi značilo da više korisnika mora potvrditi valjanost zapisa. Potvrdu o valjanosti zapisa nije jednostavno izvesti. Ona sa sastoji od niza matematičkih jednadžbi za čije rješavanje potrebno imati, ranije spomenuto, vrhunsko računalo i puno potrošnje električne energije.

Unatoč svemu spomenutom, još uvijek nije sigurno koristiti kriptovalutu. Glavni razlog nesigurnosti kriptovalute pridonosi priroda njihovih transakcija koja se jako razlikuju od drugih oblika plaćanja. Slučaj Mt.Gox, koji je uključivao američke savezne agente koji su optuživali Alexandera Vinnika za krađu više od 800.000 bitcoina, postao je jedan od najistaknutijih primjera neizvjesnosti oko bitcoina. Osim toga, zabilježeni su i česti slučajevi mikro prijevara što korisnicima govori koliko su kriptovalute nesigurne [19].

5.1.3. Utjecaj kriptovaluta na ekonomiju

Budući da se cijene kriptovaluta iz godine u godinu uvelike razlikuju, tržišni udio globalnog novca u kriptovalutama stalno se mijenja, pa je početkom 2018. godine tržište kriptovaluta bilo veće od tržišta popularnih tvrtki *Amazon* i *Facebook* [23]. Također, 2016. godine tržište kriptovaluta vrijedilo je 11,3 milijarde američkih dolara, a samo godinu dana kasnije poraslo je čak 15 puta. Iz spomenutih podataka može se zaključiti da je tržište kriptovaluta vrlo je nestabilno i postaje svake godine sve veće i veće, a isto tako porastom potražnje za digitalnim valutama raste i interes vlada i banaka za uvođenje novih digitalnih valuta. Na primjer, kineska vlada trenutno testira digitalnu verziju svoje valute. Kineska digitalna valuta kojom upravlja vlada omogućila bi joj kontrolu novčanih tokova koji nisu vezani za fizički novac. Ovo je ključni korak u uspostavljanju veće kontrole nad financijskim sustavom zemlje.

U Hrvatskoj se trgovanje kriptovalutama oporezuje 12%. U većini slučajeva, ako osoba koristi kriptovalutu više od 2 godine, ne mora platiti porez. Facebook planira lansirati kriptovalutu pod nazivom Libra, koja bi bila povezana sa stabilnom cijenom. Libra je blockchain projekt koji će omogućiti sigurne i brze transakcije. Njegovi programeri su iz raznih tvrtki kao što su *Mastercard, Visa* i *Paypal*. Zbog krize u Venezueli, prosječna stopa inflacije u zemlji je oko tisuću posto godišnje. Za usporedbu, u Europskoj uniji prosječna stopa inflacije iznosi 2 posto. U drugim zemljama, poput Brazila, kriptovalute postaju alternativni način plaćanja zbog nepovjerenja u bankarski sustav i visokih naknada. U praksi kriptovalute ne pružaju dobru alternativu za pohranu vrijednosti. Kriptovalute kao način plaćanja iako postaju sve popularnije, njihova decentralizirana priroda i dalje ostaje glavni razlog zašto nisu toliko prihvaćene kao način plaćanja. Zbog svojih tehničkih ograničenja ovaj način plaćanja još uvijek nije idealan za svakodnevne transakcije [17].

Osim toga, dokazana je teorija da Blockchain transakcije ne drže vodu. Zbog svoje velike modularnosti, za učinkovitu obradu transakcija potrebna je velika količina resursa za obradu. Budući da Bitcoin blockchain obrađuje samo 4,6 transakcija u sekundi, jamči izvršavanje samo 4 transakcije u sekundi. Drugim riječima, mnogo je brži od *Vise*. Moderni blockchaini mogu značajno povećati brzinu transakcija. Na primjer, Ethereum postiže brzinu od 4,996 transakcija u sekundi. U slučajevima velikih transakcija, poput događaja Crnog petka, važno je da je procesorska snaga potrebna za dovršetak transakcija velika.

Zbog količine električne energije utrošene za rudarenje bitcoina, procjenjuje se da je prosječna godišnja potrošnja električne energije ekvivalentna potrošnji električne enrgije u državi Alžiru gdje je potrošnja električne energije u cijeloj državi u godinu dana oko 60 TWh. Ovaj iznos je dovoljan za napajanje cijele zemlje. Zbog brzog razvoja blockchaina, bilo je moguće pronaći način za rješavanje problema skaliranja i velike količine potrošnje električne energije. Međutim, u ovom trenutku kriptovalute se ne smatraju praktičnom alternativom tradicionalnim kartičnim transakcijama.

Štoviše, nestabilnost kriptovaluta veća je nego kod ostalih financijskih instrumenata. U 2015. godini indeks S&P 500 dosegao je vrhunac od oko 2.000 američkih dolara. S&P 500 jedan je od široko korištenih financijskih instrumenata koji pokazuje kako cijena određene dionice prati veliki dio tržišta. Čak i ako cijena jedne od dionica padne, spomenuti indeks i dalje pokazuje dugoročni pozitivan trend. Iste godine cijena Bitcoina porasla je na preko 20.000 američkih dolara. U samo posljednjih pola godine cijena mu je varirala između 3858 i 10 američkih dolara. Glavni razlog zašto Bitcoin ima tako velike oscilacije je taj što ne prati unutarnju vrijednost financijskog instrumenta, koja se često naziva "fer" ili "stvarna" vrijednost poduzeća. Unutarnja vrijednost poduzeća može se odrediti analizom njegovih financijskih izvještaja. Obično se određuje količinom novca koju tvrtka godišnje zaradi. Jedina stvar koja Bitcoinu daje unutarnju vrijednost je njegova rudarska oprema. Unatoč tome, cijena Bitcoina nije se značajno promijenila tijekom godina.

Na primjer, vijest o integraciji Bitcoin emotikona u Twitter -ovu platformu dovela je do toga da je cijena Bitcoina u roku od 10 dana porasla sa 9333 na 10347 američkih dolara. Nasuprot tome, vijesti o pokretanju emotikona na društvenoj mreži Twitter ne mogu imati negativan utjecaj na cijenu Bitcoina, jer i dalje mogu dovesti do povećanog optimizma u pogledu budućnosti kriptovalute. [26].

5.1.4. Prednosti i mane plaćanja kriptovalutama u međunarodnom poslovanju

Iako mnoge tvrtke već koriste kriptovalute za međunarodno poslovanje, još nije jasno hoće li moći imati značajnu korist od ove tehnologije. Bez obzira na valutu jedinstvena vrijednost omogućiti će tvrtkama neometano obavljanje poslova i one će izbjeći rizik slučajnog izlaganja tečaju vrijednosti. Osim toga, moguće je stvoriti dodanu vrijednost korištenjem određenih strategija i metoda, ali također to može stvoriti nesigurnost u pogledu smanjenja državnog deficita i nestabilnosti financijskog tržišta. Zbog prirode kriptovaluta, tvrtkama nije lako poslovati s njima. Također, njihova nestabilnost i neizvjesnost mogli bi stvoriti negativan utjecaj na poslovno okruženje bilo kojeg poduzeća ili organizacije.

U početku je nekolicina ljudi ozbiljno shvaćalo kriptovalute. Osim što mogu poremetiti postojeći bankovni sustav, imaju i potencijal za demokratizaciju pristupa informacijama. Potencijalni utjecaj blockchaina je ogroman, pa se vjeruje u to da bi on, radi svoje decentralizirane prirode mogao promijeniti način pružanja financijskih usluga.

