Utjecaj informacijske i komunikacijske tehnologije na razvoj tržišta kriptovaluta

Peleš, Ivan

SVEUČILIŠTE U RIJECI

Fakultet za menadžment u turizmu i ugostiteljstvu

Sveučilišni diplomski studij

Ivan Peleš

Utjecaj informacijske i komunikacijske tehnologije na razvoj tržišta kriptovaluta

The influence of information and communication technology on the development of the cryptocurrency market

Diplomski rad

Opatija, 2024.

SVEUČILIŠTE U RIJECI

Fakultet za menadžment u turizmu i ugostiteljstvu

Marketing u turizmu

Utjecaj informacijske i komunikacijske tehnologije na razvoj tržišta kriptovaluta

The influence of information and communication technology on the development of the cryptocurrency market

Diplomski rad

Kolegij: **Web dizajn u turizmu i ugostiteljstvu** Student: **Ivan Peleš**

Mentor: Prof. dr. sc. **Mislav Šimunić** Matični broj: **3812/23**

Opatija, 2024.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

Ivan Peleš	**3812**
(ime i prezime studenta)	(matični broj studenta)

Utjecaj informacijske i komunikacijske tehnologije na razvoj tržišta kriptovaluta

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

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

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

U Opatiji, 17.06.2024.

_____Potpis studenta

SAŽETAK

Rad polazi od pitanja na koji je način tehnologija utjecala na razvoj kriptovaluta kao novog i modernog oblika plaćanja pomoću digitalne tehnologije. Kriptovalute predstavljaju moderan i nov koncept u cjelokupnoj svjetskoj ekonomiji te financijskim sistemima, te se s razlogom smatra kako kriptovalute ne bi postojale da se nisu razvile tehnologije poput blockchain i kriptografije. U radu se iznosi što su to kriptovalute, a zatim različite vrste digitalnih tehnologija koje omogućuju postojanje kriptovaluta te njihovo korištenje. Rad se fokusira na različite tehnologije koje su ključne za postojanje kriptovaluta kao što su kriptografija, blockchain tehnologija, rudarenje i novčanik. Istraživanje bi se provelo putem web ankete u kojoj bi se koristio nereprezentativni prigodni uzorak i uzorak snježne grude. Anketa se postavila u online Facebook grupe u kojima su mladi, to jest studenti, te ih se ispitivalo o mišljenjima vezano za kriptovalute općenito te za utjecaj tehnologije na razvoj kriptovaluta. Teorijski dio rada temelji se na analiziranju postojeće literature na temu razvoja kriptovaluta kao posljedica razvitka tehnologije u suvremenom dobu.

Ključne riječi: kriptovalute, informacijske i komunikacijske tehnologije, rudarenje, blockchain, kriptografija, Bitcoin

ABSTRACT

The paper's goal is to answer the question of how technology has influenced the development of cryptocurrencies as a new and modern form of payment using digital technology. Cryptocurrencies represent a modern and new concept in the entire world economy and financial systems, and it is rightly believed that cryptocurrencies would not exist if technologies such as blockchain and cryptography had not been developed. The paper explains what cryptocurrencies are, and then the different types of digital technologies that enable the existence of cryptocurrencies and their use. The paper focuses on various technologies that are essential to the existence of cryptocurrencies such as cryptography, blockchain technology, mining and wallet. The research would be conducted via a web survey using a non-representative convenience and snowball sample. The survey was placed in online Facebook groups where there are young people, that is, students, and they were asked about their opinions about cryptocurrencies in general and about the impact of technology on the development of cryptocurrencies. The theoretical part of the paper is based on the analysis of existing literature on the topic of the development of cryptocurrencies because of the development of technology in the modern age.

Key words: cryptocurrencies, information and communication technologies, mining, blockchain, cryptography, Bitcoin

Sadržaj:

Uvod

Kriptovalute predstavljaju relativno nov pojam koji podrazumijeva novi način plaćanja, kupovanja i investiranja novca putem digitalne tehnologije. Kriptovalute svoj razvitak i uspon duguju informacijskim, digitalnim i komunikacijskim tehnologijama, koje su zapravo i omogućile ovaj nov način upravljanja i korištenja novcem. Naime, bez razvitka informacijskih tehnologija poput Interneta i ostalih tehnologija kao što su rudarenje i blockchain kriptovalute ne bi postojale, ili bi možda i postojale, ali u drugačijem obliku. Kriptovalute su iznimno važan pojam u suvremenom dobu te se može smatrati da je većina populacije čula za njih ili ih pak koristila.

Cilj ovog rada je istražiti na koji su način informacijske i komunikacijske tehnologije utjecale na razvitak kriptovaluta. Metodologija kojom se rad koristi jest anketni upitnik u obliku web ankete koja se koristi prigodnim uzorkom i uzorkom snježne grude kako bi se prikupili podaci i ispitale hipoteze postavljene u istraživanju. Također, rad se bazira i na metodama analize i dedukcije kako bi se iščitavanjem literature došlo do relevantnih podataka o kriptovalutama i posljedicama informacijskih i komunikacijskih tehnologija na razvoj istih.

Rad se sastoji od osam dijelova. Prvi je dio uvod u kojemu se iznosi tema rada, cilj rada, metodologija koja će se koristiti u radu i kratki sažetak svakog poglavlja. Drugo se poglavlje fokusira na samu definiciju i osnovne karakteristike pojma kriptovaluta, a također se obrađuju i najznačajnije kriptovalute i njihove značajke. U trećem se poglavlju iznosi tehnologija kriptografije, a u četvrtome osnove blockchain tehnologije. Peto se poglavlje bavi rudarenjem, a šesto tehnologijom digitalnog novčanika kao jednog od glavnih načina korištenja kriptovalutama. U sedmom se poglavlju iznosi istraživanje koje čini empirijsku osnovu rada i u kojem se istražuju stavovi studenata o utjecaju tehnologije na razvitak kriptovaluta. Osmo poglavlje je zaključak nakon kojeg slijedi popis literature, popis slika i tablica i prilog radu.

1. Definicija kriptovaluta

Razvoj kriptovaluta značajno je uvjetovan razvojem nekoliko ključnih tehnologija, poput blockchaina, kriptografije, decentralizirane mreže i kvantnog računarstva. Blockchain je osnova svih kriptovaluta jer omogućava sigurnost i transparentnost transakcija; svaki blok u lancu sadrži zapis transakcija koje su vidljive svim učesnicima, a tehnologija pametnih ugovora dodatno automatizira transakcije i smanjuje potrebu za posrednicima, čime se povećava efikasnost i smanjuju troškovi. Kriptografija igra ključnu ulogu u osiguravanju autentičnosti i integriteta transakcija kroz složene algoritme koji šifriraju podatke, čime se sprječava neovlašteni pristup i manipulacija. Decentralizirane mreže, kao jedna od ključnih karakteristika kriptovaluta, osiguravaju ravnopravnost svih učesnika i otpornost na napade, eliminirajući centralne točke kontrole koje bi mogle biti meta napada. Kvantno računalstvo, iako je još u ranoj fazi razvoja, ima potencijal značajno utjecati na sigurnost kriptovaluta, jer kvantna računala mogu riješiti složene kriptografske probleme mnogo brže od klasičnih računala, što bi moglo ugroziti trenutne sigurnosne algoritme, ali također otvara mogućnosti za razvoj novih, sigurnijih metoda zaštite podataka (RUE, 2024).

Kriptovaluta je naziv za sustav koji koristi kriptografiju kako bi omogućio siguran prijenos i razmjena digitalnih tokena u distribuiranom i decentraliziranom obliku način. Ovim se tokenima može trgovati po tržišnim tečajevima za fiat valute (Dourado i Brito, 2014). Kriptovalute predstavljaju vrstu elektroničkog novca koja se „odnosi na sustav plaćanja u realnom i virtualnom svijetu čiji je cilj unaprijediti efikasnost postojećih sustava plaćanja i zamijeniti novčanice i kovanice u maloprodajnim transakcijama“ (Cunjak Mataković i Mataković, 2018: 25).

U upotrebi su također i različiti sinonimi koji se koriste za kriptovalute, poput digitalnih valuta, virtualnih valuta i elektroničkog novca. Digitalne valute nemaju fizička svojstva i dostupne su samo u digitalnom obliku. Transakcije koje uključuju digitalne valute vrše se pomoću računala ili elektroničkih novčanika povezanih s internetom ili drugim određenim mrežama. Nasuprot tome, fizičke valute, poput novčanica i kovanog novca, su opipljive, što znači da imaju određene fizičke atribute i karakteristike. Kriptovalute se smatraju podvrstom digitalnih valuta (Frankenfield, 2022).

Virtualne valute predstavljaju „digitalni prikaz vrijednosti i mogu se smatrati specifičnom vrstom imovine koju su njezini imatelji spremni držati i/ili elektronički razmjenjivati te se sporadično njome koristiti za plaćanja. Virtualne valute nisu novac jer ne ispunjavaju osnovne funkcije novca, a na to posebno utječe velika kolebljivost njihove vrijednosti, kao i činjenica

da se ponuda pojedine virtualne valute zasniva isključivo na tehnološkim rješenjima, a ne na potrebama gospodarstava ili monetarnog sustava“ (HNB, 2023). virtualne valute nisu službeno izdane od strane neke monetarne institucije, a također je važno napomenuti kako nisu niti mjerilo vrijednosti iz razloga jer se ne koriste kao mjerilo usporedivosti relativnih cijena između dobara i usluga, a također nisu niti sredstvo razmjene jer se relativno malo koriste u usporedbi s tradicionalnim fizičkim valutama.

Elektronički novac ili e-novac može se definirati kao elektronička pohrana novčane vrijednosti na tehničkom uređaju koja se može naširoko koristiti za plaćanje subjektima koji nisu izdavatelj e-novca. Uređaj djeluje kao prepaid nositeljski instrument koji nužno ne uključuje bankovne račune u transakcije. Proizvodi e-novca mogu se temeljiti na hardveru ili softveru, ovisno o tehnologiji koja se koristi za pohranjivanje novčane vrijednosti (ECB, 2023). U hrvatskom je zakonodavstvu elektronički novac definiran kao „elektronički, uključujući i magnetski, pohranjena novčana vrijednost koja je izdana nakon primitka novčanih sredstava u svrhu izvršavanja platnih transakcija u smislu zakona kojim se uređuje platni promet i koju prihvaća fizička ili pravna osoba koja nije izdavatelj toga elektroničkog novca, a koja čini novčano potraživanje prema izdavatelju (NN 64/18).

Prema Frankenfieldu (2022) digitalne valute predstavljaju općeniti pojam ili krovni pojam koji pokriva i virtualne valute i kriptovalute. Glavne prednosti digitalnih valuta, pa tako i kriptovaluta, su brže vrijeme transakcije, nepostojanje zahtjeva za fizičkom proizvodnjom, niži troškovi transakcija i olakšavanje provođenja monetarne i fiskalne politike. Glavni nedostaci digitalnih valuta su poteškoće u njihovom pohranjivanju i korištenju, opasnost od hakiranja i nestabilnost cijena.

Kriptovalute se mogu definirati i kao „fizički prethodno kalkulirani podaci koji koriste parove javnih i privatnih ključeva generiranih oko specifičnog enkripcijskog algoritma. Ključ dodjeljuje vlasništvo svakog para ključeva, ili ‚kovanice', osobi koja je u posjedu privatnog ključa. Ti parovi ključeva su pohranjeni u datoteci imena ‚wallet.dat', koja egzistira u uobičajenom skrivenom direktoriju na tvrdom disku. Privatni ključevi se šalju korisnicima korištenjem adresa dinamične lisnice generiranih od strane korisnika uključenih u transakcije. Odredišna adresa plaćanja je javni ključ para ključeva kriptovalute. Postoji konačni iznos svake kriptokovanice dostupne na mreži, i vrijednost svake jedinice se dodjeljuje temeljeno na ponudi i potražnji, kao i prema fluktuirajućim razinama težine rudarenja svake kovanice“ (Heid, 2013: 1-2).

Kriptovalute kao koncept nastale su 2008. godine, kada je osoba pod pseudonimom Satoshi Nakamoto objavio „bijeli papir“ u kojemu opisuje proces implementacije digitalne valute pod

nazivom Bitcoin, koja se koristila blockchain tehnologijom. Satoshi Nakamoto (2008) navodi kako je razvio svoj sustav tehnologije kriptovaluta zbog toga jer je želio zadovoljiti potrebu suvremenog svijeta za sustavom elektroničkog plaćanja utemeljenom na kriptografskom dokazu umjesto na povjerenju. Cilj takvog sistema elektroničkog plaćanja jest dopuštanje bilo kojim dvjema voljnim stranama da obavljaju izravne transakcije jedna s drugom bez potrebe za pouzdanom osobom ili trećom stranom. Također, transakcije putem ovog sistema plaćanja i kupovanja služile bi tome da zaštite prodavatelje od prijevare, a putem različitih mehanizama zaštitili bi se i kupci.

Sam koncept alternativnih i digitalnih valuta nije nov, no kriptovalute su specifične po tome što koriste koncept valute otvorenog koda bez središnje točke povjerenja, kao što je središnja distribucijska agencija ili državna vodeća kontrola. Kriptovalute zapravo ne koriste koncept regulacije kakav je inače poznat u svijetu kada se radi o valutama različitih država ili geografskih teritorija kao što su dolar i euro (Hardle, Harvey i Reule, 2018). Neupotrebljavanje takve procedure pri novčanim transakcijama, to jest procedure koja se koristi nekom trećom stranom ili pouzdanom osobom kao što je na primjer banka, bio je jedan od Nakamotovih ciljeva.

Međutim, kriptovalute kao monetarni sustav svejedno imaju institucije koje ih nadgledaju i prate. Dourado i Brito (2014) navode kako postoje dva tipa institucija koje upravljaju kriptovalutama:

- Algoritmičke institucije, koje upravljaju različitim kriptovalutama putem algoritama koje određuju validnost i valjanost kriptovaluta i transakcija koje se izvode putem kriptovaluta. Pravila i parametri za ono što se smatra valjanim transakcijama kriptovaluta ugrađena su u peer-to-peer softver koji pokreću rudari i korisnici kriptovaluta. Jedna od valjanih vrsta transakcija je stvaranje novih kovanica iz praktički ničega. Važno je napomenuti kako ne može svatko ovo izvršiti vrstu transakcije, te se rudari natječu za pravo izvršenja jedne od transakcija po bloku. Na Bitcoinu je učestalost takvih transakcija svakih desetak minuta. Kad rudar otkrije važeći *hash* za blok, on može zatražiti nove kovanice te ih tako zapravo i dobiva. Transakcija u kojoj rudar traži nove kovanice, kao i svaka druga transakcija, mora se uskladiti s očekivanjima mreže. Mreža će naime odbiti svaki blok koji sadrži transakciju u kojoj si rudar dodjeljuje previše novih novčića. Rast kovanica ograničen je unaprijed određenim iznosom po bloku.

- Upravljanje otvorenim kodom. Kao što je navedeno, kriptovalute poput Bitcoina i ostalih djeluju putem softvera koji se bazira na određenim pravilima i stopi dobivanja novih kovanica. Ta su pravila u softveru ugrađena putem međusobnog sudjelovanja voditelja projekta otvorenog koda koji upravlja „referentnim klijentom“, to jest drugim programerima, rudarima, zajednicom korisnika i drugim akterima od kojih neki imaju i negativne intencije za korištenje kriptovaluta. Dinamika između ovih različitih aktera na tržištu kriptovaluta može se usporediti s načinom na koji banke i ostale institucije monetarne politike utječu na tradicionalne valute. Bitcoin i druge uspješne kriptovalute koje su poznate i danas predstavljaju nevlasnički projekt otvorenog koda.

Glavne prednosti i nedostaci kriptovaluta vidljivi su u Tablici 1.

Tablica 1. Prednosti i nedostaci kriptovaluta

PREDNOSTI KRIPTOVALUTA	**NEDOSTACI KRIPTOVALUTA**
Otvoreni kod za rudarenje kriptovalute i primjenjivanje istih algoritama koji se koriste i u online bankarstvu	Snažna nestabilnost, jer usponi i padovi vrijednosti kriptovaluta izravno ovise o deklariranjima izjava vlada različitih država
Kod kriptovaluta kod kojih je količina kovanica ograničena ne postoji inflacija	Veliki rizici ulaganja u kriptovalute na srednje i duge rokove
Peer-to-peer kriptovalutna mreža u kojoj ne postoji glavni poslužitelj koji ima odgovornost za sve operacije; umjesto toga, razmjena informacija događa se između više softverskih klijenata	Rizik korisnika zbog nemogućnosti poništavanja vlastite transakcije
Neograničene mogućnosti transakcija, što znači da svaki vlasnik novčanika može platiti bilo koji iznos kriptovaluta bilo kome, bilo gdje	Izgubljene lozinke i netočne adrese za slanje
Nemogućnost poništavanja transakcija	Nejasan regulatorni status kriptovaluta od strane upravnih tijela
Nemogućnost lažiranja novčića	Nedostatak koherentnih propisa koji može uzrokovati neetičko upravljanje

Niski troškovi korištenja i djelovanja kriptovaluta	Programerski rizici poput bug-ova u softveru
Decentralizacija, to jest nepostojanje središnjeg tijela koje upravlja kriptovalutama	Skaliranje, to jest manji broj transakcija od onih koji se provode putem kompanija kao što je npr. VISA
Lakoća korištenja	
Anonimnost	
Transparentnost	
Brzina transakcija	
Kriptovalute može posjedovati samo osoba koja posjeduje novčanik	
Nemogućnost korištenja osobnih informacija kako bi se počinila prijevara ili krađa	
Mogućnost ulaganja sredstava u transparentne i profitabilne resurse	

Izvor: Bunjaku, Gjorgieva-Trajkovska i Miteva-Kacarski, 2017.

1.1. Najznačajnije kriptovalute

Postoji mnogo različitih vrsta kriptovaluta, a neke od najznačajnijih su:

- Bitcoin
- Ethereum
- Tether
- BNB
- USD Coin
- XRP
- Binance USD i drugi (Royal i Baker, 2023).

1.1.1. Bitcoin

Bitcoin predstavlja najpoznatiju kriptovalutu, te se može smatrati i sinonimom za pojam kriptovaluta. Bitcoin je kriptovaluta koja je započela novu revoluciju u digitalnom plaćanju, te je izumljena od strane Satoshija Nakamota, kao što je navedeno u ranijem tekstu. Ova

kriptovaluta djeluje pomoću softvera otvorenog koda, što znači da ju svatko može preuzeti. Njezin sustav djeluje pomoću decentralizirane peer-to-peer mreže, a također je i u potpunosti distribuiran, što znači da je svaki čvor ili računalni terminal međusobno povezan. Svaki čvor može napustiti i ponovno se pridružiti mreži po želji (Nian i Chuen, 2015), te ovi čvorovi djeluju na principu blockchaina. Prvi bitcoin izrudaren je, to jest stvoren, 2009. godine.