Poslovna klima u Hrvatskoj sporo usvaja nove tehnologije, što je dijelom posljedica dobne strukture zemlje. Glavna prepreka razvoju trgovine i ulaganja je pretjerana regulacija. Zbog sve veće popularnosti kriptovaluta u Hrvatskoj, dopušteno je osnivanje nekoliko bitcoin bankomata u različitim gradovima. Čini se da je uporaba kriptovaluta za ublažavanje sukoba i građanskih nemira idealno rješenje za probleme uzrokovane raznim svjetskim sukobima i ratovima. Velika količina imovine u kriptovalutama omogućuje tvrtkama da osiguraju svoju poziciju u sve nestabilnijem svijetu. Međutim, također je neizbježno znati da će se možda vrijednost kriptovaluta na kraju srušiti [20].

6.ANALIZA KORIŠTENJA MOBILNIH UREĐAJA U SVRHU RUDARENJA I TRGOVANJA KRIPTOVALAMA

U ovom dijelu rada prikazano je anketno istraživanje na temu kriptovaluta i mobilnih uređaja. Istraživanje je potpuno anonimno a provedeno je u Republici Hrvatskoj. Cilj ankete je prikupiti stavove od ispitanika o kriptovalutama, te saznati koriste li mobilne uređaje u svrhu trgovanja i rudarenja kriptovaluta ili u neke druge svrhe.

6.1. Metodologija istraživanja

Anketni upitnik sadržavao je 16 pitanja, gdje su najprije bila sociodemografska pitanja, a nakon toga i pitanja vezana uz temu istraživanja. Anketa je kreirana u Google Docs alatu proslijeđena putem Facebook stranice i elektroničke pošte. Anketu je ispunilo ukupno 70 ispitanika, razne životne dobi. Dobro je spomenuti kako je ovo istraživanje provedeno pomoću vlastitih sredstava zbog čega je istraživanje provedeno na manjem dijelu populacije (prigodni uzorak), što predstavlja temeljno ograničenje istraživanja. Ciljana populacija za provedbu ankete su građani grada Zagreba, životne dobi iznad 18 godina.

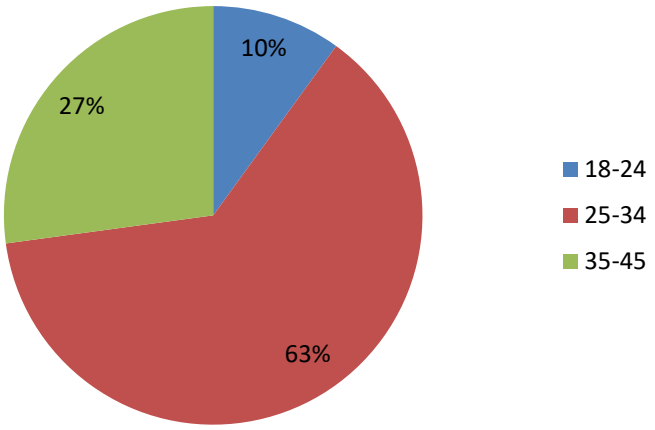
Istraživanje je provedeno tijekom listopad 2021. godine. Za popunjavanje ankete u prosjeku je bilo potrebno 8-10 minuta. Metodom anketiranja nastojalo se od ispitanika saznati kakav stav imaju prema kriptovalutama, koje kriptovalute koriste, na koji način trguju kriptovalutama te smatraju li kriptovalutu kao dobru budućnost. Također, u istraživačkom dijelu koristiti će se kvantitativna analiza te usporedba rezultata odnosno metoda komparacije.

6.2. Analiza rezultata istraživanja

Rezultati istraživanja ukazuju da je postavljenu anketu ispunio podjednjak broj i žena i muškaraca, odnosno 35 žena i 35 muškaraca. Kako se ispitivanje odnosilo na građane grada Zagreba, vrijedi istaknuti kako je u gradu 2011. godine bilo 53 % žena i 47 % muškaraca.

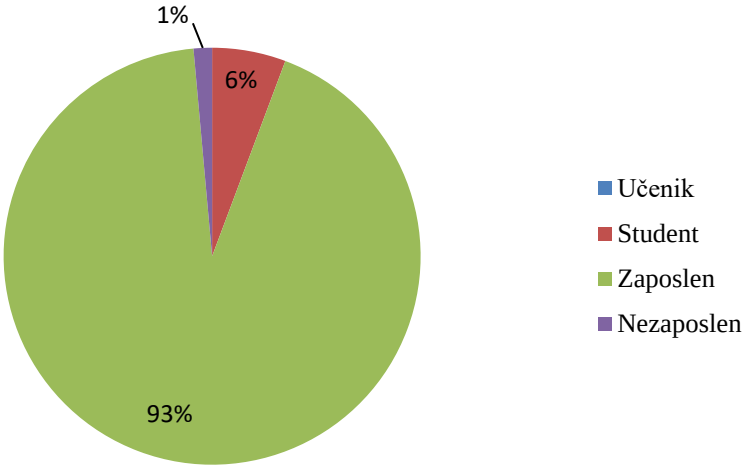
Što se tiče dobne strukture u gradu Zagrebu, od ukupnog broja stanovnika najviše je onih u dobi od 30 do 34 godine. Uvidom u odgovore na postavljeno pitanje u anketi, vidljivo je da je najviše ispitanika u dobi od 25 do 34 godine, točnije njih 44, odnosno 62,9 %. Manji postotak odnosi se na dob između 35 i 45 godina, dok je sedmero ispitanika u dobi od 18 do 24 godine. Detaljnom obradom podataka, od 44 ispitanika u dobi od 25 do 34 godine.

Već na samom početku bilo je istaknuto kako anketu mogu ispunjavati samo punoljetne osobe, a sve to jer u svijet tržišta kapitala u većini slučajeva ulaze punoljetne osobe, osobe sa vlastitim primanjima i računima.



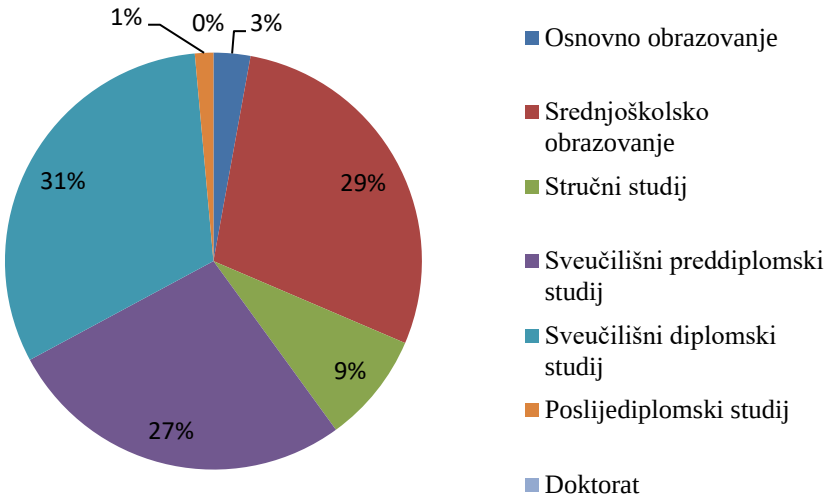
Grafikon 1. Dobna struktura

Sljedeće sociodemografsko pitanje, odnosilo se na poslovni status ispitanika. Iz grafikona 2 jasno je vidljivo kako je preko 90% ispitanika zaposleno. Očekivano je da osobe životne dobi iznad 25 godina budu zaposlene, pa su rezultati, odnosno, veliki postotak sasvim očekivani. Dalje, 4 ispitanika, odnosno 6 % su studenti, dok je 1 osoba nezaposlena.



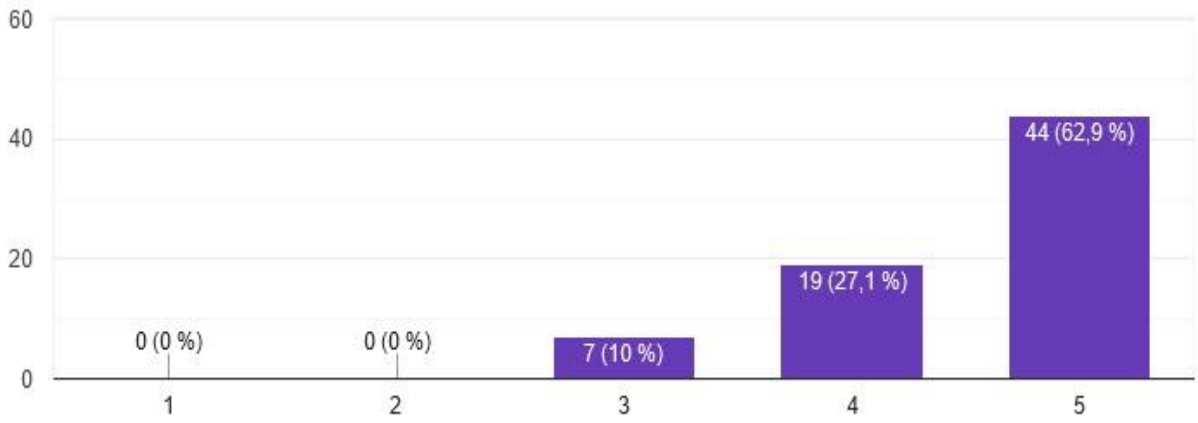
Grafikon 2. Poslovni status ispitanika

Četvrto pitanje vezano uz prethodno odnosilo se na stupanj obrazovanja. Odgovori su različiti, a najveći postotak odnose ispitanici koji su završili sveučilišni diplomski studij (22 ispitanika odnosno 31%). Nakon njih su ispitanici sa završenim srednjoškolskim obrazovanjem (29%), a slijede ih ispitanici sa završenim sveučilišnim preddiplomskim studijem. Stručni studij završilo je 6 ispitanika odnosno 9 %. Ni jedan ispitanik nema doktorat.



Grafikon 3. Struktura stupnja obrazovanja

Prvim pitanjem vezanim uz mobilno poslovanje (petim ukupno), pomoću Likertove skale (broj 5 - u potpunosti se slažem, broj 1 - uopće se ne slažem) dala se mogućnost ispitanicima da odrede smatraju li da je mobilno poslovanje drugačije i modernije poslovanje. Iz grafikona 4 vidljivi su odgovori.

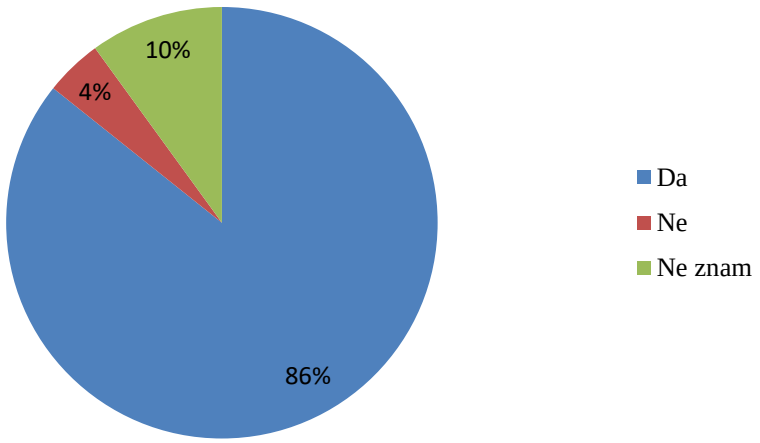


Grafikon 4. Mobilno poslovanje drugačije je i modernije poslovanje

Najviše ispitanika, točnije 44 osobe, odnosno 62,9 % izjavili su da se u potpunosti slaže s tom izjavom da je mobilno poslovanje modernije poslovanje. Manji postotak, 27,1% se slaže s tom izjavom, dok 7 ispitanika odnosno 10% se niti slaže niti ne slaže s tom izjavom. Ako se pogledaju detaljniji rezultati osobe koje se sa tim niti slažu niti ne slažu su osobe životne dobi između 35 i 45 godina. Ispitanici mlađe životne dobi skloniji su informacijskim tehnologijama i korištenju mobilnih uređaja u razne svrhe.

Na pitanje kojim se nastojalo saznati smatraju li mobilno poslovanje budućnosti, 86% ispitanika je izjavilo da je mobilno poslovanje budućnost. Upotrebom tehnologije i većim korištenjem mobilnih telefona korisnici mobilne uređaje jednostavno koriste u svim oblicima, pa čak i u poslovanju. Ponekad su neki programi poput *worda* i *excela* bili dostupni samo na računalima, sada u ovom trenutku to više nije tako, spomenuti programi nalaze se i koriste i na mobilnim uređajima.

Sedam ispitanika nije sigurno je li mobilno poslovanje budućnost, dok 3 osobe smatraju da mobilno poslovanje nije poslovanje budućnosti. Rezultat isu prikazani na grafikonu u nastavku.

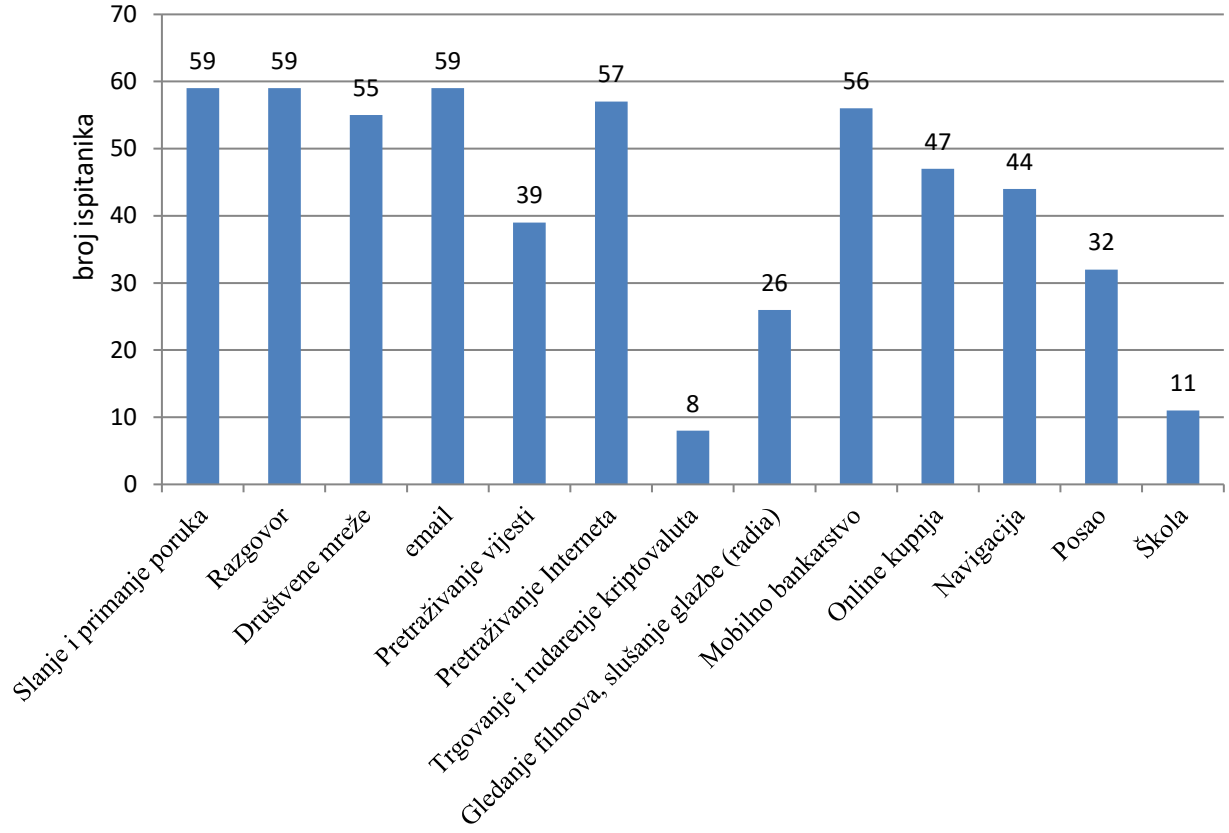


Grafikon 5. Mobilno poslovanje je poslovanje budućnosti

Na pitanje koje su usluge koje se najčešće koriste na mobilnom uređaju najviše ispitanika, njih 84,3% izjavilo je da mobilni uređaj koriste za usluge slanja i primanja poruka, razgovra te slanje i primanje elektronične pošte. Nakon toga tu su često korištene sljedeće usluge: pretraživanje interneta i društvenih mreža te usluge mobilnog bankarstva. Mobilni