Blockchain tehnologija je temelj Bitcoina, a omogućuje sigurno i transparentno vođenje zapisa o svim transakcijama unutar mreže. Blokovi transakcija su nepromjenjivi, što znači da jednom zapisani podaci ne mogu biti mijenjani ili izbrisani, čime se povećava povjerenje korisnika. Blockchain također omogućava decentralizaciju, čime eliminira potrebu za posrednicima i centralnim autoritetima. Bitcoin koristi napredne kriptografske algoritme za osiguranje transakcija i zaštitu privatnosti korisnika. Kriptografski algoritmi omogućuju stvaranje digitalnih potpisa koji potvrđuju autentičnost transakcija, što ih čini otpornima na manipulaciju i prevare. Također, kriptografske funkcije kao što su SHA-256 hash algoritmi igraju ključnu ulogu u procesu rudarenja Bitcoina. Lightning *Network* je druga slojevita tehnologija koja omogućava brže i jeftinije transakcije izvan osnovnog blockchaina. Ona omogućuje gotovo trenutne transakcije s minimalnim naknadama, čime se poboljšava skalabilnost Bitcoina i omogućuje njegova upotreba u svakodnevnim plaćanjima. Iako kvantno računalstvo još uvijek nije široko primijenjeno, njegova potencijalna primjena može značajno utjecati na sigurnost kriptovaluta. Kvantna računala imaju sposobnost brzog rješavanja složenih kriptografskih problema, što može ugroziti trenutne sigurnosne protokole Bitcoina. Međutim, kvantna kriptografija također nudi mogućnost razvoja novih, sigurnijih metoda zaštite podataka (CoinDesk, 2024).

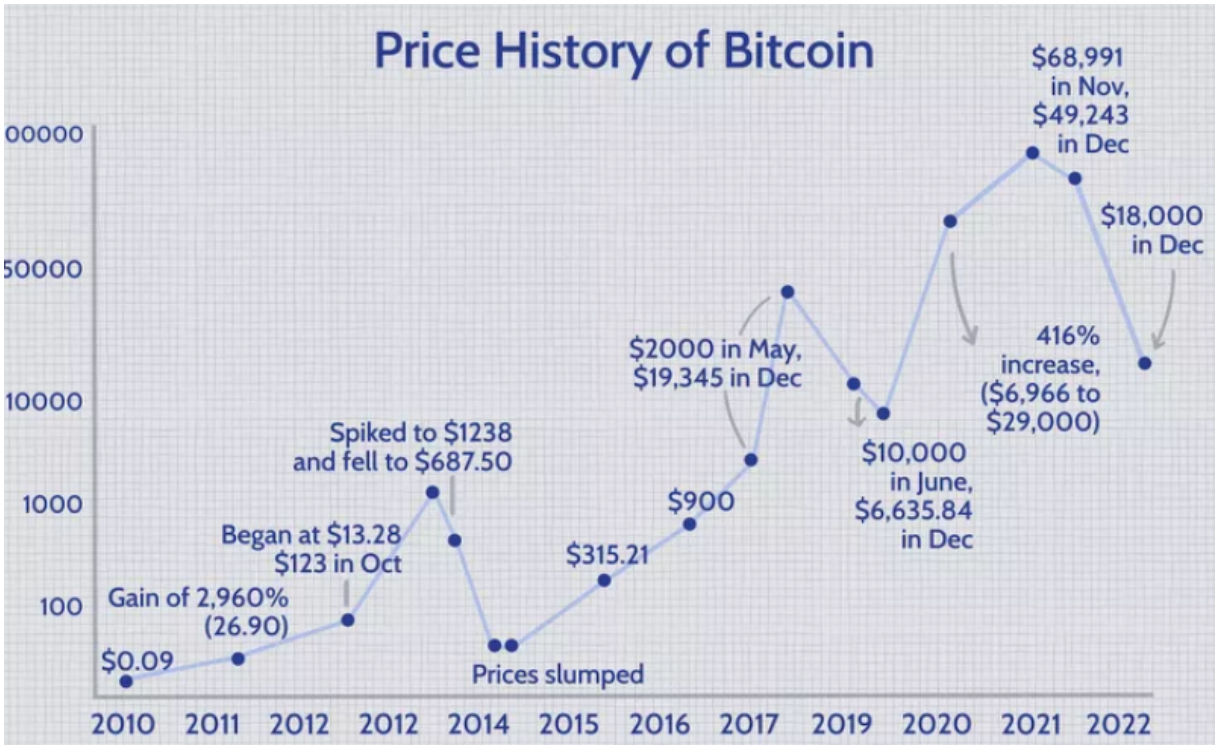
Bitcoin je decentralizirana mreža i digitalna valuta koja koristi peer-to-peer sustav za potvrđivanje i obrađivanje transakcija. Umjesto da se korisnik oslanja na pouzdane treće strane, poput banaka i procesora kartica za obradu plaćanja, Bitcoin tehnologija koristi kriptografski dokaz u svom računalnom softveru za obradu transakcija i provjeru legitimnosti kovanica. S izumom Bitcoina, plaćanja su se mogla vršiti putem interneta bez kontrolu i troškova središnjeg tijela po prvi put u svijetu. Prije ovog izuma, transakcije provedene online uvijek su zahtijevale treću stranu kao pouzdanog posrednika koji bi provjeravao njihovu pouzdanost. Funkcija usluge treće strane je pružiti jamstvo da pošiljatelj ima sredstva za prijenos i da je primatelj uspješno dobio sredstva. To je moguće jer ti posrednici pomažu u održavanju evidencije, ili knjiga, stanja za njihove vlasnike računa. Takav se način provedbe transakcija ne koristi prilikom plaćanja Bitcoinom, a također niti drugim kriptovalutama.

Kriptovaluta Bitcoin djeluje na principu otvorenog koda, što dopušta bilo kojem softverskom programeru da ispita protokol i stvori vlastite verzije softvera za testiranje ili daljnji razvoj ove kriptovalute. Nadalje, Bitcoin je dizajniran da radi samo uz potpuni konsenzus svih korisnika mreže, što osigurava da programeri koji modificiraju izvorni kod Bitcoina u svojim verzijama softvera ne mogu napraviti veliku negativnu promjenu, to jest promjenu koja bi koristila samo njima, u Bitcoin protokolu bez prekidanja kompatibilnosti s ostatkom mreže. Mijenjanje Bitcoin protokola zahtijeva punu suglasnost među korisnicima i programerima Bitcoina (Nian i Chuen, 2015).

Bitcoin je shema decentralizirane virtualne valute s dvosmjernim protokom kriptovaluta. Na općoj razini, Bitcoin funkcionira poput vrste elektroničke gotovine. Bitcoine je moguće kupiti na posebnim web stranicama gdje se mijenjaju se za nacionalnu valutu. Tečaj za Bitcoin određen je tržištem putem funkcija ponude i potražnje. Plaćanja bitcoinima mogu se vršiti od strane bilo koga tko ima potreban softver na svojem računalu, pametnom telefonu ili drugom uređaju koji omogućuje pristup softveru, koji se još naziva i novčanik. Bitcoin umjesto kao na digitalni novac, to jest digitalnu inačicu tradicionalnog novca treba promatrati kao na uložena sredstva na računu. Kada se izvrši plaćanje, uplatitelj ne šalje digitalne novčanice i kovanice primatelju nego se plaćanje odvija terećenjem računa pošiljatelja i odobravanjem računa primatelja. Plaćanja se vrše putem razmjene šifriranih poruke i provjeravaju se unutar korisničke mreže (Segendorf, 2014).

Na Bitcoin serverima postoje javni zapisi u kojima se bilježe sve bitcoin transakcije, a kopije se čuvaju na poslužiteljima diljem svijeta. Svatko sa slobodnim računalom može postaviti jedan od tih poslužitelja, poznatih kao čvor. Konsenzus o tome tko posjeduje koje kovanice postiže se kriptografski preko ovih čvorova umjesto da se oslanja na središnji izvor povjerenja poput banke. Svaka se transakcija javno emitira na mreži i dijeli od čvora do čvora. Svakih desetak minuta te transakcije rudari skupljaju zajedno u grupu koja se zove blok i trajno ih dodaju u blockchain, što predstavlja konačnu knjigu računa bitcoina (Sparkes, 2023). Na slici 1. prikazana je fluktuacija vrijednosti Bitcoina od 2010. do 2022. godine.

Slika 1. Fluktuacija vrijednosti Bitcoina od 2010. do 2022. godine



Izvor: Edwards, 2022.

Kao i kod svih kriptovaluta, vrijednost Bitcoina varira kroz vrijeme ovisno o različitim parametrima. Kada je osmišljen Bitcoin je imao cijenu od 0 dolara, što je poraslo na 0.09 dolara 2010. godine te je njegova vrijednost nastavila rasti. U prvom razdoblju njegova maksimalna vrijednost bila je 1238 dolara, no ta je vrijednost ubrzo pala na 687.50 dolara 2013. godine te je nastavila padati do 2015. godine. Tada je narasla na 315.21 dolara, a potom je vrijednost Bitcoina iznosila 2000 dolara 2017. godine. Nakon pada vrijednosti početkom 2020. godine, Bitcoin je svoju najveću vrijednost do sad dostigao 2021. godine kada je jedan novčić vrijedio 68 991 dolara. 2022. godine njegova se vrijednost značajno smanjila, no i dalje iznosi 18 000 dolara (Edwards, 2022).

1.1.2. Ethereum

Kriptovaluta Ethereum je osmišljena 2013. godine od strane Vitalika Buterina koji je prvotno koristio Bitcoin kao svoju glavnu kriptovalutu. Ethereum se financirao putem masovne prodaje 2014. godine te je za svjetsku upotrebu lansiran 2015. godine. Ethereum predstavlja

drugu po veličini kriptovalutu po svojoj tržišnoj kapitalizaciji, a također i najvrjedniju smart ugovornu platformu. Ethereum kao i Bitcoin ima određenu količinu novčića koja se može rudariti, a 2022. godine bilo je 118 milijuna neizrudarenih ethera (što je naziv za novčić kojim se ova kriptovaluta koristi), od kojih je svaki vrijedio oko 2400 dolara (Galindo i Ferraioli, 2022).

Ethereum je popularizirao koncept pametnih ugovora, samostalno izvršavajućih programa na blockchainu. Ovi ugovori omogućuju automatizaciju i izvršenje složenih transakcija bez potrebe za posrednicima, što značajno olakšava financijske usluge, upravljanje lancem opskrbe i druge poslovne procese. Ethereum je također vodeća platforma za izgradnju decentraliziranih aplikacija koje koriste pametne ugovore za pružanje usluga poput decentraliziranih financija (DeFi) i nezamjenjive tokene (NFTs). DeFi aplikacije omogućuju peer-to-peer financijske transakcije, dok NFTs predstavljaju jedinstvene digitalne imovine koje se koriste u umjetnosti, igrama i drugim industrijama. Nadogradnja na Ethereum 2.0 uvodi mehanizam konsenzusa Proof of Stake (PoS) i sharding, što omogućuje paralelnu obradu transakcija. Ove promjene značajno poboljšavaju skalabilnost i efikasnost mreže, te smanjuju transakcijske troškove i omogućuju veću propusnost transakcija. Kako bi se dodatno povećala skalabilnost, Ethereum koristi Layer 2 rješenja poput Optimism i Arbitrum, koja omogućuju brže i jeftinije transakcije tako što obrađuju transakcije izvan glavnog lanca (*off-chain*), čime se smanjuju opterećenje mreže i transakcijske naknade. Ethereum ima decentralizirani model upravljanja koji uključuje developere, rudare i korisnike. Ovaj model omogućuje fleksibilnost i prilagodljivost u donošenju odluka, iako se suočava s izazovima poput koordinacije i učinkovitosti u procesu donošenja odluka (CoinDesk, 2024).

Ethereum je programabilni blockchain, izgrađen korištenjem koncepata koje je uveo Bitcoin, ali dizajniran na drugačiji način. Umjesto da traži stvaranje decentraliziranog štednog računa, poput Bitcoina, programeri Ethereuma željeli su stvoriti decentraliziranu trgovinu aplikacija otvorenog koda. Kao i Bitcoin, Ethereum koristi blockchain. Bitcoinov blockchain sadrži zapis svih transakcija u povijesti ove kriptovalute, a Ethereumov blockchain sadrži transakcije uz još dodatno i linije koda i podataka. Linije koda i podaci se mogu kombinirati za pisanje programa koji se nazivaju pametni ugovori. Ethereum kao softver se može usporediti s „globalnim računalom“, jer se svatko može prijaviti na računalo, uploadati programe ili pokrenuti tuđe programe (Galindo i Ferraioli, 2022).

Glavne razlike između Ethereuma i Bitcoina su te da Ethereum koristi drugačiji hardver, koristi drugačije programski jezik i ima drugačiji temeljni dizajn. Njegov programski jezik, Solidity, fleksibilniji je od Bitcoinova programskog jezika *Scripta*. Iz razloga što trgovine

aplikacijama moraju podnijeti više transakcija od štednih računa, Ethereumovi blokovi se proizvodi se svakih 15 sekundi, što je mnogo brže od Bitcoinovih blokova, koji se proizvode svakih 10 minuta. Potražnja za Bitcoinom utemeljena je na želji korisnika za posjedovanjem Bitcoina, a veliki dio potražnje za Ethereumom bazira se na korisnicima koji žele ovu kriptovalutu potrošiti na transakcije.

Ethereum se sastoji od nekoliko glavnih komponenti:

- Pametnih ugovora koji predstavljaju pravila koja određuju pod kojim uvjetima novac može promijeniti vlasnika
- Ethereum blockchain koji predstavlja zapis povijesti transakcija na Ethereumu
- Mehanizam konsenzusa ili sporazuma, koji predstavlja metodu za provjeru valjanosti i zapisivanje podataka na blockchainu, a također pomaže i u zaštiti mreže te služi puštanju novih novčića u optjecaj
- Ethereum Virtual Machine ili EVM, koji predstavlja dio mreže koji izvršava pravila Ethereuma i osigurava da transakcije i pametni ugovori slijede ugovorena pravila
- Ether, to jest Ethereumov novčić koji je potreban kako bi se izvršavale transakcije i pametni ugovori (Sergeenkov, 2022).

Interakcija s Ethereumom zahtijeva kriptovalutu koja je pohranjena u novčaniku. Taj se novčanik povezuje s decentraliziarnim aplikacijama, te iz njih svatko može kupovati predmete, igrati igre, posuđivati novac i obavljati različite vrste aktivnosti kao i na tradicionalnom internetu. Tradicionalni web je besplatan za korisnike jer oni daju osobne podatke. U Ethereum mreži kriptovaluta zauzima mjesto podataka, što znači da korisnici mogu slobodno pregledavati i anonimno komunicirati (Coin Telegraph, 2023).

Ethereum je 2015. godine imao vrijednost manju od 1 dolara, no od 2016. godinu je prešao vrijednost od 10 dolara. Do 2017. Ether je stekao popularnost i dosegao 100 dolara u svibnju 2017. Do kraja 2017. godine ether je dosegao vrijednost od 774.69 USD, a unutar prvog tjedna 2018. prešao je vrijednost od 1000 dolara. No, krajem 2018. godine njegova se vrijednost smanjila na 100 dolara. Od 2019. do 2021. godine, ether je ponovno nastavio rasti, no u prvoj polovici 2022. godine vrijednost ethera je pala. Trenutačna vrijednost ethera je 1546.38 dolara (Ycharts, 2023).

1.1.3. Tether

Tether predstavlja platformu čiji je rad baziran na tehnologiji blockchaina te je dizajniran s ciljem da olakša korištenje valute putem digitalnih tehnologija. Još jedan od ciljeva Tethera kao digitalne platforme i kriptovalute je donošenje promjena u konvencionalnom financijskom sustavu na način da svojim korisnicima omogućuje moderniji pristup novcu. Ova kriptovaluta je specifična po tome što je svojim korisnicima omogućila transakcije u kojima se koriste tradicionalne valute putem tehnologije blockchaina bez volatilnosti i složenosti koja se obično povezuje s korištenjem digitalnih valuta (Tether, 2023). Tether također predstavlja i stabilni novčić (eng. *stablecoin*), koji se može definirati kao kriptovaluta čija je vrijednost povezana s vanjskom imovinom poput tradicionalnih valuta ili zlata kako bi mogla održati stabilnu i stalnu cijenu (Rosa i Pareschi, 2021).

Tether, poznati stablecoin, koristi blockchain tehnologiju za transparentnost i sigurnost transakcija, a početno je bio izgrađen na Bitcoinovom blockchainu putem Omni Layer protokola. Kasnije je proširen na druge blockchain platforme poput Ethereuma, Trona i Solane, što je omogućilo brže i jeftinije transakcije. Na Ethereum blockchainu, Tether koristi pametne ugovore za izdavanje i upravljanje tokenima, što omogućava automatizaciju i sigurnost transakcija, čime se smanjuje potreba za posrednicima. Tetherova sposobnost da radi na više blockchaina povećava njegovu korisnost i prihvaćenost u različitim ekosustavima kriptovaluta, čime se korisnicima omogućuje lakši pristup i korištenje Tethera na različitim platformama. Također, Tether je implementirao tehnologije za regulaciju i usklađenost s propisima kako bi se osiguralo da su tokeni u potpunosti pokriveni rezervama fiat valuta, čime se povećava povjerenje korisnika (CoinDesk, 2024).

Platforma Tether kao svoju kriptovalutu koristi Tether tokene, koji predstavljaju digitalne tokene izgrađene pomoću nekih od glavnih blockchaina poput Algoranda, Avalanchea, Bitcoin Cash's Simple Ledger Protocol, EOS, Liquid Network i drugih. Ovi transportni protokoli sastoje se od softvera otvorenog koda koji se povezuje na blockchain kako bi se omogućilo izdavanje i korištenje Tether tokena. Svaki Tether token je podržan putem rezervi koje se nalaze na samoj platformi, što uključuje tradicionalnu valutu i druge novčane ekvivalente, a može uključivati i drugu imovinu i potraživanja iz zajmova koje je Tether dao trećim stranama.

Tether tokeni predstavljaju sredstva koja se kreću pomoću tehnologije blockchaina kao i sve druge digitalne valute, no specifični su po tome što su vezani uz valute koje se koriste u realnom svijetu, to jest tradicionalne valute u omjeru 1:1. Navedeno znači da na primjer 1

USD₮ iznosi 1 USD, a isto vrijedi i za ostale valute. Tether tokeni nazivaju se stabilnim novčićima jer nude stabilnost cijena jer su vezani za tradicionalnu valutu. To trgovcima, trgovcima i fondovima nudi adekvatni način rješavanja niske volatilnosti prilikom provođenja različitih transakcija. Valute koje Tether platforma podržava prikazane su u Tablici 2.