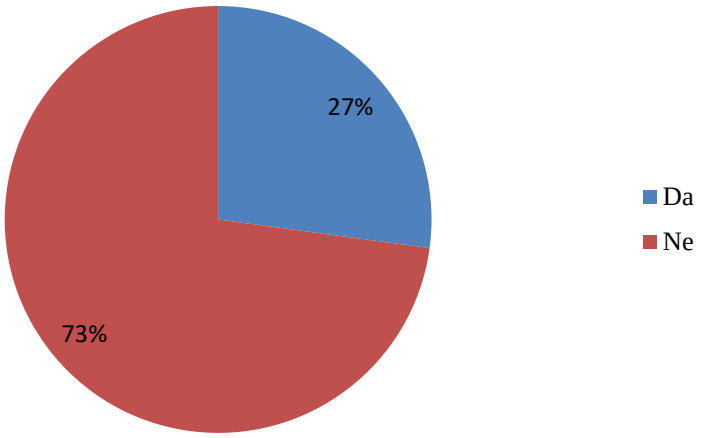
uređaj ispitanici najmanje koriste u svrhu trgovanja i rudarenja kriptovalutama (11 %) i u svrhu škole.

Kako je cilj ankete doznati od ispitanika koriste li kriptovalute, te koriste li mobilne uređaje u svrhu trgovanja i rudarenja kriptovaluta, iz rezultata je vidljivo da najmanji broj ispitanika koristi mobilni uređaj upravo za spomenute usluge.



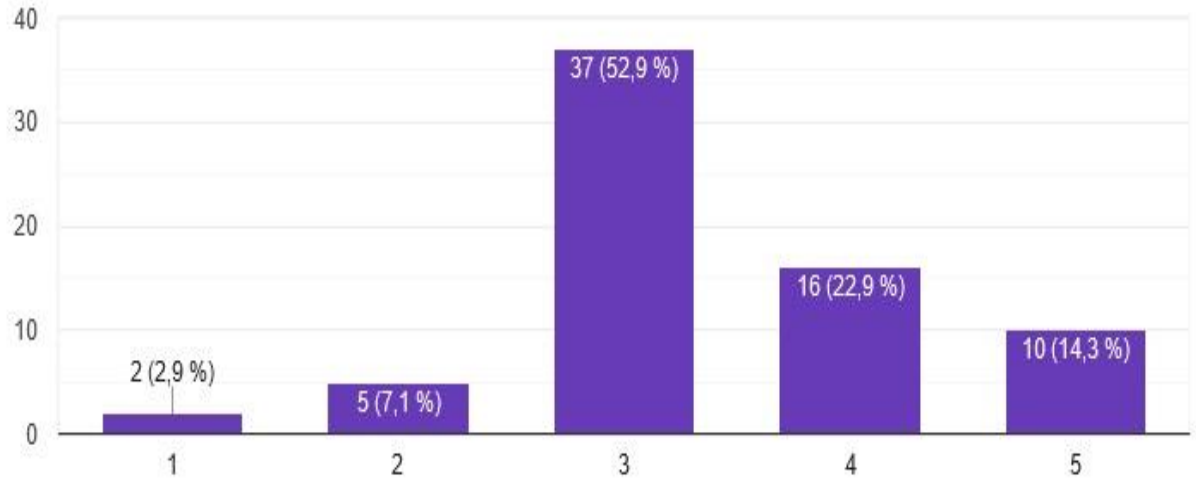
Grafikon 6. Najviše korištene usluge na mobilnom uređaju

Sljedeće pitanje, prikazano Grafikonom 7., najviše ispitanika, njih 51, odnosno 73%, izjavilo je da nikada nije ulagala u tržište kapitala, odnosno u dionice, obveznice, kriptovalute. Manji dio, 27 %, odnosno 19 ispitanika ulagalo je u prije spomenuto tržište. Ono što je jasno je da još uvijek tržište kapitala nije zastupljeno među populacijom u Hrvatskoj kao što je to možda u nekoj drugoj zemlji.



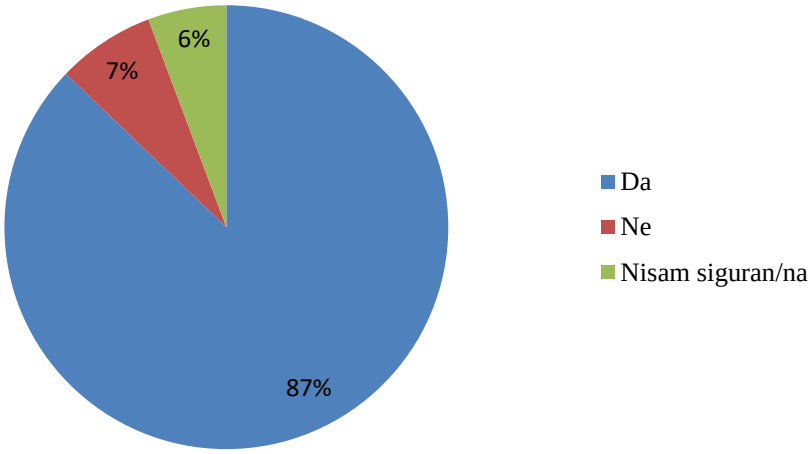
Grafikon 7. Jeste li ikada ulagali u tržište kapitala (dionice, obveznice, kriptovalute)

Nadovezajući se na prethodno pitanje, ispitanici su pomoću Likertove skale (vrijednosti skale isto kao i kod grafikona 4) morali dati mišljenje smatraju li da je ulaganje u tržište kapitala potpuno isplativo. Većina ispitanika, 53% odgovorilo da se niti slaže niti ne slaže. Ispitanici još uvijek nisu skroz upoznati sa tržištem kriptovaluta i ulaganjem u njih, zbog toga su rezultati i očekivani.



Grafikon 8. Ulaganje u tržište kapitala potpuno je isplativo

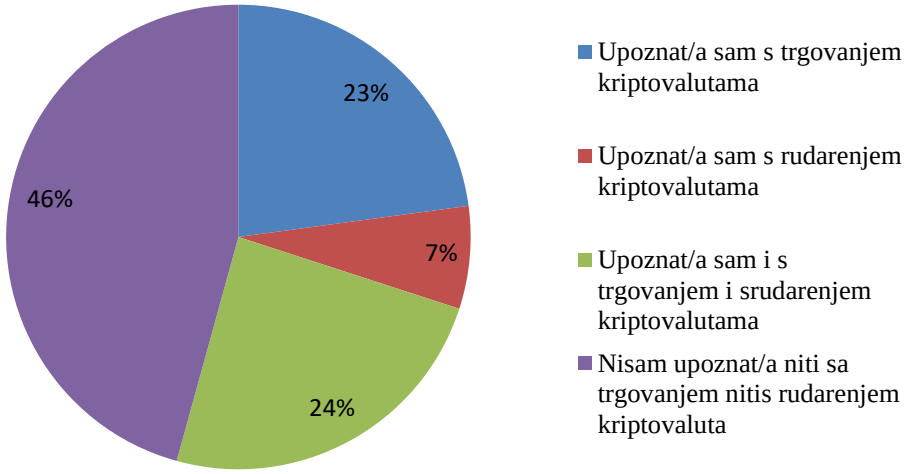
Sljedeće pitanje, usko povezano uz tržište kapitala, ispitanici su morali odgovoriti na pitanje jesu li se susreli s općenitim pojmom kriptovalute. Odgovori su vidljivi grafikonom u nastavku.