Tablica 2. Tradicionalne valute podržane na Tetheru i njihovi ekvivalentni Tether tokeni

TRADICIONALNE VALUTE KOJE SU PODRŽANE NA TETHER PLATFORMI	TETHER TOKENI
Američki dolari	USD₮
Euri	EUR₮
Meksički pesosi	MXN₮
Britanska funta	Tether GBP
Kineski yuan	CNH₮
Zlato	XAU₮

Izvor: Tether (2023). Dostupno na: https://tether.to/en/ (6.3.2023)

Tether je izvorno stvoren da koristi Bitcoin mrežu kao svoj transportni protokol za omogućavanje transakcija tokenizirane tradicionalne valute. Budući da ova izvorna verzija Tethera koristi Bitcoin blockchain, samim time se i nasljeđuje inherentna stabilnost i sigurnost koje su već dugi niz godina garantirane Bitcoinovim blockchainom. Tether platforma također je povezana i s kriptovalutom i platformom Ethereum. Naime, Tether na Ethereum blockchainu, kao ERC20 token, predstavlja prijenosni sloj novijeg datuma koji omogućuje da su Tether tokeni dostupni u Ethereum pametnim ugovorima ili decentraliziranim aplikacijama na Ethereumu. Na ovaj način se Tether tokeni također mogu poslati na bilo koju Ethereum adresu (Tether, 2023).

Tether je stabilni novčić i prvi tog tipa koji se pojavio na tržištu te se zato smatra i osnivačem prakse stvaranja *stablecoina*. No, važno je napomenuti kako je Tether kao kriptovaluta i kao platforma daleko od toga da ima besprijekoran ugled na tržištu kriptovalutu. Naprotiv, mnogi sumnjanju kako je platforma Tether sudjelovala u aktivnostima gdje se velike mase Tether tokena koriste za kupnju velikih masa Bitcoina kako bi se umjetno podigla cijena potonjeg. Posljedično tome stvaraju se tzv. mjehurići (eng. *bubbles*) koji utječu na

cijelo tržište kriptovaluta o kojemu općenito ovisi vrijednost *altcoina*, to jest alternativi Bitcoinu. Tvrtka koja je napravila Tether nikada nije dala službeni dokaz da ima dovoljno rezervi za pokrivanje količine izdanih Tether tokena Nadalje, postoje i suvlasnički i su upravni odnosi između tvrtke za izdavanje Tether tokena i Bitfinexa, jedne od najvećih mjenjačnica kriptovaluta. Ove sumnje, zajedno s nedostatkom transparentnosti u upravljanju valutom i odnosima između gore navedenih tvrtki, doveli su do niza pravnih postupaka protiv različitih fizičkih i pravnih osoba uključenih u trgovinu Tetherom (Rosa i Pareschi, 2021).

1.1.4. Druge kriptovalute

Na tržištu kriptovaluta postoji mnogo različitih vrsta kriptovaluta koje su u nekim svojim aspektima slične, a u nekima različite. U ovom potpoglavlju obrađuju se druge važne kriptovalute koje nemaju toliku vrijednost na tržištu kao Bitcoin, Ethereum ili Tether.

Osnova svih kriptovaluta je blockchain, koji osigurava decentraliziran i transparentan zapis transakcija, omogućavajući da transakcije budu javno vidljive i nepromjenjive, što povećava povjerenje korisnika u sigurnost i integritet podataka. Primjena blockchaina nije ograničena samo na kriptovalute, već se koristi i u drugim područjima poput financijskih usluga, lanca opskrbe i zdravstva. Ethereum je popularizirao pametne ugovore, samostalno izvršavajuće kodove na blockchainu koji omogućuju automatizaciju kompleksnih transakcija bez potrebe za posrednicima, čime se smanjuju troškovi i povećava učinkovitost. Pametni ugovori se široko koriste u decentraliziranim financijama i drugim aplikacijama. Također, Ethereum je vodeća platforma za izgradnju decentraliziranih aplikacija koje koriste pametne ugovore za pružanje raznih usluga, omogućujući financijske transakcije bez posrednika, stvarajući pristupačnije i transparentnije financijske usluge. *Proof of Stake* (PoS) se koristi za poboljšanje skalabilnosti i energetske učinkovitosti blockchaina; Ethereum 2.0 uvodi PoS kako bi smanjio potrošnju energije i omogućio veći broj transakcija, zamjenjujući tradicionalni mehanizam *Proof of Work* (PoW) koji zahtijeva značajnu računalnu snagu za validaciju transakcija. Mnoge kriptovalute danas koriste tehnologije koje omogućuju njihovu interoperabilnost, odnosno sposobnost da djeluju na različitim blockchain mrežama, čime se povećava njihova korisnost i prihvaćenost u različitim ekosustavima kriptovaluta. Nove tehnologije kao što su Layer 2 rješenja (npr. Lightning Network za Bitcoin) omogućuju brže i jeftinije transakcije čime se smanjuje opterećenje glavnog lanca. Ove inovacije su ključne za poboljšanje skalabilnosti i praktičnosti korištenja kriptovaluta u svakodnevnim transakcijama. Ove tehnologije nisu

samo omogućile razvoj kriptovaluta, već su i postavile temelje za daljnju inovaciju i primjenu u širem financijskom sektoru i drugim industrijama (RUE, 2024).

Binance Coin ili BNB predstavlja izvorni novčić Binance burze kriptovaluta koja je najveća burza kriptovaluta na svijetu. BNB je pokrenut 2018. i koristi se za nekoliko svrha kao što su trgovanje, plaćanja kreditnim karticama, obrada plaćanja, zajmovi i drugi prijenosi ili transakcije. Kako bi se potaknulo prihvaćanje ove kriptovalute, transakcijske naknade za razmjenu Binance manje su za korisnike koji plaćaju u BNB-u. Kako bi njegova vrijednost bila stabilna, Binance uništava ili spaljuje fiksni postotak kovanica u optjecaju. BNB trenutno ima cijenu od oko 300 dolara (Maheshwari, 2023).

Cardano predstavlja platformu koja je na tržištu konkurentna Ethereumu jer također koristi princip pametnih ugovora. Novčić platforme Cardano naziva se ADA, te je ova platforma stvorena od strane Charlesa Hoskinsona koji je također radio i na Ethereumu. U 2023. godini Cardano ima osmu najveću tržišnu kapitalizaciju, a vrijednost jednog ADA je 0,37 dolara. Platforma Cardano je ekološki prihvatljivija i energetski učinkovitija u usporedbi s drugim sličnim platformama jer koristi vlastiti algoritam nazvan Ouroboros koji je različit od Bitcoinovog algoritma na kojem se baziraju mnoge druge kriptovalute.

Solana predstavlja blockchain platformu koja je pokrenuta 2017. godine s ciljem pružanja brzog izvršavanja decentraliziranih aplikacija Kao i Cardano, Solana je također poznata kao konkurent Ethereumu jer može izvršiti mnogo više transakcija u sekundi (TPS) od Ethereuma uz niže transakcijske naknade. Solana je dizajnirana za skaliranje s industrijskom dostupnošću CPU-a, memorije i propusnosti mreže. Kriptovaluta koja predstavlja temelj Solana blockchaina zove se Solana (SOL) i trenutačno ima vrijednost od oko 24 dolara (Maheshwari, 2023).

Litecoin je kriptovaluta koja je nastala 2011. godine i poznata je po svojoj jednostavnosti, efikasnosti i učinkoviti. Litecoin je na tržištu kriptovaluta poznat kao lakša verzija Bitcoina, iako djeluje putem potpuno drugačijeg algoritma poznatog kao Scrypt. Kao i Bitcoin, i Litecoin se može rudariti, a također ima brže vrijeme obrade transakcije u usporedbi s Bitcoinom. Litecoin je lansiran sa 150 unaprijed rudarenih kovanica i ima najveću zalihu od 84 milijuna kovanica. Poput Bitcoina, ponuda Litecoina također je osmišljena tako da se s vremenom smanjuje kako bi se očuvala vrijednost kovanice (Maheshwari, 2023).

Još neke od popularnih kriptovaluta su:

- XRP koji djeluje na mreži Ripple i smatra se kriptovalutom za banke jer je napravljen da služi potrebama industrije financijskih usluga. Zamišljen kao

način za olakšavanje međunarodnih plaćanja, XRP djeluje kao most između dviju različitih valuta kako bi ponudio jeftinije i brže globalne prijenose.

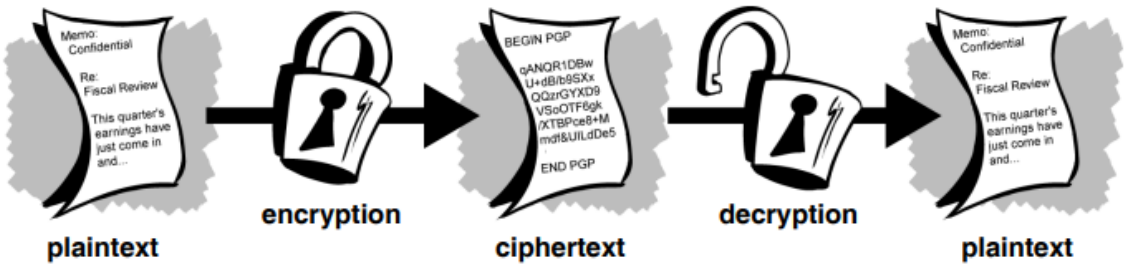
- Aave, koji je decentralizirana kriptoplatforma izgrađena putem *blockchaina* i koja koristi pametne ugovore kako bi korisnicima omogućila posuđivanje i razmjenjivanje kriptovaluta. Kao zaštitni mehanizam za klijente, Aave se specijalizirao za takozvane prekomjerno kolateralizirane zajmove, što znači da su klijenti dužni položiti kripto depozite koji vrijede više nego što posuđuju. Korisnici zatim mogu posuditi kriptovalutu do određenog postotka založene vrijednosti kolaterala, pomažući u izbjegavanju problema poput neplaćanja kredita.
- Avalanche, koji predstavlja platformu za pametne ugovore i čija je kriptovaluta AVAX. AVAX se može koristiti za plaćanje transakcijskih troškova na Avalancheu. Ova je platforma specifična po tome što korisnicima omogućuje kreiranje novih vlastitih blockchainova (N26, 2023).

2. Kriptografija

Kriptografija predstavlja znanost o korištenju matematike za šifriranje i dešifriranje podataka. Kriptografija se također može definirati i kao „znanstvena disciplina koja se bavi problemom prijenosa informacije putem nesigurnog komunikacijskog kanala između pošiljatelja i primatelja“ (Barić, Grgić i Jurić, 2020: 37). Kriptografija omogućuje pohranjivanje osjetljivih informacija ili njihov prijenos preko nesigurnih mreža kao što je Internet tako da ih ne može pročitati nitko osim namijenjenih primatelja. Dok je kriptografija znanost o osiguravanju podataka, kriptoanaliza je znanost o analizi i razbijanju sigurnih ključeva koji omogućuju sigurnu komunikaciju. Klasična kriptoanaliza uključuje kombinaciju analitičkog razmišljanja, primjene matematičkih alata i tako dalje. Kriptologija obuhvaća i kriptografiju i kriptoanalizu (PGP, 2002).

Kriptografija se koristi tehnikama enkripcije i dekripcije. Enkripcija predstavlja metodu prikrivanja otvorenog, to jest standardnog teksta na način da se sakrije njegov sadržaj i svrha, te tako nastaje šifrirani tekst. Dekripcija ili dešifriranje predstavlja postupak vraćanja šifriranog teksta u izvorni otvoreni tekst (Slika 2.).

Slika 2. Proces enkripcije i dekripcije



Izvor: PGP, 2002

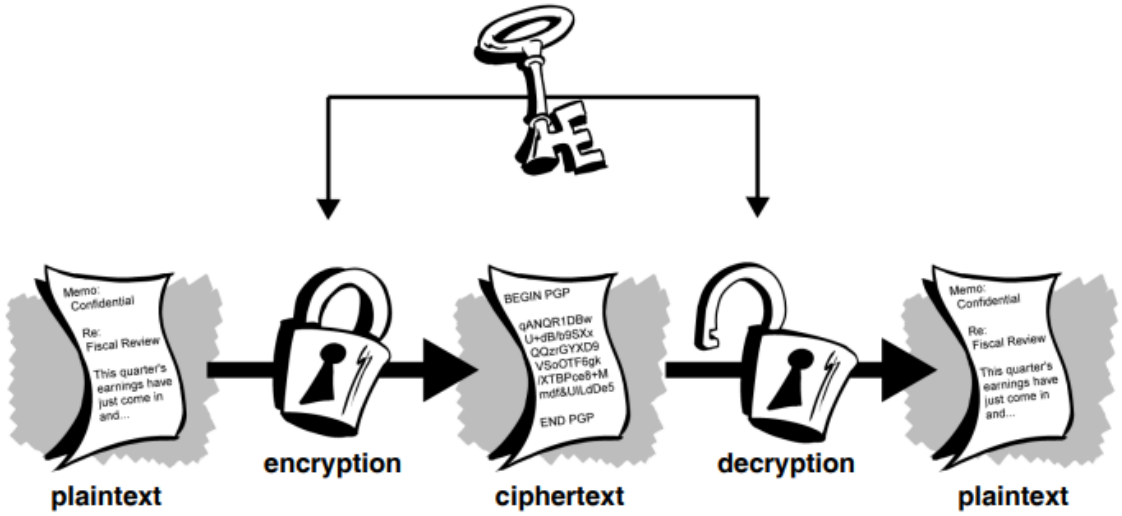
Kriptografija djeluje putem kriptografskog algoritma ili šifre, koji predstavlja matematičku funkciju koja se koristi u procesu šifriranja i dešifriranja. Kriptografski se algoritmi koriste zajedno s ključevima koji mogu biti riječi, brojevi ili izrazi kako bi se tekst šifrirao. Sigurnost šifriranih podataka u potpunosti ovisi o snazi kriptografskog algoritma kao i o tajnosti ključa kojim se služi za dešifriranje teksta ili podataka. Kriptografski algoritam i ključevi te

protokoli putem kojih algoritam djeluje nazivaju se kriptosustav (PGP, 2002). Kriptosustav je uređena petorka (α, σ, κ, ε, φ) za koju vrijedi:

- α je konačan skup svih mogućih osnovnih elementa otvorenog teksta,
- σ je konačan skup svih mogućih osnovnih elemenata šifrata,
- κ je prostor ključeva, tj. konačan skup svih mogućih ključeva,
- za svaki K ∈ κ postoji funkcija šifriranja eK ∈ ε i odgovarajuća funkcija dešifriranja dK ∈ φ. Pritom su eK : α → σ i dK : σ → α funkcije sa svojstvom da je dK(eK(x)) = x, za svaki otvoreni tekst x ∈ α (Barić, Grgić i Jurić, 2020).

Konvencionalna kriptografija, također nazvana i šifriranje tajnim ključem ili šifriranje simetričnim ključem koristi samo jedan ključ i za šifriranje i za dešifriranje (Slika 3.).

Slika 3. Primjena ključa za šifriranje i dešifriranje



Izvor: Izvor: PGP, 2002

Tri najpopularnija kriptografska sustava su Data Encryption Standard ili DES, Pretty Good Privacy ili PGP te Rivest, Shamir, Adleman sustav ili RSA (Onwutalobi, 2011). DES koristi jedan ključ i za šifriranje i za dešifriranje te gaje razvila International Business Machines Corporation i odobren je od strane Sjedinjenih Američkih Država 1976. godine. Rivest, Shamir, Adleman algoritam je popularna metoda šifriranja koja koristi dva ključa. Razvijen je za opću uporabu 1977. godine i nazvan je po tri računalna znanstvenika: Ronaldu L. Rivestu, Adi Shamiru i Leonardu Adlemanu koji su ga stvorili. Pretty Good Protection algoritam

također koristi dva ključa te se temelji na RSA algoritmu. PGP je izumljen od strane softverskog programera Philipa Zimmermana i jedan je od najčešće korištenih kriptosustava na svijetu jer je učinkovit, besplatan i jednostavan za korištenje (Onwutalobi, 2011).

Kriptografija predstavlja jedan od temeljnih koncepata kriptovaluta, te riječ „kripto“ (eng. *crypto*) znači skriveno ili tajno. Ovisno o svojoj konfiguraciji, tehnologija kriptografije može osigurati ili pseudoanonimnost ili potpunu anonimnost. U kontekstu kriptovaluta kriptografija se koristi zbog toga jer ona jamči sigurnost transakcija i korisnika kriptovaluta i kriptoplatformi, neovisnost poslovanja od središnjeg tijela te zaštitu korisnika od dvostrukog trošenja (Seth, 2022). Još neke od primjena kriptografije u kontekstu kriptovaluta su osiguravanje različitih vrsti transakcija koje se odvijaju na mreži, kontrola generiranja novih valuta i provjeravanje prijenosa digitalne imovine i tokena.

Kriptovalute koriste kriptografiju u tri glavne svrhe: za osiguranje transakcija, za kontrolu stvaranja dodatnih jedinica ili novčića i za provjeru prijenosa imovine. Kako bi postigle sve ove stvari, kriptovalute se oslanjaju na ono što se naziva kriptografija s javnim ključem (World Crypto Index, 2023). Kriptografija s javnim ključem podrazumijeva da korisnik ima i javni i privatni ključ. Oba su šifrirana i predstavljaju nasumični niz brojeva i slova. Ovi ključevi obično imaju oko 30 slova ili brojki. Svrha javnog ključa je dati ljudima adresu na koju mogu poslati novac, a svrha privatnog ključa je otključavanje javnog ključa kako bi se primio novac koji je poslan. Na taj način samo osoba koja zna privatni ključ može otključati javni ključ.

Svatko može uplatiti novac na javni ključ, to jest adresu, ali samo osobe s privatnim ključem mogu pristupiti novcu. Kriptografija s javnim ključem omogućuje ljudima da primaju novac i pristupaju mu bez da drugi ljudi mogu pristupiti novcu. Kriptografija s javnim ključem je tehnološko čudo i brzo mijenja industriju plaćanja na mreži, iako se primjenjuje već od sedamdesetih godina dvadesetog stoljeća (World Crypto Index, 2023).

Kriptografija s javnim ključem značajna je jer omogućuje dvije pojave:

- Šifriranje i dešifriranje. Podaci koji se šalju između dvije strane koje komuniciraju, to jest između pošiljatelja i primatelja, mogu se sakriti pomoću enkripcije i ponovno otkriti putem dekripcije. Prije samog slanja podataka pošiljatelj ih šifrira, a nakon primitka podataka primatelj ih dešifrira. Navedeni podaci ne mogu biti dešifrirani od strane trećih osoba dok se nalaze u transakciji.

- Neporicanje. Ova pojava označava mogućnost slanja podataka bez mogućnosti da pošiljatelj kasnije tvrdi da nikada nije poslao podatke, to jest novac, što pruža sigurnost transakcije (Franciscu i sur., 2022).

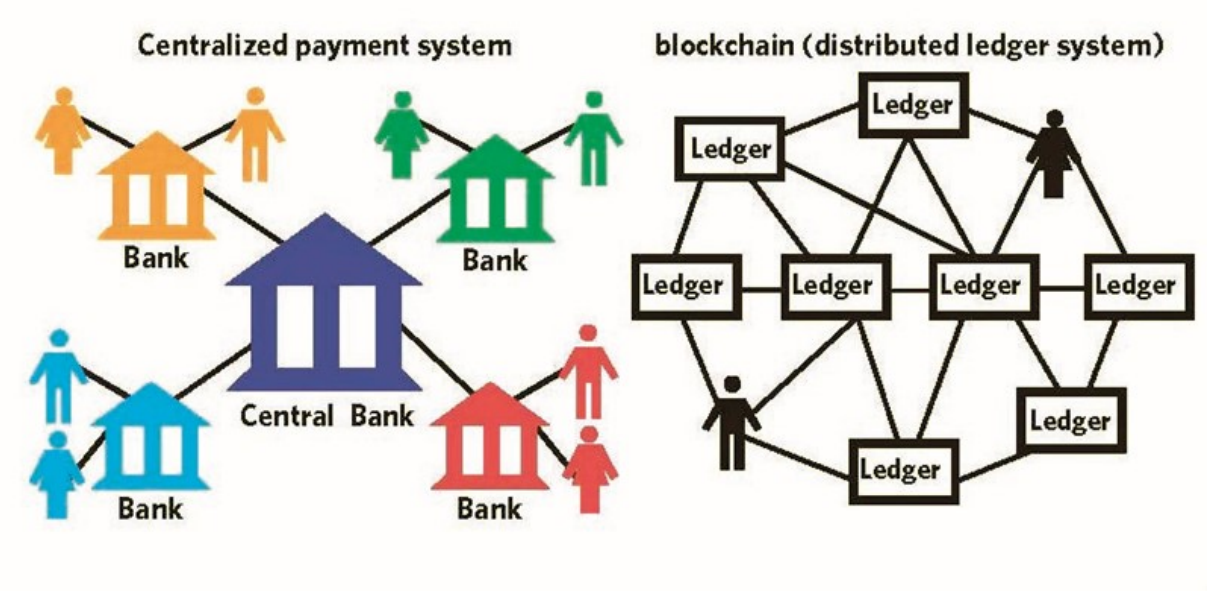
Cjelovitost poruka kreiranih u protokolu je osigurana korištenjem kriptografije s javnim ključem. Ovaj način šifriranja uvelike se koristi u izradi novčanika i potpisivanju transakcije, koje su temeljni elementi svake kriptovalute. Algoritam digitalnog potpisa eliptične krivulje (ECDSA), koji koristi Bitcoin protokol, generira nove skupove privatnih ključeva i odgovarajućih javnih ključeva. Javna adresa koju Bitcoin korisnici koriste za slanje i primanje novac se izrađuje pomoću javnog ključa i algoritma raspršivanja, a kako bi se osigurala legitimnost podrijetla digitalne transakcije i za potpisivanje transakcija, privatni ključ se mora držati tajnim.

Najveća ranjivost s kojom se tehnologija kriptografije s javnim ključem suočava su situacije u kojima korisnici slučajno izgube svoje ključeve ili otkriju svoj privatni ključ drugim ljudima. Ako osoba izgubi svoj privatni ključ, neće moći povratiti sredstva koja bi mogla biti u njegovom ili njezinom novčaniku. Ako osoba slučajno otkrije informacije o svom privatnom ključu trećoj strani, tada bi ta treća strana hipotetski mogla pristupiti računu i ukrasti sve kriptovalute koje se nalaze u novčaniku te osobe.

3. Blockchain tehnologija

Blockchain predstavlja tehnologiju javne knjige (eng. *ledger*) ili skupa zapisa koja se može programirati za zapisivanje i praćenje bilo čega vrijednog kao što su financijske transakcije, medicinska dokumentacija, vlasništvo nad zemljom i tako dalje. Blockchain tehnologija se temelji na metodi primjene javne knjige u poslovanju i financijama. Blockchain je digitalna knjiga koja čuva evidenciju svih vrsta transakcija koje se događaju u peer-to-peer mreži. Blockchain tehnologija specifična je po tome što, kada se ona koristi prilikom transakcija, više ne postoji potreba za posrednikom, to jest trećom osobom za provođenje ili autoriziranje transakcije ili prijenosa digitalne imovine (slika 4.). Blockchhain zapravo predstavlja sigurniji i decentralizirani medij (Miah i sur., 2019).

Slika 4. Usporedba između platnog sistema putem posrednika i blockchain platnog sistema bez posrednika

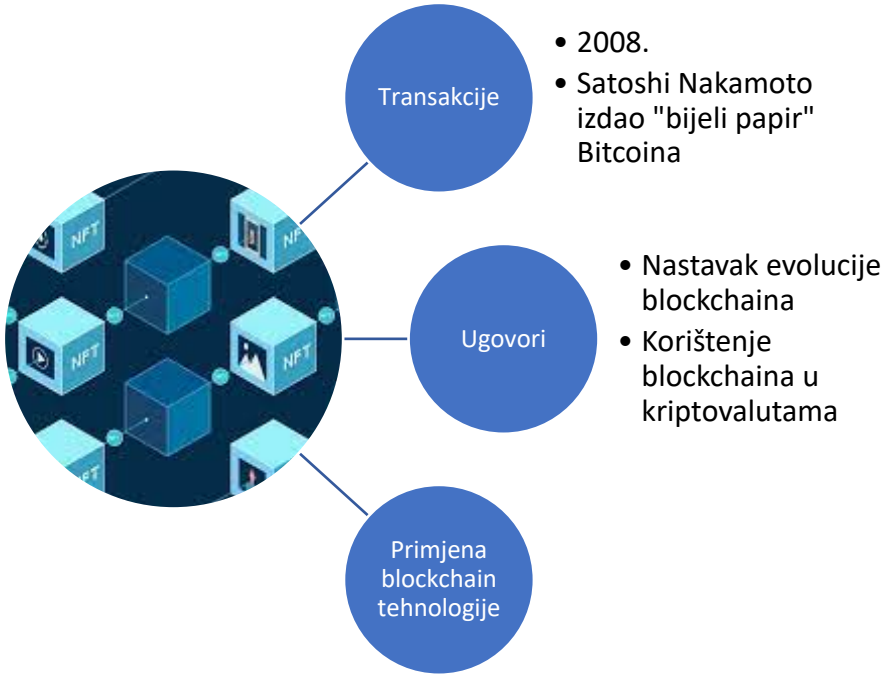


Izvor: Arunović, D. (2018). Što je u stvari blockchain i kako radi?. Dostupno na: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (6.3.2023)

3.1. Povijest blockchaina

Povijest blockchaina se može podijeliti u 3 faze: transakcije, ugovori i primjena blockchaina (slika 5.).

Slika 5. Povijest blockchaina



Izvor: Miah i sur., 2019

U fazi blockchaina koja je najviše okarakterizirana transakcijama koje su se odvijale putem blockchaina i koja je trajala od 2008. godine do 2013. godine glavna svrha blockchaina bila je izvršavanje peer-to-peer transakcija. Tijekom ove faze Bitcoin je bila najpopularnija implementacija blockchain tehnologije, a blockchain se također primjenjivao i u rudarenju novčića (Miah i sur., 2019).

Vremenski okvir za fazu ugovora pojavljuje se između 2013. i 2015 godine. U ovoj fazi zapažen je još jedan potencijal blockchain tehnologije: mogućnost blockchaina da omogući provođenje transakcija bez potrebe za posredovanjem treće osobe. Decentralizacija je stoga bila ključna značajka ove faze. Dok je bila u fazi transakcije, komunikacija se uglavnom odvijala na peer-to-peer bazi, ali ovdje je korištena na distribuirani način. Također je široko korištena i tehnologija pametnih ugovora. Pametni ugovori omogućili su da se blockchain proširi iz konteksta kriptovaluta do konteksta upotrebe u decentraliziranim aplikacijama.

Vitalik Buterin bio je jedan od prvih programera koji je shvatio primjenjivanje blockchaina na ovaj način, te je započeo izgradnju nove javne blockchain mreže, nazvane Ethereum, koja može obavljati razne funkcije uz djelovanje kao peer-to-peer mreža. Ova verziju blockchain tehnologije zove se Blockchain 2.0 (Miah i sur., 2019).

Treća faza povijesti blockchaina okarakterizirana je daljnjom primjenom blockchain tehnologije u situacijama koje nisu samo kriptovalute ili decentralizirane aplikacije poput Ethereuma. U posljednjih nekoliko godina sve se više projekata osmišlja uz pomoć blockchain tehnologije, a posebice u razdoblju nakon 2018. godine. Blockchain tehnologija se također dodatno razvila i na način da je počela implementirati tehnologiju biometrijske komplementacije kao što je prepoznavanje lica i glasa te podudaranje otisaka prstiju. Blockchain tehnologija se počela koristiti i u internetu stvari (IoT), koji predstavlja mrežu povezanih uređaja. Internet stvari se spaja s blockchain platformama te posljedično tome sve je više novih platformi i aplikacija počelo koristiti blockchain u svojim operacijama i aktivnostima (Miah i sur., 2019).

3.2. Temeljne karakteristike blockchaina

„Blockchain je distribuirana elektronička knjiga zapisa koja ne zahtijeva centralno mjerodavno tijelo da bi jamčila vjerodostojnost pohranjenih podataka. Takva se tehnologija počela koristiti s bitcoin kriptovalutom kako bi omogućila prijenos digitalne bitcoin valute bez potrebe za pouzdanim posrednikom. Međutim, blockchain tehnologija ubrzo je nadrasla bitcoin te je proširila svoju primjenu na mnoga druga područja“ (Dešić i Lenac, 2020). U ovom se radu fokusira na primjenu blockchain tehnologije u kriptovalutama iako se ona ne koristi samo za kriptovalute. Temeljna obilježja blockchain sustava su:

- Svaki sustav koji se koristi blockchain tehnologijom za svoje djelovanje djeluje po principu sustava ravnopravnih partnera (eng. *peer-to-peer* ili P2P)
- Blockchain predstavlja decentralizirani sustav u kojemu više ne postoji potreba za središnjim autoritetom ili trećom osobom koja bi nadgledala provođenje transakcije ili omogućila samo provođenje transakcije
- Svaki novi zapis u blockchainu je u realnom vremenu distribuiran između velike količine čvorova (eng. *nodes*) unutar P2P sustava
- Kako bi se identificirali sudionici ili korisnici sustava i za sam sustav transakcija koristi se tehnologija kriptografije, to jest šifriranja

- Čvorovi u sustavu mogu dodavati podatke u sustav
- Čvorovi koji se nalaze u sustavu mogu čitati podatke iz blockchaina
- Blockchain sustav napravljen je tako da onemogućuje stvaranje promjene nad podacima (Cunjak Mataković i Mataković, 2018).

3.3. Tipovi blockchaina

Postoje različite vrste blockchaina koje se mogu svrstati u tri skupine prema svojim glavnim karakteristikama: blockchain bez dopuštenja (eng. *permissionless* blockchain), blockchain s dopuštenjem (eng. *permissioned* blockchain) te hibridni blockchain. Blockchain bez dopuštenja omogućuje bilo kojem korisniku da se pseudoanonimno pridruži mreži blockchaina, to jest da na taj način postanu čvorovi u mreži. Na ovaj način blockchain ne ograničava prava čvorova na svojoj mreži (Wegryzyn i Wang, 2021). Suprotno tome, blockchainovi s dopuštenjem ograničavaju pristup mreži nekim određenim čvorovima, a također mogu ograničiti prava tih čvorova na toj mreži. Identiteti korisnika blockchaina s dopuštenjem poznati su drugim korisnicima tog dopuštenog blockchaina. Blockchainovi bez dopuštenja obično su sigurniji od blockchainova s dopuštenjem, jer postoji mnogo čvorova za provjeru valjanosti transakcija, a korisnicima koji imaju namjere koje bi imale negativni utjecaj na blockchain mrežu bilo bi teško tajno se dogovarati na mreži upravo zbog učestalosti provjera transakcija. Međutim, blockchain bez dopuštenja ima negativnu stranu koja se odražava u tome da mu treba dugo vrijeme za obradu pojedine transakcije zbog velikog broja čvorova i velike veličine transakcija. Suprotno blockchainovima bez dopuštenja, blockchainovi s dopuštenjem obično su učinkovitiji. Učinkovitiji su iz razloga da, budući da je pristup mreži ograničen, postoji i manje čvorova na blockchainu, što rezultira kraćim vremenom obrade po transakciji (Wegryzyn i Wang, 2021). Postoje četiri vrste blockchain struktura:

- Javni blockchain. Javni blockchainovi po prirodi su blockchainovi bez dopuštenja te dopuštaju svakome tko to želi da se pridruži i potpuno su decentralizirani. Javni blockchainovi omogućuju svim čvorovima na mreži jednaka prava pristupa blockchainu, stvaranje novih blokova podataka i provjeru valjanosti blokova podataka. Javni se blockchainovi trenutačno poglavito koriste u svrhu razmjenjivanja, to jest transakcija i rudarenja različitih kriptovaluta. Glavni javni blockchainovi su oni koji omogućuju postojanje i korištenje kriptovaluta kao što su Bitcoin, Ethereum i

Litecoin. Na sličnim javnim blockchainovima čvorovi rudare kriptovalute stvaranjem blokova za transakcije koje se pokušavaju pronaći na mreži rješavanjem kriptografskih jednadžbi. Čineći ove aktivnosti i sudjelujući u njima čvorovi rudara zarađuju malu količinu kriptovalute. Rudari se mogu smatrati bankovnim šalterima suvremenog doba koji formuliraju transakciju i primaju (ili rudare) naknadu za svoj trud (Wegryzyn i Wang, 2021).

- Privatni (ili upravljani) blockchain. Privatni blockchain, koji se također može nazvati i upravljanim blockchainom, predstavlja blockchain s dopuštenjem koji se nalazi pod kontrolom određene organizacije. U ovakvoj vrsti blockchaina središnje tijelo određuje tko može biti čvor. Središnje tijelo daje svakom čvoru različita prava za obavljanje funkcija, to jest različite ovlasti. Privatni blockchainovi samo su djelomično decentralizirani jer je javni pristup tim blockchainovima ograničen. Neki primjeri privatnih blockchainova su mreža za razmjenu kriptovaluta između poduzeća Ripple i Hyperledger (Wegryzyn i Wang, 2021). Važno je napomenuti kako i privatni i javni blockchainovi imaju nedostatke. Naime, javni blockchainovi obično imaju dulje vrijeme provjere valjanosti za nove podatke od privatnih blockchainova, a privatni blockchainovi su osjetljiviji na prijevare i korisnike s negativnim namjerama, to jest imaju lošiji sustav koji bi osiguravao takav blockchain od navedenih rizika. Kako bi se riješili ti nedostaci, razvijeni su konzorcijski i hibridni blockchainovi.
- Konzorcijski blockchain. Konzorcijski blockchainovi su blockchainovi s dopuštenjem kojima upravlja grupa organizacija, a ne samo jedna organizacija, kao u slučaju privatnog blockchaina. Stoga konzorcijski blockchainovi imaju i omogućuju veću decentralizaciju od privatnih blockchainova, što rezultira višim razinama sigurnosti. No, važno je napomenuti kako uspostavljanje konzorcijskih blockchainova može biti kompliciran proces jer zahtijeva suradnju između različitih organizacija, što predstavlja logističke izazove, kao i potencijalni antimonopolski rizik. Nadalje, neki članovi opskrbnog lanca možda nemaju potrebnu tehnologiju niti infrastrukturu za implementaciju blockchain alata i tehnologije, a oni koji imaju mogu odlučiti da su početni troškovi pokretanja konzorcijskog blockchaina previsoka cijena za digitalizaciju svojih podataka i povezivanje s drugim članovima opskrbnog lanca. Popularan skup konzorcijskih blockchain rješenja za industriju financijskih usluga i šire razvila je tvrtka za poslovni softver R3 (Wegryzyn i Wang, 2021).
- Hibridni blockchainovi. Hibridni blockchainovi predstavljaju blockchainove koje kontrolira jedna organizacija, ali uz razinu nadzora koju obavlja javni blockchain,

dakle kao blockchain bez dopuštenja, koji je potreban za obavljanje određenih validacija transakcija (Wegryzyn i Wang, 2021).

3.4. Kako blockchain funkcionira

Blockchain mrežu koja se koristi u kontekstu kriptovaluta čine korisnici i rudari, o kojima će biti više govora u slijedećem poglavlju. No, važno je spomenuti kako se korisnici kriptovaluta oslanjaju na rad rudara jer oni održavaju sustav i bilježe transakcije, a rudari se također oslanjaju na korisnike jer korisnici rade transakcije na čijim potvrdama rudari mogu zaraditi nove novčiće odabrane kriptovalute (Arunović, 2018).

Sudionici u mreži, to jest korisnici i rudari, se natječu za dopuštenje za dodavanje nove serije transakcija u decentraliziranu bazu podataka, to jest blockchain. Sudionici koriste snagu svog računala kako bi riješili određenu zagonetku. Rješenje, koje se smatra dokazom rada, nemoguće je pronaći analitički; do njega se može doći samo putem pokušaja i pogrešaka. Prva osoba koja riješi navedenu zagonetku može dodati blok novih transakcija u lanac postojećih transakcija—otud izraz blockchain—i stvoriti novi blok mreži, tako da svi sudionici mogu ažurirati blockchain u svojoj kopiji mreže. Iako je zagonetku teško riješiti, njezino je rješenje lako provjeriti. Stoga čvorovi u mreži kriptovaluta mogu lako odrediti je li predloženi blok valjan i treba li ga dodati u lanac. Čak i ako čvor neko vrijeme bude izvan mreže vremena, mreža nije ugrožena. Kada se čvor vrati na mrežu, on prihvaća najduži valjani lanac kao ispravan.

Ako je većina snage računala u vlasništvu poštenih sudionika, to jest sudionika s namjerama koje imaju pozitivne posljedice za mrežu, očekuje se da će oni stvarati najdulji lanac, jer je vjerojatnost da dodaju nove blokove proporcionalna snazi njihovog računala. Kao rezultat toga, najduži lanac može se smatrati konsenzusnim gledištem. Ako nepošteni sudionik, to jest sudionik čije namjere imaju negativne posljedice za mrežu doda blok koji drugi u lancu ne prihvaćaju, taj blok neće postati dio najdužeg lanca. Težina slagalice prilagođava se svaka dva tjedna, kako bi se stvorio otprilike jedan blok svakih 10 minuta. Ograničenje dodavanja novog bloka u blockchain na jedan svakih 10 minuta (u prosjeku) sprječava preopterećenje mreže i održava veličinu blockchaina promjenjivom (World Bank Group, 2018).