Grafikon 9. Jeste li se susreli s pojmom kriptovalute

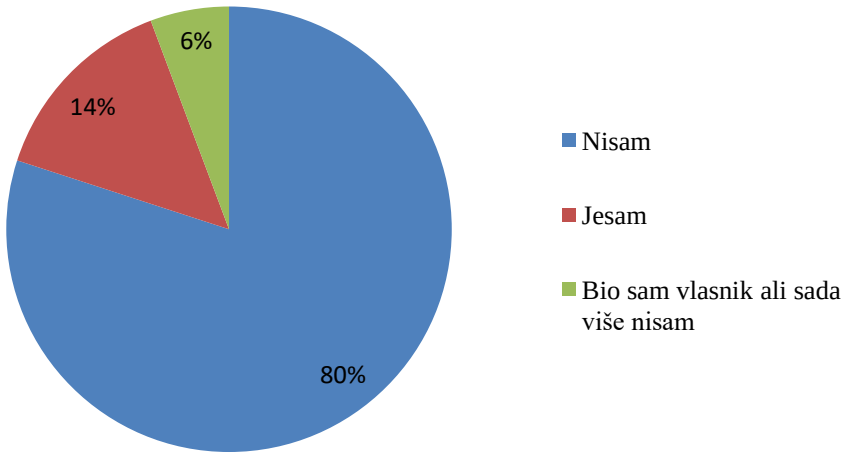
Iz priloženog je vidljivo kako je 87% ispitanika čulo za pojam kriptovaluta. 6% odnosno njih 4 nije sigurno za spomenuti pojam, dok se 5 osoba odnosno 7% nikada nije susrelo s tim pojmom. U današnje vrijeme su osobe koje barem malo vremena provode na internetu ili ispred televizora sigurno čule za pojam kriptovalute, jer su unazad par godina upravo one teme mnogih emisija, vijesti, novina i svega vezanoga uz tržište i kretanje cijena na tržištu.

Nakon što se od ispitanika saznalo jesu li se susreli s pojmom kriptovalute, postavljeno je pitanje jesu li ispitanici upoznati s načinom trgovanja i rudarenja kriptovalutama. Na odabir su ponuđena četiri odgovora, a odgovori su vidljivi u grafikonu 10. Najviše ispitanika, njih 32, odnosno 46%, nije upoznato niti sa trgovanjem niti s rudarenjem kriptovaluta. 17 ispitanika upoznato je i s rudarenjem i s trgovanjem kriptovalutama. Odgovori su iznenađujući s obzirom da većina ispitanika nikada nije imala niti jednu kriptovalutu što je vidljivo na Grafikonu 11..



Grafikon 10. Jeste upoznati s načinom trgovanja i/ili rudarenja kriptovalutama?

Što se tiče posjedovanja kriptovaluta, 80% ispitanika nikada nije bilo vlasnik ni jedne kriptovalute (grafikon 11). Od ukupnog broja, 4 ispitanika odnosno 6% je imalo kriptovalutu, ali je sada više nema. Mala nepažnja i krivo rukovanjem „*walletom*“ može dovesti u opasnost kriptovalutu, odnosno korisnik vrlo brzo može izgubiti i velike ali i male vrijednosti kriptovalute.



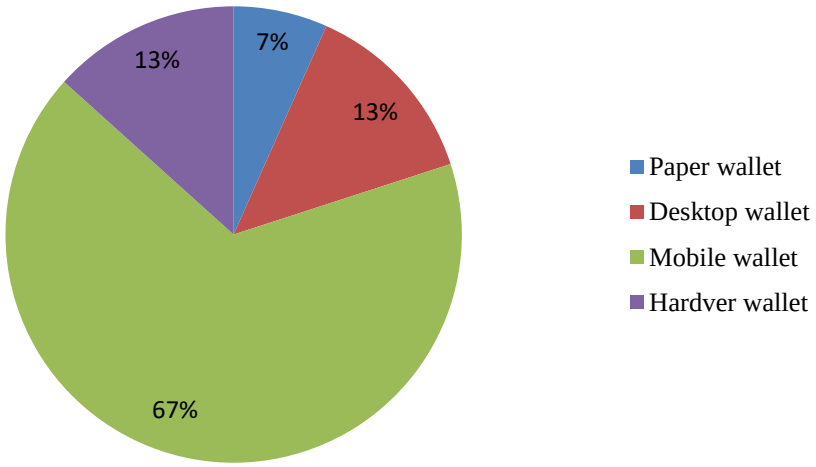
Grafikon 11. Vlasnik ste kriptovalute

Usporedbe radi, na pitanje o vlasništvu kriptovalute, vidljivo je kako je više muškaraca nego žena bio ili je vlasnik kriptovalute. Tu činjenicu potvrdila su i druga razna istraživanja

prema CNBC-a i Acorn Next Gen Investor anketama, gdje se došlo do rezultata kako muškarci imaju dvostruko veću vjerojatnost od žena da će uložiti u kriptovalute, odnosno istraživanje je pokazalo kako je od ukupnog broja ispitanika 16% muškaraca uložilo u kripto, dok je s druge strane to isto učinilo samo 7% žena [35]. Isto tako u jednom istraživanju pokazalo se da u novije vrijeme sve više žena ulaže u kriptovalute te kako žene, u odnosu na muškarce, mogu zadržati značajnije iznose svoje imovine. [35].

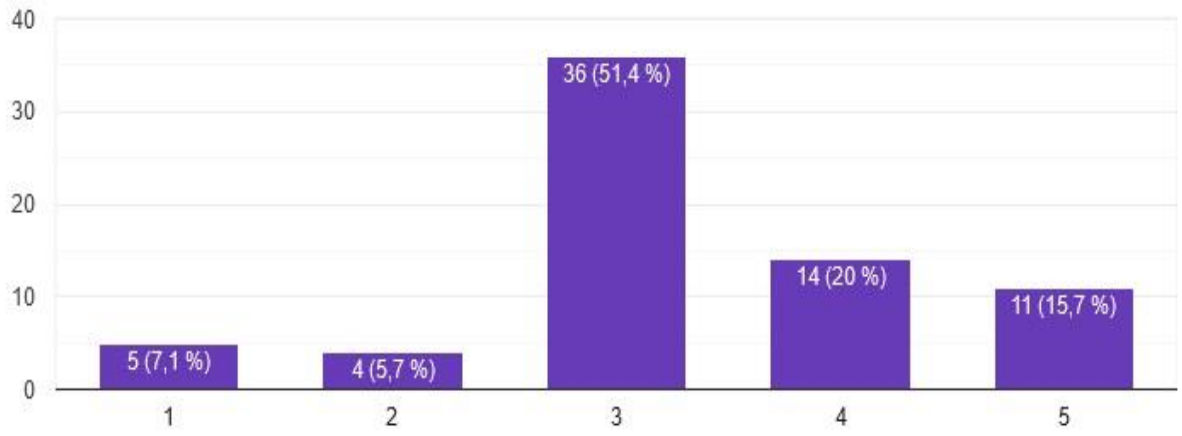
Na 12. pitanju koje u kojem se htjelo doznati na koji su način pohranili kriptovalute također je bila mogućnost da osobe koje su vlasnici neke kriptovalute istu navedu u rubriku „ostalo“. Kriptovalute koje ispitanici prema anketnom upitniku posjeduju su sljedeće: Dogecoin, Shiba Inu, Bizzcoin, Bitcoin, Cardano, BEST, ETH i druge.