Blockchain tehnologija imala je glavnu ulogu u kreiranju koncepta kriptovaluta kao sistema novčanih transakcija koje se ne odvijaju putem treće strane ili posrednika. Nasuprot

tome, blockchain tehnologija dopušta da se podaci koji se nalaze u bazi podataka, to jest podaci o transakcijama kriptovaluta rasporede među nekoliko mrežnih čvorova na različitim lokacijama. Ovaj način pohrane podataka stvara sigurnu bazu podataka a također i održava vjernost podataka koji su u njoj pohranjeni (Hayes, 2022).

Naime, ako netko pokuša promijeniti zapis podataka u jednom čvoru, drugi čvorovi neće biti promijenjeni i tako će se spriječiti gubitak ili negativno iskorištavanje podataka. Također, ako jedan korisnik pokušava promijeniti podatke koji se tiču transakcija kriptovaluta, svi drugi čvorovi će se moći međusobno upućivati o toj promjeni podataka te lako odrediti čvor s netočnim informacijama. Ovaj sustav pomaže uspostaviti točan i transparentan redoslijed događaja. Na taj način niti jedan pojedinačni čvor unutar mreže ne može promijeniti informacije koje se unutar nje nalaze. Zbog ovog načina djelovanja blockchaina su informacije i povijest, kao što su transakcije kriptovaluta nepovratne (Hayes, 2022).

4. Rudarenje

Rudarenje kriptovaluta ključan je proces koji omogućuje sigurnost i funkcioniranje blockchain mreža. Središnji elementi ovog procesa su hashing i sam proces rudarenja. Hashing je postupak korištenja kriptografskih algoritama za pretvaranje ulaznih podataka u fiksno dugačak niz znakova, čime se osigurava da svaki blok u blockchainu bude jedinstven i nepromjenjiv. Proces rudarenja uključuje validaciju transakcija i dodavanje novih blokova u blockchain, pri čemu rudari koriste snažna računala za rješavanje složenih matematičkih problema (Freeman Law, 2022).

4.1. Hashing

Hash predstavlja matematičku operaciju koja mijenja unos bilo koje duljine u kodirani izlaz određene duljine, te je važno napomenuti kako je jedinstveni hash koji se koristi prilikom kriptografije u kriptovalutama uvijek iste veličine bez obzira na veličinu ili duljinu izvornih podataka ili povezanih datoteka. Hash funkcije su također jednosmjerne, to jest nemoguće ih je obrnuti ili dekriptirati (Onwutalobi, 2011). Tipične hash funkcije uzimaju ulaze promjenjive duljine da bi vratile izlaze fiksne duljine. Kriptografska hash funkcija kombinira mogućnosti prijenosa poruka hash funkcija sa sigurnosnim svojstvima. Hash funkcije su algoritmi koji određuju način šifriranja informacija (Frankenfield, 2023). Funkcija koja se koristi za generiranje hash-a je deterministička, što znači da će proizvesti isti rezultat svaki put kada se koristi isti unos.

Proces koji šifrira virtualni novac ili kriptovalute je poznat kao "algoritam kriptovalute" ili "hash algoritam." S obzirom da ih trenutno ima više kriptovaluta nego što postoji algoritama, određeni algoritmi mogu se primijeniti na različite kriptovalute, te se ti algoritmi slamaju prilikom procesa rudarenja koji će biti objašnjen u idućim poglavljima.

Hash funkcije su strukture podataka koje se često koriste u računalnim sustavima za zadatke kao što su provjera integriteta poruka i autentifikacija informacija. Kriptografske hash funkcije dodaju sigurnosne značajke, što otežava otkrivanje sadržaja poruke ili informacija koje bi se inače željele sakriti (Frankenfield, 2023). Kriptografske hash funkcije specifične su po svoje tri značajke:

- Nemaju svojstvo kolizije, što znači da se dva različita ulazna hashiranja ne mapiraju u isti izlazni hash

- Mogu biti skriveni, te je komplicirano otkriti ulaznu vrijednost za hash funkciju iz njezina izlaza
- Imaju svojstvo zagonetke, te bi trebalo biti komplicirano odabrati hash ulaz koji daje unaprijed definirani izlaz (Frankenfield, 2023).

4.2. Proces rudarenja

Rudarenje predstavlja distribuirani konsenzusni mehanizam koji se, uključivanjem u blockchain, koristi se za provjeru valjanosti transakcija koje su na čekanju. Putem rudarenja se provodi sekvencijalni poredak u blockchainu, a također se i čuva neutralnost mreže i omogućuje da stanje sustava bude posljedica rada različitih računala, čime se omogućuje povećana sigurnost. Transakcije bi trebale biti grupirane u blok koji odgovara iznimno strogim kriptografskim smjernicama koje organizacija provjerava te ga posljedično i odobrava. Ove smjernice zabranjuju prilagodbu prošlih blokova jer bi to poništilo svaki sljedeći blok. Rudarenje također sprječava bilo koju osobu da progresivno dodaje nove blokove u blockchain, jer bi se i zbog toga stvorili problemi u blockchainu (Pawar i sur., 2021).

Rudarenje kao koncept je jedan od temelja djelovanja kriptovaluta jer se transakcije kriptovaluta odvijaju u tri koraka:

- Izvršenje uplate. Kada osoba izvrši plaćanje bitcoinom ili nekom drugom kriptovalutom, poruka o transakciji šalje se mreži i prosljeđuje svim sudionicima mreže, to jest čvorovima. U ovom trenutku transakcija je nepotvrđena, što znači da su čvorovi procesuirali da je isplata pokrenuta. Čvorovi su postojanje transakcije potvrdili prema određenim tehničkim i poslovnim logičkim pravilima, ali ona nije još uvijek upisana u nečiju blockchain knjigu.
- Čekanje da se transakcija iskopa u bloku, što u prosjeku traje do 10 minuta. Rudari uzimaju popis nepotvrđenih transakcija i spajaju ih u blok, koji zapravo predstavlja popis transakcija i slične podatke. Zatim počinju raditi na rudarenju bloka na način da pokušavaju pogoditi nasumični broj. Ako dobro pogode, blok se objavljuje ostatku mreže. Računala na mreži potvrđuju da taj blok ispunjava kriterije, a zatim ga ili ignoriraju ili pohranjuju u svoje blockchaine. Natjecanje tada ponovno počinje s

nepotvrđenim transakcijama koje su se nakupile od tada. Mreža prilagođava težinu rudarenja tako da se svakih 10 minuta stvara blok, bez obzira na količinu računalne snage u mreži, odnosno broja transakcija.

- Čekanje da se više blokova iskopa na vrhu mreže, prosječno 10 minuta po bloku. Sljedeći blok je izrudaren na vrh bloka koji je označavao transakciju koji je korisnik napravio, te se novi blok referira na taj blok kao na prethodni, čime se i stvara blockchain. Što je više blokova iznad onog s transakcijom nekog korisnika to je ta transakcija više sigurna od različitih napada na podatke u blockchainu i na mreži (Lewis, 2015).

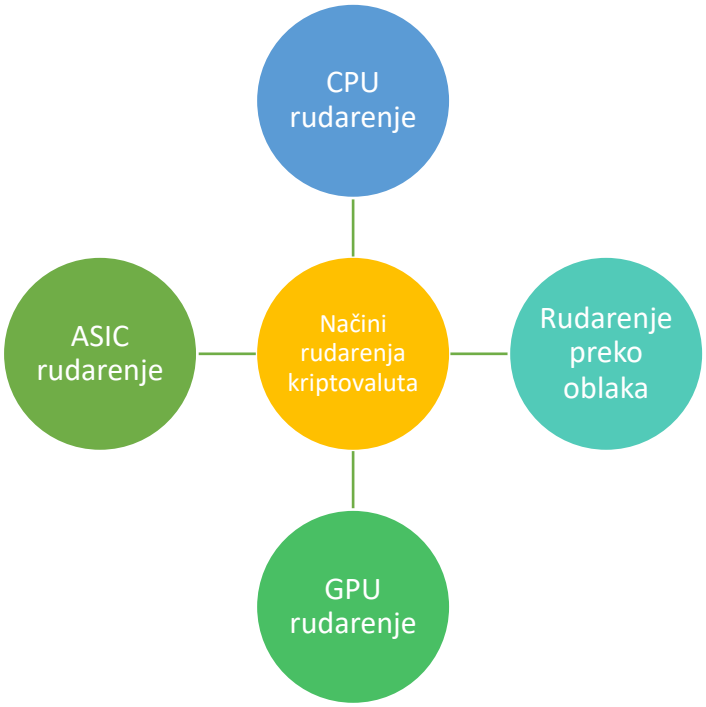
Rudarenje predstavlja ključan koncept za kriptovalute jer je potreban način da se transakcija unese u javnu knjigu, a također je potreban i način da se unošenje napravi zahtjevnim kako bi se napadači spriječili od dodavanja „nepoštenih" blokova. Transakcije se dodaju u knjigu u blokovima, stvarajući okvirni vremenski redoslijed za transakcije. U transakcijama kriptovaluta se ne može vjerovati vremenskoj oznaci bilo kojeg sudionika, tako da je redoslijed blokova ekvivalent vremenskog reda (Lewis, 2015).

Sprječavanje napadača od dodavanja blokova provodi se putem dokaza rada (eng. *proof of work*). Naime, za dodavanje blokova u blockchain pogađanje kroz koje rudari moraju proći kako bi dodali blok zapravo nije nužno, no pogađanje čini dodavanje blokova kompliciranim i zahtjevnim za računalo, a također i za korisnika. Ovaj trošak djeluje kao sredstvo zaustavljanja napadača koji bi inače htjeli dodati nepoštene blokove. Dokaz rada koristi se iz nekoliko razloga:

- Svatko može stvarati blokove na otvorenoj mreži.
- Nikome specifično se ne može vjerovati na mreži te zbog toga svaki pojedinačni čvor mora pretpostaviti da je većina mreže u pravu.
- Kako bi osoba dominirala mrežom ona zbog sustava čvorova mora stvoriti mnogo aliasa koji su svi pod vašom kontrolom i svi se međusobno slažu, što je jednostavno i lako napraviti.
- Kako bi mreža bila sigurna morao se stvoriti skuplji način stvaranja blokova, čime je nastalo rudarenje koje zahtijeva veliku računalnu snagu koja je skupa i zahtijeva ulaganje i održavanje. Posljedično tome, osobe s negativnim namjerama morat će potrošiti mnogo više novca da bi dominirali mrežom (Lewis, 2015).

Postoji nekoliko različitih strategija putem kojih se provodi rudarenje kriptovaluta (slika 6.).

Slika 6. Načini rudarenja kriptovaluta



Izvor: Pawar i sur., 2021.

CPU rudarenje specifično je po tome što zahtijeva samo CPU (eng. *central processing unit*) ili procesorske jedinice i nekoliko programa. Rudari su koristili standardne procesore kako bi nadvladali matematičke probleme u ranim danima postojanja kriptovaluta. U prošlosti se zahtijevala određena razina ulaganja kako bi se mogle rudariti različite vrste kriptovaluta, unatoč činjenici da su razine težine rudarenja bile manje nego danas. Stupnjevi težine se mijenjaju i rastu s vremenom te su iz tog razloga nastali drugi oblici rudarenja (Pawar i sur., 2021).

Rudarenje preko oblaka (eng. *cloud mining*) je trenutačno najpoznatiji način rudarenja kriptovaluta te je postao popularan zbog toga što omogućuje pojedincima koji nemaju dovoljno mogućnosti za kupovanje određenog hardvera koji je potreban za rudarenje ili ga samo ne žele kupiti da ipak sudjeluju u transakcijama vezanim uz kriptovalute, a sukladno tome i rudarenju. Rudarenje preko oblaka je tehnika pri kojoj osoba plaća određeni iznos gotovine drugoj osobi, a najčešće velikoj organizaciji kako bi iznajmila svoj stroj za rudarenje i sam proces rudarenja. Ovaj najam traje neki dogovoreni period, u pri čemu se sav prihod

koji je stvorio aparat premješta u korisnikov novčanik u kojem pohranjuje kriptovalute koje je izrudario. Osobe ili organizacije koje daju svoje strojeve za rudarenje u najam putem rudarenja u oblaku obično imaju na raspolaganju ogromne rudarske urede (Pawar i sur., 2021).

GPU rudarenje je poznato po svojoj jednostavnosti i zato je jedna od najznačajnijih strategija za rudarenje kriptovaluta. GPU rudarenje predstavlja jedan od najpriznatijih načina rudarenja kriptovaluta. GPU uređaji koriste kartice dizajna (eng. *designs cards*), te se putem jednog stroja izrađuju procesor, matična ploča, sustav za hlađenje, nacrt opreme i nekoliko ilustracijskih kartica. GPU uređaj vrijedi oko 3000 dolara (Pawar i sur., 2021).

ASIC rudarenje (eng. *application-explicit incorporated circuit* ili aplikacijski eksplicitni ugrađeni sklop) je napravljeno specifično za rudarenje Bitcoina i drugih oblika digitalnog novca. ASIC rudarenje poznato je po tome što u usporedbi s CPU i GPU načinima rudarenja rudarima pruža mogućnost zarade mnogo veće količine novca (Pawar i sur., 2021). ASIC-ovi koji se koriste u rudarenju uključuju mikroprocesore koji su posebno napravljeni i prikladni za rudarenje Bitcoina, Litecoina, Ethereum Classica i drugih kriptovaluta koje koriste algoritme dokaza rada. Ovi su sklopovi napravljeni za određenu primjenu, te su snažniji u pogledu računalne procesorske snage od središnjih procesorskih jedinica ili CPU-ova, koji su procesorske jedinice unutar osobnog računala, a također nadmašuju grafičke procesorske jedinice ili GPU-ove koje se nalaze uglavnom u računalima za igranje videoigrica.

Rudarenje se također može provoditi i putem web preglednika, te ova ideja postoji još od prvih dana postojanja Bitcoina. Međutim, s pojavom rudarenja temeljenog na GPU-u i ASIC-u, rudarenje bitcoina temeljeno na pregledniku, koje je 1,5 puta sporije od izvornog CPU rudarenja, postalo je neprofitabilno. U posljednjih nekoliko godina je nestao uzrok pada rudara kriptovaluta temeljenih na JavaScriptu. Naime zbog novih altcoina koji se mogu rudariti putem CPU-a i rastuće tržišne vrijednosti kriptovaluta, sada je ponovno isplativo rudariti kriptovalute s uobičajenim procesorima. 2017. Coinhive je bio prvi koji je preispitao ideju rudarenja u pregledniku. Programerima web stranica pružaju API-je za implementaciju rudarenja u pregledniku na njihovim web stranicama i za korištenje CPU resursa svojih posjetitelja za rudarenje altcoina Monero. Monero koristi CryptoNight algoritam [61] kao svoju kriptografsku zagonetku, koja je optimizirana prema rudarenju uobičajenim CPU-ima i pruža jaku anonimnost; stoga je idealan za kriptomarenje u pregledniku. Štoviše, razvoj novih web tehnologija koji se paralelno odvijao omogućuje učinkovitije, a time i profitabilnije, rudarenje u pregledniku (Konoth i sur., 2018).

5. Novčanik kao način korištenja kriptovaluta

Sustavi kriptovaluta održavaju svoje stanje u bazi podataka, to jest blockchainu. Stanje uključuje korisničke podatke kao i njihova stanja tokena. Kako bi promijenili svoje podatke, a posebice kako bi obavili transakcije vlastitih kriptovaluta, korisnici dodaju podatkovne strukture koje se nazivaju transakcije u blockchain. Kako bi se autentificirali, korisnici u transakciju uključuju dokaz svog identiteta, te je taj identitet obično pseudonim ili korisničko ime. Za razliku od uobičajenih centraliziranih sustava, o izboru metode autentifikacije odlučuju sami korisnici kriptovaluta (Eyal, 2021).

Korisnik definira transakcijom blockchaina predikat za autentifikaciju za pristup svojim kriptovalutama. Transakcija koja pristupa toj imovini mora uključivati ulaze kako bi taj predikat bio istinit. Predikat se naziva novčanik, a specificiran je u namjenskom programskom jeziku kao pametni ugovor. Obično novčanici zahtijevaju jedan ili više kriptografskih potpisa. Sigurnost novčanika, njegova vjerojatnost da neće zatajiti te da će transakcija kriptovaluta biti omogućena, se oslanja na čuvanje privatnih ključeva koje održava korisnik. U klasičnim sustavima poput bankovnih računa i kreditnih kartica, računi su identificirani i korisnici su osigurani od krađe na različite načine. No, mehanizmi koje banke koriste ne mogu se primijeniti na kriptovalute te bi to također delegitimiziralo sam sustav kriptovaluta koji je značajan po tome da ne koristi posrednike pri transakcijama. No, nepostojanje posrednika i kreiranje sustava koji se bazira na aktivnostima korisnika znači da ako su privatni ključevi korisnika izgubljeni ili hakirani, on ili ona odmah gube pristup svojim sredstvima (Eyal, 2021).

Novčanik za kriptovalute, kao temeljni alat kojim se koriste korisnici koji namjeravaju komunicirati s blockchain mrežom i blockchain platformom, neizostavan je dio obavljanja transakcija kriptovalute. Tradicionalni novčanik koji se koristi u svakodnevnom svijetu pohranjuje fizički oblik vrijednosti bilo koje vrste valute kao što su kovanice, novčanice i plemeniti metali. Novčanik za kriptovalute, u usporedbi s tradicionalnim novčanikom, ne pohranjuje kriptovalute i može se smatrati pristupom koji korisnicima omogućuje komunikaciju s lancem zaključavanja radi pohranjivanja ili provjere podataka svake transakcije. Novčanik kriptovalute u Ethereumu ima tri bitne komponente:

- kao što su privatni ključ,
- javni ključ i
- adresa novčanika.

Privatni ključ, kao jezgra kripto-novčanika, je cijeli broj od 256 bita koji se generira nasumično i prikazuje kao 64-znamenkasti heksadecimalni niz. Prema žutom papiru Ethereuma, privatni ključ od 256 bita cijeli broj se nasumično generira tijekom stvaranja kripto novčanika. Iz sigurnosne perspektive, privatni ključ treba čuvati na sigurnom i dostupan samo korisnicima. Javni ključ novčanika je cijeli broj od 512 bita, prikazan u heksadecimalnom nizu od 128 znamenki i izračunat na temelju nasumično generiranog privatnog ključa putem algoritma digitalnog potpisa eliptičke krivulje, a specifična krivulja secp256k1 odabrana je i u Bitcoinu i Ethereum. Koristi se za provjeru autentičnosti povezanih digitalnih potpisa kako bi se utvrdilo pripadaju li informacije priopćene u transakciji vlasniku prava ili ne. Adresa novčanika je 160-bitni cijeli broj prikazan u 40-znamenkastim heksadecimalnim nizovima i rezultat je izračuna Keccak-256 hash funkcije odgovarajućeg javnog ključa (Ji, 2023).

Vrste novčanika za kriptovalute podijeljene su u više kategorija. Novčanik za kriptovalute može se klasificirati kao hladni novčanik ili vrući novčanik te se kategoriziraju prema svojoj povezanosti s internetom. Hladni novčanik može biti bilo koji fizički hardver poput papirnatog novčanika, tvrdog diska i USB uređaja koji sadrži privatni ključ. Korisnici mogu primijeniti enkripciju na većini hladnih novčanika kako bi osigurali sigurniju pohranu ključnih informacija. Osmišljen je kako bi spriječio hakiranje s interneta budući da se proces potpisivanja transakcija prenosi na uređaje korisnika i u tom trenutku nema veze s mrežnim poslužiteljem. Na temelju toga, čak i ako protivnik ubaci zlonamjerni softver u korisnička računala, ne može pristupiti niti ukrasti korisničke privatne ključeve. Vrući novčanik je kripto novčanik povezan s internetom, poput desktop novčanika, novčanika web aplikacije, mobilnog novčanika i drugih. Budući da je vrući novčanik izravno povezan s internetom, postoje moguće prilike za protivnike da napadnu korisničke račune, što može dovesti do curenja privatnih ključeva i gubitka digitalnog vlasništva, posebno za novčanike temeljene na webu. U usporedbi s hladnim novčanikom, u zamjenu za sigurnost, vrući novčanik kriptovaluta omogućuje korisnicima da ostanu online računi radi većih pogodnosti i brže reakcije na transakcije (Ji, 2023).

Ključne vrste vrućih novčanika kriptovaluta su desktop novčanik, web novčanik i mobilni novčanik. Desktop novčanik je aplikacija koja se preuzima i instalira na stolna ili prijenosna računala korisnika. Korisnici mogu izraditi kripto novčanik korištenjem aplikacije za generiranje parova ključeva i njihovo pohranjivanje u lokalni hardver. Aplikacija je često razvijena sa sažetim sučeljem koje je prilagođeno korisniku kako bi se korisnicima omogućio lakši pristup transakcijama. Omogućuje parove ključeva, spaja se na internet i prima adresu za

slanje kriptovalute dok korisnici moraju obavljati transakcije. Iz sigurnosne perspektive, korisnici mogu koristiti kombinaciju korisničkih imena i lozinki i primijeniti višestruku autentifikaciju za veću zaštitu. Osim toga, novčanik za stolno računalo obično pruža početnu frazu i frazu za oporavak, popis nasumično generiranih riječi koje korisnicima pomažu da povrate pristup novčaniku za stolna računala. Međutim, pohranjivanje ključa na lokalnom hardveru relativno je ranjivo jer se na taj način novčanik izlaže potencijalnom zlonamjernom softveru ili virusima u korisničkim uređajima.

Web novčanik ima manje zahtjeva za pristup budući da korisnik može pristupiti web novčaniku putem bilo kojeg pouzdanog internetskog preglednika na bilo kojem uređaju umjesto preuzimanja i instaliranja specijaliziranog softvera. Tvrtke treće strane koje stoje iza ovih novčanika web aplikacije pohranjuju informacije o novčaniku korisnika i postižu vlasništvo nad imovinom kriptovalute korisnika, što zahtijeva višu razinu povjerenja između korisnika i trećih strana. S druge strane, osmišljen je alternativni plan za rješavanje ove vrste problema. Korisnici mogu biti aktivni u ugovoru s više potpisa (eng. *multi-sig*) kako bi formirali novčanik s više potpisa, što osigurava da korisnici stječu dio vlasništva nad računom. Novčanik s više potpisa zahtijeva više ključeva za generiranje digitalnog potpisa i potpisivanje transakcije. Iz sigurnosne perspektive, web aplikacija ostaje cijelo vrijeme online i ranjivija je na potencijalni zlonamjerni softver i hakere. Stoga je web novčanik najmanje siguran novčanik za korištenje. Osim toga, neke treće strane zahtijevaju osobne podatke za registraciju, kao što su kontakt broj i adresa e-pošte, tako da je manje anonimnosti sadržano u web novčaniku iz sigurnosnih razloga (Suratkar, Shirole i Bhirud, 2020).

Mobilni novčanik zahtijeva od korisnika preuzimanje i instaliranje aplikacija na svoje telefone za slanje ili primanje kriptovalute. Korisnicima donosi višu razinu pogodnosti i fleksibilnosti za obavljanje transakcija. Iz sigurnosne perspektive, međutim, mobilni novčanik nudi nisku sigurnost i privatnost budući da je mobilni uređaj ranjiviji na zlonamjerni softver ili viruse i veća je vjerojatnost da će biti fizički oštećen, izgubljen ili ukraden. Osim toga, mobilni uređaji sadrže potrebne osobne informacije kao što su identitet i geološke informacije, što može dovesti do manje anonimnosti transakcija ako su pod zlonamjernim aktivnostima.

Vrste hladnog novčanika su papirnati novčanik kriptovaluta i hardverski novčanik. Papirnati novčanik može biti bilo koji komad na kojem su ispisane ključne informacije. Samo osoba s fizičkim pristupom papiru može posjedovati taj kripto novčanik. Sa sigurnosne točke gledišta, zbog svojstava materijal može biti fizički oštećen, uništen, izgubljen ili ukraden, što će korisnicima onemogućiti pristup njihovim kripto novčanicima.

Hardverski novčanik jedna je od najsigurnijih metoda za pohranjivanje informacija o vašem privatnom ključu. Većina hardverskih novčanika, poput USB pogona, potpuno je isključena s interneta kako bi se izbjeglo izlaganje ranjivosti potencijalnom zlonamjernom softveru ili hakerima. S druge strane, povećanje sigurnosti neće utjecati na fleksibilnost korištenja hardverskih novčanika za obavljanje transakcija. Korisnici samo trebaju povezati hardverski novčanik s bilo kojim računalom ili uređajem s omogućenim internetom kako bi potpisali i autorizirali transakciju. Štoviše, privatni ključ ostat će sigurno pohranjen u hardveru čak i ako je uređaj spojen na internet. Međutim, također se može izgubiti ili ukrasti, a većina hardverskih uređaja zahtijeva određene troškove (Suratkar, Shirole i Bhirud, 2020).

Digitalni novčanik za kriptovalute je softverski program koji drži javne i privatne ključeve i uspješno radi na različitim lancima blokova koji korisnicima omogućuju međusobnu razmjenu valuta i praćenje stanja njihove valute. Digitalni novčanik može pohranjivati, slati i primati različite valute. Kriptovalute se ne pohranjuju kao fizički (fiat) novac unutar novčanika. Svaka transakcija se bilježi i pohranjuje u blockchain. Slanje Bitcoina ili neke druge valute korisniku značilo bi slanje vlastitog javnog ključa. Ako korisnik treba primiti uplatu, njegov privatni ključ mora biti u skladu s javnim ključem pošiljatelja. Ne postoji prava razmjena kovanica. Transakcija je zaključena zapisom u blockchainu i promjenom korisničkog digitalnog novčanika. Ovi ključevi su dio kriptografije.

5.1. Sigurnost novčanika kriptovaluta

Dva su osnovna modela sigurnosti novčanika kriptovaluta: simetrični i asimetrični model. Simetrični model obično dolazi s tajnim ključem, a asimetrični model dolazi s javnim i privatnim ključem. Fokus će biti na asimetričnom modelu, jer se ovaj model često koristi u izvršavanju transakcija kriptovalutama. Asimetrična enkripcija je model šifriranja koji koristi različite algoritme enkripcije i dešifriranja kao i dva ključa koji su međusobno povezani (privatni i javni ključ). Pošiljatelj bi trebao imati kopiju javnog ključa primatelja, ali u tom slučaju mora se smatrati da napadač ima istu kopiju. U tom slučaju pošiljatelj šifrira poruku odgovarajućim algoritmom za šifriranje, a primatelj ima mogućnost dekriptirati poruku svojim privatnim ključem. Dakle, svrha ovog asimetričnog modela je da napadač ne može dešifrirati poruku koja je šifrirana javnim ključem (Jokić i sur., 2019).

Novčanik kriptovaluta kao i tradicionalni novčanik mogu se osigurati. U slučaju Bitcoina postoje različite funkcionalnosti prijenosa podataka. Ove stavke mogu biti sigurnosni problem, ali Bitcoin uključuje vrlo visoku razinu sigurnosti što podrazumijeva njihovu

pravilnu upotrebu. Kada je u pitanju plasiranje novca na online platforme, pozornost treba usmjeriti na njihovu sigurnost. U slučaju kupnje novčanika za ovu kriptovalutu, preporučuje se korištenje dvofaktorske autentifikacije. Pametan način pohranjivanja novca u novčanik može se usporediti s fizičkim novčanikom. To znači da digitalni kripto novčanik treba sadržavati malu količinu novca za svakodnevnu upotrebu. Rezervni novčanik samo je još jedan izraz za spremanje novca na nekom drugom mjestu ili izradu kopije. Backup wallet može spriječiti probleme koji proizlaze iz računalnih grešaka ili krađe podataka, ali ovaj zahtjev može biti ispunjen ako su podaci šifrirani. Podaci pohranjeni na mreži nisu sto posto sigurni. Zlonamjerni softver može utjecati na svako računalo spojeno na mrežu (Jokić i sur., 2019).

Važna sigurnosna praksa je da podaci trebaju biti šifrirani kako bi se izbjegla bilo kakva mogućnost da budu ugroženi. Treba ih pohraniti na nekoliko različitih mjesta. Kada je riječ o različitim lokacijama, ne radi se samo o mrežnoj pohrani, već i na hardverskim uređajima kao što su USB, CD, vanjski tvrdi disk itd. Enkripcija je vrlo važna za digitalne novčanike. Šifriranje digitalnog novčanika jedan je od najboljih načina da osigurate svoja sredstva koja su pohranjena u digitalnom novčaniku. Na taj se način postavlja lozinka ako netko pokuša pristupiti digitalnom novčaniku. Lozinka se ne smije izgubiti jer ako se to dogodi sredstva će biti izgubljena. Razlika između kriptovalute i pravog novca je u tome što ako dođe do gubitka lozinke, korisnik može zatražiti novu lozinku. U blockchainu i kriptovaluti, puna odgovornost je na korisniku. Vrlo je važno stvoriti jaku lozinku koja uključuje slova, znakove i brojeve (Jokić i sur., 2019).

6. Istraživanje stavova građana o utjecaju tehnologije na razvoj kriptovaluta

U ovom poglavlju se analiziraju percepcije i stavovi građana prema kriptovalutama te tehnologijama koje omogućuju njihov razvoj. Cilj istraživanja je razumjeti kako građani doživljavaju utjecaj tehnologija poput blockchaina, pametnih ugovora i decentraliziranih aplikacija na sigurnost, efikasnost i svakodnevnu upotrebu kriptovaluta.

6.1. Metodologija istraživanja

Istraživanje je provedeno tijekom 2023. godine putem web ankete koja je napravljena u Google Forms obliku. Ispitanici su prikupljeni prigodnim uzorkom na način da se link za anketu postavio u Facebook grupe studentskih domova u Zagrebu, a anketa je također proslijeđena poznanicima ispitivača te su ispitanici zamoljeni da anketu proslijede svojim poznanicima. Na taj način su se podaci također prikupljali putem uzorka snježne grude. Na početku ankete je navedena uputa ispitanicima:

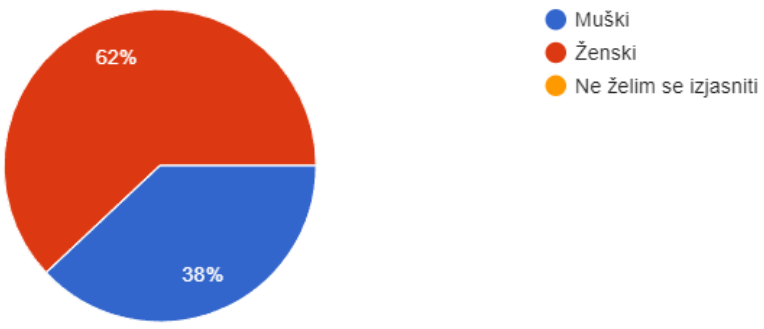
„Poštovani/Poštovana,

zahvaljujem Vam što ste odvojili vremena za ispunjavanje ovog anketnog upitnika. Istraživanje se provodi u svrhu pisanja diplomskog rada, te se ispituju stavovi studenata o utjecaju informacijske i komunikacijske tehnologije na razvoj tržišta kriptovaluta. U anketi nema točnih i netočnih odgovora, a najvažnija su vaša osobna iskustva i stavovi. Vrijeme ispunjavanja ankete je oko 5 minuta. Hvala Vam na sudjelovanju!“.

6.2. Rezultati istraživanja

Anketu je ukupno ispunilo 50 ispitanika. 38% ispitanika se izjasnilo kao muškarci kao odgovor na pitanje o spolu, a 31 osoba se izjasnila kao žena (62%). Nitko nije odabrao opciju „Ne želim se izjasniti“.

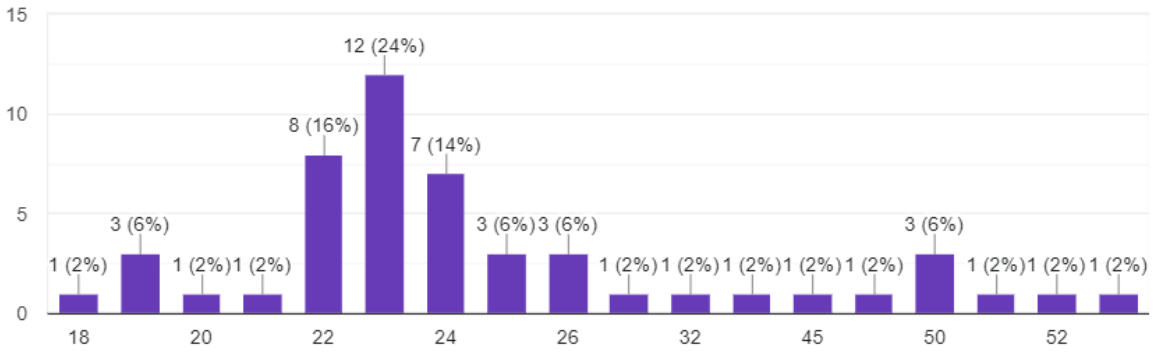
Grafikon 1. Spol ispitanika



Izvor: izrada autora

Pitanje Koliko godina imate? bilo je otvorenog tipa, te je vidljivo kako su ispitanici po svojim godinama bili u rasponu od 18 do 54 godine. Jedna je osoba odgovorila da ima 18 godina, 3 osobe 19, jedna je osoba imala 20 godina a jedna 21. Najviše ispitanika imalo je 23 godine u trenutku ispitivanja (24%), a zatim 22 godine (16%) i 24 godine (14%). 3 ispitanika imala su 25 godina, a također su se tri ispitanika izjasnila kako imaju 26 godina, kao i 50 godina. Ostalih 8 ispitanika navelo je kako imaju 27, 32, 36, 45, 48, 51, 52, i 54 godine.

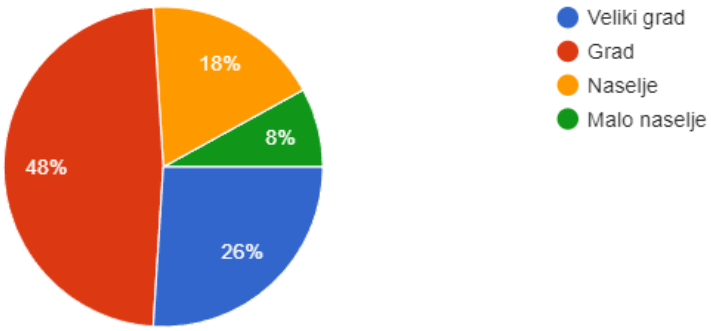
Grafikon 2. Koliko godina imate?



Izvor: izrada autora

Većina ispitanika se izjasnila kako živi u gradu (48%), a zatim je najviše ispitanika dolazilo iz velikog grada (26%). Najmanje ispitanika (8%) dolazilo je iz malog naselja, a 18% dolazi iz mjesta veličine naselja.

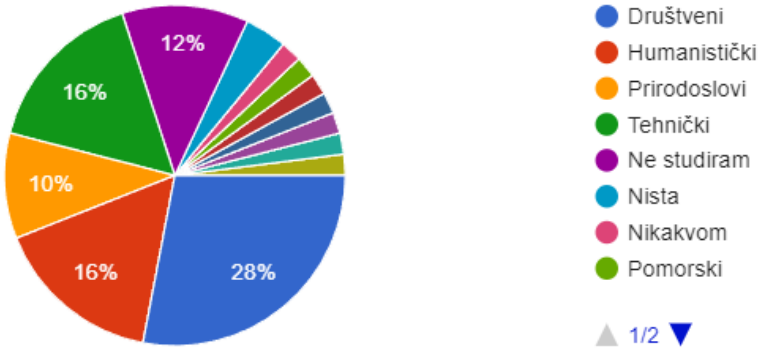
Grafikon 3. Iz kakvog mjesta dolazite?



Izvor: izrada autora

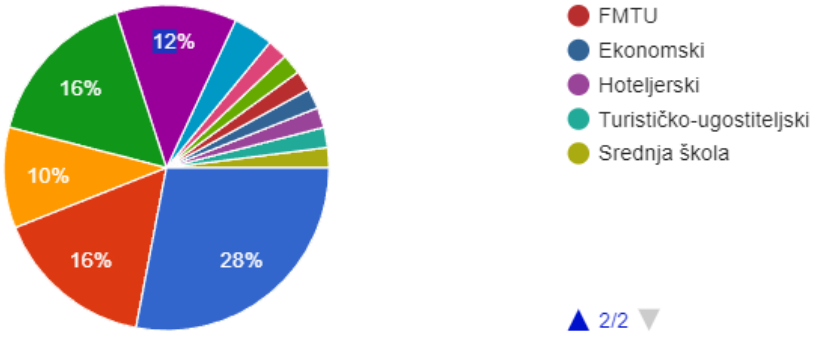
Na pitanje Na kakvom tipu fakulteta studirate ispitanici su mogli odabrati da studiraju na društvenom, humanističkom, prirodoslovnom ili tehničkom fakultetu ili opciju da ne studiraju a također su mogli odabrati opciju „Drugo“ te napisati na kojem fakultetu studiraju ili da nisu u statusu studenta. Najviše ispitanika navelo je kako studiraju na društvenom fakultetu (28%), a zatim na humanističkom fakultetu (16%) te je jednak broj studirao i na tehničkom fakultetu. 10% ispitanika studira na prirodoslovnom fakultetu. Ukupno 18% ispitanika navelo je kako ne studiraju. Jedan je ispitanik naveo kako pohađa srednju školu, jedan kako pohađa Pomorski fakultet, te jedan kako pohađa FMTU, Ekonomski fakultet, Hotelijerski fakultet ili Turističko-ugostiteljski fakultet.