Sljedeće, ispitanici koji su odgovorili da su imali kriptovalutu ili je imaju, na 13. pitanje morali su dati odgovor na koji su je način pohranili. Iz grafikona je vidljivo kako je najviše ispitanika svoju kriptovalutu pohranilo na mobile wallet. Zatim, podjednak broj ispitanika čuva ili je čuvao svoju kriptovalutu u desktop ili hardver walletu. Kao najpouzdaniji novčanik spominje se *Hardver wallet,* ali isto tako korisnik bi trebao sam odabrati novčanik za koji smatra da je najbolji za njegove potrebe.



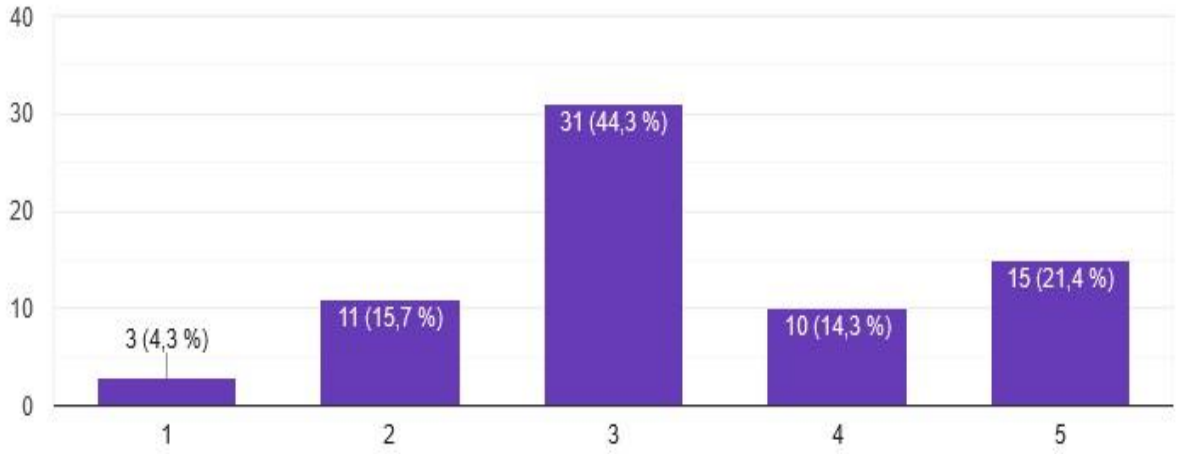
Grafikon 12. Na koji način ste pohranili kriptovalutu

Na sljedeća dva pitanja ispitanici su Likertovom skalom morali odgovoriti na dvije izjave. Prva je da je trgovanje kriptovalutama veliki izvor zarade. Najveći postotak ispitanika, 51,4% sa tom izjavom niti se slaže niti se ne slaže, dok se 11 ispitanika odnosno 16% ispitanika u potpunosti slaže sa tim. Mišljenja su podijeljena i to upravo zbog toga što se u Hrvatskoj još uvijek građani neinformirani dovoljno s trgovanjem kriptovalutama.



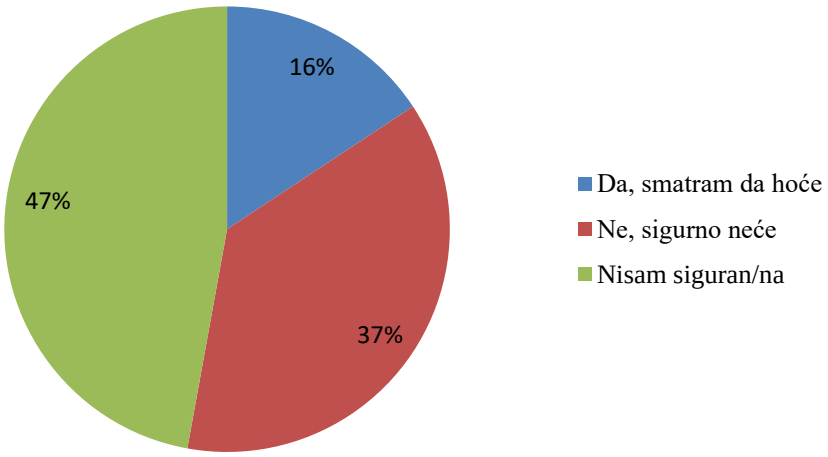
Grafikon 13. Trgovanje kriptovalutama veliki je izvor zarade

Drugo, smatraju li ispitanici da je trgovanje i ulaganje u kriptovalute izlaganje opasnosti. Isto kao i kod prethodnog većina ispitanika niti se slaže sa tim niti se ne slaže. Ispitanici nisu sigurni donose li im kriptovalute zaradu ili opasnost.



Grafikon 14. Smatram da je trgovanje i ulaganje u kriptovalute izlaganje opasnosti

Zadnje pitanje u istraživanju, kako bi se zaokružio istraživački dio, postavljeno je da ispitanici iznesu svoje mišljenje, hoće li kriptovalute zamijeniti klasičan novac u budućnosti. Od ukupnog broja ispitanika, 47,1% nije sigurno, dok 37% ispitanika smatra da neće zamijeniti klasičan novac. Manji broj, tek 11 ispitanik, smatra da će kriptovalute zamijeniti klasičan novac. Sve navedeno prikazano je na grafikonu u nastavku.



Grafikon 15. U budućnosti će kriptovalute zamijeniti klasičan novac

Nakon provedenog istraživanja kojem su ispitanici pristupili dobrovoljno, vidljivo je kako je velika većina upoznata sa tržištem i pojmom kriptovaluta, ali puno manji broj je bio vlasnik ili je vlasnik bilo koje kriptovalute. Tek 14 ispitanika od ukupnog broja bilo je ili je još uvijek vlasnik kriptovalute, a među ispitanicima vlasnicima najviše se pojavljuju Bitcoin, Ethereum, te Cardano.

Osim toga, u nastavku je završnimm tablicama prikazano kako spol, dob i obrazovanje utječe na neka pitanja o kriptovalutama. Najprije je prikazano (U Tablica 1.) kako spomenute karakteristike utječu na ulaganje u kriptovalute. Vidljivo je kako najviše muških ispitanika ulažu u kriptovalute, u dobi od 25 do 34 godine sa završenim sveučilišnim diplomskim studijem.

Tablica 2. Utjecaj spola, dobi i obrazovanja na pitanja o kriptovalutama

Ulaganje u kriptovalute		
Spol	**M**	**Ž**
Broj ispitanika	16	3
Trgovanje i rudarenje kriptovalutama		
Broj ispitanika	13	4

Ulaganje u kriptovalute			
Dob	**18-24**	**25-34**	**35-45**
Broj ispitanika	1	15	3
Trgovanje i rudarenje kriptovalutama			
Broj ispitanika	1	14	2

Ulaganje u kriptovalute				
Obrazovanje	**Sveučilišni preddiplomski studij**	**Sveučilišni diplomski studij**	**Srednjoškolko obrazovanje**	
Broj ispitanika	4	10	5	
Trgovanje i rudarenje kriptovalutama				
Obrazovanje	**Sveučilišni preddiplomski studij**	**Sveučilišni diplomski studij**	**Srednjoškolko obrazovanje**	**Poslijediplomski studij**
Broj ispitanika	7	6	2	2

Izvor: Izvor: rad autora

Što se tiče trgovanja i rudarenja kriptovalutama, tu također većina ispitanika muškog spola, u dobi od 25 do 34 godine, sa završenim sveučilišnim diplomskim studijem.

Također temeljem provedenog istraživanja vidljivo je kako većina ispitanika niti se ne slaže niti se slaže s činjenicom da je tržište kriptovaluta veliki izvor zarade, te ono što je također interesantno većina ispitanika nije sigurna hoće li ikada kriptovalute zamijeniti novac.

7. ZAKLJUČAK

Kriptovalute je potrebno gledati kao inovaciju koja započinje značajan utjecan na ekonomiju i prima velik interes javnosti. Centralne banke i državne institucije pokušavaju svim silama regulirati novo tržište, a za stručnjake se otvaraju velika vrata u raznim organizacijama. Kriptovalute imaju ogroman potencijal zbog svojih karakteristika kao što su decentralizacija i anonimnost. Ako se promotri drugačije, kriptovalute nose izniman rizik i značajnu šansu za gubitkom. Kriptovalute nisu bogate poviješću pa je teško utvrditi kako će se kriptovalute kretati i što donose u budućnosti. Budući da se kriptovalute sve teže rudare, jedini način za zaradu je ulaganje u njih, samim time se pojavljuje sve veći broj burzi i mjenjačnica koje postaju dostupne svima, a provizija je minimalna. Isto tako, korištenje kriptovaluta nosi veliki rizik za zabranu trgovanja jer iste nisu regulirane od strane države, a to može kočiti razvoj kriptovaluta. Postoje mnoge kriptovalute na tržištu, a jedna od najznačajnijih i najzastupljenijih je Bitcoin. Bitcoin je svoju vrijednost imao najveću 2017. godine, kada su mnogi ulagali upravo u ovu valutu. Kao što je poznato kriptovalute su imale veliki utjecaj na ekonomiju, pa su uz pomoć široke zajednice i uspjele održati svoju vrijednost.

Jasno je kako su kriptovalute dostupne na svim tržištima, da su im vrste i zajednica u kojoj djeluju sve šire, da su ulaganja u njih velika i sve češća, te se može zaključiti kako će se sve više govoriti upravo o tržištu kriptovaluta, i kako će spomenuto tržište svakako imati svijetlu budućnost. No, nije sve savršeno što se tiče tržišta, jer je poznato da su kriptovalute vrlo dinamične odnosno promjenjive, te ovise o popularnosti među zajednicom. Primjerice, kriptovalutama se može postati najbogatijim čovjekom na svijetu ali isto tako i prosjakom.

Osim teorijskog dijela, pomoću istraživačkog dijela rada od ispitanika se pomoću ankete željelo doznati koji je njihov stav najprije prema mobilnom poslovanju, a nakon toga prema kriptovalutama, zatim koje kriptovalute koriste, ako koriste, te na koji način trguju kriptovalutama. Među ispitanom populacijom vidljivo je kako još uvijek kriptovalute nisu popularne, te da slabo trguju njima. Također trgovanje kriptovalutama niti smatraju izvorom zarade a niti izlaganje opasnostima. Širenjem i mijenjanjem tržišta, mijenjaju se i novac i valute, pa stoga postoji potencijal da kriptovalute u budućnosti zamjene klasični novac. Najveći postotak ispitanika ipak kaže da kritpovalute neće zamijeniti klasični novac te nije sigurno hoće li to tako biti.

LITERATURA

[1] Tiwari R, Buse S, Herstatt C (2006) From electronic to mobile commerce: Technology convergence enables innovative business services. Hamburg: TUHH. Preuzeto sa: https://www.researchgate.net/publication/228635590_From_electronic_to_mobile_commerce_Technology_convergence_enables_innovative_business_services [pristupljeno listopad 2021.]

[2] Janković, M., Odadžić, B., Babić, A., Razvoj poslovnih servisa u mobilnim telekomunikacionim sistemima, INFOTEH-JAHORINA, Vol. 4, Ref. E-II-6, str. 292-295; 2005

[3] Siau K, Lim E, Shen Z (2002) Mobile Commerce: Current States and Future Trends. USA: UNL. Preuzeto sa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.6381&rep=rep1&type=pdf [pristupljeno listopad 2021.]

[4] Željko Panian ; „Elektroničko poslovanje druge generacije“, Ekonomski fakultet, Zagreb, 2013

[5] Hribar, U. (2007), Razvoj mobilnih tehnologij, Izabrani vidiki: Tehnologija, marketing, Mobilne refleksije (Vehovarur.), Sekcija 5, str. 285-322, Preuzeto sa: http://uploadi.www.ris.org/editor/1259623431Hribar%20Uros%20-%20Razvoj%20mobilnih%20tehnologij.pdf [pristupljeno listopad 2021.]

[6] May, P., Mobile Commerce, Cambridge, Cambridge University Press, 2001

[7] Lai, V., O'Day, K. (2018). Digital Currency Before Bitcoin. Preuzeto sa: https://crushcrypto.com/digital-currency-history/ [pristupljeno listopad 2021.]

[8] Stemberger, K. (2018). Koja je razlika između coina i tokena te što je ERC-20 token? Preuzeto sa: https://www.kriptovaluta.hr/tutorials/koja-je-razlika-izmedu-coina-i-tokena-te-sto-je-erc-20-token/ [pristupljeno listopad 2021.]

[9] Hrvatski Bitcoin portal, Preuzeto sa: https://crobitcoin.com/ [pristupljeno listopad 2021.]

[10] Europska komicija, 2021, Preuzeto sa : https://ec.europa.eu [pristupljeno listopad 2021.]

[11] Cunjak Mataković, I., & Mataković, H. (2018). Kriptovalute-sofisticirani kodovi manipulacije. International Journal of Digital Technology & Economy. Preuzeto sa: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=315456 [pristupljeno studeni 2021.]

[12] Sajter, D.; „Financijska analiza kriptovaluta u odnosu na standardne financijske instrumente“, Financije- teorija i suvremena pitanja, EFOS, 2017

[13] Martucci, B. (2021). The Pros & Cons of Cryptocurrency as a Digital Invesment. Preuzeto sa: https://www.moneycrashers.com/cryptocurrency-pros-cons-volatility-technology/ [pristupljeno studeni 2021.]

[14] Investopedia, preuzeto sa: https://www.investopedia.com [pristupljeno studeni 2021.]

[15] Crypto rates Exchange, preuzeto sa: https://hr.cryptoratesxe.com [pristupljeno studeni 2021.]

[16] Ammous, S.; *BITCOIN STANDARD:* Decentralizirana alternativa središnjem bankarstvu. Zagreb: MATE, 2020

[17] Europska parlamentarna istraživačka služba, preuzeto sa: https://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI%282014%29140793_REV1_EN.pdf [pristupljeno studeni 2021.]

[18] Masovne krađe bitcoina, 2013. Preuzeto sa: https://www.sciencedirect.com/science/article/abs/pii/S1361372313701064 [pristupljeno studeni 2021.]

[19] Bradbury, D.;The problem with Bitcoin. Computer Fraud & security, 2013

[20] Schumpeter. (2014). Preuzeto sa: https://www.economist.com/schumpeter/2014/02/25/mt-gone [Pristupljeno: studeni 2021.]

[21] Ethereum.org, 2020. Preuzeto sa: https://ethereum.org/en/ [Pristupljeno: studeni 2021.]

[22] Antonopoulos, A. M., & Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O'reilly Media. Preuzeto sa: https://books.google.com/books?hl=en&lr=&id=nJJ5DwAAQBAJ&oi=fnd&pg=PR4&dq=Mastering+Ethereum:+Building+Smart+Contracts+and+DApps&ots=uAPOimG_rL&sig=HtWsCciatOYewsL1HSmf2Kq_YlA [Pristupljeno 04.11.2021.]