Grafikon 4. Na kakvom tipu fakulteta studirate? 1/2



Izvor: izrada autora

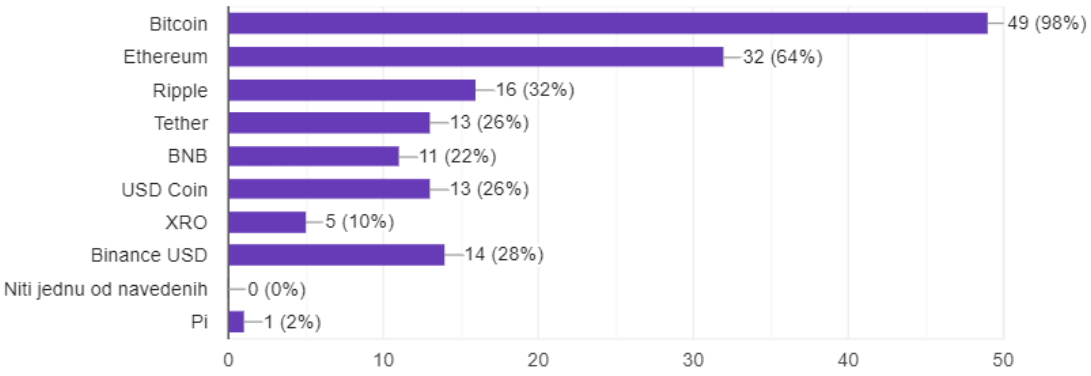
Grafikon 5. Na kakvom tipu fakulteta studirate? 2/2



Izvor: izrada autora

Najviše je ispitanika, njih 49, znalo za kriptovalutu Bitcoin (98%). Zatim je većina ispitanika (64%) navelo kako poznaju kriptovalutu Ethereum. 32% ispitanika navelo je kako poznaje kriptovalutu Ripple, a 26% poznaje Tether i USD Coin. 11 ispitanika poznaje kriptovalutu BNB, a 5 ispitanika kriptovalutu XRO. 28% ispitanika navelo je kako poznaje kriptovalutu Binance USD, a jedan ispitanik naveo je kriptovalutu Pi kao dodatnu opciju koju su ispitanici mogli sami upisati. Ni jedan ispitanik nije naveo da ne poznaje niti jednu od navedenih kriptovaluta.

Grafikon 6. Za koje kriptovalute znate?

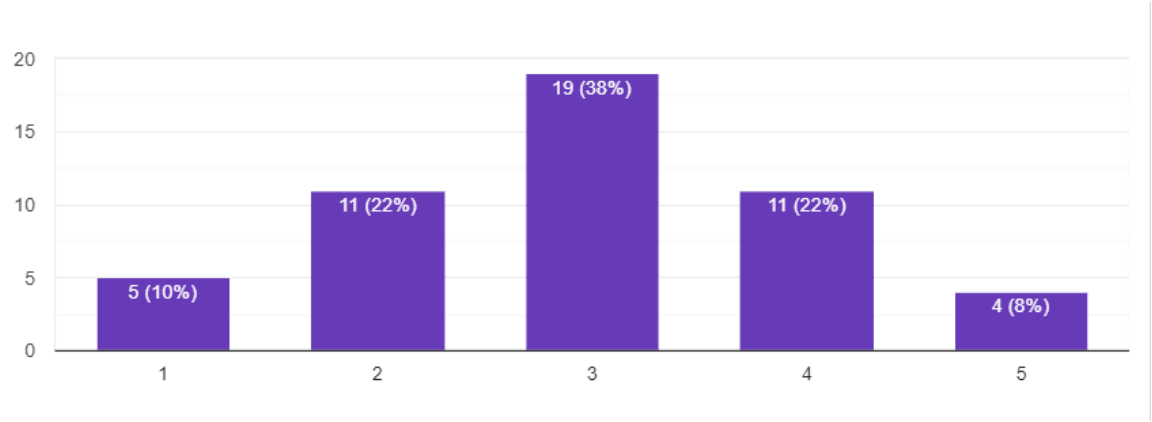


Izvor: izrada autora

Većina ispitanika (38%) ima nedefinirani stav o kriptovalutama. 11 ispitanika ili 22% ima ili relativno negativan ili relativno pozitivan stav prema kriptovalutama, a 5 ispitanika

iskazuje potpuno negativan stav prema kriptovalutama. 4 ispitanika navela su da imaju potpuno pozitivan stav prema kriptovalutama.

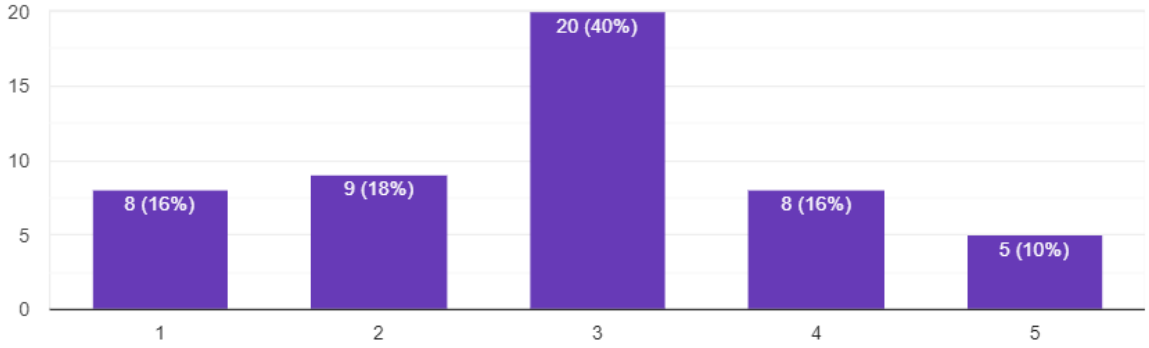
Grafikon 7. Koji je vaš stav o kriptovalutama?



Izvor: izrada autora

Većina ispitanika se niti ne slaže niti slaže s izjavom da su transakcije putem kriptovaluta povjerljive i transparentne (40% ili 20 ispitanika). 16% ispitanika navodi kako se djelomično slaže s tom izjavom, a 10% ispitanika se u potpunosti slaže s njom. 18% ispitanika navodi kako se djelomično ne slaže s navedenom izjavom, a 16% se nimalo ne slaže.

Grafikon 8. Transakcije putem kriptovaluta su povjerljive i transparentne.

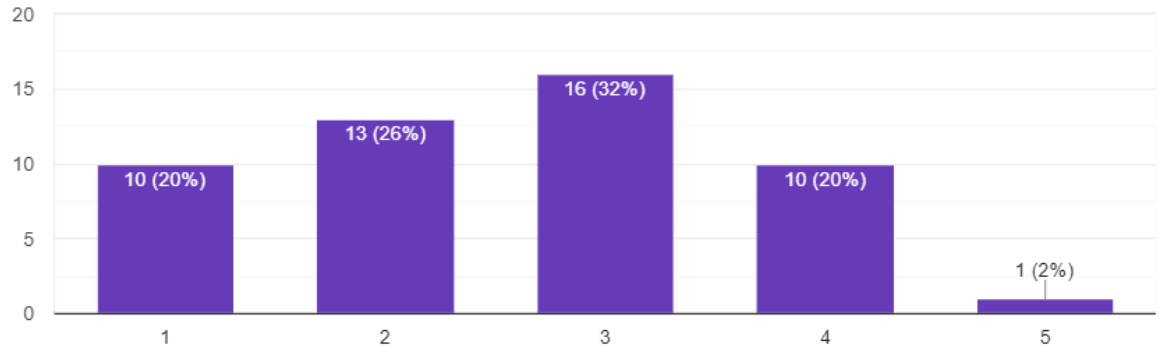


Izvor: izrada autora

Većina ispitanika navodi kako se niti ne slaže niti slaže s izjavom da je plaćanje kriptovalutama sigurnije od korištenja gotovine ili bankovnih kartica (32%), no ostatak

ispitanika pretežno je iskazao negativan stav prema ovoj izjavi. Naime, 26% ispitanika se djelomično ne slaže s tom izjavom, a 20% se nimalo ne slaže. 20% ispitanika se djelomično slaže s navedenom izjavom, a samo se jedan ispitanik u potpunosti slaže.

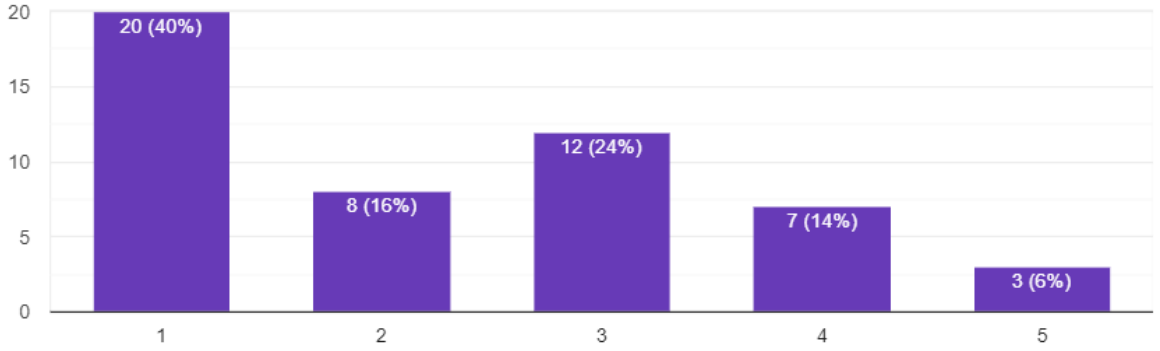
Grafikon 9. Plaćanje kriptovalutama sigurnije je od korištenja gotovine ili bankovnih kartica.



Izvor: izrada autora

40% ispitanika navodi kako se nimalo ne slaže s izjavom da mogu sa sigurnošću odrediti što znači pojam blockchain. 16% ispitanika navodi kako se djelomično ne slažu, a 24% ispitanika se niti ne slaže niti slaže s tom izjavom. 14% ispitanika navodi kako se djelomično slaže, a 3 ispitanika su navela kako sa sigurnošću mogu odrediti što znači pojam blockchain.

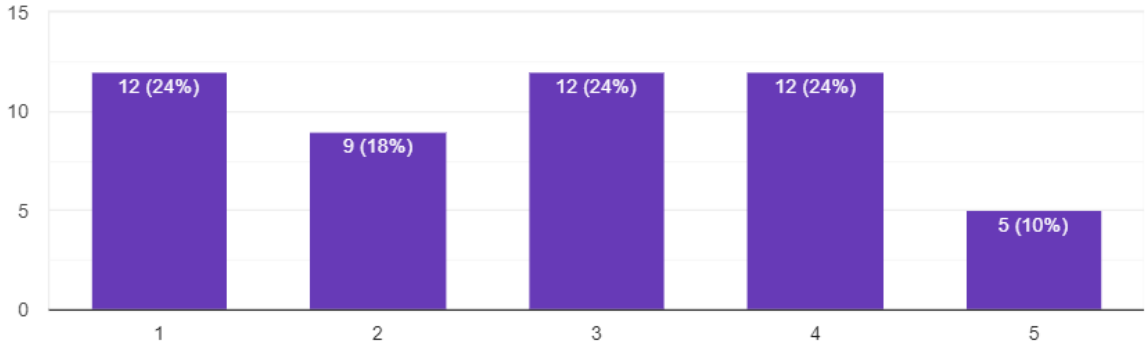
Grafikon 10. Mogu sa sigurnošću odrediti što znači blockchain.



Izvor: izrada autora

Ispitanici su u svojim stajalištima bili podijeljeni što se tiče odgovora na izjavu Mogu sa sigurnošću odrediti što znači rudarenje kriptovaluta. Isti broj ispitanika, njih 12 ili 24% navelo je kako se nimalo ne slažu s tom izjavom, kako se niti slažu niti ne slažu s tom izjavom ili kako se djelomično slažu s tom izjavom. 18% ispitanika navelo je kako se djelomično ne slaže s tom izjavom, a 5 ispitanika navelo je kako sa sigurnošću mogu navesti što je rudarenje kriptovaluta.

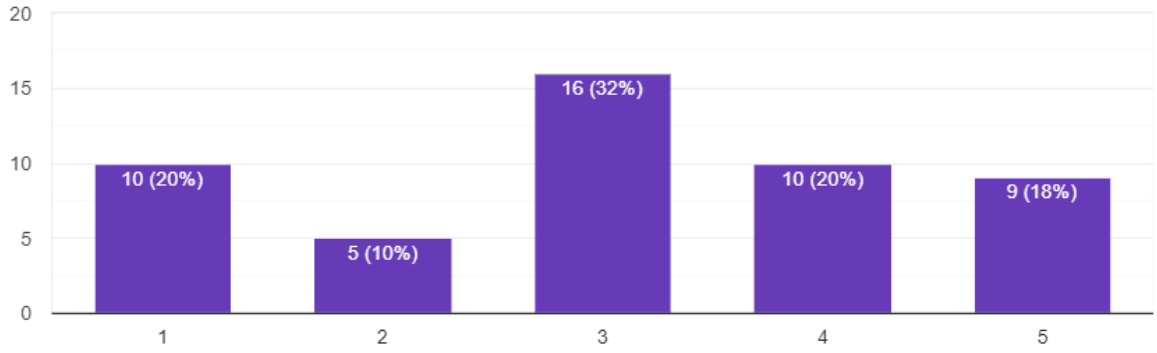
Grafikon 11. Mogu sa sigurnošću odrediti što znači rudarenje kriptovaluta.



Izvor: izrada autora

Ispitanici su većinom djelomično ili u potpunosti znali što je digitalni novčanik za kriptovalute. 32% je navelo kako se niti ne slaže niti slaže s izjavom da znaju što je digitalni novčanik za kriptovalute, a 20% se djelomično slagalo s tom izjavom. 18% ispitanika u potpunosti se slagalo s tom izjavom, a 20% ispitanika navelo je kako se u potpunosti ne slaže. 5 ispitanika navelo je kako se djelomično ne slaže s tom izjavom.

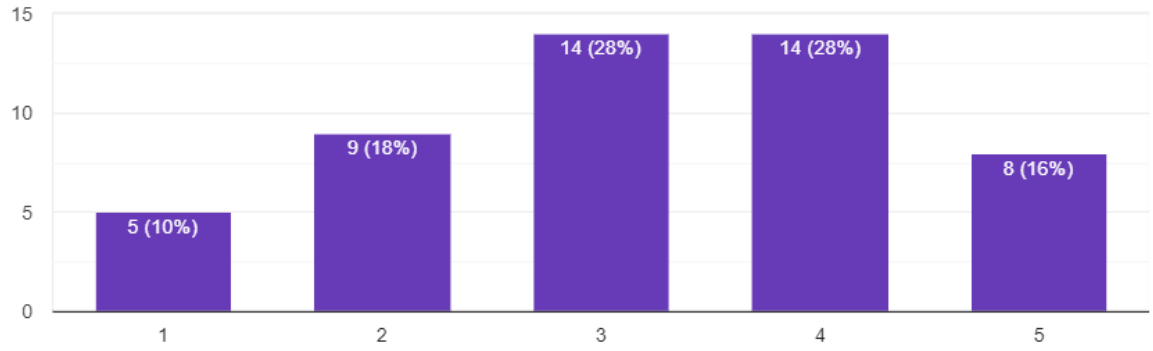
Grafikon 12. Znam što je digitalni novčanik za kriptovalute.



Izvor: izrada autora

28% ispitanika navelo je kako se niti ne slaže niti slaže s izjavom da će kriptovalute za 5 godina imati veću vrijednost nego danas, a isti broj ispitanika navelo je kako se djelomično slaže s tom izjavom. 18% ispitanika navelo je kako se djelomično ne slaže s tom izjavom, a 5 ispitanika se u potpunosti nije složilo. 16% ispitanika se u potpunosti slaže s navedenom izjavom.

Grafikon 13. Mislim da će kriptovalute za 5 godina imati veću vrijednost nego danas.

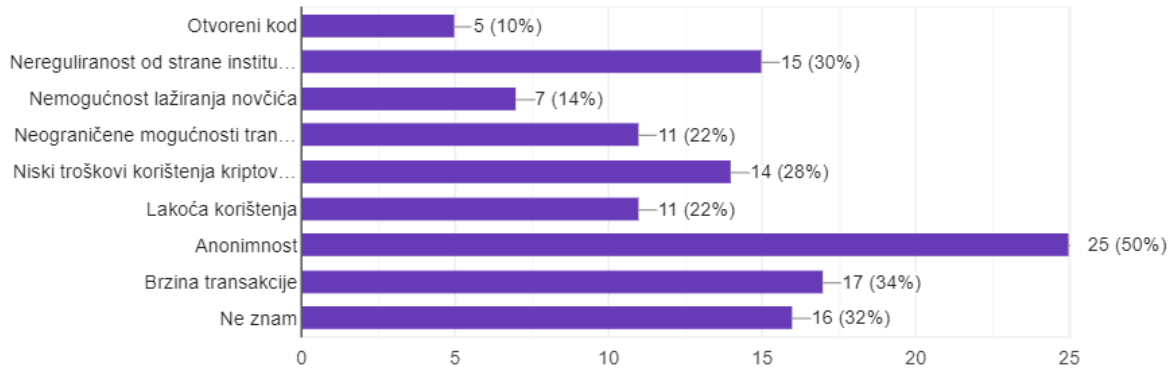


Izvor: izrada autora

Polovina ispitanika misli kako je anonimnost najveća prednost kriptovaluta, te je druge prednosti navelo značajno manji broj ispitanika. 30% ispitanika navelo je nereguliranost od strane institucija kao prednost, a 34% je navelo brzinu transakcije. 28% navodi niske troškove korištenja kriptovaluta, a 22% neograničene mogućnosti transakcije i lakoću korištenja. 5

ispitanika navelo je otvoreni kod kao prednost kriptovaluta, a 14% nemogućnost lažiranja novčića. 32% ispitanika navelo je da ne znaju koje su prednosti kriptovaluta.

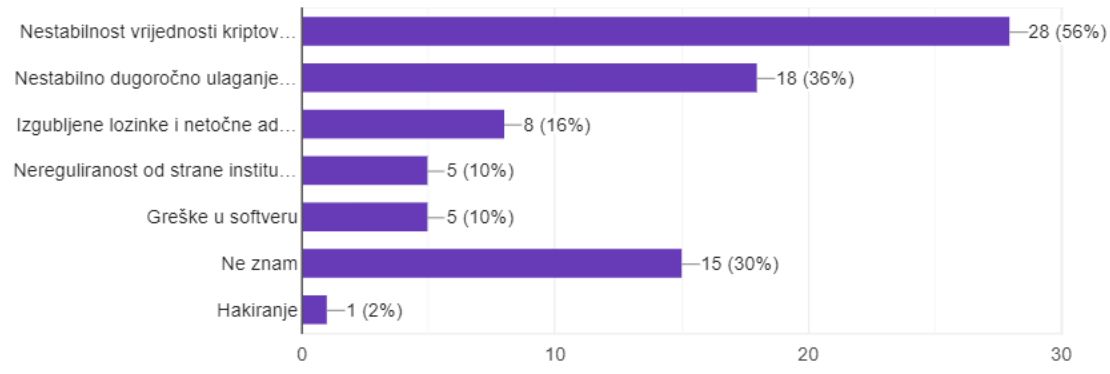
Grafikon 14. Što biste naveli kao najveću prednost kriptovaluta?



Izvor: izrada autora

Najviše ispitanika (56%) navelo je nestabilnost vrijednosti kriptovaluta kao najveći nedostatak kriptovaluta, a zatim je slijedilo nestabilno dugoročno ulaganje u kriptovalute (36%). 16% ispitanika navelo je izgubljene lozinke i netočne adrese, a 10% ispitanika navelo je nereguliranost od strane institucija kao i greške u softveru. 30% ispitanika navelo je kako ne znaju koji su najveći nedostaci kriptovaluta, a jedan je ispitanik naveo opciju hakiranja kao glavni nedostatak kriptovaluta.

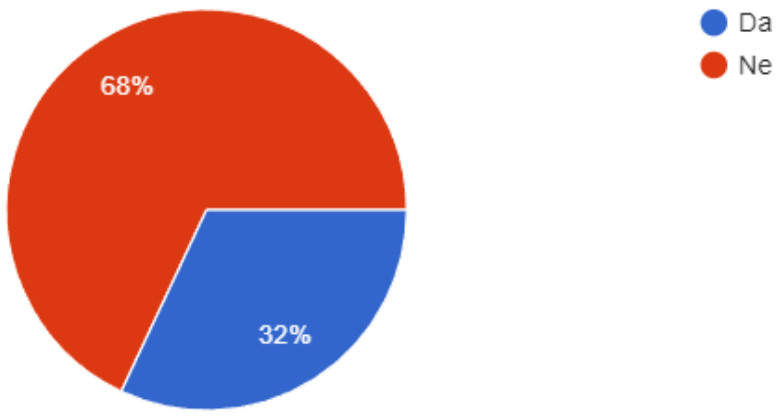
Grafikon 15. Što biste naveli kao najveći nedostatak kriptovaluta?



Izvor: izrada autora

68% ispitanika nikada nije koristilo kriptovalute, a 16 ispitanika ili 32% navelo je kako jesu koristili kriptovalute.

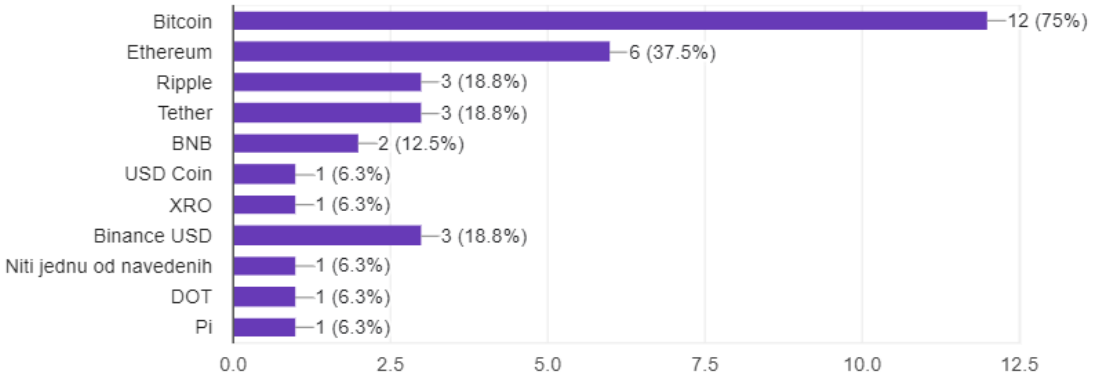
Grafikon 16. Jeste li ikada koristili kriptovalute?



Izvor: izrada autora

Najviše ispitanika koristilo je Bitcoin, njih 12 ili 75%, a zatim Ethereum (37.5%). Kriptovalute Ripple, Tether i Binance USD koristila su 3 ispitanika, a 2 su ispitanika koristila BNB. Kriptovalute USD Coin, XRO, DOT i Pi koristio je po jedan ispitanik, a 3 su ispitanika navela kako nisu koristila niti jednu od navedenih kriptovaluta.

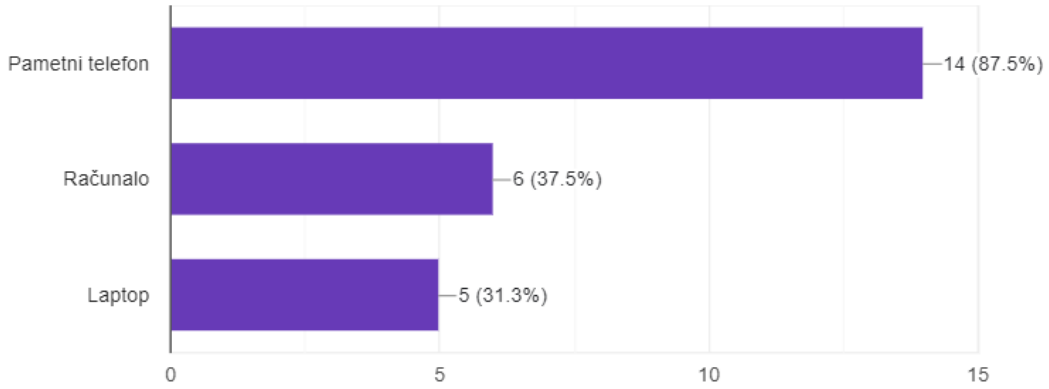
Grafikon 17. Ako jeste, koje ste kriptovalute koristili?



Izvor: izrada autora

Većina ispitanika (87,5%) navelo je kako su kriptovalute koristili na svojem pametnom telefonu, a 37,5% ih je koristilo putem računala. 31,3% ispitanika koristila je kriptovalute putem laptopa.

Grafikon 18. Putem kojeg ste uređaja koristili kriptovalute?



Izvor: izrada autora

Istraživanje je pokazalo kako mnogo ispitanika poznaje temeljne stavke o kriptovalutama, kao što su najpoznatije valute poput Bitcoina i Ethereuma. Ispitanici također većinom imaju nedefinirani stav o kriptovalutama, a također imaju nedefinirani stav o tome jesu li transakcije putem kriptovaluta povjerljive i transparentne. Ispitanici također nemaju određen stav o tome je li plaćanje kriptovalutama sigurnije od korištenja gotovine ili bankovnih kartica. Većina ispitanika je navela kako ne mogu sa sigurnošću odrediti što znači pojam blockchain, a više je ispitanika moglo navesti što znači rudarenje kriptovaluta. Većina je ispitanika navela kako zna što je digitalni novčanik kriptovaluta, a većina je također smatrala kako će vrijednost kriptovaluta rasti u idućih 5 godina. Ispitanici su naveli anonimnost, nereguliranost od strane institucija i brzinu transakcije kao najveće prednosti kriptovaluta. Kao najveće nedostatke kriptovaluta ispitanici su naveli nestabilnost vrijednosti i nestabilno dugoročno ulaganje u kriptovalute. Većina ispitanika nikada nije koristila kriptovalute, a od onih koji su ih koristili najveći je broj koristio Bitcoin ili Ethereum.

Zaključak

Kriptovalute, rudarenje, blockchain, kriptografija te novčanici za kriptovalute su izazvali značajne promjene u financijskom sektoru i društvu općenito. Kriptovalute su pružile inovativan pristup decentraliziranom financijskom sustavu, omogućavajući pojedincima veću autonomiju nad vlastitim sredstvima. Blockchain tehnologija, koja stoji iza kriptovaluta, pokazala se kao ključni element u osiguravanju transparentnosti, sigurnosti i neizmjenjivosti financijskih transakcija. Kriptografija, ključna komponenta kriptovaluta, igra ključnu ulogu u osiguravanju sigurnosti i privatnosti transakcija. Njezina priroda ključna je za očuvanje integriteta sustava kriptovaluta.

Rudarenje je omogućilo stvaranje novih kriptovaluta, a istovremeno je postalo izazovnije zbog povećane kompleksnosti i energetske potrošnje. Ova tema izaziva raspravu o održivosti i ekološkom utjecaju rudarenja na globalnoj razini. Novčanici za kriptovalute su ključni element u upravljanju digitalnim sredstvima, pružajući korisnicima sigurnost i kontrolu nad njihovim sredstvima. Raznolikost novčanika i njihove karakteristike prilagođene korisničkim potrebama stvaraju prostor za inovacije i konkurenciju.

U istraživanju je otkriveno kako velik broj ispitanika ima osnovno razumijevanje kriptovaluta, uključujući poznate valute poput Bitcoina i Ethereuma. Većina ispitanika izražava neodređene stavove prema kriptovalutama, njihovoj povjerljivosti i sigurnosti plaćanja putem kriptovaluta. Raznoliko je mišljenje ispitanika o pojmu blockchaina, dok je veći broj njih mogao preciznije opisati što podrazumijeva rudarenje kriptovaluta. Ispitanici su uglavnom bili upoznati s digitalnim novčanicima kriptovaluta, a većina je izrazila uvjerenje da će vrijednost kriptovaluta rasti u sljedećih pet godina. Ispitanici su pokazali kako su relativno upoznati s tehnologijskim aspektima kriptovaluta što je pozitivno jer znači da postoji obrazovanje u kontekstu kriptovaluta u populaciji hrvatskih građana. Ključno je educirati se o novim tehnološkim promjenama kako bi svatko mogao biti upoznat s novostima te mogao kritički promisliti o njima, te se to odnosi i na svijet kriptovaluta.

U konačnici, unatoč izazovima, kriptovalute i njihovi aspekti predstavljaju fascinantan aspekt suvremene ekonomije. Njihov daljnji razvoj i integracija u društvo zahtijevat će pažljivo balansiranje između inovacija, sigurnosti, regulacije i održivosti kako bi se osiguralo održavanje povjerenja i dugoročna stabilnost ovog dinamičnog segmenta financijskog tržišta.

Literatura

1. 10 popular types of cryptocurrency and how they work. N26. (2023). Dostupno na: https://n26.com/en-eu/blog/types-of-cryptocurrency (3.12.2023.)
2. Arunović, D. (2018). Što je u stvari blockchain i kako radi?. Dostupno na: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (6.3.2023)
3. Barić, J., Grgić, I., & Jurić, I. (2020). Osnove Kriptografije. Acta Mathematica Spalatensia. Series Didactica, 3(3), 37–53. https://doi.org/10.32817/amssd.3.3.4
4. Bunjaku, F., Gjorgieva-Trajkovska, O. i Miteva-Kacarski, E. (2017.). Cryptocurrencies-advantages and disadvantages. Journal of Economics, 2(1).
5. CoinDesk (2024). Bitcoin: About Bitcoin. URL: https://www.coindesk.com/price/bitcoin/?_gl=1*rnn2jt*_up*MQ..*_ga*NTY5NzUzOTguMTcxNzI2Mjk2NQ..*_ga_VM3STRYVN8*MTcxNzI2Mjk2NC4xLjAuMTcxNzI2Mjk2NC4wLjAuMzExMTI5NTA1
6. CoinDesk (2024). Ethereum: About Ethereum. URL: https://www.coindesk.com/price/ethereum/?_gl=1*12fu154*_up*MQ..*_ga*NTY5NzUzOTguMTcxNzI2Mjk2NQ..*_ga_VM3STRYVN8*MTcxNzI2Mjk2NC4xLjEuMTcxNzI2Mjk4MS4wLjAuMzExMTI5NTA1
7. CoinDesk (2024). Tether: About Tether. URL: https://www.coindesk.com/price/tether/?_gl=1*1x0dtir*_up*MQ..*_ga*NjI1NzE0NTMyLjE3MTcyNjQ3MTY.*_ga_VM3STRYVN8*MTcxNzI2NDcxNS4xLjAuMTcxNzI2NDcxNS4wLjAuNzMzNDg1NTE3
8. Cunjak Mataković, I. i Mataković, H. (2018). Kriptovalute - sofisticirani kodovi manipulacije. International Journal of Digital Technology & Economy, 3(1).
9. Dešić, J., & Lenac, K. (2020). Je li blockchain tehnologija budućnost digitalizacije zemljišnih knjiga? Zbornik Pravnog Fakulteta Sveučilišta u Rijeci, 41(2), 609–628. https://doi.org/10.30925/zpfsr.41.2.9
10. Dourado, E., & Brito, J. (2014). Cryptocurrency. The New Palgrave Dictionary of Economics, 1–9. https://doi.org/10.1057/978-1-349-95121-5_2895-1
11. Edwards, J. (2022). Bitcoin's price history. Investopedia. Dostupno na: https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp (3.12.2023.)
12. Ethereum Price (I:ETHUSD). Ethereum Price. (2023). Dostupno na: https://ycharts.com/indicators/ethereum_price#:~:text=Basic%20Info,52.29%25%20from%20one%20year%20ago. (3.12.2023.)

13. Eyal, I. (2021). On Cryptocurrency Wallet Design. Dostupno na: https://eprint.iacr.org/2021/1522.pdf (3.12.2023.)
14. Franciscu, S., Rukgahakotuwa, R., Keppetipola, R., Samarawickrama, Y. i Serasinghe, R. (2022). Cryptography uses Blockchain Technology to Sustainable Cryptocurrency. Cryptography-IE3082-SLIIT.
15. Frankenfield, J. (2023). Digital currency types, characteristics, Pros & Cons, future uses. Investopedia. Dostupno na: https://www.investopedia.com/terms/d/digital-currency.asp (3.12.2023.)
16. Freeman Law (2022). Mining explained: a detailed guide on how cryptocurrency mining works. URL: https://freemanlaw.com/mining-explained-a-detailed-guide-on-how-cryptocurrency-mining-works/
17. Galindo, D. i Ferraioli, F. (2022). Cryptocurrency 201: What Is Ethereum? Wealth Management Global Investment Office. Dostupno na: https://advisor.morganstanley.com/daron.edwards/documents/field/d/da/daron-edwards/Cryptocurrency_201__What_is_Ethereum_.pdf (3.12.2023.)
18. Hardle, W., Harvey, C. i Reule, R. (2018). Understanding Cryptocurrencies. IRTG 1792 Discussion Paper 2018-44.
19. Hayes, A. (2023). Blockchain facts: What is it, how it works, and how it can be used. Investopedia. Dostupno na: https://www.investopedia.com/terms/b/blockchain.asp (3.12.2023.)
20. Heid, A. (2013). Analysis of the Cryptocurrency Marketplace. Dostupno na: https://cryptochainuni.com/wp-content/uploads/HackMiami-Analysis-of-the-Cryptocurrency-Marketplace.pdf (3.12.2023.)
21. How cryptography is used in cryptocurrency. World Crypto Index. (2023). Dostupno na: https://www.worldcryptoindex.com/how-cryptography-is-used-cryptocurrency/ (3.12.2023.)
22. Ji, P. (2023). The Advance of Cryptocurrency Wallet with Digital Signature. Highlights in Science, Engineering and Technology, 39.
23. Jokić, S., Cvetković, A., Adamović, S., Ristić, N., & Spalević, P. (2019). Comparative analysis of cryptocurrency wallets vs traditional wallets. Ekonomika, 65(3), 65–75. https://doi.org/10.5937/ekonomika1903065j
24. Konoth i sur., 2018.
25. Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018). Minesweeper: an in-depth look into drive-by cryptocurrency mining and its defense. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3243734.3243858

26. Lewis, A. (2015). A Gentle Introduction To Bitcoin Mining. Dostupno na: https://assets.ctfassets.net/sdlntm3tthp6/5CbV1gD3NuCCkKauWug6aU/b24fcd5fa2a5cd4a0c32e7dd90838c8a/A-Gentle-Introduction-To-Bitcoin-Mining-WEB.pdf (3.12.2023.)
27. Maheshwari, R. (2023). Popular types of cryptocurrency & how do they work. Forbes. Dostupno na: https://www.forbes.com/advisor/in/investing/cryptocurrency/types-of-cryptocurrency/ (3.12.2023.)
28. Miah, S., Rahman, M., Hossain, S. i Rupai, A. (2019). Introduction to Blockchain. U Ahmed, M. (ur.) Blockchain for Data Analytics. Cambridge: Cambridge Scholars Publishing.
29. Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Dostupno na:https://bitcoin.org/bitcoin.pdf (3.12.2023.)
30. Nian, L. P., & Chuen, D. L. (2015). Introduction to bitcoin. Handbook of Digital Currency, 5–30. https://doi.org/10.1016/b978-0-12-802117-0.00001-1
31. Onwutalobi, A.-C. (2011). Overview of cryptography. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2741776
32. Pawar, T., Shirsat, S., Patil, Y., Sonawane, V., & Birari, D. (2021). A survey on mining cryptocurrencies. Recent Trends in Intensive Computing. https://doi.org/10.3233/apc210212
33. PGP (2002). An Introduction to Cryptography. Dostupno na: https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf (3.12.2023.)
34. Regulated United Europe (2024). History of cryptocurrency. URL: https://rue.ee/blog/cryptocurrency-history/
35. Rosa, G., & Pareschi, R. (2021). Tether: A study on bubble-networks. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.686484
36. Royal, J., & Baker, B. (2023). 12 most popular types of cryptocurrency. Bankrate. Dostupno na: https://www.bankrate.com/investing/types-of-cryptocurrency/ (3.12.2023.)
37. Segendorf, B. (2014). What is Bitcoin? Sveriges Riksbank Economic Review, 2.
38. Sergeenkov, 2022.
39. Sergeenkov, A. (2023). How does ethereum work?. CoinDesk Latest Headlines RSS. Dostupno na: https://www.coindesk.com/learn/how-does-ethereum-work/ (3.12.2023.)
40. Sparkes, M. (2023). What is bitcoin and how does it work?. New Scientist. Dostupno na: https://www.newscientist.com/definition/bitcoin/#:~:text=What%20is%20the%20purpose%20of,used%20just%20like%20traditional%20currencies. (3.12.2023.)

41. Suratkar, S., Shirole, M., i Bhirud, S. (2020). Cryptocurrency wallet: A review. 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP). IEEE.
42. Što su virtualne valute?. HNB. (2018). Dostupno na: https://www.hnb.hr/-/sto-su-virtualne-valute- (3.12.2023.)
43. Tether token. Tether. (2023).Dostupno na: https://tether.to/en/ (3.12.2023.)
44. Wegrzyn, K., & Wang, E. (2023, November 16). Types of blockchain: Public, private, or something in between. Foley & Lardner LLP. Dostupno na: https://www.foley.com/insights/publications/2021/08/types-of-blockchain-public-private-between/ (3.12.2023.)
45. World Bank Group (2018). Cryptocurrencies and Blockchain. Europe and Central Asia Economic Update. Washington: The World Bank.
46. Zakon o elektroničkom novcu, NN 64/18.

Popis slika

Popis grafikona

Popis tablica