[23] CoinMarketCap 2020. Preuzeto sa: https://coinmarketcap.com/currencies/tether/ [Pristupljeno: studeni 2021.]

[24] Kriptovalute.hr. Preuzeto sa: https://www.kriptovalute.hr/kripto-novcanik/ [Pristupljeno: listopad 2021.]

[25] CryptoCurrency Facts, Preuzeto sa: https://cryptocurrencyfacts.com/how-does-cryptocurrency-work-for-beginners/ [Pristupljeno: listopad 2021.]

[26] Desjardins Jeff (2017). The Unparalleled Explosion in Cryptocurrencies, preuzeto sa: https://www.visualcapitalist.com/unparalleled-explosioncryptocurrencies/ [Pristupljeno: listopad 2021.]

[27] Indeks.hr. Preuzeto sa: https://www.index.hr/magazin/clanak/Proslo-je-vrijeme-kad-su-mobiteli-sluzili-za-pozive-Najvise-surfamo-igramo-se-i-slusamo-glazbu/623367.aspx [Pristupljeno: studeni 2021.]

[28] GeeksforGeeks. Preuzeto sa: https://www.geeksforgeeks.org/features-of-blockchain/ [Pristupljeno: studeni 2021.]

[29] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Preuzeto sa https://bitcoin.org/bitcoin.pdf [Pristupljeno: rujan 2021.]

[30] Farell, Ryan M. (2015). An Analysis of the Cryptocurrency Industry; preuzeto sa: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1133&context=wharton_research_scholars [Pristupljeno: rujan 2021.]

[31] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32. , preuzeto sa: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf [Pristupljeno: studeni 2021.]

[32] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access, 7, 85727-85745. Preuzeto sa: https://ieeexplore.ieee.org/iel7/6287639/8600701/08746079.pdf [Pristupljeno: studeni 2021.]

[33] Cheng, 2017, Bitcoin just got a vote of confidence from Switzerland's legendary banking system, Preuzeto sa: https://www.cnbc.com/2017/07/12/switzerlands-legendary-banking-system-gave-bitcoin-vote-of-confidence.html [Pristupljeno: studeni 2021.]

[34] Coleman, Lester. 2017. Russian Bank Consortium Uses Ethereum-Based Ledger as Government Signals Support. Preuzeto sa: https://www.cryptocoinsnews.com/russian-bank-consortium-uses-ethereum-based-ledger-as-government-signals-support/ , [Pristupljeno: studeni 2021.]

[35] Lider, preuzeto sa: https://lider.media/poslovna-scena/svijet/nejednakost-muskaraca-i-zena-u-kriptu-duplo-vise-muskaraca-ulaze-u-kriptovalute-138498 [Pristupljeno: studeni 2021.]

[36] Rogina, N. (2018). Što je konsenzus i koje sve vrste postoje? preuzeto sa: https://www.kriptovaluta.hr/tutorials/sto-je-konsenzus-i-koje-sve-vrste-postoje [Pristupljeno: prosinac 2021.]

[37] Medium, Bitcoin Mining Works, preuzeto sa: https://medium.com/chaptrglobal/how-blockchain-bitcoin-mining-works-c146d446377b [Pristupljeno: prosinac 2021.]

[38] Što je Blockchain i kako radi?, preuzeto sa: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 [Pristupljeno: siječanj 2022.]

POPIS KRATICA

SMS	(Short Message Service) Usluga slanja kratkih tekstualnih poruka
MMS	(Multimedia Messaging Service) Usluga slanja većih alfanumeričkih znakova te grafika (video, slike, audio zapisi)
USSD	(Unstructured Supplementary Service Data) Komunikacijski je protokol koji koriste GSM mobilni telefoni za komunikaciju s računalima operatora mobilne mreže
WAP	(Wireless Protocol Aplication) Protokol za bežične aplikacije, koji je tehnički standard za pristup informacijama putem mobilne bežične mreže
SIM	(Subscriber Identity Module) Modul na kojem je pohranjen unikatni broj kojim se identificira preplatnik na mobilnoj telefonskoj mreži
GSM	(Slobal System for Mobile Communications) Najraširenij je svjetski standard za mobilnu telefoniju
ESB	Europska središnja banka
IoT	(Internet of things) povezivanje uređaja putem interneta. Mrežna infrastruktura u kojoj fizičke i virtualne "stvari" svih vrsta komuniciraju i nevidljivo su integrirane
FBI	(Federal Bureau of Investigation) Savezna je kriminalističko-istražna i obavještajna agencija
USB	(Universal Serial Bus) tehnološko rješenje za komunikaciju računala s vanjskim uređajima

POPIS SLIKA

POPIS GRAFIKONA

POPIS TABLICA

PRILOZI

Prilog 1. Anketni upitnik

1. Spol *
   - Ž
   - M
2. Dob *
   - 18-24
   - 25-34
   - 35-45
3. Status ispitanika *
   - učenik
   - student
   - zaposlen
   - nezaposlen
4. Stupanj obrazovanja *
   - Osnovno obrazovanje
   - Srednjoškolsko obrazovanje
   - Stručni studij
   - Sveučilišni preddiplomski studij
   - Sveučilišni diplomski studij
   - Poslijediplomski studij
   - Doktorat
5. Mobilno poslovanje je sasvim drugačije i modernije poslovanje. *
   Uopće se ne slažem ……. U potpunosti se slažem
6. Smatrate li mobilno poslovanje poslovanjem budućnosti? *
   - Da
   - Ne
   - Ne znam
7. Koje usluge najviše koristite na mobilnom uređaju? *
   - slanje i primanje poruka
   - razgovor
   - društvene mreže
   - email
   - pretraživanje vijesti
   - pretraživanje interneta
   - trgovanje i rudarenje kriptovaluta
   - gledanje filmova, slušanje radia
   - mobilno bankarstvo
   - online kupnja

- navigacija
- posao
- škola

8. Jeste li ikada ulagali u tržište kapitala (dionice, obveznice, kriptovalute) *
   - Da
   - Ne
9. Ulaganje u tržište kapitala potpuno je isplativo. *
   Uopće se ne slažem……U potpunosti se slažem
10. Jeste li se susreli s pojmom KRIPTOVALUTE? *
    - Da
    - Ne
    - Nisam siguran/na
11. Jeste li upoznati s načinom trgovanja i/ili rudarenja kriptovalutama? *
    - Upoznat/a sam s trgovanjem kriptovalutama
    - Upoznat/a sam s rudarenjem kriptovalutama
    - Upoznat/a sam i s trgovanjem i s rudarenjem kriptovalutama
    - Nisam upoznat/a niti sa trgovanjem niti s rudarenjem kriptovaluta
12. Jeste li vlasnik neke kriptovalute? Ako jeste u ostalo napišite koje *
    - Jesam
    - Nisam
    - Bio/la sam vlasnik, ali sada više nisam
    - Ostalo:
13. Na koji način ste pohranili svoju kriptovalutu? (na ovo pitanje odgovaraju samo osobe koje su posjedovale ili posjeduju kriptovalute)
    - Paper wallet
    - Desktop wallet
    - Mobile wallet
    - Hardver wallet
14. Trgovanje kriptovalutama veliki je izvor zarade. *
    Uopće se ne slažem…….U potpunosti se slažem
15. Smatram da je trgovanje i ulaganje u kriptovalute izlaganje opasnosti. *
    Uopće se ne slažem…….U potpunosti se slažem
16. Smatrate li da će u budućnosti kriptovalute zamijeniti klasičan novac? *
    - DA, smatram da hoće
    - NE, sigurno neće
    - Nisam siguran/na

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj **diplomski rad** isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu **diplomskog rada** pod naslovom **Značaj mobilnog poslovanja u svrhu trgovanja kriptovalutama**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 28.01.2022.

Studentica:

(potpis)